

配置 vRealize Automation

2021 年 7 月 21 日

vRealize Automation 7.5

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

**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

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

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

版权所有 © 2015-2021 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

配置 vRealize Automation 6

更新信息 7

1 外部蓝图置备准备 8

- 为 vRealize Automation 管理准备环境 8
 - 准备 NSX 网络与安全配置的对照表 9
 - 用于提供第三方 IPAM 提供程序支持的对照表 13
 - vRealize Automation 容器 配置检查表 15
 - 为 vRealize Automation 准备 vCloud Director 环境 16
 - 为 vRealize Automation 准备 vCloud Air 环境 17
 - 准备 Amazon AWS 环境 17
 - 准备 Red Hat OpenStack 网络与安全功能 23
 - 准备 SCVMM 环境 23
- 配置网络-Azure VPC 连接 24
- 准备进行计算机置备 25
 - 选择一种计算机置备方法进行准备 26
 - 在置备期间运行 Visual Basic 脚本的对照表 27
 - 在置备期间使用 vRealize Automation 客户机代理 28
 - 准备通过克隆进行置备的对照表 35
 - 准备 vCloud Air 和 vCloud Director 置备 46
 - 准备进行 Linux Kickstart 置备 46
 - 准备进行 SCCM 置备 49
 - 准备进行 WIM 置备 50
 - 准备进行虚拟机映像置备 57
 - 准备进行 Amazon 计算机映像置备 57
 - 场景：准备 vSphere 资源进行计算机置备 59
- 准备进行 Software 置备 61
 - 准备使用 Software 置备计算机 62
 - 为克隆计算机和软件组件蓝图准备 vSphere 模板 65
 - 场景：准备导入 Dukes Bank vSphere 示例应用程序蓝图 69

2 为蓝图置备准备租户和资源 73

- 配置租户设置 73
 - 选择身份目录管理配置选项 74
 - 升级用于身份目录管理的外部连接器 127
 - 场景：为高度可用的 vRealize Automation 配置 Active Directory 链接 135

在 vRealize Automation 中为智能卡和第三方身份提供程序的身份验证配置外部连接器	137
创建多域或多林 Active Directory 链接	143
配置组 and 用户角色	145
创建其他租户	151
删除租户	153
为多租户配置安全设置	153
配置自定义品牌	154
用于配置通知的对照表	156
为置备的计算机创建自定义 RDP 文件以支持 RDP 连接	165
场景：为跨区域部署添加数据中心位置	166
配置 vRealize Orchestrator	167
配置资源	171
用于配置 IaaS 资源的对照表	171
配置 XaaS 资源	281
创建和配置容器	292
在默认 vRealize Orchestrator 服务器上安装其他插件	311
使用 Active Directory 策略	312
通知和委派的用户首选项	315
3 向用户提供服务蓝图	316
设计蓝图	316
构建设计库	318
设计计算机蓝图	320
设计 Software 组件	404
设计 XaaS 蓝图和资源操作	414
发布蓝图	467
使用开发人员驱动的蓝图	468
导出和导入蓝图和内容	468
下载和配置提供的独立蓝图	474
在多开发人员环境中创建蓝图和其他 IaaS 内容	474
组合复合蓝图	475
了解嵌套蓝图行为	477
组合蓝图时使用计算机组件和 Software 组件	479
在蓝图组件之间创建属性绑定	480
创建依赖关系和控制置备顺序	481
自定义蓝图请求表单	482
使用 Active Directory 选项创建自定义请求表单	484
自定义表单设计器字段属性	491
在自定义表单设计器中使用 vRealize Orchestrator 操作	494
在自定义表单设计器中使用值选择器或树选择器元素	496
在自定义表单设计器中使用数据网格元素	497

在自定义表单设计器中使用外部验证	500
测试并对失败的置备请求进行故障排除	504
“恢复”操作的工作原理	506
销毁请求失败后强制销毁某个部署	507
对包含 vRealize Orchestrator 工作流的失败部署进行故障排除	508
管理服务目录	509
配置服务目录的对照表	510
创建服务	511
使用目录项和操作	513
创建授权	515
使用批准策略	521
通过使用参数化蓝图请求计算机置备	541
场景：使 CentOS with MySQL 应用程序蓝图在服务目录中可用	542

4 使用目录和管理部署 546

使用目录	546
如何提交目录请求	547
使用部署	549
监控置备请求	550
管理部署的目录项	553
使用收件箱	587

配置 vRealize Automation

《配置 vRealize Automation》提供了有关配置 vRealize Automation 和外部环境以便进行 vRealize Automation 置备和目录管理的信息。

目标读者

本文档提供的信息主要面向负责配置 vRealize Automation 环境的 IT 专业人员，以及负责在现有基础架构中准备 vRealize Automation 置备元素的基础架构管理员。本信息的目标读者为熟悉虚拟机技术和数据中心操作且具有丰富经验的 Windows 和 Linux 系统管理员。

更新信息

下表列出了对本产品版本的《配置 vRealize Automation》所做的更改。

修订版本	描述
XX TBD 202X	更新了 配置衡量指标提供程序 。
2020 年 2 月 14 日	次要更新。
2019 年 10 月 24 日	<ul style="list-style-type: none">■ 增加了对筛选时的意外条目进行故障排除。■ 次要更新。
2019 年 9 月 9 日	<ul style="list-style-type: none">■ 增加了 Microsoft Azure 端点配置。■ 次要更新。
2019 年 7 月 18 日	在 蓝图属性设置 中澄清了传播选项。
2019 年 6 月 14 日	次要更新。
2019 年 5 月 30 日	<ul style="list-style-type: none">■ 添加了一个主题，阐明对即时用户使用通配符匹配的问题。请参见对即时用户使用基于通配符的匹配。■ 更新了配置 Kerberos 身份验证。
2019 年 5 月 7 日	<ul style="list-style-type: none">■ 修复了几个超链接。■ 更新了 准备进行 SCCM 置备，描述了最新添加的配置属性。
2019 年 3 月 1 日	修订了 工作负载放置限制 中的 vSAN 说明。
2019 年 2 月 12 日	<ul style="list-style-type: none">■ 从“身份目录管理”文档中移除了过时的域控制器主题。请参见关于域控制器选择。另外，还更新了配置 OpenLDAP 目录连接，反映了相关更改。■ 对其他“身份目录管理”主题进行了少量文本编辑。
2019 年 1 月 25 日	<ul style="list-style-type: none">■ 更新了对克隆和链接克隆的蓝图进行故障排除。■ 更新了场景：为客户机代理自定义规范和软件组件准备参考机。■ 更新了查看端点源以及运行数据收集。■ 更新了 在多开发人员环境中创建蓝图和其他 IaaS 内容。
2018 年 11 月 13 日	<ul style="list-style-type: none">■ 更新了更新 vRealize Automation 中的现有虚拟机模板。
2018 年 10 月 4 日	<ul style="list-style-type: none">■ 增加了配置基于组的访问策略。■ 更新了使用 vRealize Operations Manager 连续优化。
2018 年 9 月 20 日	初始文档版本。

外部蓝图置备准备

1

为支持目录项置备，您需要在 vRealize Automation 之外创建或准备某些元素。例如，如果要为置备克隆计算机提供目录项，需要在作为克隆源的管理程序上创建模板。

本章讨论了以下主题：

- 为 vRealize Automation 管理准备环境
- 配置网络-Azure VPC 连接
- 准备进行计算机置备
- 准备进行 Software 置备




为 vRealize Automation 管理准备环境

根据工作环境，您可能需要先进行一些配置更改，然后才能使环境受 vRealize Automation 管理或利用某些功能。

表 1-1. 为 vRealize Automation 集成准备环境

环境	准备
 NSX for vSphere 和 NSX-T	如果要利用 NSX for vSphere 或 NSX-T 管理通过 vRealize Automation 置备的虚拟机的网络、安全和负载均衡器功能，请准备 NSX 实例进行集成。请参见 准备 NSX 网络与安全配置的对照表 。
 vCloud Director	安装和配置 vCloud Director 实例，设置 vSphere 和云资源，以及确定或创建 vRealize Automation 可以访问 vCloud Director 环境的合适凭据。请参见 为 vRealize Automation 准备 vCloud Director 环境 。
 vCloud Air	注册 vCloud Air 帐户，设置 vCloud Air 环境，确定或创建 vRealize Automation 可以访问环境的合适凭据。请参见 准备 vCloud Air 和 vCloud Director 置备 。

表 1-1. 为 vRealize Automation 集成准备环境（续）

环境	准备
 Amazon AWS	在 Amazon AWS 环境中准备用于 vRealize Automation 的元素和用户角色，并了解如何将 Amazon AWS 功能映射到 vRealize Automation 功能。请参见 准备 Amazon AWS 环境 。
Microsoft Azure	配置网络连接以使用 VPN 安全加密链路支持 Azure 蓝图上的软件组件。请参见 配置网络-Azure VPC 连接 。
 Red Hat OpenStack	如果要利用 Red Hat OpenStack 管理通过 vRealize Automation 置备的计算机的网络与安全功能，请准备 Red Hat OpenStack 实例进行集成。请参见 准备 Red Hat OpenStack 网络与安全功能 。
 SCVMM	配置存储和网络并了解模板和硬件配置文件的命名限制。请参见 准备 SCVMM 环境 。
外部 IPAM 提供程序	注册外部 IPAM 提供程序软件包或插件，运行配置工作流，然后将 IPAM 解决方案注册为新的 vRealize Automation 端点。请参见 用于提供第三方 IPAM 提供程序支持的对照表 。
所有其他环境	您无需对环境进行更改。通过创建模板、引导环境或计算机映像，您可以开始准备置备计算机。请参见 准备进行计算机置备 。

准备 NSX 网络与安全配置的对照表

在使用 vRealize Automation 中的 NSX 网络与安全选项之前，必须先配置要使用的外部 NSX for vSphere 或 NSX-T 网络与安全环境。

如果您想要使用 XaaS 来扩展 vRealize Automation 和 NSX for vSphere 集成，则必须在 vRealize Orchestrator 中安装 NSX 插件。该插件不支持 NSX-T。

准备在 vRealize Automation 中使用 NSX 网络、安全和负载平衡功能时，使用 NSX Manager 凭据时必须使用 NSX Manager 管理员帐户。

vRealize Automation 支持 NSX for vSphere 和 NSX-T。有关 NSX 应用程序的相关信息，请参见[NSX for vSphere 产品文档](#)或[NSX-T 产品文档](#)。

您在 vRealize Automation 中使用的大部分 NSX 网络和安全设置是外部配置的，并且在计算资源上运行数据收集后可用。

有关可为 vRealize Automation 蓝图配置的 NSX 设置的信息，请参见[配置网络与安全组件设置](#)。

表 1-2. 准备 NSX 网络与安全的对照表

任务	位置	详细信息
❑ 配置 NSX 网络设置，其中包括网关和传输区域设置。	在 NSX 应用程序中配置网络设置。	<p>根据您的 NSX 产品，请参见以下 NSX 文档中的管理主题：</p> <ul style="list-style-type: none"> ■ NSX for vSphere 产品文档 ■ NSX-T 产品文档
❑ 创建 NSX 安全策略、标记和组。	在 NSX 应用程序中配置安全设置。	<p>根据您的 NSX 产品，请参见以下 NSX 文档中的管理主题：</p> <ul style="list-style-type: none"> ■ NSX for vSphere 产品文档 ■ NSX-T 产品文档
❑ 配置 NSX 负载均衡器设置。	在 NSX 应用程序中配置 NSX 负载均衡器设置。	<p>根据您的 NSX 产品，请参见以下 NSX 文档中的管理主题：</p> <ul style="list-style-type: none"> ■ NSX for vSphere 产品文档 ■ NSX-T 产品文档 <p>另请参见 PDF 文档《自定义属性参考》（网址为 docs.vmware.com）中的“网络自定义属性”。</p>
❑ 对于 NSX for vSphere 上的跨 vCenter 部署，请验证计算 NSX 资源管理器具备主要 NSX Manager 角色。	vRealize Automation 置备要求计算 NSX Manager 在计算机所在区域内具备主要 NSX Manager 角色。	<p>请参见置备 NSX for vSphere 通用对象的管理员要求。</p> <p>有关跨 vCenter 部署、通用对象和主要 NSX manager 角色的信息，请参见 NSX for vSphere 产品文档。</p>

在 vRealize Orchestrator 上安装 NSX 插件

安装 NSX 插件要求您下载 vRealize Orchestrator 安装程序文件、使用 vRealize Orchestrator 配置界面上载插件文件并将该插件安装在 vRealize Orchestrator 服务器上。

有关常规插件的更新和故障排除信息，请参见 [vRealize Orchestrator 产品文档](#)。

前提条件

如果您想要使用 XaaS 来扩展 vRealize Automation 和 NSX for vSphere 集成，则必须在 vRealize Orchestrator 中安装 NSX 插件。该插件不支持 NSX-T。

如果您使用的是包含已安装 NSX 插件的嵌入式 vRealize Orchestrator，可以跳过此过程。

- 确认正在运行受支持的 vRealize Orchestrator 实例。
有关设置 vRealize Orchestrator 的信息，请参见 [vRealize Orchestrator 产品文档](#) 中的安装和配置 VMware vRealize Orchestrator。
- 确认您具备有权安装 vRealize Orchestrator 插件并通过 vCenter Single Sign-On 进行身份验证的帐户的凭据。
- 确认您已安装 vRealize Orchestrator 客户端，并且能够使用管理员凭据登录。
- 在 [vRealize Automation 支持列表](#) 中，确认 NSX 插件的正确版本。

步骤

- 1 将插件文件下载到可从 vRealize Orchestrator 服务器访问的位置。
具有适当版本值的插件安装程序文件名格式为 `o11nplugin-nsx-1.n.n.vmoapp`。可以从 [VMware 产品下载站点](#) 获取 NSX for vSphere 的插件安装文件。
- 2 打开浏览器并启动 vRealize Orchestrator 配置界面。
URL 格式的示例为 `https://orchestrator_server.com:8283`。
- 3 单击左窗格中的**插件**，然后滚动到“安装新插件”部分。
- 4 在**插件文件**文本框中，浏览到插件安装程序文件，然后单击**上载并安装**。
该文件必须采用 `.vmoapp` 格式。
- 5 在提示符处，接受“安装插件”窗格中的许可协议。
- 6 在“已启用插件安装状态”部分中，确认已指定正确的 NSX 插件名称。
有关版本信息，请参见 [vRealize Automation 支持列表](#)。
将显示状态插件将在服务器下次启动时安装 (Plug-in will be installed at next server startup)。
- 7 重新启动 vRealize Orchestrator 服务器服务。
- 8 重新启动 vRealize Orchestrator 配置界面。
- 9 单击**插件**，并确认状态已更改为安装完成 (Installation OK)。

10 启动 vRealize Orchestrator Client 应用程序并登录，使用**工作流**选项卡浏览库，转到 NSX 文件夹。

您可以在 NSX 插件提供的工作流之间导航。

后续步骤

在 vRealize Automation 中创建 vRealize Orchestrator 端点，用于运行工作流。请参见[创建 vRealize Orchestrator 端点](#)。

置备 NSX for vSphere 通用对象的管理员要求

使用 NSX 通用对象时，要在跨 vCenter NSX 环境中置备计算机，您必须置备到 NSX 计算资源管理器在其中具有主角色的 vCenter Server。

在跨 vCenter NSX for vSphere 环境中，可以拥有多个 vCenter Server，每个都必须与其自己的 NSX Manager 进行配对。一个 NSX Manager 分配了主 NSX Manager 的角色，其他 NSX Manager 分配了辅助 NSX Manager 的角色。

主 NSX Manager 可以创建通用对象，如通用逻辑交换机。这些对象将同步到辅助 NSX Manager。可以在辅助 NSX Manager 中查看这些对象，但无法在其中编辑这些对象。必须使用主 NSX Manager 来管理通用对象。主 NSX Manager 可用于配置环境中的任何辅助 NSX Manager。

有关跨 vCenter NSX 环境的详细信息，请参见 [NSX for vSphere 产品文档](#)的《NSX 管理指南》中的跨 vCenter 网络和安全概述。

对于与主 NSX Manager 的 NSX 端点关联的 vSphere (vCenter) 端点，vRealize Automation 支持 NSX 本地对象，例如本地逻辑交换机、本地 Edge 网关、本地负载均衡器、安全组和安全标记。它还支持具有通用传输区域的 NAT 一对一和一对多网络、具有通用传输区域和通用分布式逻辑路由器 (Distributed Logical Router, DLR) 的路由网络以及具有任意网络类型的负载均衡器。

vRealize Automation 不支持 NSX 现有和按需通用安全组或标记。

要将本地按需网络置备为主 NSX Manager，请使用特定于 vCenter 的本地传输区域。您可以配置 vRealize Automation 预留，以便对该本地 vCenter Server 的部署使用本地传输区域和虚拟线路。

如果将 vSphere (vCenter) 端点连接到相应的辅助 NSX Manager 端点，则只能置备和使用本地对象。

vRealize Automation 可以将 NSX 通用逻辑交换机用作外部网络。如果存在通用交换机，则部署中的每个计算机都会收集此通用交换机的数据，连接到该交换机或使用该交换机。

- 将按需网络置备到通用传输区域可以创建新的通用逻辑交换机。
- 将按需网络置备到主 NSX Manager 上的通用传输区域会创建通用逻辑交换机。
- 将按需网络置备到辅助 NSX Manager 上的通用传输区域会失败，因为 NSX 无法在辅助 NSX Manager 上创建通用逻辑交换机。

有关 NSX 通用对象的详细信息，请参见 VMware 知识库文章《使用 NSX 对象部署 vRealize Automation 蓝图失败 (2147240)》，网址为 <http://kb.vmware.com/kb/2147240>。

用于提供第三方 IPAM 提供程序支持的对照表

可从支持的第三方 IPAM 提供程序（例如 Infoblox）获取 IP 地址和范围，以用于网络配置文件定义。

在 vRealize Automation 网络配置文件中创建并使用外部 IPAM 提供程序端点之前，必须下载或获取 vRealize Orchestrator IPAM 提供程序插件或软件包，然后在 vRealize Orchestrator 中导入插件或软件包并运行所需的工作流，最后将 IPAM 解决方案注册为 vRealize Automation 端点。

有关使用外部 IPAM 提供程序提供可能 IP 地址范围的配置过程的概览，请参见[使用第三方 IPAM 提供程序置备 vRealize Automation 部署](#)。

表 1-3. 正在准备外部 IPAM 提供程序支持检查表

任务	描述	详细信息
❑ 获取并导入支持的外部 IPAM 提供程序 vRealize Orchestrator 插件。	<p>从 VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) 中下载 IPAM 提供程序插件或软件包（例如 Infoblox IPAM Plug-in for vRealize Orchestrator 插件和支持文档），并将插件或软件包导入 vRealize Orchestrator。</p> <p>如果 VMware Solution Exchange 不包含您需要的 IPAM 提供程序软件包，您可以使用第三方 IPAM 解决方案提供程序 SDK 和支持文档创建您自己的软件包。</p> <p>可从 https://code.vmware.com/sdks 或 https://code.vmware.com/samples 下载 vRealize Automation 特定版本的第三方 IPAM 解决方案提供程序 SDK、支持文档以及适用于 vRealize Orchestrator 和 vRealize Automation 的相关初学者软件包。</p>	请参见 获取第三方 IPAM 提供程序软件包并导入 vRealize Orchestrator 中 。
❑ 运行必需配置工作流，并将外部 IPAM 解决方案注册为 vRealize Automation 端点。	在 vRealize Orchestrator 中运行 vRealize Orchestrator 配置工作流并注册 IPAM 提供程序端点类型。	请参见 运行工作流以在 vRealize Orchestrator 中注册第三方 IPAM 端点类型 。

获取第三方 IPAM 提供程序软件包并导入 vRealize Orchestrator 中

要准备定义和使用第三方 IPAM 提供程序端点，必须先获取第三方 IPAM 提供程序软件包并将其导入 vRealize Orchestrator 中。

可以下载并使用现有的第三方 IP 地址管理提供程序插件，例如 Infoblox IPAM。您还可以使用 VMware 提供的初学者软件包和随附的 SDK 文档创建自己的第三方 IPAM 插件或软件包，以便与其他第三方 IPAM 解决方案提供程序（例如 BlueCat）结合使用。

- 从 marketplace.vmware.com 获取现有的 [Infoblox IPAM Plug-in for vRealize Orchestrator](#) 插件和支持文档。下载内容还包含有关安装和使用该插件的文档。
- 通过获取并使用第三方 IPAM 解决方案提供程序 SDK、支持文档以及适用于 vRealize Orchestrator 和 vRealize Automation 的关联初学者软件包，来创建您自己的第三方 IPAM 解决方案。请参见[vRealize Automation 示例第三方 IPAM 软件包](#)页面 (code.vmware.com/web/sdk)。

在 vRealize Orchestrator 中导入第三方 IPAM 提供程序插件或软件包后，必须运行所需的工作流并在 vRealize Orchestrator 中注册 IPAM 端点类型。

有关导入插件和软件包以及运行 vRealize Orchestrator 工作流的详细信息，请参见《使用 VMware vRealize Orchestrator 客户端》。有关使用 vRealize Orchestrator 插件、软件包和工作流扩展 vRealize Automation 的详细信息，请参见《生命周期可扩展性》。

此步骤顺序使用 Infoblox IPAM 插件作为示例。您的步骤顺序可能因 vRealize Automation 或插件版本而异。

前提条件

- 从 marketplace.vmware.com 下载软件包或插件。
- 以管理员特权登录到 vRealize Orchestrator，以便导入、配置和注册 vRealize Orchestrator 插件或软件包。

步骤

- 1 打开 marketplace.vmware.com 网站。
- 2 找到并下载插件或软件包。

例如，在 vRealize Orchestrator 和 vRealize Automation 7.1 及更高版本中导入支持 Infoblox 第三方 IPAM 端点的 Infoblox 插件。

- a 在**发布者**类别中，选择 **Infoblox**，然后单击**应用**。
- b 选择 [Infoblox Plug-in for vRealize Orchestrator](#)。
- c 单击**技术规格**，然后查看必备条件。
- d 单击**试用**了解更多信息并接收包含下载链接的电子邮件。
- e 下载电子邮件说明中指定的 zip 文件。

版本 4.0 及更高版本的插件支持 vRealize Automation 7.1 及更高版本。该 zip 文件还包含插件的相关文档。

- 3 在 vRealize Orchestrator 中，单击**管理员**选项卡，然后单击**导入软件包**。
- 4 选择要导入的软件包。
- 5 选择所有工作流和项目，然后单击**导入选定的元素**。

后续步骤

运行工作流以在 vRealize Orchestrator 中注册第三方 IPAM 端点类型。

运行工作流以在 vRealize Orchestrator 中注册第三方 IPAM 端点类型

在 vRealize Orchestrator 中运行注册工作流，以支持 vRealize Automation 使用第三方 IPAM 提供程序并注册 IPAM 端点类型，以便在 vRealize Automation 中使用。

前提条件

- 获取[第三方 IPAM 提供程序软件包](#)并导入 **vRealize Orchestrator** 中
- 确认以有权运行注册工作流的用户身份登录到 **vRealize Orchestrator**。
- 准备在注册工作流提示输入凭据时输入 **vRealize Automation** 管理员凭据。在 **vRealize Orchestrator** 中注册 IPAM 端点类型时，系统会提示您输入 **vRealize Automation** 管理员凭据。

步骤

- 1 在 **vRealize Orchestrator** 中，单击**设计**选项卡，选择**管理员 > 库**，再选择 **IPAM 服务软件包 SDK**。

每个 IPAM 提供程序软件包的名称都是唯一的，并且包含唯一的工作流。每个提供程序提供各自的注册工作流。虽然不同提供程序软件包中的工作流名称可能相似，但工作流在 **vRealize Orchestrator** 中的位置不相同，并且是特定于提供程序的。

- 2 在此示例中，运行 **Register IPAM Endpoint** 注册工作流并指定 IPAM Infoblox 端点类型。

- 3 提示输入 **vRealize Automation** 凭据时，输入 **vRealize Automation** 管理员凭据，例如架构管理员凭据。

您必须使用 **vRealize Automation** 系统管理员凭据提供注册工作流。即使非系统管理员用户登录到 **vRealize Orchestrator** 客户端，如果向工作流提供了 **vRealize Automation** 系统管理员凭据，也会成功注册。

结果

在此示例中，软件包在 **vRealize Automation** 端点服务中将 Infoblox 注册为新的 IPAM 端点类型，在 **vRealize Automation** 中创建或编辑端点时可以使用该端点类型。

注 在 **vRealize Orchestrator** 控制中心中重新启动 **vRealize Orchestrator** 服务器之后，如果 Infoblox IPAM 连接从 **vRealize Orchestrator** **清单**中消失。要解决此问题，请通过 **vRO admin > 库 > Infoblox > vRA > 助手**菜单序列运行 **Create IPAM Connection** 工作流。然后可以单击 **vRealize Orchestrator** **清单**选项卡，选择 **Infoblox IPAM**，并刷新页面以显示 Infoblox IPAM 连接。

后续步骤

现在，您可以创建 IPAM Infoblox 类型的端点，或者也可以创建适用于刚刚在 **vRealize Automation** 中注册的任何第三方软件包或插件的端点。请参见[创建第三方 IPAM 提供程序端点](#)。

vRealize Automation 容器 配置检查表

要开始使用 容器，您必须将该功能配置为支持 **vRealize Automation** 用户角色。

在 容器 中配置容器定义后，您可以在蓝图中添加和配置容器组件。

表 1-4. vRealize Automation 容器 配置检查表

任务	详细信息
分配容器管理员和容器架构师角色。	请参见《基础和概念》中的“容器”角色信息。
在 vRealize Automation 的 容器 选项卡中定义容器定义。	请参见《配置 vRealize Automation》。
在 vRealize Automation 的 设计 选项卡中向蓝图添加容器组件和容器网络组件。	请参见《配置 vRealize Automation》。

使用 vRealize Automation 设备配置 容器

可以在 vRealize AutomationvRealize Automation 设备（**vRA 设置 > Xenon**）中访问 Xenon 服务信息。

它包含有关 Xenon 主机虚拟机、侦听端口和服务状态的信息。其中还显示有关 Xenon 群集节点的信息。

您可以在 vRealize Automation 设备中使用以下 CLI 命令管理 Xenon Linux 服务。

命令	描述
service xenon-service status	将服务状态显示为正在运行或已停止。
service xenon-service start	启动服务。
service xenon-service stop	停止服务。
service xenon-service restart	重新启动服务。
service xenon-service get_host	显示正在运行服务的主机名。
service xenon-service get_port	显示服务端口。
service xenon-service status_cluster	以 JSON 格式显示有关所有群集节点的信息。
service xenon-service reset	删除 Xenon 用于保留所有配置文件的目录并重新启动服务。

群集容器

您可以结合使用 Xenon 服务与 vRealize Automation 容器 将节点加入群集。如果节点已加入群集，Xenon 服务会在启动时自动连接其他节点。

您可以在 vRealize Automation 设备中的 **Xenon** 选项卡上或通过 CLI 中运行以下命令来监控群集状态：

```
service xenon-service status_cluster
```

Xenon 对基于仲裁数的群集起作用。仲裁数的计算公式为 $(\text{number of nodes} / 2) + 1$ 。

为 vRealize Automation 准备 vCloud Director 环境

集成 vCloud Director 与 vRealize Automation 之前，必须安装和配置 vCloud Director 实例，设置 vSphere 和云资源，以及确定或创建 vRealize Automation 可以访问 vCloud Director 环境的合适凭证。

配置环境

配置 vSphere 资源和云资源，包括虚拟数据中心和网络。有关详细信息，请参见 vCloud Director 文档。

集成所需的凭据

创建或确定 vRealize Automation IaaS 管理员可用来将 vCloud Director 环境作为端点置于 vRealize Automation 管理之下的组织管理员凭据或系统管理员凭据。

用户角色注意事项

组织中的 vCloud Director 用户角色不需要与 vRealize Automation 业务组中角色一一对应。如果用户帐户不存在于 vCloud Director 中，vCloud Director 将查看关联的 LDAP 或 Active Directory；如果用户存在于身份存储中，它将创建用户帐户。如果无法创建用户帐户，则将记录警告，但置备过程不会失败。稍后，已置备的计算机将分配给配置 vCloud Director 端点所使用的帐户。

有关 vCloud Director 用户管理的相关信息，请参见 vCloud Director 文档。

为 vRealize Automation 准备 vCloud Air 环境

集成 vCloud Air 与 vRealize Automation 之前，必须注册 vCloud Air 帐户，设置 vCloud Air 环境，确定或创建 vRealize Automation 可以访问环境的合适凭据。

配置环境

按照 vCloud Air 文档中的说明，配置环境。

集成所需的凭据

创建或确定 vRealize Automation IaaS 管理员可用来将 vCloud Air 环境作为端点置于 vRealize Automation 管理之下的虚拟基础架构管理员凭据或帐户管理员凭据。

用户角色注意事项

组织中的 vCloud Air 用户角色不需要与 vRealize Automation 业务组中角色一一对应。有关 vCloud Air 用户管理的相关信息，请参见 vCloud Air 文档。

准备 Amazon AWS 环境

在 Amazon AWS 环境中准备元素和用户角色，准备 Amazon AWS 与客户机代理和 Software 引导程序代理进行通信，并了解如何将 Amazon AWS 功能映射到 vRealize Automation 功能。

vRealize Automation 所需的 Amazon AWS 用户角色和凭据

必须在 Amazon AWS 中配置具有 vRealize Automation 管理环境所需权限的凭据。

vRealize Automation 需要端点凭据的访问密钥且不支持用户名和密码。

- Amazon Web Services 中的角色和权限授权

尽管 AWS 中的“超级用户”角色为 AWS Directory Service 用户或组提供 AWS 服务和资源的完全访问权限，但它不是必需的。此外，还支持具有更低特权的用户角色。满足 vRealize Automation 功能需求的 AWS 安全策略如下：

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

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

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

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

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

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

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

      "ec2:CreateTags",
      "ec2:AssociateAddress",
      "ec2:ReportInstanceStatus",
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:ModifyInstanceAttribute",
```

```

        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

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

```

■ Amazon Web Services 中的身份验证凭据

要管理 Amazon Identity and Access Management (IAM) 用户和组，您必须配置有 AWS “完全访问管理员”凭据。

在 vRA 中创建 AWS 端点时，系统会提示您输入密钥和私有密钥。要获取创建 Amazon 端点所需的访问密钥，管理员必须向具有 AWS “完全访问管理员”凭据的用户请求密钥，或者另外配置 AWS “完全访问管理员”策略。请参见[创建 Amazon 端点](#)。

有关启用策略和角色的信息，请参见 Amazon Web Services 产品文档的 AWS Identity and Access Management (IAM) 部分。

允许 Amazon AWS 与 Software 引导程序代理和客户机代理通信

如果打算置备包含 Software 的应用程序蓝图，或者如果希望能够通过使用客户机代理进一步自定义已置备的计算机，则必须在置备计算机的 Amazon AWS 环境与代理下载软件包和接收指令的 vRealize Automation 环境之间启用连接。

使用 vRealize Automation 置备具有 vRealize Automation 客户机代理和 Software 引导程序代理的 Amazon AWS 计算机时，必须设置从网络到 Amazon VPC 连接，使已置备的计算机能够与 vRealize Automation 恢复通信以自定义计算机。

有关 Amazon AWS VPC 连接选项的详细信息，请参见 Amazon AWS 文档。

使用可选的 Amazon 功能

vRealize Automation 支持多种 Amazon 功能，其中包括 Amazon Virtual Private Cloud、弹性负载平衡器、弹性 IP 地址和弹性块存储。

使用 Amazon 安全组

创建 Amazon 预留时，请至少指定一个安全组。每个可用区域至少需要一个指定的安全组。

安全组充当控制计算机访问的防火墙。每个区域至少包括默认安全组。管理员可以使用 Amazon Web Services Management Console 创建其他安全组，配置 Microsoft Remote Desktop Protocol 或 SSH 的端口，并设置 Amazon VPN 的虚拟专用网络。

在蓝图中创建 Amazon 预留或配置计算机组件时，您可以从指定的 Amazon 帐户区域可用的安全组列表中进行选择。安全组是在数据收集期间导入的。

有关在 Amazon Web Services 中创建和使用安全组的信息，请参见 Amazon 文档。

了解 Amazon Web Service 区域

每个 Amazon Web Services 帐户均使用一个云端点表示。在 vRealize Automation 中创建 Amazon Elastic Cloud Computing 端点时，区域将收集为计算资源。IaaS 管理员选择业务组的计算资源后，系统将自动执行清单和状态数据收集。

清单数据收集每天自动运行一次，可收集计算资源中所含内容的相关数据，例如：

- 弹性 IP 地址
- 弹性负载均衡器
- 弹性块存储卷

默认情况下，状态数据收集每隔 15 分钟自动运行一次。它收集由 vRealize Automation 创建的受管实例的状态信息。以下是状态数据的示例：

- Windows 密码
- 负载均衡器中的计算机状态
- 弹性 IP 地址

架构管理员可以启动清单和状态数据收集，并停用或更改清单和状态数据收集的频率。

使用 Amazon 虚拟私有云

Amazon Virtual Private Cloud 允许您在 Amazon Web Services 的私有云部分中置备 Amazon 计算机实例。

Amazon Web Services 用户可以使用 Amazon VPC 根据规范设计虚拟网络拓扑。您可以在 vRealize Automation 中分配 Amazon VPC。但是，vRealize Automation 不跟踪使用 Amazon VPC 的成本。

使用 Amazon VPC 进行置备时，vRealize Automation 要求有一个 VPC 子网，Amazon 可从此子网中获取主 IP 地址。此地址在该实例终止之前始终为静态地址。此外，您还可以使用弹性 IP 池将弹性 IP 地址附加到 vRealize Automation 中的实例。这样一来，用户在 Amazon Web Services 中继续置备和拆卸实例时，均可保持相同的 IP。

使用 AWS Management Console 可创建以下元素：

- Amazon VPC，其中包括 Internet 网关、路由表、安全组和子网以及可用的 IP 地址。
- Amazon Virtual Private Network（如果用户需要登录到 AWS Management Console 外部的 Amazon 计算机实例）。

使用 Amazon VPC 时，vRealize Automation 用户可执行下列任务：

- 架构管理员可以将 Amazon VPC 分配给云预留。请参见 [创建 Amazon EC2 预留](#)。
- 计算机所有者可以将 Amazon 计算机实例分配给 Amazon VPC。

有关创建 Amazon VPC 的详细信息，请参见 Amazon Web Services 文档。

使用 Amazon Web Services 的弹性负载均衡器

弹性负载均衡器将入站应用程序流量分布到多个 Amazon Web Services 实例。Amazon 负载均衡可改进容错和性能。

Amazon 为使用 Amazon EC2 蓝图置备的计算机提供弹性负载均衡功能。

弹性负载均衡器在 Amazon Web Services、Amazon Virtual Private Network 和置备位置中均必须可用。例如，如果 us-east1c 中提供负载均衡器且计算机位置为 us-east1b，则该计算机无法使用可用的负载均衡器。

vRealize Automation 不会创建、管理或监控弹性负载均衡器。

有关使用 Amazon Web Services Management Console 创建 Amazon 弹性负载均衡器的信息，请参见 Amazon Web Services 文档。

使用 Amazon Web Services 的弹性 IP 地址

通过使用弹性 IP 地址，可以快速将故障切换到动态 Amazon Web Services 云环境中的其他计算机。在 vRealize Automation 中，弹性 IP 地址适用于对该区域具有相应权限的所有业务组。

管理员可以使用 AWS Management Console 将弹性 IP 地址分配给 Amazon Web Services 帐户。任何给定区域中都有两组弹性 IP 地址，一组分配给非 Amazon VPC 实例，另一组分配给 Amazon VPC。如果仅分配非 Amazon VPC 区域中的地址，则这些地址在 Amazon VPC 中不可用。反之亦然。如果仅分配 Amazon VPC 中的地址，则这些地址在非 Amazon VPC 区域中不可用。

弹性 IP 地址与 Amazon Web Services 帐户关联，而不是与特定计算机关联。每次只有一台计算机能够使用该地址。除非选择释放，否则该地址始终与 Amazon Web Services 帐户关联。您可发释放该地址，以便将其映射到特定的计算机实例。

IaaS 架构师可以将自定义属性添加到蓝图，以便在置备期间为计算机分配弹性 IP 地址。计算机所有者和管理员均可查看分配给计算机的弹性 IP 地址，计算机所有者或有权编辑计算机的管理员可以在置备后分配弹性 IP 地址。但是，如果该地址已与某个计算机实例关联，且此实例属于 Amazon Virtual Private Cloud 部署的一部分，则 Amazon 不会分配该地址。

有关创建和使用 Amazon 弹性 IP 地址的详细信息，请参见 Amazon Web Services 文档。

对 Amazon Web Services 使用弹性块存储

Amazon 弹性块存储提供了许多与 Amazon 计算机实例和 Amazon Virtual Private Cloud 配合使用的弹性块存储卷。该存储卷的生命周期比 Amazon Web Services 云环境中与其关联的 Amazon 计算机实例要长。

将 Amazon 弹性块存储卷与 vRealize Automation 结合使用时，存在以下局限：

- 置备计算机实例时，无法附加现有的弹性块存储卷。但是，如果创建新卷并一次请求多台计算机，则该卷将会创建并附加到每个实例。例如，如果创建一个名为 volume_1 的卷并请求三台计算机，则系统将为每台计算机创建一个卷。系统将创建三个名为 volume_1 的卷并将其附加到每台计算机。每个卷均具有唯一的卷 ID。它们大小相同并位于相同的位置。
- 该卷必须与连接的计算机采用相同的操作系统，并位于相同的位置。

- vRealize Automation 不管理主弹性块存储卷支持的实例。

有关 Amazon 弹性块存储的详细信息以及如何通过使用 Amazon Web Services Management Console 启用该存储的详细信息，请参见 Amazon Web Services 文档。

为概念证明环境配置从网络到 Amazon VPC 的连接

作为负责设置环境以评估 vRealize Automation 的 IT 专业人员，您需要临时配置从网络到 Amazon VPC 的连接来支持 vRealize Automation Software 功能。

仅当您希望使用客户机代理自定义置备的计算机，或者希望将 Software 组件包含在蓝图中时，才需要从网络到 Amazon VPC 的连接。对于生产环境，您将通过 Amazon Web Services 正式配置此连接，但由于您是在概念证明环境中进行操作，因此需要创建临时的网络到 Amazon VPC 的连接。建立 SSH 通道，然后将 vRealize Automation 中的 Amazonto 预留配置为通过通道进行路由。

前提条件

- 创建名为 TunnelGroup 的 Amazon AWS 安全组，并将其配置为允许访问端口 22。
- 在 Amazon AWS TunnelGroup 安全组中创建或标识 CentOS 计算机，并注意以下配置：
 - 管理用户凭据，例如 *root*。
 - 公用 IP 地址。
 - 专用 IP 地址。
- 在与 vRealize Automation 安装相同的本地网络上创建或标识 CentOS 计算机。
- 在这两台通道计算机上安装 OpenSSH SSHD 服务器。

步骤

- 1 以 root 用户身份或类似身份登录到 Amazon AWS 通道计算机。
- 2 停用 iptables。

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

- 3 编辑 `/etc/ssh/sshd_config` 以启用 `AllowTCPForwarding` 和 `GatewayPorts`。
- 4 重新启动服务。

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

- 5 以 root 用户身份登录到与 vRealize Automation 安装相同的本地网络上的 CentOS 计算机。
- 6 调用从本地网络计算机到 Amazon AWS 通道计算机的 SSH 通道。

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
```

```
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Amazon tunnel machine@Public IP Address of Amazon tunnel machine
```

您已将端口转发配置为允许 Amazon AWS 通道计算机访问 vRealize Automation 资源，但 SSH 通道并不工作，直到您将 Amazon 预留配置为通过通道进行路由。

后续步骤

- 1 在 Windows 或 Linux 参考机上安装软件引导程序代理和客户机代理，创建可供 IaaS 架构师用来创建蓝图的 Amazon 计算机映像。请参见[准备进行 Software 置备](#)。
- 2 将 vRealize Automation 中的 Amazon 预留配置为通过 SSH 通道进行路由。请参见[场景：为概念证明环境创建 Amazon 预留](#)。

准备 Red Hat OpenStack 网络与安全功能

vRealize Automation 支持多种 OpenStack 功能，其中包括安全组和浮点 IP 地址。了解这些功能如何与 vRealize Automation 配合使用并在环境中进行配置。

使用 OpenStack 安全组

安全组允许您指定用于控制通过特定端口的网络流量的规则。

您可以在请求计算机时在预留中指定安全组，也可以在设计画布中指定现有的或按需 NSX 安全组。

安全组是在数据收集期间导入的。

每个可用区域至少需要一个指定的安全组。创建预留时，将显示该区域中提供给您的可用安全组。每个区域至少包括默认安全组。

其他安全组必须在源资源中进行管理。有关为各种计算机管理安全组的详细信息，请参见 OpenStack 文档。

将浮点 IP 地址与 OpenStack 配合使用

您可以将浮点 IP 地址分配给 OpenStack 中正在运行的虚拟实例。

要启用浮点 IP 地址的分配，您必须配置 IP 转发并在 Red Hat OpenStack 中创建浮点 IP 池。有关详细信息，请参见 Red Hat OpenStack 文档。

您必须将“关联浮点 IP”和“解除浮点 IP 关联”操作授权给计算机所有者。随后，授权用户可以通过从浮点 IP 地址池中选择可用的地址，从连接到计算机的外部网络将浮点 IP 地址与已置备的计算机关联。浮点 IP 地址与计算机关联之后，vRealize Automation 用户可以选择“解除浮点 IP 关联”选项，从而查看当前分配的浮点 IP 地址并解除地址与计算机的关联。

准备 SCVMM 环境

在开始 vRealize Automation 计算机置备中要使用的 SCVMM 模板和硬件配置文件之前，您必须了解模板和硬件配置文件名称的命名限制，并配置 SCVMM 网络和存储设备。

有关准备环境的相关信息，请参见安装 vRealize Automation 中的 SCVMM 要求信息。

有关计算机置备的相关信息，请参见[创建 Hyper-V \(SCVMM\) 端点](#)。

vRealize Automation 不支持使用 SCVMM 私有云配置的部署环境。vRealize Automation 当前无法根据 SCVMM 私有云执行收集、分配或置备操作。

模板和硬件配置文件命名

由于 SCVMM 和 vRealize Automation 对模板和硬件配置文件使用命名约定，因此，请勿将模板或硬件配置文件名称以单词 temporary 或 profile 开头。例如，系统在数据收集过程中会忽略以下术语：

- TemporaryTemplate
- Temporary Template
- TemporaryProfile
- Temporary Profile
- Profile

SCVMM 群集所需的网络配置

SCVMM 群集仅向 vRealize Automation 公开虚拟网络，因此虚拟网络与逻辑网络之间必须具有一对一的关系。使用 SCVMM 控制台将每个逻辑网络映射到虚拟网络，并将 SCVMM 群集配置为通过虚拟网络访问计算机。

SCVMM 群集所需的存储配置

在 SCVMM Hyper-V 群集上，vRealize Automation 仅在共享卷中收集数据并进行置备。使用 SCVMM 控制台将群集配置为使用共享资源卷进行存储。

独立 SCVMM 主机所需的存储配置

对于独立 SCVMM 主机，vRealize Automation 在默认虚拟机路径上收集数据并进行置备。使用 SCVMM 控制台配置独立主机的默认虚拟机路径。

配置网络-Azure VPC 连接

如果需要在 Azure 蓝图中使用软件组件，则必须配置网络-Azure 连接。

前提条件

- 创建名为 TunnelGroup 的 Azure 安全组，并将其配置为允许访问端口 22。
- 在 Azure TunnelGroup 安全组中创建或标识计算机（如 CentOS 计算机），并注意以下配置：
 - 管理用户凭据，例如 *root*。
 - 公用 IP 地址。
 - 专用 IP 地址。
- 在与 vRealize Automation 安装相同的本地网络上创建或标识 CentOS 计算机。
- 在这两台通道计算机上安装 OpenSSH SSHD 服务器。

步骤

1 以 root 用户身份或类似身份登录到 Azure 通道计算机。

2 停用 iptables。

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

3 编辑 /etc/ssh/sshd_config 以启用 AllowTCPForwarding 和 GatewayPorts。

4 重新启动服务。

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

5 以 root 用户身份登录到与 vRealize Automation 安装相同的本地网络上的 CentOS 计算机。

6 调用从本地网络计算机到 Azure 通道计算机的 SSH 通道。

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Azure tunnel machine@Public IP Address of Azure tunnel machine
```

您已将端口转发配置为允许 Azure 通道计算机访问 vRealize Automation 资源，但 SSH 通道并不工作，直到您将 Azure 预留配置为通过通道进行路由。

后续步骤

- 1 在 Windows 或 Linux 参考机上安装软件引导程序代理和客户机代理，创建可供 IaaS 架构师用来创建蓝图的 Azure 计算机映像。请参见[准备进行 Software 置备](#)。
- 2 将 vRealize Automation 中的 Azure 预留配置为通过 SSH 通道进行路由。请参见[创建 Microsoft Azure 预留](#)。

准备进行计算机置备

根据环境和计算机置备方法，可能需要配置 vRealize Automation 之外的元素。

例如，可能需要配置计算机模板或计算机映像。

可能还需要配置 NSX 设置或运行 vRealize Orchestrator 工作流。

有关准备置备计算机时指定端口的相关信息，请参见 [vRealize Automation 产品文档](#) 中的《参考架构》PDF。

选择一种计算机置备方法进行准备

对于大多数计算机置备方法，您必须在 vRealize Automation 外部准备某些元素。

表 1-5. 选择一种计算机置备方法进行准备

方案	支持的端点	代理支持	置备方法	置备前准备
对 vRealize Automation 进行配置，使其在计算机置备前后将自定义 Visual Basic 脚本作为计算机生命周期中的额外步骤运行。例如，您可以在置备前使用置备前脚本生成证书或安全令牌，并在置备后通过置备后脚本使用这些证书和令牌。	您可以使用支持的任何端点运行 Visual Basic 脚本，但 Amazon AWS 除外。	取决于所选的置备方法。	支持在任何置备方法中作为额外步骤运行，但不能将 Visual Basic 脚本与 Amazon AWS 计算机结合使用。	在置备期间运行 Visual Basic 脚本的对照表
置备可自动对中间件和应用程序部署组件（例如，Oracle、MySQL、WAR 和数据库架构）进行安装、配置和生命周期管理的应用程序蓝图。	<ul style="list-style-type: none"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon AWS 	<ul style="list-style-type: none"> ■ （必需）客户机代理 ■ （必需）软件引导程序代理和客户机代理 	<ul style="list-style-type: none"> ■ 克隆 ■ 克隆（对于 vCloud Air 或 vCloud Director） ■ 链接克隆 ■ Amazon 计算机映像 	如果希望能够使用蓝图中的 Software 组件，请准备支持客户机代理和 Software 引导程序代理的置备方法。有关准备 Software 的详细信息，请参见 准备进行 Software 置备 。
置备后通过使用客户机代理进一步自定义计算机。	所有虚拟端点和 Amazon AWS。	<ul style="list-style-type: none"> ■ （必需）客户机代理 ■ （可选）软件引导程序代理和客户机代理 	除虚拟机映像以外的所有置备方法都支持。	如果能够在置备后自定义计算机，请选择支持客户机代理的置备方法。
置备没有客户机操作系统的计算机。您可以在置备后安装操作系统。	所有虚拟机端点。	不受支持	基本	无需在 vRealize Automation 外部做置备前准备。
置备节省空间的虚拟机副本，称为“链接克隆”。链接克隆以虚拟机的快照为基础，并使用增量磁盘链来跟踪与父虚拟机的差异。	vSphere	<ul style="list-style-type: none"> ■ （可选）客户机代理 ■ （可选）软件引导程序代理和客户机代理 	链接克隆	必须已经有 vSphere 虚拟机。如果要支持 Software，必须在要克隆的计算机上安装客户机代理和软件引导程序代理。在置备链接克隆虚拟机之前，应关闭蓝图中标识的虚拟机快照。
使用 Net App FlexClone 技术置备节省空间的虚拟机副本。	vSphere	（可选）客户机代理	NetApp FlexClone	请参见 准备通过克隆进行置备的对照表 。
通过从现有 Windows 或 Linux 计算机（称为“参考机”）创建的模板对象和自定义对象中克隆，以此置备计算机。	<ul style="list-style-type: none"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ （可选）客户机代理 ■ （仅对 vSphere 可选）软件引导程序代理和客户机代理 	克隆	请参见 准备通过克隆进行置备的对照表 。如果要支持 Software，必须在要克隆的 vSphere 计算机上安装客户机代理和软件引导程序代理。

表 1-5. 选择一种计算机置备方法进行准备（续）

方案	支持的端点	代理支持	置备方法	置备前准备
通过从模板和自定义对象中克隆，置备 vCloud Air 或 vCloud Director 计算机。	<ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ （可选）客户机代理 ■ （可选）软件引导程序代理和客户机代理 	vCloud Air 或 vCloud Director 克隆	<p>请参见准备 vCloud Air 和 vCloud Director 置备。</p> <p>如果要支持 Software，请创建一个包含客户机代理和软件引导程序代理的模板。对于 vCloud Air，请在 vRealize Automation 环境和 vCloud Air 环境之间配置网络连接。</p>
通过从 ISO 映像引导、使用 kickstart 或 autoYaSt 配置文件和 Linux 分发映像以便在计算机上安装操作系统，从而置备计算机。	<ul style="list-style-type: none"> ■ 所有虚拟端点 ■ Red Hat OpenStack 	在准备阶段安装客户机代理。	Linux Kickstart	准备进行 Linux Kickstart 置备
置备计算机并将控制权传递给 SCCM 任务序列，以便从 ISO 映像引导、部署 Windows 操作系统并安装 vRealize Automation 客户机代理。	所有虚拟机端点。	在准备阶段安装客户机代理。	SCCM	准备进行 SCCM 置备
通过引导到 WinPE 环境并使用现有 Windows 参考机的 Windows Imaging File Format (WIM) 映像安装操作系统，以此置备计算机。	<ul style="list-style-type: none"> ■ 所有虚拟端点 ■ Red Hat OpenStack 	需要客户机代理。创建 WinPE 映像时，必须手动插入客户机代理。	WIM	准备进行 WIM 置备
从虚拟机映像启动实例。	Red Hat OpenStack	不受支持	虚拟机映像	请参见 准备进行虚拟机映像置备 。
从 Amazon 计算机映像启动实例。	Amazon AWS	<ul style="list-style-type: none"> ■ （可选）客户机代理 ■ （可选）软件引导程序代理和客户机代理 	Amazon 计算机映像	<p>将 Amazon 计算机映像和实例类型与 Amazon AWS 帐户关联。</p> <p>如果要支持 Software，请创建包含客户机代理和软件引导程序代理的 Amazon 计算机映像，并在 Amazon AWS 和 vRealize Automation 环境之间配置从网络到 VPC 的连接。</p>

在置备期间运行 Visual Basic 脚本的对照表

您可以对 vRealize Automation 进行配置，使其在计算机置备前后将自定义 Visual Basic 脚本作为计算机生命周期中的额外步骤运行。例如，您可以在置备前使用置备前脚本生成证书或安全令牌，并在置备后通过置备后脚本使用这些证书和令牌。您可以通过任何置备方法运行 Visual Basic 脚本，但不能将 Visual Basic 脚本与 Amazon AWS 计算机结合使用。

表 1-6. 在置备期间运行 Visual Basic 脚本的对照表

任务	位置	详细信息
❑ 为 Visual Basic 脚本安装并配置 EPI 代理。	通常为 Manager Service 主机	请参见安装 vRealize Automation。
❑ 创建 Visual Basic 脚本。	安装有 EPI 代理的计算机。	<p>vRealize Automation 将示例 Visual Basic 脚本 <code>PrePostProvisioningExample.vbs</code> 包括在 EPI 代理安装目录的 <code>Scripts</code> 子目录中。此脚本包含标头（用于将所有参数加载到字典中）、正文（可将函数包含在其中）和标尾（用于将更新的自定义属性返回到 vRealize Automation）。</p> <p>执行 Visual Basic 脚本时，EPI 代理将所有计算机自定义属性作为参数传递给该脚本。要将更新的属性值返回到 vRealize Automation，请将这些属性放入字典并调用由 vRealize Automation 提供的函数。</p>
❑ 收集将脚本包括在蓝图中所需的信息。	<p>捕获信息并传输给基础架构架构师</p> <hr/> <p>注 架构管理员可以使用属性集 <code>ExternalPreProvisioningVbScript</code> 和 <code>ExternalPostProvisioningVbScript</code> 创建属性组，提供这些所需的信息。这样蓝图架构师可以更轻松地将这些信息正确包含在蓝图中。</p> <hr/>	<ul style="list-style-type: none"> ■ Visual Basic 脚本的完整路径，其中包括文件名和扩展名。例如，<code>%System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</code>。 ■ 要在置备前运行脚本，请指示基础架构架构师输入脚本的完整路径作为自定义属性 <code>ExternalPreProvisioningVbScript</code> 的值。要在置备后运行脚本，他们需要使用自定义属性 <code>ExternalPostProvisioningVbScript</code>。

在置备期间使用 vRealize Automation 客户机代理

部署后，您可以在参考机上安装客户机代理，用于进一步自定义计算机。您既可以使用预留的客户机代理自定义属性执行添加和格式化磁盘等基本自定义操作，也可以为要在已置备计算机的客户机操作系统中运行的客户机代理创建自己的自定义脚本。

完成部署并运行自定义规范（如果已提供）后，客户机代理将创建一个包含已部署计算机的所有自定义属性的 XML 文件（`c:\VRMGuestAgent\site\workitem.xml`），使用客户机代理自定义属性完成为其分配的所有任务，然后将其自身从已置备计算机中删除。

您可以为要在已部署计算机上运行的客户机代理编写自己的自定义脚本，然后使用计算机蓝图上的自定义属性指定这些脚本的位置和运行顺序。此外，您还可以使用计算机蓝图上的自定义属性将自定义属性值作为参数传递给脚本。

例如，您可以使用客户机代理在已部署的计算机上自定义以下设置：

- 更改 IP 地址

- 添加或格式化驱动器
- 运行安全脚本
- 初始化另一个代理，例如 Puppet 或 Chef

您还可以在命令行参数中提供加密字符串作为自定义属性。这使您可以将客户机代理能够解密和理解的加密信息作为有效的命令行参数进行存储。

注 对于与工作项中 vRealize Automation 自定义属性相关的 Linux Kickstart 和 PXE 置备，Linux 客户机代理将在创建和克隆操作期间分配静态 IP。分配静态 IP 时，客户机代理在 Ubuntu 16x 等中无法容纳更新的统一网络命名方案。

自定义脚本不必本地安装在计算机上。只要已置备的计算机可以通过网络访问脚本位置，客户机代理便能访问并运行这些脚本。这降低了维护成本，因为您无需重新构建所有模板即可更新脚本。

您可以通过在预留、蓝图或客户机代理脚本中指定信息来配置安全设置。如果要置备的计算机需要客户机代理，您必须将包含该要求的安全规则添加到预留或蓝图。例如，如果您使用拒绝所有计算机之间的通信的默认安全策略，并依赖不同的安全策略以允许特定计算机之间的通信，则客户机代理在自定义阶段可能无法与 vRealize Automation 通信。要避免在计算机置备期间出现此问题，请使用允许在自定义阶段进行通信的默认安全策略。

如果选择通过安装客户机代理在已置备计算机上运行自定义脚本，则蓝图必须包括相应的客户机代理自定义属性。例如，如果将客户机代理安装在克隆模板上，创建一个自定义脚本来更改已置备计算机的 IP 地址，并将该脚本放在共享位置中，则需在蓝图中包含大量自定义属性。

表 1-7. 用于通过客户机代理更改已置备计算机的 IP 地址的自定义属性

自定义属性	描述
<code>VirtualMachine.Admin.UseGuestAgent</code>	设置为 true 时，将在启动已置备的计算机后初始化客户机代理。
<code>VirtualMachine.Customize.WaitComplete</code>	设置为 True 时，可防止置备工作流在所有自定义完成之前将工作项发送到客户机代理。设置为 False 时，允许在自定义完成之前创建工作项。

表 1-7. 用于通过客户机代理更改已置备计算机的 IP 地址的自定义属性（续）

自定义属性	描述
VirtualMachine.SoftwareN.ScriptPath	<p>指定应用程序安装脚本的完整路径。该路径必须是客户机操作系统看到的有效绝对路径，且必须包含该脚本文件名的名称。</p> <p>通过在路径字符串中插入 {<i>CustomPropertyName</i>}，您可以将自定义属性值作为参数传递给脚本。例如，如果您拥有值为 1234 的自定义属性 ActivationKey，则脚本路径为 D:\InstallApp.bat -key {ActivationKey}。客户机代理运行命令 D:\InstallApp.bat -key 1234。然后，您可以对脚本文件进行编程，使其接受并使用此值。</p> <p>插入 {<i>Owner</i>} 可将计算机所有者名称传递给脚本。</p> <p>通过在路径字符串中插入 {<i>YourCustomProperty</i>}，您还可以将自定义属性值作为参数传递给脚本。例如，输入值 \\vra-scripts.mycompany.com\scripts\changeIP.bat 可从共享位置运行 changeIP.bat 脚本；但是，输入值 \\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address} 可在运行 changeIP 脚本的同时将 VirtualMachine.Network0.Address 属性的值作为参数传递给脚本。</p>
VirtualMachine.ScriptPath.Decrypt	<p>允许 vRealize Automation 获取作为格式正确的 VirtualMachine.SoftwareN.ScriptPath 自定义属性声明传递到 gugent 命令行的加密字符串。</p> <p>您可以提供加密字符串（如您的密码）作为命令行参数中的自定义属性。这允许您存储客户机代理可解密并作为有效命令行参数理解的加密信息。例如，</p> <p>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat password 自定义属性字符串由于包含实际密码，因此不安全。</p> <p>要解密该密码，可以创建 vRealize Automation 自定义属性（例如 MyPassword = password），并通过选择可用复选框启用加密。客户机代理会将 [MyPassword] 条目解密为自定义属性 MyPassword 中的值并以 c:\dosomething.bat password 运行脚本。</p> <ul style="list-style-type: none"> ■ 创建自定义属性 MyPassword = password，其中 password 是实际密码的值。通过选择可用复选框启用加密。 ■ 将自定义属性 VirtualMachine.ScriptPath.Decrypt 设置为 VirtualMachine.ScriptPath.Decrypt = true。 ■ 将自定义属性 VirtualMachine.Software0.ScriptPath 设置为 VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]。 <p>如果将 VirtualMachine.ScriptPath.Decrypt 设置为 False，或不创建 VirtualMachine.ScriptPath.Decrypt 自定义属性，则不会解密方括号（[和]）中的字符串。</p>

有关可与客户机代理配合使用的自定义属性的详细信息，请参见《自定义属性参考》。

将客户机代理配置为信任服务器

在正确的客户机代理文件夹中安装 vRealize Automation Manager Service 主机的公钥 PEM 文件，这是将客户机代理配置为信任服务器最安全的方法。

要使 Manager Service 主机信任服务器，请在 `cert.pem` PEM 文件的每个模板上找到客户机代理文件夹：

- 使用 `gugent` 的每个模板上的 Windows 客户机代理文件夹

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

- 使用 `gugent` 的每个模板上的 Linux 客户机代理文件夹

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

如果不将 `cert.pem` 文件放在此位置中，则模板参考机无法使用客户机代理。例如，如果您在启动虚拟机后尝试通过更改脚本收集公钥信息，则会带来安全风险。

根据配置的环境，还需要考虑其他注意事项：

- 对于 WIM 安装，您必须将公钥 PEM 文件内容添加到控制台可执行文件和用户界面。控制台标记为 **/cert filename**。
- 对于 RedHat kickstart 安装，您必须将公钥剪切并粘贴到示例文件中，否则客户机代理将无法运行。
- 对于 SCCM 安装，`cert.pem` 文件必须驻留在 `VRMGuestAgent` 文件夹中。
- 对于 Linux vSphere 安装，`cert.pem` 文件必须驻留在 `/usr/share/gugent` 文件夹中。

注 您可以选择将软件和客户机代理安装在一起，方法是从 <https://APPLIANCE/software/index.html> 下载以下脚本。该脚本允许您在创建模板时处理是否接受 SSL 证书指纹。

- Linux

```
prepare_vra_template.sh
```

- Windows

```
prepare_vra_template.ps1
```

如果将软件和客户机代理安装在一起，则您无需按照在 [Linux 参考机中安装客户机代理](#) 或在 [Windows 参考机中安装客户机代理](#) 中的说明进行操作。

如何从 Manager Service 主机获取 cert.pem 文件

- 1 在 Manager Service 主机上，转到“管理工具”，然后打开“Internet Information Services (IIS) 管理器”。
- 2 在左侧的树中，突出显示 Manager Service 主机。
- 3 在右侧，打开“服务器证书”。
- 4 查找颁发对象为 VMware vRA 且颁发机构为 VMware vRA 的证书。
- 5 右键单击该证书，然后将其导出。

- 6 保存的证书将采用 PFX 格式。要将其转换为 PEM，请从命令行使用 OpenSSL。

```
openssl pkcs12 -in filename.pfx -out cert.pem -nodes
```

在 Linux 参考机中安装客户机代理

在参考机上安装 Linux 客户机代理，以便部署后进一步自定义计算机。

前提条件

- 标识或创建参考机。
- 下载的客户机代理文件包含 **tar.gz** 和 **RPM** 软件包格式。如果操作系统无法安装 **tar.gz** 或 **RPM** 文件，请使用转换工具将安装文件转换为首选软件包格式。
- 在客户机代理和 Manager Service 计算机之间建立安全信任。请参见[将客户机代理配置为信任服务器](#)。

步骤

- 1 导航到 vRealize Automation 设备管理控制台页面。

例如：<https://va-hostname.domain.com>。

- 2 单击此页面 vRealize Automation 组件安装部分中的[客户机和软件代理](#)页面。

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

将打开[客户机和软件代理安装程序](#)页面，其中显示有可用下载的连接。

- 3 单击此页面客户机代理安装程序部分中的 **Linux 客户机代理软件包**，下载并保存 **LinuxGuestAgentPkgs.zip** 文件。

- 4 解压下载的 **LinuxGuestAgentPkgs.zip** 文件，生成 **VraLinuxGuestAgent** 文件夹。

- 5 安装与您在置备期间部署的客户机操作系统对应的客户机代理软件包。

- a 导航到与置备期间要部署的客户机操作系统（例如 **rhel32**）相对应的 **VraLinuxGuestAgent** 子目录。
- b 找到首选软件包格式或将软件包转换为首选软件包格式。
- c 将客户机代理软件包安装在参考机上。

例如，要安装 RPM 软件包中的文件，请运行 `rpm -i gugent-gugent-7.1.0-4201531.i386.rpm`。

- 6 通过运行 `installgugent.sh Manager_Service_Hostname_fdqn:portnumber ssl platform`，将客户机代理配置为与 Manager Service 通信。

Manager Service 的默认端口号为 443。可接受的平台值为 `ec2`、`vcd`、`vca` 和 `vsphere`。

选项	描述
如果使用负载均衡器	输入 Manager Service 负载均衡器的完全限定域名和端口号。例如： <pre>cd /usr/share/gugent ./installgugent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
没有负载均衡器	输入 Manager Service 计算机的完全限定域名和端口号。例如： <pre>cd /usr/share/gugent ./installgugent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

- 7 如果部署的计算机尚未配置为信任 Manager Service SSL 证书，则必须在参考机上安装 `cert.pem` 文件才能建立信任。
- 最安全的方法是获取 `cert.pem` 证书并将该文件手动安装在参考机上。
 - 还有一种更便捷的方法：您可以连接到 Manager Service 负载均衡器或 Manager Service 计算机，然后下载 `cert.pem` 证书。

选项	描述
如果使用负载均衡器	以参考机上的 root 用户身份运行以下命令： <pre>echo openssl s_client -connect manager_service_load_balancer.mycompany.com:443 sed -ne '/- BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>
没有负载均衡器	以参考机上的 root 用户身份运行以下命令： <pre>echo openssl s_client -connect manager_service_machine.mycompany.com:443 sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > cert.pem</pre>

- 8 如果正在 Ubuntu 操作系统上安装客户机代理，请通过运行以下命令集之一创建共享对象的符号链接。

选项	描述
64 位系统	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
32 位系统	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

后续步骤

将参考机转换为 IaaS 架构师在创建蓝图时可以使用的克隆模板、Amazon 计算机映像或快照。

在 Windows 参考机中安装客户机代理

在 Windows 参考机中安装 vRealize Automation Windows 客户机代理，使其作为 Windows 服务运行并进一步自定义计算机。

前提条件

- 标识或创建参考机。
- 在客户机代理和 Manager Service 计算机之间建立安全信任。请参见[将客户机代理配置为信任服务器](#)。

步骤

- 1 导航到 vRealize Automation 设备的[客户机和软件代理安装程序](#)页面：

`https://vrealize-automation-appliance-FQDN/software`

- 2 在[客户机代理安装程序](#)下，下载 32 位或 64 位可执行文件并将其保存到 C: 驱动器的根目录。

注 有一个命令行可替代此客户机代理的安装过程。您可以不下载可执行文件，而是转到客户机和软件代理安装程序页面上的 **Windows 软件安装程序**。在此下载并运行 `prepare_vra_template.ps1` PowerShell 脚本：

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

- 3 通过运行可执行文件提取 Windows 客户机代理文件。

提取操作将创建 `C:\VRMGuestAgent` 并在其中添加文件。

请勿重命名 `C:\VRMGuestAgent`。

- 4 将客户机代理配置为与 Manager Service 通信。

- a 打开提升的命令提示符。

- b 导航到 `C:\VRMGuestAgent`。

- c 将可信的 Manager Service PEM 文件放置在 C:\VRMGuestAgent\ 目录中，以将客户机代理配置为信任 Manager Service 计算机。
- d 运行 `win service -i -h Manager_Service_Hostname_fdn:portnumber -p ssl`。

Manager Service 的默认端口号为 443。

选项	描述
如果使用负载均衡器	输入 Manager Service 负载均衡器的完全限定域名和端口号。例如， <code>win service -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> 。
没有负载均衡器	输入 Manager Service 计算机的完全限定域名和端口号。例如， <code>win service -i -h manager_service_machine.mycompany.com:443 -p ssl</code> 。
如果准备 Amazon 计算机映像	您需要指定您正在使用 Amazon。例如， <code>win service -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code> 。

结果

Windows 服务的名称为 VCACGuestAgentService。您可以在 C:\VRMGuestAgent 中找到安装日志 VCAC-GuestAgentService.log。

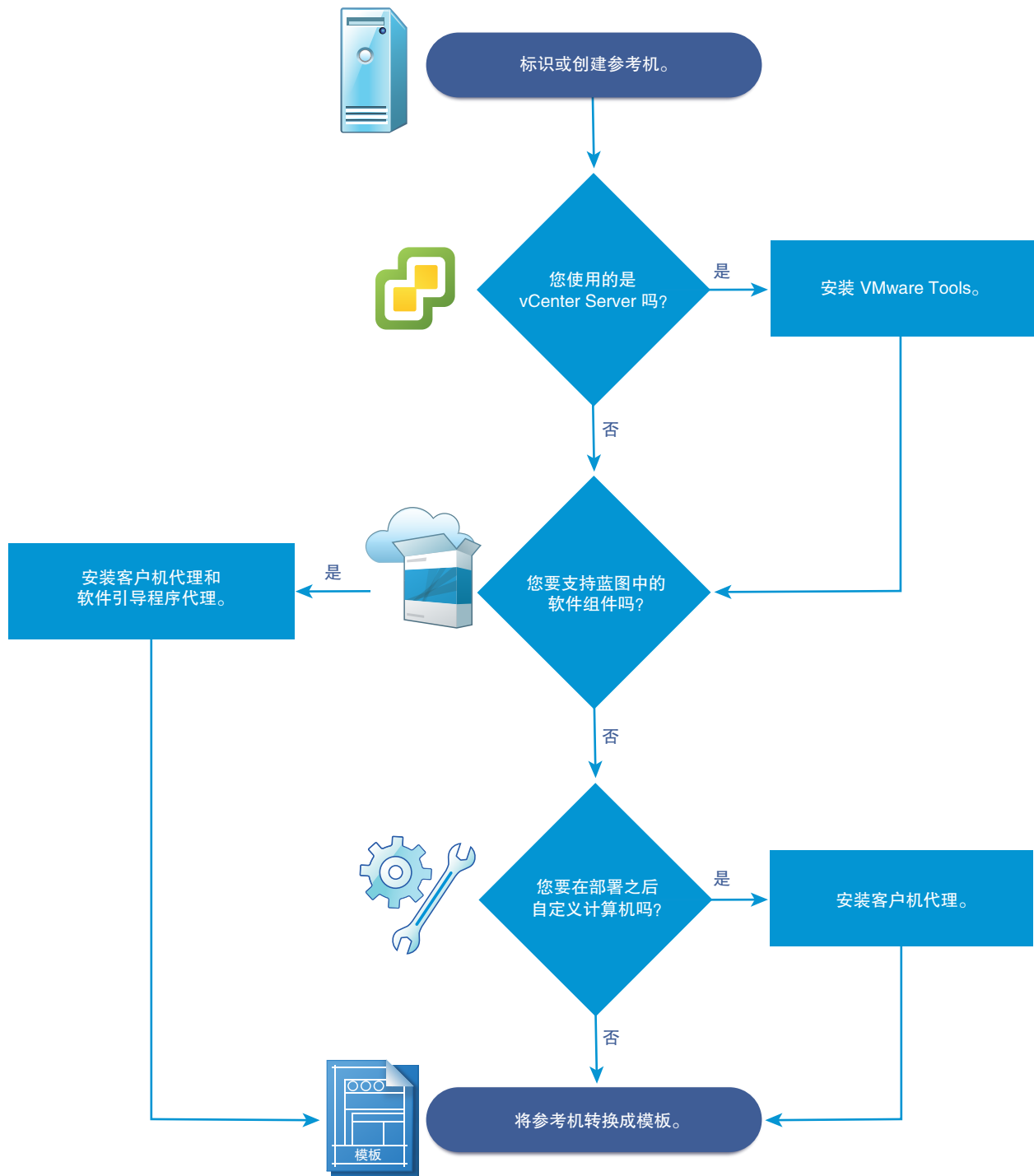
后续步骤

将参考机转换为克隆模板、Amazon 计算机映像或快照，以便 IaaS 架构师在创建蓝图时可以使用您的模板。

准备通过克隆进行置备的对照表

要创建用于克隆 Linux 和 Windows 虚拟机的模板和自定义对象，必须在 vRealize Automation 外部进行一些准备。

克隆需要使用通过参考机创建的克隆模板。



如果要通过克隆置备 Windows 计算机，则已将置备计算机加入 Active Directory 域的唯一方法是使用 vCenter Server 中的自定义规范，或者在 SCVMM 模板中包含客户机操作系统配置文件。在置备期间，通过克隆置备的计算机不能放在 Active Directory 容器中。必须在置备后手动执行此操作。

表 1-8. 准备通过克隆进行置备的对照表

任务	位置	详细信息
<input type="checkbox"/> 标识或创建参考机。	管理程序	请参见管理程序提供的文档。
<input type="checkbox"/> (可选) 如果希望克隆模板支持 Software 组件, 请在参考机上安装 vRealize Automation 客户机代理和软件引导程序代理。	参考机	对 Windows 参考机, 请参见 准备 Windows 参考机以支持 Software 。 对 Linux 参考机, 请参见 准备 Linux 参考机以支持 Software 。
<input type="checkbox"/> (可选) 如果无需克隆模板支持 Software 组件, 但希望能够自定义已部署的计算机, 请在参考机上安装 vRealize Automation 客户机代理。	参考机	请参见 在置备期间使用 vRealize Automation 客户机代理 。
<input type="checkbox"/> 如果您是在 vCenter Server 环境中进行操作, 请在参考机上安装 VMware Tools。	vCenter Server	请参见 VMware Tools 文档。
<input type="checkbox"/> 使用参考机创建克隆模板。	管理程序	参考机启动或关闭均可。如果要在 vCenter Server 中克隆, 则可直接使用参考机, 而不必创建模板。 请参见管理程序提供的文档。
<input type="checkbox"/> 通过应用 System Preparation Utility 或 Linux 自定义功能, 创建自定义对象以配置克隆计算机。	管理程序	如果要为 Linux 克隆, 则可安装 Linux 客户机代理并提供外部自定义脚本, 而不是创建自定义对象。如果要使用 vCenter Server 克隆, 则必须将自定义规范提供为自定义对象。 请参见管理程序提供的文档。
<input type="checkbox"/> 将收集创建用于克隆模板的蓝图所需的信息。	捕获信息并传输给 IaaS 架构师。	请参见 通过克隆进行虚拟置备的工作表 。

通过克隆进行虚拟置备的工作表

完成知识传授工作表, 捕获与为在环境中准备的模板创建克隆蓝图所需的模板、自定义设置和自定义属性相关的信息。并非每次实施都需要所有这些信息。使用该工作表作为指导, 或者将工作表复制并粘贴到文字处理工具中进行编辑。

所需的蓝图和预留信息

表 1-9. 模板和预留信息工作表

所需信息	我的值	详细信息
模板名称		
模板可用的预留或要应用的预留策略		为了避免置备期间出错, 请确保该模板在所有预留上均可用, 或者创建一个预留策略, 该策略可供架构师用来将蓝图限制为模板可用的预留。
(仅限 vSphere) 为此模板请求的克隆类型		<ul style="list-style-type: none"> ■ 克隆 ■ 链接克隆 ■ NetApp FlexClone

表 1-9. 模板和预留信息工作表（续）

所需信息	我的值	详细信息
自定义规范名称（使用静态 IP 地址克隆时需要）		如果不使用 vSphere 自定义规范，您无法对 Windows 计算机执行自定义。 请参见 将 Linux 计算机加入到 Windows Active Directory 域 。
（仅限 SCVMM）ISO 名称		
（仅限 SCVMM）虚拟硬盘		
（仅限 SCVMM）要附加到已置备计算机的硬件配置文件		

所需属性组

您可以完成工作表的自定义属性信息部分，或者创建属性组并要求架构师将属性组添加到其蓝图中，而不是单独添加大量自定义属性。

所需的 vCenter Server 操作系统

您必须提供用于 vCenter Server 置备的客户机操作系统自定义属性。

表 1-10. vCenter Server 操作系统

自定义属性	我的值	描述
VMware.VirtualCenter.OperatingSystem		指定 vCenter Server 创建计算机时使用的 vCenter Server 客户机操作系统版本 (VirtualMachineGuestOsIdentifier)。此操作系统版本必须与置备的计算机上要安装的操作系统版本匹配。管理员可以使用多个预定义以包括正确 VMware.VirtualCenter.OperatingSystem 值的属性集之一（如 VMware[OS_Version]Properties）创建属性组。此属性适用于虚拟置备。

Visual Basic 脚本信息

如果已对 vRealize Automation 进行配置，使其将自定义 Visual Basic 脚本作为计算机生命周期中的额外步骤运行，则必须将有关这些脚本的信息包含在蓝图中。

注 架构管理员可以使用属性集 ExternalPreProvisioningVbScript 和 ExternalPostProvisioningVbScript 创建属性组，提供这些所需的信息。这样蓝图架构师可以更轻松地将这些信息正确包含在蓝图中。

表 1-11. Visual Basic 脚本信息

自定义属性	我的值	描述
ExternalPreProvisioningVbScript		在置备前运行脚本。输入脚本的完整路径，其中包括文件名和扩展名。 <i>%System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs。</i>
ExternalPostProvisioningVbScript		在置备后运行脚本。输入脚本的完整路径，其中包括文件名和扩展名。 <i>%System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs</i>

Linux 客户机代理的自定义脚本信息

如果已将 Linux 模板配置为使用客户机代理运行自定义脚本，则必须将这些脚本的信息包含在蓝图中。

表 1-12. Linux 客户机代理的自定义脚本信息工作表

自定义属性	我的值	描述
Linux.ExternalScript.Name		指定 Linux 客户机代理在安装操作系统之后运行的可选自定义脚本的名称，例如， config.sh 。对于从模板中克隆的、安装 Linux 代理的 Linux 计算机，此属性可用。 如果指定外部脚本，则还必须使用 Linux.ExternalScript.LocationType 和 Linux.ExternalScript.Path 属性定义其位置。
Linux.ExternalScript.LocationType		指定在 Linux.ExternalScript.Name 属性中命名的自定义脚本的位置类型。此类型可以是 local 或 nfs 。 此外，您还必须使用 Linux.ExternalScript.Path 属性指定脚本位置。如果位置类型为 nfs ，请仍使用 Linux.ExternalScript.Server 属性。
Linux.ExternalScript.Server		指定在 Linux.ExternalScript.Name 中命名的 Linux 外部自定义脚本所处的 NFS 服务器的名称，例如， lab-ad.lab.local 。
Linux.ExternalScript.Path		在 NFS 服务器上指定 Linux 自定义脚本的本地路径或 Linux 自定义的导出路径。该值必须以正斜线开头且不得包括文件名，例如， /scripts/linux/config.sh 。

客户机代理的其他自定义属性

如果已在参考机上安装客户机代理，则可在部署后使用自定义属性进一步自定义计算机。

表 1-13. 用于通过客户机代理自定义克隆计算机的自定义属性工作表

自定义属性	我的值	描述
<code>VirtualMachine.Admin.AddOwnerToAdmins</code>		设置为 True （默认值），会将 VirtualMachine.Admin.Owner 属性指定的计算机所有者添加到该计算机上的本地管理员组。
<code>VirtualMachine.Admin.AllowLogin</code>		设置为 True （默认值）时，会将计算机所有者添加到 VirtualMachine.Admin.Owner 属性指定的本地远程桌面用户组。
<code>VirtualMachine.Admin.UseGuestAgent</code>		如果客户机代理作为服务安装在模板上进行克隆，则在计算机蓝图上设置为 True ，以便在从该模板中克隆的计算机上启用客户机代理服务。计算机启动时，客户机代理服务将随之启动。设置为 False 时，将停用客户机代理。如果设置为 False ，则增强的克隆工作流不会使用客户机代理执行客户机操作系统任务，从而减少其对 VMwareCloneWorkflow 的功能。如果未指定或设置为除 False 以外的其他值，则增强型克隆工作流会将工作项发送到客户机代理。
<code>VirtualMachine.DiskN.Active</code>		设置为 True （默认值）时，将指定计算机的 N 盘处于活动状态。设置为 False 时，将指定计算机的 N 盘处于非活动状态。
<code>VirtualMachine.DiskN.Label</code>		指定计算机 N 盘的标签。磁盘标签最多不超过 32 个字符。磁盘编号必须是连续的。与客户机代理结合使用时，指定客户机操作系统内计算机 N 盘的标签。
<code>VirtualMachine.DiskN.Letter</code>		指定计算机磁盘 N 的驱动器盘符或挂载点。默认值为 C 盘。例如，要指定磁盘 1 的盘符 D ，请将该自定义属性定义为 VirtualMachine.Disk1.Letter 并输入值 D 。磁盘编号必须是连续的。与客户机代理结合使用时，此值将指定客户机代理在客户机操作系统中挂载另一 N 盘时所在的驱动器盘符或挂载点。
<code>VirtualMachine.Admin.CustomizeGuestOSDelay</code>		指定自定义完成后、开始客户机操作系统自定义之前要等待的时间。该值必须采用 HH:MM:SS 格式。如果未设置该值，则默认值为一分钟 (00:01:00)。如果选择不包括此自定义属性，如果在客户机代理工作项完成之前重新引导虚拟机（导致置备失败），则置备可能会失败。
<code>VirtualMachine.Customize.WaitComplete</code>		设置为 True 时，可防止置备工作流在所有自定义完成之前将工作项发送到客户机代理。设置为 False 时，允许在自定义完成之前创建工作项。

表 1-13. 用于通过客户机代理自定义克隆计算机的自定义属性工作表（续）

自定义属性	我的值	描述
VirtualMachine.SoftwareN.Name		指定置备期间要安装或运行的软件应用程序 <i>N</i> 或脚本的描述性名称。这是一个可选属性，仅供信息参考使用。它对增强型克隆工作流或客户机代理没有实际意义，但对于用户界面中的自定义软件选择或者软件使用情况报告十分有用。
VirtualMachine.SoftwareN.ScriptPath		指定应用程序安装脚本的完整路径。该路径必须是客户机操作系统看到的有效绝对路径，且必须包含该脚本文件名的名称。 通过在路径字符串中插入 {CustomPropertyName} ，您可以将自定义属性值作为参数传递给脚本。例如，如果您拥有值为 1234 的自定义属性 ActivationKey ，则脚本路径为 D:\InstallApp.bat -key {ActivationKey} 。客户机代理运行命令 D:\InstallApp.bat -key 1234 。然后，您可以对脚本文件进行编程，使其接受并使用此值。
VirtualMachine.SoftwareN.ISOName		指定 ISO 文件相对于数据存储根的路径和文件名。格式为 /folder_name/subfolder_name/file_name.iso 。如果未指定值，则 ISO 不会挂载。
VirtualMachine.SoftwareN.ISOLocation		指定包含应用程序或脚本要使用的 ISO 映像文件的存储路径。按照路径在主机预留上的形式设置路径格式，例如 netapp-1:it_nfs_1 。如果未指定值，则 ISO 不会挂载。

网络自定义属性

可以使用自定义属性为计算机上的特定网络设备指定配置。

下表列出了与网络相关的常用自定义属性。有关其他自定义属性和相关的自定义属性，请参见《自定义属性参考》中的“克隆蓝图的自定义属性”和“网络自定义属性”。

表 1-14. 网络配置的自定义属性

自定义属性	我的值	描述
VirtualMachine.NetworkN.Addresses		在使用静态 IP 地址置备的计算机中，指定网络设备 <i>N</i> 的 IP 地址。
VirtualMachine.NetworkN.MacAddressType		<p>指示网络设备 <i>N</i> 的 MAC 地址是生成的，还是用户定义的（静态）。此属性可用于克隆。</p> <p>此时将生成默认值。如果该值是静态的，则还必须使用 VirtualMachine.NetworkN.MacAddress 指定 MAC 地址。</p> <p>VirtualMachine.NetworkN 自定义属性特定于单个蓝图和计算机。请求计算机后，系统先执行网络和 IP 地址分配，然后再将计算机分配给预留。由于蓝图并不一定会分配给特定的预留，因此请勿对预留使用此属性。按需 NAT 或按需路由网络不支持此属性。</p>
VirtualMachine.NetworkN.MacAddress		<p>指定网络设备 <i>N</i> 的 MAC 地址。此属性可用于克隆。</p> <p>如果 VirtualMachine.NetworkN.MacAddressType 的值是生成的，则此属性包含生成的地址。</p> <p>如果 VirtualMachine.NetworkN.MacAddressType 的值是静态的，则此属性指定 MAC 地址。对于在 ESX Server 主机上置备的虚拟机，该地址必须在 VMware 指定的范围内。有关详细信息，请参见 vSphere 文档。</p> <p>VirtualMachine.NetworkN 自定义属性特定于单个蓝图和计算机。请求计算机后，系统先执行网络和 IP 地址分配，然后再将计算机分配给预留。由于蓝图并不一定会分配给特定的预留，因此请勿对预留使用此属性。按需 NAT 或按需路由网络不支持此属性。</p>

表 1-14. 网络配置的自定义属性（续）

自定义属性	我的值	描述
VirtualMachine.NetworkN.Name		<p>指定要连接到的网络的名称，例如，计算机接到的网络设备 <i>N</i>。这等同于网卡 (Network Interface Card, NIC)。</p> <p>默认情况下，网络是通过置备计算机的预留中可用的网络路径分配的。另请参见 <code>VirtualMachine.NetworkN.AddressType</code>。</p> <p>通过将此属性的值设置为可用预留中的网络名称，您可以确保网络设备连接到特定的网络。例如，如果为 <i>N</i> 指定属性 <i>O</i> 和 <i>1</i>，则您将获得 2 张网卡及其分配的值，但前提是网络在关联预留中已选定。</p> <p><code>VirtualMachine.NetworkN</code> 自定义属性特定于蓝图和计算机。请求计算机后，系统先执行网络和 IP 地址分配，然后再将计算机分配给预留。由于蓝图并不一定会分配给特定的预留，因此请勿对预留使用此属性。按需 NAT 或按需路由网络不支持此属性。</p> <p>有关如何使用此自定义属性根据用户在预定义可用网络列表中所选的内容来动态设置 <code>VirtualMachine.Network0.Name</code> 的示例，请参见博客文章在 vRA 7 中添加网络选择下拉菜单。</p>
VirtualMachine.NetworkN.PortID		<p>使用具有 vSphere Distributed Switch 的 dvPort 组时，指定要用于设备网络 <i>N</i> 的端口 ID。</p> <p><code>VirtualMachine.NetworkN</code> 自定义属性特定于单个蓝图和计算机。请求计算机后，系统先执行网络和 IP 地址分配，然后再将计算机分配给预留。由于蓝图并不一定会分配给特定的预留，因此请勿对预留使用此属性。按需 NAT 或按需路由网络不支持此属性。</p>
VirtualMachine.NetworkN.NetworkProfileName		<p>指定要从中将静态 IP 地址分配给网络设备 <i>N</i> 或者要从中获取可分配给克隆计算机的网络设备 <i>N</i> 的静态 IP 地址范围的网络配置文件名称。其中，<i>N=0</i> 表示第一台设备，<i>1</i> 表示第二台设备，依此类推。</p> <p>该属性所指向的网络配置文件用于分配 IP 地址。该属性将根据预留确定计算机将连接的网络。</p>

表 1-14. 网络配置的自定义属性（续）

自定义属性	我的值	描述
<ul style="list-style-type: none"> VirtualMachine.NetworkN.SubnetMask VirtualMachine.NetworkN.Gateway VirtualMachine.NetworkN.PrimaryDns VirtualMachine.NetworkN.SecondaryDns VirtualMachine.NetworkN.PrimaryWins VirtualMachine.NetworkN.SecondaryWins VirtualMachine.NetworkN.DnsSuffix VirtualMachine.NetworkN.DnsSearchSuffixes 		<p>通过附加名称，您可以创建自定义属性的多个版本。例如，以下属性将列出针对一般用途设置的负载均衡池，以及具有高、适中和低性能要求的计算机：</p> <ul style="list-style-type: none"> VCNS.LoadBalancerEdgePool.Names VCNS.LoadBalancerEdgePool.Names.moderate VCNS.LoadBalancerEdgePool.Names.high VCNS.LoadBalancerEdgePool.Names.low <p>配置 VirtualMachine.NetworkN.NetworkProfileName 中指定的网络配置文件的属性。</p>
VCNS.LoadBalancerEdgePool.Names.name		<p>指定置备期间向其分配虚拟机的 NSX 负载均衡池。虚拟机将分配给所有指定池的所有服务端口。该值是一个 <i>edge/pool</i> 名称或用逗号分隔的 <i>edge/pool</i> 名称列表。名称区分大小写。</p> <p>通过附加名称，您可以创建自定义属性的多个版本。例如，以下属性将列出针对一般用途设置的负载均衡池，以及具有高、适中和低性能要求的计算机：</p> <ul style="list-style-type: none"> VCNS.LoadBalancerEdgePool.Names VCNS.LoadBalancerEdgePool.Names.moderate VCNS.LoadBalancerEdgePool.Names.high VCNS.LoadBalancerEdgePool.Names.low

表 1-14. 网络配置的自定义属性（续）

自定义属性	我的值	描述
VCNS.SecurityGroup.Names. <i>name</i>		<p>指定 NSX 安全组或置备期间向其分配虚拟机的组。该值是一个安全组名称或用逗号分隔的名称列表。名称区分大小写。</p> <p>通过附加名称，您可以创建属性的多个版本。这些版本既可单独使用，也可组合使用。例如，以下属性可以列出通用安全组、销售人员安全组和支持安全组：</p> <ul style="list-style-type: none"> ■ VCNS.SecurityGroup.Names ■ VCNS.SecurityGroup.Names.sale s ■ VCNS.SecurityGroup.Names.support
VCNS.SecurityTag.Names. <i>name</i>		<p>指定 NSX 安全标记或置备期间与虚拟机关联的标记。该值是一个安全标记名称或用逗号分隔的名称列表。名称区分大小写。</p> <p>通过附加名称，您可以创建属性的多个版本。这些版本既可单独使用，也可组合使用。例如，以下属性可以列出通用安全标记、销售人员安全标记和支持安全标记：</p> <ul style="list-style-type: none"> ■ VCNS.SecurityTag.Names ■ VCNS.SecurityTag.Names.sales ■ VCNS.SecurityTag.Names.support

将 Linux 计算机加入到 Windows Active Directory 域

有多种方法可以在置备计算机时将 Linux 计算机加入到 Windows Active Directory 域。

- 如果要通过克隆进行置备，必须使用自定义规范（用于置备 vSphere 计算机）或包括带有 SCVMM 模板的客户机操作系统配置文件。置备计算机时，计算机将加入到指定的域。
- 如果不通过克隆进行置备，可以在蓝图关联的网络配置文件中使用的 DNS 后缀设置以标识域。为了使用静态 IP 地址分配进行置备，您必须使用 vSphere 自定义规范。
- 如果您使用 vSphere 自定义规范，计算机在置备时将加入到自定义规范所标识的域，而不是蓝图的关联网络配置文件中指定为 DNS 后缀的域。

vSphere 自定义规范是 vSphere 对象，包含一组用于 Windows 和 Linux 客户机操作系统设置的预定义条件。您可以使用计算机的**构建信息**选项卡上的**自定义规范**设置，来将自定义规范名称添加到 vRealize Automation 蓝图。

有关在 vSphere 中创建自定义规范的信息，请参见 [vSphere 产品文档](#)，如创建和管理自定义规范中的自定义规范主题。

准备 vCloud Air 和 vCloud Director 置备

要通过使用 vRealize Automation 准备 vCloud Air 和 vCloud Director 置备，必须使用模板和自定义对象配置组织虚拟数据中心。

要使用 vRealize Automation 置备 vCloud Air 和 vCloud Director 资源，组织需要包括一种或多种计算机资源的克隆模板。

组织之间共享的模板必须为公共模板。只有预留的模板才可以供 vRealize Automation 用作克隆源。

注 如果通过从模板中克隆来创建蓝图，则此模板的唯一标识符将与蓝图关联。蓝图发布到 vRealize Automation 目录并用于置备和数据收集过程之后，将会识别关联的模板。如果删除 vCloud Air 或 vCloud Director 中的模板，后续 vRealize Automation 置备和数据收集将会失败，因为关联的模板不再存在。例如，要上载更新版本，请使用 vCloud Air 或 vCloud Director 模板替换过程替换模板，而不是删除和重新创建模板。使用 vCloud Air 或 vCloud Director 替换模板，而不是删除和重新创建模板，使模板唯一的 ID 保持不变，从而允许置备和数据收集继续正常工作。

以下概览说明了使用 vRealize Automation 来创建端点以及定义预留和蓝图之前需要执行的步骤。有关管理任务的详细信息，请参见 vCloud Air 和 vCloud Director 产品文档。

- 1 在 vCloud Air 或 vCloud Director 中，创建克隆模板，并将它添加到组织目录。
- 2 在 vCloud Air 或 vCloud Director 中，使用模板为每台计算机上的客户机操作系统指定自定义设置（例如，密码、域和脚本）。

您可以使用 vRealize Automation 替代某些设置。

自定义可以因资源的客户机操作系统而异。

- 3 在 vCloud Air 或 vCloud Director 中，配置可以与组织中每个人员共享的目录。

在 vCloud Air 或 vCloud Director 中，为适用的组织配置帐户管理员访问，以允许其中的所有用户和组可以访问目录。如果没有此共享指定，在 vRealize Automation 中，目录模板将对端点或蓝图架构师不可见。

- 4 收集以下信息，使您能够将其包含在蓝图中：
 - vCloud Air 或 vCloud Director 模板的名称。
 - 为模板指定的存储总量。

准备进行 Linux Kickstart 置备

Linux Kickstart 置备使用配置文件在新置备的计算机上自动安装 Linux。要准备进行置备，您必须创建一个可引导的 ISO 映像和 Kickstart 或 autoYaST 配置文件。

下文概述了准备 Linux Kickstart 置备时所需执行的步骤：

- 1 确认网络中具有 DHCP 服务器。除非有 DHCP，否则 vRealize Automation 无法使用 Linux Kickstart 置备方法置备计算机。
- 2 准备配置文件。在配置文件中，您必须指定 vRealize Automation 服务器和 Linux 代理安装软件包的位置。请参见[准备 Linux Kickstart 配置示例文件](#)。

- 3 编辑 `isolinux/isolinux.cfg` 或 `loader/isolinux.cfg`，指定配置文件的名称和位置以及适当的 Linux 分发源。
- 4 创建引导 ISO 映像并将其保存到虚拟化平台所要求的位置。有关所需位置的信息，请参见管理程序提供的文档。
- 5 （可选）添加自定义脚本。
 - a 要在配置文件中指定安装后自定义脚本，请参见在 [kickstart/autoYaST 配置文件中指定自定义脚本](#)。
 - b 要在蓝图中调用 Visual Basic 脚本，请参见在 [置备期间运行 Visual Basic 脚本的对照表](#)。
- 6 收集以下信息，使蓝图架构师能够将其包含在相应的蓝图中：
 - a ISO 映像的名称和位置。
 - b 对于 vCenter Server 集成，收集 vCenter Server 创建计算机使用的 vCenter Server 客户机操作系统版本。

注 您可以使用属性集 `BootIsoProperties` 创建属性组，将所需的 ISO 信息包括在内。这样可以更轻松地将这些信息正确包含在蓝图中。

准备 Linux Kickstart 配置示例文件

vRealize Automation 提供了一系列示例配置文件，您可对其进行修改和编辑以满足自己的需要。要使这些文件可用，必须进行多项更改。

步骤

- 1 导航到 vRealize Automation 设备管理控制台页面。
例如：<https://va-hostname.domain.com>。
- 2 单击此页面 vRealize Automation 组件安装部分中的 **客户机和软件代理** 页面。
例如：<https://va-hostname.domain.com/software/index.html>。
将打开 **客户机和软件代理安装程序** 页面，其中显示有可用下载的连接。
- 3 单击此页面客户机代理安装程序部分中的 **Linux 客户机代理软件包**，下载并保存 `LinuxGuestAgentPkgs.zip` 文件。
- 4 解压下载的 `LinuxGuestAgentPkgs.zip` 文件，生成 `VraLinuxGuestAgent` 文件夹。
- 5 导航至与置备期间要部署的客户机操作系统相对应 `VraLinuxGuestAgent` 子目录。
例如：`rhel32`。
- 6 打开 `samples` 子目录中与您的目标系统相对应的文件。
例如，`samples/sample-https-rhel6-x86.cfg`。

- 将字符串 `host=dcac.example.net` 的所有实例替换为 Manager Service 或 Manager Service 负载均衡器的 IP 地址或者完全限定域名和端口号。

平台	所需的格式
vSphere ESXi	IP 地址，例如： <code>--host=172.20.9.59</code>
vSphere ESX	IP 地址，例如： <code>--host=172.20.9.58</code>
SUSE 10	IP 地址，例如： <code>--host=172.20.9.57</code>
所有其他平台	FQDN，例如： <code>--host=mycompany-host1.mycompany.local:443</code>

- 找到 `gugent.rpm` 或 `gugent.tar.gz` 的每个实例，然后将 URL `rpm.example.net` 替换为客户机代理软件包的位置。

例如：

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

- 将该文件保存到新置备的计算机可以访问的位置。

在 kickstart/autoYaST 配置文件中指定自定义脚本

您可以修改配置文件，以便将自定义脚本复制或安装到新装备的计算机中。Linux 代理在工作流的指定点中运行这些脚本。

脚本可以引用任何 `./properties.xml` 文件（位于 `/usr/share/gugent/site/workitem` 目录中）。

前提条件

- 准备 kickstart 或 autoYaST 配置文件。请参见[准备 Linux Kickstart 配置示例文件](#)。
- 出现故障时，脚本必须返回非零值，防止计算机置备失败。

步骤

- 创建或标识要使用的脚本。

- 将该脚本另存为 `NN_scriptname`。

`NN` 是一个两位数的数字。脚本按照从低到高的顺序运行。如果两个脚本的编号相同，则该顺序是基于 `scriptname` 的字母顺序。

- 使脚本可运行。

- 找到 kickstart 或 autoYaST 配置文件的安装后部分。

在 kickstart 中，此部分由 `%post` 表示；在 autoYaST 中，此部分由 `post-scripts` 表示。

- 修改配置文件的安装后部分，以便脚本复制或安装到您选择 `/usr/share/gugent/site/workitem` 目录中。

自定义脚本通常针对包含工作项 SetupOS（用于创建制备）和 CustomizeOS（用于克隆置备）的虚拟 kickstart/autoYaST 运行，但您可以在工作流中的任何点运行脚本。

例如，您可以修改配置文件，以便使用下列命令将脚本 `11_addusers.sh` 复制到新置备的计算机上的 `/usr/share/gugent/site/SetupOS` 目录中：

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

结果

Linux 代理按照工作项目目录和脚本文件名指定的顺序运行该脚本。

准备进行 SCCM 置备

vRealize Automation 从 ISO 映像引导新置备的计算机，然后将控制权传递给指定的 SCCM 任务序列。

Windows 操作系统的部署支持 SCCM 置备。该系统既不支持 Linux，也不支持软件分发和更新。

默认情况下，会将 SCCM 计算机配置为在置备后每隔 10 秒确认一次相应集合中的成员资格。在某些情况下，此时间间隔会导致注册过程出现问题。有两个属性可用于自定义确认过程。第一个属性名为 **SCCM refresh collection setting**。默认情况下，此属性设置为 **true**，以确认计算机将执行成员资格检查。如果适用，您可以将其更改为 **false**，以将计算机配置为跳过成员资格检查。第二个属性名 **SCCM machine membership check interval**。如前文所述，默认值为 10 秒，但是如果遇到注册问题，可以将其设置为其他值以延长重新触发时段。这两个属性均位于 **基础架构 > 管理 > 全局设置** 下的 **laaS 全局设置** 中。

下文概述了准备 SCCM 置备时所需执行的步骤：

1 与 SCCM 通信需要 SCCM 服务器的 NetBIOS 名称。

与网络管理员协作，以确保至少一个 Distributed Execution Manager (DEM) 能将 SCCM 服务器的 FQDN 解析为其 NetBIOS 名称。

不需要直接将 DEM 置于同一个网络作为 SCCM 服务器，但 DEM 需要能够通过 IP 地址到达 SCCM 服务器。

2 创建一个包含 vRealize Automation 客户机代理的软件包。请参见 [创建用于 SCCM 置备的软件包](#)。

3 在 SCCM 中，创建置备计算机所需的任务序列。最后一个步骤必须是安装您创建的、包含 vRealize Automation 客户机代理的软件包。有关创建任务序列和安装软件包的信息，请参见 SCCM 文档。

4 为任务序列创建零接触引导 ISO 映像。默认情况下，SCCM 将创建轻触引导式 ISO 映像。有关为零接触 ISO 映像配置 SCCM 的信息，请参见 SCCM 文档。

5 将该 ISO 映像复制到虚拟化平台所需的位置。如果您不知道适当的位置，请参见管理程序提供的文档。

6 收集以下信息，使蓝图架构师能够将其包含在蓝图中：

- a 包含任务序列的集合的名称。
- b 包含该序列的集合所在 SCCM 服务器的完全限定域名。
- c SCCM 服务器的站点代码。
- d SCCM 服务器的管理员级别凭据。
- e （可选）对于 SCVMM 集成，收集要附加到已置备计算机的 ISO、虚拟硬盘或硬件配置文件。

创建用于 SCCM 置备的软件包

SCCM 任务序列中的最后一个步骤必须是安装包括 vRealize Automation 客户机代理的软件包。

步骤

- 1 导航到 vRealize Automation 设备管理控制台页面。
例如: <https://va-hostname.domain.com>。
- 2 单击此页面 vRealize Automation 组件安装部分中的**客户机和软件代理**页面。
例如: <https://va-hostname.domain.com/software/index.html>。
将打开**客户机和软件代理安装程序**页面, 其中显示有可用下载的连接。
- 3 单击此页面组件安装部分中的 Windows 客户机代理文件 (**32 位**) 或 (**64 位**), 下载并保存 GuestAgentInstaller.exe 或 GuestAgentInstaller_x64.exe 文件。
- 4 将 Windows 客户机代理文件提取到适用于 SCCM 的位置。
这样可以生成 C:\VRMGuestAgent 目录。请勿重命名此目录。
- 5 使用定义文件 SCCMPackageDefinitionFile.sms 创建软件包。
- 6 将软件包提供给分发点。
- 7 选择已提取的 Windows 客户机代理文件的内容作为源文件。

准备进行 WIM 置备

通过引导到 WinPE 环境并使用现有 Windows 参考机的 Windows Imaging File Format (WIM) 映像安装操作系统, 以此置备计算机。

下文概述了准备 WIM 置备时所需执行的步骤:

- 1 标识或创建转储区域。转储区域应为可由以下项指定为 UNC 路径或挂载为网络驱动器的网络目录:
 - 参考机。
 - 构建 WinPE 映像的系统。
 - 置备计算机的虚拟化主机。
- 2 确保网络具有 DHCP 服务器。除非有 DHCP, 否则 vRealize Automation 无法使用 WIM 映像置备计算机。
- 3 在要用于置备的虚拟化平台中, 标识或创建参考机。对于 vRealize Automation 要求, 请参见 [WIM 置备的参考机要求](#)。有关创建参考机的信息, 请参见管理程序提供的文档。
- 4 使用 System Preparation Utility for Windows, 为部署准备参考机的操作系统。请参见[参考机的 SysPrep 要求](#)。
- 5 创建参考机的 WIM 映像。请不要在 WIM 映像文件名称中包含任何空格, 否则置备会失败。

6 创建一个包含 vRealize Automation 客户机代理的 WinPE 映像。

- （可选）创建要用于自定义置备的计算机的任何自定义脚本，并将它们放入相应的工作项目录中。
- 如果要使用 VirtIO 处理网络或存储接口，则必须确保 WinPE 映像和 WIM 映像中包含所需的驱动程序。请参见[准备通过 VirtIO 驱动程序进行 WIM 置备](#)。

创建 WinPE 映像时，必须手动插入 vRealize Automation 客户机代理。请参见[将客户机代理手动插入 WinPE 映像](#)。

7 将 WinPE 映像放入虚拟化平台所需的位置中。如果您不知道此位置，请参见管理程序文档。

8 收集以下信息以包含在蓝图中：

- a WinPE ISO 映像的名称和位置。
- b WIM 文件的名称、WIM 文件的 UNC 路径以及用于从 WIM 文件中提取所需映像的索引。
- c 用于将 WIM 映像路径映射到已置备计算机上的网络驱动器的用户名和密码。
- d （可选）如果不想接受默认值 K，则收集 WIM 映像路径在已置备计算机上映射到的驱动器盘符。
- e 对于 vCenter Server 集成，收集 vCenter Server 创建计算机使用的 vCenter Server 客户机操作系统版本。
- f （可选）对于 SCVMM 集成，收集要附加到已置备计算机的 ISO、虚拟硬盘或硬件配置文件。

注 您可以创建属性组，将所有需要的信息包括在内。使用属性组可以更轻松地将所有信息正确包含在蓝图中。

步骤

1 [WIM 置备的参考机要求](#)

WIM 置备包括使用参考机创建 WIM 映像。参考机必须满足 WIM 映像的基本要求，才可用于在 vRealize Automation 中进行置备。

2 [参考机的 SysPrep 要求](#)

SysPrep 应答文件包含几个用于 WIM 置备的必需设置。

3 [准备通过 VirtIO 驱动程序进行 WIM 置备](#)

如果要使用 VirtIO 处理网络或存储接口，则必须确保 WinPE 映像和 WIM 映像中包含所需的驱动程序。使用 KVM (RHEV) 进行置备时，VirtIO 提供的性能通常更出色。

4 [将客户机代理手动插入 WinPE 映像](#)

您必须手动将 vRealize Automation 客户机代理插入 WinPE 映像。

WIM 置备的参考机要求

WIM 置备包括使用参考机创建 WIM 映像。参考机必须满足 WIM 映像的基本要求，才可用于在 vRealize Automation 中进行置备。

下文概述了准备参考机所需执行的步骤：

- 1 如果参考机上的操作系统是 Windows Server 2008 R2、Windows Server 2012、Windows 7 或 Windows 8，则除了主分区以外，默认安装还会在系统的硬盘上创建一个小分区。vRealize Automation 不支持使用在此类多分区参考机上创建的 WIM 映像。必须在安装过程中删除此分区。
- 2 在参考机上安装 NET 4.5 和适用于 Windows 7 的 Windows 自动安装工具包 (AIK)（包括 WinPE 3.0）。
- 3 如果参考机操作系统是 Windows Server 2003 或 Windows XP，请将管理员密码重置为空白。（没有密码。）
- 4 （可选）如果要启用 XenDesktop 集成，请安装并配置 Citrix Virtual Desktop Agent。
- 5 （可选）从由 vRealize Automation 管理的 Windows 计算机收集某些数据（例如，计算机所有者的 Active Directory 状态）需要 Windows Management Instrumentation (WMI) 代理。要确保成功管理 Windows 计算机，您必须安装 WMI 代理（通常安装在 Manager Service 主机上），并启用该代理从 Windows 计算机中收集数据。请参见 安装 vRealize Automation。

参考机的 SysPrep 要求

SysPrep 应答文件包含几个用于 WIM 置备的必需设置。

表 1-15. Windows Server 或 Windows XP 参考机所需的 SysPrep 设置

GuiUnattended 设置	值
AutoLogon	Yes
AutoLogonCount	1
AutoLogonUsername	username (username 和 password 是在新置备的计算机引导至客户机操作系统时用于自动登录的凭据。通常使用 administrator。)
AutoLogonPassword	password 对应于 AutoLogonUsername。

表 1-16. 未使用 Windows Server 2003 或 Windows XP 的参考机所需的 SysPrep 设置：

AutoLogon 设置	值
Enabled	Yes
LogonCount	1

表 1-16. 未使用 Windows Server 2003 或 Windows XP 的参考机所需的 SysPrep 设置：（续）

AutoLogon 设置	值
Username	<p><i>username</i></p> <p>（<i>username</i> 和 <i>password</i> 是在新置备的计算机引导至客户机操作系统时用于自动登录的凭据。通常使用 <code>administrator</code>。）</p>
Password	<p><i>password</i></p> <p>（<i>username</i> 和 <i>password</i> 是在新置备的计算机引导至客户机操作系统时用于自动登录的凭据。通常使用 <code>administrator</code>。）</p> <p>注 如果参考机使用的 Windows 平台版本高于 Windows Server 2003/Windows XP，则必须通过使用自定义属性 <code>Sysprep.GuiUnattended.AdminPassword</code> 设置自动登录密码。确保实现这一点的便捷方法是创建包含此自定义属性的属性组，使租户管理员和业务组主管能够将这些信息正确包含在蓝图</p>

准备通过 VirtIO 驱动程序进行 WIM 置备

如果要使用 VirtIO 处理网络或存储接口，则必须确保 WinPE 映像和 WIM 映像中包含所需的驱动程序。使用 KVM (RHEV) 进行置备时，VirtIO 提供的性能通常更出色。

VirtIO 的 Windows 驱动程序作为 Red Hat Enterprise Virtualization 的一部分附带提供，且位于 Red Hat Enterprise Virtualization Manager 文件系统上的 `/usr/share/virtio-win` 目录中。这些驱动程序也包括在位于 `/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso` 的 Red Hat Enterprise Virtualization Guest Tools 中。

通过 VirtIO 驱动程序进行基于 WIM 置备的简要过程如下：

- 1 从安装 VirtIO 驱动程序的 Windows 参考机创建 WIM 映像，或者将这些驱动程序插入现有的 WIM 映像中。
- 2 复制 VirtIO 驱动程序文件并将这些驱动程序插入 WinPE 映像。
- 3 使用 `rhev-m-iso-uploader` 命令将 WinPE 映像 ISO 上载到 Red Hat Enterprise Virtualization ISO 存储域。有关在 RHEV 中管理 ISO 映像的详细信息，请参见 Red Hat 文档。
- 4 创建用于 WIM 置备的 KVM (RHEV) 蓝图，然后选择 WinPE ISO 选项。自定义属性 `VirtualMachine.Admin.DiskInterfaceType` 必须随值 **VirtIO** 一起提供。架构管理员可将这些信息包含在属性组中，以便纳入蓝图。

自定义属性 `Image.ISO.Location` 和 `Image.ISO.Name` 不用于 KVM (RHEV) 蓝图。

将客户机代理手动插入 WinPE 映像

您必须手动将 vRealize Automation 客户机代理插入 WinPE 映像。

前提条件

- 选择 Windows 系统。在此系统中，可以访问您准备的转储区域且已安装用于 Windows 7 的 .NET 4.5 和 Windows 自动安装工具包 (AIK)（包括 WinPE 3.0）。

- 创建 WinPE。

步骤

1 在 WinPE 中安装客户机代理

您必须手动将客户机代理文件复制到 WinPE 映像。

2 配置 doagent.bat 文件

必须手动配置 doagent.bat 文件。

3 配置 doagentc.bat 文件

必须手动配置 doagentc.bat 文件。

4 配置客户机代理属性文件

必须手动配置客户机代理属性文件。

步骤

1 在 WinPE 中安装客户机代理。

2 配置 doagent.bat 文件。

3 配置 doagentc.bat 文件。

4 配置客户机代理属性文件。

在 WinPE 中安装客户机代理

您必须手动将客户机代理文件复制到 WinPE 映像。

前提条件

- 选择 Windows 系统。在此系统中，可以访问您准备的转储区域且已安装用于 Windows 7 的 .NET 4.5 和 Windows 自动安装工具包 (AIK)（包括 WinPE 3.0）。
- 创建 WinPE。

步骤

- ◆ 从 https://vRealize_VA_Hostname_fqdn/software/index.html 下载并安装 vRealize Automation 客户机代理。

- a 将 `GugentZip_version` 下载到参考机上的 C 盘。

根据操作系统选择 `GuestAgentInstaller.exe`（32 位）或 `GuestAgentInstaller_x64.exe`（64 位）。

- b 右键单击文件，然后选择**属性**。

- c 单击**常规**。

- d 单击**取消阻止**。
- e 将文件提取至 C:\。

这样可以生成 C:\VRMGuestAgent 目录。请勿重命名此目录。

后续步骤

配置 [doagent.bat](#) 文件。

配置 doagent.bat 文件

必须手动配置 doagent.bat 文件。

前提条件

在 [WinPE](#) 中安装客户机代理。

步骤

- 1 导航到 WinPE 映像内的 VRMGuestAgent 目录。
例如：C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent。
- 2 复制文件 doagent-template.bat，并将其命名为 doagent.bat。
- 3 在文本编辑器中打开 doagent.bat。
- 4 将字符串 #Dcac Hostname# 的所有实例替换为 IaaS Manager Service 主机的完全限定域名和端口号。

选项	描述
如果使用负载均衡器	输入 IaaS Manager Service 的负载均衡器的完全限定域名和端口。例如， <code>manager_service_LB.mycompany.com:443</code>
没有负载均衡器	输入安装 IaaS Manager Service 的计算机的完全限定域名和端口。例如， <code>manager_service.mycompany.com:443</code>

- 5 将字符串 #Protocol# 的所有实例替换为字符串 /ssl。
- 6 将字符串 #Comment# 的所有实例替换为 REM （REM 必须后跟末尾的空格）。
- 7 （可选）如果使用自签名证书，则取消 openssl 命令的注释。

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

- 8 保存并关闭文件。
- 9 编辑 WinPE 的 Startnet.cmd 脚本，使其将 doagent.bat 作为自定义脚本包括在内。

后续步骤

配置 [doagentc.bat](#) 文件。

配置 doagentc.bat 文件

必须手动配置 doagentc.bat 文件。

前提条件

配置 doagent.bat 文件。

步骤

- 1 导航到 WinPE 映像内的 VRMGuestAgent 目录。
例如: C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent。
- 2 复制文件 doagentsvc-template.bat, 并将其命名为 doagentc.bat。
- 3 在文本编辑器中打开 doagentc.bat。
- 4 移除字符串 #Comment# 的所有实例。
- 5 将字符串 #Dcac Hostname# 的所有实例替换为 Manager Service 主机的完全限定域名和端口号。
Manager Service 的默认端口为 443。

选项	描述
如果使用负载均衡器	输入用于 Manager Service 的负载均衡器的完全限定域名和端口。例如, load_balancer_manager_service.mycompany.com:443
没有负载均衡器	输入 Manager Service 的完全限定域名和端口。例如, manager_service.mycompany.com:443

- 6 将字符串 #errorlevel# 的所有实例替换为字符 1。
- 7 将字符串 #Protocol# 的所有实例替换为字符串 /ssl。
- 8 保存并关闭文件。

后续步骤

配置客户机代理属性文件。

配置客户机代理属性文件

必须手动配置客户机代理属性文件。

前提条件

配置 doagentc.bat 文件。

步骤

- 1 导航到 WinPE 映像内的 VRMGuestAgent 目录。
例如: C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent。

- 2 复制文件 `gugent.properties`，并将其命名为 `gugent.properties.template`。
- 3 复制文件 `gugent.properties.template`，并将其命名为 `gugentc.properties`。
- 4 在文本编辑器中打开 `gugent.properties`。
- 5 将字符串 `GuestAgent.log` 的所有实例替换为字符串 `X:/VRMGuestAgent/GuestAgent.log`。
- 6 保存并关闭文件。
- 7 在文本编辑器中打开 `gugentc.properties`。
- 8 将字符串 `GuestAgent.log` 的所有实例替换为字符串 `C:/VRMGuestAgent/GuestAgent.log`。
- 9 保存并关闭文件。

准备进行虚拟机映像置备

在使用 OpenStack 置备实例之前，您必须在 OpenStack 提供程序中配置虚拟机映像和功能。

虚拟机映像

为 OpenStack 资源创建蓝图时，您可以从可用映像列表中选择虚拟机映像。

虚拟机映像是一个包含软件配置（包括操作系统）的模板。虚拟机映像由 OpenStack 提供程序管理并在数据收集期间导入。

如果稍后从 OpenStack 提供程序中删除蓝图中使用的映像，则该映像也会从此蓝图中移除。如果已从某个蓝图中移除所有映像，则该蓝图处于停用状态，无法处理任何计算机请求，直到编辑该蓝图并为其添加至少一个映像为止。

OpenStack 功能

您可以在创建 OpenStack 蓝图时选择一个或多个功能。

OpenStack 功能是为 OpenStack 中置备的实例定义计算机资源规范的虚拟硬件模板。功能由 OpenStack 提供程序管理并在数据收集期间导入。

准备进行 Amazon 计算机映像置备

准备要在 vRealize Automation 中置备的 Amazon 计算机映像和实例类型。

了解 Amazon 计算机映像

在创建 Amazon 计算机蓝图时，可从可用映像列表中选择 Amazon 计算机映像。

Amazon 计算机映像是一个包含软件配置（包括操作系统）的模板。Amazon 计算机映像由 Amazon Web Services 帐户管理。vRealize Automation 管理可用于置备的实例类型。

Amazon 计算机映像和实例类型均必须在 Amazon 区域中可用。并非所有实例类型都在所有区域中可用。

您可以选择由 Amazon Web Services、用户社区或 AWS Marketplace 站点提供的 Amazon 计算机映像。此外，您也可以创建并选择共享自己的 Amazon 计算机映像。单个 Amazon 计算机映像可用于启动一个或多个实例。

以下注意事项适用于 Amazon Web Services 帐户中要用于置备云计算机的 Amazon 计算机映像：

- 每个蓝图必须指定一个 Amazon 计算机映像。

专用的 Amazon 计算机映像可用于特定的帐户及其所有区域。公共 Amazon 计算机映像则可用于所有帐户，但仅适用于每个帐户中的特定区域。

- 创建蓝图之后，系统将从已进行数据收集的区域中选择指定的 Amazon 计算机映像。如果多个 Amazon Web Services 帐户可用，则业务组主管必须对任何专用 Amazon 计算机映像具有相应权限。Amazon 计算机映像区域和指定的用户位置会将置备请求限制为与相应区域和位置匹配的预留。
- 使用预留和策略可将 Amazon 计算机映像分发至 Amazon Web Services 帐户中。使用策略可将通过蓝图进行的置备限制为一组特定的预留。
- vRealize Automation 无法在云计算机上创建用户帐户。首次连接到云计算机时，计算机所有者必须以管理员身份登录并添加 vRealize Automation 用户凭据，否则管理员必须为其执行该操作。然后，计算机所有者才可使用 vRealize Automation 用户凭据登录。

如果 Amazon 计算机映像每次引导时生成管理员密码，则“编辑计算机记录”页面将显示该密码。如果未显示，您可以在 Amazon Web Services 帐户中找到该密码。您可以对所有 Amazon 计算机映像进行配置，使其在每次引导时生成管理员密码。此外，您还可以提供管理员密码信息，从而支持为其他用户置备计算机的用户。

- 要在 Amazon Web Services 帐户中置备的云计算机上允许远程 Microsoft Windows Management Instrumentation (WMI) 请求，请启用 Microsoft Windows Remote Management (WinRM) 代理，以从由 vRealize Automation 管理的 Windows 计算机中收集数据。请参见 [安装 vRealize Automation](#)。
- 您可以查看租户中的专用 Amazon 计算机映像。

有关相关信息，请参见 Amazon 文档中的“Amazon 计算机映像 (AMI)”。

了解 Amazon 实例类型

IaaS 架构师可以在创建 Amazon EC2 蓝图时选择一个或多个 Amazon 实例类型。IaaS 管理员可以添加或删除实例类型，控制可供架构师使用的选项。

Amazon EC2 实例是指可在 Amazon Web Services 中运行应用程序的虚拟服务器。实例是通过使用 Amazon 计算机映像并选择适当的实例类型创建的。

要在 Amazon Web Services 帐户中置备计算机，应将实例类型应用于指定的 Amazon 计算机映像。可用的实例类型将在架构师创建 Amazon EC2 蓝图时列出。架构师可以选择一个或多个实例类型，这些实例类型在请求置备计算机时可供用户选择。指定的区域中必须支持这些实例类型。

有关相关信息，请参见 Amazon 文档中的“选择实例类型”和“Amazon EC2 实例详细信息”主题。

添加 Amazon 实例类型

vRealize Automation 提供了多种实例类型与 Amazon 蓝图一起使用。管理员可以添加和移除实例类型。

创建或编辑 Amazon 蓝图时，蓝图架构师可以使用由 IaaS 管理员负责管理的计算机实例类型。Amazon 计算机映像和实例类型可通过 Amazon Web Services 产品获取。

前提条件

以 **IaaS 管理员** 身份登录到 vRealize Automation。

步骤

- 1 单击**基础架构 > 管理 > 实例类型**。
- 2 单击**新建**。
- 3 添加新实例类型，从而指定以下参数。

有关可用 Amazon 实例类型以及可为这些参数指定的设置值的信息，请参见“EC2 实例类型 - Amazon Web Services (AWS)”中的 Amazon Web Services 文档（位于 aws.amazon.com/ec2）和“实例类型”（位于 docs.aws.amazon.com）。

- 名称
- API 名称
- 类型名称
- IO 性能名称
- CPU
- 内存 (GB)
- 存储 (GB)
- 计算单元

- 4 单击**保存图标** (✔)。

结果

当 IaaS 架构师创建 Amazon Web Services 蓝图时，可以使用自定义实例类型。

后续步骤

将端点中的计算资源添加到架构组。请参见 [创建架构组](#)。

场景：准备 vSphere 资源进行计算机置备

作为一名需为 vRealize Automation 创建模板的 vSphere 管理员，您需要使用 vSphere Web Client 准备在 vRealize Automation 中克隆 CentOS 计算机。

您需要将现有的一台 CentOS 参考机转换成 vSphere 模板，以便您和架构师能够在 vRealize Automation 中为克隆 CentOS 计算机创建蓝图。为了防止在部署多个具有相同设置的虚拟机时可能产生的冲突，您还需要创建一个您和架构师在为 Linux 模板创建克隆蓝图时均可使用的常规自定义规范。

前提条件

标识或创建已安装 VMware Tools 的 Linux CentOS 参考机。至少包括一个网络适配器以提供 Internet 连接。

步骤

1 场景：将 CentOS 参考机转换成适用于 Rainpole 的模板

通过使用 vSphere Client，您可以将现有 CentOS 参考机转换成 vSphere 模板，供 vRealize Automation IaaS 架构师引用为克隆蓝图基础。

2 场景：为克隆 Linux 计算机创建自定义规范

通过使用 vSphere Client，您可以创建标准自定义规范，以便 vRealize Automation IaaS 架构师在为 Linux 计算机创建克隆蓝图时使用。

场景：将 CentOS 参考机转换成适用于 Rainpole 的模板

通过使用 vSphere Client，您可以将现有 CentOS 参考机转换成 vSphere 模板，供 vRealize Automation IaaS 架构师引用为克隆蓝图基础。

步骤

1 以 root 用户身份登录到参考机，并准备要转换的计算机。

a 移除 udev 持久规则。

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

b 使从此模板中克隆的计算机拥有自身的唯一标识符。

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

c 关闭计算机电源。

```
shutdown -h now
```

2 以管理员身份登录到 vSphere Web Client。

3 单击虚拟机选项选项卡。

4 右键单击参考机并选择编辑设置。

5 在虚拟机名称文本框中输入 Rainpole_centos_63_x86。

6 即使参考机具有 CentOS 客户机操作系统，仍请从客户机操作系统版本下拉菜单中选择 Red Hat Enterprise Linux 6 (64 位)。

如果选择 CentOS，则模板和自定义规范可能无法按预期工作。

7 在 vSphere Web Client 中右键单击 Rainpole_centos_63_x86 参考机，然后选择模板 > 转换成模板。

结果

vCenter Server 将 Rainpole_centos_63_x86 参考机标记为模板，并在“近期任务”窗格中显示任务。

后续步骤

为了防止在部署多个具有相同设置的虚拟机时可能产生的冲突，您需要创建一个您和 Rainpole 架构师在为 Linux 模板创建克隆蓝图时均可使用的常规自定义规范。

场景：为克隆 Linux 计算机创建自定义规范

通过使用 vSphere Client，您可以创建标准自定义规范，以便 vRealize Automation IaaS 架构师在为 Linux 计算机创建克隆蓝图时使用。

步骤

- 1 在主页中，单击**自定义规范管理器**以打开该向导。
- 2 单击**新建**图标。
- 3 指定属性。
 - a 从**目标虚拟机操作系统**下拉菜单中选择 **Linux**。
 - b 在**自定义规范名称**文本框中输入 **Linux**。
 - c 在**描述**文本框中，输入 **Rainpole Linux cloning with vRealize Automation**。
 - d 单击**下一步**。
- 4 设置计算机名称。
 - a 选择**使用虚拟机名称**。
 - b 在**域名**文本框中，输入要置备克隆计算机的域。
 - c 单击**下一步**。
- 5 配置时区设置。
- 6 单击**下一步**。
- 7 选择**对客户机操作系统使用标准网络设置**，包括在所有网络接口上启用 **DHCP**。
- 8 按照提示输入其余的必填信息。
- 9 在**即将完成**页面上，检查所选项，然后单击**完成**。

准备进行 Software 置备

在为 vSphere、vCloud Director、vCloud Air、Amazon Web Services 和 Microsoft Azure 计算机置备 vRealize Automation 的过程中，使用 Software 部署应用程序和中间件。

如果蓝图支持 Software 且您先在参考机上安装客户机代理和软件引导程序代理，然后再将参考机转换为模板、快照或计算机映像，则可在计算机上部署 Software。

有关准备置备计算机时指定端口的相关信息，请参见 [vRealize Automation 产品文档](#) 中的《参考架构》PDF。

表 1-17. 支持 Software 的置备方法

计算机类型	准备
vSphere	克隆蓝图将根据 vCenter Server 虚拟机模板置备一个独立的完整虚拟机。如果希望克隆模板支持 Software 组件，当准备克隆模板时，请在参考机上安装客户机代理和软件引导程序代理。请参见 准备通过克隆进行置备的对照表 。
vSphere	链接克隆蓝图将根据快照置备节省空间的 vSphere 计算机副本，并使用增量磁盘链来跟踪与父虚拟机的差异。如果希望链接克隆蓝图支持 Software 组件，请先在计算机上安装客户机代理和软件引导程序代理，然后再生成快照。 如果快照计算机是从支持 Software 的模板中克隆的，则表示已安装所需的代理。
vCloud Director	克隆蓝图将根据 vCenter Server 虚拟机模板置备一个独立的完整虚拟机。如果希望克隆模板支持 Software 组件，当准备克隆模板时，请在参考机上安装客户机代理和软件引导程序代理。请参见 准备通过克隆进行置备的对照表 。
vCloud Air	克隆蓝图将根据 vCenter Server 虚拟机模板置备一个独立的完整虚拟机。如果希望克隆模板支持 Software 组件，当准备克隆模板时，请在参考机上安装客户机代理和软件引导程序代理。请参见 准备通过克隆进行置备的对照表 。
Amazon Web Services	Amazon 计算机映像是一个包含软件配置（包括操作系统）的模板。如果需要创建支持 Software 的 Amazon 计算机映像，请连接到正在运行的 Amazon Web Services 实例，该实例对 root 设备使用 EBS 卷。在参考机上安装客户机代理和软件引导程序代理，然后从该实例中创建 Amazon 计算机映像。 要使客户机代理和 Software 引导程序代理在置备的计算机上正常运行，您必须配置从网络到 VPC 的连接。 有关创建 Amazon EBS 支持的 AMI 的信息，请参见 Amazon Web Services 文档。
Microsoft Azure	有关信息，请参见 Software 组件设置 、 创建用于 Microsoft Azure 的蓝图 和 Microsoft Azure 产品文档。

准备使用 Software 置备计算机

要支持 Software 组件，必须先在参考机上安装客户机代理和 Software 引导程序代理，然后再转换为克隆模板、创建 Amazon 计算机映像或生成快照。

准备 Windows 参考机以支持 Software

您可以使用单个脚本在 Windows 参考机上安装 Java Runtime Environment、客户机代理和 Software 引导程序代理。您可以从参考机创建克隆模板、快照或支持 Software 组件的 Amazon 计算机映像。

Software 支持 Windows CMD 和 PowerShell 2.0 脚本运行。

重要事项 启动过程不得中断。配置虚拟机，确保在出现登录提示之前虚拟机启动过程不会暂停。例如，确认在虚拟机启动后不会出现进程或脚本提示用户交互。

前提条件

- 标识或创建 Windows 参考机。
- 在参考机与 IaaS Manager Service 主机之间建立安全信任。请参见[将客户机代理配置为信任服务器](#)。

- 如果为了进行故障排除或出于其他原因而计划远程访问计算机，请安装远程桌面服务 (RDS)。
- 从网络配置文件中移除网络配置项目。

步骤

- 1 以管理员身份登录到 Windows 参考服务器。
- 2 在 vRealize Automation 设备上打开浏览器访问软件下载页面。
`https://vrealize-automation-appliance-FQDN/software`
- 3 将模板 ZIP 保存到 Windows Server。
`prepare_vra_template_windows.zip`
- 4 将 ZIP 内容提取到一个文件夹，然后运行批处理文件。
`.\prepare_vra_template.bat`
- 5 按照提示进行操作。
- 6 完成后，关闭 Windows 虚拟机。

结果

该脚本将移除所有之前的客户机或 Software 引导程序代理，然后安装支持的 Java Runtime Environment、客户机代理和 Software 引导程序代理版本。

后续步骤

将参考机转换为克隆模板、快照或 Amazon 计算机映像。这些对象均支持 Software 组件，基础架构架构师可以使用它们创建蓝图。

准备 Linux 参考机以支持 Software

您可以使用单个脚本在 Linux 参考机上安装 Java Runtime Environment、客户机代理和 Software 引导程序代理。您可以从参考机创建克隆模板、快照或支持 Software 组件的 Amazon 计算机映像。

Software 支持 Bash 脚本运行。

重要事项 引导过程不得中断。配置虚拟机，确保在出现登录提示之前虚拟机引导过程不会暂停。例如，确认在虚拟机启动后不会出现进程或脚本提示用户交互。

前提条件

- 标识或创建 Linux 参考机。
- 确认以下命令可用，具体取决于您的 Linux 系统：
 - yum 或 apt-get
 - wget 或 curl
 - python
 - dmidecode（根据云提供程序的要求）

- 通用要求，如 `sed`、`awk`、`perl`、`chkconfig`、`unzip` 和 `grep`，具体取决于 Linux 分发。您还可以使用编辑器检查下载的 `prepare_vra_template.sh` 脚本，以显示它使用的命令。
- 如果为了进行故障排除或出于其他原因而计划远程访问计算机，请安装 OpenSSH。
- 从网络配置文件中移除网络配置项目。

步骤

- 1 以 root 用户身份登录到参考机。

- 2 从 vRealize Automation 设备下载模板 tar.gz 软件包。

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

如果您的环境使用的是自签名证书，您可能需要 `--no-check-certificate` 选项。

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

- 3 解压缩该软件包。

```
tar -xvf prepare_vra_template_linux.tar.gz
```

- 4 在解压缩输出中，找到安装程序脚本，并使其成为可执行文件。

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

- 5 运行安装程序脚本。

```
./prepare_vra_template.sh
```

如果您需要有关非交互式选项和预期值的信息，请参见脚本帮助。

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

- 6 按照提示进行操作。

安装成功时，将显示一条确认消息。如果显示错误和日志，请解决这些错误并重新运行脚本。

- 7 完成后，关闭 Linux 虚拟机。

结果

该脚本将移除所有之前的客户机或 Software 引导程序代理，然后安装支持的 Java Runtime Environment、客户机代理和 Software 引导程序代理版本。

后续步骤

在管理程序或云提供程序上，将参考机转换为克隆模板、快照或 Amazon 计算机映像。这些对象均支持 Software 组件，基础架构架构师可以使用它们创建蓝图。

更新 vRealize Automation 中的现有虚拟机模板

如果要为最新版本的 Windows Software 引导程序代理更新模板、Amazon 计算机映像或快照，或者如果要手动更新为最新的 Linux Software 引导程序代理，而非使用 `prepare_vra_template.sh` script，则需要移除任何现有版本并删除所有日志。

Linux

对于 Linux 参考机，运行 `prepare_vra_template.sh` script 脚本将先重置该代理并移除任何日志，然后再重新进行安装。但是，如果您打算手动进行安装，则需要以 root 用户身份登录到参考机，然后运行该命令来重置和移除项目。

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

Windows

对于 Windows 参考机，请移除现有的 Software 代理引导程序和 vRealize Automation 6.0 或更高版本的客户机代理，并删除任何现有的运行时日志文件。在 PowerShell 命令窗口中，运行以下命令移除代理和项目。

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

为克隆计算机和软件组件蓝图准备 vSphere 模板

作为 vCenter Server 管理员，您需要准备可供 vRealize Automation 架构师用于克隆 Linux CentOS 等计算机的 vSphere 模板。您需要确保模板支持包含软件组件的蓝图，因此应在将参考机转变为模板之前，先安装客户机代理和软件引导程序代理。

前提条件

- 标识或创建已安装 VMware Tools 的 Linux CentOS 参考机。至少包括一个网络适配器用于提供 Internet 连接（如果蓝图架构师未在蓝图级别添加此功能）。有关创建虚拟机的信息，请参见 vSphere 文档。
- 必须连接到 vCenter Server 才能将虚拟机转换成模板。如果将 vSphere Client 直接连接到 vSphere ESXi 主机，则不能创建模板。

步骤

1 场景：为客户机代理自定义规范和软件组件准备参考机

在参考机上安装软件引导程序代理及其必备条件和客户机代理，以使模板可以支持软件组件。这些代理将确保使用模板的 vRealize Automation 架构师可将软件组件包含在其蓝图中。

2 场景：将 CentOS 参考机转换成模板

在参考机上安装客户机代理和软件引导程序代理之后，将参考机转变为可供 vRealize Automation 架构师用于创建克隆计算机蓝图的模板。

3 场景：为 vSphere 克隆创建自定义规范

为蓝图架构师创建自定义规范以用于 `cpb_centos_63_x84` 模板。

结果

您已从参考机创建模板和自定义规范，可供蓝图架构师创建用于克隆 Linux CentOS 计算机的 vRealize Automation 蓝图。由于您在参考机上安装了 Software 引导程序代理和客户机代理，因此架构师可以使用模板创建包含 Software 组件或其他客户机自定义（例如，运行脚本或格式化磁盘）的详细目录项蓝图。由于您已安装 VMware Tools，因此架构师和目录管理员可以允许用户针对计算机执行重新配置、快照和重新引导等操作。

后续步骤

配置 vRealize Automation 用户、组以及资源后，您可以使用模板和自定义规范创建用于克隆的计算机蓝图。请参见[配置计算机蓝图](#)。

场景：为客户机代理自定义规范和软件组件准备参考机

在参考机上安装软件引导程序代理及其必备条件和客户机代理，以使模板可以支持软件组件。这些代理将确保使用模板的 vRealize Automation 架构师可将软件组件包含在其蓝图中。

为了简化该过程，请下载并运行可同时安装这两个代理的 vRealize Automation 脚本，而不是下载并安装单独的软件包。

此外，该脚本也将连接到 Manager Service 实例并下载 SSL 证书，以便在 Manager Service 与通过模板部署的计算机之间建立信任。注意：与手动获取 Manager Service SSL 证书并将其安装到参考机上的 `/usr/share/gugent/cert.pem` 中相比，让脚本下载证书不太安全。

步骤

- 1 打开浏览器访问 vRealize Automation 设备软件页面。

`https://vrealize-automation-appliance-FQDN/software`

- 2 在“Linux 软件安装程序”下，下载使用 gzip 压缩的 tar 文件。

`prepare_vra_template_linux.tar.gz`

- 3 将 tar 文件移至 Linux 参考机上的临时目录。

要传输文件，可以运行 WinSCP 等工具，或者使用熟悉的任何其他方法。

- 4 以 root 用户身份登录到 Linux 参考机上的命令提示符。

要打开终端，可以从 vRealize Automation 中启动计算机上的远程控制台，也可以使用熟悉的任何其他方法。

- 5 从临时目录中提取 tar 文件。

`gunzip prepare_vra_template_linux.tar.gz`

- 6 提取 tar 文件内容。

`tar xvf prepare_vra_template_linux.tar`

- 7 更改为脚本目录。

`cd prepare_vra_template_linux`

8 运行脚本，然后按照提示进行操作。

。 /prepare_vra_template.sh

如果您需要有关选项和值的非交互式信息，请输入 。 /prepare_vra_template.sh --help。

结果

安装完成后，将显示一条确认消息。如果显示错误消息和日志，请更正这些问题并重新运行脚本。

场景：将 CentOS 参考机转换成模板

在参考机上安装客户机代理和软件引导程序代理之后，将参考机转变为可供 vRealize Automation 架构师用于创建克隆计算机蓝图的模板。

将参考机转换成模板后，除非将模板转换回虚拟机，否则不能编辑或启动模板。

步骤

1 以 root 用户身份登录到参考机，并准备要转换的计算机。

a 移除 udev 持久规则。

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

b 使从此模板中克隆的计算机拥有自身的唯一标识符。

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

c 如果已在安装软件引导程序代理之后重新引导或重新配置参考机，请重置该代理。

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

d 关闭计算机电源。

```
shutdown -h now
```

2 以管理员身份登录到 vSphere Web Client。

3 右键单击参考机并选择**编辑设置**。

4 在**虚拟机名称**文本框中输入 **cpb_centos_63_x84**。

5 即使参考机具有 CentOS 客户机操作系统，仍请从**客户机操作系统版本**下拉菜单中选择 **Red Hat Enterprise Linux 6 (64 位)**。

如果选择 CentOS，则模板和自定义规范可能无法按预期工作。

6 在 vSphere Web Client 中右键单击参考机，然后选择**模板 > 转换成模板**。

结果

vCenter Server 将把 cpb_centos_63_x84 参考机标记为模板，并在“近期任务”窗格中显示任务。如果已将 vSphere 环境托管于 vRealize Automation，则系统会在下一个自动数据收集期间发现您的模板。如果尚未配置 vRealize Automation，则会在该过程中收集此模板。

场景：为 vSphere 克隆创建自定义规范

为蓝图架构师创建自定义规范以用于 cpb_centos_63_x84 模板。

步骤

- 1 以管理员身份登录到 vSphere Web Client。
- 2 在主页中，单击**自定义规范管理器**以打开该向导。
- 3 单击**新建**图标。
- 4 单击**新建**图标。
- 5 指定属性。
 - a 从**目标虚拟机操作系统**下拉菜单中选择 **Linux**。
 - b 在**自定义规范名称**文本框中，输入 **Customspecs**。
 - c 在**描述**文本框中，输入 **cpb_centos_63_x84 cloning with vRealize Automation**。
 - d 单击**下一步**。
- 6 设置计算机名称。
 - a 选择**使用虚拟机名称**。
 - b 在**域名**文本框中，输入要置备克隆计算机的域。
 - c 单击**下一步**。
- 7 配置时区设置。
- 8 单击**下一步**。
- 9 选择**对客户机操作系统使用标准网络设置，包括在所有网络接口上启用 DHCP**。

通过在 vRealize Automation 中创建和使用网络配置文件，架构管理员和基础架构架构师可以处理已置备计算机的网络设置。

- 10 按照提示输入其余的必填信息。
- 11 在**即将完成**页面上，检查所选项，然后单击**完成**。

结果

场景：准备导入 Dukes Bank vSphere 示例应用程序蓝图

作为 vCenter Server 管理员，您需要准备 vSphere CentOS 6.x Linux 模板和自定义规范，以便能够使用它们置备 vRealize Automation Dukes Bank 示例应用程序。

您需要确保模板支持示例应用程序的软件组件，因此请先在 Linux 参考机上安装客户机代理和软件引导程序代理，然后再将该参考机转换成模板并创建自定义规范。您需要停用参考机上的 SELinux，以确保您的模板支持在 Dukes Bank 示例应用程序中使用的 MySQL 的特定实施。

前提条件

- 标识或创建已安装 VMware Tools 的 CentOS 6.x Linux 参考机。有关创建虚拟机的信息，请参见 vSphere 文档。
- 必须连接到 vCenter Server 才能将虚拟机转换成模板。如果将 vSphere Client 直接连接到 vSphere ESXi 主机，则不能创建模板。

步骤

1 场景：为 Dukes Bank vSphere 示例应用程序准备参考机

您需要模板支持 Dukes 示例应用程序，因此必须在参考机上安装客户机代理和软件引导程序代理，以便 vRealize Automation 能够置备软件组件。要简化该过程，请下载并运行 vRealize Automation 脚本以便同时安装客户机代理和软件引导程序代理，而不是单独下载并安装这些软件包。

2 场景：将参考机转换为 Dukes Bank vSphere 应用程序的模板

在参考机上安装客户机代理和软件引导代理后，停用 SELinux 可确保模板支持在 Dukes Bank 示例应用程序中使用的特定 MySQL 实施。将参考机转换为可用来置备 Dukes Bank vSphere 示例应用程序的模板。

3 场景：为克隆 Dukes Bank vSphere 示例应用程序计算机创建自定义规范

您可以创建与 Dukes Bank 计算机模板配合使用的自定义规范。

结果

您已从参考机创建支持 vRealize Automation Dukes Bank 示例应用程序的模板和自定义规范。

场景：为 Dukes Bank vSphere 示例应用程序准备参考机

您需要模板支持 Dukes 示例应用程序，因此必须在参考机上安装客户机代理和软件引导程序代理，以便 vRealize Automation 能够置备软件组件。要简化该过程，请下载并运行 vRealize Automation 脚本以便同时安装客户机代理和软件引导程序代理，而不是单独下载并安装这些软件包。

步骤

- 1 以 root 用户身份登录到参考机。
- 2 从 vRealize Automation 设备下载安装脚本。

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

如果环境使用的是自签名证书，则您可能必须使用 `wget` 选项的 `--no-check-certificate` 选项。例如：

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

3 使 `prepare_vra_template.sh` 脚本可执行。

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

4 运行 `prepare_vra_template.sh` 安装程序脚本。

```
./prepare_vra_template.sh
```

有关非交互式选项和预期值的信息，您可以运行帮助命令 `./prepare_vra_template.sh --help`。

5 按照提示完成安装。

安装成功完成后，您会看到一条确认消息。如果在控制台中看到错误消息和日志，请解决这些错误并再次运行安装程序脚本。

结果

您已安装软件引导程序代理及其必备软件和客户机代理，确保 **Dukes Bank** 示例应用程序成功置备软件组件。此外，该脚本也已连接到 **Manager Service** 实例并下载 SSL 证书，以便在 **Manager Service** 与通过模板部署的计算机之间建立信任。与获取 **Manager Service** SSL 证书并将其手动安装在 `/usr/share/guagent/cert.pem` 中的参考机上的方式相比，这种方式的安全程度较差。如果要优先考虑安全性，则现在可以手动替换此证书。

场景：将参考机转换为 Dukes Bank vSphere 应用程序的模板

在参考机上安装客户机代理和软件引导代理后，停用 SELinux 可确保模板支持在 **Dukes Bank** 示例应用程序中使用的特定 MySQL 实施。将参考机转换为可用来置备 **Dukes Bank vSphere** 示例应用程序的模板。

将参考机转换成模板后，除非将模板转换回虚拟机，否则不能编辑或启动模板。

步骤

1 以 root 用户身份登录到参考机。

a 编辑 `/etc/selinux/config` 文件，以停用 SELinux。

```
SELINUX=disabled
```

如果不停用 SELinux，**Dukes Bank** 示例应用程序的 MySQL 软件组件可能无法按预期工作。

b 移除 `udev` 持久规则。

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

- c 使从此模板中克隆的计算机拥有自身的唯一标识符。

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

- d 如果已在安装软件引导程序代理之后重新引导或重新配置参考机，请重置该代理。

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

- e 关闭计算机电源。

```
shutdown -h now
```

- 2 以管理员身份登录到 vSphere Web Client。
- 3 右键单击参考机并选择**编辑设置**。
- 4 在**虚拟机名称**文本框中输入 **dukes_bank_template**。
- 5 如果参考机具有 CentOS 客户机操作系统，请从**客户机操作系统版本**下拉菜单中选择 **Red Hat Enterprise Linux 6 (64 位)**。

如果选择 CentOS，则模板和自定义规范可能无法按预期工作。

- 6 单击**确定**。
- 7 在 vSphere Web Client 中右键单击参考机，然后选择**模板 > 转换成模板**。

结果

vCenter Server 将把 dukes_bank_template 参考机标记为模板，并在“近期任务”窗格中显示任务。如果已将 vSphere 环境托管于 vRealize Automation，则系统会在下一个自动数据收集期间发现您的模板。如果尚未配置 vRealize Automation，则会在该过程中收集此模板。

场景：为克隆 Dukes Bank vSphere 示例应用程序计算机创建自定义规范

您可以创建与 Dukes Bank 计算机模板配合使用的自定义规范。

步骤

- 1 以管理员身份登录到 vSphere Web Client。
- 2 在主页中，单击**自定义规范管理器**以打开该向导。
- 3 单击**新建**图标。
- 4 指定属性。
 - a 从目标**虚拟机操作系统**下拉菜单中选择 **Linux**。
 - b 在**自定义规范名称**文本框中输入 **Customspecs_sample**。
 - c 在**描述**文本框中输入 **Dukes Bank customization spec**。
 - d 单击**下一步**。

- 5 设置计算机名称。
 - a 选择**使用虚拟机名称**。
 - b 在**域名**文本框中，输入要置备 Dukes Bank 示例应用程序的域。
 - c 单击**下一步**。
- 6 配置时区设置。
- 7 单击**下一步**。
- 8 选择**对客户机操作系统使用标准网络设置，包括在所有网络接口上启用 DHCP**。

通过在 vRealize Automation 中创建和使用网络配置文件，架构管理员和基础架构架构师可以处理已置备计算机的网络设置。

- 9 按照提示输入其余的必填信息。
- 10 在**即将完成**页面上，检查所选项，然后单击**完成**。

结果

您已创建可用于置备 Dukes Bank 示例应用程序的模板和自定义规范。

后续步骤

- 1 创建外部网络配置文件以提供网关和 IP 地址范围。请参见[使用第三方 IPAM 提供程序创建外部网络配置文件](#)。
- 2 将外部网络配置文件映射到 vSphere 预留。请参见[为 Hyper-V、KVM、SCVMM、vSphere 或 XenServer 创建预留](#)。如果没有外部网络配置文件，示例应用程序无法成功置备。
- 3 将 Dukes Bank 示例应用程序导入到环境中。请参见[场景：导入 Dukes Bank vSphere 示例应用程序并配置您的环境](#)。

为蓝图置备准备租户和资源

2

您可以配置多个租户环境，使每个环境拥有他们自己的用户组和对资源的唯一访问权限，并使资源受 vRealize Automation 管理。

本章讨论了以下主题：

- [配置租户设置](#)
- [配置资源](#)
- [通知和委派的用户首选项](#)

配置租户设置

租户管理员负责配置用户身份验证等租户设置，并管理用户角色和业务组。系统管理员和租户管理员负责配置用于处理通知的电子邮件服务器等选项以及 vRealize Automation 控制台的品牌。

您可以使用“配置租户设置对照表”来查看对配置租户所需执行的一系列步骤的概述。

表 2-1. 配置租户设置对照表

任务	vRealize Automation 角色	详细信息
<input type="checkbox"/> 创建本地用户帐户并分配租户管理员。	系统管理员	配置对默认租户的访问权限
<input type="checkbox"/> 配置身份目录管理以设置租户身份管理和访问控制设置。	租户管理员	选择身份目录管理配置选项
<input type="checkbox"/> 创建业务组和自定义组，并授予用户对 vRealize Automation 控制台的访问权限。	租户管理员	配置组 and 用户角色
<input type="checkbox"/> (可选) 创建其他租户，以便用户可以访问完成其工作分配所需的相关应用程序和资源。	系统管理员	创建其他租户
<input type="checkbox"/> (可选) 在 vRealize Automation 控制台的租户登录和应用程序页面上配置自定义品牌。	<ul style="list-style-type: none">■ 系统管理员■ 租户管理员	配置自定义品牌
<input type="checkbox"/> (可选) 配置 vRealize Automation，以便发生特定事件时，向用户发送通知。	<ul style="list-style-type: none">■ 系统管理员■ 租户管理员	用于配置通知的对照表
<input type="checkbox"/> (可选) 配置 vRealize Orchestrator，以支持 XaaS 和其他可扩展性。	<ul style="list-style-type: none">■ 系统管理员■ 租户管理员	配置 vRealize Orchestrator

表 2-1. 配置租户设置对照表（续）

任务	vRealize Automation 角色	详细信息
<input type="checkbox"/> （可选）创建一个自定义远程桌面协议文件。使用该文件，IaaS 架构师可在蓝图中配置 RDP 设置。	系统管理员	为置备的计算机创建自定义 RDP 文件以支持 RDP 连接
<input type="checkbox"/> （可选）定义一些数据中心位置，以便架构管理员和 IaaS 架构师可以用来支持用户在请求计算机时选择相应的置备位置。	系统管理员	有关添加数据中心位置的示例，请参见 场景：为跨区域部署添加数据中心位置 。

选择身份目录管理配置选项

您可以使用 vRealize Automation “身份目录管理” 功能配置符合用户身份验证要求的 Active Directory 链接。

身份目录管理提供了多个选项来支持高度自定义的用户身份验证。

表 2-2. 选择身份目录管理配置选项

配置选项	步骤
配置指向 Active Directory 的链接。	<ol style="list-style-type: none"> 配置指向 Active Directory 的链接。请参见配置通过 LDAP/IWA 链路访问的 Active Directory。 如果您为 vRealize Automation 配置了高可用性，请参见配置身份目录管理以实现高可用性。
（可选）通过配置与 Active Directory 联合服务的双向集成，增强基于用户 ID 和密码的目录链接的安全性。	在 vRealize Automation 与 Active Directory 之间配置双向信任关系
（可选）将用户和组添加到现有 Active Directory 链接。	将用户或组添加到 Active Directory 连接。
（可选）编辑默认策略，以便为 Active Directory 链接应用自定义规则。	管理用户访问策略。
（可选）配置网络范围以限制可供用户登录系统的 IP 地址，并管理登录限制（超时、锁定之前允许尝试的登录次数）。	添加或编辑网络范围。

身份目录管理概览

租户管理员可以使用 vRealize Automation 应用程序控制台上的身份目录管理选项配置租户身份管理并访问控制设置。

您可以从[管理 > 身份目录管理](#)选项卡中管理以下设置。

表 2-3. 身份目录管理设置

设置	描述
目录	<p>使用“目录”页面，您可以创建和管理 Active Directory 链接，以支持 vRealize Automation 租户用户身份验证和授权。您可以创建一个或多个目录，然后将这些目录与您的 Active Directory 部署相同步。此页面显示同步到目录的组和用户数量以及上次同步时间。您可以单击立即同步来手动启动目录同步。</p> <p>请参见使用身份目录管理创建 Active Directory 链接。</p> <p>当您依次单击目录和同步设置按钮时，可以编辑同步设置、导航“身份提供程序”页面并查看同步日志。</p> <p>在目录同步设置页面中，您可以计划同步频率、查看与此目录关联的域的列表、更改映射的属性列表、更新同步的用户和组列表，以及设置保护措施目标。</p>
连接器	<p>“连接器”页面列出了为企业网络部署的连接器。连接器可在 Active Directory 和身份目录管理服务之间同步用户和组数据，并且当连接器用作身份提供程序时，还可验证用户身份以允许其访问服务。默认情况下，每个 vRealize Automation 设备均包含一个连接器。请参见管理连接器和连接器集群。</p>
用户属性	<p>“用户属性”页面列出了在目录中同步的默认用户属性，您可以添加其他属性以映射到 Active Directory 属性。请参见选择要与目录同步的属性。</p>
网络范围	<p>该页面列出了为系统配置的网络范围。您可以配置网络范围，以便允许用户通过这些 IP 地址进行访问。您可以添加其他网络范围，也可以编辑现有的网络范围。请参见添加或编辑网络范围。</p>
身份提供程序	<p>“身份提供程序”页面列出了系统上可用的身份提供程序。vRealize Automation 系统包含一个充当默认身份提供程序的连接器，足以满足许多用户的需求。您可以添加第三方身份提供程序实例，或组合使用连接器实例和第三方身份提供程序实例。</p> <p>请参见配置第三方身份提供程序连接。</p>
策略	<p>“策略”页面列出了默认访问策略，以及您创建的其他任何 Web 应用程序访问策略。策略是一组规则，用于指定用户要访问其应用程序门户或启动已为其启用的 Web 应用程序所必须满足的条件。默认策略应适用于大多数 vRealize Automation 部署，但您可以根据需要进行编辑。请参见管理用户访问策略。</p>

与 Active Directory 有关的重要概念

要了解 Directories Management 如何与您的 Active Directory 环境相集成，必须掌握一些与 Active Directory 有关的概念。

连接器

连接器是服务的一个组件，可执行以下功能。

- 在 Active Directory 和服务之间同步用户和组数据。
- 当用作身份提供程序时，还可用于验证用户身份以允许其访问服务。

连接器是默认身份提供程序。有关 连接器 支持的身份验证方法，请参阅《VMware Identity Manager 管理指南》。您还可以使用支持 **SAML 2.0** 协议的第三方身份提供程序。如果根据您的企业安全策略最好是使用第三方身份提供程序，则可使用第三方身份提供程序来提供连接器不支持或连接器支持的身份验证类型。

注 即便您使用第三方身份提供程序，您也必须配置连接器以同步用户和组数据。

目录

Directories Management 服务有其自己的目录概念，该服务中的目录可使用 Active Directory 属性和参数来定义用户和组。您可以创建一个或多个目录，然后将这些目录与您的 Active Directory 部署相同步。您可以在服务中创建以下目录类型。

- 通过 LDAP 访问的 Active Directory。如果您打算连接到单个 Active Directory 域环境，可创建此目录类型。对于通过 LDAP 访问的 Active Directory 目录类型，连接器将使用简单绑定身份验证绑定到 Active Directory。
- Active Directory（集成 Windows 身份验证）。如果您打算连接到多域或多林 Active Directory 环境，可创建此目录类型。连接器将使用集成 Windows 身份验证绑定到 Active Directory。

根据您的 Active Directory 环境（如单域或多域）以及各域之间使用的信任类型的不同，您可创建的目录的类型和数量也会有所差异。在多数环境中，您可以创建一个目录。

服务不可直接访问 Active Directory。只有连接器才拥有 Active Directory 的直接访问权限。因此，您需要将在服务中创建的每个目录都与连接器实例相关联。

工作线程

在将目录与连接器实例相关联时，连接器会为关联的目录创建一个分区（称为“工作线程”）。一个连接器实例可以有多个关联的工作线程。每个工作线程都充当一个身份提供程序。您可以为每个工作线程分别定义和配置身份验证方法。

连接器通过一个或多个工作线程在 Active Directory 和服务之间同步用户和组数据。

同一连接器实例不能有两个集成 Windows 身份验证类型的工作线程。

Active Directory 环境

您可以将服务与 Active Directory 环境相集成，该环境可以包含单个 Active Directory 域、单个 Active Directory 林中的多个域或多个 Active Directory 林之间的多个域。

单个 Active Directory 域环境

单个 Active Directory 部署允许您同步单个 Active Directory 域中的用户和组。

请参见[配置通过 LDAP/IWA 链路访问的 Active Directory](#)。对于此环境，在向服务中添加目录时，请选择“通过 LDAP 访问的 Active Directory”选项。

多域、单林 Active Directory 环境

多域、单林 Active Directory 部署允许您同步单林中多个 Active Directory 域的用户和组。

对于此 Active Directory 环境，您可以将服务配置为单个 Active Directory（集成 Windows 身份验证）目录类型，或者，也可以配置为通过 LDAP 访问的 Active Directory 目录类型（通过全局目录选项进行配置）。

- 建议的选项是创建单个 Active Directory（集成 Windows 身份验证）目录类型。

请参见[配置通过 LDAP/IWA 链路访问的 Active Directory](#)。在为此环境添加目录时，请选择“Active Directory（集成 Windows 身份验证）”选项。

有信任关系的多林 Active Directory 环境

有信任关系的多林 Active Directory 部署允许您同步域间存在双向信任的林中多个 Active Directory 域的用户和组。

请参见[配置通过 LDAP/IWA 链路访问的 Active Directory](#)。在为此环境添加目录时，请选择“Active Directory (集成 Windows 身份验证)”选项。

无信任关系的多林 Active Directory 环境

无信任关系的多林 Active Directory 部署允许您同步域间不存在信任关系的林中多个 Active Directory 域的用户和组。对于此环境，您需要在服务中创建多个目录，每个林使用一个目录。

请参见[配置通过 LDAP/IWA 链路访问的 Active Directory](#)。您在服务中创建的目录类型取决于林。对于具有多个域的林，请选择“Active Directory (集成 Windows 身份验证)”选项。对于具有单个域的林，请选择“通过 LDAP 访问的 Active Directory”选项。

使用身份目录管理创建 Active Directory 链接

创建 vRealize Automation 租户之后，您必须以租户管理员身份登录到系统控制台，并创建 Active Directory 链接以支持用户身份验证。

使用身份目录管理配置 Active Directory 连接时，有三个 Active Directory 通信协议选项可供选择。

- 通过 LDAP 访问的 Active Directory - “通过 LDAP 访问的 Active Directory”协议默认情况下支持 DNS 服务位置查找。
- Active Directory (集成的 Windows 身份验证) - 使用 Active Directory (集成的 Windows 身份验证)，您可以配置要加入的域。“通过 LDAP 访问的 Active Directory”适合单域部署。对所有多域和多林部署使用“Active Directory (集成 Windows 身份验证)”。
- OpenLDAP - 可以使用开源版本的 LDAP 为身份目录管理用户身份验证提供支持。

选择通信协议并配置 Active Directory 链接之后，您可以指定要用于 Active Directory 配置的域，然后选择要与指定配置同步的用户和组。

配置通过 LDAP/IWA 链路访问的 Active Directory

您可以使用 Directories Management 功能将通过 LDAP/IWA 链路访问的 Active Directory 配置为支持用户身份验证，以便针对所有租户将指向 Active Directory 的链接配置为支持用户身份验证，并选择要与 Directories Management 目录同步的用户和组。

有关将 OpenLDAP 与身份目录管理结合使用的信息，请参见[配置 OpenLDAP 目录连接](#)。

对于 Active Directory (集成 Windows 身份验证)，如果您配置了多林 Active Directory，并且“域本地”组包含来自不同林中的域的成员，请确保将绑定用户添加到“域本地”组所在的域的“管理员”组中。如果该操作失败，“域本地”组中将缺少这些成员。

注 首先为默认租户配置 Active Directory IWA 目录，然后可以将其添加到其他租户。

前提条件

- 在“用户属性”页面上选择必需的默认属性并添加其他属性。请参见[选择要与目录同步的属性](#)。

- 要从 Active Directory 同步的 Active Directory 组和用户的列表。
- 如果 Active Directory 要求通过 SSL 或 STARTTLS 访问，则需要使用 Active Directory 域控制器的根 CA 证书。
- 以租户管理员身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 目录**。
- 2 单击**添加目录**，然后选择**添加通过 LDAP/IWA 访问的 Active Directory**。
- 3 在“添加目录”页面上，在**目录名称**文本框中指定 Active Directory 服务器的 IP 地址。
- 4 使用**目录名称**文本框下的单选按钮，选择相应的 Active Directory 通信协议。

选项	描述
Windows 身份验证	选择 Active Directory (集成 Windows 身份验证) 。对于 Active Directory (集成 Windows 身份验证)，必需的信息包括域的绑定用户 UPN 地址和密码。
LDAP	选择 通过 LDAP 访问的 Active Directory 。对于通过 LDAP 访问的 Active Directory，所需的信息包括基本 DN、绑定 DN 以及绑定 DN 密码。

- 5 在“目录同步和身份验证”部分配置用于将用户从 Active Directory 同步到 VMware Directories Management 目录的连接器。

选项	描述
同步连接器	选择适合用于系统的连接器。每个 vRealize Automation 设备均包含一个默认连接器。如需有关选择适当连接器的帮助，请咨询系统管理员。
身份验证	单击相应单选按钮，指示所选连接器是否也执行身份验证。 如果使用 Active Directory (集成 Windows 身份验证) 与第三方身份提供程序对用户进行身份验证，请单击 否 。在配置 Active Directory 连接以同步用户和组后，请使用“身份提供程序”页面添加第三方身份提供程序以进行身份验证。 有关使用 PasswordIpddAdapter、SecurIDAdapter 和 RadiusAuthAdapter 等身份验证适配器的信息，请参见《VMware Identity Manager 管理指南》。
目录搜索属性	选择包含用户名的合适帐户属性。VMware 建议使用 sAMAccount 属性，而不是 userPrincipleName。如果使用 userPrincipleName 执行同步操作，则与需要提供用户名的第二方和第三方软件的集成可能无法正确运行。 注 使用全局目录（通过在“服务器位置”区域中选择 此目录具有全局目录 复选框指示这一点）时，如果选择 sAMAccountName，用户将无法登录。

- 6 如果选择“通过 LDAP 访问的 Active Directory”，请在“服务器位置”文本框中输入适当的信息；或者，如果选择“Active Directory (集成 Windows 身份验证)”，请在“加入域详细信息”文本框中输入适当的信息。

选项	描述
服务器位置 - 选择“通过 LDAP 访问的 Active Directory”时显示	<ul style="list-style-type: none"> 如果要使用 DNS 服务位置查找 Active Directory 域，请选中该目录支持 DNS 服务位置复选框。 <p>注 如果选择此选项，您无法将端口分配更改为 636。</p> <p>系统会随目录创建 <code>domain_krb.properties</code> 文件，并在其中自动填充域控制器列表。请参见关于域控制器选择。</p> <p>如果 Active Directory 要求进行 STARTTLS 加密，请选中“证书”部分的此目录要求所有连接都使用 STARTTLS复选框，然后将 Active Directory 根 CA 证书复制并粘贴到 SSL 证书字段。</p> <ul style="list-style-type: none"> 如果指定的 Active Directory 不使用 DNS 服务位置查找，请在“服务器位置”字段中取消选中该目录支持 DNS 服务位置旁边的复选框，并在相应文本框中输入 Active Directory 服务器的主机名和端口号。 <p>如果关联的 Active Directory 使用全局目录，请选择此目录具有全局目录复选框。全局目录包含多域 Active Directory 林内每个域中所有对象的表示形式。</p> <p>要将目录配置为全局目录，请参见 Active Directory 环境 中的“多域、单林 Active Directory 环境”部分。</p> <p>如果 Active Directory 需要通过 SSL 进行访问，请选中“证书”标题下的此目录要求所有连接使用 SSL复选框并提供 Active Directory SSL 证书。</p> <p>如果选择此选项，则自动使用端口 636，并且无法进行更改。</p> <p>请确保证书采用的是 PEM 格式，并且包含 BEGIN CERTIFICATE 和 END CERTIFICATE 行。</p>
加入域详细信息 - 选择“Active Directory (集成 Windows 身份验证)”时显示	<p>在域名、域管理员用户名和域管理员密码文本框中，输入相应的凭据。</p> <p>如果 Active Directory 要求进行 STARTTLS 加密，请选中“证书”部分的此目录要求所有连接都使用 STARTTLS复选框，然后将 Active Directory 根 CA 证书复制并粘贴到 SSL 证书字段。</p> <p>请确保证书采用的是 PEM 格式，并且包含 BEGIN CERTIFICATE 和 END CERTIFICATE 行。</p> <p>如果该目录使用多个域，请添加所有域的根 CA 证书（一次添加一个证书）。</p> <p>注 如果 Active Directory 要求使用 STARTTLS，但您没有提供证书，则无法创建目录。</p>

- 7 在“绑定用户详细信息”部分，输入相应的凭据，以便执行目录同步。

对于“通过 LDAP 访问的 Active Directory”：

选项	描述
基本 DN	输入搜索基本识别名。例如， <code>cn=users,dc=corp,dc=local</code> 。
绑定 DN	输入绑定识别名。例如， <code>cn=fritz infra,cn=users,dc=corp,dc=local</code>

对于“Active Directory (集成 Windows 身份验证)”：

选项	描述
绑定用户 UPN	输入可对域进行身份验证的用户的“用户主体名称”。例如，UserName@example.com。
绑定 DN 密码	输入绑定用户密码。

- 8 单击 **测试连接** 以测试与已配置目录的连接。

如果选择“Active Directory (集成 Windows 身份验证)”，将不显示此按钮。

- 9 单击 **保存并执行下一步**。

此时将显示“选择域”页面，其中包含域的列表。

- 10 检查并更新为 Active Directory 连接列出的域。

- 对于“Active Directory (集成 Windows 身份验证)”，可选择应与此 Active Directory 连接关联的域。
- 对于“通过 LDAP 访问的 Active Directory”，所列的可用域均带有一个选中标记。

注 如果在创建目录后添加信任域，则服务不会自动检测新的信任域。要使服务能够检测信任域，连接器 必须退出域，然后再重新加入。当 连接器 重新加入域时，信任域便会出现在列表中。

- 11 单击 **下一步**。

- 12 确认 Directories Management 目录属性名称已映射到正确的 Active Directory 属性。

如果目录属性名称未正确映射，请从下拉菜单中选择正确的 Active Directory 属性。

- 13 单击 **下一步**。

- 14 单击 **+** 以选择您要从 Active Directory 同步到目录的组。

从 Active Directory 添加组时，如果该组中的成员不在“用户”列表中，则表明已添加这些成员。在同步组时，不会同步没有将“域用户”作为 Active Directory 中的主要组的任何用户。

注 Directories Management 用户身份验证系统在添加组和用户时从 Active Directory 导入数据，系统的速度受 Active Directory 功能限制。因此，导入操作可能需要很长时间，具体取决于要添加的组和用户数量。为了最大程度地减少潜在的延迟或问题，请将组和用户数量限制为 vRealize Automation 操作所需的数量。


如果系统性能降低或者如果出现错误，请关闭所有不需要的应用程序并确保系统已为 Active Directory 分配相应的内存。如果问题仍然存在，请根据需要增加 Active Directory 内存分配。对于拥有大量用户和组的系统，您可能需要将 Active Directory 内存分配增加至多达 24 GB。

- 15 单击 **下一步**。

16 单击  以添加其他用户。

相应的值如下：

- 单个用户：CN=*username*,CN=Users,OU=Users,DC=myCorp,DC=com
- 多个用户：OU=Users,OU=myUnit,DC=myCorp,DC=com

要排除用户，请单击  创建一个筛选器以排除某些类型的用户。您可以选择要作为筛选条件的用户属性、查询规则和价值。

17 单击下一步。

18 查看该页面以了解将要同步到目录的用户和组数量。

如果您要对用户和组进行更改，请单击“编辑”链接。

注 确保指定先前已在“基本 DN”下指定的用户 DN。如果用户 DN 在“基本 DN”之外，则该 DN 中的用户将会同步，但这些用户无法登录。

19 单击 **推送到 Workspace** 以开始与目录同步。

结果

将完成到 Active Directory 的连接，并将选定的用户和组添加到目录中。您现在可以通过选择**管理 > 用户和组 > 目录用户和组**，将用户和组分配给相应的 vRealize Automation 角色。有关详细信息，请参见[目录用户或组分配角色](#)。

后续步骤

如果您的 vRealize Automation 环境已配置高可用性，则必须专门为身份目录管理配置高可用性。请参见[配置身份目录管理以实现高可用性](#)。

- 设置身份验证方法。将用户和组同步到目录后，如果连接器还用于进行身份验证，则您可以在连接器上设置其他身份验证方法。如果身份验证的身份提供程序是第三方，可在连接器中配置该身份提供程序。
- 查看默认访问策略。默认访问策略配置为允许所有网络范围中的所有设备访问 Web 浏览器（会话超时设置为 8 小时）或访问客户端应用程序（会话超时设置为 2160 小时（90 天））。您可以更改默认访问策略，还可以在将 Web 应用程序添加到目录中时创建新的访问策略。
- 将自定义品牌标识应用于管理控制台、用户门户页面和登录屏幕。

配置 OpenLDAP 目录连接

您可以使用身份目录管理配置 OpenLDAP 目录连接。

尽管有几种不同的 LDAP 协议，但 OpenLDAP 是唯一经过测试和批准可用于 vRealize Automation 身份目录管理的 LDAP 协议。

要集成 LDAP 目录，您需要创建相应的 Directories Management 目录，并将用户和组从 LDAP 目录同步到 Directories Management 目录。您可以设置定期同步计划以进行后续更新。

您也可以选择要为用户同步的 LDAP 属性，然后将这些属性映射到 Directories Management 属性。

您的 LDAP 目录配置可以基于默认架构，或者您也可以创建自定义架构。您还可以定义自定义属性。为了让 Directories Management 能够查询您的 LDAP 目录，从而获取用户或组对象，您需要提供适用于 LDAP 目录的 LDAP 搜索筛选器和属性名称。

具体来说，您需要提供以下信息。

- 用于获取组、用户和绑定用户的 LDAP 搜索筛选器
- 用于组成员资格、UUID 和标识名的 LDAP 属性名称

注 身份目录管理对 LDAP 查询默认使用页面大小 1500。如果配置 OpenLDAP 目录连接，那么您必须对 OpenLDAP 启用简单页面结果控制扩展来限制显示的结果数量。无法使用此扩展可能会导致用户和组同步错误。

前提条件

- 查看“用户属性”页面中的配置，并添加任何其他要同步的属性。在创建目录时，您会将 Directories Management 属性映射到 LDAP 目录属性。系统将为目录中的用户同步这些属性。

注 更改用户属性时，请考虑此操作对服务中的其他目录的影响。如果打算同时添加 Active Directory 和 LDAP 目录，请确保不要将任何属性标记为“必需”，但 **userName** 除外。“用户属性”页面中的设置适用于服务中的所有目录。如果将某个属性标记为“必需”，则不具备该属性的用户将不会被同步到 Directories Management 服务。

- 绑定 DN 用户帐户。建议使用具有不过期密码的绑定 DN 用户帐户。
- 在您的 LDAP 目录中，用户和组的 UUID 必须为纯文本格式。
- 在您的 LDAP 目录中，所有用户和组都必须存在 domain 属性。

在创建 Directories Management 目录时，您会将此属性映射到 Directories Management **domain** 属性。

- 用户名不得包含空格。如果用户名包含空格，虽然可以同步用户，但用户无法获得授权。
- 如果使用证书身份验证，则用户必须具有 **userPrincipalName** 和电子邮件地址属性值。

步骤

- 1 选择 **管理 > 身份目录管理 > 目录**。
- 2 单击 **添加目录**，然后选择 **添加 LDAP 目录**。

3 在“添加 LDAP 目录”页面中输入必需的信息。

选项	描述
目录名称	输入 Directories Management 目录的名称。
目录同步和身份验证	<p>a 在同步连接器字段中，选择您要用于将 LDAP 目录中的用户和组同步到 Directories Management 目录的连接器。</p> <p>默认情况下，连接器组件始终可用于 Directories Management 服务。将在下拉列表中显示该连接器。如果您安装多个高可用性 Directories Management 设备，每个设备的连接器组件显示在列表中。</p> <p>您无需为 LDAP 目录使用单独的连接器。一个连接器可以支持多个目录，而不管它们是 Active Directory 还是 LDAP 目录。</p> <p>b 在身份验证字段中，如果您要使用该 LDAP 目录对用户进行身份验证，请选择是。</p> <p>如果您要使用第三方身份提供程序对用户进行身份验证，请选择否。在添加目录连接以同步用户和组后，请转到管理 > 身份目录管理 > 身份提供程序页面，以添加用于身份验证的第三方身份提供程序。</p> <p>c 对于大多数配置，请使默认值自定义在目录搜索属性文本框中保持选定状态。在自定义目录搜索属性字段中，指定要对用户名和组名称使用的 LDAP 目录属性。此属性可唯一标识 LDAP 服务器中的实体，例如，用户和组。例如，cn。</p> <p>d 如果您希望对 Active Directory 使用 DNS 服务位置查找，请进行以下选择。</p> <ul style="list-style-type: none"> ■ 在“服务器位置”部分中，选中此目录支持 DNS 服务位置复选框。 <p>身份目录管理会查找并使用最佳的域控制器。如果您不希望使用优化的域控制器选择，请跳过步骤 e。</p> <ul style="list-style-type: none"> ■ 如果 Active Directory 需要使用 STARTTLS 加密，请在“证书”部分中选中此目录要求所有连接都使用 SSL复选框，然后复制 Active Directory 根 CA 证书并将其粘贴到“SSL 证书”文本框中。 <p>确保该证书采用 PEM 格式，并包含“BEGIN CERTIFICATE”和“END CERTIFICATE”行。</p> <p>注 如果 Active Directory 要求使用 STARTTLS，但您没有提供证书，则无法创建目录。</p> <p>e 如果您不希望对 Active Directory 使用 DNS 服务位置查找，请进行以下选择。</p> <ul style="list-style-type: none"> ■ 在“服务器位置”部分中，确认未选中此目录支持 DNS 服务位置复选框，并输入 Active Directory 服务器主机名和端口号。要将目录配置为全局目录，请参见 Active Directory 环境 中的“多域、单林 Active Directory 环境”部分。 ■ 如果 Active Directory 要求通过 SSL 访问，请选中“证书”部分的此目录要求所有连接都使用 SSL复选框，然后将 Active Directory 根 CA 证书复制并粘贴到“SSL 证书”字段。 <p>确保该证书采用 PEM 格式，并包含“BEGIN CERTIFICATE”和“END CERTIFICATE”行。</p> <p>注 如果 Active Directory 要求使用 STARTTLS，但您没有提供证书，则无法创建目录。</p>
服务器位置	<p>输入 LDAP 目录服务器主机和端口号。对于服务器主机，您可以指定完全限定域名或 IP 地址。例如，myLDAPserver.example.com 或 100.00.00.0。</p> <p>如果您的服务器群集位于负载均衡器后面，请改为输入负载均衡器信息。</p>

选项	描述
LDAP 配置	<p>指定 Directories Management 可用于查询 LDAP 目录的 LDAP 搜索筛选器和属性。系统会根据核心 LDAP 架构提供默认值。</p> <p>筛选器查询</p> <ul style="list-style-type: none"> ■ 组: 用于获取组对象的搜索筛选器。 <p>例如: (objectClass=group)</p> <ul style="list-style-type: none"> ■ 绑定用户: 用于获取绑定用户对象 (即可以绑定到目录的用户) 的搜索筛选器。 <p>例如: (objectClass=person)</p> <ul style="list-style-type: none"> ■ 用户: 用于获取要同步的用户的搜索筛选器。 <p>例如: (&(objectClass=user)(objectCategory=person))</p> <p>属性</p> <ul style="list-style-type: none"> ■ 成员资格: 在您的 LDAP 目录中用于定义组成员的属性。 <p>例如: member</p> <ul style="list-style-type: none"> ■ 对象 UUID: 在您的 LDAP 目录中用于定义用户或组的 UUID 的属性。 <p>例如: entryUUID</p> <ul style="list-style-type: none"> ■ 标识名: 在您的 LDAP 目录中对用户或组的标识名使用的属性。 <p>例如: entryDN</p>
证书	<p>如果您的 LDAP 目录需要通过 SSL 访问, 请选中此目录要求所有连接都使用 SSL 复选框。然后, 将 LDAP 目录服务器的根 CA SSL 证书复制并粘贴到 SSL 证书 文本框中。请确保证书采用的是 PEM 格式, 并且包含 “BEGIN CERTIFICATE” 和 “END CERTIFICATE” 行。</p> <p>如果目录有多个域, 则逐个添加所有域的根 CA 证书。</p> <p>最后, 请确保在页面的 “服务器位置” 部分中的服务器端口字段中指定的端口号正确。</p>
绑定用户详细信息	<p>基本 DN: 输入从中开始搜索的 DN。例如, cn=users,dc=example,dc=com</p> <p>所有适用的用户均必须位于 “基本 DN” 下。如果特定用户不位于 “基本 DN” 下, 即使该用户属于 “基本 DN” 下的组, 也无法登录。</p> <p>绑定 DN: 输入用于绑定到 LDAP 目录的 DN。您还可以输入用户名, 但 DN 更适用于大多数部署。</p> <hr/> <p>注 建议使用具有不过期密码的绑定 DN 用户帐户。</p> <hr/> <p>绑定 DN 密码: 输入绑定 DN 用户的密码。</p>

- 4 要测试与 LDAP 目录服务器的连接, 请单击**测试连接**。

如果连接不成功, 请检查您输入的信息并进行相应的更改。

- 5 单击**保存并执行下一步**。

- 6 验证是否在 “选择域” 页面中选择了正确的域, 然后单击**下一步**。

- 7 在 “映射属性” 页面中, 验证 Directories Management 属性是否映射到正确的 LDAP 属性。
- 系统将为用户同步这些属性。

重要事项 您必须指定 **domain** 属性的映射。

您可以将属性添加到 “用户属性” 页面的列表。

8 单击下一步。**9 单击 +，在“选择要同步的组 (用户)”页面上，选择您要从 LDAP 目录同步到 Directories Management 目录的组。**

如果您的 LDAP 目录中有多个同名的组，则必须在组页面中为这些组指定唯一的名称。

从 Active Directory 添加组时，如果该组中的成员不在“用户”列表中，则表明已添加这些成员。在同步组时，不会同步没有将“域用户”作为 Active Directory 中的主要组的任何用户。

默认情况下，**同步嵌套的组成员**选项处于启用状态。启用此选项后，将会同步直属于所选组的所有用户以及属于该组下的嵌套组的所有用户。请注意，不会同步嵌套组；只会同步属于嵌套组的用户。在 Directories Management 目录中，这些用户将显示为您选择进行同步的顶级组的成员。实际上，选定组下的层次结构将会变平，并且所有级别的用户都会在 Directories Management 中显示为选定组的成员。

如果停用此选项，则在指定要同步的组时，将会同步直属于该组的所有用户。属于该组下的嵌套组的用户则不会被同步。在大型目录配置中，遍历组树会耗用大量资源和时间，对于这类配置，禁用此选项会非常有用。如果停用此选项，请确保选择要同步其用户的所有组。

注 Directories Management 用户身份验证系统在添加组和用户时从 Active Directory 导入数据，系统的速度受 Active Directory 功能限制。因此，导入操作可能需要很长时间，具体取决于要添加的组和用户数量。为了最大程度地减少潜在的延迟或问题，请将组和用户数量限制为 vRealize Automation 操作所需的数量。

如果系统性能降低或者如果出现错误，请关闭所有不需要的应用程序并确保系统已为身份目录管理分配相应的内存。如果问题仍然存在，请根据需要增加身份目录管理内存分配。对于拥有大量用户和组的系统，您可能需要将身份目录管理内存分配增加至多达 24 GB。

10 单击下一步。**11 单击 + 以添加其他用户。例如，输入 CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com。**

您可以在此处添加组织单位以及各个用户。

您可以创建一个筛选器以排除某些类型的用户。您可以选择要作为筛选条件的用户属性、查询规则和价值。

12 单击下一步。**13 查看该页面，了解将同步到目录的用户和组数量以及默认同步计划。**

要对用户和组或同步频率进行更改，请单击**编辑**链接。

14 单击同步目录以开始目录同步。**结果**

此时会建立与 LDAP 目录的连接，并且会将用户和组从 LDAP 目录同步到 Directories Management 目录。

您现在可以通过选择**管理 > 用户和组 > 目录用户和组**，将用户和组分配给相应的 vRealize Automation 角色。有关详细信息，请参见[为目录用户或组分配角色](#)。

LDAP 目录集成的限制

以下几项重要限制与身份目录管理中的 LDAP 目录集成相关。

- 您只能集成单域 LDAP 目录环境。
 - 要从 LDAP 目录中集成多个域，您需要为每个域创建一个额外的 Directories Management 目录。
- LDAP 目录类型的 Directories Management 目录不支持以下身份验证方法。
 - Kerberos 身份验证
 - RSA 自适应身份验证
 - ADFS 作为第三方身份提供程序
 - SecurID
 - 使用 Vasco 和短信通行码服务器进行的 Radius 身份验证
- 您无法加入 LDAP 域。
- LDAP 目录类型的 Directories Management 目录不支持与 View 或 Citrix 发布的资源相集成。
- 用户名不得包含空格。如果用户名包含空格，虽然可以同步用户，但用户无法获得授权。
- 如果打算同时添加 Active Directory 和 LDAP 目录，请确保不要将“用户属性”页面中的任何属性标记为“必需”，但 `userName` 除外，此属性可以标记为“必需”。“用户属性”页面中的设置适用于服务中的所有目录。如果将某个属性标记为“必需”，则不具备该属性的用户将不会被同步到 Directories Management 服务。
- 如果您的 LDAP 目录中有多个同名的组，则必须在 Directories Management 服务中为这些组指定唯一的名称。您可以在选择要同步的组时指定名称。
- 允许用户重置过期密码的选项不可用。
- 不支持 `domain_krb.properties` 文件。

配置身份目录管理以实现高可用性

您可以使用身份目录管理在 vRealize Automation 中配置高可用性 Active Directory 连接。

每个 vRealize Automation 设备均包含一个支持用户身份验证的连接器，但通常只会配置一个连接器来执行目录同步。选择哪个连接器作为同步连接器并不重要。要支持身份目录管理高可用性，必须手动配置与第二个 vRealize Automation 设备对应的另一个连接器，该连接器会连接到身份提供程序并指向同一个 Active Directory。在此配置中，如果一个设备出现故障，则另一个设备将接管用户身份验证。

在高可用性环境中，所有节点均必须提供一组相同的 Active Directory、用户、身份验证方法等。要实现这一点，最直接的方法是通过将负载平衡器主机设置为身份提供程序主机，将身份提供程序升级到群集。在此配置中，所有身份验证请求均会指向负载平衡器，稍后负载平衡器将根据需要将请求转发给任一连接器。

连接器还用于用户同步。但只配置一个连接器来执行目录同步。已同步的用户将保存到设备数据库，所有群集节点均可读取该设备数据库。如果负责执行目录同步的连接器失败，目录同步将停止工作。要恢复工作，租户管理员需要使用 vRealize Automation UI 来手动提示另一个连接器执行目录同步。请参见[在辅助连接器上启用目录同步](#)。

有关使用连接器的详细信息，请参见[管理连接器和连接器集群](#)。

前提条件

- 为 vRealize Automation 部署至少配置两个 vRealize Automation 设备实例。
- 在包含两个 vRealize Automation 设备实例的单个域中安装在 Enterprise 模式下运行的 vRealize Automation。
- 安装和配置要与 vRealize Automation 部署配合使用的相应负载均衡器。
- 使用随安装的 vRealize Automation 设备实例提供的连接器之一配置租户和身份目录管理。有关租户配置的信息，请参见[配置租户设置](#)。

步骤

- 1 以租户管理员身份登录到 vRealize Automation 部署的负载均衡器。
负载均衡器 URL 为 `<load balancer address>/vcac/org/tenant_name`。
- 2 选择**管理 > 身份目录管理 > 身份提供程序**。
- 3 单击系统目前正在使用的身份提供程序。
将显示为系统提供基本身份管理的现有身份目录和连接器。
- 4 在身份提供程序属性页面上，单击**添加连接器**下拉列表，然后选择与辅助 vRealize Automation 设备对应的连接器。
- 5 在选择该连接器时显示的**绑定 DN 密码**文本框中，输入相应的密码。
- 6 单击**添加连接器**。
- 7 默认情况下，主连接器显示在**IdP 主机名**文本框中。将主机名更改为指向负载均衡器。

在辅助连接器上启用目录同步

如果主连接器失效，另一个连接器实例将自动处理身份验证。如果出现故障，对于目录同步，您必须修改身份目录管理中的目录设置，才能使用相应的辅助连接器实例。您可以一次仅在一个连接器上启用目录同步。

步骤

- 1 选择**管理 > 身份目录管理 > 目录**。
- 2 选择与原始连接器实例关联的目录。

注 您可以在**目录 > 连接器**页面中查看此信息。

- 3 在“目录”页面的“目录同步和身份验证”部分，选择**同步连接器**下拉列表中的另一个连接器实例。
- 4 在“绑定用户详细信息”部分，在**绑定 DN 密码**文本框中输入您的 Active Directory 绑定帐户密码。
- 5 单击**保存**。

在 vRealize Automation 与 Active Directory 之间配置双向信任关系

您可以通过配置身份提供程序与 Active Directory 联合服务之间的双向信任关系，增强基础 vRealize Automation Active Directory 连接的系统安全性。

要在 vRealize Automation 与 Active Directory 之间配置双向信任关系，必须创建自定义身份提供程序并向其添加 Active Directory 元数据。此外，还必须修改 vRealize Automation 部署使用的默认策略。最后，必须配置 Active Directory 以识别身份提供程序。

前提条件

- 确认您已为 vRealize Automation 部署配置租户，且已设置适当的 Active Directory 链接，可以支持基本的 Active Directory 用户 ID 和密码身份验证。
- 已安装并配置 Active Directory 供网络上使用。
- 获取相应的 Active Directory 联合服务 (ADFS) 元数据。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 获取联合元数据文件。

您可以从 `https://servername.domain/FederationMetadata/2007-06/FederationMetadata.xml` 下载此文件

- 2 搜索 `logout` 一词，然后将每个实例的位置编辑为指向 `https://servername.domain/adfs/ls/logout.aspx`

例如，以下位置：

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

应更改为：

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

3 为部署创建新的身份提供程序。

- a 选择**管理 > 身份目录管理 > 身份提供程序**。
- b 单击**添加身份提供程序**并根据需要填写字段。

选项	描述
身份提供程序名称	为新身份提供程序输入一个名称
身份提供程序元数据 (URL 或 XML)	在此处粘贴 Active Directory 联合服务元数据文件的内容。
SAML 请求中的名称 ID 策略 (可选)	如果需要，请为身份策略 SAML 请求输入一个名称。
用户	选择您希望用户有权访问的域。
处理 IDP 元数据	单击以处理您添加的元数据文件。
网络	选择您希望用户有权访问的网络范围。
身份验证方法	为此身份提供程序使用的身份验证方法输入一个名称。
SAML 上下文	为您的系统选择合适的上下文。
SAML 签名证书	单击 SAML 元数据标题旁的链接，下载身份目录管理元数据。

- c 将身份目录管理元数据文件另存为 **sp.xml**。
- d 单击**添加**。

4 将规则添加到默认策略中。

- a 选择**管理 > 身份目录管理 > 策略**。
- b 单击默认策略名称。
- c 单击**策略规则**标题下的**+**图标，以添加新规则。

使用“添加策略规则”页面上的选项创建一个规则，该规则将指定用于特定网络范围和设备的相应主要和辅助身份验证方法。

例如，如果您的网络范围是“**我的电脑**”，且用户需要访问“**所有设备类型**”中的内容，则对于典型部署，您必须使用以下方法进行身份验证：**ADFS 用户名和密码**。

- d 单击**确定**保存策略更新。
- e 在“默认策略”页面上，将新规则拖动到表的顶部，使其优先于现有规则。

5 通过使用 Active Directory 联合服务管理控制台或其他适当工具，与 vRealize Automation 身份提供程序建立依赖方信任关系。

要建立此信任，必须导入以前下载的身份目录管理元数据。有关为双向信任关系配置 Active Directory 联合服务的详细信息，请参见 Microsoft Active Directory 文档。在此过程中，您必须执行以下操作：

- 建立依赖方信任。建立此信任时，必须导入您已复制和保存的 VMware 身份提供程序的服务提供程序的元数据 XML 文件。

- 创建声明规则，将在“获取属性”规则中从 LDAP 检索到的属性转换为所需的 SAML 格式。创建规则后，通过添加以下文本编辑规则：

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

在 Directories Management 与 SSO2 之间配置 SAML 联合

要支持单点登录，您可以在 vRealize Automation Directories Management 与使用 SSO2 的系统之间建立 SAML 联合。

通过在 Directories Management 与 SSO2 之间创建 SAML 连接，可在双方之间建立联合。目前，唯一受支持的端到端流是 SSO2 充当身份提供程序 (IdP)，Directories Management 充当服务提供程序 (SP)。

对于 SSO2 用户身份验证，Directories Management 和 SSO2 中必须存在相同的帐户。最起码，用户的 UserPrincipalName (UPN) 必须在两端匹配。其他属性可以不同，因为需要使用它们来标识 SAML 主题。

对于 SSO2 中的本地用户（例如，`admin@vsphere.local`），也必须在 Directories Management 中存在对应帐户，其中至少用户的 UPN 匹配。手动或利用采用 Directories Management 本地用户创建 API 的脚本创建这些帐户。

在 SSO2 与 Directories Management 之间设置 SAML 时，包括在身份目录管理和 SSO 组件上进行配置。

表 2-4. SAML 联合组件配置

组件	配置
身份目录管理	在 Directories Management 上将 SSO2 配置为第三方身份提供程序，并更新默认身份验证策略。您可以创建自动化脚本以设置 Directories Management。
SSO2 组件	通过导入 Directories Management <code>sp.xml</code> 文件将 Directories Management 配置为服务提供程序。此文件使您能够将 SSO2 配置为使用 Directories Management 作为服务提供程序 (SP)。

前提条件

- 为您的 vRealize Automation 部署配置租户。请参见[创建其他租户](#)。
- 设置相应的 Active Directory 链接，以支持基本的 Active Directory 用户 ID 和密码身份验证。
- 以[租户管理员](#)身份登录到 vRealize Automation。

步骤

- 1 通过 SSO2 用户界面下载 SSO2 身份提供程序元数据。
 - a 以管理员身份登录到 vCenter，网址：<https://<cloudvm-hostname>/>。
 - b 单击**登录到 vSphere Web Client** 链接。
 - c 在左侧导航窗格中，选择**管理 > 单点登录 > 配置**。
 - d 单击与 SAML 服务提供程序标题的元数据相邻的**下载**。
vsphere.local.xml 文件应当会开始下载。
 - e 复制 vsphere.local.xml 文件的内容。
- 2 在 vRealize Automation 身份目录管理标识提供程序页面，创建新的身份提供程序。
 - a 以**租户管理员**身份登录到 vRealize Automation。
 - b 选择**管理 > 身份目录管理 > 身份提供程序**。
 - c 单击**添加身份提供程序**，并提供配置信息。

选项	操作
身份提供程序名称	为新身份提供程序输入一个名称。
身份提供程序元数据（URI 或 XML）文本框	将 SSO2 idp.xml 元数据文件的内容粘贴到文本框中，然后单击 处理 IDP 元数据 。
SAML 请求中的名称 ID 策略（可选）	输入 http://schemas.xmlsoap.org/claims/UPN 。
用户	选择您希望用户有权访问的域。
网络	选择您希望用户有权访问的网络范围。 如果要通过 IP 地址对用户进行身份验证，请选择 所有范围 。
身份验证方法	为身份验证方法输入一个名称。然后，使用右侧的 SAML 上下文 下拉菜单将身份验证方法映射到 <code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code> 。
SAML 签名证书	单击 SAML 元数据标题旁的链接，下载身份目录管理元数据。

- d 将身份目录管理元数据文件另存为 **sp.xml**。
 - e 单击**添加**。
- 3 使用“身份目录管理策略”页面更新相关身份验证策略，以将身份验证重定向到第三方 SSO2 身份提供程序。
 - a 选择**管理 > 身份目录管理 > 策略**。
 - b 单击默认策略名称。
 - c 单击**策略规则**标题下的身份验证方法，以编辑现有的身份验证规则。
 - d 在“编辑策略规则”页面上，将密码中的身份验证方法更改为适当的方法。
在这种情况下，该方法应为 SSO2。
 - e 单击**保存**保存策略更新。

4 在左侧导航窗格中，选择**管理 > 单点登录 > 配置**，然后单击**更新**，将 `sp.xml` 文件上载到 vSphere。

将用户或组添加到 Active Directory 连接

您可以将用户或组添加到现有的 Active Directory 连接。

添加组和用户时，身份目录管理用户身份验证系统会从 Active Directory 导入数据。数据传输的速度受 Active Directory 功能限制。因此，操作可能需要很长时间，具体取决于添加的组和用户的数量。要尽可能地减少问题的发生，请将组和用户限定为 vRealize Automation 操作所需的组和用户。如果出现问题，请关闭不需要的应用程序，并确认您的部署已向 Active Directory 分配相应的内存。如果问题仍然存在，请增加 Active Directory 内存分配。对于拥有大量用户和组的部署，您可能需要将 Active Directory 内存分配增加至多达 24 GB。

同步拥有大量用户和组的 vRealize Automation 部署时，可能会经过一段延迟，才会显示 SyncLog 详细信息。日志文件的时间戳可以不同于控制台上显示的完成时间。

如果某个组的成员不在“用户”列表中，则从 Active Directory 添加该组时，其成员会添加到此列表中。在同步组时，不会同步未将“域用户”作为 Active Directory 中的主要组的任何用户。

注 启动同步操作后，无法取消该操作。

前提条件

- 已安装 连接器 并使用激活码进行了激活。在“用户属性”页面上选择必需的默认属性并添加其他属性。
- 要从 Active Directory 同步的 Active Directory 组和用户的列表。
- 对于通过 LDAP 访问的 Active Directory，所需的信息包括基本 DN、绑定 DN 以及绑定 DN 密码。
- 对于 Active Directory 集成 Windows 身份验证，所需信息包括域的绑定用户 UPN 地址和密码。
- 如果通过 SSL 访问 Active Directory，则需要 SSL 证书的副本。
- 如果已将多林 Active Directory 与 Windows 身份验证集成且“域本地”组包含来自不同林的成员，请执行以下操作。将绑定用户添加到“域本地”组的管理员组。如果未添加绑定用户，“域本地”组中将缺少这些成员。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 目录**。
- 2 单击所需的目录名称。
- 3 单击**同步设置**打开一个对话框，其中显示了同步选项。
- 4 单击相应的图标，具体取决于您是需要更改用户配置还是组配置。

要编辑组配置，请执行以下操作：

- 要添加组，请单击 **+** 图标，为组 DN 定义添加一行，然后输入相应的组 DN。
- 如果要删除组 DN 定义，请单击所需组 DN 对应的 **x** 图标。

要编辑用户配置，请执行以下操作：

- ◆ 要添加用户，请单击 **+** 图标，为用户 DN 定义添加一行，然后输入相应的用户 DN。
- 如果要删除用户 DN 定义，请单击所需用户 DN 对应的 **x** 图标。

5 单击**保存**，保存所做的更改而不立即同步更新。单击**保存并同步**，保存所做的更改并立即同步更新。

选择要与目录同步的属性

在设置 Directories Management 目录与 Active Directory 同步时，您可以指定将同步到目录的用户属性。在设置目录之前，您可以在“用户属性”页面上指定必需的默认属性，并根据需要添加要映射到 Active Directory 属性的其他属性。

在创建目录之前配置“用户属性”页面时，您可以执行下列操作：将默认属性从必需更改为不必需，将属性标记为必需，以及添加自定义属性。

有关默认映射属性的列表，请参见[管理从 Active Directory 同步的用户属性](#)。

在创建目录之后，您可以将必需属性更改为不必需，还可以删除自定义属性。但您无法将属性更改为必需属性。

在创建目录之后添加其他要同步到目录的属性时，可转到目录的“映射的属性”页面，以便将这些属性映射到 Active Directory 属性。

步骤

- 1** 以系统或租户管理员身份登录到 vRealize Automation。
- 2** 单击“管理”选项卡。
- 3** 选择**身份目录管理 > 用户属性**。
- 4** 在“默认属性”部分中，查看必需属性列表，并做出相应的更改以反映哪些属性应当是必需的。
- 5** 在“属性”部分中，将 Directories Management 目录属性名称添加到列表中。
- 6** 单击**保存**。

默认属性状态将会更新，并且您添加的属性将会添加到目录的“映射的属性”列表中。

- 7** 创建目录后，请转到“身份存储”页面并选择该目录。
- 8** 单击**同步设置 > 映射的属性**。
- 9** 在您添加的属性的下拉菜单中，选择要映射到的 Active Directory 属性。
- 10** 单击**保存**。

结果

下次该目录同步到 Active Directory 时，即会更新目录。

向身份目录管理添加内存

如果您的 Active Directory 连接包含大量用户或组，则可能需要为 Directories Management 分配额外的内存。

默认情况，将为 Directories Management 服务分配 4 GB 内存。这对许多中小型部署来说已足够。如果 Active Directory 连接使用大量用户或组，则可能需要增加此内存分配。增加内存分配适用于具有 100,000 名以上用户的系统，每名用户属于 30 个组，一共有 750 个组。对于这些系统，VMware 建议将分配给 Directories Management 的内存增加到 6 GB。

身份目录管理内存根据分配给 vRealize Automation 设备的总内存计算得出。下表显示了相关组件的内存分配。

表 2-5. vRealize Automation 设备的内存分配

虚拟设备内存	vRA 服务内存	vidm 服务内存
18 GB	3.3 GB	4 GB
24 GB	4.9 GB	6 GB
30 GB	7.4 GB	9.1 GB

注 这些分配假定所有默认服务均已在虚拟设备上启用且正在运行。如果某些服务停止，它们可能会发生更改。

前提条件

- 已在 vRealize Automation 部署中配置并运行适当的 Active Directory 连接。

步骤

- 1 停止正在运行 vRealize Automation 设备的每台计算机。
- 2 在每台计算机上增加虚拟设备的内存分配。

如果使用默认的内存分配 18 GB，VMware 建议将该内存分配增加到 24 GB。

- 3 重新启动运行 vRealize Automation 设备的计算机。

创建域主机查找文件以替代 DNS 服务位置 (SRV) 查找

启用集成 Windows 身份验证后，目录配置会更改为启用“DNS 服务位置”字段。连接器 服务位置查找不可识别站点。要覆盖随机 DC 选择，可以创建名为 `domain_krb.properties` 的文件并将域添加到主机值，这些值优先于 SRV 查找。

步骤

- 1 从 `appliance-va` 命令行中，以具有 root 权限的用户身份登录。
- 2 将目录更改为 `/usr/local/horizon/conf` 并创建名为 `domain_krb.properties` 的文件。

- 3 编辑 `domain_krb.properties` 文件以将域列表添加到主机值。以 `<AD Domain>=<host:port>`，`<host2:port2>`，`<host2:port2>` 形式添加信息。

例如，以 `example.com=examplehost.com:636`，`examplehost2.example.com:389` 形式输入列表

- 4 将 `domain_krb.properties` 文件的所有者更改为 Horizon 并将组更改为 `www`。输入 `chown horizon:www /usr/local/horizon/conf/domain_krb.properties`。

- 5 重新启动服务。输入 `service horizon-workspace restart`。

配置即时用户置备

您可以配置即时 (Just-in-Time, JIT) 置备，以支持添加用户时无需从 Active Directory 同步。

要支持即时置备，必须添加第三方身份提供程序，然后在 vRealize Automation 部署中配置与该第三方身份提供程序的连接以通过 SAML 协议将身份目录管理与其他 SSO 提供程序相集成。此外，还必须使用适当的名称创建一个新目录，例如 JIT Directory。

启用即时置备时，可以将即时用户添加到指定的自定义组中。要支持此功能，请创建一个包含适当成员的自定义组。请参见[添加具有自定义组和规则的即时用户](#)。

注 最佳做法是不要在默认的 `vsphere.local` 租户上配置即时置备。

前提条件

配置适当的第三方身份提供程序以与 JIT 置备结合使用。

步骤

- 1 为即时置备创建身份提供程序。
 - a 选择**管理 > 身份目录管理 > 身份提供程序**。
 - b 单击**添加身份提供程序**并根据需要编辑身份提供程序实例设置。
 - 对于即时置备，创建第三方身份提供程序。
 - 在“创建即时目录”部分中，输入目录以及一个或多个域的名称。
 - 您必须为第三方身份提供程序配置选择一个网络。
 - 如果使用外部 VMware Identity Manager 作为第三方身份提供程序，且使用 `userPrincipleName` 对用户进行身份验证，则必须将 `userPrincipleName` 的“名称 ID”映射配置从默认值 `x509SubjectName` 更改为 `unspecified`。

有关创建身份提供程序的详细信息，请参见[配置第三方身份提供程序连接](#)

- 2 在即时身份提供程序上配置 SAML。
 - a 从身份提供程序复制 IdP 元数据。
 - b 在 vRealize Automation 中，选择身份提供程序，然后将 IdP 元数据粘贴到**身份提供程序元数据 (URL 或 XML)** 文本框中。
 - c 单击**保存**。

- d 在 **SAML 请求中的名称 ID 策略 (可选)** 下拉菜单中，选择相应格式。

例如，如果使用电子邮件地址作为唯一用户标识符，将选择

`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`。

- e 在“用户”标题下选择相应目录。

- f 在“网络”标题下选择此身份提供程序要使用的网络。

- g 在**身份验证方法**文本框中指定相应名称。

- h 在 **SAML 上下文**下拉菜单中，选择

`urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport`

- i 右键单击**服务提供商 (SP) 元数据**链接，然后在独立浏览器选项卡中打开。

- j 使用此元数据在身份提供程序上配置 SAML 连接。

如果使用的是 VMware Identity Manager，请参见 VMware Identity Manager 文档，获取有关配置 SAML 的完整说明。

3 单击**添加**。

使用提供的目录名称创建新目录。

4 配置 vRealize Automation 访问策略。

- a 选择**管理 > 策略**。

- b 单击策略规则表右上角的绿色 + 图标。

- c 设置策略规则以应用于适用的范围和设备类型。

- d 选择为 JIT 置备配置第三方身份提供程序时创建的身份验证方法作为身份验证方法。

管理从 Active Directory 同步的用户属性

“身份目录管理用户属性”页面列出了同步到 Active Directory 连接的用户属性。

在“用户属性”页面中做出并保存的更改会添加到 Directories Management 目录的“映射的属性”页面中。属性更改会在下次与 Active Directory 同步时更新到目录。

“用户属性”页面将列出可映射到 Active Directory 属性的默认目录属性。您可以选择必需的属性，还可以添加要同步到目录的其他 Active Directory 属性。

表 2-6. 要与目录同步的默认 Active Directory 属性

目录属性名称	默认映射到的 Active Directory 属性
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName。添加对象的完全限定域名。

表 2-6. 要与目录同步的默认 Active Directory 属性（续）

目录属性名称	默认映射到的 Active Directory 属性
disabled（已禁用外部用户）	userAccountControl。带有 UF_Account_Disable 标记。 当帐户处于禁用状态时，用户无法登录以访问其应用程序和资源。 用户有权使用的资源未从帐户中移除，以便从帐户中移除该标记时，用户可以登录并访问其授权的资源。
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName:

“用户属性”页面将列出可映射到 Active Directory 属性的默认目录属性。您可以选择必需的属性，还可以添加要同步到目录的其他 Active Directory 属性。

表 2-7. 要与目录同步的默认 Active Directory 属性

目录属性名称	默认映射到的 Active Directory 属性
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeid	employeeID
domain	canonicalName。添加对象的完全限定域名。
disabled（已禁用外部用户）	userAccountControl。带有 UF_Account_Disable 标记。 当帐户处于禁用状态时，用户无法登录以访问其应用程序和资源。 用户有权使用的资源未从帐户中移除，以便从帐户中移除该标记时，用户可以登录并访问其授权的资源。
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
userName	sAMAccountName:

管理连接器和连接器集群

“连接器”页面列出了为企业网络部署的连接器。连接器可在 Active Directory 和身份目录管理服务之间同步用户和组数据，并且当连接器用作身份提供程序时，还可验证用户身份以允许其访问服务。

在 vRealize Automation 中，每个 vRealize Automation 设备 均包含其自己的连接器，这些连接器适用于大多数部署。

在将目录与连接器实例相关联时，连接器会为关联的目录创建一个分区（称为“工作线程”）。连接器实例可具有多个关联的工作线程。每个工作线程都充当一个身份提供程序。连接器通过一个或多个工作线程在 **Active Directory** 和服务之间同步用户和组数据。您可以为每个工作线程分别定义和配置身份验证方法。

您可以从“连接器”页面中管理 **Active Directory** 链接的各个方面。此页面包含一个表和多个按钮，允许您完成各种不同的管理任务。

- 在“工作线程”列中，可以选择一个工作线程以查看连接器的详细信息，还可以导航到“身份验证适配器”页面以查看可用身份验证方法的状态。有关身份验证的信息，请参见[将替代用户身份验证产品与身份目录管理集成](#)。
- 在“身份提供程序”列中，可选择 IdP 以进行查看、编辑或停用。请参见[配置第三方身份提供程序连接](#)。
- 在“关联的目录”列中，可访问与此工作线程关联的目录。
- 单击**加入域**可使连接器加入特定的 **Active Directory** 域。例如，在配置 Kerberos 身份验证时，您必须加入包含用户或与包含用户的域存在信任关系的 **Active Directory** 域。
- 如果使用 **Active Directory**（集成 Windows 身份验证）配置目录，则连接器将根据配置详细信息加入域。

集群环境中的连接器

在分布式 vRealize Automation 部署中，所有可用的连接器将执行所需的任何用户授权，而指定的单个连接器将处理所有配置同步。通常，同步包括添加、删除或更改用户配置。只要所有连接器均可用，则会自动同步。在某些特定的情况下，可能不会自动同步。

对于目录配置（例如，基本 DN）的相关更改，vRealize Automation 会尝试自动将更新推送到集群中的所有连接器。如果由于某种原因导致连接器不可操作或无法访问，则即便连接器恢复联机操作，也不会接收更新。要对可能未自动接收更新的连接器实现配置更改，系统管理员必须手动将更改保存到所有适用的连接器中。

对于目录同步配置文件相关的更改，vRealize Automation 也会尝试自动将更新推送到所有连接器。如果同步连接器可正常运行，则更新将保存并推送到所有可用的授权连接器。如果一个或多个连接器不可访问，则系统管理员将收到一条警告，指出并非所有连接器均已更新。如果同步连接器不可操作，则更新失败并出现错误。如果系统管理员更改已指定为同步连接器的连接器，则新的同步连接器将接收最新的可用配置文件信息，并将此信息推送到所有适用的可用连接器。

将连接器计算机加入域

在某些情况下，您可能需要将包含身份目录管理连接器的计算机加入域。

对于通过 LDAP 访问的 **Active Directory** 目录，可以在创建目录后加入域。对于 **Active Directory**（集成 Windows 身份验证）目录，连接器会在创建目录时自动加入域。在这两种情况下，都必须提供正确的凭据。

要加入域，您需要用到拥有“将计算机加入 AD 域”特权的 **Active Directory** 凭据。此凭据在 **Active Directory** 中进行配置，并拥有以下权限：

- 创建计算机对象

■ 删除计算机对象

在加入域时，系统会在 Active Directory 中的默认位置创建一个计算机对象。

如果没有加入域的权限，或者公司策略需要计算机对象的自定义位置，则必须要求管理员创建对象并将连接器计算机加入域。

步骤

- 1 要求您的 Active Directory 管理员在由您的公司策略确定的某个 Active Directory 位置创建计算机对象。您必须提供连接器的主机名。确保提供完全限定域名，例如 `server.example.com`。

您可以在管理控制台的“连接器”页面上的“主机名”列中找到主机名。选择**管理 > 身份目录管理 > 连接器**。

- 2 创建计算机对象后，在“连接器”页面上单击**加入域**以使用身份目录管理中的任何可用域用户帐户加入域。

关于域控制器选择

身份目录管理维护一个动态的域控制器列表，无需执行用户配置。

身份目录管理会根据 LDAP Ping 定期刷新、重新发现和重新排序域控制器，并将域控制器存储在 `domain_krb` 文件和自定义 `krb5.conf` 文件中。优先列出最佳域控制器，并用于身份验证和同步操作等各种目的。如果此域控制器在 10 毫秒内无法响应，则会再次刷新域控制器列表。这样可以确保身份目录管理始终使用最佳域控制器，即使在域控制器出现故障时也是如此。

管理访问策略

Directories Management 策略是一组规则，用于指定用户访问其应用程序门户或启动指定的 Web 应用程序时必须满足的条件。

您可以创建规则以作为策略的一部分。策略中的每个规则都可以指定以下信息。

- 用户可以从登录的网络范围，例如企业网络内部或外部。
- 可通过此策略进行访问的设备类型。
- 启用的身份验证方法的应用顺序。
- 身份验证的有效小时数。
- 自定义的访问被拒绝消息。

注 策略不会控制 Web 应用程序会话的持续时长。它们可以控制用户必须启动 Web 应用程序的时间长度。

Directories Management 服务包含一个可编辑的默认策略。此策略从总体上控制对该服务的访问权限。请参阅[应用默认访问策略](#)。要控制对特定 Web 应用程序的访问权限，您可以创建其他策略。如果没有对 Web 应用程序应用任何策略，则将应用此默认策略。

配置访问策略设置

策略包含一个或多个访问规则。每个规则由一些设置组成，您可以配置这些设置以从总体上管理用户对其应用程序门户或指定的 Web 应用程序的访问。

网络范围

对于每个规则，您通过指定网络范围来确定用户群。网络范围由一个或多个 IP 范围组成。在配置访问策略集之前，您可以从“身份和访问管理”选项卡的“设置”>“网络范围”页面创建网络范围。

设备类型

选择规则管理的设备类型。客户端类型包括“Web 浏览器”、“Identity Manager Client 应用程序”、“iOS”、“Android”和“所有设备类型”。

添加组

可以根据用户的组成员资格对身份验证应用不同的策略。要分配用户组以通过特定的身份验证流程登录，可以将组添加到访问策略规则中。可以同步企业目录中的组或在管理控制台中创建的本地组。同一个域中的组名称必须唯一。

要在访问策略规则中使用组，请从“身份目录管理”>“策略”页面配置新的策略，然后为该策略选择所需的组。必须在“用户属性”页面中映射策略，再同步到目录。

如果在访问策略规则中使用组，用户的登录体验将发生变化。将显示一个页面，提示用户输入其唯一标识符，而不是要求用户选择域并输入其凭据。Directories Management 根据唯一标识符在内部数据库中查找用户，并显示在该规则中配置的身份验证页面。

如果未选择组，访问策略规则适用于所有用户。如果配置的访问策略规则包含基于组的规则以及用于所有用户的规则，请确保为所有用户指定的规则是在策略的“策略规则”部分中列出的最后一个规则。

有关如何将规则应用于用户的详细信息，请参见 VMware Identity Manager 文档中的“使用唯一标识符的登录体验”。

身份验证方法

设置策略规则中的身份验证方法的优先级。身份验证方法将按照它们列出的先后顺序加以应用。满足策略中的身份验证方法和网络范围配置的第一个身份提供程序实例将被选中，然后用户身份验证请求将被转发到该身份提供程序实例进行身份验证。如果身份验证失败，则选择列表中的下一个身份验证方法。如果使用“证书”身份验证，则此方法必须是列表中的第一个身份验证方法。

您可以配置访问策略规则，以要求用户通过两种身份验证方法传递凭据后才能登录。如果其中一种身份验证方法失败或两种身份验证方法均失败，并且还配置了回退方法，系统会提示用户针对所配置的下一身份验证方法输入其凭据。以下两种情况介绍了身份验证链接的工作方式。

- 在第一种情况下，访问策略规则被配置为要求用户使用其密码和 Kerberos 凭据进行身份验证。回退身份验证被设置为要求使用密码和 RADIUS 凭据进行身份验证。用户正确输入了密码，但未能输入正确的 Kerberos 身份验证凭据。由于用户输入了正确的密码，因此回退身份验证请求仅要求输入 RADIUS 凭据。用户不需要重新输入密码。
- 在第二种情况下，访问策略规则被配置为要求用户使用其密码和 Kerberos 凭据进行身份验证。回退身份验证被设置为要求使用 RSA SecurID 和 RADIUS 凭据进行身份验证。用户正确输入了密码，但未能输入正确的 Kerberos 身份验证凭据。回退身份验证请求将要求同时输入 RSA SecurID 凭据和 RADIUS 凭据以进行身份验证。

身份验证会话时长

在每个规则中，您都可以设置身份验证的有效时长。该值决定了用户自其上一次身份验证事件以后，在访问其门户或启动特定 **Web** 应用程序前可以等待的最长时间。例如，如果 **Web** 应用程序规则中的值为 **4**，则表示用户将有 4 个小时可以启动 **Web** 应用程序，除非他们启动的另一个身份验证事件延长了此时间。

自定义的访问被拒绝错误消息

如果用户尝试登录时由于凭据无效、配置不正确或系统错误而失败，系统会显示一条访问被拒绝消息。默认消息为

由于未找到有效的身份验证方法，访问遭到拒绝 (Access denied as no valid authentication methods were found)。

您可以为每个访问策略规则创建一条自定义错误消息，以替代默认消息。该自定义消息可以包含文本和一个用于调用操作消息的链接。例如，在针对要管理的移动设备的策略规则中，如果用户尝试从未注册的设备登录，则可以显示下列自定义错误消息：

请单击此消息末尾的链接注册您的设备，以便访问公司资源。如果您的设备已经注册，请联系支持部门以获取帮助 (Please enroll your device to access corporate resources by clicking the link at the end of this message. If your device is already enrolled, contact support for help)。

默认策略示例

以下策略举例说明了如何配置默认策略以控制对应用程序门户的访问。请参见[管理用户访问策略](#)。

策略规则将按照列出的顺序接受评估。您可以通过拖放“策略规则”部分中的规则来更改策略的顺序。

在以下用例中，此策略示例适用于所有应用程序。

网络范围	设备类型	身份验证方法	重新进行身份验证
所有范围	Web 浏览器	Password	8 小时
所有范围	Identity Manager Client 应用程序	Password	2160 小时

- 对于内部网络（内部网络范围），为规则配置了两种身份验证方法，即，Kerberos 身份验证，以及作为回退方法的密码身份验证。要从内部网络中访问应用程序门户，该服务先尝试使用 Kerberos 身份验证对用户进行身份验证，因为这是在规则中列出的第一种身份验证方法。如果该方法失败，系统将提示用户输入其 **Active Directory** 密码。用户使用浏览器登录，并且现在可以在 8 小时会话期间访问其用户门户。
 - 对于从外部网络（所有范围）进行的访问，仅配置了一种身份验证方法，即，RSA SecurID。要从外部网络中访问应用程序门户，用户需要使用 SecurID 登录。用户使用浏览器登录，并且现在可以在 4 小时会话期间访问其应用程序门户。
- 在用户尝试访问某个资源时（特定于 **Web** 应用程序的策略涵盖的 **Web** 应用程序除外），将应用默认门户访问策略。

例如，此类资源的重新身份验证时间与默认访问策略规则的重新身份验证时间一致。根据默认访问策略规则，登录到应用程序门户的用户的时间为 8 小时，当用户在会话期间尝试启动某个资源时，将直接启动该应用程序，而无需重新对用户进行身份验证。

配置基于组的访问策略

可以配置基于组的访问策略，以根据组分配控制登录特权。

身份目录管理包含支持所有组和所有网络范围的默认访问策略。可以修改这些策略使其更加严格，也可以创建新策略以支持不同的登录策略。

步骤

1 将组添加到所需策略。

- a 选择**管理 > 身份目录管理 > 策略**。
- b 可以打开默认访问策略，也可以创建新策略。
- c 编辑配置有“Web 浏览器”设备类型的策略规则。

要编辑策略，请单击其“身份验证方法”。默认情况下，有两个策略规则可应用于所有 IP 地址和所有用户。

将针对选定策略打开“编辑策略规则”页面。可以编辑“网络范围”、“设备类型”、“身份验证方法”等各种参数以及其他策略规则参数。

- d 单击“编辑策略规则”页面上的**编辑组**，查看可用于该策略的所有组。

此页面将显示与租户关联的所有组。

- e 选择要与策略关联的组。
- f 单击**确定**。

选定组将显示在“编辑策略规则”页面上。

- g 单击“编辑策略规则”页面上的**确定**，以保存对策略规则所做的更改。

将显示“策略”页面，其中显示了为策略选择的组数。

- h 单击“策略”页面上的**保存**。

2 为组策略配置网络范围。

- a 选择**管理 > 身份目录管理 > 网络范围**

默认情况下，存在 All Ranges 的预定义设置，涵盖了所有网络范围的所有 IP 地址。可以创建新的网络范围，也可以编辑现有的网络范围。

- b 单击**添加网络范围**。

将打开“编辑网络范围”页面。

- c 输入新网络范围的**名称**，并根据需要添加**描述**。

结果

用户登录到 vRealize Automation 时，必须选择域，然后输入有效的用户名和密码。如果在适用的策略中指定组，有效用户仍必须输入用户名和密码。

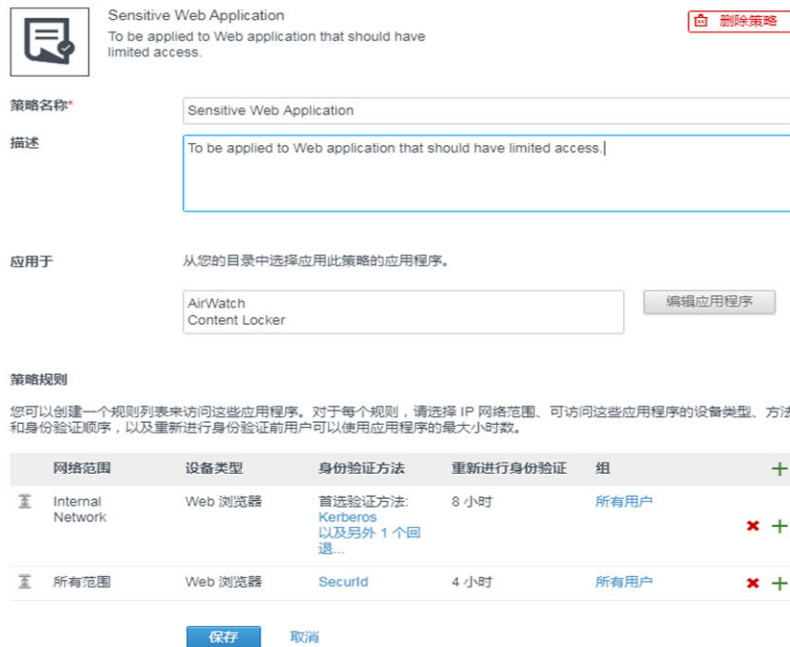
管理特定于 Web 应用程序的策略

在目录中添加 Web 应用程序时，您可以创建特定于 Web 应用程序的访问策略。例如，您可以针对某个 Web 应用程序创建一个含有规则的策略，这些规则用于指定哪些 IP 地址有权访问该应用程序，使用哪些身份验证方法进行访问，以及多久后需要重新进行身份验证。

以下特定于 Web 应用程序的策略示例说明了如何通过创建策略来控制对指定 Web 应用程序的访问权限。

示例 1 特定于 Web 应用程序的严格策略

在此示例中，将创建一个新策略并将其应用于一个敏感 Web 应用程序。



Sensitive Web Application
To be applied to Web application that should have limited access.

策略名称* Sensitive Web Application

描述 To be applied to Web application that should have limited access.

应用于 从您的目录中选择应用此策略的应用程序。
AirWatch Content Locker [编辑应用程序](#)

策略规则
您可以创建一个规则列表来访问这些应用程序。对于每个规则，请选择 IP 网络范围、可访问这些应用程序的设备类型、方法和身份验证顺序，以及重新进行身份验证前用户可以使用应用程序的最大小时数。

网络范围	设备类型	身份验证方法	重新进行身份验证	组	
Internal Network	Web 浏览器	首选验证方法: Kerberos 以及另外 1 个回退...	8 小时	所有用户	✖ +
所有范围	Web 浏览器	SecurID	4 小时	所有用户	✖ +

[保存](#) [取消](#)

- 1 要从企业网络外部访问服务，用户必须使用 RSA SecurID 进行登录。用户使用浏览器进行登录，根据默认的访问规则，用户当前在四小时的会话时间内有权访问应用程序门户。
- 2 在四个小时后，用户尝试启动某个应用了敏感 Web 应用程序策略集的 Web 应用程序。
- 3 该服务检查策略中的规则并应用具有“所有范围”网络范围的策略，这是因为用户请求来自于 Web 浏览器以及“所有范围”网络范围。

用户使用 RSA SecurID 身份验证方法登录，但会话刚刚过期。用户将被重定向，以重新进行身份验证。重新验证身份后，用户将获得另一个四小时的会话，并将能够启动应用程序。在接下来的四个小时内，用户可以继续启动应用程序而无需重新进行身份验证。

示例 2 特定于 Web 应用程序的更严格策略

要将更严格的规则应用于额外的敏感 Web 应用程序，您可能需要在 1 小时后在任何设备上使用 SecureID 重新进行身份验证。下面是如何实施这种类型的策略访问规则的示例。

- 1 用户使用密码身份验证方法从企业网络内部登录。

按照示例 1 中的设置，用户现在具有应用程序门户访问权限已达 8 个小时。

- 2 用户立即尝试启动某个应用了示例 2 策略规则的 Web 应用程序，该策略规则要求进行 RSA SecurID 身份验证。

- 3 用户将重定向到提供 RSA SecurID 身份验证的身份提供程序。

- 4 用户成功登录后，服务将启动应用程序并保存身份验证事件。

按照策略规则规定，在不超过 1 小时的时间内，用户可以继续启动此应用程序，但 1 小时之后，将要求用户重新进行身份验证。

管理用户访问策略

vRealize Automation 提供了默认用户访问策略。您既可以按原样使用该策略，也可根据需要进行编辑以管理租户对应用程序的访问。

vRealize Automation 提供了默认用户访问策略。您无法添加新策略，但可以编辑现有策略以添加规则。

前提条件

- 为您的部署选择或配置相应的身份提供程序。请参见[配置第三方身份提供程序连接](#)。
- 为您的部署配置相应的网络范围。请参见[添加或编辑网络范围](#)。
- 为您的部署配置相应的身份验证方法。请参见[将替代用户身份验证产品与身份目录管理集成](#)。
- 如果您计划编辑默认策略（从总体上控制用户对服务的访问），请在创建特定于 Web 应用程序的策略之前对其进行配置。
- 将 Web 应用程序添加到目录。Web 应用程序必须列在“目录”页面中才能添加策略。
- 以租户管理员身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 策略**。
- 2 单击**编辑策略**以添加新策略。
- 3 在相应的文本框中添加策略名称和描述。
- 4 在“应用于”部分中，单击**选择**，然后在显示的页面中选择与此策略关联的 Web 应用程序。
- 5 在“策略规则”部分中，单击 **+** 以添加规则。

将显示“添加策略规则”页。

- a 选择要应用于此规则的网络范围。
- b 为此规则选择可访问 Web 应用程序的设备类型。

- c 按照应用的先后顺序选择要使用的身份验证方法。
- d 指定 Web 应用程序会话打开的小时数。
- e 单击**保存**。

6 根据需要配置其他规则。

7 单击**保存**。

配置其他身份提供程序连接

需要时，您可以配置额外的身份提供程序连接，以支持各种不同的身份管理方案，包括额外的内置身份提供程序和第三方身份提供程序。

使用身份目录管理可以创建三种类型的身份提供程序连接。

- 创建第三方 IDP - 使用此项可以创建与外部第三方身份提供程序的连接。在添加第三方身份提供程序实例之前，确保完成以下任务。
 - 确认第三方实例符合 **SAML 2.0** 标准，并且服务可以访问第三方实例。
 - 获取相应的第三方元数据信息，以便在管理控制台中配置身份提供程序时添加该信息。从第三方实例获取的元数据信息可以是元数据的 **URL** 或实际元数据。
- 创建 Workspace IDP - 在配置身份目录管理期间启用连接器对用户进行身份验证时，会创建 Workspace IDP 作为身份提供程序并启用密码身份验证。您可以在不同负载平衡器后面配置额外的 Workspace 身份提供程序。
- 创建内置 IDP - 内置身份提供程序使用内部身份目录管理机制来支持身份验证。您可以配置内置身份提供程序来使用身份验证方法，而不需要使用内部部署的连接器。配置内置身份提供程序时，您需要关联要与内置身份提供程序一起使用的身份验证方法。
- [配置第三方身份提供程序连接](#)
vRealize Automation 附带一个默认身份提供程序连接实例。用户可能希望创建更多身份提供程序连接，以支持即时用户置备或其他自定义配置。
- [配置附加 Workspace 身份提供程序](#)
配置身份目录管理连接器对用户进行身份验证时，会创建 Workspace IDP 并启用密码身份验证。
- [配置内置身份提供程序连接](#)
您可以配置多个内置身份提供程序，并为它们关联身份验证方法。

配置第三方身份提供程序连接

vRealize Automation 附带一个默认身份提供程序连接实例。用户可能希望创建更多身份提供程序连接，以支持即时用户置备或其他自定义配置。

vRealize Automation 提供了默认身份提供程序。在大多数情况下，默认提供程序足以满足客户需求。如果使用现有的企业身份管理解决方案，则可设置自定义身份提供程序，将用户重定向到现有身份解决方案。

使用自定义身份提供程序时，身份目录管理将使用从该提供程序获得的 SAML 元数据与提供程序建立信任关系。建立此关系之后，身份目录管理可根据主题名称 ID 将 SAML 断言中的用户映射到 vRealize Automation 内部用户列表。

前提条件

- 配置要定向到此身份提供程序实例进行身份验证的网络范围。请参见[添加或编辑网络范围](#)。
- 有权访问第三方元数据文档。这可以是指向元数据的 URL 或实际元数据。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 身份提供程序**。

此页面显示所有已配置的身份提供程序。

- 2 单击**添加身份提供程序**。

将显示包含身份提供程序选项的菜单。

- 3 选择**创建第三方 IDP**。

- 4 输入相应信息以配置身份提供程序。

选项	描述
身份提供程序名称	输入此身份提供程序实例的名称。
SAML 元数据	<p>添加第三方 IdP 基于 XML 的元数据文档，以便与身份提供程序建立信任关系。</p> <ol style="list-style-type: none"> 1 在文本框中输入 SAML 元数据 URL 或 xml 内容。 2 单击处理 IdP 元数据。将从元数据中提取 IdP 支持的 NameID 格式，并将其添加到“名称 ID 格式”表中。 3 在“名称 ID 值”列中，在该服务中选择用户属性以映射到显示的 ID 格式。您可以添加自定义第三方名称 ID 格式并将其映射到服务中的用户属性值。 4 （可选）选择 NameIDPolicy 响应标识符字符串格式。
用户	选择可使用此身份提供程序进行身份验证的用户的 Directories Management 目录。
即时用户置备	<p>选择相应选项以支持使用相应第三方身份提供程序进行即时置备。</p> <p>输入要用于即时置备的目录名称。</p> <p>输入要用于即时置备的外部身份提供程序中存在的一个或多个域。</p>
网络	<p>此处列出了在服务中配置的现有网络范围。</p> <p>根据用户 IP 地址，选择要定向到此身份提供程序实例进行身份验证的用户的网络范围。</p>
身份验证方法	添加受第三方身份提供程序支持的身份验证方法。选择支持身份验证方法的 SAML 身份验证上下文类。
SAML 签名证书	单击 服务提供程序 (SP) 元数据 以查看 Directories Management SAML 服务提供程序元数据 URL。复制并保存该 URL。在第三方身份提供程序中编辑 SAML 断言以映射 Directories Management 用户时，将配置该 URL。
Hostname	如果显示 主机名 字段，请输入将身份提供程序重定向到的主机名以进行身份验证。如果使用 443 以外的非标准端口，则可以将其设置为“主机名:端口”。例如，myco.example.com:8443。

5 单击添加。

后续步骤

- 复制并保存 Directories Management 服务提供程序元数据，在配置第三方身份提供程序实例时需要该数据。此元数据在“身份提供程序”页面的“SAML 签名证书”部分中可用。
- 向服务默认策略中添加身份提供程序的身份验证方法。

有关添加资源和对添加到目录中的资源进行自定义的信息，请参见《在 Directories Management 中设置资源》指南。

配置附加 Workspace 身份提供程序

配置身份目录管理连接器对用户进行身份验证时，会创建 Workspace IDP 并启用密码身份验证。

您可以在多个负载平衡器的后面配置和运行额外的连接器。如果部署中包含多个负载平衡器，您可以在每个负载平衡器配置中为身份验证配置额外的 Workspace 身份提供程序。

步骤

1 选择管理 > 身份目录管理 > 身份提供程序。

此页面显示所有已配置的身份提供程序。

2 单击添加身份提供程序。

将显示包含身份提供程序选项的菜单。

3 选择创建 Workspace IDP。

4 输入相应信息以配置身份提供程序。

选项	描述
身份提供程序名称	为此内置身份提供程序实例输入一个名称。
用户	选择要进行身份验证的用户。将列出已配置的目录。
用户	选择可使用此 Workspace 身份提供程序进行身份验证的用户组。
网络	列出服务中配置的现有网络范围。根据 IP 地址，选择要定向到此身份提供程序实例以进行身份验证的用户的网络范围。
身份验证方法	<p>显示为该服务配置的身份验证方法。选中要关联到此身份提供程序的身份验证方法所对应的复选框。</p> <p>对于设备合规性和密码，使用 AirWatch 和 AirWatch 连接器时，请确保在 AirWatch 配置页面上启用了此选项。</p>

5 单击添加。

配置内置身份提供程序连接

您可以配置多个内置身份提供程序，并为它们关联身份验证方法。

前提条件

如果使用内置 Kerberos 身份验证，请下载 KDC 颁发者证书，以便在 iOS 设备管理配置文件的 AirWatch 配置中使用。

步骤

- 1 选择**管理 > 身份目录管理 > 身份提供程序**。

此页面显示所有已配置的身份提供程序。

- 2 单击**添加身份提供程序**。

将显示包含身份提供程序选项的菜单。

- 3 选择**创建内置 IDP**。

- 4 输入相应信息以配置身份提供程序。

选项	描述
身份提供程序名称	为此内置身份提供程序实例输入一个名称。
用户	选择要进行身份验证的用户。将列出已配置的目录。
网络	列出服务中配置的现有网络范围。根据 IP 地址，选择要定向到此身份提供程序实例以进行身份验证的用户的网络范围。
身份验证方法	<p>显示为该服务配置的身份验证方法。选中要关联到此身份提供程序的身份验证方法所对应的复选框。</p> <p>对于设备合规性和密码，使用 AirWatch 和 AirWatch 连接器时，请确保在 AirWatch 配置页面上启用相应的选项。</p>

- 5 单击**添加**。

将替代用户身份验证产品与身份目录管理集成

通常，初始配置身份目录管理时，您可以使用随现有 vRealize Automation 基础架构提供的连接器创建 Active Directory 连接，以便实现基于用户 ID 和密码的身份验证和管理。或者，您也可以将身份目录管理与 Kerberos 或 RSA SecurID 等其他身份验证解决方案集成到一起。

身份提供程序实例可以是 Directories Management 连接器实例、第三方身份提供程序实例，或两者的组合。

用于 Directories Management 服务的身份提供程序实例将创建一个使用 SAML 2.0 断言与该服务进行通信的网内联合身份验证机构。

首次部署 Directories Management 服务时，连接器是该服务的初始身份提供程序。您的现有 Active Directory 基础架构将用于进行用户身份验证和管理。

下面是受支持的身份验证方法。您可以从管理控制台中配置这些身份验证方法。

表 2-8. 身份目录管理支持的用户身份验证类型

身份验证类型	描述
密码（内部部署）	配置 Active Directory 后无需任何其他配置，Directories Management 即可支持 Active Directory 密码身份验证。此方法直接通过 Active Directory 对用户进行身份验证。
适用于桌面的 Kerberos	Kerberos 身份验证允许域用户对其应用程序门户进行单点登录式访问。用户在登录到网络后，无需再次登录。
证书（内部部署）	可以配置基于证书的身份验证，以便允许客户端在其桌面和移动设备上使用证书进行身份验证，或者使用智能卡适配器进行身份验证。 基于证书的身份验证依赖于用户拥有的资源和掌握的信息。X.509 证书使用公钥基础架构标准来验证证书内包含的公钥是否属于用户。
RSA SecurID（内部部署）	如果配置了 RSA SecurID 身份验证，则将 Directories Management 配置为 RSA SecurID 服务器中的身份验证代理。RSA SecurID 身份验证要求用户使用基于令牌的身份验证系统。RSA SecurID 是一种适用于从企业网络外部访问 Directories Management 的用户的身份验证方法。
RADIUS（内部部署）	RADIUS 身份验证提供双因素身份验证选项。您可以设置 Directories Management 服务可访问的 RADIUS 服务器。在用户使用其用户名和通行码登录时，将向 RADIUS 服务器提交访问请求以进行身份验证。
RSA 自适应身份验证（内部部署）	RSA 身份验证提供了比针对 Active Directory 的仅用户名和密码身份验证更强的多因素身份验证。启用 RSA 自适应身份验证后，在风险策略中指定的风险指标将在 RSA 策略管理应用程序中设置。自适应身份验证的 Directories Management 服务配置用于确定所需的身份验证提示。
移动 SSO（适用于 iOS）	适用于 iOS 的移动 SSO 身份验证用于 AirWatch 管理的 iOS 设备的单点登录身份验证。移动 SSO（适用于 iOS）身份验证使用 Directories Management 服务中的密钥分发中心 (KDC)。在启用这种身份验证方法之前，您必须在 VMware Identity Manager 服务中启动 KDC 服务。
移动 SSO（适用于 Android）	适用于 Android 的移动 SSO 身份验证用于 AirWatch 管理的 Android 设备的单点登录身份验证。在 Directories Management 服务和 AirWatch 之间将设置代理服务，以便从 AirWatch 中检索用于身份验证的证书。
密码（AirWatch 连接器）	AirWatch Cloud Connector 可以与 Directories Management 服务进行集成，以便进行用户密码身份验证。您可以配置 Directories Management 服务以同步 AirWatch 目录中的用户。

用户将根据您配置的身份验证方法、默认访问策略规则、网络范围和身份提供程序实例进行身份验证。在配置了身份验证方法后，您可以创建访问策略规则，以指定设备类型所使用的身份验证方法。

■ 为 Directories Management 配置 SecurID

配置 RSA SecurID 服务器时，您必须在 RSA SecurID 服务器上添加 Directories Management 服务信息作为身份验证代理，并在 Directories Management 服务上配置 RSA SecurID 服务器信息。

■ 为 Directories Management 配置 RADIUS

您可以配置 Directories Management 以要求用户使用远程身份验证拨入用户服务 (Remote Authentication Dial-In User Service, RADIUS) 身份验证。您可以在 Directories Management 服务上配置 RADIUS 服务器信息。

- **配置用于身份目录管理的证书或智能卡适配器**

您可以配置 x509 证书身份验证，以便允许客户端在其桌面和移动设备上使用证书进行身份验证，或者使用智能卡适配器进行身份验证。基于证书的身份验证依赖于用户拥有的资源（私钥或智能卡）和掌握的信息（私钥的密码或智能卡的 PIN）。X.509 证书使用公钥基础架构 (Public Key Infrastructure, PKI) 标准来确认证书内包含的公钥是否属于用户。使用智能卡身份验证时，用户需要将智能卡与计算机相连接并输入 PIN。

- **配置第三方身份提供程序实例以验证用户身份**

您可以在 Directories Management 服务中配置第三方身份提供程序，以将其用于验证用户身份。

- **管理要应用于用户的身份验证方法**

Directories Management 服务尝试基于您配置的身份验证方法、默认访问策略、网络范围和身份提供程序实例对用户进行身份验证。

- **为 Directories Management 配置 Kerberos**

Kerberos 身份验证可在没有其他凭据提示的情况下，向成功登录到 Active Directory 域的用户提供对其应用程序门户的访问权限。您可以启用 Windows 身份验证，以允许 Kerberos 协议确保用户浏览器与 Directories Management 服务之间交互的安全。您不需要直接配置 Active Directory 以使 Kerberos 在您的部署中正常工作。

为 Directories Management 配置 SecurID

配置 RSA SecurID 服务器时，您必须在 RSA SecurID 服务器上添加 Directories Management 服务信息作为身份验证代理，并在 Directories Management 服务上配置 RSA SecurID 服务器信息。

在配置 SecurID 以提供额外的安全性时，您必须确保为 Directories Management 部署正确配置了网络。特别是对于 SecurID，必须确保打开了正确的端口才能允许 SecurID 对您网络外部的用户进行身份验证。

运行 Directories Management 设置向导并配置 Active Directory 连接之后，您便拥有了准备 RSA SecurID 服务器所需的信息。为 Directories Management 准备好 RSA SecurID 服务器之后，您可以在管理控制台中启用 SecurID。

- **准备 RSA SecurID 服务器**

必须使用有关作为身份验证代理的 Directories Management 设备的信息配置 RSA SecurID 服务器。所需的信息包括主机名和网络接口的 IP 地址。

- **配置 RSA SecurID 身份验证**

在 RSA SecurID 服务器中将身份目录管理配置为身份验证代理后，必须将 RSA SecurID 配置信息添加到连接器。

准备 RSA SecurID 服务器

必须使用有关作为身份验证代理的 Directories Management 设备的信息配置 RSA SecurID 服务器。所需的信息包括主机名和网络接口的 IP 地址。

前提条件

- 确认在企业网络中安装并正常运行了下列任一版本的 RSA Authentication Manager: RSA AM 6.1.2、7.1 SP2 及更高版本和 8.0 及更高版本。Directories Management 服务器使用 AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1)，此版本仅支持上述版本的 RSA Authentication Manager (RSA SecurID 服务器)。有关安装和配置 RSA Authentication Manager (RSA SecurID 服务器) 的信息，请参阅 RSA 文档。

步骤

- 1 在受支持版本的 RSA SecurID 服务器上，将 Directories Management Connector 添加为身份验证代理。输入以下信息。

选项	描述
主机名	Directories Management 的主机名。
IP 地址	Directories Management 的 IP 地址。
备用 IP 地址	如果来自连接器的通信通过网络地址转换 (Network Address Translation, NAT) 设备抵达 RSA SecurID 服务器，请输入设备的私有 IP 地址。

- 2 下载压缩的配置文件，解压缩 `sdconf.rec` 文件。

在 Directories Management 中配置 RSA SecurID 时，需要上载此文件。

后续步骤

转到管理控制台，在“身份和访问管理”选项卡的“设备”页面中选择连接器，并在“身份验证适配器”页面中配置 SecurID。

配置 RSA SecurID 身份验证

在 RSA SecurID 服务器中将身份目录管理配置为身份验证代理后，必须将 RSA SecurID 配置信息添加到连接器。

前提条件

- 验证 RSA Authentication Manager (RSA SecurID 服务器) 已妥善安装和正确配置。
- 从 RSA SecurID 服务器中下载压缩文件，并解压缩服务器配置文件。

步骤

- 1 作为租户管理员，导航到 **管理 > 身份目录管理 > 连接器**
- 2 在“连接器”页面上，选择为其配置 RSA SecurID 的连接器所对应的“工作线程”链接。
- 3 单击 **身份验证适配器**，然后单击 **SecurIDIdpAdapter**。

将重定向到 Identity Manager 登录页面。

- 4 在“身份验证适配器”页面的“SecurIDdpAdapter”行中，单击**编辑**。
- 5 配置 SecurID “身份验证适配器”页面。

配置 SecurID 页面时需要提供在 RSA SecurID 服务器上使用的信息和生成的文件。

选项	操作
名称	名称必填。默认名称为 SecurIDdpAdapter。您可以对其进行更改。
启用 SecurID	选中此框以启用 SecurID 身份验证。
允许的身份验证尝试次数	输入在使用 RSA SecurID 令牌时的最大失败登录尝试次数。默认为尝试 5 次。
Connector 地址	输入连接器实例的 IP 地址。您输入的值必须与将连接器设备作为身份验证代理添加到 RSA SecurID 服务器时所使用的值一致。如果您的 RSA SecurID 服务器有一个值分配到备用 IP 地址提示，请输入该值作为连接器的 IP 地址。如果未分配备用 IP 地址，请输入分配在 IP 地址提示中的值。
代理 IP 地址	在 RSA SecurID 服务器中输入分配给 IP 地址提示的值。
服务器配置	上载 RSA SecurID 服务器配置文件。首先，您必须从 RSA SecurID 服务器中下载压缩文件，然后解压缩默认名称为 <code>sdconf.rec</code> 的服务器配置文件。
节点机密	保留“节点密码”字段为空将允许自动生成节点密码。建议您清除 RSA SecurID 服务器上的节点密码文件，并有意不要上载节点密码文件。确保 RSA SecurID 服务器和服务器连接器实例中的节点密码文件始终保持一致。如果您更改一个位置中的节点密码，也请相应更改另一个位置中的节点密码。

- 6 单击**保存**。

后续步骤

将该身份验证方法添加到默认访问策略。导航到**管理 > 身份目录管理 > 策略**，然后单击**编辑默认策略**以编辑默认策略规则，从而将 SecurID 身份验证方法按正确的身份验证顺序添加到该规则中。

为 Directories Management 配置 RADIUS

您可以配置 Directories Management 以要求用户使用远程身份验证拨入用户服务 (Remote Authentication Dial-In User Service, RADIUS) 身份验证。您可以在 Directories Management 服务上配置 RADIUS 服务器信息。

RADIUS 支持提供了多种不同的替代双因素基于令牌的身份验证选项。由于双因素身份验证解决方案（如 RADIUS）使用在不同的服务器上安装的身份验证管理器，您必须配置 RADIUS 服务器并且 Identity Manager 服务可以访问该服务器。

如果用户登录到其“我的应用程序”门户并启用了 RADIUS 身份验证，则会在浏览器中显示一个特殊登录对话框。用户在登录对话框中输入其 RADIUS 身份验证用户名和通行码。如果 RADIUS 服务器发出一个访问质询，Identity Manager 服务将显示一个对话框以提示输入第二个通行码。目前，RADIUS 质询支持仅限于提示输入文本。

在用户在对话框中输入凭据后，RADIUS 服务器可能使用某种其他带外机制向用户的手机发送短信、电子邮件或文本以及代码。用户可以在登录对话框中输入该文本和代码以完成身份验证。

如果 RADIUS 服务器提供了从 Active Directory 中导入用户的功能，则可能先提示最终用户提供 Active Directory 凭据，然后再提示输入 RADIUS 身份验证用户名和通行码。

准备 RADIUS 服务器

设置 RADIUS 服务器，然后将其配置为从 Directories Management 服务中接收 RADIUS 请求。

有关设置 RADIUS 服务器的信息，请参阅 RADIUS 供应商的设置指南。记下 RADIUS 配置信息，因为在该服务中配置 RADIUS 时需要使用这些信息。要查看配置 Directories Management 所需的 RADIUS 信息类型，请参见[在身份目录管理中配置 RADIUS 身份验证](#)。

您可以设置一个辅助 RADIUS 身份验证服务器以用于实现高可用性。如果主 RADIUS 服务器在为 RADIUS 身份验证配置的服务器超时内没有响应，则将请求路由到辅助服务器。在主服务器没有响应时，辅助服务器接收所有将来的身份验证请求。

在身份目录管理中配置 RADIUS 身份验证

您可以在身份验证管理器服务器上启用 RADIUS 软件。对于 RADIUS 身份验证，请按照供应商的配置文档进行操作。

前提条件

在身份验证管理器服务器上安装并配置 RADIUS 软件。对于 RADIUS 身份验证，请按照供应商的配置文档进行操作。

您需要了解以下 RADIUS 服务器信息以在该服务上配置 RADIUS。

- RADIUS 服务器的 IP 地址或 DNS 名称。
- 身份验证端口号。身份验证端口通常为 1812。
- 身份验证类型。身份验证类型包括 PAP（密码身份验证协议）、CHAP（质询握手身份验证协议）、MSCHAP1 和 MSCHAP2（Microsoft 质询握手身份验证协议版本 1 和 2）。
- 用于在 RADIUS 协议消息中加密和解密的 RADIUS 共享密钥。
- RADIUS 身份验证所需的特定超时和重试值。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 连接器**。
- 2 在“连接器”页上，选择为 RADIUS 身份验证配置的连接器的“工作线程”链接。
- 3 单击**身份验证适配器**，然后单击 **RadiusAuthAdapter**。
将重定向到 Identity Manager 登录页面。
- 4 单击**编辑**以在“身份验证适配器”页上配置这些字段。

选项	操作
名称	名称必填。默认名称为 RadiusAuthAdapter。您可以对其进行更改。
启用 Radius 适配器	选中此框以启用 RADIUS 身份验证。
允许的身份验证尝试次数	输入在使用 RADIUS 登录时的最大失败登录尝试次数。默认为尝试 5 次。

选项	操作
尝试访问 Radius 服务器的次数	指定总重试次数。如果主服务器没有响应，该服务将等待配置的时间后再重试。
Radius 服务器主机名/地址	输入 RADIUS 服务器的主机名或 IP 地址。
身份验证端口	输入 Radius 身份验证端口号。该端口通常是 1812。
计帐端口	输入 0 以作为端口号。目前不使用计帐端口。
身份验证类型	输入 RADIUS 服务器支持的身份验证协议。PAP、CHAP、MSCHAP1 或 MSCHAP2。
共享密码	输入在 RADIUS 服务器和 VMware Identity Manager 服务之间使用的共享密码。
服务器超时 (秒)	输入 RADIUS 服务器超时 (秒)；如果 RADIUS 服务器没有响应，将在这段时间过后发送重试。
领域前缀	<p>(可选) 用户帐户位置称为领域。</p> <p>如果指定领域前缀字符串，在将用户名发送到 RADIUS 服务器时，将该字符串放在名称的开头。例如，如果输入用户名 jdoe 并指定领域前缀 DOMAIN-A\，则将用户名 DOMAIN-A\jdoe 发送到 RADIUS 服务器。</p> <p>如果未配置这些字段，则仅发送输入的用户名。</p>
领域后缀	<p>(可选) 如果指定领域后缀，则将该字符串放在用户名的末尾。例如，如果后缀为 @myco.com，则将用户名 jdoe@myco.com 发送到 RADIUS 服务器。</p>
登录页密码短语提示	<p>输入在用户登录页面上的消息中显示的文本字符串，以指示用户输入正确的 RADIUS 通行码。例如，如果该字段配置为 AD password first and then SMS passcode，则登录页消息显示 Enter your AD password first and then SMS passcode。默认文本字符串为 RADIUS Passcode。</p>

5 您可以启用辅助 RADIUS 服务器以实现高可用性。

请按照步骤 4 中所述配置辅助服务器。

6 单击保存。

后续步骤

将 RADIUS 身份验证方法添加到默认访问策略中。选择 **管理 > 身份目录管理 > 策略**，然后单击 **编辑默认策略** 以编辑默认策略规则，从而将 RADIUS 身份验证方法按正确的身份验证顺序添加到该规则中。

配置用于身份目录管理的证书或智能卡适配器

您可以配置 x509 证书身份验证，以便允许客户端在其桌面和移动设备上使用证书进行身份验证，或者使用智能卡适配器进行身份验证。基于证书的身份验证依赖于用户拥有的资源（私钥或智能卡）和掌握的信息（私钥的密码或智能卡的 PIN）。X.509 证书使用公钥基础架构 (Public Key Infrastructure, PKI) 标准来确认证书内包含的公钥是否属于用户。使用智能卡身份验证时，用户需要将智能卡与计算机相连接并输入 PIN。

智能卡证书会复制到用户计算机上的本地证书存储。本地证书存储中的证书可用于在此用户的计算机上运行的所有浏览器，但有一些例外。

注 如果配置了证书身份验证并在负载均衡器后面设置了服务设备，请确保连接器在负载均衡器上配置为使用 SSL 直通且未配置为终止 SSL。这种配置可确保在连接器和客户端之间进行 SSL 握手，以便将证书传递给连接器。您可以在配置了 SSL 直通的其他负载均衡器后配置其他连接器，并在这些连接器上启用并配置基于证书的身份验证。

使用用户主体名称进行证书身份验证

您可以在 Active Directory 中使用证书映射。证书和智能卡登录使用 Active Directory 中的用户主体名称 (User Principal Name, UPN) 来验证用户帐户。对于尝试在 Directories Management 服务中进行身份验证的用户，其 Active Directory 帐户必须具有与证书中的 UPN 对应的有效 UPN。

您可以将 Directories Management 配置为在证书中不存在 UPN 时使用电子邮件地址来验证用户帐户。

您也可以启用备用 UPN 类型。

身份验证所需的证书颁发机构

要启用使用证书身份验证进行登录，必须将根证书和中间证书上载至 Directories Management。

证书会复制到用户计算机上的本地证书库。本地证书库中的证书可用于此用户计算机上运行的所有浏览器（但有一些例外情况），因此也可用于浏览器中的 Directories Management 实例。

对于智能卡身份验证，当用户初始化与 Directories Management 实例的连接时，Directories Management 服务会将受信任的证书颁发机构 (Certificate Authority, CA) 列表发送至浏览器。浏览器会根据可用的用户证书检查受信任的 CA 列表，选择合适的证书，然后提示用户输入智能卡 PIN。如果有多个可用的有效用户证书，则浏览器会提示用户选择一个证书。

如果用户无法进行身份验证，可能是因为根 CA 和中间 CA 的设置不正确，或者将根 CA 和中间 CA 上载到服务器后尚未重新启动服务。在这些情况下，浏览器无法显示安装的证书，并且用户无法选择正确的证书，所以证书身份验证将会失败。

使用证书吊销检查

您可以配置证书吊销检查，以防止已吊销其用户证书的用户进行身份验证。当用户离开组织、丢失智能卡或者从一个部门转到另一个部门时，通常会吊销证书。

系统支持使用证书吊销列表 (CRL) 和在线证书状态协议 (OCSP) 来执行证书吊销检查。CRL 是由颁发证书的 CA 所发布的吊销证书列表。OCSP 是用来获取证书吊销状态的证书验证协议。

在配置证书身份验证时，您可以在管理控制台的“连接器”>“身份验证适配器”>“CertificateAuthAdapter”页中配置证书吊销检查。

CRL 和 OCSP 可以在同一证书身份验证适配器配置中进行配置。配置这两种类型的证书吊销检查并启用“OCSP 失败时使用 CRL”复选框后，将首先检查 OCSP，如果 OCSP 失败，则吊销检查会退回到 CRL。但如果 CRL 失败，吊销检查不会退回到 OCSP。

通过 CRL 检查登录

启用证书吊销后，Directories Management 服务器会读取 CRL，以确定用户证书的吊销状态。

如果证书已吊销，则通过证书进行的身份验证会失败。

通过 OCSP 证书检查登录

配置证书状态协议 (OCSP) 吊销检查后，Directories Management 会发送请求到 OCSP 响应者，以确定特定用户证书的吊销状态。Directories Management 服务器使用 OCSP 签名证书来验证从 OCSP 响应者收到的响应是否真实。

如果证书已吊销，则身份验证会失败。

您可以将身份验证配置为在没有收到来自 OCSP 响应者的响应或在响应无效时，退回到 CRL 检查。

为身份目录管理配置证书身份验证

您可以从 vRealize Automation 管理控制台的“身份目录管理”功能中启用并配置证书身份验证。

注 如果您使用第三方身份提供程序，如 Keberos 或智能卡身份验证，系统管理员必须为您的 vRealize Automation 部署配置外部连接器。

前提条件

- 从对用户提供的证书进行签名的 CA 那里获取根证书和中间证书。
- （可选）用于证书身份验证的有效证书策略的对象标识符 (Object Identifier, OID) 列表。
- 对于吊销检查，CRL 的文件位置，以及 OCSP 服务器的 URL。
- （可选）OCSP 响应签名证书文件位置。
- 同意表单内容（如果要在身份验证前显示同意表单）。

步骤

- 1 作为租户管理员，导航到**管理 > 身份目录管理 > 连接器**
- 2 在“连接器”页面上，选择要配置的连接器的“工作线程”链接。
- 3 单击**身份验证适配器**，然后单击 **CertificateAuthAdapter**。
将重定向到 Identity Manager 登录页面。
- 4 在 CertificateAuthAdapter 行中，单击**编辑**。
- 5 配置“证书身份验证适配器”页。

注 星号表示必填字段。其他所有字段都是可选字段。

选项	描述
*名称	名称必填。默认名称为 CertificateAuthAdapter。您可以对此名称进行更改。
启用证书适配器	选中此复选框以启用证书身份验证。
*根 CA 证书和中间 CA 证书	选择要上载的证书文件。您可以选择多个编码为 DER 或 PEM 的根 CA 证书和中间 CA 证书。
上载的 CA 证书	<p>将在表单的“上载的 CA 证书”部分中列出上载的证书文件。</p> <p>必须重新启动该服务，然后才能使用新证书。</p> <p>单击重新启动 Web 服务以重新启动该服务，并将证书添加到受信任的服务中。</p>
<p>注 重新启动服务不会启用证书身份验证。在重新启动该服务后，请继续配置该页面。如果单击页面底部的保存，则会在该服务上启用证书身份验证。</p>	

选项	描述
证书中没有 UPN 时使用电子邮件	如果用户主体名称 (User Principal Name, UPN) 在证书中不存在, 请选中此复选框以将 emailAddress 属性作为使用者备用名称扩展以验证用户帐户。
接受的证书策略	创建在证书策略扩展中接受的对象标识符列表。 输入证书颁发策略的对象 ID 号 (Object ID, OID)。单击 添加其他值 以添加其他 OID。
启用证书吊销	选中此复选框以启用证书吊销检查。这可防止已吊销用户证书的用户进行身份验证。
使用证书中的 CRL	选中此复选框以使用颁发证书的 CA 发布的证书吊销列表 (Certificate Revocation List, CRL) 验证证书的状态 (吊销或未吊销)。
CRL 位置	输入从中检索 CRL 的服务器文件路径或本地文件路径。
启用 OCSP 吊销	选中此复选框以使用在线证书状态协议 (Online Certificate Status Protocol, OCSP) 证书验证协议获取证书的吊销状态。
OCSP 失败时使用 CRL	如果配置了 CRL 和 OCSP, 您可以选中此复选框以在 OCSP 检查不可用时改用 CRL。
发送 OCSP 随机值	如果您希望在响应中发送 OCSP 请求的唯一标识符, 请选中此复选框。
OCSP URL	如果启用了 OCSP 吊销, 请输入 OCSP 服务器地址以进行吊销检查。
OCSP 响应者的签名证书	输入响应者的 OCSP 证书路径 (<i>/path/to/file.cer</i>)。
在身份验证前启用同意表单	选中此复选框以包含在用户使用证书身份验证登录到其“我的应用程序”门户之前显示的同意表单页面。
同意表单内容	在此文本框中键入同意表单中显示的文本。

6 单击保存。

后续步骤

- 将证书身份验证方法添加到默认访问策略。导航到**管理 > 身份目录管理 > 策略**, 单击**编辑默认策略**以编辑默认策略规则, 然后添加“证书”并使其成为默认策略的第一个身份验证方法。证书必须是策略规则中列出的第一个身份验证方法, 否则, 证书身份验证将失败。
- 如果配置了证书身份验证并在负载均衡器后面设置服务设备, 请确保 Directories Management 连接器在负载均衡器上配置为使用 SSL 直通且未配置为终止 SSL。这种配置可确保在连接器和客户端之间进行 SSL 握手以便将证书传递给连接器。

配置第三方身份提供程序实例以验证用户身份

您可以在 Directories Management 服务中配置第三方身份提供程序, 以将其用于验证用户身份。

使用管理控制台添加第三方身份提供程序实例之前, 请完成下列任务。

- 确认第三方实例符合 SAML 2.0 标准, 并且服务可以访问第三方实例。
- 获取相应的第三方元数据信息, 以便在管理控制台中配置身份提供程序时添加该信息。您从第三方实例获取的元数据信息可以是元数据的 URL 或实际的元数据。

配置第三方身份提供程序连接

vRealize Automation 附带一个默认身份提供程序连接实例。用户可能希望创建更多身份提供程序连接，以支持即时用户置备或其他自定义配置。

vRealize Automation 提供了默认身份提供程序。在大多数情况下，默认提供程序足以满足客户需求。如果使用现有的企业身份管理解决方案，则可设置自定义身份提供程序，将用户重定向到现有身份解决方案。

使用自定义身份提供程序时，身份目录管理将使用从该提供程序获得的 SAML 元数据与提供程序建立信任关系。建立此关系之后，身份目录管理可根据主题名称 ID 将 SAML 断言中的用户映射到 vRealize Automation 内部用户列表。

前提条件

- 配置要定向到此身份提供程序实例进行身份验证的网络范围。请参见[添加或编辑网络范围](#)。
- 有权访问第三方元数据文档。这可以是指向元数据的 URL 或实际元数据。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 身份提供程序**。

此页面显示所有已配置的身份提供程序。

- 2 单击**添加身份提供程序**。

将显示包含身份提供程序选项的菜单。

- 3 选择**创建第三方 IDP**。

- 4 输入相应信息以配置身份提供程序。

选项	描述
身份提供程序名称	输入此身份提供程序实例的名称。
SAML 元数据	<p>添加第三方 IdP 基于 XML 的元数据文档，以便与身份提供程序建立信任关系。</p> <ol style="list-style-type: none"> 1 在文本框中输入 SAML 元数据 URL 或 xml 内容。 2 单击处理 IdP 元数据。将从元数据中提取 IdP 支持的 NameID 格式，并将其添加到“名称 ID 格式”表中。 3 在“名称 ID 值”列中，在该服务中选择用户属性以映射到显示的 ID 格式。您可以添加自定义第三方名称 ID 格式并将其映射到服务中的用户属性值。 4 （可选）选择 NameIDPolicy 响应标识符字符串格式。
用户	选择可使用此身份提供程序进行身份验证的用户的 Directories Management 目录。
即时用户置备	<p>选择相应选项以支持使用相应第三方身份提供程序进行即时置备。</p> <p>输入要用于即时置备的目录名称。</p> <p>输入要用于即时置备的外部身份提供程序中存在的一个或多个域。</p>
网络	<p>此处列出了在服务中配置的现有网络范围。</p> <p>根据用户 IP 地址，选择要定向到此身份提供程序实例进行身份验证的用户的网络范围。</p>
身份验证方法	添加受第三方身份提供程序支持的身份验证方法。选择支持身份验证方法的 SAML 身份验证上下文类。

选项	描述
SAML 签名证书	单击 服务提供程序 (SP) 元数据 以查看 Directories Management SAML 服务提供程序元数据 URL。复制并保存该 URL。在第三方身份提供程序中编辑 SAML 断言以映射 Directories Management 用户时，将配置该 URL。
Hostname	如果显示 主机名 字段，请输入将身份提供程序重定向到的主机名以进行身份验证。如果使用 443 以外的非标准端口，则可以将其设置为“主机名:端口”。例如，myco.example.com:8443。

5 单击添加。

后续步骤

- 复制并保存 Directories Management 服务提供程序元数据，在配置第三方身份提供程序实例时需要该数据。此元数据在“身份提供程序”页面的“SAML 签名证书”部分中可用。
- 向服务默认策略中添加身份提供程序的身份验证方法。

有关添加资源和对添加到目录中的资源进行自定义的信息，请参见《在 Directories Management 中设置资源》指南。

管理要应用于用户的身份验证方法

Directories Management 服务尝试基于您配置的身份验证方法、默认访问策略、网络范围和身份提供程序实例对用户进行身份验证。

在用户尝试登录时，服务会评估默认访问策略规则，以便选择要应用策略中的哪个规则。身份验证方法将按照它们在规则中列出的先后顺序加以应用。满足规则的身份验证方法和网络范围要求的第一个身份提供程序实例将被选中，然后用户身份验证请求将被转发到该身份提供程序实例进行身份验证。如果身份验证失败，则应用规则中配置的下一个身份验证方法。

您可以添加规则，指定按照设备类型或按照设备类型和在特定网络范围中使用的身份验证方法。例如，您可以配置一项规则，要求使用 iOS 设备从特定网络登录的用户使用 RSA SecurID 进行身份验证，并配置另一项规则，指定从内部网络 IP 地址登录的所有设备类型使用密码进行身份验证。

添加或编辑网络范围

您可以管理网络范围，定义用户可通过 Active Directory 链接登录的 IP 地址。您可以将创建的网络范围添加到特定身份提供程序实例和访问策略规则中。

根据您的网络拓扑定义 Directories Management 部署的网络范围。

将创建一个名为“所有范围”的网络范围以作为默认范围。该网络范围包括 Internet 上的所有可用 IP 地址（0.0.0.0 到 255.255.255.255）。即使您的部署只有一个身份提供程序实例，您也可以更改 IP 地址范围，以及添加其他范围以排除或包含默认网络范围中的特定 IP 地址。您可以创建其他网络范围以包含可为特定目的应用的特定 IP 地址。

注 默认网络范围（“所有范围”）及其描述（“面向所有范围的网路”）是可以编辑的。您可以通过单击“网络范围”页面上的网络范围名称来编辑此名称和描述，包括将文本更改为其他语言。

前提条件

- 您已为 vRealize Automation 部署配置租户，且已设置适当的 Active Directory 链接，可以支持基本的 Active Directory 用户 ID 和密码身份验证。

- 已安装并配置 Active Directory 供网络上使用。
- 以租户管理员身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 网络范围**。
- 2 编辑现有网络范围或添加新的网络范围。

选项	描述
编辑现有范围	单击要编辑的网络范围名称。
添加范围	单击 添加网络范围 以添加新范围。

- 3 完成表单填写。

表单项目	描述
名称	输入网络范围的名称。
描述	输入对网络范围的描述。
View 容器	“View 容器”选项仅在启用 View 模块后显示。 Client 访问 URL 主机。输入该网络范围的正确 Horizon Client 访问 URL。 Client 访问端口。输入该网络范围的正确 Horizon Client 访问端口号。
IP 范围	编辑或添加 IP 范围，直到所有需要和不需要的 IP 地址都包含在内。

后续步骤

- 将每个网络范围与身份提供程序实例相关联。
- 根据需要将网络范围与访问策略规则相关联。请参见[配置访问策略设置](#)。

选择要与目录同步的属性

在设置 Directories Management 目录与 Active Directory 同步时，您可以指定将同步到目录的用户属性。在设置目录之前，您可以在“用户属性”页面上指定必需的默认属性，并根据需要添加要映射到 Active Directory 属性的其他属性。

在创建目录之前配置“用户属性”页面时，您可以执行下列操作：将默认属性从必需更改为不必需，将属性标记为必需，以及添加自定义属性。

有关默认映射属性的列表，请参见[管理从 Active Directory 同步的用户属性](#)。

在创建目录之后，您可以将必需属性更改为不必需，还可以删除自定义属性。但您无法将属性更改为必需属性。

在创建目录之后添加其他要同步到目录的属性时，可转到目录的“映射的属性”页面，以便将这些属性映射到 Active Directory 属性。

步骤

- 1 以系统或租户管理员身份登录到 vRealize Automation。
- 2 单击“管理”选项卡。

- 3 选择**身份目录管理 > 用户属性**。
- 4 在“默认属性”部分中，查看必需属性列表，并做出相应的更改以反映哪些属性应当是必需的。
- 5 在“属性”部分中，将 Directories Management 目录属性名称添加到列表中。
- 6 单击**保存**。
默认属性状态将会更新，并且您添加的属性将会添加到目录的“映射的属性”列表中。
- 7 创建目录后，请转到“身份存储”页面并选择该目录。
- 8 单击**同步设置 > 映射的属性**。
- 9 在您添加的属性的下拉菜单中，选择要映射到的 Active Directory 属性。
- 10 单击**保存**。

结果

下次该目录同步到 Active Directory 时，即会更新目录。

应用默认访问策略

Directories Management 服务包含一个默认访问策略，可以控制用户对其应用程序门户的访问。如有必要，您可以编辑此策略来更改策略规则。

如果您启用除密码身份验证以外的身份验证方法，则必须编辑默认策略才能将启用的身份验证方法添加到策略规则中。

要允许用户访问应用程序门户，默认访问策略中的每个规则都必须满足一组条件。您可以应用网络范围、选择可访问内容的用户类型，以及选择要使用的身份验证方法。请参见[管理访问策略](#)。

服务使用给定的身份验证方法尝试让用户登录的次数因方法而异。对于 Kerberos 或证书身份验证，服务仅尝试对用户进行一次身份验证。如果用户无法通过该身份验证方法成功登录，将尝试规则中的下一个身份验证方法。对于 Active Directory 密码和 RSA SecurID 身份验证，最大的登录尝试失败次数默认设置为五次。用户尝试登录失败五次后，服务将尝试使用列表中的下一个身份验证方法使用户登录。当所有身份验证方法都已用尽时，服务会发出一条错误消息。

将身份验证方法应用于策略规则

默认策略规则中仅配置了密码身份验证方法。您必须编辑策略规则以选择配置的其他身份验证方法，并设置在身份验证时使用这些方法的顺序。

前提条件

启用并配置您的组织支持的身份验证方法。请参见[将替代用户身份验证产品与身份目录管理集成](#)

步骤

- 1 选择**管理 > 身份目录管理 > 策略**。
- 2 单击要编辑的默认访问策略。
- 3 要编辑策略规则，请在“策略规则 > 身份验证方法”列中单击要编辑的身份验证方法。

要添加新的策略规则，请单击 **+** 图标。

- 4 单击**保存**，然后在“策略”页面上再次单击**保存**。

编辑策略规则

- 5 单击**保存**，然后在“策略”页面上再次单击**保存**。

为 Directories Management 配置 Kerberos

Kerberos 身份验证可在没有其他凭据提示的情况下，向成功登录到 Active Directory 域的用户提供对其应用程序门户的访问权限。您可以启用 Windows 身份验证，以允许 Kerberos 协议确保用户浏览器与 Directories Management 服务之间交互的安全。您不需要直接配置 Active Directory 以使 Kerberos 在您的部署中正常工作。

目前，用户浏览器与服务之间的交互仅由 Windows 操作系统上的 Kerberos 进行身份验证。从其他操作系统访问服务时不会用到 Kerberos 身份验证。

■ 配置 Kerberos 身份验证

要配置 Directories Management 服务以提供 Kerberos 身份验证，您必须加入域并在 Directories Management 连接器上启用 Kerberos 身份验证。

■ 配置 Internet Explorer 以访问 Web 界面

如果您为自己的部署配置了 Kerberos，并且希望授予用户使用 Internet Explorer 访问 Web 界面的权限，则您必须配置 Internet Explorer 浏览器。

■ 配置 Firefox 以访问 Web 界面

如果您为自己的部署配置了 Kerberos，并且希望授予用户使用 Firefox 访问 Web 界面的权限，则您必须配置 Firefox 浏览器。

■ 配置 Chrome 浏览器以访问 Web 界面

如果您为自己的部署配置了 Kerberos，并且希望授予用户使用 Chrome 浏览器访问 Web 界面的权限，则您必须配置 Chrome 浏览器。

配置 Kerberos 身份验证

要配置 Directories Management 服务以提供 Kerberos 身份验证，您必须加入域并在 Directories Management 连接器上启用 Kerberos 身份验证。

前提条件

- 在 vCenter 中部署 NSX Edge 并配置 NSX 负载均衡器。有关设置负载均衡器的信息，请参见 vRealize Automation 负载均衡。

- 将域加入主租户。必须在单独的租户中创建目录连接之前执行此操作。
 - a 以 administrator@vsphere.local 身份登录到默认租户。
 - b 创建本地用户 TestUser，并输入 TestUser 作为租户管理员。
 - c 选择**管理 > 身份目录管理 > 连接器**。
 - d 在每个设备连接器上选择“加入域”。
 - e 在“加入域”上，选择“自定义域”，然后输入希望租户连接的域以及要连接的凭据和 OU。
- 为默认租户和非默认租户设置目录连接。Kerberos 身份验证与集成 Windows 身份验证以及基于 LDAP 的 Active Directory 配合使用。请参见[配置通过 LDAP/IWA 链路访问的 Active Directory](#)和[配置 OpenLDAP 目录连接](#)。
- 确保 vRealize Automation 节点主机名与要加入的 Active Directory 域相匹配。例如，如果 vRealize Automation 要加入名为 COMPANY.COM 的 Active Directory 领域，则主机名应为 node.company.com。
- 配置 Workspace 身份提供程序。确保部署中的所有节点均在 Workspace 身份提供程序中注册，并且已定义负载均衡器名称。
 - a 选择**管理 > 身份目录管理 > 身份提供程序**。
 - b 选择适当的身份提供程序链接。
例如，WorkspacelDP_1。
 - c 单击身份提供程序链接，然后找到配置的 IdP 主机名。记录主机名，因为配置 Web 浏览器时将需要该主机名。
 - d 在 Workspace IdP 中注册所有适用节点，然后输入负载均衡器 FQDN 作为主机名。
 - e 单击**保存**。
- 为默认租户配置租户目录。请参见安装 vRealize Automation 中的“配置对默认租户的访问权限”。

步骤

- 1 作为租户管理员，导航到**管理 > 身份目录管理 > 连接器**。
- 2 在“连接器”页面上，对于要为其配置 Kerberos 身份验证的连接器，单击**加入域**。
- 3 在“加入域”页面上，输入 Active Directory 域的信息。

选项	描述
域	输入 Active Directory 的完全限定域名。您输入的域名必须与连接器服务器所在的域是同一个 Windows 域。
域用户	输入有权将系统加入该 Active Directory 域的 Active Directory 帐户的用户名。
域密码	输入与该 AD 用户名关联的密码。Directories Management 不会保存此密码。 。

单击**保存**。

此时“加入域”页面将刷新并显示一条表明您当前已加入该域的消息。

- 4 在连接器的“工作线程”列中，单击**身份验证适配器**。

- 5 单击 **KerberosIdpAdapter**。

将重定向到 Identity Manager 登录页面。

- 6 单击“KerberosIdpAdapter”行中的**编辑**并配置 Kerberos 身份验证页面。

选项	描述
名称	名称必填。默认名称为 KerberosIdpAdapter。您可以对其进行更改。
目录 UID 属性	输入包含用户名的帐户属性。
启用 Windows 身份验证	选中此选项可扩展用户浏览器与 Directories Management 之间的身份验证交互。
启用 NTLM	选中此选项可仅在您的 Active Directory 基础架构依赖于 NT LAN 管理器 (NTLM) 身份验证时启用基于 NTLM 协议的身份验证。
启用重定向	如果循环 DNS 和负载均衡器不支持 Kerberos，请选中此选项。身份验证请求将重定向至“重定向主机名”。如果选中此选项，请在 重定向主机名 文本框中输入重定向主机名。这通常是该服务的主机名。

- 7 单击**保存**。

- 8 在所有适用的节点上配置 Kerberos 身份验证。

- a 选择**管理 > 身份目录管理 > 连接器**。

此页面将显示当前配置的连接。默认情况下，仅配置密码身份验证。

- b 单击与第一个 vRealize Automation 设备 关联的工作线程超链接。

- c 单击 KerberosIdpAdapter 链接以打开身份验证页面。

您可能需要输入密码并重新启动 KerberosIdpAdapter 链接。

- d 提供目录 UID 属性并输入默认值 sAMAccountName。

- e 选中**启用 Windows 身份验证**和**启用重定向**复选框。

- f 不选中 **NTLM**，因为仅旧版域控制器需要此选项。

- g 输入 VA1 设备的名称作为“重定向主机名”。

- h 单击**保存**。

- 9 配置默认访问策略。Kerberos 配置需要三个访问策略：Kerberos、密码、本地密码。

- a 选择**管理 > 身份目录管理 > 策略**。

- b 选择 default_access_policy_set。

- c 单击 Web 浏览器行上“身份验证方法”标题下的超链接值“密码”。

- d 单击绿色 + 图标，为 Kerberos、密码和密码（本地目录）创建新的身份验证方法。

- e 对于每种身份验证方法，选择“所有范围”作为用户的网络范围，选择“Web 浏览器”作为用户的内容访问方法。
- f 将第一种身份验证方法更改为 Kerberos，并将故障恢复方法设置为密码。
- g 单击**保存**，然后单击**确定**。

配置 Internet Explorer 以访问 Web 界面

如果您为自己的部署配置了 Kerberos，并且希望授予用户使用 Internet Explorer 访问 Web 界面的权限，则您必须配置 Internet Explorer 浏览器。

Kerberos 身份验证可在 Windows 操作系统中与 Directories Management 配合使用。

注 请不要在其他操作系统中执行这些与 Kerberos 相关的步骤。

前提条件

为每位用户配置 Internet Explorer 浏览器或在配置 Kerberos 后向用户提供说明。

步骤

- 1 验证您是否以隶属于域的用户身份登录 Windows。
- 2 在 Internet Explorer 中，启用自动登录。
 - a 选择 **工具 > Internet 选项 > 安全性**。
 - b 单击**自定义级别**。
 - c 选择**只在 Intranet 区域自动登录**。
 - d 单击**确定**。
- 3 确认连接器虚拟设备的此实例包含在本地 Intranet 区域中。
 - a 使用 Internet Explorer 访问 Directories Management 登录 URL `https://myconnectorhost.domain/authenticate/`。
 - b 在浏览器窗口状态栏的右下角查找该区域。
如果该区域属于本地 Intranet，则 Internet Explorer 配置完成。
- 4 如果该区域不属于本地 Intranet，请将 Directories Management 登录 URL 添加到 Intranet 区域。
 - a 选择**工具 > Internet 选项 > 安全性 > 本地 Intranet > 站点**。
 - b 选择**自动检测 Intranet 网络**。
如果之前未选择此选项，则选择此选项可能就可以将 添加到 Intranet 区域。
 - c （可选）如果您已选择**自动检测 Intranet 网络**，请单击**确定**直到所有的对话框都关闭。
 - d 在“本地 Intranet”对话框中，单击**高级**。
将显示另一个名为“本地 Intranet”的对话框。

- e 在将该网站添加到区域中文本框中输入 Directories Management URL。
https://myconnectorhost.domain/authenticate/
 - f 单击**添加 > 关闭 > 确定**。
- 5** 验证是否允许 Internet Explorer 将 Windows 身份验证传递到受信任的站点。
- a 在“Internet 选项”对话框中，单击**高级选项卡**。
 - b 选择**启用集成 Windows 身份验证**。
您只有重新启动 Internet Explorer 后此选项才可生效。
 - c 单击**确定**。
- 6** 登录到 Web 界面以检查访问情况。
- 如果 Kerberos 身份验证成功，则测试 URL 将转到 Web 界面。

结果

Kerberos 协议可以确保 Internet Explorer 浏览器实例与 Directories Management 之间的所有交互的安全性。现在，用户可以使用单点登录访问其“我的应用程序”门户。

配置 Firefox 以访问 Web 界面

如果您为自己的部署配置了 Kerberos，并且希望授予用户使用 Firefox 访问 Web 界面的权限，则您必须配置 Firefox 浏览器。

Kerberos 身份验证可在 Windows 操作系统中与 Directories Management 配合使用。

前提条件

为每位用户配置 Firefox 浏览器或在配置 Kerberos 后向用户提供说明。

步骤

- 1 在 Firefox 浏览器的 URL 文本框中，输入 **about:config** 以访问高级设置。
- 2 单击 **我保证会小心**。
- 3 双击“首选项名称”列中的 **network.negotiate-auth.trusted-uris**。
- 4 在文本框中输入您的 Directories Management URL。
https://myconnectorhost.domain.com
- 5 单击**确定**。
- 6 双击“首选项名称”列中的 **network.negotiate-auth.delegation-uris**。
- 7 在文本框中输入您的 Directories Management URL。
https://myconnectorhost.domain.com/authenticate/
- 8 单击**确定**。

- 9 通过使用 Firefox 浏览器登录到登录 URL 以测试 Kerberos 功能。例如，<https://myconnectorhost.domain.com/authenticate/>。

如果 Kerberos 身份验证成功，测试 URL 将转到 Web 界面。

结果

Kerberos 协议可以确保 Firefox 浏览器实例与 Directories Management 之间的所有交互的安全性。现在，用户可以使用单点登录访问其“我的应用程序”门户。

配置 Chrome 浏览器以访问 Web 界面

如果您为自己的部署配置了 Kerberos，并且希望授予用户使用 Chrome 浏览器访问 Web 界面的权限，则您必须配置 Chrome 浏览器。

Kerberos 身份验证可在 Windows 操作系统中与 Directories Management 配合使用。

注 请不要在其他操作系统中执行这些与 Kerberos 相关的步骤。

前提条件

- 配置 Kerberos。
- 由于 Chrome 使用 Internet Explorer 配置启用 Kerberos 身份验证，因此您必须将 Internet Explorer 配置为允许 Chrome 使用 Internet Explorer 配置。有关如何针对 Kerberos 身份验证配置 Chrome 的信息，请参阅 Google 文档。

步骤

- 1 使用 Chrome 浏览器检测 Kerberos 的功能。
- 2 通过 <https://myconnectorhost.domain.com/authenticate/> 登录到 Directories Management。

如果 Kerberos 身份验证成功，测试 URL 将与 Web 界面进行连接。

结果

如果所有相关的 Kerberos 配置是正确的，则相关协议 (Kerberos) 可以保证该 Chrome 浏览器实例与 Directories Management 之间的所有交互的安全性。用户可以使用单点登录访问其“我的应用程序”门户。

升级用于身份目录管理的外部连接器

如果将外部连接器与 vRealize Automation 身份目录管理配置结合使用，您有时可能需要升级该连接器。

升级 vRealize Automation 部署的版本时，或者新的连接器内部版本提供所需的功能时，您可能需要升级外部连接器。

本文档仅适用于已部署其他独立外部连接器设备的用户。例如，在 vRealize Automation 中，外部连接器设备与智能卡身份验证结合使用。

默认情况下，连接器使用 VMware 网站执行升级过程，该过程需要连接器设备连接到 Internet。您还必须为连接器设备配置代理服务器设置（如果适用）。

如果连接器实例未连接到 Internet，则可以执行离线升级。要执行离线升级，您需要下载升级包并设置本地 Web 服务器以托管升级文件。

目标读者

此信息适用于要安装、升级和配置身份目录管理的任何人。此信息专为熟悉虚拟机技术且经验丰富的 Windows 或 Linux 系统管理员编写。

准备升级外部连接器

要准备升级连接器，您必须检查可用升级并为设备配置代理服务器设置（如果适用）。

■ 检查能否联机升级外部连接器

如果您的连接器设备连接到 Internet，则可以从设备中检查能否在线升级。

■ 配置外部连接器设备的代理服务器设置

连接器设备可通过 Internet 访问 VMware 更新服务器。如果您的网络配置使用 HTTP 代理提供 Internet 访问权限，则必须调整设备的代理设置。

检查能否联机升级外部连接器

如果您的连接器设备连接到 Internet，则可以从设备中检查能否在线升级。

步骤

1 以 root 用户身份登录连接器设备。

2 运行以下命令

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

3 运行以下命令以检查在线升级。

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

配置外部连接器设备的代理服务器设置

连接器设备可通过 Internet 访问 VMware 更新服务器。如果您的网络配置使用 HTTP 代理提供 Internet 访问权限，则必须调整设备的代理设置。

使代理仅处理 Internet 流量。为确保代理设置正确，请在域中将用于内部流量的参数设置为 no-proxy。

注 不支持要求进行身份验证的代理服务器。

前提条件

- 确认您拥有连接器设备的 root 密码。
- 确认您拥有代理服务器信息。

步骤

- 1 以 root 用户身份登录连接器设备。
- 2 在命令提示行中输入 YaST 以运行 YaST 实用程序。
- 3 在左侧窗格中选择**网络服务**，然后选择**代理**。
- 4 在 **HTTP 代理 URL** 和 **HTTPS 代理 URL** 字段中输入代理服务器 URL。
- 5 选择**完成**，退出 YaST 实用程序。
- 6 在连接器虚拟设备上重新启动 Tomcat 服务器以使用新的代理设置。

```
service horizon-workspace restart
```

结果

VMware 更新服务器现在即可供连接器设备使用。

在线升级外部连接器

如果有相应的连接，则可以在线升级身份目录管理外部连接器。

前提条件

- 确认连接器设备可以采用 HTTP 通过端口 80 解析和访问 vapp-updates.vmware.com。
- 确认存在连接器升级。运行相应的命令以检查升级。请参见“检查能否在线升级 Directories Management 连接器”。
- 确认设备的主 root 分区上至少有 2 GB 的磁盘空间。
- 确认连接器配置正确。
- 生成连接器设备的快照以对其进行备份。有关如何生成快照的信息，请参阅 vSphere 文档。
- 如果出站 HTTP 访问需要 HTTP 代理服务器，则配置连接器设备的代理服务器设置。请参见“配置 Directories Management 连接器设备的代理服务器设置”。

步骤

- 1 以 root 用户身份登录连接器设备。
- 2 运行以下命令

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

- 3 运行以下命令以确认存在在线升级。

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

- 4 运行以下命令以更新设备。

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

升级过程中产生的消息将保存在位于 `/opt/vmware/var/log/update.log` 的 `update.log` 文件中。

- 5 再次运行 `updatemgr.hzn check` 命令以确认不存在较新的更新。

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

- 6 检查升级后的设备版本。

```
vamicli version --appliance
```

将显示新版本。

- 7 重新启动连接器设备。

```
reboot
```

离线升级外部连接器

如果现有 vRealize Automation 身份目录管理连接器设备无法连接到 Internet 进行升级，您可以执行离线升级。您必须在本地 Web 服务器上设置升级存储库，并将连接器设备配置为使用本地 Web 服务器进行升级。

前提条件

- 确认存在连接器升级。可检查位于 my.vmware.com 的 My VMware 下载站点是否提供了升级。
- 确认设备的主 root 分区上至少有 2 GB 的磁盘空间。
- 确认连接器配置正确。
- 生成连接器设备的快照以对其进行备份。有关如何生成快照的信息，请参阅 vSphere 文档。
- 将连接器设备配置为使用本地 Web 服务器托管升级文件。请参见“准备本地 Web 服务器进行离线升级”。

步骤

1 准备本地 Web 服务器进行离线升级

在开始执行连接器离线升级之前，请准备本地 Web 服务器，方法是为连接器设备创建包含子目录的目录结构。

2 配置连接器并执行离线升级

将连接器设备配置为指向本地 Web 服务器以执行离线升级。然后，升级设备。

准备本地 Web 服务器进行离线升级

在开始执行连接器离线升级之前，请准备本地 Web 服务器，方法是为连接器设备创建包含子目录的目录结构。

前提条件

- 从“我的 VMware”中下载 `identity-manager-connector-versionNumber-buildNumber-updaterepo.zip` 文件。转到 my.vmware.com，导航到“VMware Identity Manager 下载”页面，然后下载 **VMware Identity Manager Connector 离线升级包** 下面列出的文件。
- 如果使用 IIS Web 服务器，请配置该 Web 服务器以允许在文件名中使用特殊字符。您可以在 **请求筛选** 部分中选择 **允许双重转义** 选项以配置该设置。

步骤

- 1 在 Web 服务器上的 `http://YourWebServer/VM/` 下创建一个目录，并将下载的 zip 文件复制到该目录中。
- 2 确认您的 Web 服务器包含 `.sig (text/plain)` 和 `.sha256 (text/plain)` 的 mime 类型。
如果没有这些 mime 类型，您的 Web 服务器便无法检查更新。
- 3 解压缩文件。
提取的 ZIP 文件内容由 `http://YourWebServer/VM/` 提供服务。
提取的文件内容包含以下子目录：`/manifest` 和 `/package-pool`。
- 4 运行以下 `updatelocal.hzn` 命令以检查该 URL 的更新内容是否有效。

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

配置连接器并执行离线升级

将连接器设备配置为指向本地 Web 服务器以执行离线升级。然后，升级设备。

前提条件

准备本地 Web 服务器进行离线升级。

步骤

- 1 以 root 用户身份登录连接器设备。
- 2 运行以下命令以配置使用本地 Web 服务器的升级存储库。

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

注 要撤消配置并还原执行在线升级的功能，可运行以下命令。

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

3 执行升级。

- a 运行以下命令

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

- b 运行以下命令以检查可用升级的版本。

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

- c 运行以下命令以更新连接器。

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

升级过程中产生的消息将保存在位于 `/opt/vmware/var/log/update.log` 的 `update.log` 文件中。

- d 再次运行 `updatemgr.hzn check` 命令。

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

- e 检查升级后的设备版本。

```
vamicli version --appliance
```

该命令应显示新版本。

- f 重新启动连接器设备。

例如，从命令行中运行以下命令。

```
reboot
```

结果

连接器升级完成。

升级外部连接器后配置设置

升级到连接器 2016.3.1.0 或更高版本后，您可能需要配置某些设置。

使用 Kerberos 身份验证重新加入域

如果使用 Kerberos 身份验证或 Active Directory（集成 Windows 身份验证）目录，您必须退出该域，然后重新加入它。必须对部署中的所有连接器虚拟设备执行该操作。

- 1 选择**管理 > 身份目录管理 > 连接器**
- 2 在“连接器”页面中，对于正用于 Kerberos 身份验证或 Active Directory（集成的 Windows 身份验证）目录的每个连接器，单击**退出域**。

- 3 要加入域，您需要具有加入域的权限的 Active Directory 凭据。有关详细信息，请参见[将连接器计算机加入域](#)。
- 4 如果使用的是 Kerberos 身份验证，请再次启用 Kerberos 身份验证适配器。要访问“身份验证适配器”页面，请在“连接器”页面的[工作线程](#)列中单击相应链接，然后选择[身份验证适配器](#)选项卡。
- 5 请确认您所使用的其他身份验证适配器均已启用。

更新域页面

如果在此目录支持 **DNS 服务位置** 选项启用时使用 Active Directory（集成 Windows 身份验证）或通过 LDAP 访问的 Active Directory，请保存目录的域页面。

- 1 选择**管理 > 身份目录管理 > 目录**。
- 2 选择适用的目录进行编辑。
- 3 提供绑定 DN 用户的密码，然后单击**保存**。
- 4 单击页面左侧的**同步设置**，然后选择**域**选项卡。
- 5 单击**保存**。

DNS 服务位置和域控制器

注 在 Connector 2016.3.1.0 及更高版本中，当创建启用 DNS 服务位置的目录时，会自动创建 `domain_krb.properties` 文件，并使用域控制器进行自动填充。当您在升级后保存域页面时，如果原始部署中包含 `domain_krb.properties` 文件，该文件将使用您随后添加但不在该文件中的域进行更新。如果原始部署中没有 `domain_krb.properties` 文件，将创建该文件，并使用域控制器进行自动填充。有关 `domain_krb.properties` 文件的详细信息，请参见[关于域控制器选择](#)。

外部连接器升级错误故障排除

可以通过查看错误日志来对 vRA 身份目录管理外部连接器升级问题进行故障排除。如果连接器未启动，可以通过回滚到快照来还原到先前的实例。

■ [检查升级错误日志](#)

通过查看错误日志，解决在升级期间出现的错误。升级日志文件位于 `/opt/vmware/var/log` 目录中。

■ [回滚到连接器快照](#)

如果连接器在升级之后无法正常启动，并且您无法通过查看升级错误日志并再次运行升级命令来解决该问题，您可以回滚到先前的连接器实例。

■ [收集日志文件包](#)

您可以收集日志文件包，以便将其发送给 VMware 支持部门。可以从连接器配置页面获取该包。

检查升级错误日志

通过查看错误日志，解决在升级期间出现的错误。升级日志文件位于 `/opt/vmware/var/log` 目录中。

如果发生任何错误，连接器在升级之后可能无法启动。

步骤

- 1 登录连接器设备。
- 2 转到 `/opt/vmware/var/log` 目录。
- 3 打开 `update.log` 文件并查看错误消息。
- 4 解决错误并重新运行升级命令。升级命令会从其停止的位置继续运行。

注 还可以还原到快照并重新运行更新。

回滚到连接器快照

如果连接器在升级之后无法正常启动，并且您无法通过查看升级错误日志并再次运行升级命令来解决该问题，您可以回滚到先前的连接器实例。

步骤

- ◆ 还原到作为对原始连接器实例的备份而生成的某个快照。有关信息，请参阅 vSphere 文档。

收集日志文件包

您可以收集日志文件包，以便将其发送给 VMware 支持部门。可以从连接器配置页面获取该包。

该包中收集了以下日志文件。

表 2-9. 日志文件

组件	日志文件位置	描述
Apache Tomcat 日志 (catalina.log)	<code>/opt/vmware/horizon/workspace/logs/catalina.log</code>	Apache Tomcat 会记录其他日志文件未记录的消息。
Configurator 日志 (configurator.log)	<code>/opt/vmware/horizon/workspace/logs/configurator.log</code>	Configurator 从 REST 客户端和 Web 界面所接收的请求。
连接器日志 (connector.log)	<code>/opt/vmware/horizon/workspace/logs/configurator.log</code>	从 Web 界面收到的每个请求的记录。每个日志条目中还包含请求 URL、时间戳和异常情况。不记录同步操作。

步骤

- 1 登录位于 `https://connectorURL:8443/cfg/logs` 的连接器配置页面。
- 2 单击**准备日志包**。
- 3 下载该包并将其发送给 VMware 支持部门。

场景：为高度可用的 vRealize Automation 配置 Active Directory 链接

作为租户管理员，您希望配置通过 LDAP 访问的 Active Directory 目录连接，以便支持对高度可用的 vRealize Automation 部署进行用户身份验证。

每个 vRealize Automation 设备均包含一个支持用户身份验证的连接器，但通常只会配置一个连接器来执行目录同步。选择哪个连接器作为同步连接器并不重要。要支持身份目录管理高可用性，必须配置与第二个 vRealize Automation 设备对应的另一个连接器，该连接器会连接到身份提供程序并指向同一个 Active Directory。在此配置中，如果一个设备出现故障，则另一个设备将接管用户身份验证。

在高可用性环境中，所有节点均必须提供一组相同的 Active Directory、用户、身份验证方法等。要实现这一点，最直接的方法是通过将负载平衡器主机设置为身份提供程序主机，将身份提供程序升级到群集。在此配置中，所有身份验证请求均会指向负载平衡器，稍后负载平衡器将根据需要将请求转发给任一连接器。

前提条件

- 使用适当的负载平衡器安装分布式 vRealize Automation 部署。请参见安装 vRealize Automation。
- 以租户管理员身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 目录**。
- 2 单击**添加目录**。
- 3 输入您的特定 Active Directory 帐户设置并接受默认选项。

选项	输入示例
目录名称	添加 Active Directory 域名的 IP 地址。
同步连接器	所有 vRealize Automation 设备均包含一个连接器。使用任一可用的连接器。
基本 DN	输入目录服务器搜索起点的标识名 (Distinguished Name, DN)。例如， cn=users,dc=corp,dc=local 。
绑定 DN	输入有权搜索用户的 Active Directory 用户帐户的完整专有名称 (DN)，包括公用名称 (CN)。例如， cn=config_admin infra,cn=users,dc=corp,dc=local 。
绑定 DN 密码	为可以搜索用户的帐户输入 Active Directory 密码。

- 4 单击**测试连接**以测试与已配置目录的连接。
如果连接失败，请检查所有字段中的条目。如果需要，请咨询系统管理员。
- 5 单击**保存并执行下一步**。
此时将显示“选择域”页面，其中包含域的列表。
- 6 保持选中默认域，然后单击**下一步**。
- 7 确认属性名称已映射到正确的 Active Directory 属性。否则，请从下拉菜单中选择正确的 Active Directory 属性。单击**下一步**。

8 选择要同步的组和用户。

- a 单击**添加图标** (+)。
- b 输入用户域，然后单击**查找组**。
例如，**cn=users,dc=corp,dc=local**。
- c 选中**全选**复选框。
- d 单击**选择**。
- e 单击**下一步**。

- f 单击 + 以添加其他用户。例如，输入
CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com。

要排除用户，请单击 “+” 创建一个筛选器以排除某些类型的用户。您可以选择要作为筛选条件的用户属性、查询规则 and 值。

- g 单击**下一步**。

9 查看页面以了解同步到该目录的用户和组的数量，然后单击**同步目录**。

目录同步过程需要一些时间，但在后台执行，因此您可以继续工作。

10 配置第二个连接器以支持高可用性。

- a 以租户管理员身份登录到 vRealize Automation 部署的负载均衡器。
负载均衡器 URL 为 *负载均衡器地址/vcac/org/tenant_name*。
- b 选择**管理 > 身份目录管理 > 身份提供程序**。
- c 单击系统目前正在使用的身份提供程序。
将显示为系统提供基本身份管理的现有身份目录和连接器。
- d 单击**添加连接器**下拉列表，然后选择与辅助 vRealize Automation 设备对应的连接器。
- e 在选择该连接器时显示的**绑定 DN 密码**文本框中，输入相应的密码。
- f 单击**添加连接器**。
- g 将主机名编辑为指向负载均衡器。

结果

您已将企业 Active Directory 连接到 vRealize Automation 并已配置可实现高可用性的身份目录管理。

后续步骤

为了增强安全性，您可以在身份提供程序与 Active Directory 之间配置双向信任。请参见在 [vRealize Automation 与 Active Directory 之间配置双向信任关系](#)。

在 vRealize Automation 中为智能卡和第三方身份提供程序的身份验证配置外部连接器

如果您使用具有证书身份验证或智能卡身份验证的第三方身份提供程序，系统管理员必须使用身份目录管理为您的 vRealize Automation 部署配置外部连接器。此外，本文所述的过程广泛适用于所有类型的证书身份验证。

身份目录管理针对配置的每个 Active Directory 支持多个身份提供程序和连接器集群。要使用第三方身份提供程序或智能卡身份验证，您可以在负载均衡器后面设置单个外部连接器或连接器集群来连接合适的身份提供程序，以便允许 SSL 直通。有关详细信息，请参见[管理连接器和连接器集群](#)。

有关更新外部连接器的信息，请参见[升级用于身份目录管理的外部连接器](#)。

多个证书配置选项可与智能卡身份验证配合使用。请参见[配置用于身份目录管理的证书或智能卡适配器](#)。

前提条件

- 配置正确的 Active Directory 连接器以便与 vRealize Automation 部署配合使用。
- 从 [VMware vRealize Automation 工具和 SDK](#) 下载配置连接器所需的 OVA 文件。
- 以[租户管理员](#)身份登录到 vRealize Automation。

步骤

1 生成连接器激活令牌

在部署连接器虚拟设备以用于智能卡身份验证之前，先从 vRealize Automation 控制台为新的连接器生成激活码。激活码用于在身份目录管理和连接器之前建立通信。

2 部署连接器 OVA 文件

下载连接器 OVA 文件之后，您可以使用 VMware vSphere Client 或 vSphere Web Client 对其进行部署。

3 配置连接器设置

部署连接器 OVA 之后，必须运行设置向导以激活设备并配置管理员密码。

4 应用公共证书颁发机构

安装身份目录管理后，将生成一个默认的 SSL 证书。您可以使用默认证书进行测试，但是必须为生产环境生成并安装商业 SSL 证书。

5 创建 Workspace 身份提供程序

必须创建一个 Workspace 身份提供程序以与外部连接器配合使用。

6 配置证书身份验证并配置默认访问策略规则

必须配置外部连接器以便与 vRealize Automation Active Directory 和域配合使用。

生成连接器激活令牌

在部署连接器虚拟设备以用于智能卡身份验证之前，先从 vRealize Automation 控制台为新的连接器生成激活码。激活码用于在身份目录管理和连接器之前建立通信。

可以配置一个连接器或连接器群集。如果要使用连接器群集，请为所需的每个连接器重复此过程。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 连接器**
- 2 单击**添加连接器**。
- 3 在**连接器 ID 名称**文本框内输入新连接器的名称。
- 4 单击**生成激活码**。
连接器的激活码显示在**连接器激活码**框中。
- 5 复制激活码，以便使用 OVA 文件配置连接器时使用。
- 6 单击**确定**。

部署连接器 OVA 文件

下载连接器 OVA 文件之后，您可以使用 VMware vSphere Client 或 vSphere Web Client 对其进行部署。

您可以使用 vSphere Client 或 vSphere Web Client 部署 OVA 文件。

前提条件

- 标识用于 连接器 OVA 部署的 DNS 记录和主机名。
- 如果使用的是 vSphere Web Client，请使用 Firefox 或 Chrome 浏览器。不要使用 Internet Explorer 部署 OVA 文件。
- 从 [VMware vRealize Automation 工具和 SDK](#) 下载配置连接器所需的 OVA 文件。

步骤

- 1 在 vSphere Client 或 vSphere Web Client 中，选择**文件 > 部署 OVF 模板**。
- 2 在“部署 OVF 模板”页面中，输入特定于您的 连接器 部署的信息。

页面	描述
源	浏览至 OVA 软件包位置，或输入特定的 URL。
OVA 模板详细信息	确认您所选的是正确的版本。
许可证	阅读最终用户许可协议，并单击 接受 。
名称和位置	为虚拟设备输入一个名称。该名称必须在清单文件夹中是唯一的，最多可以包含 80 个字符。名称区分大小写。 为虚拟设备选择一个位置。
主机/群集	选择要运行部署的模板的主机或群集。
资源池	选择资源池。
存储	选择虚拟机文件的存储位置。

页面	描述
磁盘格式	选择文件的磁盘格式。对于生产环境，请选择 厚置备 格式。对于评估和测试，请使用 精简置备 格式。
网络映射	将您所在环境中的网络映射到 OVF 模板中的网络。
属性	<p>a 在时区设置字段中，选择正确的时区。</p> <p>b 默认情况下，将选中“客户体验改进计划”复选框。VMware 将收集有关部署的匿名数据，以改进 VMware 对用户要求的响应。如果不希望收集该数据，请取消选中该复选框。</p> <p>c 在“主机名”文本框中，输入要使用的主机名。如果该文本框为空，则使用反向 DNS 查询主机名。</p> <p>d 要为连接器配置静态 IP 地址，请输入以下各个字段的地址：“默认网关”、“DNS”、“IP 地址”和“网络掩码”。</p> <p>重要事项 如果这四个地址字段中的任何字段（包括主机名）保留空白，则使用 DHCP。</p> <p>要配置 DHCP，请将地址字段留空。</p>
即将完成	检查选择内容，然后单击 完成 。

根据网络速度，部署过程可能需要几分钟的时间。您可以在进度对话框中查看进度。

3 在部署完成后，选择 设备，右键单击，然后选择**电源 > 打开电源**。

将初始化 设备。您可以转到**控制台**选项卡以查看详细信息。在虚拟设备初始化完成后，控制台屏幕将显示 版本以及用于登录 设置向导以完成设置的 URL。

后续步骤

使用设置向导添加激活码和管理密码。

配置连接器设置

部署连接器 OVA 之后，必须运行设置向导以激活设备并配置管理员密码。

前提条件

- 已为连接器生成激活码。
- 确保已打开连接器设备的电源，并且您知道连接器 URL。
- 收集要用于连接器管理员、root 帐户和 sshuser 帐户的密码列表。

步骤

- 1 要运行设置向导，请输入部署 OVA 后在“控制台”选项卡中显示的连接器 URL。
- 2 在“欢迎”页面上，单击**继续**。

3 为以下 连接器 虚拟设备管理员帐户创建强密码。

强密码应该至少为八个字符，同时包含大写和小写字母，并且至少包含一个数字或特殊字符。

选项	描述
设备管理员	创建设备管理员密码。用户名为 admin ，并且不能更改。您可以使用此帐户和密码登录连接器服务来管理证书、设备密码和 syslog 配置。 重要事项 管理员用户密码长度必须至少为 6 个字符。
Root 帐户	安装 连接器 设备时使用的是默认的 VMware root 密码。创建新的 root 密码。
sshuser 帐户	创建用于远程访问连接器设备的密码。

4 单击**继续**。

5 在“激活连接器”页中，粘贴激活码，然后单击**继续**。

6 如果要在 vRealize Automation 内部连接器上使用自签名证书，可以通过在 vRealize Automation 设备上运行以下命令获取相应的证书：`cat /etc/apache2/server-cert.pem`

选择**终止负载平衡器**上的 **SSL** 选项卡，然后单击链接 `/horizon_workspace_rootca.pem`。

激活码已验证，并且已在服务与连接器实例之间建立通信，以完成连接器配置。

后续步骤

在该服务中，根据您的需求设置环境。例如，如果由于您希望同步两个 Integrated Windows Authentication 目录而另外添加了一个连接器，请创建该目录并将它与新的连接器关联。

应用公共证书颁发机构

安装身份目录管理后，将生成一个默认的 SSL 证书。您可以使用默认证书进行测试，但是必须为生产环境生成并安装商业 SSL 证书。

如果身份目录管理指向一个负载平衡器，SSL 证书将应用于该负载平衡器。

导入证书时，必须选中**将此密钥标记为可导出**。

如果要生成自定义证书的 CSR，您只需指定 CN 或证书颁发机构的站点域名。

前提条件

生成证书签名请求 (CSR) 并从 CA 获取有效的已签名证书。如果您所在的组织提供了由 CA 签名的 SSL 证书，则您可以使用这些证书。证书必须采用 PEM 格式。

步骤

1 以管理员用户身份登录到以下位置的连接器设备管理页面：

`https://myconnector.mycompany:8443/cfg`

2 在管理控制台中，单击**设备设置**。

默认情况下，将选择 VA 配置。

3 单击**管理配置**。

4 输入 VMware Identity Manager 服务器管理员用户密码。

5 选择**安装证书**。

6 在**终止 Identity Manager 设备上的 SSL** 选项卡中，选择**自定义证书**。

7 在 **SSL 证书链** 文本框中，依次粘贴主机证书、中间证书和根证书。

仅当您按照正确的顺序包含整个证书链时，SSL 证书才可用。对于每个证书，请复制 “-----证书开始-----” 和 “-----证书结束-----” 之间的所有内容（包括这两行）。

确保证书包含 FQDN 主机名。

8 在 “私钥” 文本框中粘贴私钥。复制 “----BEGIN RSA PRIVATE KEY” 与 “---END RSA PRIVATE KEY” 之间的所有内容。

9 单击**保存**。

示例：证书示例

证书链示例

-----BEGIN CERTIFICATE-----

jlQvt9WdR9Vpg3WQT5+C3HU17bUOwvhp/r0+

...

...

...

W53+O05j5xsxzDJfWr1lqBiff/OkiYCPcyK1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+

...

...

...

O05j5xsxzDJfWr1lqBiff/OkiYCPW53+cyK1

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

dR9Vpg3WQTjlQvt9W5+C3HU17bUOwvhp/r0+

...

...

...

5j5xsxzDJfWr1lqW53+O0Biff/OkiYCPcyK1

-----END CERTIFICATE-----

私钥示例

```
-----BEGIN RSA PRIVATE KEY-----
jIQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+
...
...
1lqBIFFW53+O05j5xsxzDJfWr/OklYCPcyK1
-----END RSA PRIVATE KEY-----
```

创建 Workspace 身份提供程序

必须创建一个 Workspace 身份提供程序以与外部连接器配合使用。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 身份提供程序**。
- 2 选择**添加身份提供程序**。
- 3 选择**创建 Workspace IDP**。
- 4 在**身份提供程序名称**字段中输入身份提供程序的名称。
- 5 选择与将使用此身份提供程序的用户相对应的目录。
您选择的目录确定可为此身份提供程序使用哪些连接器。
- 6 选择您为智能卡身份验证配置的一个或多个外部连接器。

注 如果部署位于负载均衡器后面，则输入负载均衡器 URL。

- 7 选择有权访问此身份提供程序的**网络**。
- 8 单击**添加**。

配置证书身份验证并配置默认访问策略规则

必须配置外部连接器以便与 vRealize Automation Active Directory 和域配合使用。

前提条件

以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 身份目录管理 > 连接器**。
- 2 在**工作线程**列中选择所需连接器。

所选工作线程显示在连接器**详细信息**选项卡的**工作线程名称**文本框中，连接器类型信息显示在**连接器类型**文本框中。

- 3 确保通过在**关联的目录**文本框中指定目录，将连接器链接到所需的 Active Directory。
- 4 在**关联的域**文本框中输入正确的域名。
- 5 选择 **AuthAdapters** 选项卡并启用 CertificateAuthAdapter。
- 6 根据部署需要配置证书身份验证。
请参见[为身份目录管理配置证书身份验证](#)。
- 7 选择**管理 > 身份目录管理 > 策略**。
- 8 单击**编辑默认策略**。
- 9 将证书添加到策略规则并使其成为第一个身份验证方法。

证书必须是策略规则中列出的第一个身份验证方法，否则，证书身份验证将失败。

创建多域或多林 Active Directory 链接

系统管理员需要配置多域或多林 Active Directory 链接。

配置多域 Active Directory 链接与配置多林 Active Directory 链接的过程基本相同。对于多林链接，必须在所有适用域之间建立双向信任。

前提条件

- 使用适当的负载平衡器安装分布式 vRealize Automation 部署。请参见[安装 vRealize Automation](#)。
- 以**租户管理员**身份登录到 vRealize Automation。
- 为您的部署配置合适的域和 Active Directory 林。

步骤

- 1 选择**管理 > 身份目录管理 > 目录**。
- 2 单击**添加目录**。
- 3 在“添加目录”页面上的**目录名称**文本框中，指定 Active Directory 服务器的名称。
- 4 在**目录名称**标题下方，选择 **Active Directory (集成 Windows 身份验证)**。
- 5 在“目录同步和身份验证”部分配置用于将用户从 Active Directory 同步到 VMware Directories Management 目录的连接器。

选项	描述
同步连接器	选择适合用于系统的连接器。每个 vRealize Automation 设备 均包含一个默认连接器。如需有关选择适当连接器的帮助，请咨询系统管理员。
身份验证	单击相应单选按钮，指示所选连接器是否也执行身份验证。
目录搜索属性	选择包含用户名的合适帐户属性。

根据您的部署配置，将有一个或多个连接器可供使用。

- 6 在**域名**、**域管理员用户名**和**域管理员密码**文本框中，输入相应的加入域凭据。

例如，您可能会遇到类似如下所示的内容：**域名**：hs.trcint.com、**域管理员用户名**：devadmin、**域管理员密码**： xxxx。

- 7 在**绑定用户详细信息**部分中，输入相应的 Active Directory（集成 Windows 身份验证）凭据，以便执行目录同步。

选项	描述
绑定用户 UPN	输入可对域进行身份验证的用户的“用户主体名称”。例如，UserName@example.com。
绑定 DN 密码	输入绑定用户密码。

- 8 单击**保存并执行下一步**。

此时将显示“选择域”页面，其中包含域的列表。

- 9 单击相应的复选框，选择您的系统部署所需的域。

- 10 单击**下一步**。

- 11 确认 Directories Management 目录属性名称已映射到正确的 Active Directory 属性。

如果目录属性名称未正确映射，请从下拉菜单中选择正确的 Active Directory 属性。

- 12 单击**下一步**。


- 13 单击  以选择您要从 Active Directory 同步到目录的组。

添加 Active Directory 组时，如果该组中的成员不在“用户”列表中，则表明已添加这些成员。

注 Directories Management 用户身份验证系统在添加组和用户时从 Active Directory 导入数据，系统的速度受 Active Directory 功能限制。因此，导入操作可能需要很长时间，具体取决于要添加的组和用户数量。为了最大程度地减少潜在的延迟或问题，请将组和用户数量限制为 vRealize Automation 操作所需的数量。如果系统性能降低或者如果出现错误，请关闭所有不需要的应用程序并确保系统已为 Active Directory 分配相应的内存。如果问题仍然存在，请根据需要增加 Active Directory 内存分配。对于拥有大量用户和组的系统，您可能需要将 Active Directory 内存分配增加至多达 24 GB。

- 14 单击**下一步**。

- 15 单击  以添加其他用户。例如，输入 CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com。

要排除用户，请单击  创建一个筛选器以排除某些类型的用户。您可以选择要作为筛选条件的用户属性、查询规则 and 值。

- 16 单击**下一步**。

- 17 查看该页面以了解将要同步到目录的用户和组数量。

如果您要对用户和组进行更改，请单击“编辑”链接。

- 18 单击**推送到 Workspace** 以开始与目录同步。

后续步骤

配置组 and 用户角色

租户管理员可以创建业务组和自定义组，并授予用户对 vRealize Automation 控制台的访问权限。

为目录用户或组分配角色

租户管理员通过为用户或组分配角色来授予用户访问权限。

要允许用户或组修改和触发管道，必须向这些用户和组分配权限。如果为用户和组分配发行经理的角色，他们则可以修改和触发管道。如果为用户和组分配发行工程师的角色，他们则可以触发管道。有关详细信息，请参见《vRealize Code Stream 使用指南》。

前提条件

以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 用户和组 > 目录用户和组**。
- 2 在**搜索**框中输入用户名或组名称，然后按 Enter。
请勿在名称中使用 @ 符号、反斜杠 (\) 或斜杠 (/)。通过以 user@domain 形式键入用户或组的全名，您可以优化搜索。
- 3 单击要分配角色的用户或组的名称。
- 4 从“向此用户添加角色”列表选择一个或多个角色。
“选定角色授予的权限”列表指示您所授予的特定权限。
- 5 （可选）单击**下一步**查看用户或组的详细信息。
- 6 在**用户详细信息**页面的**常规**选项卡，滚动角色列表以添加用户。
 - a 要向用户授予修改和触发管道的权限，请选中**发行经理**复选框。
 - b 要向用户授予触发管道的权限，请选中**发行工程师**复选框。
- 7 单击**更新**。

结果

当前登录到 vRealize Automation 的用户必须先从 vRealize Automation 注销后再重新登录，然后才能导航至有权访问的页面。

后续步骤

或者，您也可以从 Active Directory 连接中的用户和组中创建自己的自定义组。请参见[创建自定义组](#)。

创建自定义组

租户管理员可以创建自定义组，以便组合其他自定义组、身份存储组以及各个身份存储用户。与对应于业务范围、部门或其他组织单位的业务组相比，自定义组可以在 vRealize Automation 内提供更精细地访问控制。

使用自定义组，可以为任务授予比标准 vRealize Automation 组分配更精细的访问权限。例如，您可能想创建一个自定义组，以允许租户管理员控制租户内的哪些成员具有特定权限。

您可以为自定义组分配角色，但不是所有情况下都需要这么做。例如，您可以创建一个名为“计算机规范审批者”的自定义组，以供所有计算机预批准使用。此外，您还可以创建要映射到业务组的自定义组，以便能够集中管理所有组。在这些情况下，您无需分配角色。

前提条件

以**租户管理员**身份登录到 vRealize Automation。

步骤

1 选择**管理 > 用户和组 > 自定义组**。

2 单击**新建**。

3 在**名称**文本框中输入组名称。

自定义组名称不能包含分号 (;) 后跟等号 (=) 的组合。

4 （可选）在**描述**文本框中输入描述。

5 从“将角色添加到该组”列表选择一个或多个角色。

“选定角色授予的权限”列表指示您所授予的特定权限。

6 单击**下一步**。

7 添加用户和组以创建自定义组。

a 在**搜索**框中输入用户名或组名称，然后按 Enter。

请勿在名称中使用 @ 符号、反斜线 (\) 或斜线 (/)。通过以 user@domain 形式键入用户或组的全名，您可以优化搜索。

b 选择要添加到自定义组的用户或组。

8 单击**完成**。

结果

当前登录到 vRealize Automation 的用户必须先从 vRealize Automation 注销后再重新登录，然后才能导航至有权访问的页面。

添加具有自定义组和规则的即时用户

您可以使用即时用户配置将 vRealize Automation 用户添加到无法访问 Active Directory 的部署中。要为初次使用的用户调用即时置备，您必须创建规则以填充适用的自定义组。

首次登录时，将根据您在“高级组成员资格”向导页面上创建的规则为即时用户动态分配组成员资格。首次登录后，您可以按常规方式分配组成员资格。该向导的第二页包含四个选择框，用于根据定义即时用户的各种条件创建规则。

例如，在第一个规则选择框中，您可以选择“域”作为一个条件，然后在第二个框中选择“匹配”。然后，在第三个规则框中，您可以输入一个域。这些选项创建了一个规则，用于建立与指定域相关联的基于即时成员资格的用户。第三个选择框是自由格式的输入框，您可以输入与前两个选择框中的选项逻辑相关的任何信息。

注 当配置即时用户时，NameId 格式映射指定用于唯一标识用户的属性。用作 NameId 的此属性对于用户应唯一，并且属性本身应作为 SAML 声明的一部分提供。更改 NameId 属性或 NameId 的值会导致在尝试登录期间出错。例如，如果使用 urn:oasis:names:tc:SAML:2.0:nameid-format:transient NameId 格式将 NameId 映射到用户的 SAMAccountName，则还应单独提供 SAMAccountName.userName 和 SAMAccountName 值绝不应更改。

vRealize Automation 支持使用通配符匹配来配置即时用户。有关启用和使用通配符匹配的详细信息，请参见[对即时用户使用基于通配符的匹配](#)。

注 您可以创建多个规则，以根据各种条件填充即时用户。如果要创建多个规则，您可以使用主规则框上方的[匹配](#)规则选择框，以指示在填充即时用户时 vRealize Automation 是否应匹配任意或所有规则。

步骤

- 1 选择**管理 > 用户和组 > 自定义组**，然后查找现有组，例如适用于即时用户的组。

有关详细信息，请参见[创建自定义组](#)。

在组行中单击，但不要单击组名称。

- 2 单击**高级成员资格**。

如果需要，可以在“将用户添加到组”页面中添加各个用户。

- 3 单击**下一步**查看“组规则”页面。

- 4 使用匹配和规则选择框创建一个或多个适用于您的用户配置的规则。

在[匹配](#)规则选择框下方的三个主要规则选择框中，单击向下箭头并输入信息以激活下拉菜单以便创建所需规则。请注意，您可以使用上述 * 和 \ 字符。

- 5 单击**下一步**。

- 6 如果要从组中排除用户，请在“从组中排除用户”页面上搜索并添加这些用户。

- 7 单击**下一步**。

- 8 在“检查”页面上查看组配置，然后单击**保存**以保存并实施您的规则和配置。

结果

根据您创建的规则添加即时用户。

对即时用户使用基于通配符的匹配

vRealize Automation 支持使用基于通配符的匹配规则来配置即时用户。

启用基于通配符的匹配

默认情况下，不会启用基于通配符的匹配。要启用基于通配符的匹配，必须运行相应的 REST API 命令，如下所示。

```
PUT:- https://{VRA_HOSTNAME}/SAAS/t/VSPHERE.LOCAL/jersey/manager/api/system/config/
isDynamicGroupWildcardEnabled
Content-Type: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Accept: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Authorization: HZN <token> (edited)
{
  "name": "isDynamicGroupWildcardEnabled",
  "values": {
    "values": [
      "true"
    ]
  }
}
```

要为启用通配符配置的 API 提供的 HZN 令牌必须适用于 vsphere.local 租户中的管理员用户。

将 SAML 断言中的属性映射到 vRealize Automation 用户属性

SAML 断言中的属性名称必须完全匹配在 vRealize Automation 的“用户属性”页面上定义的属性名称。包含用户名字的 SAML 属性应命名为“firstName”，姓氏应命名为“lastName”，依此类推。如果身份提供程序发送未在“用户属性”页面上定义的其他用户属性，则管理员必须将这些属性添加到该页面中。例如，如果身份提供程序发送名为“groups”或“memberof”的 SAML 属性中的用户组成员资格信息，则必须添加 vRealize Automation 用户属性“groups”或“memberof”。请确保对属性名称使用精确的大小写。

注 要在定义用户组成员资格的多值属性中积极识别 Group_Name 等字符串，请将通配符构建为 *Group_Name*。

对于“匹配”和“不匹配”条件，您可以使用 * 作为通配符在规则中包含字符模式匹配。例如，输入 <userinput>*Smi*</userinput> 会选择 Smith、Smiley、Smirnoff 和其他类似变体，包括名称中间带有 smi 的变体。如果要查找某个模式的所有完全匹配项，请在输入该模式时在 * 之前添加一个反斜杠 (\)。例如，<userinput>*Adam* </userinput> 会查找与模式 Adam* 完全匹配的所有名字。您可以在短语中的任意位置使用 *，后面和前面跟着任何字符，包括 * & amp; *。

创建业务组

业务组可用于将一组服务和资源关联到一组用户。这些组通常对应于业务范围、部门或其他组织单位。您可以创建业务组，以便能够配置预留并授权用户为业务组成员置备服务目录项。

要将多个用户添加到业务组角色，您可以添加多个单独的用户，或者通过向角色添加身份存储组或自定义组来同时添加多个用户。例如，您可以创建自定义组“销售支持团队”并将该组添加到支持角色。此外，您还可以使用现有身份存储用户组。所选的用户和组必须在身份存储中有效。

要支持 vCloud Director 集成，vRealize Automation 业务组中的同一业务组成员还必须是 vCloud Director 组织的成员。

租户管理员创建业务组之后，业务组主管有权修改主管的电子邮件地址和成员。租户管理员可以修改所有选项。

此过程假定已安装和配置 IaaS。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation。
- 如果要将业务组成员创建的计算机添加到特定的 Active Directory 组织单位，请配置 Active Directory 策略。请参见[创建 Active Directory 策略](#)。您既可以在创建业务组时应用该策略，也可以稍后添加该策略。
- 如果要为组提供一个默认计算机前缀，以便添加到置备的计算机名称之前，需请求架构管理员提供前缀。请参见[配置计算机前缀](#)。计算机前缀不适用于 XaaS 请求。

步骤

- 1 选择**管理 > 用户和组 > 业务组**。
- 2 单击**新建**图标 (+)。
- 3 配置业务组详细信息。

选项	说明
名称	输入业务组的名称。
说明	输入描述。
将容量警示电子邮件发送至	输入必须接收容量警示通知的用户的一个或多个电子邮件地址。不支持电子邮件别名地址，每个电子邮件地址必须针对某个特定用户。 用逗号分隔多个条目。例如， JoeAdmin@mycompany.com,WeiMgr@mycompany.com 。
Active Directory 策略	选择业务组的默认 Active Directory 策略。

- 4 添加自定义属性。
- 5 单击**下一步**移至“成员”页面。
- 6 输入用户名或自定义用户组名称，然后按 Enter。

您可以将一个或多个人员或自定义用户组添加到业务组。您可以现在指定用户，也可以先创建一个空业务组，稍后再填充用户。

选项	描述
组主管角色	可以为组创建授权并分配批准策略。
支持角色	可以代表其他业务组成员请求并管理服务目录项。

选项	描述
共享访问角色	可以对其他业务组成员部署的资源使用和运行操作。
用户角色	可以请求自己获得授权的服务目录项。

7 单击**下一步**移至“基础架构”页面。

8 配置默认基础架构选项。

选项	描述
默认计算机前缀	<p>为业务组选择预配置的计算机前缀。</p> <p>此前缀由计算机蓝图使用。如果蓝图使用默认前缀且您在此处未提供，则将根据业务组名称创建计算机前缀。最佳做法是提供默认前缀。您仍可使用特定的前缀配置蓝图，或者允许服务目录用户在请求蓝图时替代默认前缀。</p> <p>XaaS 蓝图不使用默认计算机前缀。如果您在此处配置前缀并将 XaaS 蓝图授权给该业务组，则不会影响 XaaS 计算机的置备。</p>
Active Directory 容器	<p>输入 Active Directory 容器。此选项仅适用于 WIM 置备。</p> <p>其他置备方法需要另行配置才能将已置备的计算机加入 AD 容器。</p>

9 单击**完成**。

结果

租户管理员可以通过创建预留将资源分配给业务组。业务组主管可以为业务组成员创建授权。

后续步骤

- 根据业务组在何处置备计算机，为业务组创建预留。请参见[选择预留场景](#)。
- 如果目录项已发布且服务存在，则您可以为业务组成员创建授权。请参见[将服务、目录项和操作授权给用户](#)。

对显示组成员时的缓慢性能进行故障排除

查看组的详细信息时，业务组或自定义组成员显示缓慢。

问题

在具有大量用户的环境中查看用户信息时，用户名加载到用户界面的速度较慢。

原因

在包含大型 Active Directory 环境的环境中，需要较长的时间才能加载用户名。

解决方案

- ◆ 要减少检索工作负载，请尽可能使用 Active Directory 组或自定义组，而不是按名称添加大量单独成员。

对筛选时的意外条目进行故障排除

用于进行筛选选择的业务组列表显示意外或重复的条目。

问题

您在**管理 > 用户和组 > 业务组**下对业务组进行了更改。在“部署”页面上，当尝试按业务组筛选部署时，要筛选的可用业务组列表不会反映您的更改，也不会显示意外结果，例如重复的业务组。

原因

系统每 30 分钟轮询一次更改。

解决方案

等待最多 30 分钟，然后通过刷新浏览器刷新业务组筛选选择列表。

创建其他租户

作为系统管理员，您可以创建其他 vRealize Automation 租户，使用户能够访问完成工作分配所需的适当应用程序和资源。

租户是一组在软件实例内工作且具有特定特权的用户。通常，默认的 vRealize Automation 租户是在系统安装和初始配置期间创建的。随后，管理员可以创建其他租户，使用户能够登录并完成其工作分配。管理员可以为系统操作创建所需数量的租户。创建租户时，管理员必须指定名称、登录 URL、本地用户和管理员等基本配置。配置基本租户信息之后，租户管理员必须登录并使用 vRealize Automation 控制台的“管理”选项卡上的“身份目录管理”功能设置相应的 Active Directory 连接。此外，租户管理还可以将自定义品牌应用到租户。

前提条件

以**系统管理员**身份登录到 vRealize Automation 控制台。

步骤

1 （可选）指定租户信息

配置租户的第一步是命名新租户，将其添加到 vRealize Automation，并创建租户特定的访问 URL。

2 （可选）配置本地用户

vRealize Automation 系统管理员必须为每个适用的租户配置本地用户。

3 （可选）任命管理员

您可以从您为租户配置的身份存储中任命一个或多个租户管理员和 IaaS 管理员。

指定租户信息

配置租户的第一步是命名新租户，将其添加到 vRealize Automation，并创建租户特定的访问 URL。

前提条件

以**系统管理员**身份登录到 vRealize Automation 控制台。

步骤

- 1 选择**管理 > 租户**。
- 2 单击**新建**图标 (+)。
- 3 在**名称**文本框中输入名称。
- 4 (可选) 在**描述**文本框中输入描述。
- 5 在 **URL 名称**文本框中输入租户的唯一标识符。

此 URL 令牌用于将租户特定的标识符附加到 vRealize Automation 控制台 URL。

例如, 输入 **mytenant** 可创建 URL `https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant`。

注 在 vRealize Automation 7.0 和 7.1 中, 租户 URL 只能使用小写字母。

- 6 (可选) 在**联系人电子邮件**文本框中输入电子邮件地址。
- 7 单击**提交并执行下一步**。

配置本地用户

vRealize Automation 系统管理员必须为每个适用的租户配置本地用户。

管理员为租户创建常规信息之后, “本地用户”选项卡将处于活动状态, 且管理员可以指定有权访问租户的用户。当租户配置完成后, 本地租户用户可以登录到各自的租户以完成工作分配。

注 添加用户之后, 不能更改其配置。如果需要更改有关用户配置的任何内容, 必须删除用户并重新创建。

步骤

- 1 单击“本地用户”选项卡上的**添加**按钮。
- 2 在“用户详细信息”对话框上的**名字**和**姓氏**字段中, 输入用户的名字和姓氏。
- 3 在**电子邮件**字段中, 输入用户的电子邮件地址。
- 4 在**用户名**和**密码**字段中, 输入用户的用户 ID 和密码。
- 5 单击**添加**按钮。
- 6 针对租户的所有本地用户, 根据需要重复以上步骤。

结果

系统将为租户创建指定的本地用户。

任命管理员

您可以从您为租户配置的身份存储中任命一个或多个租户管理员和 IaaS 管理员。

租户管理员负责在租户的上下文中配置租户特定的品牌, 并管理身份存储、用户、组、授权和共享蓝图。

IaaS 管理员负责在 IaaS 中配置基础架构源端点、任命架构管理员并监控 IaaS 日志。

前提条件

- 任命 IaaS 管理员之前，必须先安装 IaaS。有关安装 IaaS 的详细信息，请参见安装 vRealize Automation。

步骤

- 1 在**租户管理员**搜索框中输入用户或组的名称，然后按 Enter。

要快速获得结果，请输入用户或组的全名，例如 myAdmins@mycompany.domain。重复此步骤以任命其他租户管理员。

- 2 如果安装了 IaaS，请在 **IaaS 管理员**搜索框中输入用户或组的名称，然后按 Enter。

要加快获得结果，请输入用户或组的全名，例如 IaaSAdmins@mycompany.domain。重复此步骤以任命其他基础架构管理员。

- 3 单击**添加**。

删除租户

系统管理员可从 vRealize Automation 中删除任何不需要的租户。

如果删除租户，该租户将立即从 vRealize Automation 界面中移除，但可能需要几小时才能从您的部署中完全移除。如果要删除租户并希望使用相同的 URL 创建另一个租户，请在创建新租户前等待几小时以完全删除之前的租户。

前提条件

以**系统管理员**身份登录到 vRealize Automation 控制台。

步骤

- 1 选择**管理 > 租户**。

- 2 选择要删除的租户。

请勿单击实际名称来选择租户，否则会打开租户进行编辑。

- 3 单击**删除**。

结果

租户将从您的 vRealize Automation 部署中删除。

为多租户配置安全设置

您可以在多租户环境中跨租户控制 NSX 安全对象的可用性。

在 vRealize Automation 中创建 NSX 安全对象时，其默认可用性可以是全局的，这意味着可在具有预留的关联端点的所有租户中可用，也可以对管理员之外的所有用户隐藏。

此外，租户间安全对象的可用性取决于关联端点在租户中是否具有预留或预留策略。

跨租户控制新安全对象可用性的方法以及现有安全对象呈现的行为、跨租户的相关行为、升级到此 vRealize Automation 版本后的行为，在相关主题在 [vRealize Automation 中控制安全对象的租户访问](#) 中进行了汇总。

配置自定义品牌

vRealize Automation 使您能将自定义品牌应用到租户登录和应用程序页面。

自定义品牌包括文本和背景颜色、企业徽标、公司名称、隐私权政策、版权声明和您希望出现在租户登录或应用程序页面的其他相关信息。

用于租户登录页面的自定义品牌

使用“登录屏幕品牌”页面，将自定义品牌应用到您的 vRealize Automation 租户登录页面。

您可以在租户登录页面使用默认 vRealize Automation 品牌，也可以使用“登录屏幕品牌”页面配置自定义品牌。请注意，自定义品牌会以相同的方式应用于所有租户应用程序。

使用此页面可以在所有租户登录页面配置品牌。

“登录屏幕品牌”页面会在“预览”窗格中显示当前实施的租户登录品牌。

注 保存新的租户登录页面品牌后，最长可能会延迟五分钟后，此品牌才会显示在所有登录页面上。

前提条件

要为品牌使用自定义徽标或其他图像，则必须有可用的适当文件。

步骤

- 1 以系统或租户管理员身份登录到 vRealize Automation。
- 2 单击**管理**选项卡。
- 3 选择**品牌 > 登录屏幕品牌**
- 4 要添加徽标图像，请单击“徽标”字段下的**上载**，然后导航到相应的文件夹并选择徽标图像文件。
- 5 要添加其他图像，请单击“图像”（可选）字段下的**上载**，然后导航到相应文件夹并选择其他图像文件。
- 6 要自定义背景颜色，请在**背景颜色**、**标题颜色**、**登录按钮背景颜色**以及**登录按钮前景颜色**字段中输入相应的十六进制代码。
如有需要，可上网搜索十六进制颜色代码列表。
- 7 单击**保存**应用您的设置。

结果

租户用户将在他们的登录页面看到自定义品牌。

用于租户应用程序的自定义品牌

使用应用程序品牌页面，将自定义品牌应用到 vRealize Automation 租户应用程序。

您可以在用户应用程序上使用默认 vRealize Automation 品牌，或者可以使用“应用程序品牌”页配置自定义品牌。此页面使您可以在应用程序页面的页眉和页脚上配置品牌。请注意，自定义品牌会以相同的方式应用于所有用户应用程序。

“应用程序品牌”页面会在页面底部显示当前实施的页眉或页脚品牌。

前提条件

如果要为品牌使用自定义徽标，则必须准备好徽标图像文件。

步骤

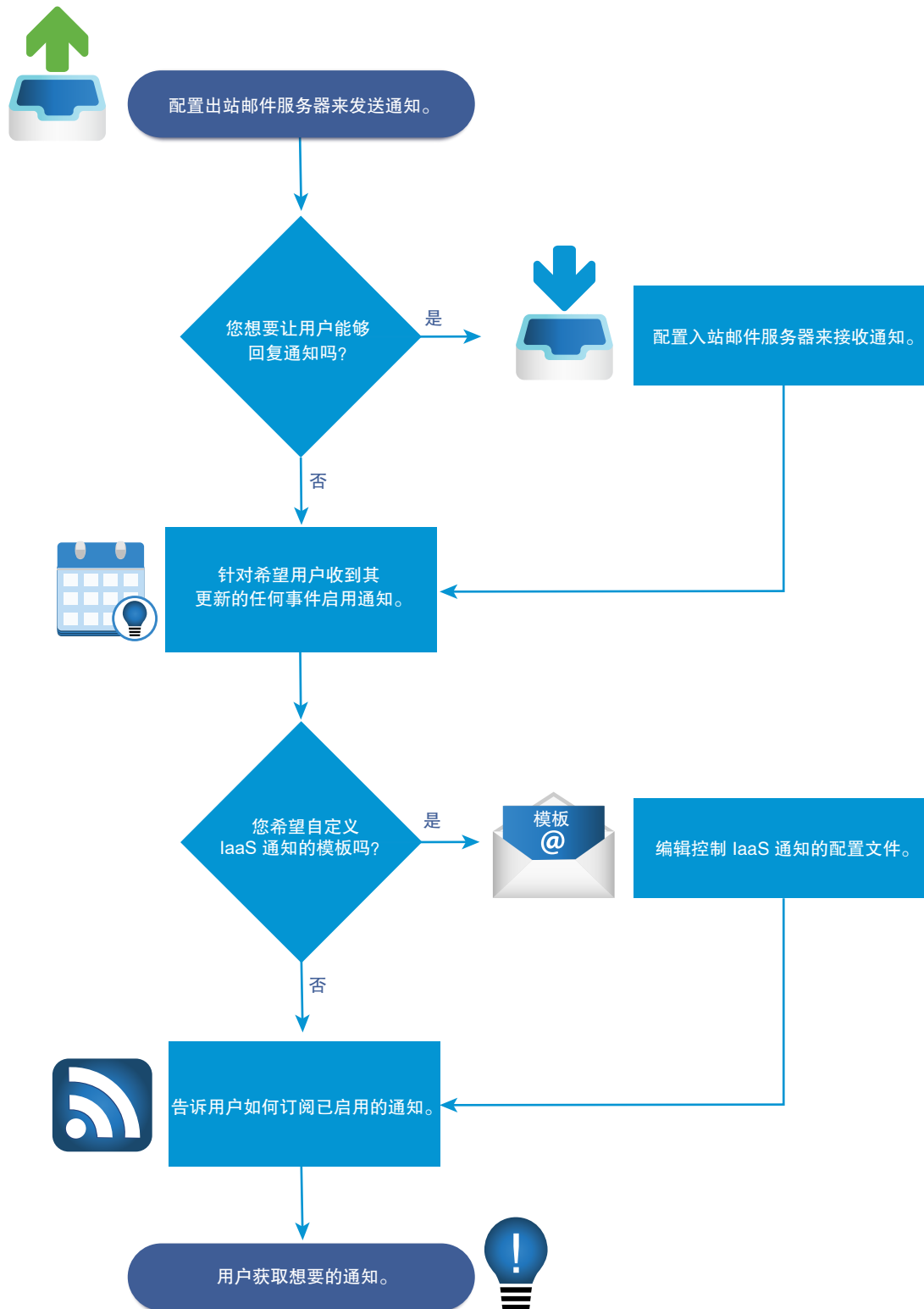
- 1 以系统或租户管理员身份登录到 vRealize Automation。
- 2 单击**管理**选项卡。
- 3 选择**品牌 > 应用程序品牌**
- 4 如果页眉没有处于活动状态，则单击**页眉**选项卡。
- 5 如果您要使用默认 vRealize Automation 品牌，则单击**使用默认值**复选框。
- 6 如果要实施自定义品牌，则在**页眉**和**页脚**选项卡上的字段中做出适当的选择。
 - a 单击**页眉徽标**字段中的**浏览**按钮，然后导航到合适的文件夹并选择徽标图像文件。
 - b 在**公司名称**字段键入相应的公司名称。
当用户将鼠标悬停在徽标上时会出现指定的名称。
 - c 在**产品名称**字段键入相应的名称。
在此处输入的名称将出现在徽标旁边的应用程序页眉中。
 - d 在**背景十六进制颜色**字段，为应用程序外围背景颜色输入恰当的十六进制颜色代码。
如有需要，可上网搜索十六进制颜色代码列表。
 - e 在**文本十六进制颜色**字段，为文本颜色输入恰当的十六进制代码。
如有需要，可上网搜索十六进制文本颜色代码列表。
 - f 单击**下一步**，激活“页脚”选项卡。
 - g 在**版权声明**字段键入所需声明。
 - h 在**隐私权政策链接**字段键入指向公司隐私权政策声明的链接。
 - i 在**联系链接**字段键入所需的公司联系信息。
- 7 单击**更新**实施品牌配置。

结果

租户用户将在他们的应用程序页面看到自定义品牌。

用于配置通知的对照表

您可以配置 vRealize Automation，以便发生特定事件时，向用户发送通知。用户可以选择订阅哪些通知，但他们只能选择启用为通知触发器的事件。



“配置通知对照表”概述了配置通知所需执行的一系列步骤，并提供了指向决策点的链接以及每一步的详细说明。

表 2-10. 用于配置通知的对照表

任务	所需角色	详细信息
<input type="checkbox"/> 配置出站电子邮件服务器以发送通知。	<ul style="list-style-type: none"> 系统管理员可以配置默认全局服务器。 租户管理员可以为他们的租户配置服务器。 	如果是首次为租户配置服务器，请参见 添加租户特定的出站电子邮件服务器 。如果需要替代默认全局服务器，请参见 替代系统默认的出站电子邮件服务器 。要为所有租户配置全局默认服务器，请参见 创建全局出站电子邮件服务器 。
<input type="checkbox"/> (可选) 配置入站电子邮件服务器，以便用户可以通过响应通知来完成任务。	<ul style="list-style-type: none"> 系统管理员可以配置默认全局服务器。 租户管理员可以为他们的租户配置服务器。 	如果是首次为租户配置服务器，请参见 添加租户特定的入站电子邮件服务器 。如果需要替代默认全局服务器，请参见 替代系统默认的入站电子邮件服务器 。要为所有租户配置全局默认服务器，请参见 创建全局入站电子邮件服务器 。
<input type="checkbox"/> (可选) 指定在计算机过期日期之前何时发送电子邮件通知。	系统管理员	请参见 自定义发送计算机过期电子邮件通知的日期 。
<input type="checkbox"/> 选择 vRealize Automation 事件以触发用户通知。用户只能订阅启用为通知触发器的事件的通知。	租户管理员	请参见 配置通知 。
<input type="checkbox"/> (可选) 针对向计算机所有者发送的有关其计算机的事件（例如租约过期）的通知，配置通知模板。	任何有权访问 vRealize Automation 服务器安装目录（通常为 %SystemDrive%\Program Files x86\VMware\VCAC\Server）下的 \Templates 目录的用户均可配置这些电子邮件通知的模板。	请参见 为自动 IaaS 电子邮件配置模板 。
<input type="checkbox"/> 用户自动订阅已配置的通知。 如有必要，可以向用户说明如何订阅启用的通知。他们只能选择订阅与他们的角色相关的通知。	所有用户	请参见 订阅通知 。

配置通知的全局电子邮件服务器

租户管理员可以在为自身租户配置通知的过程中添加电子邮件服务器。作为系统管理员，您可以设置对所有租户显示为系统默认值的全局入站和出站电子邮件服务器。如果租户管理员在启用通知前不替代这些设置，则 vRealize Automation 将使用全局配置的电子邮件服务器。

创建全局入站电子邮件服务器

系统管理员可以创建全局入站电子邮件服务器来处理诸如审批响应等入站电子邮件通知。只能创建一个入站服务器，该服务器对所有租户显示为默认值。如果租户管理员在启用通知前不替代这些设置，则 vRealize Automation 将使用全局配置的电子邮件服务器。

前提条件

以系统管理员身份登录到 vRealize Automation 控制台。

步骤

- 1 选择**管理 > 电子邮件服务器**。
- 2 单击**添加图标 (+)**。
- 3 选择**电子邮件 - 入站**。
- 4 单击**确定**。
- 5 在**名称**文本框中输入名称。
- 6 （可选）在**描述**文本框中输入描述。
- 7 （可选）选中 **SSL** 复选框，以使用 SSL 确保安全。
- 8 选择服务器协议。
- 9 在**服务器名称**文本框中键入服务器的名称。
- 10 在**服务器端口**文本框中键入服务器端口号。
- 11 在**文件夹名称**文本框中键入电子邮件的文件夹名称。
仅当选择 IMAP 服务器协议时才需要此选项。
- 12 在**用户名**文本框中输入用户名。
- 13 在**密码**文本框中输入密码。
- 14 在**电子邮件地址**文本框中，键入 vRealize Automation 用户可以回复的电子邮件地址。
- 15 （可选）选择**从服务器删除**，从服务器中删除由通知服务检索的所有已处理电子邮件。
- 16 选择 vRealize Automation 能否接受来自电子邮件服务器的自签名证书。
- 17 单击**测试连接**。
- 18 单击**添加**。

创建全局出站电子邮件服务器

系统管理员可以创建全局出站电子邮件服务器，用于处理出站电子邮件通知。只能创建一个出站服务器，该服务器对所有租户显示为默认值。如果租户管理员在启用通知前不替代这些设置，则 vRealize Automation 将使用全局配置的电子邮件服务器。

前提条件

以**系统管理员**身份登录到 vRealize Automation 控制台。

步骤

- 1 选择**管理 > 电子邮件服务器**。
- 2 单击**添加图标** (+)。
- 3 选择**电子邮件 - 出站**。
- 4 单击**确定**。
- 5 在**名称**文本框中输入名称。
- 6 （可选）在**描述**文本框中输入描述。
- 7 在**服务器名称**文本框中键入服务器的名称。
- 8 选择加密方法。
 - 单击**使用 SSL**。
 - 单击**使用 TLS**。
 - 单击**无**将发送未加密的通信。
- 9 在**服务器端口**文本框中键入服务器端口号。
- 10 （可选）如果服务器需要身份验证，请选中**必需**复选框。
 - a 在**用户名**文本框中键入用户名。
 - b 在**密码**文本框中键入密码。
- 11 在**发件人地址**文本框中，键入 vRealize Automation 电子邮件应源自的电子邮件地址。
此电子邮件地址对应于您提供的用户名和密码。
- 12 选择 vRealize Automation 能否接受来自电子邮件服务器的自签名证书。
- 13 单击**测试连接**。
- 14 单击**添加**。

添加租户特定的出站电子邮件服务器

租户管理员可以添加出站电子邮件服务器来发送请求完成工作项（如批准）的通知。

每个租户只能有一个出站电子邮件服务器。如果系统管理员已配置全局出站电子邮件服务器，请参见[替代系统默认的出站电子邮件服务器](#)。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation。
- 如果电子邮件服务器需要身份验证，则指定的用户必须位于身份存储和业务组中。

步骤

- 1 选择**管理 > 通知 > 电子邮件服务器**。
- 2 单击**添加图标** (+)。
- 3 选择**电子邮件 - 出站**。
- 4 单击**确定**。
- 5 在**名称**文本框中输入名称。
- 6 (可选) 在**描述**文本框中输入描述。
- 7 在**服务器名称**文本框中键入服务器的名称。
- 8 选择加密方法。
 - 单击**使用 SSL**。
 - 单击**使用 TLS**。
 - 单击**无**将发送未加密的通信。
- 9 在**服务器端口**文本框中键入服务器端口号。
- 10 (可选) 如果服务器需要身份验证，请选中**必需**复选框。
 - a 在**用户名**文本框中键入用户名。
 - b 在**密码**文本框中键入密码。
- 11 在**发件人地址**文本框中，键入 vRealize Automation 电子邮件应源自的电子邮件地址。
此电子邮件地址对应于您提供的用户名和密码。
- 12 选择 vRealize Automation 能否接受来自电子邮件服务器的自签名证书。
仅当已启用加密时，才可使用此选项。
 - 单击**是**接受自签名证书。
 - 单击**否**拒绝自签名证书。
- 13 单击**测试连接**。
- 14 单击**添加**。

添加租户特定的入站电子邮件服务器

租户管理员可以添加入站电子邮件服务器，以使用户能够响应请求完成工作项（如批准）的通知。

每个租户只能有一个入站电子邮件服务器。如果系统管理员已配置全局入站电子邮件服务器，请参见[替代系统默认的入站电子邮件服务器](#)。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation。
- 确认指定的用户已位于身份存储和业务组中。

步骤

- 1 选择**管理 > 通知 > 电子邮件服务器**。
- 2 单击**添加图标** (+)。
- 3 选择**电子邮件 - 入站**，然后单击**确定**。
- 4 配置以下入站电子邮件服务器选项。

选项	操作
名称	输入入站电子邮件服务器的名称。
描述	输入入站电子邮件服务器的描述。
安全	选中 使用 SSL 复选框。
协议	选择服务器协议。
服务器名称	输入服务器名称。
服务器端口	输入服务器端口号。

- 5 在**文件夹名称**文本框中键入电子邮件的文件夹名称。
仅当选择 IMAP 服务器协议时才需要此选项。
- 6 在**用户名**文本框中输入用户名。
- 7 在**密码**文本框中输入密码。
- 8 在**电子邮件地址**文本框中，键入 vRealize Automation 用户可以回复的电子邮件地址。
- 9 （可选）选择**从服务器删除**，从服务器中删除由通知服务检索的所有已处理电子邮件。
- 10 选择 vRealize Automation 能否接受来自电子邮件服务器的自签名证书。
仅当已启用加密时，才可使用此选项。
 - 单击**是**接受自签名证书。
 - 单击**否**拒绝自签名证书。
- 11 单击**测试连接**。
- 12 单击**添加**。

替代系统默认的出站电子邮件服务器

如果系统管理员已配置系统默认的出站电子邮件服务器，则租户管理员可以替代此全局设置。

前提条件

以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 通知 > 电子邮件服务器**。
- 2 选择“出站”电子邮件服务器。
- 3 单击**替代全局**。
- 4 在**名称**文本框中输入名称。
- 5 （可选）在**描述**文本框中输入描述。
- 6 在**服务器名称**文本框中键入服务器的名称。
- 7 选择加密方法。
 - 单击**使用 SSL**。
 - 单击**使用 TLS**。
 - 单击**无**将发送未加密的通信。
- 8 在**服务器端口**文本框中键入服务器端口号。
- 9 （可选）如果服务器需要身份验证，请选中**必需**复选框。
 - a 在**用户名**文本框中键入用户名。
 - b 在**密码**文本框中键入密码。
- 10 在**发件人地址**文本框中，键入 vRealize Automation 电子邮件应源自的电子邮件地址。
此电子邮件地址对应于您提供的用户名和密码。
- 11 选择 vRealize Automation 能否接受来自电子邮件服务器的自签名证书。
仅当已启用加密时，才可使用此选项。
 - 单击**是**接受自签名证书。
 - 单击**否**拒绝自签名证书。
- 12 单击**测试连接**。
- 13 单击**添加**。

替代系统默认的入站电子邮件服务器

如果系统管理员已配置系统默认的入站电子邮件服务器，则租户管理员可以替代此全局设置。

前提条件

以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 通知 > 电子邮件服务器**。
- 2 在“电子邮件服务器”表中，选择“入站”电子邮件服务器。
- 3 单击**替代全局**。

4 输入以下入站电子邮件服务器选项。

选项	操作
名称	输入入站电子邮件服务器的名称。
描述	输入入站电子邮件服务器的描述。
安全	选中 SSL 复选框，以使用 SSL 确保安全。
协议	选择服务器协议。
服务器名称	输入服务器名称。
服务器端口	输入服务器端口号。

5 在文件夹名称文本框中键入电子邮件的文件夹名称。

仅当选择 IMAP 服务器协议时才需要此选项。

6 在用户名文本框中输入用户名。

7 在密码文本框中输入密码。

8 在电子邮件地址文本框中，键入 vRealize Automation 用户可以回复的电子邮件地址。

9 （可选）选择从服务器删除，从服务器中删除由通知服务检索的所有已处理电子邮件。

10 选择 vRealize Automation 能否接受来自电子邮件服务器的自签名证书。

仅当已启用加密时，才可使用此选项。

- 单击是接受自签名证书。
- 单击否拒绝自签名证书。

11 单击测试连接。

12 单击添加。

恢复为系统默认的电子邮件服务器

替代系统默认服务器的租户管理员可以将相关设置恢复为全局设置。

前提条件

以租户管理员身份登录到 vRealize Automation。

步骤

1 选择管理 > 通知 > 电子邮件服务器。

2 选择要恢复的电子邮件服务器。

3 单击恢复全局。

4 单击是。

配置通知

每个用户可确定是否接收通知，但租户管理员可确定哪些事件触发通知。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation。
- 确认租户管理员或系统管理员已配置出站电子邮件服务器。请参见[添加租户特定的出站电子邮件服务器](#)。

步骤

- 1 选择**管理 > 通知 > 场景**。
- 2 选择一个或多个通知。
- 3 单击**激活**。

结果

现在，在首选项设置中订阅通知的用户将收到通知。

自定义发送计算机过期电子邮件通知的日期

可以指定在计算机过期日期之前何时发送电子邮件通知。

可以更改相关设置，以定义 vRealize Automation 发送过期通知电子邮件的日期距离计算机过期日期的天数。该电子邮件会通知用户计算机的过期日期。默认设置是计算机过期之前 7 天。

步骤

- 1 使用具有管理访问权限的凭据登录到 vRealize Automation 服务器。
- 2 导航到并打开 `/etc/vcac/setenv-user` 文件。
- 3 将以下行添加到该文件以指定计算机过期之前的天数，在此示例中，3 指定了计算机过期之前 3 天。

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

- 4 运行以下命令以在虚拟设备上重新启动 vCAC 服务：

```
service vcac-server restart
```

后续步骤

如果在高可用性负载平衡器环境中工作，请对 HA 环境中的所有虚拟设备重复以上过程。

为自动 IaaS 电子邮件配置模板

您可将涉及计算机的各种 vRealize Automation 事件的电子邮件通知配置为发送到计算机所有者。

触发这些通知的事件包括：存档时间段和虚拟机租约已过期或即将过期。

有关配置和启用或禁用 vRealize Automation 电子邮件通知的信息，请参见以下博客文章和知识库文章：

- [vRealize Automation 中的电子邮件自定义](#)

- [在 vRealize Automation 中自定义电子邮件模板 \(2088805\)](#)
- [在 vRealize Automation 中自定义电子邮件模板的示例 \(2102019\)](#)

订阅通知

如果您的管理员已配置通知，则会自动为您订阅。通知事件可以包括成功完成目录请求或所需批准。

如果您必须手动订阅，则可以启用您的通知。

前提条件

登录 vRealize Automation。

步骤

- 1 单击**首选项**。
- 2 在“通知”表中，选中“电子邮件”协议对应的**已启用**复选框。
- 3 单击**应用**。
- 4 单击**关闭**。

为置备的计算机创建自定义 RDP 文件以支持 RDP 连接

系统管理员可以创建一个自定义远程桌面协议文件。使用该文件，IaaS 架构师可在蓝图中配置 RDP 设置。您将创建 RDP 文件并为架构师提供该文件的完整路径名，使他们能够将其包含在蓝图中。稍后，目录管理员将授权用户执行 RDP 操作。

注 如果使用已启用“增强型安全配置”的 Internet Explorer，则无法下载 .rdp 文件。

前提条件

以管理员身份登录到 IaaS Manager Service。

步骤

- 1 将当前目录设置为 `<vRA_installation_dir>\Rdp`。
- 2 复制文件 `Default.rdp` 并在同一目录中将其重命名为 `Console.rdp`。
- 3 在编辑器中打开 `Console.rdp` 文件。
- 4 将 RDP 设置添加到该文件中。
例如，**connect to console:i:1**。
- 5 如果您是在分布式环境中进行操作，请以对安装了 Model Manager Website 组件的 IaaS 主机具有管理特权的用户身份登录。
- 6 将 `Console.rdp` 文件复制到目录 `vRA 安装目录\Server\Website\Rdp`。

7 将 VirtualMachine.Rdp.File 自定义属性添加到蓝图中。

IaaS 架构师可以将 RDP 自定义属性添加到 Windows 计算机蓝图，然后目录管理员可以授权用户执行“使用 RDP 连接”操作。请参见[将 RDP 连接支持添加到 Windows 计算机蓝图](#)。

场景：为跨区域部署添加数据中心位置

作为系统管理员，您需要定义波士顿和伦敦数据中心的位置，使架构管理员可以将适当的位置应用于每个数据中心的计算资源。蓝图架构师可以在创建蓝图时启用位置功能，使用户能够在填写目录项请求表单时选择在波士顿或伦敦置备计算机。

您在伦敦和波士顿分别设有一个数据中心，但不希望位于波士顿的用户在伦敦的基础架构中置备计算机，反之亦然。为了确保位于波士顿和伦敦的用户在各自的基础架构中置备计算机，您需要允许用户在请求计算机时选择适当的位置进行置备。



无法根据租户或业务组在 xml 文件中筛选数据中心位置。在多租户环境中工作时，您可以使用属性定义根据租户或业务组进行筛选。有关使用属性定义的信息，请参见博客文章[如何使用动态属性定义](#)。

步骤

- 1 使用管理员凭据登录 IaaS Web 服务器主机。
这是您安装了 IaaS Website 组件的计算机。
- 2 编辑 Windows 服务器安装目录（通常为 %SystemDrive%\Program Files x86\VMware\VCAC\Server）中的文件 Website\XmlData\DataCenterLocations.xml。
- 3 编辑该文件的 CustomDataType 部分，为每个位置创建“数据名称”条目。

```
<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
```

- 4 保存并关闭文件。
- 5 重新启动 Manager Service。
- 6 如果拥有多个 IaaS Web 服务器主机，请在每个冗余实例上重复此过程。

结果

架构管理员可以对每个数据中心内的计算资源应用适当的位置。请参见[场景：为跨区域部署将位置应用到计算资源](#)。

后续步骤

您可以将 `Vrm.DataCenter.Location` 属性添加到蓝图，或者在蓝图中启用**请求时显示位置**选项，要求用户在请求计算机置备时提供数据中心位置。

配置 vRealize Orchestrator

vRealize Orchestrator 是一个自动化和管理引擎，可将 vRealize Automation 扩展为支持 XaaS 和其他可扩展性功能。您可以配置并使用在 vRealize Automation 设备中预配置的 vRealize Orchestrator 服务器，也可以将 vRealize Orchestrator 部署为外部服务器实例，并将该外部实例与 vRealize Automation 相关联。

vRealize Orchestrator 允许管理员和架构师通过使用 workflow 设计器开发复杂的自动化任务，并从 vRealize Automation 中访问和运行 workflow。

vRealize Orchestrator 可以通过使用 vRealize Orchestrator 插件访问并控制外部技术和应用程序。

将 vRealize Automation 配置为使用 vRealize Orchestrator 时，可在 vRealize Orchestrator 服务目录中发布 vRealize Orchestrator workflow 来作为 XaaS 蓝图管理的一部分。

如果要运行 workflow 以扩展 IaaS 计算机的管理范围，必须将 vRealize Orchestrator 配置为端点。

配置特权

系统和租户管理员可以将 vRealize Automation 配置为使用外部或嵌入式 vRealize Orchestrator 服务器。

此外，系统管理员还可以确定每个租户可用的 workflow 文件夹。

租户管理员可以将 vRealize Orchestrator 插件配置为端点。

角色	与 vRealize Orchestrator 相关的配置特权
系统管理员	<ul style="list-style-type: none"> ■ 为所有租户配置 vRealize Orchestrator 服务器。 ■ 定义每个租户的默认 vRealize Orchestrator workflow 文件夹。
租户管理员	<ul style="list-style-type: none"> ■ 为自己的租户配置 vRealize Orchestrator 服务器。 ■ 将 vRealize Orchestrator 插件添加为端点。

配置嵌入式 vRealize Orchestrator 服务器

vRealize Automation 设备包括预配置的 vRealize Orchestrator 实例。

前提条件

部署 vRealize Automation 设备。有关详细信息，请参见安装 vRealize Automation 中的“部署 vRealize Automation 设备”。

步骤

- 1 以**系统管理员**或**租户管理员**身份登录到 vRealize Automation 控制台。
- 2 选择**管理 > VRO 配置 > 服务器配置**。
- 3 单击**使用默认 Orchestrator 服务器**。

结果

与嵌入式 vRealize Orchestrator 服务器的连接现已配置完成。系统将自动导入 **VCAC** 工作流文件夹和相关实用程序操作。**VCAC > ASD** 工作流文件夹包含用于配置端点和创建资源映射的工作流。

登录到 vRealize Orchestrator 控制中心

要编辑 vRealize Automation 中嵌入的默认 vRealize Orchestrator 实例的配置，必须登录到 vRealize Orchestrator 控制中心。

嵌入式 vRealize Orchestrator 实例的配置服务将自动启动。

注 可以通过从 vRealize Orchestrator Appliance 命令行控制台运行 `chkconfig vco-configurator` 命令验证配置是否自动启动。如果服务报告 `off`，请运行 `chkconfig vco-configurator on` 命令，然后重新引导设备。

步骤

- 1 在 Web 浏览器中连接到 vRealize Automation URL。
- 2 单击 **vRealize Orchestrator 控制中心**。
将重定向到 `https://vra-va hostname.domain.name_or_load_balancer_address: 8283/vco/controlcenter`。
- 3 输入 vRealize Automation 环境的 root 凭据。

登录到 vRealize Orchestrator Client

要执行常规的管理任务或在默认的 vRealize Orchestrator 实例中编辑并创建工作流，您必须登录 vRealize Orchestrator Client。

vRealize Orchestrator Client 界面专为具有管理权限且希望开发工作流、操作和其他自定义元素的开发人员而设计。

步骤

- 1 在 Web 浏览器中连接到 vRealize Automation URL。
- 2 单击 **vRealize Orchestrator Client**。
已下载客户端文件。
- 3 单击“下载”并按照提示操作。

4 在安全警告窗口中，选择一个选项以处理证书警告。

vRealize Orchestrator Client 使用 SSL 证书与 vRealize Orchestrator 服务器进行通信。可信 CA 在安装期间不签署证书。每次连接到 vRealize Orchestrator 服务器时，您都会收到安全警告。

选项	描述
继续	使用当前的 SSL 证书继续。 重新连接到同一 vRealize Orchestrator 服务器或者尝试将工作流与远程 vRealize Orchestrator 服务器同步时，会再次显示该警告消息。
取消	关闭该窗口并停止登录过程。

您可以使用由 CA 签名的证书更改默认 SSL 证书。有关更改 SSL 证书的详细信息，请参见《安装和配置 VMware vRealize Orchestrator》。

5 单击运行。

6 在 vRealize Orchestrator 登录页面中，在主机名文本框中输入 vRealize Automation 设备的 IP 或域名，并输入 443 作为默认端口号。

例如，输入 `vrealize_automation_appliance_ip:443`。

7 输入 vRealize Orchestrator 客户端用户名和密码，然后单击登录。

凭据是默认租户管理员的用户名和密码。

后续步骤

您可以在系统上导入软件包、开发工作流或设置根访问权限。请参见《使用 VMware vRealize Orchestrator Client》和《使用 VMware vRealize Orchestrator 进行开发》。

配置外部 vRealize Orchestrator 服务器

您可设置 vRealize Automation 以使用外部 vRealize Orchestrator 服务器。

系统管理员可以为所有租户全局配置默认的 vRealize Orchestrator 服务器。租户管理员只能为其租户配置 vRealize Orchestrator 服务器。

与外部 vRealize Orchestrator 服务器实例的连接要求用户帐户在 vRealize Orchestrator 中具有查看和运行权限。

- Single Sign-On 身份验证。用户信息通过 XaaS 请求传递给 vRealize Orchestrator，且系统将授予用户对请求的工作流具有查看和运行权限。
- 基本身份验证。提供的用户帐户必须是具有查看和运行权限的 vRealize Orchestrator 组成员，或者是 vcoadmins 组成员。

前提条件

- 安装并配置外部 vRealize Orchestrator 设备。请参见 [vRealize Orchestrator 产品文档](#) 中的《安装和配置 vRealize Orchestrator》
- 以系统管理员或租户管理员身份登录到 vRealize Automation 控制台。

步骤

- 1 选择**管理 > vRO 配置 > 服务器配置**。
- 2 单击**使用外部 Orchestrator 服务器**。
- 3 输入名称和可选描述。
- 4 在**主机**文本框中，输入运行 vRealize Orchestrator 服务器的计算机的 IP 或 DNS 名称。

注 如果外部 vRealize Orchestrator 配置为在集群模式下工作，则输入在集群中的 vRealize Orchestrator 服务器之间分发客户端请求的负载均衡器虚拟服务器的 IP 地址或主机名。

- 5 在**端口**文本框中，输入要与外部 vRealize Orchestrator 服务器通信的端口号。
8281 是 vRealize Orchestrator 的默认端口。
- 6 选择身份验证类型。

选项	描述
Single Sign-On	通过使用 vCenter Single Sign-On 连接到 vRealize Orchestrator 服务器。 此选项仅当您已将 vRealize Orchestrator 和 vRealize Automation 配置为共用一个 vCenter Single Sign-On 实例时才适用。
基本	使用您在 用户名 和 密码 文本框中输入的用户名和密码连接到 vRealize Orchestrator 服务器。 您提供的帐户必须是 vRealize Orchestrator vcoadmins 组成员，或者是具有查看和运行权限的组成员。

- 7 单击**测试连接**。
- 8 单击**确定**。
- 9 导入 `xaas.package` 软件包。
 - a 以 **root** 用户身份登录到 vRealize Automation 设备。
 - b 在 `/usr/lib/vcac/content/o11n/` 文件夹中找到 `xaas.package` 软件包。
 - c 将 `xaas.package` 软件包导入到外部客户端。

结果

您配置了与外部 vRealize Orchestrator 服务器的连接，并导入了 **VCAC** 工作流文件夹和相关实用程序操作。**VCAC > ASD** 工作流文件夹包含用于配置端点和创建资源映射的工作流。

后续步骤

[登录到 vRealize Orchestrator Client](#)。

配置资源

您可以配置端点、预留以及网络配置文件等资源来支持 vRealize Automation 蓝图定义和计算机置备。

用于配置 IaaS 资源的对照表

IaaS 管理员和架构管理员可以将 IaaS 资源配置为将现有基础架构与 vRealize Automation 集成以及将基础架构资源分配给 vRealize Automation 业务组。

您可以使用“配置 IaaS 资源对照表”，查看对配置 IaaS 资源所需执行的一系列步骤的概述。



表 2-11. 用于配置 IaaS 资源的对照表

任务	vRealize Automation 角色	详细信息
<input type="checkbox"/> 为您的基础架构创建端点，使资源受 vRealize Automation 管理。	IaaS 管理员	选择端点场景。
<input type="checkbox"/> 创建架构组，将基础架构资源组织到组中，并分配一个或多个管理员作为 vRealize Automation 架构管理员来管理这些资源。	IaaS 管理员	创建架构组。
<input type="checkbox"/> 配置计算机前缀，用于为通过 vRealize Automation 置备的计算机创建名称。	架构管理员	配置计算机前缀。
<input type="checkbox"/> (可选) 创建网络配置文件，为置备的计算机配置网络设置。	架构管理员	创建网络配置文件。
<input type="checkbox"/> 通过创建预留，或者创建预留和存储预留配置文件（可选），将基础架构资源分配给业务组。	<ul style="list-style-type: none"> IaaS 管理员（如果同时配置了架构管理员） 架构管理员 	配置预留和预留策略。

配置端点

您可以创建并配置允许 vRealize Automation 与基础架构进行通信的端点。

端点定义根据类型进行分类：

- 云

云类别包含 vCloud Air、vCloud Director、Amazon EC2 和 OpenStack 端点类型

- IPAM

只有在 vRealize Orchestrator 工作流中注册了第三方 IPAM 端点类型，如 Infoblox IPAM，此类别才可见。

- 管理

此类别仅包含 vRealize Operations Manager 端点。

- 网络 and 安全性

此类别包含代理和 NSX 端点类型。

代理端点可关联到 Amazon、vCloud Air 或 vCloud Director 端点。

NSX 端点可关联到 vSphere 端点。

- 编排

此类别仅包含 vRealize Orchestrator 端点。

- 存储

此类别包含 NetApp ONTAP 端点。

- 虚拟

虚拟类别包含 vSphere、Hyper-V (SCVMM) 和 KVM (RHEV) 端点类型。

可以在 vRealize Orchestrator 中配置其他端点类型，并将其与 vRealize Automation 中受支持的端点类型配合使用。您也可以编程方式导入和导出端点。

有关升级或迁移之后使用端点的信息，请参见[使用已升级或已迁移端点的注意事项](#)。

选择端点场景

根据目标端点类型选择端点场景。

有关可用端点设置的信息，请参见[端点设置参考](#)。

表 2-12. 选择端点场景

端点	更多信息
vSphere	请参见 创建 vSphere 端点 。
NSX	请参见 创建 NSX for vSphere 端点并关联到 vSphere 端点 或 创建 NSX-T 端点并关联到 vSphere 端点 。
vCloud Air（订阅或 OnDemand）	请参见 创建 vCloud Air 端点 。

表 2-12. 选择端点场景（续）

端点	更多信息
vCloud Director	请参见 创建 vCloud Director 端点 。
vRealize Orchestrator	请参见 创建 vRealize Orchestrator 端点 。
vRealize Operations	请参见 创建 vRealize Operations Manager 端点 。
第三方 IPAM 提供程序	请参见 创建第三方 IPAM 提供程序端点 。
Microsoft Azure	请参见 创建 Microsoft Azure 端点 。
Puppet	请参见 创建 Puppet 端点 。
Amazon	请参见 创建 Amazon 端点 和添加 Amazon 实例类型 。
OpenStack	请参见 创建 OpenStack 端点 。
代理	创建代理端点并关联到云端点
Hyper-V (SCVMM)	请参见 创建 Hyper-V (SCVMM) 端点 。
KVM (RHEV)	请参见 端点设置参考 。
NetApp ONTAP	请参见 用于虚拟置备的节省空间存储和端点设置参考 。
Hyper-V（独立），XenServer 或 Xen 池主机	请参见 创建 Hyper-V、XenServer 或 Xen 池端点 。
导入端点	请参见 以编程方式导入或导出端点 。

端点设置参考

使用端点设置可定义数据收集和服务目录部署的位置和访问凭据。

“常规”选项卡

大多数 vRealize Automation 端点包含以下选项。说明了特定端点类型所独有的设置。

表 2-13. 常规选项卡设置

设置	描述
名称	输入端点名称。
描述	输入端点描述。

表 2-13. 常规选项卡设置（续）

设置	描述
地址	<p>输入采用端点特定地址格式的端点地址。</p> <ul style="list-style-type: none"> ■ 对于 KVM (RHEV) 或 NetApp ONTAP 端点，地址必须采用以下格式之一： <ul style="list-style-type: none"> ■ <code>https://FQDN</code> ■ <code>https://IP_address</code> <p>例如：<code>https://mycompany-kvmrhev1.mycompany.local</code> 或 <code>netapp-1.mycompany.local</code>。</p> ■ 对于 OpenStack 端点，地址格式必须为 <code>https:// FQDN/powervc/openstack/ service</code>。例如：<code>https://openstack.mycompany.com/powervc/openstack/admin</code>。 ■ 对于 OpenStack 端点，地址必须采用以下格式之一： <ul style="list-style-type: none"> ■ <code>https://FQDN:500</code> ■ <code>https://IP_address:500</code> ■ 对于 vSphere 端点，地址必须为 <code>https://host/sdk</code> 格式。 ■ 对于 NSX 端点，地址必须为 <code>https://host</code> 格式。 ■ 对于 vRealize Orchestrator 端点，地址必须为 https 协议，且包括 vRealize Orchestrator 服务器的完全限定名称或 IP 地址以及 vRealize Orchestrator 端口号，例如 <code>https://vrealize-automation-appliance-hostname:443/vco</code>。 ■ 对于 vRealize Operations 端点，地址必须为 <code>https://host/suite-api</code> 格式。
集成凭据	<p>如果选择使用 vSphere 集成凭据，则不需要输入用户名和密码。 此设置仅适用于 vSphere 端点。</p>
用户名	按照用户界面中的建议，输入以端点特定格式为端点存储的管理员级别用户名。
密码	输入为端点存储的管理员级别密码。
OpenStack 项目	<p>输入 OpenStack 租户名称。 此设置仅适用于 OpenStack 端点。</p>
组织	<p>如果您是组织管理员，则可以输入 vCloud Director 组织名称。 此设置仅适用于 vCloud Director。</p>
访问密钥 ID	<p>输入 Amazon AWS 密钥 ID。 此设置仅适用于 Amazon 端点。</p>
私有访问密钥	<p>输入 Amazon AWS 私有访问密钥。 此设置仅适用于 Amazon 端点。</p>
端口	<p>在代理端点地址中输入要连接的端口值。 此设置仅适用于代理端点。</p>
优先级	<p>输入大于或等于 1 的整数作为优先级值。值越小表示优先级越高。 优先级值将关联到嵌入式 VMware.VCenterOrchestrator.Priority 自定义属性。 此设置仅适用于 vRealize Orchestrator 端点。</p>

“属性”选项卡

所有端点类型使用一个属性选项卡来捕获自定义属性或属性组和设置。有关特定端点类型的自定义属性的示例，请参见《自定义属性参考》。

关联选项卡

您可以创建与 NSX 端点或代理端点的关联，具体取决于与之关联的端点。您可以将 vSphere 端点与 NSX 端点相关联，以向 vSphere 端点分配 NSX 设置。您还可以将 vCloud Air、vCloud Director 或 Amazon 端点与代理端点相关联，以便将代理设置分配给 vCloud Air、vCloud Director 或 Amazon 端点。

测试连接

可以使用测试连接操作来验证 vSphere、NSX 或 vRealize Operations Manager 端点的凭据、主机端点地址和证书。请参见[使用测试连接时的注意事项](#)。

创建 vSphere 端点

您可以创建端点，允许 vRealize Automation 与 vSphere 环境通信并发现计算资源、收集数据和置备计算机。还可以通过与 NSX for vSphere 或 NSX-T 端点关联，将 NSX 设置关联到 vSphere 端点。

如果升级或迁移使用 NSX Manager 的 vSphere 端点，在升级时会创建新的 NSX 端点，其中包含源 vSphere 端点与新 NSX 端点之间的关联。

如果您的 vSphere 环境集成了 NSX for vSphere 或 NSX-T，请参见[创建 NSX for vSphere 端点并关联到 vSphere 端点](#)或[创建 NSX-T 端点并关联到 vSphere 端点](#)。

NSX-T 端点可以与 vRealize Automation 中的多个 vSphere 端点关联。但是，vSphere 端点只能与一个 NSX（NSX for vSphere 或 NSX-T）端点关联。

有关验证端点连接和证书信任的详细信息，请参见[使用测试连接时的注意事项](#)。

前提条件

- 以 **laaS 管理员** 身份登录到 vRealize Automation。
- 必须安装 vSphere 代理程序才能管理 vSphere 端点，并且必须为端点和代理使用完全相同的名称。有关安装代理的信息，请参见[安装 vRealize Automation](#)。
- 如果您计划使用 vSphere 端点从 OVF 模板部署虚拟机，请确认您的凭据包括与端点关联的 vCenter 中的 vSphere 特权 `VApp.Import`。

通过 `VApp.Import` 特权，可以使用从 OVF 导入的设置部署 vSphere 计算机。有关此 vSphere 特权的详细信息，请参见[vSphere SDK 文档](#)。

如果 OVF 托管在网站上，请参见[OVF 主机网站创建代理端点](#)。

- 如果您希望为 vSphere 端点配置其他 NSX 网络和安全设置，则创建 NSX for vSphere 或 NSX-T 端点，具体取决于 NSX 应用程序类型。可以在创建 vSphere 端点时关联到 NSX 端点。

步骤

- 1 选择**基础架构 > 端点 > 端点**。
- 2 选择**新建 > 虚拟 > vSphere**。

3 在**名称**文本框中输入名称。

该名称必须与安装期间提供给 vSphere 代理程序的端点名称匹配，否则数据收集将会失败。

4 （可选）在**描述**文本框中输入描述。

5 在**地址**文本框中输入 vCenter Server 实例的 URL。

该 URL 的类型必须为：**https://hostname/sdk** 或 **https://IP_address/sdk**。

例如，**https://vsphereA/sdk**。

6 输入您的 vSphere 管理员级别用户名和密码，或者改为使用 vSphere 集成凭据。

提供具有权限的凭据来修改自定义属性。

用户名格式为 *domain\username*。

选择**使用集成凭据**，使用 vSphere 代理程序的服务帐户连接到 vCenter Server。

如果选择使用 vSphere 集成凭据，则不需要输入用户名和密码。

7 （可选）单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。

8 （可选）要为端点配置 NSX 网络和安全设置，请单击**关联**，并关联到现有 NSX for vSphere 或 NSX-T 端点。

您必须至少有一个 NSX 端点才能创建关联。

9 （可选）单击**测试连接**来验证凭据、主机端点地址和证书信任。该操作还会检查 Manager Service 和代理是否正在运行，以便使端点可以进行数据收集。**确定**操作也会测试这些条件。

测试连接操作会返回与下列任一情况有关的信息：

- 证书错误

如果证书找不到、不受信任或已过期，系统将提示您接受证书指纹。如果不接受指纹，则仍可保存端点，但计算机置备可能会失败。

- 代理错误

找不到关联的 vSphere 代理。代理必须运行才能使测试成功。

- 主机错误

指定的端点地址无法访问或关联的 Manager Service 未运行。Manager Service 必须运行才能使测试成功。

- 凭据错误

指定的用户名和密码组合对于指定地址处的端点无效。

- 超时

在允许的两分钟时间内无法完成测试操作。

如果**测试连接**操作失败，则仍可保存端点，但计算机置备可能会失败。

如果有可信证书问题，例如证书已过期，系统将提示您接受证书指纹。

10 单击确定以保存端点。

确定操作与**测试连接**操作测试相同的条件。如果发现上述任何条件，则将返回一条消息。如果可以保存，则会在屏幕上保留错误以便您查看。

结果

vRealize Automation 会从端点收集数据并发现计算资源。

注 初始数据收集后不要重命名 vSphere 数据中心，否则置备可能会失败。

有关在初始数据收集后为现有端点运行数据收集的信息，请参见[查看端点源以及运行数据收集](#)。

后续步骤

将端点中的计算资源添加到架构组。请参见[创建架构组](#)。

创建 NSX for vSphere 端点并关联到 vSphere 端点

您可以创建 NSX for vSphere 端点，并将其与现有 vSphere 端点相关联。

如果升级或迁移使用 NSX Manager 的 vSphere 端点，在升级时会创建新的 NSX 端点，其中包含源 vSphere 端点与新 NSX 端点之间的关联。

NSX-T 端点可以与 vRealize Automation 中的多个 vSphere 端点关联。但是，vSphere 端点只能与一个 NSX（NSX for vSphere 或 NSX-T）端点关联。

有关创建端点时验证 NSX 连接和证书信任的信息，请参见[使用测试连接时的注意事项](#)。

前提条件

- 以 **laaS 管理员** 身份登录到 vRealize Automation。
- 必须安装 vSphere 代理程序才能管理 vSphere 端点，并且必须为端点和代理使用完全相同的名称。有关安装代理的信息，请参见[安装 vRealize Automation](#)。
- 配置 NSX for vSphere 网络设置。请参见[配置网络与安全组件设置](#)。
- [创建 vSphere 端点](#)。

准备在 vRealize Automation 中使用 NSX 网络、安全和负载平衡功能时，使用 NSX Manager 凭据时必须使用 NSX Manager 管理员帐户。

步骤

- 1** 选择**基础架构 > 端点 > 端点**。
- 2** 选择**新建 > 网络和安全 > NSX**。
- 3** 在**名称**文本框中输入名称。
- 4** （可选）在**描述**文本框中输入描述。
- 5** 在**地址**文本框中输入 NSX for vSphere 实例的 URL。

该 URL 的类型必须为：**https://hostname** 或 **https://IP_address**。

例如，**https://abx.nsx-manager.local/**。

- 6 输入为 NSX for vSphere 端点存储的 NSX 管理员级别用户名和密码。
- 7 (可选) 单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 8 要将 NSX for vSphere 网络和安全设置关联到现有 vSphere 端点，请单击**关联**，并选择现有 vSphere 端点。

您必须先创建 vSphere 端点，然后才能创建关联。

vSphere 端点只能与一个类型的网络和安全平台相关联 - NSX for vSphere 或 NSX-T。

NSX for vSphere 端点只能关联到一个 vSphere 端点。此关联限制意味着您无法置备通用按需网络并将其连接到其他 vCenter 上置备的 vSphere 计算机。

完成关联后，页面上的“描述”列将指示 NSX for vSphere 的关联类型。

- 9 (可选) 单击**测试连接**来验证凭据、主机端点地址和证书信任。该操作还会检查 Manager Service 和代理是否正在运行，以便使端点可以进行数据收集。**确定**操作也会测试这些条件。

测试连接操作会返回与下列任一情况有关的信息：

- 证书错误

如果证书找不到、不受信任或已过期，系统将提示您接受证书指纹。如果不接受指纹，则仍可保存端点，但计算机置备可能会失败。

- 代理错误

找不到关联的 vSphere 代理。代理必须运行才能使测试成功。

- 主机错误

指定的端点地址无法访问或关联的 Manager Service 未运行。Manager Service 必须运行才能使测试成功。

- 凭据错误

指定的用户名和密码组合对于指定地址处的端点无效。

- 超时

在允许的两分钟时间内无法完成测试操作。

如果**测试连接**操作失败，则仍可保存端点，但计算机置备可能会失败。

如果有可信证书问题，例如证书已过期，系统将提示您接受证书指纹。

- 10 单击**确定**以保存端点。

确定操作与**测试连接**操作测试相同的条件。如果发现上述任何条件，则将返回一条消息。如果可以保存，则会在屏幕上保留错误以便您查看。

结果

vRealize Automation 会从端点收集数据并发现计算资源。

有关在初始数据收集后为现有端点运行数据收集的信息，请参见[查看端点源以及运行数据收集](#)。

后续步骤

将端点中的计算资源添加到架构组。请参见[创建架构组](#)。

创建 NSX-T 端点并关联到 vSphere 端点

您可以创建 NSX-T 端点，并将其与现有 vSphere 端点相关联。

部署的蓝图中包含 NSX-T 端点时，部署将向部署中的所有 NSX-T 组件分配一个标记，这些组件包括 NSX-T 网络、安全和负载均衡器组件以及 NSX-T 端点的关联 vSphere 计算机组件。标记对部署是唯一的，并与初始部署中的组件以及您在部署中所做的任何后续操作相关联。标记名称与部署的名称相同。

NSX-T 端点可以与 vRealize Automation 中的多个 vSphere 端点关联。但是，vSphere 端点只能与一个 NSX（NSX for vSphere 或 NSX-T）端点关联。

有关创建端点时验证 NSX 连接和证书信任的信息，请参见[使用测试连接时的注意事项](#)。

前提条件

- 以 **laaS 管理员** 身份登录到 vRealize Automation。
- 必须安装 vSphere 代理程序才能管理 vSphere 端点，并且必须为端点和代理使用完全相同的名称。有关安装代理的信息，请参见[安装 vRealize Automation](#)。
- 配置 NSX-T 网络设置。请参见[配置网络与安全组件设置](#)。
- [创建 vSphere 端点](#)。

准备在 vRealize Automation 中使用 NSX 网络、安全和负载均衡功能时，使用 NSX Manager 凭据时必须使用 NSX Manager 管理员帐户。

vRealize Automation 使用基本身份验证连接 NSX-T 端点。

步骤

- 1 选择**基础架构 > 端点 > 端点**。
- 2 选择**新建 > 网络和安全 > NSX-T**。
- 3 在**名称**文本框中输入名称。
- 4 （可选）在**描述**文本框中输入描述。
- 5 在**地址**文本框中输入 NSX-T 实例的 URL。
该 URL 的类型必须为：**https://hostname** 或 **https://IP_address**。
例如，**https://abx-nsxt3-manager.local**。
- 6 输入为 NSX-T 端点存储的 NSX 管理员级别用户名和密码。
- 7 （可选）单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 8 要将 NSX-T 网络和安全设置关联到现有 vSphere 端点，请单击**关联**，并选择现有 vSphere 端点。
您必须先创建 vSphere 端点，然后才能创建关联。

vSphere 端点只能与一个类型的网络和安全平台相关联 - NSX for vSphere 或 NSX-T。

您可以将 NSX-T 端点关联到多个 vSphere 端点。这样，一个 NSX-T 实例可以管理不同 vCenter 上的多个 ESX 群集。

完成关联后，页面上的“描述”列将指示 NSX-T 的关联类型。

- 9 （可选）单击**测试连接**来验证凭据、主机端点地址和证书信任。该操作还会检查 Manager Service 和代理是否正在运行，以便使端点可以进行数据收集。**确定**操作也会测试这些条件。

测试连接操作会返回与下列任一情况有关的信息：

- 证书错误

如果证书找不到、不受信任或已过期，系统将提示您接受证书指纹。如果不接受指纹，则仍可保存端点，但计算机置备可能会失败。

- 代理错误

找不到关联的 vSphere 代理。代理必须运行才能使测试成功。

- 主机错误

指定的端点地址无法访问或关联的 Manager Service 未运行。Manager Service 必须运行才能使测试成功。

- 凭据错误

指定的用户名和密码组合对于指定地址处的端点无效。

- 超时

在允许的两分钟时间内无法完成测试操作。

如果**测试连接**操作失败，则仍可保存端点，但计算机置备可能会失败。

如果有可信证书问题，例如证书已过期，系统将提示您接受证书指纹。

- 10 单击**确定**以保存端点。

确定操作与**测试连接**操作测试相同的条件。如果发现上述任何条件，则将返回一条消息。如果可以保存，则会在屏幕上保留错误以便您查看。

结果

vRealize Automation 会从端点收集数据并发现计算资源。

有关在初始数据收集后为现有端点运行数据收集的信息，请参见[查看端点源以及运行数据收集](#)。

后续步骤

将端点中的计算资源添加到架构组。请参见[创建架构组](#)。

创建 vCloud Air 端点

您可以为 OnDemand 或者订阅服务创建 vCloud Air 端点。此外，还可以通过关联到代理端点来将代理设置与 vCloud Director 端点关联起来。

有关 vCloud Air 管理控制台的信息，请参见 vCloud Air 文档。

注 为 vCloud Air 端点和 vCloud Director 端点定义的预留不支持使用网络配置文件来置备计算机。

对于 vCloud Air 端点，vCloud Air 订阅实例的组织名称和 vDC 名称必须相同。

有关将代理设置与端点关联的信息，请参见[创建代理端点并关联到云端点](#)。

前提条件

- 以 **IaaS 管理员** 身份登录到 vRealize Automation。
- 确认您具有 vCloud Air 订阅服务或 OnDemand 帐户的**虚拟基础架构管理员**授权。
- 如果要配置更多安全性并强制通过代理服务器连接，请创建代理端点。创建 vCloud Director 端点时，可以将其与代理端点关联起来。请参见[创建代理端点并关联到云端点](#)。

步骤

- 1 选择**基础架构 > 端点 > 端点**。
- 2 选择**新建 > Cloud > vCloud Air**。
- 3 输入名称和可选描述。
- 4 接受**地址**文本框中的默认 vCloud Air 端点地址，或输入新地址。
默认 vCloud Air 端点地址为 Default URL for vCloud Air endpoint 全局属性中指定的 https://vca.vmware.com。
- 5 输入管理员级别用户名和密码。
凭据必须是这些 vCloud Air 订阅服务或 OnDemand 帐户管理员的凭据。
用户名格式为 *domain\username*。
提供凭据，供具有权限的组织管理员使用 VMware Remote Console 进行连接。
- 6 （可选）单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 7 （可选）要增强安装性并迫使连接通过代理服务器，请单击**关联**，并关联到现有代理端点。
您必须至少有一个代理端点才能创建关联。
- 8 单击**确定**。

后续步骤

[创建架构组](#)。

创建 vCloud Director 端点

您既可以创建 vCloud Director 端点来管理环境中的所有 vCloud Director 虚拟数据中心 (vDC)，也可以创建单独的端点来管理每个 vCloud Director 组织。此外，还可以通过关联到代理端点来将代理设置与 vCloud Director 端点关联起来。

有关组织 vDC 的信息，请参见 vCloud Director 文档。

不要针对同一 vCloud Director 实例既创建单个端点又创建组织特定的端点。

vRealize Automation 使用代理程序管理 vSphere 资源。

注 为 vCloud Air 端点和 vCloud Director 端点定义的预留不支持使用网络配置文件来置备计算机。

必须在 vRealize Automation 中（而不是 vCloud Director 中）指定 vCloud Director 计算机的租约信息。如果在 vCloud Director 中指定租约信息，则无法在 vRealize Automation 中识别或使用该租约信息。在 vRealize Automation 蓝图中输入 vCloud Director 计算机的租约信息，而不是在 vCloud Director 中输入。

有关将代理设置与端点关联的信息，请参见[创建代理端点并关联到云端点](#)。

前提条件

- 以 **iaaS 管理员** 身份登录到 vRealize Automation。
- 如果要配置更多安全性并强制通过代理服务器连接，请创建代理端点。创建 vCloud Director 端点时，可以将其与代理端点关联起来。请参见[创建代理端点并关联到云端点](#)。

步骤

- 1 选择 **基础架构 > 端点 > 端点**。
- 2 选择 **新建 > Cloud > vCloud Director**。
- 3 输入名称和可选描述。
- 4 在 **地址** 文本框中输入 vCloud Director 服务器的 URL。
该 URL 的类型必须为 *FQDN* 或 *IP_address*。
例如，<https://mycompany.com>。
- 5 输入管理员级别用户名和密码。
 - 要连接到 vCloud Director 服务器并指定用户具有管理员角色的组织，请使用组织管理员凭据。通过这些凭据，该端点只能访问关联的组织 vDC。您可以为 vCloud Director 实例中要与 vRealize Automation 集成的其他每个组织添加端点。
 - 要允许访问 vCloud Director 实例中的所有组织 vDC，请对 vCloud Director 使用系统管理员凭据并将 **组织** 文本框留空。
- 6 如果您是组织管理员，则可在 **组织** 文本框中输入 vCloud Director 组织名称。

选项	描述
发现所有组织 vCD	如果您已在私有云中实施 vCloud Director，则可将 组织 文本框留空，从而允许应用程序发现所有可用的组织 vDC。
分隔每个组织 vCD 的端点	在 组织 文本框中输入 vCloud Director 组织名称。

组织名称与您的 vCloud Director 组织名称（也有可能会显示为虚拟数据中心 (vDC) 名称）匹配。如果使用 Virtual Private Cloud，则此名称是采用 M123456789-12345 格式的唯一标识符。在专用云中，这是目标 vDC 的指定名称。

如果要在系统级别直接连接到 vCloud Director，例如将“组织”字段留空，则需要使用系统管理员凭据。如果要在端点中输入组织，则需要使用在该组织中拥有组织管理员凭据的用户。

提供具有权限的凭据以使用 VMware Remote Console 进行连接。

- 要管理带单个端点的所有组织，需要提供系统管理员凭据。

- 要管理带单独端点的每个组织虚拟数据中心 (vDC)，需要创建每个 vDC 的单独的组织管理员凭据。

不要针对同一 vCloud Director 实例既创建单个系统级别的端点又创建组织特定的端点。

- 7 (可选) 单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 8 (可选) 要增强安装性并迫使连接通过代理服务器，请单击**关联**，并关联到现有代理端点。

您必须至少有一个代理端点才能创建关联。

- 9 单击**确定**。

后续步骤

[创建架构组](#)。

创建 Amazon 端点

您可以创建一个端点以连接到 Amazon 实例。还可以通过关联到代理端点，将代理设置关联到 Amazon 端点。

vRealize Automation 提供了多种创建蓝图时可使用的 Amazon 实例类型，但如果要导入自己的实例类型，请参见[添加 Amazon 实例类型](#)。

有关将代理设置与端点关联的信息，请参见[创建代理端点并关联到云端点](#)。

前提条件

- 以 **IaaS 管理员** 身份登录到 vRealize Automation。
- 如果要配置更多安全性并强制通过代理服务器连接，请创建代理端点。可以在创建 Amazon 端点时关联到代理端点。请参见[创建代理端点并关联到云端点](#)。

步骤

- 1 选择**基础架构 > 端点 > 端点**。
- 2 选择**新建 > Cloud > Amazon EC2**。
- 3 输入名称和可选描述。

通常，此名称指示与此端点对应的 Amazon 帐户。

- 4 为 Amazon 端点输入管理级别的访问密钥 ID。

只有一个端点能够与 Amazon 访问密钥 ID 关联。

要获取创建 Amazon 端点所需的访问密钥，您必须向具有 AWS “完全访问管理员”凭据的用户请求密钥，或者另外配置 AWS “完全访问管理员”策略。有关详细信息，请参见 Amazon 文档。

- 5 为 Amazon 端点输入私有访问密钥。
- 6 (可选) 单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 7 (可选) 要增强安装性并迫使连接通过代理服务器，请单击**关联**，并关联到现有代理端点。

您必须至少有一个代理端点才能创建关联。

- 8 单击**确定**。

结果

创建端点后，vRealize Automation 开始从 Amazon Web Services 区域收集数据。

后续步骤

将端点中的计算资源添加到架构组。请参见 [创建架构组](#)。

添加 Amazon 实例类型

vRealize Automation 提供了多种实例类型与 Amazon 蓝图一起使用。管理员可以添加和移除实例类型。

创建或编辑 Amazon 蓝图时，蓝图架构师可以使用由 IaaS 管理员负责管理的计算机实例类型。Amazon 计算机映像和实例类型可通过 Amazon Web Services 产品获取。

前提条件

以 **IaaS 管理员** 身份登录到 vRealize Automation。

步骤

1 单击 **基础架构 > 管理 > 实例类型**。

2 单击 **新建**。

3 添加新实例类型，从而指定以下参数。

有关可用 Amazon 实例类型以及可为这些参数指定的设置值的信息，请参见“EC2 实例类型 - Amazon Web Services (AWS)”中的 Amazon Web Services 文档（位于 aws.amazon.com/ec2）和“实例类型”（位于 docs.aws.amazon.com）。

- 名称
- API 名称
- 类型名称
- IO 性能名称
- CPU
- 内存 (GB)
- 存储 (GB)
- 计算单元

4 单击 **保存** 图标 (👍)。

结果

当 IaaS 架构师创建 Amazon Web Services 蓝图时，可以使用自定义实例类型。

后续步骤

将端点中的计算资源添加到架构组。请参见 [创建架构组](#)。

创建代理端点并关联到云端点

您可以创建一个代理端点，并将其代理设置关联到 vCloud Air、vCloud Director 或 Amazon 端点。

如果您升级或迁移使用代理管理器的 vCloud Air、vCloud Director 或 Amazon 端点，则将创建新的 vCloud Air、vCloud Director 或 Amazon 端点，其中包含 vCloud Air、vCloud Director 或 Amazon 端点与新的代理端点之间的关联。

前提条件

- 以 **IaaS 管理员** 身份登录到 vRealize Automation。
- 创建一个以下类型的端点：
 - [创建 vCloud Air 端点](#)
 - [创建 Amazon 端点](#)
 - [创建 vCloud Director 端点](#)

您必须至少有一个 vCloud Air、vCloud Director 或 Amazon 端点才能从代理端点创建关联。

步骤

- 1 选择**基础架构 > 端点 > 端点**。
- 2 选择**新建 > 网络和安全 > 代理**。
- 3 在**名称**文本框中输入名称。
- 4 （可选）在**描述**文本框中输入描述。
- 5 在**地址**文本框中输入已安装代理程序的 URL。
- 6 在**端口**文本框中，输入连接代理服务器时要使用的端口号。
- 7 输入管理员级别用户名和密码。
- 8 （可选）单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 9 要将代理设置关联到 vCloud Air、vCloud Director 或 Amazon 端点，请单击**关联**，并选择一个或多个端点。

您必须至少有一个 vCloud Air、vCloud Director 或 Amazon 端点才能创建关联。

您可以将代理端点关联到多个端点。

- 10 单击**确定**。

结果

vRealize Automation 会从端点收集数据并发现计算资源。

后续步骤

将端点中的计算资源添加到架构组。请参见[创建架构组](#)。

为 OVF 主机网站创建代理端点

可以创建代理端点，以便在将 OVF 导入蓝图中的 vSphere 计算机组件时使用，或者 OVF 托管在网站上时用作映像组件配置文件的值集。

有关针对 OVF 部署进行配置的信息，请参见[创建 vSphere 端点](#)和[将蓝图配置为从 OVF 置备](#)。

前提条件

- 以 **laaS 管理员** 身份登录到 vRealize Automation。

步骤

- 1 选择**基础架构 > 端点 > 端点**。
- 2 选择**新建 > 网络和安全 > 代理**。
- 3 在**名称**文本框中输入名称。
- 4 （可选）在**描述**文本框中输入描述。
- 5 在**地址**文本框中，输入托管 OVF 的网站的 URL。
- 6 在**端口**文本框中，输入连接网站代理服务器时要使用的端口号。
- 7 输入管理员级别用户名和密码。
- 8 （可选）单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 9 单击**确定**。

结果

现在可以使用端点定义获取 OVF 的网站。有关详细信息，请参见[使用 OVF 定义 vSphere 组件的蓝图设置](#)和[通过使用 OVF 为组件配置文件定义映像值集](#)。

创建 vRealize Orchestrator 端点

您可以创建 vRealize Orchestrator 端点以连接到 vRealize Orchestrator 服务器。

您可以配置多个端点并让它们连接到不同的 vRealize Orchestrator 服务器，但必须配置每个端点的优先级。

执行 vRealize Orchestrator 工作流时，vRealize Automation 将先尝试使用优先级最高的 vRealize Orchestrator 端点。如果该端点不可访问，则继续尝试下一个优先级最高的端点，直到 vRealize Orchestrator 服务器可用于运行该工作流为止。

前提条件

- 以 **laaS 管理员** 身份登录到 vRealize Automation。

步骤

- 1 选择**基础架构 > 端点 > 端点**。
- 2 选择**新建 > Orchestration > vRealize Orchestrator**。
- 3 输入名称和可选描述。

- 4 输入包含 vRealize Orchestrator 服务器的完全限定名称或 IP 地址以及 vRealize Orchestrator 端口号的 URL。

传输协议必须是 HTTPS。如果未指定端口，则使用默认端口 443。

要使用 vRealize Automation 设备中嵌入的默认 vRealize Orchestrator 实例，请键入 **`https://vrealize-automation-appliance-hostname:443/vco`**。

- 5 在用户名和密码文本框中提供 vRealize Orchestrator 凭据以连接到 vRealize Orchestrator 端点。

使用的凭据应该对要从 IaaS 调用的所有 vRealize Orchestrator 工作流具有“执行”权限。

要使用 vRealize Automation 设备中嵌入的默认 vRealize Orchestrator 实例，用户名应使用 **`administrator@vsphere.local`**，且密码应使用配置 SSO 时指定的管理员密码。

- 6 在优先级文本框中输入大于或等于 1 的整数。

值越低表示优先级越高。

- 7 （可选）单击属性，并为端点添加提供的自定义属性、属性组或您自己的属性定义。

- 8 单击确定。

配置 vRealize Orchestrator 网络端点

如果使用 vRealize Automation 工作流调用 vRealize Orchestrator 工作流，则必须将 vRealize Orchestrator 实例或服务器配置为端点。

有关添加 vRealize Orchestrator 端点的信息，请参见 [创建 vRealize Orchestrator 端点](#)。

您可以将 vRealize Orchestrator 端点与计算机蓝图关联，确保通过该蓝图置备的计算机的所有 vRealize Orchestrator 工作流均在使用该端点运行。

默认情况下，vRealize Automation 包括嵌入式 vRealize Orchestrator 实例。在生产或测试环境中运行 vRealize Automation 工作流或创建概念证明时，建议您使用嵌入式实例作为 vRealize Orchestrator 端点。

还建议您使用此 vRealize Orchestrator 端点在生产环境中运行 vRealize Automation 工作流。

vRealize Orchestrator 插件随 vRealize Orchestrator 7.1 及更高版本自动安装。没有任何要单独安装的 vRealize Orchestrator 插件。

创建 vRealize Operations Manager 端点

您可以创建 vRealize Operations Manager 端点以连接到 vRealize Operations Manager 主机套件 API。

有关验证 vRealize Operations Manager 连接和证书信任的信息，请参见 [使用测试连接时的注意事项](#)。

前提条件

- 以 IaaS 管理员身份登录到 vRealize Automation。

步骤

- 1 选择基础架构 > 端点 > 端点。
- 2 选择新建 > 管理 > vRealize Operations Manager。

- 3 输入名称和可选描述。
- 4 在地址文本框中输入 vRealize Operations Manager 服务器的 URL。
该 URL 必须采用以下格式: **https://hostname/suite-api**。
- 5 输入您的 vRealize Operations Manager 用户名和密码凭据。
- 6 (可选) 单击**属性**, 并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 7 (可选) 单击**测试连接**来验证凭据、主机端点地址和证书信任。该操作还会检查 Manager Service 和代理是否正在运行, 以便使端点可以进行数据收集。**确定**操作也会测试这些条件。

测试连接操作会返回与下列任一情况有关的信息:

- 证书错误
如果证书找不到、不受信任或已过期, 系统将提示您接受证书指纹。如果不接受指纹, 则仍可保存端点, 但计算机置备可能会失败。
- 代理错误
找不到关联的 vSphere 代理。代理必须运行才能使测试成功。
- 主机错误
指定的端点地址无法访问或关联的 Manager Service 未运行。Manager Service 必须运行才能使测试成功。
- 凭据错误
指定的用户名和密码组合对于指定地址处的端点无效。
- 超时
在允许的两分钟时间内无法完成测试操作。
如果**测试连接**操作失败, 则仍可保存端点, 但计算机置备可能会失败。
如果有可信证书问题, 例如证书已过期, 系统将提示您接受证书指纹。

8 单击**确定**。

创建第三方 IPAM 提供程序端点

如果在 vRealize Orchestrator 中注册和配置了第三方 IPAM 端点类型, 您可以在 vRealize Automation 中创建该 IPAM 解决方案提供程序的端点。

如果导入了用于提供外部 IPAM 解决方案的 vRealize Orchestrator 软件包并在 vRealize Orchestrator 中注册 IPAM 端点类型, 您可以在创建 vRealize Automation 端点时选择该 IPAM 端点类型。

注 本例假定您使用 Infoblox IPAM 插件, 可以在 VMware Solution Exchange 下载该插件。如果您使用 VMware 提供的 IPAM 解决方案 SDK 创建了自己的 IPAM 提供程序软件包, 也可以使用此过程。导入和配置自己的第三方 IPAM 解决方案软件包的过程与必备条件中所述的相同。

在 vRealize Orchestrator 中注册 IPAM 解决方案提供程序插件的端点类型时, 将创建 vRealize Automation 的第一个 IPAM 端点。

前提条件

- 获取第三方 IPAM 提供程序软件包并导入 vRealize Orchestrator 中。
- 运行工作流以在 vRealize Orchestrator 中注册第三方 IPAM 端点类型。
- 以 **IaaS 管理员** 身份登录到 vRealize Automation。

在本例中，使用在第三方 IPAM 提供程序插件或软件包的 vRealize Orchestrator 中注册的端点类型创建 Infoblox IPAM 端点。

步骤

- 1 选择**基础架构 > 端点 > 端点**。

- 2 选择**新建 > IPAM > IPAM 端点类型**。

选择注册的外部 IPAM 提供程序端点类型，如 Infoblox。外部 IPAM 提供程序端点仅在已导入第三方 vRealize Orchestrator 软件包且运行软件包工作流注册端点类型后可用。

对于 Infoblox IPAM，只会列出主 IPAM 端点类型。使用自定义属性可指定辅助 IPAM 端点类型。

在本例中，选择注册的外部 IPAM 端点类型，如 **Infoblox NIOS**。

- 3 输入名称和可选描述。

- 4 使用特定于提供程序的 URL 格式（例如 `https://host_name/name`）在**地址**文本框中输入已注册 IPAM 端点的位置。

例如，在 vRealize Orchestrator 中注册 IPAM 端点类型时，可以创建几个 IPAM 端点，如 `https://nsx62-scale-infoblox` 和 `https://nsx62-scale-infoblox2`。输入主要注册的端点类型。如果还需要指定一个或多个辅助 IPAM 端点，可以使用自定义属性模拟特定于 IPAM 解决方案提供程序的可扩展属性。

- 5 输入访问 IPAM 解决方案提供程序帐户所需的用户名和密码。

在 vRealize Automation 中工作时需要使用 IPAM 解决方案提供程序帐户凭据来创建、配置和编辑端点。vRealize Automation 使用 IPAM 端点凭据与指定端点类型（例如 Infoblox）通信，以分配 IP 地址并执行其他操作。此行为与 vRealize Automation 使用 vSphere 端点凭据的方式相似。

- 6 （可选）单击**属性**，并添加对特定 IPAM 解决方案提供程序有意义的端点属性。

每个 IPAM 解决方案提供程序（例如 Infoblox 和 Bluecat）使用唯一的可扩展属性，您可以使用 vRealize Automation 自定义属性模拟这些属性。例如，Infoblox 使用可扩展属性区分主端点和辅助端点。

- 7 单击**确定**。

后续步骤

将端点中的计算资源添加到架构组。请参见 [创建架构组](#)。

创建 Microsoft Azure 端点

您可以创建 Microsoft Azure 端点，促进 vRealize Automation 与 Azure 部署之间的凭据式连接。通过使用提供的

端点与资源建立连接，可用于创建虚拟机蓝图，本例中的资源为 Azure 实例。必须使用 Azure 端点作为置备 Azure 虚拟机的蓝图基础。如果使用多个 Azure 订阅，则需要为每个订阅 ID 创建端点。

或者，您可以使用“添加 Azure 连接”命令（位于 vRealize Orchestrator 工作流树中的 **库 > Azure > 配置**下）直接从 vRealize Orchestrator 创建 Azure 连接。对于大多数情况，通过端点配置创建连接（如本文中所述）是首选选项。

vRealize Orchestrator 和 XaaS 功能支持 Azure 端点。您可以创建、删除或编辑 Azure 端点。如果更改现有端点后几个小时内不通过更新的连接在 Azure 门户上运行任何更新，可能会出现错误。您必须使用 `service vco-service restart` 命令重新启动 vRealize Orchestrator 服务。重新启动该服务失败可能会导致出现错误。

前提条件

- 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。有关配置 Azure 和获取订阅 ID 的详细信息，请参见 [Microsoft Azure 端点配置](#)。
- 确认您的 vRealize Automation 部署至少具有一个租户和一个业务组。
- 按照 <https://azure.microsoft.com/zh-cn/documentation/articles/resource-group-create-service-principal-portal> 中所述创建 Active Directory 应用程序。
- 请记录以下 Azure 相关信息，因为在配置端点和蓝图时将需要这些信息。
 - 订阅 ID
 - 租户 ID
 - 存储帐户名称
 - 资源组名称
 - 位置
 - 虚拟网络名称
 - 客户端应用程序 ID
 - 客户端应用程序密钥
 - 虚拟机映像 URN
- vRealize Automation Azure 实施支持 Microsoft Azure 支持的区域的子集。请参见 [Azure 支持的区域](#)。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > vRO 配置 > 端点**。
- 2 单击**新建**图标 (+)。

- 3 在“插件”选项卡上，单击**插件**下拉菜单并选择 **Azure**。
- 4 单击**下一步**。
- 5 输入名称和可选描述。
- 6 单击**下一步**。
- 7 根据需要为端点填充“详细信息”选项卡上的文本框。

参数	描述
连接设置	
连接名称	新端点连接的唯一名称。此名称显示在 vRealize Orchestrator 界面中，以帮助标识特定连接。
Azure 订阅 ID	Azure 订阅的标识符。该 ID 定义您具有访问权限的存储帐户、虚拟机和其他 Azure 资源。
Azure 环境	部署的 Azure 资源的地理区域。vRealize Automation 基于订阅 ID 支持当前的所有 Azure 区域。
资源管理器设置	
Azure 服务 URI	用于获取 Azure 实例访问权限的 URI。 https://management.azure.com/ 的默认值适用于许多典型实施。当您选择环境时，会自动填充此框。
租户 ID	希望端点使用的 Azure 租户 ID。
客户端 ID	希望端点使用的 Azure 客户端标识符。此参数在创建 Active Directory 应用程序时进行分配。
客户端密码	与 Azure 客户端 ID 一起使用的密钥。此密钥在创建 Active Directory 应用程序时进行分配。
Azure 存储 URI	用于访问 Azure 存储实例的 URI。当您选择环境时，会自动填充此框。
代理设置	
代理主机	如果贵公司使用代理 Web 服务器，请输入该服务器的主机名。
代理端口	如果贵公司使用代理 Web 服务器，请输入该服务器的端口号。

- 8 （可选）单击“属性”，然后添加提供的自定义属性、属性组或您自己的自定义属性定义。
- 9 单击**完成**。

后续步骤

在 Azure 中创建合适的资源组、存储帐户以及网络安全组。您还应创建负载均衡器（如果适合您的实施）。

操作	选项
创建 Azure 资源组	<ul style="list-style-type: none"> ■ 使用 Azure 门户创建资源组。请参见 Azure 文档了解具体说明。 ■ 使用 Library/Azure/Resource/Create resource group 下的相应 vRealize Orchestrator 工作流。 ■ 在 vRealize Automation 中，创建并发布包含 vRealize Orchestrator 工作流的 XaaS 蓝图。将资源组附加到服务和授权后，可以请求资源组。 <p>注 资源组资源类型不受 vRealize Automation 支持或管理。</p>
创建 Azure 存储帐户	<ul style="list-style-type: none"> ■ 使用 Azure 创建存储帐户。请参见 Azure 文档了解具体说明。 ■ 使用 Library/Azure/Storage/Create storage account 下的相应 vRealize Orchestrator 工作流。 ■ 在 vRealize Automation 中，创建并发布包含 vRealize Orchestrator 工作流的 XaaS 蓝图。将存储帐户附加到服务和授权后，可以请求存储帐户。
创建 Azure 网络安全组	<ul style="list-style-type: none"> ■ 使用 Azure 创建安全组。请参见 Azure 文档了解具体说明。 ■ 使用 Library/Azure/Network/Create Network security group 下的相应 vRealize Orchestrator 工作流。 ■ 在 vRealize Automation 中，创建并发布包含 vRealize Orchestrator 工作流的 XaaS 蓝图。将安全组附加到服务和授权后，可以请求安全组。

Microsoft Azure 端点配置

您必须收集一些信息并执行一些配置，才能在 vRealize Automation 中创建 Microsoft Azure 端点。

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 - 在 Azure 门户中单击“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，找到边栏上的“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，则必须选择“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，则 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 vRealize Automation 可以进行身份验证。

- a 在 Azure 左侧菜单上找到 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 为您的应用程序键入符合 Azure 名称验证的名称。
- 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 vRealize Automation 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 应用程序连接到您的 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 和一个可供您进行身份验证的短代码。
- 2 在浏览器中，输入从您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。

创建 Puppet 端点

您可以创建 Puppet 端点，支持将 Puppet 配置管理组件添加到 vSphere 虚拟机。通过这些组件，可以使用 Puppet Master 在虚拟机上强制执行配置管理。

端点可连接至外部资源，本例中为 Puppet Master 实例。通过该端点，可以将 Puppet 配置管理组件放置在 vSphere 虚拟机蓝图中。基于这些蓝图置备的虚拟机包含一个 Puppet 代理，可促进关联的 Puppet Master 进一步加强控制。

有关 Puppet 插件及其配置演示的详细信息，请参见 <https://www.youtube.com/watch?v=P-VglzE9o-O>。

前提条件

- 根据环境安装和配置 Puppet Enterprise。
- 在 vRealize Orchestrator 部署上下载并安装 Puppet 插件版本 3.0。可以从 <https://marketplace.vmware.com/vsx/solutions/puppet-plugin-for-vrealize-automation?ref=search> 下载此插件。有关安装和使用此插件的信息，请参见 https://docs.puppet.com/pe/latest/vro_intro.html。

步骤

- 1 选择**管理 > vRO 配置 > 端点**。
- 2 单击**新建**图标 (+)。
- 3 在“插件”选项卡上，单击**插件**下拉菜单并选择 **Puppet 插件**。
- 4 单击**下一步**。
- 5 输入名称和可选描述。
- 6 单击**下一步**。
- 7 根据需要为端点填充**详细信息**选项卡上的文本框。

参数	描述
显示此 Puppet Master 的名称	与端点连接关联的 Puppet Master 的名称。此名称显示在 vRealize Orchestrator 界面中，以帮助标识特定连接。
主机名或 IP 地址	此端点使用的 Puppet Master 的 FQDN 或 IP 地址。
SSH 端口	为此 Puppet Master 定义的安全通信端口。
SSH RBAC 和用户名	与 Puppet Master 连接所需的基于角色的访问控制用户名。
SSH 和 RBAC 密码	使用 Puppet Master 进行安全配置所需的基于角色的访问控制用户名。
在此主机上是否使用 sudo 作为 shell 命令？	如果希望管理员能够在 Linux 服务器上使用 Sudo 命令作为基于此端点的虚拟机上的安全选项，则选择此选项。

- 8 单击**确定**。

结果

现在，可以将 Puppet 配置管理组件添加到 vSphere 蓝图，以便能够部署包含 Puppet 代理的 vSphere 虚拟机。

创建 Ansible 端点

您可以创建 Ansible 端点，支持将 Ansible 配置管理组件添加到 vSphere 虚拟机。通过这些组件，可以使用 Ansible Tower 在虚拟机上强制执行配置管理。

前提条件

- 安装和配置适用于您环境的 Ansible Tower。
- 下载 Ansible 插件并安装在您的 vRealize Orchestrator 部署上。该插件可从 <https://marketplace.vmware.com/vsx/solutions/sovlabs-ansible-tower-plugin-for-vra-cm-framework-1?ref=search> 获得。

步骤

- 1 选择**管理 > vRO 配置 > 端点**。
- 2 单击**新建**图标。
- 3 在“插件”选项卡上，单击**插件**下拉菜单并选择“Ansible 插件”。
- 4 单击**下一步**。
- 5 在“端点”选项卡上输入名称和说明（可选）。
- 6 单击**下一步**。
- 7 根据需要为端点填充“详细信息”选项卡上的文本框。

详细信息标签页	描述
Ansible Tower 端点配置	添加端点配置信息。 <ul style="list-style-type: none"> ■ Ansible Tower 端点配置：在相应的文本框中输入名称和 IP 地址或主机名。 ■ Ansible Tower 凭据配置：输入与此端点相关联的 Ansible Tower 设备的登录凭据。 ■ 导入 SSL 证书：选择是否希望 vRealize Orchestrator 以静默方式接受 Ansible Tower 证书。
Ansible Tower 主机访问权限	如果适用，请输入 Ansible Tower 计算机的 SSH 凭据，以便部署的计算机可以连接到它以便配置自定义动态清单脚本。
组织和清单设置	配置您的组织名称和清单。添加动态清单配置值。
筛选器和组	配置键值对属性筛选器和 Ansible 动态组。
启动时提示覆盖（可选）	配置 Ansible 作业选项以及计算机、模板和清单选项。
vRA 属性转换	如果适用，请在置备后处理自定义属性期间输入所需的替换字符串以供 Ansible 使用。

- 8 单击**完成**。

创建 Hyper-V (SCVMM) 端点

您可以创建端点，以便允许 vRealize Automation 与 SCVMM 环境通信并发现计算资源、收集数据和置备计算机。

前提条件

- 以 **laaS 管理员**身份登录到 vRealize Automation。

- 必须安装和配置 DEM 代理来管理 Hyper-V (SCVMM) 端点。有关信息，请参见安装 vRealize Automation 中的 SCVMM 要求信息。

有关相关信息，请参见[准备 SCVMM 环境](#)。

步骤

- 1 选择**基础架构 > 端点 > 端点**。
- 2 选择**新建 > 虚拟 > Hyper-V (SCVMM)**。
- 3 在**名称**文本框中输入名称。
- 4 （可选）在**描述**文本框中输入描述。
- 5 在**地址**文本框中输入端点的 URL。
该 URL 的类型必须为：*FQDN* 或 *IP_address*。
例如：`mycompany-scvmm1.mycompany.local`。
- 6 输入为此端点存储的管理级别用户名和密码。
如果尚未存储这些凭据，则可立即执行此操作。
- 7 （可选）单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
- 8 单击**确定**。

结果

vRealize Automation 会从端点收集数据并发现计算资源。

后续步骤

将端点中的计算资源添加到架构组。请参见[创建架构组](#)。

创建 OpenStack 端点

可以通过创建端点来允许 vRealize Automation 与 OpenStack 实例进行通信。

前提条件

- 以 **IaaS 管理员** 身份登录到 vRealize Automation。
- 确认满足 Openstack 或 PowerVC 要求的计算机上已安装 vRealize Automation DEM。请参见安装 vRealize Automation。
- 确认您的 OpenStack 功能当前受支持。请参见《vRealize Automation 支持列表》。

从之前的 vRealize Automation 安装升级或迁移后，如果对 OpenStack 端点的数据收集失败，则可以向每个 Keystone V3 OpenStack 端点添加 `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` 自定义属性，以便指定有效的域名并启用数据收集。

步骤

- 1 选择**基础架构 > 端点 > 端点**。

- 2 选择**新建 > Cloud > OpenStack**。
- 3 输入名称和可选描述。
- 4 在**地址**文本框中输入端点的 URL。

选项	描述
PowerVC	URL 必须为 http://myPowerVC.com:5000 或 http://FQDN:5000 格式。
Openstack	URL 的格式必须为 FQDN:5000 或 IP_address:5000 。请勿在端点地址中包含 /v2.0 后缀。

- 5 输入您的管理级别用户名和密码。
您提供的凭据必须在与端点关联的 OpenStack 租户中具有管理员角色。
- 6 在 **OpenStack 项目** 文本框中，输入 OpenStack 租户名称。
如果设置多个具有不同 OpenStack 租户的端点，请为每个租户创建预留策略。这可确保将计算机置备到合适的租户资源。
- 7 单击**属性**，并为端点添加提供的自定义属性、属性组或您自己的属性定义。
如果 Keystone V3 有效，请添加 **VMware.Endpoint.Openstack.IdentityProvider.Domain.Name** 自定义属性以指定特定域。
- 8 单击**确定**。

结果

vRealize Automation 会从端点收集数据并发现计算资源。

后续步骤

将端点中的计算资源添加到架构组。请参见 [创建架构组](#)。

创建 Hyper-V、XenServer 或 Xen 池端点

您可以创建端点，以便允许 vRealize Automation 与 Hyper-V、XenServer 或 Xen 池主环境通信并发现计算资源、收集数据和置备计算机。

前提条件

- 以 **IaaS 管理员** 身份登录到 vRealize Automation。
- 系统管理员必须安装已存储的凭据与您端点对应的代理程序。请参见 [安装 vRealize Automation](#)。

步骤

- 1 选择**基础架构 > 端点 > 代理**。
- 2 在**计算资源**文本框中，输入 Hyper-V 服务器、Xen 服务器或 Xen 主池的完全限定 DNS 名称。

注 对于 Xen 池端点，您必须输入主池的名称。要避免 vRealize Automation 计算资源表中出现重复条目，请指定与配置的 Xen 池主地址匹配的地址。例如，如果 Xen 池主地址使用主机名，请输入主机名而非 FQDN。如果 Xen 池主地址使用 FQDN，请输入 FQDN。

- 3 从**代理程序名称**下拉菜单中，选择系统管理员为此端点安装的代理程序。
- 4 （可选）在**描述**文本框中输入描述。
- 5 单击**确定**。

结果

vRealize Automation 会从端点收集数据并发现计算资源。

后续步骤

将端点中的计算资源添加到架构组。请参见[创建架构组](#)。

使用测试连接时的注意事项

可以使用测试连接操作来验证 vSphere、NSX for vSphere、NSX-T 和 vRealize Operations Manager 端点的凭证、主机端点地址和证书。

该操作还会检查 Manager Service 和代理是否正在运行，以便使该端点可以进行数据收集。

测试连接操作会返回与下列任一情况有关的信息：

- 证书错误

如果证书找不到、不受信任或已过期，系统将提示您接受证书指纹。如果不接受指纹，则仍可保存端点，但计算机置备可能会失败。
- 代理错误

找不到关联的 vSphere 代理。代理必须运行才能使测试成功。
- 主机错误

指定的端点地址无法访问或关联的 Manager Service 未运行。Manager Service 必须运行才能使测试成功。
- 凭据错误

指定的用户名和密码组合对于指定地址处的端点无效。
- 超时

在允许的两分钟时间内无法完成测试操作。

如果在已升级或迁移的端点上运行**测试连接**时收到错误消息，请参见[使用已升级或已迁移端点的注意事项](#)，了解建立证书信任所需的步骤。

以编程方式导入或导出端点

要在 vRealize Automation 7.3 或更高版本中通过编程方式导入和导出端点，必须使用新的 vRealize Automation endpoint-configuration-service REST API 或使用 vRealize CloudClient。

vRealize CloudClient 文档包含所有适用的命令行格式、示例和用法信息。

可以从 <https://developercenter.vmware.com/tool/cloudclient> 的 vRealize CloudClient 产品页面下载 vRealize CloudClient 应用程序和文档。

查看端点源以及运行数据收集

您可以查看与特定端点相关联的计算机和计算资源。您也可以手动启动数据收集。

前提条件

- 以 **IaaS 管理员** 身份登录到 vRealize Automation。
- 验证至少存在一个端点。

步骤

- 1 选择 **基础架构 > 端点 > 端点**。
- 2 选择现有的端点行，然后单击 **操作**。

选择以下可用操作之一。

- 单击 **查看计算资源**，打开 **基础架构 > 计算资源** 页面。此页面可用于查看和编辑计算资源设置。
- 单击 **查看计算机**，打开 **基础架构 > 受管计算机** 页面。
- 单击 **数据收集**，打开数据收集页面并启动端点数据收集。您可以刷新页面以显示请求的当前状态。

使用已升级或已迁移端点的注意事项

从 vRealize Automation 7.3 之前的版本升级或迁移后，请务必了解并遵循以下注意事项。

此信息适用于升级或迁移到此 vRealize Automation 版本的端点。

- 从 vRealize Automation 7.3 之前的版本升级或迁移时，包含代理设置的每个 vCloud Air、vCloud Director 和 Amazon 端点均与包含其代理设置的新代理端点相关联。
 升级或迁移之后，新的代理端点名称是 Proxy_YYYYYY，其中 YYYYYY 是代理的 URL、端口和凭据的哈希值。如果您为不同端点（例如，vCloud Air 或 Amazon 端点）使用相同的代理设置（例如相同的 URL、端口和凭据），那么升级或迁移之后，将只有一个代理端点，而且会在 vCloud Air 和 Amazon 端点与新的代理端点之间建立关联。代理端点可关联到多个 Amazon、vCloud Air 或 vCloud Director 端点。
- 升级或迁移包含 NSX Manager 设置的 vSphere 端点时，每个 vSphere 端点将关联到包含其 NSX Manager 设置的新 NSX 端点。
 升级或迁移之后，NSX 端点名称是 NSX_XXXXXX，其中 XXXXXX 是 vRealize Automation 7.3 之前版本中的父 vSphere 端点的名称。
- vRealize Automation 升级或迁移完成之后，基础架构管理员可以更改新 NSX 和代理端点的名称。
- 已升级或迁移的端点的默认安全设置不接受不可信证书。

- 从之前的 vRealize Automation 安装升级或迁移之后，如果使用的是不可信证书，则必须为所有 vSphere 和 NSX 端点执行以下步骤，以启用证书验证。否则，端点操作将会失败并显示证书错误。有关详细信息，请参见 VMware 知识库文章《端点通信在升级到 vRA 7.3 后中断 (2150230)》（网址为 <http://kb.vmware.com/kb/2150230>）和《如何下载和安装 vCenter Server root 证书以避免出现 Web 浏览器证书警告 (2108294)》（网址为 <http://kb.vmware.com/kb/2108294>）。
 - a 升级或迁移之后，通过使用**服务**选项卡登录到 vRealize Automation vSphere 代理计算机并重新启动 vSphere 代理。
迁移可能不会重新启动所有代理，因此，请根据需要手动重新启动它们。
 - b 等待至少完成一个 ping 报告。ping 报告完成需要一到两分钟。
 - c 当 vSphere 代理已启动数据收集，请以 IaaS 管理员身份登录到 vRealize Automation。
 - d 单击**基础架构 > 端点 > 端点**。
 - e 编辑 vSphere 端点并单击**测试连接**。
 - f 如果显示证书提示，请单击**确定**以接受证书。
如果没有显示证书提示，则证书当前可能已正确存储在托管端点服务（例如，作为代理程序计算机或 DEM 计算机）的 Windows 计算机的可信根颁发机构中。
 - g 单击**确定**以接受证书并保存端点。
 - h 为每个 vSphere 端点重复此过程。
 - i 为每个 NSX 端点重复此过程。
 - j 导航到**基础架构 > 计算资源**，右键单击 **vCenter 计算资源**，然后运行**数据收集**。

如果**测试连接**操作成功，但某些数据收集或置备操作失败，则可以在为端点服务的所有代理计算机和所有 DEM 计算机上安装相同的证书。或者，您可以从现有计算机中卸载证书，并为失败的端点重复上述过程。

- vRealize Automation REST API 在 vRealize Automation 7.2 及早期版本中用来以编程方式创建、编辑和删除端点，它在 vRealize Automation 7.3 及更高版本中不再受支持。要在 vRealize Automation 7.3 或更高版本中以编程方式创建、编辑和删除端点，必须使用新的 vRealize Automation endpoint-configuration-service REST API 或使用 vRealize CloudClient。
- 从之前的 vRealize Automation 安装升级或迁移后，如果对 OpenStack 端点的数据收集失败，则可以向每个 Keystone V3 OpenStack 端点添加 `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` 自定义属性，以便指定有效的域名并启用数据收集。
- 升级第三方 IPAM 端点时，如 Infoblox IPAM，包含 `RegisterIPAMEndpoint` 工作流的 vRealize Orchestrator 软件包将升级。vRealize Automation 升级完成后，您可能需要重新运行 vRealize Orchestrator 中的工作流。
- 要更改多个端点的凭据，您可以分别编辑每个端点，也可以使用 vRealize CloudClient 执行批量更新。

- 某些端点类型（例如 vCloud Air 和 vCloud Director）无法直接从 vRealize Automation 6.2.x 升级或迁移到 vRealize Automation 7.3 或更高版本。
- 成功升级或迁移到 vRealize Automation 7.3 后，如果[基础架构 > 端点](#)页面不显示任何端点或仅显示某些端点类型和端点，请参见[知识库文章 2150252](#)，了解建议的解决办法。

删除端点时的注意事项

在某些情况下，可以删除某些端点类型。

- 可以删除尚未收集数据的端点。
- 对于 OpenStack、Amazon 和 VRO 端点，如果已收集数据但没有预留，则可以删除。对于其他端点类型，如果已收集数据，则无法删除。
- 如果第三方 IPAM 端点没有关联到某个网络配置文件，则可以删除该端点。
- 删除 vSphere 端点时，确认提示将列出以下依赖关系：
 - 已从该端点收集数据。
 - 该端点由映射到某个计算资源的预留所引用。无法删除预留中引用的端点。预留需要计算资源。
 - 该端点包含现有蓝图所引用的模板。
删除该端点时，不会删除该蓝图。
 - 该端点由当前使用的虚拟机使用。
- 可以使用 vRealize Automation 7.3 中引入新的 CREATE、EDIT 和 DELETE vRealize Automation endpoint-configuration-service REST API 或通过 vRealize CloudClient，以编程方式删除端点。无法使用 vRealize Automation 7.3 之前的 endpoint-configuration-service REST API 删除端点。

对找不到连接的 vSphere 端点进行故障排除

vSphere 端点的数据收集失败可能是由于代理名称与端点名称不匹配导致的。

问题

vSphere 端点的数据收集失败。日志消息返回类似以下内容的错误：

```
已捕获此异常：找不到连接的端点“vCenter” (This exception was caught: The attached endpoint 'vCenter' cannot be found)。
```

原因

在 vRealize Automation 中配置的端点名称必须与安装期间提供给 vSphere 代理程序的端点名称匹配。如果端点名称与代理程序名称不匹配，则 vSphere 端点的数据收集会失败。除非配置名称匹配的端点，否则日志消息将返回类似以下内容的错误：

```
已捕获此异常：找不到连接的端点“预期的端点名称” (This exception was caught: The attached endpoint 'expected endpoint name' cannot be found)。
```

解决方案

- 1 选择**基础架构 > 监控 > 日志**。
- 2 查找“找不到连接的端点 (Attached Endpoint Cannot be Found)”错误消息。

例如，

```
已捕获此异常：找不到连接的端点“预期的端点名称”(This exception was caught: The attached endpoint 'expected endpoint name' cannot be found)。
```

- 3 编辑 vSphere 端点，使其与日志消息中显示的预期端点名称匹配。
 - a 选择**基础架构 > 端点 > 端点**。
 - b 单击要编辑的端点的名称。
 - c 在**名称**文本框中输入预期的端点名称。
 - d 单击**确定**。

解决方案

代理程序可以与该端点通信，且数据收集成功完成。

创建架构组

您可以将基础架构资源组织成架构组，并分配一个或多个架构管理员来管理架构组中的资源。

虚拟和云端点需要架构组。您可以添加多个用户（每次添加一个），或者选择身份存储组或自定义组作为架构管理员，以便把架构管理员角色授予多个用户。

前提条件

- 以 **IaaS 管理员** 身份登录到 vRealize Automation。
- 创建至少一个端点。请参见[选择端点场景](#)。

步骤

- 1 选择**基础架构 > 端点 > 架构组**。
- 2 单击**新建**图标 (+)。
- 3 在**名称**文本框中输入名称。
- 4 （可选）在**描述**文本框中输入描述。
- 5 在**架构管理员**文本框中输入用户名或用户电子邮件地址，单击搜索图标，然后选择提供的用户电子邮件地址。
重复此步骤添加多个用户。
- 6 选择一个或多个**计算资源**，将其纳入架构组中。

数据收集期间只会发现为架构组选择的群集内存在的资源。例如，只有所选群集内存在的模板才会被发现且可用于在为业务组创建的预留上克隆。

7 单击**确定**。

结果

架构管理员现在可以配置计算机前缀。请参见[配置计算机前缀](#)。

当前登录到 vRealize Automation 的用户必须先从 vRealize Automation 注销后再重新登录，然后才能导航至有权访问的页面。

配置计算机前缀

您可以创建计算机前缀，用于为通过 vRealize Automation 置备的计算机创建名称。在蓝图设计画布中定义计算机组件时需要计算机前缀。

前缀是一个基本名称，后跟指定位数的计数值。所有的位数都使用时，vRealize Automation 回滚至首位数。

计算机前缀必须遵守以下限制：

- 只包含不分大小写的 ASCII 字母 a 到 z、数字 0 到 9 以及连字符 (-)。
- 不能以连字符开头。
- 不能使用其他符号、标点字符或空格。
- 包括数字在内不能超过 15 个字符，以遵守 Windows 主机名称的 15 个字符限制。
超长主机名会在置备计算机时截断，并在下次运行数据收集时更新。不过，WIM 置备名称不会截断，但指定名称超过 15 个字符时置备会失败。
- vRealize Automation 不支持在一个实例中使用多个具有相同名称的虚拟机。如果您选择的命名约定会造成计算机名称重叠，那么 vRealize Automation 不会置备具有重复名称的计算机。如有可能，vRealize Automation 会跳过已在使用的名称，并且使用指定的计算机前缀生成新的计算机名称。如果不能生成唯一名称，则置备会失败。

前提条件

以**架构管理员**身份登录到 vRealize Automation。

步骤

- 1 单击**基础架构 > 管理 > 计算机前缀**。
- 2 单击**新建**图标 (+)。
- 3 在**名称**文本框中输入计算机前缀。
- 4 在**可见性**列中指定是在所有租户中显示计算机前缀还是仅在当前租户中显示。
- 5 在**数字位数**文本框中输入计算机前缀位数。
- 6 在下一个**数字**文本框中输入计数器开始数字。
- 7 单击**保存**图标 (✓)。

结果

租户管理员可以创建业务组，这样用户便可访问 vRealize Automation 来请求计算机。

创建网络配置文件

包含网关、子网和地址范围等 IP 信息的网络配置文件。vRealize Automation 使用 vSphere DHCP 或指定的 IPAM 提供程序为其置备的计算机分配 IP 地址。

您可以创建网络配置文件来定义可用的网络类型，包括外部网络配置文件以及适用于按需网络地址转换 (Network Address Translation, NAT) 和路由网络配置文件的模板，这些模板将为新网络路径构建 NSX 逻辑交换机和相应的路由设置。将网络组件添加到蓝图时需要网络配置文件。

网络置备文件用于在置备计算机时配置网络设置。网络配置文件还会指定置备计算机时创建的 NSX Edge 设备的配置。创建预留和蓝图时，您可以确定网络配置文件。在预留中，您可以将网络配置文件分配给网络路径，并为蓝图中的计算机组件指定其中任一路径。

蓝图创建者在蓝图中定义网络组件时会指定相应的网络配置文件。在定义置备计算机的网络适配器和负载均衡器时，可以使用现有网络配置文件和按需 NAT 或路由网络配置文件。

网络配置文件还支持第三方 IP 地址管理 (IP Address Management, IPAM) 提供程序，如 Infoblox。配置 IPAM 的网络配置文件时，您的置备计算机可以从配置的 IPAM 解决方案中获取其 IP 地址数据和相关信息，如 DNS 和网关。您可以为 Infoblox 等第三方提供程序使用外部 IPAM 软件包，以便定义与网络配置文件一起使用的 IPAM 端点。

注 如果使用的是第三方 IPAM 提供程序，且需要指定要在其上部署计算机的网络，请为每个 VLAN 使用单独的网络配置文件以避免[知识库文章 2148656](#)中所述的已知问题。

如果您不使用第三方 IPAM 提供程序，而是使用 vRealize Automation 提供的 IPAM 端点，则可指定网络配置文件可以使用的 IP 地址范围。分配给计算机的指定范围内的每个 IP 地址均可回收，以便在销毁计算机时重新分配。您可以创建网络配置文件，用于定义可分配给计算机的静态 IP 地址范围。通过克隆或使用 kickstart/autoYaST 置备方法置备虚拟机时，请求计算机的所有者可以分配预定范围内的静态 IP 地址。

您可以将网络配置文件分配给预留上的特定网络路径。对于某些计算机组件类型，如 vSphere，您可以在创建或编辑蓝图时分配网络配置文件。

注 尽管您无法更改已部署虚拟机的网络配置文件，但您可以更改虚拟机所连接的网络。如果网络关联到不同的网络配置文件，vRealize Automation 会将该网络配置文件中的 IP 地址分配给虚拟机。但是，在您更新客户机操作系统上的 IP 地址之前，虚拟机会继续使用旧 IP 地址。或者，您也可以在部署的虚拟机上使用重新配置操作，这也需要更新客户机操作系统上的 IP 地址。

如果在预留和蓝图中指定网络配置文件，则优先使用蓝图值。例如，如果利用 `VirtualMachine.NetworkN.ProfileName` 自定义属性在蓝图中和蓝图所用的预留中指定网络配置文件，则优先使用在蓝图中指定的网络配置文件。但是，如果该自定义属性不用于蓝图且您为计算机网卡选择网络配置文件，则 vRealize Automation 将对已指定网络配置文件的计算机网卡使用预留网络路径。

有关这些网络类型的详细信息，请参见 NSX 信息中心内的《NSX 管理指南》，网址为 https://www.vmware.com/support/pubs/nsx_pubs.html。

表 2-14. vRealize Automation 网络配置文件的可用网络类型

网络类型	描述
外部	<p>在 vSphere Server 上配置的现有网络。它们是 NAT 和路由网络类型外部的一部分。外部网络配置文件可以定义外部网络上可用的静态 IP 地址范围。</p> <p>您可以使用从提供的 VMware IPAM 端点或已在 vRealize Orchestrator 中注册和配置的第三方 IPAM 服务提供程序端点（如 Infoblox IPAM）获取的 IP 范围。IP 范围是在分配期间从 IP 块创建的。</p> <p>包含静态 IP 范围的外部网络配置文件是 NAT 和路由网络的必备项。</p> <p>请参见为现有网络创建外部网络配置文件。</p>
NAT	<p>在置备期间创建的按需网络。NAT 网络使用一组 IP 地址进行外部通信，使用另一组 IP 地址进行内部通信。</p> <p>在一对一 NAT 网络中，每个虚拟机都会分配一个来自外部网络配置文件的外部 IP 地址，以及一个来自 NAT 网络配置文件的内部 IP 地址。在一对多 NAT 网络中，所有计算机均共享一个来自外部网络配置文件的 IP 地址进行外部通信。</p> <p>您可以使用从提供的 VMware IPAM 端点或已在 vRealize Orchestrator 中注册和配置的第三方 IPAM 服务提供程序端点（如 Infoblox IPAM）获取的 IP 范围。IP 范围是在分配期间从 IP 块创建的。</p> <p>NAT 网络配置文件定义使用转换表进行双向通信的本地和外部网络。</p> <p>请参见为按需网络创建 NAT 网络配置文件。</p>
已路由	<p>在置备期间创建的按需网络。路由网络包含一块可路由 IP 空间，该空间被划分为使用分布式逻辑路由器 (Distributed Logical Router, DLR) 链接在一起的多个子网。</p> <p>每个新路由网络均分配有下一可用的子网，并与使用同一网络配置文件的其他路由网络关联。凡通过使用同一路由网络配置文件的路由网络置备的虚拟机既可相互通信，也可与外部网络通信。</p> <p>您可以使用从提供的 VMware IPAM 端点或已在 vRealize Orchestrator 中注册和配置的第三方 IPAM 服务提供程序端点（如 Infoblox IPAM）获取的 IP 范围。IP 范围是在分配期间从 IP 块创建的。</p> <p>路由网络配置文件定义可路由空间和可用子网。</p> <p>请参见为按需网络创建路由网络配置文件。</p>

使用网络配置文件控制 IP 地址范围

您可以使用网络配置文件将预定义范围内的静态 IP 地址分配给通过克隆或使用 Linux kickstart 或 autoYaST 置备的虚拟机，或者分配给在 OpenStack 中通过使用 kickstart 置备的云计算机。

默认情况下，vRealize Automation 使用动态主机配置协议 (DHCP) 将 IP 地址分配给已置备的计算机。

您可以创建网络配置文件，用于定义可分配给计算机的静态 IP 地址范围。您可以将网络配置文件分配给预留上的特定网络路径。通过克隆或通过 kickstart 或 autoYaST 置备并连接到具有关联网络配置文件的网络路径的计算机使用分配的静态 IP 地址置备。为了使用静态 IP 地址分配进行置备，您必须使用自定义规范。

您可以在蓝图中将网络配置文件分配给 vSphere 计算机组件，具体方法为：将现有的按需 NAT 或按需路由网络组件添加到设计画布中，然后选择 vSphere 计算机组件要连接到的网络配置文件。此外，您也可以使用自定义属性 `VirtualMachine.NetworkN.ProfileName` 将网络配置文件分配给蓝图，其中，*N* 是网络标识符。

可以选择使用提供的 vRealize Automation IPAM 或网络配置文件中已注册并配置的第三方 IPAM 服务提供程序端点来获取并配置 IP 地址。有关外部 IPAM 要求的信息，请参见[用于提供第三方 IPAM 提供程序支持的对照表](#)。

在网络配置文件中选择第三方 IPAM 服务提供程序端点的情况下，vRealize Automation 将从已注册的外部 IPAM 提供程序端点（例如 Infoblox）检索 IP 范围。随后它从该端点分配 IP 值。指定的范围子网掩码用于分配 IP 块中的子网。

如果在预留和蓝图中指定网络配置文件，则优先使用蓝图值。例如，如果利用 `VirtualMachine.NetworkN.ProfileName` 自定义属性在蓝图中指定网络配置文件，则优先使用在蓝图中指定的网络配置文件。但是，如果该自定义属性不用于蓝图且您为计算机网卡选择网络配置文件，则 vRealize Automation 将对已指定网络配置文件的计算机网卡使用预留网络路径。

了解 CSV 文件格式以导入网络配置文件 IP 地址

通过使用格式正确的 CSV 文件，可以将 IP 地址网络范围导入到 vRealize Automation 网络配置文件。

CSV 文件条目必须遵守以下格式。

CSV 字段	描述
<code>ip_address</code>	IPv4 格式的 IP 地址。
<code>machine_name</code>	vRealize Automation 中的受管计算机的名称。如果字段为空，默认为无名称。如果字段为空， <code>status</code> 字段值不得为“已分配”。
<code>status</code>	“已分配”或“未分配”，区分大小写。如果字段为空，默认值为“未分配”。如果状态为“已分配”， <code>machine_name</code> 字段值不得为空。
<code>NIC_offset</code>	非负整数。 网卡偏移指示 IP 地址所分配给的虚拟机网卡。如果虚拟机为不同网卡分配了多个 IP 地址，则每个网卡都有一个 IP 地址条目，其中包含相应的网卡偏移。设置为 0 表示无偏移。

以下示例条目表示计算机 IP 地址为 100.10.100.1，名称为 mymachine01，状态为已分配且无网卡偏移。

```
100.10.100.1,mymachine01,Unallocated,0
```

场景：将 IP 地址从 CSV 文件导入网络配置文件

通过导入格式正确的 CSV 文件，您可以将 IP 地址添加到网络配置文件范围。通过在 vRealize Automation 中编辑网络配置文件范围或者导入更改或不同的 CSV 文件，还可以更改网络配置文件范围中的地址。

通过从 CSV 文件导入 IP 地址或手动输入值，可添加或更改网络配置文件范围中的 IP 地址。或者，您可以允许第三方 IPAM 提供程序提供 IP 地址。

- 将 IP 地址的初始范围导入 vRealize Automation 网络配置文件。
- 应用导入的值在网络配置文件中创建第一个命名的网络范围。
- 从网络范围 vRealize Automation 删除一个或多个 IP 地址。
- 导入已更改或不同的 CSV 文件以查看网络范围值的更改情况。

对于使用第三方 IPAM 端点的网络配置文件，您不能使用从 **CSV 导入** 选项，因为 IP 地址由第三方 IPAM 提供程序而不是 vRealize Automation 管理。

前提条件

- 以架构管理员身份登录到 vRealize Automation。

- 创建包含 IP 地址的 CSV 文件以导入到网络范围。请参见[使用第三方 IPAM 提供程序创建外部网络配置文件](#)和[了解 CSV 文件格式以导入网络配置文件 IP 地址](#)。

步骤

- 1 选择**基础架构 > 预留 > 网络配置文件**。
- 2 单击**新建**并从下拉菜单中选择一个网络配置文件类型。
在本例中，选择**外部**。
- 3 在**名称**文本框中输入**通过 CSV 创建我的网络配置文件**。
- 4 在**描述**文本框中输入**通过 CSV 测试网络范围 IP 地址**。
CSV 文件导入选项适用于**网络范围**和**IP 地址**选项卡页面上的设置。
- 5 （可选）还可以选择已配置的 IPAM 端点（如果有）。如果没有，请跳过此步骤。
- 6 在**子网掩码**和**网关**文本框中输入相应的 IP 地址值。
- 7 单击 **DNS** 选项卡。
- 8 输入适用的信息（如 DNS 后缀），然后单击**网络范围**选项卡。
单击**网络范围**选项卡时，**从 CSV 导入**选项可用。
- 9 单击**新建**以手动输入新的网络范围名称和 IP 地址，或单击**从 CSV 导入**以从格式正确的 CSV 文件中导入 IP 地址信息。
 - 单击**新建**。
 - a 输入网络范围名称。
 - b 输入网络范围描述。
 - c 输入范围的起始 IP 地址。
 - d 输入范围的结束 IP 地址。
 - 单击**从 CSV 导入**。
 - a 浏览并选择 CSV 文件，或将 CSV 文件拖入**从 CSV 导入**对话框。

CSV 文件中行的格式为 *ip_address*、*machine_name*、*status*、*NIC offset*。例如：

```
100.10.100.1,mymachine01,Unallocated,0
```

CSV 字段	描述
ip_address	IPv4 格式的 IP 地址。
machine_name	vRealize Automation 中的受管计算机的名称。如果字段为空，默认为无名称。如果字段为空，status 字段值不得为“已分配”。

CSV 字段	描述
status	“已分配”或“未分配”，区分大小写。如果字段为空，默认值为“未分配”。如果状态为“已分配”，machine_name 字段值不得为空。
NIC_offset	非负整数。 网卡偏移指示 IP 地址所分配给的虚拟机网卡。如果虚拟机为不同网卡分配了多个 IP 地址，则每个网卡都有一个 IP 地址条目，其中包含相应的网卡偏移。设置为 0 表示无偏移。

b 单击**应用**。

10 单击**确定**。

“定义的范围”列表中将显示 IP 范围名称。“定义的 IP 地址”列表中将显示该范围内的 IP 地址。

单击**应用**时，或保存并编辑网络配置文件后，已上载的 IP 地址将显示在 **IP 地址** 页面上。

11 单击 **IP 地址** 选项卡，显示指定范围地址空间的 IP 地址数据。

如果已从 CSV 文件中导入 IP 地址信息，生成的范围名称为 *已从 CSV 导入*。

12 （可选）从**网络范围**下拉菜单中选择 IP 地址信息，以筛选 IP 地址条目。

可以显示有关所有定义的网络范围、从 CSV 文件导入的网络范围或指定网络范围的信息。详细信息包括起始 IP 地址、计算机名称、上次修改时间和时间戳以及 IP 状态。

后续步骤

如果再次从 CSV 文件导入 IP 地址，先前的 IP 地址会被导入的 CSV 文件中的信息替代。

为现有网络创建外部网络配置文件

您可以创建外部网络配置文件，指定网络设置来配置现有网络以便置备计算机，其中包括配置要在置备期间使用的 NSX Edge 设备。

您可以使用 vRealize Automation 提供的 IPAM 提供程序端点或在 vRealize Orchestrator 中注册的第三方 IPAM 提供程序端点（例如 Infoblox）。

使用提供的 IPAM 端点创建外部网络配置文件

您可以创建外部网络配置文件，定义在现有网络上置备计算机时要使用的网络属性和静态 IP 地址范围。

您可以在网络配置文件中定义一个或多个用于置备计算机的静态 IP 地址网络范围。如果不指定范围，则可将网络配置文件用作网络预留策略，为虚拟机网卡 (vNIC) 选择预留网络路径。

有关创建外部网络配置文件和使用外部 IPAM 提供程序端点的信息，请参见[使用第三方 IPAM 提供程序创建外部网络配置文件](#)。

步骤

1 使用提供的 IPAM 端点指定外部网络配置文件信息

外部网络配置文件标识现有网络的网络属性和设置。NAT 和路由网络配置文件需要使用外部网络配置文件。

2 使用提供的 IPAM 端点配置外部网络配置文件 IP 范围

您可以在网络配置文件中定义一个或多个用于置备计算机的静态 IP 地址网络范围。如果不指定范围，则可将网络配置文件用作网络预留策略，为虚拟机网卡 (vNIC) 选择预留网络路径。

后续步骤

您可以将网络配置文件分配给预留中的网络路径，或者蓝图架构师可以在蓝图中指定网络配置文件。创建按需 NAT 或路由网络配置文件时，您可以使用外部网络配置文件。

使用提供的 IPAM 端点指定外部网络配置文件信息

外部网络配置文件标识现有网络的网络属性和设置。NAT 和路由网络配置文件需要使用外部网络配置文件。

有关如何通过从注册的第三方 IPAM 端点（如 Infoblox）获取 IPAM 地址信息来创建外部网络配置文件的信息，请参见[用于提供第三方 IPAM 提供程序支持的对照表](#)和[使用第三方 IPAM 提供程序创建外部网络配置文件](#)。请按照以下步骤使用 VMware 内部 IPAM 端点创建网络配置文件。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**基础架构 > 预留 > 网络配置文件**。

- 2 单击**新建**并从下拉菜单中选择 **外部**。

- 3 输入名称和可选描述。

- 4 接受提供的 **vRealize Automation IPAM** 端点的默认 **IPAM 端点值**。

- 5 在**子网掩码**文本框中，输入 IP 子网掩码。

子网掩码指定要为网络配置文件定义的整个可路由地址空间的大小。

例如，输入 255.255.0.0。

- 6 在**网关**文本框中输入 IPv4 格式的 Edge 或路由网关地址，例如 10.10.110.1。

系统会在分配过程中将网络配置文件中定义的网关 IP 地址分配给网卡。NAT 网络配置文件需要网关条目。

如果使用 NSX-T，DHCP 服务器默认网关应为 NSX-T 中的 NAT 一对多默认网关。IP 池默认网关应与 vRealize Automation 中的 NAT 一对多默认网关相匹配。

如果网络配置文件的**网关**文本框中未分配任何值，则您必须使用 `VirtualMachine.Network0.Gateway` 自定义属性来指定网关。

- 7 单击 **DNS** 选项卡。

- 8 根据需要输入 DNS 和 WINS 值。

DNS 值用于注册和解析 DNS 名称。如果使用内部 IPAM 端点，DNS 和 WINS 字段可选填。如果使用外部 IPAM 端点，则 DNS 值和 WINS 值由第三方 IPAM 提供程序提供。

a （可选）输入**主 DNS**服务器值。

b （可选）输入**辅助 DNS**服务器值。

c （可选）输入 **DNS 后缀**值。

d （可选）输入 **DNS 搜索后缀**值。

- e (可选) 输入**首选 WINS** 服务器值。
- f (可选) 输入**备用 WINS** 服务器值。

后续步骤

您可以配置静态 IP 地址的 IP 范围。请参见[使用提供的 IPAM 端点配置外部网络配置文件 IP 范围](#)。

使用提供的 IPAM 端点配置外部网络配置文件 IP 范围

您可以在网络配置文件中定义一个或多个用于置备计算机的静态 IP 地址网络范围。如果不指定范围，则可将网络配置文件用作网络预留策略，为虚拟机网卡 (vNIC) 选择预留网络路径。

您可以手动定义 IP 范围值、从 CSV 文件导入，或者使用外部 IPAM 提供程序提供的 IP 地址。您可以将手动定义的 IP 范围和通过 CSV 导入的 IP 地址合并。例如，您可以通过使用用户界面定义一些范围，而通过从 CSV 文件导入定义其他范围。

如果再次从某个 CSV 文件导入，无论 CSV 文件的名称如何，从先前的 CSV 文件导入中导入的 IP 范围将被擦除，而新的 IP 范围信息将被添加。这样当您第二次或更多次导入时，先前的导入将被覆盖。您可以无限地重复此更新 CSV 文件的流程并将该 CSV 文件重新导入到网络配置文件中。

如果外部网络配置文件未定义 IP 范围，则您可以使用它指定为虚拟网卡 (vNIC) 选择的网络。如果您在路由或 NAT 网络配置文件中存在现有网络配置文件，则必须至少具有一个静态 IP 范围。

前提条件

[使用提供的 IPAM 端点指定外部网络配置文件信息](#)。

步骤

- 1 单击**网络范围**选项卡。
- 2 单击**新建**以手动输入新的网络范围名称和 IP 地址，或单击**从 CSV 导入**以从格式正确的 CSV 文件中导入 IP 地址信息。
 - 单击**新建**。
 - a 输入网络范围名称。
 - b 输入网络范围描述。
 - c 输入范围的起始 IP 地址。
 - d 输入范围的结束 IP 地址。
 - 单击**从 CSV 导入**。
 - a 浏览并选择 CSV 文件，或将 CSV 文件拖入**从 CSV 导入**对话框。

CSV 文件中行的格式为 *ip_address*、*machine_name*、*status*、*NIC offset*。例如：

```
100.10.100.1,mymachine01,Unallocated,0
```

CSV 字段	描述
ip_address	IPv4 格式的 IP 地址。
machine_name	vRealize Automation 中的受管计算机的名称。如果字段为空，默认为无名称。如果字段为空，status 字段值不得为“已分配”。
status	“已分配”或“未分配”，区分大小写。如果字段为空，默认值为“未分配”。如果状态为“已分配”，machine_name 字段值不得为空。
NIC_offset	非负整数。 网卡偏移指示 IP 地址所分配给的虚拟机网卡。如果虚拟机为不同网卡分配了多个 IP 地址，则每个网卡都有一个 IP 地址条目，其中包含相应的网卡偏移。设置为 0 表示无偏移。

b 单击**应用**。

3 单击**确定**。

“定义的范围”列表中将显示 IP 范围名称。“定义的 IP 地址”列表中将显示该范围内的 IP 地址。

单击**应用**时，或保存并编辑网络配置文件后，已上载的 IP 地址将显示在 **IP 地址** 页面上。

4 单击 **IP 地址** 选项卡，显示指定范围地址空间的 IP 地址数据。

如果已从 CSV 文件中导入 IP 地址信息，生成的范围名称为 *已从 CSV 导入*。

5 （可选）从**网络范围**下拉菜单中选择 IP 地址信息，以筛选 IP 地址条目。

可以显示有关所有定义的网络范围、从 CSV 文件导入的网络范围或指定网络范围的信息。详细信息包括起始 IP 地址、计算机名称、上次修改时间和时间戳以及 IP 状态。

6 （可选）从 **IP 状态** 下拉菜单中选择状态类型，以筛选 IP 地址条目，只显示符合选定 IP 状态的条目。状态设置有“已分配”、“未分配”、“已销毁”与“已过期”。

对于状态为已过期或已销毁的 IP 地址，可单击**回收**，使这些 IP 地址范围可用于分配。必须保存配置文件，以使回收生效。地址无法立即回收，因此状态列不会立即从“已过期”或“已销毁”变为“已分配”。

7 单击**确定**，完成网络配置文件。

结果

您可以将网络配置文件分配给预留中的网络路径，或者蓝图架构师可以在蓝图中指定网络配置文件。如果创建了外部网络配置文件，可以在创建 NAT 或路由网络配置文件时使用此外部网络配置文件。

使用第三方 IPAM 提供程序创建外部网络配置文件

您可以使用在 vRealize Orchestrator 中导入、配置和注册的第三方 IPAM 提供程序解决方案从该第三方提供程序获取 IP 地址。

您可以创建外部网络配置文件，该配置文件使用注册的第三方 IPAM 解决方案提供程序端点获取网关、子网掩码和 DHCP/WINS 设置。

您可以在网络配置文件中定义一个或多个用于置备计算机的静态 IP 地址网络范围。如果不指定范围，则可将网络配置文件用作网络预留策略，为虚拟机网卡 (vNIC) 选择预留网络路径。

有关不使用 IPAM 提供程序或者提供的内部 IPAM 提供程序端点的情况下如何创建外部网络配置文件的信息，请参见[使用提供的 IPAM 端点创建外部网络配置文件](#)。

步骤

1 使用第三方 IPAM 端点指定外部网络配置文件信息

外部网络配置文件标识现有网络的网络属性和设置。NAT 和路由网络配置文件需要使用外部网络配置文件。如果已在 vRealize Orchestrator 中注册和配置 IPAM 端点，可指定 IP 地址信息由 IPAM 提供程序提供。

2 使用第三方 IPAM 端点配置外部网络配置文件 IP 范围

您可以在网络配置文件中定义一个或多个用于置备计算机的静态 IP 地址网络范围。如果不指定范围，则可将网络配置文件用作网络预留策略，为虚拟机网卡 (vNIC) 选择预留网络路径。

后续步骤

您可以将网络配置文件分配给预留中的网络路径，或者蓝图架构师可以在蓝图中指定网络配置文件。创建按需 NAT 或路由网络配置文件时，您可以使用外部网络配置文件。

使用第三方 IPAM 端点指定外部网络配置文件信息

外部网络配置文件标识现有网络的网络属性和设置。NAT 和路由网络配置文件需要使用外部网络配置文件。如果已在 vRealize Orchestrator 中注册和配置 IPAM 端点，可指定 IP 地址信息由 IPAM 提供程序提供。

前提条件

- 请确认已在 vRealize Orchestrator 中导入和配置外部 IPAM 提供程序插件，并且已在 vRealize Orchestrator 中注册 IPAM 提供程序端点类型。在此例中，支持的外部 IPAM 解决方案提供程序为 Infoblox。请参见[用于提供第三方 IPAM 提供程序支持的对照表](#)。
- [创建第三方 IPAM 提供程序端点](#)。
- 在全局租户 (administrator@vsphere.local) 中，使用已注册的 IPAM 端点 workflow 将 vRealize Orchestrator Appliance 配置为独立的 Orchestrator。
- 以架构管理员身份登录到 vRealize Automation。

步骤

- 1 选择**基础架构 > 预留 > 网络配置文件**。
- 2 单击**新建**并从下拉菜单中选择 **外部**。
- 3 输入名称和可选描述。
- 4 如果配置了一个或多个第三方 IPAM 提供程序端点，请在 **IPAM 端点** 下拉菜单中选择一个第三方 IPAM 端点。

如果选择已在 vRealize Orchestrator 中注册的第三方 IPAM 提供程序端点，将从指定的 IPAM 服务提供程序获取 IP 地址。诸如子网掩码和 DNS/WINS 选项等 IP 规范不可用，因为其功能由选定的第三方 IPAM 端点控制。

后续步骤

现在可以定义 IP 地址的网络范围，以完成网络配置文件定义。

使用第三方 IPAM 端点配置外部网络配置文件 IP 范围

您可以在网络配置文件中定义一个或多个用于置备计算机的静态 IP 地址网络范围。如果不指定范围，则可将网络配置文件用作网络预留策略，为虚拟机网卡 (vNIC) 选择预留网络路径。

您可以使用第三方 IPAM 提供程序提供的 IP 地址来定义 IP 范围。

vRealize Automation 仅将外部 IPAM 范围 ID 保存 to 数据库中，而不保存范围的详细信息。如果您在此页面或蓝图上编辑网络配置文件，vRealize Automation 会调用 IPAM 服务以根据所选范围 ID 获取范围的详细信息。

注 某些第三方 IPAM 提供程序存在一个已知问题：在返回网络范围时查询可能会超时，从而导致列表为空。作为解决办法，您可以提供搜索条件，从而避免超时并获取网络范围信息。

例如，根据 IPAM 提供程序，您可以在 IPAM 提供程序应用程序的每个网络中添加名为 VLAN 的属性并为该属性分配一个值，例如 4。然后，可以在 vRealize Automation 网络配置文件页面上的**选择网络范围**文本框中筛选属性和值，例如 VLAN=4。

或者，您也可以通过以下过程增加超时设置：

- 1 在每个 vRealize Automation 设备节点上，打开 `/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml` 文件。
- 2 将超时值从 30 秒更改为更大的值。
- 3 输入 `service vcac-server restart` 重新启动 vcac-server。

前提条件

使用第三方 IPAM 端点指定外部网络配置文件信息。

步骤

- 1 单击**网络范围**选项卡，创建新的网络范围，或选择现有的网络范围。

此时显示关于选定范围的详细信息，包括各个名称、描述、起始和结束 IP 地址。同时还会提供状态相关信息。

- 2 在**地址空间**下拉菜单中，从可用于端点的所有地址空间的列表中选择一个地址空间。

- 3 单击**添加**，然后选择指定地址空间的一个或多个可用网络范围。

选择网络范围可能会导致在使用第三方 IPAM 提供程序时产生空列表。有关详细信息，请参见知识库文章 2148656，网址为 <http://kb.vmware.com/kb/2148656>。

- 4 单击**确定**。

“定义的范围”列表中将显示 IP 范围名称。“定义的 IP 地址”列表中将显示该范围内的 IP 地址。

单击**应用**时，或保存并编辑网络配置文件后，已上载的 IP 地址将显示在 **IP 地址**页面上。

- 5 单击**确定**，完成网络配置文件。

后续步骤

您可以将网络配置文件分配给预留中的网络路径，或者蓝图架构师可以在蓝图中指定网络配置文件。

为按需网络创建路由网络配置文件

您可以创建按需路由网络配置文件，该配置文件使用提供的 vRealize Automation IPAM 端点或已正确配置和注册的第三方 IPAM 端点。

路由网络配置文件表示跨多个网络划分的可路由 IP 空间。每个新路由的网络从可路由 IP 空间分配下一个可用子网。路由网络可访问使用相同网络配置文件的所有其他路由网络。每个路由子网均可访问由相同网络配置文件创建的所有其他子网。

对于第三方 IPAM 提供程序，第三方 IPAM 提供程序会创建和管理可路由 IP 空间。网络管理员使用第三方 IPAM 提供程序定义可路由 IP 空间并为其创建 IP 段。创建或编辑路由网络配置文件时，您可以选择从第三方 IPAM 提供程序检索的一个或多个 IP 段。

从第三方 IPAM 提供程序分配路由网络配置文件的新实例时，vRealize Automation 会调用该提供程序以预留下一个可用子网，并使用通过路由网络配置文件和子网大小确定的 IP 块创建范围。生成的范围用于为分配给同一部署中的路由网络的计算机分配 IP 地址。

使用提供的 IPAM 端点创建路由网络配置文件

将路由网络配置文件与提供的 IPAM 端点结合使用时，您可以为按需路由网络定义可路由 IP 空间和可用子网。

通过使用 vRealize Automation 提供的 IPAM 端点，您可以将静态 IP 地址范围和基本 IP 地址分配给路由网络配置文件。

您可以使用从提供的 VMware IPAM 端点或已在 vRealize Orchestrator 中注册和配置的第三方 IPAM 服务提供程序端点（如 Infoblox IPAM）获取的 IP 范围。IP 范围是在分配期间从 IP 块创建的。

步骤

1 使用 vRealize Automation IPAM 端点指定路由网络配置文件信息

如果使用提供的 IPAM 端点，网络配置文件信息将标识路由网络属性及其基础外部网络配置文件以及置备网络时所用的其他值。

2 使用 vRealize Automation IPAM 端点配置路由网络配置文件 IP 范围

您可以定义一个或多个用于置备网络的静态 IP 地址范围。

使用 vRealize Automation IPAM 端点指定路由网络配置文件信息

如果使用提供的 IPAM 端点，网络配置文件信息将标识路由网络属性及其基础外部网络配置文件以及置备网络时所用的其他值。

如果要使用第三方 IPAM 端点创建路由网络配置文件，请参见[使用第三方 IPAM 端点指定路由网络配置文件信息](#)。

前提条件

- 以架构管理员身份登录到 vRealize Automation。
- 创建外部网络配置文件。请参见[使用提供的 IPAM 端点创建外部网络配置文件](#)。

步骤

- 1 选择**基础架构 > 预留 > 网络配置文件**。
- 2 单击**新建**并从下拉菜单中选择**已路由**。
- 3 输入名称和可选描述。
- 4 接受提供的 **vRealize Automation IPAM** 端点的默认 **IPAM 端点值**。
- 5 从**外部网络配置文件**下拉菜单中选择现有的网络配置文件。
- 6 在与外部网络配置文件关联的**子网掩码**文本框中，输入子网掩码。
子网掩码指定要为网络配置文件定义的整个可路由地址空间的大小。
例如，输入 255.255.0.0。
- 7 在**范围子网掩码**文本框下拉菜单中选择一个值，用以确定 **IP 范围**页面上的**生成范围**选项如何生成范围。
例如，输入 255.255.255.0。

范围子网掩码定义将该空间划分为单独的地址块（分配给该网络配置文件的每个部署实例）的方式。为范围子网掩码选择值时，应考虑预计将使用路由网络的部署的数量。

范围用于每个使用路由网络配置文件的部署。可用路由范围的个数等于子网掩码除以范围子网掩码，例如 $255.255.0.0/255.255.255.0 = 256$ 。

- 8 在**基本 IP** 文本框中，输入第一个可用的 IP 地址。
当选择第三方端点时，此选项不可用。
例如，输入 120.120.0.1。

- 9 单击 **DNS** 选项卡。

- 10 根据需要输入 DNS 和 WINS 值。

DNS 值用于注册和解析 DNS 名称。如果使用内部 IPAM 端点，DNS 和 WINS 字段可选填。如果使用外部 IPAM 端点，则 DNS 值和 WINS 值由第三方 IPAM 提供程序提供。

- a （可选）输入**主 DNS** 服务器值。
- b （可选）输入**辅助 DNS** 服务器值。
- c （可选）输入 **DNS 后缀值**。
- d （可选）输入 **DNS 搜索后缀值**。
- e （可选）输入**首选 WINS** 服务器值。
- f （可选）输入**备用 WINS** 服务器值。

后续步骤

使用 [vRealize Automation IPAM 端点配置路由网络配置文件 IP 范围](#)。

使用 vRealize Automation IPAM 端点配置路由网络配置文件 IP 范围

您可以定义一个或多个用于置备网络的静态 IP 地址范围。

在置备期间，每个新路由网络将分配下一可用的范围，并将其用作自己的 IP 空间。

前提条件

使用 [vRealize Automation IPAM 端点指定路由网络配置文件信息](#)。

步骤

- 1 单击**网络范围**选项卡，创建新的网络范围，或选择现有的网络范围。

此时显示关于选定范围的详细信息，包括各个名称、描述、起始和结束 IP 地址。同时还会提供状态相关信息。

- 2 单击**生成范围**根据“常规”选项卡上输入的子网掩码、范围子网掩码和基本 IP 地址信息生成网络范围。

vRealize Automation 将从基本 IP 地址开始，根据范围子网掩码生成范围。

例如，如果子网掩码为 255.255.0.0 且范围子网掩码为 255.255.255.0，vRealize Automation 使用名称“范围 1”到“范围 n ”生成 255 IP 范围。

- 3 单击**确定**。

使用第三方 IPAM 端点创建路由网络配置文件

将路由网络配置文件与第三方 IPAM 端点结合使用时，第三方 IPAM 提供程序会创建和管理可路由 IP 空间。

在路由网络配置文件中使用时，该提供程序会为按需网络的每个实例创建新的 IP 范围。

您可以使用从提供的 VMware IPAM 端点或已在 vRealize Orchestrator 中注册和配置的第三方 IPAM 服务提供程序端点（如 Infoblox IPAM）获取的 IP 范围。IP 范围是在分配期间从 IP 块创建的。

步骤

- 1 使用[第三方 IPAM 端点指定路由网络配置文件信息](#)

如果使用第三方 IPAM 端点，网络配置文件信息将标识路由网络属性及其基础外部网络配置文件以及置备网络时所用的其他值。

- 2 使用[第三方 IPAM 端点配置路由网络配置文件 IP 范围](#)

您可以管理一个或多个用于置备网络的指定静态 IPv4 网络地址范围。

使用第三方 IPAM 端点指定路由网络配置文件信息

如果使用第三方 IPAM 端点，网络配置文件信息将标识路由网络属性及其基础外部网络配置文件以及置备网络时所用的其他值。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 创建外部网络配置文件。请参见[使用提供的 IPAM 端点创建外部网络配置文件](#)或[使用第三方 IPAM 提供程序创建外部网络配置文件](#)。
- 创建和配置第三方 IPAM 端点。请参见[创建第三方 IPAM 提供程序端点](#)。

步骤

- 1 选择**基础架构 > 预留 > 网络配置文件**。
- 2 单击**新建**并从下拉菜单中选择**已路由**。
- 3 输入名称和可选描述。
- 4 如果配置了一个或多个第三方 IPAM 提供程序端点，请在 **IPAM 端点** 下拉菜单中选择一个第三方 IPAM 端点。

如果选择已在 vRealize Orchestrator 中注册的第三方 IPAM 提供程序端点，将从指定的 IPAM 服务提供程序获取 IP 地址。诸如子网掩码和 DNS/WINS 选项等 IP 规范不可用，因为其功能由选定的第三方 IPAM 端点控制。

- 5 从**外部网络配置文件**下拉菜单中选择现有的网络配置文件。

只会列出配置为使用指定的 IPAM 端点的外部网络配置文件，并且只有这些外部网络配置文件可供选择。

- 6 在**范围子网掩码**文本框下拉菜单中选择一个值，用以确定创建用于置备的网络子网数量。

例如，输入 255.255.255.0。

范围子网掩码定义将该空间划分为单独的地址块（分配给该网络配置文件的每个部署实例）的方式。为范围子网掩码选择值时，应考虑预计将使用路由网络的部署的数量。

范围用于每个使用路由网络配置文件的部署。可用路由范围的个数等于子网掩码除以范围子网掩码，例如 $255.255.0.0/255.255.255.0 = 256$ 。

- 7 单击 **IP 块** 选项卡，以定义地址空间并管理一个或多个已命名的静态 IPv4 网络地址范围。

可用 IP 块是创建或分配用于按需路由的 IP 范围的源。

后续步骤

[使用第三方 IPAM 端点配置路由网络配置文件 IP 范围。](#)

使用第三方 IPAM 端点配置路由网络配置文件 IP 范围

您可以管理一个或多个用于置备网络的指定静态 IPv4 网络地址范围。

在置备期间，每个新路由网络将分配下一可用的范围，并将分配的范围用作自己的 IP 空间。IP 块从第三方 IPAM 提供程序中获取。在置备期间，从子网掩码与提供的范围子网掩码匹配的块分配路由网络。

前提条件

[使用第三方 IPAM 端点指定路由网络配置文件信息。](#)

步骤

- 1 从**地址空间**下拉菜单中选择一个地址空间，用以限制可用于置备的 IP 块。

在“地址空间”文本框下面的部分中添加一个或多个 IP 块之后，无法再选择**地址空间**值。路由网络配置文件不能跨多个地址空间。

- 2 通过使用特定于提供程序的搜索语法或从“搜索”下拉菜单中进行选择，添加一个或多个 IP 块，或者添加 IPAM 提供程序范围。

将从第三方 IPAM 提供程序检索 IP 块。

选择网络范围可能会导致在使用第三方 IPAM 提供程序时产生空列表。有关详细信息，请参见知识库文章 2148656，网址为 <http://kb.vmware.com/kb/2148656>。

- a 单击**添加**。
- b 单击**搜索**。
- c 输入搜索语法，或从下拉菜单中选择一个或多个 IP 块。
- d 单击**确定**。

- 3 单击**应用**。

- 4 单击**确定**。

为按需网络创建 NAT 网络配置文件

您可以创建一个按需 NAT 网络配置文件，该配置文件使用提供的 vRealize Automation IPAM 端点或已正确配置和注册的第三方 IPAM 端点。

使用提供的 IPAM 端点创建 NAT 网络配置文件

您可以创建一个与外部网络配置文件相对的按需 NSX NAT 网络配置文件。使用提供的 vRealize Automation IPAM 端点时，您可以向 NAT 网络配置文件分配静态 IP 和 DHCP 地址的范围。

NAT 网络使用一组 IP 地址进行外部通信，使用另一组 IP 地址进行内部通信。外部 IP 地址从外部网络配置文件进行分配，而内部 NAT IP 地址由 NAT 网络配置文件定义。置备新的 NAT 网络时，会创建 NAT 网络配置文件的新实例并用它来分配计算机 IP 地址。

您可以使用从提供的 VMware IPAM 端点或已在 vRealize Orchestrator 中注册和配置的第三方 IPAM 服务提供程序端点（如 Infoblox IPAM）获取的 IP 范围。IP 范围是在分配期间从 IP 块创建的。

对于 NAT 一对多网络，可以定义 NAT 规则（将 NAT 网络组件添加到蓝图时可进行配置，编辑部署中的 NAT 网络时可进行更改）。

步骤

- 1 使用 [vRealize Automation IPAM 端点确定 NAT 网络配置文件信息](#)

网络配置文件通过使用嵌入式 vRealize Automation IPAM 来确定按需 NAT 网络属性、底层外部网络配置文件、NAT 类型以及置备网络时使用的其他值。

- 2 使用 [vRealize Automation IPAM 端点配置 NAT 网络配置文件 IP 范围](#)

您可以定义一个或多个用于置备网络的静态 IP 地址范围。

使用 vRealize Automation IPAM 端点确定 NAT 网络配置文件信息

网络配置文件通过使用嵌入式 vRealize Automation IPAM 来确定按需 NAT 网络属性、底层外部网络配置文件、NAT 类型以及置备网络时使用的其他值。

如果希望创建一个使用第三方 IPAM 端点的 NAT 网络配置文件，请参见[使用第三方 IPAM 端点时指定 NAT 网络配置文件信息](#)。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 创建外部网络配置文件。请参见[使用提供的 IPAM 端点创建外部网络配置文件](#)。

步骤

- 1 选择**基础架构 > 预留 > 网络配置文件**。
- 2 单击**新建**并从下拉菜单中选择 **NAT**。
- 3 输入名称和可选描述。
- 4 接受提供的 **vRealize Automation IPAM** 端点的默认 **IPAM 端点值**。
- 5 从**外部网络配置文件**下拉菜单中选择现有的网络配置文件。
- 6 从 **NAT 类型**下拉菜单中选择一对一或一对多网络地址转换类型。

选项	描述
一对一	<p>为每个网络适配器分配一个外部静态 IP 地址。每台计算机均可访问外部网络，且可从外部网络访问。</p> <p>分配给 NSX Edge 上行链路的所有外部 IP 地址都必须是同一子网的一部分。在 vRealize Automation 中使用 NAT 1:1 时，相应外部网络配置文件包含的 IP 范围必须仅存在于单个子网中。</p>
一对多	<p>一个外部 IP 地址在网络上的所有计算机之间共享。内部计算机可以具有 DHCP 或静态 IP 地址。每台计算机均可访问外部网络，但无法从外部网络访问。选中此选项，可在 DHCP 组中启用已启用复选框。</p> <p>对于 NSX for vSphere，使用 NAT 一对多转换类型，可以在将 NAT 网络组件添加到蓝图时定义 NAT 规则。</p> <p>NSX for vSphere 支持 NAT 一对一网络和 NAT 一对多网络，但 NSX-T 仅支持 NAT 一对多网络。</p>

- 7 在**子网掩码**文本框中，输入 IP 子网掩码。
 子网掩码指定要为网络配置文件定义的整个可路由地址空间的大小。
 例如，输入 255.255.0.0。
- 8 在**网关**文本框中输入 IPv4 格式的 Edge 或路由网关地址，例如 10.10.110.1。
 系统会在分配过程中将网络配置文件中定义的网关 IP 地址分配给网卡。NAT 网络配置文件需要网关条目。
 如果使用 NSX-T，DHCP 服务器默认网关应为 NSX-T 中的 NAT 一对多默认网关。IP 池默认网关应与 vRealize Automation 中的 NAT 一对多默认网关相匹配。
 如果网络配置文件的**网关**文本框中未分配任何值，则您必须使用 `VirtualMachine.Network0.Gateway` 自定义属性来指定网关。
- 9 （可选）在 DHCP 组中，选中**已启用**复选框，然后输入 **IP 范围起始**和 **IP 范围结束**的值。
 仅当将 NAT 类型设置为“一对多”时，才可选中此复选框。

对于 NSX-T，IP 池范围中的第一个 IP 应与 NSX-T 中定义为 <FirstIpInPool>/<subnetMaskOfNat> 的 DHCP 服务器 IP 地址相匹配。NSX-T 中的 IP 池应以第二个 IP 地址开头。

10 （可选）设置 DHCP 租用时间，定义计算机可以使用 IP 地址的时间长度。

11 单击 **DNS** 选项卡。

12 根据需要输入 DNS 和 WINS 值。

DNS 值用于注册和解析 DNS 名称。如果使用内部 IPAM 端点，DNS 和 WINS 字段可选填。如果使用外部 IPAM 端点，则 DNS 值和 WINS 值由第三方 IPAM 提供程序提供。

- a （可选）输入**主 DNS** 服务器值。
- b （可选）输入**辅助 DNS** 服务器值。
- c （可选）输入 **DNS 后缀** 值。
- d （可选）输入 **DNS 搜索后缀** 值。
- e （可选）输入**首选 WINS** 服务器值。
- f （可选）输入**备用 WINS** 服务器值。

后续步骤

[使用 vRealize Automation IPAM 端点配置 NAT 网络配置文件 IP 范围。](#)

使用 vRealize Automation IPAM 端点配置 NAT 网络配置文件 IP 范围

您可以定义一个或多个用于置备网络的静态 IP 地址范围。

不能将开始和结束网络范围 IP 地址与 DHCP 地址重叠。如果尝试保存包含重叠地址范围的配置文件，vRealize Automation 将显示验证错误。

前提条件

[使用 vRealize Automation IPAM 端点确定 NAT 网络配置文件信息。](#)

步骤

1 单击**网络范围**选项卡，创建新的网络范围，或选择现有的网络范围。

此时显示关于选定范围的详细信息，包括各个名称、描述、起始和结束 IP 地址。同时还会提供状态相关信息。

2 单击**新建**以手动输入新的网络范围名称和 IP 地址，或单击**从 CSV 导入**以从格式正确的 CSV 文件中导入 IP 地址信息。

- 单击**新建**。
 - a 输入网络范围名称。
 - b 输入网络范围描述。
 - c 输入范围的起始 IP 地址。
 - d 输入范围的结束 IP 地址。

- 单击**从 CSV 导入**。

- a 浏览并选择 CSV 文件，或将 CSV 文件拖入**从 CSV 导入**对话框。

CSV 文件中行的格式为 *ip_address*、*machine_name*、*status*、*NIC offset*。例如：

```
100.10.100.1,mymachine01,Unallocated,0
```

CSV 字段	描述
ip_address	IPv4 格式的 IP 地址。
machine_name	vRealize Automation 中的受管计算机的名称。如果字段为空，默认为无名称。如果字段为空， status 字段值不得为“已分配”。
status	“已分配”或“未分配”，区分大小写。如果字段为空，默认值为“未分配”。如果状态为“已分配”， machine_name 字段值不得为空。
NIC_offset	非负整数。 网卡偏移指示 IP 地址所分配给的虚拟机网卡。如果虚拟机为不同网卡分配了多个 IP 地址，则每个网卡都有一个 IP 地址条目，其中包含相应的网卡偏移。设置为 0 表示无偏移。

- b 单击**应用**。

3 单击**确定**。

“定义的范围”列表中将显示 IP 范围名称。“定义的 IP 地址”列表中将显示该范围内的 IP 地址。

单击**应用**时，或保存并编辑网络配置文件后，已上载的 IP 地址将显示在 **IP 地址** 页面上。

4 单击 **IP 地址** 选项卡，显示指定网络范围的 IP 地址。

5 （可选）从**网络范围**下拉菜单中选择 IP 地址信息，以筛选 IP 地址条目。

可以显示有关所有定义的网络范围、从 CSV 文件导入的网络范围或指定网络范围的信息。详细信息包括起始 IP 地址、计算机名称、上次修改时间和时间戳以及 IP 状态。

6 （可选）从 **IP 状态** 下拉菜单中选择状态类型，以筛选 IP 地址条目，只显示符合选定 IP 状态的条目。状态设置有“已分配”、“未分配”、“已销毁”与“已过期”。

对于状态为已过期或已销毁的 IP 地址，可单击**回收**，使这些 IP 地址范围可用于分配。必须保存配置文件，以使回收生效。地址无法立即回收，因此状态列不会立即从“已过期”或“已销毁”变为“已分配”。

7 单击**确定**。

使用第三方 IPAM 端点创建 NAT 网络配置文件

您可以创建一个与外部网络配置文件相对的按需 NSX NAT 网络配置文件。将 NSX NAT 网络配置文件与第三方 IPAM 端点结合使用时，第三方 IPAM 提供程序会创建和管理 IP 空间。

在 NAT 网络配置文件中使用时，该提供程序会为按需网络的每个实例创建新的 IP 范围。在 NAT 网络的每个实例的第三方 IPAM 提供程序端点中，均会创建由一个或多个范围定义的内部 IP 地址集。这些 IP 范围用于为分配给同一部署中的 NAT 网络的计算机分配 IP 地址。由于不能在单个地址空间中定义重复的 IP 地址，因此该提供程序会为 NAT 网络的每个实例创建一个新的地址空间。销毁 NAT 网络后，其范围会在 IPAM 提供程序端点和新地址空间中被销毁。

您可以使用从提供的 VMware IPAM 端点或已在 vRealize Orchestrator 中注册和配置的第三方 IPAM 服务提供程序端点（如 Infoblox IPAM）获取的 IP 范围。IP 范围是在分配期间从 IP 块创建的。

对于 NAT 一对多网络，可以定义 NAT 规则（将 NAT 网络组件添加到蓝图时可进行配置，编辑部署中的 NAT 网络时可进行更改）。

步骤

1 使用第三方 IPAM 端点时指定 NAT 网络配置文件信息

使用第三方 IPAM 端点时，网络配置文件信息用于标识在置备网络时使用的 NAT 网络属性及其基础外部网络配置文件以及其他值。

2 使用第三方 IPAM 端点配置 NAT 网络配置文件 IP 范围

您可以使用 NAT 定义一个或多个 IP 地址范围，以便在置备网络时使用。

使用第三方 IPAM 端点时指定 NAT 网络配置文件信息

使用第三方 IPAM 端点时，网络配置文件信息用于标识在置备网络时使用的 NAT 网络属性及其基础外部网络配置文件以及其他值。

前提条件

- 以架构管理员身份登录到 vRealize Automation。
- 创建外部网络配置文件。请参见[使用提供的 IPAM 端点创建外部网络配置文件](#)或[使用第三方 IPAM 提供程序创建外部网络配置文件](#)。
- 创建和配置第三方 IPAM 端点。请参见[创建第三方 IPAM 提供程序端点](#)。

步骤

1 选择基础架构 > 预留 > 网络配置文件。

2 单击新建并从下拉菜单中选择 NAT。

3 输入名称和可选描述。

4 如果配置了一个或多个第三方 IPAM 提供程序端点，请在 IPAM 端点下拉菜单中选择一个第三方 IPAM 端点。

如果选择已在 vRealize Orchestrator 中注册的第三方 IPAM 提供程序端点，将从指定的 IPAM 服务提供程序获取 IP 地址。诸如子网掩码和 DNS/WINS 选项等 IP 规范不可用，因为其功能由选定的第三方 IPAM 端点控制。

5 从外部网络配置文件下拉菜单中选择现有的网络配置文件。

只会列出配置为使用指定的 IPAM 端点的外部网络配置文件，并且只有这些外部网络配置文件可供选择。

6 从 **NAT 类型** 下拉菜单中选择一对一或一对多网络地址转换类型。

选项	描述
一对一	<p>为每个网络适配器分配一个外部静态 IP 地址。每台计算机均可访问外部网络，且可从外部网络访问。</p> <p>分配给 NSX Edge 上行链路的所有外部 IP 地址都必须是同一子网的一部分。在 vRealize Automation 中使用 NAT 1:1 时，相应外部网络配置文件包含的 IP 范围必须仅存在于单个子网中。</p>
一对多	<p>一个外部 IP 地址在网络上的所有计算机之间共享。内部计算机只能使用静态 IP 地址。每台计算机均可访问外部网络，但无法从外部网络访问。</p> <p>为第三方 IPAM 提供程序使用 NAT 时，不支持 DHCP。</p> <p>对于 NSX for vSphere，使用 NAT 一对多转换类型，可以在将 NAT 网络组件添加到蓝图时定义 NAT 规则。</p> <p>NSX for vSphere 支持 NAT 一对一网络和 NAT 一对多网络，但 NSX-T 仅支持 NAT 一对多网络。</p>

7 在子网掩码文本框中，输入 IP 子网掩码。

子网掩码指定要为网络配置文件定义的整个可路由地址空间的大小。

例如，输入 255.255.0.0。

8 在网关文本框中输入 IPv4 格式的 Edge 或路由网关地址，例如 10.10.110.1。

系统会在分配过程中将网络配置文件中定义的网关 IP 地址分配给网卡。NAT 网络配置文件需要网关条目。

如果使用 NSX-T，DHCP 服务器默认网关应为 NSX-T 中的 NAT 一对多默认网关。IP 池默认网关应与 vRealize Automation 中的 NAT 一对多默认网关相匹配。

如果网络配置文件的网关文本框中未分配任何值，则您必须使用 `VirtualMachine.Network0.Gateway` 自定义属性来指定网关。

9 单击 **DNS** 选项卡。

10 根据需要输入 DNS 和 WINS 值。

DNS 值用于注册和解析 DNS 名称。如果使用内部 IPAM 端点，DNS 和 WINS 字段可选填。如果使用外部 IPAM 端点，则 DNS 值和 WINS 值由第三方 IPAM 提供程序提供。

- a （可选）输入**主 DNS** 服务器值。
- b （可选）输入**辅助 DNS** 服务器值。
- c （可选）输入 **DNS 后缀** 值。
- d （可选）输入 **DNS 搜索后缀** 值。
- e （可选）输入**首选 WINS** 服务器值。
- f （可选）输入**备用 WINS** 服务器值。

后续步骤

[使用第三方 IPAM 端点配置 NAT 网络配置文件 IP 范围。](#)

使用第三方 IPAM 端点配置 NAT 网络配置文件 IP 范围

您可以使用 NAT 定义一个或多个 IP 地址范围，以便在置备网络时使用。

前提条件

使用第三方 IPAM 端点时指定 NAT 网络配置文件信息。

步骤

- 1 单击**网络范围**选项卡，创建新的网络范围，或选择现有的网络范围。

此时显示关于选定范围的详细信息，包括各个名称、描述、起始和结束 IP 地址。同时还会提供状态相关信息。

- 2 单击**新建**并定义网络范围。

- a 输入网络范围名称和描述。
- b 输入开始和结束 IP 地址以定义范围。
- c 单击**应用**。

- 3 单击**确定**。

“定义的范围”列表中将显示 IP 范围名称。“定义的 IP 地址”列表中将显示该范围内的 IP 地址。

单击**应用**时，或保存并编辑网络配置文件后，已上载的 IP 地址将显示在 **IP 地址** 页面上。

- 4 单击 **IP 地址** 选项卡，显示指定网络范围的 IP 地址。

- 5 （可选）从**网络范围**下拉菜单中选择 IP 地址信息，以筛选 IP 地址条目。

可以显示有关所有定义的网络范围、从 CSV 文件导入的网络范围或指定网络范围的信息。详细信息包括起始 IP 地址、计算机名称、上次修改时间和时间戳以及 IP 状态。

- 6 （可选）从 **IP 状态** 下拉菜单中选择状态类型，以筛选 IP 地址条目，只显示符合选定 IP 状态的条目。状态设置有“已分配”、“未分配”、“已销毁”与“已过期”。

对于状态为已过期或已销毁的 IP 地址，可单击**回收**，使这些 IP 地址范围可用于分配。必须保存配置文件，以使回收生效。地址无法立即回收，因此状态列不会立即从“已过期”或“已销毁”变为“已分配”。

- 7 单击**确定**。

通过销毁已置备的计算机释放 IP 地址

销毁部署时，将删除其 IP 地址。已分配的 IP（如，网络配置文件范围中的 IP）将释放并可用于后续置备。

销毁具有静态 IP 地址的计算机后，其 IP 地址可供其他计算机使用。未使用的地址可能不会立即可用，因为回收静态 IP 地址的过程每 30 分钟运行一次。

如果使用的是第三方 IPAM 提供程序，vRealize Automation 会使用第三方 IPAM 提供程序插件或软件包中的 vRealize Orchestrator 工作流删除关联的 IP 地址。

配置预留和预留策略

vRealize Automation 预留可以定义策略、优先级和配额，以便在置备请求时确定计算机放置。

预留策略将计算机置备限于可用预留的子集。存储预留策略允许蓝图架构师将计算机卷分配到不同的数据存储。

要确保置备成功，预留必须具有足够的可用存储。预留的存储可用性取决于：

- 数据存储/群集上的可用存储量。
- 为该数据存储/群集预留的存储量。
- vRealize Automation 中已分配的存储量。

例如，即使 vCenter Server 具有可供数据存储/群集使用的存储，如果未在预留中预留足够的存储，则置备仍会失败，并且显示“没有可分配的预留...”错误。预留上分配的存储取决于该特定预留上的虚拟机数量（无论处于何种状态）。有关详细信息，请参见 VMware 知识库文章《计算机 XXX：组 XXX 中没有可分配的预留。请求的存储总量为 XX GB (2151030)》，网址为 <http://kb.vmware.com/kb/2151030>。

预留

您可以创建 vRealize Automation 预留，将架构组中的置备资源分配到特定的业务组。

例如，您可以使用预留来指定单个计算资源中一定份额的内存、CPU、网络 and 存储资源属于某特定业务组或者分配到某特定业务组的特定计算机。

使用网络预留策略来管理蓝图部署的网络通信。请求计算机置备时，系统将使用预留策略对可以考虑部署的预留进行分组。

无法在多个业务组中共享预留。

注 在 vRealize Automation 中执行“销毁”操作删除已置备的计算机时，通过预留分配给该计算机的存储和内存将会被释放。如果在 vCenter Server 中删除该计算机，存储和内存将不会被释放。

您可以为下列计算机类型创建预留：

- vSphere
- vCloud Air
- vCloud Director
- Amazon EC2
- Microsoft Azure
- Hyper V (SCVMM)
- Hyper-V 独立
- KVM (RHEV)
- OpenStack
- XenServer

您可以通过在预留、蓝图或客户机代理脚本中指定信息来配置安全设置。如果要置备的计算机需要客户机代理，您必须将包含该要求的安全规则添加到预留或蓝图。例如，如果您使用拒绝所有计算机之间的通信的默认安全策略，并依赖不同的安全策略以允许特定计算机之间的通信，则客户机代理在自定义阶段可能无法与 vRealize Automation 通信。要避免在计算机置备期间出现此问题，请使用允许在自定义阶段进行通信的默认安全策略。

选择预留场景

您可以创建预留，将资源分配给业务组。根据您的场景，创建预留的步骤会有所不同。

根据目标端点类型选择预留场景。

每个业务组必须至少为其成员提供一个置备该类计算机的预留。例如，具有 OpenStack 预留、但无 Amazon 预留的业务组无法从 Amazon 请求计算机。在此示例中，必须为业务组分配专门针对 Amazon 资源的预留。

表 2-15. 选择预留场景

方案	步骤
创建 vSphere 预留。	为 Hyper-V 、 KVM 、 SCVMM 、 vSphere 或 XenServer 创建预留
创建预留以便为 vCloud Air 端点分配资源。	创建 vCloud Air 预留
创建预留以便为 vCloud Director 端点分配资源。	创建 vCloud Director 预留
创建预留以便分配 Amazon 资源上的资源（使用或不使用 Amazon 虚拟私有云）。	创建 Amazon EC2 预留
创建预留以便分配 OpenStack 资源上的资源。	创建 OpenStack 预留
创建预留以便为 Hyper-V 分配资源。	为 Hyper-V 、 KVM 、 SCVMM 、 vSphere 或 XenServer 创建预留
创建预留以便为 KVM 分配资源。	为 Hyper-V 、 KVM 、 SCVMM 、 vSphere 或 XenServer 创建预留
创建预留以便分配 OpenStack 资源上的资源。	创建 OpenStack 预留
创建预留以便为 SCVMM 分配资源。	为 Hyper-V 、 KVM 、 SCVMM 、 vSphere 或 XenServer 创建预留
创建预留以便为 XenServer 分配资源。	为 Hyper-V 、 KVM 、 SCVMM 、 vSphere 或 XenServer 创建预留
创建预留以便为 Microsoft Azure 分配资源。	创建 Microsoft Azure 预留

创建云类别预留

云类别类型预留给特定的 vRealize Automation 业务组提供云服务帐户置备服务的访问权限。可用的云预留类型包括 Amazon、OpenStack、vCloud Air 和 vCloud Director。

预留是指共享分配到特定 vRealize Automation 业务组的某种计算资源，包括内存、CPU、网络 and 存储资源。

业务组既可以在一个端点上具有多个预留，也可以在多个端点上具有多个预留。

预留的分配模型取决于关联数据中心内的分配模型。可用的分配模型为“分配池”、“即用即付”和“预留池”。有关分配模型的信息，请参见 vCloud Director 或 vCloud Air 文档。

除了定义分配给业务组的架构资源共享外，预留还可以定义确定计算机放置位置的策略、优先级和配额。

要确保置备成功，预留必须具有足够的可用存储。预留的存储可用性取决于：

- 数据存储/群集上的可用存储量。
- 为该数据存储/群集预留的存储量。
- vRealize Automation 中已分配的存储量。

例如，即使 vCenter Server 具有可供数据存储/群集使用的存储，如果未在预留中预留足够的存储，则置备仍会失败，并且显示“没有可分配的预留...”错误。预留上分配的存储取决于该特定预留上的虚拟机数量（无论处于何种状态）。有关详细信息，请参见 VMware 知识库文章《计算机 XXX：组 XXX 中没有可分配的预留。请求的存储总量为 XX GB (2151030)》，网址为 <http://kb.vmware.com/kb/2151030>。

了解云预留的选择逻辑

当业务组成员为云计算机创建置备请求时，vRealize Automation 将从可用于该业务组的预留之一中选择计算机。云预留包括 Amazon、OpenStack、vCloud Air 和 vCloud Director。

为其置备计算机的预留必须满足以下条件：

- 该预留的平台类型必须与从中请求计算机的蓝图相同。
- 该预留必须已启用。
- 该预留必须在其计算机配额中有剩余容量或者具有无限配额。

分配的计算机配额仅包括已打开电源的计算机。例如，如果预留的配额为 50 台计算机且已置备 40 台，但其中只有 20 台已打开电源，则该预留的配额已分配 40%，而不是 80%。

- 该预留必须在计算机请求中指定安全组。
- 该预留必须与蓝图中指定计算机映像的区域关联。
- 该预留必须具有足够的未分配内存和存储资源来置备计算机。

在“即用即付”预留中，资源可以无限制。

- 对于 Amazon 计算机，该请求指定可用性区域，以及系统是在 Virtual Private Cloud (VPC) 位置还是在非 VPC 位置为该计算机置备子网。该预留必须与网络类型（VPC 或非 VPC）匹配。
- 对于 vCloud Air 或 vCloud Director，如果该请求指定一个分配模型，则与该预留关联的虚拟数据中心均必须具有相同的分配模型。
- 对于 vCloud Director 或 vCloud Air，必须启用指定的组织。
- 任何蓝图模板均必须在该预留中可用。如果预留策略映射到多个资源，则上述模板应为公用模板。
- 如果云提供程序支持网络选择，且蓝图具有特定的网络设置，则该预留必须具有相同的网络。

如果蓝图或预留为静态 IP 地址分配指定网络配置文件，则 IP 地址必须可以分配给新计算机。

- 如果该请求指定分配模型，则该预留中的分配模型必须与请求中的分配模型匹配。
- 如果蓝图指定预留策略，则该预留必须属于此预留策略。

对于从特定蓝图中置备计算机，预留策略是一种可保证所选预留满足其任何附加要求的一种方式。例如，如果蓝图使用特定的计算机映像，则您可以使用预留策略将置备限制为与具有所需映像的区域关联的预留。

如果任何预留均不满足所有选择标准，则置备将会失败。

如果多个预留满足所有条件，则置备请求计算机所使用的预留取决于以下逻辑：

- 先选择优先级值较低的预留，之后再选择优先级值较高的预留。
- 如果多个预留具有相同的优先级，则选择分配的计算机配额比例最低的预留。
- 如果多个预留具有相同的优先级和配额使用量，则系统以循环方式将计算机分布在各预留之间。

注 尽管不支持以循环方式选择网络配置文件，但是支持以循环方式选择网络（如果有），它可以与不同的网络配置文件相关联。

如果一个预留上具有多条存储路径，且具有足够的容量来置备计算机卷，则系统将根据以下逻辑选择存储路径。

- 先选择优先级值较低的存储路径，之后再选择优先级值较高的存储路径。
- 如果蓝图或请求指定存储预留策略，则存储路径必须属于该存储预留策略。

如果将自定义属性 `VirtualMachine.DiskN.StorageReservationPolicyMode` 设置为“Not Exact”，并且存储预留策略中未提供足够的容量，则会使用指定存储预留策略外部的存储路径继续进行置备。`VirtualMachine.DiskN.StorageReservationPolicyMode` 的默认值为“Exact”。

- 如果多条存储路径具有相同的优先级，则系统将使用循环调度将计算机分布在各存储路径之间。

创建 Amazon EC2 预留

您必须先通过创建预留将资源分配给计算机，然后业务组的成员才能请求计算机置备。

可以对 Amazon Virtual Private Cloud 或 Amazon 的非 VPC 使用 Amazon 预留。Amazon Web Services 用户可以创建 Amazon Virtual Private Cloud，根据规范设计虚拟网络拓扑。如果计划使用 Amazon VPC，则必须将 Amazon VPC 分配给 vRealize Automation 预留。

在蓝图中创建 Amazon 预留或配置计算机组件时，您可以从指定的 Amazon 区域可用的安全组列表中进行选择。安全组是在数据收集期间导入的。

注 创建预留后，您无法更改业务组或计算资源关联。

有关使用 AWS Management Console 创建 Amazon VPC 的信息，请参见 Amazon Web Services 文档。

步骤

1 指定 Amazon 预留信息

每个预留均针对特定的业务组配置，以授权其访问指定计算资源上的请求计算机。

2 为 Amazon 预留指定资源和网络设置

指定用于通过此 vRealize Automation 预留置备计算机的资源和网络设置。

3 为 Amazon 预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

指定 Amazon 预留信息

每个预留均针对特定的业务组配置，以授权其访问指定计算资源上的请求计算机。

注 创建预留后，您无法更改业务组或计算资源关联。

在添加、编辑或删除预留时，可以在“预留”页面上使用**按类别筛选**选项来控制预留的显示。请注意，在按类别进行筛选时，测试代理预留不会显示在预留列表中。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 确认租户管理员至少已创建一个业务组。
- 确认已存在一个计算资源。
- 配置网络设置。
- （可选）配置网络配置文件信息。
- 确认您有权访问所需的 Amazon 网络。例如，如果要使用 VPC，请确认您有权访问 Amazon 虚拟私有云 (Amazon Virtual Private Cloud, VPC) 网络。
- 确认存在任何所需的密钥对。请参见[管理密钥对](#)。

步骤

1 选择**基础架构 > 预留 > 预留**。

2 单击**新建**图标 (+)，并选择要创建的预留类型。

选择 **Amazon EC2**。

3 在**名称**文本框中输入名称。

4 从**租户**下拉菜单中选择租户。

5 从**业务组**下拉菜单中选择业务组。

只有此业务组中的用户才能使用此预留置备计算机。

6 （可选）从**预留策略**下拉菜单中选择预留策略。

此选项要求存在一个或多个预留策略。稍后，您可以编辑预留或指定预留策略。

您可以使用预留策略将置备限制为特定的预留。

7 在**优先级**文本框中输入一个数字，设置预留的优先级。

当一个业务组具有多个预留时，系统将使用优先级。优先级为 1 的预留比优先级为 2 的预留先用于置备。

8 （可选）如果不想此预留处于活动状态，请取消选中**启用此预留**复选框。

结果

请勿导航离开此页面。您的预留尚未完成。

为 Amazon 预留指定资源和网络设置

指定用于通过此 vRealize Automation 预留置备计算机的资源和网络设置。

在蓝图中创建 Amazon 预留或配置计算机组件时，您可以从指定的 Amazon 帐户区域可用的安全组列表中进行选择。安全组是在数据收集期间导入的。安全组充当控制计算机访问的防火墙。每个区域至少包括默认安全组。管理员可以使用 Amazon Web Services Management Console 创建其他安全组，配置 Microsoft Remote Desktop Protocol 或 SSH 的端口，并设置 Amazon VPN 的虚拟专用网络。有关在 Amazon Web Services 中创建和使用安全组的信息，请参见 Amazon 文档。

有关负载均衡器的相关信息，请参见《配置 vRealize Automation》。

前提条件

指定 Amazon 预留信息。

步骤

- 1 单击**资源**选项卡。
- 2 从**计算资源**下拉菜单中，选择置备计算机要使用的计算资源。
列出了可用的 Amazon 区域。
- 3 （可选）在**计算机配额**文本框中输入一个数字，设置可以在此预留中置备的最大计算机数量。
只有已打开电源的计算机才会计入配额。留空将使预留无限制。
- 4 从**密钥对**下拉菜单中选择密钥对分配给计算实例的方法。

选项	描述
未指定	控制蓝图级别（而非预留级别）的密钥对行为。
根据业务组自动生成	同一业务组中置备的所有计算机均具有相同的密钥对，其中包括当该计算机具有相同的计算资源和业务组时在其他预留上置备的计算机。由于通过此方式生成的密钥对与业务组关联，因此删除业务组时这些密钥对也会随之删除。
根据计算机自动生成	每台计算机拥有唯一的密钥对。这是一种最安全的方法，因为密钥对不在计算机之间共享。
特定密钥对	此预留上置备的所有计算机均具有相同的密钥对。浏览此预留要使用的密钥对。

- 5 如果已在**密钥对**下拉菜单中选择**特定密钥对**，请从**特定密钥对**下拉菜单中选择密钥对值。
- 6 如果已配置用于 Amazon 虚拟私有云，请启用**分配到 VPC 的子网**中复选框。否则，不选中此框。
如果选择**分配到 VPC 的子网**中，则以下位置或子网、安全组以及负载均衡器选项将显示在弹出菜单中，而不是同一页面中。
对于 VPC 预留，请为该预留中允许的每个 VPC 指定安全组和子网。
- 7 从**位置或子网**列表选择一个或多个可用位置（非 VPC）或子网 (VPC)。
选择您希望可用于置备的每个可用位置或子网。

- 8 从**安全组**列表选择一个或多个可在置备期间分配给计算机的安全组。

选择可在置备期间分配给计算机的每个安全组。每个可用区域至少需要一个指定的安全组。

- 9 从**负载均衡器**列表选择一个或多个可用的负载均衡器。

如果使用弹性负载均衡器功能，请选择一个或多个应用于选定位置或子网的可用负载均衡器。

结果

现在，您通过单击**保存**即可保存预留。或者，您可以添加自定义属性，进一步控制预留规范。您也可以对电子邮件警示进行配置，使其在分配给此预留的资源不足时发送通知。

为 **Amazon** 预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

自定义属性和电子邮件警示是预留的可选配置。如果不想关联自定义属性或设置警示，请单击**保存**完成预留的创建。

您可以根据自身需要添加任意数量的自定义属性。

若已配置，系统将每天生成警示，而不是在达到指定阈值时生成。

重要事项 仅当已配置电子邮件警示且已启用通知时，系统才会发送通知。

前提条件

为 **Amazon** 预留指定资源和网络设置。

步骤

- 1 单击**属性**选项卡。
- 2 单击**新建**。
- 3 输入有效的自定义属性名称。
- 4 如果适用，请输入属性值。
- 5 单击**保存**。
- 6 （可选）添加任何其他自定义属性。
- 7 单击**警示**选项卡。
- 8 启用**容量警示**复选框，配置要发送的警示。
- 9 使用滑块设置可用资源分配的阈值。
- 10 在**收件人**文本框中输入 AD 用户或组名称（而不是电子邮件地址）以接收警示通知。
在每一行输入一个名称。按 **Enter** 分隔多个条目。
- 11 选择**向组主管发送警示**，将组主管包括在电子邮件警示中。
电子邮件警示将发送到业务组**发送主管电子邮件**至列表中包括的用户。
- 12 指定提醒频率（天）。

13 单击保存。

结果

该预留已保存并显示在“预留”列表中。

后续步骤

您可以配置可选预留策略或开始准备进行置备。

现在，有权创建蓝图的用户可以创建蓝图。

创建 OpenStack 预留

您必须先通过创建预留将资源分配给计算机，然后业务组的成员才能请求计算机置备。

创建 OpenStack 预留。

步骤

1 指定 OpenStack 预留信息

每个预留均针对特定的业务组配置，以授权其访问指定计算资源上的请求计算机。

2 为 OpenStack 预留指定资源和网络设置

指定通过此 vRealize Automation 预留置备的计算机可用的资源和网络设置。

3 为 OpenStack 预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

指定 OpenStack 预留信息

每个预留均针对特定的业务组配置，以授权其访问指定计算资源上的请求计算机。

注 创建预留后，您无法更改业务组或计算资源关联。

在添加、编辑或删除预留时，可以在“预留”页面上使用**按类别筛选**选项来控制预留的显示。请注意，在按类别进行筛选时，测试代理预留不会显示在预留列表中。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 确认租户管理员至少已创建一个业务组。
- 确认已存在一个计算资源。
- 确认已配置任何可选的安全组或浮点 IP 地址。
- 确认存在任何所需的密钥对。请参见[管理密钥对](#)。
- 确认已存在一个计算资源。
- 配置网络设置。

步骤

1 选择**基础架构 > 预留 > 预留**。

2 单击**新建**图标 (+)，并选择要创建的预留类型。

选择 **OpenStack**。

3 在**名称**文本框中输入名称。

4 从**租户**下拉菜单中选择租户。

5 从**业务组**下拉菜单中选择业务组。

只有此业务组中的用户才能使用此预留置备计算机。

6 (可选) 从**预留策略**下拉菜单中选择预留策略。

此选项要求存在一个或多个预留策略。稍后，您可以编辑预留或指定预留策略。

您可以使用预留策略将置备限制为特定的预留。

7 在**优先级**文本框中输入一个数字，设置预留的优先级。

当一个业务组具有多个预留时，系统将使用优先级。优先级为 1 的预留比优先级为 2 的预留先用于置备。

8 (可选) 如果不想此预留处于活动状态，请取消选中**启用此预留**复选框。

结果

请勿导航离开此页面。您的预留尚未完成。

为 OpenStack 预留指定资源和网络设置

指定通过此 vRealize Automation 预留置备的计算机可用的资源和网络设置。

前提条件

[指定 OpenStack 预留信息](#)。

步骤

1 单击**资源**选项卡。

2 从**计算资源**下拉菜单中，选择置备计算机要使用的计算资源。

只有位于所选群集中的模板才能使用此预留进行克隆。

置备期间，计算机将置于连接到本地存储的主机上。如果预留使用本地存储，则预留置备的所有计算机会在包含该本地存储的主机上进行创建。但是，如果使用 **VirtualMachine.Admin.ForceHost** 自定义属性，该属性强制计算机置备到其他主机，则置备会失败。如果克隆计算机的模板位于本地存储，但是将该模板连接到其他群集上的计算机，则置备也会失败。在这种情况下，置备由于无法访问模板而失败。

3 (可选) 在**计算机配额**文本框中输入一个数字，设置可以在此预留中置备的最大计算机数量。

只有已打开电源的计算机才会计入配额。留空将使预留无限制。

4 从密钥对下拉菜单中选择密钥对分配给计算实例的方法。

选项	描述
未指定	控制蓝图级别（而非预留级别）的密钥对行为。
根据业务组自动生成	同一业务组中置备的所有计算机均具有相同的密钥对，其中包括当该计算机具有相同的计算资源和业务组时在其他预留上置备的计算机。由于通过此方式生成的密钥对与业务组关联，因此删除业务组时这些密钥对也会随之删除。
根据计算机自动生成	每台计算机拥有唯一的密钥对。这是一种最安全的方法，因为密钥对不在计算机之间共享。
特定密钥对	此预留上置备的所有计算机均具有相同的密钥对。浏览此预留要使用的密钥对。

5 如果已在**密钥对**下拉菜单中选择**特定密钥对**，请从**特定密钥对**下拉菜单中选择密钥对值。

6 从**安全组**列表选择一个或多个可在置备期间分配给计算机的安全组。

7 单击**网络**选项卡。

8 为通过使用此预留置备的计算机配置网络路径。

a （可选）如果选项可用，从**端点**下拉菜单中选择存储端点。

如果 NetApp ONTAP 端点存在且主机为虚拟主机，则 FlexClone 选项在端点列中可见。如果存在 NetApp ONTAP 端点，则预留页面将显示分配给存储路径的端点。为存储路径添加、更新或删除端点时，您所做的更改在所有适用的预留中可见。

为存储路径添加、更新或删除端点时，您所做的更改在预留页面中可见。

b 为将要为此预留置备的计算机选择一个或多个**网络适配器**。

c （可选）为每个选定的网络适配器选择可用的**的网络配置文件**。

d （可选）如果高级设置可用，请选择**传输区域**和部署包含负载均衡器的蓝图时要使用的一个或多个**第 0 层逻辑路由器**。

传输区域定义网络适配器跨哪些群集。如果在预留和蓝图中指定传输区域，传输区域值必须匹配。

您可以在预留中选择多个网络适配器，但置备计算机时只使用一个网络。

结果

现在，您通过单击**保存**即可保存预留。或者，您可以添加自定义属性，进一步控制预留规范。您也可以对电子邮件警示进行配置，使其在分配给此预留的资源不足时发送通知。

为 OpenStack 预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

自定义属性和电子邮件警示是预留的可选配置。如果不想关联自定义属性或设置警示，请单击**保存**完成预留的创建。

您可以根据自身需要添加任意数量的自定义属性。

重要事项 仅当已配置电子邮件警示且已启用通知时，系统才会发送通知。

若已配置，系统将每天生成警示，而不是在达到指定阈值时生成。

前提条件

为 [OpenStack](#) 预留指定资源和网络设置。

步骤

- 1 单击**属性**选项卡。
- 2 单击**新建**。
- 3 输入有效的自定义属性名称。
- 4 如果适用，请输入属性值。
- 5 单击**保存**。
- 6 （可选）添加任何其他自定义属性。
- 7 单击**警示**选项卡。
- 8 启用**容量警示**复选框，配置要发送的警示。
- 9 使用滑块设置可用资源分配的阈值。
- 10 在**收件人**文本框中输入 AD 用户或组名称（而不是电子邮件地址）以接收警示通知。
在每一行输入一个名称。按 **Enter** 分隔多个条目。
- 11 选择**向组主管发送警示**，将组主管包括在电子邮件警示中。
电子邮件警示将发送到业务组**发送主管电子邮件**至列表中包括的用户。
- 12 指定提醒频率（天）。
- 13 单击**保存**。

结果

该预留已保存并显示在“预留”列表中。

后续步骤

您可以配置可选预留策略或开始准备进行置备。

现在，有权创建蓝图的用户可以创建蓝图。

创建 vCloud Air 预留

您必须先通过创建 vRealize Automation 预留将资源分配给计算机，然后业务组的成员才能请求计算机置备。

每个业务组必须至少为其成员提供一个置备该类计算机的预留。

步骤

1 指定 vCloud Air 预留信息

您可以为每个 vCloud Air 计算机订阅或 OnDemand 资源创建预留。每个预留均针对特定的业务组配置，以授权其访问请求的计算机。

2 为 vCloud Air 预留指定资源和网络设置

指定通过此 vRealize Automation 预留置备的 vCloud Air 计算机可用的资源和网络设置。

3 为 vCloud Air 预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

指定 vCloud Air 预留信息

您可以为每个 vCloud Air 计算机订阅或 OnDemand 资源创建预留。每个预留均针对特定的业务组配置，以授权其访问请求的计算机。

在添加、编辑或删除预留时，可以在“预留”页面上使用[按类别筛选](#)选项来控制预留的显示。请注意，在按类别进行筛选时，测试代理预留不会显示在预留列表中。

注 创建预留后，您无法更改业务组或计算资源关联。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 确认租户管理员至少已创建一个业务组。
- 确认已存在一个计算资源。
- 配置网络设置。
- （可选）配置网络配置文件信息。

步骤

1 选择**基础架构 > 预留 > 预留**。

2 单击**新建**图标 (+)，并选择要创建的预留类型。

可用的云预留类型为 Amazon、OpenStack、vCloud Air 和 vCloud Director。

选择 **vCloud Air**。

3 在**名称**文本框中输入名称。

4 从**租户**下拉菜单中选择租户。

5 从**业务组**下拉菜单中选择业务组。

只有此业务组中的用户才能使用此预留置备计算机。

6 （可选）从**预留策略**下拉菜单中选择预留策略。

此选项要求存在一个或多个预留策略。稍后，您可以编辑预留或指定预留策略。

您可以使用预留策略将置备限制为特定的预留。

7 在**优先级**文本框中输入一个数字，设置预留的优先级。

当一个业务组具有多个预留时，系统将使用优先级。优先级为 1 的预留比优先级为 2 的预留先用于置备。

8 （可选）如果不想此预留处于活动状态，请取消选中**启用此预留**复选框。**结果**

请勿导航离开此页面。您的预留尚未完成。

为 vCloud Air 预留指定资源和网络设置

指定通过此 vRealize Automation 预留置备的 vCloud Air 计算机可用的资源和网络设置。

通过 vCloud Director 预留置备的计算机可用的资源分配模型包括“分配池”、“即用即付”和“预留池”。对于“即用即付”，您不必指定存储量或内存量，但需要指定存储路径的优先级。有关这些分配模型的详细信息，请参见 vCloud Air 文档。

您可以指定标准或磁盘级别的存储配置文件。多级磁盘存储是可用的 vCloud Air 端点。

对于使用 Storage Distributed Resource Scheduler (SDRS) 存储的集成，您可以选择存储群集，允许 SDRS 自动为通过此预留置备的计算机处理存储放置和负载平衡。SDRS 自动化模式必须设置为“自动”。否则，在该群集内针对独立数据存储行为选择数据存储。FlexClone 存储设备不支持 SDRS。

注 为 vCloud Air 端点和 vCloud Director 端点定义的预留不支持使用网络配置文件来置备计算机。

前提条件

指定 [vCloud Director 预留信息](#)。

步骤**1** 单击**资源**选项卡。**2** 从**计算资源**下拉菜单中，选择置备计算机要使用的计算资源。

只有位于所选群集中的模板才能使用此预留进行克隆。

3 选择分配模型。**4** （可选）在**计算机配额**文本框中输入一个数字，设置可以在此预留中置备的最大计算机数量。

只有已打开电源的计算机才会计入配额。留空将使预留无限制。

5 从“内存”表中指定要分配给此预留的内存量 (GB)。

该预留的内存总量值是从您选择的计算资源中派生得出的。

6 选择列出的一个或多个存储路径。

可用的存储路径选项是从您的计算资源选择中派生得出的。

- a 在**已预留此预留**文本框中输入一个值，指定要分配给此预留的存储量。
- b 在**优先级**文本框中输入一个值，指定存储路径相对于与此预留有关的其他路径存储的优先级值。
该优先级用于多个存储路径。优先级为 0 的存储路径比优先级为 1 的路径优先使用。
- c 如果不想启用此预留使用的存储路径，请单击**禁用**选项。
- d 重复此步骤，根据需要配置群集和数据存储。

7 单击**网络**选项卡。**8** 为通过使用此预留置备的计算机配置网络路径。

- a （可选）如果选项可用，从**端点**下拉菜单中选择存储端点。

如果 NetApp ONTAP 端点存在且主机为虚拟主机，则 FlexClone 选项在端点列中可见。如果存在 NetApp ONTAP 端点，则预留页面将显示分配给存储路径的端点。为存储路径添加、更新或删除端点时，您所做的更改在所有适用的预留中可见。

为存储路径添加、更新或删除端点时，您所做的更改在预留页面中可见。

- b 为将要为此预留置备的计算机选择一个或多个**网络适配器**。
- c （可选）为每个选定的网络适配器选择可用的**的网络配置文件**。
- d （可选）如果高级设置可用，请选择**传输区域**和部署包含负载平衡器的蓝图时要使用的一个或多个**第 0 层逻辑路由器**。

传输区域定义网络适配器跨哪些群集。如果在预留和蓝图中指定传输区域，传输区域值必须匹配。您可以在预留中选择多个网络适配器，但置备计算机时只使用一个网络。

结果

现在，您通过单击**保存**即可保存预留。或者，您可以添加自定义属性，进一步控制预留规范。您也可以对电子邮件警示进行配置，使其在分配给此预留的资源不足时发送通知。

为 vCloud Air 预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

自定义属性和电子邮件警示是预留的可选配置。如果不想关联自定义属性或设置警示，请单击**保存**完成预留的创建。

您可以根据自身需要添加任意数量的自定义属性。

若已配置，系统将每天生成警示，而不是在达到指定阈值时生成。

重要事项 仅当已配置电子邮件警示且已启用通知时，系统才会发送通知。

对于在未指定限制的情况下创建的“即用即付”预留，警示不可用。

前提条件

为 [vCloud Air](#) 预留指定资源和网络设置

步骤

- 1 单击**属性**选项卡。
- 2 单击**新建**。
- 3 输入有效的自定义属性名称。
- 4 如果适用，请输入属性值。
- 5 （可选）选中**已加密**复选框，对属性值进行加密。
- 6 （可选）选中**提示用户**复选框，要求用户输入值。
在进行置备时，此选项无法替代。
- 7 单击**保存**。
- 8 （可选）添加任何其他自定义属性。
- 9 单击**警示**选项卡。
- 10 启用**容量警示**复选框，配置要发送的警示。
- 11 使用滑块设置可用资源分配的阈值。
- 12 在**收件人**文本框中输入 AD 用户或组名称（而不是电子邮件地址）以接收警示通知。
在每一行输入一个名称。按 **Enter** 分隔多个条目。
- 13 选择**向组主管发送警示**，将组主管包括在电子邮件警示中。
电子邮件警示将发送到业务组**发送主管电子邮件至**列表中包括的用户。
- 14 指定提醒频率（天）。
- 15 单击**保存**。

结果

该预留已保存并显示在“预留”列表中。

创建 vCloud Director 预留

您必须先通过创建 **vRealize Automation** 预留将资源分配给计算机，然后业务组的成员才能请求计算机置备。

每个业务组必须至少为其成员提供一个置备该类计算机的预留。

步骤**1 指定 vCloud Director 预留信息**

您可以为每个 vCloud Director 组织虚拟数据中心 (VDC) 创建预留。每个预留均针对特定的业务组配置，以授权其访问指定计算资源上的请求计算机。

2 为 vCloud Director 预留指定资源和网络设置

指定通过此 vRealize Automation 预留置备的 vCloud Director 计算机可用的资源和网络设置。

3 为 vCloud Director 预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

后续步骤

您可以配置可选预留策略或开始准备进行置备。

现在，有权创建蓝图的用户可以创建蓝图。

指定 vCloud Director 预留信息

您可以为每个 vCloud Director 组织虚拟数据中心 (VDC) 创建预留。每个预留均针对特定的业务组配置，以授权其访问指定计算资源上的请求计算机。

在添加、编辑或删除预留时，可以在“预留”页面上使用**按类别筛选**选项来控制预留的显示。请注意，在按类别进行筛选时，测试代理预留不会显示在预留列表中。

注 创建预留后，您无法更改业务组或计算资源关联。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 确认租户管理员至少已创建一个业务组。
- 确认已存在一个计算资源。
- 配置网络设置。
- （可选）配置网络配置文件信息。

步骤

1 选择**基础架构 > 预留 > 预留**。

2 单击**新建**图标 (+)，并选择要创建的预留类型。

可用的云预留类型为 Amazon、OpenStack、vCloud Air 和 vCloud Director。

选择 **vCloud Director**。

3 在**名称**文本框中输入名称。

4 从**租户**下拉菜单中选择租户。

5 从**业务组**下拉菜单中选择业务组。

只有此业务组中的用户才能使用此预留置备计算机。

6 （可选）从**预留策略**下拉菜单中选择预留策略。

此选项要求存在一个或多个预留策略。稍后，您可以编辑预留或指定预留策略。

您可以使用预留策略将置备限制为特定的预留。

- 7 在**优先级**文本框中输入一个数字，设置预留的优先级。

当一个业务组具有多个预留时，系统将使用优先级。优先级为 1 的预留比优先级为 2 的预留先用于置备。

- 8 （可选） 如果不想此预留处于活动状态，请取消选中**启用此预留**复选框。

结果

请勿导航离开此页面。您的预留尚未完成。

为 vCloud Director 预留指定资源和网络设置

指定通过此 vRealize Automation 预留置备的 vCloud Director 计算机可用的资源和网络设置。

通过 vCloud Director 预留置备的计算机可用的资源分配模型包括“分配池”、“即用即付”和“预留池”。对于“即用即付”，您不必指定存储量或内存量，但需要指定存储路径的优先级。有关这些分配模型的详细信息，请参见 vCloud Director 文档。

您可以指定标准或磁盘级别的存储配置文件。多级磁盘存储适用于 vCloud Director 5.6 及更高版本的端点。vCloud Director 5.5 端点不支持多级磁盘存储。

对于使用 Storage Distributed Resource Scheduler (SDRS) 存储的集成，您可以选择存储群集，允许 SDRS 自动为通过此预留置备的计算机处理存储放置和负载平衡。SDRS 自动化模式必须设置为“自动”。否则，在该群集内针对独立数据存储行为选择数据存储。FlexClone 存储设备不支持 SDRS。

注 为 vCloud Air 端点和 vCloud Director 端点定义的预留不支持使用网络配置文件来置备计算机。

前提条件

指定 [vCloud Director 预留信息](#)。

步骤

- 1 单击**资源**选项卡。
- 2 从**计算资源**下拉菜单中，选择置备计算机要使用的计算资源。
只有位于所选群集中的模板才能使用此预留进行克隆。
- 3 选择分配模型。
- 4 （可选） 在**计算机配额**文本框中输入一个数字，设置可以在此预留中置备的最大计算机数量。
只有已打开电源的计算机才会计入配额。留空将使预留无限制。
- 5 从“内存”表中指定要分配给此预留的内存量 (GB)。
该预留的内存总量值是从您选择的计算资源中派生得出的。
- 6 选择列出的一个或多个存储路径。
可用的存储路径选项是从您的计算资源选择中派生得出的。
 - a 在**已预留此预留**文本框中输入一个值，指定要分配给此预留的存储量。
 - b 在**优先级**文本框中输入一个值，指定存储路径相对于与此预留有关的其他路径存储的优先级值。
该优先级用于多个存储路径。优先级为 0 的存储路径比优先级为 1 的路径优先使用。

- c 如果不想启用此预留使用的存储路径，请单击**禁用**选项。
- d 重复此步骤，根据需要配置群集和数据存储。

7 单击**网络**选项卡。

8 为通过使用此预留置备的计算机配置网络路径。

- a （可选）如果选项可用，从**端点**下拉菜单中选择存储端点。

如果 NetApp ONTAP 端点存在且主机为虚拟主机，则 FlexClone 选项在端点列中可见。如果存在 NetApp ONTAP 端点，则预留页面将显示分配给存储路径的端点。为存储路径添加、更新或删除端点时，您所做的更改在所有适用的预留中可见。

为存储路径添加、更新或删除端点时，您所做的更改在预留页面中可见。

- b 为将要为此预留置备的计算机选择一个或多个**网络适配器**。
- c （可选）为每个选定的网络适配器选择可用的**的网络配置文件**。
- d （可选）如果高级设置可用，请选择**传输区域**和部署包含负载均衡器的蓝图时要使用的一个或多个**第 0 层逻辑路由器**。

传输区域定义网络适配器跨哪些群集。如果在预留和蓝图中指定传输区域，传输区域值必须匹配。您可以在预留中选择多个网络适配器，但置备计算机时只使用一个网络。

结果

现在，您通过单击**保存**即可保存预留。或者，您可以添加自定义属性，进一步控制预留规范。您也可以对电子邮件警示进行配置，使其在分配给此预留的资源不足时发送通知。

为 vCloud Director 预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

自定义属性和电子邮件警示是预留的可选配置。如果不想关联自定义属性或设置警示，请单击**保存**完成预留的创建。

您可以根据自身需要添加任意数量的自定义属性。

若已配置，系统将每天生成警示，而不是在达到指定阈值时生成。

重要事项 仅当已配置电子邮件警示且已启用通知时，系统才会发送通知。

对于在未指定限制的情况下创建的“即用即付”预留，警示不可用。

前提条件

为 vCloud Director 预留指定资源和网络设置。

步骤

- 1 单击**属性**选项卡。
- 2 单击**新建**。
- 3 输入有效的自定义属性名称。

- 4 如果适用，请输入属性值。
- 5 （可选）选中**已加密**复选框，对属性值进行加密。
- 6 （可选）选中**提示用户**复选框，要求用户输入值。
在进行置备时，此选项无法替代。
- 7 单击**保存**。
- 8 （可选）添加任何其他自定义属性。
- 9 单击**警示**选项卡。
- 10 启用**容量警示**复选框，配置要发送的警示。
- 11 使用滑块设置可用资源分配的阈值。
- 12 在**收件人**文本框中输入 AD 用户或组名称（而不是电子邮件地址）以接收警示通知。
在每一行输入一个名称。按 **Enter** 分隔多个条目。
- 13 选择**向组主管发送警示**，将组主管包括在电子邮件警示中。
电子邮件警示将发送到业务组**发送主管电子邮件至**列表中包括的用户。
- 14 指定提醒频率（天）。
- 15 单击**保存**。

结果

该预留已保存并显示在“预留”列表中。

创建 Microsoft Azure 预留

为特定业务组创建 **Azure** 预留，以授予该组用户权限，使其能够请求特定计算资源上的 **Azure** 虚拟机。

如果部署支持通过 VPN 安全加密链路进行单点登录，则可以使用“属性”选项卡上的设置，通过 **Azure** 虚拟机配置支持此功能。

注 在创建 **Azure** 预留时请忽略“警示”选项卡，因为它不适用。创建预留后，您无法更改业务组关联。此外，与其他计算机类型不同，**Azure** 预留与蓝图之间不存在直接链接。

在添加、编辑或删除预留时，可以在“预留”页面上使用**按类别筛选**选项来控制预留的显示。请注意，在按类别进行筛选时，测试代理预留不会显示在预留列表中。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 确认租户管理员至少已创建一个业务组。
- （可选）配置网络配置文件信息。
- 确认您有权访问任何所需的 **Azure** 资源。
- 确认存在任何所需的密钥对。有关密钥对的信息，请参见《配置 vRealize Automation》。

- 获取与相应 Azure 端点所用订阅 ID 匹配的有效 Azure 订阅 ID。如果使用多个 Azure 订阅，则必须为每个订阅创建预留。
- 如果部署支持通过 VPN 安全加密链路进行单点登录，则必须在创建预留之前配置适当的 VPC 连接。请参见[配置网络-Azure VPC 连接](#)。

步骤

1 配置 Microsoft Azure 预留基本信息

指定 Microsoft Azure 预留的基本信息。

2 配置 Azure 预留资源信息

设置 Azure 预留时，您可以根据所使用的 Azure 实例分配资源组和存储帐户信息。设置预留后，vRealize Automation 置备逻辑会尝试根据置备虚拟机时预留所指定的资源信息分配资源组和存储帐户等资源。

3 配置 Azure 属性

可将自定义属性添加到 Azure 预留以支持 VPN 通道等选项，从而支持多个网络之间的通信。此功能还为添加到蓝图的软件组件提供了便利。

4 配置 Azure 预留网络信息

您可以在预留中为 Azure 虚拟机配置虚拟网络和负载均衡器信息。

配置 Microsoft Azure 预留基本信息

指定 Microsoft Azure 预留的基本信息。

除“预留策略”之外，“预留信息”页面中的所有信息均为必需。后续的 Azure 预留页面上的所有信息都是可选的。

步骤

1 选择基础架构 > 管理 > 预留。

2 单击新建图标 (+)，并选择要创建的预留类型。

选择 **Azure**。

3 在名称文本框中输入名称。

4 从业务组下拉菜单中选择业务组。

只有此业务组中的用户才能使用此预留置备计算机。

5 忽略预留策略文本框，因为不适用于 Azure 预留。

6 在优先级文本框中输入一个数字，设置预留的优先级。

当一个业务组具有多个预留时，系统将使用优先级。优先级为 1 的预留比优先级为 2 的预留先用于置备。

7 （可选） 如果不想此预留处于活动状态，请取消选中启用此预留复选框。

8 单击确定。

配置 Azure 预留资源信息

设置 Azure 预留时，您可以根据所使用的 Azure 实例分配资源组和存储帐户信息。设置预留后，vRealize Automation 置备逻辑会尝试根据置备虚拟机时预留所指定的资源信息分配资源组和存储帐户等资源。

您可以在预留中为 Azure 虚拟机配置资源组和存储帐户信息，但也可以选择将预留中将这些字段留空。如果将这些字段留空，与指定 Azure 订阅 ID 相关的默认资源组和存储帐户信息将用于任何相关蓝图。您还可以在创建蓝图或置备虚拟机时更新这些信息。

前提条件

获取 Azure 实例的订阅 ID。

步骤

- 1 在**订阅 ID** 文本框中输入您的 Azure 订阅 ID。
- 2 通过单击**位置**下拉列表，选择预留对应的位置。

您可以将此字段留空来创建与位置无关的预留，否则，必须在创建蓝图或置备 Azure 虚拟机时指定位置信息。

- 3 单击“资源组”表中的**新建**。

- a 将相应的资源组名称信息从 Azure 实例粘贴到**名称**文本框中。

注 名称框不能为空。

- b 在**优先级**文本框中分配优先级数值。

此分配将在虚拟网络具有多个资源组时确定优先级，较少者优先。

- c 单击**保存**以将资源组添加到预留中。

- 4 单击“存储帐户”表中的**新建**。

- a 将相应的存储帐户名称信息从 Azure 实例粘贴到**名称**文本框中。

注 名称框不能为空。

- b 在**优先级**文本框中分配优先级数值。

- c 单击**保存**以将存储帐户添加到预留中。

此分配将在预留具有多个存储帐户时确定优先级，较少者优先。

- 5 单击**确定**转到下一个选项卡。

配置 Azure 属性

可将自定义属性添加到 Azure 预留以支持 VPN 通道等选项，从而支持多个网络之间的通信。此功能还为添加到蓝图的软件组件提供了便利。

必须创建自定义属性，以定义相应的 URL，从而支持网络上的 VPN 通道。此外，还必须创建一些属性，定义先前下载的 Azure 通道配置脚本路径。

使用 Azure 通道物理计算机和端口 1443 的专用 IP 地址。这是您在调用 SSH 通道时为 `vRealize_automation_appliance_fqdn` 分配的地址。

下表显示支持 VPN 通道所需的名称和属性值。

名称	值
Azure.Windows.ScriptPath	指定已下载的脚本的路径，该脚本将为基于 Windows 系统的配置通道。根据您的部署相应地更新路径。
Azure.Linux.ScriptPath	指定已下载的脚本的路径，该脚本将为基于 Linux 的系统配置通道。根据您的部署相应地更新路径。
agent.download.url	为部署上的 VPN 代理指定 URL。URL 格式为 <code>https://Private_IP:1443/software-service/resources/noble-agent.jar</code>
software.agent.service.url	为部署输入 VPN 软件代理服务的 URL，URL 格式为 <code>https://Private_IP:1443/software-service/api</code>
software.ebs.url	为部署输入事件代理服务 URL。URL 格式为 <code>https://Private_IP:1443/event-broker-service/api</code>

前提条件

- 从 vRealize Automation 设备上的**客户机和软件代理安装程序**页面中，下载 VMware 提供的 Azure 脚本。
 这些脚本安装支持 VPN 通道所需的 Azure 扩展。有两个脚本：`script.ps1` 和 `script.sh`。`.ps1` 文件适用于 Windows 系统，`.sh` 文件适用于 Linux 系统。
 - a 运行 `https://vrealize_automation_设备fqdn/software`，以打开 VMware vRealize Automation 设备页面。
 - b 在“安装 vRealize Automation 组件（IaaS、客户机、软件代理和工具）”标题下，单击**客户机和软件代理**链接。
 - c 在“Azure 计算机”标题下，下载 Azure 脚本文件。将脚本文件保存到适当的位置。配置 Azure 预留自定义属性时，必须指向该位置。

步骤

- 1 单击**属性**选项卡。
- 2 单击**新建**。
- 3 在“属性”对话框中，为自定义属性中输入相应的名称和值。
- 4 创建每个属性时，单击对话框中的**确定**，可添加该属性。
- 5 添加所有必需的属性之后，单击**确定**以保存设置。

后续步骤

创建自定义属性以支持 VPN 通道之后，可以为 Azure 蓝图创建软件组件。有关详细信息，请参见《配置 vRealize Automation》。

为 Azure 设置软件组件时，请在“新建软件”页面上的“容器”下拉列表中选择 **Azure 虚拟机**。

配置 Azure 预留网络信息

您可以在预留中为 **Azure** 虚拟机配置虚拟网络和负载均衡器信息。

您还可以选择将此页面部分或全部留空，并在置备虚拟机时配置虚拟网络和负载均衡器信息。

如果您指定网络配置文件且未指定子网，则指定网络配置文件的第一个现有网络范围的名称将用作子网名称。如果指定了网络配置文件，您可以选择将 **vNet** 文本框留空。在这种情况下，指定网络配置文件的第一个网络范围的名称将用作子网名称，并且 **vNet** 名称将解析为第一个包含适用子网的 **Azure vNet**。

前提条件

从 **Azure** 实例中获取相应的虚拟网络和负载均衡器信息（如果适用）。

步骤

- 1 单击“网络”表中的**新建**，配置要用于虚拟机的相应 **Azure** 虚拟网络。
 - a 将相应的 **vNet** 名称信息从 **Azure** 实例粘贴到 **vNet** 文本框中。
 - b 将相应的子网名称信息从 **Azure** 实例粘贴到**子网**文本框中。
子网规范是可选的。如果将此框留空，默认情况下会使用指定 **vNet** 的子网。
 - c 在**网络配置文件**文本框中，键入或粘贴相应的名称。您可以使用蓝图中的网络配置文件将网卡与网络相关联。
网络配置文件规范是可选的。如果您要根据 **vRealize Automation** 中定义的网络配置文件创建蓝图，而不是将蓝图与 **Azure** 网络结构相结合，请使用此规范。
 - d 在**优先级**文本框中分配优先级数值（如果适用）。
此分配将在虚拟网络具有多个预留时确定优先级，较少者优先。
 - e 单击**保存**以将资源组添加到预留中。
- 2 如果要部署多台计算机并使用负载均衡器，请单击“负载均衡器”表中的**新建**。
 - a 将相应的负载均衡器名称从 **Azure** 实例粘贴到**名称**文本框中。
 - b 将相应的名称从 **Azure** 实例粘贴到**后端地址池**文本框中。
 - c 在**优先级**文本框中分配优先级数值（如果适用）。
此分配将在虚拟网络具有多个负载均衡器时确定优先级，较少者优先。
 - d 单击**保存**以将负载均衡器添加到预留中。
- 3 如果要部署的多台计算机必须通过防火墙进行通信，请单击“安全组”表中的**新建**。
 - a 将安全组名称从 **Azure** 实例粘贴到**名称**文本框中。
 - b 在**优先级**文本框中分配优先级数值（如果适用）。
此分配将在虚拟网络具有多个安全组时确定优先级，较少者优先。
 - c 单击**保存**以将安全组添加到预留中。
- 4 单击**确定**。

场景：为概念证明环境创建 **Amazon** 预留

由于您使用 SSH 通道为概念证明环境暂时建立从网络到 Amazon VPC 连接，因此您必须将自定义属性添加到 Amazon 预留中，确保 Software 引导代理和客户机代理通过该通道运行通信。

仅当您希望使用客户机代理自定义置备的计算机，或者希望将 Software 组件包含在蓝图中时，才需要从网络到 Amazon VPC 的连接。对于生产环境，您需通过 Amazon Web Services 正式配置此连接，但由于您是在概念证明环境中工作，因此您可改为配置暂时的 SSH 通道。

通过使用您的架构管理员特权，您既可以创建一个预留以分配 Amazon Web Services 资源，也可以包括多个自定义属性以支持 SSH 通道。此外，您还可以在与通道计算机相同的区域和 VPC 上配置预留。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 配置 SSH 通道，以建立从网络到 Amazon VPC 连接。记录 Amazon AWS 通道计算机的子网、安全组和专用 IP 地址。请参见[为概念证明环境配置从网络到 Amazon VPC 的连接](#)。
- 为 IT 部门中需要在概念证明环境中架构蓝图的成员创建一个业务组。请参见[创建业务组](#)。
- 确认租户管理员至少已创建一个业务组。

步骤

1 场景：为概念证明环境指定 Amazon AWS 预留信息

您需要为蓝图架构师团队预留资源，以便他们能够在概念证明环境中测试功能。因此，您需配置此预留，将资源分配给架构师业务组。

2 场景：为概念证明环境指定 Amazon AWS 网络设置

您可以配置使用与您通道计算机使用相同区域和网络设置的预留，并限制可为此预留打开电源以管理资源使用情况的计算机数量。

3 场景：指定自定义属性以通过通道运行代理通信

如果您已配置网络-Amazon VPC 连接，则您已配置端口转发，允许 Amazon AWS 通道计算机访问 vRealize Automation 资源。

场景：为概念证明环境指定 Amazon AWS 预留信息

您需要为蓝图架构师团队预留资源，以便他们能够在概念证明环境中测试功能。因此，您需配置此预留，将资源分配给架构师业务组。

注 创建预留后，您无法更改业务组或计算资源关联。

步骤

- 1 选择**基础架构 > 预留 > 预留**。
- 2 单击**新建**图标 (+)，并选择要创建的预留类型。
选择 **Amazon**。
- 3 在**名称**文本框中，输入 **Amazon Tunnel POC**。
- 4 从**业务组**下拉菜单中，选择您已为蓝图架构师创建的业务组。

5 在 **优先级** 文本框中输入 **1**，将此预留设置为最高优先级。

结果

您已为此预留配置业务组和优先级，但您仍需要为 SSH 通道分配资源并配置自定义属性。

场景：为概念证明环境指定 Amazon AWS 网络设置

您可以配置使用与您通道计算机使用相同区域和网络设置的预留，并限制可为此预留打开电源以管理资源使用情况的计算机数量。

步骤

- 1** 单击**资源**选项卡。
- 2** 从**计算资源**下拉菜单中，选择置备计算机要使用的计算资源。
选择通道计算机所在的 Amazon AWS 区域。
- 3** （可选） 在**计算机配额**文本框中输入一个数字，设置可以在此预留中置备的最大计算机数量。
只有已打开电源的计算机才会计入配额。留空将使预留无限制。
- 4** 从**密钥对**下拉菜单中选择**指定密钥对**。
由于这是概念证明环境，因此您需为所有通过使用此预留置备的计算机选择共享一个密钥对。
- 5** 从**密钥对**下拉菜单中，选择您要与此架构师用户共享的密钥对。
- 6** 选中**分配到 VPC 的子网**中复选框。
- 7** 选择与通道计算机使用相同的子网和安全组。

结果

您已将该预留配置为使用与通道计算机相同的区域和网络设置，但您仍需添加自定义属性，确保 Software 引导代理和客户机代理可通过通道运行通信。

场景：指定自定义属性以通过通道运行代理通信

如果您已配置网络-Amazon VPC 连接，则您已配置端口转发，允许 Amazon AWS 通道计算机访问 vRealize Automation 资源。

您需要在预留中添加通道自定义属性，以便配置代理访问这些端口。

注 如果组织网络和 vRealize Automation 网络间使用的是 PAT 或 NAT 系统网络，那么您可以使用这些属性来访问您的专用 IP 地址和端口。

步骤

- 1** 单击**属性**选项卡。
- 2** 单击**新建**。

3 配置通道自定义属性。

使用 Amazon AWS 通道计算机和端口 1443 的专用 IP 地址。这是您在调用 SSH 通道时为 `vRealize_automation_appliance_fqdn` 分配的地址。

选项	值
<code>software.ebs.url</code>	<code>https://Private_IP:1443/event-broker-service/api</code>
<code>software.agent.service.url</code>	<code>https://Private_IP:1443/software-service/api</code>
<code>agent.download.url</code>	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

4 单击保存。

结果

您已创建预留，并将 Amazon AWS 资源分配给架构师业务组。您已配置预留，支持客户机代理和 Software 引导代理。架构师可以创建蓝图，从而利用客户机代理自定义部署的计算机或包括 Software 组件。

创建虚拟类别预留

虚拟类别类型预留给特定的 vRealize Automation 业务组提供虚拟机部署置备服务的访问权限。可用的虚拟预留类型包括 vSphere、Hyper-V、KVM、SCVMM 和 XenServer。

预留是指共享分配到特定 vRealize Automation 业务组的某种计算资源，包括内存、CPU、网络 and 存储资源。

业务组既可以在一个端点上具有多个预留，也可以在多个端点上具有多个预留。

要置备虚拟机，业务组必须在虚拟计算资源上至少具有一个预留。每个预留仅用于一个业务组，但每个业务组既可以在一种计算资源上具有多个预留，也可以在多种计算资源上具有多个预留。

除了定义分配给业务组的架构资源共享外，预留还可以定义确定计算机放置位置的策略、优先级和配额。

要确保置备成功，预留必须具有足够的可用存储。预留的存储可用性取决于：

- 数据存储/群集上的可用存储量。
- 为该数据存储/群集预留的存储量。
- vRealize Automation 中已分配的存储量。

例如，即使 vCenter Server 具有可供数据存储/群集使用的存储，如果未在预留中预留足够的存储，则置备仍会失败，并且显示“没有可分配的预留...”错误。预留上分配的存储取决于该特定预留上的虚拟机数量（无论处于何种状态）。有关详细信息，请参见 VMware 知识库文章《计算机 XXX：组 XXX 中没有可分配的预留。请求的存储总量为 XX GB (2151030)》，网址为 <http://kb.vmware.com/kb/2151030>。

了解预留的选择逻辑

当业务组成员为虚拟机创建置备请求时，vRealize Automation 将从可用于该业务组的预留之一中选择计算机。

为其置备计算机的预留必须满足以下条件：

- 该预留的平台类型必须与从中请求计算机的蓝图相同。

任何类型的虚拟预留上均可创建通用虚拟蓝图。

- 该预留必须已启用。
- 计算资源必须可访问且不处于维护模式。
- 该预留必须在其计算机配额中有剩余容量或者具有无限配额。

分配的计算机配额仅包括已打开电源的计算机。例如，如果预留的配额为 50 台计算机且已置备 40 台，但其中只有 20 台已打开电源，则该预留的配额已分配 40%，而不是 80%。

- 该预留必须具有足够的未分配内存和存储资源来置备计算机。

当虚拟预留的计算机配额、内存或存储全部分配完毕之后，无法从中置备其他虚拟机。预留的资源可能超过虚拟化计算资源的物理容量（过载），但是如果某计算资源的物理容量已 100% 分配，则在回收该资源之前，无法在使用该计算资源的任何预留中置备其他计算机。

- 如果蓝图具有特定的网络设置，则该预留必须具有相同的网络。

如果蓝图或预留为静态 IP 地址分配指定网络配置文件，则 IP 地址必须可以分配给新计算机。

- 如果蓝图或请求指定一个位置，则该计算资源必须与此位置关联。

如果自定义属性 `Vrm.DataCenter.Policy` 的值为 **Exact**，且与该位置关联的计算资源的预留不满足所有其他条件，则置备将会失败。

如果 `Vrm.DataCenter.Policy` 的值为 **NotExact**，且与该位置关联的计算资源的预留不满足所有其他条件，则无论位置如何，均可在其他预留上继续进行置备。此选项为默认选项。

- 如果蓝图或请求指定自定义属性 `VirtualMachine.Host.TpmEnabled`，则必须在该预留的计算资源上安装可信硬件。
- 如果蓝图指定预留策略，则该预留必须属于此预留策略。

对于从特定蓝图中置备计算机，预留策略是一种可保证所选预留满足其任何附加要求的一种方式。例如，您可以使用预留策略将置备限制为使用特定模板进行克隆的计算资源。

如果任何预留均不满足所有选择标准，则置备将会失败。

如果多个预留满足所有条件，则置备请求计算机所使用的预留取决于以下逻辑：

- 先选择优先级值较低的预留，之后再选择优先级值较高的预留。
- 如果多个预留具有相同的优先级，则选择分配的计算机配额比例最低的预留。
- 如果多个预留具有相同的优先级和配额使用量，则系统以循环方式将计算机分布在各预留之间。

注 尽管不支持以循环方式选择网络配置文件，但是支持以循环方式选择网络（如果有），它可以与不同的网络配置文件相关联。

如果一个预留上具有多条存储路径，且具有足够的容量来置备计算机卷，则系统将根据以下逻辑选择存储路径。

- 如果蓝图或请求指定存储预留策略，则存储路径必须属于该存储预留策略。

如果自定义属性 `VirtualMachine.DiskN.StorageReservationPolicyMode` 的值为 **NotExact**，且存储预留策略中的所有存储路径均没有足够的容量，则可以使用指定存储预留策略之外的存储路径继续置备。`VirtualMachine.DiskN.StorageReservationPolicyMode` 的默认值为 **Exact**。

- 先选择优先级值较低的存储路径，之后再选择优先级值较高的存储路径。
- 如果多条存储路径具有相同的优先级，则系统将使用循环方式将计算机分布在各存储路径之间。

为 NSX 网络和安全虚拟化创建 vSphere 预留

您可以创建 vSphere 预留来与关联的 NSX-T 或 NSX for vSphere 端点配合使用。

常规 NSX 注意事项

如果配置了 NSX，那么在创建或编辑蓝图时，可以指定 NSX 传输区域、网络预留策略以及应用程序隔离设置。可在[蓝图](#)和[蓝图属性](#)页面的 **NSX 设置**选项卡上找到这些设置。

添加到蓝图中的网络与安全组件设置派生自 NSX for vSphere 和 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX 清单。网络与安全组件特定于 NSX，并且只能供 vSphere 计算机组件使用。有关配置 NSX 的信息，请参见 [NSX for vSphere 产品文档](#)或 [NSX-T 产品文档](#)中的《管理指南》，具体取决于您使用的应用程序。

当计算机蓝图定义计算机网络时，如果要成功置备，那么该预留的传输区域必须与此蓝图的传输区域匹配。同样地，如果要置备计算机的路由网关，那么该预留定义的传输区域必须与此蓝图定义的传输区域匹配。

有关 NSX-T-您的部署中的特定拓扑注意事项的信息，请参见[了解网络连接、安全性和负载均衡器配置的 NSX-T 部署拓扑](#)。

NSX for vSphere 注意事项

当 vRealize Automation 通过 NAT 或路由网络置备计算机时，会将路由网关置备为网络路由器。Edge 或路由网关是使用计算资源的管理计算机。它还管理已置备计算机组件的网络通信。用于置备 Edge 或路由网关的预留将确定用于 NAT 和路由网络配置文件的外部网络。此外，它还会确定用于配置路由网络的预留 Edge 或路由网关。预留路由网关将路由网络与路由表中的条目链接在一起。

如果配置路由网络时在预留中选择 Edge 或路由网关和网络配置文件，请选择链接路由网络中要使用的网络路径，并为其分配配置路由网络配置文件使用的外部网络配置文件。系统将根据为网络接口选择的子网掩码和主 IP 地址，对可分配给网络路径的网络配置文件列表进行筛选，使其与网络路径的子网匹配。

您可以指定 Edge 或路由网关预留策略，以便确定使用 Edge 或路由网关置备计算机时要使用的预留。默认情况下，vRealize Automation 对路由网关和计算机组件使用相同的预留。

如果要在 vRealize Automation 预留中使用 Edge 或路由网关，请在 NSX 环境中以外部方式配置路由网关，然后运行清单数据收集。对于 NSX，您必须运行 NSX Edge 实例才能为 Edge 服务网关或分布式路由器配置静态路由或动态路由的默认网关。请参见 [NSX 管理指南](#)。

您可在预留中选择一个或多个安全组，以便对在 vRealize Automation 中通过该预留置备的所有组件计算机强制执行基准安全策略。每个置备的计算机都添加到这些指定的安全组。

NSX-T 注意事项

为关联到 NSX-T 端点的 vSphere 端点创建预留时，必须为预留配置以下信息：

- 定义蓝图的传输区域。
- 选择已置备部署要连接到的第 0 层逻辑路由器。
- 将外部网络配置文件映射到第 0 层逻辑路由器。

NSX-T NS 组在预留中不受支持。

有关 NSX-T -特定部署和拓扑注意事项的详细信息，请参见[了解网络连接、安全性和负载均衡器配置的 NSX-T 部署拓扑](#)。

为 Hyper-V、KVM、SCVMM、vSphere 或 XenServer 创建预留

您必须先通过创建预留将资源分配给计算机，然后业务组的成员才能请求计算机置备。

每个业务组必须至少为其成员提供一个置备该类计算机的预留。例如，具有 vSphere 预留、但无 KVM (RHEV) 预留的业务组无法请求 KVM (RHEV) 虚拟机。在此示例中，必须为业务组分配专门针对 KVM (RHEV) 资源的预留。

步骤

1 指定虚拟预留信息

每个预留均针对特定的业务组配置，以授权用户访问指定计算资源上的请求计算机。

2 为虚拟预留指定资源和网络设置

指定用于通过此 vRealize Automation 预留置备计算机的资源和网络设置。

3 为虚拟预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

指定虚拟预留信息

每个预留均针对特定的业务组配置，以授权用户访问指定计算资源上的请求计算机。

在添加、编辑或删除预留时，可以在“预留”页面上使用[按类别筛选](#)选项来控制预留的显示。请注意，在按类别进行筛选时，测试代理预留不会显示在预留列表中。

注 创建预留后，您无法更改业务组或计算资源关联。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 确认租户管理员至少已创建一个业务组。
- 确认已存在一个计算资源。
- 配置网络设置。
- （可选）配置网络配置文件信息。

步骤

1 选择**基础架构 > 预留 > 预留**。

2 单击**新建**图标 (+)，并选择要创建的预留类型。

可用的虚拟预留类型包括 Hyper-V、KVM、SCVMM、vSphere 和 XenServer。

例如，选择 **vSphere**。

3 在**名称**文本框中输入名称。

4 从**租户**下拉菜单中选择租户。

5 从**业务组**下拉菜单中选择业务组。

只有此业务组中的用户才能使用此预留置备计算机。

6 (可选) 从**预留策略**下拉菜单中选择预留策略。

此选项要求存在一个或多个预留策略。稍后，您可以编辑预留或指定预留策略。

您可以使用预留策略将置备限制为特定的预留。

7 在**优先级**文本框中输入一个数字，设置预留的优先级。

当一个业务组具有多个预留时，系统将使用优先级。优先级为 1 的预留比优先级为 2 的预留先用于置备。

8 (可选) 如果不想此预留处于活动状态，请取消选中**启用此预留**复选框。

结果

请勿导航离开此页面。您的预留尚未完成。

为虚拟预留指定资源和网络设置

指定用于通过此 vRealize Automation 预留置备计算机的资源和网络设置。

如果 vSphere 环境和存储设备使用 Net App FlexClone 技术，则可在预留中选择 FlexClone 数据存储。FlexClone 存储设备不支持 SDRS。

要确保置备成功，预留必须具有足够的可用存储。预留的存储可用性取决于：

- 数据存储/群集上的可用存储量。
- 为该数据存储/群集预留的存储量。
- vRealize Automation 中已分配的存储量。

例如，即使 vCenter Server 具有可供数据存储/群集使用的存储，如果未在预留中预留足够的存储，则置备仍会失败，并且显示“没有可分配的预留...”错误。预留上分配的存储取决于该特定预留上的虚拟机数量（无论处于何种状态）。有关详细信息，请参见 VMware 知识库文章《计算机 XXX：组 XXX 中没有可分配的预留。请求的存储总量为 XX GB (2151030)》，网址为 <http://kb.vmware.com/kb/2151030>。

如果您正创建或编辑 vSphere (vCenter) 预留以便与 NSX for vSphere 或 NSX-T 配合使用，可以使用所选网络的高级选项来指定传输区域和 第 1 层逻辑路由器信息。

前提条件

[指定虚拟预留信息。](#)

步骤

1 单击**资源**选项卡。

2 从**计算资源**下拉菜单中，选择置备计算机要使用的计算资源。

只有位于所选群集中的模板才能使用此预留进行克隆。

置备期间，计算机将置于连接到本地存储的主机上。如果预留使用本地存储，则预留置备的所有计算机会在包含该本地存储的主机上进行创建。但是，如果使用 `VirtualMachine.Admin.ForceHost` 自定义属性，该属性强制计算机置备到其他主机，则置备会失败。如果克隆计算机的模板位于本地存储，但是将该模板连接到其他群集上的计算机，则置备也会失败。在这种情况下，置备由于无法访问模板而失败。

- 3 （可选）在**计算机配额**文本框中输入一个数字，设置可以在此预留中置备的最大计算机数量。

只有已打开电源的计算机才会计入配额。留空将使预留无限制。

- 4 从“内存”表中指定要分配给此预留的内存量 (GB)。

该预留的内存总量值是从您选择的计算资源中派生得出的。

- 5 从“内存”表中指定要分配给此预留的内存量 (GB)。

该预留的内存总量值是从您选择的计算资源中派生得出的。

- 6 选择列出的一个或多个存储路径。

可用的存储路径选项是从您的计算资源选择中派生得出的。

对于使用 **Storage Distributed Resource Scheduler (SDRS)** 存储的集成，您可以选择存储群集，允许 SDRS 自动为通过此预留置备的计算机处理存储放置和负载平衡。SDRS 自动化模式必须设置为“自动”。否则，在该群集内针对独立数据存储行为选择数据存储。**FlexClone** 存储设备不支持 SDRS。

您可以在该群集或存储群集中选择单个磁盘，但不能同时在两者中进行选择。如果选择存储群集，SDRS 将为通过此预留置备的计算机控制存储放置和负载平衡。

- 7 如果适用于计算资源，请在**资源池**下拉菜单中选择资源池。

- 8 单击**网络**选项卡。

- 9 为通过使用此预留置备的计算机配置网络路径。

- a （可选）如果选项可用，从**端点**下拉菜单中选择存储端点。

如果 **NetApp ONTAP** 端点存在且主机为虚拟主机，则 **FlexClone** 选项在端点列中可见。如果存在 **NetApp ONTAP** 端点，则预留页面将显示分配给存储路径的端点。为存储路径添加、更新或删除端点时，您所做的更改在所有适用的预留中可见。

为存储路径添加、更新或删除端点时，您所做的更改在预留页面中可见。

- b 为将要为此预留置备的计算机选择一个或多个**网络适配器**。

- c （可选）为每个选定的网络适配器选择可用的**网络配置文件**。

- d （可选）如果高级设置可用，请选择**传输区域**和部署包含负载平衡器的蓝图时要使用的一个或多个**第 0 层逻辑路由器**。

传输区域定义网络适配器跨哪些群集。如果在预留和蓝图中指定传输区域，传输区域值必须匹配。您可以在预留中选择多个网络适配器，但置备计算机时只使用一个网络。

结果

现在，您通过单击**保存**即可保存预留。或者，您可以添加自定义属性，进一步控制预留规范。您也可以对电子邮件警示进行配置，使其在分配给此预留的资源不足时发送通知。

为虚拟预留指定自定义属性和警示

您可以将自定义属性与 vRealize Automation 预留关联。此外，您也可以将警示配置为预留资源不足时发送电子邮件通知。

自定义属性和电子邮件警示是预留的可选配置。如果不想关联自定义属性或设置警示，请单击**保存**完成预留的创建。

您可以根据自身需要添加任意数量的自定义属性。

重要事项 仅当已配置电子邮件警示且已启用通知时，系统才会发送通知。

若已配置，系统将每天生成警示，而不是在达到指定阈值时生成。

前提条件

[为虚拟预留指定资源和网络设置。](#)

步骤

- 1 单击**属性**选项卡。
- 2 单击**新建**。
- 3 输入有效的自定义属性名称。
- 4 如果适用，请输入属性值。
- 5 （可选）选中**已加密**复选框，对属性值进行加密。
- 6 （可选）选中**提示用户**复选框，要求用户输入值。
在进行置备时，此选项无法替代。
- 7 （可选）添加任何其他自定义属性。
- 8 单击**警示**选项卡。
- 9 启用**容量警示**复选框，配置要发送的警示。
- 10 使用滑块设置可用资源分配的阈值。
- 11 在**收件人**文本框中输入 AD 用户或组名称（而不是电子邮件地址）以接收警示通知。
在每一行输入一个名称。按 **Enter** 分隔多个条目。
- 12 选择**向组主管发送警示**，将组主管包括在电子邮件警示中。
电子邮件警示将发送到业务组**发送主管电子邮件**至列表中包括的用户。
- 13 指定提醒频率（天）。
- 14 单击**保存**。

结果

该预留已保存并显示在“预留”列表中。

后续步骤

您可以配置可选预留策略或开始准备进行置备。

现在，有权创建蓝图的用户可以创建蓝图。

编辑预留以分配网络配置文件

您可以将网络配置文件分配给预留，以便为在该预留上置备的计算机启用静态 IP 分配等。

您还可以使用**新建蓝图属性**选项卡或**蓝图属性**页面上的自定义属性

`VirtualMachine.NetworkN.ProfileName` 为蓝图分配网络配置文件。

如果在预留和蓝图中指定网络配置文件，则优先使用蓝图值。例如，如果利用 `VirtualMachine.NetworkN.ProfileName` 自定义属性在蓝图中和蓝图所用的预留中指定网络配置文件，则优先使用在蓝图中指定的网络配置文件。但是，如果该自定义属性不用于蓝图且您为计算机网卡选择网络配置文件，则 vRealize Automation 将对已指定网络配置文件的计算机网卡使用预留网络路径。

注 此信息不适用于 Amazon Web Services。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 创建网络配置文件。请参见[创建网络配置文件](#)。

步骤

- 1 选择**基础架构 > 预留 > 预留**。
- 2 指向预留并单击**编辑**。
- 3 单击**网络**选项卡。
- 4 将网络配置文件分配给网络路径。
 - a 选择要启用静态 IP 地址的网络路径。
网络路径选项从**资源**选项卡上的设置中派生。
 - b 通过从**网络配置文件**下拉菜单中选择配置文件，将可用网络配置文件映射到路径。
 - c （可选）重复此步骤，将网络配置文件分配给此预留上的其他网络路径。
- 5 单击**确定**。

预留策略

您可以使用预留策略控制处理预留请求的方式。通过蓝图置备计算机时，置备仅限于您在预留策略中指定的资源。

预留策略提供可选的方法来控制处理预留请求的方式。您可以将预留策略应用于蓝图，以让通过该蓝图置备的计算机限于可用预留的子集。

您可以使用预留策略将资源收集到不同服务级别的组中，或者用于使特定类型的资源可轻松供特定用途使用。用户请求计算机时，可以在具有足够计算机容量的任意相应类型的预留上进行置备。以下情形提供了预留策略的可能用法的多个示例：

- 用于确保已置备的计算机提供具有支持 NetApp FlexClone 的特定设备的预留。
- 用于将云计算机的置备设置限制于特定区域，该区域包含特定蓝图所需的计算机映像。
- 对于支持该功能的计算机类型，作为使用“即用即付”分配模型的附加方式。

可以向预留策略添加多个预留，但一个预留只能属于一个策略。可以为多个蓝图分配一个预留策略。一个蓝图只能具有一个预留策略。

注 为 vCloud Air 端点和 vCloud Director 端点定义的预留不支持使用网络配置文件来置备计算机。

注 如果您在平台上启用了 SDRS，则可以允许 SDRS 为各个虚拟机磁盘负载均衡存储，或者为虚拟机加载所有存储。如果您使用 SDRS 数据存储集群，则当使用预留策略和存储预留策略时会发生冲突。例如，如果在某个策略或存储策略中的其中一个预留上选择了一个独立数据存储或 SDRS 集群内的一个数据存储，您的虚拟机存储可能被冻结，而不是由 SDRS 驱动。如果请求重新置备其存储放置在 SDRS 集群上的计算机，且已停用 SDRS 自动化级别，则该计算机将被删除。有关置备和 SDRS 的相关信息，请参见 `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec` 自定义属性。

配置预留策略

您可以创建预留策略，用于将资源收集到不同服务级别的组中，或者用于使特定类型的资源可轻松供特定用途使用。创建预留策略后，您必须先在其中填充预留，然后租户管理员和业务组主管才能在蓝图中有效地使用该策略。

预留策略可以包括不同类型的预留，但只有为特定的请求选择预留时才会考虑与蓝图类型匹配的预留。

步骤

1 创建预留策略

您可以使用预留策略将类似的预留组合在一起。

2 将预留策略分配给预留

当您创建预留时，可以将预留策略分配给预留。您也可以编辑现有预留来为其分配预留策略，或者更改其预留策略分配。

创建预留策略

您可以使用预留策略将类似的预留组合在一起。

请先创建预留策略，然后将该策略添加到预留，允许蓝图创建者在蓝图中使用该预留策略。

该策略将创建为空容器。

在添加、编辑或删除预留策略时，可以在“预留策略”页面上使用**按类型筛选**选项来控制预留策略的显示。

前提条件

以**架构管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**基础架构 > 预留 > 预留策略**。
- 2 单击**新建**图标 (+)。
- 3 在**名称**文本框中输入名称。
- 4 从**类型**下拉菜单中选择**预留策略**。
- 5 在**描述**文本框中输入描述。
- 6 单击**确定**。

将预留策略分配给预留

当您创建预留时，可以将预留策略分配给预留。您也可以编辑现有预留来为其分配预留策略，或者更改其预留策略分配。

前提条件

[创建预留策略](#)。

步骤

- 1 选择**基础架构 > 预留 > 预留**。
- 2 指向预留并单击**编辑**。
- 3 从**预留策略**下拉菜单中选择预留策略。
- 4 单击**保存**。

存储预留策略

您可以创建存储预留策略，以允许蓝图架构师将虚拟机的卷分配给 vSphere、KVM (RHEV) 和 SCVMM 平台类型不同的数据存储或其他资源（例如 vCloud Air 或 vCloud Director 资源）不同的存储配置文件。

为不同的数据存储或不同的存储配置文件分配虚拟机的卷，使蓝图架构师可以更有效地控制和使用存储空间。例如，他们将操作系统卷部署到速度更慢、成本更低的数据存储或存储配置文件中，并将数据库卷部署到速度更快的数据存储或存储配置文件中。

某些计算机端点仅支持单个存储配置文件，而其他端点则支持多级磁盘存储。多级磁盘存储适用于 vCloud Director 5.6 及更高版本的端点和 vCloud Air 端点。vCloud Director 5.5 端点不支持多级磁盘存储。

创建蓝图时，您可以为卷分配单个数据存储或代表多个数据存储的存储预留策略。为卷分配单个数据存储或存储配置文件时，如有可能，vRealize Automation 将在置备过程中使用该数据存储或存储配置文件。为卷分配存储预留策略时，如果使用其他资源（例如 vCloud Air 或 vCloud Director），vRealize Automation 将在置备过程中使用其中一个数据存储或存储配置文件。

存储预留策略实质上是架构管理员用来对具有类似特征（例如，速度或价格）的数据存储或存储配置文件进行分组的一个或多个数据存储或存储配置文件的标记。您每次只能将数据存储或存储配置文件分配给一个存储预留策略，但存储预留策略可以具有许多不同的数据存储或存储配置文件。

您可以创建存储预留策略，并将其分配给一个或多个数据存储或存储配置文件。然后，蓝图创建者将存储预留策略分配给虚拟蓝图中的卷。用户请求使用该蓝图的计算机时，vRealize Automation 将使用在该蓝图中指定的存储预留策略来为计算机的卷选择数据存储或存储配置文件。

注 如果您在平台上启用了 SDRS，则可以允许 SDRS 为各个虚拟机磁盘负载均衡存储，或者为虚拟机加载所有存储。如果您使用 SDRS 数据存储集群，则当使用预留策略和存储预留策略时会发生冲突。例如，如果在某个策略或存储策略中的其中一个预留上选择了一个独立数据存储或 SDRS 集群内的一个数据存储，您的虚拟机存储可能被冻结，而不是由 SDRS 驱动。如果请求重新置备其存储放置在 SDRS 集群上的计算机，且已停用 SDRS 自动化级别，则该计算机将被删除。有关置备和 SDRS 的相关信息，请参见 `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec` 自定义属性。

在 vRealize Automation 中执行“销毁”操作删除已置备的计算机时，通过预留分配给该计算机的存储和内存将会被释放。如果在 vCenter Server 中删除该计算机，存储和内存将不会被释放。

例如，您无法删除与现有部署中的计算机关联的预留。如果您在 vCenter Server 中手动移动或删除了已部署的计算机，vRealize Automation 仍会认为该计算机有效，并阻止您删除关联的预留。

配置存储预留策略

您可以创建存储预留策略，对具有类似特征（例如，速度或价格）的数据存储进行分组。创建存储预留策略后，您必须在蓝图中使用该策略之前，先使用数据存储填充它。

步骤

1 创建存储预留策略

您可以使用存储预留策略对具有类似特征（例如，速度或价格）的数据存储进行分组。

2 将存储预留策略分配给数据存储

您可以将存储预留策略与计算资源关联。创建存储预留策略之后，使用数据存储填充该策略。一个数据存储只能属于一个存储预留策略。添加多个数据存储，可创建一组与蓝图配合使用的数据存储。

创建存储预留策略

您可以使用存储预留策略对具有类似特征（例如，速度或价格）的数据存储进行分组。

该策略将创建为空容器。

在添加、编辑或删除预留策略时，可以在“预留策略”页面上使用**按类型筛选**选项来控制预留策略的显示。

前提条件

以**架构管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**基础架构 > 预留 > 预留策略**。
- 2 单击**新建**图标 (+)。
- 3 在**名称**文本框中输入名称。
- 4 从**类型**下拉菜单中选择**存储预留策略**。

5 在**描述**文本框中输入描述。

6 单击**确定**。

将存储预留策略分配给数据存储

您可以将存储预留策略与计算资源关联。创建存储预留策略之后，使用数据存储填充该策略。一个数据存储只能属于一个存储预留策略。添加多个数据存储，可创建一组与蓝图配合使用的数据存储。

前提条件

创建存储预留策略。

步骤

1 选择**基础架构 > 计算资源 > 计算资源**。

2 指向计算资源并单击**编辑**。

3 单击**配置**选项卡。

4 在“存储”表中，找到要添加到存储预留策略的数据存储。

5 单击所需**存储路径**对象旁边的**编辑**图标 (✎)。

6 从**存储预留策略**列下拉菜单中选择存储预留策略。

置备计算机后，无法更改其存储预留策略，如果这样做会更改磁盘上的存储配置文件。

7 单击**确定**。

8 （可选）将其他数据存储分配给存储预留策略。

9 单击**确定**。

工作负载放置

部署蓝图时，工作负载放置使用收集的数据基于可用资源来建议蓝图的部署位置。vRealize Automation 和 vRealize Operations Manager 可协同工作，共同为新蓝图部署中的工作负载提供放置建议。

vRealize Automation 管理组织的策略（如业务组、预留和配额）时，它将与 vRealize Operations Manager 的容量分析集成以放置计算机。工作负载放置仅适用于 vSphere 端点。

使用的工作负载放置条款

多项条款用于工作负载放置。

- vSphere 中的群集映射到 vRealize Automation 中的计算资源。
- 预留包括计算和存储，其中存储可由单个数据存储或数据存储群集组成。预留可以包括多个数据存储、数据存储群集，或两者都包括。
- 多个预留可以引用同一群集。
- 虚拟机可以移至多个群集。
- 启用工作负载放置后，置备 workflows 将使用放置策略建议蓝图的部署位置。

使用工作负载放置置备蓝图

使用工作负载放置置备蓝图时，置备 workflow 将使用 vRealize Automation 中的预留和 vRealize Operations Manager 的放置优化。

- 1 vRealize Automation 可提供管治规则以允许放置目标。
- 2 vRealize Operations Manager 可根据分析数据提供放置优化建议。
- 3 vRealize Automation 可根据 vRealize Operations Manager 中的放置建议继续置备过程。

如果 vRealize Operations Manager 无法提供建议或建议无法使用，则 vRealize Automation 会退回到其默认的放置逻辑。

当开发人员选择目录项并填写表单以请求目录项时，vRealize Automation 将考虑以下注意事项来置备虚拟机。

表 2-16. 置备虚拟机的注意事项

注意事项	影响
策略	vRealize Automation 预留策略可能指示多个预留。
预留	<p>vRealize Automation 将评估请求，并确定哪些预留可满足请求中提出的限制。</p> <ul style="list-style-type: none"> ■ 如果放置已启用且基于 vRealize Operations Manager 分析，则 vRealize Automation 会将预留列表传递给 vRealize Operations Manager，从而根据运维衡量指标确定最适合放置的预留。 ■ 如果放置不基于 vRealize Operations Manager，则 vRealize Automation 将根据优先级和可用性决定放置。 <p>系统将更新预留，以跟踪消耗的资源。</p> <p>如果 vRealize Automation 认为 vRealize Operations Manager 建议的群集或数据存储容量不足或不再适用，则 vRealize Automation 将记录异常。vRealize Automation 根据其默认放置机制允许继续置备。</p>

为标识虚拟机的资源，vRealize Automation 会提供候选预留的列表。列表中的每个候选项可以包括群集以及一个或多个数据存储或数据存储群集。vRealize Operations Manager 使用候选预留来创建目标候选项的列表并找到最佳目标。

vRealize Operations Manager 中的策略可设置群集的平衡级别、利用率以及缓冲空间。对于单个预留（即群集或数据存储群集），vRealize Automation 将验证此放置目标建议是否可行。

- 如果该目标可行，则 vRealize Automation 将根据建议部署蓝图。
- 如果该目标不可行，vRealize Automation 将使用默认放置行为来放置虚拟机。

放置注意事项还必须考虑运行状况和利用率问题。云管理员和虚拟基础架构管理员负责管理基础架构，而开发人员则负责应用程序的运行状况。为了支持开发人员，工作负载放置策略还必须考虑运行状况和利用率问题。

表 2-17. 运行状况和利用率问题的注意事项

工作负载问题	放置解决方案
开发人员发现环境中存在运行状况问题。	vRealize Automation 在其中置备蓝图的群集出现问题，或者因工作负载较多而导致群集过度使用。vRealize Automation 必须与 vRealize Operations Manager 中的容量分析集成，从而确保在拥有足够容量的群集中置备蓝图。
开发人员发现利用率问题。	环境中的群集使用不足。vRealize Automation 必须与 vRealize Operations Manager 提供的容量分析集成，从而确保在利用率最高的群集中置备蓝图。

置备蓝图的用户

以下用户将执行各种操作来置备蓝图。

表 2-18. 置备蓝图的用户和角色

步骤	用户	操作	所需角色
1	云管理员或虚拟基础架构 (VI) 管理员	确保虚拟机的初始放置符合组织策略，且已根据运维分析数据进行优化。	IaaS 管理员角色
1	架构管理员	在 vRealize Automation 中定义预留、预留策略和放置策略。	架构管理员角色、基础架构架构师
1	IaaS 管理员	为 vSphere 和 vRealize Operations Manager 定义工作负载放置所需的端点。	IaaS 管理员角色
2	基础架构架构师	能够直接处理虚拟机组件类型的蓝图架构师可以在编写蓝图时将预留策略分配给虚拟机。将预留策略指定为蓝图中计算机组件的属性。	基础架构架构师
3	基础架构架构师、应用程序架构师、软件架构师和 XaaS 架构师	<p>创建并发布蓝图以置备虚拟机。只有基础架构架构师可直接处理计算机组件。其他架构师角色可以在嵌套中重用基础架构蓝图，但无法编辑计算机组件设置。</p> <p>蓝图可以包括单一组件，也可以包括嵌套蓝图、XaaS 组件、多层应用程序中的多个虚拟机等。</p> <p>vRealize Automation 根据预留配置放置虚拟机，还可以在蓝图的计算机组件级别包括预留策略。例如，您的蓝图可能包含两个计算机，且每个计算机应用不同的策略。</p> <p>vRealize Automation 还将根据 vRealize Operations Manager 提供的运维分析数据优化虚拟机。</p>	基础架构架构师
4	云管理员或 VI 管理员	<p>选择控制 vRealize Automation 置备的虚拟机初始放置的策略。</p> <p>管理员可执行以下操作：</p> <ul style="list-style-type: none"> ■ 使用 API 选择策略。 ■ 使用默认放置策略，即依次使用 vRealize Automation 中的每个服务器来平衡工作负载。此方法不需要 vRealize Operations Manager 中的输入。 	IaaS 管理员角色、基础架构架构师
5	VI 管理员	在 vRealize Operations Manager 中构建自定义数据中心和自定义组。然后，VI 管理员将整合和平衡工作负载使用的策略应用于这些自定义数据中心。	IaaS 管理员角色、基础架构架构师

表 2-18. 置备蓝图的用户和角色（续）

步骤	用户	操作	所需角色
6	架构管理员	选择 vRealize Automation 中的放置策略。 使用工作负载放置策略让 vRealize Automation 确定部署新蓝图时将计算机放置在何处。放置策略需要从 vRealize Operations Manager 输入。	架构管理员角色
7	开发人员	请求蓝图以置备虚拟机。 蓝图可以由多台计算机组成，以运行三层应用程序。	
8	开发人员	当开发人员部署蓝图时，vRealize Operations Manager 将搜索适合该请求的相关群集的放置策略。	

有关放置策略的详细信息，请参见[放置策略](#)。

要配置工作负载放置，请参见[配置工作负载放置](#)。

放置虚拟机需要 Distributed Resource Scheduler (DRS)

vSphere DRS 是供 vRealize Automation 和 vRealize Operations Manager 用于置备和放置虚拟机的放置引擎。

为了让 vRealize Automation 建议虚拟机的最佳放置，必须在群集上启用 DRS 并将其设置为完全自动。然后，vRealize Automation 使用 vSphere DRS API 来确定虚拟机的正确放置。

vRealize Automation 与 vRealize Operations Manager 放置服务集成。vRealize Operations Manager 仅为启用了 DRS 且设置为完全自动的群集提供放置建议。

vRealize Automation 存储预留策略的影响

存在 vRealize Automation 存储预留策略会影响 vRealize Operations Manager 的工作负载放置。

启用使用 vRealize Operations Manager 放置工作负载后，vRealize Automation 将可用预留列表传递到 vRealize Operations Manager，然后 vRealize Operations Manager 对预留进行评估以根据操作分析放置存储。

注 使用 vRealize Operations Manager 放置工作负载仅支持具有一个或多个磁盘的虚拟机，且只能有一个存储预留策略。不支持使用多个策略组合进行磁盘放置，因为不支持单个磁盘放置。

如果蓝图包含存储预留策略，则 vRealize Operations Manager 的工作负载放置建议将进行如下更改：

配置	放置
虚拟机具有一个或多个磁盘，且均未指定存储预留策略	放置正常进行。vRealize Operations Manager 评估未经筛选的完整候选预留列表。
虚拟机具有一个或多个磁盘，且全部指定了相同的存储预留策略	在存储级别筛选候选预留，以便 vRealize Operations Manager 仅评估与该存储预留策略匹配的数据存储。

配置	放置
虚拟机具有多个磁盘，部分磁盘指定了相同的存储策略，但其他磁盘尚未指定任何存储预留策略	<ul style="list-style-type: none"> ■ 当存储分配类型为默认值 COLLECTED 时，会将所有磁盘视为共享该相同策略。vRealize Operations Manager 评估与该存储预留策略匹配的数据存储。 ■ 当存储分配类型为 DISTRIBUTED 时，将无法根据 vRealize Operations Manager 建议放置虚拟机，因为不支持单个磁盘放置。放置改为默认采用 vRealize Automation 放置算法。 <p>您可以使用自定义属性设置存储分配类型。</p>
虚拟机具有多个磁盘，且磁盘指定不同的存储预留策略	由于它们的存储预留策略要求相互冲突，因此无法根据 vRealize Operations Manager 建议放置这些虚拟机。放置改为默认采用 vRealize Automation 放置算法。
虚拟机需要特定存储路径	<p>未根据 vRealize Operations Manager 建议放置这些虚拟机，因为您已经指定存储路径。放置可能与 vRealize Operations Manager 的建议相匹配，也可能不匹配。</p> <p>您可以使用自定义属性设置存储路径。</p>

放置错误 — 无法进行基于 vRealize Operations Manager 的放置时，将在错误中描述原因。原因可能包括上述列表中所述的不受支持情况，或者 vRealize Operations Manager 与 vRealize Automation 之间的通信失败等环境因素。

要查看错误，请转到[请求 > 执行](#)。单击右上角附近的[查看放置错误](#)。

工作负载放置限制

在部署新的蓝图时，如果使用工作负载放置的放置策略放置计算机，请注意限制。

- 在 vRealize Operations Manager 中，vRealize Automation 解决方案将标识 vRealize Automation 管理的集群和虚拟机。
- vRealize Automation 在 vRealize Operations Manager 中管理数据中心的子对象或自定义数据中心容器时，重新均衡或移动这些对象的功能不可用。您无法启用或禁用排除 vRealize Automation 受管对象的操作。
- 对于 vRealize Automation 管理的对象，工作负载放置行为如下所示：
 - 当自定义数据中心或数据中心包括 vRealize Automation 管理的集群时，工作负载放置不支持重新均衡集群。
 - 当集群包括 vRealize Automation 管理的虚拟机时，工作负载放置不可用于移动这些虚拟机。
- vRealize Operations Manager 不支持 vCenter Server 中资源池上的工作负载放置。
- vRealize Operations Manager 7.5 及更高版本支持 vSAN 数据存储用于工作负载放置。有关相关信息，请参见 vRealize Operations Manager 7.5 [发行说明](#)。

配置工作负载放置的权限

您必须在 vRealize Automation 和 vRealize Operations Manager 中具有权限才能配置工作负载放置和放置策略。

在 vRealize Automation，必须具有架构管理员角色才能配置工作负载布置。请参见 vRealize Automation 信息中心内的“用户角色概览”。

在 vRealize Operations Manager 中，您必须为工作负载放置创建用户角色，然后将权限分配给该角色。

- 在用户帐户上，从对象层级分配对 vSphere 主机和群集与 vSphere 存储的只读权限。

- 要让用户角色在工作负载放置中使用 API 调用，请分配对 API 的读取和写入权限。选择**管理 > 访问控制 > 权限**，然后选择 **REST API > 所有其他读写 API**。

当您注册端点时，vRealize Automation 使用 vRealize Operations Manager 角色，并在代表请求目录项的用户置备期间请求放置建议。

有关详细信息，请参见 vRealize Operations Manager 信息中心中的“访问控制”。

放置策略

可以使用放置策略让 vRealize Automation 确定部署新蓝图时将计算机放置在何处。放置策略使用 vRealize Operations Manager 的分析来标识群集上的工作负载，以便能够建议放置目标。

在可以使用放置策略之前，必须先执行以下步骤。在 vRealize Automation 中，为 vRealize Operations Manager 和 vCenter Server 实例创建端点。然后，创建架构组，将预留添加到 vCenter Server 端点。

要确保 vRealize Operations Manager 将工作负载放置分析提供给 vRealize Automation，必须执行以下操作：

- 在用于工作负载放置的 vRealize Operations Manager 实例中，安装 vRealize Automation 解决方案。
- 配置 vRealize Operations Manager 以监控 vCenter Server。

要为工作负载放置位置配置 vRealize Automation 和 vRealize Operations Manager，请参见[配置工作负载放置](#)。

找到放置策略

在 vRealize Automation 实例中，选择**基础架构 > 预留 > 放置策略**。

要使用 vRealize Operations Manager 提供的工作负载放置分析，请选择使用 **vRealize Operations Manager 提供放置建议**

如果不使用工作负载放置策略，vRealize Automation 将使用默认的放置方法。

配置工作负载放置

要使用放置策略在部署新蓝图时放置计算机，请将 vRealize Automation 配置为使用 vRealize Operations Manager 提供的分析。此外，还可以将 vRealize Operations Manager 配置为应用策略，以整合并平衡群集计算资源的工作负载。

在 vRealize Automation 中，可以配置端点，然后创建架构组并添加预留。在 vRealize Operations Manager 中，可以配置策略以支持工作负载平衡，并将该策略应用于包括自定义计算资源的自定义组。

前提条件

在放置策略可以建议蓝图的放置目标之前，您必须先执行以下几个步骤。

- 了解放置策略。请参见[放置策略](#)。
- 对于用于工作负载放置的 vRealize Operations Manager 实例，确认 vRealize Automation 中存在端点。请参见[创建 vRealize Operations Manager 端点](#)。
- 对于 vCenter Server 实例，确认 vRealize Automation 中存在端点。请参见[创建 vSphere 端点](#)。

- 将预留添加到 vCenter Server 端点。请参见[预留](#)。
- 添加架构组并确认用户是架构组管理员。请参见[创建架构组](#)。
- 确认 vRealize Operations Manager 监控的基础架构与 vRealize Automation 监控的基础架构相同，从而确保二者均包括相同的 vCenter Server 实例。请参见 vRealize Operations Manager 信息中心内的 [vRealize Operations Manager 中的 VMware vSphere 解决方案](#)。
- 了解预留、存储预留、蓝图和委派提供商。请参见 vRealize Automation 信息中心。
- 了解并定义用于工作负载放置的 vRealize Operations Manager 策略中的填充和平衡设置。请参见 vRealize Operations Manager 信息中心内的[工作负载自动化详细信息](#)。

步骤

1 为 vRealize Automation 配置工作负载放置

要在部署新蓝图时使用工作负载放置分析以放置计算机，必须准备 vRealize Automation 实例。

2 在 vRealize Automation 中为工作负载放置配置 vRealize Operations Manager

要在部署新蓝图时提供对 vRealize Automation 的工作负载放置分析以放置计算机，必须准备 vRealize Operations Manager 实例。

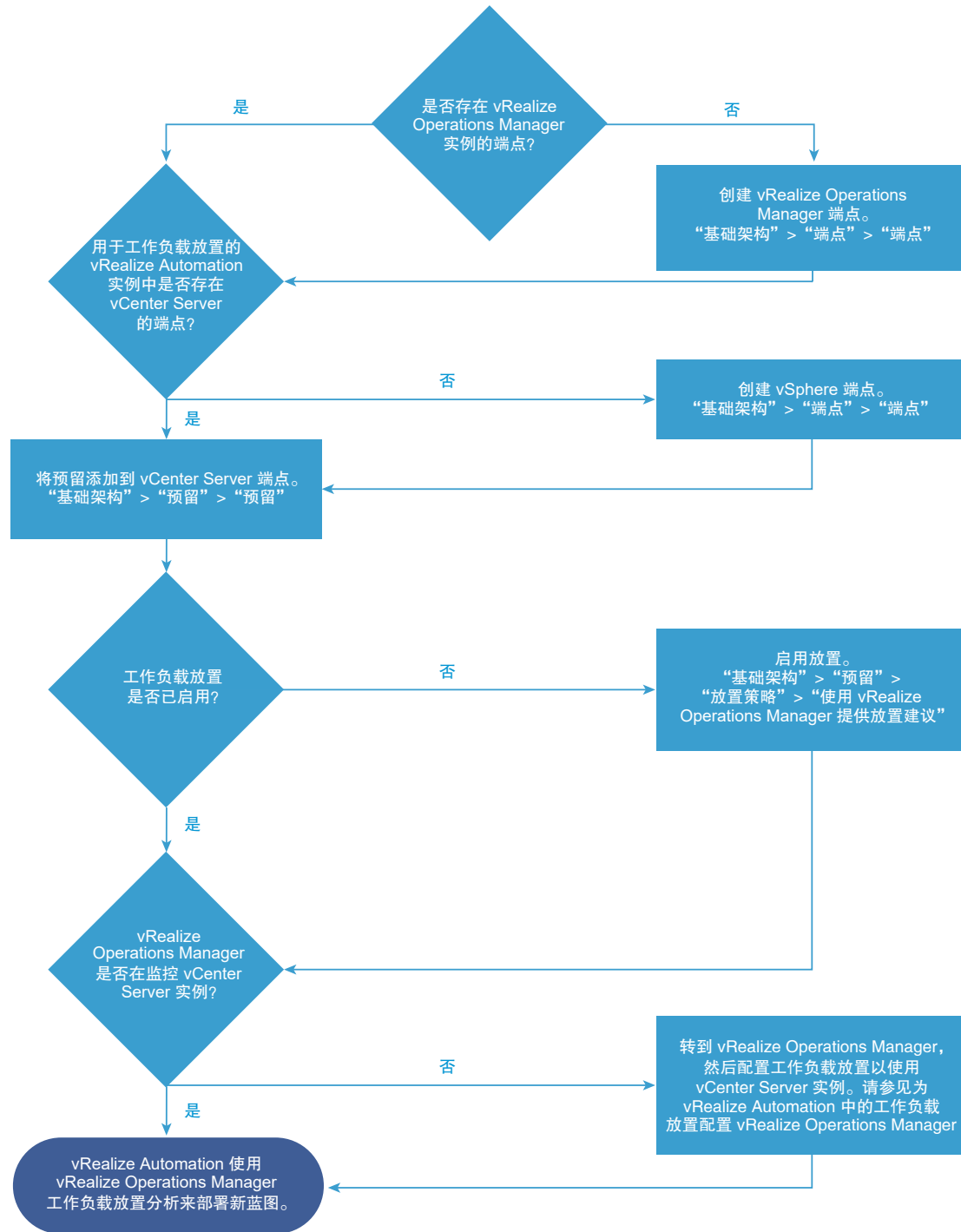
结果

至此，已配置 vRealize Automation 和 vRealize Operations Manager 使用工作负载放置分析来建议新蓝图的放置目标。

为 vRealize Automation 配置工作负载放置

要在部署新蓝图时使用工作负载放置分析以放置计算机，必须准备 vRealize Automation 实例。

要准备 vRealize Automation 实例以使用放置策略，请配置端点，然后创建架构组并添加预留。



前提条件

- 要使用工作负载放置，请了解要求。请参见[配置工作负载放置](#)。
- 在 vRealize Automation 中，为 vRealize Operations Manager 添加特定用户角色和权限以验证凭据。请参见 vRealize Automation 信息中心内的“用户角色概览”。

步骤

- 1 在 vRealize Automation 实例中，为 vRealize Operations Manager 实例添加端点并单击**确定**。
 - a 选择**基础架构 > 端点 > 端点**。
 - b 选择**新建 > 管理 > vRealize Operations Manager**。
 - c 输入 **vRealize Operations Manager** 端点的一般信息。

您无需指定该端点的属性。

- 2 在 vRealize Automation 实例中，为 vCenter Server 实例添加端点并单击**确定**。
 - a 选择**基础架构 > 端点 > 端点**。
 - b 选择**新建 > 虚拟 > vSphere (vCenter)**。
 - c 输入 vCenter Server 端点的一般信息、属性和关联。

添加端点且 vRealize Automation 从中收集数据之后，可以使用这些端点的计算资源。然后，您可以将这些计算资源添加到创建的架构组中。

- 3 创建架构组，使其他用户能够创建预留并启用放置策略。
 - a 选择**基础架构 > 端点 > 架构组**。
 - b 单击**新建**并输入架构组的相关信息。

选项	描述
名称	为架构组输入一个有意义的名称。
描述	输入有用的描述。
架构管理员	为每个指定为架构管理员的用户输入电子邮件地址。
计算资源	选择管理员可管理的计算资源群集。

将计算资源添加到架构组且 vRealize Automation 从中收集数据之后，架构管理员可为计算资源创建预留。

- 4 为 vCenter Server 实例中的计算资源创建预留。
 - a 选择**基础架构 > 预留 > 预留**。
 - b 选择**新建 > vSphere (vCenter)**。
 - c 在每个选项卡上，输入预留的信息。

选项	操作
常规	选择预留策略、策略的优先级并单击 启用此预留 。
资源	选择计算机配额、内存和存储。您无需选择资源池。
网络	选择网络适配器。无需选择网络配置文件。
属性	如果需要，请将自定义属性添加到预留。
警示	如果需要，请选择 容量警示 ，以便在容量超过预留的阈值时通知收件人。

5 启用放置策略。

- a 选择**基础架构 > 预留 > 放置策略**。
- b 选择名为**使用 vRealize Operations Manager 提供放置建议**的复选框。

结果

您已将 vRealize Automation 配置为在用户部署蓝图时使用 vRealize Operations Manager 的分析来放置计算机。

后续步骤

将 vRealize Operations Manager 配置为监控 vCenter Server 实例，并将工作负载放置策略应用于群集计算资源。请参见在 [vRealize Automation 中为工作负载放置配置 vRealize Operations Manager](#)。

在 vRealize Automation 中为工作负载放置配置 vRealize Operations Manager

要在部署新蓝图时提供对 vRealize Automation 的工作负载放置分析以放置计算机，必须准备 vRealize Operations Manager 实例。

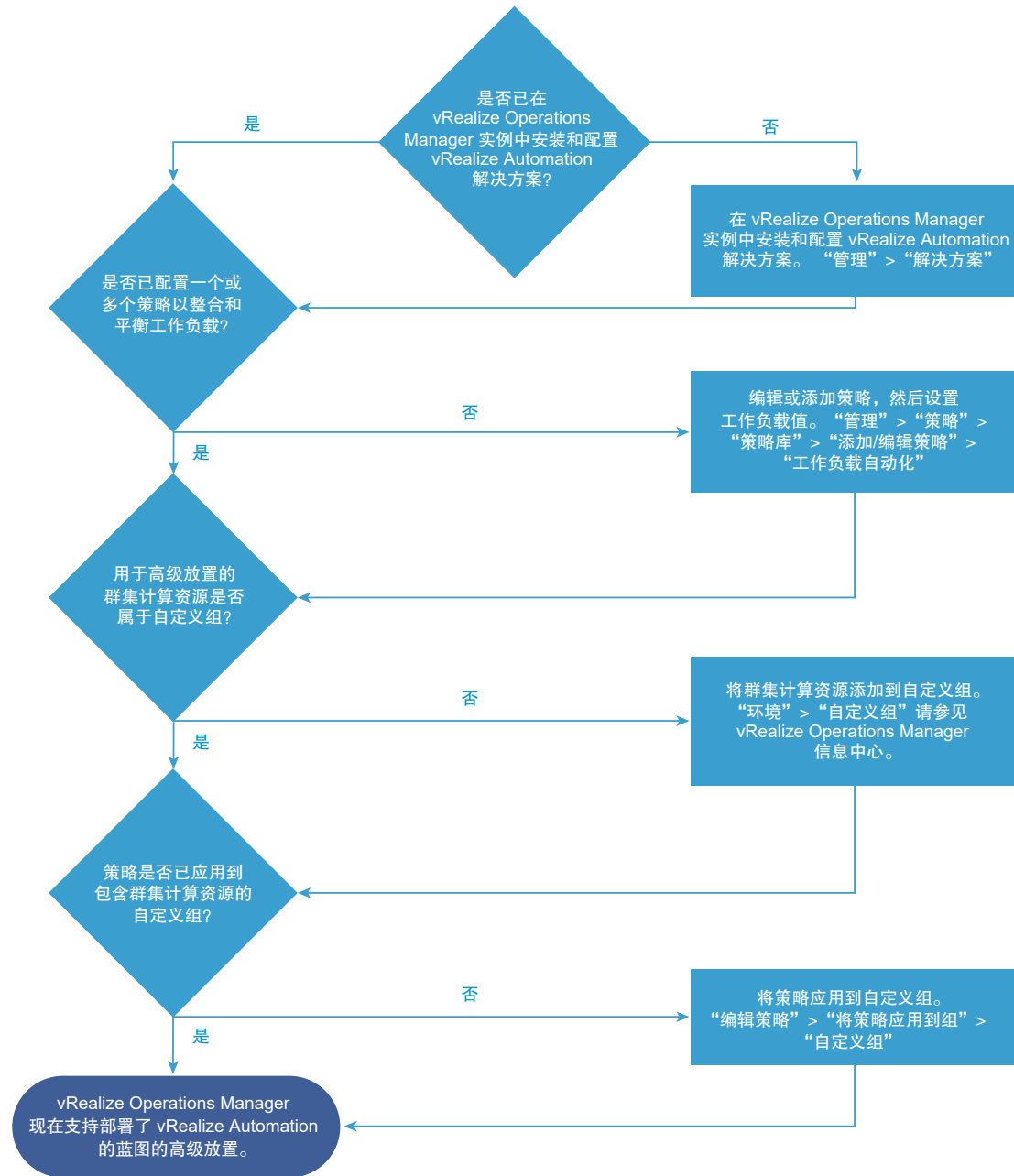
小心 您只能在单个 vRealize Operations Manager 实例上安装包括管理包的 vRealize Automation 解决方案。

要准备 vRealize Operations Manager 实例以提供对 vRealize Automation 的分析，请安装和配置 vRealize Automation 解决方案。此外，还必须配置策略，并将该策略应用于群集计算资源。

配置 vRealize Automation 解决方案之后，不能移动或重新平衡 vRealize Automation 管理的任何虚拟机。

如果 vRealize Operations Manager 实例中未安装 vRealize Automation 解决方案，工作负载放置仍可以移动或重新平衡 vRealize Automation 管理的虚拟机。

要允许工作负载放置移动虚拟机，这些虚拟机必须位于一个数据中心或自定义数据中心。



前提条件

- 将 vRealize Automation 配置为使用工作负载放置分析。请参见 [vRealize Automation 配置工作负载放置](#)。
- 确认已安装 vRealize Automation 解决方案，且已在要用于工作负载放置的 vRealize Operations Manager 实例中进行配置。有关此解决方案的详细信息，请参见 [Solution Exchange 中的 Management Pack for vRealize Automation](#)。有关工作负载放置如何在 vRealize Operations Manager 中运行的信息，请参见 [工作负载自动化详细信息](#) 以及 vRealize Operations Manager 文档中的相关主题。

步骤

- 1 在管理工作负载放置的 vRealize Operations Manager 的实例中，安装并配置 vRealize Automation 解决方案。

该解决方案可能已安装。

- a 要查看 vRealize Operations Manager 中已安装的解决方案，请单击**管理 > 解决方案**。
- b 确认是否已安装 vRealize Automation 解决方案。

如果 vRealize Automation 解决方案在列表中未显示，请下载并安装该解决方案。请参见 [Solution Exchange 中的 Management Pack for vRealize Automation](#)。

- c 如果该解决方案出现在列表中，请选择 **VMware vRealize Automation 解决方案**并单击**配置**。
- d 配置 vRealize Automation 解决方案并保存设置。

有关配置解决方案的详细信息，请参见 vRealize Operations Manager 信息中心内的 [vRealize Operations Manager 中的解决方案](#)。

- 2 如果不使用 vRealize Operations Manager 默认策略，必须创建自定义组。然后，将您的群集计算资源添加到自定义组。

要将除默认策略以外的策略应用于群集，请添加自定义组。然后，将策略应用于该自定义组。如果使用默认策略，则无需创建自定义组，因为默认策略可应用于所有对象。

- a 单击**环境 > 自定义组**。
- b 如果群集没有自定义组，请创建一个自定义组。

有关详细信息，请参见 vRealize Operations Manager 信息中心内的[用户场景：创建自定义对象组](#)。

- c 将群集添加到自定义组并保存该组。

- 3 配置策略以整合和平衡群集上的工作负载，并将该策略应用于自定义组。

您可在 vRealize Operations Manager 中配置策略，为整合、平衡、填充、CPU、内存和磁盘空间建立设置。例如，您可修改名为“整合工作负载”的设置，使其根据群集状态和容量确定新的受管工作负载的最佳放置。此外，您还可以将“平衡工作负载”的阈值设置修改为放置工作负载所需的积极性级别。您可以配置一个或多个策略，并将其应用于群集计算资源。

- a 要找到策略，请单击**管理 > 策略 > 策略库**。
- b 要设置工作负载值，请单击**添加/编辑策略**，然后单击**工作负载自动化**。

名为“整合工作负载”和“群集空间”的设置应用于虚拟机的初始放置。

- 将“整合工作负载”设置为**无**时，工作负载放置将在应用策略的所有群集之间平衡工作负载。将“整合工作负载”设置为“无”以外的值时，工作负载放置将首先填充最繁忙的群集。
- “群集空间”是在群集中预留的缓冲区空间，表示为总容量的百分比。例如，如果将群集空间设置为 20%，该缓冲区可能会阻止工作负载放置在该群集上放置虚拟机。阻止放置的原因是群集中用于 CPU、内存或磁盘空间的可用容量不到 20%。

- c 在策略工作区中，单击**将策略应用于组**。

- d 选择自定义组。
- e 保存策略。

结果

您已配置 vRealize Operations Manager，使 vRealize Automation 能够在用户部署蓝图时使用工作负载放置分析，以建议计算机的放置目标。

后续步骤

等待 vRealize Automation 和 vRealize Operations Manager 从环境中的端点和对象中收集数据。然后，部署新蓝图时，vRealize Automation 将显示工作负载放置建议、目标候选项和选定放置，供您确认。

工作负载放置的故障排除

如果遇到工作负载放置问题，可使用故障排除信息加以解决。

需要 vRealize Automation 解决方案，工作负载放置才可正常运行

工作负载放置基于单个计算机，且将在计算机级别完成放置。当 vRealize Automation 和 vRealize Operations Manager 一起安装时，还必须安装 vRealize Automation 解决方案。

该解决方案包含管理包和适配器，可识别停用重新均衡容器或移动虚拟机操作的集群。重新均衡操作在集群所属的自定义数据中心上处于停用状态。

- 对于所属的自定义数据中心不具有任何受管 vRealize Automation 集群的非受管 vRealize Automation 集群，移动虚拟机和重新均衡容器操作处于启用状态。对于受管 vRealize Automation 集群，这些操作处于停用状态。
- 在 vRealize Operations Manager 中，vRealize Automation 适配器会导致映射预留的集群上的虚拟机不可移动或重新均衡。

小心 vRealize Automation 解决方案只能安装在单个 vRealize Operations Manager 实例上。

已启用高可用性，但必须要停用

启用 HA 之后，如果 vRealize Operations Manager 已关闭，则调用 vRealize Operations Manager 的工作负载放置超时，可能会失败。

vRealize Automation 在 `catalina.out` 日志文件中记录工作负载放置错误。

不监控 vRealize Automation 中的 vSphere 端点

vRealize Operations Manager 不监控包含预留集群的 vSphere vCenter Server 实例。

如果 vRealize Operations Manager 在尝试放置集群、数据存储或数据存储集群的 vRealize Automation 候选预留时不能对其进行识别，会将其忽略。在放置响应中，vRealize Operations Manager 与不识别这些候选预留的 vRealize Automation 进行通信。

因此，在有关请求执行的放置详细信息中，vRealize Automation 在候选预留上显示警告图标，以表明该候选预留无法识别。

出现不匹配时，vRealize Automation 出现在列表顶部

vRealize Automation 和 vRealize Operations Manager 管理不同的基础架构视图。但是，它们必须管理相同基础架构中的相同 vCenter Server 实例。

必须识别断开连接和不匹配现象，并显示详细信息。

如果 vRealize Automation 适配器已关闭，该怎么做？

初始放置始终（例如，当用户在安装之后立即添加集群时）接受适配器从 vRealize Operations Manager 中接收的目标候选项列表。

如果 vRealize Automation 解决方案（其中包括管理包和适配器）在 vRealize Operations Manager 中不可用，则移动虚拟机和重新均衡容器操作将不可用。

使用 vRealize Operations Manager 连续优化

连续优化提供 vRealize Operations Manager 对 vRealize Automation 工作负载的持续、自治管理。

使用连续优化，您可以充分利用工作负载重新平衡和重新放置，并且除初始工作负载放置外，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。

- 连续优化会在 vRealize Operations Manager 中自动创建新的数据中心。

每个 vRealize Automation vCenter 端点都有一个新的数据中心。

- 新创建的数据中心包含与端点关联的每个 vRealize Automation 受管群集。

注 请勿手动创建 vRealize Automation 和非 vRealize Automation 群集的混合数据中心。

- 只能从新创建的基于 vRealize Automation 的数据中心运行连续优化。
- 优化不支持在 vCenter 的群集之间具有不同的预留要求，当您具有不同的业务组时可能会出现这种情况。

优化在基于 vRealize Automation 的数据中心级别执行，群集之间的预留要求不同可能会阻止优化成功。如果发生这种情况，则会出现错误，指出某些目标群集或存储不满足要求，会阻止某些优化执行。

- 优化永远不会制造新的违反 vRealize Automation 或 vRealize Operations Manager 策略的情况。

- 如果您现有策略违规，优化可以修复 vRealize Operations Manager 运维意图问题。

- 如果您现有策略违规，优化无法修复 vRealize Operations Manager 业务意图问题。

例如，如果您将虚拟机手动移至不属于其预留策略的群集，那么 vRealize Operations Manager 不检测违规情况，也不尝试进行解决。要修复业务意图问题，必须使用 vRealize Automation 移动工作负载。

- 本版本在数据中心级别遵循运维意图。所有成员 vRealize Automation 群集已优化为相同的设置。

要为群集设置不同的运维意图，必须与不同 vCenter 端点关联的不同 vRealize Automation 数据中心中配置它们。采用不同的测试和生产群集可能就是一个示例情况。

- vRealize Operations Manager 基于 vRealize Automation 策略和预留向 vRealize Automation 查询允许的放置。

- vRealize Operations Manager 放置标记无法应用于 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。

在 vRealize Automation 中查找不平衡的工作负载

vRealize Automation 可以显示何时置备到同一群集的工作负载过重。

步骤

- 1 要查看将工作负载置备到哪里，请单击**基础架构 > 计算资源 > 计算资源**。
记下任何不均衡的计算机放置。
- 2 预留可能会导致大量置备到同一群集。要查看预留，请单击**基础架构 > 预留 > 预留**。
记下优先级以及这可能会如何影响计算机放置。

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。

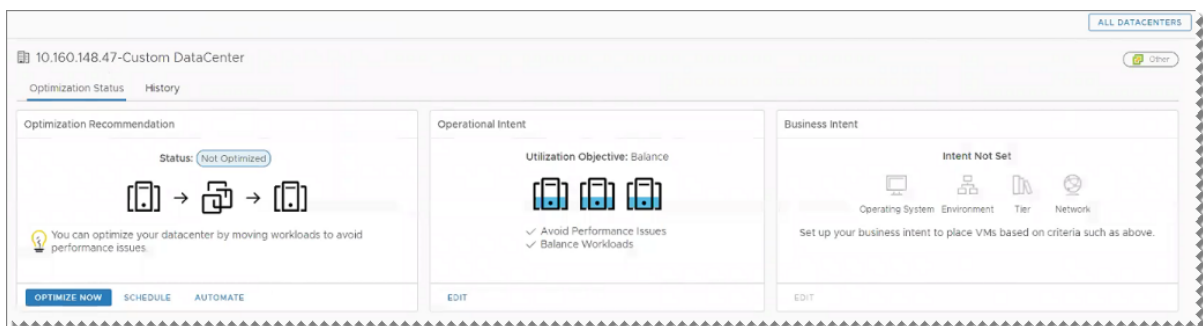
除了添加适配器，连续优化不需要执行单独的安装步骤。您可以在新数据中心中开始配置和使用 vRealize Operations Manager 进行工作负载重新放置。请参见[连续优化示例](#)。

连续优化示例

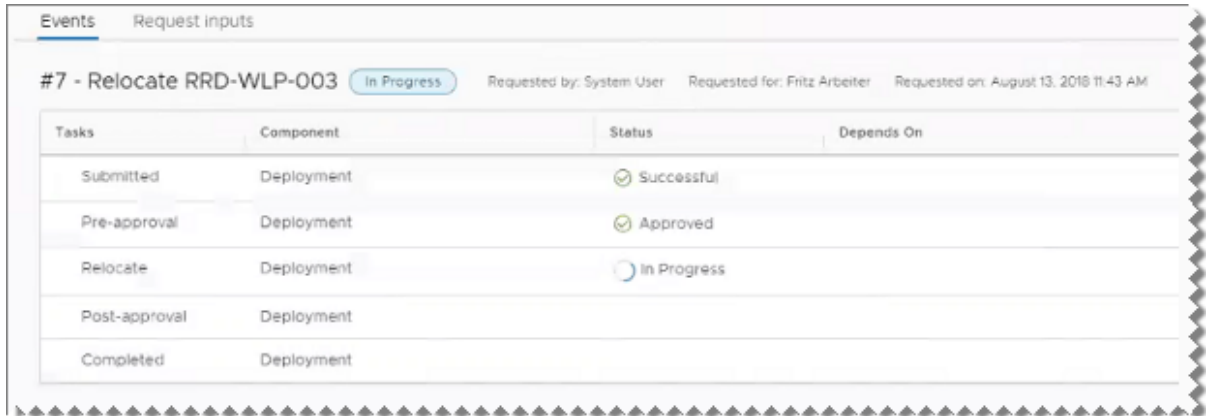
以下示例显示了使用 vRealize Operations Manager 进行 vRealize Automation 连续优化的重新均衡工作流。

- 1 在 vRealize Operations Manager 中，选择自动创建的 vRealize Automation 数据中心。
- 2 在**运维意图**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 优化时已停用这些操作。



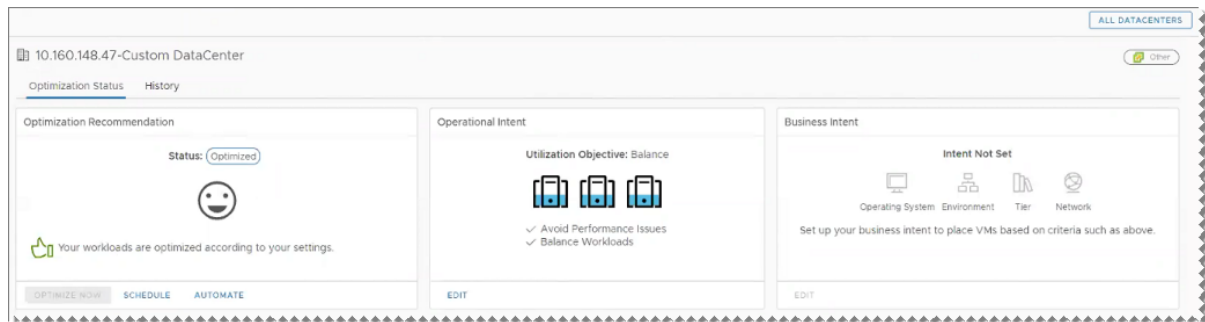
- 3 在**优化建议**下，单击**立即优化**。
vRealize Operations Manager 将显示建议操作的前后对比图。
- 4 单击**下一步**。
- 5 单击**开始操作**。
- 6 在 vRealize Automation 中，通过单击**部署**并查看事件状态来监控正在进行的操作。



Tasks	Component	Status	Depends On
Submitted	Deployment	Successful	
Pre-approval	Deployment	Approved	
Relocate	Deployment	In Progress	
Post-approval	Deployment		
Completed	Deployment		

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。



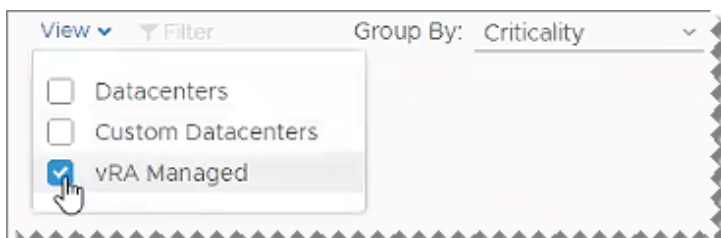
在 vRealize Operations Manager 中，可以通过单击**管理 > 历史记录 > 近期任务**来查看该操作。

在 vRealize Operations Manager 中查找 vRealize Automation 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 中，单击**所有数据中心**。
- 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。



管理密钥对

密钥对用于置备和连接到云实例。此外，密钥对还可用于解密 Windows 密码或登录到 Linux 计算机。

使用 Amazon AWS 置备时需要密钥对。对于 Red Hat OpenStack，密钥对是可选的。

添加云端点时，现有密钥对作为数据收集的一部分导入。此外，架构管理员也可以使用 vRealize Automation 控制台创建并管理密钥对。如果从 vRealize Automation 控制台中删除密钥对，则还会将其从云服务帐户中删除。

除了手动管理密钥对之外，您还可以将 vRealize Automation 配置为按计算机或业务组自动生成密钥对。

- 架构管理员可以配置密钥对在预留级别自动生成。
- 如果要在蓝图级别控制密钥对，则架构管理员必须针对该预留选择**未指定**。
- 租户管理员或业务组主管可以配置密钥对在蓝图级别自动生成。
- 如果同时在预留和蓝图级别控制密钥对的生成，则预留设置将替代蓝图设置。

创建密钥对

您可以使用 vRealize Automation 创建与端点一起使用的密钥对。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 创建云端点，并将云计算资源添加到架构组。请参见[选择端点场景](#)和[创建架构组](#)。

步骤

- 1 选择**基础架构 > 预留 > 密钥对**。
- 2 单击**新建**。
- 3 在**名称**文本框中输入名称。
- 4 从**计算资源**下拉菜单中选择云区域。
- 5 单击**确定**。

结果

当“密钥”列具有值 ***** 时，表明密钥对随时可用。

为密钥对上载私有密钥

您可以采用 PEM 格式为密钥对上载私有密钥。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 您必须已拥有密钥对。请参见[创建密钥对](#)。

步骤

- 1 选择**基础架构 > 预留 > 密钥对**。
- 2 找到要上载私有密钥的密钥对。
- 3 单击**编辑**图标 (✎)。

4 可使用以下方法之一上传该密钥。

- 浏览采用 PEM 编码的文件，然后单击**上传**。
- 粘贴以 -----BEGIN RSA PRIVATE KEY----- 开头、-----END RSA PRIVATE KEY----- 结尾的私有密钥文本。

5 单击**保存**图标 (✔)。

从密钥对导出私有密钥

您可以将私有密钥从密钥对导出到采用 PEM 编码的文件中。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 必须存在包含私有密钥的密钥对。请参见[为密钥对上载私有密钥](#)。

步骤

- 1 选择**基础架构 > 预留 > 密钥对**。
- 2 找到要从中导出私有密钥的密钥对。
- 3 单击**导出**图标 (📄)。
- 4 浏览到要保存文件的位置，然后单击**保存**。

场景：为跨区域部署将位置应用到计算资源

作为一名架构管理员，您需要将计算资源标记为属于波士顿或伦敦数据中心，从而支持跨区域部署。当蓝图架构师在其蓝图上启用位置功能时，用户能够选择是在波士顿还是伦敦数据中心置备计算机。



您在伦敦和波士顿分别设有一个数据中心，但不希望位于波士顿的用户在伦敦的基础架构中置备计算机，反之亦然。为了确保位于波士顿和伦敦的用户在各自的基础架构中置备计算机，您需要允许用户在请求计算机时选择适当的位置进行置备。

前提条件

- 以**架构管理员**身份登录到 vRealize Automation。
- 作为一名系统管理员，请定义数据中心位置。请参见[场景：为跨区域部署添加数据中心位置](#)。

步骤

- 1 选择**基础架构 > 计算资源 > 计算资源**。
- 2 指向位于波士顿数据中心的计算资源，然后单击**编辑**。
- 3 从**位置**下拉菜单中选择“波士顿”。
- 4 单击**确定**。
- 5 根据需要重复上述过程，将计算资源与“波士顿”和“伦敦”位置关联。

结果

IaaS 架构师可以启用位置功能，使用户能够在填写目录项请求表单时选择在波士顿或伦敦置备计算机。请参见[使用户能为跨区域部署选择数据中心位置](#)。

使用第三方 IPAM 提供程序置备 vRealize Automation 部署

您可以从支持的第三方 IPAM 解决方案提供程序（例如 Infoblox）获取用于 vRealize Automation 网络配置文件的 IP 地址和范围。

网络配置文件中的 IP 地址范围用于您在蓝图中指定的相关预留。当授权用户请求使用蓝图目录项置备计算机时，可以从第三方 IPAM 特定的 IP 地址范围中获取 IP 地址。部署计算机后，您可以通过查询其 vRealize Automation 项目详细信息页面查找使用的 IP 地址。

表 2-19. 使用 Infoblox IPAM 对照表，准备置备 vRealize Automation 部署

任务	描述	详细信息
获取、导入和配置第三方 IPAM 解决方案提供程序插件或软件包。	获取并导入 vRealize Orchestrator 插件，运行 vRealize Orchestrator 配置工作流，并在 vRealize Orchestrator 中注册 IPAM 提供程序端点类型。 如果 VMware Solution Exchange（网址为 https://marketplace.vmware.com/vsx ）不包含您需要的 IPAM 提供程序软件包，您可以使用 IPAM 解决方案提供程序 SDK 和支持文档创建您自己的软件包。请参见 vRealize Automation 示例第三方 IPAM 软件包 页面 (code.vmware.com/web/sdk)。	请参见 用于提供第三方 IPAM 提供程序支持的对照表 。
创建第三方 IPAM 解决方案提供程序端点。	在 vRealize Automation 中创建新的 IPAM 端点。	请参见 创建第三方 IPAM 提供程序端点 。
在外部网络配置文件中指定第三方 IPAM 解决方案提供程序端点设置。	创建外部网络配置文件，并在 vRealize Automation 中指定定义的 IPAM 端点。	请参见 使用第三方 IPAM 提供程序创建外部网络配置文件 。
也可以在路由网络配置文件中指定第三方 IPAM 解决方案提供程序端点设置。	创建按需网络配置文件，并在 vRealize Automation 中指定定义的 IPAM 端点。	请参见 使用第三方 IPAM 端点创建路由网络配置文件 或 使用第三方 IPAM 端点创建 NAT 网络配置文件 。
定义预留以使用网络配置文件。	创建在 vRealize Automation 中调用网络配置文件的预留。	请参见 为 Hyper-V、KVM、SCVMM、vSphere 或 XenServer 创建预留 。
定义使用网络配置文件的蓝图。	在 vRealize Automation 中创建使用该预留的蓝图。	请参见 第 3 章 向用户提供服务蓝图 。

表 2-19. 使用 Infoblox IPAM 对照表，准备置备 vRealize Automation 部署（续）

任务	描述	详细信息
将蓝图发布到目录，使其可供使用。	将蓝图发布到 vRealize Automation 中的目录。添加任何所需的授权。	请参见 发布蓝图 。
通过使用蓝图目录项，请求计算机置备。	使用蓝图目录项请求 vRealize Automation 中的计算机置备。	请参见 管理服务目录 。

配置 XaaS 资源

通过配置 XaaS 端点，您可以将 vRealize Automation 连接到环境。将 vRealize Orchestrator 插件配置为端点时，请使用 vRealize Automation 用户界面配置插件，而非使用 vRealize Orchestrator 配置界面。

要使用 vRealize Orchestrator 功能和 vRealize Orchestrator 插件向 vRealize Automation 公开 VMware 和第三方技术，您可以通过将 vRealize Orchestrator 插件添加为端点来配置这些插件。通过这种方式，您可以创建与不同主机和服务器的连接，例如，vCenter Server 实例、Microsoft Active Directory 主机等。

通过使用 vRealize Automation UI 将 vRealize Orchestrator 插件添加为端点时，您将在默认的 vRealize Orchestrator 服务器中运行配置工作流。配置工作流位于 **vRealize Automation > XaaS > 端点配置** 工作流文件夹中。

重要事项 不支持在 vRealize Orchestrator 和 vRealize Automation 控制台中配置单个插件，否则将导致出现错误。

将 Active Directory 插件配置为端点

您可以添加端点，将 Active Directory 插件配置为连接到正在运行的 Active Directory 实例，并管理用户和用户组、Active Directory 计算机、组织单位等。

添加 Active Directory 端点之后，可以随时更新该端点。

前提条件

- 确认您有权访问 Microsoft Active Directory 实例。请参见 Microsoft Active Directory 文档。
- 以租户管理员身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > vRO 配置 > 端点**。
- 2 单击**新建**图标 (+)。
- 3 在**插件**下拉菜单中选择 **Active Directory**。
- 4 单击**下一步**。
- 5 输入名称和可选描述。
- 6 单击**下一步**。

7 配置 Active Directory 服务器的详细信息。

- a 在 **Active Directory 主机 IP/URL** 文本框中，输入运行 Active Directory 的主机的 IP 地址或 DNS 名称。

- b 在**端口**文本框中，输入 Active Directory 服务器的查找端口。

vRealize Orchestrator 支持 Active Directory 分层域结构。如果域控制器配置为使用全局目录，则必须使用端口 3268。不能使用默认端口 389 连接到全局目录服务器。除了端口 389 和 3268 之外，您还可以对 LDAPS 使用 636。

- c 在**根**文本框中，输入 Active Directory 服务的根元素。

例如，如果域名是 *mycompany.com*，则根 Active Directory 为 **dc=mycompany,dc=com**。

输入相应凭据之后，此节点用于浏览服务目录。对于大型服务目录，在树中指定节点可缩小搜索范围并提高性能。例如，您可以指定 **ou=employees,dc=mycompany,dc=com**，而不是搜索整个目录。此根元素显示员工组中的所有用户。

- d （可选）要为 vRealize Orchestrator 与 Active Directory 之间的连接激活加密认证，请从**使用 SSL** 下拉菜单中选择**是**。

SSL 证书将自动导入，而不会提示进行确认，即便该证书是自签名证书也是如此。

- e （可选）在**默认域**文本框中，输入相应域。

例如，如果域名是 *mycompany.com*，请键入 **@mycompany.com**。

8 配置共享会话设置。

vRealize Orchestrator 可使用凭据运行所有 Active Directory 工作流和操作。

- a 在**共享会话的用户名**文本框中，输入共享会话的用户名。

- a 在**共享会话的密码**文本框中，输入共享会话的密码。

9 单击完成。

结果

您已将 Active Directory 实例添加为端点。XaaS 架构师可以使用 XaaS 将 Active Directory 插件工作流作为目录项和资源操作发布。

后续步骤

- 要使用 vRealize Automation 蓝图管理环境中的 Active Directory 用户，请创建一个基于 Active Directory 的 XaaS 蓝图。例如，请参见[创建用于创建和修改用户的 XaaS 蓝图和操作](#)。
- 要在部署计算机时使用 vRealize Automation 创建 Active Directory 记录，您可以创建不同的 Active Directory 策略并将其应用于不同的业务组和蓝图。请参见[创建并应用 Active Directory 策略](#)。

将 HTTP-REST 插件配置为端点

您可以添加端点并将 HTTP-REST 插件配置为连接到 REST 主机。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation。
- 确认您有权访问 REST 主机。

步骤

- 1 选择**管理 > vRO 配置 > 端点**。
 - 2 单击**新建**图标(+)。
 - 3 从**插件**下拉菜单中选择 **HTTP-REST**。
 - 4 单击**下一步**。
 - 5 输入名称和可选描述。
 - 6 单击**下一步**。
 - 7 提供 REST 主机的相关信息。
 - a 在**名称**文本框中输入主机的名称。
 - b 在 **URL** 文本框中输入主机的地址。
-
- 注** 如果使用 Kerberos 访问身份验证，则必须以 **FDQN** 格式提供主机地址。
-
- c (可选) 在**连接超时 (秒)** 文本框中，输入连接超时之前的秒数。
默认值为 30 秒。
 - d (可选) 在**操作超时 (秒)** 文本框中，输入操作超时之前的秒数。
默认值为 60 秒。
- 8 (可选) 配置代理设置。
 - a 从**使用代理**下拉菜单中，选择**是**以使用代理。
 - b 在**代理地址**文本框中，输入代理服务器的 IP。
 - c 在**代理端口**文本框中，输入要与代理服务器通信的端口号。
 - 9 单击**下一步**。
 - 10 选择身份验证类型。

选项	操作
无	无需进行身份验证。
OAuth 1.0	使用 OAuth 1.0 协议。必须提供 OAuth 1.0 下所需的身份验证参数。 <ol style="list-style-type: none"> a 在使用者密钥文本框中，输入用于将使用者标识为服务提供程序的密钥。 b 在使用者密钥文本框中，输入用于建立使用者密钥所有权的密钥。 c (可选) 在访问令牌文本框中，输入使用者用于访问受保护资源的访问令牌。 d (可选) 在访问令牌密钥文本框中，输入使用者用于建立令牌所有权的密钥。

选项	操作
OAuth 2.0	使用 OAuth 2.0 协议。 在 令牌 文本框中输入身份验证令牌。
基本	提供基本访问身份验证。与主机进行的通信处于共享会话模式。 a 在 身份验证用户名 文本框中，输入共享会话的用户名。 b 在 身份验证密码 文本框中，输入共享会话的密码。
摘要	提供使用加密的摘要访问身份验证。与主机进行的通信处于共享会话模式。 a 在 身份验证用户名 文本框中，输入共享会话的用户名。 b 在 身份验证密码 文本框中，输入共享会话的密码。
NTLM	在 Windows 安全支持提供者 (SSP) 框架内，提供 NT LAN Manager (NTLM) 访问身份验证。与主机进行的通信处于共享会话模式。 a 提供共享会话的用户凭据。 ■ 在 身份验证用户名 文本框中，输入共享会话的用户名。 ■ 在 身份验证密码 文本框中，输入共享会话的密码。 b 配置 NTLM 详细信息 ■ (可选) 在 NTLM 身份验证工作站 文本框中，输入工作站名称。 ■ 在 NTLM 身份验证域 文本框中，输入域名。
Kerberos	提供 Kerberos 访问身份验证。与主机进行的通信处于共享会话模式。 a 在 身份验证用户名 文本框中，输入共享会话的用户名。 b 在 身份验证密码 文本框中，输入共享会话的密码。

11 单击完成。

结果

您已配置端点并添加 REST 主机。XaaS 架构师可以使用 XaaS 将 HTTP-REST 插件 workflow 库作为目录项和资源操作发布。

将 PowerShell 插件配置为端点

您可以添加端点并将 PowerShell 插件配置为连接到正在运行的 PowerShell 主机，以便从 vRealize Orchestrator 操作和工作流中调用 PowerShell 脚本和 cmdlet 并处理结果。

前提条件

- 确认您有权访问 Windows PowerShell 主机。有关 Microsoft Windows PowerShell 的详细信息，请参见 Windows PowerShell 文档。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > vRO 配置 > 端点**。
- 2 单击**新建**图标 (+)。
- 3 从**插件**下拉菜单中选择 **PowerShell**。
- 4 单击**下一步**。

- 5 输入名称和可选描述。
- 6 单击下一步。
- 7 指定 PowerShell 主机详细信息。
 - a 在**名称**文本框中输入主机的名称。
 - b 在**主机/IP**文本框中输入主机的 IP 地址或 FDQN。
- 8 选择插件连接到的 PowerShell 主机类型。

选项	操作
WinRM	<ol style="list-style-type: none"> a 在 PowerShell 主机详细信息下的端口文本框中，输入与主机通信使用的端口号。 b 从传输协议下拉菜单中选择传输协议。 <div style="margin-top: 5px;"> <p>注 如果使用 HTTPS 传输协议，则远程 PowerShell 主机的证书将导入到 vRealize Orchestrator 密钥库。</p> </div> c 从身份验证下拉菜单中选择身份验证类型。 <div style="margin-top: 5px;"> <p>注 要使用 Kerberos 身份验证，请在 WinRM 服务上启用它。有关配置 Kerberos 身份验证的信息，请参见使用 PowerShell 插件。</p> </div>
SSH	无。

- 9 在**用户名**和**密码**文本框中，输入与 PowerShell 主机共享会话通信的凭据。
- 10 单击完成。

结果

您已将 Windows PowerShell 主机端点为添加。XaaS 架构师可以使用 XaaS 将 PowerShell 插件工作流库作为目录项和资源操作发布。

将 SOAP 插件配置为端点

您可以添加端点并配置 SOAP 插件，使其将 SOAP 服务定义为清单对象并对定义的对象执行 SOAP 操作。

前提条件

- 确认您有权访问 SOAP 主机。该插件支持 SOAP 版本 1.1 和 1.2 及 WSDL 1.1 和 2.0。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > vRO 配置 > 端点**。
- 2 单击**新建**图标 (+)。
- 3 从**插件**下拉菜单中，选择 **SOAP**。
- 4 单击下一步。
- 5 输入名称和可选描述。

6 单击下一步。**7** 提供有关 SOAP 主机的详细信息。

- a 在**名称**文本框中输入主机的名称。
- b 从**提供 WSDL 内容**下拉菜单中，选择是否将 WSDL 内容作为文本提供。

选项	操作
是	在 WSDL 内容 文本框中输入 WSDL 文本。
否	在 WSDL URL 文本框中，输入正确的路径。

- c （可选）在**连接超时 (以秒为单位)** 文本框中，输入连接超时之前的秒数。
默认值为 30 秒。
- d （可选）在**请求超时 (以秒为单位)** 文本框中，输入操作超时之前的秒数。
默认值为 60 秒。

8 （可选）指定代理设置。

- a 要使用代理，请从**代理**下拉菜单中选择**是**。
- b 在**地址**文本框中，输入代理服务器的 IP。
- c 在**端口**文本框中，输入要与代理服务器通信的端口号。

9 单击下一步。**10** 选择身份验证类型。

选项	操作
无	无需进行身份验证。
基本	提供基本访问身份验证。与主机进行的通信处于共享会话模式。 a 在 用户名 文本框中，输入共享会话的用户名。 b 在 密码 文本框中，输入共享会话的密码。
摘要	提供使用加密的摘要访问身份验证。与主机进行的通信处于共享会话模式。 a 在 用户名 文本框中，输入共享会话的用户名。 b 在 密码 文本框中，输入共享会话的密码。

选项	操作
NTLM	<p>在 Windows 安全支持提供者 (SSP) 框架内，提供 NT LAN Manager (NTLM) 访问身份验证。与主机进行的通信处于共享会话模式。</p> <ol style="list-style-type: none"> 提供用户凭据。 <ul style="list-style-type: none"> 在 用户名 文本框中，输入共享会话的用户名。 在 密码 文本框中，输入共享会话的密码。 提供 NTLM 设置。 <ul style="list-style-type: none"> 在 NTLM 域 文本框中，输入域名。 (可选) 在 NTLM 工作站 文本框中，输入工作站名称。
协商	<p>提供 Kerberos 访问身份验证。与主机进行的通信处于共享会话模式。</p> <ol style="list-style-type: none"> 提供用户凭据。 <ol style="list-style-type: none"> 在 用户名 文本框中，输入共享会话的用户名。 在 密码 文本框中，输入共享会话的密码。 在 Kerberos 服务 SPN 文本框中，输入 Kerberos 服务 SPN。

11 单击完成。

结果

您已添加 SOAP 服务。XaaS 架构师可以使用 XaaS 将 SOAP 插件工作流作为目录项和资源操作发布。

将 vCenter Server 插件配置为端点

您可以添加端点并将 vCenter Server 插件配置为连接到正在运行的 vCenter Server 实例，以便创建 XaaS 蓝图来管理 vSphere 清单对象。

前提条件

- 安装并配置 vCenter Server。请参见《vSphere 安装和设置》。
- 以 **租户管理员** 身份登录到 vRealize Automation。

步骤

- 1 选择 **管理 > vRO 配置 > 端点**。
- 2 单击 **新建** 图标 (+)。
- 3 从 **插件** 下拉菜单中选择 **vCenter Server**。
- 4 单击 **下一步**。
- 5 输入名称和可选描述。
- 6 单击 **下一步**。

7 提供 vCenter Server 实例的相关信息。

- a 在**要添加的 vCenter Server 实例的 IP 或主机名**文本框中，输入计算机的 IP 地址或 DNS 名称。
这是安装您要添加的 vCenter Server 实例的计算机 IP 地址或 DNS 名称。
- b 在**vCenter Server 实例的端口**文本框中，输入要与 vCenter Server 实例通信的端口。
默认端口为 443。
- c 在**用于连接到 vCenter Server 实例的 SDK 的位置**文本框中，输入要用于连接到 vCenter Server 实例的 SDK 的位置。
例如，`/sdk`。

8 单击下一步。**9 定义连接参数。**

- a 在**vCenter Server 实例的 HTTP 端口 - 适用于 VC 插件版本 5.5.2 或更早版本**文本框中，输入 vCenter Server 实例的 HTTP 端口。
- b 在**Orchestrator 将用于连接到 vCenter Server 实例的用户的用户名和 Orchestrator 将用于连接到 vCenter Server 实例的用户的密码**文本框中，输入 vRealize Orchestrator 用于与 vCenter Server 实例建立连接的凭据。

所选的用户必须是有权管理 vCenter Server 扩展和一组自定义特权的有效用户。

10 单击完成。**结果**

您已将 vCenter Server 实例添加为端点。XaaS 架构师可以使用 XaaS 将 vCenter Server 插件工作流程作为目录项和资源操作发布。

创建 Microsoft Azure 端点

您可以创建 Microsoft Azure 端点，促进 vRealize Automation 与 Azure 部署之间的凭据式连接。通过使用提供的

端点与资源建立连接，可用于创建虚拟机蓝图，本例中的资源为 Azure 实例。必须使用 Azure 端点作为置备 Azure 虚拟机的蓝图基础。如果使用多个 Azure 订阅，则需要为每个订阅 ID 创建端点。

或者，您可以使用“添加 Azure 连接”命令（位于 vRealize Orchestrator 工作流树中的 **库 > Azure > 配置**下）直接从 vRealize Orchestrator 创建 Azure 连接。对于大多数情况，通过端点配置创建连接（如本文中所述）是首选选项。

vRealize Orchestrator 和 XaaS 功能支持 Azure 端点。您可以创建、删除或编辑 Azure 端点。如果更改现有端点后几个小时内不通过更新的连接在 Azure 门户上运行任何更新，可能会出现问题。您必须使用 `service vco-service restart` 命令重新启动 vRealize Orchestrator 服务。重新启动该服务失败可能会导致出现错误。

前提条件

- 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。有关配置 Azure 和获取订阅 ID 的详细信息，请参见 [Microsoft Azure 端点配置](#)。
- 确认您的 vRealize Automation 部署至少具有一个租户和一个业务组。
- 按照 <https://azure.microsoft.com/zh-cn/documentation/articles/resource-group-create-service-principal-portal> 中所述创建 Active Directory 应用程序。
- 请记录以下 Azure 相关信息，因为在配置端点和蓝图时将需要这些信息。
 - 订阅 ID
 - 租户 ID
 - 存储帐户名称
 - 资源组名称
 - 位置
 - 虚拟网络名称
 - 客户端应用程序 ID
 - 客户端应用程序密钥
 - 虚拟机映像 URN
- vRealize Automation Azure 实施支持 Microsoft Azure 支持的区域的子集。请参见 [Azure 支持的区域](#)。
- 以**租户管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > vRO 配置 > 端点**。
- 2 单击**新建**图标 (+)。
- 3 在“插件”选项卡上，单击**插件**下拉菜单并选择 **Azure**。
- 4 单击**下一步**。
- 5 输入名称和可选描述。
- 6 单击**下一步**。
- 7 根据需要为端点填充“详细信息”选项卡上的文本框。

参数	描述
连接设置	
连接名称	新端点连接的唯一名称。此名称显示在 vRealize Orchestrator 界面中，以帮助标识特定连接。

参数	描述
Azure 订阅 ID	Azure 订阅的标识符。该 ID 定义您具有访问权限的存储帐户、虚拟机和其他 Azure 资源。
Azure 环境	部署的 Azure 资源的地理区域。vRealize Automation 基于订阅 ID 支持当前的所有 Azure 区域。
资源管理器设置	
Azure 服务 URI	用于获取 Azure 实例访问权限的 URI。 <code>https://management.azure.com/</code> 的默认值适用于许多典型实施。当您选择环境时，会自动填充此框。
租户 ID	希望端点使用的 Azure 租户 ID。
客户端 ID	希望端点使用的 Azure 客户端标识符。此参数在创建 Active Directory 应用程序时进行分配。
客户端密码	与 Azure 客户端 ID 一起使用的密钥。此密钥在创建 Active Directory 应用程序时进行分配。
Azure 存储 URI	用于访问 Azure 存储实例的 URI。当您选择环境时，会自动填充此框。
代理设置	
代理主机	如果贵公司使用代理 Web 服务器，请输入该服务器的主机名。
代理端口	如果贵公司使用代理 Web 服务器，请输入该服务器的端口号。

8 （可选）单击“属性”，然后添加提供的自定义属性、属性组或您自己的自定义属性定义。

9 单击完成。

后续步骤

在 Azure 中创建合适的资源组、存储帐户以及网络安全组。您还应创建负载均衡器（如果适合您的实施）。

操作	选项
创建 Azure 资源组	<ul style="list-style-type: none"> ■ 使用 Azure 门户创建资源组。请参见 Azure 文档了解具体说明。 ■ 使用 Library/Azure/Resource/Create resource group 下的相应 vRealize Orchestrator 工作流。 ■ 在 vRealize Automation 中，创建并发布包含 vRealize Orchestrator 工作流的 XaaS 蓝图。将资源组附加到服务和授权后，可以请求资源组。 <p>注 资源组资源类型不受 vRealize Automation 支持或管理。</p>
创建 Azure 存储帐户	<ul style="list-style-type: none"> ■ 使用 Azure 创建存储帐户。请参见 Azure 文档了解具体说明。 ■ 使用 Library/Azure/Storage/Create storage account 下的相应 vRealize Orchestrator 工作流。 ■ 在 vRealize Automation 中，创建并发布包含 vRealize Orchestrator 工作流的 XaaS 蓝图。将存储帐户附加到服务和授权后，可以请求存储帐户。
创建 Azure 网络安全组	<ul style="list-style-type: none"> ■ 使用 Azure 创建安全组。请参见 Azure 文档了解具体说明。 ■ 使用 Library/Azure/Network/Create Network security group 下的相应 vRealize Orchestrator 工作流。 ■ 在 vRealize Automation 中，创建并发布包含 vRealize Orchestrator 工作流的 XaaS 蓝图。将安全组附加到服务和授权后，可以请求安全组。

Azure 支持的区域

vRealize Automation Azure 实施支持 Microsoft Azure 支持的区域的子集。

vRealize Automation 中的 Azure 实施支持以下 Azure 区域。

- | | |
|----------|-----------|
| ■ 东亚 | ■ 澳大利亚东部 |
| ■ 东南亚 | ■ 澳大利亚东南部 |
| ■ 美国中部 | ■ 印度南部 |
| ■ 美国东部 | ■ 印度中部 |
| ■ 美国东部 2 | ■ 印度西部 |
| ■ 美国西部 | ■ 加拿大中部 |
| ■ 美国西部 2 | ■ 加拿大东部 |
| ■ 美国中北部 | ■ 美国中西部 |
| ■ 美国中南部 | ■ 韩国中部 |
| ■ 北欧 | ■ 韩国南部 |
| ■ 西欧 | ■ 英国西部 |
| ■ 日本西部 | ■ 英国南部 |
| ■ 日本东部 | ■ 华东 |
| ■ 巴西南部 | ■ 华北 |

创建和配置容器

您可以使用 vRealize Automation 中的 容器 选项卡打开 vRealize Automation 容器 集成应用程序，并创建和配置要提供给 vRealize Automation 蓝图架构师的容器和容器网络设置。

您可以在集成的容器应用程序中使用新的和现有的模板和映像定义容器。然后，可以将容器组件及其关联的网络设置添加到 vRealize Automation 蓝图。

管理容器主机和群集

可以查看和管理从“群集”页面添加的主机。在 容器 的上下文中，该主机是支持您运行容器的虚拟机或基础架构。

“基础架构”选项卡下的“群集”页面中包含用于添加新群集和主机的控件。要在容器环境中添加主机，必须将其添加到群集。可以监控现有主机的置备请求状态，以及从“库”和“部署”选项卡中的任何页面查看容器的事件日志。“请求”和“事件日志”面板位于页面右侧。

创建容器主机群集

必须将主机添加到群集才能部署容器。

前提条件

选择“容器”选项卡左上方的业务组。

步骤

- 1 以**容器管理员**身份登录到 vRealize Automation 控制台。
- 2 单击**容器**选项卡。
- 3 单击**基础架构 > 容器主机群集**。
- 4 单击**群集**。
- 5 输入群集名称和描述。
- 6 在**类型**下拉菜单中选择任一 Docker 虚拟容器主机 (VCH)。
- 7 使用 **http(s)://<hostname>:<port>** URL 格式输入主机 IP 地址或主机名。
- 8 从列表中选择您的登录凭据。

容器 支持凭据身份验证和公用密钥-私有密钥身份验证。可以从**身份管理**页面添加凭据。

- 9 单击**保存**。

结果

您已成功创建容器主机群集。

使用容器部署策略

您可以将部署策略链接到主机定义和容器定义。可以在 vRealize Automation 容器 中使用部署策略来设置特定主机的首选项以及部署容器时的配额。

应用到容器的部署策略的优先级高于应用到容器主机的放置。

注 部署策略已弃用，并将在 vRealize Automation 的未来版本中移除。

在主机上设置部署策略

设置特定主机的首选项以及部署容器时的配额。

注 部署策略已弃用，并将在 vRealize Automation 的未来版本中移除。

前提条件

将主机添加到群集。

步骤

- 1 以**容器管理员**身份登录到 vRealize Automation 控制台。
- 2 单击**容器**选项卡。
- 3 选择**基础架构 > 容器主机群集**。
- 4 单击要编辑的主机所在的群集。
- 5 单击**资源**。
- 6 在要配置的主机上单击选项图标，然后单击**编辑**。
- 7 选择部署策略，然后单击**更新**。

为容器定义设置部署策略

为容器定义设置部署策略。

注 部署策略已弃用，将在 vRealize Automation 的未来版本中移除。

步骤

- 1 单击**容器**选项卡。
- 2 单击**容器热群集**以开始置备容器。
- 3 从列表中选择现有容器。
- 4 在置备选项中，单击**策略**。
- 5 从**部署策略**下拉列表中，选择现有策略。
- 6 置备容器，或将其另存为模板。

配置容器设置

您可以使用新的和现有的容器配置属性和设置定义单容器或多容器应用程序。

除了核心 vRealize Automation 容器 设置外，以下 vRealize Automation 设置也可用于使用容器组件的部署：

- 运行状况配置
- 链接
- 公开的服务
- 集群大小以及缩小和扩大参数

在 容器 中配置运行状况检查

您可以配置运行状况检查方法，以便根据自定义标准更新容器状态。

对容器运行命令时，您可以使用 HTTP 或 TCP 协议。还可以指定运行状况检查方法。

前提条件

- 确认已在支持的 vRealize Automation 部署中启用 vRealize Automation 容器。
- 确认您拥有容器管理员或容器架构师角色特权。

步骤

- 1 登录 vRealize Automation。
- 2 单击容器选项卡。
- 3 在左侧窗格中选择库 > 模板。
- 4 编辑模板或映像。

选项	描述
编辑模板	<ol style="list-style-type: none"> a 在要打开的模板的右上部分中单击编辑。 b 在要打开的容器的右上部分中单击编辑。
编辑映像	单击映像的 置备 按钮旁边的箭头，然后单击 输入附加信息 。

- 5 单击运行状况配置选项卡。

6 选择运行状况模式。

表 2-20. 运行状况配置模式

模式	描述
无	默认。未配置运行状况检查。
HTTP	如果选择 HTTP ，则必须提供要访问的 API 以及要使用的 HTTP 方法和版本。该 API 是相对的，您无需输入容器的地址。还可以指定操作的超时期限并设置运行状况阈值。 例如，正常阈值为 2 表示必须连续两次调用成功，容器才会视为正常并处于 RUNNING 状态。不正常阈值为 2 表示必须连续两次调用失败，容器才会视为不正常并处于 ERROR 状态。对于介于正常和不正常阈值之间的所有状态，容器状态均为 DEGRADED 。
TCP 连接	如果选择 TCP 连接 ，则只能输入容器的端口。运行状况检查会尝试在提供的端口上与容器建立 TCP 连接。与 HTTP 一样，还可以指定操作的超时值并设置正常或不正常阈值。
命令	如果选择 命令 ，则必须输入要在容器上运行的命令。运行状况检查的成功与否取决于该命令的退出状态。
置备时忽略运行状况检查	取消选中此选项会强制在置备时执行运行状况检查。通过强制执行，只有成功通过运行状况检查后，容器才会被视为已置备容器。
Autodeploy	容器处于错误状态时自动重新部署容器。

7 单击保存。

在 容器 中配置链接

链接和公开的服务可以跨容器服务进行通信并跨主机进行负载平衡。您可以在 容器 中为容器配置链接设置。

在应用程序中，您可以使用链接启用多个服务之间的通信。容器 中的链接类似于 Docker 链接，但跨主机连接容器。链接包括两个部分：服务名称和别名。服务名称是所调用的服务或模板的名称。别名是您用来与该服务通信的主机名。

例如，如果您的应用程序包含 Web 和数据库服务，并且您使用别名 **my-db** 在 Web 服务中定义了指向数据库服务的链接，则 Web 服务应用程序会打开到 **my-db:{PORT_OF_DB}** 的 TCP 连接。**PORT_OF_DB** 是数据库侦听的端口，而不考虑容器设置分配给主机的公用端口。如果 MySQL 在其默认端口 3306 上检查是否有更新，且容器主机的发布端口为 32799，则 Web 应用程序将在 **my-db:3306** 访问数据库。

注 建议您使用网络而非链接。如今，链接是一项传统 Docker 功能，在链接容器群集时存在很大的局限性，其中包括：

- Docker 不支持多个链接使用相同的别名。建议允许 vRealize Automation 容器 为您生成链接别名。
- 不能在运行时更新容器的链接。纵向扩展或收缩链接群集时，不会更新从属容器的链接。

前提条件

- 确认已在支持的 vRealize Automation 部署中启用 vRealize Automation 容器。

- 确认您拥有**容器管理员**或**容器架构师**角色特权。
- 确认桥接网络可用于链接服务。
- 确认目标服务的内部端口已发布。对于交叉通信，该服务可以映射到任何其他端口，但是必须可从主机外部进行访问。
- 确认服务主机能够彼此访问。

步骤

- 1 登录 vRealize Automation。
- 2 单击“容器”选项卡。
- 3 在左侧窗格中选择**库 > 模板**。
- 4 编辑模板或映像。

选项	描述
编辑模板	<ol style="list-style-type: none"> a 在要打开的模板的右上部分中单击编辑。 b 在要打开的容器的右上部分中单击编辑。
编辑映像	单击映像的 置备 按钮旁边的箭头，然后单击 输入附加信息 。

- 5 单击**基本**选项卡。
- 6 在**服务**文本框中，输入容器所依赖的服务的逗号分隔列表。
- 7 在**别名**文本框中，输入服务的描述性名称或以逗号分隔的服务列表。
- 8 单击**保存**。

在 容器 中配置公开的服务

通过在容器设置中提供一个地址和占位符，您可以对负载均衡器使用唯一的主机名。

该占位符将确定 URL 的自动生成部分的位置。此值对于每个主机名是唯一的。该地址支持 **%s** 格式字符指定该占位符所处的位置。

注 如果不使用占位符，它将定位为主机名的前缀或后缀，具体取决于系统配置。

如果构建的应用程序包括必须公开并缩小和放大的服务，建议您使用可以将请求定向到每个节点的负载均衡器。置备应用程序后，每当 vRealize Automation 缩小或放大服务时，便会更新负载均衡器配置。

前提条件

- 确认已在支持的 vRealize Automation 部署中启用 vRealize Automation 容器。
- 确认您拥有**容器管理员**或**容器架构师**角色特权。

步骤

- 1 登录 vRealize Automation。
- 2 单击**容器**选项卡。

3 在左侧窗格中选择**库 > 模板**。

4 编辑模板或映像。

选项	描述
编辑模板	a 在要打开的模板的右上部分中单击 编辑 。 b 在要打开的容器的右上部分中单击 编辑 。
编辑映像	单击映像的 置备 按钮旁边的箭头，然后单击 输入附加信息 。

5 单击**网络**选项卡。

6 在**地址**文本框中，输入占位符的位置。

地址主机充当虚拟主机。要访问地址主机，您可以在 `etc/hosts` 文件中添加映射信息，或者使用将容器地址映射到主机名的 DNS。

7 在**容器端口**文本框中，输入用于公开服务的端口号。

请使用表单中提供的示例格式。如果容器应用程序公开了多个端口，请指定一个或多个可以公开服务的内部端口。

8 单击**保存**。

在 容器 中配置群集大小并进行缩放

可以通过使用 容器 放置设置指定群集大小来创建容器群集。

配置群集时，容器 会置备指定数量的容器。请求在群集中的所有容器之间进行负载平衡。

您可以在置备的容器或应用程序上修改群集大小，从而使群集的大小按 1 递增或递减。如果在运行时修改群集大小，将考虑所有关联性筛选器和放置规则。

前提条件

- 确认已在支持的 vRealize Automation 部署中启用 vRealize Automation 容器。
- 确认您拥有**容器管理员**或**容器架构师**角色特权。

步骤

1 登录 vRealize Automation。

2 单击**容器**选项卡。

3 在左侧窗格中选择**库 > 模板**。

4 编辑模板或映像。

选项	描述
编辑模板	a 在要打开的模板的右上部分中单击 编辑 。 b 在要打开的容器的右上部分中单击 编辑 。
编辑映像	单击映像的 置备 按钮旁边的箭头，然后单击 输入附加信息 。

5 单击**策略**选项卡。

6 设置容器群集大小。

7 单击**保存**。

在 容器 中配置和使用模板

容器 使用模板来置备容器。

模板是可重用配置，用于置备一个或一组容器。在模板中，可以定义包含链接服务的多层应用程序。

服务定义为具有相同类型或映像的一个或多个容器。

可以在**模板**页面上基于现有模板创建自定义容器模板，也可以导入格式正确的 **YAML** 文件。还可以置备容器模板或映像。

创建自定义容器模板

您可以创建自定义模板并用它来定义容器。

模板是一种可重用配置，您可将其用于置备一个或一系列容器。

“模板”页面根据您定义的注册表显示可用的模板映像。您既可以根据现有的模板映像创建自定义模板，也可以导入模板或 Docker Compose 文件。请参见[导入容器模板或 Docker Compose 文件](#)。

您还可以使用[从模板或映像置备容器](#)中所述的**置备 > 输入附加信息**选项创建自定义模板或映像。

前提条件

- 确认您拥有**容器管理员**角色特权。

步骤

1 以**容器管理员**身份登录到 vRealize Automation 控制台。

2 单击**容器**选项卡。

3 在左侧窗格中选择**库 > 模板**。

一个列表将显示可用于置备的模板和映像。

- “映像”视图中的已配置模板。
- **模板**视图中的现有或自定义模板。
- 基于**全部**视图中的指定注册表的所有可用模板和映像。

导入和**导出**选项也可用于导入或导出模板和映像。

4 单击要包括在模板中的映像的**置备**按钮旁边的箭头。

5 单击**输入其他信息**。

6 单击**另存为模板**以将更改另存为 Containers for vRealize Automation 中的新容器。

后续步骤

您可以编辑模板，以便将来进行置备。在置备后对模板所做的更改不会影响从模板置备的现有应用程序。

导入容器模板或 Docker Compose 文件

可以在 vRealize Automation 容器 中使用已导入的 Docker 容器模板或 Docker Compose YAML 文件作为自定义模板。

如果使用 YAML 文件，请以文本格式输入 YAML 文件的内容，或浏览到并上载 YAML 文件。YAML 文件代表模板以及各个容器的配置和连接。支持的格式类型是 Docker Compose YAML 和 vRealize Automation 容器 YAML。

vRealize Automation 容器 YAML 类似于 Docker Compose，但它使用 vRealize Automation REST API 或 vRealize CloudClient 中可见的 vRealize Automation 蓝图 YAML 格式。通过 vRealize Automation 容器 YAML，您可以导入现有 Docker Compose 应用程序，并且可以使用容器 修改、置备和管理这些应用程序。

前提条件

- 确认已在支持的 vRealize Automation 部署中启用 vRealize Automation 容器。
- 以**容器管理员**身份登录到 vRealize Automation。

有关 vRealize Automation 服务 REST API 使用的 YAML 格式的信息，请参见《vRealize Automation API 参考》。

步骤

1 单击**容器**选项卡。

2 在左侧窗格中选择**库 > 模板**。

一个列表将显示可用于置备的模板和映像。

- “映像”视图中的已配置模板。
- **模板**视图中的现有或自定义模板。
- 基于**全部**视图中的指定注册表的所有可用模板和映像。

导入和导出选项也可用于导入或导出模板和映像。

3 单击**导入模板或 Docker Compose** 图标。

此时将显示“导入模板”页面。

4 提供 YAML 文件内容。

选项	描述
从文件加载	单击 从文件加载 可浏览到目录并从中选择 YAML 文件。
输入模板或 Docker Compose	将格式正确的 YAML 文件的内容粘贴到 输入模板或 Docker Compose 文本框中。

5 单击**导入**。

新模板将显示在**模板**视图中。

从模板或映像置备容器

可以在“模板”视图中从模板或映像置备容器。

置备过程将基于从中进行置备的模板或映像中存在的配置设置创建容器。

可以通过以下方法从模板或映像置备容器：使用现有的配置设置，或者先编辑配置设置再进行置备。

还可以编辑并保存配置设置以创建新的自定义容器模板或映像。

前提条件

- 确认已在支持的 vRealize Automation 部署中启用 vRealize Automation 容器。
- 以容器管理员身份登录到 vRealize Automation。

步骤

- 1 单击**容器**选项卡。
- 2 在左侧窗格中选择**库 > 模板**。
一个列表将显示可用于置备的模板和映像。
 - “映像”视图中的已配置模板。
 - **模板**视图中的现有或自定义模板。
 - 基于**全部**视图中的指定注册表的所有可用模板和映像。

导入和导出选项也可用于导入或导出模板和映像。
- 3 使用**全部**、**映像**或**模板**视图选项查看要置备的映像或模板。
- 4 置备模板或映像。

选项	描述
使用现有设置进行置备。	a 单击 置备 。 “置备请求”视图显示有关置备结果的信息。
通过编辑设置来进行置备。	a 单击 置备 按钮旁边的箭头。 b 单击 输入其他信息 。 c 在 置备容器表单 中输入容器的其他信息。 d 完成表单更新后，单击 置备 以使用修改后的设置进行置备。 e 单击 另存为模板 以将更改另存为 vRealize Automation 容器 中的新容器。 “置备请求”视图显示有关置备结果的信息。

导出容器模板或 Docker Compose 文件

可以将容器模板导出为 Docker Compose YAML 文件或 vRealize Automation 容器 YAML 文件。

您可以导入模板，并且可以使用 vRealize Automation REST API 或 vRealize CloudClient 以编程方式修改模板，也可以在 容器 以图形方式修改模板。然后，您可以导出已修改的文件。例如，可以采用 Docker Compose 格式导入模板，然后以 vRealize Automation 复合服务 API 中使用的蓝图 YAML 格式导出模板。但是，如果以 Docker Compose 格式导出模板，则不包含某些特定于 容器 的配置（例如运行状况配置和关联性约束）。

前提条件

- 确认已在支持的 vRealize Automation 部署中启用 vRealize Automation 容器。
- 以**容器管理员**身份登录到 vRealize Automation。

有关 vRealize Automation 服务 REST API 使用的 YAML 格式的信息，请参见《vRealize Automation API 参考》。

步骤

- 1 单击**容器**选项卡。
- 2 在左侧窗格中选择**库 > 模板**。
一个列表将显示可用于置备的模板和映像。
 - “映像”视图中的已配置模板。
 - **模板**视图中的现有或自定义模板。
 - 基于**全部**视图中的指定注册表的所有可用模板和映像。

导入和**导出**选项也可用于导入或导出模板和映像。

- 3 指向模板并单击其**导出**图标。
- 4 当出现提示时，选择一种输出格式类型：
 - **YAML 蓝图**
此格式遵守 vRealize Automation 复合服务 API 中使用的蓝图 YAML 格式。
 - **Docker Compose**
此格式遵守 Docker Compose 应用程序中使用的 YAML 格式。

- 5 单击**导出**。
- 6 当出现提示时，保存文件或在合适的应用程序中打开该文件。

使用容器注册表

Docker 注册表是一个无状态的服务器端应用程序。可以使用注册表在 vRealize Automation 容器 中存储和分发 Docker 映像。

要配置注册表，您需要提供其地址、自定义注册表名称和可选凭据。该地址必须以 HTTP 或 HTTPS 开头，以指示注册表是安全的还是不安全的。如果未提供连接类型，则默认情况下会使用 HTTPS。

注 对于 HTTP，必须声明端口 80；对于 HTTPS，必须声明端口 443。如果未指定任何端口，则 Docker 引擎会假定端口 5000，这会导致断开连接。

注 建议不要使用 HTTP 注册表，因为 HTTP 会被视为不安全。如果要使用 HTTP，您必须修改每个主机上的 DOCKER_OPTS 属性，如下所示：

```
DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000"
```

有关详细信息，请参见 Docker 文档 (<https://docs.docker.com/registry/insecure/>)。

容器可以按以下方式与 Docker 注册表 HTTP API V1 和 V2 交互：

HTTP 上的 V1（不安全，普通 HTTP 注册表）

您可以随意搜索这种注册表，但必须手动为每个 Docker 主机配置 `--insecure-registry` 标记，以基于不安全注册表中的映像置备容器。设置该属性之后，必须重新启动 Docker 守护进程。

HTTPS 上的 V1

在反向代理（例如 NGINX）后面使用。可从以下开源网站获取标准实现：<https://github.com/docker/docker-registry>。

HTTPS 上的 V2

可从以下开源网站获取标准实现：<https://github.com/docker/distribution>。

HTTPS 上的 V2（带有基本身份验证）

可从以下开源网站获取标准实现：<https://github.com/docker/distribution>。

HTTPS 上的 V2（带有通过中央服务的基本身份验证）

可以在独立模式下运行 Docker 注册表，在这种模式下，不会进行任何授权检查。支持的第三方注册表包括 JFrog Artifactory 和 Harbor。默认情况下，Docker Hub 对所有租户处于启用状态且不包含在注册表列表中，但可以使用系统属性将其停用。

注 Docker 一般不与配置了由未知机构签署的证书的安全注册表交互。容器服务会通过自动将不可信证书上载到所有 Docker 主机并使主机能够连接到这些注册表来处理这种情况。如果无法将证书上载到给定主机，则该主机自动停用。

创建和管理容器注册表

您可以配置多个注册表来访问公用和专用映像。

注册表是您从中上载或下载映像的公用或专用存储。您可以取消激活、编辑或删除所创建的注册表。**模板**选项卡中显示的映像基于您定义的注册表。

创建或管理注册表时，您可以单击**凭据**或**证书**按钮来添加或管理凭据和证书。

前提条件

- 以**容器管理员**身份登录到 vRealize Automation。
- 确认至少有一个主机已配置并可用于容器网络配置。

步骤

- 1 单击**容器**选项卡。
- 2 选择**库 > 全局注册表**。
- 3 单击**注册表**创建新的注册表。
- 4 输入注册表地址。

- 5 输入注册表的名称。
- 6 从下拉列表中选择您的登录凭据。
- 7 （可选）单击**验证**以确认配置的参数有效。
- 8 单击**保存**以添加注册表。

将映像添加到收藏夹

要快速访问最常用映像或首选映像，可以将映像添加到收藏夹。

将映像添加到收藏夹时，它将显示在“存储库”主页上，无需搜索。只有容器管理员可以在收藏夹中添加和移除映像，而所有用户都可以查看每个存储库的收藏夹映像。标记为收藏的映像会在其名称旁边显示一个星标。

步骤

- 1 在“存储库”页面，从下拉菜单中选择注册表，然后搜索所需的映像。
- 2 单击**置备**旁边的箭头，然后选择**将映像添加到收藏夹**。

此时会显示一个通知，表示映像已成功添加到收藏夹，并且会在映像的名称旁边添加一颗星标。

结果

该映像将显示在“存储库”页面上，无需搜索。要从收藏夹中移除映像，请在“存储库”页面上单击**置备**旁边的箭头，然后选择**从收藏夹中移除映像**。

为容器配置网络资源

可以在 vRealize Automation 容器 应用程序中创建和修改网络配置，还可以将网络配置附加到容器和容器模板。

置备容器时，会嵌入网络配置并可用。可以自定义已添加到 vRealize Automation 蓝图的容器组件的网络设置。

为容器创建新网络

如果没有适合的网络配置，您可以在 vRealize Automation 中创建新的网络配置。

前提条件

- 确认您拥有**容器管理员**、**容器架构师**或 **IaaS 管理员**角色特权。
- 确认至少有一个主机已配置并可用于容器网络配置。

步骤

- 1 登录 vRealize Automation。
- 2 单击**容器**选项卡。

3 在左侧窗格中选择**部署 > 网络**。

主面板显示可以在容器部署过程中置备的现有网络配置。其中包括从添加的 **Docker** 主机收集的网络配置和在 **vRealize Automation** 中创建的网络配置。代表这些网络配置的图标将显示：网络和 **IPAM** 驱动程序、子网、网关和 **IP** 范围信息、使用网络配置的容器数量、主机数。

4 单击 **+网络**。

5 输入网络的名称。

完成新配置的创建后，名称值将附加唯一标识符。

6 （可选）要添加更详细的配置设置，请选中**高级**复选框。

其他网络配置设置将显示在“添加网络”面板中。

7 配置高级网络配置设置。

选项	描述
IPAM 配置	<p>子网</p> <p>提供特定于此网络配置的子网和网关地址。这些值不得与同一容器主机上的任何其他网络重叠。</p>
自定义属性	<p>（可选）指定新网络配置的自定义属性。</p> <p>containers.ipam.driver</p> <p>仅可与容器配合使用。指定将 容器 网络组件添加到蓝图时要使用的 IPAM 驱动程序。受支持的值取决于在使用这些值的容器主机环境中安装的驱动程序。例如，根据容器主机上安装的 IPAM 插件，受支持的值可能是 infoblox 或 calico。</p> <p>此属性名称和值区分大小写。在添加该属性值时，不会对其进行验证。如果在置备时容器主机上不存在指定的驱动程序，将返回一条错误消息且置备失败。</p> <p>containers.network.driver</p> <p>仅可与容器配合使用。指定将 容器 网络组件添加到蓝图时要使用的网络驱动程序。受支持的值取决于在使用这些值的容器主机环境中安装的驱动程序。默认情况下，Docker 提供的网络驱动程序包括 bridge、overlay 和 macvlan，而虚拟容器主机 (Virtual Container Host, VCH) 提供的网络驱动程序包括 bridge 驱动程序。还可以使用 weave 和 calico 等第三方网络驱动程序，具体取决于容器主机上安装的网络插件。</p> <p>此属性名称和值区分大小写。在添加该属性值时，不会对其进行验证。如果在置备时容器主机上不存在指定的驱动程序，将返回一条错误消息且置备失败。</p>

注 如果创建的网络不含高级设置，**vRealize Automation** 会自动提供这些设置。

8 从下拉菜单中，选择要连接网络的主机。

9 单击**创建**。

向容器模板添加网络

您可以将网络配置添加到容器模板来将容器彼此连接在一起。系统会自动为使用该模板的任何应用程序实施此网络配置。您可以根据需要添加现有网络或配置和添加新网络。

前提条件

- 确认您有模板可用。否则，必须先创建一个模板。
- 确认您拥有**容器管理员**、**容器架构师**或**laaS 管理员**角色特权。
- 确认至少有一个主机已配置并可用于容器网络配置。

步骤

1 登录 vRealize Automation。

2 单击**容器**选项卡。

3 在左侧窗格中选择**库 > 模板**。

一系列图标将显示可用于置备的模板和映像。

4 （可选）通过在这些图标上方的右上标题中单击**视图: 模板**，将视图修改为仅显示模板。

5 在要自定义的模板的右上部分中单击**编辑**。

此时将出现“编辑模板”页面，其中显示容器图标和带有加号的空白图标。

6 指向空白图标。

此时会出现**添加网络**图标。

7 单击**添加网络**图标。

此时会出现“添加网络”面板。

8 添加现有网络或创建和添加新网络。

选项	描述
添加现有网络。	a 单击 现有 复选框。 b 单击 名称 字段内，以显示现有网络的列表。 c 选择要使用的网络并单击 保存 。
配置和添加新网络。	a 输入网络的名称。 b 要添加更详细的配置设置，请单击 高级 复选框。 c 单击 保存 。

9 通过将网络连接器图标从容器中拖动到表示网络的水平图标上的任意点，以便将网络连接到容器。

为容器配置卷

可以在 vRealize Automation 容器 应用程序中创建和修改卷，还可以将卷附加到容器和容器模板。

vRealize Automation 容器使用 Docker 卷来实现永久数据管理。使用卷，您可以执行以下任务：

- 在同一主机内的不同容器之间共享卷。

- 即时更新数据。
- 删除容器后保存卷数据。

为容器创建新卷

要扩展容器存储，必须先创建数据卷。

前提条件

- 确认您拥有**容器管理员**、**容器架构师**或**IaaS 管理员**角色特权。
- 确认至少配置了一个主机且该主机可用于容器卷配置。

步骤

- 1 登录 vRealize Automation。
- 2 单击**容器**选项卡。
- 3 在左侧窗格中选择**部署 > 卷**。

主面板显示可以连接到已部署容器的现有卷配置。包括从添加的 **Docker** 主机收集的卷配置以及在 vRealize Automation 中创建的卷配置。卷实例显示驱动程序、范围和驱动程序选项。

- 4 单击 **+卷**。
- 5 输入卷的名称。
完成配置的创建后，名称值将附加唯一标识符。
- 6 在**驱动程序**文本框中，输入要使用的卷插件的驱动程序。如果不输入任何内容，将使用 **local** 作为默认值。
- 7 （可选）要添加更详细的配置设置，请单击**高级**复选框。
将显示其他配置设置。
- 8 （可选）配置高级卷设置。

选项	描述
驱动程序选项	指定要使用的驱动程序选项。选项取决于使用的卷插件。
自定义属性	指定新配置的自定义属性。

- 9 从下拉菜单中，选择要连接卷的主机。
- 10 单击**创建**。
“创建卷”面板会消失，且已添加的卷将显示在“卷”选项卡中。

后续步骤

[向容器模板添加卷](#)

向容器模板添加卷

可以通过将卷添加到模板将其连接到容器。

前提条件

- 确认您有模板可用。否则，必须先创建一个模板。
- 确认您拥有**容器管理员**、**容器架构师**或**IaaS 管理员**角色特权。
- 确认至少配置了一个主机且该主机可用于容器卷配置。

步骤

- 1 登录 vRealize Automation。
- 2 单击**容器**选项卡。
- 3 在左侧窗格中选择**库 > 模板**。
一系列图标将显示可用于置备的模板和映像。
- 4 （可选）通过在这些图标上方的右上标题中单击**视图: 模板**，将视图修改为仅显示模板。
- 5 在要自定义的模板的右上部分中单击**编辑**。
此时将出现“编辑模板”页面，其中显示容器图标，包括带有加号的空白图标。
- 6 将光标悬停在带加号的空白图标上，直到出现**添加卷**图标。
- 7 单击**添加卷**图标。
- 8 添加现有卷或创建并添加新卷。

选项	描述
添加现有卷。	<ol style="list-style-type: none"> a 单击现有复选框。 b 在名称字段内单击，以显示现有卷的列表。 c 选择要使用的卷并单击保存。
配置和添加新卷。	<ol style="list-style-type: none"> a 输入卷的名称。 b 在驱动程序文本框中，输入要使用的卷插件的驱动程序。如果使用的不是外部存储系统，请输入 local。 c 要添加更详细的配置设置，请单击高级复选框。 d 单击保存。

“添加卷”面板会消失，且已添加的卷将在“编辑模板”页面中的容器图标下方显示为水平图标。卷图标也会显示在容器图标的底部边框上。

- 9 通过将卷连接器图标从容器中拖动到表示卷的水平图标上的任意点，将卷连接到容器。
- 10 （可选）单击容器路径以更改挂载卷的位置。

后续步骤

[从模板或映像置备容器](#)

创建和配置 PKS 容器

Pivotal 容器服务 (PKS) 允许企业和服务提供商简化基于 Kubernetes 的容器服务的部署和操作。

使用 PKS 容器可以提供以下关键功能：

- 高可用性
 - PKS 具有内置容错功能，可完成日常运行状况检查并具备针对 Kubernetes 群集的自行更正功能。
- 高级网络和安全
 - PKS 与 NSX-T 深度集成可实现高级容器活动，包括微分段、负载平衡和安全策略。
- 优化操作
 - PKS 提供 Kubernetes 群集部署和生命周期管理。
- 多租户
 - PKS 支持多租户以便在企业 and 云服务中实现工作负载隔离和隐私保护。

添加 PKS 端点

在创建 PKS 容器之前，必须先添加 PKS 端点。

创建 PKS 容器的第一步是添加 PKS 端点。PKS 端点可用于链接计划、现有 Kubernetes 群集和业务组。

前提条件

- 容器管理员特权
- PKS 凭据
- UAA 地址
- PKS 端点地址

步骤

- 1 使用路径 **身份管理 > 凭据** 导航到凭据，以创建并保存您的 PKS 凭据。
- 2 选择 **PKS 端点 > 创建端点**。
- 3 输入 PKS 端点的详细信息并测试连接，然后再进行保存。

如果测试失败，请验证 PKS 凭据、UAA 地址和 PKS 端点地址是否正确。您可能必须对这些地址执行 ping 操作，以验证它们是否处于活动状态。重试连接。

- 4 单击 **创建** 以保存您的 PKS 端点。

注 如果显示“验证证书”窗口，您可以选择 **显示证书** 查看证书详细信息。单击 **是** 以继续保存您的端点。

结果

您的 PKS 端点已保存。保存 PKS 端点后，您可以单击该端点以查看与其关联的可用 Kubernetes 群集。如果未在 vRealize Automation 中注册该群集，“已请求”列将显示值否。要进行注册，您需要[添加群集](#)。如果您希望编辑自己的端点，请单击 PKS 端点名称并修改其详细信息。您可以通过选择并单击[移除](#)来移除端点。

将 PKS 端点分配给业务组

创建 PKS 端点后，您可以分配给特定业务组来授予访问权限。

创建 PKS 端点后，您可以通过将计划分配给特定的业务来对它授予访问权限。这用于限制某些组对特定功能的访问权限。

注 您可以在 PKS 单独创建计划。无法在 vRealize Automation 中添加或修改计划。

前提条件

- 容器管理员特权
- 现有的 PKS 端点

步骤

- 1 打开 PKS 端点，然后单击[计划分配](#)。
- 2 从组列表选择所需的组并从计划列表进行计划。

注 使用 + 和 - 按钮，您可以将多个计划分配给每个业务组并将相同的计划分配给多个业务组。

- 3 单击[保存](#)以保存您的计划分配。

请求新的 PKS 群集

如果您需要的群集配置不存在，您可以为现有 PKS 端点请求新群集。

作为容器开发人员或容器管理员，您可以为 PKS 端点请求新群集。每个 PKS 端点可以包含多个群集。创建新群集后，可以使用[添加群集](#)将其添加到您的环境，并根据需要对它进行置备。

前提条件

- 现有 PKS 端点
- 容器开发人员或容器管理员特权

步骤

- 1 选择 **PKS 群集 > 新建群集**。
- 2 选择 PKS 端点。

在选择 PKS 端点后，将根据业务组可用的计划自动填充计划。

- 3 输入群集的详细信息。

注 尽管工作线程节点数由计划定义，但是您可以根据需要修改数量。

4 选择如何连接到此群集：

- 主控主机名 - 使用群集的主机名进行连接（假设存在 DNS 记录）。
- 主节点 IP - 使用群集的 IP 地址进行连接。

5 单击**创建**。

结果

此时将创建新群集，并将其显示在 PKS 群集主页上。

添加 PKS 群集

创建 PKS 端点后，您可以将可用的关联群集注册到 vRealize Automation。

创建 PKS 端点后，可以将群集添加到 vRealize Automation 来注册关联的群集。注册群集后，可以在其上置备单个映像。

前提条件

- 容器管理员特权
- 可用群集的 PKS 端点

步骤

- 1 验证群集正添加到正确的业务组。业务组名称列在左上窗格中。要在业务组之间切换，请单击**组**。
- 2 选择 **PKS 群集 > 添加群集**。
- 3 选择 PKS 端点来填充可用的群集。
- 4 选择如何连接到此群集：
 - 主控主机名 - 使用群集的主机名进行连接（假设存在 DNS 记录）。
 - 主节点 IP - 使用群集的 IP 地址进行连接。
- 5 单击**添加**。

结果

群集将显示在 PKS 群集页面上。

PKS 群集详细信息

群集详细信息提供了编辑群集以及与群集交互的信息和工具。

您可以通过单击 **PKS 群集** 页面中的群集名称来查看和修改现有 PKS 群集。此外，群集详细信息包含可用于与群集交互的交互工具以实现更复杂的配置。

注 您只能编辑群集的 worker 节点数。

仪表板

仪表板字段状态指明了是否已安装 **Kubernetes** 仪表板。如果已安装，您可以通过单击**已安装**并登录访问仪表板。

注 必须在群集上配置仪表板，以便进行基本身份验证。如果不进行基本身份验证，则无法登录。

KubeConfig

Kubeconfig 链接是群集的可下载配置文件。您可以作为容器开发人员使用此配置文件，以在命令行提示符窗口中连接并配置 **Kubernetes** 群集。例如，使用 **kubect1** 命令。

在 **Kubernetes** 集群上置备单个映像

vRealize Automation 中的容器功能允许您在 **PKS** 群集上置备单个映像。

添加 **PKS** 群集后，您可以在其上配置单个映像，作为 **Kubernetes** 容器和部署的组合。

前提条件

- 容器开发人员特权
- **PKS** 群集

步骤

- 1 导航到**库 > 存储库**。
- 2 从下拉菜单中选择所需的注册表。
- 3 使用存储库文本框搜索该注册表中的现有映像。
- 4 在所需的图像图标上单击**置备**。
- 5 输入置备详细信息，然后单击**置备**。

结果

所选的映像置备在 **Kubernetes** 群集上，并将显示在边栏的**请求**窗口。它还显示在 **Kubernetes > 部署**和 **Kubernetes > 容器**下用于验证。

注 您可以通过下载 kubeconfig 文件并使用命令 **kubect1** 置备您的群集。有关详细信息，请参见 [PKS 群集详细信息](#)。

在默认 vRealize Orchestrator 服务器上安装其他插件

可以使用 vRealize Orchestrator 配置界面，在默认 vRealize Orchestrator 服务器上安装其他软件包和插件。

可以在默认 vRealize Orchestrator 服务器上安装其他插件并使用 XaaS 的工作流。

还可以在默认 vRealize Orchestrator 服务器上导入其他软件包，以便配置为 vRealize Automation 外部 IPAM 提供程序端点类型。例如，有关获取、导入和配置 Infoblox IPAM 软件包的信息，请参见[用于提供第三方 IPAM 提供程序支持的对照表](#)。

可以从 https://solutionexchange.vmware.com/store/category_groups/cloud-management 的 VMware Solution Exchange 获取软件包 (.package) 和插件安装文件 (.vmoapp 或 .dar)。有关插件文件的信息, 请参见 https://www.vmware.com/support/pubs/vco_plugins_pubs.html 上的 vRealize Orchestrator 插件文档。

有关安装新插件的详细信息, 请参见《安装和配置 VMware vCenter Orchestrator》。

使用 Active Directory 策略

Active Directory 策略既可定义计算机记录的属性 (例如, 域), 也可定义使用 vRealize Automation 蓝图创建记录的组织单位。

如果将策略应用于业务组, 则业务组成员的所有计算机请求均会添加到指定的组织单位。您可以为不同的组织单位创建不同的策略, 然后将不同的策略应用于不同的业务组。

使用自定义属性替代 Active Directory 策略

使用提供的 Active Directory 自定义属性, 您可以在部署特定蓝图时替代该蓝图上的 Active Directory 策略、域、组织单位以及其他值。

提供的 Active Directory 自定义属性的列表包含在《自定义属性参考》中。自定义属性前缀为 `ext.policy.activedirectory`。

除了提供的属性以外, 您还可以创建自己的自定义属性。必须为自定义属性加上前缀 `ext.policy.activedirectory`。例如, `ext.policy.activedirectory.domain.extension` 或 `ext.policy.activedirectory.yourproperty`。这些属性将传递到您自定义的 vRealize Orchestrator Active Directory 工作流程中。

有关自定义属性的详细信息, 请参见《自定义属性参考》。根据要替代的值, 您可能需要创建属性定义。例如, 您可以创建一个属性定义, 从 vRealize Automation 中检索可用的 Active Directory 策略。或者, 您也可以创建一个定义, 允许请求用户从两个或多个替代组织单位中进行选择。请参见《自定义属性参考》。

创建并应用 Active Directory 策略

创建一个或多个 Active Directory 策略, 以便将不同的策略分配给不同的业务组。您可以根据业务组成员资格, 使用不同的策略将计算机记录添加到不同的组织单位。

如果需要, 您可以替代已分配的 Active Directory 策略。

步骤

1 创建 Active Directory 策略

您可以创建一个 Active Directory 策略, 定义用户部署计算机时系统将在 Active Directory 实例中添加记录的位置。您可以将策略分配给业务组, 使业务组成员部署的所有计算机均在指定组织单位中创建一条记录。

2 场景: 将自定义属性添加到蓝图以替代 Active Directory 策略

作为开发业务组的蓝图架构师, 您的蓝图包含应用程序计算机和数据库计算机。您希望添加到组织单位的数据库计算机记录与应用的 Active Directory 策略不同。

创建 Active Directory 策略

您可以创建一个 Active Directory 策略，定义用户部署计算机时系统将在 Active Directory 实例中添加记录的位置。您可以将策略分配给业务组，使业务组成员部署的所有计算机均在指定组织单位中创建一条记录。

当您希望不同业务组部署的计算机具有不同的域或者被添加到不同的 Active Directory 实例时，您可创建不同的 Active Directory 策略。

前提条件

- 确认您已创建 Active Directory 端点。请参见[将 Active Directory 插件配置为端点](#)。
- 如果使用外部 vRealize Orchestrator 服务器，请确认该服务器设置正确。请参见[配置外部 vRealize Orchestrator 服务器](#)。
- 以租户管理员身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > Active Directory 策略**。
- 2 单击**新建**图标 (+)。
- 3 配置 Active Directory 策略的详细信息。

选项	描述
ID	输入永久值。 该值不能包含任何空格或特殊字符。 以后不能更改此值。您只能使用其他 ID 重新创建该策略。
描述	策略的描述。
Active Directory 端点	选择创建此策略的 Active Directory 端点。
Domain	输入 root 域。格式为 <i>mycompany.com</i> 。
组织单位	输入此策略的组织单位标识名。 层次结构必须作为逗号分隔列表输入。例如， ou=development,dc=corp,dc=domain,dc=com。

- 4 单击**确定**。

结果

vRealize Orchestrator Active Directory 端点已添加到列表。您可以在业务组中应用该策略，或者在蓝图或业务组中使用该策略。

后续步骤

- 要提供多个策略选项，请创建更多策略。
- 要在部署蓝图后根据业务组成员资格将记录添加到 Active Directory，请将相应的 Active Directory 策略添加到业务组。请参见[创建业务组](#)。您既可以在创建业务组时应用该策略，也可以稍后添加该策略。

- 要为特定蓝图替代业务组的 Active Directory 策略，请将 Active Directory 自定义属性添加到该蓝图。请参见[场景：将自定义属性添加到蓝图以替代 Active Directory 策略](#)。

场景：将自定义属性添加到蓝图以替代 Active Directory 策略

作为开发业务组的蓝图架构师，您的蓝图包含应用程序计算机和数据库计算机。您希望添加到组织单位的数据库计算机记录与应用的 Active Directory 策略不同。

您的现有策略已应用于开发业务组。该策略将计算机记录添加到

ou=development,dc=corp,dc=domain,dc=com。您希望将所有数据库计算机添加到

ou=databases,dc=corp,dc=domain,dc=com。在包含数据库服务器的蓝图中，您替代 Active Directory 组织单位，以便将数据库计算机记录添加到 ou=databases,dc=corp,dc=domain,dc=com。

此场景做了如下假设：

- 您的 Active Directory 包含开发和数据库组织单位。
- 您的测试蓝图包含在某服务中，且该服务已获得授权。

除了这一有关如何替代策略的简单示例以外，在部署蓝图时，您还可以使用自定义属性与 Active Directory 策略对 Active Directory 进行其他更改。请参见[使用 Active Directory 策略](#)。

前提条件

- 确认您至少有一个 Active Directory 策略。请参见[创建 Active Directory 策略](#)。例如，您创建了一个开发策略，用于将记录添加到 ou=development,dc=corp,dc=domain,dc=com。
- 确认业务组已应用 Active Directory 策略。请参见[创建业务组](#)。例如，您的开发业务组使用该开发策略。

步骤

- 1 在测试蓝图的画布中，选择数据库计算机。
- 2 单击**属性**选项卡。
- 3 单击**自定义属性**选项卡。
- 4 单击**新建**图标 (+)。
- 5 添加自定义属性以更改默认组织单位。
 - a 在**名称**文本框中，输入 **ext.policy.activedirectory.orgunit**。
 - b 在**值**文本框中，输入 **ou=databases,dc=corp,dc=domain,dc=com**。
 - c 取消选择**可覆盖**。
 - d 单击**确定**。
- 6 单击**完成**。

结果

测试蓝图包含自定义属性，但您的用户在请求表单中看不到自定义属性。

后续步骤

请求您的测试蓝图。确认数据库计算机记录已添加到数据库组织单位，且应用程序计算机记录已添加到开发组织单位。对结果感到满意后，您可以将自定义属性添加到生产蓝图。

通知和委派的用户首选项

使用用户首选项覆盖系统审批者通知和通知语言首选项的默认配置。

要访问用户首选项，请单击 vRealize Automation 页眉上的用户名并选择**首选项**。

以下选项特定于登录的用户。

表 2-21. 用户首选项的选项

选项	描述
分配委派	允许您向其他用户重新分配批准请求。例如，您是目录请求的审批者，但您即将去度假。您将所有批准通知委派给一个或多个审批者。此分配会将请求立即转发给您的委派。从列表中移除委派之前，这些委派将处于活动状态。
通知	允许您更改通知语言，以便使用您选择的语言而不是默认语言向您发送电子邮件。选择语言，然后添加支持您语言首选项的通知订阅。

向用户提供服务蓝图

3

您可以向用户交付按需服务，方法是先创建目录项和操作，然后使用授权和批准谨慎控制哪些人员可以请求这些服务。

本章讨论了以下主题：

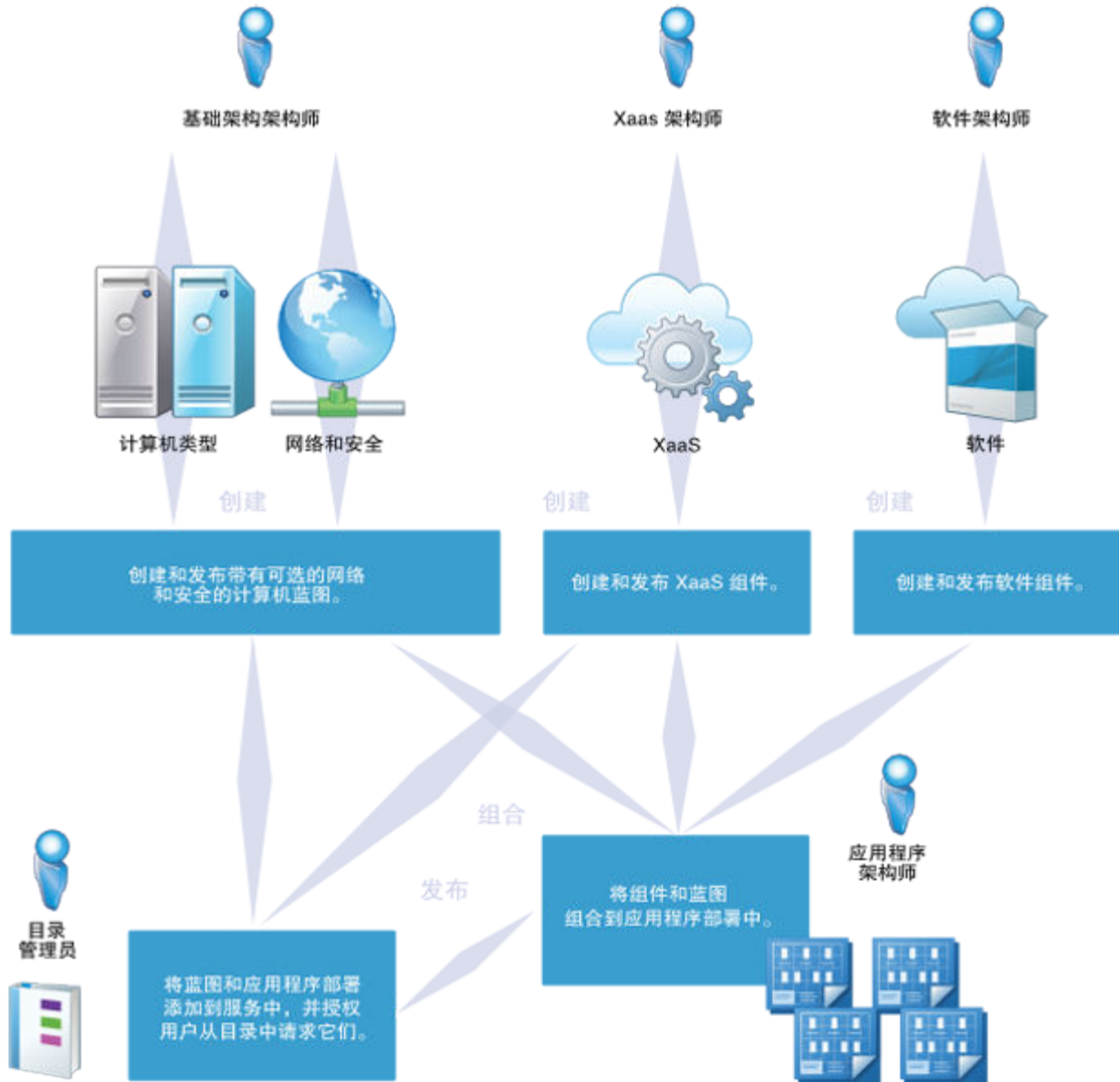
- [设计蓝图](#)
- [构建设计库](#)
- [使用开发人员驱动的蓝图](#)
- [组合复合蓝图](#)
- [自定义蓝图请求表单](#)
- [测试并对失败的置备请求进行故障排除](#)
- [管理服务目录](#)

设计蓝图

蓝图架构师构建 **Software** 组件、计算机蓝图和自定义 **XaaS** 蓝图，并将这些组件组合到蓝图中，这些蓝图定义了用户从目录中请求的项目。目录可以显示默认请求表单，您也可以为每个已发布的蓝图创建自定义表单。

您可以为单个计算机创建并发布多个蓝图，也可以创建并发布单个自定义 **XaaS** 蓝图，还可以将计算机组件和 **XaaS** 蓝图与其他构建块进行组合，设计包含多个计算机、网络与安全组件、支持完整生命周期的软件以及自定义 **XaaS** 功能的详细目录项蓝图。

根据要定义的目录项，该过程可能非常简单，只需一名基础架构架构师将一个计算机组件作为蓝图发布；也可能很复杂，需要多名架构师创建许多不同类型的组件来设计一个完整的应用程序堆栈供用户请求。



Software 组件

您可以创建并发布软件组件，以便在计算机置备过程中安装软件并支持软件生命周期。例如，您可以为开发人员创建蓝图，请求提供一台已安装和配置所需开发环境的计算机。软件组件本身不是目录项，您必须将其与计算机组件组合才能创建目录项蓝图。请参见[设计 Software 组件](#)。

计算机蓝图

可以创建并发布简单蓝图以置备单个计算机，也可以创建包含其他计算机组件和以下组件类型的任意组合（可选）的更复杂蓝图：

- Software 组件
- 现有蓝图

- NSX 网络组件和安全组件
- XaaS 组件
- 容器 组件
- 自定义组件或其他组件

请参见[设计计算机蓝图](#)。

XaaS 蓝图

您可以将 vRealize Orchestrator 工作流作为 XaaS 蓝图发布。例如，您可以为 Active Directory 用户创建自定义资源，并将 XaaS 蓝图设计为允许管理员在 Active Directory 组中置备新用户。您可以在“设计”选项卡外部创建和管理 XaaS 组件。您可以重用已发布的 XaaS 蓝图来创建应用程序蓝图，但必须至少与一个计算机组件结合使用。请参见[设计 XaaS 蓝图和资源操作](#)。

包含多计算机、XaaS 和 Software 组件的应用程序蓝图

您可以将任意数量的计算机组件、Software 组件和 XaaS 蓝图添加到计算机蓝图，为用户提供详细功能。

例如，您可以为管理员创建用于置备新雇用设置的蓝图。您可以将多个计算机组件、软件组件以及 XaaS 蓝图进行组合，以便置备新 Active Directory 用户。QE 管理员可以请求您的“新建雇用”目录项，在 Active Directory 中置备新质量工程员工，并为其分配两个工作虚拟机（分别为 Windows 和 Linux），每个工作虚拟机均具备在这些环境中运行测试案例所需的全部软件。

构建设计库

您可以构建一个可重用蓝图组件的库。架构师能够将这些组件组合到应用程序蓝图中，为用户提供详细的按需服务。

构建最小蓝图设计组件的库：单个计算机蓝图、多个 Software 组件和 XaaS 蓝图，然后采用另一种不同的新方式将这些基本构建块进行组合以创建详细的目录项，为用户提供更多级别的功能。

请注意，可以从 VMware Solution Exchange 获得示例蓝图，网址为 <https://solutionexchange.vmware.com> 和 <https://code.vmware.com>。

表 3-1. 构建设计库

目录项	角色	组件	描述	详细信息
计算机	基础架构架构师	在 蓝图 选项卡上创建计算机蓝图。	您可以创建计算机蓝图，以便向用户快速提供虚拟、私有、公有或混合云计算机。 目录管理员可使用已发布的计算机蓝图，将其作为独立蓝图包含在目录中，但是您也可以将计算机蓝图与其他组件进行组合，创建包括多个计算机蓝图、 Software 或 XaaS 蓝图的更加详细的目录项。	配置计算机蓝图
计算机上的 NSX 网络和安全	基础架构架构师	将 NSX 网络和安全组件添加到 蓝图 选项卡上的 vSphere 计算机蓝图。	您可以配置网络和安全组件，例如网络配置文件和安全组，允许虚拟机彼此通过物理网络和虚拟网络安全高效地通信。 在目录管理员将组件包含在目录之前，您必须将网络和安全组件与至少一个 vSphere 计算机组件进行组合。您只能将 NSX 网络和安全组件应用到 vSphere 计算机蓝图中。	设计带有 NSX 设置的蓝图
计算机上的软件	软件架构师 要成功将软件组件添加到设计画布，还必须具有目标目录的业务组成员、业务组管理员或租户管理员角色访问权限。	在 软件 选项卡上创建并发布 Software 组件，然后将它们与 蓝图 选项卡上的计算机蓝图进行组合。	将 Software 组件添加到计算机蓝图，从而标准化、部署、配置、更新及扩展云环境中的复杂应用程序。这些应用程序的范围可以从简单的 Web 应用程序到复杂的自定义应用程序和打包应用程序。 Software 组件不能单独出现在目录中。您必须创建并发布 Software 组件，然后组合包含至少一个计算机的应用程序蓝图。	创建 Software 组件
自定义 IT 服务	XaaS 架构师	在 XaaS 选项卡上创建并发布 XaaS 蓝图。	您可以创建 XaaS 目录项，该目录项可将 vRealize Automation 功能扩展到计算机、网络、安全和软件置备之外。使用现有的 vRealize Orchestrator 工作流和插件或者在 vRealize Orchestrator 中开发的自定义脚本，就可以将任何 IT 服务交付自动化。 目录管理员可使用已发布的 XaaS 蓝图，将其作为独立蓝图包含在目录中，但是您也可以将其与 蓝图 选项卡上的其他组件进行组合，创建更加详细的目录项。	设计 XaaS 蓝图和资源操作
将已发布的蓝图构建块组合到新目录项中	<ul style="list-style-type: none"> ■ 应用程序架构师 ■ 基础架构架构师 ■ 软件架构师 	将其他计算机蓝图、 XaaS 蓝图和 Software 组件与 蓝图 选项卡上的至少一个计算机组件或计算机蓝图进行组合。	您可以重用已发布的组件和蓝图，以新方式将其组合在一起，创建能为用户提供详细功能的 IT 服务包。	组合复合蓝图

设计计算机蓝图

计算机蓝图是计算机的完整规范，用于确定计算机的属性、置备方式及其策略和管理设置。根据所构建目录项的复杂性，您可以将蓝图中的一个或多个计算机组件与设计画布中的其他组件进行组合，从而创建包含网络和安全、Software 组件、XaaS 组件以及其他蓝图组件的更详细的目录项。

用于虚拟置备的节省空间存储

节省空间的存储技术只使用计算机操作实际需要的存储，消除了传统存储方法的低效性。通常，这仅是实际分配给计算机的存储的一部分。vRealize Automation 支持两种置备节省空间技术的方法：精简置备和 FlexClone 置备。

如果使用标准存储，分配给已置备计算机的存储将完全服务于此计算机，即使它关闭了电源。这是对存储资源的巨大浪费，因为实际上几乎没有虚拟机会使用分配给它们的所有存储，就像几乎没有物理机会 100% 满磁盘运行一样。如果使用节省空间的存储技术，系统将分别跟踪已分配的存储和已使用的存储，而且只有已使用的存储会完全服务于已置备计算机。

精简置备

精简置备支持所有虚拟置备方法。根据虚拟化平台、存储类型和默认存储配置，计算机置备期间可以始终使用精简置备。例如，对于使用 NFS 存储的 vSphere ESX Server 集成，始终会使用精简置备。但是，对于使用本地或 iSCSI 存储的 vSphere ESX Server 集成，如果蓝图中指定了自定义属性 `VirtualMachine.Admin.ThinProvision`，精简置备仅用于置备计算机。有关精简置备的详细信息，请参见虚拟化平台提供的文档。

Net App FlexClone 置备

如果您当前运行的 vSphere 环境使用网络文件系统 (NFS) 存储和 FlexClone 技术，则可以为 NetApp FlexClone 置备创建一个蓝图。

您仅可以使用 NFS 存储，否则计算机置备会失败。您可以为其他类型的计算机置备指定一个 FlexClone 存储路径，但 FlexClone 存储路径与标准存储的工作方式类似。

下文概述了置备使用 FlexClone 技术的计算机所需的一系列步骤：

- 1 IaaS 管理员创建 NetApp ONTAP 端点。请参见[端点设置参考](#)。
- 2 IaaS 管理员在端点上运行数据收集，以使得端点在计算资源和预留页面中可见。
如果存在 NetApp ONTAP 端点，并且该主机为虚拟主机，则会在预留页面上的端点列中显示 FlexClone 选项。如果存在 NetApp ONTAP 端点，则预留页面将显示分配给存储路径的端点。
- 3 架构管理员创建 vSphere 预留，启用 FlexClone 存储，并指定使用 FlexClone 技术的 NFS 存储路径。请参见[为 Hyper-V、KVM、SCVMM、vSphere 或 XenServer 创建预留](#)。
- 4 基础架构架构师或其他授权用户为 FlexClone 置备创建蓝图。

了解和使用蓝图参数化

可以使用组件配置文件对蓝图进行参数化。可以创建一个蓝图并提供小型、中型或大型虚拟机选项，而无需为某种特定部署类型创建单独的小型、中型和大型蓝图。用户可以在部署目录项时选择其中一种大小。

组件配置文件可以最大限度地限制蓝图数量增加，并简化您的目录项。可以使用组件配置文件定义蓝图中的 vSphere 计算机组件。可用的组件配置文件类型有两种，分别是 **Size** 和 **Image**。将组件配置文件添加到计算机组件时，组件配置文件设置将替代计算机组件上的其他设置，例如 CPU 数或存储量。

组件配置文件仅可用于 vSphere 计算机组件。

有关为 **Size** 和 **Image** 组件配置文件定义值集的信息，请参见《自定义属性参考》中的

有关为蓝图中的 vSphere 计算机组件添加组件配置文件和选定值集的信息，请参见 [vSphere 计算机组件设置](#)。

有关使用从 OVF 导入的设置添加组件配置文件信息的详细信息，请参见[将蓝图配置为从 OVF 置备](#)。

有关在请求计算机置备时使用组件配置文件的信息，请参见[通过使用参数化蓝图请求计算机置备](#)。

您可以创建批准策略，以便在根据 **Size** 和 **Image** 组件配置文件的值集条件为蓝图请求计算机置备时要求预先批准。有关详细信息，请参见[基于虚拟机策略类型的批准策略示例](#)。

注

有关从目录中请求计算机置备时使用蓝图参数化的信息，请参见[通过使用参数化蓝图请求计算机置备](#)。

配置计算机蓝图

您可以配置计算机组件并将其发布为独立的蓝图，然后，其他架构师就可以在应用程序蓝图中重用它作为组件，而目录管理员则可以将其包括在目录服务中。

此过程简要概述了蓝图的创建过程。有关新增的详细信息，请参见以下内容：

- [设计带有 NSX 设置的蓝图](#)
- [了解和使用蓝图参数化](#)
- [蓝图属性设置](#)
- [将蓝图配置为从 OVF 置备](#)
- [导出和导入蓝图和内容](#)
- [创建 Microsoft Azure 蓝图并整合资源操作](#)
- [在 vSphere 蓝图添加配置管理功能](#)

前提条件

- 以**基础架构架构师**身份登录到 vRealize Automation。
- 完成外部置备准备（例如，创建模板、WinPE 和 ISO），或者从管理员处收集有关外部准备的信息。
- 配置租户。请参见[配置租户设置](#)。
- 配置 IaaS 资源。请参见[用于配置 IaaS 资源的对照表](#)。

- 请参见《配置 vRealize Automation》。

步骤

- 1 选择设计 > 蓝图。
- 2 单击新建图标 (+)。
- 3 按照新建蓝图对话框上的提示配置常规设置。
- 4 单击确定。
- 5 单击“类别”区域中的计算机类型，显示可用计算机类型的列表。
- 6 将要置备的计算机类型拖动到设计画布上。
- 7 在每个选项卡上输入信息，以配置计算机置备详细信息，如蓝图属性设置中所述。
- 8 单击完成。
- 9 选择蓝图并单击发布。

结果

您已将计算机组件配置并发布为独立蓝图。目录管理员可以将此计算机蓝图包括在服务目录中，并授权用户请求此蓝图。其他架构师可以重用此计算机蓝图来创建更详细的应用程序蓝图，其中包括 Software 组件、XaaS 蓝图或其他计算机蓝图。

后续步骤

您可将计算机蓝图与 Software 组件、XaaS 蓝图或其他计算机蓝图进行组合，创建更详细的应用程序蓝图。请参见组合复合蓝图和了解嵌套蓝图行为。

计算机蓝图设置

您可以为整个蓝图定义配置设置和自定义属性。

蓝图属性设置

创建蓝图时使用蓝图属性可以指定适用于整个蓝图的设置。创建蓝图之后，可以在“蓝图属性”页面中编辑这些设置。

常规选项卡

“常规”选项卡上的“设置”适用于整个蓝图。

表 3-2. 常规选项卡设置

设置	描述
名称	输入蓝图的名称。
标识符	标识符字段根据您输入的名称自动填充。您现在可以编辑此字段，但保存蓝图之后无法更改此字段。由于标识符在租户内是永久且唯一的，因此，您可以使用它们以编程方式与蓝图进行交互并创建属性绑定。
描述	概述蓝图为其他架构师带来的优势。用户在请求表单中也将看到此描述。

表 3-2. 常规选项卡设置（续）

设置	描述
部署限制	指定使用此蓝图置备计算机时可以创建的最大部署数量。
租用天数: 最小和最大	输入最小值和最大值，以允许用户从租约长度范围中选择。租约结束后，部署将会销毁或存档。如果不指定最小值或最大值，租约将设置为永不过期。 在 vRealize Automation 蓝图中输入计算机的租约信息，而不是在源端点应用程序中。如果在外部应用程序中指定租约信息，则无法在 vRealize Automation 中识别或使用该租约信息。
存档天数	您可以指定存档时间段来暂时保留部署，而不是在租约过期后立即销毁部署。指定 0 会在租约过期后销毁部署。存档时间段从租约到期当天开始。存档时间段结束后，部署将会销毁。默认值为 0。
将更新传播到现有部署	CPU、内存或存储的已扩展最小值-最大值范围将推送到从蓝图置备的活动部署中。新范围必须完全包含旧范围。例如，对于最初的最小值 32 和最大值 128 (32, 128)，诸如 (16, 128) 或 (32, 256) 或 (2, 1000) 等更改可以在重新配置或横向扩展时生效，但 (33, 512) 或 (4, 64) 等更改则不能。

NSX 设置选项卡

如果配置了 NSX，那么在创建或编辑蓝图时，可以指定 NSX 传输区域、网络预留策略以及应用程序隔离设置。可在[蓝图](#)和[蓝图属性](#)页面的 **NSX 设置**选项卡上找到这些设置。

有关 NSX 设置的信息，请参见[带 NSX 的新蓝图和蓝图属性页面设置](#)。

属性选项卡

您在蓝图级别添加的自定义属性将应用到整个蓝图，包括所有组件。有关自定义属性优先级的信息，请参见《自定义属性参考》。

表 3-3. 属性选项卡设置

选项卡	设置	描述
属性组	属性组	属性组是属性的可重用组，旨在简化向蓝图添加自定义属性的过程。租户管理员和架构管理员可以将常用属性组合在一起，使您能够向蓝图中添加属性组，而不是分别插入各个自定义属性。
	添加	添加一个或多个现有属性组，并将其应用到整个蓝图。 与容器相关的属性组如下： <ul style="list-style-type: none"> ■ 使用证书身份验证的容器主机属性 ■ 使用用户/密码身份验证的容器主机属性
	上移/下移	通过区分属性组的优先级，控制提供给每个属性组的、相对于另一个属性组的优先级顺序。列表中的第一个组具有最高优先级，其自定义属性的优先级为第一。您还可以通过拖放操作重新排序。
	查看属性	查看选定属性组中的自定义属性。
	查看合并的属性	如果自定义属性包含在多个属性组中，则优先使用优先级最高的属性组中所包含的值。
自定义属性	自定义属性	您可以添加各个自定义属性，而不是属性组。

表 3-3. 属性选项卡设置（续）

选项卡	设置	描述
	新建	添加单个自定义属性并将其应用到整个蓝图。
	名称	输入属性名称。有关自定义属性及其定义的列表，请参见《自定义属性参考》。
	值	输入自定义属性的值。
	加密	如果属性值是密码，则您可以选择进行加密。
	可覆盖	您可以指定属性值可由使用该属性的下一个或后续用户替代。如果您选择 在请求中显示 ，则用户在请求目录项时可以查看和编辑属性值。
	在请求中显示	您可以指定置备请求表单上的用户可以查看属性名称和值。如果允许用户提供值，请选择 可替代 。

vSphere 计算机组件设置

了解在 vRealize Automation 蓝图设计画布中可以为 vSphere 计算机组件配置的设置和选项。vSphere 是可以使用设计画布中 NSX 网络和安全设置的唯一计算机组件类型。

常规选项卡

为 vSphere 计算机组件配置常规设置。

表 3-4. 常规选项卡设置

设置	描述
ID	输入计算机组件的名称，或者接受默认值。
描述	概述计算机组件为其他架构师带来的优势。
请求时显示位置	在 vCloud Air 等云环境中，此设置允许用户为已置备的计算机选择区域。 对于 vSphere 等虚拟环境，您可以配置位置功能，允许用户选择要置备请求计算机的特定数据中心位置。要完全配置此选项，系统管理员需将数据中心位置信息添加到位置文件，架构管理员需编辑计算资源，使其与某一位置关联。
预留策略	您可以将预留策略应用于蓝图，以便限制从该蓝图置备到可用预留子集的计算机。架构管理员需创建预留策略，提供有用的可选方法来控制如何处理预留请求，以便将资源收集到不同服务级别的组中，或者使特定类型的资源可轻松用于特定用途等。如果架构管理员未配置预留策略，则您在此下拉菜单中看不到任何可用的选项。仅适用于当前租户的预留策略可用。

表 3-4. 常规选项卡设置（续）

设置	描述
计算机前缀	<p>计算机前缀由架构管理员创建，用于创建已置备计算机的名称。如果选择使用组默认值，则通过蓝图置备的计算机将根据配置为用户业务组默认值的计算机前缀命名。如果未配置计算机前缀，则会根据业务组的名称为您生成一个前缀。仅适用于当前租户的计算机前缀可用。</p> <p>如果架构管理员配置其他计算机前缀供您选择，则无论请求者是谁，您均可将一个前缀应用于通过蓝图置备的所有计算机。</p>
实例: 最大和最小	<p>配置用户可以在一个部署或缩小、扩大操作中请求的最大和最小实例数。如果不希望为用户提供选择，在最小和最大字段中输入相同的值可以配置要置备的准确实例数并针对此计算机组件停用缩放操作。</p> <p>在缩放操作期间，XaaS 组件不可缩放且未更新。如果在蓝图中使用 XaaS 组件，则可以创建资源操作以便用户在缩放操作后运行，根据需要这可以是缩放或更新 XaaS 部件。或者，您也可以通过配置每个计算机组件要允许的准确实例数来停用缩放。</p>

构建信息选项卡

为 vSphere 计算机组件配置构建信息设置。

表 3-5. 构建信息选项卡

设置	描述
蓝图类型	<p>为了便于记录和许可，请选择是将通过此蓝图置备的计算机分类为“桌面”还是“服务器”。</p>
操作	<p>您在“操作”下拉菜单中看到的选项取决于所选的计算机类型。可用操作如下：</p> <ul style="list-style-type: none"> ■ 创建 <p>在不使用克隆选项的情况下创建计算机组件规范。</p> ■ 克隆 <p>从模板和自定义对象复制虚拟机。</p> ■ 链接克隆 <p>置备节省空间的虚拟机副本，称为“链接克隆”。链接克隆以虚拟机的快照为基础，并使用增量磁盘链来跟踪与父虚拟机的差异。</p> <p>在置备链接克隆虚拟机之前，应关闭蓝图中标识的虚拟机快照。</p> ■ NetApp FlexClone <p>如果架构管理员已在预留中配置使用 NetApp FlexClone 存储，那么您可以使用此技术为计算机克隆节省空间的副本。</p>

表 3-5. 构建信息选项卡（续）

设置	描述
置备 workflow	<p>您在“置备 workflow”下拉菜单中看到的选项取决于所选的计算机类型和操作。</p> <ul style="list-style-type: none"> ■ BasicVmWorkflow 置备没有客户机操作系统的计算机。 ■ ExternalProvisioningWorkflow 通过从虚拟机实例或基于云的映像启动来创建计算机。 ■ ImportOvfWorkflow 用于从 OVF 模板部署 vSphere 虚拟机，部署方式与使用 CloneWorkflow 从虚拟机模板部署 vSphere 虚拟机相同。您可以导入到计算机蓝图的 vSphere 组件中，也可以导入到参数化蓝图的 Image 组件配置文件中。 ■ LinuxKickstartWorkflow 通过从 ISO 映像引导、使用 kickstart 或 autoYaSt 配置文件和 Linux 分发映像以便在计算机上安装操作系统，从而置备计算机。 ■ VirtualSccmProvisioningWorkflow 置备计算机并将控制权传递给 SCCM 任务序列，以便从 ISO 映像引导、部署 Windows 操作系统并安装 vRealize Automation 客户机代理。 ■ WimImageWorkflow 通过引导到 WinPE 环境并使用现有 Windows 参考机的 Windows Imaging File Format (WIM) 映像安装操作系统，以此置备计算机。 在蓝图中使用 WIM 置备 workflow 时，请指定一个存储值，说明将用于计算机的每个磁盘的大小。将所有磁盘的总值用作计算机组件的最小存储值。此外，还要指定每个磁盘的大小，而且磁盘要足以容纳操作系统。
克隆源	<p>选择从中克隆的计算机模板。您可以使用每个列下拉菜单中的筛选器选项来优化可用模板列表。</p> <p>对于链接克隆，您只能看到有快照可以克隆的计算机，以及您以租户管理员或业务组主管身份管理的计算机。</p> <p>您只能从您作为业务组主管或租户管理员管理的计算机上存在的模板中克隆。</p>

表 3-5. 构建信息选项卡（续）

设置	描述
从快照克隆	<p>对于链接克隆，请选择要基于所选计算机模板进行克隆的现有快照。仅当计算机已拥有快照且您以租户管理员或业务组主管身份管理计算机时，计算机才会显示在列表中。</p> <p>如果您选择使用当前快照，则会使用与虚拟机的最新状态相同的特性定义克隆。但如果您想相对于实际快照进行克隆，则请单击下拉菜单选项，然后从列表中选择特定快照。</p> <p>注 使用“快照”一词可能会造成混淆。如果选择现有快照，此选项会创建以该快照为父项的新磁盘。使用当前快照选项不包含要用作父项的基础磁盘，并以静默方式执行完整克隆操作。作为解决办法，您可以在基础磁盘上创建快照，或者使用 vRealize Orchestrator 工作流创建一个快照，然后立即从该快照进行克隆。</p> <p>只有链接克隆操作才可使用此选项。</p>
自定义规范	<p>指定可用的自定义规范。仅当使用静态 IP 地址克隆时才需要自定义规范。</p> <p>您无法对没有自定义规范的 Windows 计算机执行自定义。对于 Linux 克隆计算机，您可以使用自定义规范和/或外部脚本执行自定义。</p>

计算机资源选项卡

为 vSphere 计算机组件指定 CPU、内存和存储设置。

表 3-6. 计算机资源选项卡

设置	描述
CPU：最小值和最大值	输入可以由此计算机置备的 CPU 最小以及最大数量。
内存 (MB)：最小值和最大值	输入可以由此计算机置备的内存最小量以及最大量。
存储 (GB)：最小值和最大值	<p>输入可以由此计算机置备的存储最小量以及最大量。</p> <p>在蓝图中使用 WIM 置备工作流时，请指定一个存储值，说明将用于计算机的每个磁盘的大小。将所有磁盘的总值用作计算机组件的最小存储值。此外，还要指定每个磁盘的大小，而且磁盘要足以容纳操作系统。</p>

存储选项卡

您可以将存储卷设置（包括一个或多个存储预留策略）添加到计算机组件以控制存储空间。

表 3-7. 存储选项卡设置

设置	描述
ID	输入存储卷的 ID 或名称。
容量 (GB)	输入存储卷的存储容量。

表 3-7. 存储选项卡设置（续）

设置	描述
驱动器盘符/挂载路径	输入存储卷的驱动器盘符或挂载路径。 在与客户机代理关联的置备期间使用此选项。计算机置备后，无法更改。如果未使用客户机代理，则会忽略此选项。
标签	输入存储卷的驱动器盘符和挂载路径的标签。 在与客户机代理关联的置备期间使用此选项。计算机置备后，无法更改。如果未使用客户机代理，则会忽略此选项。
存储预留策略	输入将与此存储卷一起使用的现有存储预留策略。仅适用于当前租户的存储预留策略可用。
自定义属性	输入将与此存储卷一起使用的任何自定义属性。
卷最大数量	输入从计算机组件置备时可以使用的存储卷的最大允许数量。输入 0 可防止其他用户添加存储卷。默认值为 60。
允许用户查看并更改存储预留策略	选中该复选框会允许用户在置备时移除相关预留策略或指定不同的预留策略。

网络选项卡

您可以根据在 vRealize Automation 外部配置的 NSX 网络和负载均衡器设置，为 vSphere 计算机组件配置网络设置。您可以使用设计画布中的一个或多个现有和按需 NSX 网络组件中的设置。

有关在使用 vSphere 计算机组件中的“网络”选项卡设置之前添加和配置 NSX 网络和安全组件的信息，请参见[配置网络与安全组件设置](#)。

有关指定适用于 vSphere 计算机组件的蓝图级别 NSX 设置的信息，请参见[带 NSX 的新蓝图和蓝图属性页面设置](#)。

表 3-8. 网络选项卡设置

设置	描述
网络	从下拉菜单中选择网络组件。只会列出设计画布中存在的网络组件。仅适用于当前租户的网络配置文件可用。
分配类型	接受从网络组件中派生的默认分配或者从下拉菜单中选择分配类型。 DHCP 和 静态 选项值根据网络组件中的设置派生。
地址	指定网络的 IP 地址。此选项仅适用于静态地址类型。
负载均衡	输入要用于负载均衡的服务。
自定义属性	显示为选定的网络组件或网络配置文件配置的自定义属性。
网络适配器的最大数量	为此计算机组件指定允许使用的网络适配器或网卡的最大数量。默认值为“无限制”。设置为 0 会停用为计算机组件添加网卡。

安全选项卡

您可以根据在 vRealize Automation 外部配置的 NSX 设置，为 vSphere 计算机组件配置安全设置。您也可以选择使用设计画布中的现有和按需 NSX 安全组件中的设置。

设计画布中的现有和按需安全组及安全标记组件中的安全设置会自动可用。

有关在使用 vSphere 计算机组件中的“安全”选项卡设置之前添加和配置 NSX 网络和安全组件的信息，请参见[配置网络与安全组件设置](#)。

有关指定适用于 vSphere 计算机组件的蓝图级别 NSX 信息的信息，请参见[带 NSX 的新蓝图和蓝图属性页面设置](#)。

表 3-9. 安全选项卡设置

设置	描述
名称	显示 NSX 安全组或标记的名称。名称派生自设计画布中的安全组件。 如果选中所列安全组或标记旁的复选框，则会使用该组或标记从此计算机组件进行置备。
类型	指示安全元素是按需安全组、现有安全组还是安全标记。
描述	显示为安全组或标记定义的描述。
端点	显示由 NSX 安全组或标记使用的端点。

属性选项卡

此外，还可以为 vSphere 计算机组件指定自定义属性和属性组信息。

您可以使用[属性](#)选项卡，将各个和各组自定义属性添加到计算机组件。使用[蓝图属性](#)页面创建或编辑蓝图时，您也可以使用[属性](#)选项卡将自定义属性和属性组添加到整个蓝图。

您可以使用[自定义属性](#)选项卡为现有自定义属性添加和配置选项。vRealize Automation 提供了自定义属性，您也可以创建属性定义。

表 3-10. 属性 > 自定义属性 选项卡设置

设置	描述
名称	输入自定义属性的名称或从下拉菜单中选择可用的自定义属性。仅当租户管理员或架构管理员已创建属性定义时，属性才会在下拉菜单中显示。
值	输入或编辑一个值，以与自定义属性名称相关联。例如，将值设置为 true ，可允许授权用户使用 SSH 连接到虚拟机。
加密	如果属性值是密码，则您可以选择进行加密。
可覆盖	您可以指定属性值可由使用该属性的下一个或后续用户替代。该用户通常是另一位架构师，但如果选择“在请求中显示”，则业务用户能够在请求目录项时查看和编辑属性值。
在请求中显示	如果要向最终用户显示属性名称和值，则可以在请求计算机置备时选择在请求表单中显示属性。如果希望用户提供值，则还必须选择“可覆盖”。

您可以使用[属性组](#)选项卡为现有自定义属性组添加和配置设置。您可以创建自己的属性组或使用已为您创建的属性组。

表 3-11. 属性 > 属性组 选项卡设置

设置	描述
名称	从下拉菜单中选择可用的属性组。
上移和下移	按降序控制列出的属性组的优先级。首先列出的属性组优先于之后列出的属性组，以此类推。
查看属性	显示选定属性组中的自定义属性。
查看合并的属性	显示列出的属性组中的所有自定义属性，并以它们在属性组列表中出现顺序显示。当同一个属性在多个属性组中出现时，该属性名称仅会在其第一次出现时所在的列表中显示。

“配置文件”选项卡

组件配置文件提供了一种参数化蓝图的方法。例如，您可以创建一个具有小型、中型和大型容量的单个蓝图，并允许在部署过程中选择其中一种容量大小，而不是创建单独的小型、中型和大型蓝图。组件配置文件设计可最大限度地减少蓝图数量增长，并简化您的目录。

如果您已经为提供的 vRealize Automation 组件配置文件 **Size** 和 **Image** 创建值集，那么您可以为蓝图中的计算机组件添加并配置这些设置。部署目录项时，您也可以选择不同的值集。

组件配置文件仅可用于 vSphere 计算机组件。

当您向蓝图中的 vSphere 计算机组件添加组件配置文件时，在配置文件的选定值集中定义的设置将替代计算机组件上的其他设置，例如 CPU 和存储数量。

这些组件配置文件值集将应用到集群中的所有 vSphere 计算机。

您无法使用 **Size** 或 **Image** 组件配置文件重新配置计算机，但是基于配置文件计算的 CPU、内存和存储范围将仍可用于重新配置操作。例如，如果您使用小型（1 个 CPU、1024 MB 内存和 10 GB 存储）、中型（3 个 CPU、2048 MB 内存、12 GB 存储）和大型（5 个 CPU、3072 MB 内存和 15 GB 存储）**Size** 值集，那么计算机重新配置期间可用的范围是 1-5 个 CPU、1024-3072 MB 内存以及 1-15 GB 存储。

有关相关信息，请参见《自定义属性参考》。

表 3-12. 配置文件选项卡设置

设置	描述
添加	添加 Size 或 Image 组件配置文件。
编辑值集	通过从定义的值集列表中进行选择，为所选组件配置文件分配一个或多个值集。您可以选择其中一个值集作为默认值。
移除	移除 Size 或 Image 组件配置文件。

vCloud Air 计算机组件设置

了解在 vRealize Automation 蓝图设计画布中可以为 vCloud Air 计算机组件配置的设置和选项。

常规选项卡

为 vCloud Air 计算机组件配置常规设置。

表 3-13. 常规选项卡设置

设置	描述
ID	输入计算机组件的名称，或者接受默认值。
描述	概述计算机组件为其他架构师带来的优势。
请求时显示位置	<p>在 vCloud Air 等云环境中，此设置允许用户为已置备的计算机选择区域。</p> <p>对于 vSphere 等虚拟环境，您可以配置位置功能，允许用户选择要置备请求计算机的特定数据中心位置。要完全配置此选项，系统管理员需将数据中心位置信息添加到位置文件，架构管理员需编辑计算资源，使其与某一位置关联。</p>
预留策略	<p>您可以将预留策略应用于蓝图，以便限制从该蓝图置备到可用预留子集的计算机。架构管理员需创建预留策略，提供有用的可选方法来控制如何处理预留请求，以便将资源收集到不同服务级别的组中，或者使特定类型的资源可轻松用于特定用途等。如果架构管理员未配置预留策略，则您在此下拉菜单中看不到任何可用的选项。仅适用于当前租户的预留策略可用。</p>
计算机前缀	<p>计算机前缀由架构管理员创建，用于创建已置备计算机的名称。如果选择使用组默认值，则通过蓝图置备的计算机将根据配置为用户业务组默认值的计算机前缀命名。如果未配置计算机前缀，则会根据业务组的名称为您生成一个前缀。仅适用于当前租户的计算机前缀可用。</p> <p>如果架构管理员配置其他计算机前缀供您选择，则无论请求者是谁，您均可将一个前缀应用于通过蓝图置备的所有计算机。</p>
实例: 最大和最小	<p>配置用户可以在一个部署或缩小、扩大操作中请求的最大和最小实例数。如果不希望为用户提供选择，在最小和最大字段中输入相同的值可以配置要置备的准确实例数并针对此计算机组件停用缩放操作。</p> <p>在缩放操作期间，XaaS 组件不可缩放且未更新。如果在蓝图中使用 XaaS 组件，则可以创建资源操作以便用户在缩放操作后运行，根据需要这可以是缩放或更新 XaaS 部件。或者，您也可以通过配置每个计算机组件要允许的准确实例数来停用缩放。</p>

构建信息选项卡

为 vCloud Air 计算机组件配置构建信息设置。

表 3-14. 构建信息选项卡

设置	描述
蓝图类型	<p>为了便于记录和许可，请选择是将通过此蓝图置备的计算机分类为“桌面”还是“服务器”。</p>
操作	<p>您在“操作”下拉菜单中看到的选项取决于所选的计算机类型。唯一可对 vCloud Air 计算机组件执行的置备操作是 Clone。</p> <ul style="list-style-type: none"> ■ 克隆 <p>从模板和自定义对象复制虚拟机。</p>

表 3-14. 构建信息选项卡（续）

设置	描述
置备工作流	<p>您在“置备工作流”下拉菜单中看到的选项取决于所选的计算机类型和操作。</p> <p>唯一可对 vCloud Air 计算机组件执行的置备操作是 CloneWorkflow。</p> <p>■ CloneWorkflow</p> <p>通过克隆、链接克隆或 NetApp Flexclone 复制虚拟机。</p>
克隆源	<p>选择从中克隆的计算机模板。您可以使用每个列下拉菜单中的筛选器选项来优化可用模板列表。</p> <p>对于链接克隆，您只能看到有快照可以克隆的计算机，以及您以租户管理员或业务组主管身份管理的计算机。</p> <p>您只能从您作为业务组主管或租户管理员管理的计算机上存在的模板中克隆。</p>

计算机资源选项卡

为 vCloud Air 计算机组件指定 CPU、内存和存储设置。

表 3-15. 计算机资源选项卡

设置	描述
CPU：最小值和最大值	输入可以由此计算机置备的 CPU 最小以及最大数量。
内存 (MB)：最小值和最大值	输入可以由此计算机置备的内存最小量以及最大量。
存储 (GB)：最小值和最大值	输入可以由此计算机置备的存储最小量以及最大量。

存储选项卡

您可以将存储卷设置（包括一个或多个存储预留策略）添加到计算机组件以控制存储空间。

表 3-16. 存储选项卡设置

设置	描述
ID	输入存储卷的 ID 或名称。
容量 (GB)	输入存储卷的存储容量。
驱动器盘符/挂载路径	<p>输入存储卷的驱动器盘符或挂载路径。</p> <p>在与客户机代理关联的置备期间使用此选项。计算机置备后，无法更改。如果未使用客户机代理，则会忽略此选项。</p>
标签	<p>输入存储卷的驱动器盘符和挂载路径的标签。</p> <p>在与客户机代理关联的置备期间使用此选项。计算机置备后，无法更改。如果未使用客户机代理，则会忽略此选项。</p>
存储预留策略	输入将与此存储卷一起使用的现有存储预留策略。仅适用于当前租户的存储预留策略可用。
自定义属性	输入将与此存储卷一起使用的任何自定义属性。

表 3-16. 存储选项卡设置（续）

设置	描述
卷最大数量	输入从计算机组件置备时可以使用的存储卷的最大允许数量。输入 0 可防止其他用户添加存储卷。默认值为 60。
允许用户查看并更改存储预留策略	选中该复选框会允许用户在置备时移除相关预留策略或指定不同的预留策略。

属性选项卡

此外，还可以为 vCloud Air 计算机组件指定自定义属性和属性组信息。

您可以使用**属性**选项卡，将各个和各组自定义属性添加到计算机组件。使用**蓝图属性**页面创建或编辑蓝图时，您也可以使用**属性**选项卡将自定义属性和属性组添加到整个蓝图。

您可以使用**自定义属性**选项卡为现有自定义属性添加和配置选项。vRealize Automation 提供了自定义属性，您也可以创建属性定义。

表 3-17. 属性 > 自定义属性 选项卡设置

设置	描述
名称	输入自定义属性的名称或从下拉菜单中选择可用的自定义属性。仅当租户管理员或架构管理员已创建属性定义时，属性才会在下拉菜单中显示。
值	输入或编辑一个值，以与自定义属性名称相关联。例如，将值设置为 true ，可允许授权用户使用 SSH 连接到虚拟机。
加密	如果属性值是密码，则您可以选择进行加密。
可覆盖	您可以指定属性值可由使用该属性的下一个或后续用户替代。该用户通常是另一位架构师，但如果选择“在请求中显示”，则业务用户能够在请求目录项时查看和编辑属性值。
在请求中显示	如果要向最终用户显示属性名称和值，则可以在请求计算机置备时选择在请求表单中显示属性。如果希望用户提供值，则还必须选择“可覆盖”。

您可以使用**属性组**选项卡为现有自定义属性组添加和配置设置。您可以创建自己的属性组或使用已为您创建的属性组。

表 3-18. 属性 > 属性组 选项卡设置

设置	描述
名称	从下拉菜单中选择可用的属性组。
上移和下移	按降序控制列出的属性组的优先级。首先列出的属性组优先于之后列出的属性组，以此类推。
查看属性	显示选定属性组中的自定义属性。
查看合并的属性	显示列出的属性组中的所有自定义属性，并以它们在属性组列表中出现顺序显示。当同一个属性在多个属性组中出现时，该属性名称仅会在其第一次出现时所在的列表中显示。

Amazon 计算机组件设置

了解您可以在 vRealize Automation 蓝图设计画布中为 Amazon 计算机组件配置的设置和选项。

常规选项卡

为 Amazon 计算机组件配置常规设置。

表 3-19. 常规选项卡设置

设置	描述
ID	输入计算机组件的名称，或者接受默认值。
描述	概述计算机组件为其他架构师带来的优势。
请求时显示位置	在 vCloud Air 等云环境中，此设置允许用户为已置备的计算机选择区域。对于 vSphere 等虚拟环境，您可以配置位置功能，允许用户选择要置备请求计算机的特定数据中心位置。要完全配置此选项，系统管理员需将数据中心位置信息添加到位置文件，架构管理员需编辑计算资源，使其与某一位置关联。
预留策略	您可以将预留策略应用于蓝图，以便限制从该蓝图置备到可用预留子集的计算机。架构管理员需创建预留策略，提供有用的可选方法来控制如何处理预留请求，以便将资源收集到不同服务级别的组中，或者使特定类型的资源可轻松用于特定用途等。如果架构管理员未配置预留策略，则您在此下拉菜单中看不到任何可用的选项。仅适用于当前租户的预留策略可用。
计算机前缀	计算机前缀由架构管理员创建，用于创建已置备计算机的名称。如果选择 使用组默认值 ，则通过蓝图置备的计算机将根据配置为用户业务组默认值的计算机前缀命名。如果未配置计算机前缀，则会根据业务组的名称为您生成一个前缀。仅适用于当前租户的计算机前缀可用。 如果架构管理员配置其他计算机前缀供您选择，则无论请求者是谁，您均可将一个前缀应用于通过蓝图置备的所有计算机。
实例: 最大和最小	配置用户可以在一个部署或缩小、扩大操作中请求的最大和最小实例数。如果不希望为用户提供选择，在 最小 和 最大 字段中输入相同的值可以配置要置备的准确实例数并针对此计算机组件停用缩放操作。 在缩放操作期间，XaaS 组件不可缩放且未更新。如果在蓝图中使用 XaaS 组件，则可以创建资源操作以便用户在缩放操作后运行，根据需要这可以是缩放或更新 XaaS 部件。或者，您也可以通过配置每个计算机组件要允许的准确实例数来停用缩放。

构建信息选项卡

为 Amazon 计算机组件配置构建信息设置。

表 3-20. 构建信息选项卡

设置	描述
蓝图类型	为了便于记录和许可，请选择是将通过此蓝图置备的计算机分类为“桌面”还是“服务器”。
置备 workflow	<p>可用于 Amazon 计算机组件的唯一置备 workflow 是 CloudProvisioningWorkflow。</p> <ul style="list-style-type: none"> ■ CloudProvisioningWorkflow <p>通过从虚拟机实例或基于云的映像启动来创建计算机。</p>

表 3-20. 构建信息选项卡（续）

设置	描述
Amazon 计算机映像	选择可用的 Amazon 计算机映像。Amazon 计算机映像是一个包含软件配置（包括操作系统）的模板。计算机映像由 Amazon Web Services 帐户管理。您可以使用 AMI ID 列下拉菜单中的 筛选器 选项来细化所显示的 Amazon 计算机映像名称列表。
密钥对	<p>使用 Amazon Web Services 置备时需要密钥对。</p> <p>密钥对用于置备和连接到云实例。它们还可用于对 Windows 密码进行解密和登录到 Linux 计算机。</p> <p>以下密钥对选项可用：</p> <ul style="list-style-type: none"> ■ 未指定 <p>控制蓝图级别（而非预留级别）的密钥对行为。</p> ■ 根据业务组自动生成 <p>指定同一业务组中置备的每台计算机均具有相同的密钥对，其中包括当该计算机具有相同的计算资源和业务组时在其他预留上置备的计算机。由于密钥对与业务组关联，因此删除业务组时这些密钥对也会随之删除。</p> ■ 根据计算机自动生成 <p>指定每台计算机拥有唯一的密钥对。“根据计算机自动生成”选项是一种最安全的方法，因为密钥对不在计算机之间共享。</p>
在计算机上启用 Amazon 网络选项	选择当用户提交请求时是允许他们在 Virtual Private Cloud (VPC) 还是非 VPC 位置上置备计算机。
实例类型	<p>选择一个或多个 Amazon 实例类型。Amazon 实例是指可在 Amazon Web Services 中运行应用程序的虚拟服务器。实例是通过使用 Amazon 计算机映像并选择适当的实例类型创建的。vRealize Automation 管理可用于置备的计算机映像实例类型。</p> <p>有关在 vRealize Automation 中使用 Amazon 实例类型的信息，请参见了解 Amazon 实例类型和添加 Amazon 实例类型。</p>

计算机资源选项卡

为 Amazon 计算机组件指定 CPU、内存、存储和 EBS 卷设置。

您也可以在部署中重新配置除根卷外的所有 Amazon 计算机存储卷。

表 3-21. 计算机资源选项卡

设置	描述
CPU：最小值和最大值	输入可以由此计算机置备的 CPU 最小以及最大数量。
内存 (MB)：最小值和最大值	输入可以由此计算机置备的内存最小量以及最大量。
存储 (GB)：最小值和最大值	输入可以由此计算机置备的存储最小量以及最大量。

表 3-21. 计算机资源选项卡 （续）

设置	描述
EBS 存储 (GB): 最小值和最大值	输入可以由此计算机置备的 Amazon Elastic Block Store (EBS) 存储卷的最小量以及最大量。 销毁包含 Amazon 计算机组件的部署时，将会分离在此计算机的生命周期内为其添加的所有 EBS 卷，而不是将这些卷销毁。 vRealize Automation 未提供销毁 EBS 卷的选项。
删除卷	指定销毁 Amazon 部署时是否可以单独或批量删除 EC2 卷。 “是”和“否”均允许在部署中进行所有卷批量销毁操作。默认值为 null 或空。 <ul style="list-style-type: none"> ■ 是 - 销毁 Amazon 部署并删除卷。 ■ 否 - 销毁 Amazon 部署并保留卷。 ■ null 或空 - 要求用户在销毁 Amazon 部署时指定 Yes 或 No 值。

属性选项卡

此外，还可以为 Amazon 计算机组件指定自定义属性和属性组信息。

您可以使用**属性**选项卡，将各个和各组自定义属性添加到计算机组件。使用**蓝图属性**页面创建或编辑蓝图时，您也可以使用**属性**选项卡将自定义属性和属性组添加到整个蓝图。

您可以使用**自定义属性**选项卡为现有自定义属性添加和配置选项。vRealize Automation 提供了自定义属性，您也可以创建属性定义。

表 3-22. 属性 > 自定义属性 选项卡设置

设置	描述
名称	输入自定义属性的名称或从下拉菜单中选择可用的自定义属性。 仅当租户管理员或架构管理员已创建属性定义时，属性才会在下拉菜单中显示。
值	输入或编辑一个值，以与自定义属性名称相关联。例如，将值设置为 true ，可允许授权用户使用 SSH 连接到虚拟机。
加密	如果属性值是密码，则您可以选择进行加密。
可覆盖	您可以指定属性值可由使用该属性的下一个或后续用户替代。该用户通常是另一位架构师，但如果选择“在请求中显示”，则业务用户能够在请求目录项时查看和编辑属性值。
在请求中显示	如果要向最终用户显示属性名称和值，则可以在请求计算机置备时选择在请求表单中显示属性。如果希望用户提供值，则还必须选择“可覆盖”。

您可以使用**属性组**选项卡为现有自定义属性组添加和配置设置。您可以创建自己的属性组或使用已为您创建的属性组。

表 3-23. 属性 > 属性组 选项卡设置

设置	描述
名称	从下拉菜单中选择可用的属性组。
上移和下移	按降序控制列出的属性组的优先级。首先列出的属性组优先于之后列出的属性组，以此类推。
查看属性	显示选定属性组中的自定义属性。
查看合并的属性	显示列出的属性组中的所有自定义属性，并以它们在属性组列表中出现的顺序显示。当同一个属性在多个属性组中出现时，该属性名称仅会在其第一次出现时所在的列表中显示。

OpenStack 计算机组件设置

了解在 vRealize Automation 蓝图设计画布中可以为 OpenStack 计算机组件配置的设置和选项。

常规选项卡

为 OpenStack 计算机组件配置常规设置。

表 3-24. 常规选项卡设置

设置	描述
ID	输入计算机组件的名称，或者接受默认值。
描述	概述计算机组件为其他架构师带来的优势。
请求时显示位置	在 vCloud Air 等云环境中，此设置允许用户为已置备的计算机选择区域。 对于 vSphere 等虚拟环境，您可以配置位置功能，允许用户选择要置备请求计算机的特定数据中心位置。要完全配置此选项，系统管理员需将数据中心位置信息添加到位置文件，架构管理员需编辑计算资源，使其与某一位置关联。
预留策略	您可以将预留策略应用于蓝图，以便限制从该蓝图置备到可用预留子集的计算机。架构管理员需创建预留策略，提供有用的可选方法来控制如何处理预留请求，以便将资源收集到不同服务级别的组中，或者使特定类型的资源可轻松用于特定用途等。如果架构管理员未配置预留策略，则您在此下拉菜单中看不到任何可用的选项。仅适用于当前租户的预留策略可用。
计算机前缀	计算机前缀由架构管理员创建，用于创建已置备计算机的名称。如果选择 使用组默认值 ，则通过蓝图置备的计算机将根据配置为用户业务组默认值的计算机前缀命名。如果未配置计算机前缀，则会根据业务组的名称为您生成一个前缀。仅适用于当前租户的计算机前缀可用。 如果架构管理员配置其他计算机前缀供您选择，则无论请求者是谁，您均可将一个前缀应用于通过蓝图置备的所有计算机。
实例: 最大和最小	配置用户可以在一个部署或缩小、扩大操作中请求的最大和最小实例数。如果不希望为用户提供选择，在 最小 和 最大 字段中输入相同的值可以配置要置备的准确实例数并针对此计算机组件停用缩放操作。 在缩放操作期间，XaaS 组件不可缩放且未更新。如果在蓝图中使用 XaaS 组件，则可以创建资源操作以使用户在缩放操作后运行，根据需要这可以是缩放或更新 XaaS 部件。或者，您也可以通过配置每个计算机组件要允许的准确实例数来停用缩放。

构建信息选项卡

为 OpenStack 计算机组件配置构建信息设置。

表 3-25. 构建信息选项卡

设置	描述
蓝图类型	<p>为了便于记录和许可，请选择是将通过此蓝图置备的计算机分类为“桌面”还是“服务器”。</p>
置备 workflow	<p>以下置备 workflow 可用于 OpenStack 计算机组件：</p> <ul style="list-style-type: none"> ■ CloudLinuxKickstartWorkflow <p>通过从 ISO 映像引导、使用 kickstart 或 autoYaSt 配置文件和 Linux 分发映像以便在计算机上安装操作系统，从而置备计算机。</p> ■ CloudProvisioningWorkflow <p>通过从虚拟机实例或基于云的映像启动来创建计算机。</p> ■ CloudWIMImageWorkflow <p>通过引导到 WinPE 环境并使用现有 Windows 参考机的 Windows Imaging File Format (WIM) 映像安装操作系统，以此置备计算机。</p> <p>在蓝图中使用 WIM 置备 workflow 时，请指定一个存储值，说明将用于计算机的每个磁盘的大小。将所有磁盘的总值用作计算机组件的最小存储值。此外，还要指定每个磁盘的大小，而且磁盘要足以容纳操作系统。</p>
OpenStack 映像	<p>选择可用的 OpenStack 映像。OpenStack 映像是一个包含软件配置（包括操作系统）的模板。这些映像由 OpenStack 帐户管理。您可以使用名称列下拉菜单中的筛选器选项来细化显示的 OpenStack 映像名称列表。</p>
密钥对	<p>使用 OpenStack 置备时密钥对是可选的。</p> <p>密钥对用于置备和连接到云实例。它们还可用于对 Windows 密码进行解密和登录到 Linux 计算机。</p> <p>以下密钥对选项可用：</p> <ul style="list-style-type: none"> ■ 未指定 <p>控制蓝图级别（而非预留级别）的密钥对行为。</p> ■ 根据业务组自动生成 <p>指定同一业务组中置备的每台计算机均具有相同的密钥对，其中包括当该计算机具有相同的计算资源和业务组时在其他预留上置备的计算机。由于密钥对与业务组关联，因此删除业务组时这些密钥对也会随之删除。</p> ■ 根据计算机自动生成 <p>指定每台计算机拥有唯一的密钥对。“根据计算机自动生成”选项是一种最安全的方法，因为密钥对不在计算机之间共享。</p>
功能	<p>选择一个或多个 OpenStack 功能。OpenStack 功能是为 OpenStack 中置备的实例定义计算机资源规范的虚拟硬件模板。功能在 OpenStack 提供程序内管理并在数据收集期间导入。</p>

计算机资源选项卡

为 OpenStack 计算机组件指定 CPU、内存和存储设置。

表 3-26. 计算机资源选项卡

设置	描述
CPU：最小值和最大值	输入可以由此计算机置备的 CPU 最小以及最大数量。
内存 (MB)：最小值和最大值	输入可以由此计算机置备的内存最小量以及最大量。
存储 (GB)：最小值和最大值	输入可以由此计算机置备的存储最小量以及最大量。 在蓝图中使用 WIM 置备工作流时，请指定一个存储值，说明将用于计算机的每个磁盘的大小。将所有磁盘的总值用作计算机组件的最小存储值。此外，还要指定每个磁盘的大小，而且磁盘要足以容纳操作系统。

属性选项卡

此外，还可为 OpenStack 计算机组件指定自定义属性和属性组信息。

您可以使用**属性**选项卡，将各个和各组自定义属性添加到计算机组件。使用**蓝图属性**页面创建或编辑蓝图时，您也可以使用**属性**选项卡将自定义属性和属性组添加到整个蓝图。

您可以使用**自定义属性**选项卡为现有自定义属性添加和配置选项。vRealize Automation 提供了自定义属性，您也可以创建属性定义。

表 3-27. 属性 > 自定义属性 选项卡设置

设置	描述
名称	输入自定义属性的名称或从下拉菜单中选择可用的自定义属性。仅当租户管理员或架构管理员已创建属性定义时，属性才会在下拉菜单中显示。
值	输入或编辑一个值，以与自定义属性名称相关联。例如，将值设置为 true ，可允许授权用户使用 SSH 连接到虚拟机。
加密	如果属性值是密码，则您可以选择进行加密。
可覆盖	您可以指定属性值可由使用该属性的下一个或后续用户替代。该用户通常是另一位架构师，但如果选择“在请求中显示”，则业务用户能够在请求目录项时查看和编辑属性值。
在请求中显示	如果要向最终用户显示属性名称和值，则可以在请求计算机置备时选择在请求表单中显示属性。如果希望用户提供值，则还必须选择“可覆盖”。

您可以使用**属性组**选项卡为现有自定义属性组添加和配置设置。您可以创建自己的属性组或使用已为您创建的属性组。

表 3-28. 属性 > 属性组 选项卡设置

设置	描述
名称	从下拉菜单中选择可用的属性组。
上移和下移	按降序控制列出的属性组的优先级。首先列出的属性组优先于之后列出的属性组，以此类推。
查看属性	显示选定属性组中的自定义属性。
查看合并的属性	显示列出的属性组中的所有自定义属性，并以它们在属性组列表中出现的顺序显示。当同一个属性在多个属性组中出现时，该属性名称仅会在其第一次出现时所在的列表中显示。

使用网络自定义属性

您可以在蓝图级别或计算机组件级别使用网络自定义属性为 vSphere 以外的计算机组件和不包含 NSX 的蓝图指定网络和安全信息。

网络与安全组件仅可与 vSphere 计算机组件结合使用。非 vSphere 计算机组件不包含**网络或安全性**选项卡。

对于具有关联 NSX 的 vSphere 计算机组件，使用用户界面中的网络、安全和负载平衡设置。对于没有**网络或安全**选项卡的计算机组件，您可以在设计画面中相应的**属性**选项卡添加网络和安全自定义属性，例如 `VirtualMachine.Network0.Name`。NSX 网络属性、安全属性和负载平衡器属性仅适用于 vSphere 计算机。

在设计画布中配置计算机组件时，您既可以使用**属性**选项卡分别定义自定义属性，也可以将自定义属性作为现有属性组的一部分进行配置。为计算机组件定义的自定义属性与通过蓝图置备的这类计算机有关。

有关可用自定义属性的信息，请参见《自定义属性参考》。

对克隆和链接克隆的蓝图进行故障排除

创建链接克隆或克隆蓝图时，缺少计算机或模板。使用共享克隆蓝图请求计算机时，计算机置备失败。

问题

使用克隆或链接克隆蓝图时，可能会遇到以下问题之一：

- 创建链接克隆蓝图时，要克隆的列表中未显示计算机，或者要克隆的计算机没有出现。
- 创建克隆蓝图时，要克隆的模板列表中未显示模板，或者所需的模板没有出现。
- 使用共享克隆蓝图请求计算机后，置备失败。
- 由于数据收集的计时问题，已移除的模板在用户创建或编辑链接克隆蓝图时仍然可见。

请注意，置备到 SDRS 时不支持链接克隆。链接克隆将在与父项相同的数据存储上创建，但不会在群集数据存储之间重新平衡。在这种情况下，父数据存储最终可能会填满。

原因

导致克隆和链接克隆蓝图出现常见问题的可能原因有很多种。

有关克隆源和从快照克隆以及创建蓝图时提供的**使用当前快照**选项的相关信息，请参见 [vSphere 计算机组件设置](#)。

表 3-29. 导致克隆和链接克隆蓝图出现常见问题的原因

问题	原因	解决方案
缺少计算机	您只能使用以租户管理员或业务组主管身份管理的计算机创建链接克隆蓝图。	租户或业务组中的用户必须请求 vSphere 计算机。如果具有适当的角色，则您自己可以执行此操作。您还可以在此对话框中看到非受管计算机。受管计算机可能已导入。不要求在此对话框中显示从 vRealize Automation 置备的计算机。
缺少模板	数据收集在给定端点上失败或者没有可用于组件平台的端点。	<ul style="list-style-type: none"> 如果端点集群在一起且包含多个计算资源，请确认 IaaS 管理员已将包含这些模板的群集添加到架构组中。 对于新模板，请确认 IT 已将这些模板放置在架构组中包含的同一群集内。
使用共享蓝图置备失败	对于蓝图，系统未提供验证，无法确保用于从共享克隆蓝图置备计算机的预留中存在您所选的模板。	请考虑使用授权，将蓝图限于那些对该模板所在计算资源具有预留的用户。
使用客户机代理置备失败	虚拟机可能在客户机操作系统自定义完成之后、但客户机代理工作项完成之前立即重新引导，从而导致置备失败。您可以使用自定义属性 <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> 增加延迟时间。	确认您已添加自定义属性 <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> 。该值必须采用 HH:MM:SS 格式。如果未设置该值，则默认值为一分钟 (00:01:00)。
由于找不到克隆所基于的模板，克隆或链接克隆蓝图置备失败	如果蓝图克隆自不再存在的模板，则无法从该蓝图置备计算机。 vRealize Automation 会定期运行数据收集，默认为每 24 小时。如果移除模板，则在下次收集数据前不会反映此更改，因此有可能基于不存在的模板创建蓝图。	使用现有模板重新定义蓝图，然后请求置备。 作为一项预防措施并且如果适用，您可以在定义克隆或链接克隆蓝图前运行数据收集。

设计带有 NSX 设置的蓝图

如果已配置 vRealize Automation 与 NSX for vSphere 或 NSX-T 的集成，则可以使用设计画布中的网络、安全和负载均衡器组件配置用于置备计算机的蓝图。

您还可以将以下 NSX 网络和安全设置添加到整个蓝图。

- 传输区域 - 包含用于已置备的计算机部署的网络。
- 网络预留策略 - 管理为已置备的计算机部署的网络通信。
- 应用程序隔离 - 仅允许已置备的计算机部署中使用的计算机之间的内部流量。

有关 vRealize Automation 和 NSX 集成的详细信息，请参见此 [vRA 和 NSX - 网络与安全自动化简介](#) 博客文章并预览 [vRealize Automation 和 NSX 网络和安全](#) 课程系列的内容。

NSX 设置仅适用于 vSphere 计算机组件类型。

带 NSX 的新蓝图和蓝图属性页面设置

在创建蓝图时使用 [新建蓝图](#) 页面，可以指定适用于整个蓝图的设置，包括一些 NSX 设置。创建蓝图之后，可以在“蓝图属性”页面中编辑这些设置。

常规选项卡

“常规”选项卡上的“设置”适用于整个蓝图。

表 3-30. 常规选项卡设置

设置	描述
名称	输入蓝图的名称。
标识符	标识符字段根据您输入的名称自动填充。您现在可以编辑此字段，但保存蓝图之后无法更改此字段。由于标识符在租户内是永久且唯一的，因此，您可以使用它们以编程方式与蓝图进行交互并创建属性绑定。
描述	概述蓝图为其他架构师带来的优势。用户在请求表单中也将看到此描述。
部署限制	指定使用此蓝图置备计算机时可以创建的最大部署数量。
租用天数: 最小和最大	输入最小值和最大值，以允许用户从租约长度范围中选择。租约结束后，部署将会销毁或存档。如果不指定最小值或最大值，租约将设置为永不过期。 在 vRealize Automation 蓝图中输入计算机的租约信息，而不是在源端点应用程序中。如果在外部应用程序中指定租约信息，则无法在 vRealize Automation 中识别或使用该租约信息。
存档天数	您可以指定存档时间段来暂时保留部署，而不是在租约过期后立即销毁部署。指定 0 会在租约过期后销毁部署。存档时间段从租约到期当天开始。存档时间段结束后，部署将会销毁。默认值为 0。
将更新传播到现有部署	CPU、内存或存储的已扩展最小值-最大值范围将推送到从蓝图置备的活动部署中。新范围必须完全包含旧范围。例如，对于最初的最小值 32 和最大值 128 (32, 128)，诸如 (16, 128) 或 (32, 256) 或 (2, 1000) 等更改可以在重新配置或横向扩展时生效，但 (33, 512) 或 (4, 64) 等更改则不能。

NSX 设置选项卡

如果配置了 NSX，那么在创建或编辑蓝图时，可以指定 NSX 传输区域、网络预留策略以及应用程序隔离设置。可在 [蓝图](#) 和 [蓝图属性](#) 页面的 **NSX 设置** 选项卡上找到这些设置。

有关配置 NSX 的信息，请参见《[NSX 管理指南](#)》。

表 3-31. NSX 设置选项卡设置

设置	描述
传输区域	<p>选择现有的 NSX 传输区域以包含已置备计算机部署可以使用的网络。</p> <p>传输区域定义网络可以跨哪些集群。置备计算机时，如果在预留和蓝图中指定传输区域，则传输区域值必须匹配。仅适用于当前租户的传输区域可用。</p> <p>对于包含 NSX for vSphere 或 NSX-T 按需网络和/或要在部署蓝图时创建的安全对象的蓝图，要求具有传输区域。</p> <p>有关详细信息，请参见将 NSX 传输区域应用于蓝图。</p>
网络预留策略	<p>对于 NSX for vSphere，请选择一个网络预留策略以帮助确定要在蓝图部署中放置 Edge 或 DLR 的位置。</p> <p>当 vRealize Automation 通过 NAT 或路由网络置备计算机时，会将路由网关置备为网络路由器。Edge 或路由网关是一个管理计算机，它像其他虚拟机一样使用计算资源，但会管理该部署中所有计算机的网络通信。用于置备 Edge 或路由网关的预留将确定用于 NAT 的外部网络和负载均衡器的虚拟 IP 地址。最佳做法是为管理计算机（例如 NSX Edge）使用单独的管理集群。</p> <p>对于 NSX-T，请选择一个网络预留策略以帮助确定要在蓝图部署中放置第 0 层逻辑路由器的位置。</p> <p>有关详细信息，请参见将 NSX 网络预留策略应用于蓝图。</p>
应用程序隔离	<p>选中应用程序隔离复选框会使用 NSX for vSphere 中配置的应用程序隔离安全策略。应用程序隔离策略将应用于蓝图中的所有 vSphere 计算机组件。此外，您也可以选择添加安全组和标记，使 vRealize Orchestrator 打开隔离网络配置，以允许其他路径进出应用程序隔离。</p> <p>有关详细信息，请参见将 NSX 应用程序隔离应用于蓝图。</p>

属性选项卡

您在蓝图级别添加的自定义属性将应用到整个蓝图，包括所有组件。有关自定义属性优先级的信息，请参见《自定义属性参考》。

表 3-32. 属性选项卡设置

选项卡	设置	描述
属性组	属性组是属性的可重用组，旨在简化向蓝图添加自定义属性的过程。租户管理员和架构管理员可以将常用属性组合在一起，使您能够向蓝图中添加属性组，而不是分别插入各个自定义属性。	
	添加	<p>添加一个或多个现有属性组，并将其应用到整个蓝图。</p> <p>与容器相关的属性组如下：</p> <ul style="list-style-type: none"> ■ 使用证书身份验证的容器主机属性 ■ 使用用户/密码身份验证的容器主机属性
	上移/下移	<p>通过区分属性组的优先级，控制提供给每个属性组的、相对于另一个属性组的优先级顺序。列表中的第一个组具有最高优先级，其自定义属性的优先级为第一。您还可以通过拖放操作重新排序。</p>
	查看属性	查看选定属性组中的自定义属性。

表 3-32. 属性选项卡设置（续）

选项卡	设置	描述
自定义属性	查看合并的属性	如果自定义属性包含在多个属性组中，则优先使用优先级最高的属性组中所包含的值。
	您可以添加各个自定义属性，而不是属性组。	
	新建	添加单个自定义属性并将其应用到整个蓝图。
	名称	输入属性名称。有关自定义属性及其定义的列表，请参见《自定义属性参考》。
	值	输入自定义属性的值。
	加密	如果属性值是密码，则您可以选择进行加密。
	可覆盖	您可以指定属性值可由使用该属性的下一个或后续用户替代。如果您选择 在请求中显示 ，则用户在请求目录项时可以查看和编辑属性值。
	在请求中显示	您可以指定置备请求表单上的用户可以查看属性名称和值。如果允许用户提供值，请选择 可替代 。

将 NSX 传输区域应用于蓝图

NSX 管理员可以创建传输区域来控制网络的群集使用。

传输区域控制逻辑交换机可以访问的主机。它可以跨一个或多个主机群集，包括跨多个 vCenter 的主机。

对于包含按需 NAT 或按需路由网络的蓝图，请指定包含置备计算机部署要使用的网络的传输区域。

对于包括 NSX-T 端点的蓝图，必须指定传输区域。

为蓝图指定的传输区域必须与为蓝图使用的预留指定的传输区域匹配。请参见[将 NSX 网络预留策略应用于蓝图](#)。

- 如果您的蓝图不使用 NSX-T 按需组件，将忽略传输区域值。
- NSX-T 支持多个覆盖网络传输区域和多个 VLAN 传输区域。
- 创建逻辑交换机需要传输区域。在传输区域内创建逻辑交换机。
- 制作蓝图时，只会显示当前租户的传输区域。当前租户中的预留使用传输区域时，这些传输区域可用。

将 NSX 网络预留策略应用于蓝图

置备蓝图时，系统将使用预留策略对可以考虑部署的预留进行分组。网络信息包含在每个预留中。

如果此预留策略中存在传输区域，则该传输区域必须与蓝图中指定的传输区域匹配。请参见[将 NSX 传输区域应用于蓝图](#)。

您可以使用[新建蓝图](#)或[蓝图属性](#)页面在蓝图级别应用网络预留策略。

NSX for vSphere 注意事项

对于 NSX for vSphere，此预留策略有助于确定 NSX Edge 的放置或与按需网络关联的分布式逻辑路由器 (DLR) 的选择。这也称为路由网关预留策略或 Edge 预留策略。

例如，对于 NSX for vSphere，NAT 网络配置文件和负载均衡器使 vRealize Automation 可以部署 NSX Edge 服务网关。路由网络配置文件使用 NSX for vSphere 逻辑分布式路由器 (DLR)。必须在 NSX 中创建 DLR，然后才能供 vRealize Automation 使用。vRealize Automation 无法创建 DLR。数据收集后，vRealize Automation 可以使用 DLR 进行虚拟机置备。

NSX Edge 为 NSX 部署外部的网络提供路由服务和连接。NSX Edge 网关提供了常见的网关服务（如 NAT）和动态路由以将隔离的子网连接到共享（上行链路）网络。NSX Edge 常见部署包括多租户环境，在这些环境中，NSX Edge 会为每个租户创建虚拟边界。

vRealize Automation 为 NAT 网络和负载均衡器提供了 Edge 服务网关等路由网关。对于路由网络，vRealize Automation 使用现有的分布式路由器。

用于置备 Edge 或路由网关的预留将确定用于 NAT 和路由网络配置文件的外部网络以及负载均衡器的虚拟 IP 地址。

NSX-T 注意事项

对于 NSX-T，此预留策略有助于选择用于部署的第 0 层逻辑路由器。

第 0 层逻辑路由器具有下行链路端口以连接到第 1 层逻辑路由器，并具有上行链路端口以连接到外部网络。vRA 将第 1 层逻辑路由器连接到第 0 层逻辑路由器进行北向物理路由器访问，并向逻辑路由器执行 NAT 和负载均衡器服务分配一个 Edge 群集。

将 NSX 应用程序隔离应用于蓝图

您可以启用应用程序隔离，以仅允许蓝图置备的组件之间的内部流量。

NSX 应用程序隔离策略充当防火墙，阻止部署中已置备计算机流入或流出的所有入站和出站流量。指定已定义的 NSX 应用程序隔离策略时，通过蓝图置备的计算机可以相互通信，但无法连接到防火墙外部。

如果指定了应用程序隔离规则，并且还使用蓝图中的安全组指定了安全规则，则应用程序隔离设置是蓝图部署期间处理的最后一个规则。

您可以使用[新建蓝图](#)或[蓝图属性](#)页在蓝图级别应用应用程序隔离。

NSX for vSphere 注意事项

已置备的组件放置在安全组中，该安全组使用防火墙规则隔离。启用要求 vSphere 端点配置为支持 NSX 应用程序隔离。

使用 NSX for vSphere 应用程序隔离策略时，仅允许通过蓝图置备的计算机之间的内部流量。请求置备时，系统将为要置备的计算机创建安全组。应用程序隔离策略是在 NSX for vSphere 中创建的，并应用于安全组。在安全策略中定义防火墙规则，确保在部署中的组件之间仅允许内部流量。

通过结合使用 NSX for vSphere Edge 负载均衡器与 NSX for vSphere 应用程序隔离安全策略的蓝图进行置备时，动态置备的负载均衡器不会添加到安全组。这会阻止负载均衡器与旨在处理连接的计算机进行通信。由于 Edge 已从 NSX for vSphere 分布式防火墙中排除，因此无法将它们添加到安全组。要支持负载均衡正常工作，请使用其他允许所需流量进入组件虚拟机的安全组或安全策略，从而实现负载均衡。

与 NSX for vSphere 中的其他安全策略相比，应用程序隔离策略的优先级较低。例如，如果置备的部署包含 Web 组件计算机和应用程序组件计算机，且 Web 组件计算机托管 Web 服务，则该服务必须允许端口 80 和 443 上的入站流量。在这种情况下，用户必须在 NSX for vSphere 中创建 Web 安全策略，并且定义允许入站流量流入这些端口的防火墙规则。在 vRealize Automation 中，用户必须对已置备的计算机部署的 Web 组件应用 Web 安全策略。

注 如果蓝图包含一个或多个负载均衡器，并且为蓝图启用了应用程序隔离，则会将负载均衡器 VIP 作为 IPSet 添加到应用程序隔离安全组中。如果蓝图包含的按需安全组所关联的计算机层同时关联了负载均衡器，该按需安全组将包含计算机层，以及负载均衡器 VIP 的 IPSet。

如果 Web 组件计算机需要在端口 8080 和 8443 上使用负载均衡器访问应用程序组件计算机，则除了允许入站流量流入端口 80 和 443 的现有防火墙规则之外，Web 安全策略还应包括允许出站流量流入这些端口的防火墙规则。

NSX-T 注意事项

已置备的组件放置在 NS 组中，该 NS 组使用防火墙规则隔离。启用要求 vSphere 端点配置为支持 NSX 应用程序隔离。

NSX-T 支持创建双层逻辑路由器拓扑：顶层逻辑路由器为第 0 层，底层逻辑路由器为第 1 层。这种结构允许提供商管理员和租户管理员完全控制其服务和策略。在 NSX-T 中，管理员控制和配置第 0 层路由和服务，租户管理员控制和配置第 1 层。

配置网络与安全组件设置

vRealize Automation 支持基于 NSX 平台的虚拟化网络。还支持集成的 vRealize Automation 容器网络。

要将 NSX 网络和安全与 vRealize Automation 集成，IaaS 管理员必须配置 vSphere 和 NSX 端点。vRealize Automation 支持 NSX for vSphere 和 NSX-T。

有关外部准备的信息，请参见《配置 vRealize Automation》。

您可以创建网络配置文件，用于指定预留和蓝图中的网络设置。外部网络配置文件将定义现有的物理网络。按需 NAT 和路由网络配置文件可以为新网络路径构建 NSX 逻辑交换机和相应的路由设置。

添加到蓝图中的网络与安全组件设置派生自 NSX for vSphere 和 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX 清单。网络与安全组件特定于 NSX，并且只能供 vSphere 计算机组件使用。有关配置 NSX 的信息，请参见 [NSX for vSphere 产品文档](#) 或 [NSX-T 产品文档](#) 中的《管理指南》，具体取决于您使用的应用程序。

对于具有关联 NSX 的 vSphere 计算机组件，使用用户界面中的网络、安全和负载均衡设置。对于没有网络或安全选项卡的计算机组件，您可以在设计画面中相应的属性选项卡添加网络 and 安全性自定义属性，例如 `VirtualMachine.Network0.Name`。NSX 网络属性、安全属性和负载均衡器属性仅适用于 vSphere 计算机。

如果在预留和蓝图中指定网络配置文件，则优先使用蓝图值。例如，如果利用 `VirtualMachine.NetworkN.ProfileName` 自定义属性在蓝图中和蓝图所用的预留中指定网络配置文件，则优先使用在蓝图中指定的网络配置文件。但是，如果该自定义属性不用于蓝图且您为计算机网卡选择网络配置文件，则 vRealize Automation 将对已指定网络配置文件的计算机网卡使用预留网络路径。

根据计算资源，您可以选择用于标识 vSphere 端点的传输区域。传输区域将指定可与在该区域中创建的逻辑交换机关联的主机和群集。传输区域可以跨多个 vSphere 群集。置备中使用的蓝图和预留必须具有相同的传输区域设置。传输区域是在 NSX 环境中定义的。

您可以通过在预留、蓝图或客户机代理脚本中指定信息来配置安全设置。如果要置备的计算机需要客户机代理，您必须将包含该要求的安全规则添加到预留或蓝图。例如，如果您使用拒绝所有计算机之间的通信的默认安全策略，并依赖不同的安全策略以允许特定计算机之间的通信，则客户机代理在自定义阶段可能无法与 vRealize Automation 通信。要避免在计算机置备期间出现此问题，请使用允许在自定义阶段进行通信的默认安全策略。

您还可以将 容器 网络组件添加到蓝图。

在 vRealize Automation 中控制安全对象的租户访问

可以在 vRealize Automation 中控制 NSX 安全对象的跨租户可用性。

在 vRealize Automation 中创建 NSX 安全对象时，其默认可用性可以是全局的，这意味着可在具有预留的关联端点的所有租户中可用，也可以对管理员之外的所有用户隐藏。

此外，租户间安全对象的可用性取决于关联端点在租户中是否具有预留或预留策略。

NSX 不支持租户安全组。但是，可以通过使用

`VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` 自定义属性在 vRealize Automation 中控制安全组的可用性。

默认情况下，新的安全对象可用于关联的 NSX 端点具有预留的所有租户。如果端点在活动租户中没有预留，则安全对象在活动租户中不可用。

如果未在 NSX 端点上设置 `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` 自定义属性，新的安全对象将默认设置为全局。升级到此 vRealize Automation 版本之前存在的安全对象均设置为全局，而与自定义属性无关。

注 升级到此 vRealize Automation 版本后，来自以前版本的安全组默认设置为全局。现有安全组和安全标记在关联的端点具有预留的所有租户中所有。

默认情况下，可以通过将 `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` 自定义属性添加到关联的 NSX 端点，隐藏新安全组。此设置将在下一次 NSX 端点进行数据收集时生效且仅应用于新的安全对象。

此外，还可以通过编程方式更改现有安全对象的租户设置。例如，如果安全组设置为全局，可以在 vRealize Automation REST API 或 vRealize CloudClient 中使用关联的 NSX 端点的租户 ID 设置更改安全对象的租户可用性。NSX 端点的可用租户 ID 设置如下所示：

- "`<global>`" - 安全对象可用于所有租户。这是升级到此版本后现有安全对象的默认设置，同时也是您创建的所有新安全对象的默认设置。
- "`<unscoped>`" - 安全对象不可用于任何租户。只有系统管理员可以访问安全对象。定义最终分配给特定租户的安全对象时，这是理想设置。
- "`tenant_id_name`" - 安全对象仅可用于单个指定租户。

可以使用 vRealize Automation REST API 或 vRealize CloudClient 工具将与特定端点关联的安全对象的租户 ID 参数 (`tenantId`) 分配为指定租户。

有关 vRealize Automation REST API 命令的信息，请参见适用于您的 vRealize Automation 7.x 版本的 [vRealize Automation API 文档](#) 部分中的《vRealize Automation API 参考》。有关其他信息，请参见适用于您的 vRealize Automation 7.x 版本的 [vRealize Automation API 文档](#) 部分中的《vRealize Automation 编程指南》。

有关 vRealize CloudClient 的信息，请参见 <https://code.vmware.com/web/dp/tool/cloudclient>。

了解网络连接、安全性和负载均衡器配置的 NSX-T 部署拓扑

您可以根据您在 vRealize Automation 蓝图中配置 NSX-T 网络和安全性及负载均衡器组件的方式建立并使用各种部署拓扑。

网络连接和安全性

■ 路由网络

如果在蓝图中将 NSX-T 路由网络组件连接到 vSphere 计算机组件，在 NSX-T 中置备以下拓扑：

- 创建第 1 层路由器。
- 创建逻辑交换机。
- 将第 1 层路由器向下链接到逻辑交换机。
- 在第 1 层路由器上通告特定路由路线。

■ NAT 网络（静态 IP）

如果在蓝图中将 NSX-T NAT 网络连接到 vSphere 计算机组件，在 NSX-T 中置备以下拓扑：

- 创建第 1 层路由器。
- 创建逻辑交换机。
- 将第 1 层路由器连接到 Edge 群集。
- 将第 1 层路由器向上链接到第 0 层路由器；从预留中选择第 0 层路由器。
- 将第 1 层路由器向下链接到逻辑交换机。
- 在第 1 层路由器上通告所有 NAT 路由。
- 从支持按需 NAT 网络配置文件的外部网络配置文件中为每个 NAT 网络分配一个外部 IP。使用此 IP 以便符合 SNAT 和 DNAT 规则。

■ NAT 网络 (DHCP)

如果在蓝图中使用 DHCP 将 NSX-T NAT 网络连接到 vSphere 计算机组件，在 NSX-T 中置备以下拓扑：

- 创建第 1 层路由器。
- 创建逻辑交换机。
- 将第 1 层路由器连接到 Edge 群集。
- 将第 1 层路由器向上链接到第 0 层路由器；从预留中选择第 0 层路由器。
- 将第 1 层路由器向下链接到逻辑交换机。
- 置备一个带有 IP 池的 DHCP 服务器。

- 在第 1 层路由器上通告所有 NAT 路由。
- 应用程序隔离

如果带 NSX-T 组件的蓝图要求应用程序隔离，在 NSX-T 中置备以下拓扑：

注 创建或编辑蓝图时，在“蓝图属性”页面上为蓝图配置应用程序隔离。

- 创建一个 NS 组。
- 创建一个带防火墙隔离规则的防火墙部分。
- 使用标记将蓝图中的计算机添加到应用程序隔离 NS 组。
- 将 IPset 中 NAT 网络的负载均衡器 VIP 和外部 IP 添加到应用程序隔离 NS 组。

为支持应用程序隔离 NS 组，必须将计算机连接到含糊网络。

- 现有 NS 组

如果在蓝图中将现有 NS 组组件连接到 vSphere 计算机组件，在 NSX-T 中置备以下拓扑：

- 在 NSX-T 中使用标记将连接到 NS 组的计算机作为成员资格条件添加到 NS 组。

为支持现有 NS 组，必须将计算机连接到含糊网络。

负载均衡器

NSX-T 蓝图部署中的负载均衡器支持以下拓扑：

- NAT 按需网络上的单臂。
- 路由按需网络上的单臂。
- 外部（现有）网络上的单臂。
- 双臂，一个在 NAT 上，一个在外部。
- 双臂，一个在路由网络上，一个在外部。

如果将 NSX-T 负载均衡器添加到蓝图，除网络拓扑外，还应在部署中置备以下拓扑：

- 对于所有拓扑（负载均衡器在外部网络上为单臂的情况除外）：
 - 即使在蓝图中有多个负载均衡器组件，也应创建单个负载均衡器服务。
 - 部署时将负载均衡器服务连接到第 1 层路由器。按需创建第 1 层路由器。
- 对于负载均衡器在外部网络上为单臂的拓扑：
 - 在预留中指定的外部网络必须是 VC 含糊网络（NSX-T 逻辑交换机）。
 - 第 1 层路由器必须存在且连接到外部网络（NSX-T 逻辑交换机）。
 - 如果第 1 层路由器尚不存在，请按需创建负载均衡器服务器并将其连接到第 1 层路由器；否则，使用现在已有的负载均衡器。
- 通告 VIP 路由，除非 VIP 在专用 NAT 网络上。
- 在负载均衡器服务上创建一个或多个虚拟服务器。

基于负载均衡器的大小，每个负载均衡器服务的虚拟服务器数量都存在一些限制。

- 为每个虚拟服务器创建一个虚拟服务器应用程序配置文件。
- 为每个已配置持久性选项的虚拟服务器创建一个虚拟服务器持久性配置文件。
- 配置一个成员资格池，使其包含成员资格池中每个计算机的静态 IP。
- 无论在蓝图中有多个负载均衡器组件，也应创建单个负载均衡器服务。
- 为每个成员池创建并配置一个运行状况监控器。

对于支持 HTTPS 的虚拟服务器，与 NSX for vSphere 中的负载均衡器不同，在 NSX-T 负载均衡器中不支持 SSL 直通。vRealize Automation 将负载均衡器虚拟服务器配置为在负载均衡器处终止 SSL，从负载均衡器到池成员使用普通 HTTP。在配置带 HTTPS 的虚拟服务器时，必须指定证书名称和 SSL 客户端配置文件名称，在 NSX-T 中必须同时存在两者。您可以将证书导入 NSX-T 信任管理器。

在蓝图上存在多个 NSX-T 组件时，将在所有组件之间共享第 1 层逻辑路由器，并对该路由器进行相应配置。外部第 1 层逻辑路由器 ID 将显示在 vRealize Automation “部署” 页面上每个组件的“详细信息”视图中。

使用蓝图中的 NSX for vSphere 网络组件

您可以将一个或多个 NSX for vSphere 网络组件添加到设计画布，为蓝图中的 vSphere 计算机组件配置设置。

添加到蓝图中的网络与安全组件设置派生自 NSX for vSphere 配置，要求您对 vSphere 群集运行数据收集以获得 NSX for vSphere 清单。网络与安全组件特定于 NSX for vSphere，并且只能供 vSphere 计算机组件使用。有关配置 NSX for vSphere 的信息，请参见 [NSX for vSphere 产品文档](#) 中的《NSX 管理指南》。

为 NSX for vSphere 添加现有网络组件

您可以将现有 NSX for vSphere 网络组件添加到设计画布中，以便将其设置与蓝图中的一个或多个 vSphere 计算机组件关联起来。

您可以使用现有网络组件将 NSX for vSphere 网络添加到设计画布，并将其设置配置为与 vSphere 计算机组件和涉及 vSphere 的 Software 或 XaaS 组件一起使用。

将现有网络组件或按需网络组件与计算机组件关联时，网卡信息随计算机组件一起存储。指定的网络配置文件信息将与网络组件一起存储。

您可以向设计画布中添加多个网络与安全组件。

对于具有关联 NSX 的 vSphere 计算机组件，使用用户界面中的网络、安全和负载均衡设置。对于没有网络或安全选项卡的计算机组件，您可以在设计画面中相应的属性选项卡添加网络 and 安全性自定义属性，例如 `VirtualMachine.Network0.Name`。NSX 网络属性、安全属性和负载均衡器属性仅适用于 vSphere 计算机。

制作蓝图时，仅显示适用于当前租户的网络配置文件。具体来说，当前租户中至少有一个预留且该预留至少将一个网络分配给配置文件时，网络配置文件可用。

前提条件

- 创建并配置 NSX 的网络设置。请参见《配置 vRealize Automation》中的 NSX 配置检查表以及 [NSX for vSphere 产品文档](#) 中的 NSX for vSphere 管理指南》。

- 确认已针对您的集群成功运行 NSX 清单。
- 要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 创建网络配置文件。
- 以**基础架构架构师**身份登录到 vRealize Automation。
- 使用**设计**选项卡在设计画布中打开新蓝图或现有蓝图。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的**网络和安全**。
- 2 将**现有网络**组件拖动到设计画布上。
- 3 单击**现有网络**文本框并选择现有网络配置文件。
描述、子网掩码和网关值根据选定的网络配置文件填充。
- 4 （可选）单击 **DNS/WINS** 选项卡。
- 5 （可选）为网络配置文件指定 DNS 和 WINS 设置。
 - 主 DNS
 - 辅助 DNS
 - DNS 后缀
 - 首选 WINS
 - 备用 WINS
 无法更改现有网络的 DNS 和 WINS 设置。
- 6 （可选）单击 **IP 范围**选项卡。
显示网络配置文件中指定的 IP 范围。您可以更改排序顺序或列显示。对于 NAT 网络，还可以更改 IP 范围值。
- 7 要将蓝图另存为草稿或继续配置蓝图，请单击**保存或完成**。

后续步骤

您可以在 vSphere 计算机组件的**网络**选项卡中添加网络设置。

创建和使用 NSX for vSphere 的 NAT 规则

当 NAT 网络组件关联到非群集 vSphere 计算机组件或按需 NSX for vSphere 负载平衡器组件时，您可以将 NAT 规则添加到蓝图中的一对多 NAT 网络组件。

您可以为 NSX for vSphere 支持的任何协议定义 NAT 规则。您可以将端口或端口范围从 Edge 的外部 IP 地址映射到 NAT 网络组件中的专用 IP 地址。

- vSphere 计算机组件

您可以为关联到非群集 vSphere 计算机组件的一对多 NAT 网络组件创建 NAT 规则。

例如，如果两台计算机与蓝图中的 NAT 一对多网络组件关联，则可定义一个 NAT 规则，允许外部 IP 上的端口 443 使用 TCP 协议通过 NAT 网络上的端口 80 连接到该计算机。

■ NSX for vSphere 负载均衡器组件

您可为关联到 NSX for vSphere 负载均衡器组件的 VIP 网络的 NAT 一对多网络组件创建 NAT 规则。

例如，如果 NAT 网络组件关联到对三台计算机进行负载均衡的负载均衡器组件，则可以定义一个 NAT 规则，允许外部 IP 上的端口 90 使用 UDP 协议通过 NAT 网络上的端口 80 连接到负载均衡器 VIP。

您可创建任意数量的 NAT 规则，且可控制这些规则的处理顺序。

NAT 规则不支持以下元素：

- 不在当前网络中的网卡
- 配置为使用 DHCP 获取 IP 地址的网卡
- 计算机群集

要将 NAT 规则添加到蓝图中的 NAT 网络组件，请参见[添加按需 NAT 或按需路由网络组件](#)。

有关使用 NAT 规则的相关信息，请参见公众文章，例如这篇 [vmwarelab 博客文章](#)。

添加按需 NAT 或按需路由网络组件

您可以在准备时将 NSX for vSphere 按需 NAT 网络组件或 NSX for vSphere 按需路由网络组件添加到设计画布中，以便将其设置与蓝图中的一个或多个 vSphere 计算机组件关联起来。

将现有网络组件或按需网络组件与计算机组件关联时，网卡信息随计算机组件一起存储。指定的网络配置文件信息将与网络组件一起存储。

您可以向设计画布中添加多个网络与安全组件。

一个蓝图中可包含多个按需网络组件。但是，蓝图中使用的所有按需网络配置文件必须引用相同的外部网络配置文件。

对于具有关联 NSX 的 vSphere 计算机组件，使用用户界面中的网络、安全和负载均衡设置。对于没有网络或安全选项卡的计算机组件，您可以在设计画面中相应的属性选项卡添加网络和安全自定义属性，例如 `VirtualMachine.Network0.Name`。NSX 网络属性、安全属性和负载均衡器属性仅适用于 vSphere 计算机。

制作蓝图时，仅显示适用于当前租户的网络配置文件。具体来说，当前租户中至少有一个预留且该预留至少将一个网络分配给配置文件时，网络配置文件可用。

前提条件

- 创建并配置 NSX for vSphere 的网络设置。请参见 [NSX for vSphere 产品文档](#) 中的《配置 vRealize Automation》和《NSX 管理指南》。
- 确认已针对您的集群成功运行 NSX 清单。
要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 创建按需网络配置文件。请参见[创建网络配置文件](#)。

例如，如果要添加按需 NAT 网络组件，请参见[为按需网络创建 NAT 网络配置文件](#)。

- 以[基础架构架构师](#)身份登录到 vRealize Automation。
- 使用[设计](#)选项卡在设计画布中打开新蓝图或现有蓝图。
- 如果要为 NAT 网络组件指定 NAT 规则，则必须使用 NAT 一对多网络配置文件。请参见[使用提供的 IPAM 端点创建 NAT 网络配置文件](#)或[使用第三方 IPAM 端点创建 NAT 网络配置文件](#)。有关 NAT 规则的信息，请参见[创建和使用 NSX for vSphere 的 NAT 规则](#)。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的[网络和安全](#)。
- 2 将按需 NAT 或按需路由网络组件拖动到设计画布上。
- 3 要在设计画布中唯一标记组件，请在 **ID** 文本框中输入组件名称。
- 4 从父[网络配置文件](#)下拉菜单中选择相应的网络配置文件。例如，如果要添加 NAT 网络组件，请选择配置为支持目标网络设置的 NAT 网络配置文件。

如果要在 NAT 网络组件中指定 NAT 规则，则必须使用为 NAT 一对多配置的父网络配置文件。

根据选择的配置文件类型，将根据网络配置文件选择填充以下网络设置。对这些值的更改必须在网络配置文件中进行：

- 外部网络配置文件名称
 - NAT 类型（按需 NAT）
 - 子网掩码
 - 范围子网掩码（按需路由）
 - 范围子网掩码（按需路由）
 - 基本 IP 地址（按需路由）
- 5 （可选）在[描述](#)文本框中输入组件描述。
 - 6 （可选）单击 **DNS/WINS** 选项卡。
 - 7 （可选）为网络配置文件指定 DNS 和 WINS 设置。
 - 主 DNS
 - 辅助 DNS
 - DNS 后缀
 - 首选 WINS
 - 备用 WINS

无法更改现有网络的 DNS 和 WINS 设置。

8 单击 **IP 范围** 选项卡。

显示网络配置文件中指定的 IP 范围。您可以更改排序顺序或列显示。对于 NAT 网络，还可以更改 IP 范围值。

- a 在 **IP 范围起始** 文本框中输入起始 IP 地址值。
- b 在 **IP 范围结束** 文本框中输入起始 IP 地址值。

9 如果使用基于使用静态 IP 范围的一对多 NAT 网络配置文件的 NAT 网络，则可以使用 **NAT 规则** 选项卡，添加允许外部 IP 访问内部 NAT 网络中组件的规则。

对于 NAT 一对多网络，可以定义 NAT 规则（将 NAT 网络组件添加到蓝图时可进行配置，编辑部署中的 NAT 网络时可进行更改）。

可供选择的选项取决于与 NAT 网络组件关联的 vSphere 计算机或 NSX for vSphere 负载均衡器组件。

- **名称** - 输入唯一的规则名称。
- **组件** - 从关联的 vSphere 计算机或与 NAT 网络关联的负载均衡器组件的列表中进行选择。
仅非群集计算机支持 NAT 规则。如果指定的群集大小大于 1，则不会列出任何组件，因为配置不受支持。
- **源端口** - 选择 ANY 选项，输入有效端口或端口范围，或者指定有效的属性绑定。
- **目标端口** - 选择 ANY 选项，输入有效端口或端口范围，或者指定有效的属性绑定。
- **协议** - 输入 NSX for vSphere 支持的任何有效协议，或选择 TCP、UDP 或“任意”选项。
- **描述** - 输入 NAT 规则设计的简要描述。

10 要将蓝图另存为草稿或继续配置蓝图，请单击 **保存** 或 **完成**。

后续步骤

您可以在 vSphere 计算机组件的 **网络** 选项卡中添加网络设置。

使用蓝图中的 NSX-T 网络组件

您可以将一个或多个 NSX-T 网络组件添加到设计画布，为蓝图中的 vSphere 计算机组件配置设置。

添加到蓝图中的网络与安全组件设置派生自 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX-T 清单。网络与安全组件特定于 NSX-T，并且只能供 vSphere 计算机组件使用。有关配置 NSX-T 的信息，请参见 [NSX-T 产品文档](#) 中的《NSX-T 管理指南》。

部署的蓝图包含 NSX-T 端点时，部署将向部署中的所有 NSX-T 组件分配一个标记，这些组件包括 NSX-T 网络、安全和负载均衡器组件以及 NSX-T 端点的关联 vSphere 计算机组件。标记对部署是唯一的，并与初始部署中的组件以及您在部署中所做的任何后续操作相关联。标记名称与部署的名称相同。

有关 NSX-T -特定部署和拓扑注意事项的详细信息，请参见 [了解网络连接、安全性和负载均衡器配置的 NSX-T 部署拓扑](#)。

为 NSX-T 添加现有网络组件

您可以将现有 NSX-T 网络组件添加到设计画布中，以便将其设置与蓝图中的一个或多个 vSphere 计算机组件关联起来。

您可以使用现有网络组件将 NSX-T 网络添加到设计画布，并将其设置配置为与 vSphere 计算机组件和涉及 vSphere 的 Software 或 XaaS 组件一起使用。

将现有网络组件或按需网络组件与计算机组件关联时，网卡信息随计算机组件一起存储。指定的网络配置文件信息将与网络组件一起存储。

您可以向设计画布中添加多个网络与安全组件。

对于具有关联 NSX 的 vSphere 计算机组件，使用用户界面中的网络、安全和负载平衡设置。对于没有网络或安全选项卡的计算机组件，您可以在设计画面中相应的属性选项卡添加网络和安全自定义属性，例如 `VirtualMachine.Network0.Name`。NSX 网络属性、安全属性和负载平衡器属性仅适用于 vSphere 计算机。

制作蓝图时，仅显示适用于当前租户的网络配置文件。具体来说，当前租户中至少有一个预留且该预留至少将一个网络分配给配置文件时，网络配置文件可用。

前提条件

- 创建并配置 NSX-T 的网络设置。请参见 [NSX-T 产品文档](#) 中的《配置 vRealize Automation》和《NSX-T 管理指南》。
- 确认已针对您的集群成功运行 NSX 清单。
要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 创建网络配置文件。
- 以基础架构架构师身份登录到 vRealize Automation。
- 使用设计选项卡在设计画布中打开新蓝图或现有蓝图。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的网络和安全。
- 2 将现有网络组件拖动到设计画布上。
- 3 单击现有网络文本框并选择现有网络配置文件。
描述、子网掩码和网关值根据选定的网络配置文件填充。
- 4 （可选）单击 DNS/WINS 选项卡。
- 5 （可选）为网络配置文件指定 DNS 和 WINS 设置。
 - 主 DNS
 - 辅助 DNS
 - DNS 后缀
 - 首选 WINS
 - 备用 WINS

无法更改现有网络的 DNS 和 WINS 设置。

6 （可选）单击 **IP 范围** 选项卡。

显示网络配置文件中指定的 IP 范围。您可以更改排序顺序或列显示。对于 NAT 网络，还可以更改 IP 范围值。

7 要将蓝图另存为草稿或继续配置蓝图，请单击**保存或完成**。

后续步骤

您可以在 vSphere 计算机组件的**网络**选项卡中添加网络设置。

创建和使用 NSX-T 的 NAT 规则

当 NAT 网络组件关联到非群集 vSphere 计算机组件时，您可以向蓝图中的一对多 NAT 网络组件添加 NAT 规则。

您可以为 NSX-T 支持的任何协议定义 NAT 规则。您可以将端口或端口范围从 Edge 的外部 IP 地址映射到 NAT 网络组件中的专用 IP 地址。

您可以为关联到非群集 vSphere 计算机组件的一对多 NAT 网络组件创建 NAT 规则。例如，如果两台计算机与蓝图中的 NAT 一对多网络组件关联，则可定义一个 NAT 规则，允许外部 IP 上的端口 443 使用 TCP 协议通过 NAT 网络上的端口 80 连接到这些计算机。

对于 NSX-T 负载均衡器或 NSX-T 版本 2.2，不支持 NAT 规则。

您可创建任意数量的 NAT 规则，且可控制这些规则的处理顺序。

NAT 规则不支持以下元素：

- 不在当前网络中的网卡
- 配置为使用 DHCP 获取 IP 地址的网卡
- 计算机群集

要将 NAT 规则添加到蓝图中的 NAT 网络组件，请参见[添加 NSX-T 按需 NAT 或 NSX-T 按需路由网络组件](#)。

添加 NSX-T 按需 NAT 或 NSX-T 按需路由网络组件

您可以在准备时将 NSX-T 按需 NAT 网络组件或 NSX-T 按需路由网络组件添加到设计画布中，以便将其设置与蓝图中的一个或多个 vSphere 计算机组件关联起来。

将现有网络组件或按需网络组件与计算机组件关联时，网卡信息随计算机组件一起存储。指定的网络配置文件信息将与网络组件一起存储。

您可以向设计画布中添加多个网络与安全组件。

一个蓝图中可包含多个按需网络组件。但是，蓝图中使用的所有按需网络配置文件必须引用相同的外部网络配置文件。

对于 NSX-T，蓝图中的不同网络所使用的网络范围不能重叠。此限制将在配置 NSX-T 第 1 层路由器网络时出现。

对于具有关联 NSX 的 vSphere 计算机组件，使用用户界面中的网络、安全和负载平衡设置。对于没有网络或安全选项卡的计算机组件，您可以在设计画面中相应的属性选项卡添加网络和安全自定义属性，例如 `VirtualMachine.Network0.Name`。NSX 网络属性、安全属性和负载平衡器属性仅适用于 vSphere 计算机。

制作蓝图时，仅显示适用于当前租户的网络配置文件。具体来说，当前租户中至少有一个预留且该预留至少将一个网络分配给配置文件时，网络配置文件可用。

前提条件

- 创建并配置 NSX for vSphere 的网络设置。请参见 [NSX-T 产品文档](#) 中的《配置 vRealize Automation》和《NSX for vSphere 管理指南》。
- 确认已针对您的集群成功运行 NSX 清单。
要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 创建按需网络配置文件。请参见 [创建网络配置文件](#)。
例如，如果要添加按需 NAT 网络组件，请参见 [为按需网络创建 NAT 网络配置文件](#)。
- 以基础架构架构师身份登录到 vRealize Automation。
- 使用设计选项卡在设计画布中打开新蓝图或现有蓝图。
- 如果要为 NAT 网络组件指定 NAT 规则，则必须使用 NAT 一对多网络配置文件。请参见 [使用提供的 IPAM 端点创建 NAT 网络配置文件](#) 或 [使用第三方 IPAM 端点创建 NAT 网络配置文件](#)。有关 NAT 规则的信息，请参见 [创建和使用 NSX for vSphere 的 NAT 规则](#)。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的网络和安全。
- 2 将 NSX-T 按需 NAT 或 NSX-T 按需路由网络组件拖动到设计画布上。
- 3 要在设计画布中唯一标记组件，请在 ID 文本框中输入组件名称。
- 4 从父网络配置文件下拉菜单中选择相应的网络配置文件。例如，如果要添加 NAT 网络组件，请选择配置为支持目标网络设置的 NAT 网络配置文件。

如果要在 NAT 网络组件中指定 NAT 规则，则必须使用为 NAT 一对多配置的父网络配置文件。

根据选择的配置文件类型，将根据网络配置文件选择填充以下网络设置。对这些值的更改必须在网络配置文件中进行的：

- 外部网络配置文件名称
- NAT 类型（NSX-T 按需 NAT）
- 子网掩码
- 范围子网掩码（NSX-T 按需路由）
- 范围子网掩码（NSX-T 按需路由）
- 基本 IP 地址（NSX-T 按需路由）

- 5 (可选) 在**描述**文本框中输入组件描述。
- 6 (可选) 单击 **DNS/WINS** 选项卡。
- 7 (可选) 为网络配置文件指定 DNS 和 WINS 设置。

- 主 DNS
- 辅助 DNS
- DNS 后缀
- 首选 WINS
- 备用 WINS

无法更改现有网络的 DNS 和 WINS 设置。

- 8 单击 **IP 范围**选项卡。

显示网络配置文件中指定的 IP 范围。您可以更改排序顺序或列显示。对于 NAT 网络，还可以更改 IP 范围值。

- a 在 **IP 范围起始**文本框中输入起始 IP 地址值。
- b 在 **IP 范围结束**文本框中输入起始 IP 地址值。

- 9 如果使用基于使用静态 IP 范围的一对多 NAT 网络配置文件的 NAT 网络，则可以使用 **NAT 规则**选项卡，添加允许外部 IP 访问内部 NAT 网络中组件的规则。

对于 NAT 一对多网络，可以定义 NAT 规则（将 NAT 网络组件添加到蓝图时可进行配置，编辑部署中的 NAT 网络时可进行更改）。

可供选择的选项取决于与 NAT 网络组件关联的 vSphere 计算机组件。

- **名称** - 输入唯一的规则名称。
- **组件** - 从关联的 vSphere 计算机或与 NAT 网络关联的负载均衡器组件的列表中进行选择。
仅非群集计算机支持 NAT 规则。如果指定的群集大小大于 1，则不会列出任何组件，因为配置不受支持。
- **源端口** - 选择 ANY 选项，输入有效端口或端口范围，或者指定有效的属性绑定。
- **目标端口** - 选择 ANY 选项，输入有效端口或端口范围，或者指定有效的属性绑定。
- **协议** - 输入 NSX-T 支持的任何有效协议，或选择 TCP、UDP 或“任意”选项。
- **描述** - 输入 NAT 规则设计的简要描述。

- 10 要将蓝图另存为草稿或继续配置蓝图，请单击**保存或完成**。

后续步骤

您可以在 vSphere 计算机组件的**网络**选项卡中添加网络设置。

使用蓝图中的 NSX for vSphere 负载均衡器组件

您可以将一个或多个按需 NSX for vSphere 负载均衡器组件添加到设计画布，为蓝图中的 vSphere 计算机组件配置设置。

添加到蓝图中的网络与安全组件设置派生自 NSX for vSphere 和 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX 清单。网络与安全组件特定于 NSX，并且只能供 vSphere 计算机组件使用。有关配置 NSX 的信息，请参见 [NSX for vSphere 产品文档](#) 或 [NSX-T 产品文档](#) 中的《管理指南》，具体取决于您使用的应用程序。

以下规则适用于蓝图中的负载均衡器池和 VIP 网络设置：

- 如果池网络配置文件为 NAT，则 VIP 网络配置文件可以是 NAT 网络配置文件的一部分。
- 如果池网络配置文件为路由网络配置文件，则 VIP 网络配置文件只能位于同一路由网络上。
- 如果池网络配置文件为外部网络配置文件，则 VIP 网络配置文件只能是同一外部网络配置文件。

每个负载均衡器组件可以有多个虚拟服务器（也称为负载均衡器服务）。负载均衡器组件中的每个虚拟服务器均有一个端口和协议。例如，可以对 HTTP 服务或 HTTPS 服务进行负载平衡。一个负载均衡器可以对多个服务进行负载平衡。

NSX Edge 是包含负载均衡器虚拟服务器的网络设备。尽管蓝图中可以有多个负载均衡器组件，但置备部署时，单个 NSX Edge 中只能包含在单个负载均衡器组件中定义的虚拟服务器。

如果蓝图包含一个或多个负载均衡器，并且为蓝图启用了应用程序隔离，则会将负载均衡器 VIP 作为 IPSet 添加到应用程序隔离安全组中。如果蓝图包含的按需安全组所关联的计算机层同时关联了负载均衡器，该按需安全组将包含计算机层，以及负载均衡器 VIP 的 IPSet。

您可以在现有部署中重新配置负载均衡器设置，添加、编辑或删除虚拟服务器。

使用升级或迁移的负载均衡器组件时的注意事项

对于目标 vRealize Automation 版本中的 NSX 负载均衡器组件，请务必了解以下注意事项并采取相应的操作。

此信息适用于升级或迁移到此 vRealize Automation 版本的 NSX for vSphere 负载均衡器组件。

- 在升级或迁移到此版本之前以及之后，必须运行 NSX 网络与安全清单数据收集，以避免在运行“重新配置负载均衡器”操作时出现问题。新部署的“重新配置负载均衡器”操作不受影响。

有关详细信息，请参见从 vRealize Automation 7.1 及更高版本升级和迁移 vRealize Automation。

- 您可以重新配置负载均衡器。所需的目录授权是“重新配置负载均衡器”。
- 对于从 vRealize Automation 7.x 升级或迁移到此 vRealize Automation 版本的部署，负载均衡器重新配置限制到包含单个负载均衡器的部署。
- 对于从 vRealize Automation 6.2.x 升级或迁移到此 vRealize Automation 版本的部署，不支持重新配置负载均衡器操作。

添加按需负载均衡器组件

您可以将 NSX 按需负载平衡器组件拖动到设计画布中并配置其设置，以便用于蓝图中的 vSphere 计算机组件和容器组件。

有关创建 NSX for vSphere 应用程序配置文件以定义特定类型的网络流量行为的相关信息，请参见 [NSX for vSphere 产品文档](#) 中的《NSX 管理指南》。

步骤

1 定义负载平衡器成员设置

您可以定义按需 NSX 负载平衡器组件，以便在网络中置备的 vSphere 成员计算机或容器计算机之间分发任务处理。

2 定义虚拟服务器常规设置

您可以为负载平衡器定义一个虚拟服务器协议和端口，也可以添加更多虚拟服务器来自定义更多 NSX 负载平衡器选项。

3 定义虚拟服务器分布设置

通过选择常规选项卡上的自定义选项，可以指定有关池成员的信息，例如，成员接收流量的端口、NSX 负载平衡器可用于访问该端口的协议类型、负载均衡使用的算法以及持久性设置。

4 定义虚拟服务器运行状况检查设置

通过选择常规选项卡上的自定义选项，可以指定 NSX 负载平衡器如何或是否对虚拟服务器内的池成员执行运行状况检查。

5 定义虚拟服务器高级设置

通过选择常规选项卡上的自定义选项，您可以自定义 NSX 负载平衡器组件，以指定单个池成员可以识别的并发连接数和虚拟服务器可以处理的最大并发连接数等设置。

6 定义负载平衡器日志记录选项

您可以定义负载平衡器日志记录操作的类型，以便将相应日志捕获并记录到负载平衡器日志。

定义负载平衡器成员设置

您可以定义按需 NSX 负载平衡器组件，以便在网络中置备的 vSphere 成员计算机或容器计算机之间分发任务处理。

在向设计画布中的蓝图添加负载平衡器组件时，可以选择默认或自定义选项来在该负载平衡器组件中创建或编辑虚拟服务器定义。使用默认选项可以指定虚拟服务器协议、端口和描述，并对所有其他设置使用默认值。使用自定义选项可以定义更多详细信息。

如果负载平衡器使用外部网络进行置备，则 VIP（VIP 网络）和成员池（成员网络）必须位于同一个现有网络上。如果 VIP 和成员池不在同一外部网络上，则置备将失败。

前提条件

- 创建并配置 NSX 的负载平衡器设置。请参见《配置 vRealize Automation》和《NSX 管理指南》。
- 确认已针对您的集群成功运行 NSX 清单。
 - 要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 创建网络配置文件。

- 以**基础架构架构师**身份登录到 vRealize Automation。
- 使用**设计**选项卡在设计画布中打开新蓝图或现有蓝图。
- 确认蓝图中至少存在一个 vSphere 计算机组件或容器组件。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的**网络和安全**。
- 2 将**按需负载均衡器**组件拖动到设计画布上。
- 3 要在设计画布中唯一标记组件，请在 **ID** 文本框中输入组件名称。
- 4 从**成员**下拉菜单中选择 vSphere 计算机组件或容器组件名称。
此列表仅包含活动蓝图中的 vSphere 计算机组件和容器组件。
- 5 选择要从**成员网络**下拉菜单中进行负载均衡的网卡。
该列表包含为选定 vSphere 计算机成员定义的网卡。
- 6 从 **VIP 网络**下拉菜单中选择可用的虚拟 IP 地址网络。例如，选择可用的外部或 NAT 网络。
虽然在蓝图中可以有多个 NSX 负载均衡器和 NSX 按需网络组件，但它们必须连接到同一 VIP 网络。
- 7 （可选）在 **IP 地址**文本框中输入网卡的有效 IP 地址。
默认设置是与 VIP 网络关联的静态 IP 地址。您可以指定其他 IP 地址或 IP 地址范围。默认情况下，会从相关联的 VIP 网络中分配下一个可用的 IP 地址。
将 IP 地址字段留空，以便允许在置备期间从关联的 VIP 网络分配 IP 地址。
如果为任何其他类型的网络指定 IP 地址，则只能置备一个部署。后续部署将无法进行 IP 分配，因为 IP 已由第一个部署使用。
- 8 要创建虚拟服务器定义，请单击**新建**，然后参见[定义虚拟服务器常规设置](#)。
每个负载均衡器组件都需要至少一个虚拟服务器。
要指定日志记录选项，请参见[定义负载均衡器日志记录选项](#)。

定义虚拟服务器常规设置

您可以为负载均衡器定义一个虚拟服务器协议和端口，也可以添加更多虚拟服务器来自定义更多 NSX 负载均衡器选项。

例如，您可以自定义负载均衡器组件，以定义运行状况检查协议和端口、算法、持久性和透明度等设置。

前提条件

[定义负载均衡器成员设置](#)。

步骤

- 1 单击**新建虚拟服务器**页面上的**常规**选项卡。
- 2 在**协议**下拉菜单中选择用于对虚拟服务器进行负载均衡的网络流量协议。
协议选项包括 HTTP、HTTPS、TCP 和 UDP。

3 在端口文本框中输入端口值。

所选协议可决定默认端口设置。

协议	默认端口
HTTP	80
HTTPS	443
TCP	8080
UDP	无默认值

HTTP、HTTPS 和 TCP 协议可以与 UDP 共享端口。例如，如果服务 1 在端口 80 上使用 TCP、HTTP 或 HTTPS，服务 2 可在端口 80 上使用 UDP。不过，如果服务 1 在端口 80 上使用 UDP，则服务 2 不能在端口 80 上使用 UDP。

4 （可选）输入虚拟服务器组件描述。

5 选择一个设置选项。

■ 对所有其他设置使用默认值

接受所有其他默认设置。单击**确定**以完成负载平衡器组件定义并继续使用蓝图。

通过单击**自定义**并检查其他选项卡选项，可以显示默认值。如果默认设置可接受，请单击**常规**选项卡上的**对所有其他设置使用默认值**。

■ 自定义

为负载平衡器组件配置其他设置，例如，为运行状况监控定义其他协议或为监控成员流量定义其他端口。

此时将显示其他选项卡，您可以在其中添加自定义设置。

选择**对所有其他设置使用默认值**并单击**确定**后，此过程即完成，您可以继续在设计画布中定义或编辑您的蓝图。如果选择**自定义**，请继续执行此步骤。

6 单击**分布**选项卡，然后进入**定义虚拟服务器分布设置**主题，以继续定义 NSX 负载平衡器组件中的虚拟服务器。

定义虚拟服务器分布设置

通过选择**常规**选项卡上的**自定义**选项，可以指定有关池成员的信息，例如，成员接收流量的端口、NSX 负载均衡器可用于访问该端口的协议类型、负载均衡使用的算法以及持久性设置。

池表示由要进行负载均衡的计算机组成的集群。池成员表示该集群中的一台计算机。

默认成员协议和成员端口设置与**常规**页面上的协议和端口设置一致。

成员计算机池显示在蓝图负载均衡器组件用户界面的**成员**选项值中。**成员**条目将设置为计算机池或集群。

前提条件

[定义虚拟服务器常规设置](#)。

步骤

- 1 （可选） **成员协议** 设置与您在 **常规** 选项卡上指定的协议一致。该设置用于定义池成员接收网络流量的方式。
- 2 （可选） 在 **成员端口** 文本框中输入端口号，以指定池成员用于接收网络流量的端口。

例如，假设负载均衡器虚拟 IP 地址 (VIP) 上的进站请求使用端口 80，您可能希望将该请求路由到池成员上的另一端口，例如端口 8080。

- 3 （可选） 为该池选择算法均衡方法。

下表介绍了算法选项以及这些选项所需的算法参数。

选项	描述及算法参数
ROUND_ROBIN	<p>根据为每个服务器分配的权重，依次使用各服务器。</p> <p>如果在 vRealize Automation 中已创建负载均衡器，则所有成员的权重相同。</p> <p>当服务器的处理时间保持均匀分布时，这是最顺畅、最公平的算法。</p> <p>为该选项停用算法参数。</p>
IP-HASH	<p>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。</p> <p>为该选项停用算法参数。</p>
LEASTCONN	<p>根据服务器上已存在的连接数将客户端请求分发到多个服务器。</p> <p>新连接会被发送到连接数最少的服务器。</p> <p>为该选项停用算法参数。</p>
URI	<p>对 URI 左侧部分（问号之前）进行哈希并除以运行的服务器的总权重。</p> <p>结果可指定接收请求的服务器。这样可以确保只要没有服务器启动或关闭，URI 将始终定向到同一服务器。</p> <p>URI 算法参数具有两个选项：uriLength=<len> 和 uriDepth=<dep>。在 算法参数 文本框中的不同行上输入长度和深度参数。</p> <p>长度和深度参数后跟一个正整数。这些选项可以仅根据 URI 开头均衡服务器。</p> <p>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。长度参数范围应该为 1<=len<256。</p> <p>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。深度参数范围应该为 1<=dep<10。</p> <p>如果指定了两个参数，在到达任一参数时，计算将停止。</p>
HTTPHEADER	<p>在每个 HTTP 请求中查找 HTTP 标头名称。</p> <p>圆括号中的标头名称不区分大小写，这类似于 ACL 函数“hdr()”。</p> <p>HTTPHEADER 算法参数具有一个选项：headerName=<name>。例如，可以将 host 作为 HTTPHEADER 算法参数。</p> <p>如果标头不存在或不包含任何值，将应用循环算法。</p>
URL	<p>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。</p> <p>URL 算法参数具有一个选项：urlParam=<url>。</p> <p>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。</p> <p>结果可指定接收请求的服务器。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。</p> <p>如果找不到任何值或参数，则应用循环算法。</p>

4 （可选）为该池选择持久性方法。

持久性可跟踪和存储会话数据，例如处理客户端请求的特定池成员。通过持久性，可以在整个会话期间或后续会话期间将客户端请求定向到同一池成员。

协议	支持的持久性方法
HTTP	无、Cookie、源 IP
HTTPS	“无”、“源 IP”和“SSL 会话 ID”
TCP	无、源 IP、MSRDP
UDP	无、源 IP

- 选择 **Cookie** 可在客户端首次访问站点时插入一个唯一 Cookie 以标识会话。系统将在后续请求中引用该 Cookie，以永久保留与相应服务器的连接。
- 选择**源 IP** 可根据源 IP 地址跟踪会话。当客户端请求连接到支持源地址关联性持久性的虚拟服务器时，负载均衡器将检查该客户端之前是否曾建立连接；如果是，则将客户端返回给同一个池成员。
- 选择 **SSL 会话 ID**，并选择“SSL 直通” HTTPS 流量模式。
 - SSL 直通 -> 客户端 -> HTTPS -> LB (SSL 直通) -> HTTPS -> 服务器
 - 客户端 - HTTP-> LB -> HTTP -> 服务器

注 vRealize Automation 当前仅支持“SSL 直通”。无论您选择哪个选项，都会使用“SSL 直通”方法。

- 选择 **MSRDP** 可在 Windows 客户端和运行 Microsoft 远程桌面协议 (RDP) 服务的服务器之间保持持久会话。启用 MSRDP 持久性的推荐场景是，创建一个负载均衡池，该池由运行受支持 Windows Server 的成员组成，其中所有成员均属于一个 Windows 集群并加入 Windows 会话目录。
- 选择**无**，不会存储会话操作供后续重新调用。

5 如果使用 Cookie 持久性设置，请输入 Cookie 名称。

6 （可选）从**模式**下拉菜单中选择插入 Cookie 的模式。

选项	描述
插入	NSX Edge 发送一个 Cookie。 如果服务器发送一个或多个 Cookie，客户端将收到一个额外的 Cookie（服务器 Cookie + NSX Edge Cookie）。如果服务器不发送 Cookie，客户端将收到 NSX Edge Cookie。
前缀	服务器发送一个 Cookie。如果客户端不支持多个 Cookie，则使用该选项。 如果某个专有应用程序使用一个专有客户端，而该客户端仅支持一个 Cookie，则 Web 服务器将发送一个 Cookie，而 NSX Edge 会将其 Cookie 信息（作为前缀）插入服务器 Cookie 值中
应用程序会话	服务器不发送 Cookie，而是将用户会话信息作为 URL 发送。 例如，http://mysite.com/admin/UpdateUserServlet;jsessionid=X000X0XXX0XXXX，其中 jsessionid 是用户会话信息并用于持久性。

7 （可选）输入 Cookie 的持久性过期时间（秒）。

例如，对于使用 TCP 源 IP 的 L7 负载均衡，如果在指定的过期时间内没有建立新的 TCP 连接，则即使现有连接仍然有效，持久性条目也将超时。

8 （可选）单击**运行状况检查**选项卡，然后进入**定义虚拟服务器运行状况检查设置**主题，以继续定义 NSX 负载均衡器组件中的虚拟服务器。

定义虚拟服务器运行状况检查设置

通过选择**常规**选项卡上的**自定义**选项，可以指定 NSX 负载均衡器如何或是否对虚拟服务器内的池成员执行运行状况检查。

默认运行状况检查协议和运行状况检查端口设置与**常规**选项卡上的协议和端口设置一致。

有关相关信息，请参见 NSX 产品文档中的创建服务监视器，网址为：https://www.vmware.com/support/pubs/nsx_pubs.html。请注意，在 NSX 文档中，虚拟服务器成员被称为池成员。

前提条件

[定义虚拟服务器常规设置](#)。

步骤

1 （可选）在**运行状况检查协议**下拉菜单中选择运行状况检查协议，以指定负载均衡器为确定池成员的运行状况而进行侦听时访问此池成员的方式。

协议选项包括 **HTTP**、**HTTPS**、**TCP**、**ICMP**、**UDP** 和**无**。

您也可以接受“常规”选项卡上指定的默认协议。

2 （可选）在**运行状况检查端口**框中输入值，指定负载均衡器将侦听哪个端口来监控虚拟服务器成员或池成员的运行状况。

请注意，在 NSX 文档中，虚拟服务器成员被称为池成员。

HTTP、HTTPS 和 TCP 协议可以与 UDP 共享端口。例如，如果服务 1 在端口 80 上使用 TCP、HTTP 或 HTTPS，服务 2 可在端口 80 上使用 UDP。不过，如果服务 1 在端口 80 上使用 UDP，则服务 2 不能在端口 80 上使用 UDP。

- 3 输入对服务器执行 ping 命令的**时间间隔值**（秒）。
- 4 输入必须从服务器接收到响应的时间段的最大**超时值**（秒）。
- 5 输入声明服务器出现故障之前必须对服务器执行 ping 命令的**最大重试次数值**。
- 6 根据选定的**运行状况检查协议**，指定其他运行状况检查设置。
 - a 输入用来检测服务器状态的**方法**。选项包括 GET、OPTIONS 和 POST。
 - b 输入在检测服务器状态请求中使用的 **URL**。这是 GET 和 POST（默认为“/”）方法选项使用的 URL。
 - c 在**发送**文本框中，输入建立连接之后发送到服务器的字符串。
在**发送**文本框中，输入建立连接之后发送到服务器的字符串。
 - d 在**接收**文本框中，输入要从服务器接收的字符串。
只有在收到的字符串与该定义匹配时，才会将服务器视为正在运行。
此字符串可以是响应的标头或正文。
- 7 单击**高级**选项卡，然后进入**定义虚拟服务器高级设置**主题，以继续定义 NSX 负载均衡器组件中的虚拟服务器。

要指定日志记录选项，请参见**定义负载均衡器日志记录选项**。

定义虚拟服务器高级设置

通过选择**常规**选项卡上的**自定义**选项，您可以自定义 NSX 负载均衡器组件，以指定单个池成员可以识别的并发连接数和虚拟服务器可以处理的最大并发连接数等设置。

前提条件

[定义虚拟服务器常规设置](#)。

步骤

- 1 在**连接限制**文本框中输入一个值，以指定 NSX 中可由虚拟服务器处理的最大并发连接数。
此设置会计入所有成员连接数。
输入值 0 表示不指定限制。
- 2 在**连接速率限制**文本框中输入一个值，以指定 NSX 中每秒可接受的最大入站请求数。
此设置会计入所有成员连接数。
输入值 0 表示不指定限制。
- 3 （可选）选中**启用加速**复选框，以指定每个虚拟 IP (VIP) 均使用速度较快的 L4 负载均衡器，而不是 L7 负载均衡器。

- 4 （可选）选中**透明**复选框，以允许负载均衡器池成员查看正在调用负载均衡器的计算机的 IP 地址。
如果未选中，则负载均衡器池成员会将流量源 IP 地址视为负载均衡器内部 IP 地址。
- 5 在**最大连接数**文本框中输入一个值，以指定单个池成员可以识别的最大并发连接数。
如果入站请求数高于此值，则这些请求将排队，并在释放连接时按照接收这些请求的顺序进行处理。
输入值 0 表示不指定最大值。
- 6 在**最小连接数**文本框中输入一个值，以指定单个池成员必须始终接受的最小并发连接数。
输入值 0 表示不指定最小值。
- 7 单击**确定**以完成虚拟服务器定义。
- 8 要指定日志记录选项，请参见[定义负载均衡器日志记录选项](#)，否则单击**保存或完成**。

定义负载均衡器日志记录选项

您可以定义负载均衡器日志记录操作的类型，以便将相应日志捕获并记录到负载均衡器日志。

定义负载均衡器组件后，或在定义负载均衡器组件期间，您可以指定收集负载均衡器流量日志时使用的日志记录级别。在蓝图上为任何负载均衡器组件定义的日志记录级别会应用于该蓝图中定义的所有负载均衡器。

日志记录级别包括调试、信息、警告、错误和严重。调试和信息选项会记录用户请求，而警告、错误和严重选项不会记录用户请求。

有关 NSX 负载均衡器日志记录的其他信息，请参见《NSX 管理指南》。

前提条件

[定义负载均衡器成员设置](#)。

步骤

- 1 在设计画布中的负载均衡器组件上选择**全局**选项卡。
- 2 从**日志记录级别**下拉菜单中选择一个或多个日志记录选项。

选择用于收集负载均衡器流量日志的日志记录级别。该设置适用于蓝图中的所有 NSX 负载均衡器组件。

日志记录设置在 vSphere Web Client 中定义。

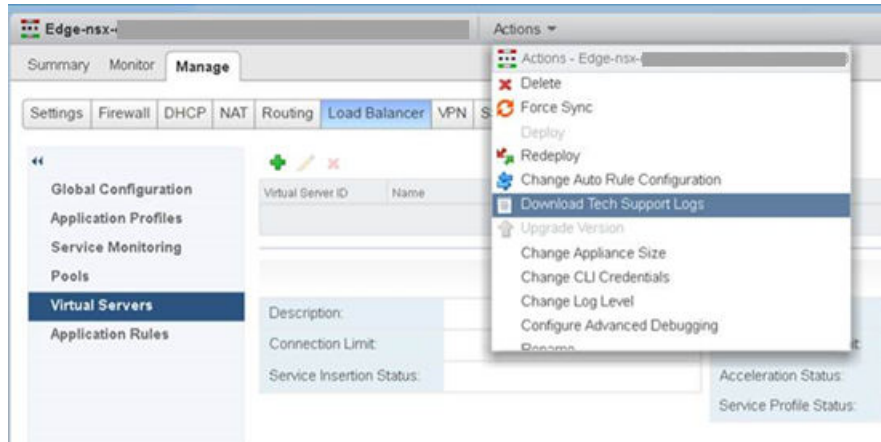
- 无
- 信息
- 紧急
- 警示
- 严重
- 错误
- 警告

- 通知
- 调试

3 单击保存。

结果

通过使用 NSX Edge 的**操作**菜单，可以查看和下载 vSphere Web Client 中的日志，如 NSX 产品文档中的“下载 NSX Edge 的技术支持日志”所述，网址为：https://www.vmware.com/support/pubs/nsx_pubs.html。



使用蓝图中的 NSX-T 负载均衡器组件

您可以将一个或多个按需 NSX-T 负载均衡器组件添加到设计画布，为蓝图中的 vSphere 计算机组件配置设置。

添加到蓝图中的网络与安全组件设置派生自 NSX for vSphere 和 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX 清单。网络与安全组件特定于 NSX，并且只能供 vSphere 计算机组件使用。有关配置 NSX 的信息，请参见 [NSX for vSphere 产品文档](#) 或 [NSX-T 产品文档](#) 中的《管理指南》，具体取决于您使用的应用程序。

添加到蓝图中的网络与安全组件设置派生自 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX-T 清单。网络与安全组件特定于 NSX-T，并且只能供 vSphere 计算机组件使用。有关配置 NSX-T 的信息，请参见 [NSX-T 产品文档](#) 中的《NSX-T 管理指南》。

以下规则适用于蓝图中的负载均衡器池和 VIP 网络设置：

- 如果池网络配置文件为 NAT，则 VIP 网络配置文件可以是 NAT 网络配置文件的一部分。
- 如果池网络配置文件为路由网络配置文件，则 VIP 网络配置文件只能位于同一路由网络或同一外部网络上。
- 如果池网络配置文件为外部网络配置文件，则 VIP 网络配置文件只能是同一外部网络配置文件。

每个负载均衡器组件可以有多个虚拟服务器（也称为负载均衡器服务）。负载均衡器组件中的每个虚拟服务器均有一个端口和协议。例如，可以对 HTTP 服务或 HTTPS 服务进行负载平衡。一个负载均衡器可以对多个服务进行负载平衡。

NSX 负载均衡器是包含负载均衡器虚拟服务器的服务。

如果蓝图包含一个或多个负载均衡器，并且为蓝图启用了应用程序隔离，则会将负载均衡器 VIP 作为 IPSet 添加到应用程序隔离安全组中。如果蓝图包含的按需安全组所关联的计算机层同时关联了负载均衡器，该按需安全组将包含计算机层，以及负载均衡器 VIP 的 IPSet。

有关 NSX-T -特定部署和拓扑注意事项的详细信息，请参见[了解网络连接、安全性和负载均衡器配置的 NSX-T 部署拓扑](#)。

添加 NSX-T 按需负载均衡器

您可以将 NSX-T 按需负载均衡器组件拖动到设计画布中并配置其设置，以便用于蓝图中的 vSphere 计算机组件和容器组件。

NSX-T 负载均衡器将入站服务请求均匀分布在多个服务器中，以确保负载分配对用户透明。负载均衡有助于实现最佳的资源利用，最大程度地提高吞吐量和减少响应时间，并避免过载。

您可以将虚拟 IP 地址映射到一组池服务器以实现负载均衡。负载均衡器可接受虚拟 IP 地址上的 TCP、UDP、HTTP 或 HTTPS 请求，并确定要使用的池成员。负载均衡器连接到第 1 层逻辑路由器。

根据您的环境需求，您可以通过增加现有虚拟服务器和池成员来扩展负载均衡器性能，从而处理繁重的网络流量负载。

有关创建 NSX-T 负载均衡器以定义网络流量行为的信息，请参见 [NSX-T 产品文档](#) 中《NSX-T 管理指南》中的逻辑负载均衡器和配置负载均衡器组件。

步骤

1 定义 NSX-T 负载均衡器成员设置

您可以定义 NSX-T 按需负载均衡器组件，以便在网络中置备的 vSphere 成员计算机或容器计算机之间分发任务处理。

2 为 NSX-T 定义虚拟服务器常规设置

您可以为负载均衡器定义一个虚拟服务器协议和端口，也可以添加更多虚拟服务器来自定义更多 NSX-T 负载均衡器选项。

3 为 NSX-T 定义虚拟服务器分布设置

定义虚拟服务器时，通过选择**自定义选项**，可以指定池成员信息，例如，成员接收流量的端口、NSX-T 负载均衡器可用于访问该端口的协议类型、负载均衡使用的算法以及持久性设置。

4 为 NSX-T 定义虚拟服务器运行状况检查设置

通过选择**常规**选项卡上的**自定义**选项，可以指定 NSX-T 负载均衡器如何或是否对虚拟服务器内的池成员执行运行状况检查。

5 为 NSX-T 定义虚拟服务器高级设置

通过选择**常规**选项卡上的**自定义**选项，您可以自定义 NSX-T 负载均衡器组件，以指定单个池成员可以识别的并发连接数和虚拟服务器可以处理的最大并发连接数等设置。

6 定义 NSX-T 负载均衡器日志记录选项

您可以定义负载均衡器日志记录操作的类型，以便将相应日志捕获并记录到负载均衡器日志。

定义 NSX-T 负载均衡器成员设置

您可以定义 **NSX-T** 按需负载平衡器组件，以便在网络中置备的 **vSphere** 成员计算机或容器计算机之间分发任务处理。

在向设计画布中的蓝图添加负载平衡器组件时，可以选择默认或自定义选项来在该负载平衡器组件中创建或编辑虚拟服务器定义。使用默认选项可以指定虚拟服务器协议、端口和描述，并对所有其他设置使用默认值。使用自定义选项可以定义更多详细信息。

如果负载均衡器使用外部网络进行置备，则 **VIP**（**VIP 网络**）和成员池（成员网络）必须位于同一个现有网络上。如果 **VIP** 和成员池不在同一外部网络上，则置备将失败。

前提条件

- 创建并配置 **NSX** 的负载平衡器设置。请参见[准备 NSX 网络与安全配置的对照表](#)。
- 确认已针对您的集群成功运行 **NSX** 清单。
要在 **vRealize Automation** 中使用 **NSX** 配置，必须运行数据收集。
- 创建网络配置文件。请参见[创建网络配置文件](#)。
- 以**基础架构架构师**身份登录到 **vRealize Automation**。
- 使用**设计**选项卡在设计画布中打开新蓝图或现有蓝图。
- 确认蓝图中至少存在一个 **vSphere** 计算机组件或容器组件。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的**网络和安全**。
- 2 将 **NSX-T 按需负载平衡器**组件拖动到设计画布上。
- 3 要在设计画布中唯一标记组件，请在 **ID** 文本框中输入组件名称。
- 4 从**成员**下拉菜单中选择 **vSphere** 计算机组件或容器组件名称。
此列表仅包含活动蓝图中的 **vSphere** 计算机组件和容器组件。
- 5 选择要从**成员网络**下拉菜单中进行负载均衡的网卡。
该列表包含为选定 **vSphere** 计算机成员定义的网卡。
- 6 从 **VIP 网络**下拉菜单中选择可用的虚拟 IP 地址网络。例如，选择可用的外部或 **NAT** 网络。
虽然在蓝图中可以有多个 **NSX** 负载均衡器和 **NSX** 按需网络组件，但它们必须连接到同一 **VIP** 网络。
- 7 （可选）在 **IP 地址**文本框中输入网卡的有效 IP 地址。
默认设置是与 **VIP** 网络关联的静态 IP 地址。您可以指定其他 IP 地址或 IP 地址范围。默认情况下，会从相关联的 **VIP** 网络中分配下一个可用的 IP 地址。
将 IP 地址字段留空，以便允许在置备期间从关联的 **VIP** 网络分配 IP 地址。
如果为任何其他类型的网络指定 IP 地址，则只能置备一个部署。后续部署将无法进行 IP 分配，因为 IP 已由第一个部署使用。
- 8 要创建虚拟服务器定义，请单击**新建**，然后参见[为 NSX-T 定义虚拟服务器常规设置](#)。
每个负载平衡器组件都需要至少一个虚拟服务器。

要指定日志记录选项，请参见[定义 NSX-T 负载均衡器日志记录选项](#)。

为 NSX-T 定义虚拟服务器常规设置

您可以为负载均衡器定义一个虚拟服务器协议和端口，也可以添加更多虚拟服务器来自定义更多 NSX-T 负载均衡器选项。

例如，您可以自定义负载均衡器组件，以定义运行状况检查协议和端口、算法、持久性和透明度等设置。

前提条件

[定义 NSX-T 负载均衡器成员设置](#)。

步骤

- 1 单击**虚拟服务器**页面上的**常规**选项卡。
- 2 在**协议**下拉菜单中选择用于对虚拟服务器进行负载均衡的网络流量协议。

协议选项包括 HTTP、HTTPS、TCP 和 UDP。

NSX-T 负载均衡不支持 SSL 直通模式，而是使用 SSL 终止模式。如果指定 HTTPS，您将需要提供以下其他信息，这些信息必须已存在于 NSX-T manager 中：

- NSX-T 证书清单中的证书名称。负载均衡器会将此证书提供给客户端。
- 客户端 SSL 配置文件名称。

- 3 在**端口**文本框中输入端口值。

所选协议可决定默认端口设置。

协议	默认端口
HTTP	80
HTTPS	443
TCP	8080
UDP	无默认值

HTTP、HTTPS 和 TCP 协议可以与 UDP 共享端口。例如，如果服务 1 在端口 80 上使用 TCP、HTTP 或 HTTPS，服务 2 可在端口 80 上使用 UDP。不过，如果服务 1 在端口 80 上使用 UDP，则服务 2 不能在端口 80 上使用 UDP。

- 4 （可选）输入虚拟服务器组件描述。
- 5 单击**分布**选项卡，然后进入[为 NSX-T 定义虚拟服务器分布设置](#)主题，以继续定义 NSX-T 负载均衡器组件中的虚拟服务器。

为 NSX-T 定义虚拟服务器分布设置

定义虚拟服务器时，通过选择**自定义选项**，可以指定池成员信息，例如，成员接收流量的端口、NSX-T 负载均衡器可用于访问该端口的协议类型、负载均衡使用的算法以及持久性设置。

池表示由要进行负载均衡的计算机组成的群集。池成员表示该群集中的一台计算机。

默认成员协议和成员端口设置与**常规**页面上的协议和端口设置一致。

成员计算机池显示在蓝图负载平衡器组件用户界面的**成员**选项值中。**成员**条目将设置为计算机池或群集。

前提条件

定义 [NSX-T 负载平衡器成员设置](#)。

步骤

- 1 （可选） **成员协议** 设置与您在**常规**选项卡上指定的协议一致。该设置用于定义池成员接收网络流量的方式。
- 2 （可选） 在**成员端口**文本框中输入端口号，以指定池成员用于接收网络流量的端口。

例如，假设负载平衡器虚拟 IP 地址 (VIP) 上的进站请求使用端口 80，您可能希望将该请求路由到池成员上的另一端口，例如端口 8080。

- 3 （可选） 为该池选择算法平衡方法。

下表介绍了算法选项以及这些选项所需的算法参数。

相关信息请参见 [NSX-T 产品文档](#)中的添加用于负载平衡的服务器池。

选项	描述及算法参数
ROUND_ROBIN	进站客户端请求通过能够处理请求的可用服务器列表进行循环。即使已配置服务器池成员权重，也会忽略它们。
加权循环	每个服务器分配有一个权重值，该值表示该服务器相对于池中其他服务器的执行情况。该值可确定与池中其他服务器相比向服务器发送的客户端请求数。此负载平衡算法侧重于在可用服务器资源之间公平分配负载。
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。
LEASTCONN	根据服务器上已有的连接数量将客户端请求分发给多个服务器。将新连接发送给连接最少的服务器。即使已配置服务器池成员权重，也会忽略它们。
加权最小连接数目	每个服务器分配有一个权重值，该值表示该服务器相对于池中其他服务器的执行情况。该值可确定与池中其他服务器相比向服务器发送的客户端请求数。此负载平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，如果未配置该值并且启用了慢启动，则权重值为 1。

- 4 （可选） 为该池选择持久性方法。

持久性可跟踪和存储会话数据，例如处理客户端请求的特定池成员。通过持久性，可以在整个会话期间或后续会话期间将客户端请求定向到同一池成员。有关持久性方法的详细信息，请参见 [NSX-T 产品文档](#)中的配置持久性配置文件。

- 选择**无**，不会存储会话操作供后续重新调用。
- 选择**Cookie** 可在客户端首次访问站点时插入一个唯一 Cookie 以标识会话。系统将在后续请求中引用该 Cookie，以永久保留与相应服务器的连接。
- 选择**源 IP** 可根据源 IP 地址跟踪会话。当客户端请求连接到支持源地址关联性持久性的虚拟服务器时，负载平衡器将检查该客户端之前是否曾建立连接；如果是，则将客户端返回给同一个池成员。

- 5 如果使用 Cookie 持久性，请输入 Cookie 名称。

- 6 （可选）从**模式**下拉菜单中选择插入 Cookie 的模式。

选项	描述
插入	创建唯一的 cookie 来标识该会话。
前缀	添加到现有 cookie。
重写	覆盖现有 cookie。

- 7 （可选）输入 Cookie 的持久性过期时间（秒）。

例如，对于使用 TCP 源 IP 的 L7 负载平衡，如果在指定的过期时间内没有建立新的 TCP 连接，则即使现有连接仍然有效，持久性条目也将超时。

- 8 （可选）单击**运行状况检查**选项卡，然后进入为 [NSX-T 定义虚拟服务器运行状况检查设置](#) 主题，以继续定义 NSX-T 负载平衡器组件中的虚拟服务器。

为 NSX-T 定义虚拟服务器运行状况检查设置

通过选择**常规**选项卡上的**自定义**选项，可以指定 NSX-T 负载平衡器如何或是否对虚拟服务器内的池成员执行运行状况检查。

默认运行状况检查协议和运行状况检查端口设置与**常规**选项卡上的协议和端口设置一致。

有关相关信息，请参见 [NSX-T 产品文档](#)。请注意，在 NSX-T 文档中，虚拟服务器成员被称为池成员。

前提条件

为 [NSX-T 定义虚拟服务器分布设置](#)。

步骤

- 1 （可选）在**运行状况检查协议**下拉菜单中选择运行状况检查协议，以指定负载平衡器为确定池成员的运行状况而进行侦听时访问此池成员的方式。

协议选项包括**无**、**HTTP**、**HTTPS**、**TCP**、**ICMP** 和 **UDP**。

您也可以接受“常规”选项卡上指定的默认协议。

- 2 （可选）在**运行状况检查端口**框中输入值，指定负载平衡器将侦听哪个端口来监控虚拟服务器成员或池成员的运行状况。

请注意，在 NSX 文档中，虚拟服务器成员被称为池成员。

HTTP、HTTPS 和 TCP 协议可以与 UDP 共享端口。例如，如果服务 1 在端口 80 上使用 TCP、HTTP 或 HTTPS，服务 2 可在端口 80 上使用 UDP。不过，如果服务 1 在端口 80 上使用 UDP，则服务 2 不能在端口 80 上使用 UDP。

- 3 输入对服务器执行 ping 命令的**时间间隔值**（秒）。
- 4 输入必须从服务器接收到响应的时间段的**最大超时值**（秒）。
- 5 输入声明服务器出现故障之前必须对服务器执行 ping 命令的**最大重试次数值**。
- 6 如果已指定 HTTP 或 HTTPS 协议，输入要用于检测服务器状态的方法。

- 7 如果可能，请输入用于服务器状态检测请求的 **URL**。这是 GET 和 POST（默认为“/”）方法选项使用的 URL。
- 8 如果可能，请在**发送**和**接收**文本框中输入发送和接收的字符串。
 在**发送**文本框中，输入建立连接之后发送到服务器的字符串。
 在**接收**文本框中，输入要从服务器接收的字符串。只有在收到的字符串与该定义匹配时，才会将服务器视为正在运行。
- 9 单击**高级**选项卡，然后进入**为 NSX-T 定义虚拟服务器高级设置**主题，以继续定义 NSX-T 负载均衡器组件中的虚拟服务器。
 要指定日志记录选项，请参见**定义 NSX-T 负载均衡器日志记录选项**。

为 NSX-T 定义虚拟服务器高级设置

通过选择**常规**选项卡上的**自定义**选项，您可以自定义 NSX-T 负载均衡器组件，以指定单个池成员可以识别的并发连接数和虚拟服务器可以处理的最大并发连接数等设置。

前提条件

为 **NSX-T 定义虚拟服务器常规设置**。

步骤

- 1 在**连接限制**文本框中输入一个值，以指定 NSX-T 中可由虚拟服务器处理的最大并发连接数。
 此设置会计入所有成员连接数。
 输入值 0 表示不指定限制。
- 2 在**连接速率限制**文本框中输入一个值，以指定 NSX-T 中每秒可接受的最大入站请求数。
 此设置会计入所有成员连接数。
 输入值 0 表示不指定限制。
- 3 （可选）选中**透明**复选框，以允许负载均衡器池成员查看正在调用负载均衡器的计算机的 IP 地址。
 如果未选中，则负载均衡器池成员会将流量源 IP 地址视为负载均衡器内部 IP 地址。
- 4 在**最大连接数**文本框中输入一个值，以指定单个池成员可以识别的最大并发连接数。
 如果入站请求数高于此值，则这些请求将排队，并在释放连接时按照接收这些请求的顺序进行处理。
 输入值 0 表示不指定最大值。
- 5 单击**确定**以完成虚拟服务器定义。
- 6 要指定日志记录选项，请参见**定义 NSX-T 负载均衡器日志记录选项**，否则单击**保存或完成**。

定义 NSX-T 负载均衡器日志记录选项

您可以定义负载均衡器日志记录操作的类型，以便将相应日志捕获并记录到负载均衡器日志。

可以指定用于收集负载均衡器流量日志的日志记录级别。在蓝图上为任何 NSX-T 负载均衡器组件定义的日志记录级别会应用于该蓝图中的所有负载均衡器。

日志记录级别包括调试、信息、警告、错误和严重。调试和信息选项会记录用户请求，而警告、错误和严重选项不会记录用户请求。

有关 NSX-T 负载均衡器日志记录的其他信息，请参见 [NSX-T 产品文档](#) 中的《NSX-T 管理指南》。

前提条件

定义 NSX-T 负载均衡器成员设置

步骤

- 1 在设计画布中的负载均衡器组件上选择**全局**选项卡。
- 2 从**日志记录级别**下拉菜单中选择一个或多个日志记录选项。

日志记录设置在 vSphere Web Client 中定义。

- 无
- 紧急
- 警示
- 严重
- 错误
- 警告
- 信息
- 调试

- 3 选择小、中或大负载均衡器。
- 4 单击**保存**，然后单击**完成**。

使用蓝图中的 NSX for vSphere 安全组件

您可以将 NSX for vSphere 安全组件添加到设计画布，使其已配置的设置可用于蓝图中的一个或多个 vSphere 计算机组件。

在 NSX 应用程序中，安全组、标记和策略在 vRealize Automation 外部配置。

添加到蓝图中的网络与安全组件设置派生自 NSX for vSphere 和 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX 清单。网络与安全组件特定于 NSX，并且只能供 vSphere 计算机组件使用。有关配置 NSX 的信息，请参见 [NSX for vSphere 产品文档](#) 或 [NSX-T 产品文档](#) 中的《管理指南》，具体取决于您使用的应用程序。

通过在 NSX 中为 vSphere 计算资源配置安全组、标记和策略，您可以向蓝图添加安全控件。运行数据收集之后，即可在 vRealize Automation 中选择安全配置。

有关示例 NSX for vSphere 安全策略，请参见此 [vRealize](#) 和 [NSX](#) 博客文章。

NSX for vSphere 的现有安全组和按需安全组

安全组是 vSphere 清单中映射到一组安全策略的一系列资产或分组对象，例如，Distributed Firewall 规则以及防病毒和入侵检测等第三方安全服务集成。使用分组功能，您可以创建可分配虚拟机和网络适配器等资源的自定义容器，使之受 Distributed Firewall 保护。定义组后，可以将该组作为源或目标添加到防火墙规则，使之受到保护。

除了在预留中指定的安全组外，您还可以在蓝图中添加 vSphere 现有或按需安全组。

可以创建一个或多个按需安全组。可以选择要为安全组配置的一个或多个安全策略。

安全策略是可以应用于安全组的一组端点、防火墙和网络自检服务。通过使用蓝图中的按需安全组，您可以将安全策略添加到 vSphere 虚拟机。但是，您不能将安全策略直接添加到预留。数据收集完成后，即可在蓝图中选择在 NSX for vSphere 中为计算资源定义的安全策略。

安全组在源资源中进行管理。有关为各种资源类型管理安全组的信息，请参见 NSX for vSphere 文档。

注 启用“应用程序隔离”后，将创建单独的安全策略。应用程序隔离使用逻辑防火墙阻止所有入站和出站流量流向蓝图中的应用程序。通过包含应用程序隔离策略的蓝图置备的组件计算机可以相互通信，但无法连接到防火墙外部，除非向蓝图中添加其他安全组，并配置相应的安全策略以允许访问。

如果蓝图包含一个或多个负载均衡器，并且为蓝图启用了应用程序隔离，则会将负载均衡器 VIP 作为 IPSet 添加到应用程序隔离安全组中。如果蓝图包含的按需安全组所关联的计算机层同时关联了负载均衡器，该按需安全组将包含计算机层，以及负载均衡器 VIP 的 IPSet。

NSX for vSphere 的现有安全标记

可以添加 NSX for vSphere 的现有安全标记组件。安全标记是可用作分组机制的限定符对象或分类条目。您可定义对象添加到所创建的安全组时必须满足的条件。这样，您可以通过定义支持大量参数的筛选标准，将与搜索条件匹配的计算机包括在内。例如，您可以将所有具有指定安全标记的计算机添加到安全组。

为 NSX for vSphere 添加现有安全组组件

您可以在准备时将现有 NSX for vSphere 安全组组件添加到设计画布中，以便将其设置与蓝图中的一个或多个 vSphere 计算机组件关联起来。

您可以使用现有安全组组件将 NSX 安全组添加到设计画布，并将其设置配置为与 vSphere 计算机组件和涉及 vSphere 的 Software 或 XaaS 组件一起使用。

默认情况下，制作蓝图时，显示适用于当前租户的安全组。具体来说，关联端点在当前租户中有预留时，安全组可用。有关控制租户访问的其他信息，请参见在 [vRealize Automation 中控制安全对象的租户访问](#)。

前提条件

- 创建并配置 NSX 的安全组。请参见《配置 vRealize Automation》中的 NSX 配置检查表以及 [NSX for vSphere 产品文档](#) 中的 NSX for vSphere 管理指南》。
- 确认已针对您的集群成功运行 NSX 清单。
要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 查看安全组件概念。请参见 [使用蓝图中的 NSX for vSphere 安全组件](#)。
- 以 **基础架构架构师** 身份登录到 vRealize Automation。

- 使用**设计**选项卡在设计画布中打开新蓝图或现有蓝图。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的**网络和安全**。
- 2 将**现有安全组**组件拖动到设计画布上。
- 3 从**安全组**下拉菜单中选择现有安全组。
- 4 单击**确定**。
- 5 要将蓝图另存为草稿或继续配置蓝图，请单击**保存或完成**。

结果

您可以在 vSphere 计算机组件的**安全**选项卡中添加安全设置。

为 NSX for vSphere 添加现有安全标记组件

您可以在准备时将现有 **NSX for vSphere** 安全标记组件添加到蓝图设计画布中，以便将其设置与蓝图中的一个或多个 vSphere 组件关联起来。

您可以使用安全标记组件将现有 vSphere 安全标记添加到设计画布，并将其设置配置为与 vSphere 计算机组件和涉及 vSphere 的 **Software** 组件一起使用。

默认情况下，制作蓝图时，显示适用于当前租户的安全标记。具体来说，关联端点在当前租户中有预留时，安全标记可用。有关控制租户访问的其他信息，请参见在 [vRealize Automation 中控制安全对象的租户访问](#)。

您可以向设计画布中添加多个网络与安全组件。

有关详细信息，请参见[使用蓝图中的 NSX for vSphere 安全组件](#)。

前提条件

- 创建并配置 NSX 的安全标记。请参见《配置 vRealize Automation》中的 NSX 配置检查表以及 [NSX for vSphere 产品文档](#)中的《NSX for vSphere 管理指南》。
- 确认已针对您的集群成功运行 NSX 清单。
要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 以**基础架构架构师**身份登录到 vRealize Automation。
- 使用**设计**选项卡在设计画布中打开新蓝图或现有蓝图。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的**网络和安全**。
- 2 将**现有安全标记**组件拖动到设计画布上。
- 3 单击**安全标记**文本框并选择现有安全标记。
- 4 单击**确定**。
- 5 要将蓝图另存为草稿或继续配置蓝图，请单击**保存或完成**。

结果

您可以在 vSphere 计算机组件的**安全**选项卡中添加安全设置。

添加按需安全组组件

您可以在准备时将按需 NSX 安全组组件添加到设计画布中，以便将其设置与蓝图中的一个或多个 vSphere 计算机组件或者其他可用组件类型关联起来。

创建按需安全组时，会添加安全策略以创建该组。默认情况下，可以全局显示或隐藏安全策略。仅当关联的 NSX 端点在租户中具有预留时，才会在该租户中显示策略。

默认情况下，制作蓝图时，显示适用于当前租户的安全组。具体来说，关联端点在当前租户中有预留时，安全组可用。有关控制租户访问的其他信息，请参见在 [vRealize Automation 中控制安全对象的租户访问](#)。

前提条件

- 在 NSX 中创建和配置安全策略。请参见 [NSX 管理指南](#)。
- 确认已针对您的集群成功运行 NSX 清单。
要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 以[基础架构架构师](#)身份登录到 vRealize Automation。
- 查看安全组件概念。请参见[使用蓝图中的 NSX for vSphere 安全组件](#)。
- 使用[设计](#)选项卡在设计画布中打开新蓝图或现有蓝图。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的**网络和安全**。
- 2 将**按需安全组**组件拖动到设计画布上。
- 3 输入名称和可选描述。
- 4 通过单击**安全策略**区域中的**添加**图标并选择可用的安全策略，添加一个或多个安全策略。
- 5 单击**确定**。
- 6 要将蓝图另存为草稿或继续配置蓝图，请单击**保存或完成**。

结果

您可以在 vSphere 计算机组件的**安全**选项卡中添加安全设置。

使用蓝图中的 NSX-T 安全组件

您可以将 NSX-T 网络安全组件添加到设计画布，使其已配置的设置可用于蓝图中的一个或多个关联的 vSphere 计算机组件。

使用 NSX-T 现有 NS 组，您可以分配虚拟机和网络适配器等资源，使之受分布式防火墙保护。

通过在 NSX-T 中为 vSphere 计算资源配置 NS 组，您可以向蓝图添加安全控件。运行数据收集之后，即可在 vRealize Automation 中选择安全配置。可以将 NSX-T 现有 NS 组组件作为防火墙规则的源或目标添加到蓝图。

在 NSX-T 应用程序的 vRealize Automation 外部管理 NSX-T NS 安全组。有关管理 NS 组的信息，请参见 NSX-T 产品文档。

添加到蓝图中的网络与安全组件设置派生自 NSX for vSphere 和 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX 清单。网络与安全组件特定于 NSX，并且只能供 vSphere 计算机组件使用。有关配置 NSX 的信息，请参见 [NSX for vSphere 产品文档](#) 或 [NSX-T 产品文档](#) 中的《管理指南》，具体取决于您使用的应用程序。

部署的蓝图包含 NSX-T 端点时，部署将向部署中的所有 NSX-T 组件分配一个标记，这些组件包括 NSX-T 网络、安全和负载均衡器组件以及 NSX-T 端点的关联 vSphere 计算机组件。标记对部署是唯一的，并与初始部署中的组件以及您在部署中所做的任何后续操作相关联。标记名称与部署的名称相同。

启用应用程序隔离时，将为部署创建包含新规则的防火墙区域。应用程序隔离使用逻辑防火墙阻止所有入站和出站流量流向蓝图中的应用程序。通过包含应用程序隔离策略的蓝图置备的组件计算机可以相互通信，但无法连接到防火墙外部，除非向蓝图中添加其他 NS 组，并配置相应的安全规则以允许访问。

如果蓝图包含一个或多个负载均衡器，并且为蓝图启用了应用程序隔离，则会将负载均衡器 VIP 作为 IPSet 添加到应用程序隔离安全组中。如果蓝图包含的按需安全组所关联的计算机层同时关联了负载均衡器，该按需安全组将包含计算机层，以及负载均衡器 VIP 的 IPSet。

对于 NSX-T，应用程序隔离是仅创建按需 NS 组。它包含一个 IP 集，其中包括负载均衡器 VIP 和 NAT 一对多网络外部 IP。

有关 NSX-T -特定部署和拓扑注意事项的详细信息，请参见 [了解网络连接、安全性和负载均衡器配置的 NSX-T 部署拓扑](#)。

添加 NSX-T NS 组组件

您可以将现有 NSX-T NS 组组件添加到设计画布，并将其设置配置为与 vSphere 计算机组件及其他关联组件（如软件组件和网络组件）一起使用。

NSX-T NS 组可以包含 IP 集、MAC 集、逻辑端口、逻辑交换机和其他 NS 组的组合。您可以在防火墙规则中将 NS 组指定为源和目标。有关 NS 组特性的详细信息，请参见 [NSX-T 产品文档](#) 中《NSX-T 管理指南》中的“创建 NS 组”。

注 NS 组安全性将应用于连接到 NSX-T 管理的含糊 (opaque) 网络的虚拟机。如果虚拟机连接到 vSphere dvPortGroup，该网络将无法使用微分段。

默认情况下，创建或编辑蓝图时会显示应用于当前租户的 NS 组。关联端点在当前租户中有预留时，安全组可用。有关控制租户访问的其他信息，请参见在 [vRealize Automation 中控制安全对象的租户访问](#)。

前提条件

- 在 NSX-T 中创建并配置 NS 组。请参见 [准备 NSX 网络与安全配置的对照表](#)。
- 确认已针对您的集群成功运行 NSX 清单。

要在 vRealize Automation 中使用 NSX 配置，必须运行数据收集。
- 查看安全组件概念。请参见 [使用蓝图中的 NSX-T 安全组件](#)。
- 以 **基础架构架构师** 身份登录到 vRealize Automation。
- 使用 **设计** 选项卡在设计画布中打开新蓝图或现有蓝图。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的**网络和安全**。
- 2 将 **NSX-T NS 组** 组件拖动到设计画布上。
- 3 从下拉菜单中选择 NS 组。
- 4 如果出现提示，请输入关联的端点。
- 5 要将蓝图另存为草稿或继续配置蓝图，请单击**保存或完成**。

结果

您可以在 vSphere 计算机组件的**安全**选项卡中添加安全设置。

关联网络与安全组件

您可以将网络与安全组件拖动到设计画布上，使其设置可用于蓝图中的计算机组件配置。为计算机定义网络与安全设置后，您可以选择关联负载均衡器组件中的设置。

将 NSX 网络或安全组件添加到设计画布并定义其可用设置后，您可以在画布中打开 vSphere 计算机组件的网络与安全选项卡，然后配置其设置。

例如，您可以将按需 NAT 网络组件拖动到设计画布上，并将其与蓝图中的 vSphere 计算机组件或 NSX 负载均衡器组件相关联。

添加到蓝图中的网络与安全组件设置派生自 NSX for vSphere 和 NSX-T 配置，要求您对 vSphere 群集运行数据收集以获得 NSX 清单。网络与安全组件特定于 NSX，并且只能供 vSphere 计算机组件使用。有关配置 NSX 的信息，请参见 [NSX for vSphere 产品文档](#) 或 [NSX-T 产品文档](#) 中的《管理指南》，具体取决于您使用的应用程序。

注 如果蓝图包含一个或多个负载均衡器，并且为蓝图启用了应用程序隔离，则会将负载均衡器 VIP 作为 IPSet 添加到应用程序隔离安全组中。如果蓝图包含的按需安全组所关联的计算机层同时关联了负载均衡器，该按需安全组将包含计算机层，以及负载均衡器 VIP 的 IPSet。

有关使用 NAT 规则以允许 TCP 或 UDP 端口从 Edge（源端口）的外部 IP 地址映射到 NAT 网络组件（目标端口）中的专用 IP 地址的信息，请参见 [创建和使用 NSX for vSphere 的 NAT 规则](#) 或 [创建和使用 NSX-T 的 NAT 规则](#)。

有关 NSX-T -特定部署和拓扑注意事项的详细信息，请参见 [了解网络连接、安全性和负载均衡器配置的 NSX-T 部署拓扑](#)。

将蓝图配置为从 OVF 置备

可以使用 OVF 定义 vSphere 计算机属性和硬件设置，这通常是在 vRealize Automation 中蓝图配置页面上定义或者使用 vRealize Automation REST API 或 vRealize CloudClient 以编程方式定义的。

此外，还可以通过从 OVF 导入设置来为映像组件配置文件定义值集。参数化蓝图使用映像和大小组件配置文件类型。

OVF 是用于打包和分发虚拟机软件应用程序的开源标准。

OVF 置备类似于克隆，只不过源计算机是在服务器或网站上托管的 OVF 模板，而不是在 vCenter 中托管的虚拟机模板。

通常，使用 OVF 文件描述单个虚拟机或虚拟设备。它不仅可以包含有关虚拟磁盘映像文件格式的信息，还可以包含应模拟运行磁盘映像上包含的操作系统或应用程序的虚拟硬件的描述。OVA 文件是一个虚拟设备软件包，其中包含用于描述虚拟机的文件，包括 OVF 描述符文件、可选清单和证书文件以及其他相关文件。

定义蓝图时，可以在 vSphere 计算机组件上使用 **ImportOvfWorkflow** 置备选项。在属性字典中为映像组件配置文件定义值集时，也可以使用该置备选项。

可以将蓝图配置设置添加到 OVF 中以用于描述以下类型的信息：

- 最小 CPU、内存和存储分配。
- 用户可配置的自定义属性。
- 蓝图参数化的组件配置文件设置。

不支持具有多个计算机的 OVF 和 OVA。

基本注意事项包括以下声明：

- 支持 OVF 文件和 OVA 软件包。
- 支持托管 OVF 或 OVA 的 HTTP 服务器的基本用户名和密码身份验证。指定的 URL 在蓝图中验证。
- 不从 vCenter Server 收集 OVF 和 OVA 相关数据。
- 支持 EBS 订阅。
- 将用户可配置的 OVF 设置导入蓝图时，可以定义自定义属性。
- 请求 vSphere 计算机置备时，可以添加、更改或移除从 OVF 导入获得的设置。
- 您可以在虚拟机重新配置期间添加、更改或移除设置。

使用 OVF 定义 vSphere 组件的蓝图设置

您可以从 OVF 导入设置，以便简化在 vRealize Automation 蓝图中配置 vSphere 计算机组件设置的过程。

此过程假定您基本了解 vRealize Automation 蓝图的创建过程。

前提条件

- 以**基础架构架构师**身份登录到 vRealize Automation。
- 满足**配置计算机蓝图**中指定的其他必备条件。

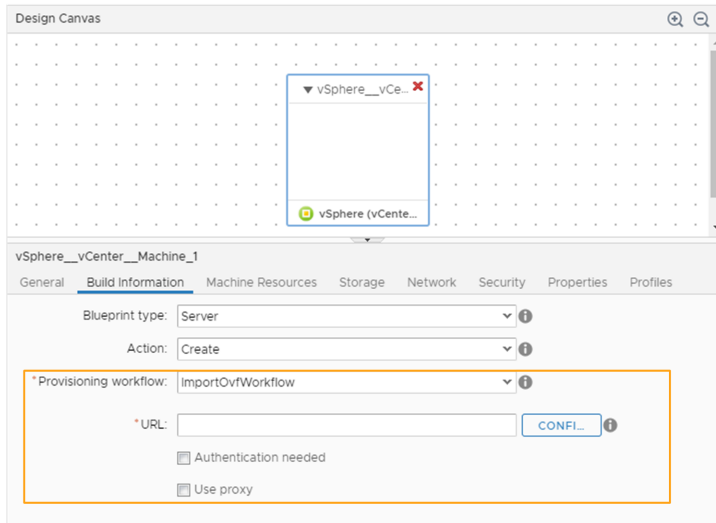
步骤

- 1 选择**设计 > 蓝图**。
- 2 单击**新建**图标 (+)。
- 3 输入蓝图名称和描述，然后单击**确定**。
- 4 单击“类别”区域中的**计算机类型**，然后将 **vSphere (vCenter) 计算机** 组件拖动到设计画布上。

5 单击**构建信息**选项卡，并指定以下选项：

- **蓝图类型：**服务器
- **操作：**创建
- **置备 workflow：**ImportOvfWorkflow

ImportOvfWorkflow 设置提供 **URL** 选项。



6 指定 OVF 的位置。

- 使用格式 `https://server/folder/name.ovf` 或 `name.ova` 输入 OVF URL 的路径。
如果对托管 OVF 的服务器启用身份验证，请输入对用户进行身份验证的凭据。
- 如果 OVF 托管在网站上，并且您创建了访问网站时可使用的代理端点，请选择**使用代理**，然后选择可用的代理端点。

7 单击**配置**。

注 如果您收到身份验证错误消息，说明托管 OVF 的服务器需要身份验证凭据。如果发生这种情况，请选中**需要身份验证**复选框，输入用于对 OVF 所在 HTTP 服务器进行身份验证的**用户名**和**密码**凭据，然后再次单击**配置**。

“配置”选项会打开一个向导，其中显示可作为自定义属性从 OVF 导入的所有用户可配置属性和值。如果没有要导入的可配置属性，则该窗格为空。

- a 使用向导接受要导入的默认值，或者在导入之前更改蓝图的这些值。
- b 单击**确定**以导入属性和值。

OVF 模板中所有用户可配置属性均作为可编辑 vRealize Automation 自定义属性导入到蓝图中，并以 `VMware.Ovf` 开头，而导入后不进行编辑的其他属性则作为隐藏属性导入。

8 单击**计算机资源**选项卡以显示 **CPU**、**内存 (MB)** 和 **存储 (GB)** 选项的最小值项中反映的 OVF 导入结果。

导入后，可以更改这些值。

- 9 单击**存储**选项卡以显示 OVF 导入的结果。
- 10 依次单击**属性 > 自定义属性**选项卡以显示 OVF 导入的结果。
- 11 单击**保存**。

后续步骤

继续定义蓝图设置或单击**完成**。

通过使用 OVF 为组件配置文件定义映像值集

可以通过从 OVF 导入设置来为要在参数化 vRealize Automation 蓝图中使用的映像组件配置文件创建一个或多个值集。

为 **Image** 组件配置文件导入值集定义后，可以向蓝图中 **vSphere** 虚拟机组件的组件配置文件中添加一个或多个值集。用户请求目录项时，可以选择可用的 **Image** 并使用映像值集中定义的参数进行部署。

导入 OVF 时，OVF 中的用户可配置属性和值不会作为值集中的自定义属性导入。如果要从导入的 OVF 中使用与映像值集相关的新自定义属性，必须在 **vSphere** 计算机组件或整个蓝图中手动定义新自定义属性。在参数化蓝图中创建的自定义属性应适用于每个组件配置文件映像的值集。

注 vRealize Automation 的 OVF 自定义属性不适用于 vSphere 的 OVF 自定义属性。请考虑分别为 vRealize Automation 和 vSphere 创建一个映像值集。

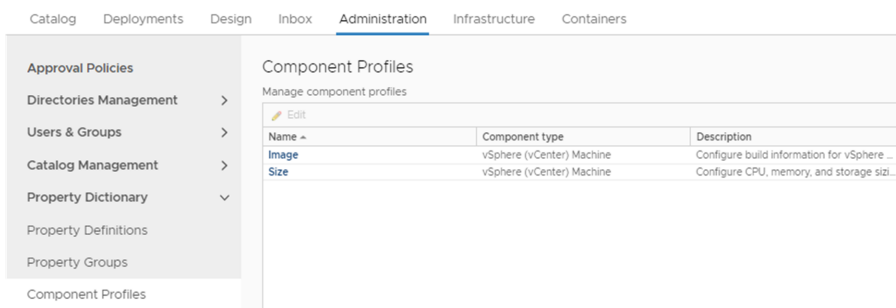
有关使用组件配置文件进行蓝图参数化的更多信息，请参见[了解和使用蓝图参数化](#)。

前提条件

- 以具有**租户管理员**和 **IaaS 管理员**访问权限的管理员身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 属性字典 > 组件配置文件**。



- 2 单击“名称”列中的**映像**。
将显示有关提供的映像组件属性的信息。
- 3 单击**值集**选项卡。

4 要定义新值集，请单击**新建**并配置 **Image** 设置。

- a 在**显示名称**字段中输入一个值以附加到 **ValueSet** 分隔符，例如 **ProdOVF**。
- b 接受**名称**文本框中显示的默认值，或输入自定义名称。
- c 在**描述**文本框中输入描述，例如**克隆方案 A 的构建设置**。
- d 在**状态**下拉菜单中选择**活动**或**非活动**。
选择**活动**可使值集显示在目录置备请求表单中。
- e 选择**创建**构建操作。
- f 选择**服务器**或**桌面**作为蓝图类型。
- g 选择 **ImportOvfWorkflow** 置备工作流。
- h 使用格式 `https://server/folder/name.ovf` 或 `name.ova` 输入 OVF URL 的路径。
- i 如果对托管 OVF 的服务器启用身份验证，请输入对用户进行身份验证的凭据。
- j 如果 OVF 托管在网站上，并且您创建了访问网站时可使用的代理端点，请选择**使用代理**，然后选择可用的代理端点。

5 单击**保存**。

6 对设置感到满意时，单击**完成**。

后续步骤

创建映像并导入 OVF 以定义映像值集后，可以将映像添加到蓝图中的 vSphere 计算机组件。

使用蓝图中的容器组件

您可以在蓝图中配置和使用容器组件。

容器管理员在 vRealize Automation 容器 中创建容器定义后，容器架构师可以在设计画布中为 vRealize Automation 蓝图添加和配置容器组件。

容器组件设置

您可以在 vRealize Automation 设计画布中为 vRealize Automation 容器 容器组件配置蓝图设置和选项。

常规选项卡

在设计画布中为蓝图容器组件配置常规设置。

表 3-33. 常规选项卡设置

设置	描述
名称	输入蓝图中的容器组件的名称。
描述	概述容器组件为其他架构师带来的优势。
映像	输入专用注册表或 Docker Hub 注册表等受管注册表中的映像全名，例如， <code>registry.hub.docker.com/library/python</code> 。

表 3-33. 常规选项卡设置（续）

设置	描述
命令	输入适用于指定映像的命令，例如， <code>python app.py</code> 。该命令在容器置备过程启动时运行。
链接	链接提供了另外一种方法来连接单个主机上的容器或跨主机连接容器。输入此容器要链接到的一个或多个服务，例如， <code>redis</code> 或 <code>datadog</code> 。

网络选项卡

在设计画布中为蓝图容器组件配置网络设置。

您可以将容器连接到网络。该网络在设计画布上表示为容器网络组件。有关可用网络的信息在容器组件表单的“网络”页面中指定。

表 3-34. 网络选项卡设置

设置	描述
网络	指定为选定映像定义的现有网络。您还可以创建新网络。 将网络容器组件添加到设计表单时，您在此处指定的网络将作为可供选择的选项列出。
端口绑定	指定选定网络的端口绑定。点绑定包含协议主机、主机端口和容器端口。
发布所有端口	选中该复选框可向所有用户公开在容器映像中使用的端口。
主机名称	指定容器主机名。如果未指定名称，则该值默认为蓝图中的容器组件的名称。
网络模式	指定容器的网络堆栈。如果未指定值，则容器在“桥接网络”模式下配置。

存储选项卡

在设计画布中为蓝图容器组件配置存储设置。

表 3-35. 存储选项卡设置

设置	描述
卷	指定从将由容器使用的主机映射的存储卷。
源卷	指定要从其他容器继承的存储卷。
工作目录	指定要从中运行命令的目录。

策略选项卡

在设计画布中为蓝图容器组件配置策略设置，例如，部署策略和关联性限制。

表 3-36. 策略选项卡设置

设置	描述
部署策略	指定部署策略，以便为要用于部署此容器的一组主机设置首选项。您可以在部署容器时将部署策略与主机、策略和容器定义相关联，以便为主机、策略和配额设置首选项。 您可以使用 vRealize Automation 中的 容器 选项卡添加部署策略。
集群大小	指定要从此容器生成为集群的实例数。
重新启动策略	为容器退出时如何重新启动指定重新启动策略。
重新启动上限	如果您选择“出现错误时”作为重新启动策略，可以指定最大重新启动次数。
CPU 份额	指定为已置备资源分配的 CPU 份额值。
内存限制	指定一个介于 0 和放置区域中的可用内存之间的数字。这是可供此放置中的资源使用的总内存。0 表示没有限制。
内存交换	总内存限制。
关联性限制	定义用于在相同或不同主机上置备容器的规则。 <ul style="list-style-type: none"> ■ 关联性类型 <p>对于反关联性，容器放置在不同主机上，否则放置在同一主机上。</p> ■ 服务 <p>下拉菜单中提供的服务名称与在常规选项卡上的名称字段中指定的容器组件名称匹配。</p> ■ 限制 <p>硬性限制规定如果不能满足限制，置备将失败。软性限制规定如果不能满足限制，置备应继续。</p>

环境选项卡

在设计画布中为蓝图容器组件配置环境设置，例如，属性绑定。

表 3-37. 环境选项卡设置

设置	描述
名称	变量名称。
绑定	将变量绑定到属于模板的其他属性。选择绑定时，必须在 <code>_resource~TemplateComponent~TemplateComponentProperty</code> 语法中输入值。
值	环境变量的值或者（如果选择绑定）要绑定的属性的值。

“属性”选项卡

在设计画布中为蓝图容器组件配置各个自定义属性和自定义属性组。

如果选择**属性组**选项卡并单击**添加**，可以使用以下选项：

- 使用证书身份验证的容器主机属性
- 使用用户/密码身份验证的容器主机属性

如果定义其他属性组，也会将其列出。

如果选择**自定义属性**选项卡并单击**添加**，可以将各个自定义属性添加到容器组件。

表 3-38. 自定义属性的属性选项卡设置

设置	描述
名称	输入自定义属性的名称或从下拉菜单中选择可用的自定义属性。
值	输入或编辑一个值，以与自定义属性名称相关联。
加密	如果属性值是密码，则您可以选择进行加密。
可覆盖	您可以指定属性值可由使用该属性的下一个或后续用户替代。该用户通常是另一位架构师，但如果选择“在请求中显示”，则业务用户能够在请求目录项时查看和编辑属性值。
在请求中显示	如果要向最终用户显示属性名称和值，则可以在请求计算机置备时选择在请求表单中显示属性。如果希望用户提供值，则还必须选择 可覆盖 。

运行状况配置选项卡

在设计画布中为蓝图容器组件指定运行状况配置模式。

表 3-39. 运行状况配置选项卡设置

模式设置	描述
无	默认。未配置运行状况检查。
HTTP	如果选择 HTTP ，则必须提供要访问的 API 以及要使用的 HTTP 方法和版本。该 API 是相对的，您无需输入容器的地址。还可以指定操作的超时期限并设置运行状况阈值。 例如，正常阈值为 2 表示必须连续两次调用成功，容器才会视为正常并处于 RUNNING 状态。不正常阈值为 2 表示必须连续两次调用失败，容器才会视为不正常并处于 ERROR 状态。对于介于正常和不正常阈值之间的所有状态，容器状态均为 DEGRADED 。
TCP 连接	如果选择 TCP 连接 ，则只能输入容器的端口。运行状况检查会尝试在提供的端口上与容器建立 TCP 连接。与 HTTP 一样，还可以指定操作的超时值并设置正常或不正常阈值。
命令	如果选择 命令 ，则必须输入要在容器上运行的命令。运行状况检查的成功与否取决于该命令的退出状态。
置备时忽略运行状况检查	取消选中此选项会强制在置备时执行运行状况检查。通过强制执行，只有成功通过运行状况检查后，容器才会被视为已置备容器。
Autodeploy	容器处于错误状态时自动重新部署容器。

日志配置选项卡

在设计画布中为蓝图容器组件指定日志记录模式和可选的日志记录选项。

表 3-40. 日志配置选项卡设置

设置	描述
驱动程序	从下拉菜单中选择日志记录格式。
选项	使用遵循日志记录格式的名称和值格式输入驱动程序选项。

在蓝图中使用容器属性和属性组

可以向 vRealize Automation 蓝图中的容器组件添加预定义的属性组。使用包含这些属性的蓝图置备计算机时，已置备的计算机将注册为 Docker 容器主机。

vRealize Automation 容器 提供了以下两个属性组，其中包含特定于容器的自定义属性。向蓝图添加容器组件时，您可以将这两个属性组添加到容器中，以将已置备计算机注册为容器主机。

- 使用证书身份验证的容器主机属性
- 使用用户/密码身份验证的容器主机属性

当您选择**管理 > 属性字典 > 属性组**时，这两个属性组会显示在 vRealize Automation 中。

由于属性组由所有租户共享，因此在多租户环境中工作时，应考虑克隆属性并对其进行自定义。通过为属性组和组中的属性分配唯一名称，您可以编辑这两个属性组及其中的属性，以定义供特定租户使用的自定义值。

最常用的属性是 `Container.Auth.PublicKey` 和 `Container.Auth.PrivateKey`，在这两个属性中，容器管理员将提供客户端证书以用于向容器主机进行身份验证。

表 3-41. 容器 自定义属性

属性	描述
<code>containers.ipam.driver</code>	仅可与容器配合使用。指定将 容器 网络组件添加到蓝图时要使用的 IPAM 驱动程序。受支持的值取决于在使用这些值的容器主机环境中安装的驱动程序。例如，根据容器主机上安装的 IPAM 插件，受支持的值可能是 <code>infoblox</code> 或 <code>calico</code> 。
<code>containers.network.driver</code>	仅可与容器配合使用。指定将 容器 网络组件添加到蓝图时要使用的网络驱动程序。受支持的值取决于在使用这些值的容器主机环境中安装的驱动程序。默认情况下，Docker 提供的网络驱动程序包括 <code>bridge</code> 、 <code>overlay</code> 和 <code>macvlan</code> ，而虚拟容器主机 (Virtual Container Host, VCH) 提供的网络驱动程序包括 <code>bridge</code> 驱动程序。还可以使用 <code>weave</code> 和 <code>calico</code> 等第三方网络驱动程序，具体取决于容器主机上安装的网络插件。
<code>Container</code>	仅可与容器配合使用。默认值为 <code>App.Docker</code> ，是必需的。请勿修改此属性。
<code>Container.Auth.User</code>	仅可与容器配合使用。指定用于连接到 容器 主机的用户名。
<code>Container.Auth.Password</code>	仅可与容器配合使用。指定该用户名的密码或要使用的公用密钥或私有密钥密码。支持加密属性值。

表 3-41. 容器 自定义属性 （续）

属性	描述
Container.Auth.PublicKey	仅可与容器配合使用。指定用于连接到 容器 主机的公用密钥。
Container.Auth.PrivateKey	仅可与容器配合使用。指定用于连接到 容器 主机的私有密钥。支持加密属性值。
Container.Connection.Protocol	仅可与容器配合使用。指定通信协议。默认值为 API ，是必需的。请勿修改此属性。
Container.Connection.Scheme	仅可与容器配合使用。指定通信方案。默认值为 https 。
Container.Connection.Port	仅可与容器配合使用。指定 容器 连接端口。默认值为 2376 。
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.MachineActivated	仅可与容器配合使用。指定要公开所有 容器 属性并用于注册已置备主机的事件代理属性。默认值为 Container* ，是必需的。请勿修改此属性。
Extensibility.Lifecycle.Properties.VMPSMasterWorkflow32.Disposing	仅可与容器配合使用。指定要公开上述所有 容器 属性并用于取消注册已置备主机的事件代理属性。默认值为 Container* ，是必需的。请勿修改此属性。

在设计画布中使用 容器 网络组件

可以将一个或多个 容器 网络组件添加到设计画布，为蓝图中的 vSphere 计算机组件配置设置。

向蓝图添加组件时，可以将 **containers.ipam.driver** 和 **containers.network.driver** 添加到该组件中。

添加容器网络组件

您可以将容器网络信息添加到包含容器组件的 vRealize Automation 蓝图。

您可以使用 vRealize Automation **容器**选项卡在 vRealize Automation 容器 中配置容器。通过使用 vRealize Automation **设计**选项卡中的选项，您可以将这些容器及其网络设置作为组件添加到蓝图中。

前提条件

- 以**容器架构师**身份登录到 vRealize Automation。
- 使用**设计**选项卡在设计画布中打开新蓝图或现有蓝图。

步骤

- 1 要显示可用网络和安全组件的列表，请单击“类别”部分中的**网络和安全**。
- 2 将**容器网络**组件拖动到设计画布上。
- 3 要在设计画布中唯一标记组件，请在**名称**文本框中输入名称。
- 4 （可选）在**描述**文本框中输入组件描述。
- 5 （可选）如果不希望指定外部 IPAM 设置，请选中**外部**复选框。

如果选中**外部**复选框，将移除 **IPAM 配置**选项卡。

- 6 单击 **IPAM 配置** 选项卡，为在蓝图的容器组件中指定的网络指定新子网、IP 范围和网关或编辑现有子网、IP 范围和网关。

IPAM 配置将应用于由 vRealize Automation 创建的新网络，而不是以前在 Docker 或其他支持的容器应用程序中创建的网络。这些设置未经验证，如果与其他网络重叠，置备将失败。例如，子网和网关在容器主机中必须是唯一的。

- 7 单击 **属性** 选项卡以指定组件的自定义属性。

如果选择 **属性组** 选项卡并单击 **添加**，可以使用以下选项：

- 使用证书身份验证的容器主机属性
- 使用用户/密码身份验证的容器主机属性

如果定义其他属性组，也会将其列出。

如果选择 **自定义属性** 选项卡并单击 **添加**，可以将各个自定义属性添加到容器组件。

表 3-42. 自定义属性的属性选项卡设置

设置	描述
名称	输入自定义属性的名称或从下拉菜单中选择可用的自定义属性。
值	输入或编辑一个值，以与自定义属性名称相关联。
加密	如果属性值是密码，则您可以选择进行加密。
可覆盖	您可以指定属性值可由使用该属性的下一个或后续用户替代。该用户通常是另一位架构师，但如果选择“在请求中显示”，则业务用户能够在请求目录项时查看和编辑属性值。
在请求中显示	如果要向最终用户显示属性名称和值，则可以在请求计算机置备时选择在请求表单中显示属性。如果希望用户提供值，则还必须选择 可覆盖 。

- 8 要将蓝图另存为草稿或继续配置蓝图，请单击 **保存或完成**。

后续步骤

您可以在容器组件的 **网络** 选项卡中添加容器网络设置。

推送容器模板以在蓝图中使用

您可以使容器模板在 vRealize Automation 蓝图中可用。

一个容器模板可以包含多个容器。将多容器模板推送到 vRealize Automation 时，将在 vRealize Automation 中以多组件蓝图的形式创建该模板。

添加到容器模板的特定于容器的属性在 vRealize Automation 蓝图中会得到识别。请参见 [在蓝图中使用容器属性和属性组](#)。

当您请求置备已在 vRealize Automation 目录中发布的蓝图时，应置备该蓝图的源容器应用程序。

可以将其他组件添加到 vRealize Automation 蓝图，包括以下组件类型：

- 计算机类型
- 软件组件
- 其他蓝图
- NSX 网络组件和安全组件
- XaaS 组件
- 自定义组件

可以从 容器 将模板推送到 vRealize Automation。对 vRealize Automation 蓝图进行的更改不会影响 容器 模板。

可以在 容器 模板中进行后续更改并重新推送，以覆盖 vRealize Automation 中的蓝图。将模板推送到 vRealize Automation 会覆盖蓝图，并且在两次推送之间对 vRealize Automation 中的蓝图进行的任何更改都会丢失。要避免蓝图更改丢失，请使用 vRealize CloudClient 克隆新蓝图或导出蓝图。

从蓝图置备 Docker 容器或主机

可以创建 vRealize Automation 蓝图并用来将计算机置备为已注册的 Docker 容器主机。

要使已置备的计算机注册为容器主机，该计算机必须满足以下要求：

- 该计算机是通过包含特定于 容器 的自定义属性的蓝图置备的。
所需的特定于容器的自定义属性在两个属性组中提供。请参见[在蓝图中使用容器属性和属性组](#)。
有关在 vRealize Automation 中使用自定义属性和属性组的信息，请参见《自定义属性参考》。
- 可以通过网络访问该计算机。
例如，该计算机必须具有有效的 IP 地址并且已打开电源。

您可以定义一个 vRealize Automation 蓝图，使其包含用于在使用该蓝图进行置备时将计算机指定为容器主机的特定自定义属性。

如果成功置备具有所需蓝图属性的计算机，该计算机将注册到 容器 中，并且可以从 vRealize Automation 接收事件和操作。

创建 Microsoft Azure 蓝图并整合资源操作

作为云或架构管理员，您可以创建 Microsoft Azure 虚拟机蓝图，业务组管理员将这些蓝图用作构建块，为使用者创建自定义的已置备计算机。DevOps 管理员也可以创建 Azure 计算机蓝图，或者可以使用现有的 Azure 计算机蓝图创建复合蓝图。

- [创建用于 Microsoft Azure 的蓝图](#)
可以创建用于提供对 Azure 虚拟机资源的访问的 Microsoft Azure 虚拟机蓝图。
- [创建 Azure 自定义资源操作](#)
您可以创建并使用自定义资源操作控制 Azure 虚拟机。

创建用于 Microsoft Azure 的蓝图

可以创建用于提供对 Azure 虚拟机资源的访问的 Microsoft Azure 虚拟机蓝图。

默认的“Azure 计算机”模板显示在 vRealize Automation “编辑蓝图”页面上的**计算机类型**类别中。可以使用此虚拟机模板作为 Azure 蓝图的基础，如以下过程中所述。创建 Azure 蓝图之后，可以按设计发布并部署该蓝图，也可以将该蓝图与自定义 Azure 资源或其他蓝图结合使用以创建复合蓝图。

创建并发布蓝图后，具有相应特权的用户可以通过 vRealize Automation 服务目录请求并置备 Azure 实例。

请注意，Azure 蓝图定义了虚拟机要求。vRealize Automation 会利用这些要求选择最适用于部署的预留。

有关“新建蓝图”对话框上“NSX 设置”和“属性”选项卡的信息，请参见《配置 vRealize Automation》。

如果要从一个部署同时创建两个计算机，您必须创建两个网络接口名称和两个虚拟机名称。

注 避免使用相同的命名前缀将同一个部署置备到 Azure 和 vSphere，因为这可能会导致在 Azure 和 vSphere 上出现名称重复，进而可能会对某些用户带来问题。

前提条件

- 获取有效的 Azure 订阅 ID 和相关信息，其中包括创建蓝图时可能需要的资源组、存储帐户和虚拟网络信息。
- 配置 Azure 端点，创建 Azure 连接以便与 vRealize Automation 部署结合使用。
- 根据业务组需要配置 Azure 预留。

步骤

1 选择**设计 > 蓝图**。

2 单击**新建**图标(+)。

3 在**名称**文本框中输入蓝图名称。

您输入的名称还会填充 **ID** 文本框。在大多数情况下，您可以忽略 **NSX 设置**和**属性**选项卡。

4 单击**确定**。

5 单击“类别”菜单中的**计算机类型**。

6 将 **Azure 计算机**虚拟机模板拖动到设计画布。

如果已创建自定义 Azure 资源以用作蓝图的基础，则可以从“类别”列表中的已分配类别中选择该资源。

7 在位于设计画布下半部分的选项卡式页面（在将“Azure 计算机”模板拖动到设计画布时显示）上的文本框中输入 Azure 虚拟机所需的信息。

所有这些选项卡上的文本框及其他参数的可用选项主要取决于配置为蓝图基础的 Azure 端点。

对于大多数参数，如果可以单击参数名称旁边的文本框，将在页面的右侧打开一个新窗格。在此窗格中，可以在**值**文本框中输入参数值并指示值是否为**必需**。请注意，在某些情况下，还可以输入**最小值**和**最大值**。单击右窗格中的**应用**以填充初始文本框。

图 3-1. Azure 蓝图右侧菜单

The screenshot displays the configuration page for 'Azure_Machine_1' with the 'Machine Resources' tab selected. It features two main configuration sections: 'Resource Group' and 'Availability Set'. The 'Resource Group' section includes radio buttons for 'Create New' and 'Use Existing', and a text input field for 'Resource Group Name' which contains the value 'RG1-vAficionado'. The 'Availability Set' section includes radio buttons for 'None', 'Create New', and 'Use Existing'. To the right of these sections, there is a 'Required' dropdown menu set to 'No' and a 'Value' text input field containing 'RG1-vAficionado'. An orange arrow points from the 'Value' field back to the 'Resource Group Name' field, indicating a relationship or data flow between the two.

大多数参数还有一个**高级选项**按钮。通过这些选项，不但可以指定参数长度，甚至还可以针对最终用户隐藏参数。

注 为了继续进行蓝图配置，必须填充每个选项卡上的必填参数。如果要将某个字段留空，可以返回并删除输入，然后再保存。

选项卡	描述	重要参数
常规	选择 Azure 虚拟机的基本连接信息，例如要使用的端点。	<p>ID - 标识所创建的 Azure 虚拟机。如果更改此名称，设计画布上的 Azure 虚拟机映像也会自动更新。</p> <p>描述 - 标识所创建的虚拟机以及描述是否为必需。</p> <p>实例 - 使用此选项，您可以创建可扩展的虚拟机。使用最小值和最大值字段标识可从此计算机生成的 Azure 实例数量。</p> <p>使用密码身份验证：选择“是”将使用密码身份验证，选择“否”将使用 SSH。</p> <p>管理员用户名 - 将该字段留空，这可由置备计算机的用户进行分配。</p> <p>管理员密码 - 将该字段留空，置备计算机的个人可以提供相应的密码。</p>
构建信息	使用此选项卡，可以配置有关所创建的虚拟机的信息。	<p>位置 - 选择将该虚拟机部署到的地理位置。</p> <p>计算机前缀 - 选择相应的单选按钮，以指示是要使用关联的业务组中的计算机前缀还是要创建自定义前缀。如果要使用自定义前缀，请在自定义计算机前缀文本框中输入该前缀。</p> <p>虚拟机映像类型 - 选中自定义或备用虚拟机映像的相应单选按钮。自定义虚拟机是从 Azure 经典部署创建的，并提供有关云服务、存储帐户和可用性集的更多配置选项。</p> <p>虚拟机映像 e - 标识蓝图将基于的 Azure 虚拟机映像。</p> <ul style="list-style-type: none"> ■ 对于备用虚拟机映像，计算机映像 URN 应与以下格式匹配：(发布者):(提供者):(sku):(版本)。 ■ 对于受管磁盘，计算机映像 URN 应与以下格式匹配： (ResourceGroupName):(CustomImageName) ■ 对于自定义虚拟机映像，计算机映像 URN 应与以下格式匹配： <code>https://storageaccount.blob.core.windows.net/ container/image.vhd</code> <p>对于“自定义”映像，还必须填写“OS 映像类型”（Windows 或 Linux）文本框。</p> <p>管理员用户 - 键入为基于该蓝图的虚拟机配置的指定管理员用户的名称。或者，也可以在请求表中将此参数留空。</p> <p>身份验证 - 选中相应的单选按钮以指示基于该蓝图的虚拟机要求密码身份验证还是 SSH 身份验证。</p> <p>管理员密码 - 虚拟机实例的管理员密码。</p> <p>系列 - 定义虚拟机实例的常规大小。有关系列信息，请参见 Azure 文档（网址为 https://azure.microsoft.com/zh-cn/documentation/articles/virtual-machines-windows-sizes/）。</p> <p>大小 - 定义某个实例中的特定虚拟机实例大小。大小与所选系列相关。如果已建立 Azure 实例的有效连接，则系统将根据订阅以及所选位置和系列动态填充可用的大小。有关大小信息，请参见 Azure 文档。</p> <p>实例大小详细信息 - 有关虚拟机实例系列和大小的可选信息。</p>

选项卡	描述	重要参数
计算机资源	<p>将虚拟机资源按段进行组织。资源组是一种组织结构，用于分组诸如网站、帐户、数据库和网络等虚拟机资源。</p> <p>可用性集是一种通过管理两个或更多虚拟机而支持冗余的机制。有关 Azure 可用性集的详细信息，请参见 https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/。</p> <p>注 如果配置最大 Azure 实例数设置为大于 1 的值，则应使用现有的资源组和可用性集，而不应创建新的资源组和可用性集。在同一个部署中的多个实例上使用新的资源组或可用性集会导致发生错误和其他问题（如果与负载均衡器关联）。</p>	<p>创建或重用资源组： 选中相应的单选按钮以指示是要使用现有 Azure 资源组还是要创建新的资源组。可以在 Azure 门户中的“资源组”页面上找到现有资源组的名称。如果选择创建新的资源组，则新组的相应名称会自动显示在资源组文本框中。</p> <p>创建或重用可用性集： 根据要执行的操作选中相应的单选按钮。如果选择“新建”，则新的可用性集信息的相应信息会显示在文本框中。</p>
存储	<p>让您可以选择 Azure 受管磁盘或此蓝图的存储帐户。使用受管磁盘，Azure 能够处理大多数存储相关的配置和维护。存储帐户可用于访问不同类型的 Azure 存储，例如 Azure Blob、队列表及文件存储。对于大多数蓝图，可以接受默认值。</p>	<p>存储类型 - 选择是要提供受管磁盘还是手动管理的存储帐户。</p> <ul style="list-style-type: none"> 如果选择的是受管磁盘，请在虚拟机磁盘类型框中选择是要使用高级磁盘还是标准磁盘。您可以忽略其余选择框。 如果选择的是存储帐户，请在操作系统磁盘存储帐户框中输入虚拟机的存储帐户名称。Azure 虚拟机操作系统磁盘部署到此存储帐户。可在 Azure 门户中找到存储组信息。可以有一个或多个存储帐户。 <p>注 如果存储帐户名称包含下划线或其他特殊字符，可能会引发错误。</p> <p>启用引导诊断 - 如果将诊断数据与 Azure 实例结合使用，请选中此复选框。</p> <p>数据磁盘数 - 选择与虚拟机结合使用的数据存储磁盘的相应数量。最多可以指定四个磁盘。除了存储帐户文本框中指定的操作系统磁盘之外，还有这些磁盘。</p> <p>存储磁盘编号</p> <ul style="list-style-type: none"> 磁盘名称 - 标识分配给磁盘的名称。 磁盘类型 - 存储设备类型。 磁盘大小 - 存储大小。 复制 - 用于磁盘备份的冗余方法。 主机缓存 - 指示是否缓存读取/写入以提高性能。

选项卡	描述	重要参数
网络	<p>使用此选项卡，可为虚拟机蓝图选择网络。对于大多数蓝图，您可以接受默认值，使用者将在部署期间输入相应的网络信息。</p> <p>注 只能在每个接口上创建一个虚拟机，但每个虚拟机最多可以具有四个接口。</p>	<p>单击表可在右侧打开一个对话框，其中包含另一个具有以下字段的可编辑表。</p> <ul style="list-style-type: none"> ■ 负载均衡器名称 - 与 Azure 实例结合使用的负载均衡器。 ■ 网络接口数 - 选择与 Azure 实例结合使用的网络接口的数量。在“存储”选项卡上选择的虚拟机大小必须支持该网络接口数。 ■ 网络接口 - 选择适用于虚拟机蓝图的网络接口。如果输入现有网络，可以忽略所有其他网络选项卡。如果输入的网络接口名称不存在，系统将会使用该名称创建一个新接口，您可以使用其他网络选项卡来配置该接口。 ■ NIC 名称前缀 - 网卡的前缀。 ■ IP 地址类型 - 指示虚拟机使用静态还是动态 IP 地址。 ■ 网络配置 - 输入相应的网络配置。支持网络配置文件。此字段具有两个选项，即指定 Azure 网络和使用网络配置文件，后续的字段因选择的选项而异。 <ul style="list-style-type: none"> ■ 当选择指定 Azure 网络时，以下选项可用。如果将这些文本框留空，则会根据适用预留中指定的信息使用默认网络构造。 <ul style="list-style-type: none"> ■ vNet 名称 - 虚拟网络的名称 ■ 子网名称 - Azure 子网的域名。 <p>注 在实施后操作期间，您可以为 Azure 设置公共 IP 地址。</p> <ul style="list-style-type: none"> ■ 当选择使用网络配置文件时，网络配置将与基础 Azure 构造分离并转而与 vRealize Automation 网络配置文件相结合。 <ul style="list-style-type: none"> ■ 如果将网络配置文件文本框留空，则会根据指定了网络配置文件的适用预留解析默认 Azure vNet 和子网对。 ■ 如果输入网络配置文件，则会根据匹配的预留解析 Azure vNet 和子网。
属性	<p>让您可以将自定义属性添加到蓝图中。此处应用的自定义属性可能会被后续优先级链中分配的属性覆盖。有关自定义属性的优先级顺序的详细信息，请参见《自定义属性参考》。</p>	<p>“属性”对话框上有两个选项卡可用于添加自定义属性。</p> <ul style="list-style-type: none"> ■ 属性组：这些可重用组可以简化添加自定义属性的过程。有四个选项用于选择属性组： <ul style="list-style-type: none"> ■ 添加 - 将可用属性组添加到蓝图。 ■ 上移/下移 - 控制属性组的优先级。第一组具有最高优先级，其自定义属性的优先级最高。 ■ 查看属性 - 查看所选组中的自定义属性。 ■ 查看合并的属性 - 如果自定义属性包含在多个属性组中，则优先使用优先级最高的属性组中的值。查看这些合并的属性可帮助您确定属性组的优先级。 ■ 自定义属性：使用此选项卡可以添加单个自定义属性。 <ul style="list-style-type: none"> ■ 新建 - 将单个自定义属性添加到蓝图。 ■ 名称 - 输入用于标识属性的名称。有关自定义属性及其定义的列表，请参见《自定义属性参考》。 ■ 值 - 输入自定义属性的值。 ■ 加密 - 可以对属性进行加密。 ■ 可覆盖 - 可以指定属性值可由下一个或后续用户覆盖。该用户通常是另一位架构师，但如果选择“在请求中显示”，则业务用户可在请求目录项时查看和编辑属性值。

选项卡	描述	重要参数
		<ul style="list-style-type: none"> 在请求中显示 - 如果要向最终用户显示属性名称和值，则可以在请求计算机置备时选择在请求表单中显示属性。如果希望用户提供值，则还必须选择“可覆盖”。

8 单击**完成**以保存蓝图配置并返回到“蓝图”主页。

后续步骤

如果已经在 Azure 预留中配置自定义属性以支持 VPN 安全加密链路，则可以将软件组件添加到 Azure 蓝图。

- 1 选择“类别”菜单上的**软件组件**。已配置 Azure 蓝图的软件组件将显示在下面的窗格中。
- 2 在容器下拉值中选择“Azure 虚拟机”。
- 3 选择所需的软件组件，并将其拖动到设计画布上的 Azure 虚拟机上。
- 4 如果具有软件组件所需的属性，则在设计画布下的相应参数文本框中输入这些属性。
- 5 单击**保存**。

如果要发布蓝图，请在“蓝图”主页上选择该蓝图，然后单击**发布**。已发布的蓝图会显示在“目录项”页面上。此外，业务组主管或具有同等角色的人员可以使用该已发布的蓝图作为复合蓝图的基础。

创建 Azure 自定义资源操作

您可以创建并使用自定义资源操作控制 Azure 虚拟机。

以下两个自定义资源操作附带提供了即时可用的 vRealize Automation Azure 实施：

- 启动虚拟机
- 停止虚拟机

此外，您还可以使用可通过 vRealize Automation 界面提供的 vRealize Orchestrator 库访问的工作流创建自定义资源操作。

您可以像在 vRealize Automation 中使用任何其他 XaaS 资源操作一样使用 Azure 资源操作。有关 XaaS 资源操作的详细信息，请参见《配置 vRealize Automation》中的创建 XaaS 蓝图和资源操作和 vRealize Automation 中的 vRealize Orchestrator 集成。

前提条件

为 vRealize Automation 部署配置有效的 Azure 端点。

步骤

- 1 选择**设计 > XaaS > 资源操作**。
- 2 单击**新建**。
- 3 导航到 vRealize Orchestrator 工作流库中的 **Orchestrator > 库 > Azure**。
- 4 选择所需的文件夹和工作流。

5 如同任何其他 XaaS 资源操作一样，您可根据自身需要配置该操作。

在 vSphere 蓝图添加配置管理功能

您可以将配置管理组件添加到 vSphere 蓝图以支持 vSphere 虚拟机的配置管理。

vRealize Automation 支持在 vSphere 蓝图添加 Puppet 和 Ansible 配置管理功能。

Puppet 配置管理通常使用角色和环境来定义和管理基于 Puppet Enterprise 应用程序的软件配置。请注意，Puppet 中角色和环境的含义因 IT 通用含义而异。

Ansible 配置管理基于 Ansible Tower 实施上定义的作业模板。您可以选择并重新排序多个模板。部署计算机后，从 vRealize Automation 销毁之前，您可以运行这些模板。

端点与现有的 Puppet 或 Ansible Enterprise 部署建立连接。创建端点时，vRealize Automation 将从指定部署检索相应信息。配置启用了 Puppet 或 Ansible 的虚拟机蓝图时，可以指定早期绑定或后期绑定场景。

注 当前仅在 vSphere 蓝图和虚拟机上支持 Ansible 和 Puppet 组件。

将 Puppet 组件添加到 vSphere 蓝图

可以将 Puppet 配置管理组件添加到 vSphere 蓝图，促进使用 Puppet Master 强制管理 vSphere 虚拟机。

将 Puppet 组件添加到 vSphere 蓝图时，可将 Puppet 代理添加到从该蓝图中创建的虚拟机。

创建已启用 Puppet 的 vSphere 蓝图时，必须选择是否创建早期绑定或后期绑定配置。

通过早期绑定，当 Puppet 组件添加到蓝图时，用户将根据特定的蓝图为所有虚拟机定义 Puppet 角色和环境设置。这些设置在蓝图的生命周期保持静态。对于后期绑定，有多种选项。

- 在蓝图中将 **Puppet 环境**和 **Puppet 角色**文本框留空，由用户在请求时提供这些设置。
- 指定 **Puppet 环境**，将 **Puppet 角色**框留空。用户必须在请求时指定角色。

前提条件

创建相应的 vSphere 蓝图。有关详细信息，请参见 [vSphere 计算机组件设置](#)。

步骤

- 1 选择**设计 > 蓝图**。
- 2 从蓝图的“设计”页面上的“类别”菜单中，选择**配置管理**。
- 3 选择 Puppet 组件，并将其拖动到“设计画布”上的 vSphere 组件。
- 4 在页面底部的“常规”选项卡上，输入 Puppet 组件的 **ID** 和**描述**。
ID 和描述可为任意内容。
- 5 单击“服务器”选项卡。
- 6 单击下拉列表并为蓝图选择相应的 Puppet Master。

- 7 如果要为此组件使用早期绑定，则选择相应的 **Puppet 环境**和 **Puppet 角色**。

要配置早期绑定，请选择 Puppet 环境和角色。如果要使用后期绑定创建组件，请选择 **Puppet 环境**，或将 **Puppet 环境**和 **Puppet 角色**文本框留空，然后选中在请求表单中设置复选框。

注 在请求表单中设置复选框已绑定在一起。如果选择一个，则会自动选择另一个。

- 8 单击**完成**以保存 Puppet 组件配置并返回到蓝图“设计”主页。

将 Ansible 组件添加到 vSphere 蓝图

可以将 Ansible 配置管理组件添加到 vSphere 蓝图，以便使用 Ansible Tower 强制管理 vSphere 虚拟机。

将 Ansible 组件添加到 vSphere 蓝图使 Ansible Tower 能够与已部署的资源进行通信以运行命令。

前提条件

创建相应的 vSphere 蓝图。有关详细信息，请参见 [vSphere 计算机组件设置](#)。

步骤

- 1 选择**设计 > 蓝图**。
- 2 从蓝图的“设计”页面上的“类别”菜单中，选择**配置管理**。
- 3 选择 Ansible 组件，将其拖动到“设计画布”上的 vSphere 组件。
- 4 在页面底部的“常规”选项卡上，输入 Ansible 组件的 **ID** 和**描述**。
ID 和描述可为任意内容。
- 5 单击“详细信息”选项卡，然后输入 Ansible Tower、项目和模板的相应信息。
 - a 选择相应的 **Ansible Tower** 以及将使用此组件的**组织**。
 - b 为 Ansible 组件配置早期或后期绑定。
 - 如果要为此组件使用早期绑定，选择相应的**项目**和**作业模板**。在**取消置备作业模板**文本框中，选择当计算机遭到破坏时要运行的相应模板。将在请求表单中设置复选框留空。选择相应的 Ansible 环境和角色。
 - 如果您想要使用后期绑定创建组件，可以选择在请求表单中设置复选框，而无需在**项目**、**作业模板**和**取消置备作业模板**框设置值。

注 在请求表单中设置复选框已绑定在一起。如果选择一个，下面的会自动选择。出现此功能是因为**项目**字段充当作业模板的筛选器。如果您指定项目，作业模板列表将按项目自动筛选。因此，如果您为项目选择在请求表单中设置，将自动选中以下两个字段。

- 6 单击**完成**保存 Ansible 组件配置并返回到蓝图“设计”主页。

将 RDP 连接支持添加到 Windows 计算机蓝图

要允许目录管理员授权用户使用为 Windows 蓝图中使用 RDP 操作进行连接，请将 RDP 自定义属性添加到该蓝图，并引用系统管理员准备的 RDP 文件。

注 如果架构管理员创建的属性组包含所需的自定义属性且您将该组包含在蓝图中，则无需将这些自定义属性分别添加到蓝图中。

前提条件

- 以**租户管理员**或**业务组主管**身份登录到 vRealize Automation。
- 获取系统管理员为您创建的自定义 RDP 文件的名称。请参见[为置备的计算机创建自定义 RDP 文件以支持 RDP 连接](#)。
- 至少创建一个 Windows 计算机端点。

步骤

- 1 选择**设计 > 蓝图**。
- 2 指向要更新的蓝图，然后单击**编辑**。
- 3 选择画布上的计算机组件以编辑详细信息。
- 4 单击**属性**选项卡。
- 5 单击**自定义属性**选项卡。
- 6 配置 RDP 设置。
 - a 单击**新建属性**。
 - b 在**名称**文本框中输入 RDP 自定义属性名称，并在**值**文本框中输入对应的值。

选项	描述和值
VirtualMachine.Rdp.File	指定从中获取设置的 RDP 文件，例如 <code>My_RDP_Settings.rdp</code> 。该文件必须位于 vRealize Automation 安装目录的 <code>Website\Rdp</code> 子目录中。
VirtualMachine.Rdp.SettingN	指定打开计算机 RDP 链接时要使用的 RDP 设置。 <i>N</i> 是用于区分各 RDP 设置的唯一编号。例如，要指定 RDP 身份验证级别以便不指定身份验证要求，请定义自定义属性 <code>VirtualMachine.Rdp.Setting1</code> 并将该值设置为 <code>authentication level:i:3</code> 。有关可用 RDP 设置及其正确语法的信息，请参见 Microsoft Windows RDP 文档，例如 《Windows Server 中远程桌面服务的 RDP 设置》 。
VirtualMachine.Admin.NameCompletion	指定要包括在 RDP 或 SSH 文件为用户界面选项 使用 RDP 连接 或 使用 SSH 连接 选项生成的计算机完全限定域名中的域名。例如，将该值设置为 <code>myCompany.com</code> 时，将在 RDP 或 SSH 文件中生成完全限定域名 <code>my-machine-name.myCompany.com</code> 。

- c 单击**保存**。

- 7 选择该蓝图行并单击**发布**。

结果

目录管理员可以针对通过蓝图置备的计算机将**使用 RDP 连接**操作授权给用户。如果未授权用户执行该操作，则用户无法使用 RDP 连接。

将 Active Directory 清理添加到您的 CentOS 蓝图

作为一名 IaaS 架构师，您需要将 vRealize Automation 配置为每次从 Hypervisor 中移除置备的计算机时便清理 Active Directory 环境。因此，您需编辑蓝图，以配置 Active Directory 清理插件。

使用 Active Directory 清理插件，您可以指定从 Hypervisor 中删除计算机时发生的以下 Active Directory 帐户操作：

- 删除 AD 帐户
- 停用 AD 帐户
- 重命名 AD 帐户
- 将 AD 帐户移动到其他 AD 组织单位 (Organizational Unit, OU)

前提条件

注 此信息不适用于 Amazon Web Services。

- 以**基础架构架构师**身份登录到 vRealize Automation。
- 收集有关 Active Directory 环境的以下信息：
 - 具有足够权限删除、停用、重命名或移动 AD 帐户的 Active Directory 帐户的用户名和密码。该用户名必须采用“域\用户名”格式。
 - （可选）移动已销毁计算机的目标 OU 的名称。
 - （可选）要附加到已销毁计算机的前缀。
- 创建计算机蓝图。请参见[配置计算机蓝图](#)。

步骤

- 1 选择**设计 > 蓝图**。
- 2 指向蓝图，并单击**编辑**。
- 3 选择画布上的计算机组件以显示“详细信息”选项卡。
- 4 单击**属性**选项卡。
- 5 单击**自定义属性**选项卡，以配置 Active Directory 清理插件。
 - a 单击**新建属性**。
 - b 在**名称**文本框中键入 `Plugin.AdMachineCleanup.Execute`。
 - c 在**值**文本框中键入 `true`。
 - d 单击**保存**图标 (🟢)。

6 通过添加自定义属性配置 Active Directory 清理插件。

选项	描述和值
Plugin.AdMachineCleanup.UserName	在 值 文本框中，输入 Active Directory 帐户用户名。此用户必须具有足够的特权，能够删除、停用、移动和重命名 Active Directory 帐户。该用户名必须采用“域\用户名”格式。
Plugin.AdMachineCleanup.Password	在 值 文本框中，输入 Active Directory 帐户用户名的密码。
Plugin.AdMachineCleanup.Delete	设置为 True 时，将删除（而不是禁用）已销毁的计算机的帐户。
Plugin.AdMachineCleanup.MoveToOu	将已销毁的计算机的帐户移动到新的 Active Directory 组织单位。该值是帐户要移动到的组织单位。此值必须采用 <code>ou=OU, dc=dc</code> 格式，例如， <code>ou=trash,cn=computers,dc=lab,dc=local</code> 。
Plugin.AdMachineCleanup.RenamePrefix	通过添加前缀重命名已销毁的计算机的帐户。该值是要预置的前缀字符串，例如 <code>destroyed_</code> 。

7 单击**确定**。

结果

每次从 Hypervisor 中删除通过蓝图置备的计算机时，便会更新 Active Directory 环境。

允许请求者指定计算机主机名称

作为蓝图架构师，您需要允许用户在请求蓝图时选择其自己的计算机名称。因此，您需编辑蓝图，以添加“主机名”自定义属性并将其配置为在请求期间提示用户输入值。

注 如果架构管理员创建的属性组包含所需的自定义属性且您将该组包含在蓝图中，则无需将这些自定义属性分别添加到蓝图中。

前提条件

- 以**基础架构架构师**身份登录到 vRealize Automation。
- 创建计算机蓝图。请参见[配置计算机蓝图](#)。

步骤

- 1 选择**设计 > 蓝图**。
- 2 指向蓝图，并单击**编辑**。
- 3 选择画布上的计算机组件以打开“详细信息”选项卡。
- 4 单击**属性**选项卡。
- 5 单击**新建属性**。
- 6 在**名称**文本框中输入 **Hostname**。
- 7 将**值**文本框留空。

8 将 vRealize Automation 配置为在请求期间提示用户输入主机名值。

- a 选择**可覆盖**。
- b 选择**在请求中显示**。

由于主机名必须是唯一的，因此用户每次只能从该蓝图请求一台计算机。

9 单击**保存**图标 (✓)。

10 单击**确定**。

结果

从蓝图请求计算机的用户需要指定计算机的主机名。vRealize Automation 将验证指定的主机名是否唯一。

使用户能为跨区域部署选择数据中心位置

作为一名蓝图架构师，您需要允许用户选择是在波士顿还是伦敦的基础架构中置备计算机，因此请编辑您的蓝图以启用位置功能。



您在伦敦和波士顿分别设有一个数据中心，但不希望位于波士顿的用户在伦敦的基础架构中置备计算机，反之亦然。为了确保位于波士顿和伦敦的用户在各自的基础架构中置备计算机，您需要允许用户在请求计算机时选择适当的位置进行置备。

前提条件

- 以**基础架构架构师**身份登录到 vRealize Automation。
- 作为一名系统管理员，请定义数据中心位置。请参见[场景：为跨区域部署添加数据中心位置](#)。
- 作为一名架构管理员，请将适当的位置应用于计算资源。请参见[场景：为跨区域部署将位置应用到计算资源](#)。
- 创建计算机蓝图。请参见[配置计算机蓝图](#)。

步骤

- 1 选择**设计 > 蓝图**。
- 2 指向蓝图，并单击**编辑**。
- 3 选择画布上的计算机组件以打开**常规详细信息**选项卡。
- 4 选中**请求时显示位置**复选框。

- 5 单击**完成**。
- 6 指向蓝图，并单击**发布**。

结果

现在，请求要通过蓝图置备的计算机时，系统提示业务组用户选择数据中心位置。

设计 Software 组件

作为软件架构师，您需创建可重用的软件组件，将配置属性标准化并使用操作脚本准确指定在部署缩放操作过程中如何安装、配置、卸载或更新组件。您可以随时重新编写这些操作脚本并实时发布以将更改推送到置备的软件组件。

通过定义和使用称为软件属性的名称和值对并将其作为参数传递给操作脚本，可将操作脚本设计为通用和可重用脚本。如果软件属性中包含未知值或需要在将来定义的值，您可以要求或允许其他蓝图架构师或最终用户提供这些值。如果需要蓝图中其他组件的值，例如某台计算机的 IP 地址，则您可以将软件属性绑定到该计算机的 IP 地址属性。使用软件属性参数化操作脚本可使脚本成为通用和可重用脚本，以便您可以在不同的环境中部署软件组件，而无需修改您的脚本。

表 3-43. 生命周期操作

生命周期操作	描述
安装	安装软件。例如，您可能会下载 Tomcat 服务器安装位并安装 Tomcat 服务。为“安装”生命周期操作编写的脚本将在初始部署请求期间或执行扩大操作期间首次置备软件时运行。
配置	配置软件。以 Tomcat 为例，您可能会设置 JAVA_OPTS 和 CATALINA_OPTS。配置脚本会在安装操作完成后运行。
开始	启动软件。例如，您可能会使用 Tomcat 服务器中的启动命令启动 Tomcat 服务。启动脚本会在配置操作完成后运行。
更新	如果要使设计的软件组件支持可缩放蓝图，请处理在执行缩小或扩大操作后所需的任何更新。例如，您可能会使用负载均衡器更改已缩放的部署的群集大小以及管理群集节点。设计更新脚本以使其运行多次（幂等），并处理缩小和扩大情形。执行缩放操作后，更新脚本会在所有相关的软件组件上运行。
卸载	卸载软件。例如，您可能会在应用程序中执行特定操作，然后再销毁部署。卸载脚本会在销毁软件组件后运行。

您可以从 VMware Solution Exchange 下载各种中间件服务和应用程序的预定义的 Software 组件。使用 vRealize CloudClient 或 vRealize Automation REST API，您可以编程方式将预定义的 Software 组件导入到 vRealize Automation 实例。

- 要访问 VMware Solution Exchange，请参见 https://solutionexchange.vmware.com/store/category_groups/cloud-management。
- 有关 vRealize Automation REST API 的信息，请参见《编程指南》和 [vRealize Automation 内容服务 API](https://code.vmware.com)，网址为 <https://code.vmware.com>。
- 有关 vRealize CloudClient 的信息，请参见 <https://developercenter.vmware.com/tool/cloudclient>。

属性类型和设置选项

通过定义和使用称为软件属性的名称和值对并将其作为参数传递给操作脚本，可将操作脚本设计为通用和可重用脚本。可以创建要求使用字符串、数组、内容、布尔或整数值的软件属性。可以自己提供值，也可以要求其他人提供值，或者通过创建绑定来从其他蓝图组件检索值。

属性选项

您可以通过选中“计算”复选框来计算任何字符串属性的值；配置 **Software** 属性时，可以通过选中相应的复选框将任何属性设置为“已加密”、“可覆盖”或“必需”。将这些选项与值结合使用可实现不同的目的。例如，您要求蓝图架构师提供一个密码值，然后在蓝图中使用您的软件组件时对该值进行加密。创建密码属性，但将值文本框留空。选择“可覆盖”、“必需”和“已加密”。如果您所需的密码属于最终用户，则蓝图架构师可以选择**在请求中显示**以要求您的用户在填写请求表单时输入密码。

选项	描述
加密	将属性标记为加密以屏蔽值，并在 vRealize Automation 中显示为星号。如果将属性从加密更改为未加密，vRealize Automation 将重置属性值。出于安全考虑，必须为此属性设置新值。
可覆盖	当架构师组合应用程序蓝图时，允许他们编辑此属性的值。如果输入值，它将作为默认值显示。
必需	要求架构师为此属性提供一个值，或者接受您提供的默认值。
计算	计算属性的值由 INSTALL 、 CONFIGURE 、 START 或 UPDATE 生命周期脚本分配。分配的值会传播到后续可用生命周期阶段和绑定到蓝图中的这些属性的组件。如果选择“计算”作为非字符串属性，则属性类型将更改为字符串。

如果选择“计算”属性选项，请将自定义属性值留空。为计算的属性设计脚本。

表 3-44. 计算属性选项的脚本示例

字符串属性示例	脚本语法	使用示例
my_unique_id = ""	Bash - \$my_unique_id	<pre>export my_unique_id="0123456789"</pre>
	Windows CMD - %my_unique_id%	<pre>set my_unique_id=0123456789</pre>
	Windows PowerShell - \$my_unique_id	<pre>\$my_unique_id = "0123456789"</pre>

字符串属性

字符串属性要求使用字符串值。可以自己提供字符串，也可以要求其他人提供该值，或者通过创建与其他字符串属性的绑定来从其他蓝图组件检索值。字符串值可以包含任何 **ASCII** 字符。要创建属性绑定，请使用设计画布中的**属性**选项卡来选择要绑定的适当属性。属性值随后则会作为原始字符串数据传递到操作脚本。在绑定到蓝图字符串属性时，请确保要绑定到的蓝图组件不可加入群集。如果该组件已加入群集，则该字符串值将成为一个数组，您将无法检索所需的值。

字符串属性示例	脚本语法	使用示例
admin_email = "admin@email987.com"	Bash - \$admin_email	echo \$admin_email
	Windows CMD - %admin_email%	echo %admin_email%
	Windows PowerShell - \$admin_email	write-output \$admin_email

数组属性

数组属性要求使用以 [“value1”、“value2”、“value3”...] 形式定义的字符串、整数、十进制或布尔值数组。可以自己提供值，也可以要求其他人提供值，或者通过创建属性绑定来从其他蓝图组件检索值。

创建数组类型的软件属性时（数据类型为整数或小数），不管区域设置如何，都必须使用分号作为数组元素分隔符。请勿使用逗号 (,) 或点 (.)。对于某些区域设置，您可以使用逗号 (,) 作为十进制分隔符。例如：

- 法语区域设置的有效数组类似于：[1,11;2,22;3,33]
- 英语区域设置的有效数组类似于：[1.11,2.22,3.33]

将大量数字传递到数组时，请勿使用分组格式。例如：请勿使用 **4444 444.000**（法语）、**4.444.444,000**（意大利语）或 **4,444,444.000**（英语），因为包含区域设置特定格式的数据文件在传输到区域设置不同的计算机时，可能会解释错误。不允许使用分组格式，因为诸如 **4,444,444.000** 的数字将视为三个不同的数字。改为仅输入 **4444444.000**。

定义数组属性的值时，必须将数组用方括号括起来。对于字符串数组，数组元素中的值可以包含任何 **ASCII** 字符。要在数组属性值中正确编码反斜线字符，请再添加一个反斜线，例如 ["c:\\test1\\test2"]。对于绑定属性，使用设计画布中的**属性**选项卡选择相应的属性进行绑定。如果要绑定到数组，您必须对软件组件进行设计，使其不要求值数组遵循任何特定的顺序。

例如，假设某个负载均衡器虚拟机正在平衡一个应用程序服务器虚拟机群集的负载。在这种情况下，可为负载均衡器服务定义一个数组属性，并将该属性设置为应用程序服务器虚拟机的 IP 地址数组。

这些负载均衡器服务配置脚本将使用该数组属性在 Red Hat、Windows 和 Ubuntu 操作系统上配置相应的负载均衡方案。

数组属性示例	脚本语法	使用示例
operating_systems = ["Red Hat","Windows","Ubuntu"]	Bash - \${operating_systems[@]} 用于整个字符串数组 \${operating_systems[N]} 用于单个数组元素	<pre>for ((i = 0 ; i < \$ {#operating_systems[@]}; i++)); do echo \${operating_systems[\$i]} done</pre>
	Windows CMD - %operating_systems_% 其中 <i>N</i> 表示元素在数组中的位置	<pre>for /F "delims== tokens=2" %%A in ('set operating_systems_') do (echo %%A)</pre>
	Windows PowerShell - \$operating_systems 用于整个字符串数组 \$operating_systems[N] 用于单个数组元素	<pre>foreach (\$os in \$operating_systems){ write-output \$os }</pre>

内容属性

内容属性值是要下载内容的文件的 URL。Software 代理将从 URL 将内容下载到虚拟机并将虚拟机中本地文件的位置传递到脚本。

必须将内容属性定义为使用 HTTP 或 HTTPS 协议的有效 URL。例如，Dukes Bank 示例应用程序中的 JBOSS 应用程序服务器 Software 组件指定内容属性 cheetah_tgz_url。这些项目托管在 Software 设备中，并且 URL 指向设备中的该位置。Software 代理将从指定的位置将项目下载到部署的虚拟机中。

有关可用于内容属性的 software.http.proxy 设置的信息，请参见《自定义属性参考》。

字符串属性示例	脚本语法	使用示例
cheetah_tgz_url = "http:// app_content_server_ip:port/artifacts/ software/jboss/cheetah-2.4.4.tar.gz"	Bash - \$cheetah_tgz_url	tar -zxvf \$cheetah_tgz_url
	Windows CMD - %cheetah_tgz_url%	start /wait c:\unzip.exe %cheetah_tgz_url%
	Windows PowerShell - \$cheetah_tgz_url	& c:\unzip.exe \$cheetah_tgz_url

布尔属性

使用布尔属性类型在“值”下拉菜单中提供 True 和 False 这两个选项。

整数属性

对零以及正整数或负整数使用整数属性类型。

十进制属性

对表示非重复十进制小数的值使用十进制属性类型。

当您的 Software 组件需要其他组件中的信息时

在一些部署方案中，组件需要其他组件的属性值以对其自身进行自定义。通过创建属性绑定，可以在 vRealize Automation 中实现此目的。您可以为属性绑定设计 Software 操作脚本，但实际绑定是由组合蓝图的架构师配置。

除了将属性设置为硬编码值外，软件架构师、IaaS 架构师或应用程序架构师还可以将 Software 组件属性绑定到蓝图中的其他属性，例如，IP 地址或安装位置。将 Software 属性绑定到其他属性时，可以基于其他组件属性或虚拟机属性的值自定义脚本。例如，WAR 组件可能需要 Apache Tomcat 服务器的安装位置。在脚本中，可以对 WAR 组件进行配置，使其在脚本中将 server_home 属性值设置为 Apache Tomcat 服务器的 install_path 属性值。只要组合蓝图的架构师将 server_home 属性绑定到 Apache Tomcat 服务器的 install_path 属性，系统便会正确设置 server_home 属性值。

您的操作脚本仅可使用这些脚本中定义的属性，且您仅可使用字符串和阵列值创建属性绑定。蓝图属性阵列不以任何特定顺序返回，因此绑定到可群集或可缩放的组件可能不会产生预期的值。例如，您的软件组件需要计算机群集的所有计算机 ID，而您允许用户请求 1-10 的群集，并从 1-10 台计算机缩放部署。如果您将软件属性配置为字符串类型，将会从群集获得单个随机选择的计算机 ID。如果您将软件属性配置为阵列类型，将会获得群集中所有计算机 ID 的阵列，但无特定顺序。如果您的用户缩放部署，则每个操作的值的顺序可能不同。为了确保永远不会丢失群集组件的值，您可以为任何软件属性使用阵列类型。但是，您必须设计自己的软件组件，以便不会出现以任何特定顺序排列的值阵列。

绑定到不同类型的属性时，请参见“字符串属性绑定示例”表，了解字符串属性值的示例。

表 3-45. 字符串属性绑定示例

属性类型示例	可绑定属性类型	绑定结果（A 绑定到 B）
字符串（属性 A）	字符串（属性 B="Hi"）	A="Hi"
字符串（属性 A）	内容（属性 B="http://my.com/content"）	A="http://my.com/content"
字符串（属性 A）	数组（属性 B=["1","2"]）	A=["1","2"]
字符串（属性 A）	计算（属性 B="Hello"）	A="Hello"

绑定到不同类型的属性时，请参见“数组属性绑定示例”表，了解数组属性值的示例。

表 3-46. 数组属性绑定示例

属性类型示例	可绑定属性类型	绑定结果（A 绑定到 B）
数组（属性 A）	字符串（属性 B="Hi"）	A="Hi"
数组（属性 A）	内容（属性 B="http://my.com/content"）	A="http://my.com/content"
数组（属性 A）	计算（属性 B="Hello"）	A="Hello"

有关支持的属性类型的详细说明，请参见[属性类型和设置选项](#)。

在生命周期各阶段之间传递属性值

您可以修改属性值并使用操作脚本在生命周期各阶段之间进行传递。

对于计算属性，您可以修改属性值并将该值传递到操作脚本的下一个生命周期阶段。例如，如果组件 A 的 `progress_status` 值定义为 `staged`，则您应在 `INSTALL` 和 `CONFIGURE` 生命周期阶段的相应操作脚本中，将该值更改为 `progress_status=installed`。如果组件 B 绑定到组件 A，则操作脚本的生命周期阶段中的 `progress_status` 属性值与组件 A 相同。

在软件组件中定义组件 B 依赖于 A。这种依赖关系可定义在这两个组件之间传递正确的属性值，无论它们位于同一节点中还是跨不同节点。

例如，您可以使用支持的脚本更新操作脚本中的属性值。

- `Bash progress_status="completed"`
- `Windows CMD set progress_status=completed`
- `Windows PowerShell $progress_status="completed"`

注 数组和内容属性不支持在生命周期阶段的操作脚本之间传递已修改的属性值。

开发组件的最佳做法

要熟悉定义属性和操作脚本的最佳做法，您可以从 VMware Solution Exchange 下载并导入 Software 组件和应用程序蓝图。

开发 Software 组件时，请遵循以下最佳做法。

- 为了使脚本无中断地运行，必须将返回值设置为零 (0)。此设置允许代理捕获所有属性并将其发送到 Software 服务器。
- 一些安装程序可能需要访问 `tty` 控制台。从 `/dev/console` 重定向输入。例如，RabbitMQ Software 组件可以使用其安装脚本中的 `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console` 命令。
- 如果组件使用多个生命周期阶段，可以在 `INSTALL` 生命周期阶段中更改属性值。新值将发送到下一个生命周期阶段。操作脚本可以在部署过程中计算属性值，以便将该值提供给其他从属脚本。例如，在群集化的 Dukes Bank 示例应用程序中，JBossAppServer 服务将在安装生命周期阶段的过程中计算 `JVM_ROUTE` 属性。JBossAppServer 服务使用此属性配置生命周期。然后，Apache 负载均衡器服务会将其 `JVM_ROUTE` 属性绑定到 `all(appserver:JbossAppServer:JVM_ROUTE)` 属性以获取 `node0` 和 `node1` 的最终计算值。如果某一组件需要使用另一个组件的属性值才能成功完成应用程序部署，则必须在应用程序蓝图中声明这些明确的依赖关系。

注 对于使用多个生命周期阶段的组件，无法更改其内容属性值。

创建 Software 组件

配置并发布可供其他软件架构师、IaaS 架构师以及应用程序架构师组合应用程序蓝图的 Software 组件。

前提条件

以软件架构师身份登录到 vRealize Automation。

步骤

1 选择**设计 > 软件组件**。

2 单击**添加图标 (+)**。

3 输入名称和可选描述。

使用您为 **Software** 组件指定的名称，vRealize Automation 将在租户内为 **Software** 组件创建一个唯一 ID。您现在可以编辑此字段，但保存蓝图之后无法更改此字段。由于 ID 在租户内是永久且唯一的，因此，您可以使用它们以编程方式与蓝图进行交互并创建属性绑定。

4 （可选）如果要控制将 **Software** 组件包括在蓝图中的方式，请从**容器**下拉菜单中选择容器类型。

选项	描述
计算机	Software 组件必须直接放置在计算机上。
已发布的 Software 组件之一	如果您专门将 Software 组件设计为安装在您创建的其他 Software 组件上，请从列表中选择该 Software 组件。例如，如果要安装 EAR 组件设计为安装在您以前创建的 JBOSS 组件上，请从列表中选择 JBOSS 组件。
软件组件	如果要设计不应直接安装在计算机上、但可安装在多个不同 Software 组件上的 Software 组件，请选择“软件组件”选项。例如，如果要设计 WAR 组件并希望将其安装在 Tomcat Server Software 组件和 Tcserver Software 组件上，请选择“软件组件”容器类型。

5 单击**下一步**。

6 定义要在操作脚本中使用的任何属性。

a 单击**添加图标 (+)**。

b 输入属性名称。

c 输入属性描述。

此描述将显示给使用蓝图中的 **Software** 组件的架构师。

- d 选择属性值的预期类型。
- e 定义属性值。

选项	描述
立即使用提供的值	<ul style="list-style-type: none"> ■ 输入值。 ■ 取消选择可覆盖。 ■ 选择必需。
要求架构师提供值	<ul style="list-style-type: none"> ■ 要提供默认值，请输入一个值。 ■ 选择可覆盖。 ■ 选择必需。
允许架构师根据需要提供值	<ul style="list-style-type: none"> ■ 要提供默认值，请输入一个值。 ■ 选择可覆盖。 ■ 取消选择必需。

架构师可以将 **Software** 属性配置为在请求表单中显示给用户。架构师可以使用“在请求中显示”选项，要求或请求用户填写您标记为“可覆盖”的属性的值。

- 7 按照提示至少为一个软件生命周期操作提供脚本。

表 3-47. 生命周期操作

生命周期操作	描述
安装	安装软件。例如，您可能会下载 Tomcat 服务器安装位并安装 Tomcat 服务。为“安装”生命周期操作编写的脚本将在初始部署请求期间或执行扩大操作期间首次置备软件时运行。
配置	配置软件。以 Tomcat 为例，您可能会设置 JAVA_OPTS 和 CATALINA_OPTS。配置脚本会在安装操作完成后运行。
开始	启动软件。例如，您可能会使用 Tomcat 服务器中的启动命令启动 Tomcat 服务。启动脚本会在配置操作完成后运行。
更新	如果要使设计的软件组件支持可缩放蓝图，请处理在执行缩小或扩大操作后所需的任何更新。例如，您可能会使用负载均衡器更改已缩放的部署的群集大小以及管理群集节点。设计更新脚本以使其运行多次（幂等），并处理缩小和扩大情形。执行缩放操作后，更新脚本会在所有相关的软件组件上运行。
卸载	卸载软件。例如，您可能会在应用程序中执行特定操作，然后再销毁部署。卸载脚本会在销毁软件组件后运行。

在操作脚本中包括退出和状态代码。支持的每种脚本类型均具有唯一的退出和状态代码要求。

脚本类型	成功状态	错误状态	不支持的命令
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	无
Windows CMD	exit /b 0	exit /b non-zero	请勿使用 exit 0 或 exit non-zero 代码。
PowerShell	exit 0	exit non-zero;	请勿使用 warning、verbose、debug 或 host 调用。

- 8 对于需要重新引导计算机的所有脚本，选中**重新引导**复选框。

脚本运行后，计算机将在启动下一个生命周期脚本之前先重新引导。

9 单击**完成**。

10 选择 **Software** 组件并单击**发布**。

结果

您已配置并发布 **Software** 组件。其他软件架构师、IaaS 架构师和应用程序架构师可以使用此 **Software** 组件将软件添加到应用程序蓝图。

后续步骤

将已发布的 **Software** 组件添加到应用程序蓝图。请参见[组合复合蓝图](#)。

Software 组件设置

为安装、配置、更新或卸载已置备计算机中的 **Software** 组件，配置常规设置，创建属性，并编写自定义操作脚本。

作为软件架构师，单击**设计 > 软件组件**，然后单击**添加**图标创建新的 **Software** 组件。

新建 Software 常规设置

将常规设置应用于 **Software** 组件。

表 3-48. 新建 Software 常规设置

设置	描述
名称	输入 Software 组件的名称。
ID	使用您为 Software 组件指定的名称，vRealize Automation 将在租户内为 Software 组件创建一个唯一 ID。您现在可以编辑此字段，但保存蓝图之后无法更改此字段。由于 ID 在租户内是永久且唯一的，因此，您可以使用它们以编程方式与蓝图进行交互并创建属性绑定。
描述	为方便其他架构师使用，概述 Software 组件。
容器	<p>在设计画布中，蓝图架构师只能将 Software 组件置于您选择的容器类型中。</p> <ul style="list-style-type: none"> ■ 选择计算机，以要求架构师将 Software 组件直接置于设计画布中的计算机组件上。 ■ 如果要设计的 Software 组件不应直接置于计算机组件中，但可以嵌套在一个不同的 Software 组件中，请选择软件组件。 ■ 如果要专门设计一个 Software 组件以嵌套在您创建的另一个 Software 组件中，请选择一个已发布的特定 Software 组件。 ■ 如果要专门为 Azure 蓝图设计一个 Software 组件，请选择 Azure 虚拟机。

新建 Software 属性

Software 组件属性用于参数化脚本，以便可以将定义的属性作为环境变量传递到在虚拟机中运行的脚本。运行脚本之前，已置备计算机中的 Software 代理将与 vRealize Automation 进行通信以解析属性。随后，该代理通过这些属性创建脚本特定的变量并将其传递到脚本。

表 3-49. 新建 Software 属性

设置	描述
名称	输入 Software 属性的名称。属性名称区分大小写并且只能包含字母、数字、连字符 (-) 或下划线 (_) 字符。
描述	为方便其他用户使用，概述属性和值的任何要求。
类型	Software 支持字符串、数组、内容、布尔和整数类型。有关支持的属性类型的详细说明，请参见 属性类型和设置选项 。有关属性绑定的信息，请参见 当您的 Software 组件需要其他组件中的信息时和在蓝图组件之间创建属性绑定 。
值	<ul style="list-style-type: none"> ■ 要使用您提供的值，请执行以下操作： <ul style="list-style-type: none"> ■ 输入值。 ■ 选择必需。 ■ 取消选择可覆盖。 ■ 如要求架构师提供值，请执行以下操作： <ul style="list-style-type: none"> ■ （可选）输入值以提供默认值。 ■ 选择可覆盖。 ■ 选择必需。 ■ 允许架构师提供一个值，或将此值留空： <ul style="list-style-type: none"> ■ （可选）输入值以提供默认值。 ■ 选择可覆盖。 ■ 取消选择必需。
加密	<p>将属性标记为加密以屏蔽值，并在 vRealize Automation 中显示为星号。如果将属性从加密更改为未加密，vRealize Automation 将重置属性值。出于安全考虑，必须为此属性设置新值。</p> <p>重要事项 如果在脚本中使用 echo 命令或其他类似命令打印安全属性，则这些值会以纯文本的形式显示在日志文件中。日志文件中的这些值不会被屏蔽。</p>
可覆盖	当架构师组合应用程序蓝图时，允许他们编辑此属性的值。如果输入值，它将作为默认值显示。
必需	要求架构师为此属性提供一个值，或者接受您提供的默认值。
计算	计算属性的值由 INSTALL 、 CONFIGURE 、 START 或 UPDATE 生命周期脚本分配。分配的值会传播到后续可用生命周期阶段和绑定到蓝图中的这些属性的组件。如果选择“计算”作为非字符串属性，则属性类型将更改为字符串。

新建 Software 操作

创建 Bash、Windows CMD 或 PowerShell 操作脚本，以准确指定在部署缩放操作期间如何安装、配置、卸载或更新组件。

表 3-50. 生命周期操作

生命周期操作	描述
安装	安装软件。例如，您可能会下载 Tomcat 服务器安装位并安装 Tomcat 服务。为“安装”生命周期操作编写的脚本将在初始部署请求期间或执行扩大操作期间首次置备软件时运行。
配置	配置软件。以 Tomcat 为例，您可能会设置 JAVA_OPTS 和 CATALINA_OPTS。配置脚本会在安装操作完成后运行。
开始	启动软件。例如，您可能会使用 Tomcat 服务器中的启动命令启动 Tomcat 服务。启动脚本会在配置操作完成后运行。
更新	如果要使设计的软件组件支持可缩放蓝图，请处理在执行缩小或扩大操作后所需的任何更新。例如，您可能会使用负载均衡器更改已缩放的部署的群集大小以及管理群集节点。设计更新脚本以使其运行多次（幂等），并处理缩小和扩大情形。执行缩放操作后，更新脚本会在所有相关的软件组件上运行。
卸载	卸载软件。例如，您可能会在应用程序中执行特定操作，然后再销毁部署。卸载脚本会在销毁软件组件后运行。

对于需要重新引导计算机的所有脚本，选中**重新引导**复选框。脚本运行后，计算机将在启动下一个生命周期脚本之前先重新引导。确认操作脚本运行期间不提示任何需要用户交互的进程。中断会暂停脚本，导致其无限期处于闲置状态，并最终失败。另外，您的脚本还必须包括适用于应用程序部署的适当退出代码。如果脚本缺少退出代码和返回代码，则脚本中运行的最后一个命令会变为退出状态。退出代码和返回代码会因 Bash、Windows CMD、PowerShell 等不同的受支持脚本类型而异。

脚本类型	成功状态	错误状态	不支持的命令
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	无
Windows CMD	exit /b 0	exit /b non-zero	请勿使用 exit 0 或 exit non-zero 代码。
PowerShell	exit 0	exit non-zero;	请勿使用 warning、verbose、debug 或 host 调用。

设计 XaaS 蓝图和资源操作

XaaS 蓝图既可以作为目录项发布，也可以在蓝图设计画布中使用。资源操作是在已部署的项目上运行的操作。

XaaS 使用 vRealize Orchestrator 运行置备项目的工作流或运行操作。例如，您可以将工作流配置为创建 vSphere 虚拟机、组中的 Active Directory 用户或运行 PowerShell 脚本。如果创建自定义 vRealize Orchestrator 工作流，则可在服务目录中将该工作流作为项目提供，以便授权用户可以运行该工作流。

您既可以将 XaaS 蓝图用作在设计画布中所创建蓝图的组件，也可以直接将其发布到服务目录。

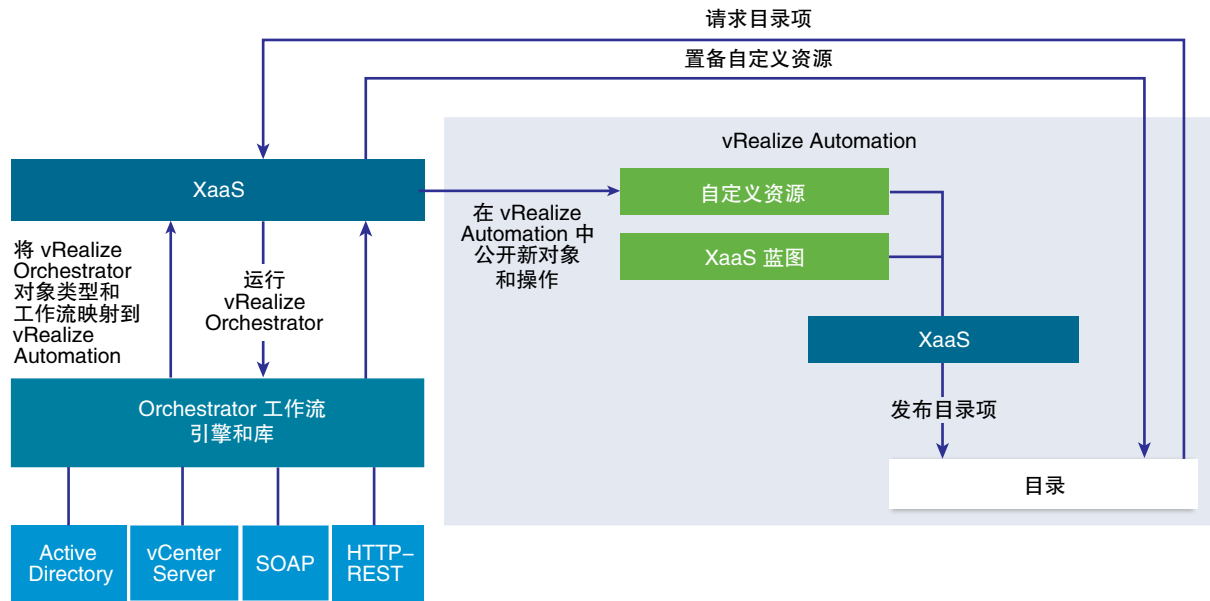
如果将某个蓝图用作其他蓝图中的组件，则可将其配置为在部署的蓝图缩小或放大时进行缩放。

vRealize Orchestrator 集成至 vRealize Automation

vRealize Orchestrator 是集成至 vRealize Automation 中的工作流引擎。

随 vRealize Automation 分发的 vRealize Orchestrator 服务器已预配置。因此，当系统管理员部署 vRealize Automation Appliance 后，vRealize Orchestrator 服务器便已启动且正在运行。

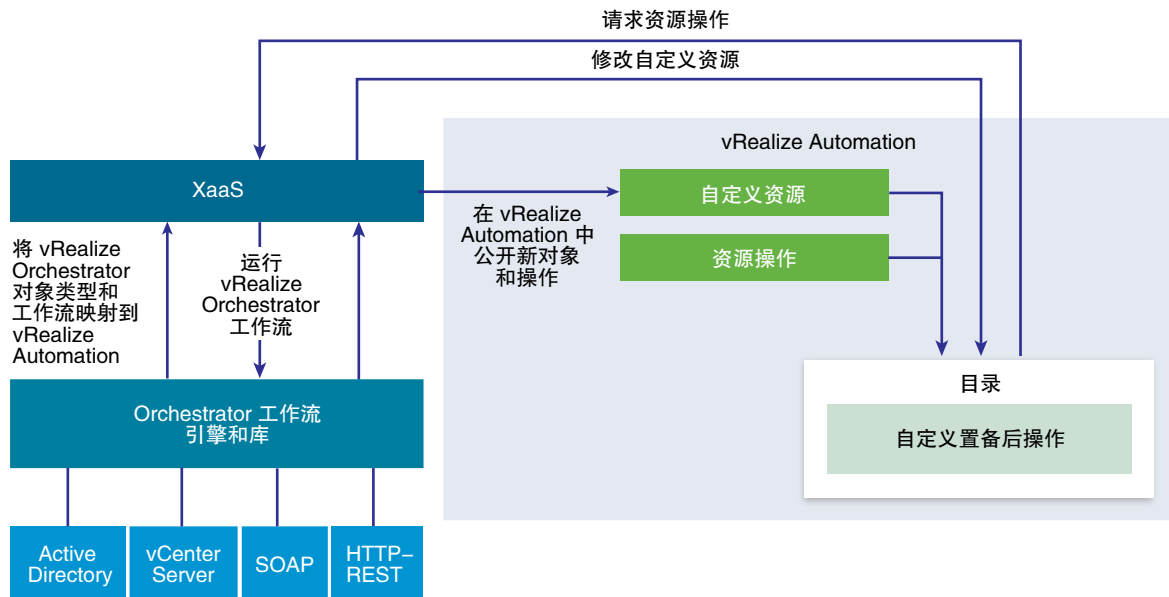
图 3-2. 创建并请求 XaaS 中包括的目录项以置备自定义资源



XaaS 架构师添加与受支持的端点和提供的工作流相关的自定义资源，然后根据这些资源创建 XaaS 蓝图和操作。租户管理员和业务组主管可以将 XaaS 蓝图和操作添加到服务目录。XaaS 蓝图也可在蓝图设计器中使用。

当服务目录用户请求项目时，vRealize Automation 将运行 vRealize Orchestrator 工作流以置备自定义资源。

图 3-3. 创建并请求自定义资源操作以修改自定义资源



XaaS 架构师也可将 vRealize Orchestrator 工作流添加为资源操作，以扩展 vRealize Automation 功能。服务目录用户置备自定义资源之后，可以运行置备后操作。通过这种方式，使用者可运行 vRealize Orchestrator 工作流，并修改已置备的自定义资源。

当服务目录用户请求将 XaaS 蓝图或资源操作作为目录项时，XaaS 服务会运行对应的 vRealize Orchestrator 工作流，将以下数据作为全局参数传递给该工作流：

表 3-51. XaaS 全局参数

参数	描述
__asd_tenantRef	请求工作流的用户的租户。
__asd_subtenantRef	请求工作流的用户的业务组。
__asd_catalogRequestId	目录中为运行此工作流而分配的请求 ID。
__asd_requestedFor	请求的目标用户。如果代表某位用户提出请求，则被代表用户便是请求工作流的用户，否则是请求工作流的用户本人。
__asd_requestedBy	请求工作流的用户。

如果 XaaS 蓝图或资源操作使用的 vRealize Orchestrator 工作流包含用户交互方案元素，则当使用者请求服务时，该工作流的运行将挂起，并等待用户提供所需的数据。要应答处于等待状态的用户交互，用户必须导航到**收件箱 > 手动用户操作**。

vRealize Orchestrator 服务器默认清单由所有租户共享，不能按租户使用。例如，如果服务架构师为创建群集计算资源而创建了一个服务蓝图，则来自不同租户的使用者必须浏览所有 vCenter Server 实例的清单项目（尽管这些项目可能属于不同的租户）。

系统管理员可以单独安装 vRealize Orchestrator 或部署 vRealize Orchestrator Appliance 以设置外部 vRealize Orchestrator 实例，并配置 vRealize Automation 使用该外部 vRealize Orchestrator 实例。

系统管理员也可以按租户配置 vRealize Orchestrator 工作流类别，并定义每个租户可使用哪些工作流。

此外，租户管理员还可以配置仅供其自身租户使用的外部 vRealize Orchestrator 实例。

有关配置外部 vRealize Orchestrator 实例和 vRealize Orchestrator 工作流类别的信息，请参见《配置 vCenter Orchestrator 和插件》。

vRealize Orchestrator 插件列表

利用插件，您可以使用 vRealize Orchestrator 访问并控制外部技术和应用程序。通过在 vRealize Orchestrator 插件中公开外部技术，您可以将对象和功能入工作流，用于访问外部技术的对象和函数。

通过使用插件，您可访问的外部技术可能包含虚拟化管理工具、电子邮件系统、数据库、目录服务、远程控制接口等。

您可以使用一组标准的 vRealize Orchestrator 插件将 vCenter Server API 和电子邮件功能等外部技术纳入工作流。此外，还可以使用 vRealize Orchestrator 开放式插件架构，开发用于访问其他应用程序的插件。

表 3-52. vRealize Orchestrator 中默认包括的插件

插件	用途
vCenter Server	提供 vCenter Server API 的访问权限，使您能够将所有 vCenter Server 对象和功能纳入通过使用 vRealize Orchestrator 自动执行的管理流程。
配置	提供用于配置 vRealize Orchestrator 身份验证、数据库连接、SSL 证书等的工作流。
vCO 库	为客户端流程的自定义和自动化提供充当基本构建块的工作流。工作流库包括用于生命周期管理、置备、灾难恢复、热备份以及其他标准流程的模板。您可以复制和编辑这些模板，根据需要对其进行修改。
SQL	提供 Java 数据库连接 (JDBC) API，它是一种专为 Java 编程语言和各种数据库之间的连接建立的行业标准，这些连接与所使用的数据库无关。这些数据库包括 SQL 数据库以及其他表格数据源，例如电子表格或平面文件。JDBC API 提供了调用级 API，以便从工作流访问基于 SQL 的数据库。
SSH	支持实现安全 Shell v2 (SSH-2) 协议。允许在工作流中采用基于密码和公钥的身份验证运行远程命令和文件传输会话。支持键盘交互式身份验证。（可选）SSH 插件可以支持在 vRealize Orchestrator 客户端清单中直接浏览远程文件系统。
XML	一种可在工作流中实施的完整文档对象模型 (DOM) XML 分析程序。或者，您也可以使用 vRealize Orchestrator JavaScript API 中使用 ECMAScript for XML (E4X) 实施。
Mail	使用简单邮件传输协议 (SMTP) 从工作流发送电子邮件。
Net	包装 Jakarta Apache Commons Net 库。支持实现 Telnet、FTP、POP3 和 IMAP。POP3 和 IMAP 部分用于读取电子邮件。Net 插件与 Mail 插件结合使用，在工作流中提供完整的电子邮件收发功能。
枚举	提供其他插件可在工作流中使用的常见枚举类型。
工作流文档	提供一些工作流，支持您以 PDF 格式生成工作流或工作流类别的相关信息。
HTTP-REST	通过提供 vCenter Orchestrator 与 REST 主机之间的交互，使您可以管理 REST Web 服务。
SOAP	通过提供 vCenter Orchestrator 与 SOAP 主机之间的交互，使您可以管理 SOAP Web 服务。
AMQP	允许您与高级消息队列协议 (Advanced Message Queuing Protocol, AMQP) 服务器（也称为“代理”）进行交互。
SNMP	使 vCenter Orchestrator 能够连接到已启用 SNMP 的系统和设备，并从中接收信息。
Active Directory	提供 vCenter Orchestrator 与 Microsoft Active Directory 之间的交互。
vCO WebOperator	一个 Web 视图，允许您通过网络使用 Web 浏览器访问 vRealize Orchestrator 库中的工作流并与其进行交互。
动态类型	允许您定义动态类型并创建和使用这些动态类型的对象。
PowerShell	用于管理 PowerShell 主机并运行自定义 PowerShell 操作。

表 3-52. vRealize Orchestrator 中默认包括的插件（续）

插件	用途
多节点	包含用于分层编排、管理 Orchestrator 实例和扩展 Orchestrator 活动的工作流。
vRealize Automation	支持您创建并运行工作流，以便在 vRealize Orchestrator 与 vRealize Automation 之间进行交互。

有关 VMware 开发和分发的 vRealize Orchestrator 插件的详细信息，请参见 VMware vRealize™ Orchestrator™ 文档登录页面。

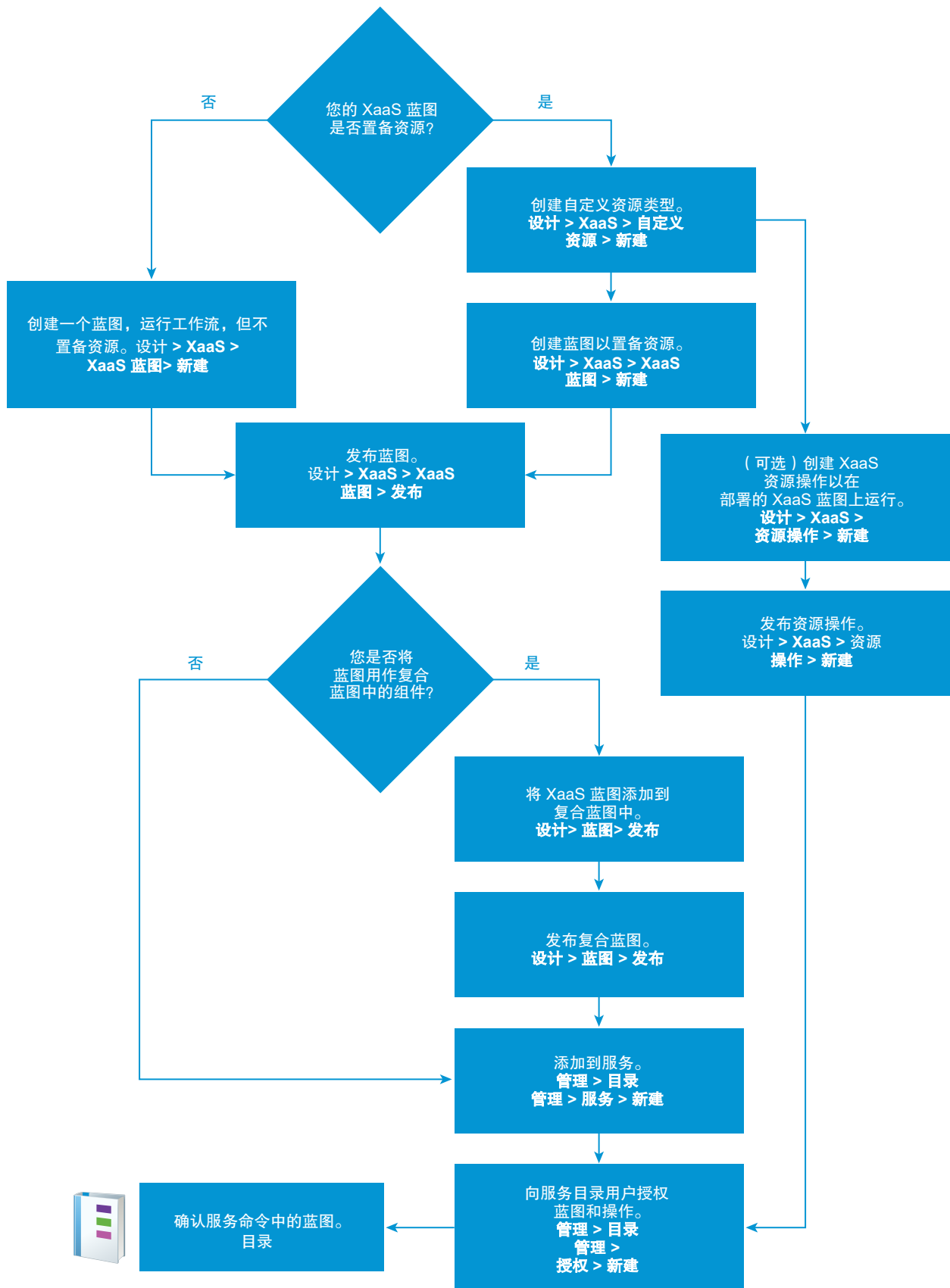
创建 XaaS 蓝图和资源操作

XaaS 蓝图既可以作为目录项授权给用户，也可以使用设计画布组合到复合蓝图中。资源操作在已置备的项目上运行，用于管理置备后的项目。

例如，您可以使用 XaaS 蓝图在组中创建 Active Directory 用户。然后，可以使用资源操作要求用户更改密码。

XaaS 蓝图工作流

您在创建 XaaS 蓝图以及任何可选资源操作时遵循的工作流因该蓝图的预期使用方法而异。以下工作流说明了基本过程。



XaaS 蓝图术语

XaaS 蓝图是 vRealize Orchestrator 工作流，这些工作流可以置备资源以及对已置备资源进行更改，或者可以像在环境中执行任务的服务一样工作。蓝图和资源操作存在几处细微差别，在为服务目录用户设计蓝图时，您必须了解这些差别。

以下定义可帮助您了解在处理 XaaS 蓝图时使用的术语。

自定义资源

vRealize Orchestrator 对象类型通过 vRealize Orchestrator 插件的 API 公开为资源。您可以创建自定义资源，以定义 XaaS 置备蓝图的输出参数和资源操作的输入参数。

XaaS 蓝图组件

可在蓝图设计画布中使用的置备蓝图或无置备蓝图。此蓝图还可以是独立 XaaS 蓝图。

独立 XaaS 蓝图

已发布并直接授权给服务目录的置备蓝图或无置备蓝图。

置备蓝图

置备蓝图将运行 vRealize Orchestrator 工作流，以使用适用于目标端点的 vRealize Orchestrator 插件 API 在该端点上置备资源。例如，将虚拟网卡添加到 vSphere 中的网络设备。要创建置备蓝图，您必须具有用于定义 vRealize Orchestrator 资源类型的自定义资源。

当服务目录用户请求此类型的目录项时，工作流会置备该项，并且已部署的项会存储在**部署**选项卡上。可为此类型的已置备资源定义置备后操作。还可以使蓝图变为可扩展，即根据需要添加或移除实例。

无置备蓝图

无置备蓝图将运行 vRealize Orchestrator 工作流以执行不要求 API 对端点进行更改的任务。例如，所运行的工作流将生成报告，然后通过电子邮件发送该报告或将其发布到目标通信系统。

当服务目录用户请求此类型的目录项时，工作流会运行以执行脚本任务，但该项不会添加到**部署**选项卡上。无法对此类型的蓝图执行置备后操作。可以使用无置备蓝图作为可扩展蓝图中的支持工作流。例如，您可以创建用于更新高可用性负载平衡器的蓝图。

复合蓝图

使用设计画布创建的蓝图。复合蓝图使用一个或多个组件。例如，一个计算机组件和一个软件组件或一个 XaaS 组件。将该蓝图添加到服务之后，它会作为部署列出。将该蓝图添加到授权以使其对服务目录用户可用之后，它会作为复合蓝图列出。复合蓝图可以包含一个蓝图组件，也可以包含整个应用程序（具有多个计算机、软件和网络）。

资源操作

可对已部署的置备蓝图运行的工作流。已部署的蓝图可以是 XaaS 蓝图或蓝图组件，也可以是映射到 vRealize Orchestrator 资源类型的计算机类型。

XaaS 蓝图设计注意事项

创建 XaaS 蓝图之前，您必须先了解蓝图的用途，以确保所创建的蓝图能够正确置备资源。

您可以创建 XaaS 蓝图并将其用作设计画布中的蓝图组件，也可以将其用作独立蓝图。蓝图可以是置备蓝图或无置备蓝图。

表 3-53. XaaS 蓝图类型和结果

XaaS 蓝图类型	是否需要自定义资源?	蓝图在部署中是否可扩展?	能否对已部署的蓝图运行资源操作?
将置备资源的蓝图组件	是	是。 如果将蓝图配置为可扩展，则该蓝图会随部署一起扩展。	是。 该蓝图会随部署一起扩展，并且您可以对已部署的组件执行其他资源操作。 蓝图组件会显示在“部署”选项卡上。
将运行工作流但不置备资源的蓝图组件	否。 该蓝图使用 vRealize Orchestrator 服务器配置，但不需要 XaaS 自定义资源。	否。 该蓝图不会置备资源，但在扩展操作中运行。 例如，根据扩展操作使用新配置更新负载均衡器。	否。 无法对无置备组件运行资源操作。
将置备资源的独立蓝图	是	否。 必须创建资源操作才能添加或销毁实例。	是。 可以对已部署的资源运行资源操作，包括已创建用于支持扩展的任何操作。 蓝图会显示在“部署”选项卡上。
将运行工作流但不置备资源的独立蓝图	否。 该蓝图使用 vRealize Orchestrator 服务器配置，但不需要 XaaS 自定义资源。	否。 该蓝图不会置备资源，但在资源操作中运行。	否。 无法对无置备组件运行资源操作。

添加 XaaS 自定义资源

您可创建自定义资源以定义用于置备的 XaaS 项目。在创建 XaaS 蓝图或操作之前，您必须拥有与蓝图或操作工作流的对象类型兼容的自定义资源。

创建自定义资源之后，您可以将通过 vRealize Orchestrator 插件的 API 公开的对象类型映射为资源。该自定义资源可为置备定义 XaaS 蓝图的输出参数，并定义资源操作的输入参数。

如果蓝图或资源操作工作流未置备资源或未在部署的蓝图上运行，则无需创建自定义资源。例如，如果工作流在置备操作后更新数据库值或发送电子邮件，则不需要自定义资源。

在创建自定义资源时，您可以指定已置备项目的只读详细信息表单的字段。请参见[设计自定义资源表单](#)。

前提条件

- 以 **XaaS 架构师** 身份登录到 vRealize Automation。
- 使用详细的选项信息配置该自定义资源。请参见 [XaaS “自定义资源” 向导选项](#)。

步骤

1 选择 **设计 > XaaS > 自定义资源**。

2 单击 **新建** 图标 (+)。

3 配置 **资源类型** 选项卡上的值。

a 在 **Orchestrator 类型** 文本框中，输入或选择 vRealize Orchestrator 对象类型。

例如，输入 **v** 可查看包含字母 v 的类型。要查看所有类型，请输入一个空格。

b 输入名称和可选描述。

c 输入一个版本。

支持的格式扩展为 major.minor.micro-revision。

d 单击 **下一步**。

4 根据需要编辑 **详细信息** 表单选项卡。

您可以通过删除、编辑和重新排列元素来编辑自定义资源。此外，您也可以添加表单和表单页面，并将元素拖动到新表单和表单页面。

5 单击 **完成**。

结果

您已创建自定义资源，并且可以在“自定义资源”页面中看到它。您可以根据此自定义资源创建 XaaS 蓝图或操作。

后续步骤

- 创建 XaaS 蓝图。请参见 [添加 XaaS 蓝图](#)。
- 创建 XaaS 资源操作。请参见 [创建 XaaS 资源操作](#)。

XaaS “自定义资源” 向导选项

您可以使用以下自定义资源选项创建或修改自定义资源，以便运行 XaaS 蓝图和用于置备资源或修改已置备资源的资源操作 workflow。

可以仅为一个对象类型创建一个自定义资源。可以将自定义资源用于多个蓝图和资源操作。

要创建自定义资源操作，请选择 **设计 > XaaS > 自定义资源**

资源类型

资源类型 选项卡上显示的可能对象类型的列表，具体取决于已配置的 vRealize Orchestrator 实例中安装的插件。vRealize Automation 将从已配置的 vRealize Orchestrator 实例收集值。

表 3-54. 资源类型选项

选项	描述
Orchestrator 类型	<p>输入或选择支持要用于置备的工作流的类型。</p> <p>类型由脚本 API（例如适用于 vCenter 的 VC）中显示的插件名称和对象类型（例如 VirtualMachine）组成。在此示例中，API 使用值 VC:VirtualMachine。</p> <p>此类型可以是蓝图工作流输出参数，也可以是资源操作工作流输入参数。</p>
名称	为自定义资源输入一个提供有用信息的名称，以便于在创建 XaaS 蓝图或资源操作时确定。
描述	输入详细描述。
版本	支持的格式扩展为 major.minor.micro-revision。

详细信息表单

当服务目录用户置备使用此自定义资源的项时，这些表单字段显示为只读值。您可以修改现有字段，也可以添加新的在外部定义的字段。

有关配置表单的详细信息，请参见[设计自定义资源表单](#)。

使用位置

由于可以仅为一个对象类型创建一个自定义资源，因此您可以使用此向导页面了解自定义资源的使用方式。

此选项卡对已保存的自定义资源可用，但在创建资源时不可用。

表 3-55. “使用位置”选项

选项	描述
XaaS 蓝图	<p>配置为使用此自定义资源的蓝图的列表。</p> <p>在此页面中，您可以执行以下操作：</p> <ul style="list-style-type: none"> ■ 编辑。打开蓝图，以便查看该蓝图的配置方式或修改该蓝图。 ■ 发布/取消发布。通过使蓝图在复合蓝图中可用或将其添加到服务中来更改该蓝图的状态。如果取消发布某个蓝图，可能会使其在复合蓝图或服务目录中不可用，或者使其不可用于添加到服务中。 ■ 删除。从系统中移除该蓝图。
资源操作	<p>配置为使用此自定义资源的资源操作的列表。</p> <p>在此页面中，您可以执行以下操作：</p> <ul style="list-style-type: none"> ■ 编辑。打开资源操作，以便查看该资源操作的配置方式或修改该资源操作。 ■ 发布/取消发布。通过使其在授权中可用来更改资源操作的状态。如果取消发布某个资源操作，可能会使其不可用于添加到服务中，或使其不可用于在已部署的蓝图上运行。 ■ 删除。从系统中移除该资源操作。

创建 XaaS 蓝图

XaaS 蓝图是置备或非置备蓝图。它提供的一些 vRealize Orchestrator 置备工作流包括：创建虚拟机、向 Active Directory 添加用户或创建虚拟机快照。您可以创建的某些非置备工作流包括：更新负载平衡器或构建报告并将其发送给收件人。

您既可以根据 vRealize Orchestrator 中提供的工作流创建 XaaS 蓝图，也可以使用为实现特定于自身环境的目标而创建的工作流。

步骤

1 添加 XaaS 蓝图

XaaS 蓝图是运行 vRealize Orchestrator 工作流的规范，用于在您的环境中更改目标系统。该蓝图包括此工作流，并且可以包括输入参数、提交和只读表单、操作序列以及置备或非置备操作。

2 将 XaaS 蓝图添加到复合蓝图

您可以将 XaaS 蓝图添加为复合蓝图的组件，这类似于在设计画布中添加其他蓝图组件。

添加 XaaS 蓝图

XaaS 蓝图是运行 vRealize Orchestrator 工作流的规范，用于在您的环境中更改目标系统。该蓝图包括此工作流，并且可以包括输入参数、提交和只读表单、操作序列以及置备或非置备操作。

您可以使用以下一种或多种方式创建 XaaS 蓝图：

- 创建 XaaS 蓝图组件。蓝图组件是可在蓝图设计画布中用作复合蓝图一部分的置备或非置备蓝图。如果您将其用作组件，则必须配置支持对部署的复合蓝图执行缩小和扩大操作的组件生命周期选项。
此蓝图类型还可以作为独立蓝图发布。
- 创建独立 XaaS 蓝图。独立蓝图是发布后直接授权给服务目录的置备或非置备蓝图。

有关如何使用 XaaS 蓝图创建 Active Directory 用户的示例，请参见[创建用于创建和修改用户的 XaaS 蓝图和操作](#)。

前提条件

- 以 **XaaS 架构师** 身份登录到 vRealize Automation。
- 如果该蓝图必须置备资源，请创建与服务蓝图的输出参数对应的自定义资源。请参见[添加 XaaS 自定义资源](#)。如果它不使用 vRealize Orchestrator 插件 API，则您无需配置自定义资源。
- 通过创建 XaaS 蓝图，将 vRealize Orchestrator 工作流作为潜在的组件蓝图或目录项发布。该蓝图包括您可编辑的表单。请参见[设计 XaaS 蓝图表单](#)。
- 使用详细的选项信息配置该蓝图。请参见[XaaS 新建蓝图或编辑向导选项](#)。

步骤

- 1 选择 **设计 > XaaS > XaaS 蓝图**。
- 2 单击 **新建** 图标 (+)。

3 在**工作流**选项卡上，选择该蓝图置备资源时运行的工作流。

如果要编辑蓝图，则此选项卡不可用。

- a 浏览 vRealize Orchestrator 工作流库，选择一个与您的自定义资源相关的工作流。
- b 查看输入和输出参数，确保稍后可以提供正确的值。
- c 单击**下一步**。

4 在**常规**选项卡上配置选项，然后单击**下一步**。

- a 在**名称**文本框中，输入一个用于区分此蓝图和类似蓝图的名称。
- b 如果不希望将此蓝图用作复合蓝图中的组件，请取消选中**可在设计画布中用作组件**复选框。

5 在**蓝图表单**选项卡上，根据需要编辑表单，然后单击**下一步**。**6** 在**已置备资源**页面中，选择一个值，然后单击**下一步**。

选项	描述
无置备	如果工作流未置备资源，您可以选择此选项或将字段留空。
<以前创建的自定义资源>	选择支持该置备工作流的自定义资源。

7 在**组件生命周期**选项卡上，定义此蓝图在缩小、扩大和销毁操作期间的行为方式。

这些工作流在将此蓝图作为组件的已部署复合蓝图上运行。不同选项的可用性取决于蓝图。并非所有蓝图工作流都支持或需要所有选项。

8 单击**完成**。**9** 选择蓝图所在的行，然后单击**发布**。**结果**

您已创建并发布 XaaS 蓝图。

后续步骤

- 要直接将此蓝图作为独立蓝图添加到服务目录，请添加服务并将该蓝图添加到服务中。请参见[添加服务](#)。
- 要将此蓝图用作复合蓝图中的组件，请参见[将 XaaS 蓝图添加到复合蓝图](#)。

XaaS 新建蓝图或编辑向导选项

可以使用以下选项创建在部署蓝图时运行 vRealize Orchestrator 工作流的 XaaS 蓝图。工作流会更改环境中的目标系统。

有关创建蓝图时应遵循的步骤，请参见[添加 XaaS 蓝图](#)。

要使用此向导，请选择**设计 > XaaS > XaaS 蓝图**。

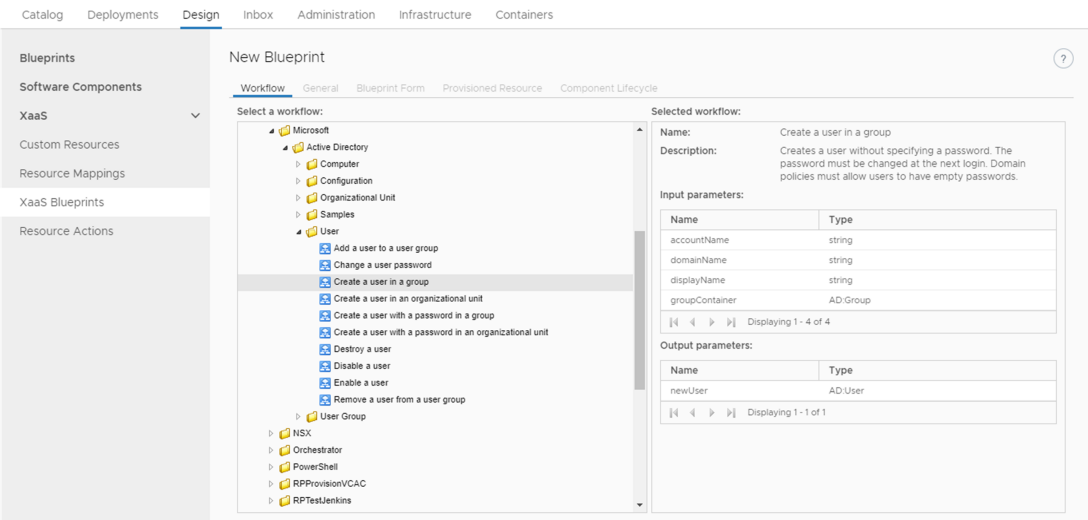
“工作流”选项卡

选择在蓝图置备资源时运行的工作流。

如果要编辑蓝图，则此选项卡不可用。

在下图中，工作流树位于左侧，参数位于右侧。

图 3-4. XaaS 蓝图向导中的“工作流”选项卡



检查输入参数和输出参数，以确保您或您的服务目录用户在下列情况下能够提供正确值：

- 如果您在此向导或蓝图设计画布中自定义蓝图表单。
- 如果您将所有输入参数留空，则服务目录用户可以设置值。

“常规”选项卡

配置有关蓝图行为的元数据。

表 3-56. “常规”选项卡选项

选项	描述
名称	希望在以下位置显示的蓝图名称： <ul style="list-style-type: none">■ 设计画布。如果选择“可在设计画布中用作组件”，则此值是类别列表中显示的名称。■ 服务。如果使用此蓝图作为独立蓝图，则此值是将目录项添加到服务时显示的名称。■ 授权。如果作为单个项授权蓝图，则此值是“添加项目”列表中显示的名称。
描述	提供有助于区分相似项的详细描述。
隐藏目录请求信息页面	如果不想要求服务目录使用者在请求项时提供描述和原因，请选中此复选框。此复选框在默认情况下选中。

表 3-56. “常规”选项卡选项（续）

选项	描述
版本	支持的格式扩展为 major.minor.micro-revision。
可在设计画布中用作组件	<p>如果打算使用蓝图作为设计画布蓝图中的组件，请选择此选项。发布后，蓝图会显示在配置自定义资源时选择的类别中。</p> <p>如果不选择此选项，则蓝图不会显示在设计画布中。但是，您仍可以将该蓝图添加到服务中，还可以授权让用户将其部署为独立蓝图。</p>

“蓝图表单”选项卡

此向导页面上显示的字段是 workflow 输入参数。可以进行以下一项或多项更改：

- 向表单添加字段。
- 修改现有字段，例如删除或重新排列字段。
- 提供默认值作为输入参数。

任何更改都会影响提供给以下对象的表单：

- 该 XaaS 蓝图用作蓝图组件时正在设计画布中工作的应用程序架构师。
- 服务目录用户（如果作为独立蓝图发布该蓝图）。

有关配置表单的详细信息，请参见[设计 XaaS 蓝图表单](#)。

已置备资源

已置备资源将蓝图链接到已在“自定义资源”页面（可从[设计 > XaaS > 自定义资源访问](#)）上配置的相关 XaaS 自定义资源。

表 3-57. 已置备资源选项

选项	描述
以前创建的自定义资源	<p>选择定义了运行置备蓝图所需的 vRealize Orchestrator 资源类型的自定义资源。</p> <p>置备蓝图将运行 vRealize Orchestrator 工作流，以使用适用于目标端点的 vRealize Orchestrator 插件 API 在该端点上置备资源。例如，将虚拟网卡添加到 vSphere 中的网络设备。</p> <p>可为此类型的已置备资源定义置备后操作。还可以使蓝图变为可扩展，即根据需要添加或移除实例。</p> <p>结果</p> <ul style="list-style-type: none"> ■ 该蓝图可进行扩展。 ■ 在设计画布中，该蓝图会显示在为选定的自定义资源指定的类别中。 ■ 部署包含该蓝图的蓝图时，该蓝图会显示在部署选项卡上，您可以在部署后对项目运行任何操作。
无置备	<p>无置备蓝图将运行 vRealize Orchestrator 工作流以执行不要求 API 对端点进行更改的任务。例如，生成报告和电子邮件，或将其发布到目标通信系统。</p> <p>结果</p> <ul style="list-style-type: none"> ■ 该蓝图不可进行扩展。可以使用无置备蓝图作为可扩展蓝图中的支持工作流。例如，您可以创建用于更新高可用性负载均衡器的蓝图。 ■ 在设计画布中，该蓝图会显示在 XaaS 类别中。 ■ 部署包含该蓝图的蓝图时，该蓝图不会显示在部署选项卡上，而且您不能在部署后对项目运行任何操作。

“组件生命周期”选项卡

如果在**常规**选项卡上选择了**可在设计画布中用作组件**，则“组件生命周期”选项卡可用。

如果该蓝图用作复合蓝图中的组件，则可以使用以下选项定义该蓝图在部署后在缩小操作和扩大操作期间的行为。

各个选项的可用性取决于蓝图。并非所有蓝图工作流都支持或需要所有选项。由于可以在复合蓝图中使用 XaaS，因此您应配置更新选项和销毁选项以及分配和取消分配（如果这些选项对蓝图可用），以使蓝图正确扩展。

表 3-58. 组件生命周期选项

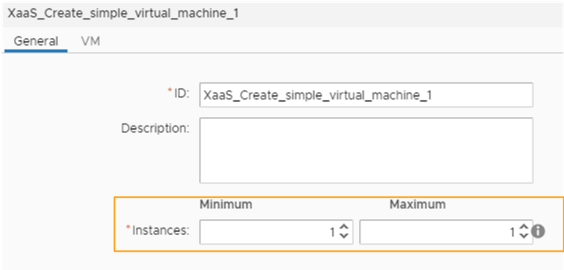
选项	描述
可扩展	<p>选择此选项可允许服务目录用户在部署后在缩小或扩大操作中更改该蓝图组件的实例数。</p> <p>如果在“已置备资源”选项卡上选择了自定义资源，则此选项可用。如果选择了“无置备”选项，则此选项不可用。</p> <p>如果使该蓝图变为可扩展，则“实例”选项会添加到设计画布中的“常规”选项卡。请参见以下示例。如果不选择“可扩展”，则“实例”选项在设计画布中不可用。</p> 
置备 workflow	<p>在置备或扩大操作期间运行的 workflow。在创建该蓝图时选择了此 workflow，您无法编辑值。</p>
分配 workflow	<p>选择在任何初始置备或扩大操作之前运行的 workflow。</p> <p>此生命周期 workflow 类型可用于 Azure 分配。如果要创建用于扩展操作的分配 workflow，该 workflow 必须包含以下值：</p> <ul style="list-style-type: none"> ■ 输入参数 <ul style="list-style-type: none"> ■ 参数名称为 requestData，参数类型为 Properties。 ■ 参数名称为 subtenant，参数类型为 Properties。 ■ reservations，参数类型为 Arrays/Properties。 ■ 输出参数 <ul style="list-style-type: none"> ■ 必须包含参数类型为 Properties 的参数。
更新 workflow	<p>选择在对不可扩展但可更新的组件执行更新操作（包括缩小或扩大）期间运行的 workflow。</p> <p>例如，负载均衡器会使用通过对复合蓝图中任何组件执行缩小或扩大操作而创建的新配置进行更新。</p> <p>更新 workflow 可能会应用到与已扩展组件绑定的但本身不可扩展的组件。此更新 workflow 可以基于更新操作更改不可扩展组件。</p> <p>如果要创建用于扩展操作的更新 workflow，该 workflow 必须包含以下值：</p> <ul style="list-style-type: none"> ■ 输入参数。 <ul style="list-style-type: none"> ■ 无论参数名称是什么，都必须包含与置备 workflow 的输出参数类型匹配的参数。 ■ 参数名称为 data，参数类型为 Properties。

表 3-58. 组件生命周期选项 （续）

选项	描述
销毁 workflow	<p>选择在缩小或销毁操作期间运行的 workflow。</p> <p>如果要创建用于扩展操作的销毁 workflow，该 workflow 必须包含以下值：</p> <ul style="list-style-type: none"> ■ 输入参数。 <ul style="list-style-type: none"> ■ 无论参数名称是什么，都必须包含与置备 workflow 的输出参数类型匹配的输入参数。 <p>例如，如果“创建简单的虚拟机”置备 workflow 包含输出参数 <code>VC:VirtualMachine</code>，则销毁 workflow 必须包含类型为 <code>VC:VirtualMachine</code> 的输入参数。</p>
取消分配 workflow	<p>选择在任何销毁或缩小操作之后运行的 workflow。如果取消分配在操作期间失败，销毁 workflow 仍会按预期运行。</p> <p>取消分配是缩小或销毁复合蓝图时的最终过程。它在销毁操作之后运行，并且会释放资源。</p> <p>此生命周期 workflow 类型可用于 Azure 分配。如果要创建用于扩展操作的取消分配 workflow，该 workflow 必须包含以下值：</p> <ul style="list-style-type: none"> ■ 输入参数。 <ul style="list-style-type: none"> ■ 参数名称为 <code>data</code>，参数类型为 <code>Properties</code>。
类别	<p>要指定 XaaS 蓝图在设计画布中的显示位置，请在设计画布类别下拉菜单中选择一个值。</p> <p>如果不选择类别，则会在发布该蓝图时将其添加到 XaaS 类别中。</p>

将 XaaS 蓝图添加到复合蓝图

您可以将 XaaS 蓝图添加为复合蓝图的组件，这类似于在设计画布中添加其他蓝图组件。

使用此方法可将 XaaS 添加到复合蓝图。此蓝图既可以是唯一的蓝图组件，也可以是构成应用程序蓝图的若干组件之一。

如果只想将 XaaS 蓝图提供给用户，可以将该蓝图添加到服务中并授权给用户，而无需将其添加到复合蓝图中。

如果对部署的应用程序蓝图运行缩小或扩大操作，XaaS 蓝图会根据您配置蓝图生命周期选项的方式进行缩放。

前提条件

- 以**基础架构架构师**身份登录到 vRealize Automation。
- 创建并发布 XaaS 蓝图。请参见[创建 XaaS 蓝图](#)。创建该蓝图后，在设计画布中指定该蓝图所处的类别。
- 查看如何在复合蓝图中自定义 XaaS 蓝图表单。请参见[设计 XaaS 蓝图和操作的表单](#)。

步骤

- 1 选择**设计 > 蓝图**。

2 选择要向其中添加 XaaS 的蓝图的名称。

此时将显示设计画布。其中包含当前应用程序组件蓝图和其他组件。

3 在“类别”列表中，找到该蓝图。**4** 将您的蓝图拖动到画布中。**5** 在“常规”和“创建”选项卡上配置默认值。

当用户请求目录项时，这些默认值便会显示在服务目录表单中。

6 单击**完成**。**7** 选择蓝图并单击**发布**。**结果**

XaaS 蓝图现在是复合蓝图的一部分。

后续步骤

将复合蓝图添加到服务中。请参见[管理服务目录](#)。

创建 XaaS 资源操作

您可以创建资源操作，以便能够使用 vRealize Orchestrator 工作流管理已置备的项目。

前提条件

- 以 **XaaS 架构师** 身份登录到 vRealize Automation。
- 确认您具有支持该操作的自定义资源。请参见[添加 XaaS 自定义资源](#)。
- 如果创建要在没有置备为 XaaS 目录项的项目上运行的操作，请确认已映射目标资源。请参见[映射要与 XaaS 资源操作一起使用的其他资源](#)。

步骤**1** [创建资源操作](#)

资源操作是服务目录用户可在已置备目录项上运行的 XaaS 工作流。作为 XaaS 架构师，您可以创建一个资源操作，定义使用者可对已置备项目执行的操作。

2 [发布资源操作](#)

新创建的资源操作处于草稿状态，您必须发布该资源操作。

3 [为 XaaS 资源操作分配图标](#)

创建并发布资源操作后，您可以编辑该操作并为其分配图标。

创建资源操作

资源操作是服务目录用户可在已置备目录项上运行的 XaaS 工作流。作为 XaaS 架构师，您可以创建一个资源操作，定义使用者可对已置备项目执行的操作。

通过创建资源操作，您可以将 vRealize Orchestrator 工作流作为置备后操作进行关联。在此过程中，您可以编辑默认提交和只读表单。请参见[设计资源操作表单](#)。

前提条件

- 以 **XaaS 架构师** 身份登录到 vRealize Automation。
- 创建与资源操作的输入参数对应的自定义资源。

步骤

1 选择 **设计 > XaaS > 资源操作**。

2 单击 **新建** 图标 (+)。

3 浏览 vRealize Orchestrator 工作流库，选择一个与您的自定义资源相关的工作流。

您可以查看选定工作流的名称和描述以及输入和输出参数，如 vRealize Orchestrator 中所定义。

4 单击 **下一步**。

5 从 **资源类型** 下拉菜单中，选择您以前创建的自定义资源。

6 从 **输入参数** 下拉菜单中，选择资源操作的输入参数。

7 单击 **下一步**。

8 输入名称和可选描述。

名称 和 **描述** 文本框使用工作流的名称和描述预填充，如 vRealize Orchestrator 中所定义。

9 （可选） 如果不想提示使用者输入请求此资源操作的描述和原因，请选中 **隐藏目录请求信息** 页面复选框。

10 输入一个版本。

支持的格式扩展为 major.minor.micro-revision。

11 （可选） 选择操作类型。

选项	描述
处置	处置资源操作工作流的输入参数且项目将从 部署 选项卡中移除。例如，该资源操作用于删除已置备的计算机。
置备	该资源操作用于置备。例如，该资源操作用于复制目录项。 从下拉菜单中，选择输出参数。您可以选择以前创建的自定义资源，以便使用者请求此资源操作时，已置备项目添加到 部署 选项卡中。如果只有 无置备 选项，则要么该资源操作不用于置备，要么您没有为输出参数创建适当的自定义资源，且无法继续操作。

根据操作工作流，您可以选择一或两个选项，也可以不选择任何选项。

12 选择用户可以使用该资源操作的条件，然后单击 **下一步**。

13 （可选）在表单选项卡中，编辑该资源操作的表单。

该资源操作的表单映射 vRealize Orchestrator 工作流展示。您可以通过删除、编辑和重新排列元素来更改此表单。此外，您也可以添加新表单和表单页面，并将必要的元素拖动到新表单和表单页面。

选项	操作
添加表单	单击表单名称旁边的 新建表单 图标 ()，提供所需的信息，然后单击 提交 。
编辑表单	单击表单名称旁边的 编辑 图标 ()，进行必要的更改，然后单击 提交 。
重新生成工作流展示	单击表单名称旁边的 重新构建 图标 ()，然后单击 确定 。
删除表单	单击表单名称旁边的 删除 图标 ()，然后在确认对话框中单击 确定 。
添加表单页面	单击表单页面名称旁边的 新建页面 图标 ()，提供所需的信息，然后单击 提交 。
编辑表单页面	单击表单页面名称旁边的 编辑 图标 ()，进行必要的更改，然后单击 提交 。
删除表单页面	单击表单名称旁边的 删除 图标 ()，然后在确认对话框中单击 确定 。
向表单页面添加元素	将元素从左侧的“新字段”窗格拖动到右侧窗格。然后，您可以提供所需的信息并单击 提交 。
编辑元素	单击要编辑的元素旁边的 编辑 图标 ()，进行必要的更改，然后单击 提交 。
删除元素	单击要删除的元素旁边的 删除 图标 ()，然后在确认对话框中单击 确定 。

14 单击完成。

结果

您已创建资源操作，并且可以看到它在“资源操作”页面中列出。

后续步骤

发布资源操作。请参见[发布资源操作](#)。

发布资源操作

新创建的资源操作处于草稿状态，您必须发布该资源操作。

前提条件

以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

- 1 选择**设计 > XaaS > 资源操作**。
- 2 选择要发布的资源操作所在的行，然后单击**发布**。

结果

该资源操作的状态将变为“已发布”。

后续步骤

为该资源操作分配图标。请参见 [为 XaaS 资源操作分配图标](#)。然后，业务组主管和租户管理员可以在创建授权时使用该操作。

为 XaaS 资源操作分配图标

创建并发布资源操作后，您可以编辑该操作并为其分配图标。

前提条件

以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

- 1 选择 **管理 > 目录管理 > 操作**。
- 2 选择您创建的资源操作。
- 3 单击 **配置**。
- 4 单击 **浏览** 并选择要添加的图标。
- 5 单击 **打开**。
- 6 单击 **更新**。

结果

您已为该资源操作分配图标。业务组主管和租户管理员可以在授权中使用该资源操作。

映射要与 XaaS 资源操作一起使用的其他资源

您可以映射不使用 XaaS 置备的项目，以便运行要在这些项目上运行的资源操作。

资源映射脚本操作和工作流

您既可以使用为 vSphere、vCloud Director 或 vCloud Air 虚拟机提供的资源映射，也可以创建自定义 vRealize Orchestrator 脚本操作或工作流，来将其他 vRealize Automation 目录资源类型映射到 vRealize Orchestrator 清单类型。

随 vRealize Automation 提供的资源映射

vRealize Automation 包括 IaaS vSphere 虚拟机、IaaS vCloud Director 和部署的资源映射。

vRealize Automation 包括每个提供的 XaaS 资源映射的 vRealize Orchestrator 资源映射脚本操作。提供的资源映射的脚本操作位于嵌入式 vRealize Orchestrator 服务器的 `com.vmware.vcac.asd.mappings` 软件包中。

创建资源操作时，如果该操作在已部署的复合蓝图上运行，而该蓝图使用 vRealize Orchestrator 工作流且将 `VCACAFE:CatalogResource` 作为输入参数，则将应用“部署”映射作为输入资源类型。只有所选工作流将 `VCACAFE:CatalogResource` 作为输入参数时，才会应用“部署”映射。例如，如果要创建的操作用于代表用户请求资源操作，则由于该工作流使用 `VCACAFE:CatalogResource`，“输入资源”选项卡上的资源类型为“部署”。

IaaS vCD 虚拟机和 IaaS VC 虚拟机资源映射可供操作用于将与 IaaS 资源匹配的虚拟机映射到 vRealize Orchestrator vSphere 或 vCloud Director 虚拟机。

开发资源映射

根据您的 vRealize Orchestrator 版本，您可以创建 vRealize Orchestrator 工作流或脚本操作，从而在 vRealize Orchestrator 与 vRealize Automation 之间映射资源。

要开发资源映射，请使用 **Properties** 类型的输入参数（包含定义已置备资源的键-值对）和对应的 vRealize Orchestrator 插件所需的 vRealize Orchestrator 清单类型的输出参数。映射可用的属性取决于资源类型。例如，**EXTERNAL_REFERENCE_ID** 属性是定义各个虚拟机的常用密钥参数，您可以使用此属性查询目录资源。如果要为不使用 **EXTERNAL_REFERENCE_ID** 的资源创建映射，则可以使用为各虚拟机传递的其他某个属性，例如，名称、描述等。

有关开发工作流和脚本操作的详细信息，请参见《使用 VMware vCenter Orchestrator 进行开发》。

创建资源映射

vRealize Automation 提供了 vSphere、vCloud Director 和 vCloud Air 计算机的资源映射。您可以为其他类型的目录资源创建更多资源映射。

前提条件

- 以 **XaaS 架构师** 身份登录到 vRealize Automation。
- 确认映射脚本或工作流在 vRealize Orchestrator 中可用。请参见[资源映射脚本操作和工作流](#)

步骤

- 1 选择 **设计 > XaaS > 资源映射**。
- 2 单击 **新建** 图标 (+)。
- 3 输入名称和可选描述。
- 4 输入一个版本。
支持的格式扩展为 major.minor.micro-revision。
- 5 在 **目录资源类型** 文本框中输入目录资源的类型，然后按 Enter。
目录资源的类型显示在已置备项目的详细信息视图中。
- 6 在 **Orchestrator 类型** 文本框中输入 vRealize Orchestrator 对象类型，然后按 Enter。
这是资源映射工作流的输出参数。

7 （可选）添加目标标准，从而限制通过使用此资源映射创建的资源操作的可用性。

此外，资源操作还受批准和授权的限制。

- a 选择**基于条件可用**。
- b 选择条件类型。

选项	描述
以下所有项	如果满足定义的所有子句，则通过使用此资源映射创建的资源操作可供用户使用。
以下任一	如果满足定义的任一子句，则通过使用此资源映射创建的资源操作可供用户使用。
非以下项	如果定义子句存在，则通过使用此资源映射创建的资源操作不可用。

- c 按照提示构建子句并完成条件。

8 从 vRealize Orchestrator 库中选择资源映射脚本操作或工作流。

9 单击**确定**。

设计 XaaS 蓝图和操作的表单

XaaS 包括表单设计器，可用于设计蓝图和资源操作的提交表单和详细信息表单。根据工作流的展示，表单设计器会动态生成默认表单，以及可用于修改默认表单的字段。

您可以创建交互式表单，用户可填写这些表单以提交目录项和资源操作。还可以创建只读表单，用于定义用户可以在目录项或已置备资源的详细信息视图上查看的信息。

创建 XaaS 自定义资源、XaaS 蓝图和资源操作时，系统将为常见用例生成表单。

表 3-59. XaaS 对象类型及关联表单

对象类型	默认表单	其他表单
自定义资源	资源详细信息表单基于 vRealize Orchestrator 插件清单类型的属性（只读）。	■ 无
XaaS 蓝图	请求提交表单基于所选工作流的显示。	■ 目录项详细信息（只读） ■ 已提交请求的详细信息（只读）
资源操作	操作提交表单基于所选工作流的显示。	■ 已提交操作的详细信息（只读）

可以修改默认表单和设计新表单。可以通过拖动字段以将其添加到表单中并对其重新排序。您可以限制某些字段值、指定默认值或为填写表单的最终用户提供说明文本。

由于操作的不同目的，与设计提交表单的操作相比，可以为设计只读表单而执行的操作有限。

表单设计器中的字段

通过将预定义的新字段添加到默认生成的资源操作和 XaaS 蓝图，您可以扩展工作流展示和功能。

如果在 vRealize Orchestrator 工作流中定义输入参数，则在 vRealize Automation 中，该参数将出现在默认生成的表单上。如果不想在该表单中使用默认生成的字段，则可将其删除，然后从调色板中拖放新字段。如果使用相同 ID 作为要替换的字段，则可在不中断工作流映射的情况下替换默认生成的字段。

在以下情况下，您还可以添加新字段，而不是根据 vRealize Orchestrator 工作流程输入生成的字段，以便扩展工作流程展示和功能：

- 向现有字段添加限制

例如，您可以创建一个新下拉菜单并将其命名为 **dd**。还可以创建预定义的“金级”、“银级”、“铜级”和“自定义”选项。如果存在“CPU”等预定义的字段，则可向此字段添加以下限制：

- 如果 **dd** 等于“金级”，则 CPU 为 2000 MHz
- 如果 **dd** 等于“银级”，则 CPU 为 1000 MHz
- 如果 **dd** 等于“铜级”，则 CPU 为 500 MHz
- 如果 **dd** 等于“自定义”，则“CPU”字段可编辑，并且使用者可以指定自定义值

- 向字段添加外部值定义

您可以向字段添加外部值定义，以便运行 vRealize Orchestrator 脚本操作并为使用者提供有关所设计表单的附加信息。例如，您可能需要创建一个工作流程来更改虚拟机的防火墙设置。在“资源操作请求”页面上，您要为用户提供更改已打开端口设置的功能，但同时也想将这些选项限于已打开的端口。您可以向双列表字段添加外部值定义，然后选择自定义的 vRealize Orchestrator 脚本操作用于查询已打开的端口。加载请求表单时，会运行脚本操作，并且已打开的端口将作为选项提供给用户。

- 将 vRealize Orchestrator 工作流程中处理的新字段添加为全局参数

例如，该工作流程提供与第三方系统的集成，并且工作流程开发人员定义了在一般情况下要处理的输入参数，但是也提供了用于传递自定义字段的方式。例如，在脚本框中，将处理所有以 **my3rdparty** 开头的全局参数。然后，如果 XaaS 架构师要传递使用者提供的特定值，则 XaaS 架构师可以添加名为 **my3rdparty_CPU** 的新字段。

表 3-60. 资源操作或 XaaS 蓝图表单中的新字段

字段	描述
文本字段	单行文本框
文本区域	多行文本框
链接	使用者在其中输入 URL 的字段。您可以使用 http、https、ftp、mailto 或 /。请勿使用 file://。
电子邮件	使用者用来输入电子邮件地址的字段
密码字段	使用者用来输入密码的字段
整数字段	使用者用来输入整数的文本框 您可以将此字段设置为包含最小值、最大值以及增量的滑块。
小数字段	使用者用来输入小数的文本框 您可以将此字段设置为包含最小值、最大值以及增量的滑块。
日期和时间	使用者用来指定日期（通过从日历菜单中选择日期）并可在其中选择时间（通过使用上下箭头）的文本框。
双列表	使用者用来在两个列表之间移动一组预定义值的列表构建器，第一个列表包含所有未选中的选项，第二个列表包含用户的选项。

表 3-60. 资源操作或 XaaS 蓝图表单中的新字段（续）

字段	描述
复选框	复选框
是/否	用于选择 是 或 否 的下拉菜单
下拉字段	下拉菜单
列表	列表
复选框列表	复选框列表
单选按钮组	一组单选按钮
搜索	自动完成查询并供使用者选择对象的搜索文本框
树	使用者用来浏览和选择可用对象的树
映射	使用者用来为属性定义键-值对的映射表

还可以使用**部分标题**表单字段将表单页面拆分成各个具有单独标题的部分，并使用**文本**表单字段添加只读信息性文本。

表单设计器中的限制和值

编辑蓝图或资源操作表单的某个元素时，您可以将各种限制和值应用于该元素。

限制

您可应用于元素的限制因编辑或添加到表单的元素类型而异。有些限制值可以在 vRealize Orchestrator 工作流中配置。这些值不会显示在“限制”选项卡上，因为它们通常依赖于工作流运行时所评估的条件。为蓝图表单配置的任何限制值都会替代 vRealize Orchestrator 工作流中包含的限制。

针对字段计算后，仅当请求蓝图时，才会重新计算最小和最大绑定。

对于应用于元素的每个限制，您可选择以下选项之一定义该限制：

未设置

从 vRealize Orchestrator 工作流展示中获取属性。

常数

将编辑的元素设置为必需或可选。

字段

将该元素绑定到表单中的其他元素。例如，您可以将该元素设置为仅当选中了其他元素（例如，复选框）时才需要提供。

条件

应用条件。使用条件可以创建各种子句和表达式，并将其应用于该元素的状态或限制。

外部

选择定义值的 vRealize Orchestrator 脚本操作。

表 3-61. 表单设计器中的限制

限制	描述
必需	指示该元素是否为必需。
只读	指示该字段是否为只读。
值	设置元素的值。
可见	指示使用者能否看到该元素。 如果在 vRealize Orchestrator 工作流中将可见性限制应用于显示组，则会忽略 XaaS “已提交请求的详细信息” 表单中的限制，且您要隐藏的字段会显示在表单中。 要隐藏您不希望显示在“已提交请求的详细信息”表单中的字段，并且请求用户不需要这些字段，请从 XaaS 蓝图设计器的“蓝图表单”选项卡上的“已提交请求的详细信息”表单中移除这些字段。要找到此选项卡，请参见 添加新 XaaS 蓝图表单 。
最小长度	设置字符串输入元素的最小字符数。
最大长度	设置字符串输入元素允许的最大字符数。
最小值	设置数字输入元素的最小值。
最大值	设置数字输入元素的最大值。
增量	设置元素（例如 小数 或 整数 字段）的增量。例如，如果您希望 整数 字段以 滑块 的形式呈现出来，则可以使用该步骤的值。
最小计数	设置元素可选的最小项数。 例如，在添加或编辑 复选框列表 时，您可以设置使用者继续操作之前必须选中的最小复选框数。
最大计数	设置元素可选的最大项数。 例如，在添加或编辑 复选框列表 时，您可以设置使用者继续操作之前必须选中的最大复选框数。

值

您可以将值应用于某些元素，并定义使用者查看部分字段的哪些内容。可用选项取决于所编辑或添加到表单的元素类型。

表 3-62. 表单设计器中的值

值	描述
未设置	从 vRealize Orchestrator 工作流展示中获取所编辑元素的值。
预定义值	从 vRealize Orchestrator 清单的相关对象列表中选择值。
值	使用标签定义静态自定义值。
外部值	选择一个 vRealize Orchestrator 脚本操作，该脚本操作使用工作流不直接公开的信息来定义值。

表单设计器中的外部值定义

编辑表单设计器中的某些元素时，您可以分配使用自定义 vRealize Orchestrator 脚本操作的外部值定义，提供工作流不直接公开的信息。

例如，您可能需要发布资源操作，以便在已置备的计算机上安装软件。如果不希望为用户提供所有可供下载的软件静态列表，则可使用与计算机操作系统相关的软件、用户之前未安装在计算机上的软件或者计算机上已过期且需要更新的软件动态填充该列表。

要为用户提供自定义的动态内容，您可以创建 vRealize Orchestrator 脚本操作，检索要向用户显示的信息。您可以将脚本操作作为外部值定义分配给表单设计器中的字段。向用户展示资源或服务蓝图表单之后，该脚本操作将检索自定义信息并将其显示给用户。

您可以使用外部值定义提供默认值或只读值、构建布尔表达式、定义限制或提供用户可从列表中选择的事项和复选框等。

如果使用包含必填字段的工作流创建蓝图，则该字段在请求表单中为必填字段，即使您将其设置为非必填字段也是如此。

使用表单设计器

创建 XaaS 蓝图、自定义资源操作和自定义资源时，您可以使用表单设计器编辑这些蓝图、操作和资源的表单。您可以编辑表示形式，并定义项目或操作的使用者在请求目录项或运行置备后操作时看到的内容。

默认情况下，任何 XaaS 蓝图、资源操作或自定义资源表单均以 vRealize Orchestrator 中的工作流展示为基础生成。

Start Workflow : Create cluster

1 Common parameters

2 vCloud Distributed Storage

* Parent host folder
Not set

* Name of the new cluster

* Enable VMware HA
☐ Yes ☒ No

* Enable VMware DRS
☐ Yes ☒ No

Cancel Back Next Submit

vRealize Orchestrator 展示中的步骤以表单页面表示，vRealize Orchestrator 展示组以单独的区域表示。选定工作流的输入类型显示为表单中的各种字段。例如，vRealize Orchestrator 类型 `string` 以文本框表示。VC:VirtualMachine 等复杂类型以搜索框后树表示，这样使用者可以键入字母数字值来搜索虚拟机或浏览并选择虚拟机。

您可以编辑对象在表单设计器中的表示形式。例如，您可以编辑默认的 VC:VirtualMachine 表示形式，并使其成为树而不是搜索框。此外，您还可以添加复选框、下拉菜单等新字段，并应用各种限制。如果添加的新字段无效或未正确映射到 vRealize Orchestrator 工作流输入，则使用者运行该工作流时，vRealize Orchestrator 将跳过无效或未映射的字段。

设计自定义资源表单

使用者置备您的自定义资源时，资源详细信息表单上的所有字段在项的详细信息页面中对其显示为只读。您可以对表单执行删除、修改或重新排列字段等基本的编辑操作，也可以添加外部定义的新字段，以使用 vRealize Orchestrator 脚本操作为使用者提供其他只读信息。

■ 编辑自定义资源元素

您可以在自定义资源的“详细信息表单”页面中编辑元素的某些特征。该页面上的每个默认字段均表示自定义资源的一个属性。您无法更改属性类型或默认值，但可以编辑名称、大小和描述。

■ 添加新的自定义资源表单页面

您可以添加新页面，将表单重新排列成多个选项卡。

■ 在自定义资源表单中插入部分标题

您可以插入部分标题，将表单拆分为多个部分。

■ 在自定义资源表单中插入文本元素

您可以插入文本框，向表单添加一些描述性文本。

■ 在自定义资源表单中插入外部定义的字段

您可以插入新字段并为其分配外部值定义，从而动态提供使用者在置备自定义资源时可以在“项目详细信息”页面上看到的只读信息。

编辑自定义资源元素

您可以在自定义资源的“详细信息表单”页面中编辑元素的某些特征。该页面上的每个默认字段均表示自定义资源的一个属性。您无法更改属性类型或默认值，但可以编辑名称、大小和描述。

前提条件

- 以**租户管理员**或 **XaaS 架构师** 身份登录到 vRealize Automation。
- [添加 XaaS 自定义资源](#)。

步骤

- 1 选择**设计 > XaaS > 自定义资源**。
- 2 单击要编辑的自定义资源。
- 3 单击**详细信息表单**选项卡。
- 4 指向要编辑的元素，然后单击**编辑**图标。
- 5 在**标签**文本框中输入字段的新名称以更改标签。
- 6 在**描述**文本框中编辑描述。
- 7 从**大小**下拉菜单中选择一个选项，更改元素的大小。
- 8 从**标签大小**下拉菜单中选择一个选项，更改标签的大小。
- 9 单击**提交**。
- 10 单击**完成**。

添加新的自定义资源表单页面

您可以添加新页面，将表单重新排列成多个选项卡。

前提条件

- 以**租户管理员**或 **XaaS 架构师** 身份登录到 vRealize Automation。
- [添加 XaaS 自定义资源](#)。

步骤

- 1 选择**设计 > XaaS > 自定义资源**。
- 2 单击要编辑的自定义资源。
- 3 单击**详细信息表单**选项卡。
- 4 单击**表单页面**名称旁边的**新建页面**图标 (+)。
- 5 选择未使用的屏幕类型并单击**提交**。

如果您已拥有资源详细信息或资源列表视图，则无法创建两个类型相同的屏幕。

- 6 单击**提交**。
- 7 配置表单。
- 8 单击**完成**。

结果

您可以从原始表单页面中删除某些元素并将其插入新表单页面，也可以添加使用外部值定义的新字段，为用户提供 vRealize Orchestrator 工作流不直接公开的信息。

在自定义资源表单中插入部分标题

您可以插入部分标题，将表单拆分为多个部分。

前提条件

- 以**租户管理员**或 **XaaS 架构师**身份登录到 vRealize Automation。
- 添加 [XaaS 自定义资源](#)。

步骤

- 1 选择**设计 > XaaS > 自定义资源**。
- 2 单击要编辑的自定义资源。
- 3 单击**详细信息表**选项卡。
- 4 将**部分标题**元素从“表单”窗格拖动到“表单页面”窗格。
- 5 键入该部分的名称。
- 6 单击该元素的外部以保存更改。
- 7 单击**完成**。

在自定义资源表单中插入文本元素

您可以插入文本框，向表单添加一些描述性文本。

前提条件

- 以**租户管理员**或 **XaaS 架构师**身份登录到 vRealize Automation。
- 添加 [XaaS 自定义资源](#)。

步骤

- 1 选择**设计 > XaaS > 自定义资源**。
- 2 单击要编辑的自定义资源。
- 3 单击**详细信息表**选项卡。
- 4 将**文本**元素从“表单”窗格拖动到“表单页面”窗格。
- 5 输入要添加的文本。
- 6 单击该元素的外部以保存更改。
- 7 单击**完成**。

在自定义资源表单中插入外部定义的字段

您可以插入新字段并为其分配外部值定义，从而动态提供使用者在置备自定义资源时可以在“项目详细信息”页面上看到的只读信息。

前提条件

- 以**租户管理员**或**XaaS 架构师**身份登录到 vRealize Automation。
- 添加 **XaaS 自定义资源**。
- 开发或导入 vRealize Orchestrator 脚本操作，以检索要提供给使用者的信息。

步骤

- 1 选择**设计 > XaaS > 自定义资源**。
- 2 单击要编辑的自定义资源。
- 3 单击**详细信息**表单选项卡。
- 4 从“新字段”窗格中拖动一个元素，并将其放入“表单页面”窗格。
- 5 在 **ID** 文本框中输入该元素的 ID。
- 6 在**标签**文本框中输入一个标签。
标签通过表单呈现给用户。
- 7 （可选）从**类型**下拉菜单中选择字段的类型。
- 8 在**实体类型**搜索框中键入 vRealize Orchestrator 脚本操作的结果类型，然后按 Enter。
例如，如果要使用脚本操作显示当前用户且该脚本返回 vRealize Orchestrator 结果类型 **LdapUser**，请在**实体类型**搜索框中键入 **LdapUser**，然后按 Enter。
- 9 单击**添加外部值**。
- 10 选择自定义的 vRealize Orchestrator 脚本操作。
- 11 单击**提交**。
- 12 再次单击**提交**。
- 13 单击**完成**。

结果

向使用者展示该表单之后，该脚本操作将检索自定义信息并将其显示给使用者。

设计 XaaS 蓝图表单

创建 XaaS 蓝图时，您可以采用以下方式编辑该蓝图的表单：向表单添加新字段、修改现有字段、删除或重新排列字段。此外，您还可以创建新表单和表单页面，并将新字段拖放到其中。

- **添加新 XaaS 蓝图表单**
当您编辑工作流默认生成而且要作为 XaaS 蓝图发布的表单时，您可以添加新 XaaS 蓝图表单。
- **编辑 XaaS 蓝图元素**
您可以在 XaaS 蓝图的“蓝图表单”页面中编辑元素的某些特征。您可以更改元素的类型及其默认值，并应用各种限制和值。

■ 添加新元素

当您编辑 XaaS 蓝图默认生成的表单时，您可以向表单添加预定义的新元素。例如，如果不想使用默认生成的字段，则可将其删除并替换为新字段。

■ 在 XaaS 蓝图表单中插入部分标题

您可以插入部分标题，将表单拆分为多个部分。

■ 向 XaaS 蓝图表单添加文本元素

您可以插入文本框，向表单添加一些描述性文本。

添加新 XaaS 蓝图表单

当您编辑 workflow 默认生成而且要作为 XaaS 蓝图发布的表单时，您可以添加新 XaaS 蓝图表单。

通过添加新 XaaS 蓝图表单，您可定义目录项详细信息页面和已提交请求的详细信息页面的外观。如果不添加目录项详细信息和已提交请求的详细信息表单，则使用者将看到请求表单中定义的内容。

前提条件

- 以租户管理员或 XaaS 架构师身份登录到 vRealize Automation。
- 添加 XaaS 蓝图。

步骤

- 1 选择设计 > XaaS > XaaS 蓝图。
- 2 单击要编辑的 XaaS 蓝图。
- 3 单击蓝图表单选项卡。
- 4 单击新建表单图标 (+)。
- 5 输入名称和可选描述。
- 6 从屏幕类型菜单中选择屏幕类型。

选项	描述
目录项详细信息	使用者在单击目录项时看到的目录项详细信息页面。
请求表单	默认的 XaaS 蓝图表单。使用者在请求目录项时会看到该请求表单。
已提交请求的详细信息	使用者请求项目后在查看部署选项卡中查看请求详细信息时看到的请求详细信息页面。

- 7 单击提交。

后续步骤

通过将所需的字段从“新字段”窗格拖动到“表单页面”窗格，即可添加这些字段。

编辑 XaaS 蓝图元素

您可以在 XaaS 蓝图的“蓝图表单”页面中编辑元素的某些特征。您可以更改元素的类型及其默认值，并应用各种限制和值。

前提条件

- 以租户管理员或 XaaS 架构师身份登录到 vRealize Automation。
- 添加 XaaS 蓝图。

步骤

- 1 选择设计 > XaaS > XaaS 蓝图。
- 2 单击要编辑的 XaaS 蓝图。
- 3 单击蓝图表单选项卡。
- 4 找到要编辑的元素。
- 5 单击编辑图标 (✎)。
- 6 在标签文本框中输入字段的新名称，更改使用者看到的标签。
- 7 在描述文本框中编辑描述。
- 8 从类型下拉菜单中选择一个选项，更改元素的显示名称。
这些选项因编辑的元素类型而异。
- 9 从大小下拉菜单中选择一个选项，更改元素的大小。
- 10 从标签大小下拉菜单中选择一个选项，更改标签的大小。
- 11 编辑元素的默认值。

选项	描述
未设置	从 vRealize Orchestrator 工作流展示中获取所编辑元素的值。
常数	将编辑元素的默认值设置为指定的常数值。
字段	将元素的默认值绑定到表示中另一个元素的参数。
条件	应用条件。通过使用条件，您可以创建各种子句和表达式并将其应用于元素。
外部	选择 vRealize Orchestrator 脚本操作以定义该值。

- 12 将限制选项卡中的限制应用于元素。

选项	描述
未设置	从 vRealize Orchestrator 工作流展示中获取所编辑元素的值。
常数	将编辑元素的默认值设置为指定的常数值。
字段	将元素的默认值绑定到表示中另一个元素的参数。
条件	应用条件。通过使用条件，您可以创建各种子句和表达式并将其应用于元素。
外部	选择 vRealize Orchestrator 脚本操作以定义该值。

13 在**值**选项卡中添加元素的一个或多个值。

可用选项取决于编辑的元素类型。

选项	描述
未设置	从 vRealize Orchestrator 工作流展示中获取所编辑元素的值。
预定义值	<p>从 vRealize Orchestrator 清单的相关对象列表中选择值。</p> <ol style="list-style-type: none"> 在预定义值搜索框中输入一个值来搜索 vRealize Orchestrator 清单。 从搜索结果中选择一个值，然后按 Enter。
值	<p>使用标签定义自定义值。</p> <ol style="list-style-type: none"> 在值文本框中输入一个值。 在标签文本框中输入该值的标签。 单击添加图标 。
外部值	<p>选择 vRealize Orchestrator 脚本操作，使用工作流不直接公开的信息定义值。</p> <ul style="list-style-type: none"> 选择添加外部值。 选择 vRealize Orchestrator 脚本操作。 单击提交。

14 单击**提交**。**15** 单击**完成**。

添加新元素

当您编辑 XaaS 蓝图默认生成的表单时，您可以向表单添加预定义的新元素。例如，如果不想使用默认生成的字段，则可将其删除并替换为新字段。

前提条件

- 以**租户管理员**或 **XaaS 架构师**身份登录到 vRealize Automation。
- [添加 XaaS 蓝图](#)。

步骤

- 1 选择**设计 > XaaS > XaaS 蓝图**。
- 2 单击要编辑的 XaaS 蓝图。
- 3 单击**蓝图表单**选项卡。
- 4 从“新字段”窗格中拖动一个元素，并将其放入“表单页面”窗格。
- 5 在 **ID** 文本框中输入工作流输入参数的 ID。
- 6 在**标签**文本框中输入一个标签。
标签通过表单呈现给用户。
- 7 （可选）从**类型**下拉菜单中选择字段的类型。

- 8 在**实体类型**文本框中输入 vRealize Orchestrator 对象，然后按 Enter。

并非所有字段类型均需执行该步骤。

选项	描述
结果类型	如果使用脚本操作定义字段的外部值，请输入 vRealize Orchestrator 脚本操作的结果类型。
输入参数	如果使用该字段接受使用者输入并将参数传递回 vRealize Orchestrator，请输入 vRealize Orchestrator 工作流接受的输入参数的类型。
输出参数	如果使用该字段向使用者显示信息，请输入 vRealize Orchestrator 工作流的输出参数的类型。

- 9 （可选）选中**多个值**复选框，允许使用者选择多个对象。

该选项并非对所有字段类型均可用。

- 10 单击**提交**。

- 11 单击**更新**。

后续步骤

您可以编辑元素来更改默认设置，并应用各种限制或值。

在 XaaS 蓝图表单中插入部分标题

您可以插入部分标题，将表单拆分为多个部分。

前提条件

- 以**租户管理员**或 **XaaS 架构师**身份登录到 vRealize Automation。
- 添加 **XaaS 蓝图**。

步骤

- 1 选择**设计 > XaaS > XaaS 蓝图**。
- 2 单击要编辑的 XaaS 蓝图。
- 3 单击**蓝图表单**选项卡。
- 4 将**部分标题**元素从“表单”窗格拖动到“表单页面”窗格。
- 5 键入该部分的名称。
- 6 单击该元素的外部以保存更改。
- 7 单击**更新**。

向 XaaS 蓝图表单添加文本元素

您可以插入文本框，向表单添加一些描述性文本。

前提条件

- 以**租户管理员**或 **XaaS 架构师**身份登录到 vRealize Automation。

- 添加 XaaS 蓝图。

步骤

- 1 选择设计 > XaaS > XaaS 蓝图。
- 2 单击要编辑的 XaaS 蓝图。
- 3 单击**蓝图表单**选项卡。
- 4 将**文本**元素从“新字段”窗格拖动到“表单页面”窗格。
- 5 输入要添加的文本。
- 6 单击该元素的外部以保存更改。
- 7 单击**更新**。

设计资源操作表单

创建资源操作时，您可以采用以下方式编辑该操作的表单：向表单添加新字段、修改现有字段、删除或重新排列字段。此外，您还可以创建新表单和表单页面，并将新字段拖放到其中。

添加新资源操作表单

当您编辑工作流默认生成而且要作为资源操作发布的表单时，您可以添加新资源操作表单。

通过添加新资源操作表单，您可定义已提交操作的详细信息页面的外观。如果不添加已提交操作的详细信息表单，则使用者将看到操作表单中定义的内容。

前提条件

- 以**租户管理员**或 **XaaS 架构师**身份登录到 vRealize Automation。
- [创建资源操作](#)。

步骤

- 1 选择设计 > XaaS > 资源操作。
- 2 单击要编辑的资源操作。
- 3 单击**表单**选项卡。
- 4 单击**新建表单**图标 (+)。
- 5 输入名称和可选描述。
- 6 从**屏幕类型**菜单中选择屏幕类型。

选项	描述
操作表单	使用者在决定运行置备后操作时看到的默认资源操作表单。
已提交操作的详细信息	使用者请求操作后决定在 部署 选项卡中查看请求详细信息时看到的请求详细信息页面。

- 7 单击**提交**。

后续步骤

通过将所需的字段从“新字段”窗格拖动到“表单页面”窗格，即可添加这些字段。

向资源操作表单添加新元素

当您编辑资源操作默认生成的表单时，您可以向表单添加预定义的新元素。例如，如果不想使用默认生成的字段，则可将其删除并替换为新字段。

前提条件

- 以**租户管理员**或**XaaS 架构师**身份登录到 vRealize Automation。
- [创建资源操作](#)。

步骤

- 1 选择**设计 > XaaS > 资源操作**。
- 2 单击要编辑的资源操作。
- 3 单击**表单**选项卡。
- 4 从“新字段”窗格中拖动一个元素，并将其放入“表单页面”窗格。
- 5 在 **ID** 文本框中输入 workflow 输入参数的 ID。
- 6 在**标签**文本框中输入一个标签。
- 7 （可选）从**类型**下拉菜单中选择字段的类型。
- 8 在**实体类型**文本框中输入 vRealize Orchestrator 对象，然后按 Enter。

并非所有字段类型均需执行该步骤。

选项	描述
结果类型	如果使用脚本操作定义字段的外部值，请输入 vRealize Orchestrator 脚本操作的结果类型。
输入参数	如果使用该字段接受使用者输入并将参数传递回 vRealize Orchestrator，请输入 vRealize Orchestrator 工作流接受的输入参数的类型。
输出参数	如果使用该字段向使用者显示信息，请输入 vRealize Orchestrator 工作流的输出参数的类型。

- 9 （可选）选中**多个值**复选框，允许使用者选择多个对象。

该选项并非对所有字段类型均可用。

- 10 单击**提交**。
- 11 单击**完成**。

后续步骤

您可以编辑元素来更改默认设置，并应用各种限制或值。

编辑资源操作元素

您可以在资源操作的“表单”页面中编辑元素的某些特征。您可以更改元素的类型及其默认值，并应用各种限制和值。

前提条件

- 以租户管理员或 **XaaS 架构师** 身份登录到 vRealize Automation。
- [创建资源操作](#)。

步骤

- 1 选择 **设计 > XaaS > 资源操作**。
- 2 单击要编辑的资源操作。
- 3 单击 **表单** 选项卡。
- 4 找到要编辑的元素。
- 5 单击 **编辑** 图标 (✎)。
- 6 在 **标签** 文本框中输入字段的新名称，更改使用者看到的标签。
- 7 在 **描述** 文本框中编辑描述。
- 8 从 **类型** 下拉菜单中选择一个选项，更改元素的显示名称。
这些选项因编辑的元素类型而异。
- 9 从 **大小** 下拉菜单中选择一个选项，更改元素的大小。
- 10 从 **标签大小** 下拉菜单中选择一个选项，更改标签的大小。
- 11 编辑元素的默认值。

选项	描述
未设置	从 vRealize Orchestrator 工作流展示中获取所编辑元素的值。
常数	将编辑元素的默认值设置为指定的常数值。
字段	将元素的默认值绑定到表示中另一个元素的参数。
条件	应用条件。通过使用条件，您可以创建各种子句和表达式并将其应用于元素。
外部	选择 vRealize Orchestrator 脚本操作以定义该值。

- 12 将 **限制** 选项卡中的限制应用于元素。

选项	描述
未设置	从 vRealize Orchestrator 工作流展示中获取所编辑元素的值。
常数	将编辑元素的默认值设置为指定的常数值。
字段	将元素的默认值绑定到表示中另一个元素的参数。

选项	描述
条件	应用条件。通过使用条件，您可以创建各种子句和表达式并将其应用于元素。
外部	选择 vRealize Orchestrator 脚本操作以定义该值。

13 在值选项卡中添加元素的一个或多个值。

可用选项取决于编辑的元素类型。

选项	描述
未设置	从 vRealize Orchestrator 工作流展示中获取所编辑元素的值。
预定义值	<p>从 vRealize Orchestrator 清单的相关对象列表中选择值。</p> <ol style="list-style-type: none"> 在预定义值搜索框中输入一个值来搜索 vRealize Orchestrator 清单。 从搜索结果中选择一个值，然后按 Enter。
值	<p>使用标签定义自定义值。</p> <ol style="list-style-type: none"> 在值文本框中输入一个值。 在标签文本框中输入该值的标签。 单击添加图标 ()。
外部值	<p>选择 vRealize Orchestrator 脚本操作，使用工作流不直接公开的信息定义值。</p> <ul style="list-style-type: none"> ■ 选择添加外部值。 ■ 选择 vRealize Orchestrator 脚本操作。 ■ 单击提交。

14 单击**提交**。

15 单击**更新**。

在资源操作表单中插入部分标题

您可以插入部分标题，将表单拆分为多个部分。

前提条件

- 以**租户管理员**或 **XaaS 架构师**身份登录到 vRealize Automation。
- [创建资源操作](#)。

步骤

- 1 选择**设计 > XaaS > 资源操作**。
- 2 单击要编辑的资源操作。
- 3 单击**表单**选项卡。
- 4 将**部分标题**元素从“表单”窗格拖动到“表单页面”窗格。
- 5 键入该部分的名称。
- 6 单击该元素的外部以保存更改。
- 7 单击**完成**。

向资源操作表单添加文本元素

您可以插入文本框，向表单添加一些描述性文本。

前提条件

- 以**租户管理员**或 **XaaS 架构师** 身份登录到 vRealize Automation。
- [创建资源操作](#)。

步骤

- 1 选择**设计 > XaaS > 资源操作**。
- 2 单击要编辑的资源操作。
- 3 单击**表单**选项卡。
- 4 将**文本**元素从“新字段”窗格拖动到“表单页面”窗格。
- 5 输入要添加的文本。
- 6 单击该元素的外部以保存更改。
- 7 单击**完成**。

XaaS 示例和场景

这些示例和场景提供了许多建议方式，供您在使用 XaaS 蓝图和资源操作时有效利用 vRealize Automation 完成常见任务。

创建用于创建和修改用户的 XaaS 蓝图和操作

通过使用 XaaS，您可以创建和发布目录项，以便在组中置备用户。还可以将新的置备后操作与已置备用户相关联。例如，将某个操作与已置备用户相关联，以便服务目录用户更改用户密码。

作为 XaaS 架构师，您可以创建自定义资源、XaaS 蓝图并发布用于创建用户的目录项。此外，您还可以创建用于更改用户密码的资源操作。

作为目录管理员，您可以创建服务并将蓝图目录项包括在该服务中。此外，您还可以通过使用表单设计器来编辑目录项的工作流展示，并更改使用者查看请求表单的方式。

作为业务组主管或租户管理员，您可以将新创建的服务、目录项和资源操作授权给使用者。

前提条件

确认已正确配置 Active Directory 插件，且您有权在 Active Directory 中创建用户。

步骤

- 1 [将测试用户创建为自定义资源](#)

您可以创建自定义资源并将其映射到 vRealize Orchestrator 对象类型 **AD:User**。

2 创建用于创建用户的 XaaS 蓝图

您可以创建 XaaS “在组中创建用户” 蓝图，以便运行相应的工作流，从而添加 Active Directory 用户并将该用户分配给 Active Directory 组。您可以将该蓝图创建为独立 XaaS 蓝图或蓝图组件。在此场景中，您创建的是独立蓝图。

3 创建资源操作以更改用户密码

您可以创建资源操作，允许 XaaS 使用者创建用户蓝图，以便在置备用户后更改用户的密码。

4 创建服务并将“创建测试用户”蓝图添加到服务中

您可以创建服务，使“创建用户”目录项显示在服务目录中。

5 将服务和资源操作授权给使用者

业务组主管和租户管理员可以将该服务和资源操作授权给用户或用户组。向用户或用户组授权之后，他们可以在其目录中查看该服务，还可以请求该服务中包含的“创建测试用户”目录项。使用者置备该项后，可以请求更改用户密码。

将测试用户创建为自定义资源

您可以创建自定义资源并将其映射到 vRealize Orchestrator 对象类型 AD:User。

前提条件

以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

1 选择 **设计 > XaaS > 自定义资源**。

2 单击 **新建** 图标 (+)。

3 在 **Orchestrator 类型** 文本框中输入 **AD:User**，然后按 Enter。

4 在列表中选择 **AD:User**。

5 键入该资源的名称。

例如，**Test User**。

6 输入该资源的描述。

例如，

This is a test custom resource that I will use for my catalog item to create a user in a group.

7 单击 **下一步**。

8 保留表单中的默认值。

9 单击 **完成**。

结果

您已创建“测试用户”自定义资源，并且可以在“自定义资源”页面中看到它。

后续步骤

创建 XaaS 蓝图。

创建用于创建用户的 XaaS 蓝图

您可以创建 XaaS “在组中创建用户” 蓝图，以便运行相应的工作流，从而添加 Active Directory 用户并将该用户分配给 Active Directory 组。您可以将该蓝图创建为独立 XaaS 蓝图或蓝图组件。在此场景中，您创建的是独立蓝图。

前提条件

- 确认您已创建支持置备 Active Directory 用户的自定义资源操作。请参见[将测试用户创建为自定义资源](#)。
- 以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

- 1 选择 **设计 > XaaS > XaaS 蓝图**。
- 2 单击 **新建** 图标 (+)。
- 3 在“选择工作流”窗格中，导航到 **Orchestrator > 库 > Microsoft > Active Directory > 用户**，然后选择 **在组中创建用户** 工作流。
- 4 单击 **下一步**。
- 5 配置 **常规** 选项卡选项。
 - a 将蓝图的名称更改为 **创建测试用户**，并使描述保持不变。
 - b 取消选中 **可在设计画布中用作组件** 复选框。
 您直接将此蓝图发布到服务目录，而不是在设计画布中将其用作蓝图组件。无需配置任何缩小或扩大工作流。
组件生命周期 选项卡即会从用户界面中移除。
- 6 单击 **下一步**。
- 7 编辑蓝图表单。
 - a 单击 **Win2000** 表单中的域名。
 - b 单击 **限制** 选项卡。
 - c 单击 **值** 下拉箭头，在下拉菜单中选择 **常数**，然后输入 **test.domain**。
 - d 单击 **可见** 下拉箭头，在下拉菜单中选择 **常数**，然后在下拉菜单中选择 **否**。
 您已将域名设置为对目录项的使用者不可见。
 - e 单击 **应用** 以保存更改。
- 8 单击 **下一步**。
- 9 选择 **newUser [Test User]** 作为要置备的输出参数。
- 10 单击 **下一步**。

11 单击**完成**。

12 在 **XaaS 蓝图** 页面上，选择**创建测试用户**行并单击**发布**。

结果

您已创建用于创建测试用户的蓝图，并使该蓝图可供添加到服务中。

后续步骤

创建要在已置备用户帐户上运行的操作。请参见[创建资源操作以更改用户密码](#)。

创建资源操作以更改用户密码

您可以创建资源操作，允许 XaaS 使用者创建用户蓝图，以便在置备用户后更改用户的密码。

前提条件

- 以 **XaaS 架构师** 身份登录到 vRealize Automation。
- 确认您已创建支持置备 Active Directory 用户的自定义资源操作。请参见[将测试用户创建为自定义资源](#)。

步骤

- 1 选择**设计 > XaaS > 资源操作**。
- 2 单击**新建**图标 (+)。
- 3 导航到 vRealize Orchestrator 工作流库中的 **Orchestrator > 库 > Microsoft > Active Directory > 用户**，然后选择**更改用户密码**工作流。
- 4 单击**下一步**。
- 5 从**资源类型**下拉菜单中选择**测试用户**。
此选项是您以前创建的自定义资源。
- 6 从**输入参数**下拉菜单中选择 **user**。
- 7 单击**下一步**。
- 8 将资源操作的名称更改为**更改测试用户的密码**，然后使描述与**详细信息**选项卡上显示的一样。
- 9 单击**下一步**。
- 10 （可选）将表单保持不变。
- 11 单击**完成**。
- 12 在“资源操作”页面上，选择**更改测试用户的密码**行并单击**发布**。

结果

您已创建用于更改用户密码的资源操作，并使其可供添加到授权中。

后续步骤

将“创建测试用户”蓝图添加到服务中。请参见[创建服务并将“创建测试用户”蓝图添加到服务中](#)。

创建服务并将“创建测试用户”蓝图添加到服务中

您可以创建服务，使“创建用户”目录项显示在服务目录中。

前提条件

- 以**租户管理员**或**目录管理员**身份登录到 vRealize Automation。
- 确认您已创建 XaaS 蓝图。请参见[创建用于创建用户的 XaaS 蓝图](#)。

以**租户管理员**或**目录管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 目录管理 > 服务**。
- 2 单击**新建**图标 (+)。
- 3 输入 **Active Directory 测试用户** 作为该服务的名称。
- 4 从**状态**下拉菜单中选择**活动**。
- 5 将其他文本框留空。
- 6 单击**确定**。
- 7 在“服务”列表中，选择 **Active Directory 测试用户** 行并单击**管理目录项**。
- 8 单击**新建**图标 (+)。
- 9 选择**创建测试用户**，然后单击**确定**。

XaaS “创建测试用户”蓝图已添加到目录项列表中。

- 10 单击**关闭**。

结果

“Active Directory 测试用户”服务现在包括“创建测试用户”蓝图。无需向服务添加操作。

后续步骤

您可以授权用户请求该蓝图并运行相应操作。请参见[将服务和资源操作授权给使用者](#)。

将服务和资源操作授权给使用者

业务组主管和租户管理员可以将该服务和资源操作授权给用户或用户组。向用户或用户组授权之后，他们可以在其目录中查看该服务，还可以请求该服务中包含的“创建测试用户”目录项。使用者置备该项后，可以请求更改用户密码。

前提条件

- 以**租户管理员**或**业务组主管**身份登录到 vRealize Automation。
- 验证“创建用户”蓝图是否已添加到服务中。请参见[创建服务并将“创建测试用户”蓝图添加到服务中](#)。
- 验证“更改用户密码”资源操作是否存在。请参见[创建资源操作以更改用户密码](#)。

步骤

- 1 选择**管理 > 目录管理 > 授权**。
- 2 单击**新建**图标 (+)。
- 3 在**名称**文本框中输入 **Create an Active Directory user**。
- 4 将**描述**和**过期日期**文本框留空。
- 5 从**状态**下拉菜单中选择**活动**。
- 6 从**业务组**下拉菜单中选择目标业务组。

例如 IT 客户经理。

- 7 选择**所有用户和组**以授权让业务组（例如 IT 客户经理）的所有成员创建用户帐户。

所选用户可以在目录中查看服务及其包含的目录项。这些用户可以在创建用户帐户之后对该用户帐户运行“更改密码”操作。

- 8 单击**下一步**。
- 9 在**授权的服务**文本框中，输入 **Active Directory Test User**，然后按 Enter 键。
- 10 在**授权的操作**文本框中，输入 **Change the password of the Test User**，然后按 Enter 键。
- 11 单击**完成**。

结果

您已创建活动授权，因此属于 IT 客户经理业务组成员的用户可以创建用户。置备用户之后，上述用户可以对已置备的用户帐户运行“更改密码”资源操作。

后续步骤

以已获授权创建 Active Directory 用户的用户身份登录。在**目录**选项卡上，验证 XaaS 蓝图是否按预期创建用户。创建用户之后，从**部署**选项卡中运行“更改密码”操作。

创建并发布一个迁移虚拟机的 XaaS 操作

您可以创建并发布 XaaS 资源操作，用于扩展使用者可对 IaaS 置备的 vSphere 虚拟机执行的操作。

在此方案中，您可以创建用于快速迁移 vSphere 虚拟机的资源操作。

前提条件

以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

- 1 **创建资源操作以迁移 vSphere 虚拟机**

您可以创建自定义资源操作，允许使用者在通过 IaaS 置备 vSphere 虚拟机后迁移 vSphere 虚拟机。

2 发布迁移 vSphere 虚拟机的操作

要将“快速迁移虚拟机”资源操作用作置备后操作，您必须发布该资源操作。

创建资源操作以迁移 vSphere 虚拟机

您可以创建自定义资源操作，允许使用者在通过 IaaS 置备 vSphere 虚拟机后迁移 vSphere 虚拟机。

步骤

- 1 选择设计 > XaaS > 资源操作。
- 2 单击添加 (+)。
- 3 导航到 vRealize Orchestrator 工作流库中的 **Orchestrator > 库 > vCenter > 虚拟机管理 > 移动和迁移**，然后选择**快速迁移虚拟机**工作流。
- 4 单击下一步。
- 5 从**资源类型**下拉菜单中选择 **IaaS VC VirtualMachine**。
- 6 从**输入参数**下拉菜单中选择 **vm**。
- 7 单击下一步。
- 8 使资源操作的名称和描述与**详细信息**选项卡上显示的一样。
- 9 单击下一步。
- 10 将表单保持不变。
- 11 单击完成。

结果

您已创建用于迁移虚拟机的资源操作，并且可以看到它在“资源操作”页面中列出。

后续步骤

发布迁移 vSphere 虚拟机的操作

发布迁移 vSphere 虚拟机的操作

要将“快速迁移虚拟机”资源操作用作置备后操作，您必须发布该资源操作。

步骤

- 1 选择设计 > XaaS > 资源操作。
- 2 选择“快速迁移虚拟机”资源操作所在的行，然后单击**发布**按钮。

结果

您已创建 vRealize Orchestrator 工作流并将其作为资源操作发布。您可以导航到**管理 > 目录管理 > 操作**，并在操作列表中查看“快速迁移虚拟机”资源操作。您可以为该资源操作分配图标。请参见[为 XaaS 资源操作分配图标](#)。

后续步骤

将该操作添加到包含已置备 IaaS 的 vSphere 虚拟机的授权中。请参见[将服务、目录项和操作授权给用户](#)。

创建一个通过 vMotion 迁移虚拟机的 XaaS 操作

通过使用 XaaS，您可以创建和发布资源操作，用于通过 vMotion 迁移 IaaS 置备的虚拟机。

在此方案中，您可以创建资源操作，通过 vMotion 迁移 vSphere 虚拟机。此外，还可以通过使用表单设计器来编辑工作流展示，并更改使用者在提交请求后查看该操作的方式。

前提条件

以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

1 创建一个通过 vMotion 迁移 vSphere 虚拟机的操作

您可以创建自定义资源操作，允许服务目录用户在通过 IaaS 置备计算机后通过 vMotion 迁移 vSphere 虚拟机。

2 编辑资源操作表单

资源操作表单映射 vRealize Orchestrator 工作流展示。您可以编辑该表单，并定义资源操作的使用者在决定运行置备后操作时看到的内容。

3 添加已提交操作的详细信息表单并保存操作

您可以将新表单添加到“通过 vMotion 迁移虚拟机”资源操作，定义使用者在请求运行置备后操作之后将看到哪些内容。

4 发布通过 vMotion 迁移虚拟机的操作

要将“通过 vMotion 迁移虚拟机”资源操作用作置备后操作，您必须发布该资源操作。

创建一个通过 vMotion 迁移 vSphere 虚拟机的操作

您可以创建自定义资源操作，允许服务目录用户在通过 IaaS 置备计算机后通过 vMotion 迁移 vSphere 虚拟机。

步骤

- 1 选择 **设计 > XaaS > 资源操作**。
- 2 单击 **添加 (+)**。
- 3 导航到 vRealize Orchestrator 工作流库中的 **Orchestrator > 库 > vCenter > 虚拟机管理 > 移动和迁移**，然后选择 **通过 vMotion 迁移虚拟机** 工作流。
- 4 单击 **下一步**。
- 5 从 **资源类型** 下拉菜单中选择 **IaaS VC VirtualMachine**。
- 6 从 **输入参数** 下拉菜单中选择 **vm**。
- 7 单击 **下一步**。

8 使资源操作的名称和描述与**详细信息**选项卡上显示的一样。

9 单击**下一步**。

后续步骤

[编辑资源操作表单](#)。

编辑资源操作表单

资源操作表单映射 vRealize Orchestrator 工作流程展示。您可以编辑该表单，并定义资源操作的使用者在决定运行置备后操作时看到的内容。

步骤

1 单击**删除**图标 (✖) 以删除**池**元素。

2 编辑**主机**元素。

- a 单击**主机**字段旁边的**编辑**图标 (✎)。
- b 在**标签**文本框中键入 **Target host**。
- c 从**类型**下拉菜单中选择**搜索**。
- d 单击**限制**选项卡。
- e 从**必需**下拉菜单中选择**常数**，然后选择**是**。
您已将“主机”字段设置为“始终需要”。
- f 单击**提交**。

3 编辑**优先级**元素。

- a 单击**优先级**字段旁边的**编辑**图标 (✎)。
- b 在**标签**文本框中键入 **Priority of the task**。
- c 从**类型**下拉菜单中选择**单选按钮组**。
- d 单击**值**选项卡，然后取消选中**未设置**复选框。
- e 在**预定义值**搜索文本框中输入 **lowPriority**，然后按 Enter。
- f 在**预定义值**搜索文本框中输入 **defaultPriority**，然后按 Enter。
- g 在**预定义值**搜索文本框中输入 **highPriority**，然后按 Enter。
- h 单击**提交**。

当使用者请求资源操作时，会看到一个单选按钮组，其中包含以下三个单选按钮：**lowPriority**、**defaultPriority** 和 **highPriority**。

4 编辑**状态**元素。

- a 单击**状态**字段旁边的**编辑**图标 (✎)。
- b 在**标签**文本框中键入 **Virtual machine state**。

- c 从**类型**下拉菜单中选择**下拉字段**。
- d 单击**值**选项卡，然后取消选中**未设置复选框**。
- e 在**预定义值**搜索文本框中输入 **poweredOff**，然后按 Enter。
- f 在**预定义值**搜索文本框中输入 **poweredOn**，然后按 Enter。
- g 在**预定义值**搜索文本框中输入 **suspended**，然后按 Enter。
- h 单击**提交**。

当使用者请求资源操作时，会看到一个下拉菜单，其中包含以下三个选项：**poweredOff**、**poweredOn** 和 **suspended**。

结果

您已编辑“通过 vMotion 迁移虚拟机”工作流的工作流展示。



后续步骤

[添加已提交操作的详细信息表单并保存操作。](#)

添加已提交操作的详细信息表单并保存操作

您可以将新表单添加到“通过 vMotion 迁移虚拟机”资源操作，定义使用者在请求运行置备后操作之后将看到哪些内容。

步骤

- 1 单击**新建表单**图标 ()，该图标位于**表单**下拉菜单旁边。
- 2 在**名称**文本框中键入 **Submitted action**。
- 3 将**描述**字段留空。
- 4 从**屏幕类型**菜单中选择**已提交操作的详细信息**。
- 5 单击**提交**。
- 6 单击**表单**页面下拉菜单旁边的**编辑**图标 ()。
- 7 在**标题**文本框中键入**详细信息**。
- 8 单击**提交**。
- 9 从“表单”窗格中拖动**文本**元素，并将其放入**表单**页面。
- 10 键入
You submitted a request to migrate your machine with vMotion. Wait until the process completes successfully.
- 11 单击该文本框的外部以保存更改。
- 12 单击**提交**。
- 13 单击**添加**。

结果

您已创建要通过 vMotion 迁移虚拟机的资源操作，并且可以看到它在“资源操作”页面中列出。

后续步骤

发布通过 [vMotion 迁移虚拟机的操作](#)。

发布通过 vMotion 迁移虚拟机的操作

要将“通过 vMotion 迁移虚拟机”资源操作用作置备后操作，您必须发布该资源操作。

步骤

- 1 选择设计 > **XaaS** > 资源操作。
- 2 选择“通过 vMotion 迁移虚拟机”操作所在的行，然后单击**发布**按钮。

结果

您已创建 vRealize Orchestrator 工作流并将其作为资源操作发布。您可以导航到**管理 > 目录管理 > 操作**，并在操作列表中查看“通过 vMotion 迁移虚拟机”资源操作。您可以为该资源操作分配图标。请参见 [为 XaaS 资源操作分配图标](#)。

您还编辑了工作流展示并定义了该操作的外观。

后续步骤

业务组主管和租户管理员可以将“通过 vMotion 迁移虚拟机”资源操作包括在授权中。有关如何为虚拟平台创建和发布 IaaS 蓝图的信息，请参见[设计计算机蓝图](#)。

创建并发布一个生成快照的 XaaS 操作

通过使用 XaaS，您可以创建和发布资源操作，为通过 IaaS 置备的 vSphere 虚拟机生成快照。

在此方案中，您可以创建资源操作，为通过 IaaS 置备的 vSphere 虚拟机生成快照。此外，还可以通过使用表单设计器来编辑工作流展示，并更改使用者在提交请求后查看该操作的方式。

前提条件

以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

- 1 [创建一个生成 vSphere 虚拟机快照的操作](#)
您可以创建自定义资源操作，允许使用者在通过 IaaS 置备计算机后生成 vSphere 虚拟机的快照。
- 2 [发布生成快照的操作](#)
要将“创建快照”资源操作用作置备后操作，您必须发布该资源操作。

创建一个生成 vSphere 虚拟机快照的操作

您可以创建自定义资源操作，允许使用者在通过 IaaS 置备计算机后生成 vSphere 虚拟机的快照。

步骤

- 1 选择设计 > **XaaS** > 资源操作。

- 2 单击**添加 (+)**。
- 3 导航到 vRealize Orchestrator 工作流库中的 **Orchestrator > 库 > vCenter > 虚拟机管理 > 快照**，然后选择**创建快照**工作流。
- 4 单击**下一步**。
- 5 从**资源类型**下拉菜单中选择 **IaaS VC VirtualMachine**。
- 6 从**输入参数**下拉菜单中选择 **vm**。
- 7 单击**下一步**。
- 8 使资源操作的名称和描述与**详细信息**选项卡上显示的一样。
- 9 单击**下一步**。
- 10 将表单保持不变。
- 11 单击**添加**。

结果

您已创建用于生成虚拟机快照的资源操作，并且可以看到它在“资源操作”页面中列出。

后续步骤

[发布生成快照的操作](#)。

发布生成快照的操作

要将“创建快照”资源操作用作置备后操作，您必须发布该资源操作。

步骤

- 1 选择**设计 > XaaS > 资源操作**。
- 2 选择“创建快照”操作所在的行，然后单击**发布**按钮。

结果

您已创建 vRealize Orchestrator 工作流并将其作为资源操作发布。您可以导航到**管理 > 目录管理 > 操作**，并在操作列表中查看“创建快照”资源操作。您可以为该资源操作分配图标。请参见[为 XaaS 资源操作分配图标](#)。

后续步骤

业务组主管和租户管理员可以将“创建快照”资源操作包括在授权中。有关如何为虚拟平台创建和发布 IaaS 蓝图的信息，请参见[设计计算机蓝图](#)。

创建并发布一个启动 Amazon 虚拟机的 XaaS 操作

通过使用 XaaS，您可以创建和发布操作，用于扩展使用者可对第三方置备的资源执行的操作。

在此方案中，您可以创建和发布用于快速启动 Amazon 虚拟机的资源操作。

前提条件

- 在默认的 vRealize Orchestrator 服务器上安装适用于 Amazon Web Services 的 vRealize Orchestrator 插件。
- 为 Amazon 实例的资源映射创建或导入 vRealize Orchestrator 工作流。

步骤

1 为 Amazon 实例创建资源映射

您可以创建资源映射，把使用 IaaS 置备的 Amazon 实例与 Amazon Web Services 插件公开 vRealize Orchestrator 类型 AWS:EC2Instance 关联起来。

2 创建资源操作以启动 Amazon 虚拟机

您可以创建资源操作，让使用者能够启动已置备的 Amazon 虚拟机。

3 发布启动 Amazon 实例的操作

要使用新创建的“启动实例”资源操作在 Amazon 虚拟机上进行置备后操作，您必须发布该资源操作。

为 Amazon 实例创建资源映射

您可以创建资源映射，把使用 IaaS 置备的 Amazon 实例与 Amazon Web Services 插件公开 vRealize Orchestrator 类型 AWS:EC2Instance 关联起来。

前提条件

- 以 **XaaS 架构师** 身份登录到 vRealize Automation。
- 创建或导入 vRealize Orchestrator 资源映射工作流或脚本操作。

步骤

- 1 选择设计 > **XaaS** > 资源映射。
- 2 单击添加 (+)。
- 3 在名称文本框中输入 **EC2 实例**。
- 4 在目录资源类型文本框中输入 **云计算机**。
- 5 在 **Orchestrator 类型** 文本框中输入 **AWS:EC2Instance**。
- 6 选择 **始终可用**。
- 7 选择要使用的资源映射类型。
- 8 从 vRealize Orchestrator 库中选择自定义资源映射脚本操作或工作流。
- 9 单击添加。

结果

您可以使用 Amazon 资源映射为通过使用 IaaS 置备的 Amazon 计算机创建资源操作。

后续步骤

创建资源操作以启动 Amazon 虚拟机。

创建资源操作以启动 Amazon 虚拟机

您可以创建资源操作，让使用者能够启动已置备的 Amazon 虚拟机。

前提条件

以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

- 1 选择 **设计 > XaaS > 资源操作**。
- 2 单击 **添加 (+)**。
- 3 选择 **Orchestrator > 库 > Amazon Web Services > Elastic Cloud > 实例**，然后选择工作流文件夹中的 **启动实例** 工作流。
- 4 单击 **下一步**。
- 5 从 **资源类型** 下拉菜单中选择 **EC2 实例**。
这是您以前创建的资源映射的名称。
- 6 从 **输入参数** 下拉菜单中选择 **instance**。
这是要与资源映射匹配的资源操作工作流的输入参数。
- 7 单击 **下一步**。
- 8 将名称和描述保持不变。
资源操作的默认名称为“启动实例”。
- 9 单击 **下一步**。
- 10 使这些字段与 **表单** 选项卡上显示的一样。
- 11 单击 **添加**。

结果

您已创建用于启动 Amazon 虚拟机的资源操作，并且可以在“资源操作”页面中看到它。

后续步骤

发布启动 Amazon 实例的操作。

发布启动 Amazon 实例的操作

要使用新创建的“启动实例”资源操作在 Amazon 虚拟机上进行置备后操作，您必须发布该资源操作。

前提条件

以 **XaaS 架构师** 身份登录到 vRealize Automation。

步骤

- 1 选择设计 > **XaaS** > 资源操作。
- 2 选择“启动实例”资源操作所在的行，然后单击发布。

结果

“启动实例”资源操作的状态会变为“已发布”。

后续步骤

将“启动实例”操作添加到包括 Amazon 目录项的授权中。请参见[将服务、目录项和操作授权给用户](#)。

对 XaaS 蓝图中不正确的重音字符和特殊字符进行故障排除

针对使用非 ASCII 字符串的语言创建 XaaS 蓝图时，重音字符和特殊字符显示为不可用字符串。

原因

可能已启用默认情况下未设置的 vRealize Orchestrator 配置属性。

解决方案

- 1 在 Orchestrator 服务器系统中，导航到 `/etc/vco/app-server/`。
- 2 在文本编辑器中打开 `vmo.properties` 配置文件。
- 3 验证是否已停用以下属性。

```
com.vmware.o11n.webview.htmlescaping.disabled
```

- 4 保存 `vmo.properties` 文件。
- 5 重新启动 vRealize Orchestrator 服务器。

发布蓝图

蓝图以草稿状态保存。您必须先手动发布蓝图，然后才能将其配置为目录项或用作设计画布中的蓝图组件。

发布蓝图之后，您可以对其授权，使其可用于服务目录中的置备请求。

只需发布蓝图一次即可。您对已发布蓝图所作的任何更改都会自动反映在目录和嵌套蓝图组件中。

发布蓝图

您可以发布蓝图供计算机置备使用，也可以选择发布蓝图供其他蓝图重用。要使用该蓝图请求计算机置备，您必须在蓝图发布后为该蓝图授权。在其他蓝图中用作组件的蓝图不需要授权。

前提条件

- 以**基础架构架构师**身份登录到 vRealize Automation。
- 创建蓝图。请参见《用于创建 vRealize Automation 蓝图的对照表》。

步骤

- 1 单击**设计**选项卡。
- 2 单击**蓝图**。
- 3 指向要发布的蓝图，然后单击**发布**。
- 4 单击**确定**。

结果

该蓝图作为目录项发布，但您必须先对其授权，将其提供给服务目录中的用户。

后续步骤

将该蓝图添加到服务目录，并授权用户请求该目录项进行计算机置备，如蓝图中所定义。

使用开发人员驱动的蓝图

除了用户界面驱动的 vRealize Automation 蓝图创建方法，您也可以通过编程方式使用 vRealize CloudClient 等工具，使用独立提供或采购的蓝图，以及与其他开发人员协作使用 vRealize Suite 应用程序、工作流和第三方工具。

有关这些方法的信息，请参见以下主题：

- [导出和导入蓝图和内容](#)
- [下载和配置提供的独立蓝图](#)
- [在多开发人员环境中创建蓝图和其他 IaaS 内容](#)

导出和导入蓝图和内容

使用 vRealize Automation REST API 或使用 vRealize CloudClient，可以通过编程方式将一个 vRealize Automation 环境中的蓝图和内容导出到另一个环境。

例如，您可以在开发环境中创建和测试蓝图，然后将它们导入生产环境。或者，您也可以将社区论坛中的属性定义导入活动的 vRealize Automation 租户实例。

您可以通过编程方式导入和导出以下任何 vRealize Automation 内容项：

- 应用程序蓝图及其所有组件
- IaaS 计算机蓝图
- Software 组件
- XaaS 蓝图
- 组件配置文件
- 属性组

属性组信息是特定于租户的，仅当目标 vRealize Automation 实例中已存在属性组，才能随蓝图导入该信息。

将蓝图从一个 vRealize Automation 实例租户导出到另一个时，如果目标租户实例中不存在该属性组，则为该蓝图定义的属性组信息不会被导入的蓝图识别。例如，如果导入的蓝图包含名为 `mica1` 的属性组，如果 `mica1` 属性组不存在于导入蓝图的 vRealize Automation 实例中，则 `mica1` 属性组不会显示在导入的蓝图中。为避免从一个 vRealize Automation 实例向另一个实例导出蓝图时丢失属性组信息，请使用 vRealize CloudClient 创建包含该属性组的导出包 zip 文件，并在导入蓝图前将该导出包 zip 文件导入目标租户。有关使用 vRealize CloudClient 列出、打包、导出和导入属性组以及有关其他 vRealize Automation 项的详细信息，请参见 <https://developercenter.vmware.com/tool/cloudclient> 的 VMware 开发人员中心。

表 3-63. 选择导入和导出工具

工具	更多信息
vRealize CloudClient	请参见 VMware code.vmware.com 站点上的 vRealize CloudClient 页面，网址为： https://developercenter.vmware.com/tool/cloudclient 。
vRealize Automation REST API	请参见 VMware API Explorer 中 vRealize Automation 对应的 API 文档，网址为： https://code.vmware.com/apis/vrealize-automation 。

注 在 vRealize Automation 部署中采用编程方式导出和导入蓝图时，例如在测试和生产环境之间或者在一个组织和另一个组织之间，识别克隆模板数据是否包含在软件包中十分重要。导入蓝图软件包时，将基于软件包中的信息对默认设置进行填充。例如，如果导出使用克隆工作流创建的蓝图后，再将其导入，而在导入蓝图的 vRealize Automation 部署的端点中，派生克隆数据的模板不存在，那么某些导入的蓝图设置将不适用于该部署。

场景：导入 Dukes Bank vSphere 示例应用程序并配置您的环境

作为评估或学习 vRealize Automation 的 IT 专业人员，您希望将稳健的示例应用程序导入到 vRealize Automation 实例，这样可以快速探索可用的功能，确定如何构建可以满足组织需求的 vRealize Automation 蓝图。

前提条件

- 准备 CentOS 6.x Linux 参考机，将它转换成模板，然后创建自定义规范。请参见[场景：准备导入 Dukes Bank vSphere 示例应用程序蓝图](#)。
- 创建外部网络配置文件以提供网关和 IP 地址范围。请参见[使用第三方 IPAM 提供程序创建外部网络配置文件](#)。
- 将外部网络配置文件映射到 vSphere 预留。请参见[为 Hyper-V、KVM、SCVMM、vSphere 或 XenServer 创建预留](#)。如果没有外部网络配置文件，示例应用程序无法成功置备。

- 验证您是否同时具有**基础架构架构师**和**软件架构师**特权。导入 Dukes Bank 示例应用程序以及与 Dukes Bank 蓝图和软件组件交互需要这两个角色。

步骤

1 场景：导入 Dukes Bank vSphere 示例应用程序

从 vRealize Automation 设备下载 Dukes Bank for vSphere 应用程序。将示例应用程序导入 vRealize Automation 租户可查看多层 vRealize Automation 蓝图的工作示例，其中包括多个含有网络与软件组件的计算机组件。

2 场景：为您的环境配置 Dukes Bank vSphere 示例组件

使用您的基础架构架构师特权配置每个 Dukes Bank 计算机组件，以便使用为环境创建的自定义规范、模板和计算机前缀。

结果

您已为环境配置了 Dukes Bank vSphere 示例应用程序，现在可以将它作为开发您自己的蓝图的起点，作为评估 vRealize Automation 的工具，或作为帮助您了解 vRealize Automation 功能和组件的学习资源。

场景：导入 Dukes Bank vSphere 示例应用程序

从 vRealize Automation 设备下载 Dukes Bank for vSphere 应用程序。将示例应用程序导入 vRealize Automation 租户可查看多层 vRealize Automation 蓝图的工作示例，其中包括多个含有网络与软件组件的计算机组件。

步骤

- 1 使用 SSH 以 root 身份登录到 vRealize Automation 设备。
- 2 将 Dukes Bank for vSphere 示例应用程序从 vRealize Automation 设备下载到 /tmp。

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/DukesBankAppForvSphere.zip
```

请勿解压缩软件包。

- 3 将 vRealize CloudClient 从 <http://developercenter.vmware.com/tool/cloudclient> 下载到 /tmp。
- 4 解压 cloudclient-4x-dist.zip 软件包。
- 5 在 /bin 目录下运行 vRealize CloudClient。

```
$>./bin/cloudclient.sh
```

- 6 如果出现提示，请接受许可协议。
- 7 使用 vRealize CloudClient，以具有**软件架构师**和**基础架构架构师**特权的用户身份登录到 vRealize Automation 设备。

```
CloudClient>vra login userpass --server https://vRealize_VA_Hostname_fqdn --user <user@domain.com> --tenant <TenantName>
```

- 8 出现提示时，输入登录密码。
- 9 验证 DukesBankAppForvSphere.zip 内容是否可用。

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run true --resolution OVERWRITE
```

请注意，OVERWRITE 条目对大小写敏感，需要使用大写。

通过将解析配置为覆盖，而不是跳过，允许 vRealize Automation 尽可能解决冲突。

- 10 导入 Dukes Bank 示例应用程序。

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run false --resolution OVERWRITE
```

请注意，OVERWRITE 条目对大小写敏感，需要使用大写。

结果

以具有软件架构师和基础架构架构师特权的用户身份登录到 vRealize Automation 控制台后，您可以在 **设计 > 蓝图** 选项卡和 **设计 > 软件组件** 选项卡上查看 Dukes Bank 蓝图和软件组件。

场景：为您的环境配置 Dukes Bank vSphere 示例组件

使用您的基础架构架构师特权配置每个 Dukes Bank 计算机组件，以便使用为环境创建的自定义规范、模板和计算机前缀。

此场景通过在 vSphere Web Client 中创建的模板配置用于克隆计算机的计算机组件。如果要基于快照创建可以节省空间的虚拟机副本，示例应用程序同样支持链接克隆。链接克隆使用增量磁盘链来跟踪与父虚拟机的差异；它可快速置备，减少存储成本，并且在性能优先级不高时使用最为理想。

步骤

- 1 以 **基础架构架构师** 身份登录到 vRealize Automation 控制台。

您可以仅使用 **基础架构架构师** 角色将 Dukes Bank 示例应用程序配置为在您的环境中工作，但若要看或编辑示例软件组件，则还需要 **软件架构师** 角色。

- 2 选择 **设计 > 蓝图**。

- 3 选择 **DukesBankApplication** 蓝图并单击 **编辑** 图标。

- 4 编辑 appserver-node，使 vRealize Automation 可以在环境中置备此计算机组件。

可以为置备此计算机组件的多个实例配置蓝图，以便验证负载均衡器节点的功能。

- a 单击设计画布中的 **appserver-node** 组件。

底部面板上将显示配置详细信息。

- b 从 **计算机前缀** 下拉菜单中选择计算机前缀。

- c 配置蓝图，通过选择实例（最少 2 个，最多 10 个）为此节点置备最少 2 个、最多 10 个实例。

在请求表单上，用户可以置备最少 2 个、最多 10 个 appserver 节点。如果已授权用户执行缩小和扩大操作，则用户可以缩放其部署以满足不断变化的需求。

- d 单击**构建信息**选项卡。
 - e 从**置备工作流**下拉菜单中选择 **CloneWorkflow**。
 - f 从**克隆源**对话框中选择 **dukes_bank_template**。
 - g 在**自定义规范**文本框中输入 **Customspecs_sample**。
此字段区分大小写。
 - h 单击**计算机资源**选项卡。
 - i 确认内存设置至少为 2048 MB。
- 5** 编辑 **loadbalancer-node**，这样 vRealize Automation 可以在环境中置备此计算机组件。
- a 单击设计画布中的 **loadbalancer-node** 组件。
 - b 从**计算机前缀**下拉菜单中选择计算机前缀。
 - c 单击**构建信息**选项卡。
 - d 从**置备工作流**下拉菜单中选择 **CloneWorkflow**。
 - e 从**克隆源**对话框中选择 **dukes_bank_template**。
 - f 在**自定义规范**文本框中输入 **Customspecs_sample**。
此字段区分大小写。
 - g 单击**计算机资源**选项卡。
 - h 确认内存设置至少为 2048 MB。
- 6** 对 **database-node** 计算机组件重复。
- 7** 单击**保存并完成**。
保存更改，并返回到**蓝图**选项卡。
- 8** 选择 **DukesBankApplication** 蓝图并单击**发布**。

结果

您为环境配置了 Dukes Bank 示例应用程序蓝图，并发布了已完成的蓝图。

后续步骤

在配置目录服务、将蓝图添加到服务并授权用户请求蓝图之前，已发布的蓝图不会显示给目录中的用户。
请参见[配置服务目录的对照表](#)。

配置在目录中显示 Dukes Bank 蓝图之后，可以请求置备示例应用程序。请参见[场景：测试 Dukes Bank 示例应用程序](#)。

场景：测试 Dukes Bank 示例应用程序

您请求 Dukes Bank 目录项，然后登录到示例应用程序验证所做的工作并查看 vRealize Automation 蓝图功能。

前提条件

- 导入 Dukes Bank 示例应用程序并配置蓝图组件，使其在环境中起作用。请参见[场景：导入 Dukes Bank vSphere 示例应用程序并配置您的环境](#)。
- 配置服务目录，使得已发布的 Dukes Bank 蓝图可供用户请求。请参见[配置服务目录的对照表](#)。
- 确认置备的虚拟机可以访问 YUM 存储库。

步骤

- 1 以有权访问 Dukes Bank 目录项的用户身份登录到 vRealize Automation 控制台。
- 2 单击**目录**选项卡。
- 3 找到 Dukes Bank 示例应用程序目录项，然后单击**请求**。
- 4 为每个带红色星号的组件填写所需的请求信息。
 - a 导航到 JBossAppServer 组件，填写所需的请求信息。
 - b 在 **app_content_server_ip** 文本框中，输入 vRealize Automation 设备的完全限定域名。
 - c 导航到 Dukes_Bank_App 软件组件，填写所需的请求信息。
 - d 在 **app_content_server_ip** 文本框中，输入 vRealize Automation 设备的完全限定域名。
- 5 单击**提交**。

根据网络和 vCenter Server 实例，可能需要大约 15-20 分钟时间来完全置备 Dukes Bank 示例应用程序。您可以在**部署**选项卡下监控状态。应用程序置备后，可以在**部署**选项卡上查看目录项详细信息。

- 6 置备应用程序后，找到负载均衡器服务器的 IP 地址，以便访问 Dukes Bank 示例应用程序。
 - a 单击**部署**。
 - b 找到 Dukes Bank 示例应用程序部署，然后单击部署名称。
 - c 在**组件**选项卡上，选择 Apache 负载均衡器服务器。
 - d 选择**网络**选项卡。
 - e 记下 IP 地址。

7 登录到 Dukes Bank 示例应用程序。

- a 导航到您的负载均衡器服务器，地址为：http://IP_Apache_Load_Balancer:8081/bank/main.faces。

如果您想要直接访问应用程序服务器，您可以导航到：http://IP_AppServer:8080/bank/main.faces。

- b 在用户名文本框中输入 **200**。
- c 在密码文本框中输入 **foobar**。

结果

您具有正常运行的 Dukes Bank 示例应用程序，现在可以将它作为开发您自己的蓝图的起点，作为评估 vRealize Automation 的工具，或作为帮助您了解 vRealize Automation 功能和组件的学习资源。

下载和配置提供的独立蓝图

您可以从 vRealize Automation 设备下载提供的独立蓝图及其关联的软件组件。

[下载和配置 vRealize Automation 独立蓝图](#)文档将指导您完成从 vRealize Automation 设备下载独立 vRealize Automation 蓝图，然后结合使用若干个 vRealize Orchestrator 工作流在 vRealize Automation 中导入、配置和使用该蓝图的整个过程。

在多开发人员环境中创建蓝图和其他 IaaS 内容

多个开发人员可以将 vRealize Orchestrator 工作流与 vRealize Suite 和第三方开发人员工具结合使用，以便在不同的 vRealize Automation 蓝图项目上同时处理相同或不同的 vRealize Automation 蓝图。

您可以使用 vRealize Suite Lifecycle Manager 等工具为 vRealize Automation 和其他 vRealize Suite 工具、OVA 以及 GitLab/GitHub、Houdini 等第三方工具和来自 [VMware Solutions Exchange](#) 的其他应用程序项目提供多开发人员环境。

要了解有关在多开发人员环境中创建 vRealize Automation 蓝图和其他 IaaS 内容（如属性、事件代理订阅、软件组件和 vRealize Orchestrator 工作流）的更多信息，请参见以下资源：

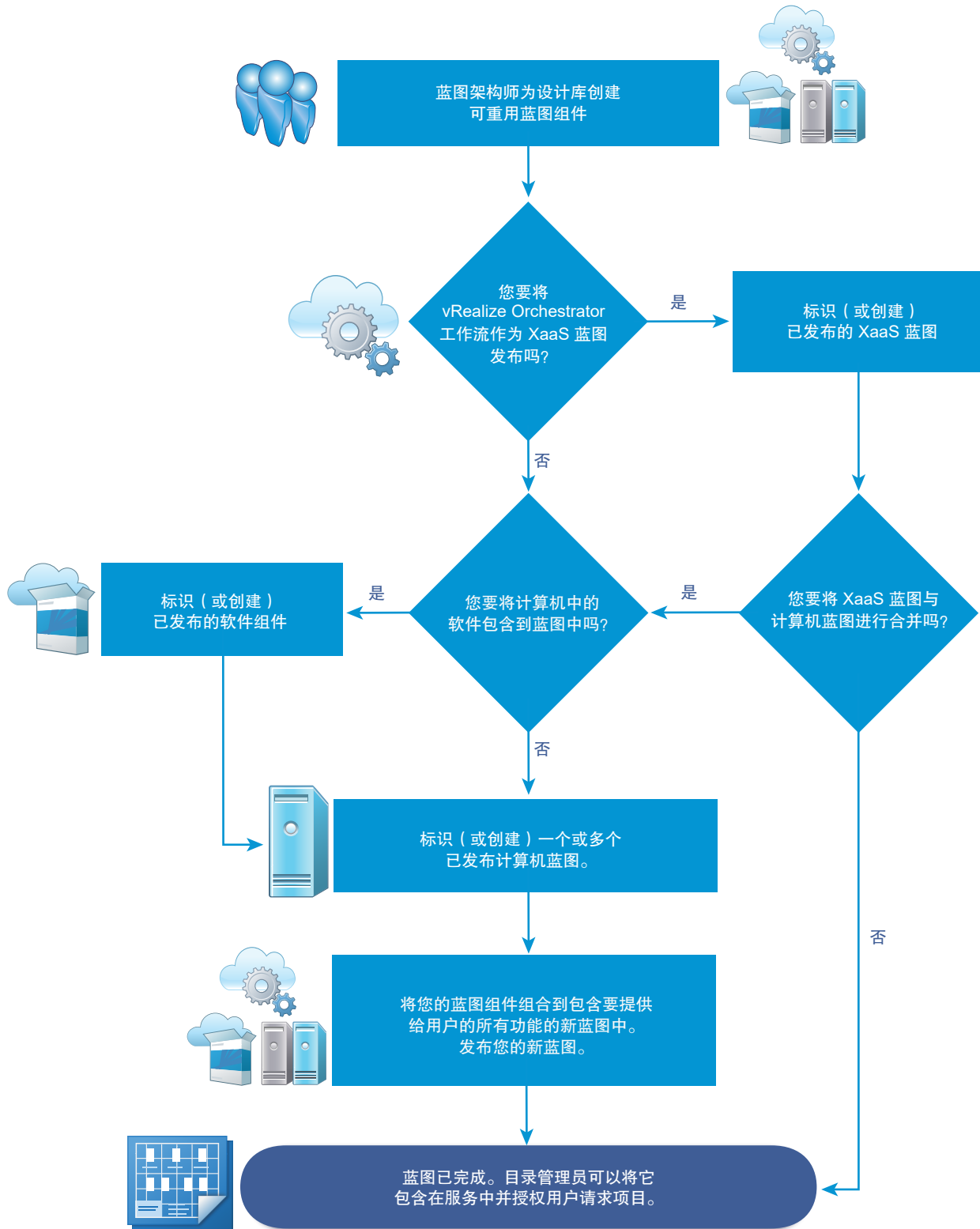
- [视频 - Lifecycle Manager 新增功能](#)
- [博客文章 - 具有基础架构蓝图的 vRealize Automation - 配置多开发人员环境](#)
- [文档 - 下载和配置提供的独立蓝图](#)
- [博客文章 - Lifecycle Manager 与 GitLab 集成](#)
- [博客文章 - LifeCycle Manager 概览](#)

组合复合蓝图

您可以重用已发布的蓝图和蓝图组件，以新方式将其组合在一起，创建能够为用户提供详细功能的 IT 服务包。

如果组件蓝图具有自定义表单，不会将自定义请求表单应用于新蓝图。您必须为新蓝图创建新表单。有关自定义请求表单的详细信息，请参见[自定义蓝图请求表单](#)。

图 3-5. 组合复合蓝图的工作流



■ 了解嵌套蓝图行为

可通过将蓝图作为组件嵌套在其他蓝图中来重用这些蓝图。可以通过嵌套蓝图来重用蓝图并在置备计算机时进行模块化控制，但是，使用嵌套蓝图时，需要注意一些特定规则和事项。

- **组合蓝图时使用计算机组件和 Software 组件**

在组合蓝图时将 Software 组件置于支持的计算机组件的顶部，以此来提供这些组件。

- **在蓝图组件之间创建属性绑定**

在一些部署方案中，组件需要其他组件的属性值以对其自身进行自定义。您可以将 XaaS、计算机、Software 的属性和自定义属性绑定到蓝图中的其他属性。

- **创建依赖关系和控制置备顺序**

如果需要其中一个蓝图组件的信息才能完成其他组件的置备，您可以在设计画布中绘制显式依赖关系以错开置备，以便从属组件不会过早置备。显式依赖关系可控制部署的构建顺序，并在缩小或扩大操作期间触发从属更新。软件组件需要在蓝图中进行排序。

了解嵌套蓝图行为

可通过将蓝图作为组件嵌套在其他蓝图中来重用这些蓝图。可以通过嵌套蓝图来重用蓝图并在置备计算机时进行模块化控制，但是，使用嵌套蓝图时，需要注意一些特定规则和事项。

包含一个或多个嵌套蓝图的蓝图称为外部蓝图。如果在创建或编辑其他蓝图时将某个蓝图组件添加到设计画布中，则该蓝图组件称为“嵌套蓝图”，而将其添加到的容器蓝图称为“外部蓝图”。

通过使用嵌套蓝图，可以提出一些有时并不明显的注意事项。要充分利用计算机置备功能，必须了解这些规则和注意事项。

嵌套蓝图的一般规则和注意事项

- 最佳做法是尽可能降低蓝图的复杂性，将蓝图限制于三层，并让顶层蓝图充当其中一层。
- 如果已授权用户访问外部蓝图，则该用户还有权访问该外部蓝图的嵌套蓝图。
- 您可以将批准策略应用于蓝图。获得批准之后，将置备蓝图目录项及其所有组件（包括嵌套蓝图）。此外，您还可以将不同的批准策略应用于不同组件。所有批准策略必须先经过批准，然后才能置备请求的蓝图。
- 在编辑已发布的蓝图时，不要更改已使用该蓝图置备的部署。置备时，生成的部署将从蓝图中读取当前值，包括从其嵌套蓝图中读取。可对已置备的部署进行的唯一更改是对软件组件进行编辑，例如对更新或卸载脚本进行编辑。
- 在外部蓝图中定义的设置会覆盖在嵌套蓝图中配置的设置，但下列情况除外：
 - 您可以更改嵌套蓝图的名称，但无法更改计算机组件或嵌套蓝图内任何其他组件的名称。
 - 不能为嵌套蓝图中的计算机组件添加或删除自定义属性。但是，可以编辑这些自定义属性。不能为嵌套蓝图中的计算机组件添加、编辑或删除属性组。
- 您或其他架构师对嵌套蓝图设置进行的更改会显示在外部蓝图中，除非您在外部蓝图中覆盖了这些设置。
- 将外部蓝图上的最长租用时间限制为组件蓝图的最大租用值中的最低值。

尽管在嵌套蓝图和外部蓝图上指定的租用时间可以设置为任意值，但外部蓝图上的最大租用时间应该限制为嵌套蓝图最大租用值中的最低值。这使得应用程序架构师可以设计具有统一的可变租用值但在基础架构架构师指定的限制范围内的复合蓝图。如果嵌套蓝图上定义的最大租用值小于外部蓝图上定义的值，置备请求将失败。

- 在外部蓝图中进行操作时，您可以替代为嵌套蓝图中的计算机组件配置的计算机资源设置。
- 在外部蓝图中进行操作时，您可以将软件组件拖到嵌套蓝图内的计算机组件上。
- 如果您打开一个蓝图，其中嵌套蓝图中的计算机组件已移除或其 ID 已更改，并且该计算机组件与当前蓝图中的组件关联，则会移除关联的组件并显示以下消息或类似消息：

嵌套蓝图中由当前蓝图中的组件引用的计算机组件已移除，或其计算机组件 ID 已更改。当前蓝图中与缺失的或已更改的计算机组件 ID 关联的所有组件都已移除。单击“取消”以保留嵌套蓝图中缺失的或已更改的计算机组件 ID 与当前蓝图中的组件的关联历史记录，并更正嵌套蓝图中的问题。打开嵌套蓝图并使用原始 ID 重新添加缺失的计算机组件，或将计算机组件 ID 重新更改为其原始 ID。单击“保存”以移除嵌套蓝图中缺失的或已更改的计算机组件 ID 与当前蓝图中的组件的所有关联历史记录。

- 发布蓝图时，将软件组件数据视为快照。如果稍后对软件组件属性进行更改，则该软件组件所在蓝图只能识别新属性。对于发布蓝图时存在于软件组件中的属性，不会在蓝图中应用更新。蓝图仅继承发布蓝图后添加的属性。但是，您可以对软件组件所在蓝图中的软件组件实例进行更改，以便更改该特定蓝图。

嵌套蓝图的网络和安全规则及注意事项

- 外部蓝图中的网络与安全组件均可与嵌套蓝图中定义的计算机关联。
- 嵌套蓝图不支持 NSX 网络、安全和负载均衡器组件及其设置。
- 将应用程序隔离应用于外部蓝图时，它将替代在嵌套蓝图中指定的应用程序隔离设置。
- 在外部蓝图中定义的传输区域设置将替代在嵌套蓝图中指定的传输区域设置。
- 在外部蓝图中进行操作时，您可以相对于在内部或嵌套蓝图中配置的网络组件设置和计算机组件设置来配置负载均衡器设置。
- 对于包含按需 NAT 网络组件的嵌套蓝图，在该按需 NAT 网络组件中指定的 IP 范围在外部蓝图中不可编辑。
- 外部蓝图无法包含此类内部蓝图：包含按需网络设置或按需负载均衡器设置的内部蓝图。不支持使用包含 NSX 按需网络组件或 NSX 负载均衡器组件的内部蓝图。
- 对于包含 NSX 网络或安全组件的嵌套蓝图，您无法更改在嵌套蓝图中指定的网络配置文件或安全策略信息。但是，您可以对添加到外部蓝图中的其他 vSphere 计算机组件重用这些设置。
- 为确保嵌套蓝图中的 NSX 网络与安全组件在复合蓝图中都是唯一的，vRealize Automation 会添加嵌套蓝图 ID 作为非唯一网络与安全组件名称的前缀。例如，如果将 ID 名称为 `xbp_1` 的蓝图添加到外部蓝图，且这两个蓝图均包含名为 `OD_Security_Group_1` 的按需安全组组件，则嵌套蓝图中的组件将在蓝图设计画布中重命名 `xbp_1-OD_Security_Group_1`。外部蓝图中的网络与安全组件名称没有前缀。

- 组件设置会根据组件所在蓝图而异。例如，如果内部蓝图级别和外部蓝图级别都包含安全组、安全标记或按需网络，则外部蓝图中的设置将替代内部蓝图中的设置。网络和安全组件仅在外蓝图级别受支持，在内部蓝图级别工作的现有网络除外。为了避免出现问题，请将所有安全组、安全标记和按需网络仅添加到外部蓝图中。

嵌套蓝图的软件组件注意事项

对于可缩放蓝图，最佳做法是创建不重用其他蓝图的单层蓝图。通常，在缩放操作期间，隐式依赖关系（例如将软件属性绑定到计算机属性时创建的依赖关系）会触发更新过程。但是，嵌套蓝图中的隐式依赖关系并不总是触发更新进程。如果需要在可缩放蓝图中使用嵌套蓝图，可手动绘制嵌套蓝图中的组件之间的依赖关系，创建始终触发更新的显式依赖关系。

组合蓝图时使用计算机组件和 Software 组件

在组合蓝图时将 Software 组件置于支持的计算机组件的顶部，以此来提供这些组件。

要支持 Software 组件，所选的计算机蓝图必须根据模板、快照或包含客户机代理和 Software 引导程序代理的 Amazon 计算机映像包含计算机组件，同时必须使用支持的置备方法。

由于 Software 代理不支持 Internet 协议版本 6 (IPv6)，因此请使用 IPv4 设置。

注 软件组件必须在蓝图中具有有序依赖关系。无序软件组件可能会导致蓝图置备失败。如果软件组件没有实际的顺序依赖关系，可以通过在软件组件之间添加虚假依赖关系来满足蓝图排序要求。

如果要蓝图设计为可缩放，最佳做法是创建不会重用其他蓝图的单层蓝图。通常，缩放操作期间使用的更新进程由隐式依赖关系（例如，属性绑定）加以触发。但是，嵌套蓝图中的隐式依赖关系并不总是触发更新进程。

尽管 IaaS 架构师、应用程序架构师和软件架构师均可组合蓝图，但只有 IaaS 架构师能够配置计算机组件。如果您不是 IaaS 架构师，则无法配置自己的计算机组件，但可以重用 IaaS 架构师创建和发布的计算机蓝图。

要成功将软件组件添加到设计画布，还必须具有目标目录的业务组成员、业务组管理员或租户管理员角色访问权限。

如果需要在可缩放蓝图中使用嵌套蓝图，可手动绘制嵌套蓝图中的组件之间的依赖关系，创建始终触发更新的显式依赖关系。

注 发布蓝图时，将软件组件数据视为快照。如果稍后对软件组件属性进行更改，则该软件组件所在蓝图只能识别新属性。对于发布蓝图时存在于软件组件中的属性，不会在蓝图中应用更新。蓝图仅继承发布蓝图后添加的属性。但是，您可以对软件组件所在蓝图中的软件组件实例进行更改，以便更改该特定蓝图。

表 3-64. 支持 Software 的置备方法

计算机类型	置备方法
vSphere	克隆
vSphere	链接克隆
vCloud Director	克隆

表 3-64. 支持 Software 的置备方法（续）

计算机类型	置备方法
vCloud Air	克隆
Amazon AWS	Amazon 计算机映像

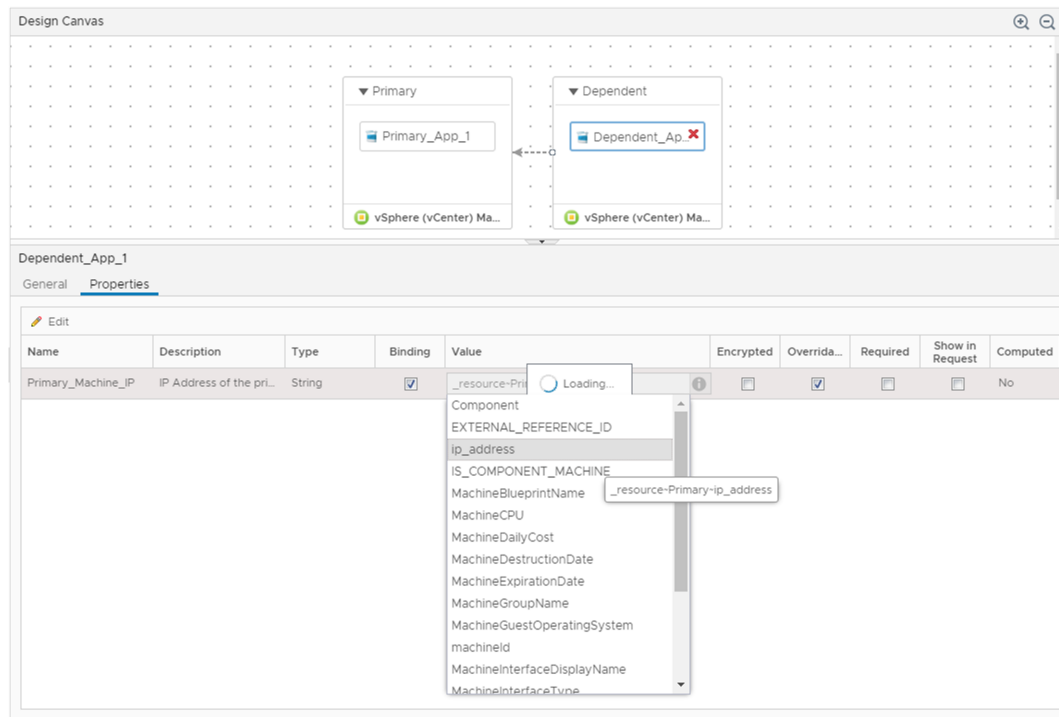
在蓝图组件之间创建属性绑定

在一些部署方案中，组件需要其他组件的属性值以对其自身进行自定义。您可以将 XaaS、计算机、Software 的属性和自定义属性绑定到蓝图中的其他属性。

例如，软件架构师可以在 WAR 组件的生命周期脚本中修改属性定义。WAR 组件可能需要 Apache Tomcat 服务器组件的安装位置，以便软件架构师能够对 WAR 组件进行配置，使其将 `server_home` 属性值设置为 Apache Tomcat 服务器的 `install_path` 属性值。作为组合蓝图的架构师，要成功置备 Software 组件，您必须将 `server_home` 属性绑定到 Apache Tomcat 服务器的 `install_path` 属性。

在蓝图中配置组件时，您可以设置属性绑定。在“蓝图”页面上，将组件拖动到画布上并单击**属性**选项卡。要将属性绑定到蓝图中的其他属性，请选中**绑定**复选框。您既可以在“值”文本框中输入 `ComponentName~PropertyName`，也可以使用向下箭头生成可用绑定选项的列表。您可将波形符 ~ 用作组件与属性之间的分隔符。例如，要绑定到属性 `dp_port`，您可在 MySQL 软件组件上键入 `mysql~db_port`。要绑定到在置备期间配置的属性（例如，计算机的 IP 地址或 Software 组件的主机名），请输入 `_resource~ComponentName~PropertyName`。例如，要绑定到计算机的预留名称，您可以输入 `_resource~vSphere_Machine_1~MachineReservationName`。

图 3-6. 将软件属性绑定到计算机的 IP 地址



创建依赖关系和控制置备顺序

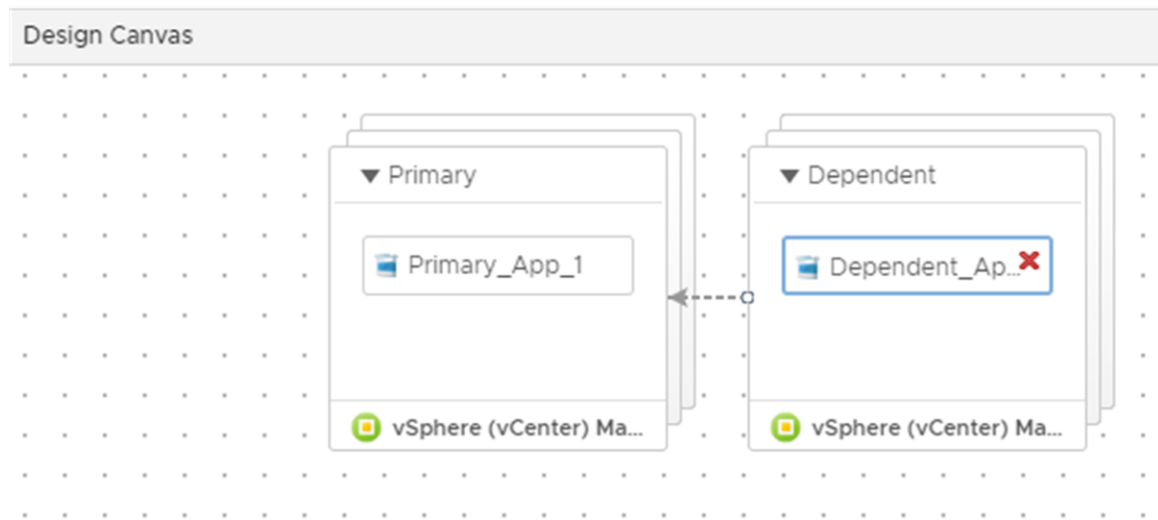
如果需要其中一个蓝图组件的信息才能完成其他组件的置备，您可以在设计画布中绘制显式依赖关系以错开置备，以便从属组件不会过早置备。显式依赖关系可控制部署的构建顺序，并在缩小或扩大操作期间触发从属更新。软件组件需要在蓝图中进行排序。

借助多个计算机和应用程序设计蓝图时，可以使用一台计算机上的所需属性完成另一台计算机上的应用程序安装。例如，如果要构建一个 **Web** 服务器，可能需要数据库服务器的主机名，然后才能安装应用程序并实例化数据库表。如果要映射显式依赖关系，您的数据库服务器将在 **Web** 服务器完成置备后开始置备。

注 软件组件必须在蓝图中具有有序依赖关系。无序软件组件可能会导致蓝图置备失败。如果软件组件没有实际的顺序依赖关系，可以通过在软件组件之间添加虚假依赖关系来满足蓝图排序要求。

要在设计画布上映射依赖关系，您需要从从属组件开始画一条指向依赖组件的线。完成后，您要构建的第二个组件会有一个箭头指向要构建的第一个组件。例如，在“通过映射依赖关系控制构建顺序”图中，构建主计算机后才会置备从属计算机。或者，您可以配置两个计算机以同时进行置备，但在软件组件之间绘制依赖关系。

图 3-7. 通过映射依赖关系控制构建顺序



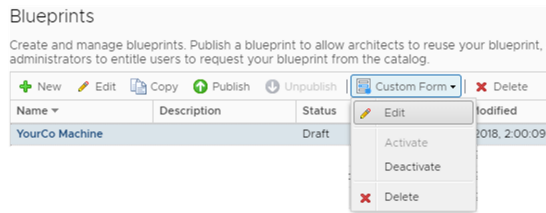
如果要将蓝图设计为可缩放，最佳做法是创建不会重用其他蓝图的单层蓝图。通常，在缩放操作期间，隐式依赖关系（例如将软件属性绑定到计算机属性时创建的依赖关系）会触发更新过程。但是，嵌套蓝图中的隐式依赖关系并不总是触发更新进程。如果需要在可缩放蓝图中使用嵌套蓝图，可手动绘制嵌套蓝图中的组件之间的依赖关系，创建始终触发更新的显式依赖关系。

自定义蓝图请求表单

当用户请求目录中的蓝图时，您创建和发布的每个蓝图都会显示一个表单。创建或编辑蓝图时，您可以使用默认表单，也可以自定义蓝图请求表单。如果默认表单上提供的信息或所需信息不是您要提供给用户的信息，您可以自定义表单。

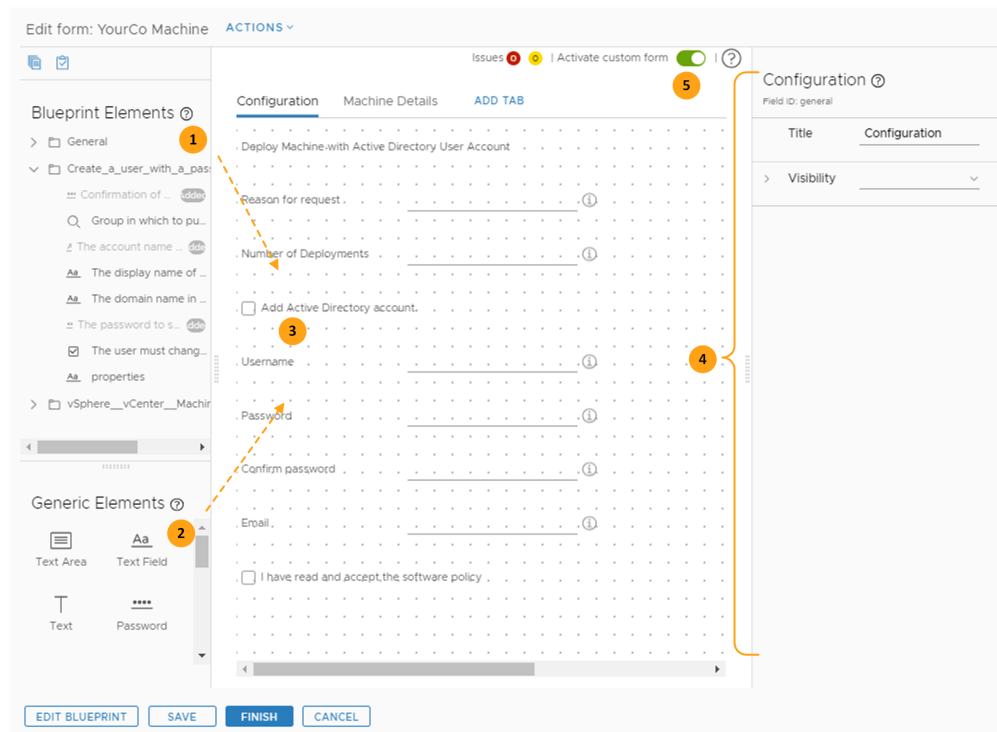
自定义请求表单

您可以从蓝图数据网格或从蓝图画布访问自定义请求表单设计器。



自定义请求表单设计器

您可以使用表单设计器创建自定义表单。



要创建自定义表单，请执行以下操作：

- 1 将元素（1 和 2）拖动到设计画布（3）上。
- 2 使用属性窗格（4）配置每个元素。
- 3 激活表单（5）。

除非将属性配置为禁止覆盖，否则蓝图元素列表将包括自定义属性。如果属性的可覆盖选项设置为否，则字段无法进行自定义。

验证和限制

自定义表单设计器支持通过向字段添加限制或使用外部验证源进行数据验证。有关创建表单时适用的限制选项，请参见[自定义表单设计器字段属性](#)。

- 有关限制示例，请参见[使用 Active Directory 选项创建自定义请求表单](#)。
- 有关外部验证，请参见[在自定义表单设计器中使用外部验证](#)。

在表单中添加验证和依赖关系时，请求用户必须提供或系统必须验证字段，否则从属字段可能不会显示在表单中。

例如，如果第一个选项卡上具有后续字段所依赖的字段，则只有在前面的选项卡上提供从属值后，从属字段才会显示在后续选项卡上。

自定义请求表单操作

您可以使用操作菜单项填充表单，并与其他系统共享表单。

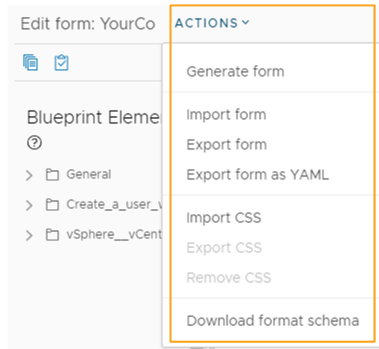


表 3-65. 自定义请求表单操作菜单项

操作菜单项	描述
生成表单	<p>将与每个蓝图组件关联的所有字段添加到表单设计器。每个组件都将添加到选项卡中。如果创建或修改表单后使用此菜单项，则生成的表单会覆盖当前的表单。</p> <p>使用此菜单项时，可以隐藏或移除不希望提供给目录中的用户的字段。如果不生成表单，仍然可以添加和配置希望用户可以查看的文本。</p>
导入表单	导入自定义表单 JSON 或 YAML 文件。
导出表单	<p>将当前自定义表单导出为 JSON 文件。</p> <p>如果要使用该表单中与您在其他蓝图中使用的组件相匹配的一部分，请导出该文件。</p>

表 3-65. 自定义请求表单操作菜单项（续）

操作菜单项	描述
将表单导出为 YAML	<p>将当前自定义表单导出为 YAML。</p> <p>如果要自定义表单从一个 vRealize Automation 实例移动到另一个实例，请将文件导出为 YAML。例如，从测试环境到生产环境。如果要自定义表单作为 YAML 进行编辑，可以导出表单并进行编辑，然后再将其导入回蓝图。</p>
导入 CSS	<p>导入 CSS 文件以增强目录请求表单。</p> <p>文件可能类似于以下示例。此示例将更改字体大小，并将文本设置为粗体。引用的字段是“使用 Active Directory 用户帐户部署计算机”文本字段，该字段显示在前述“自定义请求表单设计器”部分的图像中。</p> <pre>#<field-ID> .grid-item { font-size: 16px; font-weight: bold; width: 600px; }</pre> <p>在此示例中，<field-ID> 是画布中字段的 ID。要查找值，请在画布中选择该字段。值位于右侧窗格中，在名称的下方。在上面的图像中，值为 text_d947bc97。</p> <p>导入该文件。将其另存为 <filename>.css。</p>
导出 CSS	导出所导入的 CSS。
移除 CSS	<p>放弃您自定义的 CSS。</p> <p>放弃的 CSS 不可恢复。</p>
下载格式结构定义	<p>下载包含自定义表单所用控件和状态的结构与描述的 JSON 文件。</p> <p>您可以使用此结构定义创建表单或修改现有表单。您可以导入修改后的 JSON 文件作为自定义表单。</p>

使用 Active Directory 选项创建自定义请求表单

默认表单为请求用户提供的信息太多或太少时，可以创建自定义表单。可以将更多字段添加到表单，可以隐藏表单上的字段，还可以预填充字段，然后显示或隐藏这些字段。

此用例基于蓝图，该蓝图包含一个 vSphere 虚拟机类型和一个 XaaS 蓝图（用于在虚拟机上配置 Active Directory 管理员帐户）。XaaS 蓝图基于“在组中创建用户和密码”工作流。

在此用例中，您需要执行以下任务：

- 为用户提供配置管理员密码的选项。
- 预配置计算机详细信息，以便 CPU 和内存值都以 GB 为单位。

此用例可提供哪些优势？此用例包括以下表单自定义示例：

- 将特定字段添加到空白表单。
- 配置显示/隐藏复选框。

- 请求用户选择复选框之前隐藏字段。
- 向字段中添加验证。
- 以 GB 为单位显示内存字段（尽管蓝图字段以 MB 为单位进行计算）。
- 使用正则表达式。

前提条件

- 以应用程序架构师、软件架构师或基础架构架构师身份登录到 vRealize Automation。
- 创建一个 YourCo Machine and User 蓝图，其中包含一个 vSphere 蓝图和一个 XaaS 蓝图（用于在组中创建 Active Directory 用户帐户和密码）。例如，请参见[创建用于创建用户的 XaaS 蓝图](#)。

步骤

- 1 选择**设计 > 蓝图**。
- 2 突出显示包含 YourCo Machine and User 蓝图的行，然后单击**自定义表单 > 编辑**。
- 3 重命名“常规”选项卡。
 - a 单击该选项卡。
 - b 在右侧属性窗格的**标题**属性中，输入**配置**。
- 4 在新的“配置”选项卡上，使用提供的值添加并配置以下字段。

The screenshot displays the 'Edit form' window for 'YourCo Machine'. The main area is titled 'Configuration' and contains several form fields: 'Deploy Machine with Active Directory User Account', 'Reason for request', 'Number of Deployments', 'Add Active Directory account' (checkbox), 'Username', 'Password', 'Confirm password', 'Email', and 'I have read and accept the software policy' (checkbox). The left sidebar shows 'Blueprint Elements' and 'Generic Elements'. The right sidebar shows the 'Configuration' tab settings, including 'Title' and 'Visibility'.

使用提供的“外观”、“值”和“限制”值。

解决构建表单时出现的错误。

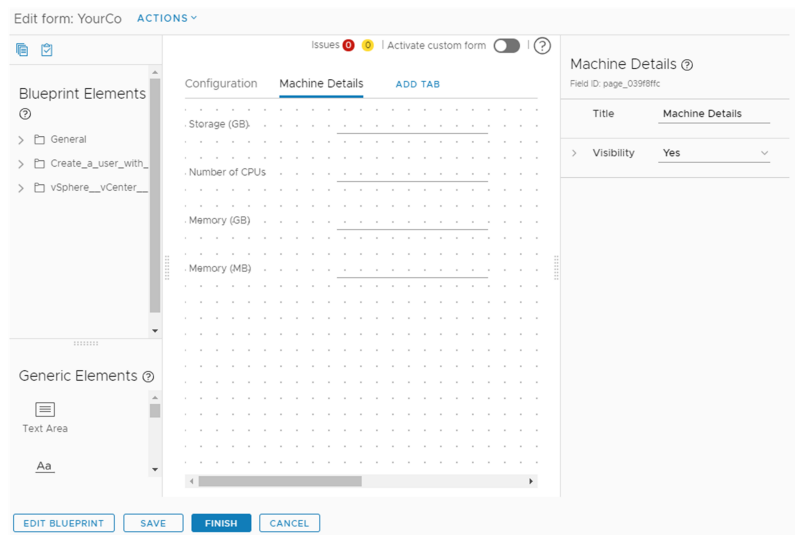
屏幕截图中的 的字段	蓝图元素源	外观	值	限制
使用 Active Directory 用户帐户部 署计算机	通用元素 > 文本	标签和类型 <ul style="list-style-type: none"> ■ 显示类型 = 文本 可见性 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 可见 = 是 	默认值 <ul style="list-style-type: none"> ■ 默认值 = 使用 Active Directory 用户 帐户部署计算机 ■ 值源 = 常数 	
请求原因	蓝图元素 > vSphere_vCenter_Machine > 描述	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 请求原因 ■ 显示类型 = 文本字段 可见性 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 可见 = 是 只读 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 只读 = 否 自定义帮助 <ul style="list-style-type: none"> ■ 标志帮助 = 提供请求原因。 		必需 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 必需 = 是
部署数	蓝图元素 > 常规 > 部署数	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 部署数 ■ 显示类型 = 整数 可见性 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 可见 = 是 只读 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 只读 = 否 自定义帮助 <ul style="list-style-type: none"> ■ 标志帮助 = 选择要部署的蓝图的实例数。 	默认值 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 默认值 = 1 	必需 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 必需 = 是 最小值 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 最小值 = 1
“添加 Active Directory 帐户” 复选 框	通用元素 > 复选框	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 添加 Active Directory 帐户。 ■ 显示类型 = 复选框 可见性 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 可见 = 是 		

屏幕截图中的 的字段	蓝图元素源	外观	值	限制
用户名	蓝图元素 > 在组中创建用户和密码 > 用户的帐户名称	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 用户名 ■ 显示类型 = 文本字段 可见性 <p>注 此可见性属性（在后续字段中以相同方式配置）会隐藏字段，除非选中“添加 Active Directory 帐户”复选框。</p> <ul style="list-style-type: none"> ■ 值源 = 条件值 ■ 表达式 = 设定值 = 是 如果“添加 Active Directory 帐户”为“是” 自定义帮助 <ul style="list-style-type: none"> ■ 标志帮助 = 提供管理员用户名。 	默认值 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 默认值 = admin 	必需 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 必需 = 是 正则表达式 <p>注 正则表达式必须遵循 JavaScript 语法。</p> <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 正则表达式 = "[a-z]*\$" ■ 验证错误消息 = 用户名不得包含任何特殊字符或数字。
密码	蓝图元素 > 在组中创建用户和密码 > 要为新创建帐户设置的密码	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 密码 ■ 显示类型 = 密码 可见性 <ul style="list-style-type: none"> ■ 值源 = 条件值 ■ 表达式 = 设定值 = 是 如果“添加 Active Directory 帐户”为“是” 自定义帮助 <ul style="list-style-type: none"> ■ 标志帮助 = 提供管理员帐户的密码。 		必需 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 必需 = 是 正则表达式 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 正则表达式 = "^(?=.*[A-Z])(?=.*[0-9])(?=.*[a-z]).{8,}\$" ■ 消息 = 管理员密码长度必须至少为 8 个字符，且可以包括字母数字和特殊字符。

屏幕截图中的字段	蓝图元素源	外观	值	限制
确认密码	蓝图元素 > 在组中创建用户和密码 > 确认密码	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 确认密码 显示类型 = 密码 可见性 <ul style="list-style-type: none"> ■ 值源 = 条件值 ■ 表达式 = 设定值 = 是 如果“添加 Active Directory 帐户”为“是” 自定义帮助 <ul style="list-style-type: none"> ■ 标志帮助 = 重新输入管理员帐户的密码。 		必需 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 必需 = 是 匹配字段 <ul style="list-style-type: none"> ■ 匹配字段 = 密码
电子邮件	通用元素 > 文本字段	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 电子邮件 ■ 显示类型 = 文本字段 可见性 <ul style="list-style-type: none"> ■ 值源 = 条件值 ■ 表达式 = 设定值 = 是 如果“添加 Active Directory 帐户”为“是” 自定义帮助 <ul style="list-style-type: none"> ■ 标志帮助 = 提供管理员电子邮件。 	默认值 <ul style="list-style-type: none"> ■ 值源 = 计算的值 ■ 运算符 = 连接 ■ 添加值 = 字段。选择用户名 ■ 添加值 = 常数。输入 @yourco.com 	正则表达式 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 正则表达式 = <code>^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$</code> ■ 验证错误消息 = 提供有效电子邮件。
“我已阅读并接受软件策略”复选框。	通用元素 > 复选框	标签和类型 <ul style="list-style-type: none"> ■ 元素标签 = 我已阅读并接受软件策略 ■ 显示类型 = 复选框 可见性 <ul style="list-style-type: none"> ■ 值源 = 条件值 ■ 表达式 = 设定值 = 是 如果“添加 Active Directory 帐户”为“是”		

5 单击**添加选项卡**，然后在右侧的**标题**属性中输入**计算机详细信息**。

6 在“计算机详细信息”选项卡中配置以下字段。



使用提供的“外观”、“值”和“限制”值。

屏幕截图中的字段	蓝图元素源	外观	值	限制
存储 (GB)	蓝图元素 > vSphere_vCenter_Machine > 存储 (GB)	标签和类型 ■ 标签 = 存储 (GB) ■ 显示类型 = 整数 可见性 ■ 值源 = 常数 ■ 可见性 = 是 只读 ■ 值源 = 常数 ■ 只读 = 否	默认值 ■ 值源 = 常数 ■ 默认值 = 4	最小值 ■ 值源 = 常数 ■ 最小值 = 2
CPU 数量	蓝图元素 > vSphere_vCenter_Machine > CPU	标签和类型 ■ 标签 = CPU 数量 ■ 显示类型 = 整数 可见性 ■ 值源 = 常数 ■ 可见性 = 是	默认值 ■ 值源 = 常数 ■ 默认值 = 1	最小值 ■ 值源 = 常数 ■ 最小值 = 1

屏幕截图中的字段	蓝图元素源	外观	值	限制
内存 (GB)	通用元素 > 整数	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 内存 (GB) ■ 显示类型 = 整数 可见性 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 可见性 = 是 	默认值 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 默认值 = 1 	最小值 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 最小值 = 1
内存 (MB)	蓝图元素 > vSphere_vCenter_Machine > 内存 (MB)	标签和类型 <ul style="list-style-type: none"> ■ 标签 = 内存 (MB) ■ 显示类型 = 整数 可见性 <ul style="list-style-type: none"> ■ 值源 = 常数 ■ 可见性 = 否 	默认值 <ul style="list-style-type: none"> ■ 值源 = 计算的值 ■ 运算符 = 乘 ■ 添加值 = 字段。选择内存 (GB) ■ 添加值 = 常数。输入 1024 	

- 7 解决所有错误。您可以保存表单，但只有确保表单没有任何错误后，才能激活表单。
- 8 要保存表单并关闭表单设计器，请单击**完成**。
- 9 选择蓝图并单击**发布**。
- 10 要在用户请求服务目录中的项时提供自定义表单，请在“蓝图”页面工具栏上选择**自定义表单 > 激活**。

后续步骤

- 在服务目录中提供蓝图。请参见[管理服务目录](#)。
- 在目录中，确认请求表单类似以下示例。

自定义表单设计器字段属性

字段属性确定了所选字段的外观和提供给用户的默认值。此外，还确定了要应用于字段的规则，以确保用户在 vRealize Automation 的目录请求表单中提供有效的条目。

可以分别配置每个字段。选择字段，然后编辑字段属性。

值源

对于许多属性，可以从各种值源选项中进行选择。并非所有源选项都可用于所有字段类型或属性。

- **常数。**值不会更改。根据属性，值可能是字符串、整数、正则表达式或从有限列表中选择选项，例如“是”或“否”。例如，可以提供 1 作为默认值整数，选择“否”作为“只读”属性，或提供正则表达式来验证字段条目。
- **条件值。**值基于一个或多个条件。按列出的顺序处理条件。如果多个条件为 True，最后为 True 的条件将确定该属性的字段行为。例如，您可以创建一个条件，确定某字段的可见性是否基于另一个字段中的值。
- **外部源。**值基于 vRealize Orchestrator 操作的结果。例如，根据脚本式 vRealize Orchestrator 操作计算成本。例如，请参见[在自定义表单设计器中使用 vRealize Orchestrator 操作](#)。
- **绑定字段。**值与绑定到的字段相同。可用字段仅限于相同的字段类型。例如，将“需要身份验证”复选框字段的默认值绑定到另一个复选框字段。在请求表单中选择一个目标字段复选框时，会选中当前字段的复选框。
- **计算的值。**值根据运算符处理选定字段和值的方式确定。文本字段使用连接运算符。整数字段使用所选的加、减、乘或除运算。例如，可以将整数字段配置为使用乘运算将兆字节转换为千兆字节。

字段外观

可以使用外观属性确定是否在表单上显示字段，以及确定您要提供给目录用户的标签和自定义帮助。

某些蓝图可能包括包含固定值的字段。如果将这种类型的字段添加到自定义表单，那么仅“外观”选项可用，并且该字段始终为只读。

表 3-66. “外观”选项卡选项

选项	描述
标签和类型	<p>提供标签，并选择显示类型。</p> <p>可用的显示类型取决于字段。一些字段支持多个文本类型，而一些字段仅支持整数。可能的值：</p> <ul style="list-style-type: none"> ■ 小数 ■ 下拉字段 ■ 映像 ■ 整数 ■ 多选 ■ 密码 ■ 单选组 ■ Text ■ 文本区域 ■ 文本字段 <p>下拉字段和数据网格字段包含占位符设置。输入的值在下拉菜单中显示为内部标签或说明，在数据网格中显示为常规标签或说明。</p> <p>值选择器和树选择器字段包含引用类型设置。引用类型是指用于将值选择器或树选择器的搜索范围限制到支持该类型的 vRealize Orchestrator 服务器清单的 vRealize Orchestrator 资源类型。之后，可以通过选择支持引用类型的操作进一步限制搜索范围。有关这两个选择器的详细信息，请参见在自定义表单设计器中使用值选择器或树选择器元素。</p>
可见性	<p>显示或隐藏请求表单上的字段。</p> <ul style="list-style-type: none"> ■ 常数。选择“是”在表单上显示字段。选择“否”隐藏字段。 ■ 条件值。可见性取决于第一个为 True 的表达式。例如，如果在表单上选中复选框，则字段可见。 ■ 外部源。可见性取决于所选 vRealize Orchestrator 操作的结果。
只读	<p>防止用户更改字段值。</p> <ul style="list-style-type: none"> ■ 常数。选择“是”显示值，但会阻止更改。选择“否”允许更改。 ■ 条件值。状态取决于第一个为 True 的表达式。例如，如果存储字段中的值大于 2 GB，则字段为只读。 ■ 外部源。状态取决于所选 vRealize Orchestrator 操作的结果。

表 3-66. “外观” 选项卡选项（续）

选项	描述
每页行数	仅适用于数据网格元素。 输入行数。
自定义帮助	向用户提供有关字段的信息。这些信息显示在字段的标志帮助中。 您可以使用简单文本或 HTML，包括 href 链接。例如 <code>vRealize Automation documentation</code> 。

字段值

可以使用值属性提供任何默认值。

表 3-67. “值” 选项卡选项

选项	描述
列	仅适用于数据网格元素。 为表中的每一列提供标签、ID 和值类型。 数据网格的默认值所包含的标题数据必须匹配定义的列。例如，如果一列是 user_name ID，另一列是 user_role ID，则第一行是 user_name,user_role。 有关配置示例，请参见 在自定义表单设计器中使用数据网格元素 。
默认值	根据值源在字段中填充默认值。 可能的值源取决于字段。 <ul style="list-style-type: none"> ■ 常数。输入的字符串。 ■ 条件值。默认值取决于第一个为 True 的表达式。例如，如果内存字段小于 512 MB，则存储字段的默认值为 1 GB。 contains 运算符检查所选字段是否包含提供的值。within 运算符检查所选字段是否具有提供的字符串。例如，如果表达式为 Field A within development，则 Field A = dev 或 lop 或 ment 时，该表达式为 true，但 Field A = prod 或 test 时，则评估为 false。 ■ 外部源。值基于所选 vRealize Orchestrator 操作的结果。 ■ 绑定字段。值与所选字段相同。 ■ 计算的值。值基于所提供字段值和所选运算符的结果。例如，内存 (MB) 的默认值基于内存 (GB) 乘以 1024 的结果。
值选项	填充下拉字段、多选、单选组或值选择器字段。 <ul style="list-style-type: none"> ■ 常数。列表的格式为 Value Label,Value Label,Value Label。例如 2 Small,4 Medium,8 Large。 ■ 外部源。值基于所选 vRealize Orchestrator 操作的结果。
步骤	对于整数或小数字段，定义增量或减量值。 例如，如果默认值为 1 且将步骤值设置为 3，则允许的值为 4、7、10 等。

字段限制

可以通过使用限制属性确保请求用户在请求表单中提供有效值。

此外，还可以使用外部验证作为确保有效值的备选方法。请参见[在自定义表单设计器中使用外部验证](#)。

表 3-68. “限制” 选项卡选项

选项	描述
必需	<p>请求用户必须为此字段提供值。</p> <ul style="list-style-type: none"> ■ 常数。选择“是”要求请求用户提供值。如果字段为可选，请选择“否”。 ■ 条件值。是否为必填字段取决于第一个为 True 的表达式。例如，如果操作系统系列在另一个字段中以 Darwin 开头，则此字段为必填字段。 ■ 外部源。状态基于所选 vRealize Orchestrator 操作的结果。
正则表达式	<p>提供正则表达式以验证值和验证失败时显示的消息。</p> <p>正则表达式必须遵循 JavaScript 语法。有关概述，请参见创建正则表达式。有关更多详细指导，请参见语法。</p> <ul style="list-style-type: none"> ■ 常数。提供正则表达式。例如，对于电子邮件地址，正则表达式可能为 <code>^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$</code>，验证错误消息为电子邮件地址格式无效。请重试。 ■ 条件值。使用的正则表达式取决于第一个为 True 的表达式。
最小值	<p>指定最小数值。例如，密码长度必须至少为 8 个字符。</p> <p>提供错误消息。例如，密码长度必须至少为 8 个字符。</p> <ul style="list-style-type: none"> ■ 常数。输入整数。 ■ 条件值。最小值取决于第一个为 True 的表达式。例如，如果操作系统不等于 Linux，则最小 CPU 值为 4。 ■ 外部源。值基于所选 vRealize Orchestrator 操作的结果。
最大值	<p>最大数值。例如，字段限制为 50 个字符。</p> <p>提供错误消息。例如，此描述不能超过 50 个字符。</p> <ul style="list-style-type: none"> ■ 常数。输入整数。 ■ 条件值。最大值取决于第一个为 True 的表达式。例如，如果部署位置等于 AMEA，则最大存储值为 2 GB。 ■ 外部源。值基于所选 vRealize Orchestrator 操作的结果。
匹配字段	<p>此字段的值必须与所选字段的值匹配。</p> <p>例如，密码确认字段必须与密码字段匹配。</p>

在自定义表单设计器中使用 vRealize Orchestrator 操作

自定义 vRealize Automation 蓝图的请求表单时，您可以根据 vRealize Orchestrator 操作的结果确定某些字段的行为。

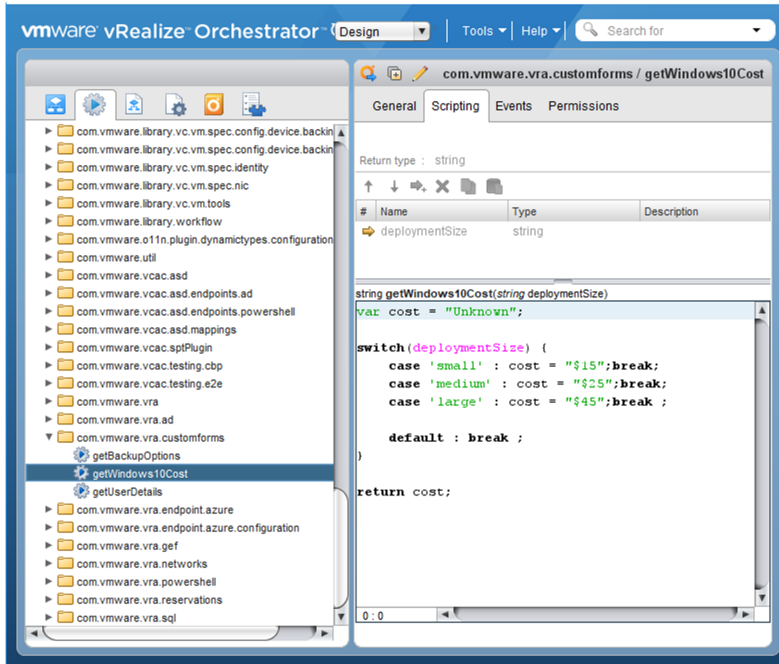
可以通过多种方法使用 vRealize Orchestrator 操作。您可以从第三个源提取数据，也可以使用定义大小和成本的脚本。以下示例使用脚本。

创建脚本以使用操作填充字段时，请勿使用数组 [任意] 类型。

示例： 大小和成本字段示例

在此用例中，您希望目录用户选择虚拟机大小，然后显示该计算机的每日成本。在此示例中，您通过 vRealize Orchestrator 将大小和成本关联起来，然后将大小字段和成本字段添加到蓝图自定义表单。大小字段可确定将在成本字段中显示的值。

- 1 在 vRealize Orchestrator 中，使用类似以下示例的 `deploymentSize` 脚本配置操作 `getWindows10Cost`。



使用以下脚本示例。

```
var cost = "Unknown";

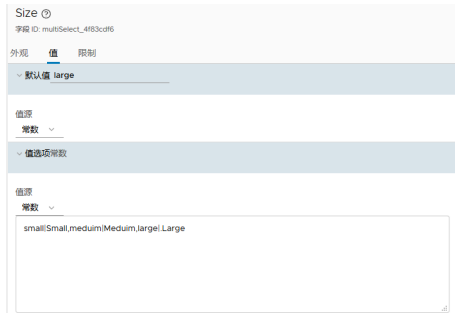
switch(deploymentSize) {
    case 'small' : cost = "$15";break;
    case 'medium' : cost = "$25";break;
    case 'large' : cost = "$45";break ;

    default : break ;
}

return cost;
```

- 2 在 vRealize Automation 中，将大小字段和成本字段添加到蓝图自定义表单并进行配置。

将大小字段配置为多选字段，提供“小”、“中”和“大”值。

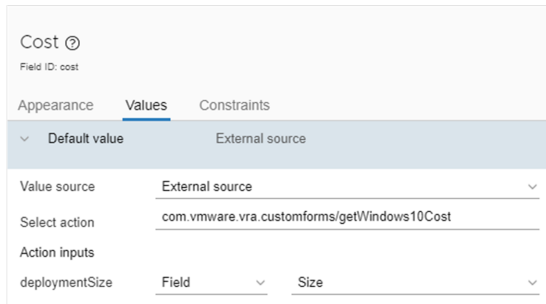


在 vRealize Automation 中，将大小字段和成本字段添加到蓝图自定义表单并进行配置。

在“值”选项卡上，配置以下属性值。

- 默认值 = 大
- 值选项
 - 值源 = 常数
 - 值定义 = **small|Small,medium|Medium,large|Large**

3 配置成本字段，使其根据大小字段中选择的值按照 vRealize Orchestrator 操作中的定义来显示成本。



在“值”选项卡上，配置以下属性值。

- 默认值 = 外部源
- 选择操作 = <您的 vRealize Orchestrator 操作文件夹>/getWindows10Cost
- 操作输入
 - deploymentSize。在操作中配置此值。
 - 字段
 - 大小

在自定义表单设计器中使用值选择器或树选择器元素

自定义请求表单时，可以提供元素，用户可以在元素中从搜索结果列表进行选择或浏览树以找到匹配的值。

值选择器和树选择器与在自定义表单“外观”选项卡上定义的引用类型配合使用。引用类型为 vRealize Orchestrator 资源。例如，AD:UserGroup 或 VC:Datastore。通过定义引用类型，当用户输入搜索字符串时，结果或树选项会限于具有匹配参数的资源。

对于值选择器，可以通过配置外部源再进一步限制可能的值。对于树选择器，可以通过配置外部源提供默认值。

使用值选择器

值选择器在目录表单中显示为搜索选项。用户输入字符串后，该选择器会基于对其所做的配置提供选项。您可以基于以下用例使用选择器。值选择器最有价值的应用是与外部源值搭配使用。

- 值选择器与常数值源。如果您希望请求用户从预定义的静态值列表中选择，请使用此方法。与组合框、下拉菜单、多选和单选组元素类似，此方法基于定义的常数值和标签在列表中提供搜索结果。
- 值选择器与未定义的值源。如果您希望请求用户在 vRealize Orchestrator 清单中搜索具有已配置引用类型的特定对象，请使用此方法。例如，引用类型为 VC:Datastore，您希望用户从检索到的列表中选择数据存储。
- 值选择器与外部值源。如果您希望请求用户从基于 vRealize Orchestrator 操作的结果中选择，请使用此方法。例如，您的某项操作为从一个集成数据库检索两个或多个值，且您希望用户从检索到的列表中选择值。该操作必须包含筛选器 `var filter = System.getContext().getParameter("__filter");`。

使用树选择器

树选择器在目录表单中显示为搜索选项。用户输入字符串后便会显示树选择器。用户可以通过树选择与引用类型匹配的值。例如，如果引用类型为 VC:Datastore，请求用户可以选择数据存储对象。如果引用类型为 VC:VirtualMachine，用户可以选择虚拟机。

- 树选择器与未定义的值源。如果您希望请求用户通过浏览层次树找到具有已配置引用类型的特定对象，请使用此方法。例如，引用类型为 VC:Datastore，您希望用户从检索到的树中选择数据存储。
- 树选择器与外部值源。如果您希望在树中提供默认选择，请使用此方法。请求用户可以选择预设值或浏览不同的值。例如，对于引用类型 VC:Datastore，您希望基于指定网络的操作输入值的结果将树中的数据存储预设为特定数据存储。


在自定义表单设计器中使用数据网格元素

自定义蓝图的请求表单时，以表格式添加信息。表中显示的数据可以手动提供也可以基于外部源。

示例：提供的 CSV 数据示例

在此用例中，您有一个在自定义请求表单中提供的数值表。您在表中将信息作为常数值源提供。该源基于 CSV 数据结构，其中第一行是标头。标头是以逗号分隔的列 ID。额外增加的每一行数据都将显示在表的每一行中。

- 1 将数据网格通用元素添加到设计画布上。
- 2 选择数据网格，然后在属性窗格中定义值。




Data Grid 

Field ID: datagrid_0a3999da

Appearance **Values**

Columns

ADD COLUMN

Label	Username	
Id	username	
Type	String	
Label	Employee ID	
Id	employeeId	
Type	Integer	
Label	Manager	
Id	manager	
Type	String	

Default value Constant

Value source Constant

CSV

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

标签	ID	类型
用户名	username	String
员工 ID	employeeId	整数
经理	manager	String

定义 CSV 值。

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

- 3 确认数据网格显示蓝图请求表单中的预期数据。

<input type="checkbox"/>	Username	Employee ID	Manager
<input checked="" type="checkbox"/>	leonardo	95621	Farah
<input type="checkbox"/>	vindhya	15496	Farah
<input type="checkbox"/>	martina	52648	Nikolai

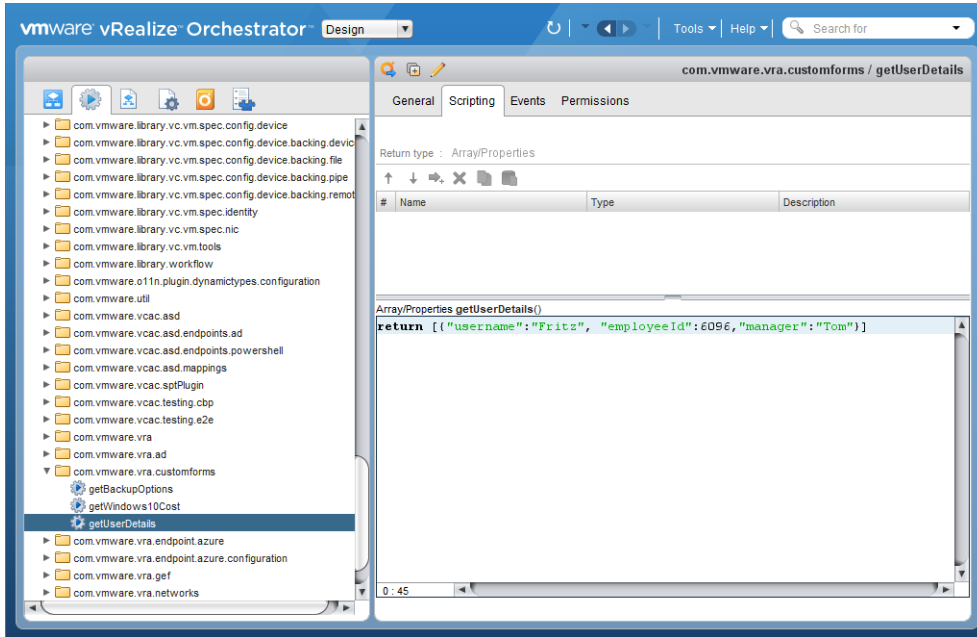
1 1-3/3

示例：外部源示例

此示例使用前面的示例，但值基于 vRealize Orchestrator 操作。尽管这是一个简单的操作示例，但您可以使用更复杂的操作，从本地数据库或系统检索这类信息。

用作验证的操作必须具有数组/属性输入参数。

- 1 在 vRealize Orchestrator 中，使用类似以下示例的数组配置操作 `getUserDetails`。



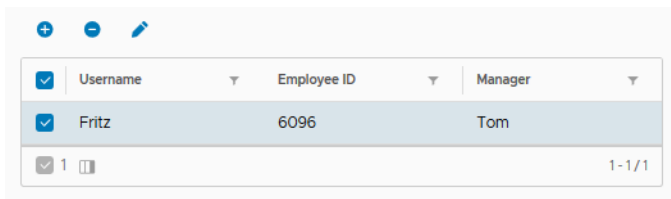
使用以下脚本示例。

```
return [{"username": "Fritz", "employeeId": 6096, "manager": "Tom"}]
```

- 2 在 vRealize Automation 中，添加数据网格并使用以下值配置数据网格列。

标签	ID	类型
用户名	username	String
员工 ID	employeeId	整数
经理	manager	String

- 3 在“值源”列表中，选择**外部源**。
- 4 在“选择操作”中，输入 `getUserDetails` 并选择在 vRealize Orchestrator 中创建的操作。
- 5 保存并确认请求表单中的表。



在自定义表单设计器中使用外部验证

您可以通过向字段添加限制或使用外部验证源来自定义请求表单，以确保用户在请求时提供有效的值。

可以为某些字段属性配置限制以确保提供的值有效，例如最小值、最大值、正则表达式、匹配字段或不为空。请参见[自定义表单设计器字段属性](#)。

外部验证使用 vRealize Orchestrator 操作从外部源检查值是否有效。

如果要验证数据网格值，则用作验证的操作必须具有数组/属性输入参数。

您可能需要使用外部验证的一些示例包括：

- 在外部源中定义了有效值。例如 vRealize Orchestrator。
- 验证必须涉及多个字段。例如，vRealize Orchestrator 操作收集磁盘大小和存储池容量，并根据可用空间验证提供的大小值。

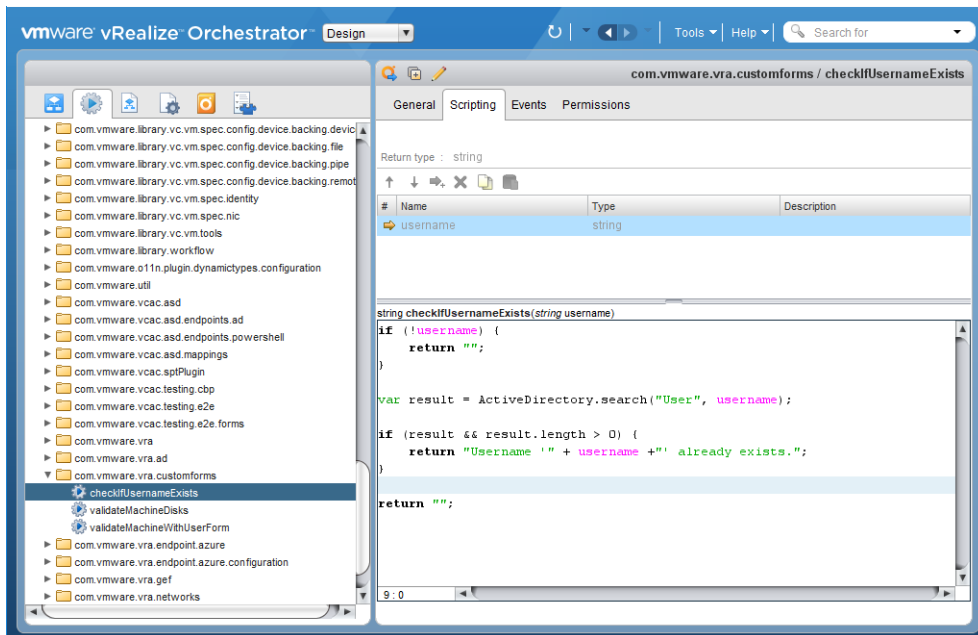
如何对一个蓝图中的多个外部验证进行排序？按照外部验证画布中的显示顺序处理验证。如果您有两个验证可以验证同一字段，则第二个验证结果将覆盖第一个。要对验证进行重新排序，您可以单击并拖动画布上的卡。

示例：vRealize Orchestrator 用户示例

在此用例中，您希望目录用户仅提供新用户名。在此示例中，您通过 vRealize Orchestrator 操作检查表单中提供的用户名是否存在于您的 Active Directory 数据库中。如果此名称存在，将在请求表单上显示一条错误消息。

此用例已应用于[使用 Active Directory 选项创建自定义请求表单](#)示例。

- 1 在 vRealize Orchestrator 中，使用类似以下示例的脚本配置操作 `checkIfUsernameExists`。



使用以下脚本示例。在此示例中，**return** 是验证失败时显示的消息。

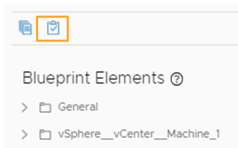
```
if (!username) {
    return "";
}

var result = ActiveDirectory.search("User", username);

if (result && result.length > 0) {
    return "Username '" + username + "' already exists.";
}

return "";
```

- 在 vRealize Automation 中，打开蓝图的自定义表单设计器，单击**外部验证**，然后将 **Orchestrator 验证** 类型拖到画布上。



- 配置外部验证选项。

- 验证标签 = 检查用户名是否存在
- 选择操作 = <您的 vRealize Orchestrator 操作文件夹>/checkIfUsernameExists
- 操作输入
 - 用户名 = “字段” 和 “用户名”
- 突出显示的字段
 - 单击**添加字段**并选择“用户名”。

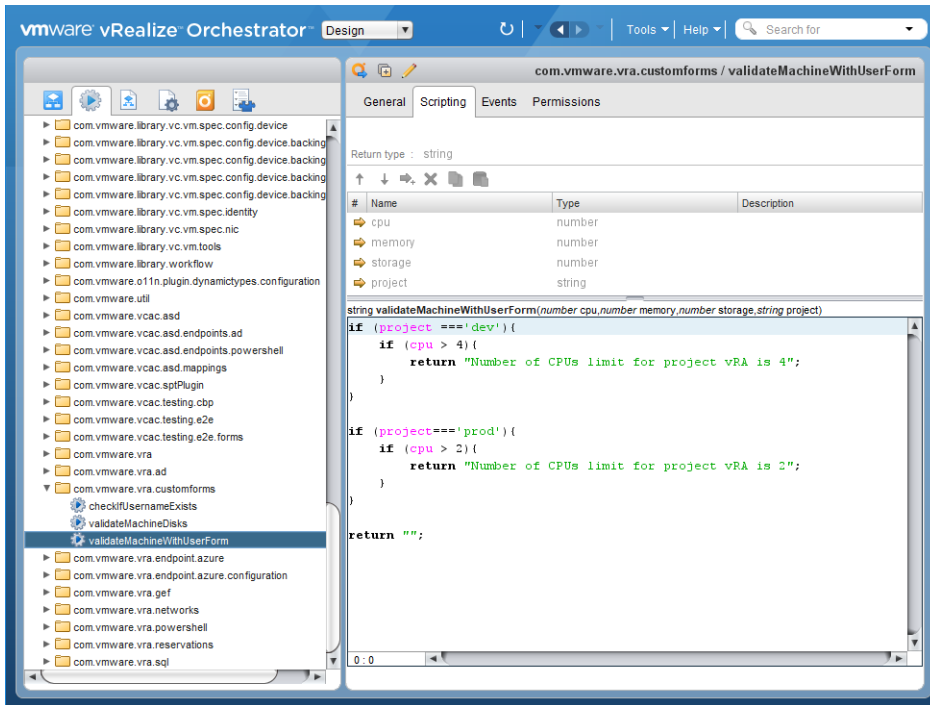
如果输入的值验证失败，将在目录请求表单中显示字段级别验证错误。如果您希望显示全局错误，请勿配置突出显示字段。

示例： vRealize Orchestrator 多个字段示例

在此用例中，您希望基于项目值验证 CPU、内存和存储值。例如，如果用户选择 Dev 项目，则最大 CPU 数量为 4。如果他们选择 Prod，则最大值为 2。

对于此用例，可向[使用 Active Directory 选项创建自定义请求表单](#)示例中添加一个项目字段。将 Dev 和 Prod 项目配置为下拉列表。

- 1 在 vRealize Orchestrator 中，使用类似以下示例的脚本配置操作 `validateMachineWithUserForm`。



使用以下脚本作为 CPU 检查的脚本示例。根据需要进行添加内存和存储值。在此示例中，`return` 是验证失败时显示的消息。

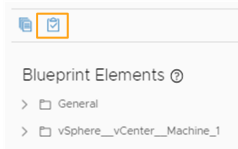
```

if (project === 'dev'){
    if (cpu > 4){
        return "Number of CPUs limit for project vRA is 4";
    }
}

if (project === 'prod'){
    if (cpu > 2){
        return "Number of CPUs limit for project vRA is 2";
    }
}

return "";
  
```

- 2 在 vRealize Automation 中，打开蓝图的自定义表单设计器，单击[外部验证](#)，然后将 **Orchestrator 验证**类型拖到画布上。



3 配置外部验证选项。

- 验证标签 = 验证计算机详细信息
- 选择操作 = <您的 vRealize Orchestrator 操作文件夹>/validateMachineWithUserForm
- 操作输入
 - cpu = “字段” 和 “CPU 数”
 - 内存 = “字段” 和 “内存 (GB)”
 - 存储 = “字段” 和 “存储 (GB)”
 - 项目 = “字段” 和 “项目”
- 突出显示的字段
 - 单击**添加字段**并选择**项目**。

在目录中，您的目录用户可能会看到类似于以下示例的验证错误。

测试并对失败的置备请求进行故障排除

作为蓝图架构师或管理员，您需要确保向用户交付正常使用的蓝图。

目录请求可能会由于多种原因失败。可能的原因有，网络流量问题、端点资源不足或蓝图规范存在缺陷。或者，置备请求成功，但部署无法正常工作。作为蓝图架构师，您需要避免提供用户无法成功部署的蓝图。

您可以创建测试服务和授权，以便可以从目录部署蓝图。请参见[配置服务目录的对照表](#)。

如果未成功置备资源，则可以使用 vRealize Automation 对失败的部署进行故障排除。

可能的故障状态

如果置备请求失败，则会看到以下状态之一。

- **失败。**请求可能会由于多种原因失败。一种原因是，目标端点上缺少资源、用于支持蓝图的资源不足或必须修复设计糟糕的蓝图，这些导致置备过程不工作。另一种原因是，请求需要您组织中的人员进行批准，而审批者拒绝了该请求。还有可能是在部署上运行的操作失败。上面提到的环境或批准原因都可能会导致失败。

使用以下故障排除工作流程调查问题的原因。如果您能够解决问题，请查看有关[取消](#)和[重新提交](#)的操作选项。请参见[已置备资源的操作菜单命令](#)。

- **部分成功。**请求可能部分成功，这意味着某些组件已部署，但并非所有置备步骤都已成功完成。

使用以下故障排除工作流程确定哪些组件仅部分成功并调查问题的原因。如果您能够解决问题，请查看有关[取消](#)以及您能否使用[恢复](#)的操作选项。请参见[已置备资源的操作菜单命令](#)和[“恢复”操作的工作原理](#)。

故障排除 workflow

可以使用此 workflow 开始调查失败的部署。如果调查表明故障是暂时性环境问题所致，您可以解决错误，并重新提交请求。如果问题与请求规范有关，您可以更新蓝图并提交新请求。

表 3-69. 如何开始对错误进行故障排除

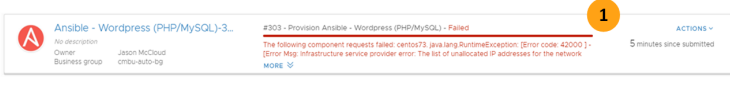
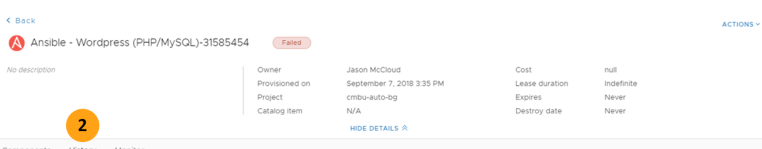
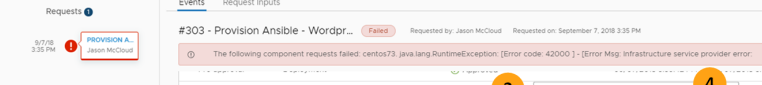
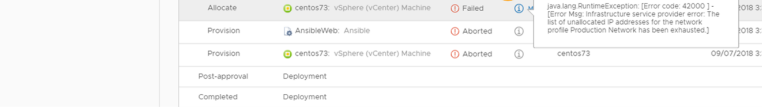
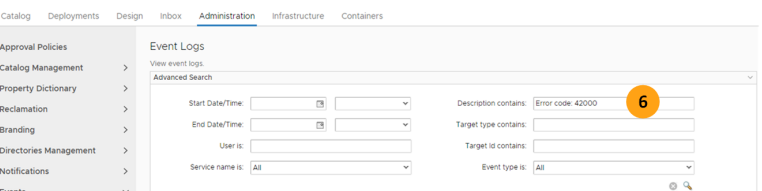
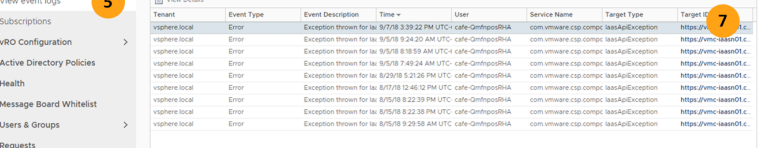
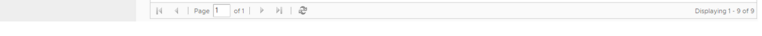
工作流	故障排除步骤	示例
1	在部署选项卡上，状态栏上指示失败的部署。部署卡包括最近一次失败的消息。有关详细信息，请单击部署名称或进度条。	
2	在部署详细信息历史记录选项卡上，可以使用事件工作流查看置备过程失败的位置。在部署上运行操作但更改失败时，此工作流也非常有用。	
3	失败状态指示工作流失败的位置。	
4	信息提供更详细的错误消息。 如果标志帮助中的此信息不足以确定并解决问题，可以查看事件日志，做进一步研究。	
5	以下步骤需要具有管理员角色。 要在其他错误和警告上下文中查找错误，请选择 管理 > 事件 > 查看事件日志 。	
6	可以使用高级搜索根据部署详细信息中的消息查找错误。	
7	要查看事件详细信息，请单击“目标 ID”链接。	

表 3-69. 如何开始对错误进行故障排除（续）

工作流	故障排除步骤	示例
8	事件详细信息提供其他置备信息，可能会帮助您进行故障排除。	
9	<p>作为管理员，您还可以在您的用户发出的其他请求上下文中查看请求。</p> <p>选择管理 > 请求，然后单击请求编号以查看请求输入和事件。</p>	

“恢复”操作的工作原理

在特定情况下，您可以对失败的部署使用“恢复”，以从故障点重新启动置备流程。启用后，可针对失败置备请求或适用操作使用“恢复”操作。

要针对置备请求使用恢复，必须在蓝图中添加 `_debug_deployment = true` 自定义属性。默认情况下，会回滚和清理失败的部署，以便回收资源。`_debug_deployment = true` 属性会保留发生故障时的部署，如果受支持，则会根据其工作原理允许“恢复”操作。如果仅对受支持的操作使用恢复，则不需要启用 `_debug_deployment` 属性。

有关 `_debug_deployment` 的详细信息，请参见《自定义属性参考》。

要对置备请求或可用操作使用恢复，您需要授权用户使用“恢复”操作。请参见[将服务、目录项和操作授权给用户](#)。

您可以授权用户对以下置备活动使用“恢复”操作。

- 置备请求
- “恢复”操作
- “缩小”操作
- “扩大”操作
- “销毁”操作

“恢复”操作限制

在决定是否可以使用“恢复”，而不是请求新的蓝图实例时，请考虑这些限制。

- 从请求之时起蓝图不可修改。

请求时，蓝图的不可修改版本与目录请求相关联。该静态版本包含所有规范，包括属性、自定义属性、设置等，与开始置备时一样。蓝图中存在会导致故障的错误时，修复错误后使用“恢复”不起作用，因为它引用的版本与请求相关联。在这种情况下，您必须置备新的实例。

示例

- 蓝图 A 请求 5 GB 的 RAM，但该请求会失败，因为您只有 3 GB 的预留。如果更新蓝图以便仅需要 3 GB 的 RAM，然后运行“恢复”，“恢复”操作会失败。当“恢复”运行时，它会检查原始请求，并且仍需要 5 GB 的 RAM。但是，如果您将业务组的系统预留增加到 5 GB，然后运行“恢复”，则“恢复”操作会成功。
- 请求蓝图 B（包括客户机自定义规范）时，请求会失败。调查显示客户机自定义规范在 vCenter Server 实例上已重命名。如果使用新名称更新蓝图并运行“恢复”，操作将会失败。蓝图已更新，但“恢复”操作仍使用原始版本。如果您打算从此使用新名称，那么请部署新的蓝图实例而不是使用“恢复”操作。否则，必须将 vCenter Server 实例上的客户机自定义规范的名称更改回原始版本所需的名称，并运行“恢复”。如果您不希望下一次置备请求失败，请记得使用正确的客户机自定义规范更新蓝图。

如果您可以更新目标部署环境以支持蓝图规范（如请求时存在），则“恢复”可以正常运行。

- “重试”只能从故障点开始。

“恢复”操作将从故障点开始重试组件任务。它不会重新提交整个置备请求。

示例

- 蓝图 C 会创建一个应用程序虚拟机和一个数据库虚拟机。数据库虚拟机将成功部署，但应用程序虚拟机上的置备会失败。如果运行“恢复”操作，则仅会重试应用程序虚拟机置备。

如果某个组件被标记为“失败”，则将其视为从未运行过。如果安装过程因脚本编制错误等原因在数据库虚拟机配置阶段失败，但数据库没有受到损坏，则在恢复操作期间运行脚本时数据库仍存在。安装脚本（包括配置脚本）不会再次运行。恢复不成功。必须修复脚本并置备新的实例。

- 要考虑的另一种情况是，步骤分配成功，但置备失败。在此示例中，当您进行恢复时，“恢复”操作会从失败的置备点开始重试，恢复请求处理的是失效的分配信息且恢复将失败。

销毁请求失败后强制销毁某个部署

可以强制销毁因销毁请求失败而处于不一致状态的部署。

在销毁部署操作期间，当 vRealize Automation 销毁部署资源失败时，销毁操作将立即停止，而不会销毁剩余的部署资源。此故障会导致部署处于不一致的状态，耗尽资源而不会通过明显方式销毁部署。业务组管理员可以强制销毁这种处于不一致状态的部署。

前提条件

- 确认以**业务组管理员**身份登录到 vRealize Automation。

- 运行“强制销毁”操作之前，请查看[已置备资源的操作菜单命令](#)中的“销毁”操作描述。

步骤

- 1 在**部署**选项卡上，找到要销毁的部署。
- 2 单击**操作**，然后单击**销毁**。
- 3 输入请求的描述和原因。
- 4 选择**强制销毁**并单击**提交**。

结果

vRealize Automation 将尝试完全销毁部署，其中包括部署中的所有资源。如果 vRealize Automation 无法销毁部署资源，则会跳过该资源并继续销毁部署中剩余的资源。

后续步骤

验证部署中的所有资源是否已成功销毁。强制销毁操作期间所有未销毁的资源均必须手动销毁。此外，确保销毁任何已置备的虚拟机对象，因为 vRealize Automation 可能会尝试在后续置备操作中重用其主机名、IP 地址和其他配置详细信息。

对包含 vRealize Orchestrator 工作流的失败部署进行故障排除

如果失败的蓝图部署包含 vRealize Orchestrator 工作流，则可以使用令牌 ID 对 workflow 问题进行故障排除。您可以使用令牌 ID 找到 vRealize Orchestrator 中的日志。

解决方案

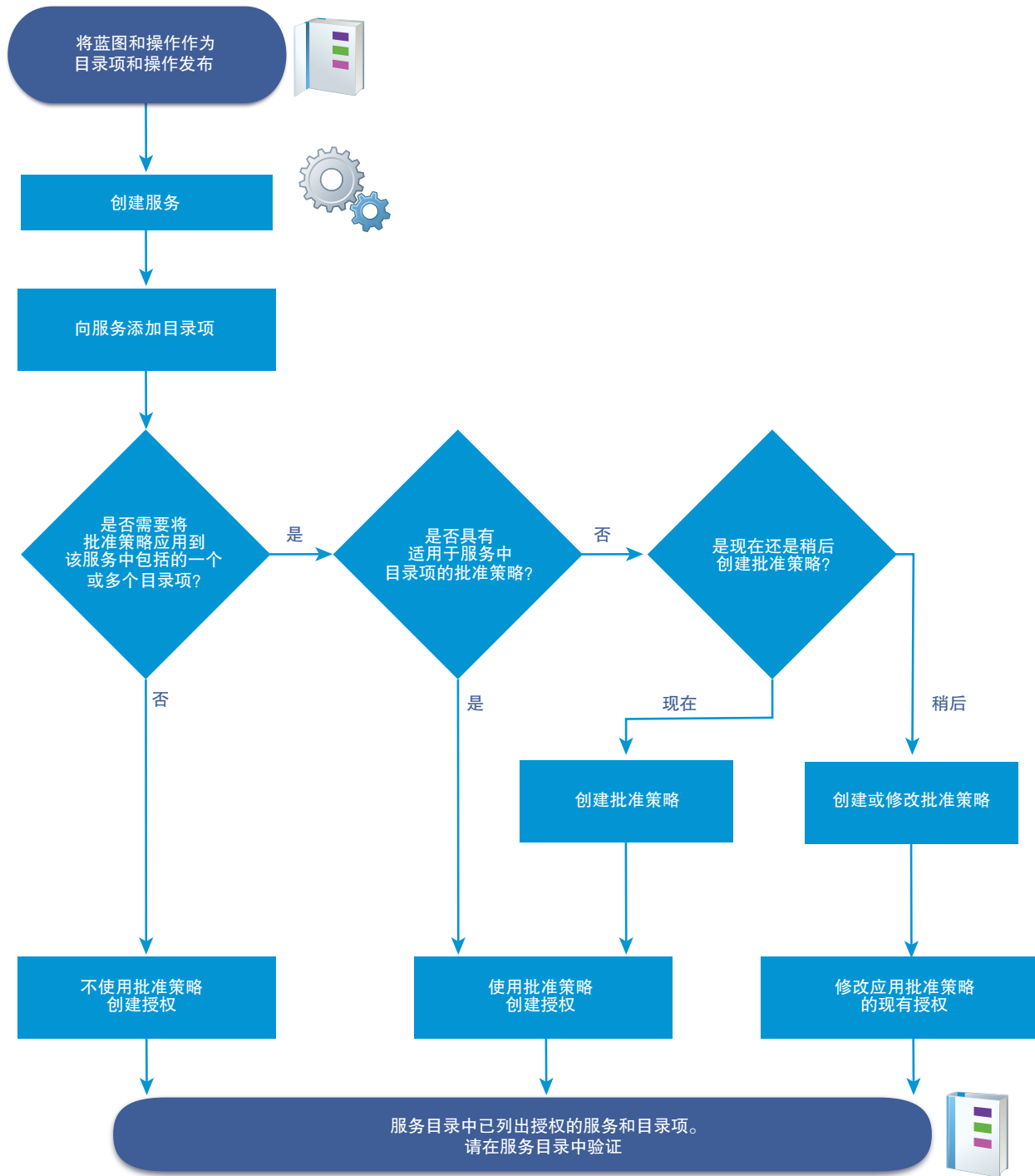
- 1 找到失败工作流的令牌 ID。
 - a 在 vRealize Automation 中，单击**部署**选项卡，然后找到部署或操作。
 - b 单击部署名称。
该请求可以是部署或操作。
 - c 单击**历史记录**选项卡，然后单击**请求输入**选项卡。
如果蓝图基于 vRealize Orchestrator 工作流，则页面标题为“vRealize Orchestrator 工作流执行详细信息”。
 - d 找到令牌 ID 并将其复制到剪贴板或文本文件。
例如，ff8080815a685352015a6c8d450801ee。
- 2 使用控制中心找到 vRealize Orchestrator 中的工作流日志
 - a 在浏览器搜索框中，输入 vRealize Automation 的基本 URL。
此时将显示 VMwarevRealize Automation 设备页面。
 - b 单击 **vRealize Orchestrator 控制中心**。
 - c 以具有 root 特权的用户身份登录。

- d 单击**检查**工作流。
- e 单击**完成**的工作流。
- f 将工作流令牌粘贴到“令牌 ID”文本框中。
该列表显示在与令牌 ID 匹配的工作流中。
- g 单击该行并检查日志，了解失败的原因。

管理服务目录

服务目录支持您的客户请求置备要使用的计算机和其他项。您可以根据构建服务、向用户授权一项或多项以及应用管治的方式来管理用户对服务目录项的访问。

将项目添加到服务目录时遵循的工作流有所不同，具体取决于是否创建和应用批准策略。



配置服务目录的对照表

创建并发布蓝图和操作之后，您可以创建 vRealize Automation 服务、配置目录项并分配授权和批准。

“配置服务目录对照表”概述了配置目录所需执行的步骤，并提供了指向决策点的链接以及每一步的详细说明。

表 3-70. 配置服务目录对照表

任务	所需角色	详细信息
❑ 添加服务。	租户管理员或目录管理员	请参见 添加服务 。
❑ 向服务添加目录项。	租户管理员或目录管理员	请参见 向服务添加目录项 。
❑ 在服务中配置目录项。	租户管理员或目录管理员	请参见 配置目录项 。
❑ 创建授权并将其应用于目录项。	租户管理员或业务组主管	请参见 将服务、目录项和操作授权给用户 。
❑ 创建批准策略并将其应用于目录项。	租户管理员或批准管理员可以创建批准策略 租户管理员或业务组主管可以应用批准策略	请参见 创建批准策略 。

创建服务

服务是一组您希望包括在服务目录中的目录项。您可以授权服务，服务将向业务组用户授权所有关联的目录项，您可以对服务应用批准策略。

服务作为一组动态目录项运行。如果授权某服务，则指定用户可在服务目录中使用与该服务关联的所有目录项，并且您在服务中添加或移除的任何目录项均会影响服务目录。

创建服务后，您可将其用作服务目录，以便您能够为附录目录用户组合服务产品，例如：包括 Windows 7、8 和 10 操作系统目录项的 Windows 桌面服务；或者包括 CentOS 和 RHEL 操作系统项的 Linux 服务。

添加服务

您可以添加服务，为服务目录用户提供目录项。所有目录项必须与某个服务关联，以便能够将该项目授权给用户。

服务授权给用户时，目录项将一起显示在服务目录中。您也可以将单个目录项授权给用户。

前提条件

以[租户管理员](#)或[目录管理员](#)身份登录到 vRealize Automation。

步骤

1 选择**管理 > 目录管理 > 服务**。

2 单击**新建**图标 (+)。

3 输入名称和描述。

这些值将显示在目录用户的服务目录中。

4 要在服务目录中添加该服务的特定图标，请单击**浏览**并选择映像。

支持的映像文件类型为 GIF、JPG 和 PNG。显示的图像为 40 x 40 像素。如果不选择自定义映像，则服务目录中将显示默认图标。

5 从**状态**下拉菜单中选择状态。

选项	描述
非活动	服务在服务目录中不可用。当服务处于此状态时，您可以将目录项与该服务关联，但无法将该服务授权给用户。如果为处于活动状态且已授权的服务选择 非活动 ，则该服务将从服务目录中移除，直到重新激活为止。
活动	（默认）服务和关联的目录项可授权给用户。授权后，它们即可用于这些用户的服务目录。
已删除	从 vRealize Automation 中移除服务。所有关联的目录项仍然存在，但与服务目录中该服务关联的任何项目不可用于目录用户。

6 配置服务设置。

以下设置为服务目录用户提供信息。这些设置不影响服务可用性。

选项	描述
小时	将时间配置为符合支持团队的可用性。时间以本地时间为准。 服务时间不能横跨两天。例如，您无法将服务时间设置为下午 4 点到凌晨 4 点。要横跨夜晚，请创建两个授权。一个授权为下午 4 点至午夜 12 点，另一个授权为午夜 12 点至凌晨 4 点。
所有者	指定充当服务和关联目录项的主所有者的用户或用户组。
支持团队	指定可以为服务目录用户使用该服务置备项目遇到的任何问题提供支持的自定义用户组或用户。
更改窗口	选择计划更改服务的日期和时间。指定的日期和时间仅供参考，不影响服务的可用性。

7 单击**添加**。

后续步骤

将目录项与某个服务关联，以便能够将项目授权给用户。请参见[向服务添加目录项](#)。

向服务添加目录项

向服务添加目录项，以便授权用户请求服务目录中的项目。目录项只能与一个服务关联。

前提条件

- 以**租户管理员**或**目录管理员**身份登录到 vRealize Automation。
- 确认服务已存在。请参见[添加服务](#)。
- 确认已发布一个或多个目录项。请参见[配置目录项](#)。

步骤

- 1 选择**管理 > 目录管理 > 服务**。
- 2 选择要添加目录项的服务，然后单击**管理目录项**。
- 3 单击**目录项图标 (+)**。
 - a 选择要包括在此服务中的目录项。
“选择目录项”对话框仅显示尚未与服务关联的项目。
 - b 单击**添加**。
- 4 单击**关闭**。

后续步骤

- 您可以向目录项添加要与其一起显示在服务目录中的自定义图标。请参见[配置目录项](#)。
- 向用户授权服务或目录项，使用户能够在服务目录中请求服务或目录项。请参见[创建授权](#)。

使用目录项和操作

目录项是计算机、软件组件和其他对象的已发布蓝图。目录管理区域中的操作是您可在置备的目录项上运行的已发布操作。您可以使用这些列表确定哪些蓝图和操作已发布，以便服务目录用户能够使用。

发布的目录项

目录项是指已发布的蓝图。已发布的蓝图组还可以在其他蓝图中使用。目录项列表中不会显示其他蓝图中重用的蓝图。

已发布的目录项还可以包含仅作为蓝图组件的项目。例如，已发布的软件组件列为目录项，但只能作为部署的一部分提供。

部署目录项必须与某个服务关联，才能在服务目录中提供给授权用户。服务目录中仅显示活动项。您可以将目录项配置为其他服务，将其停用（如果要暂时将其从服务目录中移除），并添加显示在目录中的自定义图标。

发布的操作

操作是指您可以对已置备的目录项进行的更改。例如，您可以重新引导虚拟机。

操作可以包括内置操作或使用 XaaS 创建的操作。添加计算机或提供的其他蓝图时，将添加内置操作。必须创建并发布 XaaS 操作。

操作不与服务关联。您必须将操作包括在包含运行该操作的目录项的授权中。授权给用户的操作不显示在服务目录中。操作对服务目录用户的**部署**选项卡中已置备项目的可用性取决于这些操作是适用于项目，还是适用于其当前状态。

您可以为**部署**选项卡中显示的操作添加自定义图标。

配置目录项

目录项是一个可以授权给用户的已发布蓝图。您既可以使用目录项选项更改状态或相关联的服务，也可以查看包含选定目录项的授权。

只有与服务关联并授权给用户的目录项才会显示在服务目录中。目录项只能与一个服务关联。

如果不希望目录项显示在服务目录中，且不将其从授权或已发布目录项列表中移除，则可以取消激活它。取消激活的目录项在网格中为已弃用状态，在配置详细信息中为非活动状态。你可以稍后激活它。

前提条件

- 以**租户管理员**或**目录管理员**身份登录到 vRealize Automation。
- 确认至少已将一个蓝图作为目录项发布。请参见[发布蓝图](#)。

步骤

- 1 选择**管理 > 目录管理 > 目录项**。
- 2 选择目录项，然后单击**配置**。
- 3 配置目录项设置。

选项	描述
图标	浏览图像。支持的映像文件类型为 GIF、JPG 和 PNG。显示的图像为 40 x 40 像素。如果不选择自定义映像，则服务目录中将显示默认目录图标。
状态	可能的值包括 活动 、 非活动 和 转储 。 <ul style="list-style-type: none"> ■ 活动。目录项显示在服务目录中，授权用户可以使用它来置备资源。项目在目录项列表中显示为“已发布”。 ■ 非活动。目录项在服务目录中不可用。项目在目录项列表中显示为“已弃用”。 ■ 转储。目录项在服务目录中不可用。如果菜单项曾处于非活动状态且您使用“转储”表示正在考虑重新激活该项目，请选择此菜单项。在目录项列表中显示为“转储”。
配额	设置用户可以部署的此目录项的实例数量。 如果用户部署的数量超出该值，将在目录请求显示一条通知，且无法提交请求。
服务	选择一种服务。所有目录项必须与某个服务关联，才能在服务目录中向授权用户显示。该列表包括活动和非活动服务。

- 4 要查看将目录项提供给用户的授权，请单击**授权**选项卡。
- 5 单击**更新**。

后续步骤

- 要使目录项在服务目录中可用，必须将与项目关联的服务或各个项目授权给用户。请参见[创建授权](#)。
- 要指定授权处理顺序以便正确应用各个用户的批准策略，请为同一业务组的多个授权设置优先级顺序。请参见[区分授权优先级](#)。

为服务目录配置操作

操作是指可以在置备项上运行的更改或工作流。您可以添加图标或查看包括所选操作的授权。

操作要么是已置备计算机、网络和其他蓝图组件的内置操作，要么是已发布的 XaaS 操作。

图标支持的图像文件类型为 GIF、JPG 和 PNG。显示的图像为 40 x 40 像素。如果不选择自定义图像，则部署选项卡上将显示默认操作图标。

前提条件

- 以租户管理员或目录管理员身份登录到 vRealize Automation。
- 确认至少有一个已发布的操作。请参见[发布蓝图](#)和[发布资源操作](#)。

步骤

- 1 选择**管理 > 目录管理 > 操作**。
- 2 选择共享操作，然后单击**查看详细信息**或（对于 XaaS 操作）**配置**。
- 3 浏览图像。
- 4 要查看使用户可以采取操作的授权，请单击**授权**选项卡。
- 5 单击**完成**。

后续步骤

[将服务、目录项和操作授权给用户](#)。

创建授权

授权控制服务目录中可供选定业务组成员使用的项目和操作。授权必须处于活动状态，项目才会显示在服务目录中。如果项目需要管治，则您可以使用授权将批准策略应用于不同的项目。

要配置授权，服务中必须包含目录项。授权可以包括多个服务、其他授权包含的服务中的目录项，以及可以在部署的目录项中运行的操作。

理解授权选项交互

配置授权的方式决定服务目录中显示的内容。服务、目录项和组件、操作以及批准策略的交互影响用户可请求的服务目录以及批准策略的应用方式。

创建授权时，您必须考虑服务、目录项、操作和批准的交互。

- [授权中的服务](#)
授权的服务作为一组动态目录项运行。如果目录项添加到已经过授权的服务，则指定用户可以使用新目录项，而无需进行任何其他配置。
- [授权中的目录项和组件](#)
已授权目录项是可以在服务目录中请求的蓝图。已授权组件是蓝图的一部分，但是您不能在服务目录中专门请求它们。

■ 授权中的操作

操作在已部署目录项上运行。已置备目录项以及您有权在其上运行的操作会显示在“部署”选项卡中。要在已部署项目上运行操作，该操作必须包含在与通过服务目录置备项目的目录项相同的授权中。

■ 授权中的批准策略

批准策略会应用到授权中，以便您可以在环境中管理资源。

授权中的服务

授权的服务作为一组动态目录项运行。如果目录项添加到已经过授权的服务，则指定用户可以使用新目录项，而无需进行任何其他配置。

如果将批准策略应用于服务，则在请求时，所有项目将使用相同的批准策略。

授权中的目录项和组件

已授权目录项是可以在服务目录中请求的蓝图。已授权组件是蓝图的一部分，但是您不能在服务目录中专门请求它们。

已授权目录项和组件可以包括以下任一项目：

目录项

- 要提供给授权用户的任何服务（甚至是当前授权中未包含的服务）中的项目。

例如，作为目录管理员，您将多个不同版本的 Red Hat Enterprise Linux 与 Red Hat 服务关联，并将该服务授权给产品 A 的质量工程师。然后，您收到一项请求：为培训团队创建仅包含基于 Linux 操作系统的最新版本的服务目录项。您为培训团队创建授权，将最新版本的其他操作系统包括在服务中。您已将最新版本的 RHEL 与其他服务关联，因此将 RHEL 添加为目录项，而不是添加整个 Red Hat 服务。

- 包括在当前授权中所含服务中的项目，但您希望对各个目录项应用另一种批准策略，这种策略与应用到该服务的策略不同。

例如，作为业务组主管，您可以授权开发团队使用包括三个虚拟机目录项的服务。您将应用一项批准策略，该策略需由管理具有四个以上 CPU 的计算机的虚拟基础架构管理员批准。其中一个虚拟机用于性能测试，因此您可以将其添加为目录项，并对同一组的用户应用限制较少的批准策略。

组件

- 由于组件是目录项的一部分，它们在服务目录中不是按名称提供的。您可以单独授权它们，以便可以应用与其所在目录项不同的特定批准策略。

例如，项目包括计算机和软件。计算机作为可置备项提供，且其批准策略需要站点管理员批准。软件不作为独立的可置备项提供，仅充当计算机请求的一部分，但是软件的批准策略需要组织的软件许可管理员批准。在服务目录中请求计算机时，计算机必须先经过站点管理员和软件许可管理员批准，然后才能进行置备。置备后，计算机与软件条目作为计算机的一部分显示在请求者的“部署”选项卡中。

授权中的操作

操作在已部署目录项上运行。已置备目录项以及您有权在其上运行的操作会显示在“部署”选项卡中。要在已部署项目上运行操作，该操作必须包含在与通过服务目录置备项目的目录项相同的授权中。

例如，授权 1 包括 vSphere 虚拟机和“创建快照”操作，授权 2 仅包括 vSphere 虚拟机。通过授权 1 部署 vSphere 计算机时，“创建快照”操作可用。通过授权 2 部署 vSphere 计算机时，没有任何操作。要将该操作提供给授权 2 用户，请将“创建快照”操作添加到授权 2。

如果选择的操作不适用于授权中的任何目录项，则不会以操作的形式显示在“部署”选项卡上。例如，授权包括 vSphere 计算机，并且您为云计算授权销毁操作。销毁操作不适用于在已置备的计算机上运行。

您可以对操作应用另一批准策略，这种策略与应用到授权中目录项的策略不同。

如果服务目录用户是多个业务组的成员，且某一组仅有权打开电源和关闭电源，而另一个组仅有权进行销毁，则对于适用的置备计算机，该用户将使所有这三个操作可供这些业务组使用。

向用户授权操作的最佳做法

蓝图比较复杂。当授权在已置备蓝图上运行操作时，可能会导致出现意外行为。授权服务目录用户在已置备的项目上运行操作时，请遵循以下最佳做法。

- 将“销毁计算机”操作授权给用户时，便会授权他们“销毁部署”。已置备的蓝图是一个部署。
部署可以包含计算机。如果服务目录用户有权运行“销毁计算机”操作、但无权运行“销毁部署”，则当用户在部署中的最后一个或唯一一个计算机上运行“销毁计算机”操作时，将显示一条消息，指出他们无权运行该操作。同时授权这两个操作可确保从环境中移除该部署。要管理“销毁部署”操作的管治情况，您可以创建预批准策略并将其应用于该操作。此策略将允许指定的审批者在运行“销毁部署”请求之前验证该请求。
- 将“更改租约”、“更改所有者”、“过期”、“重新配置”以及其他可应用于计算机和部署的操作授权给服务目录用户时，即向他们授权这两个操作。

授权中的批准策略

批准策略会应用到授权中，以便您可以在环境中管理资源。

要在创建授权时应用批准策略，该策略必须已存在。否则，您仍可创建授权并使其处于草稿或非活动状态，直到为此授权中的目录项和操作创建所需的批准策略为止，然后再应用这些策略。

无需对任何项目或操作应用批准策略。如果未应用批准策略，则会在不触发批准请求的情况下部署已请求的项目和操作。

将服务、目录项和操作授权给用户

将服务、目录项或操作添加到授权时，即表示您允许该授权中标识的用户请求服务目录中的可置备项。操作将与这些项目关联，并显示在请求用户的部署选项卡上。

存在多个用户角色有权为业务组创建授权。

- 租户管理员可以为其租户中的任意业务组创建授权。
- 业务组主管可以为他们管理的组创建授权。
- 目录管理员可以为其租户中的任意业务组创建授权。

创建授权时，必须为该授权选择业务组和业务组成员。

要了解如何创建授权以便可以使用具有批准的服务、目录项和操作进行交互，请参见[创建授权](#)。

前提条件

- 以**租户管理员**或**目录管理员**身份登录到 vRealize Automation。
- 确认授权给用户的目录项与服务关联。请参见[向服务添加目录项](#)。
- 确认您为其定义授权的业务组已存在，且成员用户和用户组已定义。请参见[创建业务组](#)。
- 如果计划在创建此授权时添加批准，则确认该批准策略已存在。请参见[创建批准策略](#)。如果要將服务目录中的项授权给用户但不添加批准，您可以在以后修改授权以添加批准。

步骤

- 1 选择**管理 > 目录管理 > 授权**。
- 2 单击**新建**图标(+)。
- 3 配置“**详细信息**”选项。

“详细信息”确定授权在授权列表中的显示方式，以及哪些用户有权访问服务目录中的项目。

选项	描述
名称和描述	授权列表中显示的授权的相关信息。
过期日期	如果希望授权在某一特定日期变成非活动状态，请设置该日期和时间。
状态	可能值包括“活动”、“非活动”和“已删除”。 <ul style="list-style-type: none"> ■ 活动。项目在服务目录中可用。添加或编辑授权时，此选项可用。 ■ 非活动。项目在服务目录中不可用。该授权因过期日期已到而取消激活或由用户取消激活。 ■ 已删除。删除该授权。
业务组	选择业务组。只能为一个业务组创建授权，且授权用户必须是该业务组的成员。 如果要使授权对所有用户可用，您必须具有“所有用户”业务组，或者必须为每个业务组创建授权。 如果您以业务组主管身份登录，则只能为相应的业务组创建授权。
用户和组	选择 所有用户和组 以将目录项和操作授权给业务组的所有成员，或者也可以向各个用户或组授权。要激活授权，您必须选择至少一个业务组用户或组。

- 4 单击**下一步**。

5 单击新建图标 (+)，可利用此授权向用户授权服务、目录项或操作。

您可以使用服务、项目和操作的各种组合创建授权。

选项	描述
授权的服务	需要允许授权用户访问与某个服务关联的所有已发布目录项时，可添加该服务。 授权的服务是动态授权。如果以后将某个项目添加到该服务，则会将该项目添加到授权用户的服务目录中。授权既可以包括服务也可以包括单独的目录项。
授权目录项和组件	添加授权用户可用的单独项目。 授权既可以包括服务也可以包括单独的目录项。要为服务中的某个项目应用不同的批准策略，请将其添加为目录项。当项目及其所属服务位于相同的授权中时，项目的批准策略优先于项目所属服务的批准策略。如果位于不同的授权中，则其顺序根据设置的优先级而异。 目录项必须与服务关联，才能在服务目录中使用。目录项可与任何服务关联，而不仅仅是当前授权中的服务。 组件是目录项的一部分，但在服务目录中无法按名称提供。例如，MySQL 软件是 CentOS 虚拟机目录项的组件。组件会随目录项一同授权。如果要应用特定于软件的批准策略，可以单独授权项目。否则，您无需授权组件使其随父项部署。
授权的操作	当您需要允许用户为已置备的项目运行操作时，可添加这些操作。 要针对通过此授权置备的项目运行的操作必须包含在同一授权中。 授权的操作不显示在服务目录中，而显示在已置备项目的“部署”选项卡上。
操作仅适用于在此授权中定义的项目	确定授权操作是授予所有适用的服务目录项，还是仅授予此授权中的项目。 如果选择此选项，这些操作将授予给此授权中适用项目的业务组成员。使用这种操作授权方法，您可以指定特定项的操作。 如果未选择此选项，这些操作将授予给在所有适用目录项的授权中指定的用户，无论这些项目是否包含在此授权中均如此。这些操作在应用的所有批准策略也均会处于活动状态。

6 使用每个部分中的下拉菜单筛选可用的项目。

7 选中相应的复选框，将项目包括在授权中。

8 要将批准策略添加到选定服务、项目或操作，请从将此策略应用于选定的项目下拉菜单中选择批准策略。

如果将批准策略应用于服务，则服务中的所有项目将采用相同的批准策略。要为某个项目应用不同的策略，请将其添加为应用适当策略的目录项。

9 单击确定。

服务、项目或操作已添加到授权中。

10 单击完成保存该授权。

结果

如果授权状态为“活动”，则服务和项目将添加到服务目录中。

后续步骤

确认授权的服务和目录项显示在授权用户的服务目录中，且请求的项目已按预期置备目标对象。您可以代表选定用户请求项目。

区分授权优先级

如果同一业务组存在多个授权，您可以区分授权的优先级，以便在服务目录用户提出请求时，系统按照指定的顺序处理授权和关联的批准策略。

如果配置用户组的批准策略并希望组成员对一个或多个服务、目录项或操作使用唯一的策略，请设置成员授权优先于组授权。当成员请求服务目录中的项目时，应用的批准策略以业务组授权的优先级顺序为准。第一次发现成员名称（作为自定义用户组的一部分或作为单个用户）时，应用的批准策略便是如此。

例如，您可以为同一目录项创建两个授权，以便能够对会计用户组应用一项批准策略，而对该组的成员 Chris 应用另一项批准策略。

表 3-71. 示例授权

授权 1	授权 2
业务组：财务	业务组：财务
用户和组：会计部门	用户和组：Chris
目录项 1：策略 A	目录项 1：策略 C

Chris 请求服务目录中的目录项 1。根据“财务”业务组的授权优先级顺序，另一策略将应用到 Chris 的请求。

表 3-72. 示例结果

配置和结果	优先级顺序	优先级顺序
优先级顺序	1: 授权 1 2: 授权 2	1: 授权 2 2: 授权 1
应用的策略	应用策略 A。 Chris 是“会计”用户组的成员。对授权用户 Chris 的搜索在授权 1 处停止，系统将应用该批准策略。	应用策略 C。 对授权用户 Chris 的搜索在授权 2 处停止，系统将应用该批准策略。

前提条件

以**租户管理员**或**目录管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 目录管理 > 授权**。
- 2 单击**优先级**图标 (🔍)。
- 3 从**业务组**下拉列表中选择业务组。
- 4 将授权拖动到列表中的新位置以更改其优先级。

5 选择更新方法。

选项	描述
更新	保存更改。
更新并关闭	保存您所做的更改，并关闭 区分元素优先级 窗口。

使用批准策略

批准策略是添加到服务目录请求的管治，使您能够管理环境中的资源。每个策略是一组定义的条件，可在向用户进行授权时应用于服务、目录项和操作。

批准策略过程

首先，租户管理员或批准管理员在需要管治置备的位置创建批准策略。

批准策略针对批准策略类型或特定项目而创建。如果策略基于策略类型，则可将其应用于匹配的目录项类型。例如，如果策略基于软件策略类型，则可为授权中的任意软件项定义策略，并将策略应用于该项目。如果策略针对特定项目，则仅可将其应用于该项目。例如，如果项目是特定的软件项，则仅可将策略应用于授权中的这个特定数据库软件项。

策略可以包含预批准和后批准要求。对于预批准，请求必须先经过批准，然后才能置备请求的项目。后批准策略要求审批者先接受请求，然后再将请求的项目提供给请求用户。

预批准和后批准配置由一个或多个级别组成，以便确定触发批准策略的时间和批准请求的人员或方式。您可以包含多个级别。例如，批准策略可包含用于管理员批准的级别，后跟用于财务批准的级别。

接下来，租户管理员或业务组主管根据需要将批准策略应用于服务、目录项和操作。

最后，服务目录用户请求应用批准策略的项目时，审批者在其**收件箱**选项卡上批准或拒绝请求。请求用户可以在其**部署**选项卡上跟踪特定请求的批准状态。

基于虚拟机策略类型的批准策略示例

您可以创建一个能够应用于同一目录项类型的批准策略，但在服务目录中请求项目时，这将产生不同的结果。根据定义和应用批准策略的方式，对服务目录用户和审批者产生的影响也会有所不同。

下表中包括所有基于同一批准策略类型的不同批准策略示例。这些示例说明了您可采用哪些方式配置批准策略以完成不同类型的管治。

表 3-73. 批准策略和结果示例

管治目标	选定策略类型	预批准或后批准	何时需要批准	谁是审批者	如何在授权中应用策略	在服务目录中请求项目的结果
业务组主管必须批准任何虚拟机请求。 批准策略必须适用于多个授权中的多个业务组。	服务目录 - 目录项请求 - 虚拟机	添加到“预批准”选项卡	选择“始终需要”	选择 根据请求确定审批者 。 选择条件 业务组 > 管理员 > 用户 > 主管 。 选择 任何人都可批准 。	授权基于业务组。此批准可在虚拟机需要主管批准的授权中使用。	服务目录用户请求应用此批准的虚拟机时，业务组主管必须在置备计算机之前批准请求。
向请求用户发布虚拟机之前，虚拟基础架构管理员必须确认虚拟机的置备正确并批准请求。	服务目录 - 目录项请求 - 虚拟机	添加到“后批准”选项卡	选择“始终需要”	选择 特定用户和组 。 选择虚拟基础架构管理员的自定义用户组。 选择 任何人都可批准 。	此批准可在您希望虚拟基础架构管理员检查 vCenter Server 上的已置备虚拟机的任何授权中使用。	服务目录用户请求应用此批准的虚拟机时，将置备该虚拟机。如果 VI 管理员组的每个成员均批准请求，则向用户发布计算机。
要管理虚拟基础架构资源和控制价格，请添加两个预批准级别，因为一个批准用于管理计算机资源，另一个用于控制计算机每日价格。	服务目录 - 目录项请求 - 虚拟机	添加到“预批准”选项卡	1 级 选择 基于条件需要 。 配置条件，其中 CPU > 6、内存 > 8 GB 或存储 > 100 GB。	选择 根据请求确定审批者 。 选择条件“请求者” > “主管”。 选择。 单击 系统属性 ，然后选择 CPU、内存和存储 ，使审批者能够将值更改为可接受的级别。	此批准策略可在您希望请求用户的管理员和财务部门的成员批准请求的授权中使用。	服务目录用户在请求虚拟机时，系统将评估请求，确定请求的 CPU、内存或存储量是否超出在 1 级条件中指定的数量。如果未超出，则将评估 2 级条件。如果请求至少超出一个 1 级条件，则管理员必须批准请求。管理员可以选择减少请求的配置量并批准请求，或者也可以拒绝请求。
			2 级 选择 基于条件需要 。 配置条件“价格” > “每天 15.00”。	选择 特定用户和组 。 选择财务部门的自定义用户组。 选择 任何人都可批准 。		
对于参数化蓝图目录项，云管理员必须批准部署请求，即将 size 的 vSphere 计算机组件配置文件设置为 large。	服务目录 - 目录项请求 - 虚拟机	添加到“预批准”选项卡	1 级 选择 基于条件需要 。 2 级 选择 单个条件 。 选择 组件配置文件 > vSphere 计算机大小 。 配置条件大小 = 大。	选择 特定用户和组 。 选择经允许批准请求的用户和组。 选择 任何人都可批准 。	在需要云管理员批准置备请求的授权中，可以使用此批准策略。	服务目录用户请求应用此批准的虚拟机时，云管理员必须在置备计算机之前批准请求。

在复合部署中应用批准策略的操作示例

将批准策略应用于可在复合蓝图中的各种组件上运行的操作时，根据配置授权和应用批准策略的方式的不同，批准过程也有所不同。

此示例使用具体细节构建蓝图，然后将批准策略应用于各种操作。您可从不同授权的已置备蓝图上的服务目录中运行这些操作。该蓝图是包含另一蓝图的复合蓝图。这些操作用于销毁已置备项目、蓝图部署和计算机的虚拟机。产生的行为包括销毁的对象以及应用的批准策略何时触发批准请求。

示例蓝图

在此示例中，您将使用虚拟机配置包含嵌套蓝图的蓝图。

- 蓝图 1 - 持续集成蓝图
 - 蓝图 2 - 生产前蓝图
 - 虚拟机 1 - TestAsAService vSphere 虚拟机

销毁操作的批准策略

配置两个批准策略来销毁已置备项目。在此示例中，“销毁 - 部署”操作可在蓝图 1 或蓝图 2 上运行。“销毁 - 虚拟机”操作可在虚拟机 1 上运行。创建批准策略，以便能够将其应用于授权中的操作。

批准策略名称	批准策略类型
批准策略 A	服务目录 - 资源操作请求 - 销毁 - 部署
批准策略 B	服务目录 - 资源操作请求 - 销毁 - 虚拟机

应用于操作的授权和批准策略

您可以配置三个授权。每个授权均包含复合蓝图。在每个授权中，添加销毁操作并应用批准策略。

授权名称	对已置备计算机的授权操作	应用的批准策略
授权 1	销毁 - 部署	批准策略 A
授权 2	销毁 - 虚拟机	批准策略 B
授权 3	销毁 - 部署	批准策略 A
	销毁 - 虚拟机	批准策略 B

服务目录中的用户操作

服务目录用户运行该操作时，将根据用户在其中运行操作的项目销毁蓝图或计算机。

服务目录中的用户操作	所选操作	已销毁的蓝图或计算机
操作 1	销毁 - 部署操作在蓝图 1 上运行 - 持续集成蓝图	蓝图 1、蓝图 2 和虚拟机 1
操作 2	销毁 - 部署操作在嵌套蓝图 2 上运行 - 生产前蓝图	蓝图 2 和虚拟机 1
操作 3	销毁 - 虚拟机操作在位于部署内部的计算机上运行，虚拟机 1 - TestAsAService vSphere 虚拟机	虚拟机 1

应用于授权中操作的批准策略

您应用批准策略，审批者将接收一个批准请求，具体取决于服务目录用户在其上运行操作的蓝图或计算机。

授权名称	操作的批准策略	用户操作	触发的批准请求	已销毁的蓝图或计算机（如果获准）
授权 1 - 销毁部署批准策略	仅限“销毁 - 部署”操作的策略 A（销毁部署批准策略）	操作 1（在蓝图 1 上运行“销毁 - 部署”操作）	仅针对蓝图 1 触发批准请求	蓝图 1、蓝图 2 和虚拟机 1
		操作 2（在蓝图 2 上运行“销毁 - 部署”操作）	仅针对蓝图 2 触发批准请求	蓝图 2 和虚拟机 1
		操作 3（在虚拟机 1 上运行“销毁 - 虚拟机”操作）	未触发批准请求	虚拟机 1
授权 2	仅限“销毁 - 虚拟机”操作的策略 B（销毁 - 虚拟机策略）	操作 1（在蓝图 1 上运行“销毁 - 部署”操作）	未触发批准请求	蓝图 1、蓝图 2 和虚拟机 1
		操作 2（在蓝图 2 上运行“销毁 - 部署”操作）	未触发批准请求	蓝图 2 和虚拟机 1
		操作 3（在虚拟机 1 上运行“销毁 - 虚拟机”操作）	仅针对虚拟机 1 触发批准请求	虚拟机 1
授权 3	“销毁 - 部署”操作的策略 A（销毁部署批准策略）和“销毁 - 虚拟机”操作的策略 B（销毁 - 虚拟机策略）	操作 1（在蓝图 1 上运行“销毁 - 部署”操作）	仅针对蓝图 1 触发批准请求	蓝图 1、蓝图 2 和虚拟机 1
		操作 2（在蓝图 2 上运行“销毁 - 部署”操作）	仅针对蓝图 2 触发批准请求	蓝图 2 和虚拟机 1
		操作 3（在虚拟机 1 上运行“销毁 - 虚拟机”操作）	仅针对虚拟机 1 触发批准请求	虚拟机 1

多个授权中的批准策略示例

如果将批准策略应用于某个项目，且该项目在授权给业务组中多个相同用户的多个授权中使用，则即便在批准策略未明确应用于授权的服务中，亦会触发该项目的批准策略。

例如，您可创建以下蓝图、服务、批准策略和授权。

蓝图

- RHEL vSphere 虚拟机
- QE 测试包括 RHEL vSphere 虚拟机
- QE 培训包括 RHEL vSphere 虚拟机

服务

- QE 测试蓝图与测试服务关联

■ QE 培训蓝图与培训服务关联

授权

- 授权 1
- 授权 2

表 3-74. 授权配置

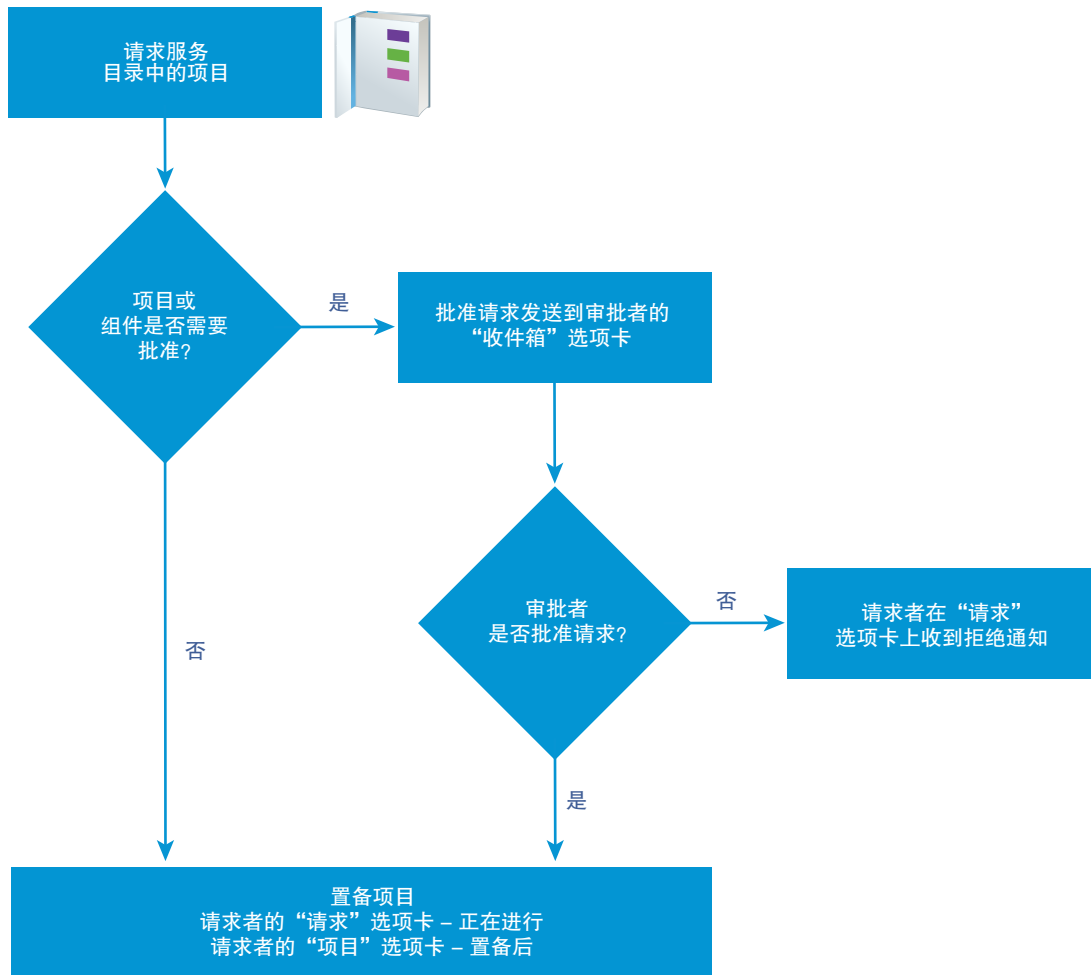
授权名称	业务组	授权的服务	授权的项目
授权 1	QE	正在测试	目录项请求 - 应用于虚拟机组件的虚拟机
授权 2	QE	培训	

结果

用户选择服务目录中的“QE 培训”时，将触发 RHEL vSphere 虚拟机的批准策略，因为它是以 QE 培训蓝图中使用的虚拟机组件为基础的蓝图。

处理服务目录中的批准策略

用户请求服务目录中已应用批准策略的项目时，该请求由审批者和请求用户进行处理。工作流如下所示：



创建批准策略

租户管理员和批准管理员可以定义批准策略并在授权中使用这些策略。您可以为预批准和后批准事件配置具有多个级别的批准策略。

如果修改软件组件蓝图中的设置且批准策略使用该设置触发批准请求，则批准策略可能无法按预期工作。如果必须修改组件中的设置，请确认所做的更改不会影响一个或多个批准策略。

前提条件

以**租户管理员**或**批准管理员**身份登录到 vRealize Automation。

步骤

1 指定批准策略信息

创建批准策略时，定义批准策略类型、名称、描述和状态。

2 创建批准级别

创建批准策略时，可以添加预批准级别和后批准级别。

3 将批准表单配置为包括系统和自定义属性

您可以添加批准表单中显示的系统 and 自定义属性。添加这些属性后，审批者能够在完成批准请求之前更改计算机资源设置（例如，CPU 或内存）的系统属性值和自定义属性值。

4 批准策略设置

创建批准策略时，您可以配置各种选项，确定何时必须批准服务目录用户请求的项目。在请求开始置备之前或者项目置备之后、但在向请求用户发布项目之前，可能需要批准。

指定批准策略信息

创建批准策略时，定义批准策略类型、名称、描述和状态。

前提条件

以**租户管理员**或**批准管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 批准策略**。
- 2 单击**新建**图标 (+)。
- 3 为软件组件选择策略类型。

选项	描述
选择批准策略类型	<p>根据策略请求类型创建批准策略。</p> <p>选择此选项可定义适用于此类所有目录项的批准策略。请求类型可以是通用请求、目录项请求或资源操作请求。</p> <p>可用条件配置选项因类型不同而异。类型越具体，配置字段就越具体。例如，“服务目录 - 目录项请求”仅提供所有目录项请求共用的字段，但“服务目录 - 目录项请求 - 虚拟机”还提供通用选项和特定于虚拟机的选项。</p> <p>请求类型限制了可以应用批准策略的目录项或操作。</p>
选择项目	<p>根据特定项目创建批准策略。</p> <p>选择此选项可定义适用于在服务目录中不作为单独项目提供、而仅作为计算机或其他部署一部分的特定项目的批准策略。例如，软件组件。</p> <p>可用的条件配置字段特定于项目，且可能会比为策略类型项目提供的标准更详细。</p>
列表	<p>列出可用的策略类型或目录项。</p> <p>搜索或排序各列，以便查找特定的项目或类型。</p>

- 4 单击**确定**。
- 5 输入名称和可选描述。
- 6 从**状态**下拉菜单中选择策略的状态。

选项	描述
草稿	以可编辑的状态保存批准策略。
活动	以只读状态保存可在授权中使用的批准策略。
非活动	以只读状态保存无法在授权中使用的批准策略，直到激活该策略为止。

后续步骤

创建预批准级别和后批准级别。

创建批准级别

创建批准策略时，可以添加预批准级别和后批准级别。

您可以为批准策略创建多个批准级别。服务目录用户请求要应用具有多个级别的批准策略的项目时，第一个级别的批准请求始终必须在被接受之后才能发送到下一个审批者。请参见[使用批准策略](#)。

如果配置由租期请求触发的批准策略，则必须选择“始终需要”作为批准要求。

前提条件

[指定批准策略信息](#)。

步骤

- 1 在**预批准**或**后批准**选项卡中，单击**新建**图标 (+)。
- 2 输入名称和可选描述。
- 3 选择批准要求。

选项	描述
始终需要	针对每个请求触发批准策略。
基于条件需要	<p>批准策略基于一个或多个条件子句。</p> <p>如果选择此选项，则必须创建条件。当此批准策略应用于授权中的合格服务、目录项或操作时，系统将评估条件。如果条件成立，则请求在置备之前必须先使用指定的审批者方法批准。如果条件不成立，则在不要批准的情况下置备请求。例如，针对具有 4 个或更多 CPU 的虚拟机的任何请求均必须由虚拟基础架构管理员批准。</p> <p>条件所依据的字段的可使用性取决于选定的批准策略类型或目录项。</p> <p>输入条件的值时，这些值区分大小写。</p> <p>要配置多个条件子句，请为子句选择布尔运算。</p>

- 4 选择审批者。

选项	操作
特定用户和组	将批准请求发送给选定用户。
根据请求确定审批者	<p>根据定义的条件将批准请求发送给用户。</p> <p>注 确保 vRealize Automation 中存在将由请求和请求者动态确定的所有用户，且这些用户已在 Active Directory 中同步，并且能够从管理 > 用户和组 > 目录用户和组浏览这些用户。</p> <p>如果用户在身份目录管理身份提供程序中未同步，并且在目录请求期间以任何方式引用该用户，则请求将失败，并显示请求项批准运行时错误。</p>
使用事件订阅	<p>根据定义的事件订阅处理批准请求。</p> <p>您必须在管理 > 事件 > 订阅中定义工作流订阅。适用的工作流订阅为预批准和后批准。</p>

5 指示必须批准请求或操作的人员。

选项	描述
任何人均可批准	请求必须至少经过一个审批者批准方可处理。 请求服务目录中的项目时，批准请求将发送给所有审批者。如果一个审批者批准请求，则该请求将会获准，然后批准请求将从其他审批者的收件箱中移除。
所有人都必须批准	请求必须至少经过所有指定的审批者批准方可处理。

6 将属性添加到批准表单或保存该级别。

- 要将属性添加到批准表单，请单击**系统属性**或**自定义属性**。
- 要保存级别，请单击**确定**。

后续步骤

要将属性添加到批准表单，请参见[将批准表单配置为包括系统和自定义属性](#)。

将批准表单配置为包括系统和自定义属性

您可以添加批准表单中显示的系统 and 自定义属性。添加这些属性后，审批者能够在完成批准请求之前更改计算机资源设置（例如，CPU 或内存）的系统属性值和自定义属性值。

可用的系统属性取决于批准策略类型和蓝图的配置方式。对于某些属性，蓝图中配置的字段必须先包括最小值和最大值，属性才会显示在系统属性列表中。

当您添加批准级别时，可以添加自定义属性。如果已在蓝图中配置并包括自定义属性，则添加到批准表单的自定义属性将覆盖该自定义属性的任何其他实例，例如，蓝图、属性组或端点中的实例。

审批者可以修改批准表单中的选定属性或配置属性。

前提条件

- 以**租户管理员**或**批准管理员**身份登录到 vRealize Automation。
- [创建批准级别](#)。

步骤

- 1 在**预批准**或**后批准**选项卡中，单击**新建**图标 (+)。
- 2 单击**系统属性**选项卡。
- 3 选中希望审批者在批准过程中配置的每个系统属性对应的复选框。
- 4 配置自定义属性。

添加一个或多个希望审批者在批准过程中配置的自定义属性。

- a 单击**自定义属性**选项卡。
- b 单击**新建**图标 (+)。

- c 输入自定义属性值。

选项	描述
名称	输入属性名称。
标签	输入批准表单中显示给审批者的标签。
描述	输入审批者的扩展信息。 此信息在表单中显示为字段工具提示。

- d 单击**保存**。

- e 要删除多个自定义属性，请选择相应行并单击**删除**。

5 单击**确定**。

后续步骤

- 添加其他预批准级别或后批准级别。
- 保存批准策略。该策略必须处于活动状态，才可应用于**授权**中的服务、项目或操作。

批准策略设置

创建批准策略时，您可以配置各种选项，确定何时必须批准服务目录用户请求的项目。在请求开始置备之前或者项目置备之后、但在向请求用户发布项目之前，可能需要批准。

选择**管理 > 批准策略**。单击**新建**。

■ [批准策略类型设置](#)

批准策略类型将确定如何配置批准策略，以及您可以在授权中应用哪些项目或操作。添加批准级别时，策略类型或项目将影响哪些字段可用来为批准级别创建条件。

■ [添加批准策略设置](#)

您可以配置批准策略的基本信息（包括策略的状态），以便能够管理策略。

■ [将级别信息添加到批准策略设置](#)

批准级别包括服务目录用户在请求项目时将触发批准过程的条件，以及您希望包括的任何系统属性和自定义属性。触发后，批准请求将发送给指定的审批者。

■ [将系统属性添加到批准策略设置](#)

您已选择要添加到批准表单并允许审批者修改值的系统属性。

■ [将自定义属性添加到批准策略设置](#)

您可以配置要添加到批准表单的自定义属性，以允许审批者修改值。

批准策略类型设置

批准策略类型将确定如何配置批准策略，以及您可以在授权中应用哪些项目或操作。添加批准级别时，策略类型或项目将影响哪些字段可用来为批准级别创建条件。

选择**管理 > 批准策略**。单击**新建**。

表 3-75. 批准策略类型选项

选项	描述
选择批准策略类型	<p>根据策略请求类型创建批准策略。</p> <p>选择此选项可定义适用于此类所有目录项的批准策略。请求类型可以是通用请求、目录项请求或资源操作请求。</p> <p>可用条件配置选项因类型不同而异。类型越具体，配置字段就越具体。例如，“服务目录 - 目录项请求”仅提供所有目录项请求共用的字段，但“服务目录 - 目录项请求 - 虚拟机”还提供通用选项和特定于虚拟机的选项。</p> <p>请求类型限制了可以应用批准策略的目录项或操作。</p>
选择项目	<p>根据特定项目创建批准策略。</p> <p>选择此选项可定义适用于在服务目录中不作为单独项目提供、而仅作为计算机或其他部署一部分的特定项目的批准策略。例如，软件组件。</p> <p>可用的条件配置字段特定于项目，且可能会比为策略类型项目提供的标准更详细。</p>
列表	<p>列出可用的策略类型或目录项。</p> <p>搜索或排序各列，以便查找特定的项目或类型。</p>

添加批准策略设置

您可以配置批准策略的基本信息（包括策略的状态），以便能够管理策略。

要定义批准策略的基本信息，请选择**管理 > 批准策略**。单击**新建**。选择策略类型，然后单击**确定**。

表 3-76. 批准策略选项

选项	描述
名称	在授权中应用批准策略时显示的名称。
描述	详细描述如何构建批准策略。此信息将帮助您管理批准策略。
状态	<p>可能的值包括：</p> <ul style="list-style-type: none"> ■ 草稿。批准策略无法应用于授权。使策略处于活动状态之后，无法将其恢复为草稿。 ■ 活动。批准策略可以应用于授权。 ■ 非活动。批准策略无法应用于授权。如果策略尚未应用于授权且您将其设置为非活动状态，则可删除策略，但不能重新激活。如果策略已应用且您将其设置为非活动状态，则应用该策略的项目必须链接到其他策略，否则项目处于未链接状态。未链接的项目和操作仍可授权给用户，但没有应用批准策略。
策略类型	<p>显示批准策略的请求类型。</p> <p>如果已选择批准策略所依据的目录项，则将显示关联的请求类型。</p>
项目	<p>显示选定的目录项。</p> <p>如果已选择批准策略所依据的请求类型，则此字段为空。</p>
上次更新者	更改批准策略的用户的名称。
上次更新日期	上次更改批准策略的日期。

表 3-76. 批准策略选项（续）

选项	描述
预批准级别	如果要求在置备请求的项目或操作运行之前批准，请配置一个或多个在服务目录用户请求项目时触发批准过程的条件。
后批准级别	如果要求在置备项目之后、但在向请求服务目录用户发布已置备或已修改的项目之前批准，请配置一个或多个触发批准过程的条件。 例如，虚拟基础架构管理员需在向服务目录用户发布之前确认虚拟机处于可正常工作状态。
查看链接授权	显示将批准策略应用于服务、目录项或操作的所有授权。您可以将一个授权中的项目链接到其他策略。 此选项仅当查看活动的批准策略时才可用。

将级别信息添加到批准策略设置

批准级别包括服务目录用户在请求项目时将触发批准过程的条件，以及您希望包括的任何系统属性和自定义属性。触发后，批准请求将发送给指定的审批者。

要定义批准策略的基本信息，请选择**管理 > 批准策略**。单击**新建**。选择策略类型，然后单击**确定**。在“预批准”或“后批准”选项卡中，单击**新建**图标 (+)。

您可以根据希望处理级别的顺序区分其优先级。触发批准策略后，如果第一级批准被拒，则请求将被拒绝。

表 3-77. 级别信息选项

选项	描述
名称	输入名称。 查看包含批准策略的请求时，将显示级别名称。
描述	输入级别描述。 例如，CPU>4 to VI Admin。
何时需要批准？	选择何时触发批准策略。
始终需要	针对每个请求触发批准策略。 如果选择此选项并在授权中将该批准策略应用于合格服务、目录项或操作，则该请求在置备之前必须先使用指定的审批者方法批准。例如，所有请求均必须经过请求用户的管理员批准。

表 3-77. 级别信息选项 （续）

选项	描述
基于条件需要	<p>批准策略基于一个或多个条件子句。</p> <p>如果选择此选项，则必须创建条件。当此批准策略应用于授权中的合格服务、目录项或操作时，系统将评估条件。如果条件成立，则请求在置备之前必须先使用指定的审批者方法批准。如果条件不成立，则在不要求批准的情况下置备请求。例如，针对具有 4 个或更多 CPU 的虚拟机的任何请求均必须由虚拟基础架构管理员批准。</p> <p>条件所依据的字段的可用性取决于选定的批准策略类型或目录项。</p> <p>输入条件的值时，这些值区分大小写。</p> <p>要配置多个条件字句，请为子句选择布尔运算。</p> <ul style="list-style-type: none"> ■ 以下所有项。当所有子句成立时触发批准。这是每个子句之间的布尔运算符 AND。 ■ 以下任一项。至少一个子句成立时触发批准级别。这是每个子句之间的布尔运算符 OR。 ■ 非以下项。当所有子句均不成立时触发批准级别。这是每个子句之间的布尔运算符 NOT。
审批者	选择审批者方法。
特定用户和组	<p>将批准请求发送给选定用户。</p> <p>选择在置备服务目录请求或运行操作之前必须批准该请求的用户或用户组。例如，在选中任何人均可批准的情况下，该请求将转给虚拟基础架构管理员组。</p>
根据请求确定用户	<p>根据定义的条件将批准请求发送给用户。</p> <p>例如，如果要在多个业务组中应用此批准策略且希望业务组主管批准请求，请选择业务组 > 使用者 > 用户 > 管理员。</p>
使用事件订阅	<p>根据定义的事件订阅处理批准请求。</p> <p>您必须在管理 > 事件 > 订阅中定义工作流订阅。适用的工作流订阅为预批准和后批准。</p>
任何人均可批准	<p>请求必须至少经过一个审批者批准方可处理。</p> <p>请求服务目录中的项目时，批准请求将发送给所有审批者。如果一个审批者批准请求，则该请求将会获准，然后批准请求将从其他审批者的收件箱中移除。</p> <p>如果第一个审批者拒绝请求，则请求用户将收到拒绝通知，且批准请求将从审批者的收件箱中移除。</p> <p>如果第一个审批者批准、但批准请求在第二个审批者的控制台中打开，则不允许该审批者提交批准请求。第一个审批者的响应视为操作完成。</p> <p>如果选择特定用户和组或根据请求确定审批者且有多审批者，那么这是附加选项之一。如果只有一个审批者，则此选项不适用。</p>
所有人都必须批准	<p>请求必须至少经过所有指定的审批者批准方可处理。</p> <p>如果选择特定用户和组或根据请求确定审批者且有多审批者，那么这是附加选项之一。如果只有一个审批者，则此选项不适用。</p>

将系统属性添加到批准策略设置

您已选择要添加到批准表单并允许审批者修改值的系统属性。

例如，对于虚拟机批准，如果要允许审批者修改 4-6 个 CPU 的请求，请选择 CPU。

要选择系统属性，请选择**管理 > 批准策略**。单击**新建**。选择策略类型，然后单击**确定**。在“预批准”或“后批准”选项卡中，单击**新建**图标 (+)，然后单击**系统属性**选项卡。

表 3-78. 系统属性选项

选项	描述
属性	<p>可用的系统属性列表取决于选定的请求类型或目录项以及项目是否存在系统属性。</p> <p>某些属性仅当以特定方式配置蓝图时才可用。例如，CPU。您必须将应用含 CPU 系统属性的批准策略蓝图配置为范围。例如，CPU 下限为 2，上限为 8。</p>

将自定义属性添加到批准策略设置

您可以配置要添加到批准表单的自定义属性，以允许审批者修改值。

例如，对于虚拟机批准，如果要允许审批者在 vCenter Server 中指定将计算机添加到的文件夹，请添加 **VMware.VirtualCenter.Folder**。

您还可以添加特定于此批准策略表单的自定义属性。

要选择系统属性，请选择**管理 > 批准策略**。单击**新建**。选择策略类型，然后单击**确定**。在“预批准”或“后批准”选项卡中，单击**新建**图标 (+)，然后单击**自定义属性**选项卡。

表 3-79. 自定义属性

选项	描述
名称	输入属性名称。
标签	输入批准表单中显示给审批者的标签。
描述	<p>输入审批者的扩展信息。</p> <p>此信息在表单中显示为字段工具提示。</p>

修改批准策略

您无法修改活动的或非活动的批准策略。必须创建原始策略的副本并替换无法产生所需结果的策略。活动和非活动的批准策略为只读。您可以修改处于草稿状态的批准策略。


复制批准策略时，新策略以原始策略类型为基础。您可以编辑除策略类型外的所有其他属性。如果要修改批准级别以修改、添加或移除级别，或者将系统属性或自定义属性添加到表单中，则可执行此操作。

您可以创建预批准级别和后批准级别。有关创建批准级别的说明，请参见[创建批准级别](#)。

前提条件

以**租户管理员**或**批准管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 批准策略**。
- 2 选择要复制的批准策略所在的行。
- 3 单击**复制**图标 ()。

已创建批准策略的副本。
- 4 选择要编辑的新批准策略。
- 5 在**名称**文本框中输入名称。
- 6 （可选）在**描述**文本框中输入描述。
- 7 从**状态**下拉菜单中选择策略的状态。

选项	描述
草稿	以可编辑的状态保存批准策略。
活动	以只读状态保存可在授权中使用的批准策略。
非活动	以只读状态保存无法在授权中使用的批准策略，直到激活该策略为止。

- 8 编辑预批准级别和后批准级别。
- 9 单击**确定**。

结果

您已根据现有的批准策略创建新批准策略。

后续步骤

在授权中应用新批准策略。请参见[将服务、目录项和操作授权给用户](#)。

取消激活批准策略

确定批准策略过时后，您可以取消激活该策略，使其在置备期间不可用。

要取消激活批准策略，必须为当前应用该批准策略的每个授权分配新策略。

稍后，您可以重新激活已停用的批准策略，或者删除已停用的策略。

前提条件

以**租户管理员**或**批准管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 批准策略**。
- 2 单击批准策略名称。

- 3 单击**查看链接授权**。
 - a 在**全部替换为**下拉菜单中，选择新批准策略。

如果该列表包括多个授权，则新批准策略将应用于列出的所有授权。
 - b 单击**确定**。
- 4 确认没有授权链接到该批准策略之后，从“状态”下拉菜单中选择**非活动**。
- 5 单击**确定**。
- 6 要删除批准策略，请选择包含非活动策略的行。
 - a 单击**删除**。
 - b 单击**确定**。

结果

批准策略与使用和停用该策略的任何授权取消链接。稍后，您可以重新激活批准策略并将其重新应用于授权中的项目。

后续步骤

如果不再需要批准策略，则可将其删除。请参见[删除批准策略](#)。

删除批准策略

如果停用且无需某些批准策略，则可将其从 vRealize Automation 中删除。

前提条件

- 取消链接并取消激活批准策略。请参见[取消激活批准策略](#)。
- 以**租户管理员**或**批准管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**管理 > 批准策略**。
- 2 选择包含非活动策略的行。
- 3 单击**删除**。
- 4 单击**确定**。

结果

批准策略已删除。

场景：创建并应用 CentOS with MySQL 批准策略

作为开发和质量工程业务组的租户管理员，您需要严格管治目录项请求。在用户置备 CentOS with MySQL 目录项之前，您需要 vSphere 虚拟基础架构管理员批准计算机请求，且软件管理员批准软件请求。

可以为 vSphere CentOS with MySQL 服务目录请求创建并应用一个批准策略，以要求 vSphere 虚拟基础架构管理员根据特定条件批准该计算机，并为 MySQL Software 组件创建另一个批准策略，以要求软件管理员对每个请求予以批准。

批准管理员只能创建批准，业务组主管可以将其应用到授权。作为租户管理员，您既能创建批准，又可将其应用于授权。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation 控制台。只有租户管理员可以创建和应用批准策略。
- 确保 CentOS with MySQL 目录项包括在服务中。请参见[场景：使 CentOS with MySQL 应用程序蓝图在服务目录中可用](#)。

场景：创建 CentOS with MySQL 虚拟机批准策略

作为租户管理员，您希望确保开发和质量工程组收到已在环境中正确置备的虚拟机，因此，您需创建批准策略，以要求对某些类型的请求进行预批准。

由于 CentOS with MySQL 虚拟机消耗 vCenter Server 资源，因此您需要 vSphere 虚拟基础架构管理员在请求的内存超出 2048 MB 或 2 个 CPU 时批准请求，以确保资源得到合理使用。此外，您还允许审批者在批准请求之前修改请求的 CPU 和内存值。

步骤

- 1 选择**管理 > 批准策略**。
- 2 创建用于虚拟机置备的批准策略。
 - a 单击**新建**图标 (+)。
 - b 选择**选择批准策略类型**。
 - c 在列表中，选择**服务目录 - 目录项请求 - 虚拟机**。
 - d 单击**确定**。
 - e 配置以下选项：

选项	配置
名称	输入 CentOS on vSphere CPU or Memory VM 。
描述	输入 Requires VI Admin approval for CPU>2 or Memory>2048 。
状态	选择 活动 。

- 3 在**预批准**选项卡上，单击**添加**图标 (+)。

4 使用触发条件和批准操作配置**级别信息**选项卡。

- a 在**名称**文本框中，输入 **CPU>2 or Memory>2048 – VI Admin**。
- b 在**描述**文本框中，输入 **VI Admin approval for CPU and Memory**。
- c 选择**基于条件需要**。
- d 在“子句”下拉列表中，选择**以下任一项**。
- e 在新的“子句”下拉列表中，选择 **CPU** 并使用值 **CPU > 2** 配置子句。
- f 单击**添加表达式**，然后使用值 **Memory (MB) > 2048** 配置子句。
- g 选择**特定用户和组**。
- h 在搜索文本框中，输入 vSphere 虚拟基础架构管理员或管理员组的名称，然后单击搜索图标 (🔍)。
- i 选择该用户或组。
- j 选择**任何人均可批准**。

该请求仅需一名虚拟基础架构管理员验证资源并批准请求。

5 单击**系统属性**选项卡，然后选择允许审批者在批准请求之前修改请求的 CPU 和内存值的属性。

- a 选中 **CPU** 和**内存 (MB)** 复选框。
- b 单击**确定**。

6 单击**确定**。**结果**

您已为虚拟机请求创建批准策略，但仍需为 MySQL 组件创建批准。将策略应用于授权之前，不会触发批准。

场景：创建 MySQL Software 组件批准策略

作为租户管理员，软件管理员要求您为 MySQL 安装创建并应用批准策略，以跟踪许可使用情况。您创建一个策略，在每次请求 MySQL for Linux Virtual Machines Software 组件时通知软件许可证管理员。

在某些环境中，许可证密钥必须由软件管理员提供，因此您可能需要此类批准。在这种情况下，您只需软件管理员跟踪并批准请求。创建批准策略之后，将策略应用于 MySQL for Linux Virtual Machines 目录项。此批准策略非常具体，只能应用于授权中的 MySQL for Linux Virtual Machines Software 组件。

步骤

- 1** 选择**管理 > 批准策略**。
- 2** 为 MySQL Software 组件创建批准策略。
 - a 单击**新建**图标 (➕)。
 - b 选择**选择项目**。
 - c 选择 **MySQL for Linux Virtual Machines**。

- d 单击**确定**。
- e 配置以下选项：

选项	配置
名称	输入 MySQL tracking approval 。
描述	输入 Approval request sent to software manager 。
状态	选择 活动 。

3 在**预批准**选项卡上，单击**添加图标** (+)。

4 使用触发条件和批准操作配置**级别信息**选项卡。

- a 在**名称**文本框中，输入 **MySQL software deployment notice**。
- b 在**描述**文本框中，输入 **Software mgr approval of software installation**。
- c 选择**始终需要**。
- d 选择**特定用户和组**。
- e 在搜索文本框中输入软件管理员的名称，然后单击搜索图标 (🔍) 并选择该用户。
- f 选择**任何人均可批准**。

该请求只需一个软件管理员批准即可。

单击**确定**。

5 单击**确定**。

结果

您已为虚拟机和 MySQL for Linux Virtual Machines Software 组件创建批准策略。将批准策略应用于授权之前，不会触发批准。

场景：将批准策略应用到 CentOS with MySQL 组件

租户管理员可以创建批准策略和授权。修改 Dev 和 QE 授权，以应用所创建的批准策略，这样，在服务目录用户请求项目时即会触发批准。

尽管将整个目录服务授权给业务组可能会更容易，但无法达到与为目录项创建单个授权时相同的控制和管治效果。例如，如果将服务授权给用户，则用户可以请求服务中的任何目录项以及将来要添加到服务中的所有项目。这也意味着您只能使用适用于服务中每个目录项的非常高级的批准策略，例如，始终需要主管批准。如果选择分别授权目录项，则可为每个项目创建并应用非常具体的批准策略，同时严格控制哪些人员可以请求服务中的哪些项目。如果选择分别授权目录项的各个组件，您甚至可以进一步加强控制。

如果您不知道要在授权中将哪些批准策略应用于项目，可在以后返回并应用它们。在此场景中，您将不同的批准策略应用于同一个已发布应用程序蓝图的两个组件。

步骤

1 选择**管理 > 目录管理 > 授权**。

2 单击 **Dev** 和 **QE** 授权。

3 单击**项目和批准**选项卡。

4 添加 CentOS with MySQL 计算机并应用批准策略。

a 单击“授权的项目”标题旁的**添加项目**图标 (+)。

b 选中 **CentOS with MySQL** 复选框。

c 单击**将此策略应用于选定的项目**下拉箭头。

列表中未出现“vSphere 上的 CentOS CPU 和内存”策略。

d 单击**全部显示**，然后单击下拉箭头查看所有批准策略。

e 选择 **vSphere 上的 CentOS CPU 和内存 [服务目录 - 目录项请求 - 虚拟机]**。

vSphere CentOS 计算机是应用程序蓝图中的计算机蓝图。查看策略名称，选择适合目录项类型的策略。如果应用错误的批准策略，则该策略将会失败或基于错误条件触发批准请求。

f 单击**确定**。

5 将 MySQL for Linux Virtual Machine 软件组件添加为项目，然后对该 MySQL 项目应用一个批准策略。

a 单击“授权的目录项和组件”标题旁的**添加目录项和组件**图标 (+)。

b 在**目录项和组件**下拉菜单中，选择**否**。

软件组件始终与计算机相关联。不能在服务目录中单独请求它们。

c 选中 **MySQL for Linux Virtual Machine** 复选框。

d 单击**将此策略应用于选定的项目**下拉箭头。

e 选择 **MySQL 跟踪批准 [服务目录 - 目录项请求 - 软件组件]**。

由于已为添加到虚拟机的这一特定软件组件创建批准策略，因此您无需使用高级选项。

f 单击**确定**。

6 添加用户可对已置备计算机运行的操作。

批准策略不适用于此场景中的操作。

- a 单击“授权的操作”标题旁边的**添加操作**图标 (+)。
- b 选择下列操作。

名称/类型	描述
创建快照/虚拟机	创建虚拟机的快照，包括已安装软件。允许开发人员创建可在开发期间恢复到的快照。
销毁/部署	销毁已置备的整个蓝图，而不仅仅是计算机。使用此操作可避免出现孤立组件。
关闭电源/计算机	关闭虚拟机电源。
打开电源/计算机	打开虚拟机电源。
恢复快照/虚拟机	恢复之前创建的快照。

- c 单击**确定**。

7 单击**完成**。

结果

利用此授权，您可以要求针对不同的蓝图组件应用不同的批准。

后续步骤

请求服务目录中的 CentOS with MySQL 项目作为业务组的成员，以验证授权和批准的行为与预期相同。

通过使用参数化蓝图请求计算机置备

为旨在包括大小或映像组件配置文件的 vSphere 计算机蓝图请求计算机置备时，可以通过选择可用的值集来指定置备设置。

请求置备时，可以从可用的 **Size** 和 **Image** 选项中进行选择。当选择某个值集时，相应的属性值将绑定到该请求。

这些组件配置文件值集将应用到集群中的所有 vSphere 计算机。

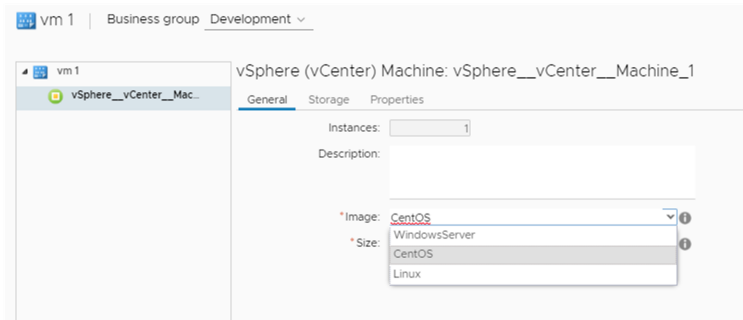
有关组件配置文件配置的信息，请参见[了解和使用蓝图参数化](#)。

前提条件

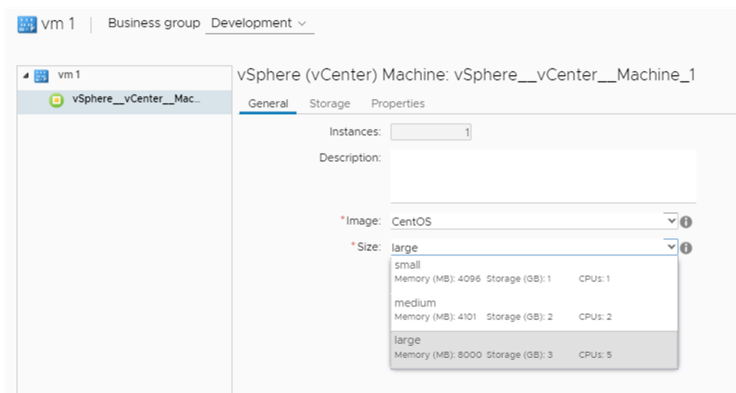
- 定义 **Size** 或 **Image** 组件配置文件的值集。请参见《自定义属性参考》中的和。
- 创建包含 vSphere 计算机组件（其中包含 **Image** 或 **Size** 组件配置文件）的蓝图。请参见[配置计算机蓝图](#)和[vSphere 计算机组件设置](#)。
- 将蓝图发布到目录。请参见[发布蓝图](#)。
- 在目录中配置蓝图。请参见[配置服务目录的对照表](#)和[基于虚拟机策略类型的批准策略示例](#)。

步骤

- 1 单击**目录**。
- 2 选择要请求的目录服务并单击**请求**。
- 3 选择要置备的 vSphere 计算机组件并指定要置备的实例数。
- 4 从**映像**下拉菜单中选择映像值集选项。



- 5 从**大小**下拉菜单中选择大小值集选项。



- 6 单击**提交**。

后续步骤

现在，在目录置备请求表单的**目录**选项卡上的**映像**和**大小**下拉菜单中，将显示您为 **Size** 和 **Image** 组件配置文件定义的值集。

场景：使 CentOS with MySQL 应用程序蓝图在服务目录中可用

作为租户管理员，您已请求蓝图架构师为 MySQL on CentOS 创建一个目录项，开发和工程组可在该目录项上运行测试案例。软件架构师已通知您该目录项随时可供用户使用。为使业务用户能够使用该目录项，您需要将蓝图和 **Software** 组件与目录服务关联，然后授权业务组成员请求目录项。

前提条件

- 以**租户管理员**或**目录管理员**身份登录到 vRealize Automation。
- 在 vSphere CentOS 虚拟机上发布适用于 MySQL 的蓝图。请参见[构建设计库](#)中创建计算机和软件组件蓝图的过程。

- 如果在开发环境中创建蓝图，请将蓝图导入生产环境中。请参见[导出和导入蓝图和内容](#)。
- 创建预留以便将 vSphere 资源分配给 Dev 和 QE 业务组。请参见[为 Hyper-V、KVM、SCVMM、vSphere 或 XenServer 创建预留](#)。

步骤

1 场景：创建开发和质量工程目录服务

作为租户管理员，您需要为开发和质量工程组创建单独的目录服务，使财务和人力资源等其他组无法查看专用的目录项。创建名为“Dev 和 QE 服务”的目录服务，以发布开发和工程组运行测试案例所需的全部目录项。

2 场景：将 CentOS with MySQL 添加到 Dev 和 QE 服务

作为一名租户管理员，您需要将 CentOS with MySQL 目录项添加到 Dev 和 QE 服务。

3 场景：授权用户将 Dev 和 QE 服务项作为目录项请求

作为租户管理员，您创建 Dev 和 QE 授权并添加目录项和某些相关操作，使开发和质量工程用户能够请求 CentOS with MySQL 目录项，并针对计算机和部署运行操作。

场景：创建开发和质量工程目录服务

作为租户管理员，您需要为开发和质量工程组创建单独的目录服务，使财务和人力资源等其他组无法查看专用的目录项。创建名为“Dev 和 QE 服务”的目录服务，以发布开发和工程组运行测试案例所需的全部目录项。

步骤

- 1 选择**管理 > 目录管理 > 服务**。
- 2 单击**新建**图标 (+)。
- 3 在**名称**文本框中，输入名称 **Dev and QE Service**。
- 4 在**描述**文本框中，输入描述 **Dev and QE application catalog items for test cases**。
- 5 从**状态**下拉菜单中选择**活动**。
- 6 作为负责创建服务的目录管理员，使用搜索选项将您的姓名添加为“所有者”。
- 7 添加“支持团队”自定义用户组。

例如，添加包括 IaaS 架构师和软件架构师的自定义用户组，这样一旦在置备目录项时遇到问题，您和服务目录用户便能够与相应的人员联系。

- 8 单击**确定**。

结果

您已创建并激活 Dev 和 QE 目录服务，但其中尚未包含任何目录项。

场景：将 CentOS with MySQL 添加到 Dev 和 QE 服务

作为一名租户管理员，您需要将 CentOS with MySQL 目录项添加到 Dev 和 QE 服务。

步骤

- 1 选择**管理 > 目录管理 > 服务**。
- 2 在**服务**列表中选择“Dev 和 QE 服务”所在的行，然后单击**管理目录项**。
- 3 单击**新建**图标 (+)。
- 4 选择 **CentOS with MySQL**。

只有尚未与服务关联的已发布蓝图和组件才会显示在该列表中。如果未看到蓝图，请验证蓝图是已发布还是未包括在其他服务中。

- 5 单击**确定**。
- 6 单击**关闭**。

结果

您已将 CentOS with MySQL 目录项发布到 Dev 和 QE 服务，但在将项目或服务授权给用户之前，任何人都无法查看或请求项目。

场景：授权用户将 Dev 和 QE 服务项作为目录项请求

作为租户管理员，您创建 Dev 和 QE 授权并添加目录项和某些相关操作，使开发和质量工程用户能够请求 CentOS with MySQL 目录项，并针对计算机和部署运行操作。

在此场景中，您授权服务，因为您希望用户有权访问此服务中添加的任何其他目录项。您还希望允许用户管理置备的部署，因此将打开电源和关闭电源、快照以及销毁部署等操作添加到授权。

步骤

- 1 选择**管理 > 目录管理 > 授权**。
- 2 单击**新建**图标 (+)。
- 3 配置详细信息。
 - a 在**名称**文本框中，输入名称 **Dev and QE Entitlement**。
 - b 在**状态**下拉菜单中选择**活动**。
 - c 在**业务组**下拉菜单中选择 **Dev 和 QE** 组。
 - d 在“用户和组”区域中，添加一个或多个用户。

除非您确定蓝图按照预期运行，否则仅添加您本人。如果确实正常运行，则可添加各个用户和自定义用户组。

- e 单击**下一步**。

4 添加服务。

尽管您是单独添加 CentOS 和 MySQL 目录项，但添加服务可确保以后添加到服务中的任何附加项均可供服务目录中的业务组成员使用。

- a 单击“授权的服务”标题旁边的**添加服务**图标 (+)。
- b 选择 **Dev** 和 **QE** 服务。
- c 单击**确定**。

Dev 和 QE 服务将添加到“授权的服务”列表中。

5 添加操作。

- a 单击“授权的操作”标题旁边的**添加操作**图标 (+)。
- b 单击“类型”列标题对列表进行排序。

根据类型选择以下操作。这些操作对使用测试案例计算机的开发和质量工程用户非常有用，同时也是您希望这些业务组成员使用的唯一操作。

类型	操作名称
计算机	打开电源
计算机	关闭电源
虚拟机	创建快照
虚拟机	恢复快照
部署	销毁
部署销毁操作将销毁整个部署，而不仅仅是销毁虚拟机。	

- c 单击**确定**。

这五个操作将添加到“授权的操作”列表中。

6 单击**完成**。

结果

您已将 CentOS with MySQL 目录项添加到新 Dev 和 QE 目录服务，且授权业务组成员请求和管理项目。

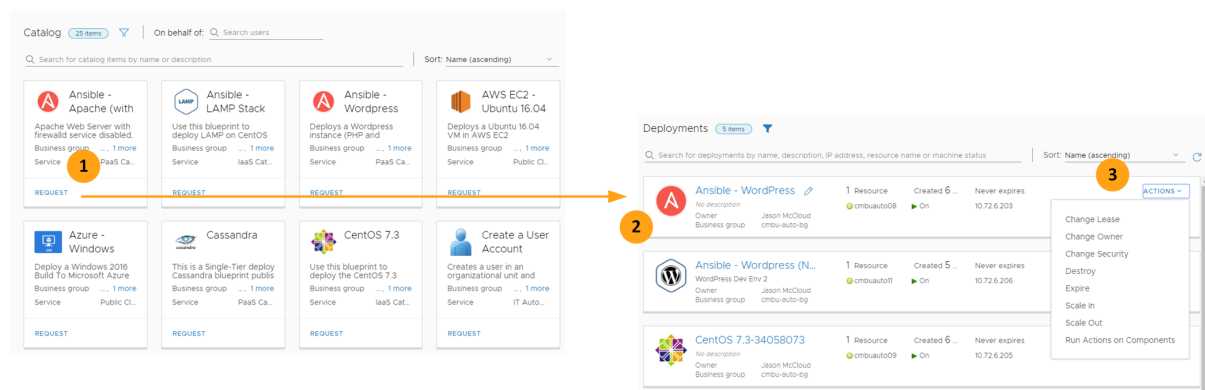
后续步骤

通过置备 CentOS with MySQL 目录项验证所做的工作之后，您可以将其他用户添加到授权，以便向开发和质量工程用户公开目录项。如果要进一步控制环境中的资源置备，则可为 MySQL Software 组件和 CentOS for Software Testing 计算机创建批准策略。请参见[场景：创建并应用 CentOS with MySQL 批准策略](#)。

使用目录和管理部署

4

目录是您可以使用的蓝图，而部署是您置备的蓝图。您的管理员提供目录项。之后，您可以作为部署请求和管理资源。管理部署过程中，可以通过运行操作执行更改。



以下工作流从目录开始。

- 1 请求目录项。目录包含已授予您所属业务组的已发布蓝图。
- 2 已置备的资源作为部署进行管理。可以监控置备过程，管理部署以及在部署上运行操作。
- 3 使用操作在部署后对部署进行更改。操作可能包括增加内存，减少 CPU 或销毁不再需要的部署。

本章讨论了以下主题：

- 使用目录
- 使用部署
- 使用收件箱

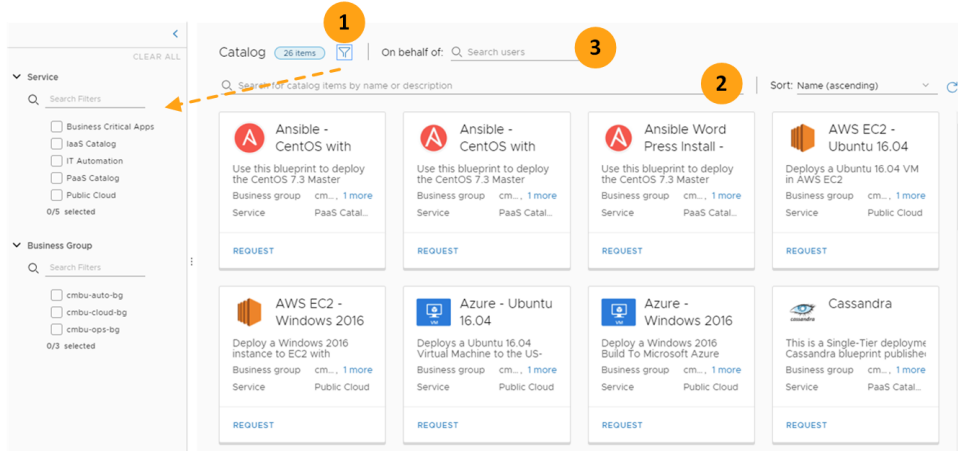
使用目录

目录是可以部署的蓝图的列表。蓝图架构师确定组件的设计、请求项时可以选择的自定义选项，以及基于组织 vRealize Automation 端点的部署位置。

可用的目录项基于您在一个或多个业务组的成员资格，以及您的业务组是否有权置备蓝图。

查找目录项

此示例显示了一个小目录。在大型企业环境中，目录可能需要多页才能完全显示。

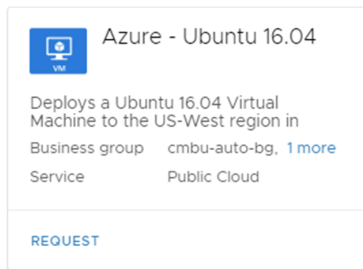


使用以下选项查找您要部署的蓝图。

- 1 基于服务和业务组**筛选**列表。
- 2 **搜索和排序**以查找和组织目录项。
- 3 选择**代表**用户限制目录项的数量，然后为该用户请求项目。您只能部署该用户所在业务组可使用的蓝图。选择用户名时，可用的目录项列表反映了该成员资格。代表权限可用于管理员、业务组主管，且可以在配置业务组时分配给一个或多个业务组成员。请参见[创建业务组](#)。

目录卡

目录卡表示可部署单个计算机或整个应用程序的蓝图。也可以表示通过其他方式置备的 XaaS 工作流。例如，将用户添加到 Active Directory。



卡上的信息包括授权请求目录项的业务组，以及与项目关联的服务。

如何提交目录请求

提交目录请求时，每个蓝图的请求表单可能会有所不同。表单中的差异由蓝图设计器来配置。

表单内容取决于您可以在多大程度上自定义请求。您可以选择多个选项来自定义您的请求，也可能没有任何选项。

例如，蓝图架构师可能设计了一个蓝图，以便您能够选择特定数量的 CPU 或选择大、中、小作为预先确定的 CPU 数量。或者蓝图可能存在限制，在提交前不允许对蓝图做任何更改。

请求置备成功后，您可以管理部署的工作负载或服务。

前提条件

- 您必须是有权使用一个或多个目录项的业务组的成员。请参见[创建授权](#)。
- 如果您代表其他用户进行部署，则必须分配有该业务组的支持角色。请参见[创建业务组](#)。

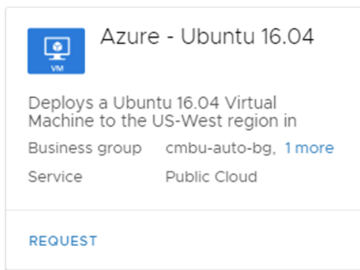
步骤

- 1 单击**目录**。
- 2 如果您分配有一个或多个业务组中的支持角色并代表其他组成员进行部署，请在**代表**搜索区域中输入用户或自定义组名称。

目录项列表仅限于选定用户或组所在业务组可使用的项。

如果未选择用户，将为您提交请求。

- 3 使用搜索和排序选项查找要部署的项目，然后单击**请求**。



- 4 如果您是可使用蓝图的多个业务组的成员，请选择业务组以便与部署关联。

5 在请求表单上，配置任何必要的和可用的选项。

根据蓝图的配置方式，表单可能会有所不同。以下是从简单到复杂的多个选项卡示例。

The image displays three overlapping screenshots of vRealize Automation request forms:

- Top-left form (vSphere (vCenter) Machine: centos73):** Shows the 'General' tab with fields for Instances (1), CPUs (1), Memory (MB) (2048), Storage (GB) (50), and a Description field.
- Top-right form (GCP Connection):** Shows fields for GCP Connection (Select), Cloud Storage Bucket, Storage class (MULTI_REGIONAL), Default ACL for Bucket (private), and Default ACL for Objects in Bucket (private).
- Bottom form (XaaS: Azure_Machine_1):** Shows the 'Build Information' tab with sections for Deployment settings (Location: West US, Naming Prefix: Use Business Group Default), Image (Virtual Machine Image Type: Custom, Virtual Machine Image: Canonical:UbuntuServer:16.04-LTS:latest, Virtual Machine Image OS Type: Linux), and Authentication (Admin User: admin, Authentication Type: Password, Password: *****, Confirm Password: *****)

6 单击提交。

结果

提交该请求以进行置备，将打开“部署”选项卡，以便跟踪请求的进度。

后续步骤

验证您的请求已部署。请参见[监控置备请求](#)。

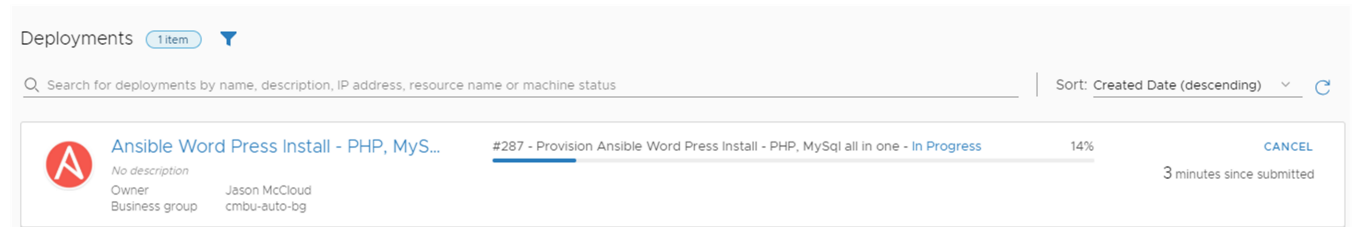
使用部署

部署是从目录请求的已置备蓝图。您可以在整个置备过程中监控已提交请求的状态，跟踪已部署的资源以及使用操作管理这些已部署资源。

监控请求状态

正在进行的请求会显示在“部署”选项卡上。可以使用部署卡跟踪要完成的置备过程。

如果置备过程失败，则可以查看错误消息和事件，确定请求失败的位置，并解决问题。请参见[测试并对失败的置备请求进行故障排除](#)。



管理已部署的资源

在“部署”选项卡上管理请求。

管理包括验证部署是否已启用。可能还需要通过缩小或扩展部署来进行更改以满足您的需求。或者，您可能需要查看部署详细信息。有关详细信息，请参见[管理部署的目录项](#)。

监控置备请求

可以使用部署监控所发出的目录请求的进度。如果成功置备资源，您还可以管理已部署的资源。

如果看不到正在进行的请求，说明该请求未提交或已完成。

监控请求

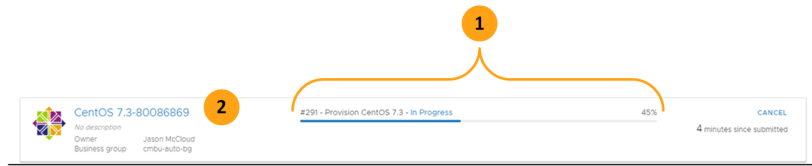
要监控目录请求，请选择**部署**。

在部署列表中跟踪请求的状态。

- 1 在部署卡 (1) 上跟踪请求的状态。
如果是首次请求目录项，则状态栏上的进度不显示百分比。首次部署后，后续请求提供计算出的已完成百分比。

如果在已部署的资源上运行操作，则状态栏将指示所选更改的状态。

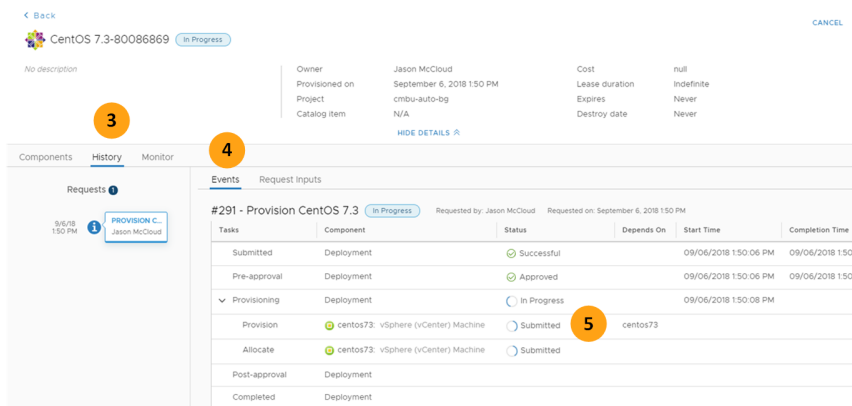
- 2 要查看正在进行部署的详细信息，请单击部署状态栏 (1) 或部署名称 (2)。



在部署过程中查看置备详细信息。

- 1 “历史记录”选项卡 (3) 提供部署事件和输入的值。
- 2 “事件”选项卡 (4) 提供置备请求的详细信息。
- 3 可以查看置备 workflow (5)，确定当前正在部署哪些组件。

如果请求未完成置备过程，请参见[测试并对失败的置备请求进行故障排除](#)。



取消正在进行的请求

如果您已提交请求，但又决定取消，则置备过程停止，并回滚和清理任何已部署的资源。

如果取消过程所用时间太长，可以请求您的管理员强制取消。作为管理员，您可以取消处于正在取消状态的请求。如果强制取消，回滚操作可能无法完成，且您必须手动清理目标系统上的资源。

对失败的目录请求进行故障排除

请求目录项时，可能会由于多种原因失败。可能的原因有，网络流量问题、端点资源不足或蓝图规范存在缺陷。或者，置备请求成功，但部署无法正常工作。可以使用 **vRealize Automation** 检查部署，查看任何错误消息，并确定问题是否位于您可以解决的环境中。

如果您在 **vRealize Automation** 中的角色是目录使用者且没有管理员特权，则可以使用此 workflow 执行初始故障排除。您可能需要您组织中的某位人员执行更深入的研究。

可能的故障状态

如果置备请求失败，则会看到以下状态之一。

- **失败。** 请求可能会由于多种原因失败。一种原因是，目标端点上缺少资源、用于支持蓝图的资源不足或必须修复设计糟糕的蓝图，这些导致置备过程不工作。另一种原因是，请求需要您组织中的人员进行批准，而审批者拒绝了该请求。还有可能是在部署上运行的操作失败。上面提到的环境或批准原因都可能会导致失败。

使用以下故障排除工作流程调查问题的原因。如果您能够解决问题，请查看有关**取消**和**重新提交**的操作选项。请参见**已置备资源的操作菜单命令**。

- **部分成功。**请求可能部分成功，这意味着某些组件已部署，但并非所有置备步骤都已成功完成。

使用以下故障排除工作流程确定哪些组件仅部分成功并调查问题的原因。如果您能够解决问题，请查看有关**取消**以及您能否使用**恢复**的操作选项。请参见**已置备资源的操作菜单命令**和“**恢复**”操作的**工作原理**。

适用于目录使用者的故障排除工作流程

可以使用此工作流程开始调查失败的部署。如果调查表明故障是暂时性环境问题所致，您可以解决错误，并重新提交请求。如果问题与请求规范有关，则可能需要联系您的蓝图架构师。

表 4-1. 如何开始对错误进行故障排除

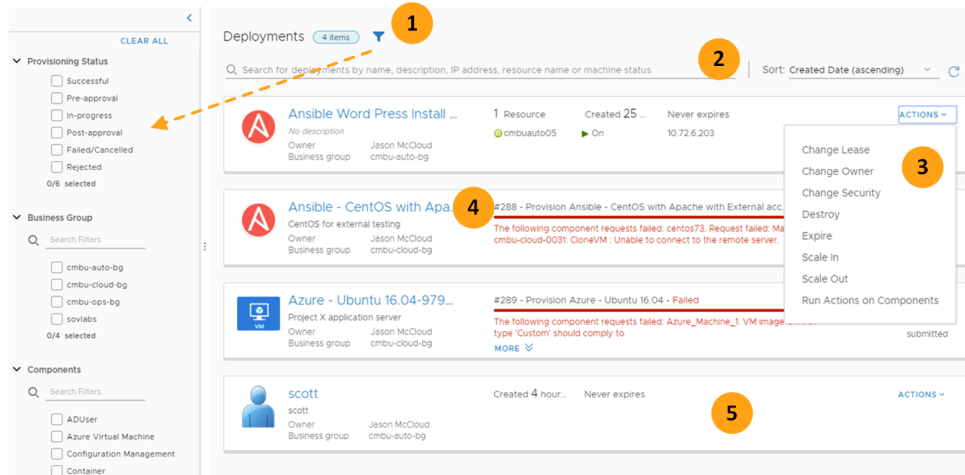
工作流	故障排除步骤	示例
1	在 部署 选项卡上，状态栏上指示失败的部署。部署卡包括最近一次失败的消息。有关详细信息，请单击部署名称或进度条。	
2	在部署详细信息 历史记录 选项卡上，可以使用事件工作流查看置备过程失败的位置。在部署上运行操作但更改失败时，此工作流也非常有用。	
3	失败状态指示工作流失败的位置。	
4	信息提供更详细的错误消息。 如果标志帮助中的此信息不足以确定并解决问题，可以查看事件日志，做进一步研究。 要查看事件日志，必须具有必要的用户角色。您的蓝图架构师或管理员可以执行更多的故障排除工作。请参见 测试并对失败的置备请求进行故障排除 。	

管理部署的目录项

作为部署所有者或协助其他用户的管理员，您可以使用部署详细信息管理已部署项目的生命周期。部署详细信息提供有关每个组件的最新信息，并使用历史记录跟踪随时间发生的更改。使用部署时，可以使用操作修改已部署的项目。此外，还可以不使用操作进行某些更改。

从卡管理部署

部署卡列表提供了部署概览。已成功？正在运行？



使用以下方法可从 vRealize Automation 查找并管理已部署的资源。

- 1 基于请求的当前状态、部署所针对的业务组、包括的子组件、所有者用户以及置备或过期日期范围**筛选**列表。“置备状态”和“请求编号”筛选器仅适用于初始置备过程，不适用于可能运行的任何后续操作。其他筛选器通常适用于部署。
- 2 执行**搜索**和**排序**以查找并组织部署。
- 3 要管理部署，请单击**操作**以运行授权的部署级别操作。您必须打开部署详细信息，才能在各个组件上运行操作。这些操作可能是授予设计蓝图的标准操作，也可能是创建并授予 XaaS 蓝图的自定义 XaaS 资源操作。有关详细信息，请参见 [对已部署资源运行操作](#)。
- 4 要查看和管理部署详细信息（包括置备事件、历史记录和组件级别的操作），请单击部署名称。前三项是标准蓝图的初始置备请求。
- 5 您还可以管理运行工作流的 XaaS 部署请求。工作流可使资源或工作流在外部系统上运行。在此示例中，XaaS 将用户添加到了 Active Directory 域中。

使用部署详细信息管理部署

可以使用部署详细信息完善以下管理信息。

- **详细信息。**卡上提供的基本信息。您还可以更改部署名称和描述，以及运行部署级别的操作。
- **“组件”选项卡。**每个组件的完整配置。您还可以运行组件级别的操作。
- **“历史记录”选项卡。**对部署所做更改的完整历史记录。您还可以找到有关放置的详细信息以及为每个更改提供的输入值。

- **“监控”选项卡。**如果与 vRealize Operations Manager 集成，会针对部署和组件显示监控衡量指标数据和警示。
- **操作。**您还可以使用详细信息来运行部署级别的操作或组件级别的操作。

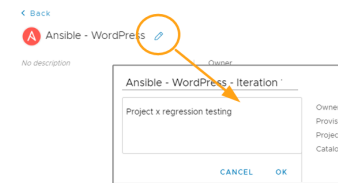
使用部署详细信息

部署详细信息提供的信息比卡上的基本信息更多。您还可以更改部署名称和描述，以及运行部署级别和组件级别的操作。

查看有关部署的基本信息，其中包括部署所基于的蓝图和成本。

更改部署名称

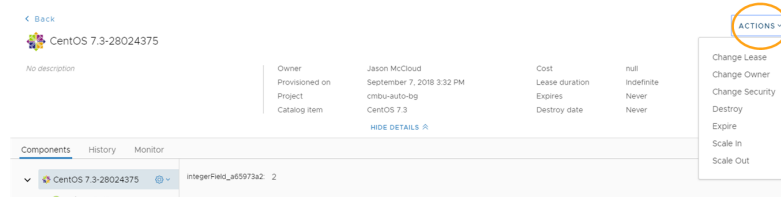
部署从蓝图获得其名称。当您使用自己的部署时，此名称对您而言并不总是有意义。您可以根据自己的需求更新名称和描述。



- 1 指向名称，然后单击铅笔图标。
- 2 更新为对您有意义的名称和描述。

运行部署级别的操作

部署级别的操作仅限于影响整个部署的更改。可用操作列表取决于您的业务组有权使用操作的方式。

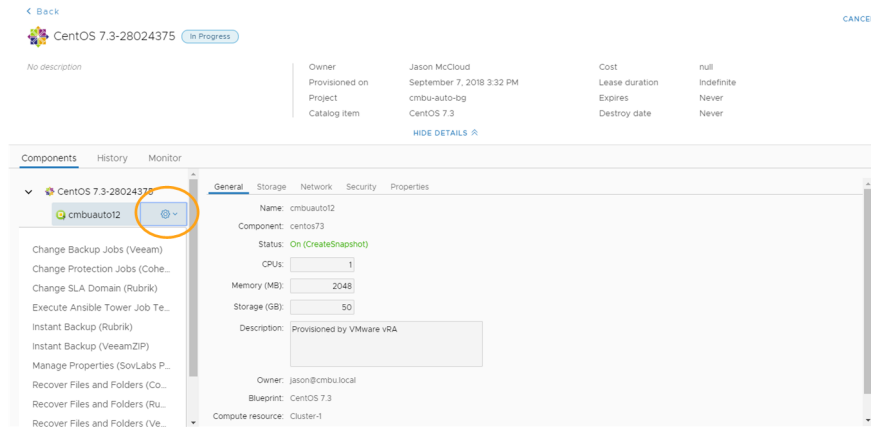


部署组件

部署详细信息中的“组件”选项卡提供了所有部署组件的完整配置。您可以查看计算机和网络的配置方式。此外，还可以运行组件级别的操作以更改配置。

必须了解提供给您的部署或对实例问题进行故障排除时，请查看组件详细信息。

通过操作进行的任何更改都会反映在详细信息中。



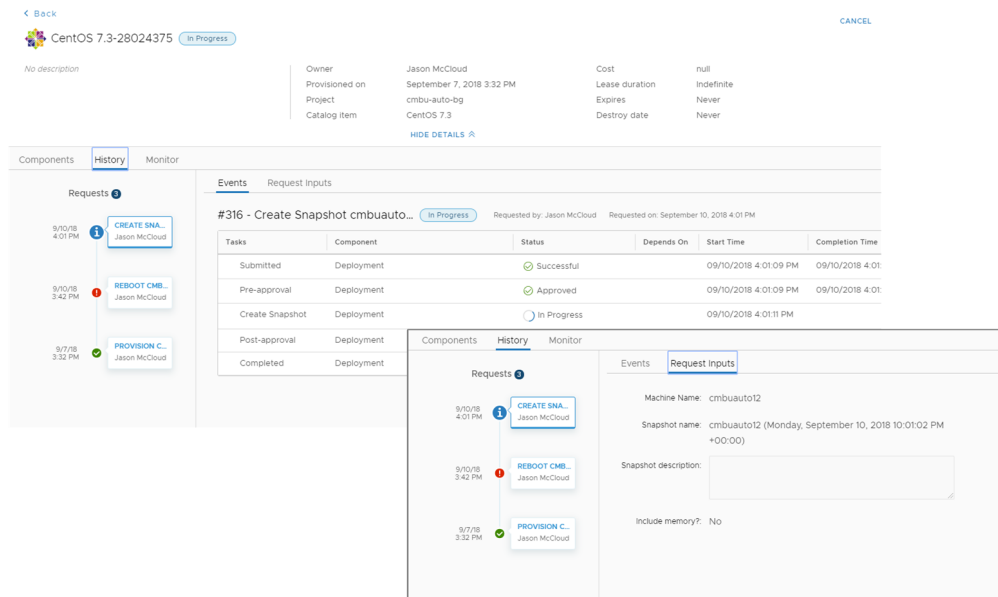
运行组件级别的操作

组件级别的操作特定于组件。可用操作取决于您的业务组有权使用操作的方式。如果您的管理员没有授权您运行操作，您将看不到齿轮图标或操作列表。

部署历史记录

部署详细信息中的“历史记录”选项卡提供从初始置备到使用一个或多个操作执行的任何更改的完整部署历史记录。您可以使用完整的置备历史记录了解发生更改的时间以及提供了哪些值。

如果必须确定发生更改的时间或调查实例问题时，请查看历史记录详细信息。此外，还可以使用历史记录对失败的部署进行故障排除。请参见[测试并对失败的置备请求进行故障排除](#)。



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。

- 部署级警示
- 计算机级衡量指标

直接在 vRealize Automation 中查看筛选后的警示和衡量指标集可节省您访问或搜索 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将 vRealize Operations Manager 用于其他数据。

启用 vRealize Operations Manager 数据

为了让 vRealize Automation 显示 vRealize Operations Manager 数据，应首先配置设置和适配器。

安装程序要求执行 vRealize Operations Manager 和 vRealize Automation 中的步骤。

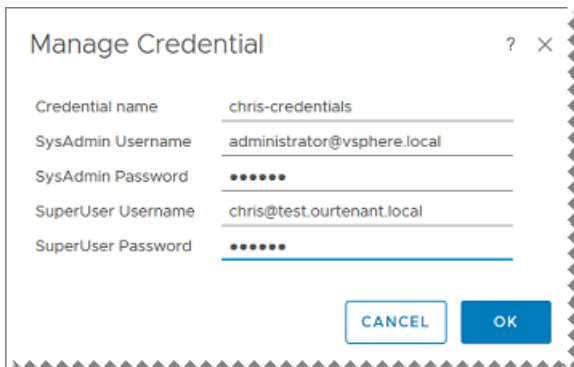
前提条件

确认您安装的是 vRealize Operations Manager 6 或更高版本。

步骤

- 1 在 vRealize Operations Manager 中，转到**管理 > 解决方案**。
- 2 在**解决方案**下，确认存在 **vRealize Automation 解决方案**并且它正在接收数据。
 - a 选择 vRealize Automation 解决方案。
 - b 在解决方案上方的工具栏中，单击齿轮“配置”图标。
 - c 在**实例设置**下，转到**凭据**，然后单击绿色的加号添加凭据。

凭据名称	这组凭据的描述
SysAdmin	vRealize Automation 默认租户管理员的用户名和密码，通常是 administrator@vsphere.local
SuperUser	vRealize Automation 工作租户的高访问权限帐户的用户名和密码



- d 保存并测试凭据以正确连接。

- 3 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 端点有 vCenter 适配器。

图 4-1. vRealize Operations Manager 解决方案和适配器

Solutions					
Name	Description	Version	Provided by	Licensing	Adapter Status
VMware vRealize Business for Management Pack for VMwar...		6.0.7963016	VMware Inc.	Not applicable	None Configured
VMware vRealize Automation		4.0.9272301	VMware Inc.	Not applicable	Data receiving (1)

Configured Adapter Instances					
Adapter Type	Adapter Instance Name	Credential name	Collector	Collection State	Collection Status
vCenter Adapter	vCenter_BLR_Lab	cred_BLR_Lab	vRealize Operations Manager ...	Collecting	Data receiving

- 4 在 vRealize Operations Manager 中，转到警告 > 警告设置。
- 5 确认警告和症状定义会生成所需 vRealize Automation 警告。

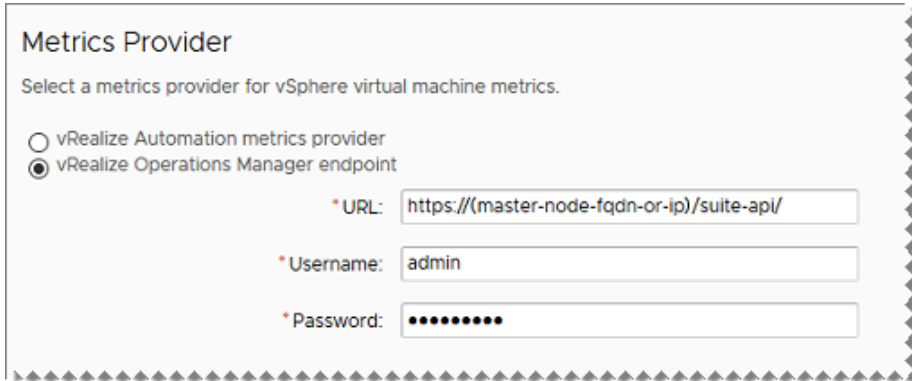
大多数 vRealize Automation 用户只需确保部署正常运行即可。虚拟机级别的其他警告可能会无休无止，且包含无法使用 vRealize Automation 管理的详细信息。

对于 vRealize Automation 警告，整体部署是父对象。部署中的虚拟机是子对象。默认情况下，警告在部署这个父级别。

您可以自由地使用 vRealize Operations Manager 创建部署级别的警告公开其他的特定症状。例如，您可能希望显示部署中的所有 SQL Server 问题。

- 6 在 vRealize Automation 中，转到管理 > 回收 > 衡量指标提供程序。
- 7 选择 vRealize Operations Manager 端点。

- 8 输入 vRealize Operations Manager URL `https://master-node-FQDN-or-IP/suite-api/` 和具有 vRealize Operations Manager 管理员权限的帐户的用户名和密码。



Metrics Provider

Select a metrics provider for vSphere virtual machine metrics.

☐ vRealize Automation metrics provider

☒ vRealize Operations Manager endpoint

*URL:

*Username:

*Password:

注 存在多个身份验证源时，请输入 `user@domain@source` 格式的用户名，其中 `@source` 是 vRealize Operations Manager 中的 LDAP 导入源。用户帐户需要至少具有只读角色，以及 vCenter 适配器和云 vCenter Server 的对象权限。

- 9 测试连接并保存。
- 10 单击**部署**，选择一个部署，然后确认显示“监控”选项卡。

仅当选择 vRealize Operations Manager 作为衡量指标提供程序时，才会显示“监控”选项卡。

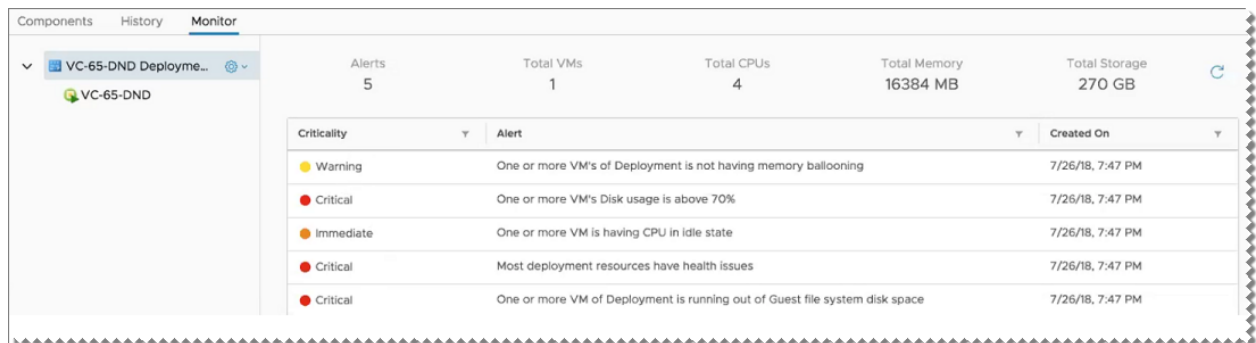
vRealize Operations Manager 提供的警示

启用监控后，vRealize Automation 将检索有关您的部署的 vRealize Operations Manager 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，请在左侧的组件树顶部突出显示部署名称。

- 您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。
- 仅显示运行状况警示。不支持效率或风险等其他警示类型。



Components		History	Monitor
<div>VC-65-DND Deployment</div> <div>VC-65-DND</div>		Alerts 5	Total VMs 1 Total CPUs 4 Total Memory 16384 MB Total Storage 270 GB
Criticality	Alert	Created On	
Warning	One or more VM's of Deployment is not having memory ballooning	7/26/18, 7:47 PM	
Critical	One or more VM's Disk usage is above 70%	7/26/18, 7:47 PM	
Immediate	One or more VM is having CPU in idle state	7/26/18, 7:47 PM	
Critical	Most deployment resources have health issues	7/26/18, 7:47 PM	
Critical	One or more VM of Deployment is running out of Guest file system disk space	7/26/18, 7:47 PM	

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](#)。

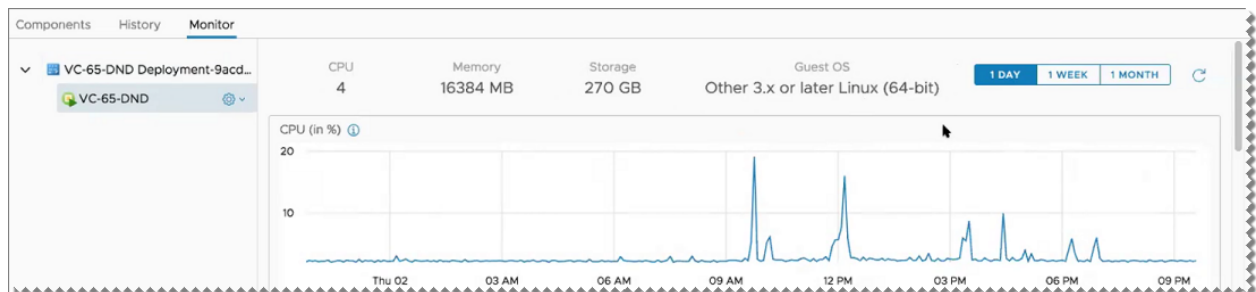
要查看衡量指标，请展开左侧的组件树，并突出显示某个虚拟机。

- 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。



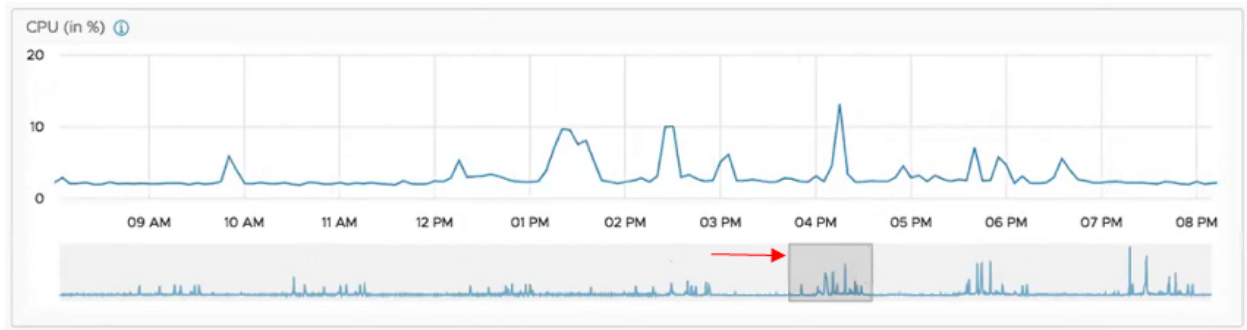
处理 vRealize Operations Manager 提供的数据

当 vRealize Operations Manager 提供的衡量指标出现问题时，您可以直接在 vRealize Automation 中执行某些纠正措施。

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](#)。

查找问题

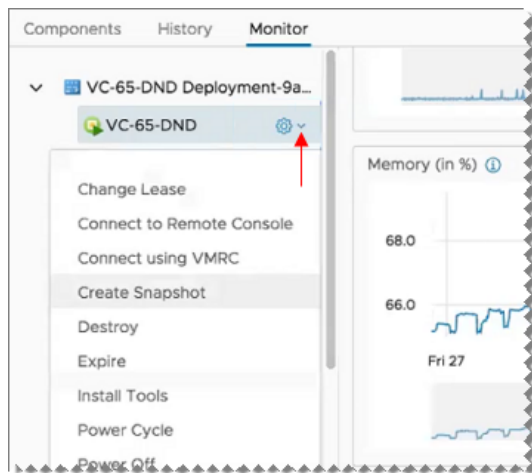
过去一天、一周或一月的衡量指标可供使用。要放大关注的区域，请选择任何衡量指标时间轴下方阴影部分的小区域：



进行更改

发生问题时，您可以直接在同一界面中采取某些纠正措施。

例如，如果显示的内存一直处于使用峰值状态，您可以决定添加内存。在左侧的组件树中，单击虚拟机下拉菜单，然后使用上下文菜单选项执行维护或重新配置。



对已部署资源运行操作

已部署资源可用的操作取决于资源的类型、为已置备项目配置和提供操作的方式以及项目的运行状态。

可用于部署或部署组件的已配置操作显示在选定部署或组件的**操作**菜单中。

可用操作列表由为部署授权运行的业务组以及资源或计算机类型组件确定。操作的可用性取决于计算机类型或状态。

如果项目是使用 XaaS 蓝图置备的，则必须在置备项目使用的同一服务中创建、发布和授权资源操作。可用操作的列表取决于项目的类型和当前状况。

对于置备为 IaaS 计算机的项目，可用的操作可能还包含 XaaS 资源操作，前提是这些操作已映射到该项目。

已置备资源的操作菜单命令

操作是指您可以对已置备资源进行的更改，vRealize Automation 操作用于管理资源的生命周期。

操作菜单上的可用命令取决于业务组主管或租户管理员如何配置包含运行操作的资源的授权。菜单选项的可用性还取决于资源类型和项目的运行状态。

一次只能运行一个操作。要在资源上运行第二个操作，请等待第一个操作完成请求的更改。

表 4-2. 操作菜单命令

操作	资源类型	描述
关联浮动 IP	计算机 (OpenStack)	将浮动 IP 地址与 OpenStack 计算机关联。
取消	计算机	取消正在运行的重新配置操作。 用户只能取消可回滚到以前状态的操作。 如果某个操作不支持回滚到以前的状态（例如，关闭电源），则只有具有租户管理员特权的用户才能取消该请求。
更改租约	部署和计算机	为特定计算机或某部署中包含的所有资源更改租约中的剩余天数。如果未提供值，则租约不会过期。
更改 NAT 规则	NAT 网络	添加新的 NAT 端口转发规则、重新排序规则、编辑现有规则或删除规则。
更改所有者	部署	更改部署以及包含的所有资源的所有者。只有业务组主管和支持用户可以更改部署的所有权。 启动更改所有者操作时，计算机必须处于“开启”、“关闭”或“活动”状态，否则该操作将失败并显示以下消息： 计算机的操作无效 (The action is invalid for the machine)。
更改安全性	部署	可以添加或移除现有 NSX 安全组和安全标记。还可以移除按需安全组。 有关详细信息，请参见 在部署中添加或移除安全项目 。
使用 VMRC 连接	计算机	使用 VMRC 8.x 应用程序连接到虚拟机。 要使用此操作，必须在运行该操作的服务目录用户的本地系统上安装 VMRC 应用程序。 有关安装和用户使用说明，请参见 VMware Remote Console 文档 。要下载，请参见 下载 VMware Remote Console 。 VMRC 8.x 将替换之前的 VMware Remote Console。
连接到远程控制台	计算机	使用 VMware Remote Console 连接到选定计算机。 虚拟机控制台将显示在浏览器中。VMRC 8.x 将替换 VMware Remote Console。
使用控制台票证连接	计算机 (OpenStack 和 KVM)	使用 VMware Remote Console 连接的控制台票证连接到 OpenStack 或 KVM 虚拟机。

表 4-2. 操作菜单命令（续）

操作	资源类型	描述
使用 ICA 连接	计算机 (Citrix)	使用独立计算架构连接到 Citrix 计算机。
使用 RDP 连接	计算机	使用 Microsoft Remote Desktop Protocol 连接到计算机。
使用 SSH 连接	计算机	<p>使用 SSH 连接到选定计算机。</p> <p>使用 SSH 连接选项需要在浏览器中安装支持 SSH 的插件，例如用于 Mozilla Firefox 和 Google Chrome 的 FireSSH SSH 终端客户端。存在插件时，选择使用 SSH 连接会显示 SSH 控制台并提示提供管理员凭据。</p> <p>要使用此操作，必须以属性组或单个自定义属性的形式在蓝图的计算机组件中包含 Machine.SSH 自定义属性并设置为 true。</p>
使用虚拟桌面连接	计算机	使用 Microsoft 虚拟桌面连接到选定计算机。
创建快照	虚拟机	创建虚拟机的快照。如果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。
删除快照	虚拟机	删除虚拟机的快照。

表 4-2. 操作菜单命令（续）

操作	资源类型	描述
销毁	部署、计算机和按需安全组	<p>立即销毁已置备的资源。</p> <p>除 XaaS 以外，销毁部署的组件并非最佳做法。使用缩小操作可减少部署中的计算机数量或者销毁整个部署。</p> <p>必须运行此操作才能销毁 XaaS 资源，即使这些资源是正销毁的部署的一部分时也是如此。当租约或存档时间段结束时，其他资源会被销毁。</p> <p>“销毁”操作不适用于以下部署情况：</p> <ul style="list-style-type: none"> ■ 物理机部署 ■ 使用 NSX 现有网络或 NSX 现有安全资源的部署 ■ 使用 NSX 按需负载均衡器资源的部署 <p>由于 NSX 负载均衡器属于 NSX Edge，因此在销毁 NSX Edge 时，也会销毁负载均衡器资源，并释放资源。负载均衡的计算机层销毁后，将从相应 NSX Edge 上的负载均衡器池中移除。</p> <p>注 “销毁”操作可能会返回一条成功消息，即使无法从其端点中移除计算机部署。例如，如果 vSphere 计算机位于非 vSAN 数据存储，并且其 VMX 文件中包含已损坏或其他无效数据。即使“销毁”消息指示销毁操作成功，也可以查看请求日志以获得其他信息。强制销毁处于此状态的计算机可能使其仍在端点上运行，并引起 IP 冲突。如果在端点（vRealize Automation 之外）上更正损坏，您可以重试销毁操作。</p> <p>业务组管理员可在销毁请求失败后强制销毁部署。强制销毁指示 vRealize Automation 忽略在销毁部署时无法销毁各个资源。有关使用强制销毁的详细信息，请参见销毁请求失败后强制销毁某个部署。</p> <p>注 在 vRealize Automation 中执行“销毁”操作删除已置备的计算机时，通过预留分配给该计算机的存储和内存将会被释放。如果在 vCenter Server 中删除该计算机，存储和内存将不会被释放。</p> <p>销毁包含 Amazon 计算机组件的部署时，可以一次销毁多个 EBS 卷，具体取决于蓝图中删除卷设置的配置方式。有关详细信息，请参见Amazon 计算机组件设置。</p> <p>销毁包含 Amazon 计算机组件的部署时，将会分离在此计算机的生命周期内为其添加的所有 EBS 卷，而不是将这些卷销毁。vRealize Automation 未提供销毁 EBS 卷的选项。</p>
解除浮点 IP 关联	计算机 (Openstack)	从 Openstack 计算机中移除浮点 IP。

表 4-2. 操作菜单命令（续）

操作	资源类型	描述
取消	没有资源类型。初始置备请求失败或操作失败。	<p>可以取消失败的请求。可以取消正在进行的请求。</p> <ul style="list-style-type: none"> ■ 如果取消的请求是部署请求，则取消会从部署列表中移除失败的部署。 ■ 如果取消的请求是一个操作，则取消会从卡视图中移除失败的操作请求，部署仍保持以前的状态。 <p>必须取消失败的操作请求，才能查看在关联部署上运行的其他操作。此外，还必须取消失败的操作，部署用户才能查看计算机历史记录。</p> <p>无法对通过 API 提交的请求运行取消，并且不会阻止通过 API 提交的操作。</p> <p>此操作可用于所有失败的初始置备请求。不需要授权。</p>
执行重新配置	计算机	立即重新配置计算机或安排稍后的重新配置操作。
过期	部署和计算机	结束部署或部署中包含的所有资源的计算机租约。
导出证书	计算机	从云计算机中导出证书。
获取过期提醒	计算机	下载当前租约过期日期对应的日历事件文件。
安装 VMware Tools	计算机	在 vSphere 虚拟机上安装 VMware Tools。
重新启动	计算机	关闭计算机电源，然后重新开启。
关闭电源	计算机	关闭计算机电源，而不关闭客户机操作系统。
打开电源	计算机	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	在 vSphere 虚拟机上重新引导客户机操作系统。要使用此操作，必须在计算机上安装 VMware Tools。

表 4-2. 操作菜单命令（续）

操作	资源类型	描述
重新配置	计算机	<p>业务组主管、支持用户或计算机所有者可以对所选的 vSphere 虚拟机执行以下重新配置操作：</p> <ul style="list-style-type: none"> ■ 更改描述 ■ 更改 CPU、内存、网络和磁盘设置 ■ 添加、编辑和删除自定义属性和属性组 ■ 添加、编辑、重新排序或删除 NAT 端口转发规则的网络适配器 ■ 重新配置关机 ■ 更改计算机所有者（仅可用于业务组主管和支持用户） <p>如果更改存储预留策略可能会更改磁盘上的存储配置文件，则不要进行此更改。</p> <p>有关详细信息，请参见指定计算机重新配置设置以及重新配置注意事项。</p> <p>如果在源蓝图的蓝图设置页面上选择了将更新传播到现有部署选项，则蓝图中 CPU、内存或存储最小值和最大值设置的任何增加或扩大都会推送到通过该蓝图置备的活动部署。有关详细信息，请参见蓝图属性设置。</p> <p>您不应在 vRealize Automation 外部管理由 vRealize Automation 管理的 NSX 对象。例如，如果您在 NSX 中（而不是在 vRealize Automation 中）修改了部署的 NSX 负载均衡器的成员端口，那么 NSX 数据收集将断开部署的计算机及其原本关联的负载均衡器成员池之间的关联。如果在 vRealize Automation 外部更改了部署的负载均衡器成员端口，那么缩小和扩大操作也会产生意外结果。</p>
重新配置	负载均衡器	<p>授权的计算机所有者、支持用户、租户管理员或业务组主管可以更改虚拟服务器中的任何设置，并且可以在 NSX 负载均衡器中添加或移除虚拟服务器：</p> <p>有关详细信息，请参见重新配置部署中的负载均衡器。</p> <p>有关负载均衡器中的虚拟服务器设置的信息，请参见添加按需负载均衡器组件。</p> <p>您不应在 vRealize Automation 外部管理由 vRealize Automation 管理的 NSX 对象。例如，如果您在 NSX 中（而不是在 vRealize Automation 中）修改了部署的 NSX 负载均衡器的成员端口，那么 NSX 数据收集将断开部署的计算机及其原本关联的负载均衡器成员池之间的关联。如果在 vRealize Automation 外部更改了部署的负载均衡器成员端口，那么缩小和扩大操作也会产生意外结果。</p>
注册 VDI	虚拟机 (XenServer)	在 XenServer 项目上注册虚拟磁盘映像。

表 4-2. 操作菜单命令（续）

操作	资源类型	描述
从目录中移除	部署	从目录中移除 XaaS 置备的资源。可以对现有对象和不再位于 Orchestrator 清单中的对象执行此操作。
重新置备	计算机	<p>销毁计算机，然后启动置备 workflow 创建同名的计算机。</p> <p>请求计算机重新置备时，已知问题可能会导致 vRealize Automation 在目录中显示重新置备状态为“完成”，但实际状态为“正在进行”。提交重新置备计算机的请求之后，您可以通过以下任一操作检查重新置备的计算机的状态：</p> <ul style="list-style-type: none"> ■ 基础架构 > 受管计算机 ■ 部署 选项卡 ■ 管理 > 事件 > 事件日志 <p>注 您不能重新置备 Amazon 计算机。</p> <p>有关相关信息，请参见 VMware 知识库文章《重新置备的计算机任务》(2065873)，网址为： http://kb.vmware.com/kb/2065873。</p>
重新提交	没有资源类型。初始置备请求失败。	<p>重新提交失败的置备请求。重新提交的请求在置备过程开始时使用已输入的值开始执行。</p> <p>如果请求失败且问题可以解决，则可以重新提交请求，而不是创建新请求。如果错误是值不正确所致，例如数据存储不支持您的请求，则必须使用新值创建新请求。</p> <p>此操作可用于所有失败的初始置备请求。不需要授权。</p>
恢复	部署	<p>恢复部分成功的置备请求。恢复将从故障点继续。</p> <p>如果在置备过程中由于临时环境或基础架构问题、超时或其他可在请求外纠正的问题导致部署失败，您可以恢复置备过程中而不是创建新的置备请求。如果是蓝图中的错误导致失败，则恢复不起作用。您必须请求新的部署，而不是尝试恢复。</p> <p>如果部署请求仅部分成功，且问题可以解决，则可以使用恢复操作。恢复的请求将从故障点继续。</p> <p>有关详细信息，请参见“恢复”操作的工作原理。</p>
恢复快照	虚拟机	恢复为该计算机的先前快照。要使用此操作，必须存在现有快照。

表 4-2. 操作菜单命令（续）

操作	资源类型	描述
缩小	部署	<p>销毁部署中不需要的计算机实例以适应降低的容量要求。计算机组件及其上安装的任何软件组件均会被销毁。从属软件组件以及网络和安全组件均会针对新部署配置进行更新。在缩放操作期间，XaaS 组件不可缩放且未更新。</p> <p>可通过尝试再次缩放部署来尝试修复部分成功的缩放操作。但是，无法将部署缩放到其当前大小，并且以这种方式修复部分成功的缩放不会取消分配待定资源。您可以查看请求执行详细信息屏幕并找出哪些任务在哪些节点上失败，以帮助您决定是否通过另一个缩放操作修复部分成功的缩放。失败和部分成功的缩放操作不会影响原始部署的功能，您可以在对任何失败进行故障排除时继续使用您的目录项。</p>
扩大	部署	<p>在部署中置备计算机的其他实例以适应增长的容量要求。计算机组件及其上安装的任何软件组件均会被置备。从属软件组件以及网络和安全组件均会针对新部署配置进行更新。在缩放操作期间，XaaS 组件不可缩放且未更新。</p> <p>可通过尝试再次缩放部署来尝试修复部分成功的缩放操作。但是，无法将部署缩放到其当前大小，并且以这种方式修复部分成功的缩放不会取消分配待定资源。您可以查看请求执行详细信息屏幕并找出哪些任务在哪些节点上失败，以帮助您决定是否通过另一个缩放操作修复部分成功的缩放。失败和部分成功的缩放操作不会影响原始部署的功能，您可以在对任何失败进行故障排除时继续使用您的目录项。</p> <p>如果在源蓝图的蓝图设置页面上选择了将更新传播到现有部署选项，则蓝图中 CPU、内存或存储最小值和最大值设置的任何增加都会推送到通过该蓝图置备的活动部署。有关详细信息，请参见蓝图属性设置。</p>
关机	计算机	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 VMware Tools 。
挂起	计算机	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。
取消注册	计算机	从清单中移除计算机，但不销毁。取消注册的计算机不可用。
取消注册	网络	从清单中移除网络，但不销毁。取消注册的网络不可用。
取消注册 VDI	虚拟机 (XenServer)	在 XenServer 项目上取消注册虚拟磁盘映像。

对资源操作菜单中缺少的操作进行故障排除

作为计算机或资源所有者，您无法看到已置备项目的所有授权操作。

问题

在已知为用户或业务组授予了操作的环境中，您希望在**部署**列表中选择某个项目时看到所有操作。

原因

操作的可用性取决于已置备资源的类型、资源的操作状况以及配置和提供资源的方式。以下列表提供了一些您为何看不到所有已配置操作的原因。

- 根据已置备资源的当前状况，该操作不适用。例如，“关闭电源”仅当计算机已打开电源时才可用。
- 该操作不适用于所选项目类型。如果项目不支持该操作，则不会显示在列表中。例如，“创建快照”操作不适用于物理机；如果选定的项目是 **Linux** 计算机，则“使用 RDP 连接”操作不可用。
- 该操作适用于已置备的资源类型，但在“基础架构”蓝图中处于停用状态。如果该操作处于停用状态，则永远不会对使用此蓝图置备的任何项目显示为可用操作。
- 该操作未包括在用于置备需要运行该操作的项目授权中。只有授权操作（作为 **IaaS** 蓝图的一部分或作为 **XaaS** 资源操作）才能显示在“操作”菜单中。
- 该操作创建为 **XaaS** 资源操作，但未包括在用于置备需要运行操作的项目授权中。只有授权操作才会显示在“操作”菜单中。
- 根据为 **XaaS** 资源操作或指向已置备的 **IaaS** 计算机的资源映射配置的目标标准，该操作可能会受限。

解决方案

- ◆ 确认该操作适用于已置备项目或已置备项目的状况。
- ◆ 确认该操作已配置且已包括在用于置备项目的授权中。

创建计算机快照

根据管理员配置环境的方式，您有可能能够创建虚拟机的快照。快照是某一特定时刻的虚拟机映像。这是原始虚拟机映像的节省空间的副本。使用快照，可以在遇到损坏、数据丢失或安全威胁时轻松恢复系统。创建虚拟机的快照之后，您可以应用该快照，并将系统重置回生成快照时的点。

创建内存快照时，该快照将捕获虚拟机电源设置的状态和虚拟机的内存（可选）。捕获虚拟机内存状况时，完成快照操作所需的时间更长。您还可能会看到通过网络响应时短暂失效的情况。

前提条件

- 已打开电源、关闭电源或挂起的现有虚拟机。
- 如果已为一个或多个独立磁盘配置虚拟机，请在创建快照之前关闭计算机电源。您无法在打开计算机电源后创建快照。有关磁盘配置信息，请参见“自定义属性虚拟表”。
- 租户管理员或业务组主管已授权您执行快照操作。

步骤

- 1 单击**部署**。

- 2 找到包括希望创建快照的计算机的部署，然后单击部署名称。
- 3 在**组件**选项卡上，单击虚拟机，然后单击操作齿轮图标。
将显示组件操作菜单。
- 4 单击“操作”菜单中的**创建快照**。
- 5 输入名称和可选描述。
- 6 如果要捕获计算机的内存和电源设置，请选择**包括内存**。
- 7 单击**提交**。

远程连接到计算机

您可以从 vRealize Automation 控制台远程连接到计算机。

如果使用 VMware Remote Console 进行连接，请参见知识库文章[对 vRealize Automation 中的 VMRC 连接进行故障排除 \(2114235\)](#)。

前提条件

- 以**计算机所有者、租户管理员或业务组主管**身份登录到 vRealize Automation。
- 确认已安装 VMware Tools。
要在与 VMware Remote Console 连接时支持完全正常的访问，必须在 vRealize Automation 客户端上安装 VMware Tools。如果未安装 VMware Tools，则会出现问题，例如：鼠标指针和鼠标键在连接到目标计算机之后无法正常运行。有关受支持的 VMware Tools 版本的信息，请参见 [vRealize Automation 产品文档](#)中的 vRealize Automation 支持列表。
- 确认置备的计算机已打开电源。
- 允许通过端口 902 在 vRealize Automation 设备和 ESXi 服务器之间传输网络流量。
- 允许通过端口 8444 在 vRealize Automation 设备和客户端浏览器之间传输网络流量。
- 允许通过端口 443 在 IaaS Web 组件 Windows Server 与关联的 vSphere 端点之间传输网络流量。

步骤

- 1 单击**部署**。
- 2 找到包括必须连接的计算机的部署，然后单击部署名称。
- 3 在**组件**选项卡上，找到计算机，然后单击操作齿轮图标。
将显示组件操作菜单。
- 4 选择远程连接方法。
 - 选择**使用 RDP 连接**可使用 RDP 连接。
 - 选择**连接到远程控制台**可使用 VMware Remote Console 进行连接。
对所有提示做出响应。
- 5 单击**连接**并按照指示登录到计算机。

6 完成后，注销并关闭浏览器窗口。

为使用不可信 SSL 证书的 vSphere 配置远程控制台

如果 vRealize Automation 部署使用不可信证书，则必须先将客户端浏览器配置为信任该证书，然后才能将远程控制与 VMware Remote Console 一起使用。执行此操作所需的步骤因浏览器而异。

如果已针对您的环境将 vRealize Automation 配置为使用可信的 SSL 证书，则 VMware Remote Console 不需要在客户端浏览器上进行其他配置。将 vRealize Automation 设备证书替换为可信证书后，无需更新 Web 浏览器客户端的证书信息。

如果要替换证书，请参见 vRealize Automation 《系统管理》指南中有关替换 vRealize Automation 设备证书的主题。

对于 vSphere 上置备的计算机，使用 VMware Remote Console 的远程连接均由 vRealize Automation 设备证书通过代理控制台加以保护。VMware Remote Console 需要浏览器提供 WebSocket 支持，且浏览器必须信任 vRealize Automation 设备证书。通过转到 root 级别的虚拟设备（其地址格式为 `https://vra-vx.eng.mycompany.com/`），可以获取该证书。

有关浏览器和 vSphere 支持要求的信息，请参见《vRealize Automation 支持列表》。

将 Firefox 配置为信任 vRealize Automation 的证书

要支持在 vSphere 上置备的客户端中使用 VMware Remote Console，必须手动将不可信的 vRealize Automation 设备证书导入客户端浏览器。

有关受支持的 Firefox 版本的信息，请参见 vRealize Automation [信息中心](#) 的 VMware vRealize 支持列表。

注 如果已针对您的环境将 vRealize Automation 配置为使用可信的 SSL 证书，则 VMware Remote Console 不需要在客户端浏览器上进行其他配置。

步骤

1 在 Firefox 浏览器中，登录到 vRealize Automation 设备。

此时将显示一条消息，指出证书不受信任。

2 选择**打开菜单 > 选项**。

3 单击**隐私和安全**，然后单击**查看证书**。

4 在“证书管理器”对话框中，单击**服务器**，然后单击**添加例外**。

5 为 vRealize Automation 设备添加带有 8444 端口的 URL。

例如 `https://your-vra-fqdn-domain:8444`。

6 单击**获取证书**，然后单击**确认安全例外**。

7 单击**确定**。

结果

您可以连接到远程控制台，且不会显示证书错误。

将 Internet Explorer 配置为信任 vRealize Automation Appliance 的证书

要支持在 vSphere 上置备的客户端中使用 VMware Remote Console，必须手动将不可信的 vRealize Automation 设备证书导入客户端浏览器。

注 如果已针对您的环境将 vRealize Automation 配置为使用可信的 SSL 证书，则 VMware Remote Console 不需要在客户端浏览器上进行其他配置。

此过程中的步骤适用于自签名证书和证书颁发机构颁发的证书。

有关支持的 Internet Explorer 版本的信息，请参见 VMware 网站上的 VMware vRealize 支持列表。

步骤

- 1 在 Internet Explorer 浏览器中，登录到 vRealize Automation 设备。
- 2 在浏览器地址栏显示的证书错误消息上，单击**查看证书**。
- 3 单击“证书信息”窗口的**常规**选项卡。
- 4 验证证书的信息是否正确，然后单击**安装证书**。
- 5 选择“证书存储”对话框中的**将所有的证书放入下列存储**。
- 6 单击**浏览**查找证书存储。
- 7 选择**受信任的根证书颁发机构**，然后单击**确定**。
- 8 在“证书存储”对话框上单击**下一步**。
- 9 单击“安全警告”对话框中的**是**以安装证书。
- 10 重新启动浏览器。

结果

您可以连接到远程控制台，且不会显示证书错误。

将 Chrome 配置为信任 vRealize Automation Appliance 的证书

要支持在 vSphere 上置备的客户端中使用 VMware Remote Console，必须手动将不可信的 vRealize Automation 设备证书导入客户端浏览器。

有关受支持的 Chrome 版本的信息，请参见 [vRealize Automation 产品文档](#)中的 vRealize Automation 支持列表。

注 如果已针对您的环境将 vRealize Automation 配置为使用可信的 SSL 证书，则 VMware Remote Console 不需要在客户端浏览器上进行其他配置。

在 Windows 上，Chrome 和 Internet Explorer 使用相同的证书存储。这意味着受 Internet Explorer 信任的证书也受 Chrome 信任。要为 Chrome 建立可信证书，请通过 Internet Explorer 导入这些证书。有关此过程的信息，请参见[将 Internet Explorer 配置为信任 vRealize Automation Appliance 的证书](#)。

完成该过程之后，请重新启动 Chrome。

要永久信任 Macintosh 操作系统上的证书，请下载证书文件，并将该证书作为可信证书安装在证书管理工具中。

步骤

- 1 在 Chrome 浏览器中，登录到 vRealize Automation 设备。
- 2 单击浏览器地址栏旁边的 **查看站点信息** 图标，然后单击 **证书** 图标以显示证书信息。
- 3 保存该证书。
- 4 启动 Keychain Access 应用程序，该应用程序通常位于应用程序文件夹的实用程序文件夹中。
- 5 选择 **文件 > 导入项目**。
- 6 在 Keychain Access 屏幕上，选择之前保存的证书文件。
将 **目标密钥** 的值设置为 **系统**。
- 7 单击 **打开** 以导入证书。
- 8 重新启动浏览器。

指定计算机重新配置设置以及重新配置注意事项

vSphere、vCloud Air 和 vCloud Director 平台支持重新配置部署中的现有计算机，以修改 CPU、内存和存储等规范。

重新配置请求需要根据授权、策略以及为蓝图中的计算机组件启用的操作进行批准。

不支持重新配置分配给按需网络的虚拟机。无法重新配置连接到按需网络的网卡。如果您尝试重新配置按需 NAT 或路由网络，将显示错误 **Original network [<network>] is not selected in the machine's reservation.**，计算机上的网络保持不变，并且计算机上的 IP 地址也保持不变。

如果您有权执行“取消重新配置 (计算机)”和“执行重新配置 (计算机)”，则可取消重新配置或重试已失败的重新配置。

不支持扩展从链接克隆蓝图置备的虚拟机上的磁盘。

您无法使用 **Size** 或 **Image** 组件配置文件重新配置计算机，但是基于配置文件计算的 CPU、内存和存储范围将仍可用于重新配置操作。例如，如果您使用小型（1 个 CPU、1024 MB 内存和 10 GB 存储）、中型（3 个 CPU、2048 MB 内存、12 GB 存储）和大型（5 个 CPU、3072 MB 内存和 15 GB 存储）Size 值集，那么计算机重新配置期间可用的范围是 1-5 个 CPU、1024-3072 MB 内存以及 1-15 GB 存储。

vRealize Automation 在部署时会生成蓝图快照。如果更新部署中的 CPU 和 RAM 等计算机属性时遇到重新配置问题，请参见知识库文章 [2150829 vRA 7.x 蓝图快照](#)。

前提条件

- 以计算机所有者、支持用户、具有共享访问角色的业务组用户或业务组主管的身份登录到 vRealize Automation。
- 要重新配置的计算机必须处于“开启”或“关闭”状态，而不处于活动的重新配置状态。
- 尽管 NSX 设置仅适用于 vSphere，但计算机类型必须是 vSphere、vCloud Air 或 vCloud Director。
- 确认您有权重新配置计算机。

步骤

- 1 单击**部署**。
- 2 找到包括必须重新配置的计算机的部署，然后单击部署名称。
- 3 在**组件**选项卡上，单击虚拟机，然后单击操作齿轮图标。
将显示组件操作菜单。
- 4 选择**重新配置**。
- 5 选择要重新配置的设置的相应选项卡。

表 4-3. 请求重新配置更改

选项卡	主题
常规	重新配置 CPU 和内存
存储	编辑存储设置
网络	更改网络设置 要更改 NAT 规则，请参见 更改部署中的 NAT 规则 。
安全	要重新配置安全设置，请参见 在部署中添加或移除安全项目 。
属性	更改自定义属性和属性组设置

后续步骤

[运行请求的计算机重新配置](#)。

重新配置 CPU 和内存

您可以在置备蓝图设置的限制内更改已置备计算机使用的 CPU 数量或内存和存储量。

对于已置备的 Amazon 部署，您可以重新配置部署中除根卷外的所有存储卷。

不支持扩展从链接克隆蓝图置备的虚拟机上的磁盘。

前提条件

[指定计算机重新配置设置以及重新配置注意事项](#)。

步骤

- 1 单击**常规**选项卡。
- 2 在 **CPU 数量** 文本框中输入 CPU 数量。
- 3 在 **内存 (MB)** 文本框中输入内存量。
- 4 在 **存储 (GB)** 文本框中输入存储量。

后续步骤

指定其他计算机重新配置设置。如果您已完成计算机设置更改，请启动计算机重新配置请求。请参见[运行请求的计算机重新配置](#)。

编辑存储设置

您可以在已置备的虚拟机上添加、删除存储卷或更改存储卷的大小。

无法重新配置 IDE 磁盘类型的存储。

在 vRealize Automation 中执行“销毁”操作删除已置备的计算机时，通过预留分配给该计算机的存储和内存将会被释放。如果在 vCenter Server 中删除该计算机，存储和内存将不会被释放。

例如，您无法删除与现有部署中的计算机关联的预留。如果您在 vCenter Server 中手动移动或删除了已部署的计算机，vRealize Automation 仍会认为该计算机有效，并阻止您删除关联的预留。

在计算机置备和部署后，可以更改某些设置，例如容量和存储预留策略。

在置备时，**驱动器盘符/挂载路径**和**标签**值将应用于客户机代理。这些值在置备后不会更新，因此可能不是最新的。要收集数据并显示其当前值，可以创建并运行自定义 vRealize Orchestrator 工作流。

前提条件

[指定计算机重新配置设置以及重新配置注意事项。](#)

对于已置备的 Amazon 部署，可以重新配置部署中除根卷外的所有存储卷。

步骤

1 单击**存储**选项卡。

2 根据需要查看或编辑存储选项。

- 添加新卷（如可用）。
- 删除卷（如可用）。

不可选择的图标表示不可删除的卷，例如来自链接克隆的卷。

- 更改卷大小（如可用）。

无法减小现有卷的大小。卷大小受在蓝图中指定的存储总量限制，小于分配给其他卷的数量。

后续步骤

指定其他计算机重新配置设置。如果您已完成计算机设置更改，请启动计算机重新配置请求。请参见[运行请求的计算机重新配置](#)。

更改网络设置

您可以添加、移除或编辑网络适配器。

在计算机重新配置过程中，可以更改以下网络设置：

- 添加或移除网卡。
- 为现有网卡分配 IP 地址或释放现有网卡的 IP 地址。
- 将新的 IP 地址分配给网卡，前提是网络不是按需 NAT 或按需路由网络。

您不能重新配置按需路由或按需 NAT 网络。

网络重新配置要求在预留中选择源网络和目标网络。

添加网卡时，将分配 IP 地址。移除网卡时，将释放 IP 地址。

基于预留信息和网络配置文件信息更改网络设置之后，将在 vRealize Automation 中分配新的网络 IP，但不会使用新的 IP 信息在端点上更新已部署的计算机。您必须在重新配置过程完成之后手动为计算机分配 IP。

不支持重新配置分配给按需网络的虚拟机。无法重新配置连接到按需网络的网卡。如果您尝试重新配置按需 NAT 或路由网络，将显示错误 `Original network [<network>] is not selected in the machine's reservation.`，计算机上的网络保持不变，并且计算机上的 IP 地址也保持不变。

对于从 vRealize Automation 6.2.x 升级或迁移到此 vRealize Automation 版本的部署，不支持更改 NSX 网络设置。

前提条件

[指定计算机重新配置设置以及重新配置注意事项。](#)

步骤

- 1 单击**网络**选项卡。
- 2 （可选）添加网络适配器。
 - a 单击**新建网络适配器**。
 - b 从**网络路径**下拉菜单中选择网络。
您在计算机预留上选择的所有网络均可用。
 - c 在**地址**文本框中键入网络的静态 IP 地址。
预留内已分配的网络配置文件中必须未分配该 IP 地址。
 - d 单击**保存**图标 (👍)。
- 3 （可选）移除网络适配器。
 - a 找到网络适配器。
 - b 单击**删除**图标 (🗑️)。
无法移除网络适配器 O。
- 4 （可选）编辑网络适配器。
 - a 找到网络适配器。
 - b 单击**编辑**图标 (✎)。
 - c 从**网络路径**下拉菜单中选择网络。
 - d 单击**保存**图标 (👍)。

后续步骤

指定其他计算机重新配置设置。如果您已完成计算机设置更改，请启动计算机重新配置请求。请参见[运行请求的计算机重新配置](#)。

更改自定义属性和属性组设置

您可以编辑、添加或删除部署的计算机中的自定义属性。

不能使用自定义属性输入卷的磁盘号、容量、标签或存储预留策略值。您必须通过在“存储卷”表中添加或编辑卷来输入这些值。请参见[编辑存储设置](#)。

前提条件

[指定计算机重新配置设置以及重新配置注意事项](#)。

步骤

- 1 单击**属性**选项卡。
- 2 要添加属性，请单击**新建属性**。
- 3 在**名称**文本框中输入属性名称。
- 4 在**值**文本框中输入属性值。
- 5 选中**已加密**复选框，对该值进行加密。
- 6 选中**提示用户**复选框，提示用户在请求计算机时输入该值。
- 7 添加其他属性、编辑现有属性或删除属性。

后续步骤

指定其他计算机重新配置设置。如果您已完成计算机设置更改，请启动计算机重新配置请求。请参见[运行请求的计算机重新配置](#)。

运行请求的计算机重新配置

您可以立即开始请求的计算机重新配置或计划在特定的日期和时间开始。此外，您还可以在重新配置前指定计算机的电源选项。

前提条件

[指定计算机重新配置设置以及重新配置注意事项](#)。

步骤

- 1 如果**执行**选项卡可见，则可选择该选项卡，以指定其他重新配置设置。如果不可见，请单击**提交**以启动计算机重新配置。
- 2 如果**执行**选项卡可见，请单击**执行**以调度重新配置操作。
- 3 （可选）从**执行请求**下拉菜单中选择一个选项。

选项	描述
紧急	在批准后尽快开始重新配置。
已调度	在指定的日期和时间开始重新配置。在显示的文本框中输入日期和时间。

调度的时间是 vRealize Automation Web 服务器所处的本地时间。如果**执行请求**不可用，则会立即开始重新配置。

4 （可选）从电源操作下拉菜单中选择电源操作。

选项	描述
根据需要重新引导	（默认）如果需要，请在重新配置前重新启动计算机。
重新引导	无论是否需要重新启动，都在重新配置前重新启动计算机。
不重新引导	即使需要重新启动，也不在重新配置前重新启动计算机。

以下条件要求在重新配置之前重新启动计算机：

- CPU 发生更改，但不支持或已停用热添加
- 内存发生更改，但不支持或已停用热内存
- 存储发生更改，但已停用热存储

如果计算机处于关闭状态，则不会重新启动。

注 可以使用 `VirtualMachine.Reconfigure.DisableHotCpu` 自定义属性停用 vSphere 热添加选项。

5 单击确定。

后续步骤

您可以通过观察用户界面中显示的工作流状态来监控重新配置的进度。请参见 [重新配置操作的工作流状态](#)。

重新配置操作的工作流状态

当重新配置启动并逐步执行工作流时，您可以从“编辑”页面监控进度。

表 4-4. 重新配置操作的工作流状态

状态	描述
重新配置挂起	已创建状态操作。
已调度	已为 Distributed Execution Manager (DEM) 创建调度的工作流。
重新配置	正在运行接口特定的工作流。
重新配置失败，正在等待重试	重新配置失败，正在等待所有者请求重试如果计算机所有者有权重新配置或取消重新配置操作，则所有者可以重试或取消重新配置。
重新配置失败	重新配置失败，正在等待工作流执行下一个操作。
重新配置成功	重新配置成功，正在等待工作流执行下一个操作。
已取消	用户已取消重新配置。获得权利的计算机所有者可以取消重新配置。
完成	完成工作流将在完成清理后设置此状态，以便工作流能够继续清理状态操作和批准。完成状态表示来自 vRealize Automation 的请求已完成，但并不表示计算机重新配置已成功完成。

重新配置部署中的负载均衡器

您可以在已部署的 NSX 负载均衡器中添加、编辑或删除虚拟服务器。

以下注意事项适用于源自 vRealize Automation 7.2 或更早版本的部署。

- 负载均衡器重新配置仅限于包含单个负载均衡器的部署。
- 部署中任何负载均衡器的“项目详细信息”页面显示了部署中的所有负载均衡器使用的虚拟服务器。有关详细信息，请参见[知识库文章 2150276](#)。
- 对于从 vRealize Automation 6.2.x 升级或迁移到此 vRealize Automation 版本的部署，不支持重新配置负载均衡器操作。

有关升级的负载均衡器和当前 vRealize Automation 版本中部署的负载均衡器，请勿在同一个请求中编辑虚拟服务器并添加虚拟服务器。有关详细信息，请参见[知识库文章 2150240](#)。

注 NSX-T 负载均衡器不支持**重新配置**操作。

如果部署上正在执行另一项操作（如扩大操作），这时您提交了重新配置负载均衡器请求，重新配置将失败并显示支持消息。在这种情况下，您可以等待直到完成操作为止，然后提交重新配置请求。

注 从 YAML 文件导入与部署相关联的蓝图，且该文件包含的按需负载均衡器的名称字段与 ID 字段的值不同时，**重新配置**操作将失败。要为基于导入蓝图的部署启用负载均衡器重新配置选项，请在蓝图中执行以下步骤，以在将来的部署中允许对负载均衡器组件执行置备后操作。

- 1 在 vRealize Automation 控制台中，选择蓝图。
- 2 单击**编辑**并更改蓝图名称。这会将名称和嵌入式 ID 设置为相同的值。
- 3 选择蓝图中的负载均衡器组件。
- 4 单击**编辑**并重新输入组件名称。这会将名称和嵌入式 ID 设置为相同的值。
- 5 针对蓝图中的所有负载均衡器组件重复此操作。
- 6 保存蓝图。

使用编辑后的蓝图置备新的部署时，重新配置负载均衡器操作将运行。要避免出现此问题，请确保在导入之前所有 YAML 文件的所有负载均衡器、网络和安全组件均具有相同的名称和 ID 值。

您不应在 vRealize Automation 外部管理由 vRealize Automation 管理的 NSX 对象。例如，如果您在 NSX 中（而不是在 vRealize Automation 中）修改了部署的 NSX 负载均衡器的成员端口，那么 NSX 数据收集将断开部署的计算机及其原本关联的负载均衡器成员池之间的关联。如果在 vRealize Automation 外部更改了部署的负载均衡器成员端口，那么缩小和扩大操作也会产生意外结果。

有关添加或编辑虚拟服务器时有哪些设置可用的信息，请参见[添加按需负载均衡器组件](#)。

在 vRealize Automation 中重新配置负载均衡器时，在 NSX 中配置或在 vRealize Automation 中不可用作设置的某些设置会恢复至其默认值。在 vRealize Automation 中运行负载均衡器重新配置操作后，根据需要确认并更新 NSX 中的以下设置：

- HTTP 标头的 Insert-X-Forwarded
- HTTP 重定向 URL

■ 服务监控扩展

前提条件

- 以计算机所有者、支持用户、具有共享访问角色的业务组用户或业务组主管的身份登录到 vRealize Automation。
- 确认您有权在部署中重新配置负载均衡器。所需的目录授权是“重新配置负载均衡器”。

步骤

- 1 单击**部署**。
- 2 找到包括必须重新配置的负载均衡器的部署，然后单击部署名称
- 3 在**组件**选项卡上，单击负载均衡器，然后单击操作齿轮图标。
将显示组件操作菜单。
- 4 选择**重新配置**。
- 5 添加、编辑或删除虚拟服务器。

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

- 6 单击**提交**。

更改部署中的 NAT 规则

在部署的一对多 NAT 网络中，可以添加、编辑和删除现有的 NSX NAT 规则。

还可以更改 NAT 规则的处理顺序。

注 如果从包含 NAT 网络组件的 YAML 文件导入部署的源蓝图且 NAT 网络组件的名称和 ID 值不相同，则**更改 NAT 规则**操作将失败。要允许对基于已导入蓝图的部署执行**更改 NAT 规则**操作，请在置备部署之前在蓝图中执行以下步骤。

- 1 启动 vRealize Automation，单击“设计”选项卡，然后打开蓝图。
- 2 单击**编辑**并更改蓝图名称。这会将名称和嵌入式 ID 设置为相同的值。
- 3 选择蓝图中的 NAT 网络组件。
- 4 单击**编辑**并重新输入组件名称。这会将名称和嵌入式 ID 设置为相同的值。
- 5 针对蓝图中的所有 NAT 网络组件重复此操作。
- 6 保存蓝图。

要避免出现此问题，请确保在导入之前所有 YAML 文件的所有蓝图和负载均衡器、网络和安全组件均具有相同的名称和 ID 值。

有关相关信息，请参见[创建和使用 NSX for vSphere 的 NAT 规则](#)和[添加按需 NAT 或按需路由网络组件](#)。

前提条件

- 以计算机所有者、支持用户、具有共享访问角色的业务组用户或业务组主管的身份登录到 vRealize Automation。
- 确认您有权更改网络中的 NAT 规则。
- 确认 NAT 网络已配置为一对多 NAT 网络。此操作不适用于 NAT 一对一网络。

NSX for vSphere 支持 NAT 一对一网络和 NAT 一对多网络，但 NSX-T 仅支持 NAT 一对多网络。

步骤

- 1 单击**部署**。
- 2 找到包括必须更改的网络组件的部署，然后单击部署名称
- 3 在**组件**选项卡上，单击 NAT 网络组件。

对于与第三方 IPAM 提供程序关联的按需 NAT 网络，无法编辑该组件。但是，可以手动添加新的目标 IP 地址。添加新的目标 IP 地址时，组件值为 null。提交重新配置请求时，将处理新的目标 IP 地址和 null 计算机 ID。

- 4 单击操作齿轮图标。
将显示组件操作菜单。
- 5 单击**更改 NAT 规则**。
- 6 添加新的 NAT 端口转发规则、重新排序规则、编辑现有规则或删除规则。
- 7 单击**提交**。

显示现有 NSX Edge 的所有 NAT 规则

可以显示活动部署中使用的 NSX Edge 的 NAT 规则信息。

NAT 规则在 Edge 视图中显示为部署中使用的所有 NAT 规则的汇总。在 Edge 视图中，规则不一定按处理顺序显示。

要查看并（可选）更改 NAT 规则在 NAT 一对多网络中的处理顺序，请参见[更改部署中的 NAT 规则](#)。

前提条件

- 以计算机所有者、支持用户、具有共享访问角色的业务组用户或业务组主管的身份登录到 vRealize Automation。

步骤

- 1 单击**部署**。
- 2 找到包括您在查看的 NSX Edge 的部署，然后单击部署名称。
- 3 在**组件**选项卡上，找到 NSX Edge 组件。
- 4 选择要查看的 NSX Edge。
- 5 完成之后，单击**关闭**。

在部署中添加或移除安全项目

可以在计算机部署中添加或移除现有 NSX 安全组和安全标记。您不能添加按需安全组，但可以移除它们。

更改安全性操作取决于计算机组件或群集。例如，如果安全性与名为 **AppTier2** 的群集（包括 2 台计算机）相关联，则可在 **AppTier2** 群集上执行更改安全性操作，但不能在群集内的各个计算机上执行更改操作。

对于从 vRealize Automation 6.2.x 升级或迁移到此 vRealize Automation 版本的部署，不支持更改安全性操作。

前提条件

- 以计算机所有者、支持用户、具有共享访问角色的业务组用户或业务组主管的身份登录到 vRealize Automation。
- 确认您有权更改部署中的安全性。所需的目录授权为“更改安全部署”。

步骤

- 1 单击**部署**。
- 2 找到包括安全组和标记的部署，然后单击部署名称。
- 3 在**组件**选项卡上，单击安全组件，然后单击操作齿轮图标。
将显示组件操作菜单。
- 4 单击**更改安全性**。
- 5 选择要在其中添加或移除安全项目的已部署的计算机组件或群集。
- 6 根据需要，在部署中添加或移除每个计算机组件或群集的现有安全组和安全标记。
- 7 根据需要，在部署中移除每个计算机组件或群集的按需安全组。
- 8 （可选）单击**原因**选项卡并输入请求的原因。
- 9 单击**提交**。

其他部署管理方法

可以使用授权操作管理已部署的资源，但是还有其他未作为操作包括在内的方法。

这些方法未在“部署”选项卡上提供，但可用于更改已置备的资源。

基于 vRealize Operations Manager 衡量指标回收资源

回收有助于高效使用资源。如果还使用 vRealize Operations Manager 管理环境中的资源，则可以将 vRealize Automation 配置为使用衡量指标计算可以回收部署资源的位置。

步骤

1 配置衡量指标提供程序

您可以配置 vRealize Automation，让它对 vSphere 虚拟机使用 vRealize Operations Manager 运行状况和资源衡量指标。

2 发送回收请求

可以查看和管理部署，以及向部署所有者发送回收请求。回收请求将指定新的租约长度（以天为单位）、部署所有者的响应时间范围以及要进行回收的目标计算机。

3 跟踪回收请求

您可以跟踪回收请求的当前状态和其他详细信息。

配置衡量指标提供程序

您可以配置 vRealize Automation，让它对 vSphere 虚拟机使用 vRealize Operations Manager 运行状况和资源衡量指标。

有关 vRealize Operations Manager 运行状况标志和衡量指标的详细信息，请参见 vRealize Operations Manager 文档。

前提条件

- 以**租户管理员、业务组主管或计算机所有者**身份登录到 vRealize Automation 控制台。
回收 - 创建回收请求的用户需要租户管理员角色，且该租户管理员帐户必须是租户中至少一个业务组的成员。
如果未将租户管理员帐户添加到业务组，则会导致在打开**回收 > 部署**选项卡时出现系统异常。
- 创建 vRealize Operations Manager 用户帐户，并为其分配与 vSphere 集成的所有 vRealize Automation 服务器的视图和资源衡量指标查询特权。
- 为 vRealize Automation 中添加为端点的所有 vSphere 服务器创建 vRealize Operations Manager 适配器实例。有关创建适配器实例的信息，请参见 vRealize Operations Manager 文档。

步骤

- 1 选择**管理 > 回收 > 衡量指标提供程序**。
- 2 选择衡量指标提供程序。

选项	描述
（默认）vRealize Automation 衡量指标提供程序	如果没有 vRealize Operations Manager 实例，则 vRealize Automation 将提供基本计算机衡量指标。
vRealize Operations Manager 端点	为要用作 vSphere 虚拟机的衡量指标提供程序的 vRealize Operations Manager 实例提供连接信息。

- 3 单击**测试连接**。
- 4 单击**保存**。

结果

计算机所在组的租户管理员、计算机所有者和业务组主管可以在项目详细信息页面上查看 vSphere 虚拟机的运行状况标志和运行状况警示。在回收页面上按平台类型 vSphere 进行筛选时，也可以查看 vRealize Operations Manager 衡量指标和运行状况标志。

后续步骤

[发送回收请求](#)。

发送回收请求

可以查看和管理部署，以及向部署所有者发送回收请求。回收请求将指定新的租约长度（以天为单位）、部署所有者的响应时间范围以及要进行回收的目标计算机。

前提条件

- 以**租户管理员**身份登录到 vRealize Automation。
- （可选）要查看运行状况标志或 vRealize Operations Manager 提供的衡量指标，请参见[配置衡量指标提供程序](#)。

步骤


- 1 选择**管理 > 回收 > 部署**。

2 查找与搜索条件匹配的虚拟机部署。

必须选择平台类型 **vSphere** 才能查看 vRealize Operations Manager 提供的衡量指标。

- a 单击**高级搜索**向下箭头，打开搜索框。
- b 输入或选择一个或多个搜索值。

选项	操作
虚拟机名称包含	在文本框中输入一个或多个字符以查找匹配的虚拟机名称。
所有者名称包含	在文本框中输入一个名称以查找匹配的所有者名称。
业务组名称包含	在文本框中输入一个名称以查找匹配的业务组名称。
平台类型	从下拉菜单中选择平台类型。选择 vSphere 以查看 vRealize Operations Manager 提供的衡量指标。 对于 vRealize Operations Manager 是必需的。
电源状况	从下拉菜单中选择电源状况值，查找具有匹配电源状况的虚拟机。
过期日期介于	单击日历图标并选择开始日期和结束日期，查找范围内的过期日期。
CPU 使用情况	从下拉菜单中选择一个值，查找 CPU 使用率高（超过 80%）、CPU 使用率低（低于 5%）的虚拟机，或者选择“无”以查找没有值的虚拟机。 如果查询 vRealize Operations Manager 衡量指标，则无法使用此筛选器查询，且不能按 CPU 使用情况对结果排序。
内存使用情况	从下拉菜单中选择一个值，查找内存使用率高（超过 80%）、内存使用率低（低于 10%）的虚拟机，或者选择“无”以查找没有值的虚拟机。 如果要查询 vRealize Operations Manager 衡量指标，则无法使用此筛选器查询，且不能按内存使用情况对结果排序。
磁盘使用情况	从下拉菜单中选择一个值，查找硬盘使用率低（每秒少于 2 KB）的虚拟机，或者选择“无”以查找没有值的虚拟机。 如果要查询 vRealize Operations Manager 衡量指标，则无法使用此筛选器查询，且不能按磁盘使用情况对结果排序。
网络使用情况	从下拉菜单中选择一个值，查找网络使用率低（每秒少于 1 KB）的虚拟机，或者选择“无”以查找没有值的虚拟机。 如果要查询 vRealize Operations Manager 衡量指标，则无法使用此筛选器查询，且不能按网络使用情况对结果排序。
复杂衡量指标	从下拉菜单中选择一个值，以便根据复杂衡量指标查找虚拟机。例如，选择“闲置”，查找 CPU、网络、内存和磁盘使用情况值均低于 20% 的计算机。 如果查询 vRealize Operations Manager 衡量指标，则无法使用此筛选器。

- c 单击搜索图标 ()。

3 在“部署”页面中，选择要回收其父部署的一个或多个计算机。

只会回收在当前结果页面中选择的可见计算机。

4 单击回收。

包含在当前页面中选择的虚拟机的部署会包括在请求中。

注 “回收部署”页面会列出无法回收的计算机，例如，租约已过期的计算机。如果指定的计算机无法回收，则会收到以下错误：

```
Selection Error: Virtual machine name is not in valid state for reclamation.
```

5 在**新租约长度 (天)** 文本框中，输入新租约的持续时间。

最小值为 1 天，最大值为 365 天，默认值为 7 天。

6 在**强制租用前等待的天数**文本框中，输入部署所有者必须响应回收请求的天数。

这段时间过后，部署将获得一个具有新的租约长度的新租约。最短等待时间为 1 天，最长等待时间为 365 天，默认等待时间为 3 天。

7 在**请求原因**文本框中输入请求的原因。

8 单击**提交**。

9 单击**确定**。

结果

发送回收请求时，该请求会显示在部署所有者的收件箱中。如果所有者在要求的天数内未响应请求，部署将获得一个具有指定长度的新租约，除非当前租约的时间更短。如果所有者单击回收请求上的**正在使用中的项目**，则部署的租约保持不变。如果所有者单击**释放以回收**，则部署租约将立即过期。

后续步骤

[跟踪回收请求](#)。

跟踪回收请求

您可以跟踪回收请求的当前状态和其他详细信息。

以下替代方法可用于检查最近的回收请求：

- 单击**收件箱**选项卡并选择**回收请求**，以查看回收请求信息。
- 单击**回收请求**选项卡并查看最近的请求的列表。
- 单击**部署**以查看最近的部署更改。

前提条件

以**租户管理员**身份登录到 vRealize Automation。

步骤

1 选择**管理 > 回收 > 回收请求**。

2 查找与搜索条件匹配的虚拟机。

- a 单击**高级搜索**向下箭头，打开搜索框。
- b 键入或选择一个或多个搜索值。

选项	操作
虚拟机名称包含	在文本框中键入一个或多个字符以查找匹配的虚拟机名称。
所有者名称包含	在文本框中键入一个或多个字符，查找匹配的所有者名称。
请求原因包含	在文本框中键入一个或多个字符，查找匹配的请求原因。
请求状态	从下拉菜单中选择请求状态值，查找具有匹配请求状态的虚拟机。

- c 单击**搜索**图标 (🔍) 或按 **Enter** 开始搜索。
- d 单击**高级搜索**向上箭头关闭搜索框。

3 （可选）单击**刷新数据**更新显示的回收请求。

更改受管计算机的预留

您可以更改受管计算机的预留或存储设置。当计算机移动到在其当前预留中不可用的新存储路径时，此功能非常有用。对于单个计算机部署，您还可以更改计算机的业务组。

如果某个计算机部署中的计算机的所有者是另一个业务组的成员，则可以将该计算机移动到该目标业务组。要更改业务组设置，您必须是原始业务组和目标业务组的业务组主管。

注 如果为计算机分配了预留策略，则无法更改其业务组。

您可以使用**管理 > 计算资源**菜单选项为相关计算资源创建其他预留。

在 vRealize Automation 中执行“销毁”操作删除已置备的计算机时，通过预留分配给该计算机的存储和内存将会被释放。如果在 vCenter Server 中删除该计算机，存储和内存将不会被释放。

例如，您无法删除与现有部署中的计算机关联的预留。如果您在 vCenter Server 中手动移动或删除了已部署的计算机，vRealize Automation 仍会认为该计算机有效，并阻止您删除关联的预留。

如果更改预留会将 vCenter Server 中的计算机移动到不属于 vRealize Automation 中该计算机预留的新存储路径，请确认更改计算机的预留之前，在计算机的目标预留中选择目标或新的存储路径。

前提条件

以**架构管理员**身份登录到 vRealize Automation。

步骤

- 1 选择**基础架构 > 受管计算机**。
- 2 找到要更改预留的计算机。
- 3 单击下拉菜单中的**更改预留**。

通过单击下拉菜单中的**查看**，可以查看有关受管计算机的信息，例如与其相关的蓝图和计算资源。

- 4 （可选）从**业务组**下拉菜单中选择业务组。
- 5 （可选）从**预留**下拉菜单中选择一个预留。
- 6 （可选）从**存储**下拉菜单中选择一个存储策略。
- 7 单击**确定**。

使用收件箱

收件箱提供目录请求批准、置备过程中请求的交互以及基于任何 vRealize Operations Manager 衡量指标的回收请求状态方面的动态通知。

可以查看每个选项卡，了解是否存在需要执行操作的任何挂起通知。

- **批准**。可以跟踪需要批准的目录请求。如果在某个目录请求中将您指定为审批者，则您可以响应批准请求。请参见[将级别信息添加到批准策略设置](#)。
- **手动用户操作**。某些目录请求需要在置备过程期间进行交互。您可以响应交互请求。请参见 [vRealize Orchestrator 集成至 vRealize Automation](#)。
- **回收请求**。如果使用 vRealize Operations Manager 确定是否可以回收资源，则可以跟踪回收请求。请参见[跟踪回收请求](#)。