Red Hat Ansible Automation Platform 2.4

Ansible Automation Platform에 대한 중앙 인증 설치 및 구성

Ansible Automation Platform의 중앙 인증 기능 활성화

Last Updated: 2024-06-13

Red Hat Ansible Automation Platform 2.4 Ansible Automation Platform에 대한 중앙 인증 설치 및 구성

Ansible Automation Platform의 중앙 인증 기능 활성화

법적 공지

초록

이 가이드에서는 플랫폼 관리자에게 Ansible Automation Platform에서 중앙 인증을 활성화하고 구성하는 데 필요한 정보 및 절차를 제공합니다.

차례

머리말

Ansible Automation Platform Central Authentication은 타사 ID 공급자(idP) 솔루션이므로 Ansible Automation Platform에서 사용할 수 있는 간단한 Single Sign-On 솔루션을 사용할 수 있습니다. 플랫폼 관리자는 중앙 인증을 사용하여 연결 및 인증을 테스트하고 새 사용자를 온보딩하고 그룹에 할당하여 사용자 권한을 관리할 수 있습니다. OpenID Connect 기반 및 LDAP 지원과 함께 중앙 인증은 고객 사용 부트스트랩에 사용할 수 있는 지원되는 REST API도 제공합니다.

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 **docs-product** 구성 요소를 사용하여 Ansible Automation Platform Jira 프로젝트에 문제를 생성하십시오.

1장. 자동화 허브를 위한 ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION

자동화 허브에 대한 Ansible Automation Platform 중앙 인증을 활성화하려면 Red Hat Ansible Automation Platform 설치 프로그램을 다운로드하여 시작한 다음 이 가이드에 설명된 대로 필요한 설정 절차를 진행합니다.

중요

이 가이드의 설치 프로그램은 기본 독립 실행형 배포에 대한 중앙 인증을 설치합니다. 독립 실행형 모드는 하나의 중앙 인증 서버 인스턴스만 실행하므로 클러스터형 배포에는 사용할 수 없습니다. 독립 실행형 모드는 중앙 인증의 기능을 사용하여 드라이브를 테스트하고 플레이하는 데 유용할 수 있지만 단일 장애 지점만 있으므로 프로덕션에서 독립 실행형 모드를 사용하는 것은 권장되지 않습니다.

중앙 인증을 다른 배포 모드로 설치하려면 자세한 배포 옵션은 이 가이드를 참조하십시오.

1.1. 시스템 요구 사항

Ansible Automation Platform Central 인증을 설치하고 실행하려면 몇 가지 최소 요구 사항이 있습니다.

- Java를 실행하는 모든 운영 체제
- Java 8 JDK
- zip 또는 gzip 및 tar
- 최소 512MB의 RAM
- 최소 1GB의 디스크 공간
- 클러스터에서 중앙 인증을 실행하려는 경우 PostgreSQL, MySQL, Oracle 등과 같은 공유 외부 데이터베이스입니다. 자세한 내용은 *Red Hat Single Sign-On 서버 설치 및 구성 가이드의 데이터베이스 구성섹션을* 참조하십시오.
- 클러스터에서 실행하려는 경우 머신에서 네트워크 멀티 캐스트를 지원합니다. 멀티 캐스트 없이 중앙 인증을 클러스터링할 수 있지만 이 경우 일부 구성을 변경해야 합니다. 자세한 내용은 *Red Hat Single Sign-On 서버 설치 및 구성 가이드의* Cryostat *섹션을* 참조하십시오.
- Linux에서는 **/dev/urandom** 을 보안 정책에서 **/dev/random** 사용을 요구하지 않는 한 사용 가능한 엔트로피 부족으로 인해 중앙 인증이 중단되는 것을 방지하기 위해 임의의 데이터 소스로 /dev/urandom을 사용하는 것이 좋습니다. Oracle JDK 8 및 OpenJDK 8에서 시작 시 **java.security.egd** 시스템 속성을 **file:/dev/urandom** 로 설정합니다.

1.2. 자동화 허브와 함께 사용할 ANSIBLE AUTOMATION PLATFORM 중앙 인증 설치

Ansible Automation Platform 중앙 인증 설치는 Red Hat Ansible Automation Platform 설치 프로그램에 포함됩니다. 다음 절차를 사용하여 Ansible Automation Platform을 설치한 다음 Ansible Automation Platform 및 중앙 인증 모두를 성공적으로 설치하도록 인벤토리 파일에 필요한 매개변수를 구성합니다.

1.2.1. Red Hat Ansible Automation Platform 설치 프로그램 선택 및 가져오기

Red Hat Enterprise Linux 환경 인터넷 연결을 기반으로 필요한 Red Hat Ansible Automation Platform 설치 프로그램을 선택합니다. 다음 시나리오를 검토하고 요구 사항을 충족하는 Red Hat Ansible Automation Platform 설치 프로그램을 결정합니다.

참고

Red Hat 고객 포털에서 Red Hat Ansible Automation Platform 설치 프로그램에 액세스하려면 유효한 Red Hat 고객 계정이 필요합니다.

인터넷 액세스로 설치

Red Hat Enterprise Linux 환경이 인터넷에 연결된 경우 Red Hat Ansible Automation Platform 설치 프로그램을 선택합니다. 인터넷 액세스를 사용하여 설치하면 최신 필수 리포지토리, 패키지 및 종속 항목을 검색합니다. 다음 방법 중 하나를 선택하여 Ansible Automation Platform 설치 프로그램을 설정합니다.

Tarball 설치

1. Red Hat Ansible Automation Platform 다운로드 페이지로 이동합니다.
2. **Ansible Automation Platform <latest-version> 설정에 대해지금 다운로드를 클릭합니다.**
3. 파일을 추출합니다.

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

rpm install

1. Ansible Automation Platform 설치 프로그램 패키지 설치
   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
```

참고

dnf install 은 리포지토리가 기본적으로 비활성화되어 있으므로 리포지토리를 활성화합니다.

RPM 설치 프로그램을 사용하면 파일이 **/opt/ansible-automation-platform/installer** 디렉터리에 배치됩니다.

인터넷 액세스없이 설치

인터넷에 액세스할 수 없거나 온라인 리포지토리와 별도의 구성 요소 및 종속 항목을 설치하지 않으려는 경우 Red Hat Ansible Automation Platform **Bundle** 설치 관리자를 사용합니다. Red Hat Enterprise Linux 리포지토리에 대한 액세스는 여전히 필요합니다. 다른 모든 종속 항목은 tar 아카이브에 포함되어 있습니다.

1. Red Hat Ansible Automation Platform 다운로드 페이지로 이동합니다.

2. Ansible Automation Platform <latest-version> Setup Bundle에 대해 **지금 다운로드를** 클릭합니다.

3. 파일을 추출합니다.

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

1.2.2. Red Hat Ansible Automation Platform 설치 프로그램 구성

설치 프로그램을 실행하기 전에 설치 프로그램 패키지에 있는 인벤토리 파일을 편집하여 자동화 허브 및 Ansible Automation Platform 중앙 인증 설치를 구성합니다.

참고

[automationhub] 호스트에 연결할 수 있는 IP 주소를 제공하여 사용자가 다른 노드에서 프라이빗 Automation Hub에서 콘텐츠를 동기화하고 새 이미지를 컨테이너 레지스트리에 푸시할 수 있도록 합니다.

1. 설치 프로그램 디렉터리로 이동합니다.

   a. 온라인 설치 프로그램:

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

   b. 번들 설치:

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

2. 텍스트 편집기를 사용하여 **인벤토리** 파일을 엽니다.

3. **[automationhub]** 아래의 인벤토리 파일 매개변수를 편집하여 자동화 허브 호스트 설치를 지정합니다.

   a. 자동화 허브 위치에 IP 주소 또는 FQDN을 사용하여 **[automationhub]** 아래에 그룹 호스트 정보를 추가합니다.

   b. Automation **hub_admin_password**,**automationhub_pg_password**, 설치 사양에 따라 추가 매개변수를 입력합니다.

4. **sso_keystore_password** 필드에 암호를 입력합니다.

5. **[SSO]** 아래의 인벤토리 파일 매개변수를 편집하여 중앙 인증을 설치할 호스트를 지정합니다.

   a. **sso_console_admin_password** 필드에 암호를 입력하고 설치 사양에 따라 추가 매개변수를 입력합니다.

1.2.3. Red Hat Ansible Automation Platform 설치 프로그램 실행

인벤토리 파일이 업데이트되면 설치 프로그램 패키지에 있는 **setup.sh** 플레이북을 사용하여 설치 프로그램을 실행합니다.

1. **setup.sh** 플레이북을 실행합니다.

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

1.2.4. 중앙 인증 관리자로 로그인

Red Hat Ansible Automation Platform을 설치하면 인벤토리 파일에서 지정한 admin 자격 증명을 사용하여 중앙 인증 서버에 admin 사용자로 로그인합니다.

1. Ansible Automation Platform Central Authentication 인스턴스로 이동합니다.
2. **sso_console_admin_username** 및 sso_console_ **admin_password 필드에서** 인벤토리 파일에 지정한 관리자 인증 정보를 사용하여 로그인합니다.

Ansible Automation Platform Central Authentication이 성공적으로 설치되고 admin 사용자가 로그인한 상태에서 다음 절차를 사용하여 사용자 스토리지 공급자(예: LDAP)를 추가하여 진행할 수 있습니다.

2장. ANSIBLE AUTOMATION PLATFORM CENTRAL 인증에 사용자 스토리지 공급자(LDAP/KERBEROS) 추가

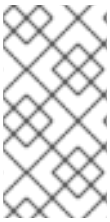
Ansible Automation Platform Central 인증은 기본 제공 LDAP/AD 공급자와 함께 제공됩니다. LDAP 데이터베이스에서 사용자 속성을 가져올 수 있도록 LDAP 공급자를 중앙 인증에 추가할 수 있습니다.

사전 요구 사항

- SSO 관리자로 로그인되어 있습니다.

절차

1. Ansible Automation Platform 중앙 인증에 SSO 관리자로 로그인합니다.
2. 탐색 패널에서 **Configure section → User Federation** 을 선택합니다.



참고

RH-SSO에서 LDAP 사용자 페더를 사용하는 경우 ID 공급자(IDP) 그룹을 SAML 인증에 노출하려면 클라이언트 구성인 ansible-automation-platform에 그룹 매퍼를 추가해야 합니다. SAML 어설션 매퍼에 대한 자세한 내용은 OIDC 토큰 및 SAML Assertion Mappings 를 참조하십시오.

1. **Add provider** 목록에서 LDAP 공급자를 선택하여 LDAP 구성 페이지로 이동합니다.

다음 표에는 LDAP 구성에 사용 가능한 옵션이 나열되어 있습니다.

구성 옵션	설명
스토리지 모드	사용자를 중앙 인증 사용자 데이터베이스로 가져오려면 **On** 으로 설정합니다. 자세한내용은 스토리지 모드를 참조하십시오.
편집 모드	관리자가 사용자 메타데이터에 대해 수행할 수 있는 수정 유형을 결정합니다. 자세한 내용은 편집 모드를 참조하십시오.
콘솔 표시 이름	관리자 콘솔에서 이 공급자를 참조할 때 사용되는 이름
우선 순위	사용자를 조회하거나 사용자를 추가할 때 이 공급자의 우선 순위
동기화 등록	관리 콘솔에서 Ansible Automation Platform Central Authentication에서 생성한 새 사용자를 활성화하거나 등록 페이지를 LDAP에 추가하려는 경우 활성화
Kerberos 인증 허용	LDAP에서 프로비저닝된 사용자 데이터를 사용하여 영역에서 Kerberos/SPNEGO 인증을 활성화합니다. 자세한 내용은 Kerberos 를 참조하십시오.

3장. 자동화 허브 관리자 권한 할당

Hub 관리 사용자에게는 사용자 권한 및 그룹을 관리하려면 *hubadmin* 의 역할이 할당되어야 합니다. Ansible Automation Platform Central Authentication 클라이언트를 통해 *hubadmin* 의 역할을 사용자에게 할당할 수 있습니다.

사전 요구 사항

- 사용자 스토리지 공급자(예: LDAP)가 중앙 인증에 추가되었습니다.

절차

1. SSO 클라이언트의 **ansible-automation-platform** 영역으로 이동합니다.
2. 탐색 패널에서 **사용자 액세스 → 사용자를** 선택합니다.
3. ID를 클릭하여 목록에서 사용자를 선택합니다.
4. **역할 매핑 탭을** 클릭합니다.
5. **클라이언트 역할** 목록에서 **automation-hub** 를 선택합니다.
6. **사용 가능한 역할** 필드에서 **hubadmin** 을 클릭한 다음 **Add selected > 을 클릭합니다**.

사용자는 이제 *hubadmin* 입니다. 3-6단계를 반복하여 *hubadmin* 역할을 추가 사용자에게 할당합니다.

4장. ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION에 ID 브로커 추가

Ansible Automation Platform Central 인증은 소셜 및 프로토콜 기반 공급자를 모두 지원합니다. 영역에 대한 소셜 인증을 사용하도록 중앙 인증에 ID 브로커를 추가하여 사용자가 Google, Facebook, GitHub 등과 같은 기존 소셜 네트워크 계정을 사용하여 로그인할 수 있습니다.

참고

지원되는 소셜 네트워크 목록과 이를 활성화하는 자세한 내용은 이 섹션을 참조하십시오.

프로토콜 기반 공급자는 사용자를 인증하고 권한을 부여하기 위해 특정 프로토콜에 의존하는 공급자입니다. 이를 통해 특정 프로토콜을 준수하는 모든 ID 공급자에 연결할 수 있습니다. Ansible Automation Platform Central 인증은 SAML v2.0 및 OpenID Connect v1.0 프로토콜을 지원합니다.

절차

1. Ansible Automation Platform Central Authenticationas에 admin 사용자로 로그인합니다.
2. 사이드 탐색 모음의 **Configure** (구성) 섹션에서 **Identity Providers** (ID 공급자)를 클릭합니다.
3. **공급자 추가** 목록에서 ID 공급자를 선택하여 ID 공급자 구성 페이지로 이동합니다.

다음 표에는 ID 공급자 구성에 사용할 수 있는 옵션이 나열되어 있습니다.

표 4.1. ID 브로커 구성 옵션

구성 옵션	설명
별칭	별칭은 ID 공급자의 고유 식별자입니다. 내부적으로 ID 공급자를 참조하는 데 사용됩니다. **OpenID Connect** 와 같은 일부 프로토콜은 ID 공급자와 통신하기 위해 리디렉션 URI 또는 콜백 URL이 필요합니다. 이 경우 별칭은 리디렉션 URL을 빌드하는 데 사용됩니다.
enabled	공급자를 켜거나 끄십시오.
로그인 페이지에서 숨기기	활성화하면 이 공급자가 로그인 페이지에 로그인 옵션으로 표시되지 않습니다. 클라이언트는 로그인을 요청하는 데 사용하는 URL에서 **kc_idp_hint** 매개변수를 사용하여 이 공급자를 계속 사용하도록 요청할 수 있습니다.
계정 연결만 해당	활성화하면 이 공급자를 사용하여 사용자를 로그인할 수 없으며 로그인 페이지에 옵션으로 표시되지 않습니다. 기존 계정을 이 공급자와 계속 연결할 수 있습니다.
저장소 토큰	ID 공급자로부터 수신된 토큰을 저장할지 여부입니다.
저장된 토큰을 읽을 수 있음	사용자가 저장된 ID 공급자 토큰을 검색할 수 있는지 여부입니다. 이는 브로커 클라이언트 수준 역할 읽기 토큰에도 적용됩니다.

신뢰 이메일	ID 공급자가 제공한 이메일 주소를 신뢰할 수 있는지 여부입니다. 영역에 이메일 유효성 검사가 필요한 경우 이 IDP에서 로그인하는 사용자는 이메일 확인 프로세스를 거치지 않아도 됩니다.
GUI 순서	사용 가능한 IDP가 로그인 페이지에 나열된 방식을 정렬하는 순서 번호입니다.
첫 번째 로그인 흐름	이 IDP를 통해 중앙 인증에 로그인하는 사용자에 대해 트리거될 인증 흐름을 선택합니다.
로그인 흐름 게시	사용자가 외부 ID 공급자로 로그인을 완료한 후 트리거되는 인증 흐름을 선택합니다.

4.1. ANSIBLE AUTOMATION PLATFORM CENTRAL 인증을 사용하여 그룹 권한 관리

특정 권한을 역할로 그룹화한 다음 해당 역할을 그룹에 할당하여 Ansible Automation Platform에서 사용자 액세스를 관리할 수 있습니다. Ansible Automation Platform에 처음 로그인하면 **사용자**, **그룹**, 역할이 자동화 허브의 사용자 액세스 페이지에 표시되면 각 그룹에 사용자 액세스 및 역할을 할당할 수 있습니다.

자동화 허브에는 발생할 수 있는 사용 사례와 호환되는 관리 역할 세트가 포함되어 있습니다. 고유한 관리 역할 세트를 생성하거나 사용자 액세스 페이지의 역할 섹션에 있는 사전 정의된 역할을 사용할 수 있습니다.

4.1.1. 역할로 권한 그룹화

시스템의 기능에 대한 특정 사용자 액세스 권한을 사용하여 역할로 권한을 그룹화할 수 있습니다.

사전 요구 사항

- **hubadmin 사용자로 로그인했습니다.**

절차

1. **프라이빗 자동화 허브에 로그인합니다.**
2. **User Access 드롭다운 메뉴로 이동합니다.**
3. **역할을 클릭합니다.**
4. **역할 추가를 클릭합니다.**
5. **이름 필드에 역할 이름을 입력합니다.**
6. **Description (설명) 필드에 역할 설명을 입력합니다.**
7. **각 권한 유형 옆에 있는 드롭다운 메뉴를 클릭하고 역할에 적절한 권한을 선택합니다.**

8. 저장을 클릭합니다.

특정 권한으로 새 역할을 생성했습니다. 이제 이 역할을 그룹에 할당할 수 있습니다.

4.1.1.1. 그룹에 역할 할당

그룹에 역할을 할당하여 그룹 메뉴와 네임스페이스 메뉴에서 시스템의 특정 기능에 액세스할 수 있습니다. 그룹 메뉴에서 그룹에 할당된 역할에는 전역 범위가 있습니다. 예를 들어 사용자에게 네임스페이스 소유자 역할이 할당되면 해당 권한이 모든 네임스페이스에 적용됩니다. 그러나 *네임스페이스* 메뉴에서 그룹에 할당된 역할은 사용자에게 특정 오브젝트 인스턴스에 대한 액세스 권한만 부여합니다.

사전 요구 사항

- **hubadmin** 사용자로 로그인했습니다.

절차

그룹 메뉴에서 역할 할당.

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 사용자 액세스 → 그룹을 선택합니다.
3. 표시된 그룹 목록에서 그룹을 선택합니다.
4. 역할 추가를 클릭합니다.
5. 추가할 역할 옆에 있는 확인란을 클릭합니다.
6. 다음을 클릭하여 그룹에 적용할 역할을 미리 봅니다.
7. **Add** 를 클릭하여 선택한 역할을 그룹에 적용합니다.

참고

뒤로 를 클릭하여 역할 메뉴로 돌아가거나취소 를 클릭하여 이전 페이지로 돌아갑니다.

절차

네임스페이스 메뉴에서 역할 할당.

1. 프라이빗 자동화 허브에 로그인합니다.
2. 탐색 패널에서 컬렉션 → 네임스페이스를 선택합니다.
3. 내 네임스페이스 탭을 클릭하고 네임스페이스를 선택합니다.
4. 편집하려면 액세스 탭을 클릭합니다.

사용자는 할당된 권한과 연결된 자동화 허브의 기능에 액세스할 수 있습니다.

4.1.2. 자동화 허브 권한

권한은 각 그룹이 지정된 오브젝트에서 수행할 수 있는 정의된 작업 세트를 제공합니다. 이 표에 설명된 권한에 따라 그룹에 필요한 액세스 수준을 결정합니다.

표 4.2. 권한 참조 표

개체	권한	설명
컬렉션 네임스페이스	네임스페이스 추가 네임스페이스에 업로드 네임스페이스 변경 네임스페이스 삭제	이러한 권한이 있는 그룹은 네임스페이스를 생성, 업로드 및 삭제할 수 있습니다.
컬렉션	Ansible 리포지토리 콘텐츠 수정 컬렉션 삭제	이 권한이 있는 그룹은 다음 작업을 수행할 수 있습니다. 승인 기능을 사용하여 리포지토리 간에 콘텐츠를 이동합니다. **스테이징** 에서 **게시** 되거나 거부된 리포지토리로 콘텐츠를 이동하는 기능을 인증하거나 **거부합니다**. 컬렉션을 삭제합니다.
사용자	사용자 보기 사용자 삭제 사용자 추가 사용자 변경	이러한 권한이 있는 그룹은 개인 자동화 허브에서 사용자 구성을 관리하고 액세스할 수 있습니다.
groups	그룹 보기 그룹 삭제 그룹 추가 그룹 변경	이러한 권한이 있는 그룹은 그룹 구성을 관리하고 프라이빗 자동화 허브에서 액세스할 수 있습니다.
원격 컬렉션	원격 컬렉션 변경 원격 컬렉션 보기	이러한 권한이 있는 그룹은 **Collection → Repositories** 로 이동하여 원격 리포지토리를 구성할 수 있습니다.
컨테이너	컨테이너 네임스페이스 권한 변경 컨테이너 변경 이미지 태그 변경 새 컨테이너 만들기 기존 컨테이너로 푸시 컨테이너 리포지토리 삭제	이러한 권한이 있는 그룹은 프라이빗 자동화 허브에서 컨테이너 리포지토리를 관리할 수 있습니다.

개체	권한	설명
원격 레지스트리	원격 레지스트리 추가 원격 레지스트리 변경 원격 레지스트리 삭제	이러한 권한이 있는 그룹은 프라이빗 자동화 허브에 추가된 원격 레지스트리를 추가, 변경 또는 삭제할 수 있습니다.
작업 관리	작업 변경 작업 삭제 모든 작업 보기	이러한 권한이 있는 그룹은 개인 자동화 허브에서 **작업 관리에** 추가된 작업을 관리할 수 있습니다.

5장. ANSIBLE AUTOMATION PLATFORM CENTRAL AUTHENTICATION GENERIC OIDC 설정 및 RED HAT SSO/KEYCLOAK FOR RED HAT SSO 및 ANSIBLE AUTOMATION PLATFORM 구성

Ansible Automation Platform Central 인증을 사용하면 일반 OIDC 설정 및 Red Hat SSO/keycloak for Red Hat SSO 및 Ansible Automation Platform을 설정할 수 있습니다.

5.1. 사전 요구 사항

- admin 사용자로 로그인할 수 있습니다.

5.2. 중앙 인증 일반 OIDC 설정 구성

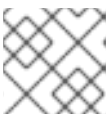
절차

1. RH-SSO에 admin으로 로그인합니다.

참고

기존 영역이 있는 경우 6 단계로 이동할 수 있습니다.

2. add Cryostat를 추가합니다.
3. 이름을 입력하고 생성 을 클릭합니다.
4. 클라이언트 탭을 클릭합니다.
5. 이름을 입력하고 생성 을 클릭합니다.
6. 탐색 패널에서 클라이언트 프로토콜 → openid-connect 를 선택합니다.
7. 탐색 패널에서 Access Type → confidential 를 선택합니다.
8. Root URL 필드에 Ansible Automation Platform 서버 IP 또는 호스트 이름을 입력합니다.
9. Valid Redirect 필드에 Ansible Automation Platform 서버 IP 또는 호스트 이름을 입력합니다. 프로덕션 환경에 없는 경우 *로 설정합니다.
10. Web origins 필드에 Ansible Automation Platform 서버 IP 또는 호스트 이름을 입력합니다. 프로덕션 환경에 없는 경우 *로 설정합니다.
11. Credentials 탭을 클릭합니다.



참고

나중에 사용할 수 있도록 보안을 추적합니다.

12. Ansible Automation Platform Controller에 admin으로 로그인합니다.
13. 탐색 패널에서 설정을 선택합니다.

14. 인증 옵션 목록에서 일반 OIDC 설정을 선택합니다.
15. 편집을 클릭합니다.
16. OIDC 키 필드에 5단계에서 클라이언트 이름을 입력합니다.
17. OIDC 시크릿 필드에 8단계에서 저장된 시크릿을 입력합니다.
18. OIDC 공급자 URL 필드에 키클로킹 서버 URL 및 포트를 입력합니다.
19. 저장을 클릭합니다.

OIDC는 로그인에 대한 옵션으로 표시되어야 합니다. OIDC로 로그인을 클릭하면 로그인 및 Ansible Automation Platform으로 리디렉션하려면 SSO 서버로 리디렉션됩니다.