



# Red Hat Ansible Automation Platform 2.2

## Automation Hub での Red Hat 認定コレクション および Ansible Galaxy コレクションの管理

Automation Hub を設定して、Red Hat 認定コレクションおよび Ansible Galaxy コレクションのコンテンツをユーザーに配布する



## Red Hat Ansible Automation Platform 2.2 Automation Hub での Red Hat 認定コレクションおよび Ansible Galaxy コレクションの管理

---

Automation Hub を設定して、Red Hat 認定コレクションおよび Ansible Galaxy コレクションのコンテンツをユーザーに配布する

## 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 での RED HAT 認定コレクション同期リストの管理 .....	5
1.1. RED HAT 認定コレクション同期リストについて .....	5
1.2. RED HAT 認定コレクションの同期リストの作成 .....	5
第2章 RED HAT 認定コレクションおよび ANSIBLE GALAXY コレクションのコンテンツを同期するための AUTOMATION HUB リモートリポジトリの設定 .....	7
2.1. リモートリポジトリについて .....	7
2.2. RED HAT 認定コレクションの同期 URL および API トークンの取得 .....	7
2.3. RH-CERTIFIED リモートリポジトリを設定し、RED HAT ANSIBLE CERTIFIED CONTENT COLLECTION を同期します。 .....	8
2.4. コミュニティーリモートリポジトリの設定および ANSIBLE GALAXY コレクションの同期 .....	8
第3章 PRIVATE AUTOMATION HUB のコレクションおよびコンテンツ署名 .....	10
3.1. PRIVATE AUTOMATION HUB でのコンテンツ署名の設定 .....	10
3.2. PRIVATE AUTOMATION HUB でのコンテンツ署名サービスの使用 .....	11
3.3. コレクションを検証するための ANSIBLE-GALAXY CLI の設定 .....	12
第4章 まとめ .....	14



## はじめに

Automation Hub を同期し、Ansible Automation Platform サブスクリプションを通じて利用可能な Red Hat 認定コレクションまたは Ansible Galaxy を通じて利用可能なコミュニティコレクションを使用できます。

組織は、console.redhat.com でホストされている Automation Hub サービス内のすべての Red Hat 認定コンテンツからの独自のコレクションセットにアクセスし、それらをキュレートできます。

Private Automation Hub を設定して、組織固有のニーズに合わせて調整された Ansible コンテンツコレクションの署名および公開を設定することもできます。

## 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 での RED HAT 認定コレクション同期リストの管理

Automation Hub を使用して、同期リストを作成し、関連する Red Hat 認定コレクションコンテンツをユーザーに配布できます。

## 1.1. RED HAT 認定コレクション同期リストについて

同期リストは、ローカル Automation Hub に同期する組織管理者によってアセンブルされた Red Hat 認定コレクションのキュレートされたグループです。同期リストを使用して、必要なコンテンツのみを管理し、不要なコレクションを除外します。console.redhat.com の Red Hat 認定コレクションの一部として利用可能なコンテンツから、同期リストを設計および管理できます

各同期リストには、Automation Hub のコンテンツのリモートソースとして指定するために使用できる独自の一意のリポジトリ URL があり、API トークンを使用して安全にアクセスできます。

## 1.2. RED HAT 認定コレクションの同期リストの作成

console.redhat.com の Automation Hub で、Red Hat 認定コレクションの同期リストを作成できます。同期リストリポジトリは **Automation Hub → Repo Management** にあります。これは、Red Hat 認定コレクション内でコンテンツを管理するたびに更新されます。

デフォルトでは、すべての Red Hat 認定コレクションは最初の組織の同期リストに含まれています。

### 前提条件

- 有効な Ansible Automation Platform サブスクリプションがある。
- consoleredhat.com の組織管理者パーミッションがある。
- 以下のドメイン名が、接続成功のファイアウォールまたはプロキシの許可リストに含まれており、Automation Hub または Galaxy サーバーからコレクションをダウンロードするようにしてください。
  - **galaxy.ansible.com**
  - **cloud.redhat.com**
  - **console.redhat.com**
  - **sso.redhat.com**
- Automation Hub リソースは Amazon Simple Storage に保存されます。次のドメイン名を許可リストに追加します。
  - **automation-hub-prd.s3.us-east-2.amazonaws.com**
  - **ansible-galaxy.s3.amazonaws.com**
- 自己署名証明書または Red Hat ドメインを使用する場合に SSL インспекションは無効になります。

### 手順

1. console.redhat.com にログインします。

2. **Automation Hub → Collections** に移動します。

3. 各コレクションで切り替えスイッチを使用して、同期リストから除外するかどうかを判断します。

同期リストのコレクションの管理が終了したら、**Automation Hub → Repo Management** に移動して、ローカル Automation Hub へのリモートリポジトリ同期を開始できます。リモートリポジトリがすでに設定されている場合は、Red Hat 認定コレクションを手動でローカルの Automation Hub に同期して、ローカルユーザーが利用できるようにしたコレクションコンテンツを更新できます。

## 第2章 RED HAT 認定コレクションおよび ANSIBLE GALAXY コレクションのコンテンツを同期するための AUTOMATION HUB リモートリポジトリの設定

ローカルの Automation Hub を設定して、console.redhat.com の組織リポジトリでホストされている Red Hat 認定コレクションと同期するか、Ansible Galaxy で選択したコレクションと同期することができます。

### 2.1. リモートリポジトリについて

リモートリポジトリを設定することで、console.redhat.com の組織リポジトリでホストされている Red Hat 認定コレクション、および Ansible Galaxy で選択したコレクションと同期するようにローカルの Automation Hub を設定できます。

**Repo Management → Remote** にある各リモートリポジトリは、リポジトリが **最後に更新された** 日時とコンテンツが **最後に同期された** 日時について、**community** および **rh-certified** の両方に情報を提供します。**Repo Management → Remote** ページに含まれる **編集** および **同期** 機能を使用して、いつでも Automation Hub に新しいコンテンツを追加できます。

### 2.2. RED HAT 認定コレクションの同期 URL および API トークンの取得

組織がキュレーションした Red Hat 認定コレクションを console.redhat.com からローカルの Automation Hub に同期できます。

#### 前提条件

- console.redhat.com の組織管理者パーミッションがある。

#### 手順

1. 組織管理者として console.redhat.com にログインします。
2. **Automation Hub → Repo Management** に移動します。
3. **Sync URL** を探して、**Copy to clipboard** アイコン (  ) をクリックします。rh-certified リモートの設定時に使用するファイルに **Sync URL** を貼り付けます。
4. **More actions** アイコン (  ) をクリックし、**Get token** をクリックします。
5. **Token management** ページで **Load token** をクリックします。
6. **Copy to clipboard** をクリックし、API トークンをコピーします。
7. API トークンをファイルに貼り付け、安全な場所に保存します。



#### 重要

API トークンは、コンテンツを保護するために使用されるシークレットトークンです。API トークンを安全な場所に保存します。

## 2.3. RH-CERTIFIED リモートリポジトリを設定し、RED HAT ANSIBLE CERTIFIED CONTENT COLLECTION を同期します。

**rh-certified** リモートリポジトリを編集して、cloud.redhat.com でホストされる Automation Hub からローカルの Automation Hub にコレクションを同期します。デフォルトでは、ローカル Automation Hub **rh-certified** リポジトリには、cloud.redhat.com で利用可能な Red Hat 認定コレクションのグループ全体の URL が含まれています。組織によって指定されたコレクションのみを使用するには、一意の URL を含める必要があります。

### 前提条件

- **Modify Ansible repo content** パーミッションがある。パーミッションの詳細は、[Managing user access in Automation Hub](#) を参照してください。
- console.redhat.com で Automation Hub がホストするサービスから同期 URL および API トークンを取得している。
- ポート 443 へのアクセスを設定している。これは、認定されたコレクションを同期するために必要です。詳細については、Red Hat Ansible Automation Platform 計画ガイドの [ネットワークポートとプロトコル](#) の章にある Automation Hub の表を参照してください。

### 手順

1. ローカルの Automation Hub にログインします。
2. **Repo Management** に移動します。
3. **Remotes** タブをクリックします。
4. **rh-certified** リモートで  をクリックしてから、**Edit** をクリックします。
5. モーダルで、cloud.redhat.com から取得した同期 URL およびトークンを貼り付けます。
6. **Save** をクリックします。

モーダルが閉じて、**Repo Management** ページに戻ります。console.redhat.com の組織の同期リストと Private Automation Hub の間でコレクションを同期できるようになりました。

+ **.Sync** をクリックしてコレクションを同期します。

同期ステータス 通知が更新され、Red Hat 認定コレクションの同期が完了したことが通知されます。

### 検証

コレクションコンテンツのドロップダウンリストから **Red Hat 認定** を選択して、コレクションコンテンツが正常に同期されていることを確認できます。

## 2.4. コミュニティリモートリポジトリの設定および ANSIBLE GALAXY コレクションの同期

コミュニティー リモートリポジトリを編集して、ローカルの Automation Hub に選択した Ansible Galaxy のコレクションを同期できます。デフォルトでは、ローカルの Automation Hub **community** リポジトリは <https://galaxy.ansible.com/api/> に送信されます。


## 前提条件

- **Modify Ansible repo content** パーミッションがある。パーミッションの詳細は、[Managing user access in Automation Hub](#) を参照してください。
- Ansible Galaxy から同期するコレクションを識別する **requirements.yml** ファイルがあります。以下の例を参照してください。

## requirements.yml の例

```
collections:
  # Install a collection from Ansible Galaxy.
  - name: community.aws
    version: 5.2.0
    source: https://galaxy.ansible.com
```

## 手順

1. ローカルの Automation Hub にログインします。
2. **Repo Management** に移動します。
3. **Remotes** タブをクリックします。
4. **community** リモートで、**More Actions** アイコン  をクリックし、**Edit** をクリックします。
5. モーダルで **Browse** をクリックし、ローカルマシンで **requirements.yml** ファイルを見つけます。
6. **Save** をクリックします。

モーダルが閉じて、**Repo Management** ページに戻ります。**requirements.yml** ファイルで識別されたコレクションを Ansible Galaxy からローカルの Automation Hub に同期できるようになりました。

1. **Sync** をクリックして、Ansible Galaxy および Automation Hub からコレクションを同期します。

**同期ステータス** 通知が更新され、Ansible Galaxy コレクションの Automation Hub への同期の完了または失敗が通知されます。

## 検証

コレクションコンテンツのドロップダウンリストから **Community** を選択して、同期が正常に行われたことを確認できます。

## 第3章 PRIVATE AUTOMATION HUB のコレクションおよびコンテンツ署名

組織の自動化管理者は、組織内の異なるグループから Ansible コンテンツコレクションの署名および公開に Private Automation Hub を設定できます。

セキュリティを強化するために、自動化作成者は Ansible-Galaxy CLI を設定してこのコレクションを検証し、Automation Hub へのアップロード後に変更されていないことを確認できます。

### 3.1. PRIVATE AUTOMATION HUB でのコンテンツ署名の設定

Ansible 認定コンテンツコレクションを正常に署名して公開するには、署名する Private Automation Hub を設定する必要があります。

#### 前提条件

- GnuPG キーペアがセキュアに設定され、組織で管理されている。
- 公開鍵と秘密鍵のペアには、Private Automation Hub でコンテンツ署名を設定するのに適切なアクセスがある。

#### 手順

1. ファイル名のみを受け入れる署名スクリプトを作成します。



#### 注記

このスクリプトは署名サービスとして機能し、**PULP\_SIGNING\_KEY\_FINGERPRINT** 環境変数で指定されたキーを使用して、そのファイルの ascii-armored 分離 **gpg** 署名を生成する必要があります。

次に、スクリプトは、以下の形式で JSON 構造を出力します。

```
{"file": "filename", "signature": "filename.asc"}
```

すべてのファイル名は、現在の作業ディレクトリー内の相対パスです。ファイル名は、以下に示すようにデタッチされた署名と同じである必要があります。

以下の例は、コンテンツの署名を生成するスクリプトを示しています。

```
#!/usr/bin/env bash

FILE_PATH=$1
SIGNATURE_PATH="$1.asc"

ADMIN_ID="$PULP_SIGNING_KEY_FINGERPRINT"
PASSWORD="password"

# Create a detached signature
gpg --quiet --batch --pinentry-mode loopback --yes --passphrase \
    $PASSWORD --homedir ~/.gnupg/ --detach-sign --default-key $ADMIN_ID \
    --armor --output $SIGNATURE_PATH $FILE_PATH
```

```
# Check the exit status
STATUS=$?
if [ $STATUS -eq 0 ]; then
    echo {"file": \"$FILE_PATH\", \"signature\": \"$SIGNATURE_PATH\"}
else
    exit $STATUS
fi
```

署名が有効なプライベート Automation Hub を Ansible Automation Platform クラスターにデプロイした後、コレクションを操作すると、新しい UI の追加が表示されます。

2. **automationhub\_\*** で始まるオプションについては、AAP インストーラーのインベントリファイルを確認してください。

```
[all:vars]
.
.
.
automationhub_create_default_collection_signing_service = True
automationhub_auto_sign_collections = True
automationhub_require_content_approval = True
automationhub_collection_signing_service_key = /abs/path/to/galaxy_signing_service.gpg
automationhub_collection_signing_service_script = /abs/path/to/collection_signing.sh
```

2 つの新しいキー (**automationhub\_auto\_sign\_collections** および **automationhub\_require\_content\_approval**) は、コレクションに署名する必要がある、Private Automation Hub へのアップロード後に承認が必要であることを示しています。

## 3.2. PRIVATE AUTOMATION HUB でのコンテンツ署名サービスの使用

Private Automation Hub でコンテンツ署名を設定したら、新しいコレクションに手動で署名するか、既存の署名を新しい署名に置き換えることができ、特定のコレクションをダウンロードする場合に、確実にそのコレクションが自分のものであることが、認定後に変更されていないことが分かります。

Private Automation Hub のコンテンツ署名は、以下のシナリオのソリューションを提供します。

- システムに自動署名が設定されていないため、手動署名プロセスを使用してコレクションに署名する必要がある場合。
- 自動設定されたコレクションの現在の署名が破損しているため、新規署名に置き換える必要がある場合。
- 以前に署名されたコンテンツに追加の署名が必要な場合。
- コレクションで署名をローテーションする必要がある場合。

### 手順

1. Automation Hub UI で Private Automation Hub インスタンスにログインします。
2. 左側のナビゲーションで、**コレクション → 承認** をクリックします。Approval ダッシュボードがコレクションのリストと共に表示されます。
3. 署名するコレクションごとに、**Sign and approve** をクリックします。

4. 手動で署名および承認されたコレクションが Collections タブに表示されていることを確認します。

### 3.3. コレクションを検証するための ANSIBLE-GALAXY CLI の設定

Ansible-Galaxy CLI を設定して、コレクションを検証することができます。これにより、ダウンロードしたコレクションは組織によって承認され、Automation Hub にアップロードされた後に変更されません。

コレクションが Automation Hub によって署名されている場合に、サーバーは ASCII 版の GPG 割り当て解除署名を提供して、コレクションのコンテンツを検証する前に **MANIFEST.json** の信頼性を検証します。**ansible-galaxy** の [キーリングを設定する](#) か、**--keyring** オプションでパスを指定して、署名検証をオプトインする必要があります。

#### 前提条件

- 署名付きコレクションが Automation Hub で署名を検証するために利用できる。
- 認定コレクションが組織内の承認済みのロールによって署名できる。
- 検証用の公開鍵がローカルシステムキーリングに追加されている。

#### 手順

1. **ansible-galaxy** で使用するデフォルト以外のキーリングに公開鍵をインポートするには、以下のコマンドを実行します。

```
gpg --import --no-default-keyring --keyring ~/.ansible/pubring.kbx my-public-key.asc
```



#### 注記

Automation Hub が提供する署名のほかに、署名ソースは要件ファイルとコマンドラインで指定することもできます。署名ソースは URI である必要があります。

2. **--signature** オプションを使用して、CLI で提供されたコレクション名を追加の署名で検証します。

```
ansible-galaxy collection install namespace.collection
--signature https://examplehost.com/detached_signature.asc
--signature file:///path/to/local/detached_signature.asc --keyring ~/.ansible/pubring.kbx
```

このオプションを複数回使用して、複数の署名を指定できます。

3. 以下の例のように、要件ファイルのコレクションに、コレクションの署名キーの後に追加の署名ソースが表示されていることを確認します。

```
# requirements.yml
collections:
  - name: ns.coll
    version: 1.0.0
  signatures:
    - https://examplehost.com/detached_signature.asc
```

```
- file:///path/to/local/detached_signature.asc
```

```
ansible-galaxy collection verify -r requirements.yml --keyring ~/.ansible/pubring.kbx
```

Automation Hub からコレクションをインストールすると、サーバーが提供する署名はインストールされたコレクションと共に保存され、コレクションの信頼性を検証します。

4. (オプション) Ansible Galaxy サーバーにクエリーを実行せずにコレクションの内部整合性を再度確認する必要がある場合は、**--offline** オプションを使用して、以前に使用したのと同じコマンドを実行します。

## 第4章 まとめ

これまでの手順をすべて完了したら、以下が達成できます。

- Red Hat 認定コレクションコンテンツの同期リストを作成する。
- コンテンツをローカルの Automation Hub に同期する。
- Ansible Galaxy からの指定されたコミュニティコレクションをユーザーに配布する。
- Private Automation Hub でコンテンツ署名を設定した。
- 組織の固有のニーズにあったコレクションを署名して承認した。
- Ansible-Galaxy CLI を設定して、コレクションに署名する前に検証する。

ユーザーは、ローカル Automation Hub のコレクションコンテンツを表示し、ダウンロードできるようになりました。