Red Hat Ansible Automation Platform 2.4

Installing and Configuring Central Authentication for the Ansible Automation Platform

Enable central authentication functions for your Ansible Automation Platform

Last Updated: 2024-04-19

Red Hat Ansible Automation Platform 2.4 Installing and Configuring Central Authentication for the Ansible Automation Platform

Enable central authentication functions for your Ansible Automation Platform

Legal Notice

Abstract

This guide provides platform administrators with the information and procedures required to enable and configure central authentication on Ansible Automation Platform.

Table of Contents

PREFACE

Ansible Automation Platform Central Authentication is a third-party identity provider (idP) solution, allowing for a simplified single sign-on solution that can be used across the Ansible Automation Platform. Platform administrators can utilize central authentication to test connectivity and authentication, as well as onboard new users and manage user permissions by configuring and assigning them to groups. Along with OpenID Connect-based and LDAP support, central authentication also provides a supported REST API which can be used to bootstrap customer usage.

MAKING OPEN SOURCE MORE INCLUSIVE

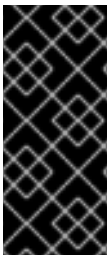
Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases.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

PROVIDING FEEDBACK ON RED HAT DOCUMENTATION

If you have a suggestion to improve this documentation, or find an error, please contact technical support at https://access.redhat.com to create an issue on the Ansible Automation Platform Jira project using the **docs-product** component.

CHAPTER 1. ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION FOR AUTOMATION HUB

To enable Ansible Automation Platform Central Authentication for your automation hub, start by downloading the Red Hat Ansible Automation Platform installer then proceed with the necessary set up procedures as detailed in this guide.



IMPORTANT

The installer in this guide will install central authentication for a basic standalone deployment. Standalone mode only runs one central authentication server instance, and thus will not be usable for clustered deployments. Standalone mode can be useful to test drive and play with the features of central authentication, but it is not recommended that you use standalone mode in production as you will only have a single point of failure.

To install central authentication in a different deployment mode, please see this guide for more deployment options.

1.1. SYSTEM REQUIREMENTS

There are several minimum requirements to install and run Ansible Automation Platform Central Authentication:

- Any operating system that runs Java
- Java 8 JDK
- zip or gzip and tar
- At least 512mb of RAM
- At least 1gb of disk space
- A shared external database like PostgreSQL, MySQL, Oracle, etc. if you want to run central authentication in a cluster. See the Database Configuration section of the *Red Hat Single Sign-On Server Installation and Configuration guide* for more information.
- Network multicast support on your machine if you want to run in a cluster. central authentication can be clustered without multicast, but this requires some configuration changes. See the Clustering section of the *Red Hat Single Sign-On Server Installation and Configuration guide* for more information.
- On Linux, it is recommended to use **/dev/urandom** as a source of random data to prevent central authentication hanging due to lack of available entropy, unless **/dev/random** usage is mandated by your security policy. To achieve that on Oracle JDK 8 and OpenJDK 8, set the **java.security.egd** system property on startup to **file:/dev/urandom**.

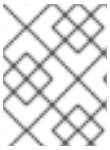
1.2. INSTALLING ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION FOR USE WITH AUTOMATION HUB

The Ansible Automation Platform Central Authentication installation will be included with your Red Hat Ansible Automation Platform installer. Install the Ansible Automation Platform using the following procedures, then configure the necessary parameters in your inventory file to successfully install both

the Ansible Automation Platform and central authentication.

1.2.1. Choosing and obtaining a Red Hat Ansible Automation Platform installer

Choose the Red Hat Ansible Automation Platform installer you need based on your Red Hat Enterprise Linux environment internet connectivity. Review the following scenarios and decide on which Red Hat Ansible Automation Platform installer meets your needs.



NOTE

A valid Red Hat customer account is required to access Red Hat Ansible Automation Platform installer downloads on the Red Hat Customer Portal.

Installing with internet access

Choose the Red Hat Ansible Automation Platform installer if your Red Hat Enterprise Linux environment is connected to the internet. Installing with internet access retrieves the latest required repositories, packages, and dependencies. Choose one of the following ways to set up your Ansible Automation Platform installer.

Tarball install

1. Navigate to the Red Hat Ansible Automation Platform download page.
2. Click **Download Now** for the **Ansible Automation Platform <latest-version> Setup**.
3. Extract the files:

```
$ tar xvzf ansible-automation-platform-setup-<latest-version>.tar.gz
```

RPM install

1. Install Ansible Automation Platform Installer Package
   v.2.4 for RHEL 8 for x86_64

```
$ sudo dnf install --enablerepo=ansible-automation-platform-2.4-for-rhel-8-x86_64-rpms
ansible-automation-platform-installer
```

   v.2.4 for RHEL 9 for x86-64

```
$ sudo dnf install --enablerepo=ansible-automation-platform-2.4-for-rhel-9-x86_64-rpms
ansible-automation-platform-installer
```

NOTE

dnf install enables the repo as the repo is disabled by default.

When you use the RPM installer, the files are placed under the **/opt/ansible-automation-platform/installer** directory.

Installing without internet access

Use the Red Hat Ansible Automation Platform **Bundle** installer if you are unable to access the internet,

or would prefer not to install separate components and dependencies from online repositories. Access to Red Hat Enterprise Linux repositories is still needed. All other dependencies are included in the tar archive.

1. Navigate to the Red Hat Ansible Automation Platform download page.
2. Click **Download Now** for the **Ansible Automation Platform <latest-version> Setup Bundle**
3. Extract the files:

```
$ tar xvzf ansible-automation-platform-setup-bundle-<latest-version>.tar.gz
```

1.2.2. Configuring the Red Hat Ansible Automation Platform installer

Before running the installer, edit the inventory file found in the installer package to configure the installation of automation hub and Ansible Automation Platform Central Authentication.

NOTE

Provide a reachable IP address for the [automationhub] host to ensure users can sync content from Private Automation Hub from a different node and push new images to the container registry.

1. Navigate to the installer directory:
   a. Online installer:

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

   b. Bundled installer:

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

2. Open the **inventory** file using a text editor.
3. Edit the inventory file parameters under **[automationhub]** to specify an installation of automation hub host:
   a. Add group host information under **[automationhub]** using an IP address or FQDN for the automation hub location.
   b. Enter passwords for **automationhub_admin_password**, **automationhub_pg_password**, and any additional parameters based on your installation specifications.
4. Enter a password in the **sso_keystore_password** field.
5. Edit the inventory file parameters under **[SSO]** to specify a host on which to install central authentication:
   a. Enter a password in the **sso_console_admin_password** field, and any additional parameters based on your installation specifications.

1.2.3. Running the Red Hat Ansible Automation Platform installer

With the inventory file updated, run the installer using the **setup.sh** playbook found in the installer package.

1. Run the **setup.sh** playbook:

```
$ ./setup.sh
```

1.2.4. Log in as a central authentication admin user

With Red Hat Ansible Automation Platform installed, log in as an admin user to the central authentication server using the admin credentials that you specified in your inventory file.

1. Navigate to your Ansible Automation Platform Central Authentication instance.
2. Login using the admin credentials you specified in your inventory file, in the **sso_console_admin_username** and **sso_console_admin_password fields**.

With Ansible Automation Platform Central Authentication successfully installed, and the admin user logged in, you can proceed by adding a user storage provider (such as LDAP) using the following procedures.

CHAPTER 2. ADDING A USER STORAGE PROVIDER (LDAP/KERBEROS) TO ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION

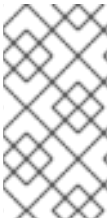
Ansible Automation Platform Central Authentication comes with a built-in LDAP/AD provider. You can add your LDAP provider to central authentication to be able to import user attributes from your LDAP database.

Prerequisites

- You are logged in as an SSO admin user.

Procedure

1. Log in to Ansible Automation Platform Central Authentication as an SSO admin user.
2. From the navigation bar, select **Configure section → User Federation**.



NOTE

When using an LDAP User Federation in RH-SSO, a group mapper must be added to the client configuration, ansible-automation-platform, to expose the identity provider (IDP) groups to the SAML authentication. Refer to OIDC Token and SAML Assertion Mappings for more information on SAML assertion mappers.

1. Using the dropdown menu labeled *Add provider*, select your LDAP provider to proceed to the LDAP configuration page.

The following table lists the available options for your LDAP configuration:

Configuration Option	Description
Storage mode	Set to **On** if you want to import users into the central authentication user database. See Storage Mode for more information.
Edit mode	Determines the types of modifications that admins can make on user metadata. See Edit Mode for more information.
Console Display Name	Name used when this provider is referenced in the admin console
Priority	The priority of this provider when looking up users or adding a user
Sync Registrations	Enable if you want new users created by Ansible Automation Platform Central Authentication in the admin console or the registration page to be added to LDAP

Allow Kerberos authentication	Enable Kerberos/SPNEGO authentication in the realm with users data provisioned from LDAP. See Kerberos for more information.

CHAPTER 3. ASSIGNING AUTOMATION HUB ADMINISTRATOR PERMISSIONS

Hub administrative users will need to be assigned the role of *hubadmin* in order to manage user permissions and groups. You can assign the role of *hubadmin* to a user through the Ansible Automation Platform Central Authentication client.

Prerequisites

- A user storage provider (e.g., LDAP) has been added to your central authentication

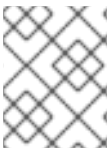
Procedure

1. Navigate to the **ansible-automation-platform** realm on your SSO client.
2. From the navigation bar, select **Manage → Users**.
3. Select a user from the list by clicking their ID.
4. Click the **Role Mappings** tab.
5. Using the dropdown menu under *Client Roles*, select **automation-hub**.
6. Click **hubadmin** from the *Available Roles* field, then click **Add selected >**.

The user is now a *hubadmin*. Repeat steps 3-6 to assign any additional users the *hubadmin* role.

CHAPTER 4. ADDING AN IDENTITY BROKER TO ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION

Ansible Automation Platform Central Authentication supports both social and protocol-based providers. You can add an identity broker to central authentication to enable social authentication for your realm, allowing users to log in using an existing social network account, such as Google, Facebook, GitHub etc.



NOTE

For a list of supported social networks and for more information to enable them, please see this section.

Protocol-based providers are those that rely on a specific protocol in order to authenticate and authorize users. They allow you to connect to any identity provider compliant with a specific protocol. Ansible Automation Platform Central Authentication provides support for SAML v2.0 and OpenID Connect v1.0 protocols.

Procedure

1. Log in to Ansible Automation Platform Central Authenticationas an admin user.
2. Under the *Configure* section on the side navigation bar, click **Identity Providers**.
3. Using the dropdown menu labeled *Add provider*, select your identity provider to proceed to the identity provider configuration page.

The following table lists the available options for your identity provider configuration:

Table 4.1. Identity Broker Configuration Options

Configuration Option	Description
Alias	The alias is a unique identifier for an identity provider. It is used to reference an identity provider internally. Some protocols such as **OpenID Connect** require a redirect URI or callback url in order to communicate with an identity provider. In this case, the alias is used to build the redirect URL.
Enabled	Turns the provider on/off.
Hide on Login Page	If enabled, this provider will not be shown as a login option on the login page. Clients can still request to use this provider by using the **kc_idp_hint** parameter in the URL they use to request a login.
Account Linking Only	If enabled, this provider cannot be used to login users and will not be shown as an option on the login page. Existing accounts can still be linked with this provider.

Store Tokens	Whether or not to store the token received from the identity provider.
Stored Tokens Readable	Whether or not users are allowed to retrieve the stored identity provider token. This also applies to the broker client-level role read token.
Trust Email	Whether an email address provided by the identity provider will be trusted. If the realm requires email validation, users that log in from this IDP will not have to go through the email verification process.
GUI Order	The order number that sorts how the available IDPs are listed on the login page.
First Login Flow	Select an authentication flow that will be triggered for users that log in to central authentication through this IDP for the first time.
Post Login Flow	Select an authentication flow that is triggered after the user finishes logging in with the external identity provider.

4.1. MANAGING GROUP PERMISSIONS WITH ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION

You can manage user access on the Ansible Automation Platform by grouping specific permissions into roles, and then assigning those roles to groups. As you log in to the Ansible Automation Platform for the first time, **Users**, **Groups**, and **Roles** appear in the user access page in automation hub, then you can assign user access and roles to each group.

Automation hub includes a set of managed roles that are compatible with use cases you may encounter. You can create your own set of managed roles or use the predefined roles located in the **Roles** section of the **User Access** page.

4.1.1. Grouping permissions into Roles

You can group permissions into roles with specific user access to features in the system.

Prerequisites

- You are signed in as a **hubadmin** user.

Procedure

1. Log in to your private automation hub.
2. Navigate to the **User Access** drop-down menu.
3. Click **Roles**.
4. Click **Add roles**.

5. Enter role name in the **Name** field.
6. Enter role description in the **Description** field.
7. Click the drop-down menu next to each **Permissions** type and select the appropriate permissions for the role.
8. Click **Save**.

You have created a new role with specific permissions. You can now assign this role to groups.

4.1.1.1. Assigning roles to groups

You can assign roles to groups, giving users access to specific features in the system, from both the **Groups** menu and the **Namespaces** menu. Roles assigned to a group from the **Groups** menu have a global scope. For example, if a user is assigned a namespace owner role, that permission applies to all namespaces. However, roles assigned to a group from the *Namespaces* menu will only give a user access to a specific instance of an object.

Prerequisites

- You are signed in as a **hubadmin** user.

Procedure

Assigning roles from the **Groups** menu.

1. Log in to your private automation hub.
2. Navigate to the **User Access** drop-down menu.
3. Click **Groups** and select a group name.
4. Click **Add roles**.
5. Click the checkbox next to the role that you want to add.
6. Click **Next** to preview the role that will be applied to the group.
7. Click **Add** to apply the selected role to the group.

NOTE

Click **Back** to return to the roles menu, or click **Cancel** to return to the previous page.

Procedure

Assigning roles from the **Namespaces** menu.

1. Log in to your private automation hub.
2. Navigate to the **Collections** drop-down menu.
3. Click the **My Namespaces** tab, and select a namespace.
4. Click the **Namespace owners** tab to edit.

Users can now access features in automation hub associated with their assigned permissions.

4.1.2. Automation hub permissions

Permissions provide a defined set of actions each group can perform on a given object. Determine the required level of access for your groups based on the permissions described in this table.

Table 4.2. Permissions Reference Table

Object	Permission	Description
collection namespaces	Add namespace Upload to namespace Change namespace Delete namespace	Groups with these permissions can create, upload collections, and delete a namespace.
collections	Modify Ansible repo content Delete collections	Groups with this permission can perform these actions: Move content between repositories by using the Approval feature. Certify or reject features to move content from the **staging** to **published** or **rejected** repositories. Delete collections.
users	View user Delete user Add user Change user	Groups with these permissions can manage user configuration and access in private automation hub.
groups	View group Delete group Add group Change group	Groups with these permissions can manage group configuration and access in private automation hub.
collection remotes	Change collection remote View collection remote	Groups with these permissions can configure remote repository by navigating to **Collections → Repo Management**.

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

CHAPTER 5. CONFIGURING ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION GENERIC OIDC SETTINGS AND RED HAT SSO/KEYCLOAK FOR RED HAT SSO AND ANSIBLE AUTOMATION PLATFORM

Ansible Automation Platform Central Authentication allows for the setting of generic OIDC settings and Red Hat SSO/keycloak for Red Hat SSO and Ansible Automation Platform.

5.1. PREREQUISITES

- You are able to log in as an admin user.

5.2. CONFIGURING CENTRAL AUTHENTICATION GENERIC OIDC SETTINGS

Procedure

1. Log in to RH-SSO as admin.

NOTE

If you have an existing realm you may go to step 6.

2. Add Realm.
3. Enter Name and click **Create**.
4. Click the Clients tab.
5. Enter name and click **Create**.
6. From the navigation panel, select **Client Protocol → openid-connect**.
7. From the navigation panel, select **Access Type → confidential**.
8. In the Root URL field, enter your Ansible Automation Platform server IP or hostname.
9. In the Valid Redirect field, enter your Ansible Automation Platform server IP or hostname. If not in production, set to *.
10. In the Web origins field, enter your Ansible Automation Platform server IP or hostname. If not in production, set to *.
11. Click the **Credentials** tab.

NOTE

Keep track of the Secret to be used later.

12. Log in to Ansible Automation Platform Controller as admin.

13. Click Settings.
14. Click Generic OIDC settings.
15. Click **Edit**.
16. In the OIDC Key field, enter the name of your client from step 5.
17. In the OIDC Secret field, enter the secret saved from step 8.
18. In the OIDC Provider URL field, enter your keycloak server URL and port.
19. Click **Save**.

OIDC should appear as an option for login. Click **Sign in with OIDC** and it will redirect you to the SSO server for login and redirection back to Ansible Automation Platform.