VRealize Orchestrator 中的多租户功能

vRealize Orchestrator 7.6

vmware®

您可以从 VMware 网站下载最新的技术文档：
https://docs.vmware.com/cn/。
VMware 网站还提供了最近的产品更新。
如果您对本文档有任何意见或建议，请将反馈信息发送至：
docfeedback@vmware.com

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

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 © 2008 – 2019 VMware, Inc. 保留所有权利。 版权和商标信息。

目录

VMware, Inc. 保留所有权利。

VMware vRealize Orchestrator 中的多租户功能

1

多租户 VMware vRealize Orchestrator 提供了有关 VMware® vRealize Orchestrator 7.4 中引入的多租户架构的一般信息。

目标读者

此信息面向 vRealize Automation 系统管理员、租户管理员和 Orchestrator 管理员。

vRealize Orchestrator 中的多租户功能概述

vRealize Orchestrator 7.4 引入了多租户架构，其中多个 vRealize Automation 租户可以共享一个外部或嵌入式 vRealize Automation 实例。

租户是 vRealize Automation 部署中的组织单位。vRealize Orchestrator 7.4 引入了多租户架构，其中多个 vRealize Automation 租户可以共享一个外部或嵌入式 vRealize Orchectration 实例。这是 Orchestrator 用作身份验证提供程序的 vRealize Automation 实例。有关 vRealize Automation 中的多租户功能的详细信息，请参见准备和使用 vRealize Automation 中的服务蓝本中的租户和用户角色。

默认情况下，vRealize Automation 中的多租户功能处于禁用状态，以保持向后兼容性，并且启用该功能会给产品的用户体验带来重大改变。如果您在 vRealize Orchestrator 中启用了多租户功能，之后将无法安全地将其禁用。

注　只有多租户功能处于启用状态，vRealize Automation 身份验证才受支持。

VMware, Inc. 保留所有权利。

启用 vRealize Orchestrator 中的多租户功能

2

仅当 Orchestrator 配置为使用 vRealize Automation 作为身份验证提供程序时，您才能启用多租户功能。默认情况下，多租户功能处于禁用状态。

启用 vRealize Orchestrator 多租户功能

新的 vRealize Orchestrator 安装配置为在单租户模式下运行。要在多租户模式下运行 Orchestrator，必须明确启用多租户功能。

注 启用多租户功能是不可逆转的更改操作。如果您不了解该功能的用途，请勿启用。

步骤

1 以 root 用户身份登录到 Orchestrator Appliance Linux 控制台。

2 停止 Orchestrator 服务器服务和控制中心服务。

```
service vco-server stop && service vco-configurator stop
```

3 导航到 `/var/lib/vco/tools/configuration-cli/bin` 目录。

```
cd /var/lib/vco/tools/configuration-cli/bin
```

4 要启用多租户功能，请运行 `vro-configure.sh` 脚本。

```
./vro-configure.sh enable-multi-tenancy
```

5 启动 Orchestrator 服务器服务和控制中心服务。

```
service vco-server start && service vco-configurator start
```

您即成功启用 vRealize Orchestrator 中的多租户功能。

VMware, Inc. 保留所有权利。

vRealize Orchestrator 中的租户隔离

3

Orchestrator 多租户功能在租户间实现了一定程度的隔离。

在启用多租户功能后，Orchestrator 管理的对象将拆分为系统范围的对象和特定于租户的范围的对象。这些对象包括工作流、操作、软件包、配置、类别、策略、策略模板、任务、工作流运行和其他内容。

系统范围

系统范围是容纳在所有租户之间共享的所有 Orchestrator 内容的语义空间。系统内容包括以下项目：

- 默认 Orchestrator 插件中包含的所有对象。
- 在启用多租户功能之前创建的自定义对象。
- vRealize Automation 系统管理员创建的对象。
- 预定义的自动化内容（工作流、操作和其他内容），由系统租户管理，并且可由所有非系统租户读取和调用。

租户对于此内容拥有只读访问权限，并且无法创建、修改或删除任何系统范围的对象。

特定于租户的范围

特定于租户的对象与创建它们的租户相关联。这些对象可以包括工作流、操作、策略、策略模板、资源和其他内容。租户可以编辑或删除自己创建的内容。他们可以运行和查看系统内容以及他们自己的特定于租户的内容。

租户无法查看、编辑或删除系统范围的对象或由其他租户创建的对象。

多租户环境中的 Orchestrator 插件

vRealize Orchestrator 7.4 不支持 Orchestrator 插件和插件清单对象的多租户功能。属于插件清单的对象是系统范围的一部分。

注　您通过从插件库运行工作流创建的对象（如端点和清单项目）对所有租户可见并且可供他们访问。

VMware, Inc. 保留所有权利。

资源分配

Orchestrator 服务器资源（如 CPU、内存、存储、网络带宽、数据库空间、最大工作流运行数量、线程池和其他资源）在所有租户之间共享。如果其中一个租户达到所分配资源的限制，使用同一 Orchestrator 实例的所有其他租户都会受到影响。

安全

vRealize Orchestrator 7.4 中租户之间的安全隔离使用 vRealize Automation 中定义的系统管理员和租户管理员用户角色。有关 vRealize Automation 中用户角色的详细信息，请参见准备和使用 vRealize Automation 中的服务蓝本中的用户角色概述。

注　vRealize Automation 系统管理员必须是 Orchestrator 管理员组的成员，该管理员组是您在控制中心配置身份验证提供程序时在**管理员组**文本框中输入的。

可从 Orchestrator 客户端配置的用户权限与任何 vRealize Automation 用户角色都没有对应关系。您必须为特定用户或组明确配置用户权限。有关设置用户权限的详细信息，请参见使用 VMware vRealize Orchestrator 客户端。

隔离多租户 Orchestrator 环境中的访问权限

启用多租户功能后，系统管理员和租户用户将具有不同的权限来操作 Orchestrator 中的对象。这些权限具体取决于对象属于系统范围还是特定于租户的范围。

表 3-1. 租户之间的隔离

角色	系统内容	租户 A 内容	租户 B 内容
系统管理员	■ 创建、查看、编辑、删除和还原系统范围的对象 ■ 运行系统工作流 ■ 监控系统管理员启动的工作流的运行	注　除非指定为系统管理员的帐户也是某个现有租户的管理员，否则该系统管理员将无法访问或操作任何特定于租户的内容。	
租户 A 管理员	■ 查看系统内容 ■ 运行系统工作流 ■ 监控任何租户 A 用户启动的系统工作流	■ 创建、查看、编辑、删除和还原属于租户 A 的对象 ■ 运行租户 A 工作流 ■ 监控任何租户 A 用户启动的租户 A 工作流的运行	除租户 B 用户通过从插件库运行工作流创建的资源外，租户 A 中的用户无法访问租户 B 用户创建的任何对象。
租户 B 管理员	■ 查看系统内容 ■ 运行系统工作流 ■ 监控任何租户 B 用户启动的系统工作流	除租户 A 用户通过从插件库运行工作流创建的资源外，租户 B 中的用户无法访问租户 A 用户创建的任何对象。	■ 创建、查看、编辑、删除和还原属于租户 B 的对象 ■ 运行租户 B 工作流 ■ 监控任何租户 B 用户启动的租户 B 工作流的运行
解决方案用户	■ 创建、查看、编辑、删除和还原系统范围的对象 ■ 运行系统工作流	■ 创建、查看、编辑、删除和还原属于租户 A 的对象 ■ 运行租户 A 工作流	■ 创建、查看、编辑、删除和还原属于租户 B 的对象 ■ 运行租户 B 工作流

单租户和多租户 Orchestrator 部署的比较

4

从版本 7.4 开始，Orchestrator 可以根据具体业务需求在单租户模式或多租户模式下工作。

单租户部署

除非启用了多租户功能，否则 Orchestrator 将在单租户模式下工作。这意味着所有用户之间将共享构成 Orchestrator 内容和运行时的所有对象。您可以对对象设置不同权限级别，限制不同用户或用户组对该对象的访问权限。有关设置用户权限的详细信息，请参见使用 VMware vRealize Orchestrator 客户端。

多租户部署

启用多租户功能后，Orchestrator 中特定于租户的对象将在 vRealize Automation 租户间彼此隔离，并且与系统范围的对象隔离开来。租户用户可以使用其用户名、密码和租户 ID 登录 Orchestrator 客户端，查看特定于租户的内容。

注　来自插件清单的对象不是多租户。这些对象是系统范围的一部分。

VMware, Inc. 保留所有权利。

管理旧版自定义内容

5

在启用 vRealize Orchestrator 中的多租户功能后，所有现有的对象都将成为系统范围的对象。

与即时可用的 Orchestrator 平台中包含的对象和资源类似，您在启用多租户功能之前创建的自定义对象将在只读模式下在所有租户之间共享，并且只有系统管理员可以对其进行修改或删除。

隔离旧版自定义内容

如果您想要防止自定义内容成为系统范围的内容，您可在启用多租户功能之前将自定义对象和资源导出为软件包，并将其从 Orchestrator 服务器删除。在启用多租户功能后，您可以将这些对象导入到一个特定租户或多个租户。

注　您可以将同一软件包分别导入到多个租户。您无法将系统范围内的软件包导入到租户，也无法将以租户特定内容的形式存在的软件包导入到系统范围。

前提条件

确认多租户功能在 vRealize Orchestrator 7.4 上处于禁用状态。

步骤

1. 以管理员身份登录到 Orchestrator 客户端。
2. 创建软件包，以供导出。

   请参见创建软件包。
3. 导出软件包。

   请参见导出软件包。
4. 删除从 Orchestrator 服务器中导出的软件包。

   请参见移除软件包。
5. 启用多租户功能。

   请参见启用 vRealize Orchestrator 多租户功能。
6. 以租户管理员身份登录 Orchestrator 客户端，以将软件包导入到特定租户。
7. 导入软件包。

   请参见导入软件包。

VMware, Inc. 保留所有权利。