Red Hat Ansible Automation Platform 2.4

管理自动化中心中的内容

在自动化中心中创建和管理集合、内容和存储库

Last Updated: 2024-07-03

Red Hat Ansible Automation Platform 2.4 管理自动化中心中的内容

在自动化中心中创建和管理集合、内容和存储库

法律通告

摘要

本指南介绍了如何在自动化中心中创建、编辑、删除和移动内容。

目录

对红帽文档提供反馈

如果您对本文档有任何改进建议，或发现了任何错误，请联系 https://access.redhat.com 的技术支持，以使用 **docs-product** 组件在 Ansible Automation Platform JIRA 项目中创建一个问题。

第 1 章 在自动化中心中红帽认证的、经过验证的 ANSIBLE GALAXY 内容

Ansible 认证的内容集合包括在订阅 Red Hat Ansible Automation Platform 中。Red Hat Ansible 内容包括两种类型的内容：Ansible 认证内容集合和 Ansible 验证的内容。使用 Ansible 自动化中心（Automation hub），您可以从所有形式的 Ansible 内容访问并策展一组唯一的集合。

Red Hat Ansible 内容包含两种类型的内容：

- Ansible 认证的内容集合
- Ansible 验证的内容集合

Ansible 验证的集合可通过平台安装程序在私有自动化中心中可用。当您使用捆绑的安装程序下载 Red Hat Ansible Automation Platform 时，验证的内容默认预先填充到私有自动化中心中，但这需要您将私有自动化中心作为清单的一部分启用。

如果您不使用捆绑包安装程序，您可以使用红帽提供的 Ansible playbook 来安装验证的内容。如需更多信息，请参阅 Ansible 验证的内容。

您可以通过下载其软件包来手动更新这些集合。

为什么认证 Ansible 集合？

Ansible 认证计划为红帽与生态系统合作伙伴之间的 Red Hat Ansible 认证内容提供共享支持声明。最终客户在 Ansible 和认证合作伙伴内容时遇到问题，可以创建支持问题单，例如：请求信息，或者红帽的问题，并期望红帽及生态系统合作伙伴可以解决票据。

红帽为认证合作伙伴提供了"进入市场"的优势，以促进市场意识、生成需求和销售协作方式。

Red Hat Ansible 认证的内容集合通过 Ansible Automation Hub （需要订阅）发布，它是一个集中支持 Ansible 内容的存储库。作为经过认证的合作伙伴，向 Ansible Automation Hub 发布集合可让最终客户管理其生产环境中如何使用可信自动化内容及已知支持生命周期的能力。

有关认证解决方案的更多信息，请参阅 Red Hat Partner Connect。

如何获得集合认证？

有关认证您的集合的说明，请参阅 Red Hat Partner Connect 上的 Ansible 认证策略指南。

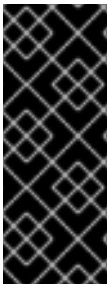
认证集合的联合支持协议如何工作？

当用户针对一个认证的集合报告一个问题时，红帽支持团队会评估这个问题，并检查问题是否存在于 Ansible 或 Ansible 的使用情况中。红帽支出团队检查这个问题是否与认证的集合相关。如果是认证集合的问题，红帽支持团队将根据预先同意的方式（如 TSANet）将问题传送到认证集合的供应商所有者。

我能否创建并认证仅包含 Ansible 角色的集合？

您可以创建并认证仅包含角色的集合。当前测试要求侧重于包含模块的集合，我们目前正在进行开发用于测试仅包含角色的集合的认证过程。如需更多信息，请联系 ansiblepartners@redhat.com。

1.1. 在自动化中心中同步 ANSIBLE 内容集合



重要

从 2.4 发行版本开始，您仍然可以同步内容，但同步列表已弃用，并将在以后的发行版本中删除。

要同步内容，您现在可以从 rh-certified remote 上传手动创建的要求文件。

远程是允许您从外部集合源将内容同步到自定义存储库的配置。

您可以通过创建同步列表或要求文件，使用 Ansible Automation hub 来向用户分发相关的 Red Hat Ansible 认证内容集合。有关使用要求文件的更多信息，请参阅*使用 Ansible 集合*指南中的安装带有要求文件的多个集合。

1.1.1. Red Hat Ansible 认证内容集合同步列表的说明

同步列表(synclist)是红帽认证集合的策展组，由您的机构管理员组装。它将与本地 Ansible Automation hub 同步。使用同步列表，可以管理您需要的内容，并排除不必要的集合内容。从 console.redhat.com 上作为红帽内容的一部分提供的同步列表，并管理您的同步列表

每个同步列表都有自己的唯一的存储库 URL，您可以使用它们指定为自动化中心中内容的远程源。您可以使用 API 令牌安全地访问每个同步列表。

1.1.2. 创建 Red Hat Ansible 认证内容集合的同步列表

您可以在 console.redhat.com 上的 Ansible 自动化中中创建一个策展的 Red Hat Ansible 认证内容的同步列表。您的同步列表存储库位于 **Collection → Repositories** 下的自动化中心导航面板中，每当您在 Ansible 认证的内容集合中管理内容时，都会更新它。

在您的初始机构同步列表中，默认包含所有 Ansible 认证的内容集合。

前提条件

- 有一个有效的 Ansible Automation Platform 订阅。
- 具有 console.redhat.com 的机构管理员权限。
- 以下域名是防火墙或代理的允许列表的一部分。从自动化中心或 Galaxy 服务器成功连接并下载集合需要它们：
  - **galaxy.ansible.com**
  - **cloud.redhat.com**
  - **console.redhat.com**
  - **sso.redhat.com**
- Ansible Automation hub 资源存储在 Amazon Simple Storage 中。以下域名必须位于允许列表中：
  - **automation-hub-prd.s3.us-east-2.amazonaws.com**
  - **ansible-galaxy.s3.amazonaws.com**
- 在使用自签名证书或红帽域时，SSL 检查会被禁用。

流程

流程

1. 登录到 **console.redhat.com**。
2. 进入 **Automation Hub → Collections**。
3. 在每个集合上设置切换开关，以排除或将其包含在同步列表中。
4. 要启动远程存储库同步，请导航到自动化中心并选择 **Collection → Repositories**。
5. 点 **More Actions** 图标， ⋮ ，选择 **Sync** 将远程存储库同步启动到您的私有自动化中心。
6. 可选： 如果已经配置了远程存储库，请通过手动将 Red Hat Ansible 认证 Content Collections 同步到私有自动化中心，来更新您提供给本地用户可用的集合内容。

1.2. 配置 ANSIBLE 自动化中心远程存储库以同步内容

使用远程配置配置您的私有自动化中心，使其与 **console.redhat.com** 上托管的 Ansible 认证内容集合或 Ansible Galaxy 中的集合同步。

重要

从 2.4 发行版本开始，您仍然可以同步内容，但同步列表已弃用，并将在以后的发行版本中删除。

要同步内容，您现在可以从 rh-certified remote 上传手动创建的要求文件。

远程是允许您从外部集合源将内容同步到自定义存储库的配置。

Ansible Galaxy 和 Ansible 自动化中心之间的区别是什么？
发布到 Ansible Galaxy 的集合是 Ansible 社区发布的最新内容，没有与它们关联的联合支持声明。Ansible Galaxy 是 Ansible 社区访问内容的推荐前端目录。

发布到 Ansible 自动化中（Ansible Automation Hub）的集合面向红帽及所选合作伙伴的合作。客户需要 Ansible 订阅才能访问和下载 Ansible 自动化中心中的集合。认证的集合（certified collection）代表红帽和相关的合作伙伴已制定了战略性的合作关系，并可以一起为客户提供帮助，其内容已经过了额外的测试和验证。

如何在 Ansible Galaxy 上请求命名空间？
要通过 Ansible Galaxy GitHub 问题请求命名空间，请按照以下步骤执行：

- 发送电子邮件到 ansiblepartners@redhat.com
- 包括用于在 Ansible Galaxy 上注册的 GitHub 用户名。

您必须至少登录一次才能验证系统。

用户添加为命名空间的管理员后，您可以使用自助式进程添加更多管理员。

Ansible Galaxy 命名空间命名是否存在任何限制？
集合命名空间必须遵循 python 模块名称惯例。这意味着集合应具有简短的、由小写字符组成的名称。您可以在名称中使用下划线以提高它的可读性。

1.2.1. 创建远程配置的原因

位于 Collections Remote 中的每个远程配置都提供关于存储库 **最后一次更新** 时的 **社区和 rh-certified** 存储库的信息。**您可以使用 Collection → Repositories 页面中包含的 Edit 和 Sync 功能随时向 Ansible Automation hub 添加新内容。**

1.2.2. 检索红帽认证集合的同步 URL 和 API 令牌

您可以将您的机构从 **console.redhat.com** 提供的 Ansible 认证内容集合同步到私有自动化中心。API 令牌是用于保护内容的 secret 令牌。

前提条件

- 您有机构管理员权限在 console.redhat.com 上创建同步列表。

流程

1. 以机构管理员身份登录到 **console.redhat.com**。
2. 进入 **Automation Hub → Connect to Hub**。
3. 在 **离线令牌** 下，点 **Load token**。
4. 点 **Copy to clipboard** 复制 API 令牌。
5. 将 API 令牌粘贴到文件中，并存储在安全位置。

1.2.3. 配置 rh-certified 远程仓库并同步 Red Hat Ansible 认证的内容集合

您可以编辑 **rh-certified** 远程存储库，将 console.redhat.com 上托管的自动化中心的集合同步到私有自动化中心。默认情况下，您的私有自动化中心 **rh- certified** 存储库包含整个 Ansible 认证内容集合组的 URL。

要只使用您的机构指定的集合，私有自动化中心管理员可以从 **rh-certified** remote 中手动创建要求文件。

有关使用要求文件的更多信息，请参阅 *使用 Ansible 集合* 指南中的安装带有要求文件的多个集合。

如果您的要求文件中有集合 **A**、**B** 和 **C**，并且新的集合 **X** 被添加到要使用的 console.redhat.com 中，则必须将 **X** 添加到您的私有自动化中心要求文件中以同步它。

前提条件

- 您有有效的**修改 Ansible 仓库内容**权限。有关权限的更多信息，请参阅为您的私有自动化中心配置用户访问权限。
- 您已从 console.redhat.com 上的自动化中心托管服务中检索 Sync URL 和 API Token。
- 您已配置了端口 443 的访问权限。这是同步认证集合所必需的。如需更多信息，请参阅 Red Hat Ansible Automation Platform 规划指南中的网络 端口和协议 部分中的自动化中心表。

流程

1. 登录到您的私有自动化中心。
2. 在导航面板中，选择 **Collections → Remotes**。
3. 在 **rh-certified** 远程仓库中，点 **More Actions** 图标 ⋮ 并点k **Edit**。

4. 在 **URL** 字段中，粘贴 **Sync URL**。
5. 在 **Token** 字段中，粘贴您从 console.redhat.com 获取的令牌。
6. 点击 **Save**。
   现在，您可以在 console.redhat.com 上的机构同步列表和私有自动化中心之间同步集合。
7. 点 **More Actions** 图标 ⋮ 并选择 **Sync**。

验证

Sync status 通知会更新，以通知您红帽认证内容集合同步已完成。

- 从集合内容下拉列表中选择 **Red Hat certified**，以确认您的集合内容已成功同步。

1.2.4. 配置社区远程存储库并同步 Ansible Galaxy 集合。

您可以编辑 **community** 远程存储库，将所选集合从 Ansible Galaxy 同步到私有自动化中心。默认情况下，您的私有自动化中心 community 存储库定向到 **galaxy.ansible.com/api/**。

前提条件

- 您有**修改 Ansible 存储库内容**的权限。有关权限的更多信息，请参阅为您的私有自动化中心配置用户访问权限。
- 您有一个 **requirements.yml** 文件，用于标识要从 Ansible Galaxy 同步的集合，如下例所示：

  Requirements.yml 示例

```
collections:
  # Install a collection from Ansible Galaxy.
  - name: community.aws
    version: 5.2.0
    source: https://galaxy.ansible.com
```

流程

1. 登录到自动化中心。
2. 在导航面板中，选择 **Collections → Remotes**。
3. 在 **Community** 远程中，点 **More Actions** 图标 ⋮ and select **Edit**。
4. 在 **YAML requirements** 字段中，点 **Browse** 并在本地机器上找到 **requirements.yml** 文件。
5. 点击 **Save**。
   现在，您可以将 **requirements.yml** 文件中标识的集合从 Ansible Galaxy 同步到私有自动化中心。
6. 点 **More Actions** 图标 **HBAC**，然后选择 **Sync** 以同步来自 Ansible Galaxy 和 Ansible Automation Hub 的集合。

验证

Sync status 通知会更新，以告知您与 Ansible Automation Hub 同步 Ansible Galaxy 集合的完成或失败。

- 从集合内容下拉列表中选择 **Community** 以确认同步成功。

1.2.5. 配置代理设置

如果您的私有自动化中心位于网络代理后面，您可以在远程上配置代理设置，以同步位于本地网络中的内容。

前提条件

- 您有有效的**修改 Ansible 仓库内容**权限。有关权限的更多信息，请参阅为您的私有自动化中心配置用户访问权限。
- 您有来自本地网络管理员的代理 URL 和凭证。

流程

1. 登录到私有自动化中心。
2. 在导航面板中，选择 **Collections → Remotes**。
3. 在 **rh-certified** 或 **Community** 远程中，点 **More Actions** 图标 uild **Defaults**，然后选择 **Edit**。
4. 展开 **Show advanced options** 下拉菜单。
5. 在适当的字段中输入代理 URL、代理用户名和代理密码。
6. 点击 **Save**。

1.3. 在私有自动化中心中的集合和内容签名

作为机构的自动化管理员，您可以配置私有自动化中心，以根据机构中的不同组签名和发布 Ansible 内容集合。

为提高安全性，自动化创建者可以配置 Ansible-Galaxy CLI 以验证这些集合，确保在上传到自动化中心后不会更改它们。

1.3.1. 在私有自动化 hub 中配置内容签名

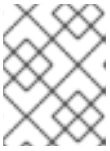
要成功签名并发布 Ansible 认证的内容集合，您必须配置私有自动化中心进行签名。

前提条件

- 您的 TIPC 密钥对已安全设置并管理您的机构。
- 您的公钥-私钥对有权在私有自动化中心上配置内容签名。

流程

1. 创建只接受文件名的签名脚本。



注意

此脚本充当签名服务，必须使用通过 **PULP_SIGNING_KEY_FINGERPRINT** 环境变量指定的密钥为该文件生成 ascii-armored 分离 **gpg** 签名。

该脚本打印一个 JSON 结构，其格式如下：

```
{"file": "filename", "signature": "filename.asc"}
```

所有文件名都是当前工作目录中的相对路径。对于分离的签名，文件名必须保持相同。

Example:

以下脚本为内容生成签名：

```
#!/usr/bin/env bash

FILE_PATH=$1
SIGNATURE_PATH="$1.asc"

ADMIN_ID="$PULP_SIGNING_KEY_FINGERPRINT"
PASSWORD="password"

# Create a detached signature
gpg --quiet --batch --pinentry-mode loopback --yes --passphrase \
  $PASSWORD --homedir ~/.gnupg/ --detach-sign --default-key $ADMIN_ID \
  --armor --output $SIGNATURE_PATH $FILE_PATH

# Check the exit status
STATUS=$?
if [ $STATUS -eq 0 ]; then
  echo {\"file\": \"$FILE_PATH\", \"signature\": \"$SIGNATURE_PATH\"}
else
  exit $STATUS
fi
```

部署私有自动化中心后，为 Ansible Automation Platform 集群启用了签名后，会在集合中会显示新的 UI。

2. 查看 Ansible Automation Platform 安装程序清单文件中的以 **automationhub_*** 开头的选项。

```
[all:vars]
.
.
.
automationhub_create_default_collection_signing_service = True
automationhub_auto_sign_collections = True
automationhub_require_content_approval = True
automationhub_collection_signing_service_key = /abs/path/to/galaxy_signing_service.gpg
automationhub_collection_signing_service_script = /abs/path/to/collection_signing.sh
```

两个新密钥(**automationhub_auto_sign_collections** 和 **automationhub_require_content_approval**)表示必须签名集合，并在上传到私有自动化中心后需要批准。

1.3.2. 在私有自动化中心中使用内容签名服务

在私有自动化中心上配置内容签名后，您可以手动为新集合签名，或使用新签名替换现有签名。当用户下载特定集合时，此签名表示它们的集合是它们，在认证后没有被修改。

在以下情况下，您可以在私有自动化中心上使用内容签名：

- 您的系统没有配置自动签名，您必须使用手动签名过程来签署集合。
- 自动配置的集合中的当前签名已损坏，需要新的签名。
- 对于之前签名的内容，您需要额外的签名。
- 您希望在集合中轮转签名。

流程

1. 登录到您的 Ansible Automation Platform。
2. 在导航面板中，选择 **Collections → Approval**。Approval dashboard 将打开并显示一个集合列表。
3. 对于您要签名的每个集合，点 **Sign and approve**。

验证

- 验证您签名和手动批准的集合是否在 **Collections** 选项卡中显示。

1.3.3. 下载签名公钥

为和批准集合签名后，从自动化中心 UI 下载签名公钥。您必须下载公钥，然后才能将其添加到本地系统密钥环中。

流程

1. 登录到您的自动化中心。
2. 在导航面板中，选择 **Signature Keys**。签名密钥仪表板显示多个键的列表：集合和容器镜像。
   - 要验证集合，请下载前缀为 **collections-** 的密钥。
   - 要验证容器镜像，请下载前缀为 **container-** 的密钥。
3. 选择以下方法之一下载您的公钥：
   - 选择菜单图标，然后点 **Download Key** 以下载公钥。
   - 从列表中选择公钥，然后点 *Copy to clipboard* 图标。
   - 点 ***Public Key*** 选项卡中的下拉菜单，再复制整个公钥块。

使用您复制的公钥来验证您要安装的内容集合。

1.3.4. 配置 Ansible-Galaxy CLI 以验证集合

您可以配置 Ansible-Galaxy CLI 来验证集合。这样可确保下载的集合由您的机构批准，且在上传到自动化中心后没有改变。

如果某个集合由自动化中心签名，服务器会提供 ASCII armored，GPG-detached 签名在使用它验证集合的内容前验证 **MANIFEST.json** 的真实性。您必须通过为 **ansible-galaxy** 配置密钥环或使用 **--keyring** 选项提供路径来选择签名验证。

前提条件

- 签名的集合在自动化中心中可用于验证签名。
- 认证的集合可以由机构中的批准角色签名。
- 验证的公钥已添加到本地系统密钥环中。

流程

1. 要将公钥导入到用于 **ansible-galaxy** 的非默认密钥环中，请运行以下命令：

```
gpg --import --no-default-keyring --keyring ~/.ansible/pubring.kbx my-public-key.asc
```

注意

除了自动化中心提供的任何签名外，也可在要求文件和命令行中提供签名源。签名源应当是 URI。

2. 要使用额外签名验证 CLI 上提供的集合名称，请运行以下命令：

```
ansible-galaxy collection install namespace.collection
--signature https://examplehost.com/detached_signature.asc
--signature file:///path/to/local/detached_signature.asc --keyring ~/.ansible/pubring.kbx
```

您可以多次使用这个选项提供多个签名。

3. 确认要求文件中的集合在集合的签名密钥后列出任何其他签名源，如下例所示。

```
# requirements.yml
collections:
  - name: ns.coll
    version: 1.0.0
    signatures:
      - https://examplehost.com/detached_signature.asc
      - file:///path/to/local/detached_signature.asc

ansible-galaxy collection verify -r requirements.yml --keyring ~/.ansible/pubring.kbx
```

当您从自动化中心安装集合时，服务器提供的签名会与安装的集合一起保存，以验证集合的真实性。

4. （可选）如果您需要在不查询 Ansible Galaxy 服务器的情况下再次验证集合的内部一致性，请使用 **--off 命令行选项运行之前使用的相同命令**。

有集合命名建议吗？

创建具有 **company_name.product** 格式的集合。这种格式意味着多个产品可以在 company 命名空间下具有不同的集合。

如何在 Ansible Automation Hub 上获取命名空间？
默认情况下，Ansible Galaxy 上使用的命名空间也由 Ansible 合作伙伴团队在 Ansible Automation Hub 上使用。有关任何查询和澄清，请联系 ansiblepartners@redhat.com。

1.4. ANSIBLE 验证的内容

Red Hat Ansible Automation Platform 包括 Ansible 验证的内容（Ansible validated content），可补充现有 Red Hat Ansible 认证的内容。

Ansible 验证的内容提供了一个由专家领导的路径，用于在各种平台（包括红帽和合作伙伴的平台）上执行操作任务，。

1.4.1. 使用安装程序配置验证的集合

当您下载并运行捆绑包安装程序时，认证和验证的集合会自动上传。认证的集合上传到 **rh-certified** 存储库中。验证的集合上传到 **validated** 的存储库。

您可以使用两个变量修改默认配置：

- **automationhub_seed_collections** 是一个布尔值，用于定义是否启用预加载。
- **automationhub_collection_seed_repository**.可让您指定在设置为 **true** 时上传的内容类型的变量。可能的值是 **certified** 或 **validated**。如果缺少这两个，内容集会被上传。

1.4.2. 使用 tarball 安装验证的内容

如果您不使用捆绑包安装程序，您可以使用独立 tarball **ansible-validated-content-bundle-1.tar.gz**。您还可以稍后使用此独立 tarball 更新任何环境中验证的内容，当一个较新的 tarball 可用时，无需重新运行捆绑包安装程序。

前提条件

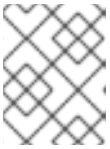
您需要以下变量来运行 playbook。

Name	描述
automationhub_admin_password	您的管理密码。
automationhub_api_token	为自动化中心生成的 API 令牌。
automationhub_main_url	例如 ：**https://automationhub.example.com**
automationhub_require_content_approval	布尔值(**true** 或 **false**) 这必须与自动化中心部署期间使用的值匹配。 安装程序将此变量设置为 **true**。

流程

1. 要获取 tarball，进入到 Red Hat Ansible Automation Platform 下载 页，然后选择 **Ansible Validated Content**。
2. 上传内容并定义变量（本例使用 **automationhub_api_token**）：

```
ansible-playbook collection_seed.yml
-e automationhub_api_token=<api_token>
-e automationhub_main_url=https://automationhub.example.com
-e automationhub_require_content_approval=true
```



注意

使用 **automationhub_admin_password** 或 **automationhub_api_token**，而不是两者同时使用。

完成后，集合会在私有自动化中心的验证集合部分中看到。用户现在可以从私有自动化中心查看和下载集合。

其它资源

如需有关运行 ansible playbook 的更多信息，请参阅 ansible-playbook。

第 2 章 在自动化 HUB 中管理集合

作为内容创建者，您可以使用自动化中心中的命名空间来策展和管理集合，以实现以下目的：

- 使用命名空间创建组来策展命名空间，并将集合上传到私有自动化中心
- 在命名空间中添加信息和资源，以帮助在其自动化任务中集合的最终用户
- 将集合上传到命名空间
- 查看命名空间导入日志，以确定上传集合及其当前批准状态是否成功或失败。

有关创建内容的详情，请查看 Red Hat Ansible Automation Platform Creator 指南 。

2.1. 使用命名空间管理 AUTOMATION HUB 中的集合

命名空间是 Automation Hub 中的唯一位置，您可以上传并发布内容集合。对 Automation Hub 中的命名空间的访问取决于有权管理相应内容和相关信息的组。

您可以使用 Automation Hub 中的命名空间组织在您的机构内开发的集合，以用于内部发布和使用。

如果使用命名空间，您必须有一个具有创建、编辑集合并上传到命名空间的组。上传到命名空间的集合需要管理员批准，然后才能发布并供使用。

2.1.1. 为内容 Curator 创建新组

您可以在私有自动化中心中创建一个新组，旨在支持机构中的内容策展。这个组可以贡献内部开发的集合，以便在私有自动化中心中发布。

为帮助内容开发人员创建命名空间并将其内部开发的集合上传到私有自动化中心，您必须首先创建和编辑组并分配所需的权限。

前提条件

- 在私有自动化中心中具有管理权限，并可创建组。

流程

1. 登录到您的私有自动化中心。
2. 在导航面板中，选择 **User Access → Groups**，再点 **Create**。
3. 在界面中输入 **Content Engineering** 作为组的 **Name**，再点 **Create**。您已创建了新组，组页将打开。
4. 在 **Permissions** 选项卡中，点 **Edit**。
5. 在 **Namespaces** 下，为 **Add Namespace**、**Upload to Namespace** 和 **Change Namespace** 添加权限。
6. 点击 **Save**。
   使用您分配的权限创建新组。然后您可以将用户添加到组中。
7. 点 **Groups** 页面中的 **Users** 选项卡。

8. 点**Add**。
9. 选择用户并点 **Add**。

2.1.2. 创建命名空间

您可以创建一个命名空间来组织内容开发人员上传到自动化中心的集合。在创建命名空间时，您可以在自动化中心中分配一个组作为该命名空间的所有者。

前提条件

- 您有 Add Namespaces 和 Upload to Namespaces 权限。

流程

1. 登录到您的私有自动化中心。
2. 在导航面板中，选择 **Collections → Namespaces**。
3. 点 **Create** 并输入 **命名空间名称**。
4. 分配一组 **Namespace owners**。
5. 点 **Create**。

您的内容开发人员现在可以将集合上传到您的新命名空间中，并允许分配给所有者的组中的用户上传集合。

2.1.3. 在命名空间中添加额外信息和资源

您可以将信息添加到命名空间中包含的集合中,并为用户提供资源。添加徽标和描述，并将用户链接到 GitHub 存储库、发布跟踪程序或其他在线资产。您还可以在 **Edit resources** 选项卡中输入标记文本，使其包含更多信息。这对在自动化任务中使用集合的用户非常有用。

前提条件

- 您有**更改命名空间**的权限。

流程

1. 登录到您的私有自动化中心。
2. 在导航面板中，选择 **Collections → Namespaces**。
3. 点 **More Actions** icon ⋮ 选择 **Edit namespace**。
4. 在 **Edit details** 选项卡中，在字段中输入信息。
5. 点 **Edit resources** 选项卡在文本字段中输入标记。
6. 点击 **Save**。

您的内容开发人员现在可以将集合上传到您的新命名空间中，并允许分配给所有者的组中的用户上传集合。

当您创建命名空间时，具有上传权限的组可以开始添加其集合以进行批准。批准后，命名空间中的集合会出现在 **Published** 存储库中。

2.1.4. 将集合上传到您的命名空间中

您可以将 **tar.gz** 文件格式内部开发的集合上传到私有自动化中心命名空间中，供自动化 hub 管理员审核和批准。批准后，集合将移到自动化中心用户可以查看并下载它的 **Published** 内容存储库。

注意

按如下方式格式化您的集合文件名：<my_namespace-my_collection-1.0.0.tar.gz>

前提条件

- 您有一个命名空间，可以将集合上传到这个命名空间。

流程

1. 登录到您的私有自动化中心。
2. 在导航面板中，选择 **Collections → Namespaces** 并选择命名空间。
3. 点 **Upload collection**。
4. 从 **New collection** 对话框中，点 **Select file**。
5. 选择要上传的集合。
6. 点 **Upload**。

My Imports 屏幕显示测试摘要，并在集合上传成功或失败时通知您。

2.1.5. 查看命名空间导入日志

您可以查看上传到命名空间的集合状态，以评估进程是否成功或失败。

导入的集合信息包括：

Status
完成或失败

批准状态
等待批准或批准

版本
上传的集合的版本

导入日志
在集合导入过程中执行的活动

前提条件

- 您可以访问可上传集合的命名空间。

流程

1. 登录到您的私有自动化中心。
2. 在导航面板中，选择 **Collections → Namespaces**。
3. 选择一个命名空间。
4. 点 **More Actions** 图标 ⋮ 选择 **My imports**。
5. 使用 search 字段或找到列表中导入的集合。
6. 点导入的集合。
7. 查看集合导入详情，以确定命名空间中的集合状态。

2.1.6. 删除命名空间

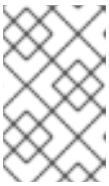
您可以删除不需要的命名空间来管理自动化中心服务器上的存储。您必须首先确保命名空间不包含依赖项的集合。

前提条件

- 您要删除的命名空间没有依赖项集合。
- 有 **Delete namespace** 权限。

流程

1. 登录到您的私有自动化中心。
2. 在导航面板中，选择 **Collections → Namespaces**。
3. 点要删除的命名空间。
4. 点 **More Actions** 图标 ⋮，然后点 **Delete namespace**。



注意

如果 **Delete namespace** 按钮被禁用，命名空间会包含带有依赖项的集合。检查此命名空间中的集合，并删除任何依赖项。如需更多信息，请参阅删除自动化中心上的集合。

您删除的命名空间及其关联的集合现已从命名空间列表视图中删除。

2.2. 管理 AUTOMATION HUB 中内部集合的发布过程

使用自动化中心管理和发布您机构中开发的内容集合。您可以在命名空间中上传和组集合。它们需要管理批准才能出现在 **发布的**内容存储库中。发布集合后，您的用户可以访问并下载它以供使用。

您可以拒绝未满足机构认证标准的集合。

2.2.1. 关于批准

您可以使用导航面板中的 **Approval** 功能管理自动中心中上传的集合。

批准仪表板

默认情况下，Approval 仪表板列出所有具有 Needs Review 状态的集合。您可以检查它们是否包含在您的 Published 存储库中。

查看集合详情

您可以点击 Version 号来查看有关集合的更多信息。

过滤集合

根据 Namespace, Collection Name or Repository 过滤集合来找到内容并更新它的状态。

2.2.2. 为内部发布批准集合

您可以批准上传到各个命名空间的集合供内部发布和使用。所有等待检查的集合都位于 Staging 存储库的 Approval 选项卡下。

前提条件

- 您有**修改 Ansible 存储库内容**的权限。

流程

1. 在导航面板中，选择 Collections → Approval。
   需要批准的集合会检查状态 Needs review。
2. 选择要进行检查（review）的集合。
3. 点 Version 查看集合的内容。
4. 点 **Certify** 批准集合。

批准的集合将移到 Published 存储库，用户可以在其中查看并下载它们以供使用。

2.2.3. 拒绝上传的集合以检查

您可以拒绝上传到单个命名空间的集合。所有等待检查的集合都位于 Staging 存储库的 Approval 选项卡下。

需要批准的集合会检查状态 Needs review。点 Version 查看集合的内容。

前提条件

- 您有**修改 Ansible 存储库内容**的权限。

流程

1. 在导航面板中，选择 Collections → Approval。
2. 找到要检查的集合。
3. 点 **Reject** 以拒绝集合。

您拒绝发布的集合将移到 Rejected 仓库中。

2.3. 使用自动化中心进行存储库管理

作为自动化中心管理员，您可以在存储库之间创建、编辑、删除和移动自动化内容集合。

2.3.1. Automation hub 中的仓库类型

在自动化中心中，您可以根据是否要验证集合，将集合发布到两种类型的存储库：

Staging 软件仓库

任何有权上传到命名空间的用户都可以将集合发布到这些存储库中。这些存储库中的集合在搜索页面中不可用。相反，它们会显示在管理员验证的批准仪表板中。staging 存储库使用 **pipeline=staging** 标签标记。

自定义软件仓库

对存储库具有写入权限的任何用户都可以将集合发布到这些存储库。自定义软件仓库可以是公共的，其中所有用户都可以查看它们，或者只有具有查看权限的用户可以看到它们。这些存储库不会在批准仪表板中显示。如果存储库所有者启用了搜索，则集合可能会出现在搜索结果中。

默认情况下，Automation hub 附带了一个 staging 存储库，当没有指定存储库来上传集合时会自动使用。用户可以在存储库创建期间创建新的暂存 存储库。

2.3.2. 在自动化中心中批准自定义软件仓库的批准管道

在自动化中心中，您可以将集合批准到带有 **pipeline=approved** 标签的任何存储库中。默认情况下，自动化中心附带了一个用于批准的内容的存储库，但您可以选择从存储库创建屏幕中添加更多。您不能直接发布到带有 **pipeline=approved** 标签的存储库。集合必须首先经过 staging 存储库，然后才能发布到 'pipleline=approved' 存储库。

自动批准

启用自动批准后，任何上传到 staging 存储库的集合将自动提升到标记为 **pipeline=approved** 的所有存储库。

批准需要

禁用自动批准后，管理员可以查看批准仪表板并查看上传到任何 staging 存储库的集合。点 **Approve** 显示批准的存储库列表。从此列表中，管理员可以选择要提升内容的一个或多个存储库。
如果只有一个已批准的存储库，集合会自动移到其中，管理员不会被提示选择存储库。

拒绝

拒绝的集合会自动放入被拒绝的存储库，该存储库已预安装。

2.3.3. 基于角色的访问控制来限制对自定义存储库的访问

使用基于角色的访问控制(RBAC)通过基于用户角色定义访问权限来限制用户对自定义存储库的访问。默认情况下，用户可以查看其自动化中心中的所有公共存储库，但它们无法修改存储库，除非其角色允许他们这样做。相同的逻辑适用于存储库上的其他操作。例如，您可以通过更改其角色权限，删除用户从自定义存储库下载内容的能力。有关 在自动化中心中管理用户访问权限 的信息，请参阅为私有自动化中心配置用户访问。

2.3.4. 在自动化中心中创建自定义存储库

当使用 Red Hat Ansible Automation Platform 创建软件仓库时，您可以将存储库配置为私有，或者从搜索结果中隐藏它。

流程

1. 登录到自动化中心。

2. 在导航面板中，选择 **Collection → Repositories**。
3. 点 **Add repository**。
4. 输入**存储库名称**。
5. 在 **Description** 字段中，描述存储库的目的。
6. 要在每次进行更改时保留您的仓库的早期版本，请选择 **保留的版本数量**。保留的版本数量范围是 0 到无限。要保存所有版本，将此设置为 null。

注意

如果对自定义存储库有更改有问题，您可以恢复到保留的不同存储库版本。

7. 在 **Pipeline** 字段中，为仓库选择一个管道。此选项定义可以将集合发布到存储库的人员。

Staging

任何人都被允许将自动化内容发布到存储库中。

已批准

需要添加到此存储库的集合，才能通过暂存存储库通过批准过程进行。如果启用了自动批准，任何上传到 staging 存储库的集合将自动提升到所有批准的存储库。

None

任何具有存储库权限的用户都可以直接发布到存储库，存储库不是批准管道的一部分。

8. 可选： 要从搜索结果中隐藏存储库，选择 **Hide from search**。默认选择这个选项。
9. 可选： 要使存储库私有，请选择 **Make private**。这会防止没有权限的用户查看存储库。
10. 要将远程存储库中的内容同步到此存储库中，请选择 **Remote**，然后选择包含您要包含在自定义存储库中的集合的远程。如需更多信息，请参阅存储库同步。
11. 点击 **Save**。

后续步骤

- 创建存储库后，会显示详情页面。
  在这里，您可以提供对存储库的访问、检查或添加集合，并使用自定义存储库的保存版本。

2.3.5. 提供对自定义自动化中心存储库的访问权限

默认情况下，私有存储库和自动化内容集合在系统的所有用户中是隐藏的。所有用户都可以查看公共存储库，但不能修改。使用这个流程提供对自定义存储库的访问。

流程

1. 登录到私有自动化中心。
2. 在导航面板中，选择 **Collection → Repositories**。
3. 在列表中找到您的存储库，点 **More Actions** icon ⋮, 然后选择 **Edit**。
4. 选择 **Access** 选项卡。

5. 为 **Repository owners** 选择一个组。
   有关实施 用户访问的信息，请参阅为私有自动化中心 配置用户访问。
6. 选择您要分配给所选组的角色。
7. 点击 **Save**。

2.3.6. 在自动化中心存储库中添加集合

创建存储库后，您可以开始向其中添加自动化内容集合。

流程

1. 在导航面板中，选择 **Collection → Repositories**。
2. 在列表中找到您的存储库，点 **More Actions** icon ⋮, 然后选择 **Edit**。
3. 选择 **Collections version** 选项卡。
4. 点 **Add Collection** 并选择您要添加到存储库中的集合。
5. 点 **Select**。

2.3.7. 恢复到不同的自动化中心存储库版本

当从存储库添加或删除自动化内容集合时，会创建一个新版本。如果对存储库的更改出现问题，您可以恢复到以前的版本。恢复是一种安全操作，且不会从系统中删除集合，而是更改与存储库关联的内容。保存的版本数量在创建存储库时由 **Retained number of versions** 设置定义。

流程

1. 登录到私有自动化中心。
2. 在导航面板中，选择 **Collection → Repositories**。
3. 在列表中找到您的存储库，点 **More Actions** icon ⋮, 然后选择 **Edit**。
4. 找到您要恢复到的版本，然后点击 **More Actions** 图标，然后选择 **Revert to this version**。
5. **点 Revert。**

2.3.8. 在自动化中心中管理远程配置

您可以将远程配置设置为运行自动化中心的任何服务器。远程配置允许您从外部集合源将内容同步到自定义存储库。

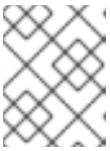
2.3.8.1. 在自动化中心中创建远程配置

您可以使用 Red Hat Ansible Automation Platform 创建到外部集合源的远程配置。然后，您可以将内容从这些集合同步到自定义存储库。

流程

1. **登录到自动化中心。**

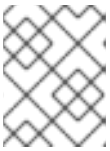
2. 在导航面板中，选择 Collections → Remotes。
3. 点 Add Remote。
4. 为远程配置输入一个名称。
5. 输入远程服务器的 URL，包括特定存储库的路径。



注意

要查找远程服务器 URL 和存储库路径，请导航到 Collection → Repositories，选择您的存储库，再单击 Copy CLI configuration。

6. 输入访问外部集合所需的 Token 或 Username 和 Password，将凭证配置为远程服务器。



注意

要从导航面板中生成令牌，请选择 Collections → API 令牌，点 Load token 并复制载入的令牌。

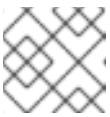
7. 要从 console.redhat.com 访问集合，输入 SSO URL 以登录到身份提供程序(IdP)。
8. 选择或创建 YAML 要求文件来标识集合和版本范围，以与自定义存储库同步。例如，要只下载 kubernetes 和 AWS 集合版本 5.0.0 或更高版本，要求文件类似如下：

```
Collections:
  - name: community.kubernetes
 - name: community.aws
 version:">=5.0.0"
```

注意

所有集合依赖项都会在同步过程中下载。

9. 可选：要进一步配置远程，请使用高级配置下可用的选项：
   a. 如果您的机构有一个公司代理，请输入 Proxy URL, Proxy Username 和 Proxy Password。
   b. 使用 TLS 验证复选框启用或禁用传输层安全性。
   c. 如果验证需要数字证书，输入客户端密钥和客户端证书。
   d. 如果您的服务器使用自签名 SSL 证书，在 CA certificate 字段中输入用于身份验证的 PEM 编码客户端证书。
   e. 要加快下载此远程集合的速度，在 Download concurrency 字段中指定可下载的集合数量。
   f. 要限制此远程上每秒的查询数量，指定 Rate Limit。



注意

有些服务器可以设置特定的速率限制，如果超过，则同步失败。

2.3.8.2. 提供对远程配置的访问

创建远程配置后，您必须先提供对它的访问，然后任何人都可以使用它。

流程

1. 登录到私有自动化中心。
2. 在导航面板中，选择 Collections → Remotes。
3. 在列表中找到您的存储库，点 More Actions 图标 PROFILE，然后选择 Edit。
4. 选择 Access 选项卡。
5. 为 Repository owners 选择一个组。有关实施用户访问的信息，请参阅为私有自动化中心配置用户访问。
6. 为所选组选择适当的角色。
7. 点击 Save。

2.3.9. 在自动化中心中同步软件仓库

您可以通过将存储库从一个自动化中心同步到另一个自动化中心，将相关的自动化内容集合分发到您的用户。为确保您有最新的集合更新，请定期将自定义存储库与远程同步。

流程

1. 登录到自动化中心。
2. 在导航面板中，选择 Collection → Repositories。
3. 在列表中找到您的存储库，然后点 Sync。
   配置的远程中的所有集合都下载到您的自定义存储库中。要检查集合同步的状态，请从导航面板中选择 Task Management。

注意

要将存储库同步限制为远程中的特定集合，您可以使用 requirements.yml 文件识别要拉取的特定集合。如需更多信息，请参阅创建远程。

其他资源

有关使用要求文件的更多信息，请参阅 *使用 Ansible 集合* 指南中的安装带有要求文件的多个集合。

2.3.10. 在自动化中心中导出和导入集合

Ansible 自动化中心（Automation hub）在存储库中存储自动化内容集合。这些集合由自动化内容创建者版本。同一集合的许多版本可以同时存在于相同或不同的存储库中。

集合存储为 .tar 文件，可以导入和导出。此存储格式可确保您导入到新存储库的集合与最初创建和导出的集合相同。

2.3.10.1. 在自动化中心中导出自动化内容集合

完成集合后，您可以将其导入到可在您的机构中的其他位置。

流程

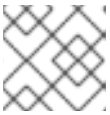
1. 登录到私有自动化中心。
2. 在导航面板中，选择 Collections → Collections。Collections 页面显示所有存储库的所有集合。您可以搜索特定集合。
3. 选择您要导出的集合。集合详情页面将打开。
4. 在 Install 选项卡中，选择 Download tarball。.tar 文件下载到您的默认浏览器下载文件夹中。现在，您可以将其导入到您选择的位置。

2.3.10.2. 在自动化中心中导入自动化内容集合

作为自动化内容创建者，您可以导入要在自定义存储库中使用的集合。要在自定义存储库中使用集合，您必须首先将集合导入到命名空间中，以便自动化中心管理员可以批准它。

流程

1. 登录到自动化中心。
2. 在导航面板中，选择 Collections → Namespaces。Namespaces 页面显示所有可用的命名空间。
3. 点 View Collections。
4. 点 Upload Collection。
5. 进入到集合 tarball 文件，选择文件并点 打开。
6. 点 Upload。
   My Imports 屏幕显示测试摘要，并在集合上传成功或失败时通知您。



注意

如果集合没有被批准，它不会显示在已发布的存储库中。

其他资源

- 有关集合和存储库批准的更多信息，请参阅批准管道。

第 3 章 在私有自动化中心中管理容器

了解用于配置私有自动化中心容器 registry 和存储库的管理员工作流和流程。

3.1. 管理私有自动化中心容器 REGISTRY

使用自动化中心容器 registry 管理 Ansible Automation Platform 基础架构中的容器镜像存储库。您可以使用自动化中心执行以下任务：

- **控制谁可以访问单个容器存储库**
- **更改镜像上的标签**
- **查看活动和镜像层**
- **提供有关每个容器存储库的附加信息**

3.1.1. 容器注册中心

自动化 hub 容器 registry 用于存储和管理容器镜像。构建或提供容器镜像后，您可以将该容器镜像推送到私有自动化中心的 registry 部分，以创建容器存储库。

后续步骤

- **将容器镜像推送到自动化 hub 容器 registry。**
- **创建可访问 registry 中的容器存储库的组。**
- **将新组添加到容器存储库。**
- **将 README 添加到容器存储库，以为用户提供信息和相关链接。**

3.2. 在私有自动化 HUB 中配置容器仓库的用户访问权限

要确定谁可以访问和管理 Ansible Automation Platform 中的镜像，您必须在私有自动化中心中配置容器存储库的用户访问权限。

3.2.1. 容器 registry 组权限

您可以控制用户如何与私有自动化中心中管理的容器交互。使用以下权限列表，为容器注册表创建具有正确特权的组。

表 3.1. 用于在私有自动化中心中管理容器的组权限列表

权限名称	描述
创建新容器	用户可以创建新容器
更改容器命名空间权限	用户可以更改容器存储库的权限
更改容器	用户可以更改容器的信息

权限名称	描述
更改镜像标签	用户可以修改镜像标签
拉取私有容器	用户可以从私有容器中拉取镜像
推送到现有容器	用户可以将镜像推送到现有容器中
查看私有容器	用户可以查看标记为私有的容器

3.2.2. 在私有自动化中心中创建新组

您可以创建并为私有自动化中心中的组分配权限，该组可让用户访问系统中指定的功能。默认情况下，自动化中心中的 Admin 组分配了所有权限，并在初始登录时可用。使用安装私有自动化中心时创建的凭证。

如需更多信息，请参阅开始使用 自动化中心指南中的在私有自动化中心中创建新组。

3.2.3. 为组分配权限

默认情况下，新组没有任何分配的权限。您可以为私有自动化中心中的组分配权限，以便用户访问系统中的特定功能。

您可在首次创建一个组，或编辑现有的组，来添加或删除权限

如需更多信息，请参阅 Automation hub 入门指南中的将权限分配给组。

其他资源

- **请参阅 Container registry group permissions来了解更多有关特定权限的信息。**

3.2.4. 将用户添加到现有组中

您可以在创建组时将用户添加到组中。但是，您也可以手动将用户添加到现有组中。

如需更多信息，请参阅开始使用自动化中心指南中的 向现有组添加用户。

3.3. 填充私有自动化中（AUTOMATION HUB）容器 REGISTRY

默认情况下，私有自动化中心不包括容器镜像。要填充容器 registry，您需要将容器镜像推送到其中。

您必须遵循特定的工作流来填充私有自动化中心容器 registry：

- **从红帽生态系统目录 (registry.redhat.io) 中拉取镜像**
- **标记它们**
- **将它们推送到您的私有自动化中心容器 registry**

重要

最初，镜像清单和文件系统 Blob 都直接由 registry.redhat.io 和 registry.access.redhat.com 提供。从 2023 年 5 月 1 日起，文件系统 Blob 由quay.io 提供。

- 确保 *Table 5.10 中列出的网络端口和协议。执行环境(EE)* 可用，以避免拉取容器镜像出现问题。

对任何特别启用到 registry.redhat.io 或 registry.access.redhat.com 的出站连接进行此更改。

在配置防火墙规则时使用主机名而不是 IP 地址。

完成此更改后，您可以继续从 registry.redhat.io 和 registry.access.redhat.com 拉取镜像。您不需要 quay.io 登录，或以任何方式直接与 quay.io registry 交互，以继续拉取红帽容器镜像。

但是，在基于 Web 的 Red Hat Subscription Management 上，清单（有时称为"订阅分配）"不再受支持（在 Red Hat Satellite 6.16 发布前）。对于 Red Hat Satellite 6.16 的发布日期，保持最新的 Red Hat Satellite 发行日期。

3.3.1. 拉取 (pull) 用于自动化中心的镜像

在将容器镜像推送到私有自动化中心之前，您必须首先从现有 registry 中拉取容器镜像并标记它们以供使用。以下示例详细介绍了如何从红帽生态系统目录 (registry.redhat.io) 拉取镜像。

重要

从 2024 年初期，红帽不再支持 Red Hat Subscription Management Web 平台上的清单或清单列表，这些列表与"订阅分配"互换使用。红帽不再支持 Red Hat Satellite 中的大多数清单功能，但有一个例外：在 Red Hat Satellite 6.16 发布之前，Red Hat Satellite 用户处于封闭的网络或"air gapped"网络，目前仍然可以使用 access.redhat.com。

新的红帽帐户自动为其订阅工具使用简单内容访问。新的红帽帐户和可以连接到红帽服务器的现有 Satellite 客户可以在 console.redhat.com 上找到其清单。

前提条件

- 有从 registry.redhat.io 拉取镜像的权限
- 启用简单内容访问的红帽帐户。

流程

1. 如果需要访问容器镜像的清单，请登录 红帽控制台。
2. 单击您容器镜像所需的清单的三ot菜单，再单击 导出清单。
3. 使用您的 registry.redhat.io 凭证登录到 Podman：

```
$ podman login registry.redhat.io
```

4. 输入您的用户名和密码。

5. 拉取容器镜像：

```
$ podman pull registry.redhat.io/<container_image_name>:<tag>
```

验证

要验证您最近拉取的镜像是否包含在列表中，请执行以下步骤：

1. 列出本地存储中的镜像：

```
$ podman images
```

2. 检查镜像名称，并验证标签是否正确。

其他资源

- 有关注册和获取镜像的信息，请参阅 Red Hat Ecosystem Catalog Help。
- 请参阅创建和管理连接的 Satellite 服务器的清单，以了解更多有关红帽订阅工具的更改的信息

3.3.2. 用于自动化中心的标记镜像

从 registry 中拉取镜像后，标记它们以便在私有自动化中心容器 registry 中使用。

前提条件

- 您已从外部 registry 中提取容器镜像。
- 有自动化中心实例的 FQDN 或 IP 地址。

流程

- 使用自动化中心容器存储库标记本地镜像：

```
$ podman tag registry.redhat.io/<container_image_name>:<tag>
<automation_hub_hostname>/<container_image_name>
```

验证

1. 列出本地存储中的镜像：

```
$ podman images
```

2. 验证您最近使用自动化中心信息标记的镜像是否包含在列表中。

3.3.3. 将容器镜像推送到私有自动化中心

您可以将标记的容器镜像推送到私有自动化中心，以创建新容器并填充容器 registry。

前提条件

- 有创建新容器的权限。

- 有自动化中心实例的 FQDN 或 IP 地址。

流程

1. 使用您的自动化中心位置和凭证登录到 Podman：

```
$ podman login -u=<username> -p=<password> <automation_hub_url>
```

2. 将容器镜像推送到自动化中心容器 registry：

```
$ podman push <automation_hub_url>/<container_image_name>
```

故障排除

push 操作会在上传期间重新编译镜像层，无法保证可重复生成，依赖于客户端实施。这可能会导致镜像层摘要的变化，并导致推送操作失败，Error: Copying this image requires changing layer representation, which is not possible (image is signed or the destination specifies a digest)。

验证

1. 登录到您的自动化中心。
2. 进入 Container Registry。
3. 在 container 存储库列表中找到容器。

3.4. 设置容器存储库

设置容器存储库时，您必须添加描述，包括 README，添加可访问存储库的组，以及标签镜像。

3.4.1. 设置容器 registry 的先决条件

- 已登陆到一个私有自动化中心。
- 您有更改存储库的权限。

3.4.2. 将 README 添加到容器存储库中

将 README 添加到容器存储库，以向用户提供如何使用容器的说明。自动化中心容器存储库支持 Markdown 创建 README。默认情况下，README 为空。

前提条件

- 有更改容器的权限。

流程

1. 登录到自动化中心。
2. 在导航面板中，选择 Execution Environments → Execution Environments。
3. 选择您的容器存储库。

4. 在 Details 标签页中，点 Add。
5. 在 Raw Markdown 文本字段中，使用 Markdown 格式输入您的 README 文本。
6. 完成后点 Save。

添加 README 后，您可以随时通过点 Edit 并重复步骤 4 和 5 对其进行编辑。

3.4.3. 提供对容器存储库的访问

为需要使用镜像的用户提供容器存储库的访问权限。通过添加组，您可以修改组对容器存储库的权限。您可以使用这个选项根据组分配的内容来扩展或限制权限。

前提条件

- 您具有改变容器命名空间的权限。

流程

1. 登录到自动化中心。
2. 在导航面板中，选择 Execution Environments → Execution Environments。
3. 选择您的容器存储库。
4. 在 Access 选项卡中，点 Select a group。
5. 选择您要授予访问权限的组，然后点 Next。
6. 选择您要添加到此执行环境的角色，然后点 Next。
7. 点Add。

3.4.4. 标记容器镜像

标记镜像，为存储在自动化中心容器存储库中的镜像添加额外名称。如果没有向镜像添加任何标签，则自动化中心名称默认为 latest。

前提条件

- 您有更改镜像标签的权限。

流程

1. 在导航面板中，选择 Execution Environments → Execution Environments。
2. 选择您的容器存储库。
3. 点 Images 选项卡。
4. 点 More Actions 图标 ⋮，点 Manage tags。
5. 在文本字段中添加新标签，然后点 Add。
6. 可选：通过点该镜像的任何标签上的 x 来删除当前标签。

7. 点击 Save。

验证

- 点 Activity 选项卡，再检查最新的变化。

3.4.5. 在自动化控制器中创建凭证

要从密码保护的 registry 中拉取容器镜像，您必须在自动化控制器中创建凭证。

在早期版本的 Ansible Automation Platform 中，您需要部署 registry 来存储执行环境镜像。在 Ansible Automation Platform 2.0 及更新的版本中，系统会象您已启动并运行容器 registry 一样运行。要存储执行环境镜像，请仅添加所选容器 registry 的凭证。

流程

1. 进入自动化控制器。
2. 在导航面板中，选择 Resources → Credentials。
3. 点 Add 以创建新凭据。
4. 输入授权 Name、 Description 和 Organization。
5. 选择凭据类型。
6. 输入身份验证 URL。这是容器 registry 地址。
7. 输入登录到容器 registry 所需的 Username 和 Password or Token。
8. 可选： 要启用 SSL 验证，请选择 Verify SSL。
9. 点击 Save。

3.5. 从容器存储库中拉取镜像

从自动化中心容器 registry 中拉取镜像，以便将镜像复制到本地机器。自动化中心为容器存储库中的每个 latest 镜像提供 podman pull 命令。您可以将此命令复制并粘贴到终端中，或者使用 podman pull 根据镜像标签复制镜像。

3.5.1. 拉取镜像

您可以从自动化中心容器 registry 中拉取镜像，以在本地机器中创建副本。

前提条件

- 您需要有从私有容器存储库查看和拉取的权限。

流程

1. 如果您要从密码保护的 registry 中拉取容器镜像，请在拉取镜像前 在自动化控制器中创建凭证。
2. 在导航面板中，选择 Execution Environments → Execution Environments。
3. 选择您的容器存储库。

4. 在 Pull this image条目中，点 Copy to clipboard。
5. 在终端中粘贴并运行命令。

验证

- 运行 podman images 以查看本地机器上的镜像。

3.5.2. 从容器存储库同步镜像

您可以从自动化中心容器 registry 拉取镜像，将镜像同步到本地机器。要从远程容器注册表同步镜像，您必须首先配置远程 registry。

前提条件

您需要有从私有容器存储库查看和拉取的权限。

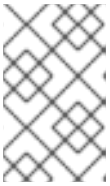
流程

1. 在导航面板中，选择 Execution Environments → Execution Environments。
2. 将 https://registry.redhat.io 添加到 registry。
3. 添加所需的任何凭证进行验证。

注意

有些容器 registry 有速率限制。在 Advanced Options 下设置速率限制。

4. 在导航面板中，选择 Execution Environments → Execution Environments。
5. 在页面标头中点 Add execution environment。
6. 选择您要从中拉取的 registry。Name 字段显示本地 registry 中显示的镜像名称。



注意

Upstream name 字段是远程服务器上的镜像名称。例如，如果上游名称被设置为 "alpine"，并且 Name 字段为 "local/alpine"，则 alpine 镜像会从远程下载，并重命名为 "local/alpine"。

7. 设置要包含或排除的标签列表。将镜像与大量标签同步会非常耗时，并且需要使用大量磁盘空间。

其他资源

- 如需 registry 列表，请参阅 Red Hat Container Registry Authentication。
- 有关拉取镜像时要使用的选项，请参阅 Podman 是什么？ 文档。

3.6. 使用签名的容器

自动化执行环境是 Ansible 自动化控制器用来运行作业的容器镜像。您可以将此内容下载到私有自动化中心，并在您的机构内发布它。

3.6.1. 为容器签名部署您的系统

自动化中心实施镜像签名，以便为执行环境容器镜像提供更好的安全性。

要部署您的系统，使其准备好进行容器签名，请创建一个签名脚本。

注意

安装程序会在安装程序所在的同一服务器上查找脚本和密钥。

流程

1. **在终端中，创建一个签名脚本，并将脚本路径作为安装程序参数传递。**
   示例 ：

```
#!/usr/bin/env bash

# pulp_container SigningService will pass the next 4 variables to the script.
MANIFEST_PATH=$1
FINGERPRINT="$PULP_SIGNING_KEY_FINGERPRINT"
IMAGE_REFERENCE="$REFERENCE"
SIGNATURE_PATH="$SIG_PATH"

# Create container signature using skopeo
skopeo standalone-sign \
  $MANIFEST_PATH \
  $IMAGE_REFERENCE \
  $FINGERPRINT \
  --output $SIGNATURE_PATH

# Optionally pass the passphrase to the key if password protected.
# --passphrase-file /path/to/key_password.txt

# Check the exit status
STATUS=$?
if [ $STATUS -eq 0 ]; then
  echo {\"signature_path\": \"$SIGNATURE_PATH\"}
else
  exit $STATUS
fi
```

2. **查看 Ansible Automation Platform 安装程序清单文件，了解以 automationhub -4.4 开头的容器签名选项。**

```
[all:vars]
.
.
.

automationhub_create_default_container_signing_service = True
automationhub_container_signing_service_key = /absolute/path/to/key/to/sign
automationhub_container_signing_service_script = /absolute/path/to/script/that/signs
```

3. 安装完成后，进入您的自动化中心。
4. 在导航面板中，选择 Signature Keys。
5. 确保有一个名为 container-default 或 container-*anyname* 的密钥。

注意

container-default 服务由 Ansible Automation Platform 安装程序创建的。

3.6.2. 在自动化中心远程添加容器

您可以使用以下两种方式之一将容器远程添加到自动化中心：

- 创建远程
- 执行环境

流程

1. 登录到自动化中心。
2. 在导航面板中，选择 Execution Environments → Remote Registries。
3. 点 **Add remote registry**。
   - 在 Name 字段中输入容器所在的 registry 的名称。
   - 在 URL 字段中输入容器所在的 registry 的 URL。
   - 如果需要，在 Username 字段中输入用户名。
   - 在 Password 字段中，根据需要输入密码。
   - 点击 **Save**。

3.6.3. 添加执行环境

自动化执行环境是容器镜像，可以纳入系统级别的依赖项和基于集合的内容。每个执行环境都允许您有一个自定义镜像来运行作业，每个镜像只包含运行作业时所需的内容。

流程

1. 在导航面板中，选择 Execution Environments → Execution Environments。
2. 点 **Add execution environment**。
3. 输入执行环境的名称。
4. 可选：输入上游名称。
5. 在 Registry 下，从下拉菜单中选择 registry 的名称。
6. 在 Add tag(s) to include 字段中输入标签。如果字段为空，则将传递所有标签。您必须指定要传递的存储库特定标签。

7. 剩余的字段是可选的：
   - 当前包括的标签
   - 添加要排除的标签
   - 当前排除的标签
   - 描述
8. 点击 Save。
9. 同步镜像。

3.6.4. 从本地环境推送容器镜像

使用以下步骤为本地系统中的镜像签名，并将这些签名的镜像推送到自动化中心 registry。

流程

1. 在终端中登录 podman，或登录到当前正在使用的任何容器客户端。

```
> podman pull <container-name>
```

2. 拉取镜像后，添加标签（例如： latest、rc、beta 或版本号，如 1.0、2.3 等）：

```
> podman tag <container-name> <server-address>/<container-name>:<tag name>
```

3. 在进行了更改后为镜像签名，并将其推送到自动化中心 registry：

```
> podman push <server-address>/<container-name>:<tag name> --tls-verify=false --sign-by
<reference to the gpg key on your local>
```

如果镜像未签名，则只能使用嵌入的任何当前签名推送。另外，您可以使用以下脚本推送镜像而不签名镜像：

```
> podman push <server-address>/<container-name>:<tag name> --tls-verify=false
```

4. 推送镜像后，进入您的自动化中心。
5. 在导航面板中，选择 Execution Environments → Execution Environments。
6. 要显示新执行环境，点 Refresh 图标。
7. 点镜像的名称查看您的推送的镜像。

故障排除

Automation Hub 中的详情页面指示镜像是否已签名。如果详情页面表示镜像为 Unsigned，您可以按照以下步骤从自动化中心签名镜像：

1. 点镜像名称导航到详情页面。
2. 点 More Actions 图标 ⋮。有三个选项可用：

- 在 Controller 中使用
- 删除
- 签发

3. 从下拉菜单中选择 Sign。

签名服务为镜像签名。在镜像签名后，状态将变为"签名"。

3.6.5. 带有签名镜像的策略

podman 或其他镜像客户端可以使用策略来确保镜像的有效性，方法是将特定策略分配给该签名。

3.6.6. 使用 podman 确保镜像由特定的签名签名

当确保签名由特定的签名进行签名时，签名必须位于您的本地。

流程

1. 在导航面板中，选择 Signature Keys。
2. 点您使用的签名旁边的 More Actions 图标 ⋮。
3. 从下拉菜单中选择 Download key。此时会打开一个新窗口。
4. 在 Name 字段中输入密钥的名称。
5. 点击 Save。

3.6.7. 配置客户端以验证签名

为确保从远程 registry 拉取的容器镜像被正确签名，您必须首先在策略文件中使用正确的公钥配置镜像。

前提条件

- 客户端必须配置 sudo 权限才能验证签名。

流程

1. 打开终端并使用以下命令：

```
> sudo <name of editor> /etc/containers/policy.json
```

显示的文件类似如下：

```
{
  "default": [{"type": "reject"}],
  "transports": {
   "docker": {
     "quay.io": [{"type": "insecureAcceptAnything"}],
     "docker.io": [{"type": "insecureAcceptAnything"}],
     "<server-address>": [
       {
```

```
            "type": "signedBy",
            "keyType": "GPGKeys",
            "keyPath": "/tmp/containersig.txt"
        }]
    }
  }
}
```

此文件显示 quay.io 或 docker.io 都不执行验证，因为类型是 insecureAcceptAnything，它会覆盖默认的 reject 类型。但是 *<server-address>* 将执行验证，因为参数 type 被设置为 "signedBy"。

注意

目前唯一支持的 keyType 是 GPG 密钥。

2. **在 *<server-address>* 条目下，修改 keyPath <1> 使其包含您的密钥文件的名称。**

```
{
    "default": [{"type": "reject"}],
    "transports": {
        "docker": {
            "quay.io": [{"type": "insecureAcceptAnything"}],
            "docker.io": [{"type": "insecureAcceptAnything"}],
            "<server-address>": [{
                "type": "signedBy",
                "keyType": "GPGKeys",
                "keyPath": "/tmp/<key file name>",
                "signedIdentity": {
                    "type": "matchExact"
                }
            }]
        }
    }
}
```

3. **保存并关闭该文件。**

验证

- **使用 Podman 或您选择的客户端拉取文件：**

```
> podman pull <server-address>/<container-name>:<tag name> --tls-verify=false
```

此响应验证镜像是否已签名，且无错误。如果镜像没有签名，命令会失败。

其他资源

- **如需有关 policy.json 的更多信息，**请参阅 containers-policy.json 的文档。

3.7. 删除容器仓库

从私有自动化中心中删除容器存储库，以管理您的磁盘空间。您可以从 Container Repository 列表视图中的 Red Hat Ansible Automation Platform 接口删除存储库。

前提条件

- 有管理存储库的权限。

流程

1. 进入自动化中心。
2. 在导航面板中，选择 Execution Environments → Execution Environments。
3. 在您要删除的容器存储库中，点 More Actions 图标 ⋮，然后点 Delete。
4. 显示确认消息时，点复选框并点 Delete。

验证

- 返回到 Execution Environments 列表视图。如果容器存储库已被成功删除，则容器存储库将不再位于列表中。