계정을 관리합니다

Astra Control Center

NetApp
August 11, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/astra-control-center-2310/use/manage-local-users-and-roles.html on August 11, 2025. Always check docs.netapp.com for the latest.

목차

계정을 관리합니다 1
로컬 사용자 및 역할 관리 1
LDAP를 사용합니다 1
사용자 추가 1
암호 관리 2
사용자를 제거합니다 2
역할을 관리합니다 3
를 참조하십시오 4
원격 인증을 관리합니다 4
LDAPS 인증을 위한 인증서를 추가합니다 4
원격 인증을 사용합니다 5
원격 인증을 비활성화합니다 5
원격 인증 설정을 편집합니다 6
원격 인증 연결을 끊습니다 6
원격 사용자 및 그룹 관리 6
원격 사용자를 추가합니다 7
원격 그룹을 추가합니다 7
알림을 보고 관리합니다 8
자격 증명을 추가 및 제거합니다 9
자격 증명을 추가합니다 9
자격 증명을 제거합니다 9
계정 활동을 모니터링합니다 9
기존 라이센스를 업데이트합니다 10
를 참조하십시오 11

계정을 관리합니다

로컬 사용자 및 역할 관리

Astra Control Center 설치 사용자는 Astra Control UI를 사용하여 추가, 제거 및 편집할 수 있습니다. Astra Control UI 또는 를 사용할 수 있습니다 "Astra Control API를 참조하십시오" 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 Control 사용자에 대한 인증을 수행할 수 있습니다. 이 구성에는 Astra와 LDAP를 통합하고 LDAP 정의에 해당하는 Astra Control 사용자 및 그룹을 정의하는 작업이 포함됩니다. Astra Control API 또는 웹 UI를 사용하여 LDAP 인증과 LDAP 사용자 및 그룹을 구성할 수 있습니다. 자세한 내용은 다음 설명서를 참조하십시오.

- "Astra Control API를 사용하여 원격 인증 및 사용자를 관리합니다"
- "Astra Control UI를 사용하여 원격 사용자 및 그룹을 관리합니다"
- "Astra Control UI를 사용하여 원격 인증을 관리합니다"

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 "로컬 사용자 및 역할 관리".

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.

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 API를 참조하십시오" 역할을 관리합니다.

역할에 네임스페이스 제약 조건을 추가합니다

관리자 또는 소유자 사용자는 구성원 또는 뷰어 역할에 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"

원격 인증을 관리합니다

LDAP는 분산된 디렉터리 정보에 액세스하기 위한 업계 표준 프로토콜이며 엔터프라이즈 인증에 널리 사용되는 프로토콜입니다. Astra Control Center를 LDAP 서버에 연결하여 선택한 Astra Control 사용자에 대한 인증을 수행할 수 있습니다.

이 구성에는 Astra와 LDAP를 통합하고 LDAP 정의에 해당하는 Astra Control 사용자 및 그룹을 정의하는 작업이 포함됩니다. Astra Control API 또는 웹 UI를 사용하여 LDAP 인증과 LDAP 사용자 및 그룹을 구성할 수 있습니다.

Astra Control Center는 원격 인증이 활성화될 때 구성된 사용자 로그인 속성을 사용하여 원격 사용자를 검색하고 추적합니다. Astra Control Center에 표시하고자 하는 원격 사용자의 경우 이메일 주소("메일") 또는 사용자 주체 이름("userPrincipalName")의 속성이 이 필드에 있어야 합니다. 이 속성은 인증을 위한 Astra Control Center의 사용자 이름과 원격 사용자를 검색하는 데 사용됩니다.

LDAPS 인증을 위한 인증서를 추가합니다

LDAPS 연결을 사용할 때 Astra Control Center가 LDAP 서버를 인증할 수 있도록 LDAP 서버에 대한 개인 TLS 인증서를 추가합니다. 이 작업은 한 번만 수행하거나 설치한 인증서가 만료되면 수행해야 합니다.

단계

1. 계정 * 으로 이동합니다.
2. 인증서 * 탭을 선택합니다.
3. 추가 * 를 선택합니다.
4. 를 업로드하거나 `.pem` 클립보드에서 파일의 내용을 파일 또는 붙여 넣습니다.
5. 신뢰할 수 있는 * 확인란을 선택합니다.

6. 인증서 추가 * 를 선택합니다.

원격 인증을 사용합니다

LDAP 인증을 설정하고 Astra Control과 원격 LDAP 서버 간의 연결을 구성할 수 있습니다.

시작하기 전에

LDAPS를 사용하려는 경우 Astra Control Center에서 LDAP 서버를 인증할 수 있도록 LDAP 서버의 개인 TLS 인증서가 Astra Control Center에 설치되어 있는지 확인합니다. 을 참조하십시오 LDAPS 인증을 위한 인증서를 추가합니다 를 참조하십시오.

단계

1. 계정 > 연결 * 으로 이동합니다.
2. Remote Authentication* 창에서 구성 메뉴를 선택합니다.
3. Connect * 를 선택합니다.
4. 서버 IP 주소, 포트 및 기본 설정 연결 프로토콜(LDAP 또는 LDAPS)을 입력합니다.

> 가장 좋은 방법은 LDAP 서버와 연결할 때 LDAPS를 사용하는 것입니다. LDAPS에 연결하기 전에 Astra Control Center에 LDAP 서버의 개인 TLS 인증서를 설치해야 합니다.

5. 서비스 계정 자격 증명을 이메일 형식(administrator@example.com 입력합니다. Astra Control은 LDAP 서버에 연결할 때 이러한 자격 증명을 사용합니다.
6. 사용자 일치 * 섹션에서 다음을 수행합니다.
   a. LDAP 서버에서 사용자 정보를 검색할 때 사용할 기본 DN과 적절한 사용자 검색 필터를 입력합니다.
   b. (선택 사항) 디렉터리에서 사용자 로그인 속성을 사용하는 경우 `userPrincipalName` 대신 `mail`를 입력합니다 `userPrincipalName` 사용자 로그인 속성 * 필드의 올바른 속성
7. 그룹 일치 * 섹션에서 그룹 검색 기준 DN과 적절한 사용자 지정 그룹 검색 필터를 입력합니다.

> 올바른 기본 DN(고유 이름)과 * 사용자 일치 * 및 * 그룹 일치 * 에 대한 적절한 검색 필터를 사용해야 합니다. 기본 DN은 Astra Control에 검색을 시작할 디렉토리 트리의 수준을 알리고 검색 필터는 디렉토리 트리 Astra Control의 검색 부분을 제한합니다.

8. 제출 * 을 선택합니다.

결과

원격 인증 * 창 상태는 * Pending * 으로 이동한 다음 LDAP 서버 연결이 설정되면 * Connected * 로 이동합니다.

원격 인증을 비활성화합니다

LDAP 서버에 대한 활성 연결을 일시적으로 해제할 수 있습니다.

> LDAP 서버에 대한 연결을 비활성화하면 모든 설정이 저장되고 해당 LDAP 서버에서 Astra Control에 추가된 모든 원격 사용자 및 그룹은 유지됩니다. 언제든지 이 LDAP 서버에 다시 연결할 수 있습니다.

단계

1. 계정 > 연결 * 으로 이동합니다.
2. Remote Authentication* 창에서 구성 메뉴를 선택합니다.
3. 비활성화 * 를 선택합니다.

결과

원격 인증* 창 상태가 * 사용 안 함 * 으로 이동합니다. 모든 원격 인증 설정, 원격 사용자 및 원격 그룹이 보존되며 언제든지 연결을 다시 활성화할 수 있습니다.

원격 인증 설정을 편집합니다

LDAP 서버에 대한 연결을 해제했거나 * 원격 인증 * 창이 "연결 오류" 상태인 경우 구성 설정을 편집할 수 있습니다.

원격 인증* 창이 "사용 안 함" 상태이면 LDAP 서버 URL 또는 IP 주소를 편집할 수 없습니다. 다음 작업을 수행해야 합니다 원격 인증 연결을 끊습니다 먼저,

단계

1. 계정 > 연결 * 으로 이동합니다.
2. Remote Authentication* 창에서 구성 메뉴를 선택합니다.
3. 편집 * 을 선택합니다.
4. 필요한 내용을 변경하고 * Edit * 를 선택합니다.

원격 인증 연결을 끊습니다

LDAP 서버에서 연결을 끊고 Astra Control에서 구성 설정을 제거할 수 있습니다.

LDAP 사용자인 경우 연결을 끊으면 세션이 즉시 종료됩니다 LDAP 서버에서 연결을 끊으면 해당 LDAP 서버에 대한 모든 구성 설정이 Astra Control에서 제거되고 해당 LDAP 서버에서 추가된 모든 원격 사용자 및 그룹이 제거됩니다.

단계

1. 계정 > 연결 * 으로 이동합니다.
2. Remote Authentication* 창에서 구성 메뉴를 선택합니다.
3. Disconnect * 를 선택합니다.

결과

원격 인증 * 창 상태가 * 연결 끊김 * 으로 이동합니다. 원격 인증 설정, 원격 사용자 및 원격 그룹은 Astra Control에서 제거됩니다.

원격 사용자 및 그룹 관리

Astra Control 시스템에서 LDAP 인증을 활성화한 경우 LDAP 사용자 및 그룹을 검색하여 승인된 시스템 사용자에게 포함시킬 수 있습니다.

원격 사용자를 추가합니다

계정 소유자와 관리자는 Astra Control에 원격 사용자를 추가할 수 있습니다. Astra Control Center는 최대 10,000명의 LDAP 원격 사용자를 지원합니다.

> Astra Control Center는 원격 인증이 활성화될 때 구성된 사용자 로그인 속성을 사용하여 원격 사용자를 검색하고 추적합니다. Astra Control Center에 표시하고자 하는 원격 사용자의 경우 이메일 주소("메일") 또는 사용자 주체 이름("userPrincipalName")의 속성이 이 필드에 있어야 합니다. 이 속성은 인증을 위한 Astra Control Center의 사용자 이름과 원격 사용자를 검색하는 데 사용됩니다.

> 시스템에 동일한 이메일 주소("메일" 또는 "사용자 기본 이름" 속성에 기반함)를 가진 로컬 사용자가 이미 있는 경우 원격 사용자를 추가할 수 없습니다. 사용자를 원격 사용자로 추가하려면 먼저 시스템에서 로컬 사용자를 삭제합니다.

단계

1. 계정 * 영역으로 이동합니다.
2. 사용자 및 그룹 * 탭을 선택합니다.
3. 페이지 맨 오른쪽에서 * 원격 사용자 * 를 선택합니다.
4. 추가 * 를 선택합니다.
5. 선택적으로 * Filter by email * 필드에 사용자의 이메일 주소를 입력하여 LDAP 사용자를 검색합니다.
6. 목록에서 한 명 이상의 사용자를 선택합니다.
7. 사용자에게 역할을 할당합니다.

   > 사용자와 사용자 그룹에 서로 다른 역할을 할당하면 더 많은 권한을 허용하는 역할이 우선합니다.

8. 필요한 경우 이 사용자에게 하나 이상의 네임스페이스 제약 조건을 할당하고 * 제약 조건으로 역할 제한 * 을 선택하여 해당 제약 조건을 적용합니다. 제약 조건 추가 * 를 선택하여 새 네임스페이스 제약 조건을 추가할 수 있습니다.

   > 사용자가 LDAP 그룹 구성원 자격을 통해 여러 역할을 할당하면 가장 허용 가능한 역할의 제약 조건만 적용됩니다. 예를 들어, 로컬 뷰어 역할을 가진 사용자가 멤버 역할에 바인딩된 세 개의 그룹에 참여하는 경우 멤버 역할의 제약 조건의 합계가 적용되고 뷰어 역할의 모든 제약 조건은 무시됩니다.

9. 추가 * 를 선택합니다.

결과

새 사용자가 원격 사용자 목록에 나타납니다. 이 목록에서 사용자의 활성 제약 조건을 확인하고 * Actions * 메뉴에서 사용자를 관리할 수 있습니다.

원격 그룹을 추가합니다

한 번에 많은 원격 사용자를 추가하려면 계정 소유자와 관리자가 Astra Control에 원격 그룹을 추가할 수 있습니다. 원격 그룹을 추가하면 해당 그룹의 모든 원격 사용자가 Astra Control에 로그인할 수 있으며 그룹과 동일한 역할을 상속합니다.

Astra Control Center는 최대 5,000개의 LDAP 원격 그룹을 지원합니다.

단계

1. 계정 * 영역으로 이동합니다.
2. 사용자 및 그룹 * 탭을 선택합니다.
3. 페이지 맨 오른쪽에서 * 원격 그룹 * 을 선택합니다.
4. 추가 * 를 선택합니다.

   이 창에서는 Astra Control이 디렉토리에서 검색한 LDAP 그룹의 공통 이름과 고유 이름 목록을 볼 수 있습니다.

5. 선택적으로 * Filter by common name * 필드에 그룹의 공통 이름을 입력하여 LDAP 그룹을 검색합니다.
6. 목록에서 그룹을 하나 이상 선택합니다.
7. 그룹에 역할을 할당합니다.

   선택한 역할은 이 그룹의 모든 사용자에게 할당됩니다. 사용자와 사용자 그룹에 서로 다른 역할을 할당하면 더 많은 권한을 허용하는 역할이 우선합니다.

8. 필요한 경우 이 그룹에 하나 이상의 네임스페이스 제약 조건을 할당하고 * 제약 조건으로 역할 제한 * 을 선택하여 해당 제약 조건을 적용합니다. 제약 조건 추가 * 를 선택하여 새 네임스페이스 제약 조건을 추가할 수 있습니다.

   사용자가 LDAP 그룹 구성원 자격을 통해 여러 역할을 할당하면 가장 허용 가능한 역할의 제약 조건만 적용됩니다. 예를 들어, 로컬 뷰어 역할을 가진 사용자가 멤버 역할에 바인딩된 세 개의 그룹에 참여하는 경우 멤버 역할의 제약 조건의 합계가 적용되고 뷰어 역할의 모든 제약 조건은 무시됩니다.

9. 추가 * 를 선택합니다.

결과

원격 그룹 목록에 새 그룹이 나타납니다. 이 그룹의 원격 사용자는 각 원격 사용자가 로그인할 때까지 원격 사용자 목록에 나타나지 않습니다. 이 목록에서 그룹에 대한 세부 정보를 볼 수 있을 뿐 아니라 * Actions * 메뉴에서 그룹을 관리할 수 있습니다.

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".

> 고유한 kubecononfig 파일을 만드는 경우 해당 파일에 * 하나의 * 컨텍스트 요소만 정의해야 합니다. 을 참조하십시오 "Kubernetes 문서" kubecononfig 파일을 만드는 방법에 대한 자세한 내용은

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 Control Center UI 또는 를 사용할 수 있습니다 "Astra Control API를 참조하십시오" 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"

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.