

管理 vRealize Automation

2022 年 10 月

vRealize Automation 8.7

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 © 2022 VMware, Inc. 保留所有权利。 版权和商标信息

目录

- 1 管理 vRealize Automation 5**
- 2 管理用户 6**
 - 如何为项目启用 Active Directory 组 7
 - 如何在 vRealize Automation 中移除用户 8
 - 如何在 vRealize Automation 中编辑用户角色 8
 - 如何在 vRealize Automation 中编辑组角色分配 9
 - vRealize Automation 用户角色是什么 9
 - 启用美国国防部通知和同意横幅 19
- 3 维护您的设备 21**
 - 启动和停止 vRealize Automation 21
 - 将 vRealize Automation 从一个节点横向扩展到三个节点 23
 - 为集群 Workspace ONE Access 实例配置反关联性规则和虚拟机组 24
 - 替换 设备节点 24
 - 增加 vRealize Automation 设备的磁盘空间 26
 - 更新 vRealize Automation 的 DNS 分配 26
 - 更改节点或集群的 IP 地址 27
 - 如何启用时间同步 28
 - 如何重置 root 密码 29
- 4 在 vRealize Automation 中使用多组织租户配置 31**
 - 为 vRealize Automation 设置多组织租户 33
 - 管理单节点多组织部署中的证书和 DNS 配置 35
 - 在集群 vRealize Automation 部署下管理证书和 DNS 配置 36
 - 登录到租户并在 vRealize Automation 中添加用户 38
 - 结合使用 vRealize Orchestrator 和 vRealize Automation 多组织部署 39
- 5 使用日志 40**
 - 如何使用日志和日志包 40
 - 如何配置将日志转发到 vRealize Log Insight 43
 - 如何创建或更新 Syslog 集成 47
 - 如何删除用于日志记录的 Syslog 集成 49
 - 如何使用内容包 49
- 6 参与客户体验提升计划 52**
 - 如何加入或退出计划 52

如何配置计划的数据收集时间 53

7 打开产品内置反馈表单 54

管理 vRealize Automation

1

本指南介绍了如何监控和管理 vRealize Automation 部署的关键基础架构和用户管理方面。

本文档中所述的任务对于保持 vRealize Automation 部署正常运行至关重要。这些任务包括用户和组管理以及系统日志监控。

此外，它还介绍了如何配置和管理多组织部署。

虽然某些 vRealize Automation 管理任务在 vRealize Automation 中完成，但其他任务需要使用 vRealize Suite Lifecycle Manager 和 Workspace ONE Access 等相关产品。在完成适用的任务之前，用户应先熟悉这些产品及其功能。

例如，有关备份、还原和灾难恢复的信息，请参见 [vRealize Suite 产品文档的备份和还原以及灾难恢复 > 2019](#) 部分。

注 vRealize Automation 8.0.1 及更高版本支持灾难恢复。

有关使用 vRealize Suite Lifecycle Manager 安装、升级和管理的信息，请参见 [Lifecycle Manager 产品文档](#)。

在 vRealize Automation 中管理用户和组

2

vRealize Automation 使用 VMware Workspace ONE Access (VMware 提供的身份管理应用程序) 导入和管理用户和组。在导入或创建用户和组后, 可以使用“身份与访问管理”页面管理单租户部署的角色分配。

vRealize Automation 通过使用 VMware Lifecycle Manager (vRSLCM 或 LCM) 进行安装。安装 vRealize Automation 时, 必须导入现有的 Workspace ONE Access 实例, 或部署新实例以支持身份管理。这两种方案都会定义管理选项。

- 如果部署新的 Workspace ONE Access 实例, 则可以通过 LCM 管理用户和组。在安装过程中, 可以使用 Workspace ONE Access 设置 Active Directory 连接。或者, 您也可以按本文中所述使用“身份与访问管理”页面查看和编辑 vRealize Automation 中用户和组的某些方面。
- 如果使用现有的 Workspace ONE Access 实例, 则可以将其导入, 以便在安装过程中通过 LCM 将其用于 vRealize Automation。在这种情况下, 您可以继续使用 Workspace ONE Access 管理用户和组, 也可以使用 LCM 中的管理功能。

有关在多组织部署下管理用户的详细信息, 请参见[登录到租户并在 vRealize Automation 中添加用户](#)。

必须为 vRealize Automation 用户分配角色。角色定义了对应用程序中功能的访问权限。当 vRealize Automation 安装有 Workspace ONE Access 实例时, 将创建一个默认组织, 并为安装者分配“组织所有者”角色。所有其他 vRealize Automation 角色均由组织所有者分配。

vRealize Automation 中有三种类型的角色: 组织角色、服务角色和项目角色。对于 Cloud Assembly、Service Broker 和 Code Stream, 通常情况下, 用户级别角色可以使用资源, 而创建和配置资源则需要管理员级别角色。组织角色定义租户中的权限; 组织所有者具有管理员级别权限, 而组织成员具有用户级别权限。组织所有者可以添加和管理其他用户。

组织角色	服务角色
■ 组织所有者	■ Cloud Assembly 管理员
■ 组织成员	■ Cloud Assembly 用户
	■ Cloud Assembly 查看者
	■ Service Broker 管理员
	■ Service Broker 用户
	■ Service Broker 查看者
	■ Code Stream 管理员
	■ Code Stream 用户
	■ Code Stream 查看者

此外，该表中未显示两个主要项目级别角色：项目管理员和项目用户。这些角色针对每个项目通过 Cloud Assembly 临时分配。这些角色有些不固定。同一个用户可以是一个项目的管理员，也可以是另一个项目的用户。有关详细信息，请参见 [vRealize Automation 用户角色是什么](#)。

有关使用 vRealize Suite Lifecycle Manager 和 Workspace ONE Access 的详细信息，请参见以下内容。

本章讨论了以下主题：

- [如何在 vRealize Automation 中为项目启用 Active Directory 组](#)
- [如何在 vRealize Automation 中移除用户](#)
- [如何在 vRealize Automation 中编辑用户角色](#)
- [如何在 vRealize Automation 中编辑组角色分配](#)
- [vRealize Automation 用户角色是什么](#)
- [启用美国国防部通知和同意横幅](#)

如何在 vRealize Automation 中为项目启用 Active Directory 组

如果在将用户添加到项目时某组在“添加组”页面上不可用，请检查“身份与访问管理”页面并添加该组（如果可用）。如果在 vRealize Automation 的“身份与访问管理”页面中未列出该组，则该组可能不会在 Workspace ONE Access 实例中同步。您可以验证它是否已同步，然后使用此过程添加组，如下所示。

要将 Active Directory 组的成员添加到项目中，必须确保该组与 Workspace ONE Access 实例同步，并且该组已添加到组织中。

前提条件

如果这些组未同步，则当您尝试将它们添加到项目时，这些组不可用。验证您已将 Active Directory 组与 Lifecycle Manager 实例同步。

步骤

- 1 以要添加的同一 Active Directory 域中的用户身份登录到 vRealize Automation。例如，@mycompany.com
- 2 在 Cloud Assembly 中，单击标题右侧导航中的“身份与访问管理”。
- 3 单击**企业组**，然后单击**分配角色**。
- 4 使用搜索功能查找您要添加的组并将其选中。
- 5 分配组织角色。

该组必须至少具有“组织成员”角色。有关详细信息，请参见 [vRealize Automation Cloud Assembly 用户角色是什么](#)。

- 6 单击**添加服务访问权限**，添加一个或多个服务，然后为每个服务选择一个角色。
- 7 单击**分配**。

结果

现在，您可以将 Active Directory 组添加到项目中。

如何在 vRealize Automation 中移除用户

可以根据需要在 vRealize Automation 中移除用户。

默认情况下会列出所有用户，您无法使用“身份与访问管理”页面添加用户。可以删除用户。

步骤

- 1 在“身份与访问管理”页面上选择“活动用户”选项卡。
- 2 找到并选择要删除的用户。
- 3 单击**移除用户**。

结果

将移除选定用户。

如何在 vRealize Automation 中编辑用户角色

您可以编辑分配给已导入到 vRealize Automation 的 Workspace ONE Access 用户的角色。

前提条件

步骤

- 1 在 Cloud Assembly 中，单击标题右侧导航中的“身份与访问管理”。
- 2 在“活动用户”选项卡上选择所需的用户，然后单击**编辑角色**。

- 3 您可以编辑用户的组织角色和服务角色。
 - 选择“分配组织角色”标题旁边的下拉列表，以更改用户与组织的关系。
 - 单击“添加服务访问权限”以为用户添加新的服务角色。
 - 要移除用户角色，单击适用服务旁边的 X。
- 4 单击**保存**。

结果

用户角色分配将按指定的方式更新。

如何在 vRealize Automation 中编辑组角色分配

您可以在 vRealize Automation 中编辑组的角色分配

前提条件

用户和组已从与您的 vRealize Automation 部署关联的有效 vIDM 实例中导入。

步骤

- 1 在 Cloud Assembly 中，单击标题右侧导航中的“身份与访问管理”。
- 2 选择“企业组”选项卡。
- 3 在搜索字段中，键入要为其编辑角色分配的组的名称。
- 4 编辑所选组的角色分配。您有两个选项。
 - 分配组织角色
 - 分配服务角色
- 5 单击**分配**。

结果

角色分配将按指定的方式更新。

vRealize Automation 用户角色是什么

作为组织所有者，您可以为用户分配组织角色和服务角色。角色决定了用户可以执行的操作或查看的内容。然后，在服务中，服务管理员可以分配项目角色。要确定要分配的角色，请评估下表中的任务。

Cloud Assembly 服务角色

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

表 2-1. Cloud Assembly 服务角色说明

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

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

项目角色是在 Cloud Assembly 中定义的，可能会因项目而异。

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

项目角色说明可帮助您决定为用户提供哪些权限。

- 项目管理员利用服务管理员创建的基础架构来确保项目成员具有进行开发工作所需的资源。
- 项目成员在其项目中工作，以设计和部署云模板。在下表中，您的项目只能包含您拥有的资源或与其他项目成员共享的资源。
- 项目查看者仅具有只读访问权限，但在某些情况下，他们可以执行诸如下载云模板之类的非破坏性操作。
- 项目主管是 Service Broker 中批准策略定义了项目主管审批者的项目的审批者。要向主管提供批准上下文，还应考虑授予他们项目成员或查看者角色。

表 2-2. Cloud Assembly 服务角色和项目角色

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

表 2-2. Cloud Assembly 服务角色和项目角色 (续)

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

表 2-2. Cloud Assembly 服务角色和项目角色 (续)

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。			
				项目管理员	项目成员	项目查看者	项目主管
	查看发现的计算资源	是	是				
资源 - 网络	修改网络标记、IP 范围、IP 地址	是					
	查看发现的网络资源	是	是				
资源 - 安全	将标记添加到已发现的安全组	是					
	查看已发现的安全组	是	是				
资源 - 存储	向发现的存储中添加标记	是					
	查看存储	是	是				
资源 - Kubernetes	部署或添加 Kubernetes 集群，以及创建或添加命名空间	是					
	查看 Kubernetes 集群和命名空间	是	是	是。您的项目	是。您的项目	是。您的项目	
活动 - 请求	删除部署请求记录	是					
	查看部署请求记录	是	是	是。您的项目	是。您的项目	是。您的项目	
活动 - 事件日志	查看事件日志	是	是	是。您的项目	是。您的项目	是。您的项目	
连接 - 云帐户	创建、更新或删除云帐户	是					
	查看云帐户	是	是				
连接 - 集成	创建、更新或删除集成	是					
	查看集成	是	是				
载入	创建、更新或删除载入计划	是					
	查看载入计划	是	是				是。您的项目
可扩展性							
	查看并打开“可扩展性”选项卡	是	是				是
事件	查看可扩展性事件	是	是				
订阅	创建、更新或删除可扩展性订阅	是					
	停用订阅	是					
	查看订阅	是	是				

表 2-2. Cloud Assembly 服务角色和项目角色 (续)

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。			
				项目管理员	项目成员	项目查看者	项目主管
库 - 事件主题	查看事件主题	是	是				
库 - 操作	创建、更新或删除可扩展性操作	是					
	查看可扩展性操作	是	是				
库 - 工作流	查看可扩展性工作流	是	是				
活动 - 操作运行	取消或删除可扩展性操作运行	是					
	查看可扩展性操作运行	是	是			是。您的项目	
活动 - 工作流运行	查看可扩展性工作流运行	是	是				
设计							
设计	打开“设计”选项卡	是	是	是。	是。	是。	是
云模板	创建、更新和删除云模板	是		是。您的项目	是。您的项目		
	查看云模板	是	是	是。您的项目	是。您的项目	是。您的项目	
	下载云模板	是	是	是。您的项目	是。您的项目	是。您的项目	
	上载云模板	是		是。您的项目	是。您的项目		
	部署云模板	是		是。您的项目	是。您的项目		
	版本控制和还原云模板	是		是。您的项目	是。您的项目		
	将云模板发布到目录	是		是。您的项目	是。您的项目		
	自定义资源	创建、更新或删除自定义资源	是				
	查看自定义资源	是	是	是。您的项目	是。您的项目	是。您的项目	
自定义操作	创建、更新或删除自定义操作	是					
	查看自定义操作	是	是	是。您的项目	是。您的项目	是。您的项目	
资源							
	查看并打开“资源”选项卡	是	是	是	是	是	是

表 2-2. Cloud Assembly 服务角色和项目角色 (续)

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。			
				项目管理员	项目成员	项目查看者	项目主管
部署	查看部署, 包括部署详细信息、部署历史记录、价格、监控、警示、优化和故障排除信息	是	是	是。您的项目	是。您的项目	是。您的项目	
	管理警示	是		是。您的项目	是。您的项目		
	基于策略对部署运行实施后操作	是		是。您的项目	是。您的项目		
资源 - 所有资源	查看所有发现的资源	是	是				
	对已发现的资源运行实施后操作。 操作仅适用于计算机, 仅限于打开和关闭所有计算机的电源, 以及 vSphere 计算机的远程控制台。	是					
资源 - 所有资源	查看已部署、已载入、已迁移的资源	是	是	是。您的项目。	是。您的项目。	是。您的项目。	
	根据策略对已部署、已载入和已迁移的资源运行实施后操作	是	是	是。您的项目。	是。您的项目。		
资源 - 虚拟机	查看发现的计算机	是	是				
	对已发现的计算机运行实施后操作。 操作仅限于打开和关闭电源以及 vSphere 计算机的远程控制台。	是					
	创建新的虚拟机	是					
	查看已部署、已载入和已迁移的资源。	是		是。您的项目。	是。您的项目。	是。您的项目。	
	根据策略对已部署、已载入和已迁移的资源运行实施后操作	是		是。您的项目。	是。您的项目。		
资源 - 卷	查看已发现的卷	是	是				
	没有可用的实施后操作						
	查看已部署、已载入和已迁移的卷	是	是	是。您的项目。	是。您的项目。	是。您的项目。	

表 2-2. Cloud Assembly 服务角色和项目角色（续）

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。			
				项目管理员	项目成员	项目查看者	项目主管
	根据策略对已部署、已载入和已迁移的卷运行实施后操作	是		是。您的项目。	是。您的项目。		
资源 - 网络和安全	查看发现的网络、负载均衡器和安全组	是	是				
	没有可用的实施后操作						
	查看已部署、已载入和已迁移的网络、负载均衡器和安全组	是	是	是。您的项目。	是。您的项目。	是。您的项目。	
	根据策略对已部署、已载入和已迁移的网络、负载均衡器和安全组运行实施后操作	是		是。您的项目。	是。您的项目。		
警示							
	查看并打开“警示”选项卡	是	是	是	是	是	
	管理警示	是		是。您的项目	是。您的项目		
	查看警示	是	是	是。您的项目	是。您的项目	是。您的项目	

Service Broker 服务角色

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

表 2-3. Service Broker 服务角色说明

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

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

项目角色是在 Service Broker 中定义的，可能会因项目而异。

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

在您决定为用户提供哪些权限时，可以使用以下项目角色描述为您提供帮助。

- 项目管理员利用服务管理员创建的基础架构来确保项目成员具有进行开发工作所需的资源。
- 项目成员在其项目中工作，以设计和部署云模板。在下表中，您的项目只能包含您拥有的资源或与其他项目成员共享的资源。
- 项目查看者仅限于只读访问权限。
- 项目主管是 Service Broker 中批准策略定义了项目主管审批者的项目的审批者。要向主管提供批准上下文，还应考虑授予他们项目成员或查看者角色。

表 2-4. Service Broker 服务角色和项目角色

UI 上下文	任务	Service Broker 管理员	Service Broker 查看者	Service Broker 用户			
				用户必须是项目管理员才能查看和执行项目相关任务。			
				项目管理 员	项目成员	项目查看者	项目主管
访问 Service Broker							
控制台	在控制台中，您可以查看和打开 Service Broker	是	是	是	是	是	是
基础架构							
	查看并打开“基础架构”选项卡	是	是				
配置 - 项目	创建项目	是					
	更新或删除项目摘要、置备、Kubernetes、集成和测试项目配置中的值。	是					
	在项目中添加用户和组并分配角色。	是		是。您的项目。			
	查看项目	是	是	是。您的项目	是。您的项目	是。您的项目	
配置 - 云区域	创建、更新或删除云区域	是					
	查看云区域	是	是				
配置 - Kubernetes 区域	创建、更新或删除 Kubernetes 区域	是					
	查看 Kubernetes 区域	是	是				
连接 - 云帐户	创建、更新或删除云帐户	是					

表 2-4. Service Broker 服务角色和项目角色 (续)

UI 上下文	任务	Service Broker 管理员	Service Broker 查看者	Service Broker 用户			
				用户必须是项目管理员才能查看和执行项目相关任务。			
				项目管理 员	项目成员	项目查 看者	项目主 管
	查看云帐户	是	是				
连接 - 集成	创建、更新或删除集成	是					
	查看集成	是	是				
活动 - 请求	删除部署请求记录	是					
	查看部署请求记录	是					
活动 - 事件日志	查看事件日志	是					
内容和策略							
	查看并打开“内容和策略”选项卡	是	是				
内容源	创建、更新或删除内容源	是					
	查看内容源	是	是				
内容共享	添加或移除共享内容	是					
	查看共享内容	是	是				
内容	自定义表单和配置项目	是					
	查看内容	是	是				
策略 - 定义	创建、更新或删除策略定义	是					
	查看策略定义	是	是				
策略 - 实施	查看实施日志	是	是				
通知 - 电子邮件服务器	配置电子邮件服务器	是					
目录							
	查看并打开“目录”选项卡	是	是	是	是	是	是
	查看可用目录项	是	是	是。您的项目	是。您的项目	是。您的项目	
	请求目录项	是		是。您的项目	是。您的项目		
资源							
	查看并打开“资源”选项卡	是	是	是。	是	是	是

表 2-4. Service Broker 服务角色和项目角色 (续)

UI 上下文	任务	Service Broker 管理员	Service Broker 查看者	Service Broker 用户 用户必须是项目管理员才能查看和执行项目相关任务。			
				项目管理 员	项目成员	项目查看者	项目主管
部署	查看部署, 包括部署详细信息、部署历史记录、价格、监控、警示、优化和故障排除信息	是	是	是。您的项目	是。您的项目	是。您的项目	
	管理警示	是		是。您的项目	是。您的项目		
	基于策略对部署运行实施后操作	是		是。您的项目	是。您的项目		
资源 - 所有资源	查看所有发现的资源	是	是				
	对已发现的资源运行实施后操作。操作仅适用于计算机, 仅限于打开和关闭所有计算机的电源, 以及 vSphere 计算机的远程控制台。	是					
资源 - 所有资源	查看已部署、已载入、已迁移的资源	是	是	是。您的项目。	是。您的项目。	是。您的项目。	
	根据策略对已部署、已载入和已迁移的资源运行实施后操作	是	是	是。您的项目。	是。您的项目。		
资源 - 虚拟机	查看发现的计算机	是	是				
	对已发现的计算机运行实施后操作。操作仅限于打开和关闭电源以及 vSphere 计算机的远程控制台。	是					
	创建新的虚拟机	是					
	查看已部署、已载入和已迁移的资源。	是		是。您的项目。	是。您的项目。	是。您的项目。	
	根据策略对已部署、已载入和已迁移的资源运行实施后操作	是		是。您的项目。	是。您的项目。		
资源 - 卷	查看已发现的卷	是	是				
	没有可用的实施后操作						
	查看已部署、已载入和已迁移的卷	是	是	是。您的项目。	是。您的项目。	是。您的项目。	
	根据策略对已部署、已载入和已迁移的卷运行实施后操作	是		是。您的项目。	是。您的项目。		
资源 - 网络和安全	查看发现的网络、负载均衡器和安全组	是	是				

表 2-4. Service Broker 服务角色和项目角色 (续)

UI 上下文	任务	Service Broker 管理员	Service Broker 查看者	Service Broker 用户			
				用户必须是项目管理员才能查看和执行项目相关任务。			
				项目管理 员	项目成员	项目查 看者	项目主 管
没有可用的实施后操作							
	查看已部署、已载入和已迁移的网络、负载均衡器和安全组	是	是	是。您的项目。	是。您的项目。	是。您的项目。	
	根据策略对已部署、已载入和已迁移的网络、负载均衡器和安全组运行实施后操作	是		是。您的项目。	是。您的项目。		
批准							
	查看并打开“批准”选项卡	是	是	是	是	是	是
	响应批准请求	是		是。您的项目和策略审批者是项目管理员	仅当您是指定审批者时	仅当您是指定审批者时	是。您的项目和策略审批者是项目主管

启用美国国防部通知和同意横幅

对于某些政府客户，管理员必须在 Workspace ONE Access 中配置标准美国国防部 (DoD) 通知和同意横幅，用户才能访问 vRealize Automation。

“标准强制性 DoD 通知和同意横幅”文本如下所示：

您正在访问的美国政府 (USG) 信息系统 (IS) 仅由 USG 授权使用。使用此 IS (包括连接到此 IS 的任何设备) 即表示您同意以下条件：

- USG 会定期截获和监控此 IS 上的通信，以用于各种目的，包括但不限于：渗透测试、COMSEC 监控、网络操作和防御、人员不当行为 (PM)、法律实施 (LE) 和反间谍 (CI) 调查。
- USG 可随时检查并获取存储在此 IS 上的数据。
- 使用此 IS 进行通信或存储在此 IS 上的数据不受隐私保护，会定期进行监控、截获和搜索，并且可能会出于任何 USG 授权目的而进行披露或使用。

以下步骤介绍了如何在 Workspace ONE Access 中配置此横幅。有关详细信息，请参阅 Workspace ONE Access 管理控制台文档。

步骤

- 1 以管理员身份登录到 Workspace ONE 管理控制台。
- 2 在 VMware Identity Manager 控制台中，单击“身份和访问管理”选项卡。

- 3 单击“设置”，然后单击“连接器”选项卡。
- 4 单击要配置的每个连接器对应的 Worker 链接。
- 5 单击“身份验证适配器”选项卡，然后单击 CertificateAuthAdapter。
- 6 单击“身份验证前启用同意表单”复选框。
- 7 将“标准强制性 DoD 通知和同意横幅”文本粘贴到“同意表单内容”框中。
- 8 保存更改。

结果

维护您的 vRealize Automation 设备

3

作为系统管理员，您可能需要执行各种任务以确保已安装的 vRealize Automation 应用程序正常运行。

如果您刚刚开始使用 vRealize Automation，则不需要执行这些任务。如果您需要解决性能问题或产品行为问题，了解如何执行这些任务对您很有帮助。

本章讨论了以下主题：

- 启动和停止 vRealize Automation
- 将 vRealize Automation 从一个节点横向扩展到三个节点
- 为集群 Workspace ONE Access 实例配置反关联性规则和虚拟机组
- 替换 vRealize Automation 设备节点
- 增加 vRealize Automation 设备的磁盘空间
- 更新 vRealize Automation 的 DNS 分配
- 更改 vRealize Automation 节点或集群的 IP 地址
- 如何启用 vRealize Automation 的时间同步
- 如何重置 vRealize Automation 的 root 密码

启动和停止 vRealize Automation

启动或关闭 vRealize Automation 时，请遵守正确的过程。

要关闭和启动 vRealize Automation 组件，建议使用 vRealize Suite Lifecycle Manager 的**生命周期操作 > 环境**部分中提供的“关闭电源”和“打开电源”功能。以下过程概述了关闭和启动 vRealize Automation 组件的手动方法，以防 vRealize Suite Lifecycle Manager 由于某种原因而不可用。

关闭 vRealize Automation

为保持数据完整性，请先关闭 vRealize Automation 服务，再关闭虚拟设备电源。使用 SSH 或 VMRC，可以关闭或启动任何单个设备中的所有节点。

注 请尽一切可能避免使用 `vracli reset vidm` 命令。此命令会重置 Workspace ONE Access 的所有配置，并中断用户与已置备资源之间的关联。

- 1 使用 SSH 或 VMRC 登录到任何 vRealize Automation 设备的控制台。
- 2 要关闭所有集群节点上的 vRealize Automation 服务，请运行以下命令集。

注 如果您将其中的任何命令复制到运行，但运行失败，请先将其粘贴到记事本中，然后在运行之前重新复制它们。此过程会去除文档源中可能存在的任何隐藏字符和其他工件。

```
/opt/scripts/deploy.sh --shutdown
```

- 3 关闭 vRealize Automation 设备。

现在，您的 vRealize Automation 部署已关闭。

启动 vRealize Automation

在意外关机、受控关机或恢复过程后，必须按特定顺序重新启动 vRealize Automation 组件。vRLCM 是一个非关键组件，因此可以随时启动该组件。必须先启动 VMware Workspace ONE Access（以前称为 VMware Identity Management）组件，然后再启动 vRealize Automation。

注 在启动 vRealize Automation 组件之前，请确认适用的负载均衡器正在运行。

- 1 打开所有 vRealize Automation 设备的电源，并等待它们启动。
- 2 使用 SSH 或 VMRC 登录到任何设备的控制台，并运行以下命令，以在所有节点上还原服务。

```
/opt/scripts/deploy.sh
```

- 3 执行以下命令，验证所有服务是否均已启动且正在运行。

```
kubectl get pods --all-namespaces
```

注 您应看到每个服务有三个实例，并且这些实例应处于“正在运行”或“已完成”状态。

当所有服务均列为“正在运行”或“已完成”时，vRealize Automation 可以立即使用。

重新启动 vRealize Automation

可以从集群中的任何设备集中重新启动所有 vRealize Automation 服务。按照上述说明关闭 vRealize Automation，然后按照说明启动 vRealize Automation。重新启动 vRealize Automation 之前，确认所有适用的负载均衡器和 VMware Workspace ONE Access 组件正在运行。

当所有服务均列为“正在运行”或“已完成”时，vRealize Automation 可以立即使用。

运行以下命令，验证所有服务是否都正在运行：

```
kubectl -n prelude get pods
```

将 vRealize Automation 从一个节点横向扩展到三个节点

随着需求扩增，可以将 vRealize Automation 部署从一个节点横向扩展到三个节点。

必须使用 vRealize Suite Lifecycle Manager 的功能完成此过程的多个步骤。有关使用 vRealize Suite Lifecycle Manager 安装、升级和管理的信息，请参见 [Lifecycle Manager 产品文档](#)。

如果使用的是三节点集群部署，vRealize Automation 通常可以承受一个节点出现故障而仍能正常运行。三节点集群中的两个节点出现故障将导致 vRealize Automation 无法正常运行。

前提条件

此过程假设您已具有正常运行的单节点 vRealize Automation 部署。

步骤

- 1 关闭所有 vRealize Automation 设备。

要关闭所有集群节点上的 vRealize Automation 服务，请运行以下命令集。

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

现在，可以关闭 vRealize Automation 设备。

- 2 生成部署快照。

使用 vRealize Suite Lifecycle Manager [生命周期操作 > 环境 > vRA > 查看详细信息](#) 中的“创建快照”选项。

注 从 8.0.1 开始，支持无需关闭 vRealize Automation 节点即可生成联机快照。对于 vRealize Automation 8.0 环境，必须先停止 vRealize Automation 节点。

- 3 打开 vRealize Automation 设备的电源，并启动所有容器。
- 4 使用位于 vRealize Suite Lifecycle Manager 的 [LCM > Locker > 证书](#) 中的 Locker 功能，为所有组件生成或导入 vRealize Automation 证书，包括 vRealize Suite Lifecycle Manager 节点 FQDN 和 vRealize Automation 负载均衡器完全限定域名。
在“主体备用名称”中添加全部三个设备的名称。
- 5 将新证书导入到 vRealize Suite Lifecycle Manager。
- 6 通过使用 LCM [生命周期操作 > 环境 > vRA > 查看详细信息](#) 中的“替换证书”选项，将现有 vRealize Suite Lifecycle Manager 证书替换为上一步中生成的证书。

7 通过使用 **LCM > 生命周期操作 > 环境 > vRA > 查看详细信息** 中的“添加组件”选项将 vRealize Automation 横向扩展到三个节点。

结果

vRealize Automation 已扩展为三节点部署。

为集群 Workspace ONE Access 实例配置反关联性规则和虚拟机组

如果 vRealize Automation 环境使用集群 Workspace ONE Access 实例，请创建反关联性规则和计算机集群，以确保正确的 vSphere High Availability workflow。

要防止任何集群 Workspace ONE Access 节点发生主机级别故障，请配置反关联性规则以运行默认 vSphere 管理集群中不同主机上的虚拟机。创建反关联性规则后，请配置虚拟机组以定义所需的计算机启动顺序。通过使用定义的计算机启动顺序，可以确保 vSphere High Availability 按照您环境的正确顺序打开集群 Workspace ONE Access 节点的电源。

有关如何配置反关联性规则和虚拟机组的信息，请参见 [VMware Cloud Foundation 产品文档](#) 中的 [为集群 Workspace ONE Access 实例配置反关联性规则和虚拟机组](#)。

从一个 vRealize Automation 版本升级到另一个版本时的关联性规则注意事项

vRealize Suite Lifecycle Manager 对 vRealize Automation 8.x 不支持反关联性规则。由于 vRealize Suite Lifecycle Manager 在 vRealize Automation 升级期间由 vRealize Easy Installer 使用，并且在升级期间没有特定的关闭和打开 vRealize Automation 节点电源的顺序，因此，如果使用的顺序与定义关闭和打开计算机电源的顺序的关联性规则冲突，则可能会出现这个问题。使用 vRealize Suite Lifecycle Manager 或 vRealize Easy Installer 从一个 vRealize Automation 版本升级到另一个版本时，请在开始升级之前禁用关联性规则。

有关如何从一个 vRealize Automation 版本升级到另一个版本的信息，请参见 [vRealize Automation 产品文档](#) 中的 [使用 vRealize Easy Installer 安装 vRealize Automation](#)。

替换 vRealize Automation 设备节点

多站点、高可用性 (HA) 配置中的某个 vRealize Automation 设备失败时，可能需要替换故障节点。

小心 继续操作之前，VMware 建议联系技术支持人员以对 HA 问题进行故障排除，并确认问题已隔离到一个节点上。

如果技术支持人员确定需要替换节点，请执行以下步骤。

- 1 在 vCenter 中，为 HA 配置中的每个设备生成备份快照。
在备份快照中，不包括虚拟机内存。
- 2 关闭出现故障的节点。

- 3 记下故障节点的 vRealize Automation 软件内部版本号和网络设置。

记下 FQDN、IP 地址、网关、DNS 服务器，尤其是 MAC 地址。稍后，您需要将相同的值分配给替换节点。

- 4 主数据库节点必须为正常节点之一。按照以下步骤操作：

- a 以 root 用户登录正常节点的命令行。
- b 通过运行以下命令查找主数据库节点的名称。

```
vracli status | grep primary -B 1
```

结果应类似于以下示例，其中 **postgres-1** 是主数据库节点。

```
"Conninfo":
"host=postgres-1.postgres.prelude.svc.cluster.local
dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
connect_timeout=10",
"Role": "primary",
```

- c 运行以下命令，验证主数据库节点是否正常。

```
kubectl -n prelude get pods -o wide | grep postgres
```

结果应类似于以下示例，其中 **postgres-1** 包含在列表中，并显示为正在运行且正常。

```
postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
```

重要说明 如果主数据库节点出现故障，请与技术支持人员联系，而不是继续操作。

- 5 从正常节点的根命令行中，移除故障节点。

```
vracli cluster remove faulty-node-FQDN
```

- 6 使用 vCenter 部署新的替换 vRealize Automation 节点。

部署相同的 vRealize Automation 内部版本号，并应用故障节点的网络设置。包括 FQDN、IP 地址、网关、DNS 服务器，尤其是前面记录的 MAC 地址。

- 7 打开替换节点的电源。
- 8 以 root 用户登录替代节点的命令行。
- 9 运行以下命令，验证初始引导顺序是否已完成。

```
vracli status first-boot
```

查找 `First boot complete` 消息。

- 10 从替换节点中，加入 vRealize Automation 集群。

```
vracli cluster join primary-DB-node-FQDN
```

- 11 以 root 用户登录主数据库节点的命令行。
- 12 通过运行以下脚本部署已修复的群集。

```
/opt/scripts/deploy.sh
```

增加 vRealize Automation 设备的磁盘空间

您可能需要增加 vRealize Automation 设备的磁盘空间以用于日志文件存储等用途。

步骤

- 1 使用 vSphere 扩展 vRealize Automation 设备上的 VMDK。
- 2 以 root 用户身份登录到 vRealize Automation 设备的命令行。
- 3 在命令提示符处，运行以下 vRealize Automation 命令。

```
vracli disk-mgr resize
```

如果 vRealize Automation 大小调整失败，请参见知识库文章 [79925](#)。

更新 vRealize Automation 的 DNS 分配

管理员可以更新 vRealize Automation 的 DNS 分配。

步骤

- 1 使用 SSH 或 VMRC 登录到任何 vRealize Automation 设备的控制台。
- 2 运行以下命令。

```
vracli network dns set --servers DNS1,DNS2
```

- 3 使用 `vracli network dns status` 命令验证新的 DNS 服务器是否已正确应用于所有 vRealize Automation 节点。
- 4 运行以下命令集，关闭所有集群节点上的 vRealize Automation 服务。

```
/opt/scripts/svc-stop.sh  
sleep 120  
/opt/scripts/deploy.sh --onlyClean
```

- 5 重新启动 vRealize Automation 节点并等待它们完全启动。
- 6 使用 SSH 登录到每个 vRealize Automation 节点，并验证是否在 `/etc/resolv.conf` 中列出了新的 DNS 服务器。
- 7 在其中一个 vRealize Automation 节点上，运行以下命令以启动 vRealize Automation 服务：`/opt/scripts/deploy.sh`

结果

vRealize Automation DNS 设置将按指定的内容进行更改。

更改 vRealize Automation 节点或集群的 IP 地址

您可以更改 vRealize Automation 节点或集群的 IP 地址。

例如，您可能希望将部署的 vRealize Automation 环境迁移到更方便的 vCenter 或支持 vRealize Automation 故障切换。

作为 vRealize Automation 管理员，您可以使用以下过程为 vRealize Automation 节点或集群设置新的 IP 地址，然后将服务重新部署到新的 IP 地址。

注 在继续更改 vRealize Automation 节点或集群的 IP 之前，必须先确认该节点或集群处于正常状态。尝试在处于不正常状态的节点或集群上运行此过程可能会导致非常难以解决的问题。

在此过程中，您将以特定顺序重新启动 vRealize Automation。有关关闭和重新启动 vRealize Automation 的相关信息，请参见[启动和停止 vRealize Automation](#)。

- 1 使用以下命令验证 vRealize Automation 节点或集群是否处于正常状态。

```
vracli service status
```

- 2 vRealize Automation 处于正常状态时，请使用以下命令设置节点或集群设备的备用 IP。

```
vracli network alternative-ip set --dns DNSIPAddress1,DNSIPAddress2 IPV4_address  
Gateway_IPV4_address
```

如果使用的是集群，请设置集群中每个适用节点的备用 IP。

- 3 使用以下命令关闭服务。

```
/opt/scripts/deploy.sh - shutdown
```

- 4 如果需要，请执行 vRealize Automation 故障切换或迁移操作。请参见有关 [VMware Site Recovery Manager](#) 的信息以及您自己的内部过程和实践。
- 5 使用以下命令更改 vRealize Automation 的 IP。

```
vracli network alternative-ip swap
```

如果使用的是 vRealize Automation 集群，则必须更改集群中每个节点的 IP 地址。

- 6 使用以下命令重新引导 vRealize Automation。

```
shutdown -r now
```

如果使用的是 vRealize Automation 集群，则必须重新引导集群中的每个节点。

- 7 使用以下命令重新部署 vRealize Automation 服务。

```
/opt/scripts/deploy.sh
```

重新引导 vRealize Automation 且重新部署的服务正在运行后，vRealize Automation 应在新的 IP 地址上可用。

如何启用 vRealize Automation 的时间同步

可以使用 vRealize Automation 设备命令行在 vRealize Automation 部署上启用时间同步。

可以使用网络时间协议 (NTP) 网络协议为独立或集群 vRealize Automation 部署配置时间同步。vRealize Automation 支持两个互斥的 NTP 配置：

NTP 配置	说明
ESXi	<p>当托管 vRealize Automation 的 ESXi 服务器与 NTP 服务器同步时，可以使用此配置。如果使用的是集群部署，则所有 ESXi 主机都必须与 NTP 服务器同步。有关为 ESXi 配置 NTP 的详细信息，请参见知识库文章 57147 使用 vSphere Web Client 在 ESXi 主机上配置网络时间协议 (NTP)。</p> <p>注 如果 vRealize Automation 部署迁移到与 NTP 服务器不同步的 ESXi 主机，可能会遇到时钟偏移问题。</p>
systemd	<p>此配置使用 systemd-timesyncd 守护进程同步 vRealize Automation 部署的时钟。</p> <p>注 默认情况下，systemd-timesyncd 守护进程处于启用状态，但未配置 NTP 服务器。如果 vRealize Automation 设备使用动态 IP 配置，则设备可以使用通过 DHCP 协议接收的任何 NTP 服务器。</p>

步骤

- 1 以 **root** 用户身份登录到 vRealize Automation 设备命令行。
- 2 对 ESXi 启用 NTP。
 - a 运行 `vracli ntp esxi` 命令。
 - b （可选）要确认 NTP 配置的状态，请运行 `vracli ntp status` 命令。
您也可以运行 `vracli ntp reset` 命令，将 NTP 配置重置为默认状态。
- 3 对 systemd 启用 NTP。
 - a 运行 `vracli ntp systemd --set FQDN_or_IP_of_systemd_server` 命令。

注 可以添加多个 systemd NTP 服务器，用逗号分隔其网络地址即可。每个网络地址都必须放在单引号内。例如，`vracli ntp systemd --set 'ntp_address_1','ntp_address_2'`

- b （可选）要确认 NTP 配置的状态，请运行 `vracli ntp status` 命令。

结果

为 vRealize Automation 设备部署启用了时间同步。

后续步骤

如果 NTP 服务器和 vRealize Automation 部署之间的时间差超过 10 分钟，则 NTP 配置可能会失败。要解决此问题，请重新引导 vRealize Automation 设备。

如何重置 vRealize Automation 的 root 密码

您可以重置丢失或忘记的 vRealize Automation root 密码。

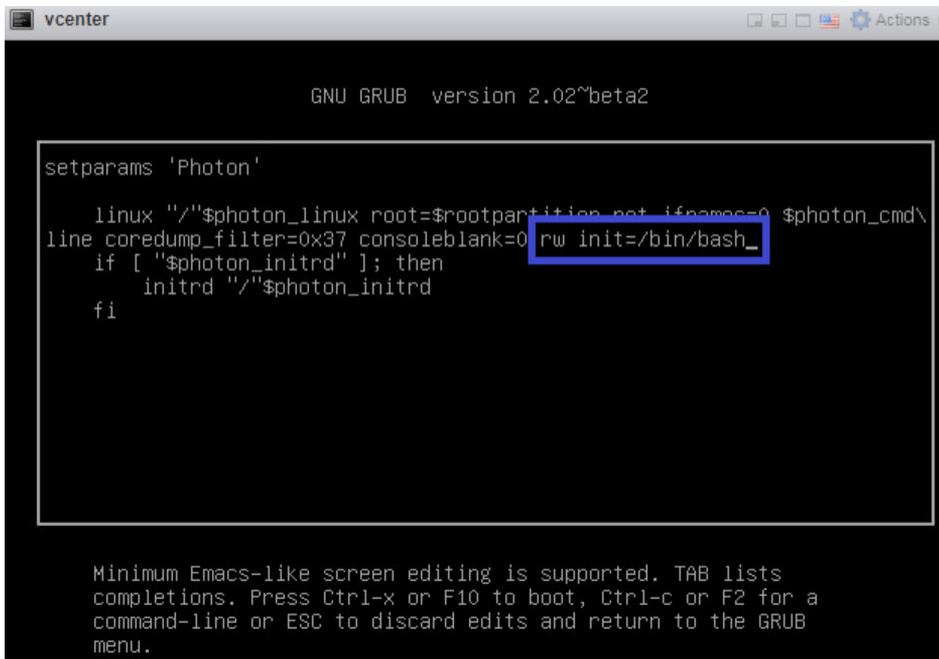
在此过程中，您将在主机 vCenter Appliance 上使用命令行窗口来重置您组织的 vRealize Automation root 密码。

前提条件

此过程适用于 vRealize Automation 管理员，需要使用访问主机 vCenter Appliance 所需的凭据。

步骤

- 1 使用启动和停止 vRealize Automation 中所述的步骤关闭并启动 vRealize Automation。
- 2 当 Photon 操作系统命令行窗口出现时，输入 e，然后按 **Enter** 键以打开 GNU GRUB 引导菜单编辑器。
- 3 在 GNU GRUB 编辑器中，在以 `linux "/" $photon_linux root=rootpartition` 开头的行末尾输入 `rw init=/bin/bash`，如下所示：



```

vcenter
GNU GRUB version 2.02~beta2

setparams 'Photon'

linux "/"$photon_linux root=$rootpartition not ifnames=0 $photon_cmd\
line coredump_filter=0x37 consoleblank=0 rw init=/bin/bash_
if [ "$photon_initrd" ]; then
  initrd "/"$photon_initrd
fi

Minimum Emacs-like screen editing is supported. TAB lists
completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for a
command-line or ESC to discard edits and return to the GRUB
menu.

```

- 4 按 **F10** 键以推送更改并重新启动 vRealize Automation。
- 5 等待 vRealize Automation 重新启动。
- 6 在 `root [/]#` 提示符处，输入 `passwd`，然后按 **Enter** 键。
- 7 在 `New password:` 提示符处，输入新密码，然后按 **Enter** 键。
- 8 在 `Retype new password:` 提示符处，重新输入新密码，然后按 **Enter** 键。

- 9 在 root [/]# 提示符下，输入 `reboot -f`，然后按 **Enter** 键以完成 root 密码重置过程。

```
root [ / ]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [ / ]# reboot -f_
```

后续步骤

作为 vRealize Automation 管理员，您现在可以使用新的 root 密码登录 vRealize Automation。

在 vRealize Automation 中使用多组织租户配置

4

vRealize Automation 使 IT 提供商能够在每个部署中设置多个租户或组织。提供商可以在每个部署中设置多个租户组织并分配基础架构。提供商还可以为租户管理用户。每个租户负责管理自己的项目、资源和部署。

在 vRealize Automation 多组织配置中，提供商可以创建多个组织，每个租户组织都使用自己的项目、资源和部署。虽然提供商无法远程管理租户基础架构，但他们可以登录到租户那里管理租户内的基础架构。

多租户依赖于以下三个 VMware 产品的协调和配置，概述如下：

- **Workspace ONE Access**- 此产品为多租户和在租户组织内提供用户和组管理的 Active Directory 域连接提供基础架构支持。
- **vRealize Suite Lifecycle Manager**- 此产品支持为受支持的产品（如 vRealize Automation）创建和配置租户。此外，它还提供一些证书管理功能。
- **vRealize Automation**- 提供商和用户可登录到 vRealize Automation 以访问租户，并可在租户中创建和管理部署。

配置多租户时，用户应熟悉所有这三个产品及其相关文档。

有关使用 vRealize Suite Lifecycle Manager 和 Workspace ONE Access 的详细信息，请参见以下内容。

- **vRealize Suite Lifecycle Manager** - 请参见 [Lifecycle Manager 产品文档](#)
- **Workspace ONE Access** - 请参见[使用 VMware Identity Manager 管理用户和 VMware Workspace ONE Access 管理](#)

具有 vRealize Suite Lifecycle Manager 特权的管理员使用 Lifecycle Manager 的“租户”页面（位于“身份与租户管理”服务下）创建和管理租户。使用 Active Directory IWA 或 LDAP 连接构建租户，并且部署 vRealize Automation 所需的关联 VMware Workspace ONE Access 实例对他们提供支持。有关使用 Lifecycle Manager 的信息，请参见相关文档。

配置多租户时，可以从基本租户或主租户开始。此租户是在部署底层 Workspace ONE Access 应用程序时创建的默认租户。其他租户（称为子租户）可以基于主租户。vRealize Automation 当前最多支持使用标准三节点部署的 20 个租户组织。

为多租户启用 vRealize Automation 之前，必须先单个组织配置中安装该应用程序，然后使用 Lifecycle Manager 设置多组织配置。Workspace ONE Access 部署支持对租户和关联的 Active Directory 域连接进行管理。

最初设置多租户时，会在 Lifecycle Manager 中指定一个提供商管理员。如果需要，可以稍后更改此指定或添加管理员。在多组织配置下，vRealize Automation 用户和组主要通过 Workspace ONE Access 进行管理。

创建组织后，授权用户可以登录到其应用程序，创建或使用项目和资源以及创建部署。管理员可以在 vRealize Automation 中管理用户角色。

为多组织配置进行设置

完成 vRealize Automation 安装后，可以启用多组织部署。设置多组织配置时，必须配置外部 Workspace ONE Access 供多租户使用，然后使用 Lifecycle Manager 创建并配置租户。这同时适用于新部署和现有部署。作为设置租户的初始步骤，您必须使用 Lifecycle Manager 为在 Workspace ONE Access 上默认创建的主租户设置别名。基于此主租户创建的子租户会从此主租户继承 Active Directory 域配置。

在 Lifecycle Manager 中，可以将租户分配给产品（如 vRealize Automation）和特定环境。设置租户时，还必须指定租户管理员。默认情况下，会基于租户主机名启用多租户。用户可以选择按 DNS 名称手动配置租户名称。在此过程中，必须设置多个标志支持多租户，并且还必须配置负载均衡器。

如果使用集群实例，则基于 Workspace ONE Access 和 vRealize Automation 租户的主机名都将指向负载均衡器。

如果集群 vRealize Automation 和 Workspace ONE Access 负载均衡器不使用通配符证书，则用户必须将租户主机名添加为证书上的 SAN 条目（对于创建的每个新租户）。

您无法删除 vRealize Automation 或 Lifecycle Manager 中的租户。如果需要将租户添加到现有的多租户部署中，您可以使用 Lifecycle Manager 执行此操作，但这需要三到四个小时的停机时间。

有关使用 vRealize Suite Lifecycle Manager Workspace ONE Access 的详细信息，请参阅本主题开头的文档链接。

主机名和多租户

在以前版本的 vRealize Automation 中，用户使用基于目录路径的 URL 访问租户。在当前的多租户实施中，用户将根据主机名访问租户。

此外，vRealize Automation 用户用于访问租户的主机名格式与 Workspace ONE Access 中用于访问租户的格式不同。例如，有效的主机名如下所示：`tenant1.example.eng.vmware.com`，而不是 `vidm-node1.eng.vmware.com`。

多租户和证书

必须为多组织配置中涉及的所有组件创建证书。对于 Workspace ONE Access、Lifecycle Manager 和 vRealize Automation，您将需要一个或多个证书，具体取决于使用的是单节点配置还是集群配置。

配置证书时，可以将通配符与 SAN 名称配合使用，也可以使用专用名称。使用通配符将在一定程度上简化证书管理，因为每当添加新租户时，都必须更新证书。如果 vRealize Automation 和 Workspace ONE Access 负载均衡器不使用通配符证书，则对于创建的每个新租户，您都必须将租户主机名添加为证书上的 SAN 条目。此外，如果使用 SAN，则在添加或删除主机或更改主机名时，必须手动更新证书。还必须为租户更新 DNS 条目。

请注意，Lifecycle Manager 不会为每个租户创建单独的证书。相反，它会对列出的每个租户主机名创建单个证书。对于基本配置，租户的 CNAME 使用以下格式：*tenantname.vrahostname.domain*。对于高可用性配置，名称使用以下格式：*tenantname.vraLBhostname.domain*。

如果使用的是集群 Workspace ONE Access 配置，请注意，Lifecycle Manager 无法更新负载均衡器证书，因此您必须手动更新它。此外，如果您需要重新注册 Lifecycle Manager 外部的产品或服务，这是一个手动过程。

本章讨论了以下主题：

- 为 vRealize Automation 设置多组织租户
- 登录到租户并在 vRealize Automation 中添加用户
- 结合使用 vRealize Orchestrator 和 vRealize Automation 多组织部署

为 vRealize Automation 设置多组织租户

可以使用 vRealize Suite Lifecycle Manager 为 vRealize Automation 设置多组织租户。

下面简要介绍了为 vRealize Automation 设置多租户的过程，包括配置 DNS 和证书。此过程重点介绍单节点部署，但也包含集群配置的说明。

有关配置 vRealize Automation 多组织配置的详细信息和视频演示，请参见 <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/>。

前提条件

- 安装和配置 Workspace ONE Access 版本 3.3.4 或更高版本。
- 安装和配置 vRealize Suite Lifecycle Manager 版本 8.5。

步骤

1 创建所需的 A 类型和 CNAME 类型的 DNS 记录。

- 对于主租户和每个子租户，必须创建并应用 SAN 证书。
- 对于单节点部署，vRealize Automation FQDN 指向 vRealize Automation 设备，Workspace ONE Access FQDN 指向 Workspace ONE Access 设备。
- 对于集群部署，基于 Workspace ONE Access 和 vRealize Automation 租户的 FQDN 必须指向各自的负载均衡器。Workspace ONE Access 配置了 SSL 终端，因此将在 Workspace ONE Access 集群和负载均衡器上应用该证书。vRealize Automation 负载均衡器使用 SSL 直通，因此仅在 vRealize Automation 集群上应用该证书。

有关更多详细信息，请参见管理单节点多组织部署中的证书和 DNS 配置和在集群 vRealize Automation 部署下管理证书和 DNS 配置。

2 为 Workspace ONE Access 和 vRealize Automation 创建或导入所需的多域 (SAN) 证书。

您可以使用让您能够创建证书许可证和密码的锁定程序服务在 Lifecycle Manager 中创建证书。或者，您也可以使用 CA 服务器或某些其他机制来生成证书。

如果需要添加或创建其他租户，则必须重新创建并应用 vRealize Automation 和 Workspace ONE Access 租户。

创建证书之后，可以使用“生命周期操作”功能在 Lifecycle Manager 中应用证书。您必须选择环境和产品，然后在右侧菜单中选择“替换证书”选项。然后可以选择产品。替换证书时，必须重新信任环境中的所有关联产品。

您必须等待证书应用和所有服务重新启动完成，再继续执行下一步。

有关更多详细信息，请参见管理单节点多组织部署中的证书和 DNS 配置和在集群 vRealize Automation 部署下管理证书和 DNS 配置。

3 在 Workspace ONE Access 实例或集群上应用 Workspace ONE Access SAN 证书。

4 在 vRealize Suite Lifecycle Manager 中，运行“启用租户”向导以启用多租户并为默认的主租户创建别名。

要启用租户，需要为提供者组织主租户或默认租户创建别名。启用租户后，您可以通过主租户 FQDN 访问 Workspace ONE Access。

例如，如果现有 Workspace ONE Access FQDN 为 `idm.example.local`，并且您创建了默认租户的别名，则在启用租户后，Workspace ONE Access FQDN 将更改为 `default-tenant.example.local`，并且与 Workspace ONE Access 通信的所有客户端现在将通过 `default-tenant.example.local` 进行通信。

5 在 vRealize Automation 实例或集群上应用 vRealize Automation SAN 证书。

您可以通过 Lifecycle Manager 生命周期操作服务应用 SAN 证书。您需要查看环境的详细信息，然后在右侧菜单中选择“替换证书”。您必须等待证书替换任务完成，然后再添加租户。作为证书替换的一部分，vRealize Automation 服务将重新启动。

6 在 Lifecycle Manager 中，运行“添加租户”向导以配置所需的租户。

您可以使用位于“身份与租户管理”下的“Lifecycle Manager 租户管理”页面添加租户。您只能添加之前已经配置了证书和 DNS 设置的租户。

创建租户时，您必须指定租户管理员，并且可以为此租户选择 Active Directory 连接。可用连接基于在默认租户或主租户中配置的连接。您还必须选择租户将关联到的产品或产品实例。

后续步骤

创建租户后，您可以使用“身份与租户管理”下的“Lifecycle Manager 租户管理”页面更改或添加租户管理员，以及将 Active Directory 目录添加到租户中并更改租户的产品关联。

您还可以登录到 Workspace ONE Access 实例以查看和验证租户配置。

管理单节点多组织部署中的证书和 DNS 配置

多组织租户 vRealize Automation 配置依赖于多个产品之间的协调配置，您必须确保 DNS 设置和证书配置正确无误，多组织租户配置才能正常发挥作用。

此多组织配置假设以下组件使用单节点部署：

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

此外，还假设您从默认租户（即提供商组织）开始，并创建两个子租户，分别称为 `tenant-1` 和 `tenant-2`。

可以在 vRealize Suite Lifecycle Manager 中使用 Locker 服务创建并应用证书，也可以使用其他机制。通过 Lifecycle Manager，还可以在 vRealize Automation 或 Workspace ONE Access 上替换或重新信任证书。

DNS 要求

必须为系统组件创建主 A 类型记录和 CNAME 类型记录，如下所述。

- 为每个系统组件和将在启用多租户时创建的每个租户同时创建两个主 A 类型记录。
- 为将要创建的每个租户以及主租户创建多租户 A 类型记录。
- 为将要创建的每个租户（不包括主租户）创建多租户 CNAME 类型记录。

单节点多租户部署的证书要求

必须创建两个主体备用名称 (SAN) 证书，一个用于 Workspace ONE Access，另一个用于 vRealize Automation。

- vRealize Automation 证书列出了 vRealize Automation 服务器的主机名和您将创建的租户的名称。
- Workspace ONE Access 证书列出了 Workspace ONE Access 服务器的主机名和您正在创建的租户名称。
- 如果使用专用 SAN 名称，则在添加或删除主机或者更改主机名时，必须手动更新证书。还必须为租户更新 DNS 条目。作为简化配置的选项，您可以对 Workspace ONE Access 和 vRealize Automation 证书使用通配符。例如，`*.example.com` 和 `*.vra.example.com`。

注 vRealize Automation 8.x 仅对符合公共后缀列表 (<https://publicsuffix.org>) 中的规范的 DNS 名称支持通配符证书。例如，`*.myorg.com` 是有效名称，而 `*.myorg.local` 无效。

请注意，Lifecycle Manager 不会为每个租户创建单独的证书。相反，它会对列出的每个租户主机名创建单个证书。对于基本配置，租户的 CNAME 使用以下格式：`tenantname.vrahostname.domain`。对于高可用性配置，名称使用以下格式：`tenantname.vraLBhostname.domain`。

汇总

下表汇总了单节点 Workspace ONE Access 和单节点 vRealize Automation 部署的 DNS 和证书要求。

DNS 要求	SAN 证书要求
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate 主机名称: WorkspaceOne.example.local、default-tenant.example.local、 tenant-1.vra.example.local、tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate 主机名称: vra.example.local、tenant-1.vra.example.local、tenant-2.vra.example.local

在集群 vRealize Automation 部署下管理证书和 DNS 配置

必须协调所有适用组件之间的证书和 DNS 配置，才能设置多组织集群 vRealize Automation 部署。

在典型的集群配置中，有三个 Workspace ONE Access 设备和三个 vRealize Automation 设备以及一个 Lifecycle Manager 设备。

此配置为以下组件采用集群部署：

- Workspace ONE Access Identity Manager 设备：
 - idm1.example.local
 - idm2.example.local
 - idm3.example.local
 - idm-lb.example.local
- vRealize Automation 设备：
 - vra-1.example.local
 - vra-2.example.local
 - vra-3.example.local
 - vra-lb.example.local
- Lifecycle Manager 设备

DNS 要求

您必须为每个组件和将在启用多租户时创建的每个租户同时创建两个主 A 类型记录。此外，您还必须为将要创建的每个租户（不包括主租户）创建多租户 CNAME 类型记录。最后，您还必须为 Workspace ONE Access 和 vRealize Automation 负载均衡器创建主 A 类型的记录。

- 为三个 Workspace ONE Access 设备以及指向各自 FQDN 的 vRealize Automation 设备创建 A 类型记录。

- 此外，为 Workspace ONE Access 负载均衡器以及指向各自 FQDN 的 vRealize Automation 负载均衡器创建 A 类型记录。
- 为默认租户以及指向 Workspace ONE Access 负载均衡器 IP 地址的 tenant-1 和 tenant-2 创建多租户 A 类型记录。
- 为指向 vRealize Automation 负载均衡器 IP 地址的 tenant-1 和 tenant-2 创建 CNAME 记录。

主体备用名称 (SAN) 证书要求

您必须创建两个 Workspace ONE Access 证书，一个证书应用于集群设备，另一个应用于负载均衡器。此外，还需创建一个应用于 vRealize Automation 设备、您将要创建的租户（不包括默认租户）和负载均衡器的证书。

- 为 Workspace ONE Access 设备创建一个证书，该证书将列出 Workspace ONE Access 设备的 FQDN 以及默认租户和您创建的其他租户。此证书应包含 Workspace ONE Access 设备的 IP 地址。
- 最佳做法是在负载均衡器上创建 SSL 终端。要支持此终端，请为 Workspace ONE Access 负载均衡器创建一个证书，该证书将列出 Workspace ONE Access 负载均衡器的 FQDN 以及默认租户和您创建的所有其他租户。此证书应包含负载均衡器的 IP 地址。
- 您必须为 vRealize Automation 创建一个证书，该证书将列出三个 vRealize Automation 设备的主机名、相关负载均衡器和您要创建的租户。此外，它还应列出三个 vRealize Automation 设备的 IP 地址。
- 作为简化配置的选项，您可以对 Workspace ONE Access 和 vRealize Automation 证书使用通配符。例如，*.example.com、*.vra.example.com 和 *.vra-lb.example.com。

注 vRealize Automation 8.x 仅对符合公共后缀列表 (<https://publicsuffix.org>) 中的规范的 DNS 名称支持通配符证书。例如，*.myorg.com 是有效名称，而 *.myorg.local 无效。

如果使用的是集群 Workspace ONE Access 配置，请注意，Lifecycle Manager 无法更新负载均衡器证书，因此您必须手动进行更新。此外，如果您需要重新注册 Lifecycle Manager 外部的产品或服务，这是一个手动过程。

集群多组织配置的 DNS 条目和证书汇总

下表概述了集群 Workspace ONE Access 和集群 vRealize Automation 多组织部署的 DNS 主 A 类型记录和 C 名称类型记录以及证书的要求。

DNS 要求	SAN 证书要求
<p>Main A Type Records</p> <ul style="list-style-type: none"> ■ lcm.example.local ■ WorkspaceOne-1.example.local ■ WorkspaceOne-2.example.local ■ WorkspaceOne-3.example.local ■ WorkspaceOne-lb.example.local ■ vra-1.example.local ■ vra-2.example.local ■ vra-3.example.local ■ vra-lb.example.local 	<p>Workspace One Certificate</p> <p>主机名称:</p> <ul style="list-style-type: none"> ■ WorkspaceOne-1.example.local ■ WorkspaceOne-2.example.local ■ WorkspaceOne-3.example.local ■ default-tenant.example.local ■ tenant-1.example.local ■ tenant-2.example.local
<p>Multi-Tenancy A Type Records</p> <ul style="list-style-type: none"> ■ default-tenant.example.local ■ tenant-1.vra.example.local ■ tenant-2.vra.example.local <p>注 所有多租户 A 类型记录必须指向 vIDM/WS1A 负载均衡器 IP 地址。</p>	<p>Workspace One LB Certificate (LB Terminated)</p> <p>主机名称:</p> <ul style="list-style-type: none"> ■ WorkspaceOne-lb.example.local ■ default-tenant.example.local ■ tenant-1.example.local ■ tenant-2.example.local
<p>Multi-Tenancy CNAME Type Records</p> <ul style="list-style-type: none"> ■ tenant-1.vra-lb.example.local - vra-lb.example.local ■ tenant-2.vra-lb.example.local - vra-lb.example.local 	<p>vRealize Automation Certificate</p> <p>主机名称:</p> <ul style="list-style-type: none"> ■ vra-1.example.local ■ vra-2.example.local ■ vra-3.example.local ■ vra-lb.example.local ■ tenant-1.example.local ■ tenant-2.example.local <p>在 vRealize Automation 负载均衡器上, 不需要任何证书, 因为它使用 SSL 直通。</p>

注 添加的每个额外租户都必须在 vRealize Automation 证书、多租户 CNAME 记录、多租户类型 A 记录、Workspace One 证书和 Workspace One LB 证书中单独列出。

注 例如, *.local 文件名仅供示例使用, 可能不适用于大多数业务环境。

登录到租户并在 vRealize Automation 中添加用户

在 Lifecycle Manager 中为 vRealize Automation 创建租户后, 可以登录到 Workspace ONE Access 以查看租户和添加用户。

您可以通过登录到关联的 Workspace ONE Access 实例来查看为 vRealize Automation 部署创建的租户。要使用的 URL 为 `https://default-tenant name.domainname.local`, 对于非集群部署, 则为 `https://idm.domainname.local`, 它会将您定向回到默认租户 Workspace ONE Access URL。

可以使用以下 URL 验证 Workspace ONE Access 中的特定租户：`https://tenant-1.domainname.local`。此 URL 将打开一个页面，其中显示指定租户的用户。您可以单击**添加用户**以临时创建其他用户。

授权用户可以使用 `https://vra.domainname.local` 登录到 vRealize Automation 中的主提供者组织。通过此视图，可以访问所有 vRealize Automation 相关服务。

授权用户可以使用 `https://tenantname.vra.domainname.local` 登录到 vRealize Automation 中的适用租户。

有关在 Workspace ONE Access 中管理用户的详细信息，请参见[管理用户和组](#)。

添加本地用户

可以使用关联的 Workspace ONE Access 实例将本地用户添加到部署中。本地用户是指未存储在任意外部身份提供程序中的用户。

结合使用 vRealize Orchestrator 和 vRealize Automation 多组织部署

您可以将 vRealize Orchestrator 与 vRealize Automation 多组织租户部署结合使用。

默认租户支持与现成的嵌入式 vRealize Orchestrator 集成进行集成。vRealize Orchestrator 可在默认租户的“集成”页面上预配置。子租户没有任何预先注册的 vRealize Orchestrator 集成。他们有多个选项可用于添加 vRealize Orchestrator 集成。

- 子租户可以通过导航到**基础架构 > 连接 > 集成**，添加与嵌入式 vRealize Orchestrator 的集成。

注 如果将嵌入式 vRealize Orchestrator 作为集成添加到多个租户，则所有 vRealize Orchestrator 内容（包括插件清单）都将在这些租户之间共享。

- 子租户可以添加一个使用多组织 vRealize Automation 作为身份验证提供程序的外部 vRealize Orchestrator 实例。

使用 vRealize Automation 多组织部署作为身份验证提供程序的任何 vRealize Orchestrator 实例都可以通过创建新的集成并提供 vRealize Orchestrator FQDN（而不提供任何凭据）向任何租户注册。

在 vRealize Automation 中使用日志

5

可以使用提供的 `vracli` 命令行实用程序在 vRealize Automation 中创建和使用日志。

可以在 vRealize Automation 中直接使用日志，也可以将所有日志转发到 vRealize Log Insight。

本章讨论了以下主题：

- 如何在 vRealize Automation 中使用日志和日志包
- 如何在 vRealize Automation 中配置将日志转发到 vRealize Log Insight
- 如何在 vRealize Automation 中创建或更新 Syslog 集成
- 如何使用内容包

如何在 vRealize Automation 中使用日志和日志包

各种服务会自动生成日志。可以在 vRealize Automation 中生成日志包。此外，还可以将环境配置为将日志发送到 vRealize Log Insight。

有关 `vracli` 命令行实用程序的信息，请在 `vracli` 命令行中使用 `--help` 参数（例如，`vracli log-bundle --help`）。

有关 vRealize Log Insight 的相关信息，请参见[如何在 vRealize Automation 中配置将日志转发到 vRealize Log Insight](#)。

日志包命令

可以创建日志包，以包含所运行服务生成的所有日志。日志包中包含所有服务日志。可以使用日志包进行故障排除。

在集群环境（高可用性模式）中，仅在一个节点上运行 `vracli log-bundle` 命令。将从环境中的所有节点中提取日志。但是，如果发生网络或其他集群问题，则从尽可能多的可访问节点中提取日志。例如，如果一个节点在包含三个节点的集群中断开连接，则仅从两个正常节点收集日志。`vracli log-bundle` 命令输出包含有关发现的任何问题及其解决办法步骤的信息。

- 要创建日志包，请通过 SSH 登录到任何节点，然后运行以下 `vracli` 命令：

```
vracli log-bundle
```

- 要更改从每个节点收集日志的超时值，请运行以下 `vracli` 命令：

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

例如，如果您的环境中包含大型日志文件、网络连接速度慢或 CPU 使用率较高，则可以将超时设置为大于默认值 1000 秒。

- 要确定特定服务日志（例如 `ebs` 或 `vro`）使用的磁盘空间，请运行以下 `vracli` 命令并检查命令输出：

```
vracli disk-mgr
```

- 要配置其他选项（如程序集超时和缓冲区位置），请使用以下 `vracli help` 命令：

```
vracli log-bundle --help
```

日志包结构

日志包是一个带时间戳的 `tar` 文件。包的名称符合模式 `log-bundle-<date>T<time>.tar` 文件，例如 `log-bundle-20200629T131312.tar`。日志包通常包含环境中所有节点的日志。如果出现错误，则包含尽可能多的日志。至少包含本地节点的日志。

日志包中包含以下内容：

- 环境文件

环境文件包含各种 **Kubernetes** 维护命令的输出。该文件提供有关每个节点和每个 `pod` 的当前资源使用情况的信息。此外，该文件还包含所有可用 **Kubernetes** 实体的集群信息和描述。

- 主机日志和配置

收集每个主机的配置（例如，其 `/etc` 目录）和主机特定的日志（例如 `journald`）时，对每个集群节点或主机使用一个目录。目录的名称与节点的主机名相匹配。目录的内部内容与主机的文件系统相匹配。目录数与集群节点数相匹配。

- 服务日志

Kubernetes 服务的日志位于以下文件夹结构中：

- `<hostname>/services-logs/<namespace>/<app-name>/file-logs/<container-name>.log`
- `<hostname>/services-logs/<namespace>/<app-name>/console-logs/<container-name>.log`

示例文件名为 `my-host-01/services-logs/prelude/vco-app/file-logs/vco-server-app.log`。

- `hostname` 是当前运行或过去运行应用程序容器的节点的主机名。通常情况下，每个服务的每个节点都有一个实例。例如，3 个节点 = 3 个实例。
- `namespace` 是在其中部署应用程序的 **Kubernetes** 命名空间。对于面向用户的服务，此值为 `prelude`。
- `app-name` 是生成日志的 **Kubernetes** 应用程序的名称（例如 `provisioning-service-app`）。
- `container-name` 是生成日志的容器的名称。某些应用程序包含多个容器。例如，`vco-app` 容器包括 `vco-server-app` 和 `vco-controlcenter-app` 容器。
- （旧版）Pod 日志

在 vRealize Automation 8.2 中进行日志记录架构更改之前，服务日志位于日志包中的每个 pod 的目录中。虽然可以使用 `vracli log-bundle --include-legacy-pod-logs` 命令继续在包中生成 pod 日志，但不建议这样做，因为所有日志信息都已位于每个服务的日志中。包含 pod 日志可能会不必要地增加生成日志包所需的时间和空间。

减少日志包的大小

要生成较小的日志包，请使用以下任一 `vracli log-bundle` 命令：

- `vracli log-bundle --since-days n`

使用此命令可以仅收集过去几天内生成的日志文件。否则，将保留并收集过去 2 天的日志。例如：

```
vracli log-bundle --since-days 1
```

- `vracli log-bundle --services service_A,service_B,service_C`

使用以下命令仅收集指定提供的服务的日志。例如：

```
vracli log-bundle --services ebs-app,vco-app
```

- `vracli log-bundle --skip-heap-dumps`

使用此命令可以从生成的日志包中排除所有堆转储。

显示日志

可以使用 `vracli logs <pod_name>` 命令输出服务 pod 或应用程序的日志。

可以使用以下命令选项：

- `--service`

显示应用程序的所有节点（而不是单个 pod）的合并日志

示例：`vracli logs --service abx-service-app`

- `--tail n`

显示日志的最后 *n* 行。*n* 的默认值为 10。

示例：`vracli logs --tail 20 abx-service-app-8598fcd4b4-tjwhk`

- `--file`

仅显示指定的文件。如果未提供文件名，则显示所有文件。

示例：`vracli logs --file abx-service-app.log abx-service-app-8598fcd4b4-tjwhk`

了解日志轮换

关于日志轮换，请了解以下服务日志注意事项：

- 所有服务都生成日志。服务日志存储在专用的 `/var/log/services-logs` 磁盘中。
- 所有日志都定期轮换。每小时进行一次轮换，或者在达到特定大小限制时进行轮换。
- 最终会压缩所有旧日志轮换。

- 日志轮换没有服务级配额。
- 系统会保留尽可能多的日志。Automation 会定期检查日志的已用磁盘空间。当空间达到 70% 时，将清除较旧的日志，直到日志的磁盘空间达到 60%。
- 如果需要更多空间，可以调整日志磁盘的大小。请参见[增加 vRealize Automation 设备的磁盘空间](#)。

要检查日志磁盘空间，请运行以下 `vracli` 命令。对于每个节点，`/dev/sdc(/var/log)` 的可用空间应接近 30% 或更多。

```
# vracli cluster exec -- bash -c 'current_node; vracli disk-mgr; exit 0'
sc1-10-182-1-103.eng.vmware.com
/dev/sda4(/):
  Total size: 47.80GiB
  Free: 34.46GiB(72.1%)
  Available(for non-superusers): 32.00GiB(66.9%)
  SCSI ID: (0:0)
/dev/sdb(/data):
  Total size: 140.68GiB
  Free: 116.68GiB(82.9%)
  Available(for non-superusers): 109.47GiB(77.8%)
  SCSI ID: (0:1)
/dev/sdc(/var/log):
  Total size: 21.48GiB
  Free: 20.76GiB(96.6%)
  Available(for non-superusers): 19.64GiB(91.4%)
  SCSI ID: (0:2)
/dev/sdd(/home):
  Total size: 29.36GiB
  Free: 29.01GiB(98.8%)
  Available(for non-superusers): 27.49GiB(93.7%)
  SCSI ID: (0:3)
```

如何在 vRealize Automation 中配置将日志转发到 vRealize Log Insight

您可以将日志从 vRealize Automation 转发到 vRealize Log Insight，以利用更可靠的日志分析和报告生成。

vRealize Automation 与基于 [fluentd](#) 的日志记录代理捆绑在一起。此代理会收集和存储日志，以将这些日志包含在日志包中并随后进行检查。可以将此代理配置为通过 vRealize Log Insight REST API 将日志副本转发到 vRealize Log Insight 服务器。该 API 允许其他程序与 vRealize Log Insight 进行通信。

有关 vRealize Log Insight 的详细信息（包括 vRealize Log Insight REST API 的文档），请参见 [vRealize Log Insight 文档](#)。

将日志记录代理配置为使用提供的 `vracli` 命令行实用程序持续地将 vRealize Automation 日志转发到 vRealize Log Insight。

所有日志行都使用主机名和环境标记进行标记，并可以在 vRealize Log Insight 中进行检查。在高可用性 (HA) 环境中，日志使用不同的主机名进行标记，具体取决于它们源自的节点。环境标记可使用 `--environment ENV` 选项进行配置，如下面的配置或更新 vRealize Log Insight 的集成部分所述。在 HA 环境中，环境标记对所有日志行使用相同的值，无论它们源于哪个节点。

有关如何使用 `vracli` 命令行实用程序的信息，可通过在 `vracli` 命令行中使用 `--help` 参数获得。例如：`vracli vrli --help`。要获得用户友好的响应，请在运行该命令时以 `vracli -j vrli` 开头。

注 只能配置单个远程日志记录集成。vRealize Log Insight 服务器和 Syslog 服务器同时可用时，优先使用 vRealize Log Insight。

检查 vRealize Log Insight 的现有配置

Command

```
vracli vrli
```

Arguments

没有命令行参数。

Output

vRealize Log Insight 集成的当前配置以 JSON 格式输出。

Exit codes

以下是可能的退出代码：

- 0 - 已配置与 vRealize Log Insight 的集成。
- 1 - 命令执行过程中出现异常。请查看错误消息以了解详细信息。
- 61 (ENODATA) - 未配置与 vRealize Log Insight 的集成。请查看错误消息以了解详细信息。

Example - check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
  "agentId": "0",
  "environment": "prod",
  "host": "my-vrli.local",
  "port": 9543,
  "scheme": "https",
  "sslVerify": false
}
```

配置或更新 vRealize Log Insight 的集成

Command

```
vracli vrli set [options] FQDN_OR_URL
```

注 运行该命令后，日志记录代理可能需要长达 2 分钟的时间才能应用指定的配置。

Arguments

- FQDN_OR_URL

指定用于发布日志的 vRealize Log Insight 服务器的 FQDN 或 URL 地址。默认情况下，使用端口 9543 和 https。如果必须更改这些设置中的任何一个，则可以改为使用 URL。

```
vracli vrli set <options> https://FQDN:9543
```

注 您可以设置不同的主机方案（默认值为 https）和端口（对于 https，默认值为 9543；对于 http，默认值为 9000）以用于发送日志，如以下示例中所示：

```
vracli vrli set https://HOSTNAME:9543
vracli vrli set --insecure HOSTNAME
vracli vrli set http://HOSTNAME:9000
```

vRealize Log Insight 摄取 REST API 使用端口 9543（对于 https）和 9000（对于 http），如 [vRealize Log Insight 文档](#) 中的《管理 vRealize Log Insight》主题“端口和外部接口”中所述。

- 选项

- --agent-id SOME_ID

设置此设备的日志记录代理的 ID。默认值为 0。用于在使用 vRealize Log Insight REST API 将日志发布到 vRealize Log Insight 时标识代理。

- --environment ENV

设置当前环境的标识符。该选项在 vRealize Log Insight 日志中作为每个日志条目的标记提供。默认值为 prod。

- --ca-file /path/to/server-ca.crt

指定一个文件，其中包含用于对 vRealize Log Insight 服务器的证书进行签名的证书颁发机构 (CA) 的证书。这会强制日志记录代理信任指定的 CA，并使其验证 vRealize Log Insight 服务器的证书（如果该证书由不可信的颁发机构签名）。该文件可能包含整个证书链以验证证书。如果是自签名证书，将传递证书本身。

- --ca-cert CA_CERT

定义与上述 --ca-file 的定义一样，只是将证书（链）内嵌为字符串进行传递。

- --insecure

停用服务器证书的 SSL 验证。这会强制日志记录代理在发布日志时接受任何 SSL 证书。

- 高级选项

- --request-max-size BYTES

可以通过一个 API 调用摄取多个日志事件。此参数控制每个请求的最大负载大小（以字节为单位）。有效值介于 4000 和 4000000 之间。默认值为 256000。有关允许值的相关信息，请参见 vRealize Log Insight REST API 文档中的 vRealize Log Insight 事件摄取。将此值设置得过低可能会导致丢弃超过所允许大小的日志记录事件。

- `--request-timeout SECONDS`

对 API 的调用可能会因多种原因而挂起，其中包括远程问题、网络问题等等。此参数控制等待每个操作（例如，打开连接、写入数据或等待响应）完成的秒数，超出此值后，会将调用识别为失败。该值不能小于 1 秒。默认值为 30。

- `--request-immediate-retries RETRIES`

将日志发送到 vRealize Log Insight 之前，日志会以聚合块的形式进行缓冲（请参见下面的 `--buffer-flush-thread-count`）。如果 API 请求失败，将立即重试日志。默认立即重试次数为 3 次。如果所有重试都未成功，则会回滚整个日志块，稍后再重试。

- `--request-http-compress`

要降低网络流量，可以对发送到 vRealize Log Insight 服务器的请求进行 gzip 压缩。如果未指定此参数，则不使用压缩。

- `--buffer-flush-thread-count THREADS`

为了实现更佳的性能并限制网络流量，在将日志刷新并发送到日志服务器之前，日志会在本地以块的形式进行缓冲。每个块包含一个服务的日志。根据您的环境，块可能会增长得很大，刷新也会很耗时。此参数控制可同时刷新的块数。默认值为 2。

注 通过 https 配置集成时，如果将 vRealize Log Insight 服务器配置为使用不可信证书（如自签名证书或由不可信颁发机构签名的证书），则必须使用 `--ca-file`、`--ca-cert` 或 `--insecure` 选项之一，否则日志记录代理将无法验证服务器身份，并且不会发送日志。使用 `--ca-file` 或 `--ca-cert` 时，vRealize Log Insight 服务器证书必须对服务器的主机名有效。在所有情况下，都要留出几分钟进行处理，然后检查 vRealize Log Insight 是否收到了日志，以便验证集成。

Output

将不输出任何内容。

Exit codes

以下是可能的退出代码：

- 0 - 配置已更新。
- 1 - 执行过程中出现异常。请查看错误消息以了解详细信息。

Examples - Configure or update integration configuration

以下示例语句显示在单独的命令行中，但参数可以在单个命令行中组合使用。例如，使用 `vracli vrli set {somehost}` 或 `vracli vrli set --ca-file path/to/server-ca.crt` 修改默认代理 ID 或环境值时，可以包含多个参数。有关相关信息，请参见联机命令帮助：`vracli vrli --help`。

```
$ vracli vrli set my-vrli.local
$ vracli vrli set 10.20.30.40
$ vracli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40
$ vracli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40
$ vracli vrli set --insecure http://my-vrli.local:8080
$ vracli vrli set --agent-id my-vrli-agent my-vrli.local
$ vracli vrli set --request-http-compress
$ vracli vrli set --environment staging my-vrli.local
$ vracli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --
request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

清除 vRealize Log Insight 的集成

Command

```
vracli vrli unset
```

注 运行该命令后，日志记录代理可能需要长达 2 分钟的时间才能应用指定的配置。

Arguments

没有命令行参数。

Output

确认信息以纯文本格式输出。

Exit codes

以下是可用的退出代码：

- 0 - 已清除配置或不存在任何配置。
- 1 - 执行过程中出现异常。请查看错误消息以了解详细信息。

Examples - Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

如何在 vRealize Automation 中创建或更新 Syslog 集成

您可以将 vRealize Automation 配置为将日志记录信息发送到远程 Syslog 服务器。

`vracli remote-syslog set` 命令用于创建 Syslog 集成或覆盖现有集成。

vRealize Automation 远程 Syslog 集成支持以下连接类型：

- 通过 UDP。
- 通过 TCP（不使用 TLS）。

注 要在不使用 TLS 的情况下创建 Syslog 集成，请向 `vracli remote-syslog set` 命令添加 `--disable-ssl` 标记。

- 通过 TCP（使用 TLS）。

注 只能配置单个远程日志记录集成。vRealize Log Insight 服务器和 Syslog 服务器同时可用时，优先使用 vRealize Log Insight。

有关配置日志记录与 vRealize Log Insight 集成的信息，请参见[如何在 vRealize Automation 中配置将日志转发到 vRealize Log Insight](#)。

前提条件

配置远程 syslog 服务器。

步骤

- 1 以 **root** 用户身份登录到 vRealize Automation 设备命令行。
- 2 要创建与 Syslog 服务器的集成，请运行 `vracli remote-syslog set` 命令。

```
vracli remote-syslog set -id name_of_integration protocol_type://
syslog_URL_or_FQDN:syslog_port
```

注 如果未在 `vracli remote-syslog set` 命令中输入端口，则端口值默认为 514。

注 可以将证书添加到 Syslog 配置中。要添加证书文件，请使用 `--ca-file` 标记。要以纯文本形式添加证书，请使用 `--ca-cert` 标记。

- 3 （可选）要覆盖现有 Syslog 集成，请运行 `vracli remote-syslog set`，并将 `-id` 标记值设置为要覆盖的集成的名称。

注 默认情况下，vRealize Automation 设备会请求您确认要覆盖 Syslog 集成。要跳过确认请求，请向 `vracli remote-syslog set` 命令添加 `-f` 或 `--force` 标记。

后续步骤

要查看设备中的当前 Syslog 集成，请运行 `vracli remote-syslog` 命令。

如何删除用于 vRealize Automation 中日志记录的 Syslog 集成

可以通过运行 `vracli remote-syslog unset` 命令从 vRealize Automation 设备中删除 Syslog 集成。

前提条件

在 vRealize Automation 设备中创建一个或多个 Syslog 集成。请参见[如何在 vRealize Automation 中创建或更新 Syslog 集成](#)。

步骤

- 1 以 **root** 用户身份登录到 vRealize Automation 设备命令行。
- 2 使用以下任一方法从 vRealize Automation 设备中删除 Syslog 集成：
 - 要删除特定 Syslog 集成，请运行 `vracli remote-syslog unset -id Integration_name` 命令。
 - 要删除 vRealize Automation 设备上的所有 Syslog 集成，请在不使用 `-id` 标记的情况下运行 `vracli remote-syslog unset` 命令。

注 默认情况下，vRealize Automation 设备会请求您确认要删除所有 Syslog 集成。要跳过确认请求，请向 `vracli remote-syslog unset` 命令添加 `-f` 或 `--force` 标记。

如何使用内容包

内容包托管在 Log Insight 中，包含与特定产品或日志集相关的仪表板、提取的字段、保存的查询和警示。可以从 VMware Sample Exchange 安装社区支持的内容包，以及从内容包商城安装其他内容包。

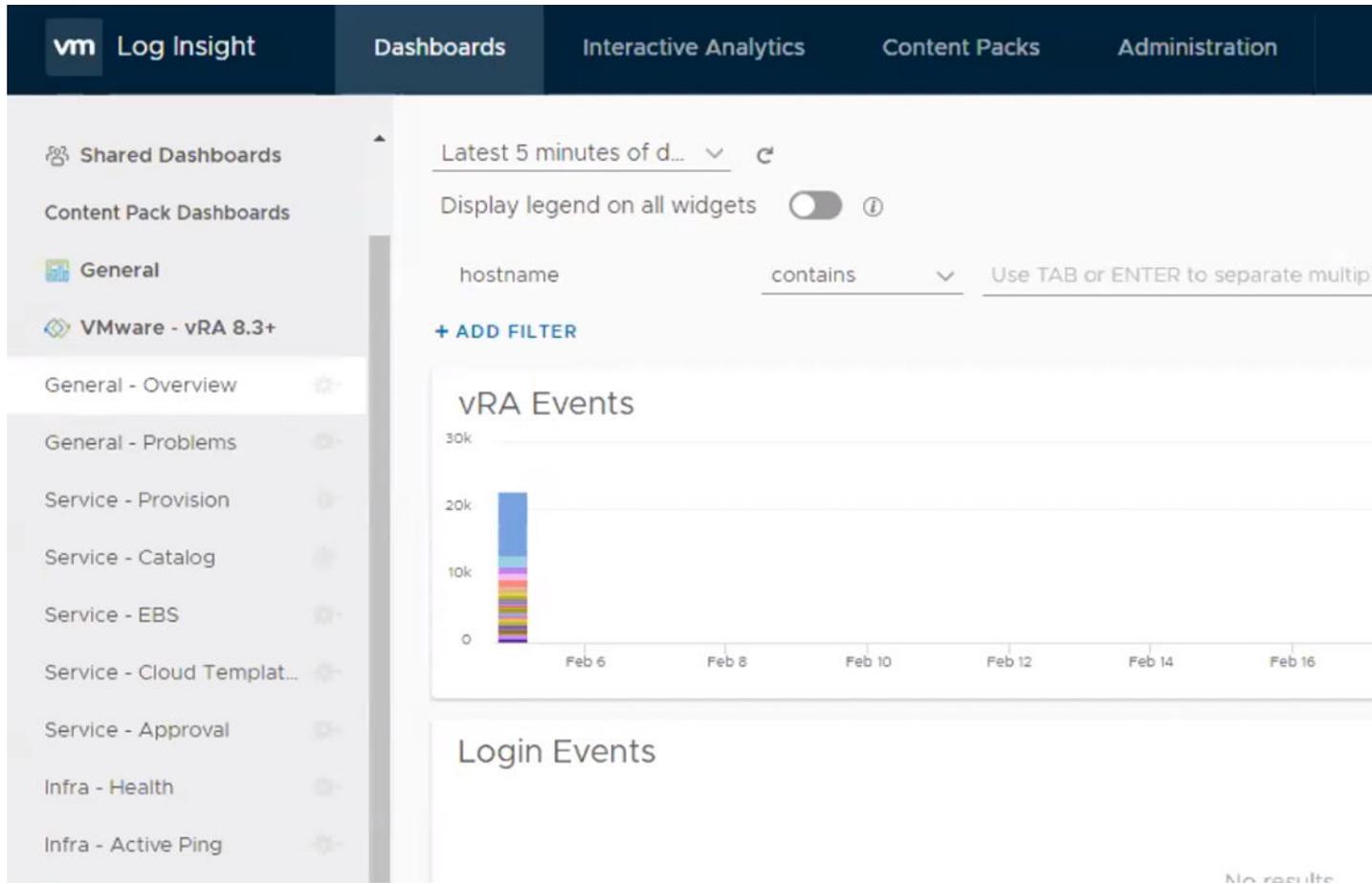
VMware vRealize Log Insight 通过汇总、分析和搜索实现日志管理自动化，从而在动态混合云环境中实现了运维智能和企业级可见性。内容包是 VMware vRealize Log Insight 中的插件，提供有关特定类型事件（如日志消息）的预定义信息。

要下载内容包，请从 Log Insight 导航到[内容包 > 商城](#)。还可以通过单击 **+** [导入内容包](#) 来导入内容包。

vRA 8.x 内容包

VMware vRealize Automation 内容包提供了所有 vRA 环境组件的日志事件的综合摘要。包括多个仪表板，这些仪表板提供了概要信息、有关错误和操作的洞察以及 vRA 实例的整体运行状况。这些仪表板与其他 Log Insight 仪表板一起在[仪表板](#)选项卡上列出。加载后，仪表板可能需要长达 30 秒的时间来填充衡量指标。

注 无法从 vRA 7.5+ 内容包升级到 vRA 8.3 内容包。必须安装 vRA 8.3 内容包。安装后，8.3 和 7.5 内容包单独运行。



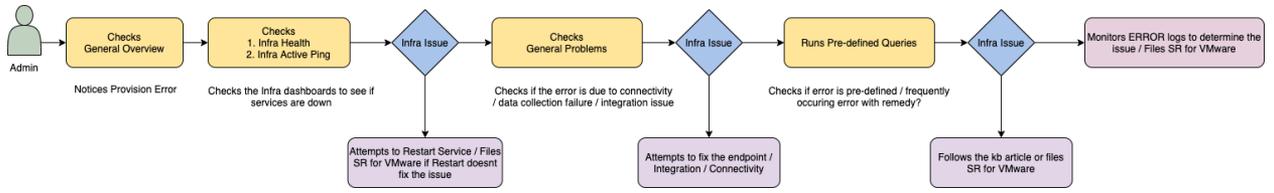
该 vRealize Automation 包包括以下仪表盘：

- 常规 - 概览：捕获 vRA 概括性衡量指标的概要信息。
- 常规 - 问题：
- 服务 - 置备：捕获与置备服务相关的问题。
- 服务 - 目录：捕获与目录服务相关的问题。
- 服务 - EBS：捕获与事件代理服务相关的问题。
- 服务 - 云模板：捕获与 Cloud Assembly 云模板、自定义资源和资源操作相关的错误和衡量指标。
- 服务 - 批准：捕获与批准相关的错误和衡量指标。
- 基础架构 - 运行状况：捕获一段时间内 pod 重新启动的情况。此仪表盘对于检测由于资源限制而造成的中断至关重要。
- Infra - Active Ping：捕获一段时间的运行状况检查 URL。

每个仪表盘都包含单独的小组件，可提供更有针对性的分析。要查看在每个小组件中执行的分析类型，请

单击信息  图标。

作为 vRealize Automation 管理员，您可以按照此常规内容包 workflows 识别错误并排除故障。



有关 vRealize Automation 8.3 内容包的详细信息，请参见 [vRealize Automation 8.3+ Log Insight 内容包](#)和如何配置将日志转发到 [vRealize Log Insight](#)。

参与 vRealize Automation 的客户体验提升计划

6

本产品参与 VMware 的客户体验提升计划 (CEIP)。CEIP 将向 VMware 提供相关信息，以帮助 VMware 改进产品和服务，解决问题，以及向您建议如何以最佳方式部署和使用我们的产品。

有关通过 CEIP 收集的数据以及 VMware 使用该数据的用途的详情，请参见[客户体验提升计划](#)页面。

本章讨论了以下主题：

- 如何加入或退出 vRealize Automation 的客户体验提升计划
- 如何配置 vRealize Automation 客户体验提升计划的数据收集时间

如何加入或退出 vRealize Automation 的客户体验提升计划

从 vRealize Automation 设备命令行加入或退出客户体验提升计划 (CEIP)。

可以在安装 vRealize Automation 时使用 vRealize Lifecycle Manager (LCM) 加入 CEIP 计划。也可以在安装后使用命令行选项加入或退出计划。

要使用命令行选项加入客户体验提升计划，请执行以下操作：

- 1 以 **root** 用户身份登录到 vRealize Automation 设备命令行。
- 2 运行 `vracli ceip on` 命令。
- 3 查看客户体验提升计划信息，然后运行 `vracli ceip on --acknowledge-ceip` 命令。
- 4 要重新启动 vRealize Automation 服务，请运行 `/opt/scripts/deploy.sh` 命令。

要使用命令行选项退出客户体验提升计划，请执行以下操作：

- 1 以 **root** 用户身份登录到 vRealize Automation 设备命令行。
- 2 运行 `vracli ceip off` 命令。
- 3 要重新启动 vRealize Automation 服务，请运行 `/opt/scripts/deploy.sh` 命令。

如何配置 vRealize Automation 客户体验提升计划的数据收集时间

您可以设置客户体验提升计划 (CEIP) 向 VMware 发送数据的日期和时间。

步骤

1 以 **root** 用户身份登录到 vRealize Automation 设备命令行。

2 使用文本编辑器打开以下文件。

```
/etc/telemetry/telemetry-collector-vami.properties
```

3 编辑星期几 (dow) 和一天中小时 (hod) 的属性。

属性	说明
<code>frequency.dow=<day-of-week></code>	在星期几进行数据收集。
<code>frequency.hod=<hour-of-day></code>	在一天中的当地时间几点进行数据收集。可能的值为 0 - 23。

4 保存并关闭 `telemetry-collector-vami.properties`。

5 通过输入以下命令来应用设置。

```
vcac-config telemetry-config-update --update-info
```

所做更改将应用于部署中的所有节点。

在 vRealize Automation 中打开产品 内置反馈表单

7

您可以让用户向 vRealize Automation 开发团队提供反馈。您的反馈对于我们的开发流程非常重要。

什么是反馈表单

反馈表单位于支持面板中标记为“反馈”的选项卡上。要打开表单，请单击**帮助**按钮，然后单击**反馈**。

The screenshot shows the vRealize Automation user interface. At the top, the user's name 'Fritz Arbeiter' and ID 'CAVA-R-90-065' are displayed. Below this, there are two tabs: 'SUPPORT' and 'FEEDBACK'. The 'FEEDBACK' tab is selected. The main content area contains the following text and form elements:

- A heading: "You can rate your experience and send us feedback about vRealize Automation."
- A question: "How satisfied are you with vRealize Automation?"
- A rating scale with seven numbered circles (1-7). Below the scale, it says "Extremely Dissatisfied" on the left and "Extremely Satisfied" on the right.
- A question: "Do you have any other feedback about vRealize Automation? Let us know what's on your mind:"
- A text input field for providing additional feedback.
- A question: "Your voice matters, and sometimes we want to hear more! Can we contact you for a follow-up conversation?"
- A dropdown menu with "Yes" selected.
- A question: "If yes, what's the best way to reach you?"
- A text input field for providing contact information.
- A privacy notice at the bottom: "We will use any information that you share with us, in addition to information about your account, to fix problems, improve our products and services, and provide you with recommendations. If you choose to share your contact information, we will only use it to..."

如何使反馈表单可供我的用户使用

反馈表单要求您的 vRealize Automation 主机能够访问 Internet，并且以下基本 URL 包含在您的 Internet 允许列表中。

- <https://lumos.vmware.com/>
- <https://feedback.esp.vmware.com/>

如果主机无法访问 Internet，则无法在“帮助”窗格中使用表单。