계정을 관리합니다

Astra Control Center

NetApp
November 21, 2023

목차

계정을 관리합니다

사용자 관리

Astra Control Center 설치 사용자를 Astra Control UI를 사용하여 초대, 추가, 제거 및 편집할 수 있습니다. Astra Control UI 또는 를 사용할 수 있습니다 "Astra Control API" 를 눌러 사용자를 관리합니다.

LDAP를 사용하여 선택한 사용자에 대한 인증을 수행할 수도 있습니다.

LDAP를 사용합니다

LDAP는 분산된 디렉터리 정보에 액세스하기 위한 업계 표준 프로토콜이며 엔터프라이즈 인증에 널리 사용되는 프로토콜입니다. Astra Control Center를 LDAP 서버에 연결하여 선택한 Astra 사용자에 대한 인증을 수행할 수 있습니다. 이 구성에는 Astra와 LDAP를 통합하고 LDAP 정의에 해당하는 Astra 사용자 및 그룹을 정의하는 작업이 포함됩니다. 을 참조하십시오 "LDAP 인증" 를 참조하십시오.

사용자를 초대합니다

계정 소유자와 관리자는 새 사용자를 Astra Control Center에 초대할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭을 선택합니다.
3. 사용자 초대 * 를 선택합니다.
4. 사용자의 이름과 이메일 주소를 입력합니다.
5. 적절한 시스템 권한이 있는 사용자 역할을 선택합니다.

   각 역할은 다음과 같은 권한을 제공합니다.

   - Viewer * 는 리소스를 볼 수 있습니다.
   - 구성원 * 은 뷰어 역할 권한을 가지며 앱 및 클러스터를 관리하고, 앱을 관리하고, 스냅샷 및 백업을 삭제할 수 있습니다.
   - Admin * 은 구성원 역할 권한을 가지며 소유자를 제외한 다른 사용자를 추가 및 제거할 수 있습니다.
   - 소유자 * 는 관리자 역할 권한을 가지며 모든 사용자 계정을 추가 및 제거할 수 있습니다.
6. 멤버 또는 뷰어 역할이 있는 사용자에게 제약 조건을 추가하려면 * 제약 조건으로 역할 제한 * 확인란을 활성화합니다.

   제약 조건 추가에 대한 자세한 내용은 을 참조하십시오 "역할을 관리합니다".

7. 사용자 초대 * 를 선택합니다.

   사용자에게 Astra Control Center에 초대되었음을 알리는 이메일이 전송됩니다. 이 이메일에는 임시 암호가 포함되어 있으며, 이 암호는 처음 로그인할 때 변경해야 합니다.

사용자 추가

계정 소유자와 관리자는 Astra Control Center 설치에 사용자를 더 추가할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭을 선택합니다.
3. 사용자 추가 * 를 선택합니다.
4. 사용자 이름, 이메일 주소 및 임시 암호를 입력합니다.

   사용자는 처음 로그인할 때 암호를 변경해야 합니다.

5. 적절한 시스템 권한이 있는 사용자 역할을 선택합니다.

   각 역할은 다음과 같은 권한을 제공합니다.

   - Viewer * 는 리소스를 볼 수 있습니다.
   - 구성원 * 은 뷰어 역할 권한을 가지며 앱 및 클러스터를 관리하고, 앱을 관리하고, 스냅샷 및 백업을 삭제할 수 있습니다.
   - Admin * 은 구성원 역할 권한을 가지며 소유자를 제외한 다른 사용자를 추가 및 제거할 수 있습니다.
   - 소유자 * 는 관리자 역할 권한을 가지며 모든 사용자 계정을 추가 및 제거할 수 있습니다.

6. 멤버 또는 뷰어 역할이 있는 사용자에게 제약 조건을 추가하려면 * 제약 조건으로 역할 제한 * 확인란을 활성화합니다.

   제약 조건 추가에 대한 자세한 내용은 을 참조하십시오 "역할을 관리합니다".

7. 추가 * 를 선택합니다.

암호 관리

Astra Control Center에서 사용자 계정의 암호를 관리할 수 있습니다.

암호를 변경합니다

언제든지 사용자 계정의 암호를 변경할 수 있습니다.

단계

1. 화면 오른쪽 상단에서 사용자 아이콘을 선택합니다.
2. 프로파일 * 을 선택합니다.
3. 작업 * 열의 옵션 메뉴에서 * 암호 변경 * 을 선택합니다.
4. 암호 요구 사항에 맞는 암호를 입력합니다.
5. 암호를 다시 입력하여 확인합니다.
6. 암호 변경 * 을 선택합니다.

다른 사용자의 암호를 재설정합니다

계정에 관리자 또는 소유자 역할 권한이 있는 경우 다른 사용자 계정과 사용자의 암호를 재설정할 수 있습니다. 암호를 재설정할 때 사용자가 로그인할 때 변경해야 하는 임시 암호를 할당합니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 작업 * 드롭다운 목록을 선택합니다.
3. 암호 재설정 * 을 선택합니다.
4. 암호 요구 사항에 맞는 임시 암호를 입력합니다.
5. 암호를 다시 입력하여 확인합니다.

   다음에 사용자가 로그인할 때 암호를 변경하라는 메시지가 표시됩니다.

6. 비밀번호 재설정 * 을 선택합니다.

사용자의 역할을 변경합니다

소유자 역할을 가진 사용자는 모든 사용자의 역할을 변경할 수 있지만 관리자 역할을 가진 사용자는 관리자, 구성원 또는 뷰어 역할을 가진 사용자의 역할을 변경할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 작업 * 드롭다운 목록을 선택합니다.
3. 역할 편집 * 을 선택합니다.
4. 새 역할을 선택합니다.
5. 역할에 제약 조건을 적용하려면 * 제약 조건으로 역할 제한 * 확인란을 선택하고 목록에서 제약 조건을 선택합니다.

   구속조건이 없으면 구속조건을 추가할 수 있습니다. 자세한 내용은 을 참조하십시오 "역할을 관리합니다".

6. Confirm * 을 선택합니다.

결과

Astra Control Center는 선택한 새 역할에 따라 사용자의 권한을 업데이트합니다.

사용자를 제거합니다

소유자 또는 관리자 역할을 가진 사용자는 언제든지 계정에서 다른 사용자를 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭에서 제거할 각 사용자의 행에서 확인란을 선택합니다.
3. Actions * 열의 Options 메뉴에서 * Remove user/s * 를 선택합니다.
4. 메시지가 표시되면 "remove(제거)"라는 단어를 입력한 다음 * Yes, Remove User(예, 사용자 제거) * 를 선택하여

삭제를 확인합니다.

결과

Astra Control Center는 계정에서 사용자를 제거합니다.

역할을 관리합니다

네임스페이스 제약 조건을 추가하고 이러한 제약 조건에 대한 사용자 역할을 제한하여 역할을 관리할 수 있습니다. 이렇게 하면 조직 내의 리소스에 대한 액세스를 제어할 수 있습니다. Astra Control UI 또는 를 사용할 수 있습니다 "Astra Control API" 역할을 관리합니다.

역할에 네임스페이스 제약 조건을 추가합니다

관리자 또는 소유자 사용자는 네임스페이스 제약 조건을 추가할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭을 선택합니다.
3. Actions * 열에서 Member 또는 Viewer 역할을 가진 사용자의 메뉴 버튼을 선택합니다.
4. 역할 편집 * 을 선택합니다.
5. 제약 조건으로 역할 제한 * 확인란을 활성화합니다.

   이 확인란은 구성원 또는 뷰어 역할에만 사용할 수 있습니다. 역할 * 드롭다운 목록에서 다른 역할을 선택할 수 있습니다.

6. 구속 조건 추가 * 를 선택합니다.

   네임스페이스 또는 네임스페이스 레이블별로 사용 가능한 제약 조건 목록을 볼 수 있습니다.

7. 네임스페이스 구성 방법에 따라 * 제약 조건 유형 * 드롭다운 목록에서 * Kubernetes 네임스페이스 * 또는 * Kubernetes 네임스페이스 레이블 * 을 선택합니다.
8. 목록에서 하나 이상의 네임스페이스 또는 레이블을 선택하여 해당 네임스페이스로 역할을 제한하는 제약 조건을 구성합니다.
9. Confirm * 을 선택합니다.

   역할 편집 * 페이지에는 이 역할에 대해 선택한 제약 조건 목록이 표시됩니다.

10. Confirm * 을 선택합니다.

    계정 * 페이지의 * 역할 * 열에서 구성원 또는 뷰어 역할에 대한 제약 조건을 볼 수 있습니다.

> 역할에 대한 제약 조건을 설정하고 제약 조건을 추가하지 않고 * 확인 * 을 선택하면 역할이 전체 제한 사항으로 간주됩니다(역할에 네임스페이스가 할당된 리소스에 대한 액세스가 거부됨).

역할에서 네임스페이스 제약 조건을 제거합니다

관리자 또는 소유자 사용자는 역할에서 네임스페이스 제약 조건을 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 사용자 * 탭을 선택합니다.
3. Actions * 열에서 활성 제약 조건이 있는 Member 또는 Viewer 역할을 가진 사용자의 메뉴 버튼을 선택합니다.
4. 역할 편집 * 을 선택합니다.

   역할 편집 * 대화 상자에 해당 역할에 대한 활성 제약 조건이 표시됩니다.

5. 제거할 구속 조건의 오른쪽에 있는 * X * 를 선택합니다.
6. Confirm * 을 선택합니다.

를 참조하십시오

- "사용자 역할 및 네임스페이스"

알림을 보고 관리합니다

Astra는 작업이 완료되거나 실패했을 때 알려줍니다. 예를 들어, 앱 백업이 성공적으로 완료되면 알림이 표시됩니다.

인터페이스의 오른쪽 상단에서 이러한 알림을 관리할 수 있습니다.

단계

1. 오른쪽 상단에서 읽지 않은 알림 수를 선택합니다.
2. 알림을 검토한 후 * 읽은 상태로 표시 * 또는 * 모든 알림 표시 * 를 선택합니다.

   모든 알림 표시 * 를 선택한 경우 알림 페이지가 로드됩니다.

3. 알림 * 페이지에서 알림을 보고 읽음으로 표시할 알림을 선택하고 * 작업 * 을 선택한 다음 * 읽음으로 표시 * 를 선택합니다.

자격 증명을 추가 및 제거합니다

ONTAP S3, OpenShift로 관리되는 Kubernetes 클러스터, 또는 관리되지 않는 Kubernetes 클러스터와 같은 로컬 프라이빗 클라우드 공급자의 자격 증명을 언제든지 계정에서 추가 및 제거할 수 있습니다. Astra Control Center는 이러한 자격 증명을 사용하여 Kubernetes 클러스터 및 클러스터의 앱을 검색하고 대신 리소스를 프로비저닝합니다.

Astra Control Center의 모든 사용자는 동일한 자격 증명 세트를 공유합니다.

자격 증명을 추가합니다

클러스터를 관리할 때 Astra Control Center에 자격 증명을 추가할 수 있습니다. 새 클러스터를 추가하여 자격 증명을 추가하려면 을 참조하십시오 "Kubernetes 클러스터 추가".

> 직접 만드는 경우 `kubeconfig` 파일에서 * 하나의 * 컨텍스트 요소만 정의해야 합니다. 을 참조하십시오 "Kubernetes 문서" 을 참조하십시오 `kubeconfig` 파일.

자격 증명을 제거합니다

언제든지 계정에서 자격 증명을 제거합니다. 자격 증명은 이후에 제거해야 합니다 "연결된 모든 클러스터의 관리를 취소합니다".

> Astra Control Center에 추가하는 첫 번째 자격 증명 세트는 항상 사용 중입니다. Astra Control Center는 자격 증명을 사용하여 백업 버킷에 인증하기 때문입니다. 이러한 자격 증명을 제거하지 않는 것이 좋습니다.

단계

1. 계정 * 을 선택합니다.
2. 자격 증명 * 탭을 선택합니다.
3. 제거할 자격 증명에 대한 * 상태 * 열의 옵션 메뉴를 선택합니다.
4. 제거 * 를 선택합니다.
5. 삭제를 확인하려면 "remove(제거)"라는 단어를 입력한 다음 * Yes(예), Remove Credential(자격 증명 제거) * 을 선택합니다.

결과

Astra Control Center는 계정에서 자격 증명을 제거합니다.

계정 활동을 모니터링합니다

Astra Control 계정의 활동에 대한 세부 정보를 볼 수 있습니다. 예를 들어, 새 사용자를 초대하거나, 클러스터를 추가하거나, 스냅샷을 생성할 때 사용할 수 있습니다. 계정 활동을 CSV 파일로 내보낼 수도 있습니다.

> Astra Control에서 Kubernetes 클러스터를 관리하고, Astra Control이 Cloud Insights에 연결된 경우, Astra Control은 이벤트 로그를 Cloud Insights로 보냅니다. POD 배포 및 PVC 첨부 파일에 대한 정보를 포함한 로그 정보가 Astra Control Activity 로그에 표시됩니다. 이 정보를 사용하여 관리하고 있는 Kubernetes 클러스터의 문제를 식별할 수 있습니다.

Astra Control에서 모든 계정 활동을 봅니다

1. Activity * 를 선택합니다.
2. 필터를 사용하여 활동 목록의 범위를 좁히거나 검색 상자를 사용하여 원하는 항목을 정확하게 찾을 수 있습니다.
3. CSV로 내보내기 * 를 선택하여 계정 활동을 CSV 파일로 다운로드합니다.

특정 앱의 계정 활동을 봅니다

1. 응용 프로그램 * 을 선택한 다음 앱 이름을 선택합니다.
2. Activity * 를 선택합니다.

클러스터의 계정 활동을 봅니다

1. 클러스터 * 를 선택한 다음 클러스터 이름을 선택합니다.
2. Activity * 를 선택합니다.

주의가 필요한 이벤트를 해결하기 위한 조치를 취하십시오

1. Activity * 를 선택합니다.
2. 주의가 필요한 이벤트를 선택합니다.
3. 실행 * 드롭다운 옵션을 선택합니다.

   이 목록에서 수행할 수 있는 수정 조치를 확인하고, 문제와 관련된 문서를 보고, 문제 해결을 위한 지원을 받을 수 있습니다.

기존 라이센스를 업데이트합니다

평가판 라이센스를 전체 라이센스로 변환하거나 기존 평가판 또는 전체 라이센스를 새 라이센스로 업데이트할 수 있습니다. 전체 라이센스가 없는 경우 NetApp 세일즈 담당자와 협력하여 전체 라이센스 및 일련 번호를 받으십시오. Astra UI 또는 를 사용할 수 있습니다 "Astra Control API" 기존 라이센스를 업데이트합니다.

단계

1. 에 로그인합니다 "NetApp Support 사이트".
2. Astra Control Center 다운로드 페이지에 액세스하여 일련 번호를 입력한 다음 전체 NetApp 라이센스 파일(NLF)을 다운로드하십시오.
3. Astra Control Center UI에 로그인합니다.
4. 왼쪽 탐색 창에서 * 계정 * > * 라이센스 * 를 선택합니다.
5. 계정 * > * 라이선스 * 페이지에서 기존 라이선스의 상태 드롭다운 메뉴를 선택하고 * 교체 * 를 선택합니다.
6. 다운로드한 라이센스 파일을 찾습니다.
7. 추가 * 를 선택합니다.

Account * > * Licenses * 페이지에는 라이센스 정보, 만료 날짜, 라이센스 일련 번호, 계정 ID 및 사용된 CPU 단위가 표시됩니다.

를 참조하십시오

- "Astra Control Center 라이센스"

리포지토리 연결을 관리합니다

저장소를 Astra Control에 연결하여 소프트웨어 패키지 설치 이미지 및 아티팩트에 대한 참조로 사용할 수 있습니다. 소프트웨어 패키지를 가져올 때 Astra Control은 이미지 리포지토리의 설치 이미지 및 바이너리 및 기타 아티팩트의 아티팩트를 참조합니다.

필요한 것

- Astra Control Center가 설치된 Kubernetes 클러스터
- 액세스할 수 있는 실행 중인 Docker 리포지토리입니다
- 액세스할 수 있는 실행 아티팩트 저장소(예: Artifactory)

Docker 이미지 저장소를 연결합니다

Docker 이미지 저장소를 연결하여 Astra Data Store와 같은 패키지 설치 이미지를 보관할 수 있습니다. 패키지를 설치할 때 Astra Control은 이미지 저장소에서 패키지 이미지 파일을 가져옵니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 연결 * 탭을 선택합니다.
3. Docker Image Repository * 섹션에서 오른쪽 상단의 메뉴를 선택합니다.
4. Connect * 를 선택합니다.
5. 리포지토리의 URL 및 포트를 추가합니다.
6. 리포지토리의 자격 증명을 입력합니다.
7. Connect * 를 선택합니다.

결과

리포지토리가 연결되었습니다. Docker Image Repository * 섹션에서 리포지토리가 연결됨 상태를 표시해야 합니다.

Docker 이미지 리포지토리 연결을 끊습니다

더 이상 필요하지 않은 경우 Docker 이미지 저장소에 대한 연결을 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 연결 * 탭을 선택합니다.
3. Docker Image Repository * 섹션에서 오른쪽 상단의 메뉴를 선택합니다.
4. Disconnect * 를 선택합니다.
5. 예, Docker 이미지 리포지토리 * 를 연결 해제합니다.

결과

리포지토리의 연결이 끊겼습니다. Docker Image Repository * 섹션에서 리포지토리의 연결 끊김 상태가 표시되어야 합니다.

아티팩트 리포지토리를 연결합니다

아티팩트 리포지토리를 소프트웨어 패키지 바이너리와 같은 호스트 아티팩트에 연결할 수 있습니다. 패키지를 설치할 때 Astra Control은 이미지 저장소에서 소프트웨어 패키지에 대한 아티팩트를 가져옵니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 연결 * 탭을 선택합니다.
3. Artifact Repository * 섹션에서 오른쪽 상단의 메뉴를 선택합니다.
4. Connect * 를 선택합니다.
5. 리포지토리의 URL 및 포트를 추가합니다.
6. 인증이 필요한 경우 * Use authentication *(인증 사용 *) 확인란을 선택하고 리포지토리의 자격 증명을 입력합니다.
7. Connect * 를 선택합니다.

결과

리포지토리가 연결되었습니다. Artifact Repository * 섹션에서 리포지토리는 연결된 상태를 표시해야 합니다.

아티팩트 저장소의 연결을 해제합니다

더 이상 필요하지 않은 경우 아티팩트 리포지토리에 대한 연결을 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 연결 * 탭을 선택합니다.
3. Artifact Repository * 섹션에서 오른쪽 상단의 메뉴를 선택합니다.
4. Disconnect * 를 선택합니다.
5. Yes, disconnect artifact repository * 를 선택합니다.

결과

리포지토리의 연결이 끊겼습니다. Artifact Repository * 섹션에서 리포지토리는 연결된 상태를 표시해야 합니다.

자세한 내용을 확인하십시오

- "소프트웨어 패키지를 관리합니다"

소프트웨어 패키지를 관리합니다

NetApp은 NetApp Support 사이트에서 다운로드할 수 있는 소프트웨어 패키지가 포함된 Astra Control Center에 대한 추가 기능을 제공합니다. Docker 및 아티팩트 저장소를 연결한 후 패키지를 업로드 및 가져와 Astra Control Center에 이 기능을 추가할 수 있습니다. CLI 또는 Astra Control Center 웹 UI를 사용하여 소프트웨어 패키지를 관리할 수 있습니다.

필요한 것

- Astra Control Center가 설치된 Kubernetes 클러스터
- 소프트웨어 패키지 이미지를 보관할 연결된 Docker 이미지 리포지토리입니다. 자세한 내용은 을 참조하십시오 "리포지토리 연결을 관리합니다".
- 소프트웨어 패키지 바이너리 및 아티팩트를 보관하는 연결된 아티팩트 리포지토리입니다. 자세한 내용은 을 참조하십시오 "리포지토리 연결을 관리합니다".
- NetApp Support 사이트의 소프트웨어 패키지입니다

소프트웨어 패키지 이미지를 리포지토리에 업로드합니다

Astra Control Center는 연결된 저장소의 패키지 이미지 및 아티팩트를 참조합니다. CLI를 사용하여 이미지 및 아티팩트를 리포지토리에 업로드할 수 있습니다.

단계

1. NetApp Support 사이트에서 소프트웨어 패키지를 다운로드하여 가 있는 컴퓨터에 저장합니다 `kubectl` 유틸리티가 설치되었습니다.
2. 압축된 패키지 파일의 압축을 풀고 디렉토리를 Astra Control 번들 파일의 위치로 변경합니다(예: `acc.manifest.yaml`)를 클릭합니다.
3. 패키지 이미지를 Docker 저장소로 푸시합니다. 다음 대체 작업을 수행합니다.
   - Bundle_file을 Astra Control 번들 파일 이름으로 바꿉니다(예: `acc.manifest.yaml`)를 클릭합니다.
   - my_registry를 Docker 리포지토리의 URL로 바꿉니다.
   - my_registry_user를 사용자 이름으로 바꿉니다.
   - my_registry_token을 레지스트리에 대한 인증된 토큰으로 바꿉니다.

   ```
   kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY -u
   MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
   ```

4. 패키지에 아티팩트가 있는 경우 아티팩트를 아티팩트 저장소로 복사합니다. bundle_file을 Astra Control 번들 파일의 이름으로 바꾸고 network_location을 네트워크 위치로 교체하여 다음 위치에 아티팩트 파일을 복사합니다.

   ```
   kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
   ```

소프트웨어 패키지를 추가합니다

Astra Control Center 번들 파일을 사용하여 소프트웨어 패키지를 가져올 수 있습니다. 이렇게 하면 패키지가 설치되고 Astra Control Center에서 소프트웨어를 사용할 수 있습니다.

Astra Control 웹 **UI**를 사용하여 소프트웨어 패키지를 추가합니다

Astra Control Center 웹 UI를 사용하여 연결된 저장소에 업로드된 소프트웨어 패키지를 추가할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 패키지 * 탭을 선택합니다.
3. 추가 * 버튼을 선택합니다.
4. 파일 선택 대화 상자에서 업로드 아이콘을 선택합니다.
5. 에서 Astra Control 번들 파일을 선택합니다 `.yaml` 형식, 업로드할 형식.
6. 추가 * 를 선택합니다.

결과

번들 파일이 유효하고 패키지 이미지 및 아티팩트가 연결된 저장소에 있으면 패키지가 Astra Control Center에 추가됩니다. 상태 * 열의 상태가 * 사용 가능 * 으로 변경되면 패키지를 사용할 수 있습니다. 패키지 상태 위로 마우스를 가져가면 추가 정보를 볼 수 있습니다.

> 리포지토리에 패키지에 대한 하나 이상의 이미지 또는 아티팩트가 없으면 해당 패키지에 대한 오류 메시지가 나타납니다.

CLI를 사용하여 소프트웨어 패키지를 추가합니다

CLI를 사용하여 연결된 리포지토리에 업로드한 소프트웨어 패키지를 가져올 수 있습니다. 이를 위해서는 먼저 Astra Control Center 계정 ID와 API 토큰을 기록해야 합니다.

단계

1. 웹 브라우저를 사용하여 Astra Control Center 웹 UI에 로그인합니다.
2. 대시보드에서 오른쪽 상단의 사용자 아이콘을 선택합니다.
3. API 액세스 * 를 선택합니다.
4. 화면 위쪽에 있는 계정 ID를 확인합니다.
5. API 토큰 생성 * 을 선택합니다.
6. 결과 대화 상자에서 * API 토큰 생성 * 을 선택합니다.
7. 결과 토큰을 기록하고 * Close * 를 선택합니다. CLI에서 디렉토리를 의 위치로 변경합니다 `.yaml` 압축을 푼 패키지 내용물의 번들 파일입니다.
8. 번들 파일을 사용하여 패키지를 가져오고 다음 대체 항목을 만듭니다.
   - Bundle_file을 Astra Control 번들 파일의 이름으로 바꿉니다.
   - 서버를 Astra Control 인스턴스의 DNS 이름으로 바꿉니다.
   - account_ID 및 토큰을 이전에 기록한 계정 ID 및 API 토큰으로 교체합니다.

```
kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
-k TOKEN
```

결과

번들 파일이 유효하고 패키지 이미지 및 아티팩트가 연결된 저장소에 있으면 패키지가 Astra Control Center에 추가됩니다.

> 리포지토리에 패키지에 대한 하나 이상의 이미지 또는 아티팩트가 없으면 해당 패키지에 대한 오류 메시지가 나타납니다.

소프트웨어 패키지를 제거합니다

Astra Control Center 웹 UI를 사용하여 이전에 Astra Control Center에서 가져온 소프트웨어 패키지를 제거할 수 있습니다.

단계

1. 계정 관리 * 탐색 영역에서 * 계정 * 을 선택합니다.
2. 패키지 * 탭을 선택합니다.

   이 페이지에서는 설치된 패키지 목록과 해당 상태를 확인할 수 있습니다.

3. 패키지의 * Actions * 열에서 Actions 메뉴를 엽니다.
4. 삭제 * 를 선택합니다.

결과

패키지는 Astra Control Center에서 삭제되지만 패키지의 이미지 및 아티팩트는 저장소에 남아 있습니다.

자세한 내용을 확인하십시오

- "리포지토리 연결을 관리합니다"