# Red Hat Ansible Automation Platform 2.4

## 자동화 허브의 콘텐츠 관리

자동화 허브에서 컬렉션, 콘텐츠 및 리포지토리 생성 및 관리

Last Updated: 2024-07-27

# Red Hat Ansible Automation Platform 2.4 자동화 허브의 콘텐츠 관리

자동화 허브에서 컬렉션, 콘텐츠 및 리포지토리 생성 및 관리

## 법적 공지



## 초록

이 가이드에서는 자동화 허브에서 콘텐츠를 생성, 편집, 삭제 및 이동하는 방법을 보여줍니다.

# 차례

# RED HAT 문서에 관한 피드백 제공

이 문서를 개선하기 위한 제안이 있거나 오류를 찾을 수 있는 경우 https://access.redhat.com 에서 기술 지원에 문의하여 요청을 열 수 있습니다.

# 1장. 자동화 허브에서 RED HAT 인증, 검증 및 ANSIBLE GALAXY 콘텐츠

Ansible 인증 콘텐츠 컬렉션은 Red Hat Ansible Automation Platform 서브스크립션에 포함되어 있습니다. Red Hat Ansible 콘텐츠에는 Ansible 인증 콘텐츠 컬렉션 및 Ansible 검증 컨텐츠의 두 가지 유형이 포함되어 있습니다. Ansible 자동화 허브를 사용하면 모든 Ansible 콘텐츠 양식에서 고유한 컬렉션 집합에 액세스하고 큐레이트할 수 있습니다.

Red Hat Ansible 콘텐츠에는 다음 두 가지 유형의 콘텐츠가 포함되어 있습니다.

- Ansible 인증 콘텐츠 컬렉션
- Ansible 검증 콘텐츠 컬렉션

Ansible 검증 컬렉션은 플랫폼 설치 관리자를 통해 프라이빗 자동화 허브에서 사용할 수 있습니다. 번들 설치 프로그램이 있는 Red Hat Ansible Automation Platform을 다운로드할 때 기본적으로 검증된 콘텐츠는 기본적으로 프라이빗 자동화 허브에 미리 채워져 있지만 인벤토리의 일부로 프라이빗 자동화 허브를 활성화하는 경우에만 해당됩니다.

번들 설치 프로그램을 사용하지 않는 경우 Red Hat에서 제공하는 Ansible 플레이북을 사용하여 검증된 콘텐츠를 설치할 수 있습니다. 자세한 내용은 Ansible 검증 콘텐츠를 참조하십시오.

패키지를 다운로드하여 이러한 컬렉션을 수동으로 업데이트할 수 있습니다.

## Ansible 컬렉션을 인증하는 이유는 무엇입니까?

Ansible 인증 프로그램을 사용하면 Red Hat과 에코시스템 파트너 간의 Red Hat Ansible Certified Content에 대한 공유 지원을 제공할 수 있습니다. Ansible 및 인증된 파트너 콘텐츠에 문제가 발생한 최종 고객은 지원 티켓(예: 정보 요청 또는 Red Hat의 문제)을 열 수 있으며 Red Hat과 에코시스템 파트너가 티켓을 해결할 것으로 예상합니다.

Red Hat은 Certified Partners가 시장 인식을 높이고 수요를 생성하며 공동으로 판매할 수 있도록 시장 출시 이점을 제공합니다.

Red Hat Ansible Certified Content Collections는 공동으로 지원되는 Ansible 콘텐츠를 위한 중앙 집중식 리포지토리인 Ansible 자동화 허브(서브스크립션 필요)를 통해 배포됩니다. 인증된 파트너로서 Ansible 자동화 허브에 컬렉션을 게시하면 최종 고객은 잘 알려진 지원 라이프 사이클을 사용하여 프로덕션 환경에서 신뢰할 수 있는 자동화 콘텐츠를 사용하는 방법을 관리할 수 있습니다.

솔루션 인증 시작에 대한 자세한 내용은 Red Hat Partner Connect 를 참조하십시오.

## 컬렉션을 어떻게 인증 받을 수 있습니까?

컬렉션 인증 방법에 대한 자세한 내용은 Red Hat Partner Connect 에 대한 Ansible 인증 정책 가이드를 참조하십시오.

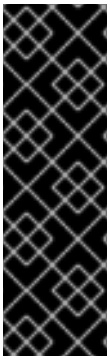
## Certified Collections에 대한 공동 지원 계약은 어떻게 수행됩니까?

고객이 인증된 컬렉션에 대해 Red Hat 지원 팀에서 문제를 제기하는 경우 Red Hat 지원은 문제를 평가하고 Ansible 또는 Ansible 사용 내에 문제가 있는지 확인합니다. 또한 이 문제가 인증된 컬렉션에 있는지 확인합니다. 인증된 컬렉션에 문제가 있는 경우 지원 팀은 TSANet과 같은 합의된 도구를 통해 인증된 컬렉션의 공급 업체 소유자로 문제를 전송합니다.

## Ansible 역할만 포함된 컬렉션을 생성하고 인증할 수 있습니까?

역할만 포함된 컬렉션을 생성하고 인증할 수 있습니다. 현재 테스트 요구 사항은 모듈이 포함된 컬렉션에 중점을 두고 있으며, 현재 역할이 포함된 컬렉션을 테스트하는 데 추가 리소스가 진행 중입니다. 자세한 내용은 ansiblepartners@redhat.com 에 문의하십시오.

## 1.1. 자동화 허브에서 ANSIBLE 콘텐츠 컬렉션 동기화



**중요**

2.4 릴리스에서는 계속 콘텐츠를 동기화할 수 있지만 동기화 목록은 더 이상 사용되지 않으며 향후 버전에서 제거됩니다.

콘텐츠를 동기화하려면 rh- certified remote에서 수동으로 생성된 요구 사항 파일을 업로드할 수 있습니다.

원격은 외부 컬렉션 소스에서 사용자 지정 리포지토리에 콘텐츠를 동기화할 수 있는 구성입니다.

Ansible 자동화 허브를 사용하여 동기화 목록 또는 요구 사항 파일을 생성하여 관련 Red Hat Ansible 인증 콘텐츠 컬렉션을 사용자에게 배포할 수 있습니다. 요구 사항 파일 사용에 대한 자세한 내용은 *Ansible 컬렉션 사용 가이드의 요구 사항 파일을 사용하여 여러 컬렉션 설치*를 참조하십시오.

### 1.1.1. Red Hat Ansible Certified Content Collections 동기화 목록에 대한 설명

동기화 목록은 조직 관리자가 조립한 Red Hat Certified Collections 그룹입니다. 로컬 Ansible 자동화 허브와 동기화됩니다. 동기화 목록을 사용하여 원하는 콘텐츠만 관리하고 불필요한 컬렉션을 제외합니다. console.redhat.com에서 Red Hat 콘텐츠의 일부로 제공되는 컨텐츠에서 동기화 목록을 설계 및 관리

각 동기화 목록에는 자동화 허브의 콘텐츠의 원격 소스로 지정하는 데 사용할 수 있는 고유한 리포지토리 URL이 있습니다. API 토큰을 사용하여 각 동기화 목록에 안전하게 액세스합니다.

### 1.1.2. Red Hat Ansible 인증 콘텐츠 컬렉션의 동기화 목록 생성

console.redhat.com에서 Ansible 자동화 허브에서 선별된 Red Hat Ansible 인증 컨텐츠의 동기화 목록을 생성할 수 있습니다. 동기화 목록 리포지토리는 Ansible 인증 콘텐츠 컬렉션 내의 콘텐츠를 관리할 때마다 업데이트되는 **Collection → Repositories** 의 자동화 허브 탐색 패널에 있습니다.

모든 Ansible 인증 콘텐츠 컬렉션은 기본적으로 초기 조직 동기화 목록에 포함됩니다.

**사전 요구 사항**

- 유효한 Ansible Automation Platform 서브스크립션이 있어야 합니다.
- console.redhat.com에 대한 조직 관리자 권한이 있습니다.
- 다음 도메인 이름은 방화벽 또는 프록시의 허용 목록에 포함됩니다. 자동화 허브 또는 Galaxy 서버에서 컬렉션을 성공적으로 연결하고 다운로드하는 데 필요합니다.
  - **galaxy.ansible.com**
  - **cloud.redhat.com**
  - **console.redhat.com**
  - **sso.redhat.com**
- Ansible 자동화 허브 리소스는 Amazon Simple Storage에 저장됩니다. 다음 도메인 이름은 허용 목록에 있어야 합니다.
  - **automation-hub-prd.s3.us-east-2.amazonaws.com**

- **ansible-galaxy.s3.amazonaws.com**

- 자체 서명된 인증서를 사용하는 경우 또는 Red Hat 도메인에 대해 SSL 검사가 비활성화됩니다.

**프로세스**

1. **console.redhat.com** 에 로그인합니다.
2. **Automation Hub → 컬렉션** 으로 이동합니다.
3. 각 컬렉션에 토글 스위치를 제외하거나 동기화 목록에 포함하십시오.
4. 원격 리포지토리 동기화를 시작하려면 자동화 허브로 이동하여 **Collection → Repositories** 를 선택합니다.
5. **More Actions** 아이콘 Cryostat 를 클릭하고 **Sync** 를 선택하여 프라이빗 자동화 허브에 대한 원격 리포지토리 동기화를 시작합니다.
6. 선택 사항: 원격 리포지토리가 이미 구성된 경우 Red Hat Ansible 인증 콘텐츠 컬렉션을 프라이빗 자동화 허브에 수동으로 동기화하여 로컬 사용자가 사용할 수 있는 컬렉션 콘텐츠를 업데이트합니다.

## 1.2. 콘텐츠를 동기화하도록 ANSIBLE 자동화 허브 원격 리포지토리 구성

원격 구성을 사용하여 **console.redhat.com** 에서 호스팅되는 Ansible 인증 콘텐츠 컬렉션 또는 Ansible Galaxy의 컬렉션과 동기화되도록 프라이빗 자동화 허브를 구성합니다.

**중요**

2.4 릴리스에서는 계속 콘텐츠를 동기화할 수 있지만 동기화 목록은 더 이상 사용되지 않으며 향후 버전에서 제거됩니다.

콘텐츠를 동기화하려면 rh- certified remote에서 수동으로 생성된 요구 사항 파일을 업로드할 수 있습니다.

원격은 외부 컬렉션 소스에서 사용자 지정 리포지토리에 콘텐츠를 동기화할 수 있는 구성입니다.

**Ansible Galaxy와 Ansible 자동화 허브의 차이점은 무엇입니까?**
Ansible Galaxy에 게시된 컬렉션은 Ansible 커뮤니티에서 게시한 최신 콘텐츠이며 이와 관련된 공동 지원 클레임이 없습니다. Ansible Galaxy는 콘텐츠에 액세스하는 Ansible 커뮤니티에 권장되는 프런트 엔드 디렉터리입니다.

Ansible 자동화 허브에 게시된 컬렉션은 Red Hat 및 선택한 파트너사의 공동 고객을 대상으로 합니다. 고객은 Ansible 자동화 허브에서 컬렉션에 액세스하고 다운로드하려면 Ansible 서브스크립션이 필요합니다. 인증된 컬렉션은 Red Hat과 파트너사가 전략적 관계를 맺고 공동 고객을 지원할 준비가 되어 있으며 추가 테스트 및 검증을 수행했을 수 있음을 의미합니다.

**Ansible Galaxy에서 네임스페이스를 요청하려면 어떻게 해야 합니까?**
Ansible Galaxy GitHub 문제를 통해 네임스페이스를 요청하려면 다음 단계를 따르십시오.

- mailto:ansiblepartners@redhat.com로 이메일을 보내주십시오.
- Ansible Galaxy에 등록하는 데 사용되는 GitHub 사용자 이름을 포함합니다.

시스템의 유효성을 검사하려면 한 번 이상 로그인해야 합니다.

사용자가 네임스페이스 관리자로 추가되면 self-serve 프로세스를 사용하여 관리자를 추가할 수 있습니다.

**Ansible Galaxy 네임스페이스 이름 지정에 대한 제한 사항이 있습니까?**
컬렉션 네임스페이스는 python 모듈 이름 규칙을 따라야 합니다. 즉, 컬렉션에는 모두 소문자 이름이 짧아야 합니다. 가독성을 향상시키는 경우 컬렉션 이름에 밑줄을 사용할 수 있습니다.

### 1.2.1. 원격 구성을 생성하는 이유

**Collections → Remotes** 에 있는 각 원격 구성은 리포지토리가 **마지막으로 업데이트된** 시기에 대한 **커뮤니티** 및 **rh-인증** 리포지토리 모두에 대한 정보를 제공합니다. **컬렉션 → 리포지토리** 페이지에 포함된 **편집** 및 **동기화** 기능을 사용하여 언제든지 Ansible 자동화 허브에 새 콘텐츠를 추가할 수 있습니다.

### 1.2.2. Red Hat Certified Collection을 위한 동기화 URL 및 API 토큰 검색

console.redhat.com에서 선별한 Ansible 인증 콘텐츠 컬렉션을 **console.redhat.com** 에서 프라이빗 자동화 허브에 동기화할 수 있습니다. API 토큰은 콘텐츠를 보호하는 데 사용되는 시크릿 토큰입니다.

**사전 요구 사항**

- console.redhat.com에서 동기화 목록을 생성할 수 있는 조직 관리자 권한이 있습니다.

**프로세스**

1. **console.redhat.com** 에 조직 관리자로 로그인합니다.
2. **Automation Hub → Connect to Hub** 이동합니다.
3. **오프라인 토큰** 에서 **로드 토큰** 을 클릭합니다.
4. **복사를 클릭하여 API** 토큰을 복사합니다.
5. API 토큰을 파일에 붙여넣고 안전한 위치에 저장합니다.

### 1.2.3. rh- certified remote repository 구성 및 Red Hat Ansible Certified Content Collection 동기화

**rh- certified** remote repository를 편집하여 console.redhat.com에서 호스팅되는 자동화 허브의 컬렉션을 프라이빗 자동화 허브에 동기화할 수 있습니다. 기본적으로 프라이빗 자동화 허브 **rh- certified** repository에는 Ansible 인증 콘텐츠 컬렉션의 전체 그룹에 대한 URL이 포함되어 있습니다.

조직에서 지정한 컬렉션만 사용하기 위해 프라이빗 자동화 허브 관리자는 **rh- certified** remote에서 수동으로 생성된 요구 사항 파일을 업로드할 수 있습니다.

요구 사항 파일 사용에 대한 자세한 내용은 *Ansible 컬렉션 사용 가이드의 요구 사항 파일을 사용하여 여러 컬렉션 설치를* 참조하십시오.

요구 사항 파일에 컬렉션 **A**,**B** 및 **C** 가 있고 사용하려는 새 컬렉션 **X** 가 console.redhat.com에 추가되는 경우 프라이빗 자동화 허브를 동기화하려면 요구 사항 파일에 **X** 를 추가해야 합니다.

**사전 요구 사항**

- 유효한 **Modify Ansible repo 콘텐츠 권한이 있습니다**. 권한에 대한 자세한 내용은 프라이빗 자동화 허브에 대한 사용자 액세스 구성을 참조하십시오.
- console.redhat.com의 자동화 허브 호스팅 서비스에서 동기화 URL 및 API 토큰을 검색했습니다.
- 포트 443에 대한 액세스를 구성했습니다. 인증된 컬렉션을 동기화하는 데 필요합니다. 자세한 내용은 Red Hat Ansible Automation Platform 계획 가이드의 네트워크 포트 및 프로토콜 장에 있는 자동화 허브 표를 참조하십시오.

**프로세스**

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 **Collections → Remotes** 를 선택합니다.
3. **rh- certified** remote repository에서 **More Actions** 아이콘을 클릭하고 **Edit** 를 클릭합니다.
4. **URL** 필드에 **동기화 URL** 을 붙여넣습니다.
5. **토큰** 필드에 console.redhat.com에서 얻은 토큰을 붙여넣습니다.
6. **저장**을 클릭합니다.
   console.redhat.com과 프라이빗 자동화 허브의 조직 동기화 목록 간에 컬렉션을 동기화할 수 있습니다.
7. **More Actions** 아이콘 Cryostat를 **클릭하고 동기화** 를 선택합니다.

**검증**

**Sync status** notification updates to notify you that the Red Hat Certified Content Collections synchronization is complete.

- 컬렉션 콘텐츠 드롭다운 목록에서 **Red Hat Certified**를 선택하여 컬렉션 콘텐츠가 동기화되었는지 확인합니다.

### 1.2.4. 커뮤니티 원격 리포지토리 구성 및 Ansible Galaxy 컬렉션 동기화

**커뮤니티** 원격 리포지토리를 편집하여 선택한 컬렉션을 Ansible Galaxy에서 프라이빗 자동화 허브로 동기화할 수 있습니다. 기본적으로 프라이빗 자동화 허브 커뮤니티 리포지토리는 **galaxy.ansible.com/api/** 로 이동합니다.

**사전 요구 사항**

- **수정 Ansible 리포지토리 콘텐츠 권한이 있습니다**. 권한에 대한 자세한 내용은 프라이빗 자동화 허브에 대한 사용자 액세스 구성을 참조하십시오.
- 다음 예제와 같이 Ansible Galaxy에서 동기화할 컬렉션을 식별하는 **requirements.yml** 파일이 있습니다.

**requirements.yml 예**

```
collections:
  # Install a collection from Ansible Galaxy.
  - name: community.aws
```

```
version: 5.2.0
source: https://galaxy.ansible.com
```

프로세스

1. 자동화 허브에 로그인합니다.
2. 탐색 패널에서 **Collections → Remotes** 를 선택합니다.
3. **커뮤니티** 원격에서 **More Actions** 아이콘을 클릭하고 **Edit** 를 선택합니다.
4. **YAML 요구 사항** 필드에서 **찾아보기** 를 클릭하고 로컬 시스템에서 **requirements.yml** 파일을 찾습니다.
5. **저장**을 클릭합니다.
   이제 Ansible Galaxy의 **requirements.yml** 파일에서 식별된 컬렉션을 프라이빗 자동화 허브로 동기화할 수 있습니다.
6. **More Actions** 아이콘 Cryostat를 클릭하고 Sync 를 선택하여 Ansible Galaxy 및 Ansible 자동화 허브에서 컬렉션을 동기화합니다.

검증

Ansible 자동화 허브에 대한 Ansible Galaxy 컬렉션 동기화의 완료 또는 실패를 알리는 동기화 상태 알림 업데이트입니다.

- 컬렉션 콘텐츠 드롭다운 목록에서 커뮤니티를 선택하여 동기화를 확인합니다.

### 1.2.5. 프록시 설정 구성

프라이빗 자동화 허브가 네트워크 프록시 뒤에 있는 경우 로컬 네트워크 외부에 있는 콘텐츠를 동기화하도록 원격에 프록시 설정을 구성할 수 있습니다.

사전 요구 사항

- 유효한 Modify Ansible repo 콘텐츠 권한이 있습니다. 권한에 대한 자세한 내용은 프라이빗 자동화 허브에 대한 사용자 액세스 구성을 참조하십시오.
- 로컬 네트워크 관리자의 프록시 URL 및 인증 정보가 있습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 Collections →Remotes 를 선택합니다.
3. rh- certified 또는 Community 원격에서 **More Actions** 아이콘을 클릭하고 Edit 를 선택합니다.
4. 고급 옵션 표시 드롭다운 메뉴를 확장합니다.
5. 적절한 필드에 프록시 URL, 프록시 사용자 이름 및 프록시 암호를 입력합니다.
6. 저장을 클릭합니다.

## 1.3. 프라이빗 자동화 허브에서 콘텐츠 서명 컬렉션 및 콘텐츠 서명

조직의 자동화 관리자는 조직 내의 다양한 그룹에서 Ansible 콘텐츠 컬렉션에 서명하고 게시하도록 프라이빗 자동화 허브를 구성할 수 있습니다.

추가 보안을 위해 자동화 작성자는 Ansible-Galaxy CLI를 구성하여 자동화 허브에 업로드된 후 이러한 컬렉션이 변경되지 않았는지 확인할 수 있습니다.

### 1.3.1. 프라이빗 자동화 허브에서 콘텐츠 서명 구성

Ansible 인증 콘텐츠 컬렉션에 성공적으로 서명하고 게시하려면 서명을 위해 프라이빗 자동화 허브를 구성해야 합니다.

사전 요구 사항

- GnuPG 키 쌍은 조직에서 안전하게 설정 및 관리합니다.
- 공개-개인 키 쌍은 프라이빗 자동화 허브에서 콘텐츠 서명을 구성하기 위한 적절한 액세스 권한을 갖습니다.

프로세스

1. 파일 이름만 허용하는 서명 스크립트를 생성합니다.

참고

이 스크립트는 서명 서비스 역할을 하며 **PULP_SIGNING_KEY_FINGERPRINT** 환경 변수를 통해 지정된 키를 사용하여 해당 파일의 ascii-armored detached **gpg** 서명을 생성해야 합니다.

스크립트는 다음 형식을 사용하여 JSON 구조를 출력합니다.

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

모든 파일 이름은 현재 작업 디렉터리 내부의 상대 경로입니다. 분리된 서명에는 파일 이름이 동일해야 합니다.

예제:

다음 스크립트는 콘텐츠에 대한 서명을 생성합니다.

```
#!/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
```

Ansible Automation Platform 클러스터에 서명이 활성화된 프라이빗 자동화 허브를 배포하면 컬렉션에 새로운 UI 추가 기능이 표시됩니다.

2. **automationhub_*** 로 시작하는 옵션은 Ansible Automation Platform 설치 프로그램 인벤토리 파일을 검토하십시오.

```
[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
```

두 개의 새 키(automationhub_auto_sign_collections 및 Automation hub_require_content_approval)는 컬렉션이 프라이빗 자동화 허브에 업로드된 후 서명하고 승인되어야 함을 나타냅니다.

### 1.3.2. 프라이빗 자동화 허브에서 콘텐츠 서명 서비스 사용

프라이빗 자동화 허브에 콘텐츠 서명을 구성한 후 새 컬렉션에 수동으로 서명하거나 기존 서명을 새 서명으로 교체할 수 있습니다. 사용자가 특정 컬렉션을 다운로드할 때 이 서명은 컬렉션이 해당 컬렉션을 위한 것이며 인증 후 수정되지 않았음을 나타냅니다.

다음 시나리오에서 프라이빗 자동화 허브에서 콘텐츠 서명을 사용할 수 있습니다.

- 시스템에 자동 서명이 구성되지 않았으며 수동 서명 프로세스를 사용하여 컬렉션에 서명해야 합니다.
- 자동으로 구성된 컬렉션의 현재 서명이 손상되어 새 서명이 필요합니다.
- 이전에 서명된 콘텐츠에 대한 추가 서명이 필요합니다.
- 컬렉션에서 서명을 교체하려고 합니다.

프로세스

1. Ansible Automation Platform에 로그인합니다.
2. 탐색 패널에서 컬렉션 → 승인 을 선택합니다. 승인 대시보드가 열리고 컬렉션 목록이 표시됩니다.
3. 서명 을 클릭하고 서명할 각 컬렉션에 대해 승인 합니다.

검증

- 서명하고 수동으로 승인한 컬렉션이 컬렉션 탭에 표시되는지 확인합니다.

### 1.3.3. 서명 공개 키 다운로드

컬렉션에 서명하고 승인한 후 자동화 허브 UI에서 서명 공개 키를 다운로드합니다. 로컬 시스템 인증 키에 추가하기 전에 공개 키를 다운로드해야 합니다.

프로세스

1. 자동화 허브에 로그인합니다.
2. 탐색 패널에서 서명 키를 선택합니다. 서명 키 대시보드에는 컬렉션 및 컨테이너 이미지 등 여러 키 목록이 표시됩니다.
   - 컬렉션을 확인하려면 **collections-** 접두사가 붙은 키를 다운로드합니다.
   - 컨테이너 이미지를 확인하려면 **container-** 접두사가 붙은 키를 다운로드합니다.
3. 공개 키를 다운로드하려면 다음 방법 중 하나를 선택합니다.
   - 메뉴 아이콘을 선택하고 **Download Key** 를 클릭하여 공개 키를 다운로드합니다.
   - 목록에서 공개 키를 선택하고 *클립보드에 복사* 아이콘을 클릭합니다.
   - *공개 키* 탭에서 드롭다운 메뉴를 클릭하고 전체 공개 키 블록을 복사합니다.

복사한 공개 키를 사용하여 설치 중인 콘텐츠 컬렉션을 확인합니다.

### 1.3.4. 컬렉션을 확인하도록 Ansible-Galaxy CLI 구성

컬렉션을 확인하도록 Ansible-Galaxy CLI를 구성할 수 있습니다. 이렇게 하면 다운로드한 컬렉션이 조직에서 승인되고 자동화 허브에 업로드된 후 변경되지 않았습니다.

컬렉션이 자동화 허브에 의해 서명된 경우 서버는 ASCII, GPG-detached 서명을 제공하여 컬렉션의 내용을 확인하기 전에 **MANIFEST.json** 의 진위 여부를 확인합니다.**ansible-galaxy** 의 인증 키를구성하거나 **--keyring** 옵션을 사용하여 경로를 제공하여 서명 확인을 선택해야 합니다.

사전 요구 사항

- 서명된 컬렉션은 자동화 허브에서 서명을 확인하는 데 사용할 수 있습니다.
- 인증된 컬렉션은 조직 내에서 승인된 역할로 서명할 수 있습니다.
- 확인을 위한 공개 키가 로컬 시스템 인증 키에 추가되었습니다.

프로세스

1. **ansible-galaxy** 와 함께 사용할 기본이 아닌 인증 키로 공개 키를 가져오려면 다음 명령을 실행합니다.

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

참고

자동화 허브에서 제공하는 서명 외에도 요구 사항 파일과 명령줄에 서명 소스를 제공할 수 있습니다. 서명 소스는 URI여야 합니다.

2. 추가 서명으로 CLI에 제공된 컬렉션 이름을 확인하려면 다음 명령을 실행합니다.

```
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
```

이 옵션을 여러 번 사용하여 여러 서명을 제공할 수 있습니다.

3. 다음 예제와 같이 요구 사항 파일의 컬렉션에 컬렉션 서명 키 뒤에 추가 서명 소스가 나열되는지 확인합니다.

```
# 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
```

자동화 허브에서 컬렉션을 설치하면 서버에서 제공한 서명이 설치된 컬렉션과 함께 저장되므로 컬렉션의 진위 여부를 확인할 수 있습니다.

4. (선택 사항) Ansible Galaxy 서버를 쿼리하지 않고 컬렉션의 내부 일관성을 다시 확인해야 하는 경우 **--offline** 옵션을 사용하여 이전에 사용한 것과 동일한 명령을 실행합니다.

컬렉션 이름 지정에 대한 권장 사항이 있습니까?
**company_name.product** 형식으로 컬렉션을 생성합니다. 이 형식은 회사 네임스페이스 아래에 여러 제품이 서로 다른 컬렉션을 가질 수 있음을 의미합니다.

Ansible 자동화 허브에 네임스페이스를 가져오려면 어떻게 해야 합니까?
기본적으로 Ansible Galaxy에 사용되는 네임스페이스는 Ansible 파트너 팀의 Ansible 자동화 허브에서도 사용됩니다. 모든 문의 및 설명이 필요한 경우 ansiblepartners@redhat.com.

## 1.4. ANSIBLE 검증 콘텐츠

Red Hat Ansible Automation Platform에는 기존 Red Hat Ansible 인증 콘텐츠를 보완하는 Ansible 검증 컨텐츠가 포함되어 있습니다.

Ansible 검증 콘텐츠는 Red Hat과 신뢰할 수 있는 파트너 모두의 다양한 플랫폼에서 운영 작업을 수행할 수 있는 전문가 주도의 경로를 제공합니다.

### 1.4.1. 설치 프로그램을 사용하여 검증된 컬렉션 구성

번들 설치 프로그램을 다운로드하여 실행하면 인증된 컬렉션이 자동으로 업로드됩니다. 인증된 컬렉션은 **rh- certified** repository에 업로드됩니다. 검증된 컬렉션은검증된 리포지토리에 업로드됩니다.

다음 두 변수를 사용하여 기본 구성으로 변경할 수 있습니다.

- **Automationhub_seed_collections** 는 사전 로드 여부를 정의하는 부울입니다.
- **automationhub_collection_seed_repository. true** 로 설정할 때 업로드할 콘텐츠 유형을 지정할 수 있는 변수입니다. 가능한 값은 인증 또는검증 입니다. 누락된 경우 두 콘텐츠 세트가 모두 업로드됩니다.

### 1.4.2. tarball을 사용하여 검증된 콘텐츠 설치

**번들 설치 프로그램을 사용하지 않는 경우 독립 실행형 tarball, ansible-validated-content-bundle-1.tar.gz 를 사용할 수 있습니다. 나중에 이 독립 실행형 tarball을 사용하여 번들 설치 프로그램을 다시 실행할 필요 없이 최신 tarball을 사용할 수 있게 되면 모든 환경에서 검증된 콘텐츠를 업데이트할 수도 있습니다.**

**사전 요구 사항**

**플레이북을 실행하려면 다음 변수가 필요합니다.**

| 이름 | 설명 |
|---|---|
| **automationhub_admin_password** | 관리 암호입니다. |
| **automationhub_api_token** | 자동화 허브용으로 생성된 API 토큰입니다. |
| **automationhub_main_url** | 예: **https://automationhub.example.com** |
| **automationhub_require_content_approval** | 부울(**true** 또는 **false**)<br><br>이는 자동화 허브 배포 중에 사용되는 값과 일치해야 합니다.<br><br>이 변수는 설치 프로그램에서 **true** 로 설정합니다. |

**프로세스**

1. **tarball을 얻으려면 Red Hat Ansible Automation Platform 다운로드페이지로 이동하여 Ansible 검증 콘텐츠를 선택합니다.**
2. **콘텐츠를 업로드하고 변수를 정의합니다. (이 예제에서는 automationhub_api_token사용)**

```
ansible-playbook collection_seed.yml
-e automationhub_api_token=<api_token>
-e automationhub_main_url=https://automationhub.example.com
-e automationhub_require_content_approval=true
```

**참고**

**automationhub_admin_password 또는 automationhub_api_token 둘 중 하나를 사용합니다.**

**완료되면 개인 자동화 허브의 검증된 컬렉션 섹션에 컬렉션이 표시됩니다. 이제 프라이빗 자동화 허브에서 컬렉션을 보고 다운로드할 수 있습니다.**

**추가 리소스**

**ansible 플레이북 실행에 대한 자세한 내용은 ansible-playbook 을 참조하십시오.**

# 2장. 자동화 허브에서 컬렉션 관리

콘텐츠 작성자는 자동화 허브에서 네임스페이스를 사용하여 다음과 같은 목적으로 컬렉션을 큐레이트하고 관리할 수 있습니다.

- 네임스페이스를 선별하고 개인 자동화 허브에 컬렉션을 업로드할 수 있는 권한이 있는 그룹을 생성
- 자동화 작업에서 컬렉션의 최종 사용자를 돕기 위해 네임스페이스에 정보와 리소스를 추가합니다.
- 네임스페이스에 컬렉션 업로드
- 네임스페이스 가져오기 로그를 확인하여 컬렉션 및 현재 승인 상태를 업로드 성공 또는 실패 여부를 확인합니다.

콘텐츠 생성에 대한 자세한 내용은 Red Hat Ansible Automation Platform Creator Guide를 참조하십시오.

## 2.1. 네임스페이스를 사용하여 자동화 허브의 컬렉션 관리

네임스페이스는 콘텐츠 컬렉션을 업로드하고 게시할 수 있는 자동화 허브의 고유한 위치입니다. 자동화 허브의 네임스페이스에 대한 액세스는 그룹에 의해 관리되며 여기에 표시되는 콘텐츠 및 관련 정보를 관리할 수 있는 권한이 있습니다.

자동화 허브에서 네임스페이스를 사용하여 내부 배포 및 사용을 위해 조직 내에서 개발된 컬렉션을 구성할 수 있습니다.

네임스페이스를 사용하는 경우 컬렉션을 생성, 편집 및 업로드할 수 있는 권한이 있는 그룹이 네임스페이스에 있어야 합니다. 네임스페이스에 업로드된 컬렉션에는 게시하고 사용할 수 있도록 하기 전에 관리 승인이 필요합니다.

### 2.1.1. 콘텐츠 큐레이터를 위한 새 그룹 생성

조직의 콘텐츠 큐레이션을 지원하도록 설계된 프라이빗 자동화 허브에서 새 그룹을 생성할 수 있습니다. 이 그룹은 프라이빗 자동화 허브에 게시하기 위해 내부적으로 개발한 컬렉션에 기여할 수 있습니다.

콘텐츠 개발자가 네임스페이스를 생성하고 내부적으로 개발한 컬렉션을 프라이빗 자동화 허브에 업로드하려면 먼저 그룹을 생성 및 편집하고 필요한 권한을 할당해야 합니다.

사전 요구 사항

- 프라이빗 자동화 허브에서 관리 권한이 있으며 그룹을 생성할 수 있습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 사용자 액세스 → 그룹을 선택하고 생성 을 클릭합니다.
3. 모달에 그룹의 이름으로 Content Engineering 을 입력하고 생성 을 클릭합니다. 새 그룹을 생성하고 그룹 페이지가 열립니다.
4. 권한 탭에서 편집 을 클릭합니다.
5. 네임스페이스 에서 네임스페이스 추가, 네임스페이스에 업로드, 네임스페이스 변경을 위한 권한을 추가합니다 .

6. 저장을 클릭합니다.
   새 그룹은 사용자가 할당한 권한으로 생성됩니다. 그런 다음 그룹에 사용자를 추가할 수 있습니다.

7. 그룹 페이지에서 사용자 탭을 클릭합니다.

8. 추가 를 클릭합니다.

9. 사용자를 선택하고 추가 를 클릭합니다.

### 2.1.2. 네임스페이스 생성

네임스페이스를 생성하여 콘텐츠 개발자가 자동화 허브에 업로드하는 컬렉션을 구성할 수 있습니다. 네임스페이스를 생성할 때 자동화 허브의 그룹을 해당 네임스페이스 소유자로 할당할 수 있습니다.

사전 요구 사항

- 네임스페이스 추가 및 네임스페이스에 업로드 권한이 있습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.

2. 탐색 패널에서 컬렉션 → 네임스페이스를 선택합니다.

3. 생성 을 클릭하고 네임스페이스 이름을 입력합니다.

4. 네임스페이스 소유자 그룹을 할당합니다.

5. 생성을 클릭합니다.

이제 콘텐츠 개발자가 새 네임스페이스에 컬렉션을 업로드하고 소유자로 할당된 그룹의 사용자가 컬렉션을 업로드할 수 있습니다.

### 2.1.3. 네임스페이스에 추가 정보 및 리소스 추가

네임스페이스에 포함된 정보를 추가하고 사용자를 위한 리소스를 회사 컬렉션에 제공할 수 있습니다. 로고 및 설명을 추가하고 사용자를 GitHub 리포지토리, 문제 추적기 또는 기타 온라인 자산에 연결합니다. 자세한 정보를 포함하도록 리소스 편집 탭에 마크다운 텍스트를 입력할 수도 있습니다. 이 기능은 컬렉션을 자동화 작업에서 사용하는 사용자에게 유용합니다.

사전 요구 사항

- 네임스페이스 권한 변경이 있습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.

2. 탐색 패널에서 컬렉션 → 네임스페이스를 선택합니다.

3. **More Actions** 아이콘 Cryostat를 클릭하고 네임스페이스 편집을 선택합니다.

4. **Edit details** 탭에서 필드에 정보를 입력합니다.

5. **Edit resources** 탭을 클릭하여 텍스트 필드에 마크다운을 입력합니다.

6. 저장을 클릭합니다.

이제 콘텐츠 개발자가 새 네임스페이스에 컬렉션을 업로드하거나 소유자로 할당된 그룹의 사용자가 컬렉션을 업로드할 수 있습니다.

네임스페이스를 생성할 때 업로드할 권한이 있는 그룹은 승인을 위해 컬렉션을 추가하기 시작할 수 있습니다. 승인 후 네임스페이스의 컬렉션은 게시 리포지토리에 표시됩니다.

### 2.1.4. 네임스페이스에 컬렉션 업로드

**tar.gz** 파일 형식의 내부적으로 개발한 컬렉션을 프라이빗 자동화 허브 네임스페이스에 업로드하여 자동화 허브 관리자의 검토 및 승인을 받을 수 있습니다. 승인되면 컬렉션은 자동화 허브 사용자가 보고 다운로드할 수 있는 게시 콘텐츠 리포지토리로 이동합니다.

참고

컬렉션 파일 이름을 다음과 같이 포맷합니다. <my_namespace-my_collection-1.0.0.tar.gz>

사전 요구 사항

- 컬렉션을 업로드할 수 있는 네임스페이스가 있습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 컬렉션 → 네임스페이스를 선택하고 네임스페이스를 선택합니다.
3. **Upload collection** 을 클릭합니다.
4. 새 컬렉션 대화 상자에서 파일 선택을 클릭합니다.
5. 업로드할 컬렉션을 선택합니다.
6. 업로드를 클릭합니다.

내 가져오기 화면에 테스트 요약이 표시되고 컬렉션이 성공적으로 업로드되었는지 또는 실패한지 알려줍니다.

### 2.1.5. 네임스페이스 가져오기 로그 검토

네임스페이스에 업로드된 컬렉션의 상태를 검토하여 프로세스의 성공 또는 실패를 평가할 수 있습니다.

가져온 컬렉션 정보에는 다음이 포함됩니다.

상태
: 완료 또는 실패

승인 상태
: 승인 또는 승인 대기 중

버전
: 업로드된 컬렉션의 버전

로그 가져오기

컬렉션 가져오기 중 실행되는 활동

사전 요구 사항

- 컬렉션을 업로드할 수 있는 네임스페이스에 액세스할 수 있습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 컬렉션 → 네임스페이스를 선택합니다.
3. 네임스페이스를 선택합니다.
4. **More Actions** 아이콘 Cryostat를 클릭하고 내 가져오기 를 선택합니다.
5. 검색 필드를 사용하거나 목록에서 가져온 컬렉션을 찾습니다.
6. 가져온 컬렉션을 클릭합니다.
7. 컬렉션 가져오기 세부 정보를 검토하여 네임스페이스의 컬렉션 상태를 확인합니다.

### 2.1.6. 네임스페이스 삭제

원하지 않는 네임스페이스를 삭제하여 자동화 허브 서버에서 스토리지를 관리할 수 있습니다. 먼저 네임스페이스에 종속성이 있는 컬렉션이 포함되어 있지 않은지 확인해야 합니다.

사전 요구 사항

- 삭제 중인 네임스페이스에 종속 항목이 있는 컬렉션이 없습니다.
- 네임스페이스 권한이 삭제되었습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 컬렉션 → 네임스페이스를 선택합니다.
3. 삭제할 네임스페이스를 클릭합니다.
4. **More Actions** 아이콘 Cryostat를 클릭한 다음 네임스페이스 삭제 를 클릭합니다.

참고

**Delete namespace** 버튼이 비활성화된 경우 네임스페이스에 종속성이 있는 컬렉션이 포함됩니다. 이 네임스페이스의 컬렉션을 검토하고 종속성을 삭제합니다. 자세한 내용은 자동화 허브의 컬렉션 삭제 를 참조하십시오.

이제 사용자가 삭제한 네임스페이스와 관련 컬렉션이 이제 네임스페이스 목록 뷰에서 삭제 및 제거됩니다.

## 2.2. AUTOMATION HUB에서 내부 컬렉션의 게시 프로세스 관리

자동화 허브를 사용하여 조직 내에서 개발된 콘텐츠 컬렉션을 관리하고 게시합니다. 네임스페이스에 컬렉션을 업로드하고 그룹화할 수 있습니다. 게시된 콘텐츠 리포지토리에 표시하려면 관리 승인이 필요합니다. 컬렉션을 게시한 후 사용자는 사용하기 위해 액세스 및 다운로드할 수 있습니다.

조직의 인증 기준을 충족하지 않는 제출된 컬렉션을 거부할 수 있습니다.

### 2.2.1. 승인 정보

탐색 패널에 있는 승인 기능을 사용하여 자동화 허브에서 업로드된 컬렉션을 관리할 수 있습니다.

승인 대시보드

기본적으로 승인 대시보드에는 Needs Review 상태의 모든 컬렉션이 나열됩니다.게시 리포지토리에 포함되어 있는지 확인할 수 있습니다.

컬렉션 세부 정보 보기

버전 번호를 클릭하여 컬렉션에 대한 자세한 정보를 볼 수 있습니다.

컬렉션 필터링

네임스페이스, 컬렉션 이름 또는 리포지토리 별로 컬렉션을 필터링하여 콘텐츠를 찾고 해당 상태를 업데이트합니다.

### 2.2.2. 내부 게시에 대한 컬렉션 승인

내부 게시 및 사용을 위해 개별 네임스페이스에 업로드된 컬렉션을 승인할 수 있습니다. 검토 대기 중인 모든 컬렉션은 스테이징 리포지토리의 승인 탭에 있습니다.

사전 요구 사항

- 수정 Ansible 리포지토리 콘텐츠 권한이 있습니다.

프로세스

1. 탐색 패널에서 컬렉션 → 승인 을 선택합니다.
   승인이 필요한 컬렉션 상태는 검토가 필요합니다.
2. 검토할 컬렉션을 선택합니다.
3. 버전 을 클릭하여 컬렉션의 내용을 확인합니다.
4. 인증서 를 클릭하여 컬렉션을 승인합니다.

승인된 컬렉션은 사용자가 볼 수 있고 사용할 수 있는 게시 리포지토리로 이동합니다.

### 2.2.3. 검토를 위해 업로드된 컬렉션 거부

개별 네임스페이스에 업로드된 컬렉션을 거부할 수 있습니다. 검토 대기 중인 모든 컬렉션은 스테이징 리포지토리의 승인 탭에 있습니다.

승인이 필요한 컬렉션 상태는 검토가 필요합니다. 버전 을 클릭하여 컬렉션의 내용을 확인합니다.

사전 요구 사항

- 수정 Ansible 리포지토리 콘텐츠 권한이 있습니다.

프로세스

1. 탐색 패널에서 컬렉션 → 승인 을 선택합니다.
2. 검토할 컬렉션을 찾습니다.
3. 거부를 클릭하여 컬렉션을 거부합니다.

게시를 거부한 컬렉션은 거부 된 리포지토리로 이동합니다.

## 2.3. 자동화 허브를 사용한 리포지토리 관리

자동화 허브 관리자는 리포지토리 간에 자동화 콘텐츠 컬렉션을 생성, 편집, 삭제 및 이동할 수 있습니다.

### 2.3.1. 자동화 허브의 리포지토리 유형

자동화 허브에서는 컬렉션을 확인할지 여부에 따라 두 가지 유형의 리포지토리에 컬렉션을 게시할 수 있습니다.

스테이징 리포지토리

네임스페이스에 업로드할 권한이 있는 모든 사용자는 이러한 리포지토리에 컬렉션을 게시할 수 있습니다. 이러한 리포지토리의 컬렉션은 검색 페이지에서 사용할 수 없습니다. 대신 관리자가 확인할 승인 대시보드에 표시됩니다. 스테이징 리포지토리는 **pipeline=staging** 레이블로 표시됩니다.

사용자 정의 리포지토리

리포지토리에 대한 쓰기 권한이 있는 모든 사용자는 이러한 리포지토리에 컬렉션을 게시할 수 있습니다. 사용자 지정 리포지토리는 모든 사용자가 볼 수 있는 퍼블릭 또는 보기 권한이 있는 사용자만 볼 수 있는 프라이빗 리포지토리일 수 있습니다. 이러한 리포지토리는 승인 대시보드에 표시되지 않습니다. 리포지토리 소유자가 검색을 활성화하면 검색 결과에 컬렉션이 표시될 수 있습니다.

기본적으로 자동화 허브에는 컬렉션을 업로드하는 데 리포지토리를 지정하지 않으면 자동으로 사용되는 하나의 스테이징 리포지토리가 포함되어 있습니다. 사용자는 리포지토리 생성 중에 새 스테이징 리포지토리를 생성할 수 있습니다.

### 2.3.2. 자동화 허브의 사용자 정의 리포지토리에 대한 승인 파이프라인

자동화 허브에서는 **pipeline=approved** 라벨이 표시된 모든 리포지토리에 컬렉션을 승인할 수 있습니다. 기본적으로 자동화 허브에는 승인된 콘텐츠를 위한 리포지토리가 하나 포함되어 있지만 리포지토리 생성 화면에서 더 추가할 수 있는 옵션이 있습니다. **pipeline=approved** 레이블이 표시된 리포지토리에 직접 게시할 수 없습니다. 컬렉션은 먼저 스테이징 리포지토리를 통해 이동하고 'pipleline=approved' 리포지토리에 게시되기 전에 승인해야 합니다.

자동 승인

자동 승인이 활성화되면 스테이징 리포지토리에 업로드하는 모든 컬렉션이 **pipeline=approved** 로 표시된 모든 리포지토리로 자동으로 승격됩니다.

승인 필요

자동 승인이 비활성화되면 관리자는 승인 대시보드를 보고 스테이징 리포지토리에 업로드된 컬렉션을 확인할 수 있습니다. **Approve** 를 클릭하면 승인된 리포지토리 목록이 표시됩니다. 이 목록에서 관리자는 콘텐츠를 승격해야 하는 하나 이상의 리포지토리를 선택할 수 있습니다.
승인된 리포지토리가 하나만 있는 경우 컬렉션이 자동으로 승격되고 관리자가 리포지토리를 선택하라는 메시지가 표시되지 않습니다.

거부

거부된 컬렉션은 사전 설치된 거부된 리포지토리에 자동으로 배치됩니다.

### 2.3.3. 사용자 정의 리포지토리에 대한 액세스를 제한하는 역할 기반 액세스 제어

RBAC(역할 기반 액세스 제어)를 사용하여 사용자 역할에 따라 액세스 권한을 정의하여 사용자 지정 리포지토리에 대한 사용자 액세스를 제한합니다. 기본적으로 사용자는 자동화 허브의 모든 공용 리포지토리를 볼 수 있지만 역할에서 액세스를 허용하지 않는 한 리포지토리를 수정할 수 없습니다. 리포지토리의 다른 작업에 동일한 논리가 적용됩니다. 예를 들어 역할 권한을 변경하여 사용자 지정 리포지토리에서 콘텐츠를 다운로드할 수 있는 사용자의 기능을 제거할 수 있습니다. 자동화 허브 의 사용자 액세스 관리에 대한 정보는 프라이빗 자동화 허브에 대한 사용자 액세스 구성 을 참조하십시오.

### 2.3.4. 자동화 허브에서 사용자 정의 리포지토리 생성

Red Hat Ansible Automation Platform을 사용하여 리포지토리를 생성하면 리포지토리를 비공개로 구성하거나 검색 결과에서 숨길 수 있습니다.

프로세스

1. 자동화 허브에 로그인합니다.
2. 탐색 패널에서 Collection → Repositories 를 선택합니다.
3. 리포지토리 추가를 클릭합니다.
4. 리포지토리 이름을 입력합니다.
5. Description (설명) 필드에서 리포지토리의 목적을 설명합니다.
6. 변경할 때마다 이전 버전의 리포지토리를 유지하려면 버전 수를 선택합니다. 유지된 버전 수는 0에서 무제한까지 지정할 수 있습니다. 모든 버전을 저장하려면 이 값을 null로 설정합니다.

참고

사용자 지정 리포지토리를 변경하는 데 문제가 있는 경우 보존한 다른 리포지토리 버전으로 되돌릴 수 있습니다.

7. Pipeline 필드에서 리포지토리의 파이프라인을 선택합니다. 이 옵션은 컬렉션을 리포지토리에 게시할 수 있는 사용자를 정의합니다.

   스테이징
   : 누구나 자동화 콘텐츠를 리포지토리에 게시할 수 있습니다.

   승인됨
   : 이 리포지토리에 추가된 컬렉션은 스테이징 리포지토리를 통해 승인 프로세스를 거쳐야 합니다. 자동 승인이 활성화되면 스테이징 리포지토리에 업로드된 모든 컬렉션이 승인된 모든 리포지토리로 자동으로 승격됩니다.

   없음
   : 리포지토리에 대한 권한이 있는 모든 사용자는 리포지토리에 직접 게시할 수 있으며 리포지토리는 승인 파이프라인의 일부가 아닙니다.

8. 선택 사항: 검색 결과에서 리포지토리를 숨기려면 검색에서 숨기기 를 선택합니다. 이 옵션은 기본적으로 선택됩니다.
9. 선택 사항: 리포지토리를 비공개로 만들려면 개인용으로 만들기 를 선택합니다. 리포지토리를 볼 수 있는 권한이 없는 모든 사용자가 리포지토리를 숨깁니다.

10. 원격 리포지토리의 콘텐츠를 이 리포지토리에 동기화하려면 Remote 를 선택하고 사용자 지정 리포지토리에 포함할 컬렉션이 포함된 원격을 선택합니다. 자세한 내용은 리포지토리 동기화를 참조하십시오.

11. 저장을 클릭합니다.

다음 단계

- 리포지토리가 생성되면 세부 정보 페이지가 표시됩니다.
  여기에서 리포지토리에 대한 액세스 권한을 제공하고, 컬렉션을 검토하거나 추가하고, 저장된 사용자 지정 리포지토리 버전에서 작업할 수 있습니다.

### 2.3.5. 사용자 정의 자동화 허브 리포지토리에 대한 액세스 제공

기본적으로 개인 리포지토리 및 자동화 콘텐츠 컬렉션은 시스템의 모든 사용자에게 숨겨집니다. 공용 리포지토리는 모든 사용자가 볼 수 있지만 수정할 수는 없습니다. 사용자 지정 리포지토리에 대한 액세스 권한을 제공하려면 다음 절차를 사용하십시오.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.

2. 탐색 패널에서 Collection → Repositories 를 선택합니다.

3. 목록에서 리포지토리를 찾아서 **More Actions** (추가 작업) 아이콘을 클릭한 다음 Edit 를 선택합니다.

4. 액세스 탭을 선택합니다.

5. 리포지토리 소유자에 대한 그룹을 선택합니다.
   사용자 액세스 구현에 대한 정보는 프라이빗 자동화 허브에 대한 사용자 액세스 구성을 참조하십시오.

6. 선택한 그룹에 할당할 역할을 선택합니다.

7. 저장을 클릭합니다.

### 2.3.6. 자동화 허브 리포지토리에 컬렉션 추가

리포지토리를 생성한 후 자동화 콘텐츠 컬렉션을 추가할 수 있습니다.

프로세스

1. 탐색 패널에서 Collection → Repositories 를 선택합니다.

2. 목록에서 리포지토리를 찾아서 **More Actions** (추가 작업) 아이콘을 클릭한 다음 Edit 를 선택합니다.

3. 컬렉션 버전 탭을 선택합니다.

4. 컬렉션 추가 를 클릭하고 리포지토리에 추가할 컬렉션을 선택합니다.

5. **Select** 를 클릭합니다.

### 2.3.7. 다른 자동화 허브 리포지토리 버전으로 되돌리기

리포지토리에서 자동화 콘텐츠 컬렉션이 추가되거나 제거되면 새 버전이 생성됩니다. 리포지토리에 변경해도 문제가 발생하면 이전 버전으로 되돌릴 수 있습니다. 되돌리기는 안전한 작업이며 시스템에서 컬렉션을 삭제하지 않고 리포지토리와 연결된 콘텐츠를 변경합니다. 저장된 버전 수는 리포지토리가 생성 될 때 Retained 버전 설정 수에 정의되어 있습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 Collection → Repositories 를 선택합니다.
3. 목록에서 리포지토리를 찾아서 **More Actions** (추가 작업) 아이콘을 클릭한 다음 Edit 를 선택합니다.
4. 되돌리려는 버전을 찾은 다음 **More Actions** 아이콘 을 클릭하고이 버전으로 Revert를 선택합니다.
5. **Revert** 를 클릭합니다.

## 2.3.8. 자동화 허브에서 원격 구성 관리

자동화 허브를 실행하는 모든 서버에 원격 구성을 설정할 수 있습니다. 원격 구성을 사용하면 외부 컬렉션 소스에서 사용자 지정 리포지토리에 콘텐츠를 동기화할 수 있습니다.

### 2.3.8.1. 자동화 허브에서 원격 구성 생성

Red Hat Ansible Automation Platform을 사용하여 외부 컬렉션 소스에 대한 원격 구성을 생성할 수 있습니다. 그런 다음 해당 컬렉션의 콘텐츠를 사용자 지정 리포지토리에 동기화할 수 있습니다.

프로세스

1. 자동화 허브에 로그인합니다.
2. 탐색 패널에서 Collections → Remotes 를 선택합니다.
3. 원격 추가를 클릭합니다.
4. 원격 구성 의 이름을 입력합니다.
5. 특정 리포지토리의 경로를 포함하여 원격 서버의 URL 을 입력합니다.

참고

원격 서버 URL 및 리포지토리 경로를 찾으려면 Collection → Repositories 로 이동하여 리포지토리를 선택한 다음 **CLI** 구성 복사를 클릭합니다.

6. 외부 컬렉션에 액세스하는 데 필요한 토큰 또는 사용자 이름 및 암호를 입력하여 원격 서버에 대한 인증 정보를 구성합니다.

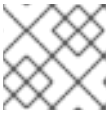
참고

탐색 패널에서 토큰을 생성하려면 컬렉션 → API 토큰을 선택하고 토큰 를 클릭하고 로드된 토큰을 복사합니다.

7. console.redhat.com에서 컬렉션에 액세스하려면 SSO URL 을 입력하여 ID 공급자(IdP)에 로그인합니다.

8. YAML 요구 사항 파일을 선택하거나 생성하여 사용자 지정 리포지토리와 동기화할 컬렉션 및 버전 범위를 식별합니다. 예를 들어 kubernetes 및 AWS 컬렉션 버전 5.0.0 이상만 다운로드하려면 요구 사항 파일은 다음과 같습니다.

```
Collections:
  - name: community.kubernetes
 - name: community.aws
 version:">=5.0.0"
```



참고

모든 컬렉션 종속 항목은 동기화 프로세스 중에 다운로드됩니다.

9. 선택 사항: 원격을 추가로 구성하려면 고급 구성에서 사용할 수 있는 옵션을 사용합니다.

   a. 조직의 회사 프록시가 있는 경우 프록시 URL , Proxy Username 및 Proxy Password 를 입력합니다.

   b. TLS 검증 확인란을 사용하여 전송 계층 보안을 활성화하거나 비활성화합니다.

   c. 인증에 디지털 인증서가 필요한 경우 클라이언트 키 및 클라이언트 인증서 를 입력합니다.

   d. 서버에 자체 서명된 SSL 인증서를 사용하는 경우 CA 인증서 필드에 인증에 사용되는 PEM 인코딩 클라이언트 인증서를 입력합니다.

   e. 이 원격에서 컬렉션을 다운로드할 수 있는 속도를 가속화하려면 Download concurrency 필드에서 tandem에서 다운로드할 수 있는 컬렉션 수를 지정합니다.

   f. 이 원격에서 초당 쿼리 수를 제한하려면 속도 제한을 지정합니다.

참고

일부 서버에는 특정 속도 제한이 있을 수 있으며, 이를 초과하면 동기화가 실패합니다.

#### 2.3.8.2. 원격 구성에 대한 액세스 제공

원격 구성을 생성한 후 누구나 사용할 수 있으려면 액세스 권한을 제공해야 합니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.

2. 탐색 패널에서 Collections → Remotes 를 선택합니다.

3. 목록에서 리포지토리를 찾고 **More Actions** (추가 작업) 아이콘을 클릭한 다음 Edit 를 선택합니다.

4. 액세스 탭을 선택합니다.

5. 리포지토리 소유자에 대한 그룹을 선택합니다.사용자 액세스 구현에 대한 정보는 프라이빗 자동화 허브에 대한 사용자 액세스 구성 을 참조하십시오.

6. 선택한 그룹에 적절한 역할을 선택합니다.

7. 저장을 클릭합니다.

### 2.3.9. 자동화 허브에서 리포지토리 동기화

하나의 자동화 허브에서 다른 자동화 허브로 리포지토리를 동기화하여 사용자에게 관련 자동화 콘텐츠 컬렉션을 배포할 수 있습니다. 최신 컬렉션 업데이트가 있는지 확인하려면 사용자 지정 리포지토리를 원격과 정기적으로 동기화합니다.

프로세스

1. 자동화 허브에 로그인합니다.

2. 탐색 패널에서 Collection → Repositories 를 선택합니다.

3. 목록에서 리포지토리를 찾아 동기화 를 클릭합니다.
구성된 원격의 모든 컬렉션은 사용자 지정 리포지토리에 다운로드됩니다. 컬렉션 동기화 상태를 확인하려면 탐색 패널에서 작업 관리를 선택합니다.

참고

원격 내의 특정 컬렉션으로 리포지토리 동기화를 제한하려면 requirements.yml 파일을 사용하여 가져올 특정 컬렉션을 식별할 수 있습니다. 자세한 내용은 원격 만들기 를 참조하십시오.

추가 리소스

요구 사항 파일 사용에 대한 자세한 내용은 *Ansible 컬렉션 사용 가이드의 요구 사항 파일을 사용하여 여러 컬렉션 설치를* 참조하십시오.

### 2.3.10. 자동화 허브에서 컬렉션 내보내기 및 가져오기

Ansible 자동화 허브는 리포지토리 내에 자동화 콘텐츠 컬렉션을 저장합니다. 이러한 컬렉션은 자동화 콘텐츠 작성자가 버전입니다. 동일한 컬렉션의 여러 버전이 동일하거나 다른 리포지토리에 동시에 존재할 수 있습니다.

컬렉션은 가져오고 내보낼 수 있는 .tar 파일로 저장됩니다. 이 스토리지 형식을 사용하면 새 리포지토리로 가져오는 컬렉션이 원래 생성 및 내보낸 것과 동일합니다.

#### 2.3.10.1. 자동화 허브에서 자동화 콘텐츠 컬렉션 내보내기

컬렉션이 완료되면 조직 전체의 다른 사용자에게 배포할 수 있는 위치로 가져올 수 있습니다.

프로세스

1. 프라이빗 자동화 허브에 로그인합니다.

2. 탐색 패널에서 컬렉션을 선택합니다 . 컬렉션 페이지에는 모든 리포지토리의 모든 컬렉션이 표시됩니다. 특정 컬렉션을 검색할 수 있습니다.

3. 내보낼 컬렉션을 선택합니다. 컬렉션 세부 정보 페이지가 열립니다.

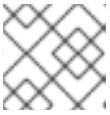
4. Install 탭에서 tarball 다운로드를 선택합니다. .tar 파일은 기본 브라우저 다운로드 폴더에 다운로드됩니다. 이제 선택한 위치로 가져올 수 있습니다.

### 2.3.10.2. 자동화 허브에서 자동화 콘텐츠 컬렉션 가져오기

자동화 콘텐츠 작성자는 사용자 지정 리포지토리에 사용할 컬렉션을 가져올 수 있습니다. 사용자 지정 리포지토리에서 컬렉션을 사용하려면 먼저 자동화 허브 관리자가 승인할 수 있도록 컬렉션을 네임스페이스로 가져와야 합니다.

프로세스

1. 자동화 허브에 로그인합니다.
2. 탐색 패널에서 컬렉션 → 네임스페이스를 선택합니다. 네임스페이스 페이지에는 사용 가능한 모든 네임스페이스가 표시됩니다.
3. 컬렉션 보기를 클릭합니다.
4. **Upload Collection** 을 클릭합니다.
5. tarball 컬렉션으로 이동하여 파일을 선택한 다음 열기 를 클릭합니다.
6. 업로드를 클릭합니다.
   내 가져오기 화면에 테스트 요약이 표시되고 컬렉션 업로드 성공 또는 실패 여부를 알려줍니다.



참고

컬렉션이 승인되지 않으면 게시된 리포지토리에 표시되지 않습니다.

추가 리소스

- 컬렉션 및 리포지토리 승인에 대한 자세한 내용은 승인 파이프라인 을 참조하십시오.

# 3장. 프라이빗 자동화 허브에서 컨테이너 관리

**프라이빗 자동화 허브 컨테이너 레지스트리 및 리포지토리 구성을 위한 관리자 워크플로 및 프로세스에 대해 알아봅니다.**

## 3.1. 프라이빗 자동화 허브 컨테이너 레지스트리 관리

**자동화 허브 컨테이너 레지스트리를 사용하여 Ansible Automation Platform 인프라에서 컨테이너 이미지 리포지토리를 관리합니다. 자동화 허브를 사용하여 다음 작업을 수행할 수 있습니다.**

- **개별 컨테이너 리포지토리에 액세스할 수 있는 사용자 제어**
- **이미지의 태그 변경**
- **활동 및 이미지 계층 보기**
- **각 컨테이너 리포지토리와 관련된 추가 정보 제공**

### 3.1.1. 컨테이너 레지스트리

**자동화 허브 컨테이너 레지스트리는 컨테이너 이미지를 저장하고 관리하는 데 사용됩니다. 컨테이너 이미지를 빌드하거나 소싱한 경우 해당 컨테이너 이미지를 프라이빗 자동화 허브의 레지스트리 부분에 내보내 컨테이너 리포지토리를 생성할 수 있습니다.**

**다음 단계**

- **컨테이너 이미지를 자동화 허브 컨테이너 레지스트리로 내보냅니다.**
- **레지스트리의 컨테이너 리포지토리에 액세스할 수 있는 그룹을 생성합니다.**
- **컨테이너 리포지토리에 새 그룹을 추가합니다.**
- **컨테이너 리포지토리에 README를 추가하여 사용자에게 정보 및 관련 링크를 제공합니다.**

## 3.2. 프라이빗 자동화 허브에서 컨테이너 리포지토리에 대한 사용자 액세스 구성

**Ansible Automation Platform에서 이미지에 액세스하고 관리할 수 있는 사용자를 확인하려면 프라이빗 자동화 허브에서 컨테이너 리포지토리에 대한 사용자 액세스를 구성해야 합니다.**

### 3.2.1. 컨테이너 레지스트리 그룹 권한

**사용자가 프라이빗 자동화 허브에서 관리되는 컨테이너와 상호 작용하는 방법을 제어할 수 있습니다. 다음 권한 목록을 사용하여 컨테이너 레지스트리에 대한 올바른 권한으로 그룹을 생성합니다.**

**표 3.1. 프라이빗 자동화 허브에서 컨테이너를 관리하는 데 사용되는 그룹 권한 목록**

| 권한 이름 | 설명 |
|---|---|
| 새 컨테이너 만들기 | 사용자가 새 컨테이너를 만들 수 있음 |

| 권한 이름 | 설명 |
|---|---|
| 컨테이너 네임스페이스 권한 변경 | 사용자는 컨테이너 리포지토리에 대한 권한을 변경할 수 있습니다. |
| 컨테이너 변경 | 사용자는 컨테이너에 대한 정보를 변경할 수 있습니다. |
| 이미지 태그 변경 | 사용자가 이미지 태그를 수정할 수 있음 |
| 개인 컨테이너 가져오기 | 사용자는 개인 컨테이너에서 이미지를 가져올 수 있습니다. |
| 기존 컨테이너로 푸시 | 사용자는 기존 컨테이너에 이미지를 푸시할 수 있습니다. |
| 개인 컨테이너 보기 | 사용자는 비공개로 표시된 컨테이너를 볼 수 있습니다. |

### 3.2.2. 프라이빗 자동화 허브에서 새 그룹 생성

**사용자가 시스템의 지정된 기능에 액세스할 수 있는 프라이빗 자동화 허브의 그룹에 권한을 생성하고 할당할 수 있습니다. 기본적으로 자동화 허브 의 관리 그룹에는 모든 권한이 할당되어 있으며 초기 로그인 시 사용할 수 있습니다. 프라이빗 자동화 허브를 설치할 때 생성된 인증 정보를 사용합니다.**

**자세한 내용은 자동화 허브 시작하기 가이드 의 프라이빗 자동화 허브에서 새 그룹 생성을 참조하십시오.**

### 3.2.3. 그룹에 권한 할당

**기본적으로 새 그룹에는 할당된 권한이 없습니다. 사용자가 시스템의 특정 기능에 액세스할 수 있도록 개인 자동화 허브의 그룹에 권한을 할당할 수 있습니다.**

**그룹을 처음 만들거나 기존 그룹을 편집하여 권한을 추가하거나 제거할 때 권한을 추가할 수 있습니다.**

**자세한 내용은 자동화 허브 시작하기 가이드의 그룹에 권한 할당 을 참조하십시오.**

**추가 리소스**

- **특정 권한에 대한 자세한 내용은 컨테이너 레지스트리 그룹권한을 참조하십시오.**

### 3.2.4. 기존 그룹에 사용자 추가

**그룹을 생성할 때 그룹에 사용자를 추가할 수 있습니다. 그러나 기존 그룹에 사용자를 수동으로 추가할 수도 있습니다.**

**자세한 내용은 자동화 허브 시작하기 가이드에서 기존 그룹에 사용자 추가 를 참조하십시오.**

## 3.3. 프라이빗 자동화 허브 컨테이너 레지스트리 채우기

**기본적으로 프라이빗 자동화 허브에는 컨테이너 이미지가 포함되어 있지 않습니다. 컨테이너 레지스트리를 채우려면 컨테이너 이미지를 푸시해야 합니다.**

**프라이빗 자동화 허브 컨테이너 레지스트리를 채우려면 특정 워크플로우를 따라야 합니다.**

- Red Hat Ecosystem Catalog에서 이미지 가져오기(registry.redhat.io)
- 태그
- 프라이빗 자동화 허브 컨테이너 레지스트리로 푸시

중요

이미지 매니페스트 및 파일 시스템 Blob은 원래 **registry.redhat.io** 및 **registry.access.redhat.com** 에서 직접 제공되었습니다. 2023년 5월 1일부터 파일 시스템 Blob은 **quay.io** 에서 대신 제공됩니다.

- *Table 5.10에 나열된 네트워크 포트 및 프로토콜이 있는지 확인합니다. 실행 환경 (EE)* 을 사용하여 컨테이너 이미지를 가져오는 문제를 방지할 수 있습니다.

구체적으로 **registry.redhat.io** 또는 **registry.access.redhat.com** 에 대한 아웃 바운드 연결을 활성화하는 방화벽 구성을 변경합니다.

방화벽 규칙을 구성할 때 IP 주소 대신 호스트 이름을 사용합니다.

이 변경 후 **registry.redhat.io** 및 **registry.access.redhat.com** 에서 이미지를 계속 가져올 수 있습니다. **quay.io** 로그인이 필요하지 않거나 Red Hat 컨테이너 이미지를 계속 가져오려면 **quay.io** 레지스트리와 직접 상호 작용할 필요가 없습니다.

그러나 웹 기반 Red Hat 서브스크립션 관리에서 "서브스크립션 할당"이라고 하는 매니페스트는 한 가지 예외를 제외하고 2024년 초반부터 더 이상 지원되지 않습니다. 시스템이 폐쇄된 네트워크 또는 "air gapped" 시스템의 일부인 경우 Red Hat 서버에서 직접 업데이트를 받지 못하는 경우 Red Hat Satellite 6.16이 릴리스될 때까지 매니페스트가 지원됩니다. Red Hat Satellite 6.16의 릴리스 날짜 발표 날짜는 Red Hat Satellite 릴리스 날짜를 참조하십시오.

### 3.3.1. 자동화 허브에서 사용할 이미지 가져오기

컨테이너 이미지를 프라이빗 자동화 허브로 푸시하려면 먼저 기존 레지스트리에서 이미지를 가져와서 사용할 태그를 지정해야 합니다. 다음 예제에서는 Red Hat Ecosystem Catalog(registry.redhat.io)에서 이미지를 가져오는 방법을 자세히 설명합니다.

중요

2024년 초부터 Red Hat은 Red Hat 서브스크립션 관리 웹 플랫폼의 매니페스트 또는 매니페스트 목록을 더 이상 지원하지 않습니다. 이는 "서브스크립션 할당"과 동일한 방식으로 사용되었습니다. 또한 Red Hat은 하나의 예외로 Red Hat Satellite에서 대부분의 매니페스트 기능을 지원하지 않습니다. *종료된 네트워크의 Red Hat Satellite 사용자 또는 Red Hat 서버에서 직접 업데이트를 수신하지 않는 "공충된" 네트워크는 현재 Red Hat Satellite 6.16이 릴리스될 때까지 **access.redhat.com** 을 계속 사용할 수 있습니다.

새로운 Red Hat 계정은 서브스크립션 툴링에 Simple Content Access를 자동으로 사용합니다. Red Hat 서버에 연결할 수 있는 새로운 Red Hat 계정 및 기존 Satellite 고객은 **console.redhat.com** 에서 해당 매니페스트를 찾을 수 있습니다.

사전 요구 사항

- registry.redhat.io에서 이미지를 가져올 수 있는 권한이 있습니다.
- Simple Content Access가 활성화된 Red Hat 계정입니다.

프로세스

1. 컨테이너 이미지의 매니페스트에 액세스해야 하는 경우 Red Hat 콘솔에 로그인합니다.
2. 컨테이너 이미지에 필요한 매니페스트의 3 점 메뉴를 클릭하고 내보내기 매니페스트 를 클릭합니다.
3. registry.redhat.io 인증 정보를 사용하여 Podman에 로그인합니다.

```
$ podman login registry.redhat.io
```

4. 사용자 이름과 암호를 입력합니다.
5. 컨테이너 이미지를 가져옵니다.

```
$ podman pull registry.redhat.io/<container_image_name>:<tag>
```

검증

최근 가져온 이미지가 목록에 포함되어 있는지 확인하려면 다음 단계를 따르십시오.

1. 로컬 스토리지의 이미지를 나열합니다.

```
$ podman images
```

2. 이미지 이름을 확인하고 태그가 올바른지 확인합니다.

추가 리소스

- 이미지 등록 및 수신에 대한 정보는 Red Hat Ecosystem Catalog 도움말을 참조하십시오.
- Red Hat 서브스크립션 툴의 변경 사항에 대한 자세한 내용은 연결된 Satellite Server의 매니페스트 생성 및 관리를 참조하십시오.

### 3.3.2. 자동화 허브에서 사용할 이미지 태그

레지스트리에서 이미지를 가져온 후 프라이빗 자동화 허브 컨테이너 레지스트리에 사용하도록 태그를 지정합니다.

사전 요구 사항

- 외부 레지스트리에서 컨테이너 이미지를 가져왔습니다.
- 자동화 허브 인스턴스의 FQDN 또는 IP 주소가 있습니다.

프로세스

- 자동화 허브 컨테이너 리포지터리를 사용하여 로컬 이미지에 태그를 지정합니다.

```
$ podman tag registry.redhat.io/<container_image_name>:<tag>
<automation_hub_hostname>/<container_image_name>
```

검증

1. 로컬 스토리지의 이미지를 나열합니다.

```
$ podman images
```

2. 최근에 자동화 허브 정보로 태그한 이미지가 목록에 포함되어 있는지 확인합니다.

### 3.3.3. 프라이빗 자동화 허브로 컨테이너 이미지 푸시

태그된 컨테이너 이미지를 프라이빗 자동화 허브로 내보내 새 컨테이너를 생성하고 컨테이너 레지스트리를 채울 수 있습니다.

사전 요구 사항

- 새 컨테이너를 생성할 수 있는 권한이 있습니다.
- 자동화 허브 인스턴스의 FQDN 또는 IP 주소가 있습니다.

프로세스

1. 자동화 허브 위치 및 인증 정보를 사용하여 Podman에 로그인합니다.

```
$ podman login -u=<username> -p=<password> <automation_hub_url>
```

2. 컨테이너 이미지를 자동화 허브 컨테이너 레지스트리로 푸시합니다.

```
$ podman push <automation_hub_url>/<container_image_name>
```

문제 해결

푸시 작업에서는 업로드 중에 이미지 계층을 다시 압축하여 재현할 수 없으며 클라이언트에 따라 다릅니다. 이로 인해 이미지 계층 다이제스트 변경 및 실패한 푸시 작업으로 이어질 수 있으므로 오류: 이 이미지를 복사하려면 계층 표현이 필요하므로 (이미지가 서명되거나 대상이 다이제스트를 지정)할 수 없습니다.

검증

1. 자동화 허브에 로그인합니다.
2. 컨테이너 레지스트리로 이동합니다.
3. 컨테이너 리포지토리 목록에서 컨테이너를 찾습니다.

## 3.4. 컨테이너 리포지토리 설정

컨테이너 리포지토리를 설정할 때 설명을 추가하고 README를 포함하고 리포지토리에 액세스할 수 있는 그룹을 추가하고 이미지를 태그해야 합니다.

### 3.4.1. 컨테이너 레지스트리를 설정하기 위한 사전 요구 사항

- 프라이빗 자동화 허브에 로그인되어 있습니다.
- 리포지토리를 변경할 수 있는 권한이 있습니다.

### 3.4.2. 컨테이너 리포지토리에 README 추가

**컨테이너 리포지토리에 README를 추가하여 컨테이너 작업 방법에 대한 지침을 사용자에게 제공합니다. Automation Hub 컨테이너 리포지토리는 Markdown을 지원하여 README를 생성합니다. 기본적으로 README는 비어 있습니다.**

**사전 요구 사항**

- **컨테이너를 변경할 수 있는 권한이 있습니다.**

**프로세스**

1. **자동화 허브에 로그인합니다.**
2. **탐색 패널에서 실행 환경 실행 환경을선택합니다.**
3. **컨테이너 리포지토리를 선택합니다.**
4. **세부 정보 탭에서 추가 를 클릭합니다.**
5. **Raw Markdown 텍스트 필드에 Markdown에 README 텍스트를 입력합니다.**
6. **완료되면 저장을 클릭합니다.**

**README를 추가한 후 편집을 클릭하고 4단계와 5단계를 반복하여 언제든지 편집할 수 있습니다.**

### 3.4.3. 컨테이너 리포지토리에 대한 액세스 제공

**이미지를 사용해야 하는 사용자를 위해 컨테이너 리포지토리에 대한 액세스 권한을 제공합니다. 그룹을 추가하면 그룹이 컨테이너 리포지토리에 보유할 수 있는 권한을 수정할 수 있습니다. 이 옵션을 사용하여 그룹이 할당된 내용에 따라 권한을 확장하거나 제한할 수 있습니다.**

**사전 요구 사항**

- **컨테이너 네임스페이스 권한을 변경합니다.**

**프로세스**

1. **자동화 허브에 로그인합니다.**
2. **탐색 패널에서 실행 환경 실행 환경을선택합니다.**
3. **컨테이너 리포지토리를 선택합니다.**
4. **액세스 탭에서 그룹 선택을 클릭합니다.**
5. **액세스 권한을 부여할 그룹 또는 그룹을 선택하고 다음을 클릭합니다.**
6. **이 실행 환경에 추가할 역할을 선택하고 다음을 클릭합니다.**
7. **추가 를 클릭합니다.**

### 3.4.4. 컨테이너 이미지 태그

이미지를 태그하여 자동화 허브 컨테이너 리포지토리에 저장된 이미지에 추가 이름을 추가합니다. 이미지에 태그가 추가되지 않으면 자동화 허브의 기본값은 **latest** 입니다.

사전 요구 사항

- 이미지 태그 권한을 변경합니다.

프로세스

1. 탐색 패널에서 실행 환경 실행 환경을선택합니다.
2. 컨테이너 리포지토리를 선택합니다.
3. 이미지 탭을 클릭합니다.
4. **More Actions** 아이콘 Cryostat를 클릭하고 태그 관리를 클릭합니다.
5. 텍스트 필드에 새 태그를 추가하고 추가 를 클릭합니다.
6. 선택 사항: 해당 이미지의 태그에서 **x** 를 클릭하여 현재 태그를 제거합니다.
7. 저장을 클릭합니다.

검증

- 활동 탭을 클릭하고 최신 변경 사항을 검토합니다.

### 3.4.5. 자동화 컨트롤러에서 인증 정보 생성

암호 또는 토큰 보호 레지스트리에서 컨테이너 이미지를 가져오려면 자동화 컨트롤러에 인증 정보를 생성해야 합니다.

이전 버전의 Ansible Automation Platform에서는 실행 환경 이미지를 저장하기 위해 레지스트리를 배포해야 했습니다. Ansible Automation Platform 2.0 이상에서는 이미 컨테이너 레지스트리가 실행 중인 것처럼 시스템이 작동합니다. 실행 환경 이미지를 저장하려면 선택한 컨테이너 레지스트리의 인증 정보만 추가합니다.

프로세스

1. 자동화 컨트롤러로 이동합니다.
2. 탐색 패널에서 리소스 자격증명을 선택합니다.
3. 추가 를 클릭하여 새 인증 정보를 생성합니다.
4. 권한 부여 이름, 설명 및 조직을 입력합니다.
5. 인증 정보 유형을 선택합니다.
6. 인증 URL 을 입력합니다. 이는 컨테이너 레지스트리 주소입니다.
7. 컨테이너 레지스트리에 로그인하는 데 필요한 사용자 이름 및 암호 또는 토큰을 입력합니다.
8. 선택 사항: SSL 확인을 활성화하려면 SSL 확인을 선택합니다.
9. 저장을 클릭합니다.

## 3.5. 컨테이너 리포지토리에서 이미지 가져오기

자동화 허브 컨테이너 레지스트리에서 이미지를 가져와 로컬 머신에 복사합니다. Automation Hub는 컨테이너 리포지토리의 각 최신 이미지에 대해 **podman pull** 명령을 제공합니다. 이 명령을 터미널에 복사하여 붙여넣거나 **podman pull** 을 사용하여 이미지 태그를 기반으로 이미지를 복사할 수 있습니다.

### 3.5.1. 이미지 가져오기

자동화 허브 컨테이너 레지스트리에서 이미지를 가져와 로컬 머신에 복사할 수 있습니다.

사전 요구 사항

- 개인 컨테이너 리포지토리에서 보고 가져올 수 있는 권한이 있어야 합니다.

프로세스

1. 암호 또는 토큰 보호 레지스트리에서 컨테이너 이미지를 가져오는 경우 이미지를 가져오기 전에 자동화 컨트롤러에 인증 정보를 생성합니다.
2. 탐색 패널에서 실행 환경 실행 환경을선택합니다.
3. 컨테이너 리포지토리를 선택합니다.
4. 이 이미지 가져오기 항목에서 클립보드에 복사를 클릭합니다.
5. 터미널에서 명령을 붙여 넣습니다.

검증

- **podman** 이미지를 실행하여 로컬 머신의 이미지를 확인합니다.

### 3.5.2. 컨테이너 리포지토리에서 이미지 동기화

자동화 허브 컨테이너 레지스트리에서 이미지를 가져와서 이미지를 로컬 머신에 동기화할 수 있습니다. 원격 컨테이너 레지스트리에서 이미지를 동기화하려면 먼저 원격 레지스트리를 구성해야 합니다.

사전 요구 사항

개인 컨테이너 리포지토리에서 보고 가져올 수 있는 권한이 있어야 합니다.

프로세스

1. 탐색 패널에서 실행 환경 실행 환경을선택합니다.
2. 레지스트리에 https://registry.redhat.io 를 추가합니다.
3. 인증에 필요한 인증 정보를 추가합니다.

참고

일부 컨테이너 레지스트리는 속도 제한으로 공격적입니다. Advanced Options 에서 유량 제한을 설정합니다.

4. 탐색 패널에서 실행 환경 실행 환경을선택합니다.

5. 페이지 헤더에서 실행 환경 추가 를 클릭합니다.

6. 가져올 레지스트리를 선택합니다. 이름 필드에는 로컬 레지스트리에 표시되는 이미지의 이름이 표시됩니다.

참고

Upstream 이름 필드는 원격 서버의 이미지 이름입니다. 예를 들어 업스트림 이름이 "alpine"로 설정되고 Name 필드가 "local/alpine"인 경우 alpine 이미지가 원격에서 다운로드되고 "local/alpine"로 이름이 변경됩니다.

7. 포함하거나 제외할 태그 목록을 설정합니다. 많은 수의 태그와 이미지를 동기화하는 것은 시간이 많이 소요되며 많은 디스크 공간을 사용합니다.

추가 리소스

- 레지스트리 목록은 Red Hat Container Registry Authentication을 참조하십시오.
- 이미지를 가져올 때 사용할 옵션은 What is Podman? 문서를 참조하십시오.

## 3.6. 서명된 컨테이너 작업

자동화 실행 환경은 Ansible 자동화 컨트롤러에서 작업을 실행하는 데 사용하는 컨테이너 이미지입니다. 이 콘텐츠를 프라이빗 자동화 허브로 다운로드하여 조직 내에 게시할 수 있습니다.

### 3.6.1. 컨테이너 서명을 위해 시스템 배포

Automation Hub는 이미지 서명을 구현하여 실행 환경 컨테이너 이미지에 대한 보안을 개선합니다.

컨테이너 서명이 준비되도록 시스템을 배포하려면 서명 스크립트를 생성합니다.

참고

설치 프로그램은 설치 프로그램이 있는 동일한 서버에서 스크립트와 키를 찾습니다.

프로세스

1. 터미널에서 서명 스크립트를 생성하고 설치 프로그램 매개 변수로 스크립트 경로를 전달합니다. 예:

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

# pulp_container SigningService will pass the next 4 variables to the script.
MANIFEST_PATH=$1
FINGERPRINT="$PULP_SIGNING_KEY_FINGERPRINT"
IMAGE_REFERENCE="$REFERENCE"
SIGNATURE_PATH="$SIG_PATH"

# Create container signature using skopeo
skopeo standalone-sign \
  $MANIFEST_PATH \
  $IMAGE_REFERENCE \
  $FINGERPRINT \
```

```
  --output $SIGNATURE_PATH

# Optionally pass the passphrase to the key if password protected.
# --passphrase-file /path/to/key_password.txt

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

2. **automationhub_*** 로 시작하는 컨테이너 서명 옵션을 보려면 Ansible Automation Platform 설치 프로그램 인벤토리 파일을 검토하십시오.

```
[all:vars]
.
.
.

automationhub_create_default_container_signing_service = True
automationhub_container_signing_service_key = /absolute/path/to/key/to/sign
automationhub_container_signing_service_script = /absolute/path/to/script/that/signs
```

3. 설치가 완료되면 자동화 허브로 이동합니다.
4. 탐색 패널에서 서명 키를 선택합니다.
5. container-default 또는 컨테이너-*anyname* 이라는 키가 있는지 확인합니다.

참고

**container-default** 서비스는 Ansible Automation Platform 설치 프로그램에서 생성합니다.

### 3.6.2. 자동화 허브에 원격으로 컨테이너 추가

다음 두 가지 방법 중 하나로 자동화 허브에 원격으로 컨테이너를 추가할 수 있습니다.

- 원격 생성
- 실행 환경

프로세스

1. 자동화 허브에 로그인합니다.
2. 탐색 패널에서 실행 환경 원격 레지스트리 를 선택합니다.
3. 원격 레지스트리 추가를 클릭합니다.
   - 이름 필드에 컨테이너가 있는 레지스트리의 이름을 입력합니다.
   - URL 필드에 컨테이너가 있는 레지스트리의 URL을 입력합니다.

- 필요한 경우 Username 필드에 사용자 이름을 입력합니다.
- 필요한 경우 암호 필드에 암호를 입력합니다.
- 저장을 클릭합니다.

### 3.6.3. 실행 환경 추가

자동화 실행 환경은 시스템 수준의 종속성 및 컬렉션 기반 콘텐츠를 통합할 수 있는 컨테이너 이미지입니다. 각 실행 환경을 사용하면 작업을 실행할 수 있는 사용자 지정 이미지를 사용할 수 있으며, 각 실행 환경에는 작업을 실행할 때 필요한 항목만 포함됩니다.

프로세스

1. 탐색 패널에서 실행 환경 실행 환경을선택합니다.
2. 실행 환경 추가를 클릭합니다.
3. 실행 환경의 이름을 입력합니다.
4. 선택 사항: 업스트림 이름을 입력합니다.
5. 레지스트리 의 드롭다운 메뉴에서 레지스트리 이름을 선택합니다.
6. Add tag(s) to include 필드에 태그를 입력합니다. 필드가 비어 있으면 모든 태그가 전달됩니다. 전달할 리포지토리별 태그를 지정해야 합니다.
7. 나머지 필드는 선택 사항입니다.
   - 현재 포함된 태그
   - 제외할 태그 추가
   - 현재 제외된 태그
   - description
8. 저장을 클릭합니다.
9. 이미지를 동기화합니다.

### 3.6.4. 로컬 환경에서 컨테이너 이미지 푸시

다음 절차에 따라 로컬 시스템의 이미지에 서명하고 서명된 이미지를 자동화 허브 레지스트리로 푸시합니다.

프로세스

1. 터미널에서 Podman 또는 현재 사용 중인 컨테이너 클라이언트에 로그인합니다.

```
> podman pull <container-name>
```

2. 이미지를 가져온 후 태그를 추가합니다(예: latest, rc, beta 또는 버전 번호(예: 1.0; 2.3 등):

```
> podman tag <container-name> <server-address>/<container-name>:<tag name>
```

3. 변경 사항이 적용된 후 이미지에 서명하고 자동화 허브 레지스트리로 다시 푸시합니다.

```
> podman push <server-address>/<container-name>:<tag name> --tls-verify=false --sign-by
<reference to the gpg key on your local>
```

이미지에 서명되지 않은 경우 현재 서명을 포함하는 경우에만 푸시할 수 있습니다. 또는 다음 스크립트를 사용하여 서명하지 않고 이미지를 내보낼 수 있습니다.

```
> podman push <server-address>/<container-name>:<tag name> --tls-verify=false
```

4. 이미지를 푸시한 후 자동화 허브로 이동합니다.
5. 탐색 패널에서 실행 환경 실행 환경을선택합니다.
6. 새 실행 환경을 표시하려면 새로 고침 아이콘을 클릭합니다.
7. 내보낸 이미지를 보려면 이미지의 이름을 클릭합니다.

문제 해결

자동화 허브의 세부 정보 페이지는 이미지에 서명되었는지 여부를 나타냅니다. 세부 정보 페이지에 이미지가 Unsigned 임을 나타내는 경우 다음 단계를 사용하여 자동화 허브의 이미지에 서명할 수 있습니다.

1. 이미지 이름을 클릭하여 세부 정보 페이지로 이동합니다.
2. **More Actions** 아이콘 Cryostat를클릭합니다. 세 가지 옵션을 사용할 수 있습니다.
   - 컨트롤러에서 사용
   - delete
   - 서명
3. 드롭다운 메뉴에서 Sign 을 클릭합니다.

서명 서비스는 이미지에 서명합니다. 이미지에 서명되면 상태가 "signed"로 변경됩니다.

### 3.6.5. 서명된 이미지가 있는 정책

podman 또는 기타 이미지 클라이언트에서 해당 서명에 특정 정책을 할당하여 이미지의 유효성을 보장하기 위해 정책을 사용할 수 있습니다.

### 3.6.6. podman을 사용하여 특정 서명으로 이미지에 서명되었는지 확인

서명이 특정 서명으로 서명되었는지 확인하는 경우 서명이 로컬 환경에 있어야 합니다.

프로세스

1. 탐색 패널에서 서명 키를 선택합니다.
2. 사용 중인 서명 옆에 있는 **More Actions** 아이콘을 클릭합니다.
3. 드롭다운 메뉴에서 다운로드 키를 선택합니다. 새 창이 열립니다.
4. 이름 필드에 키 이름을 입력합니다.

5. 저장을 클릭합니다.

### 3.6.7. 서명을 확인하도록 클라이언트 구성

원격 레지스트리에서 가져온 컨테이너 이미지가 올바르게 서명되었는지 확인하려면 먼저 정책 파일에서 적절한 공개 키를 사용하여 이미지를 구성해야 합니다.

사전 요구 사항

- 클라이언트에는 서명을 확인하도록 sudo 권한이 구성되어 있어야 합니다.

프로세스

1. 터미널을 열고 다음 명령을 사용합니다.

```
> sudo <name of editor> /etc/containers/policy.json
```

표시되는 파일은 다음과 유사합니다.

```
{
  "default": [{"type": "reject"}],
  "transports": {
   "docker": {
     "quay.io": [{"type": "insecureAcceptAnything"}],
     "docker.io": [{"type": "insecureAcceptAnything"}],
     "<server-address>": [
      {
             "type": "signedBy",
             "keyType": "GPGKeys",
             "keyPath": "/tmp/containersig.txt"
      }]
   }
  }
}
```

이 파일은 **quay.io** 또는 **docker.io** 가 모두 확인을 수행하지 않음을 보여줍니다. 유형은거부 의 기본 유형을 재정의하는 **insecureAcceptAnything** 이기 때문입니다. 그러나 매개변수유형은 **"signedBy"** 로 설정되어 있으므로 <***server-address*** >는 확인을 수행합니다.

참고

현재 지원되는 유일한 **keyType** 은 GPG 키입니다.

2. &lt ***;server-address*** > 항목에서 키 파일의 이름을 포함하도록**keyPath** <1>를 수정합니다.

```
{
    "default": [{"type": "reject"}],
    "transports": {
        "docker": {
            "quay.io": [{"type": "insecureAcceptAnything"}],
            "docker.io": [{"type": "insecureAcceptAnything"}],
            "<server-address>": [{
                "type": "signedBy",
                "keyType": "GPGKeys",
```

```
                "keyPath": "/tmp/<key file name>",
                "signedIdentity": {
                    "type": "matchExact"
                }
            }]
        }
    }
}
```

3. 파일을 저장하고 닫습니다.

검증

- Podman을 사용하여 파일을 가져오거나 선택한 클라이언트를 가져옵니다.

```
> podman pull <server-address>/<container-name>:<tag name> --tls-verify=false
```

이 응답은 이미지가 오류 없이 서명되었는지 확인합니다. 이미지에 서명되지 않은 경우 명령이 실패합니다.

추가 리소스

- policy.json에 대한 자세한 내용은 containers-policy.json 설명서 를 참조하십시오.

## 3.7. 컨테이너 리포지토리 삭제

프라이빗 자동화 허브에서 컨테이너 리포지토리를 삭제하여 디스크 공간을 관리합니다. 컨테이너 리포지토리 목록 보기의 Red Hat Ansible Automation Platform 인터페이스에서 리포지토리를 삭제할 수 있습니다.

사전 요구 사항

- 리포지토리를 관리할 수 있는 권한이 있습니다.

프로세스

1. 자동화 허브로 이동합니다.
2. 탐색 패널에서 실행 환경 실행 환경을선택합니다.
3. 삭제하려는 컨테이너 리포지토리에서 **More Actions** (추가 작업) 아이콘을 클릭하고 삭제 를 클릭합니다.
4. 확인 메시지가 표시되면 확인란을 클릭하고 삭제 를 클릭합니다.

검증

- 실행 환경 목록 보기로 돌아갑니다. 컨테이너 리포지토리가 성공적으로 삭제되면 컨테이너 리포지토리가 더 이상 목록에 없습니다.