



Red Hat Ansible Automation Platform 2.1

Managing user access in Private Automation Hub

Create groups for your automation hub users to provide them with appropriate system permissions, or allow view-only access to unauthorized users.

Red Hat Ansible Automation Platform 2.1 Managing user access in Private Automation Hub

Create groups for your automation hub users to provide them with appropriate system permissions, or allow view-only access to unauthorized users.

Legal Notice

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

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

PREFACE	3
MAKING OPEN SOURCE MORE INCLUSIVE	4
CHAPTER 1. CONFIGURING USER ACCESS FOR YOUR LOCAL AUTOMATION HUB	5
1.1. ABOUT USER ACCESS	5
1.1.1. How to implement user access	5
1.1.2. Default user access	5
1.1.3. Getting started	5
1.2. CREATING A NEW GROUP	5
1.3. ASSIGNING PERMISSIONS TO GROUPS	6
1.4. CREATING A NEW USER	6
1.5. CREATING A SUPER USER	7
1.6. ADDING USERS TO GROUPS	7
1.7. CREATING A NEW GROUP FOR CONTENT CURATORS	7
1.8. AUTOMATION HUB PERMISSIONS	8
1.9. DELETING A USER FROM AUTOMATION HUB	10
CHAPTER 2. ENABLING VIEW-ONLY ACCESS FOR YOUR PRIVATE AUTOMATION HUB	11

PREFACE

Configure user access in Automation Hub to provide the appropriate level of system permissions to groups in your organization, or provide view-only access to unauthorized users.

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. CONFIGURING USER ACCESS FOR YOUR LOCAL AUTOMATION HUB

1.1. ABOUT USER ACCESS

You can manage user access to content and features in Automation Hub by creating groups of users that have specific permissions.

1.1.1. How to implement user access

User access is based on managing permissions to system objects (users, groups, namespaces) rather than by assigning permissions individually to specific users.

You assign permissions to the groups you create. You can then assign users to these groups. This means that each user in a group has the permissions assigned to that group.

Groups created in Automation Hub can range from system administrators responsible for governing internal collections, configuring user access, and repository management to groups with access to organize and upload internally developed content to Automation Hub.

- See [Automation Hub permissions](#) for information on system permissions.

1.1.2. Default user access

When you install Automation hub, the default **admin** user is created in the **Admin** group. This group is assigned all permissions in the system.

1.1.3. Getting started

Log in to your local Automation Hub using credentials for the **admin** user configured during installation.

The following sections describe the workflows associated with organizing your users who will access Automation Hub and providing them with required permissions to reach their goals. See the permissions reference table for a full list and description of all permissions available.

1.2. 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 menu:User Access[Groups].

3. Click btn:[Create].
4. Provide a **Name** and click btn:[Create].

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

1.3. 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 menu:User Access[Groups].
3. Click on a group name.
4. Select the **Permissions** tab, then click btn:[Edit].
5. Click in the field for each permission type and select permissions that appear in the list.
6. Click btn:[Save] when finished assigning permissions.

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

1.4. CREATING A NEW USER

You can create a user in Automation Hub and add them to groups that can access features in the system associated by the level of assigned permissions.

Prerequisites

- You have **user** permissions and can create users in Automation Hub.

Procedure

1. Log in to your local Automation Hub.
2. Navigate to menu:Users[.].
3. Click btn:[Create user].
4. Provide information in each of the fields. **Username** and **Password** are required.
5. [Optional] Assign the user to a group by clicking in the **Groups** field and selecting from the list of groups.
6. Click btn:[Save].

The new user will now appear in the list on the **Users** page.

1.5. CREATING A SUPER USER

You can create a super user in automation hub and spread administration work across your team.

Prerequisites

- You have **Super user** permissions and can create users in automation hub.

Procedure

1. Log in to your local automation hub.
2. Navigate to menu:User Access[.].
3. Click btn:[Users].
4. Select the user you want to be a super user to see the User details page.
5. Select **Super User** under User type.

The user now has **Super user** permissions.

1.6. 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 menu:User Access[Groups].
3. Click on a Group name.
4. Navigate to the menu:Users[] tab, then click btn:[Add].
5. Select users to add from the list and click btn:[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.

1.7. CREATING A NEW GROUP FOR CONTENT CURATORS

You can create a new group in Automation Hub designed to support content curation in your organization who will contribute internally developed collections for publication in Automation Hub.

In this section you will create a new group and assign the required permissions to help content developers create namespaces and upload their collections to Automation Hub.

Prerequisites

- You have **admin** permissions in Automation Hub and create groups.

Procedure

- Log in to your local Automation Hub.
- Navigate to menu:Groups[] and click btn:[Create].
- Enter **Content Engineering** as a **Name** for the group in the modal and click btn:[Create]. The new group is created and the **Groups** page will appear.
- On the **Permissions** tab, click btn:[Edit].
- Under **Namespaces**, add permissions for **Add Namespace**, **Upload to Namespace** and **Change Namespace**.
- Click btn:[Save].
The new group is created with the permissions you assigned. Next you can add users to the group.
- Click the **Users** tab on the **Groups** page.
- Click btn:[Add].
- Select users from the modal and click btn:[Add].

Conclusion

You now have a new group who can use Automation Hub to:

- create a namespace,
- edit the namespace details and resources page
- upload internally developed collections to the namespace.

1.8. AUTOMATION HUB PERMISSIONS

Permissions provide a defined set of actions each group performs on a given object. Determine the required level of access for your groups based on the following permissions:

Table 1.1. Permissions Reference Table

Object	Permission	Description
--------	------------	-------------

Object	Permission	Description
namespace	Add namespace Upload to namespace Change namespace Delete namespace	Groups with these permissions can create, upload collections, or delete a namespace.
collections	Modify Ansible repo content Delete collections	Groups with this permission can move content between repositories using the Approval feature, certify or reject features to move content from the staging to published or rejected repositories, and delete collections.
users	View user Delete user Add user Change user	Groups with these permissions can manage user configuration and access in automation hub.
groups	View group Delete group Add group Change group	Groups with these permissions can manage group configuration and access in automation hub.
collection remotes	Change collection remote View collection remote	Groups with these permissions can configure remote repository by navigating to menu:Collections[Repo Management].
containers	Change container namespace permissions Change containers Change image tags Create new containers Push to existing containers Delete container repository	Groups with these permissions can manage container repositories in automation hub.
remote registries	Add remote registry Change remote registry Delete remote registry	Groups with these permissions can add, change, or delete remote registries added to automation hub.

Object	Permission	Description
task management	Change task Delete task View all tasks	Groups with these permissions can manage tasks added to Task Management in automation hub.


1.9. DELETING A USER FROM AUTOMATION HUB

When you delete a user account, the name and email of the user are permanently removed from automation hub.

Prerequisites

- You have **user** permissions in automation hub.

Procedure

1. Log in to automation hub.
2. Expand menu:User Access[[]].
3. Click btn:[Users] to display a list of the current users.
4. Click the action menu () beside the user that you want to remove, then click btn:[Delete].
5. Click btn:[Delete] in the warning message to permanently delete the user.

CHAPTER 2. ENABLING VIEW-ONLY ACCESS FOR YOUR PRIVATE AUTOMATION HUB

By enabling view-only access, you can grant access for users to view collections or namespaces on your private automation hub without the need for them to log in. View-only access allows you to share content with unauthorized users while restricting their ability to only view or download source code, without permissions to edit anything on your private automation hub.

Enable view-only access for your private automation hub by editing the inventory file found on your Red Hat Ansible Automation Platform installer.

- If you are installing a new instance of Ansible Automation Platform, follow these steps to add the **automationhub_enable_unauthenticated_collection_access** and **automationhub_enable_unauthenticated_collection_download** parameters to your **inventory** file along with your other installation configurations:
- If you are updating an existing Ansible Automation Platform installation to include view-only access, add the **automationhub_enable_unauthenticated_collection_access** and **automationhub_enable_unauthenticated_collection_download** parameters to your **inventory** file then run the **setup.sh** script to apply the updates:

Procedure

1. Navigate to the installer.

Bundled installer

```
$ cd ansible-automation-platform-setup-bundle-<latest-version>
```

Online installer

```
$ cd ansible-automation-platform-setup-<latest-version>
```

2. Open the **inventory** file with a text editor.
3. Add the **automationhub_enable_unauthenticated_collection_access** and **automationhub_enable_unauthenticated_collection_download** parameters to the inventory file and set both to **True**, following the example below:

```
[all:vars]
automationhub_enable_unauthenticated_collection_access = True 1
automationhub_enable_unauthenticated_collection_download = True 2
```

- 1 Allows unauthorized users to view collections
- 2 Allows unauthorized users to download collections

4. Run the **setup.sh** script. The installer will now enable view-only access to your automation hub.

Verification

Once the installation completes, you can verify that you have view-only access on your private automation hub by attempting to view content on your automation hub without logging in.

1. Navigate to your private automation hub.
2. On the login screen, click btn:[View only mode].

Verify that you are able to view content on your automation hub, such as namespaces or collections, without having to log in.