管理 vRealize Automation

2020 年 12 月 21 日
vRealize Automation 8.1

vmware®

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

目录

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 vRealize Automation 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 ■ 组织成员	■ Cloud Assembly 管理员 ■ 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 LCM 和 Workspace ONE Access 的详细信息，请参见使用 VMware Identity Manager 管理用户。

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

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

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

表 2-1. vRealize Automation Cloud Assembly 服务角色说明

角色	说明
Cloud Assembly 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。这是唯一可以查看和执行所有操作的用户角色，包括添加云帐户、创建新项目以及分配项目管理员。
Cloud Assembly 用户	不具有 Cloud Assembly 管理员角色的用户。 在 vRealize Automation Cloud Assembly 项目中，管理员将用户作为项目成员添加到项目中。管理员还可以添加项目管理员。下面定义了这两个角色的权限。
Cloud Assembly 查看者	可以查看信息但不能创建、更新或删除值的用户。这是只读用户。

除了服务角色外，vRealize Automation Cloud Assembly 还具有项目角色。

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

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

在您决定为用户提供哪些权限时，项目角色说明可为您提供帮助。

- 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，以设计和部署蓝图。
- 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蓝图之类的非破坏性操作。

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

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
访问 Cloud Assembly						
控制台	在 vRA 控制台中，您可以查看并打开 Cloud Assembly	是	是	是	是	是
基础架构						
	查看并打开“基础架构”选项卡	是	是	是	是	是
配置 - 项目	创建项目	是				
	更新或删除项目摘要、用户、置备、Kubernetes、集成和测试项目配置中的值。	是		是。您的项目		
	在项目中添加用户并分配角色。	是		是。您的项目。		
	查看项目	是	是	是。您的项目	是。您的项目	是。您的项目
配置 - 云区域	创建、更新或删除云区域	是				
	查看云区域	是	是			
配置 - Kubernetes 区域	创建、更新或删除 Kubernetes 区域	是				
	查看 Kubernetes 区域	是	是			
配置 - 特定实例	创建、更新或删除特定实例	是				
	查看特定实例	是	是			
配置 - 映像映射	创建、更新或删除映像映射	是				
	查看映像映射	是	是			
配置 - 网络配置文件	创建、更新或删除网络配置文件	是				
	查看映像网络配置文件	是	是			
配置 - 存储配置文件	创建、更新或删除存储配置文件	是				
	查看映像存储配置文件	是	是			
配置 - 定价卡	创建、更新或删除定价卡	是				
	查看定价卡	是	是			

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

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
配置 - 标记	创建、更新或删除标记	是				
	查看标记	是	是			
资源 - 计算	将标记添加到已发现的计算资源	是				
	查看发现的计算资源	是	是			
资源 - 网络	修改网络标记、IP 范围、IP 地址	是				
	查看发现的网络资源	是	是			
资源 - 安全	将标记添加到已发现的安全组	是				
	查看已发现的安全组	是	是			
资源 - 存储	向发现的存储中添加标记	是				
	查看存储	是	是			
资源 - 计算机	添加和删除计算机	是				
	查看计算机	是	是	是。您的项目	是。您的项目	是。您的项目
资源 - 卷	删除发现的存储卷	是				
	查看发现的存储卷	是	是	是。您的项目	是。您的项目	是。您的项目。
资源 - Kubernetes	部署或添加 Kubernetes 群集，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
商城						

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

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
	查看并打开“商城”选项卡	是	是			
	在“设计”选项卡上使用已下载的蓝图	是		是。如果与项目相关联。	是。如果与项目相关联。	
商城 - 蓝图	下载蓝图	是				
	查看蓝图	是	是			
商城 - 映像	下载映像	是				
	查看映像	是	是			
商城 - 下载	查看所有已下载项目的日志	是	是			
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				
	禁用订阅	是				
	查看订阅	是	是			
库 - 事件主题	查看事件主题	是	是			
库 - 操作	创建、更新或删除可扩展性操作	是				
	查看可扩展性操作	是	是			
库 - 工作流	查看可扩展性工作流	是	是			
活动 - 操作运行	取消或删除可扩展性操作运行	是				
	查看可扩展性操作运行	是	是			是。您的项目
活动 - 工作流运行	查看可扩展性工作流运行	是	是			
设计						
设计	打开“设计”选项卡并查看蓝图列表	是	是	是。您的项目	是。您的项目	是。您的项目
蓝图	创建、更新和删除蓝图	是		是。您的项目	是。您的项目	
	查看蓝图	是	是	是。您的项目	是。您的项目	是。您的项目
	下载蓝图	是	是	是。您的项目	是。您的项目	是。您的项目
	上载蓝图	是		是。您的项目	是。您的项目	

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

UI 上下文	任务	Cloud Assembly 管理员	Cloud Assembly 查看者	Cloud Assembly 用户 用户必须是项目管理员或成员才能查看和执行项目相关任务。		
				项目管理员	项目成员	项目查看者
	部署蓝图	是		是。您的项目	是。您的项目	
	版本和还原蓝图	是		是。您的项目	是。您的项目	
	将蓝图发布到目录中	是		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
部署						
	查看并打开“部署”选项卡	是	是	是	是	是
	查看部署，包括部署详细信息、部署历史记录和故障排除信息。	是	是	是。您的项目	是。您的项目	是。您的项目
	基于策略对部署运行实施后操作	是		是。您的项目	是。您的项目	

Service Broker 服务角色

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

表 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 vRealize Automation Service Broker 管理员角色的任何用户。 在 vRealize Automation Service Broker 项目中，管理员将用户作为项目成员添加到项目中。管理员还可以添加项目管理员。下面定义了这两个角色的权限。
Service Broker 查看者	具有只读权限的用户，可以查看信息，但不能创建、更新或删除值。

除了服务角色外，vRealize Automation Service Broker 还具有项目角色。

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

下表介绍了不同的服务和项目角色可以查看的内容和执行的操作，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，以设计和部署蓝图。
- 项目查看者仅限于只读访问权限。

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
访问 Service Broker						
控制台	在控制台中，您可以查看和打开 Service Broker	是	是	是	是	是
基础架构						
	查看并打开“基础架构”选项卡	是	是			
配置 - 项目	创建项目	是				
	更新或删除项目摘要、用户、置备、Kubernetes 和集成中的值	是				
	查看项目	是	是			
配置 - 云区域	创建、更新或删除云区域	是				
	查看云区域	是	是			
配置 - Kubernetes 区域	创建、更新或删除 Kubernetes 区域	是				
	查看 Kubernetes 区域	是	是			
连接 - 云帐户	创建、更新或删除云帐户	是				
	查看云帐户	是	是			
连接 - 集成	创建、更新或删除集成	是				
	查看集成	是	是			
活动 - 请求	删除部署请求记录	是				
	查看部署请求记录	是				
活动 - 事件日志	查看事件日志	是				
内容和策略						
	查看并打开“内容和策略”选项卡	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
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
	查看可用目录项	是	是	是。您的项目	是。您的项目	是。您的项目
	请求目录项	是		是。您的项目	是。您的项目	
部署						
	查看并打开“部署”选项卡	是	是	是。	是	是
	查看部署，包括部署详细信息、部署历史记录和故障排除信息。	是	是	是。您的项目	是。您的项目	是。您的项目
	基于策略对部署运行实施后操作	是		是。您的项目	是。您的项目	
批准						
	查看并打开“批准”选项卡	是	是	是	是	是
	响应批准请求	是		仅 Service Broker 用户角色	仅 Service Broker 用户角色	仅 Service Broker 用户角色

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
- 更新 vRealize Automation 的 DNS 分配
- 如何启用 vRealize Automation 的时间同步
- 如何停用时间同步
- 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。

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。

注 请尽一切可能避免使用 `vracli reset vidm` 命令。此命令将重置 Workspace One Access 的所有配置，并会断开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/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

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
```

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 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
```

3 登录到 vCenter，然后使用 `Shut Down Guest OS` 命令关闭所有 vRealize Automation 节点。

4 更新每个 vRealize Automation 节点的 OVF DNS 属性。

   a 导航到 vCenter 清单中的 vRealize Automation 节点。

   b 选择“配置”选项卡，然后展开“设置”。

   c 选择 vApp 选项。

   d 在 OVF 属性列表中，找到并选择 `vami.DNS.vRealize_Automation`。

   e 单击**设定值**，然后在“属性值”文本框中输入新的 DNS 条目。

   f 单击**确定**。

5 启动所有 vRealize Automation 节点并等待它们完全启动，控制台上的蓝色屏幕将提供相关指示。

6 再次重新启动 vRealize Automation 节点并等待它们完全启动。

7 使用 SSH 登录到每个 vRealize Automation 节点，并验证是否在 `/etc/resolve.conf` 中列出了新的 DNS 服务器。

8 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。

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	当托管 vRealize Automation 设备的 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。 **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。 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)。
systemd	此配置使用 systemd-timesyncd 守护进程同步 vRealize Automation 部署的时钟。 **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。

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 运行 `vracli ntp apply` 命令。

ESXi NTP 配置将应用于 vRealize Automation 部署。

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。

b 运行 `vracli ntp apply` 命令。

systemd NTP 配置将应用于 vRealize Automation 部署。

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

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，请重新引导与 NTP 服务器同步的 vRealize Automation 设备。

如何停用时间同步

可以使用 vRealize Automation 设备命令行在 vRealize Automation 部署上停用网络时间协议 (NTP) 时间同步。

也可以通过运行 `vracli ntp reset` 命令重置 vRealize Automation 设备的 NTP 配置，然后通过运行 `vracli ntp apply` 命令应用新配置。

前提条件

确认您配置了与 ESXi 或 systemd 保持时间同步。请参见如何启用 vRealize Automation 的时间同步。

步骤

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

2 要停用与 ESXi 或 systemd 保持时间同步，请运行 `vracli ntp disable` 命令。

3 运行 `vracli ntp apply` 命令。

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

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

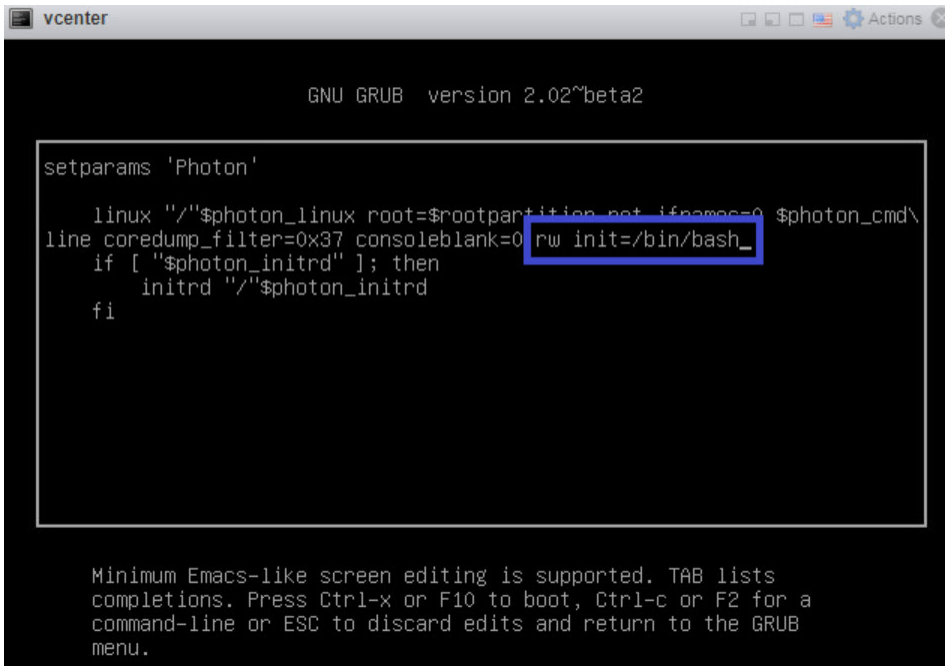
此过程适用于 vRealize Automation 管理员，需要使用访问主机 vCenter Appliance 所需的凭据。

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：



4 按 **F10** 键以推送更改并重新启动 vRealize Automation。

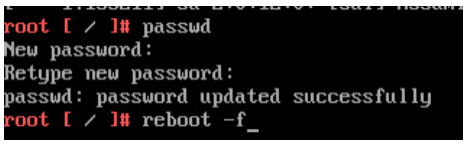
5 等待 vRealize Automation 重新启动。

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。



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 使客户 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 LCM 和 Workspace ONE Access 的详细信息，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。

为多租户配置 vRealize Automation 时，必须先在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 Actice Directory 域连接进行管理。

最初配置多租户时，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。

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，Lifecyle 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 3.3.2。
- 安装和配置 vRealize Suite Lifecycle Manager 版本 8.1。

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 3.3.2 和 vRA 8.1 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 SAN 证书。

4 在 vRealize Suite Lifecycle Manager 8.1 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，Lifecyle 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：
  - vra1.example.local
  - vra2.example.local
  - vra3.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 和证书要求。

DNS 要求	SAN 证书要求
`Main A Type Records` lcm.example.local WorkspaceOne-1.example.local WorkspaceOne-2.example.local WorkspaceOne-3.example.local vra.example-1.local vra.example-2.local vra.example-3.local	`Workspace One Certificate` 主机名称： WorkspaceOne.example.local、default-tenant、example.local、tenant-1.example.local、tenant-2.example.local
`Multi-Tenancy A Type Records` default-tenant.example.local tenant-1.vra.example.local tenant-2.vra.example.local	`Workspace One LB Certificate (LB Terminated)` 主机名称： WorkSpaceOne-lb.example.local、default-tenant.example.local、vra.example.local、tenant-1.example.local、tenant-2.example.local
`Multi-Tenancy CNAME Type Records` tenant-1.vra-lb.example.local - vra-lb.example.local tenant-2.vra-lb.example.local - vra.lb.exmple.local	`vRealize Automation Certificate` 主机名称： vra-1.example.local、vra-2.example.local、vra-3.example.local、vra-lb.example.local、tenant-1.example.local、tenant-2.example.local 在 vRealize Automation 负载均衡器上，不需要任何证书，因为它使用 SSL 直通。

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 管理用户的详细信息，请参见 https://docs.vmware.com/cn/VMware-Workspace-ONE-Access/3.3/idm-administrator.pdf

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何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。“集成”页面上提供了预配置的 vRealize Orchestrator。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。

- 他们可以通过导航到 vRealize Orchestrator 中的“配置身份验证提供程序”并使用适用 vRealize Automation 租户的主机地址进行连接来添加与嵌入式 vRealize Orchestrator 的集成。然后，他们可以选择**基础架构 > 连接 > 集成**并将嵌入式 vRO 添加为集成。
- 他们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

如何在 vRealize Automation 中使用日志和日志包

可以在 vRealize Automation 中创建并使用 vRealize Automation 日志和日志包。

或者，也可以自动将日志转发到 vRealize Log Insight。有关如何将日志转发到 vRealize Log Insight 的信息，请参见如何配置将日志转发到 vRealize Log Insight。

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 log-bundle --help`。

日志包命令

可以创建简单日志包，也可以创建所有服务的聚合（冷存储）日志。尽管这两个日志包都包含服务的所有日志，但冷存储包中包含服务日志备份版本的聚合流副本，具有更大的故障排除价值。冷存储代理会不断从服务中聚合日志，并将其存储在本地文件系统中。一般情况下，只需要简单日志包即可进行故障排除。

此外，还可以更改从每个节点收集日志的默认超时值。

在集群环境中，只需要在一个节点上运行 `vracli log-bundle` 命令。

- 显示日志包命令帮助：

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

- 创建简单日志包。

  ```
  vracli log-bundle
  ```

- 创建冷存储日志包：

  ```
  vracli log-bundle --include-cold-storage
  ```

- 更改从每个节点收集日志的超时值。例如，如果您的环境中包含大型日志文件且存在网络连接速度慢、CPU 使用率较高等情况，则可能需要将超时设置为大于默认值 1000 秒。

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

日志包结构

vRealize Automation 服务在 Kubernetes Pod 中进行了容器化。生成的日志包是 `tar.xz` 存档，使用 `log-bundle-{{TIMESTAMP}}.tar.xz` 名称格式，其中 TIMESTAMP 是时间戳（以秒为单位）。正常日志包中包含环境中所有节点的日志。如果由于任何原因无法生成正常日志包，则会创建回退包。回退包仅包含当前节点的日志。这两种日志包的结构稍有不同。

- 正常日志包

  正常日志包分为以下几类：

  - 主机日志和配置

    在每个集群节点（主机）的一个目录中收集每个主机的配置及其主机特定的日志。目录名称与节点主机名相匹配。目录内容与主机文件系统相匹配。目录数与集群节点数相匹配。

    冷存储日志位于结构化 JSON 日志 (`/hostname/services-logs/all/aggregated.log`) 中。

  - Pod 日志

    服务在 Kubernetes Pod 中进行了容器化。服务日志位于 `pods` 目录中，其中，每个命名空间包含一个目录，且文件名与命名空间名称相匹配。通常，在每个集群节点上，每个 Pod 有一个实例。在 Pod 目录中，对于每个容器应用程序，包含一个日志文件。

    例如，vRealize Orchestrator 控制中心日志位于每个 `/pods/prelude/vco-app-hash/`目录下的 `vco-controlcenter-app.log` 文件中。

  - 环境文件

    环境文件包含有关每个节点和每个 Pod 的当前资源使用情况的信息。此外，还包含所有可用 Kubernetes 实体的集群信息和描述。

- 回退日志包

  如果在等待 `vracli` 命令完成时收到错误消息，则会生成回退包。如果您收到此错误，则应在集群中的每个主机或节点上运行 `vracli log-bundle` 命令，以收集尽可能多的信息。

  - 回退容器日志

    回退日志位于`/fallback-containers` 目录中。可以通过检查日志文件名来确定日志是由哪个 Pod 中的哪个容器生成的：

    pod-name-some-hash-container-name-other-hash.log

  - 回退冷存储

    如果收集的是包形式的冷存储日志，则当前主机的回退日志位于 `/fallback-cold-storage` 目录中。

如何配置将日志转发到 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。您可以将此代理配置为通过 vRealize Log Insight API 将日志副本转发到 vRealize Log Insight 服务器。提供的 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（包括适用于 vRealize Log Insight API 的文档），请参见 vRealize Log Insight 文档和 /api/v1/events/ingest/{agentId} 页面。

使用提供的 `vracli` 命令行实用程序将日志记录代理配置为自动、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`。

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": 443,
    "scheme": "https",
    "sslVerify": false
}
```

注 您可以设置不同的主机方案（默认值为 https）和端口（默认值为 443）以用于发送日志，如以下示例中所示：

```
vracli vrli set some-host
vracli vrli set some-host:9543
vracli vrli set http://some-host:9543
```

vRealize Log Insight 载入 API 使用端口 9543，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。

配置或更新 vRealize Log Insight 的集成

Command

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

Arguments

可用命令行参数如下：

- FQDN_OR_URL - vRealize Log Insight 服务器的 FQDN 或 IP 地址，用于通过 vRealize Log Insight API 配置发布日志。默认情况下，将使用端口 443 和 HTTPS 方案。如果必须更改这些设置中的任何一个，则可以改为使用 URL。
- 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`。用于标识通过使用 vRealize Log Insight API 配置发布到 vRealize Log Insight 的日志的日志记录代理。
  - `--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行事件的标记提供。默认值为 `prod`。
  - `--ca-file/path/to/server-ca.crt` - 指定包含用于对 vRealize Log Insight 服务器证书进行签名的证书颁发机构 (CA) 证书的文件。强制日志记录代理信任指定的 CA，并使该 CA 验证 vRealize Log Insight 服务器的证书。如果需要，该文件可以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` - 指定文件的方式与 `--ca-file` 相同，但将证书（链）内嵌为字符串进行传递。
  - `--insecure` - 停用服务器证书的 SSL 验证。强制日志记录代理在发布日志时接受任何 SSL 证书。

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

```
$ 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 --environment staging my-vrli.local
```

清除 vRealize Log Insight 的集成

Command

```
vracli vrli unset
```

Arguments

没有命令行参数。

Output

确认信息以纯文本格式输出。

Exit codes

以下是可能的退出代码：

- 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）。

有关配置日志记录与 vRealize Log Insight 集成的信息，请参见如何配置将日志转发到 vRealize Log Insight。

前提条件

配置一个或多个远程 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。

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、并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 使用这些数据的目的的详细信息，请参见信任与保证中心 (http://www.vmware.com/trustvmware/ceip.html)。

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
`frequency.dow=<day-of-week>`	在星期几进行数据收集。
`frequency.hod=<hour-of-day>`	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。