



# Red Hat Ansible Automation Platform 2.1

## Ansible Automation Platform の Central Authentication のインストールおよび設定

Ansible Automation Platform の Central Authentication 機能の有効化



# Red Hat Ansible Automation Platform 2.1 Ansible Automation Platform の Central Authentication のインストールおよび設定

---

Ansible Automation Platform の Central Authentication 機能の有効化

## 法律上の通知

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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

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

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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.

## 概要

フィードバックの提供: このドキュメントを改善するための提案がある場合、またはエラーを見つけた場合は、テクニカルサポート () に連絡し、Docs コンポーネントを使用して Ansible Automation Platform Jira プロジェクトで issue を作成してください。

---

## 目次

はじめに .....	3
多様性を受け入れるオープンソースの強化 .....	4
第1章 AUTOMATION HUB 向けの ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION .....	5
1.1. システム要件 .....	5
1.2. AUTOMATION HUB で使用する ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION のイン ストール .....	5
第2章 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION へのユーザーストレージプロバイ ダー (LDAP/KERBEROS) の追加 .....	8
第3章 AUTOMATION HUB 管理者権限の割り当て .....	9
第4章 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION へのアイデンティティブローカー の追加 .....	10
4.1. ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION を使用したグループパーミッションの管 理 .....	11



## はじめに

Ansible Automation Platform Central Authentication はサードパーティーのアイデンティティプロバイダー (idP) ソリューションで、Ansible Automation Platform 全体で利用できる、シンプルなシングルサインオンソリューションを実現します。プラットフォーム管理者は、Central Authentication を使用して接続性と認証をテストし、新規ユーザーをオンボードしてグループに割り当てて設定し、ユーザーパーミッションを管理できます。Central Authentication は、OpenID Connect ベースのサポートおよび LDAP サポートだけでなく、お客様の使用状況をブートストラップ化するのに使用できるサポート対象の REST API も提供します。

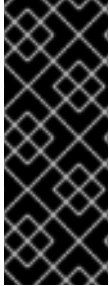
## 多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、[Red Hat CTO である Chris Wright のメッセージ](#) をご覧ください。



# 第1章 AUTOMATION HUB 向けの ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION

Automation Hub の Ansible Automation Platform Central Authentication を有効にするには、まず Red Hat Ansible Automation Platform インストーラーをダウンロードし、本書で詳しく記載されている必須手順に従って進めます。



## 重要

本書のインストーラーは、基本的なスタンドアロンデプロイメント向けに Central Authentication をインストールします。スタンドアロンモードは Central Authentication Server インスタンスのみを実行するため、クラスター化されたデプロイメントでは利用できません。スタンドアロンモードは、中央認証の機能をテストドライブおよび試行するために便利ですが、単一障害点しかいないため、実稼働環境でスタンドアロンモードを使用することは推奨しません。

別のデプロイメントモードで Central Authentication をインストールするには、[本書](#) でデプロイメントオプションを確認してください。

## 1.1. システム要件

Ansible Automation Platform Central Authentication のインストールおよび実行には、最小要件がいくつかあります。

- Java を実行するオペレーティングシステム
- Java 8 JDK
- zip または gzip および tar
- 512 MB 以上のメモリー
- 1GB 以上のディスク領域
- クラスターで Central Authentication を実行する場合は、PostgreSQL、MySQL、Oracle などの共有外部データベース。詳細は、[本書のデータベースの設定](#) セクションを参照してください。
- クラスターで実行する必要がある場合は、マシンでのネットワークマルチキャストサポート。Central Authentication はマルチキャストなしでクラスター化できますが、これには設定変更が複数必要になります。詳細は、[本書のクラスターリング](#) セクションを参照してください。
- Linux では、`/dev/random` の使用がセキュリティポリシーで義務付けられていない限り、利用可能なエントロピーの不足による Central Authentication のハングを防ぐために、ランダムデータのソースとして `/dev/urandom` を使用することをお勧めします。これを行うには、Oracle JDK 8 および OpenJDK 8 で、システムの起動時に `java.security.egd` システムプロパティを `file:/dev/urandom` に設定します。

## 1.2. AUTOMATION HUB で使用する ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION のインストール

Ansible Automation Platform Central Authentication のインストールは、Red Hat Ansible Automation Platform インストーラーに含まれています。以下の手順を使用して Ansible Automation Platform をイ

インストールしてから、インベントリーファイルに必要なパラメーターを設定して、Ansible Automation Platform と Central Authentication の両方を正常にインストールします。

### 1.2.1. Red Hat Ansible Automation Platform インストーラーの選択および取得

Red Hat Enterprise Linux 環境のインターネット接続に基づいて、必要な Ansible Automation Platform インストーラーを選択します。以下のシナリオを確認し、ニーズを満たす Red Hat Ansible Automation Platform インストーラーを決定してください。



#### 注記

Red Hat カスタマーポータルで Red Hat Ansible Automation Platform インストーラーのダウンロードにアクセスするには、有効な Red Hat カスタマーアカウントが必要です。

#### インターネットアクセスを使用したインストール

Red Hat Enterprise Linux 環境がインターネットに接続している場合は、Ansible Automation Platform インストーラーを選択します。インターネットアクセスを使用してインストールすると、必要な最新のリポジトリ、パッケージ、および依存関係が取得されます。

1. <https://access.redhat.com/downloads/content/480> に移動します。
2. **Ansible Automation Platform <latest-version> Setup** の **Download Now** をクリックします。
3. ファイルを展開します。

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

#### インターネットアクセスなしでのインストール

インターネットにアクセスできない場合や、オンラインリポジトリから個別のコンポーネントおよび依存関係をインストールしたくない場合は、Red Hat Ansible Automation Platform の **Bundle** インストーラーを使用します。Red Hat Enterprise Linux リポジトリへのアクセスは依然として必要です。その他の依存関係はすべて tar アーカイブに含まれます。

1. <https://access.redhat.com/downloads/content/480> に移動します。
2. **Ansible Automation Platform <latest-version> Setup Bundle** の **Download Now** をクリックします。
3. ファイルを展開します。

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

### 1.2.2. Red Hat Ansible Automation Platform インストーラーの設定

インストーラーを実行する前に、インストーラーパッケージにあるインベントリーファイルを編集して、Automation Hub および Ansible Automation Platform 認証のインストールを設定します。



#### 注記

[automationhub] ホストの到達可能な IP アドレスを指定して、ユーザーが別のノードから Private Automation Hub のコンテンツを同期して、新しいイメージをコンテナレジストリーにプッシュできるようにします。

1. インストーラーのディレクトリーに移動します。
  - a. オンラインインストーラー:
 

```
$ cd ansible-automation-platform-setup-<latest-version>
```
  - b. バンドルのインストーラー:
 

```
$ cd ansible-automation-platform-setup-bundle-<latest-version>
```
2. テキストエディターで **inventory** ファイルを開きます。
3. **[automationhub]** 配下にあるインベントリーファイルパラメーターを編集して、Automation Hub ホストのインストールを指定します。
  - a. Automation Hub の場所の IP アドレスまたは FQDN を使用して、**[automationhub]** 配下にグループホスト情報を追加します。
  - b. インストール仕様に基づいて、**automationhub\_admin\_password**、**automation\_pg\_password**、および追加のパラメーターのパスワードを入力します。
4. **sso\_keystore\_password** フィールドにパスワードを入力します。
5. **[SSO]** のインベントリーファイルパラメーターを編集して、Central Authentication のインストール先のホストを指定します。
  - a. **sso\_console\_admin\_password** フィールドにパスワードを入力し、インストール仕様に基づいて追加パラメーターを入力します。

### 1.2.3. Red Hat Ansible Automation Platform インストーラーの実行

インベントリーファイルが更新されたら、インストーラーパッケージにある **setup.sh** Playbook を使用してインストーラーを実行します。

1. **setup.sh** Playbook を実行します。

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

### 1.2.4. Central Authentication の管理者ユーザーとしてログインします。

Red Hat Ansible Automation Platform がインストールされたら、inventory ファイルに指定した admin 認証情報を使用して、管理ユーザーとしてログインして Central Authentication Server にログインします。

1. Ansible Automation Platform Central Authentication インスタンスに移動します。
2. インベントリーファイルの **sso\_console\_admin\_username** および **sso\_console\_admin\_password fields** に指定した admin 認証情報を使用して、ログインします。

Ansible Automation Platform Central Authentication が正常にインストールされており、管理者ユーザーでログインしている場合は、以下の手順に従ってユーザーストレージプロバイダー (LDAP など) を追加して続行できます。

## 第2章 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION へのユーザーストレージプロバイダー (LDAP/KERBEROS) の追加

Ansible Automation Platform Central Authentication には、LDAP/AD プロバイダーが組み込まれています。LDAP プロバイダーを Central Authentication に追加して、LDAP データベースからユーザー属性をインポートできます。

### 前提条件

- SSO admin ユーザーとしてログインしている。

### 手順

1. Ansible Automation Platform Central Authentication に SSO 管理ユーザーとしてログインします。
2. ナビゲーションバーから、**Configure section** → **User Federation** を選択します。
3. **Add provider** というドロップダウンメニューを使用して LDAP プロバイダーを選択し、LDAP 設定ページに進みます。

以下の表には、LDAP 設定で利用可能なオプションをまとめています。

設定オプション	説明
ストレージモード	ユーザーを Central Authentication ユーザーデータベースにインポートする場合は <b>On</b> に設定します。詳細は、 <a href="#">こちらのセクション</a> を参照してください。
モードの編集	管理者がユーザーメタデータで実行できる変更の種類を決定します。詳細は、 <a href="#">こちらのセクション</a> を参照してください。
コンソール表示名	このプロバイダーが管理コンソールで参照される場合に使用される名前
優先度	ユーザーを検索する、またはユーザーを追加する際のこのプロバイダーの優先度
登録の同期	管理コンソールで Ansible Automation Platform Central Authentication で作成した新規ユーザー、または登録ページを LDAP に追加する必要がある場合に有効にします。
Kerberos 認証を許可	LDAP からプロビジョニングされたユーザーデータを使用して、レルムで Kerberos/SPNEGO 認証を有効にします。詳細は、 <a href="#">こちらのセクション</a> を参照してください。

## 第3章 AUTOMATION HUB 管理者権限の割り当て

ハブの管理者ユーザーには、ユーザーのパーミッションとグループの管理用に、**hubadmin** のロールを割り当てる必要があります。Ansible Automation Platform Central Authentication クライアントを使用して、**hubadmin** のロールをユーザーに割り当てることができます。

### 前提条件

- ユーザーストレージプロバイダー (LDAP など) が Central Authentication に追加されている。

### 手順

1. SSO クライアントで **ansible-automation-platform** レルムに移動します。
2. ナビゲーションバーから **Manage → Users** を選択します。
3. ID をクリックして、一覧からユーザーを選択します。
4. **Role Mappings** タブをクリックします。
5. **Client Roles** のドロップダウンメニューを使用して、**automation-hub** を選択します。
6. **Available Roles** フィールドから **hubadmin** をクリックし、**Add selected >** をクリックします。

これで、ユーザーは **hubadmin** に設定されました。ステップ 3-6 を繰り返して、**hubadmin** ロールを割り当てます。

## 第4章 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION へのアイデンティティプロバイダーの追加

Ansible Automation Platform Central Authentication は、ソーシャルプロバイダーとプロトコルベースのプロバイダーの両方をサポートします。アイデンティティプロバイダーを Central Authentication に追加してレルムのソーシャル認証を有効化でき、ユーザーは Google、Facebook、GitHub などの既存のソーシャルネットワークアカウントを使用してログインできます。



### 注記

サポート対象のソーシャルネットワークの一覧と、そのネットワークの有効化の詳細は、[本セクション](#)を参照してください。

プロトコルベースのプロバイダーは、ユーザーの認証および承認に特定のプロトコルに依存するものです。これにより、特定のプロトコルに準拠するアイデンティティプロバイダーに接続できます。Ansible Automation Platform Central Authentication は、SAML v2.0 プロトコルおよび OpenID Connect v1.0 プロトコルをサポートします。

### 手順

1. Ansible Automation Platform Central Authentication に管理ユーザーとしてログインします。
2. ナビゲーションバーの **Configure** セクションで、**Identity Providers** をクリックします。
3. **Add provider** というドロップダウンメニューを使用して、アイデンティティプロバイダーを選択し、アイデンティティプロバイダー設定ページに進みます。

以下の表は、アイデンティティプロバイダー設定で利用できるオプションの一覧です。

表4.1 Identity Broker 設定オプション

設定オプション	説明
エイリアス	エイリアスはアイデンティティプロバイダーの一意の ID です。これはアイデンティティプロバイダーを内部で参照するために使用されます。 <b>OpenID Connect</b> などのプロトコルには、アイデンティティプロバイダーと通信するためにリダイレクト URI またはコールバック URL が必要です。この場合、エイリアスはリダイレクト URL の構築に使用されます。
有効	プロバイダーのオン/オフを切り替えます。
Hide on Login Page	有効にすると、このプロバイダーは、ログインページにログインオプションとして表示されません。クライアントは、ログインの要求に使用する URL の <b>kc_idp_hint</b> パラメーターを使用して、このプロバイダーの使用を引き続き要求できます。

Account Linking Only	これが有効な場合は、このプロバイダーを使用したユーザーのログインはできず、ログインページのオプションとしては表示されません。既存のアカウントをこのプロバイダーにリンクできます。
Store Tokens	アイデンティティプロバイダーから受け取ったトークンを保存するかどうか。
保存されたトークンの読み取り可能	ユーザーが保存されたアイデンティティプロバイダートークンを取得できるかどうか。これは、broker クライアントレベルのロール read token にも適用されます。
Trust Email	アイデンティティプロバイダーが提供するメールアドレスが信頼されているかどうか。レルムにメール検証が必要な場合、この IDP からログインするユーザーはメールの検証プロセスを行う必要はありません。
GUI Order	ログインページに、利用可能な IDP がどのように表示されているかを並べ替える注文番号。
First Login Flow	初めてこの IDP を使用して Central Authentication にログインするユーザーに対してトリガーされる認証フローを選択します。
Post Login Flow	ユーザーが外部アイデンティティプロバイダーでのログインを終了するとトリガーされる認証フローを選択します。

## 4.1. ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION を使用したグループパーミッションの管理

Ansible Automation Platform では、ユーザーグループに特定のパーミッションを割り当てることで、ユーザーアクセスを管理できます。Ansible Automation Platform に初めてログインすると、そのグループは Automation Hub のユーザーアクセスページに表示され、各グループにユーザーアクセスとパーミッションを割り当てることができます。

### 4.1.1. グループへのパーミッションの割り当て

ユーザーがシステム内の特定の機能にアクセスできるパーミッションを Automation Hub のグループに割り当てることができます。

#### 前提条件

**hubadmin** ユーザーとしてログインしている。

#### 手順

1. ローカルの Automation Hub にログインします。

2. **Groups** に移動します。
3. グループ名をクリックします。
4. **Edit** をクリックします。
5. パーミッションタイプのフィールドをクリックし、一覧に表示されるパーミッションを選択します。
6. パーMISSIONの割り当てが完了したら、**Save** をクリックします。

このグループは、割り当てられたパーミッションに関連付けられた Automation Hub の機能にアクセスできるようになりました。

#### 4.1.2. Automation Hub のパーミッション

パーミッションは、各グループが特定のオブジェクトに対して実行する一連の定義済みのアクションを提供します。以下のパーミッションに基づいて、グループに必要なアクセスレベルを決定します。

表4.2 パーMISSION参照テーブル

オブジェクト	パーMISSION	説明
<b>namespace</b>	namespace の追加 namespace へのアップロード 名前空間の変更 名前空間の削除	これらのパーMISSIONが割り当てられたグループは、名前空間の作成、コレクションのアップロード、または削除を行うことができます。
<b>collections</b>	Ansible リポジトリコンテンツの変更 コレクションの削除	このパーMISSIONが割り当てられたグループは、承認機能を使用してリポジトリ間でコンテンツを移動でき、確定または拒否機能で <b>staging</b> から <b>published</b> または <b>rejected</b> リポジトリにコンテンツを移動して、コレクションを削除します。
<b>users</b>	ユーザーの表示 ユーザーの削除 ユーザーの追加 ユーザーの変更	これらのパーMISSIONが割り当てられたグループは、ユーザー設定の管理および Automation Hub へのアクセスが可能です。
<b>groups</b>	グループの表示 グループの削除 グループの追加 グループの変更	これらのパーMISSIONが割り当てられたグループは、グループ設定の管理および Automation Hub へのアクセスが可能です。



オブジェクト	パーミッション	説明
コレクション リモート	コレクションリモートの変更 コレクションリモートの表示	これらの権限を持つグループは、 <b>Collections → Repo Management</b> に移動して、リモートリポジトリを設定できます。
containers	コンテナの名前空間パーミッションの変更 コンテナの変更 イメージタグの変更 新規コンテナの作成 既存コンテナへのプッシュ コンテナリポジトリの削除	これらのパーミッションが割り当てられたグループは、Automation Hub でコンテナリポジトリを管理できます。
リモートレジ ストリー	リモートレジストリーの追加 リモートレジストリーの変更 リモートレジストリーの削除	これらのパーミッションが割り当てられたグループは、Automation Hub に追加されたリモートレジストリーを追加、変更、または削除できます。
タスク管理	タスクの変更 タスクの削除 全タスクの表示	これらのパーミッションが割り当てられたグループは、Automation Hub の <b>Task Management</b> に追加されたタスクを管理できます。