Red Hat Ansible Automation Platform 2.4

为 Ansible Automation Platform 安装和配置中央身份验证

为 Ansible Automation Platform 启用中央身份验证功能

Last Updated: 2024-07-03

Red Hat Ansible Automation Platform 2.4 为 Ansible Automation Platform 安装和配置中央身份验证

为 Ansible Automation Platform 启用中央身份验证功能

法律通告

摘要

本指南为平台管理员提供了在 Ansible Automation Platform 上启用和配置中央身份验证所需的信息和流程。

目录

前言 3

对红帽文档提供反馈 4

第 1 章 用于自动化的 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION 5
1.1. 系统要求 5
1.2. 安装 ANSIBLE AUTOMATION PLATFORM CENTRAL 身份验证以用于自动化 HUB 5

第 2 章 将用户存储提供程序(LDAP/KERBEROS)添加到 ANSIBLE 自动化平台中央身份验证中 9

第 3 章 分配自动化 HUB 管理员权限 10

第 4 章 将身份代理添加到 ANSIBLE AUTOMATION PLATFORM 中央身份验证中 11
4.1. 使用 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION 管理组权限 12

第 5 章 为 RED HAT SSO 和 ANSIBLE AUTOMATION PLATFORM 配置 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION GENERIC OIDC 设置和 RED HAT SSO/KEYCLOAK 16
5.1. 先决条件 16
5.2. 配置中央身份验证通用 OIDC 设置 16

前言

Ansible Automation Platform Central Authentication 是第三方身份提供程序(idP)解决方案，允许在 Ansible Automation Platform 中使用简化的单点登录解决方案。平台管理员可以利用集中身份验证来测试连接和身份验证，也可添加新用户，并通过配置和管理用户权限来管理用户权限。除了基于 OpenID Connect 和 LDAP 支持，中央身份验证还提供受支持的 REST API，可用于引导客户使用。

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，请通过 https://access.redhat.com 联系技术支持，以使用 **docs-product** 组件在 Ansible Automation Platform JIRA 项目中创建一个问题。

第 1 章 用于自动化的 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION

要为您的自动化中心启用 Ansible Automation Platform 中央身份验证，请从下载 Red Hat Ansible Automation Platform 安装程序开始，然后执行本指南中详述的必要的设置步骤。

重要

本指南中的安装程序将为基本单机部署安装中央身份验证。单机模式仅运行一个中央身份验证服务器实例，因此不适用于集群部署。单机模式可用于测试和试用中央身份验证功能，但不建议在生产环境中使用它，因为其具有单点故障。

要在不同的部署模式下安装中央身份验证，请参阅本指南以了解更多部署选项。

1.1. 系统要求

安装和运行 Ansible Automation Platform Central 身份验证有几个最低要求：

- 任何运行 Java 的操作系统
- Java 8 JDK
- zip 或 gzip 和 tar
- 至少 512mb RAM
- 至少 1gb 磁盘空间
- 如果要在集群中运行中央身份验证，需要一个如 PostgreSQL、MySQL、Oracle 等的共享外部数据库。如需更多信息，*请参阅红帽单点登录服务器安装和配置指南中的数据库配置部分*。
- 如果要在集群中运行，需要在您的机器上支持网络多播。中央身份验证虽然可以在没有多播的情况下实现，但这需要一些配置更改。如需更多信息，*请参阅红帽单点登录服务器安装和配置指南中的集群部分*。
- 在 Linux 上，建议使用 **/dev/urandom** 作为随机数据源，以防止因为缺少可用熵而导致集中身份验证挂起，除非安全策略强制使用 **/dev/random**。要在 Oracle JDK 8 和 OpenJDK 8 上达到此目的，请在启动时将 **java.security.egd** 系统属性设置为 **file:/dev/urandom**。

1.2. 安装 ANSIBLE AUTOMATION PLATFORM CENTRAL 身份验证以用于自动化 HUB

Ansible Automation Platform Central Authentication 安装将包含在您的 Red Hat Ansible Automation Platform 安装程序中。按照以下步骤安装 Ansible Automation Platform，然后在清单文件中配置必要的参数，以成功安装 Ansible Automation Platform 和中央身份验证。

1.2.1. 选择并获取 Red Hat Ansible Automation Platform 安装程序

根据您的 Red Hat Enterprise Linux 环境互联网连接，选择您需要的 Red Hat Ansible Automation Platform 安装程序。查看以下场景，并决定哪个 Red Hat Ansible Automation Platform 安装程序满足您的需要。

注意

需要有效的红帽客户帐户才能访问红帽客户门户上的 Red Hat Ansible Automation Platform 安装程序下载。

使用互联网访问进行安装

如果您的 Red Hat Enterprise Linux 环境连接到互联网，请选择 Red Hat Ansible Automation Platform 安装程序。使用互联网访问进行安装会检索最新的软件仓库、软件包和依赖项。选择以下方法之一来设置 Ansible Automation Platform 安装程序。

Tarball 安装

1. 进入 Red Hat Ansible Automation Platform 下载 页面。
2. 为 **Ansible Automation Platform <latest-version> Setup** 点 **Download Now**。
3. 解压文件：

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

RPM 安装

1. 安装 Ansible Automation Platform 安装程序软件包
   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
```

注意

dnf install 启用存储库，因为默认禁用存储库。

使用 RPM 安装程序时，文件位于 **/opt/ansible-automation-platform/installer** 目录下。

在没有互联网访问的情况下安装

如果您无法访问互联网，或者不想从在线存储库安装独立的组件和依赖项，请使用 Red Hat Ansible Automation **PlatformBundle** 安装程序。仍然需要访问 Red Hat Enterprise Linux 软件仓库。所有其他依赖项都包含在 tar 归档中。

1. 进入 Red Hat Ansible Automation Platform 下载 页面。
2. 为 **Ansible Automation Platform <latest-version> Setup Bundle** 点 **Download Now**。
3. 解压文件：

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

1.2.2. 配置 Red Hat Ansible Automation Platform 安装程序

在运行安装程序前，请编辑安装程序软件包中找到的清单文件，以配置自动化中心和 Ansible Automation Platform Central 身份验证的安装。

注意

为 [automationhub] 主机提供可访问的 IP 地址，以确保用户可以从不同节点同步私有 Automation Hub 中的内容，并将新镜像推送到容器注册表。

1. 进入安装程序目录：
   a. 在线安装程序：

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

   b. 捆绑的安装程序：

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

2. 使用文本编辑器打开 **inventory** 文件。
3. 编辑 **[automationhub]** 下的清单文件参数以指定自动化 hub 主机的安装：
   a. 使用 IP 地址或 FQDN 作为自动化中心位置，在 **[automationhub]** 下添加组主机信息。
   b. 根据您的安装规格，输入 **automationhub_admin_password**,**automationhub_pg_password** 的密码，以及任何额外的参数。
4. 在 **sso_keystore_password** 字段中输入密码。
5. 编辑 **[SSO]** 下的清单文件参数，以指定要在其上安装中央身份验证的主机：
   a. 在 **sso_console_admin_password** 字段中输入密码，并根据您的安装规格输入其他参数。

1.2.3. 运行 Red Hat Ansible Automation Platform 安装程序

更新清单文件后，使用安装程序软件包中找到的 **setup.sh** playbook 运行安装程序。

1. 运行 **setup.sh** playbook:

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

1.2.4. 以中央身份验证管理员用户身份登录

安装 Red Hat Ansible Automation Platform 后，以 admin 用户身份使用您在清单文件中指定的 admin 凭据登录中央身份验证服务器。

1. 进入到您的 Ansible Automation Platform Central Authentication 实例。
2. 使用在清单文件的 **sso_console_admin_username** 和 **sso_console_admin_password fields** 中指定的 admin 凭证进行登录。

成功安装 Ansible Automation Platform Central 身份验证后，并且登录 admin 用户后，您可以按照以下步骤添加用户存储提供商（如 LDAP）。

第 2 章 将用户存储提供程序(LDAP/KERBEROS)添加到 ANSIBLE 自动化平台中央身份验证中

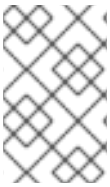
Ansible Automation Platform Central 身份验证附带内置 LDAP/AD 提供程序。您可以添加 LDAP 提供程序到中央身份验证，以便能够从 LDAP 数据库导入用户属性。

先决条件

- 以 SSO admin 用户身份登录。

步骤

1. 以 SSO admin 用户身份登录 Ansible 自动化平台中央身份验证。
2. 在导航面板中，选择 **Configure section → User Federation**。



注意

在 RH-SSO 中使用 LDAP 用户联邦时，必须将组映射器添加到客户端配置 ansible-automation-platform 中，以将身份提供程序(IDP)组公开给 SAML 身份验证。有关 SAML 断言映射的更多信息，请参阅 OIDC 令牌和 SAML 断言映射。

1. 从 **Add provider** 列表中，选择您的 LDAP 供应商以进入 LDAP 配置页面。

下表列出了 LDAP 配置的可用选项：

配置选项	描述
存储模式	如果要将用户导入到中央身份验证用户数据库，请将用户设置为 **On**。如需更多信息，请参阅 存储模式。
编辑模式	决定管理员可以对用户元数据进行的修改类型。如需更多信息， 请参阅编辑模式。
控制台显示名称	在管理控制台中引用此提供程序时使用的名称
优先级	查找用户或添加用户的优先级
同步注册	如果要在管理控制台或注册页面中添加 Ansible Automation Platform Central Authentication 创建的新用户，请启用
允许 Kerberos 身份验证	通过从 LDAP 调配的用户数据，在域中启用 Kerberos/SPNEGO 身份验证。如需更多信息，请参阅 Kerberos。

第 3 章 分配自动化 HUB 管理员权限

需要为 hub 管理用户分配 *hubadmin* 角色，以便管理用户权限和组。您可以通过 Ansible Automation Platform Central Authentication 客户端将 *hubadmin* 角色分配给用户。

先决条件

- 用户存储提供程序（如 LDAP）已添加到您的中央身份验证中

步骤

1. 进入 SSO 客户端上的 **ansible-automation-platform** 域。
2. 在导航面板中，选择 **User Access → Users**。
3. 点用户 ID，从列表中选择用户。
4. 点 **Role Mappings** 选项卡。
5. 从 **Client Roles** 列表中，选择 **automation-hub**。
6. 从 **Available Roles** 字段中点 **hubadmin**，然后点 **Add selected >**。

用户现在是 *hubadmin*。重复步骤 3-6，为 *hubadmin* 角色分配任何其他用户。

第 4 章 将身份代理添加到 ANSIBLE AUTOMATION PLATFORM 中央身份验证中

Ansible Automation Platform Central Authentication 支持社交供应商和基于协议的提供程序。您可以将身份代理添加到中央身份验证中，以便为域启用社交身份验证，允许用户使用现有的社交网络帐户（如 Google、Facebook、GitHub 等）登录。

注意

有关支持的社交网络列表以及启用它们的更多信息，请参阅本节。

基于协议的供应商是指那些依赖特定协议来验证和授权用户的供应商。它们允许您连接到符合特定协议的任何身份提供程序。Ansible Automation Platform Central Authentication 提供对 SAML v2.0 和 OpenID Connect v1.0 协议的支持。

步骤

1. 以管理员用户身份登录 Ansible Automation Platform 中央身份验证。
2. 在侧面导航栏上的 **Configure** 部分下，单击 **Identity Providers**。
3. 从 **Add provider** 列表中，选择您的身份提供程序以进入身份提供程序配置页面。

下表列出了您的身份提供程序配置的可用选项：

表 4.1. Identity Broker 配置选项

配置选项	描述
Alias	alias 是身份提供程序的唯一标识符。它用于在内部引用身份提供程序。**OpenID Connect** 等协议需要重定向 URI 或回调 URL，以便与身份提供程序通信。在这种情况下，别名用于构建重定向 URL。
Enabled	打开/关闭提供程序。
在登录页中隐藏	如果启用，此提供程序不会在登录页面中显示为登录选项。客户端仍然可以通过在用于请求登录的 URL 中使用 **kc_idp_hint** 参数来请求使用此提供程序。
仅限客户链接	如果启用，则此提供程序无法用于登录用户，也不会在登录页面中显示为选项。现有帐户仍可与此供应商相关联。
存储令牌	是否存储从身份提供程序收到的令牌。
存储的令牌可读	是否允许用户检索已存储的身份提供商令牌。这也适用于代理客户端级别的角色读取令牌。

信任电子邮件	身份提供商提供的电子邮件地址是否受信任。如果域需要验证电子邮件，则从此 IDP 登录的用户不必通过电子邮件验证过程。
GUI 顺序	登录页面中列出了如何列出可用 IDP 的排序顺序号。
第一个登录流	选择将为首次通过此 IDP 登录集中身份验证的用户触发的身份验证流程。
后登录流	选择用户完成与外部身份提供程序登录后触发的身份验证流。

4.1. 使用 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION 管理组权限

您可以通过将特定权限分组到角色中来管理 Ansible Automation Platform 上的用户访问权限，然后将这些角色分配到组。当您第一次登录到 Ansible Automation Platform 时，**Users**, **Groups**, and **Roles** 会出现在自动化中心的用户访问页面中，然后您可以为每个组分配用户访问权限和角色。

Automation hub 包括了一组与您可能会遇到的用例兼容的受管角色。您可以创建自己的一组受管角色，或使用 **User Access** 页的 **Roles** 部分中的预定义角色。

4.1.1. 将权限分组到角色中

您可以将权限分组到角色中，使特定用户对系统中的功能具有访问权限。

先决条件

- 以 **hubadmin** 用户身份登录。

步骤

1. 登录到您的私有自动化中心。
2. 进入到 **User Access** 下拉菜单。
3. 点 **Roles**。
4. 点 **Add roles**。
5. 在 **Name** 字段中输入角色名称。
6. 在 **Description** 字段中输入角色描述。
7. 点每个 **Permissions** 类型旁边的下拉菜单，并为角色选择适当的权限。
8. 点击 **Save**。

您已创建了具有特定权限的新角色。现在，您可以将此角色分配给组。

4.1.1.1. 将角色分配给组

您可以将角色分配给组，从 **Groups** 菜单和 **Namespaces** 菜单中授予用户对系统中特定功能的访问权限。从 **Groups** 菜单中分配给组的角色具有全局范围。例如，如果用户被分配一个命名空间所有者角色，则该权限适用于所有命名空间。但是，从 *Namespaces* 菜单中分配给组的角色将只授予用户对对象的特定实例的访问权限。

先决条件

- 以 **hubadmin** 用户身份登录。

步骤

从 **Groups** 菜单分配角色。

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**。
3. 从显示的组列表中选择组。
4. 点 **Add roles**。
5. 点您要添加的角色旁边的复选框。
6. 点 **Next** 以预览将应用到该组的角色。
7. 点 **Add** 将所选角色应用到组。

注意

点 **Back** 以返回到角色菜单，或者点 **Cancel** 以返回到上一页。

步骤

从 **Namespaces** 菜单中分配角色。

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 **My Namespaces** 选项卡，然后选择一个命名空间。
4. 点 **Access** 选项卡编辑。

用户现在可以访问自动化 hub 中的功能，与其分配的权限相关联。

4.1.2. 自动化中心权限

权限提供一组定义的操作，每个组都可以对给定对象执行。根据此表中描述的权限，为您的组确定所需的访问权限级别。

表 4.2. 权限参考表

对象	权限	描述

对象	权限	描述
集合命名空间	添加命名空间 Upload to namespace（上传到命名空间） 更改命名空间 删除命名空间	具有这些权限的组可以创建、上传集合和删除命名空间。
collections	修改 Ansible repo 内容 删除集合	具有此权限的组可以执行以下操作： 使用 Approval 功能在仓库间移动内容。 认证或拒绝将内容从 **staging** 移到 **published** 或 **rejected** 存储库的功能。 删除集合。
users	查看用户 Delete user（删除用户） Add user（添加用户） 更改用户	具有这些权限的组群可以在私有自动化中心中管理用户配置和访问。
groups	View group（查看组） Delete group（删除组） Add group（添加组） 更改组	具有这些权限的组可以在私有自动化中心中管理组配置和访问。
collection remotes	更改集合远程 查看集合远程	具有这些权限的组可以通过导航到 **Collection → Repositories** 来配置远程存储库。
containers	更改容器命名空间权限 更改容器 更改镜像标签 创建新容器 推送到现有容器 删除容器仓库	具有这些权限的组可以在私有自动化中心中管理容器存储库。

对象	权限	描述
remote registries	添加远程 registry 更改远程 registry 删除远程 registry	具有这些权限的组可以添加、更改或删除添加到私有自动化中心的远程 registry。
task management	更改任务 删除任务 查看所有任务	具有这些权限的组可以管理添加到私有自动化中心中的 **Task Management** 中的任务。

第 5 章 为 RED HAT SSO 和 ANSIBLE AUTOMATION PLATFORM 配置 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION GENERIC OIDC 设置和 RED HAT SSO/KEYCLOAK

Ansible Automation Platform Central Authentication 允许为 Red Hat SSO 和 Ansible Automation Platform 设置通用 OIDC 设置和 Red Hat SSO/keycloak。

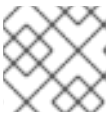
5.1. 先决条件

- 您可以以 admin 用户身份登录。

5.2. 配置中央身份验证通用 OIDC 设置

流程

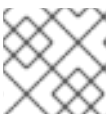
1. 以 admin 用户身份登录 RH-SSO。



注意

如果您有一个现有域，则可能要第 6 步。

2. 添加域.
3. 输入 Name，再单击 **Create**。
4. 点 **Clients** 选项卡。
5. 输入名称并点 **Create**。
6. 在导航面板中，选择 **Client Protocol → openid-connect**。
7. 在导航面板中，选择 **Access Type → confidential**。
8. 在 **Root URL** 字段中，输入您的 Ansible Automation Platform 服务器 IP 或主机名。
9. 在 **Valid Redirect** 字段中，输入您的 Ansible Automation Platform 服务器 IP 或主机名。如果没有在生产环境中，设置为 If。
10. 在 Web origins 字段中，输入 Ansible Automation Platform 服务器 IP 或主机名。如果没有在生产环境中，设置为 If。
11. 点 **Credentials** 选项卡。



注意

跟踪要稍后使用的 Secret。

12. 以 admin 用户身份登录 Ansible Automation Platform Controller。
13. 在导航面板中，选择 **Settings**。

14. 从 **Authentication** 选项列表中选择 **Generic OIDC 设置**。
15. 点 **Edit**。
16. 在 **OIDC Key** 字段中，从第 5 步输入您的客户端名称。
17. 在 **OIDC Secret** 字段中，输入从第 8 步保存的 secret。
18. 在 **OIDC Provider URL** 字段中，输入您的 keycloak 服务器 URL 和端口。
19. 点击 **Save**。

OIDC 应该显示为登录的选项。点 **带有 OIDC 的 Sign in**，它会将您重定向到 SSO 服务器以登录并重定向到 Ansible Automation Platform。