# Red Hat Ansible Automation Platform 2.1

## Managing containers in private automation hub

Administrator workflows and processes for configuring private automation hub container registry and repositories.

Last Updated: 2023-05-03

# Red Hat Ansible Automation Platform 2.1 Managing containers in private automation hub

Administrator workflows and processes for configuring private automation hub container registry and repositories.

## Legal Notice



## Abstract

Providing Feedback: If you have a suggestion to improve this documentation, or find an error, please contact technical support at to create an issue on the Ansible Automation Platform Jira project using the Docs component.

# Table of Contents

# MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

# CHAPTER 1. MANAGING YOUR PRIVATE AUTOMATION HUB CONTAINER REGISTRY

Manage container image repositories in your {PlatfomNameShort} infrastructure using the automation hub container registry. Automation hub provides features to govern who can access individual container repositories, change tags on images, view activity and image layers, and provide additional information related to each container repository.

## 1.1. CONTAINER REGISTRIES

The automation hub container registry is used for storing and managing container images. Once you have built or sourced a container image, you can push that container image to the registry portion of private automation hub to create a container repository.

## 1.2. NEXT STEPS

- Push a container image to the automation hub container registry.
- Create a group with access to the container repository in the registry.
- Add the new group to the container repository.
- Add a README to the container repository to provide users with information and relevant links.

# CHAPTER 2. CONFIGURING USER ACCESS FOR CONTAINER REPOSITORIES IN PRIVATE AUTOMATION HUB

Configure user access for container repositories in your private automation hub to provide permissions that determine who can access and manage images in your Ansible Automation Platform.

## 2.1. PREREQUISITES

- You can create groups and assign permissions in private automation hub.

## 2.2. CONTAINER REGISTRY GROUP PERMISSIONS

User access provides granular controls to how users can interact with containers managed in private automation hub. Use the list of permissions below to create groups with the right privileges for your container registries.

**Table 2.1. List of group permissions used to manage containers in private automation hub**

| Permission name | Description |
|---|---|
| Create new containers | Users can create new containers |
| Change container namespace permissions | Users can change permissions on the container repository |
| Change container | Users can change information on a container |
| Change image tags | Users can modify image tags |
| Pull private containers | Users can pull images from a private container |
| Push to existing container | Users can push an image to an existing container |
| View private containers | Users can view containers marked as private |

## 2.3. CREATING A NEW GROUP

You can create and assign permissions to a group in Automation Hub that enables users to access specified features in the system. By default, there is an **admins** group in Automation Hub that has all permissions assigned and is available on initial login with credentials created when installing Automation Hub.

**Prerequisites**

- You have **groups** permissions and can create and manage group configuration and access in Automation Hub.

**Procedure**

1. Log in to your local Automation Hub.

2. Navigate to **User Access → Groups**.
3. Click **Create**.
4. Provide a **Name** and click **Create**.

You can now assign permissions and add users on the new group edit page.

## 2.4. ASSIGNING PERMISSIONS TO GROUPS

You can assign permissions to groups in Automation Hub that enable users to access specific features in the system. By default, new groups do not have any assigned permissions. You can add permissions upon initial group creation or edit an existing group to add or remove permissions

### Prerequisites

- You have **Change group** permissions and can edit group permissions in Automation Hub.

### Procedure

1. Log in to your local Automation Hub.
2. Navigate to **User Access → Groups**.
3. Click on a group name.
4. Select the **Permissions** tab, then click **Edit**.
5. Click in the field for each permission type and select permissions that appear in the list.
6. Click **Save** when finished assigning permissions.

The group can now access features in Automation Hub associated the their assigned permissions.

### Additional resources

- See Container registry group permissions to learn more about specific permissions.

## 2.5. ADDING USERS TO GROUPS

You can add users to groups when creating a group or manually add users to existing groups. This section describes how to add users to an existing group.

### Prerequisites

- You have **groups** permissions and can create and manage group configuration and access in Automation Hub.

### Procedure

1. Log in to Automation Hub
2. Navigate to **User Access → Groups**.
3. Click on a Group name.

4. Navigate to the **Users** tab, then click **Add**.

5. Select users to add from the list and click **Add**.

You have now added the users you selected to the group. These users now have permissions to use Automation Hub assigned to the group.

# CHAPTER 3. POPULATING YOUR PRIVATE AUTOMATION HUB CONTAINER REGISTRY

By default, private automation hub does not include container images. To populate your container registry, you need to push a container image to it. The procedures in this section describe how to pull images from the Red Hat Ecosystem Catalog (registry.redhat.io), tag them, and push them to your private automation hub container registry.

## 3.1. PREREQUISITES

- You have permissions to create new containers and push containers to private automation hub.

## 3.2. OBTAINING IMAGES FOR USE IN AUTOMATION HUB

Before you can push container images to your private automation hub, you must first pull them from an existing registry and tag them for use. This example details how to pull an image from the Red Hat Ecosystem Catalog (registry.redhat.io).

### Prerequisites

- You have permissions to pull images from registry.redhat.io

### Procedure

1. Log in to Podman using your registry.redhat.io credentials:

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

2. Enter your username and password at the prompts.
3. Pull a container image:

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

### Verification

1. List the images in local storage:

```
$ podman images
```

2. Verify that the image you recently pulled is contained in the list.
3. Verify that the tag is correct.

### Additional resources

- See Red Hat Ecosystem Catalog Help for information on registering and getting images.

## 3.3. TAGGING IMAGES FOR USE IN AUTOMATION HUB

After you pull images from a registry, tag them for use in your private automation hub container registry.

**Prerequisites**

- You have pulled a container image from an external registry.

**Procedure**

- Tag a local image with the automation hub container repository

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

**Verification**

1. List the images in local storage:

```
$ podman images
```

2. Verify that the image you recently tagged with your automation hub information is contained in the list.

## 3.4. PUSHING A CONTAINER IMAGE TO PRIVATE AUTOMATION HUB

You can push tagged container images to private automation hub to create new containers and populate the container registry.

**Prerequisites**

- You have permissions to create new containers.
- You have the FQDN or IP address of the automation hub instance.

**Procedure**

1. Log in to Podman using your automation hub location and credentials:

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

2. Push your container image to your automation hub container registry:

```
$ podman push <automation_hub_url>/<container_image_name> --remove-signatures
```

NOTE

The **--remove-signatures** flag is required when signed images from registry.redhat.io are pushed to the automation hub container registry. The **push** operation re-compresses image layers during the upload, which is not guaranteed to be reproducible and is client implementation dependent. This may lead to image-layer digest changes and a failed push operation, resulting in **Error: Copying this image requires changing layer representation, which is not possible (image is signed or the destination specifies a digest)**.

**Verification**

1. Log in to your automation hub.
2. Navigate to **Container Registry**.
3. Locate the container in the container repository list.

# CHAPTER 4. SETTING UP YOUR CONTAINER REPOSITORY

You can setup your container repository to add a description, include a README, add groups who can access the repository, and tag images.

## 4.1. PREREQUISITES

- You have permissions to change the repository.

## 4.2. ADDING A README TO YOUR CONTAINER REPOSITORY

Add a README to your container repository to provide instructions to your users for how to work with the container. Automation hub container repositories support Markdown for creating a README. By default, the README will be empty.

**Prerequisites**

- You have permissions to change containers.

**Procedure**

1. Navigate to **Execution Environments**.
2. Select your container repository.
3. On the **Detail** tab, click **Add**.
4. In the **Raw Markdown** text field, enter your README text in Markdown.
5. Click **Save** when finished.

Once you add a README, you can edit it at any time by clicking **Edit** and repeating steps 4 and 5.

## 4.3. PROVIDING ACCESS TO YOUR CONTAINER REPOSITORY

Provide access to your container repository to users who need to work the images. Adding a group allows you to modify the permissions the group can have to the container repository. You can use this option to extend or restrict permissions based on what the group is assigned.

**Prerequisites**

- You have **change container namespace** permissions.

**Procedure**

1. Navigate to **Execution Environments**.
2. Select your container repository.
3. Click **Edit** at the top right of your window.
4. Under **Groups with access**, select a group or groups to grant access to.

- Optional: Add or remove permissions for a specific group using the drop down under that group name.

5. Click **Save**.

## 4.4. TAGGING CONTAINER IMAGES

Tag images to add an additional name to images stored in your automation hub container repository. If no tag is added to an image, automation hub defaults to **latest** for the name.

### Prerequisites

- You have **change image tags** permissions.

### Procedure

1. Navigate to **Execution Environments**.
2. Select your container repository.
3. Click the **Images** tab.
4. Click  , then click **Manage tags**.
5. Add a new tag in the text field and click **Add**.
    - Optional: Remove **current tags** by clicking the **x** on any of the tags for that image.
6. Click **Save**.

### Verification

1. Click the **Activity** tab and review the latest changes.

# CHAPTER 5. PULLING IMAGES FROM A CONTAINER REPOSITORY

Pull images from the automation hub container registry to make a copy to your local machine. Automation hub provides the **podman pull** command for each **latest** image in the container repository. You can copy and paste this command into your terminal, or use **podman pull** to copy an image based on an image tag.

## 5.1. PREREQUISITES

- You can view and pull from private containers.

## 5.2. PULLING AN IMAGE

You can pull images from the automation hub container registry to make a copy to your local machine. Automation hub provides the **podman pull** command for each **latest** image in the container repository.

### Prerequisites

- You can view and pull images from a private container.

### Procedure

1. Navigate to **Execution Environments**.
2. Select your container repository.
3. In the **Pull this image** entry, click **Copy to clipboard**.
4. Paste and run the command in your terminal.

### Verification

1. Run **podman images** to view images on your local machine.

## 5.3. ADDITIONAL RESOURCES

- See the Podman documentation for options to use when pulling images.