ID 및 액세스 관리

NetApp Console setup and administration

NetApp
February 11, 2026

목차

ID 및 액세스 관리

NetApp Console ID 및 액세스 관리에 대해 알아보세요

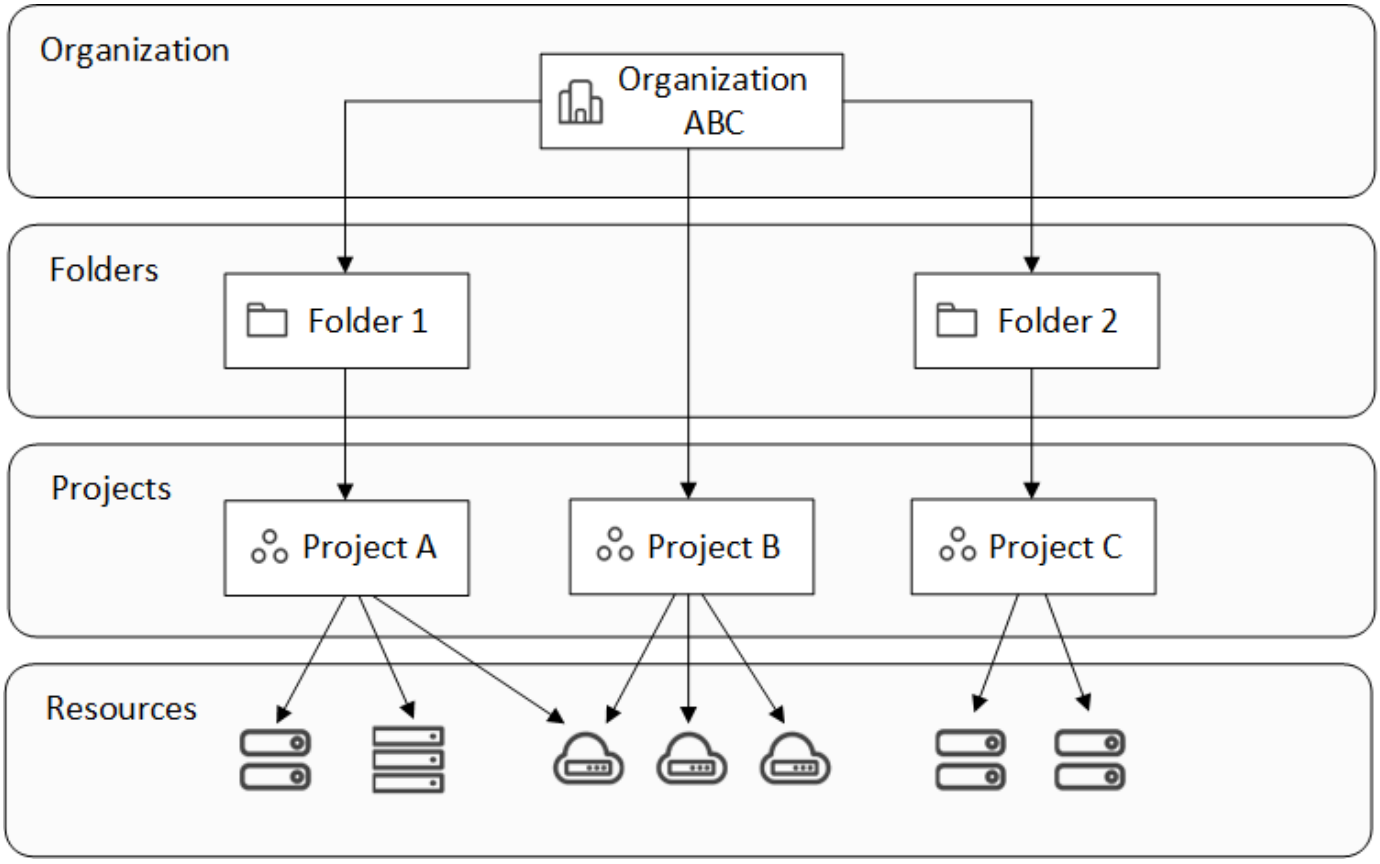
NetApp 콘솔의 ID 및 액세스 관리(IAM)를 사용하여 NetApp 리소스를 구성하고 위치, 부서 또는 프로젝트와 같은 비즈니스 구조에 따라 액세스를 제어하십시오.

리소스는 계층적으로 구성됩니다. 최상위에는 조직이 있고, 그 아래에 폴더(다른 폴더나 프로젝트를 포함할 수 있음)가 있으며, 그 아래에는 스토리지 시스템, 워크로드 및 에이전트를 포함하는 프로젝트가 있습니다.

조직, 폴더 또는 프로젝트 수준에서 액세스 역할을 할당하여 사용자가 리소스에 대한 올바른 액세스 권한을 갖도록 합니다.

NetApp Console 에서 IAM을 관리하려면 슈퍼 관리자, 조직 관리자 또는 폴더 또는 프로젝트 관리자 역할이 있어야 합니다.

다음 이미지는 기본적인 수준의 계층 구조를 보여줍니다.



]

신원 및 접근 관리 구성 요소

NetApp Console 에서는 조직 구성 요소, 리소스 구성 요소 및 사용자 액세스 구성 요소라는 세 가지 주요 구성 요소를 사용하여 스토리지 리소스를 구성합니다.

조직 내 프로젝트 및 폴더

IAM 구조 내에서 조직, 프로젝트 및 폴더라는 세 가지 구성 요소를 사용합니다. 이러한 레벨 중 하나에서 사용자에게 역할을 할당하여 액세스 권한을 부여할 수 있습니다.

조직

_조직_은 콘솔 IAM 시스템의 최상위 수준이며 일반적으로 회사를 나타냅니다. 조직은 폴더, 프로젝트, 구성원, 역할 및 리소스로 구성됩니다. 에이전트는 조직 내의 특정 프로젝트와 연관되어 있습니다.

프로젝트

프로젝트는 스토리지 리소스에 대한 접근 권한을 제공하는 데 사용됩니다. 리소스에 접근하려면 먼저 해당 리소스가 프로젝트에 할당되어야 합니다. 하나의 프로젝트에 여러 리소스를 할당할 수 있으며, 여러 개의 프로젝트를 생성할 수도 있습니다. 그런 다음 사용자에게 프로젝트 권한을 할당하여 프로젝트 내 리소스에 대한 접근 권한을 부여합니다.

예를 들어, 필요에 따라 온프레미스 ONTAP 시스템을 단일 프로젝트 또는 조직 내 모든 프로젝트와 연결할 수 있습니다.

"조직에 프로젝트를 추가하는 방법을 알아보세요."

폴더

관련 프로젝트를 위치, 사이트 또는 사업부별로 정리하려면 폴더로 그룹화하세요. 리소스를 폴더에 직접 연결할 수는 없지만, 폴더 수준에서 사용자에게 역할을 할당하면 해당 폴더에 있는 모든 프로젝트에 대한 액세스 권한을 부여할 수 있습니다.

"조직에 폴더를 추가하는 방법을 알아보세요."

리소스

_리소스_는 NetApp Console이 인식하고 프로젝트에 할당할 수 있는 엔티티입니다. _리소스_에는 스토리지 시스템, Keystone 구독, 일부 NetApp Backup and Recovery 워크로드 및 NetApp Console 에이전트가 포함됩니다.

+ 리소스에 접근하려면 먼저 해당 리소스를 프로젝트와 연결해야 합니다.

+

예를 들어, Cloud Volumes ONTAP 시스템을 특정 프로젝트 또는 조직 내 모든 프로젝트와 연결할 수 있습니다. 리소스를 연결하는 방법은 조직의 요구 사항에 따라 다릅니다.

+

"프로젝트에 리소스를 연결하는 방법을 알아보세요."

스토리지 시스템 및 **Keystone** 구독

스토리지 시스템은 NetApp Console에서 관리하는 주요 리소스입니다. NetApp Console은 온프레미스 및 클라우드 스토리지 시스템 모두의 관리를 지원합니다. 프로젝트에 할당된 사용자가 스토리지 시스템에 액세스할 수 있도록 프로젝트에 스토리지 시스템을 추가해야 합니다.

스토리지 시스템

스토리지 시스템은 추가되는 프로젝트에 자동으로 연결되지만, 리소스 페이지에서 다른 프로젝트 또는 폴더와 연결할 수도 있습니다. FSx for NetApp ONTAP 스토리지 시스템은 프로젝트 또는 폴더와 연결할 수 없지만, 시스템 페이지 또는 워크로드에서 확인할 수 있습니다.

Keystone 구독

Keystone 구독은 NetApp Console 에서 사용자가 구독에 액세스할 수 있도록 프로젝트와 연결할 수 있는 리소스이기도 합니다.

백업 및 복구 워크로드**(Oracle** 및 **Microsoft SQL Server)**

일부 Backup and Recovery 워크로드도 리소스로 간주됩니다. 사용자에게 Backup and

콘솔 에이전트

조직 관리자는 스토리지 시스템을 관리하고 NetApp 데이터 서비스를 활성화하기 위해 콘솔 에이전트를 생성합니다. 에이전트는 처음에 생성된 프로젝트에 연결되지만, 관리자는 에이전트 페이지에서 다른 프로젝트나 폴더에 에이전트를 추가할 수 있습니다.

에이전트를 프로젝트와 연결하면 해당 프로젝트의 리소스를 관리할 수 있으며, 에이전트를 폴더와 연결하면 폴더 또는 프로젝트 관리자가 어떤 프로젝트에서 해당 에이전트를 사용할지 결정할 수 있습니다. 에이전트는 관리 기능을 제공하기 위해 특정 프로젝트와 연결되어야 합니다.

"프로젝트에 에이전트를 연결하는 방법을 알아보세요."

구성원 및 역할

회원들

조직의 구성원은 사용자 계정 또는 서비스 계정입니다. 서비스 계정은 일반적으로 애플리케이션에서 사람의 개입 없이 지정된 작업을 완료하는 데 사용됩니다.

NetApp Console 에 가입한 구성원을 조직에 추가해야 합니다. 추가한 후에는 역할을 할당하여 리소스에 대한 액세스 권한을 부여할 수 있습니다. 콘솔 내에서 수동으로 서비스 계정을 추가하거나 NetApp Console IAM API를 통해 생성 및 관리를 자동화할 수 있습니다.

"조직에 구성원을 추가하는 방법을 알아보세요."

액세스 역할

콘솔은 조직의 구성원에게 할당할 수 있는 액세스 역할을 제공합니다.

구성원에게 역할을 연결할 때, 해당 역할을 조직 전체, 특정 폴더 또는 특정 프로젝트에 대해 부여할 수 있습니다. 선택한 역할은 해당 계층 구조의 선택한 부분에 있는 리소스에 대한 권한을 구성원에게 부여합니다.

NetApp Console "최소 권한" 원칙을 준수하는 세분화된 역할을 제공합니다. 즉, 액세스 역할은 사용자가 필요한 기능에만 접근할 수 있도록 설계되었습니다.

이는 사용자의 업무 범위가 확장됨에 따라 여러 역할을 부여받을 수 있음을 의미합니다.

"액세스 역할에 대해 알아보세요" .

IAM 전략 사례

소규모 조직 전략

사용자 수가 50명 미만이고 스토리지 관리가 중앙 집중식으로 이루어지는 조직의 경우, 슈퍼 관리자 및 슈퍼 뷰어 역할을 사용하는 간소화된 접근 방식을 고려해 보세요.

예시**: ABC** 회사 **(5**인 팀**)**

- 구조**:** 3개의 프로젝트(운영, 개발, 백업)를 보유한 단일 조직
- 역할**:**
  - 2명의 고위 멤버: 완전한 관리자 권한을 가진 슈퍼 관리자 역할
  - 팀 구성원 3명: 수정 권한 없이 모니터링만 가능한 슈퍼 뷰어 역할
- 에이전트 전략**:** 모든 프로젝트에 연결된 단일 에이전트를 사용하여 공유 리소스에 액세스합니다.
- 장점**:** 관리 간소화, 역할 복잡성 감소, 광범위한 접근 권한이 필요한 팀에 적합

다지역 기업 전략

지역별 운영 및 전문 팀을 보유한 대규모 조직의 경우, 지리적 또는 사업부 경계를 나타내는 폴더를 사용하는 계층적 접근 방식을 구현하십시오.

예시**: XYZ** 주식회사**(**다국적 기업**)**

- 구조**:** 조직 > 지역별 폴더(북미, 유럽, 아시아 태평양) > 지역별 프로젝트 폴더
- 플랫폼 역할**:**
  - 1. 조직 관리: 글로벌 총괄 및 정책 관리
  - 3 폴더 또는 프로젝트 관리자: 지역별 관리 (지역당 1명)
  - 1. 연합 관리: 기업 ID 공급자 통합
- 지역별 스토리지 역할**:**
  - 9 스토리지 관리자: 지정된 지역의 스토리지 시스템을 검색하고 관리합니다.
  - 2. 스토리지 뷰어: 여러 지역의 스토리지 리소스를 모니터링합니다.
  - 1. 시스템 상태 전문가: 시스템 수정 없이 스토리지 상태를 관리합니다.
- 데이터 서비스 역할**:**
  - 백업 및 복구 관리자: 백업 책임 범위에 따라 프로젝트별로 책정됩니다.
  - 랜섬웨어 복원력 관리자: 프로젝트 전반에 걸친 보안 팀 모니터링
- 에이전트 전략**:** 해당 지역 프로젝트에 적합한 지역 에이전트를 배정합니다.
- 장점**:** 역할 분리, 지역 자율성 및 현지 규정 준수를 통한 보안 강화

학과별 전문화 전략

특정 데이터 서비스 접근 권한이 필요한 전문 팀을 보유한 조직의 경우, 기능적 책임에 기반한 맞춤형 역할 할당을 활용하십시오.

예시**: TechCorp (**중견 기술 기업**)**

- 구조**:** 조직 > 부서 폴더(IT, 보안, 개발) > 프로젝트별 리소스
- 전문적인 역할**:**
  - 보안팀: 랜섬웨어 복원력 관리자 및 분류 보기 담당자 역할
  - 백업 팀: 포괄적인 백업 작업을 위한 백업 및 복구 최고 관리자

    - 개발팀: 테스트 환경 관리를 위한 저장소 관리자
    - 규정 준수 팀: 모니터링 및 지원 사례 관리를 담당할 운영 지원 분석가
- 에이전트 전략**:** 리소스 소유권을 기반으로 부서 프로젝트에 에이전트를 연결합니다.
- 장점**:** 맞춤형 접근 제어, 운영 효율성 향상, 전문 업무에 대한 명확한 책임 소재 규명

NetApp Console 에서 IAM 관련 다음 단계

- "NetApp Console 에서 IAM 시작하기"
- "IAM 활동 모니터링 또는 감사"
- "NetApp Console IAM에 대한 API에 대해 알아보세요"

NetApp Console 에서 ID 및 액세스 시작하기

NetApp Console 에 가입하면 새 조직을 만들라는 메시지가 표시됩니다. 조직에는 한 명의 구성원(조직 관리자)과 한 개의 기본 프로젝트가 포함됩니다. 비즈니스 요구 사항에 맞게 ID 및 액세스 관리(IAM)를 설정하려면 조직의 계층 구조를 사용자 지정하고, 추가 구성원을 추가하고, 리소스를 추가하거나 검색하고, 계층 구조 전반에 걸쳐 해당 리소스를 연결해야 합니다.

조직의 ID 및 액세스를 관리하려면 조직 관리자 또는 슈퍼 관리자 권한이 필요합니다. 폴더 또는 프로젝트 관리자 권한이 있으면 접근 권한이 있는 폴더와 프로젝트만 관리할 수 있습니다.

새로운 조직을 설정하려면 다음 단계를 따르세요. 순서는 조직의 요구 사항에 따라 달라질 수 있습니다.

1 기본 프로젝트를 편집하거나 조직의 계층 구조에 추가하세요**.**

기본 프로젝트를 사용하거나 비즈니스 계층 구조에 맞는 추가 프로젝트와 폴더를 만드세요.

"폴더와 프로젝트를 사용하여 리소스를 구성하는 방법을 알아보세요." .

2 귀하의 조직과 회원을 연결하세요

사용자가 NetApp Console 에 가입한 후에는 콘솔 조직에 해당 사용자를 명시적으로 추가해야 합니다. 조직에 서비스 계정을 추가하는 옵션도 있습니다.

"멤버와 멤버의 권한을 관리하는 방법을 알아보세요" .

3 리소스 추가 또는 검색

콘솔에 리소스(시스템)를 추가하거나 검색합니다. 조직 구성원은 프로젝트 내에서 시스템을 관리합니다.

리소스를 만들거나 검색하는 방법을 알아보세요.

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"

- "Cloud Volumes ONTAP"
- "E-시리즈 시스템"
- "온프레미스 ONTAP 클러스터"
- "StorageGRID"

4 추가 프로젝트와 리소스 연결

콘솔에서 시스템을 추가하거나 검색하면 해당 리소스가 현재 선택된 프로젝트와 자동으로 연결됩니다. 해당 리소스를 조직의 다른 프로젝트에서 사용할 수 있도록 하려면 해당 프로젝트와 연결하세요. 콘솔 에이전트를 사용하여 리소스를 관리하는 경우 콘솔 에이전트를 해당 프로젝트와 연결합니다.

- "조직의 리소스 계층을 관리하는 방법을 알아보세요" .
- "콘솔 에이전트를 폴더 또는 프로젝트와 연결하는 방법을 알아보세요." .

관련 정보

- "NetApp Console 에서 ID 및 액세스 관리에 대해 알아보세요"
- "ID 및 액세스를 위한 API에 대해 알아보세요"

콘솔 구성을 설정하세요

NetApp Console 조직에 폴더와 프로젝트를 추가하세요.

비즈니스 구조에 맞게 폴더와 프로젝트를 추가하세요. 폴더와 프로젝트를 생성한 후에는 해당 폴더에 리소스를 연결하고 프로젝트에 대한 구성원의 액세스 권한을 관리할 수 있습니다.

콘솔은 새 조직을 생성할 때 자동으로 하나의 프로젝트를 생성합니다. 대부분의 조직은 하나 이상의 프로젝트를 필요로 하며, 자료를 정리하기 위한 폴더도 필요합니다. "NetApp Console 의 리소스 계층 구조에 대해 알아보세요.".

폴더와 프로젝트를 사용하여 리소스를 정리하세요

NetApp Console 에서 조직은 리소스를 구성하는 데 도움이 되는 폴더와 프로젝트로 구성됩니다. 폴더를 사용하면 관련 프로젝트를 그룹화할 수 있고, 프로젝트를 사용하면 리소스와 구성원 접근 권한을 관리할 수 있습니다.

폴더

폴더는 관련된 프로젝트를 정리하는 데 도움이 됩니다. 조직 구조의 다양한 계층을 나타내기 위해 중첩 폴더를 만들 수 있습니다. 예를 들어, 각 사업부별로 최상위 폴더를 만들고 그 안에 해당 사업부 내의 여러 팀별로 하위 폴더를 만들 수 있습니다. 그다음에는 폴더 안에 프로젝트를 생성합니다.

폴더를 사용하면 역할 상속을 통해 구성원 접근 권한을 더욱 효율적으로 관리할 수 있습니다. 폴더 수준에서 멤버에게 역할을 할당하면 해당 멤버는 모든 하위 프로젝트 및 폴더에 대한 권한을 상속받습니다.

ⓘ 폴더는 조직 관리를 위한 도구이며, 조직 관리자, 폴더 관리자, 프로젝트 관리자 또는 슈퍼 관리자 역할과 같은 IAM 권한이 없는 구성원에게는 표시되지 않습니다. 회원은 폴더가 아닌 프로젝트에 접근할 수 있습니다.

조직 관리자는 폴더를 생성하여 관리 책임을 위임할 수 있습니다. 폴더를 생성한 후, 조직 관리자는 특정 폴더에 대해

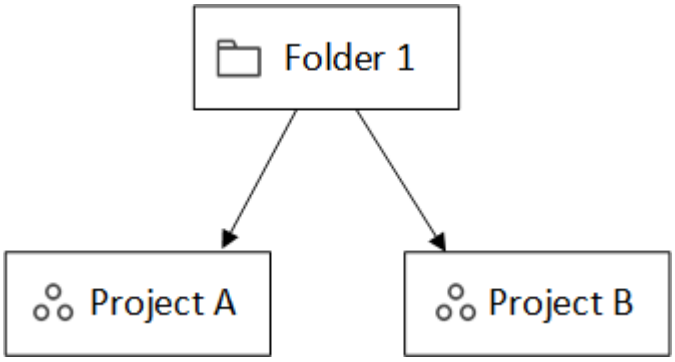
구성원에게 폴더 관리자 또는 프로젝트 관리자 역할을 할당할 수 있습니다. 이러한 구성원들은 전체 조직에 대한 접근 권한 없이도 해당 폴더 내의 모든 프로젝트를 관리할 수 있습니다.

폴더는 다른 폴더나 프로젝트를 하위 폴더로 포함할 수 있지만, 리소스를 직접적으로 연결할 수는 없습니다. 리소스는 프로젝트와 연관되어야 합니다.

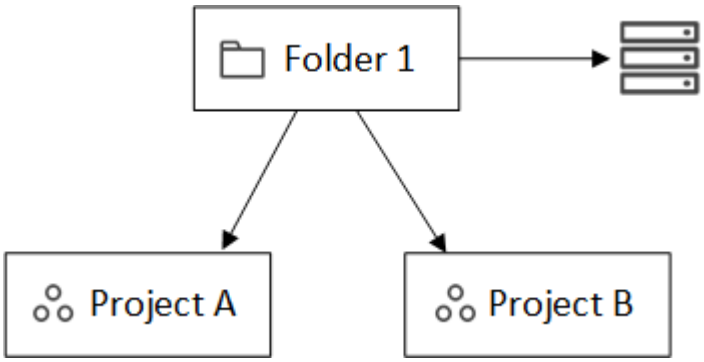
리소스를 폴더와 연결할 때

_조직 관리자_는 리소스를 폴더와 연결할 수 있으므로 _폴더 또는 프로젝트 관리자_는 이를 폴더 내의 적절한 프로젝트에 연결할 수 있습니다.

예를 들어, 두 개의 프로젝트가 포함된 폴더가 있다고 가정해 보겠습니다.

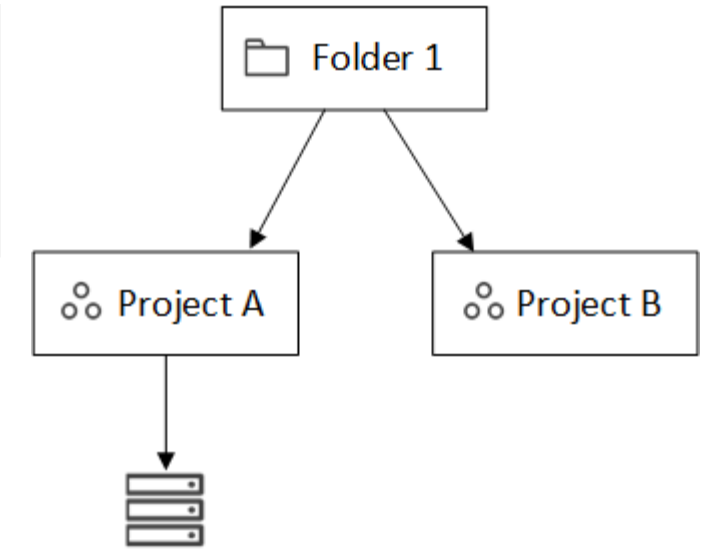


_조직 관리자_는 리소스를 폴더와 연결할 수 있습니다.



리소스를 폴더와 연결해도 모든 프로젝트에서 액세스할 수 있는 것은 아닙니다. 폴더 또는 프로젝트 관리자만 볼 수 있습니다. _폴더 또는 프로젝트 관리자_는 어떤 프로젝트가 액세스할 수 있는지 결정하고 리소스를 적절한 프로젝트와 연결합니다.

이 예에서 관리자는 리소스를 프로젝트 A와 연결합니다.



프로젝트 A에 대한 권한이 있는 멤버는 이제 리소스에 액세스할 수 있습니다.

프로젝트

구성원이 리소스를 관리할 수 있도록 리소스와 프로젝트를 연결하세요. 리소스는 관리 및 사용자 접근을 위해 프로젝트와 연결되어야 합니다.

조직은 하나 또는 여러 개의 프로젝트를 가질 수 있습니다. 프로젝트는 조직 바로 아래에 있거나 폴더 안에 있을 수 있습니다. 프로젝트 내 리소스를 검색하는 데 에이전트를 사용하는 경우 해당 에이전트를 프로젝트와 연결해야 합니다.

사용자는 시스템 페이지에서 할당된 프로젝트 간을 탐색하여 각 프로젝트와 관련된 리소스를 관리할 수 있습니다.

폴더 또는 프로젝트 추가

프로젝트를 추가하여 리소스를 관리하고, 폴더를 추가하여 관련 프로젝트를 그룹화하세요. 새 조직을 생성하면 콘솔에 프로젝트 하나가 포함됩니다.

조직의 리소스 구조에서 최대 7단계의 폴더와 프로젝트를 생성할 수 있습니다. 필요에 따라 하위 폴더를 만들어 리소스를 정리하세요.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *조직*을 선택하세요.
3. 조직 페이지에서 *폴더 또는 프로젝트 추가*를 선택합니다.
4. 폴더 또는 *프로젝트*를 선택하세요.
5. 폴더 또는 프로젝트 세부 정보를 입력하세요:
    - 이름 및 위치: 폴더 또는 프로젝트의 이름을 입력하고 위치를 선택하세요. 폴더나 프로젝트는 조직 아래에 또는 다른 폴더 안에 배치할 수 있습니다.
    - 리소스: 이 폴더 또는 프로젝트와 연결할 리소스를 선택하세요. 콘솔에 스토리지 시스템을 아직 추가하지 않았다면 나중에 이 단계를 진행할 수 있습니다.

구성원은 해당 리소스가 프로젝트에 할당되기 전까지는 폴더 내의 리소스에 접근할 수 없습니다. 필요한 프로젝트를 만들 때까지 리소스를 임시로 보관하려면 폴더를 사용하세요. 이 기능을 통해 조직 관리자는 리소스 할당을 폴더 또는 프로젝트 관리자에게 위임할 수 있으며, 폴더 또는 프로젝트 관리자는 해당 폴더 내의 프로젝트에 리소스를 할당할 수 있습니다.

- 접근 권한: *멤버 추가*를 선택하여 접근 권한과 역할을 할당하세요. 프로젝트 또는 폴더에서 언제든지 구성원을 추가하거나 삭제할 수 있습니다.

  "액세스 역할에 대해 알아보세요" .

6. *추가*를 선택하세요.

폴더 또는 프로젝트 이름 바꾸기

필요에 따라 폴더 또는 프로젝트 이름을 변경하세요. 이름 변경은 관련 리소스나 회원 접근 권한에 영향을 미치지 않습니다.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
2. 편집 페이지에서 새 이름을 입력하고 *적용*을 선택합니다.

폴더 또는 프로젝트 삭제

팀 재편성이나 프로젝트 완료 후 더 이상 필요하지 않은 폴더와 프로젝트를 삭제하세요.

폴더나 프로젝트를 삭제하기 전에 해당 폴더에 리소스가 포함되어 있지 않은지 확인하십시오. 리소스를 제거하는 방법을 알아보세요.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 *삭제*를 선택하세요.
2. 폴더나 프로젝트를 삭제할지 확인하세요.

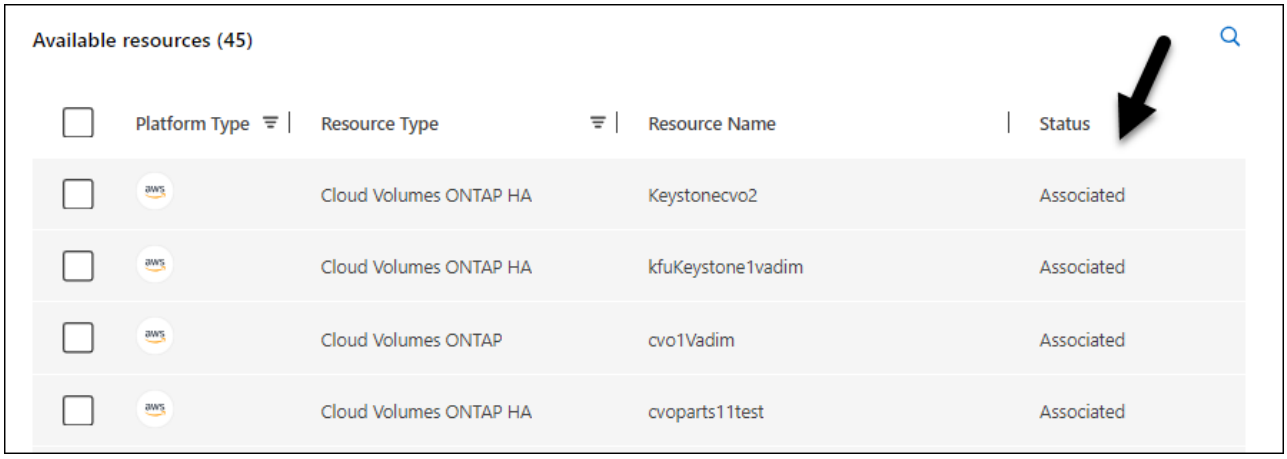
폴더 또는 프로젝트와 관련된 리소스 보기

폴더나 프로젝트와 연관된 리소스와 멤버를 확인하세요.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.

2. 편집 페이지에서 리소스 또는 액세스 섹션을 확장하여 선택한 폴더나 프로젝트에 대한 세부 정보를 볼 수 있습니다.
   - 연관된 리소스를 보려면 리소스*를 선택하세요. 표에서 *상태 열은 폴더나 프로젝트와 연관된 리소스를 식별합니다.



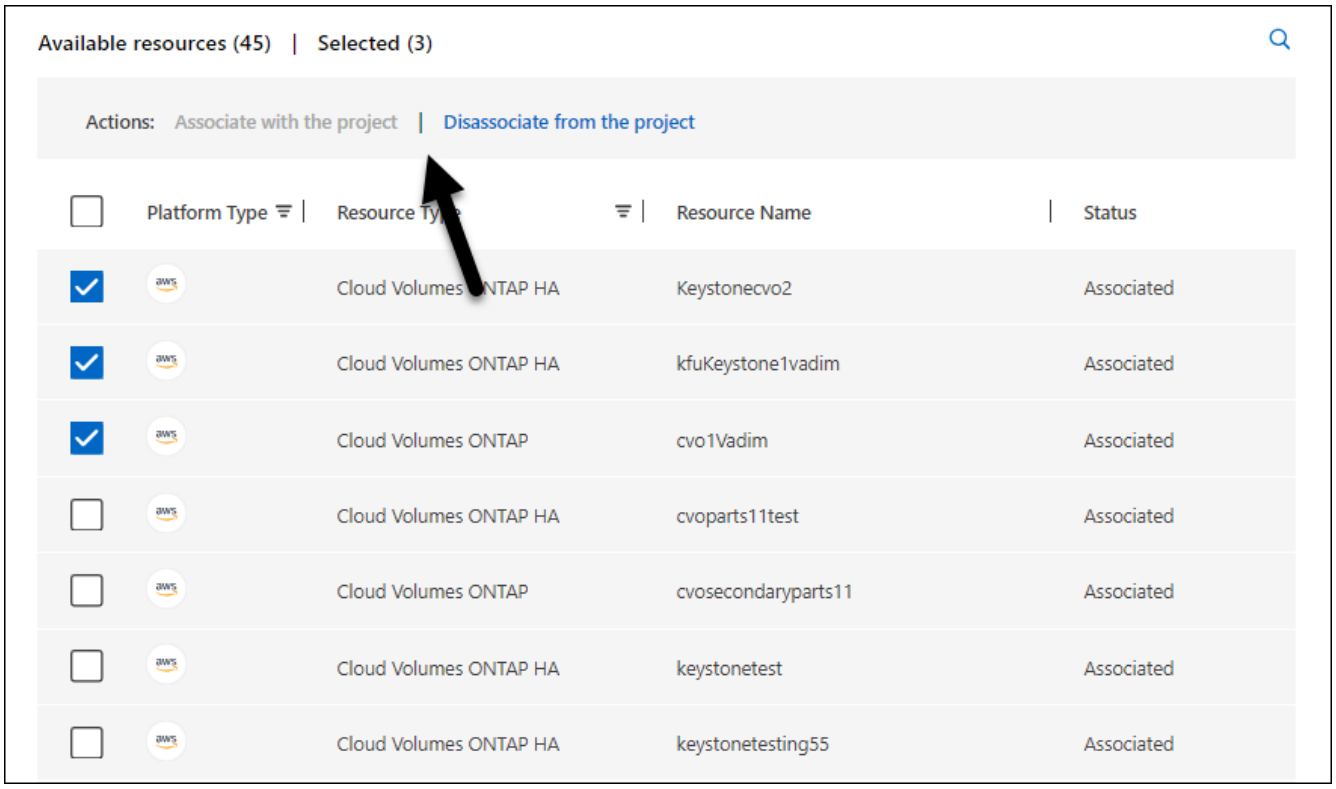
폴더 또는 프로젝트와 관련된 리소스를 변경합니다.

조직의 요구 사항이 변경됨에 따라 폴더 또는 프로젝트와 연결된 리소스를 변경할 수 있습니다.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
2. 편집 페이지에서 *리소스*를 선택합니다.

   표에서 상태 열은 폴더나 프로젝트와 연관된 리소스를 식별합니다.
3. 연결하거나 연결 해제할 리소스를 선택하세요.
4. 선택한 리소스를 기반으로 프로젝트에 연결 또는 *프로젝트에서 연결 해제*를 선택하십시오.



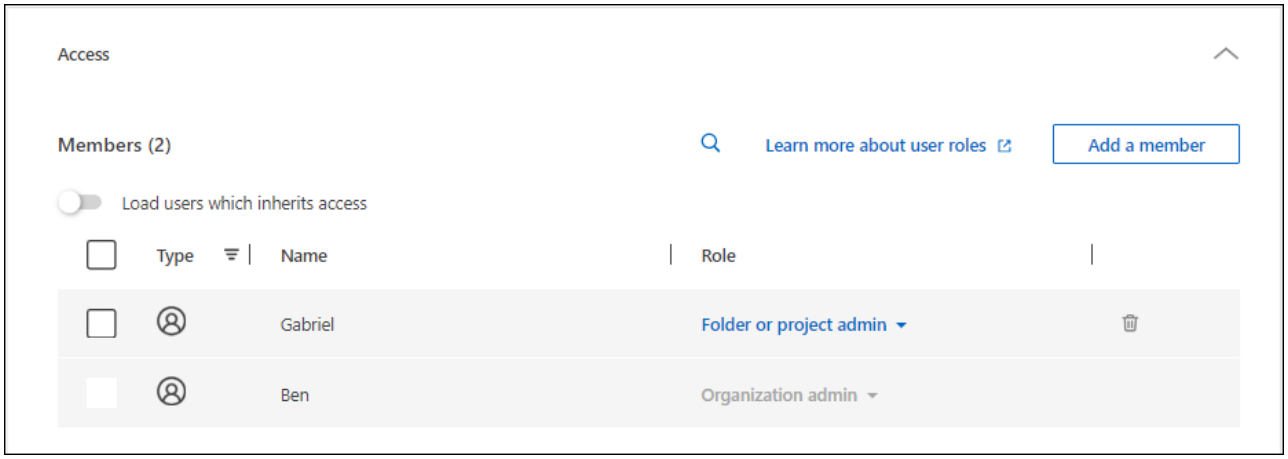
5. *적용*을 선택하세요.

폴더 또는 프로젝트와 연관된 멤버 보기

조직 페이지에서 폴더 또는 프로젝트와 관련된 구성원을 볼 수 있습니다.

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
2. 편집 페이지에서 *액세스*를 선택하면 선택한 폴더나 프로젝트에 액세스할 수 있는 멤버 목록을 볼 수 있습니다.
   - 폴더나 프로젝트에 접근할 수 있는 멤버를 보려면 *접근*을 선택하세요.



폴더 또는 프로젝트에 대한 멤버 액세스 수정

리소스 접근을 제어하려면 멤버 접근 권한을 수정하세요. 폴더 수준에서 할당된 역할은 모든 하위 프로젝트 및 폴더에 상속된다는 점을 기억하십시오.

폴더 또는 조직 수준에서 상속된 구성원 액세스 권한은 하위 수준에서 변경할 수 없습니다. 상위 계층에서 구성원의 권한을 변경하여 접근 권한을 변경하세요. 또는 다음과 같은 방법도 있습니다. "회원 페이지에서 권한 관리".

단계

1. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
2. 편집 페이지에서 *액세스*를 선택하면 선택한 폴더나 프로젝트에 액세스할 수 있는 멤버 목록을 볼 수 있습니다.
3. 멤버 접근 권한 수정:
   - 멤버 추가: 폴더나 프로젝트에 추가하려는 멤버를 선택하고 역할을 할당합니다.
   - 멤버 역할 변경: 조직 관리자 이외의 역할을 가진 멤버의 경우 기존 역할을 선택한 다음 새 역할을 선택합니다.
   - 멤버 접근 권한 제거: 보고 있는 폴더나 프로젝트에 역할이 정의된 멤버의 경우, 해당 접근 권한을 제거할 수 있습니다.
4. *적용*을 선택하세요.

관련 정보

- "NetApp Console 에서 ID 및 액세스에 대해 알아보세요"
- "신원 및 액세스 시작하기"
- "ID 및 액세스 API에 대해 알아보세요"

NetApp Console 에서 폴더 및 프로젝트에 리소스를 추가합니다.

NetApp Console 조직의 프로젝트 및 폴더에 사용자를 추가하여 리소스에 대한 사용자 액세스를 제어하십시오. 프로젝트 수준에서 사용자에게 액세스 권한을 부여하세요.

리소스는 콘솔이 인식하는 엔티티로, 스토리지 리소스, 콘솔 에이전트 또는 백업 및 복구 워크로드 등이 있습니다.

콘솔의 리소스 페이지에서 리소스를 보고 관리할 수 있습니다.

콘솔 리소스 유형

NetApp Console 조직의 프로젝트에는 여러 유형의 리소스를 연결할 수 있습니다.

저장 리소스

스토리지 리소스는 조직에서 가장 일반적인 리소스 유형이며 온프레미스 스토리지 시스템과 클라우드 스토리지 시스템을 모두 포함합니다. 콘솔에 스토리지 시스템을 추가할 때 폴더 또는 프로젝트에 추가할 수 있습니다. 그때까지 콘솔은 해당 항목을 발견되지 않은 것으로 표시하고 리소스 페이지에 표시하지 않습니다.

콘솔 에이전트

콘솔 에이전트를 사용하여 스토리지 시스템을 검색한 경우, 해당 에이전트를 동일한 폴더 또는 프로젝트에 추가하십시오. 이를 통해 사용자는 데이터 서비스 또는 콘솔 기본 스토리지 관리와 같은 에이전트 지원 기능을 수행할 수 있습니다. 콘솔의 에이전트 페이지에서 폴더 또는 프로젝트에 에이전트를 추가할 수 있습니다. "콘솔

에이전트를 폴더 또는 프로젝트와 연결하는 방법을 알아보세요.".

Keystone 구독

조직에 Keystone 구독이 있는 경우 리소스 페이지에서 확인할 수 있습니다. Keystone 구독을 폴더 또는 프로젝트와 연결하여 해당 폴더 또는 프로젝트에 대한 권한이 있는 구성원에게 액세스 권한을 부여할 수 있습니다.

귀하의 조직의 리소스를 확인하세요

귀하의 조직과 관련된 발견된 리소스와 발견되지 않은 리소스를 모두 볼 수 있습니다. 시스템은 스토리지 리소스를 찾고 사용자가 콘솔에 추가할 때까지 해당 리소스를 검색되지 않은 상태로 표시합니다.

콘솔에서는 사용자가 해당 리소스를 역할과 연결할 수 없기 때문에 리소스 페이지에서 Amazon FSx for NetApp ONTAP 리소스를 제외합니다. 이러한 리소스는 시스템 페이지 또는 워크로드에서 확인할 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *리소스*를 선택하세요.
3. *고급 검색 및 필터링*을 선택하세요.
4. 제공되는 옵션을 활용하여 필요한 자료를 찾아보세요.
   - 리소스 이름으로 검색: 텍스트 문자열을 입력하고 *추가*를 선택합니다.
   - 플랫폼: Amazon Web Services 등 하나 이상의 플랫폼을 선택하세요.
   - 리소스: Cloud Volumes ONTAP 과 같은 하나 이상의 리소스를 선택합니다.
   - 조직, 폴더 또는 프로젝트: 전체 조직, 특정 폴더 또는 특정 프로젝트를 선택합니다.
5. *검색*을 선택하세요.

리소스를 폴더 및 프로젝트와 연결

리소스를 폴더 또는 프로젝트에 연결하면 해당 폴더 또는 프로젝트에 대한 권한이 있는 구성원만 해당 리소스를 사용할 수 있습니다.

단계

1. 리소스 페이지에서 표의 리소스로 이동하여 다음을 선택합니다. ••• 그런 다음 *폴더 또는 프로젝트에 연결*을 선택합니다.
2. 폴더나 프로젝트를 선택한 다음 *수락*을 선택하세요.
3. 추가 폴더나 프로젝트를 연결하려면 *폴더 또는 프로젝트 추가*를 선택한 다음 폴더나 프로젝트를 선택합니다.

   관리자 권한이 있는 폴더와 프로젝트에서만 선택할 수 있습니다.

4. *리소스 연결*을 선택하세요.
   - 리소스와 프로젝트를 연결한 경우 해당 프로젝트에 대한 권한이 있는 멤버는 이제 콘솔에서 리소스에 액세스할 수 있습니다.
   - 리소스를 폴더와 연결한 경우, 폴더 또는 프로젝트 관리자는 이제 리소스에 액세스하여 폴더 내의 프로젝트와 연결할 수 있습니다. "리소스를 폴더와 연결하는 방법에 대해 알아보세요".

당신이 완료한 후

콘솔 에이전트를 사용하여 리소스를 발견한 경우 콘솔 에이전트를 프로젝트와 연결하여 액세스 권한을 부여합니다. 그렇지 않으면 조직 관리자 역할이 없는 구성원은 콘솔 에이전트와 관련 리소스에 액세스할 수 없습니다.

"콘솔 에이전트를 폴더 또는 프로젝트와 연결하는 방법을 알아보세요.".

리소스와 연관된 폴더 및 프로젝트 보기

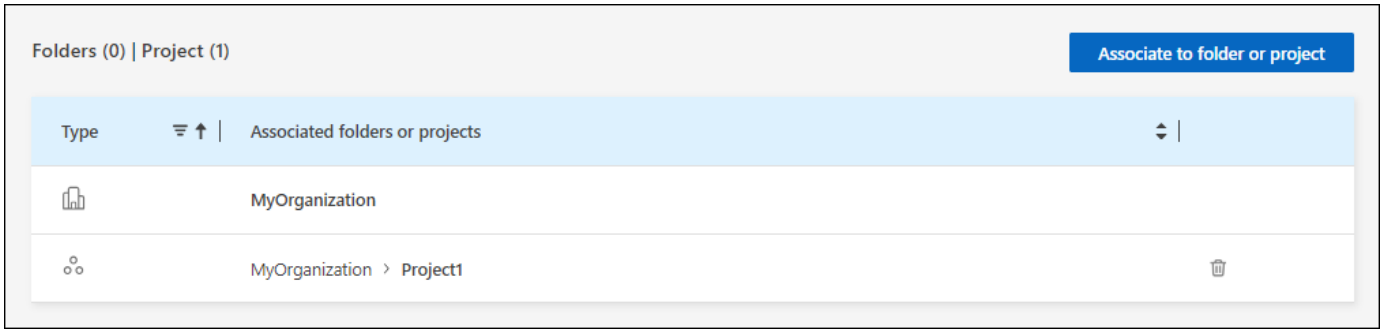
특정 리소스와 관련된 폴더와 프로젝트를 볼 수 있습니다.

리소스에 액세스할 수 있는 조직 구성원을 찾아야 하는 경우 다음을 수행할 수 있습니다."리소스와 연관된 폴더 및 프로젝트에 액세스할 수 있는 멤버를 봅니다." .

단계

1. 리소스 페이지에서 표의 리소스로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.

다음 예에서는 하나의 프로젝트와 연관된 리소스를 보여줍니다.



어떤 조직 구성원이 해당 리소스에 접근할 수 있는지 확인하려면,"관련 폴더 및 프로젝트에 대한 액세스 권한이 있는 구성원을 봅니다." .

폴더 또는 프로젝트에서 리소스 제거

폴더 또는 프로젝트에서 리소스를 제거하려면 해당 리소스와의 연결을 제거하십시오. 이렇게 하면 구성원이 해당 폴더 또는 프로젝트의 리소스를 관리할 수 없게 됩니다.

검색된 리소스를 조직 전체에서 제거하려면 시스템 페이지로 이동하여 해당 시스템을 제거하십시오.

단계

1. 리소스 페이지에서 표의 리소스로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.
2. 폴더 또는 프로젝트에서 리소스를 제거하려면 다음을 선택하세요. 폴더 또는 프로젝트 옆에 있습니다.
3. 연결을 제거하려면 *삭제*를 선택하세요.

관련 정보

- "NetApp Console 에서 ID 및 액세스에 대해 알아보세요"
- "NetApp Console 에서 ID 및 액세스 시작하기"

- "ID 및 액세스를 위한 API에 대해 알아보세요"

콘솔 에이전트를 다른 폴더 및 프로젝트와 연결합니다.

콘솔 에이전트를 특정 프로젝트와 연결하여 리소스 관리 및 데이터 서비스 액세스를 활성화하십시오. 콘솔 에이전트를 통해 검색된 리소스는 팀 액세스를 위해 해당 리소스와 에이전트가 동일한 프로젝트에 연결되어 있어야 합니다.

최고 관리자 및 조직 관리자는 에이전트를 생성하고 모든 에이전트를 모든 프로젝트 또는 폴더와 연결할 수 있습니다. 폴더 또는 프로젝트 관리자는 자신이 권한을 가진 폴더 및 프로젝트에만 기존 에이전트를 연결할 수 있습니다. "_폴더 또는 프로젝트 관리자_가 완료할 수 있는 작업에 대해 자세히 알아보세요.".

단계

1. 관리 **> ID** 및 액세스 > *에이전트*를 선택합니다.
2. 표에서 연결하려는 콘솔 에이전트를 찾으세요.

   표 위의 검색을 사용하여 특정 콘솔 에이전트를 찾거나 리소스 계층 구조로 표를 필터링하세요.
3. 콘솔 에이전트에 연결된 폴더와 프로젝트를 보려면 다음을 선택하세요. ••• 그런 다음 *세부 정보 보기*를 선택하세요.

   이 페이지에는 콘솔 에이전트와 관련된 폴더와 프로젝트에 대한 세부 정보가 표시됩니다.
4. *폴더 또는 프로젝트에 연결*을 선택합니다.
5. 폴더나 프로젝트를 선택한 다음 *수락*을 선택하세요.
6. 콘솔 에이전트를 추가 폴더나 프로젝트와 연결하려면 *폴더 또는 프로젝트 추가*를 선택한 다음 폴더나 프로젝트를 선택합니다.
7. *협력사 에이전트*를 선택하세요.

당신이 완료한 후

리소스 페이지에서 콘솔 에이전트의 리소스를 동일한 폴더 및 프로젝트와 연결합니다.

"리소스를 폴더 및 프로젝트와 연결하는 방법을 알아보세요." .

관련 정보

- "NetApp Console 에이전트에 대해 알아보세요"
- "NetApp Console ID 및 액세스 관리에 대해 알아보세요"
- "신원 및 액세스 시작하기"
- "ID 및 액세스 관리를 위한 API에 대해 알아보세요"

콘솔 조직에 사용자를 추가하세요

NetApp Console 조직에 사용자 추가

콘솔 내에서 액세스 역할에 따라 사용자에게 프로젝트 또는 폴더에 대한 액세스 권한을 부여할 수

있습니다. 액세스 역할은 구성원(사용자 또는 서비스 계정)이 리소스 계층 구조의 지정된 수준에서 특정 작업을 수행할 수 있도록 하는 권한 집합을 포함합니다.

필수 접근 권한 역할

최고 관리자, 조직 관리자 또는 폴더/프로젝트 관리자(해당 폴더 및 프로젝트를 관리하는 경우에 한함). "액세스 역할에 대해 알아보세요".

NetApp Console 에서 액세스 권한이 부여되는 방식을 이해하십시오**.**

NetApp Console 역할 기반 액세스 제어(RBAC)를 사용하여 권한을 관리합니다. 사용자에게 개별적으로 또는 연합 그룹을 통해 역할을 할당합니다. 각 역할은 특정 리소스에 대해 허용되는 작업을 정의합니다.

NetApp Console 에서 액세스 권한을 부여할 때 다음 사항에 유의하십시오.

- 모든 사용자는 리소스에 액세스하기 전에 먼저 NetApp Console 에 가입해야 합니다.
- 콘솔에서 각 사용자가 리소스에 액세스하려면 해당 사용자에게 명시적으로 역할을 할당해야 합니다. 이는 역할이 할당된 연합 그룹의 구성원인 경우에도 마찬가지입니다.
- 콘솔에서 직접 서비스 계정을 추가하고 역할을 할당할 수 있습니다.

조직에 구성원 추가

NetApp Console 사용자 계정, 서비스 계정 및 페더레이션 그룹의 세 가지 유형의 멤버를 지원합니다.

연합 그룹에 속해 있더라도 사용자를 추가하고 역할을 할당하려면 먼저 NetApp Console 에 가입해야 합니다. 콘솔에서 직접 서비스 계정을 생성하세요.

모든 구성원은 리소스에 접근하기 위해 최소한 하나의 역할이 명시적으로 할당되어 있어야 합니다.

멤버를 추가할 때는 리소스 수준(조직, 폴더 또는 프로젝트)을 선택하고 필요한 권한이 있는 역할을 할당하세요.

사용자 추가

사용자는 NetApp Console 에 가입하지만, 조직 관리자, 폴더 관리자 또는 프로젝트 관리자가 해당 사용자를 조직, 폴더 또는 프로젝트에 추가해야 리소스에 액세스할 수 있습니다.

시작하기 전에**:**

사용자는 이미 NetApp Console 에 가입되어 있어야 합니다. 아직 가입하지 않았다면, 가입 페이지로 안내해 주세요. "NetApp Console 에 가입하세요."

연합 그룹에 속한 사용자를 추가하는 경우, 해당 사용자가 이미 NetApp Console 에 가입되어 있고 콘솔에서 명시적으로 역할을 할당받았는지 확인하십시오. NetApp 조직 뷰어와 같은 최소 액세스 역할을 할당하는 것을 권장합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. *멤버 추가*를 선택하세요.
4. *회원 유형*에서 *사용자*를 선택된 상태로 둡니다.

5. *사용자 이메일*에는 사용자가 만든 로그인과 연결된 이메일 주소를 입력합니다.
6. 조직, 폴더 또는 프로젝트 선택 섹션을 사용하여 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

   다음 사항에 유의하세요.

   - 권한이 있는 폴더와 프로젝트만 선택할 수 있습니다.
   - 조직이나 폴더를 선택하면 해당 구성원에게 모든 콘텐츠에 대한 접근 권한이 부여됩니다.
   - 조직 관리자 역할은 조직 수준에서만 할당할 수 있습니다.
7. 카테고리를 선택한 다음 해당 조직, 폴더 또는 프로젝트에 연결된 리소스에 대한 권한을 멤버에게 제공하는 *역할*을 선택합니다.

   "액세스 역할에 대해 알아보세요" .
8. 더 많은 폴더, 프로젝트 또는 역할에 대한 액세스 권한을 부여하려면 *역할 추가*를 선택하고 폴더, 프로젝트 또는 역할 범주를 선택한 다음 역할을 선택하세요.
9. *추가*를 선택하세요.

   콘솔은 사용자에게 이메일로 지침을 보냅니다.

서비스 계정 추가

서비스 계정을 사용하면 작업을 자동화하고 콘솔 API에 안전하게 연결할 수 있습니다. 간단한 설정을 위해서는 클라이언트 ID와 암호를 선택하고, 자동화 환경이나 클라우드 네이티브 환경에서 보안을 강화하려면 JWT(JSON Web Token)를 선택하십시오. 보안 요구 사항에 맞는 방법을 선택하십시오.

시작하기 전에:

JWT 인증을 위해서는 공개 키 또는 인증서를 준비하십시오.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. *멤버 추가*를 선택하세요.
4. *회원 유형*에서 *서비스 계정*을 선택하세요.
5. 서비스 계정의 이름을 입력하세요.
6. JWT 인증을 사용하려면 *개인 키 JWT 인증 사용*을 선택하고 공개 RSA 키 또는 인증서를 업로드하세요. 클라이언트 ID와 시크릿을 사용하는 경우 이 단계를 건너뛰세요.

   귀하의 X.509 인증서. PEM, CRT 또는 CER 형식이어야 합니다.

   a. 인증서 만료 알림을 설정하세요. 7일 또는 30일 중에서 선택하세요. 만료 알림은 슈퍼 관리자 또는 조직 관리자 역할을 가진 사용자에게 이메일로 전송되고 콘솔에 표시됩니다.
7. 조직, 폴더 또는 프로젝트 선택 섹션을 사용하여 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

   다음 사항에 유의하세요.

   - 권한이 있는 폴더와 프로젝트에서만 선택할 수 있습니다.

- 조직이나 폴더를 선택하면 구성원에게 해당 조직의 모든 내용에 대한 권한이 부여됩니다.
- 조직 관리자 역할은 조직 수준에서만 할당할 수 있습니다.

8. 범주를 선택한 다음, 선택한 조직, 폴더 또는 프로젝트의 리소스에 대한 권한을 구성원에게 부여할 역할(Role)을 선택하십시오.

   "액세스 역할에 대해 알아보세요" .

9. 더 많은 폴더, 프로젝트 또는 역할에 대한 액세스 권한을 부여하려면 *역할 추가*를 선택하고 폴더, 프로젝트 또는 역할 범주를 선택한 다음 역할을 선택하세요.
10. JWT 인증을 사용하지 않기로 선택한 경우 클라이언트 ID와 클라이언트 비밀번호를 다운로드하거나 복사하세요.

    콘솔에는 클라이언트 비밀 키가 한 번만 표시됩니다. 안전하게 복사해 두세요. 나중에 분실하더라도 다시 만들 수 있습니다.

11. JWT 인증을 선택한 경우 클라이언트 ID와 JWT 대상 그룹을 다운로드하거나 복사하십시오. 콘솔에는 이 정보가 한 번만 표시되며, 이후에는 다시 불러올 수 없습니다.
12. *닫기*를 선택하세요.

조직에 연합 그룹을 추가하세요

ID 공급자(IdP)에서 페더레이션 그룹을 조직에 추가하고 하나 이상의 역할을 할당할 수 있습니다. 연합 그룹의 구성원은 콘솔에서 그룹에 할당한 역할을 상속받습니다.

연합 그룹에 역할을 할당하기 전에 다음 사항을 확인하십시오.

- IdP와 콘솔 간의 페더레이션을 설정하십시오. "연합 설정 방법을 알아보세요."
- 해당 그룹은 이미 IdP에 존재해야 하며 콘솔에 대한 앱 액세스 권한이 할당되어 있어야 합니다.
- 해당 그룹에 속한 사용자는 NetApp Console 에 이미 가입되어 있어야 하며 콘솔에서 명시적으로 역할을 할당받아야 합니다. NetApp 조직 뷰어와 같은 최소 액세스 역할을 할당하는 것을 권장합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. *멤버 추가*를 선택하세요.
4. *회원 유형*에서 *연합 그룹*을 선택하십시오.
5. 해당 그룹이 소속된 연맹을 선택하세요.
6. *그룹 이름*에는 IdP에 등록된 그룹의 정확한 이름을 입력하세요.
7. 조직, 폴더 또는 프로젝트 선택 섹션을 사용하여 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

   다음 사항에 유의하세요.

   - 권한이 있는 폴더와 프로젝트에서만 선택할 수 있습니다.
   - 조직이나 폴더를 선택하면 구성원에게 해당 조직의 모든 내용에 대한 권한이 부여됩니다.
   - 조직 관리자 역할은 조직 수준에서만 할당할 수 있습니다.

8. 범주를 선택한 다음, 선택한 조직, 폴더 또는 프로젝트의 리소스에 대한 권한을 구성원에게 부여할 역할(Role)을 선택하십시오.

   "액세스 역할에 대해 알아보세요" .

9. 더 많은 폴더, 프로젝트 또는 역할에 대한 액세스 권한을 부여하려면 *역할 추가*를 선택하고 폴더, 프로젝트 또는 역할 범주를 선택한 다음 역할을 선택하세요.

관련 정보

- "NetApp Console 에서 ID 및 액세스 관리에 대해 알아보세요"
- "신원 및 액세스 시작하기"
- "NetApp Console 액세스 역할"
- "ID 및 액세스를 위한 API에 대해 알아보세요"

사용자 접근 권한 및 보안 관리

NetApp Console 역할 기반 액세스 제어**(RBAC)**에 대해 알아보세요**.**

역할 기반 액세스 제어(RBAC)를 사용하여 NetApp Console 에 대한 사용자 액세스를 관리하고, 조직, 폴더 또는 프로젝트 수준에서 미리 정의된 역할을 할당할 수 있습니다. 각 역할은 사용자가 할당된 범위 내에서 수행할 수 있는 작업을 정의하는 특정 권한을 부여합니다.

NetApp 최소 권한 원칙에 따라 콘솔 역할을 설계하므로 각 역할에는 해당 작업에 필요한 권한만 포함됩니다. 이러한 접근 방식은 각 구성원에게 필요한 권한만 허용함으로써 보안을 강화합니다.

리소스를 폴더와 프로젝트로 정리한 후에는 조직 구성원에게 특정 폴더 또는 프로젝트에 대한 역할을 할당하여 각자가 자신의 책임만 수행할 수 있도록 하세요.

예를 들어, 특정 프로젝트 수준에 대해 구성원에게 랜섬웨어 복원력 관리자 역할을 할당하여 해당 프로젝트 내의 리소스에 대한 랜섬웨어 복원력 작업을 수행할 수 있도록 허용하되, 조직 전체에 대한 광범위한 액세스 권한은 부여하지 않을 수 있습니다. 이 사용자는 조직 내 여러 프로젝트에 대해 동일한 역할을 부여받을 수 있습니다.

사용자의 책임에 따라 동일한 범위 또는 서로 다른 범위에 대해 여러 역할을 할당할 수 있습니다. 예를 들어, 소규모 조직에서는 동일한 사용자가 조직 차원에서 랜섬웨어 복원력과 백업 및 복구 작업을 모두 관리할 수 있는 반면, 대규모 조직에서는 프로젝트 차원에서 각 역할에 서로 다른 사용자를 할당할 수 있습니다.

콘솔 조직 구성원의 유형

NetApp Console 조직에는 세 가지 유형의 구성원이 있습니다. * 사용자 계정: 리소스를 관리하기 위해 NetApp Console 에 로그인하는 개별 사용자입니다. 사용자를 조직에 추가하려면 먼저 NetApp Console 에 가입해야 합니다. * 서비스 계정: 애플리케이션 또는 서비스가 API를 통해 NetApp Console 과 상호 작용하는 데 사용하는 비인간 계정입니다. 콘솔 조직에 서비스 계정을 직접 추가할 수 있습니다. * 연합 그룹: ID 공급자(IdP)에서 동기화된 그룹으로, 여러 사용자의 액세스 권한을 일괄적으로 관리할 수 있습니다. 연합 그룹 내의 각 사용자는 그룹에 부여된 리소스에 액세스하기 전에 NetApp Console 에 가입하고 액세스 역할을 통해 조직에 추가되어야 합니다.

"조직에 구성원을 추가하는 방법을 알아보세요."

NetApp Console 의 사전 정의된 역할

NetApp Console 조직 구성원에게 할당할 수 있는 사전 정의된 역할이 포함되어 있습니다. 각 역할에는 구성원이 할당된 범위(조직, 폴더 또는 프로젝트) 내에서 수행할 수 있는 작업을 지정하는 권한이 포함되어 있습니다.

NetApp Console 역할은 최소 권한 원칙을 사용하여 구성원이 작업에 필요한 권한만 갖도록 보장하며, 제공하는 액세스 유형에 따라 역할을 분류합니다.

- 플랫폼 역할: 콘솔 관리 권한 제공
- 데이터 서비스 역할: 랜섬웨어 복원력 및 백업/복구와 같은 특정 데이터 서비스를 관리하기 위한 권한을 제공합니다.
- 애플리케이션 역할: 스토리지 관리 및 콘솔 이벤트와 알림 감사에 대한 권한을 제공합니다.

구성원의 책임에 따라 여러 역할을 할당할 수 있습니다. 예를 들어 특정 프로젝트에 대해 멤버에게 랜섬웨어 복원력 관리자 역할과 백업 및 복구 관리자 역할을 모두 할당할 수 있습니다.

"NetApp Console 에서 사용 가능한 사전 정의된 역할에 대해 알아보세요.".

NetApp Console 에서 멤버 액세스를 관리하세요

콘솔 조직에서 구성원 액세스를 관리하세요. 권한을 설정하려면 역할을 할당하세요. 회원이 탈퇴하면 명단에서 삭제합니다.

필수 접근 권한 역할

최고 관리자, 조직 관리자 또는 폴더/프로젝트 관리자(해당 폴더 및 프로젝트를 관리하는 경우에 한함). 링크:reference-iam-predefined-roles.html[접근 권한 역할에 대해 알아보세요].

프로젝트 또는 폴더 단위로 액세스 역할을 할당할 수 있습니다. 예를 들어, 특정 두 프로젝트에 대해 사용자에게 역할을 할당하거나, 폴더 수준에서 역할을 할당하여 해당 폴더 내의 모든 프로젝트에 대해 사용자에게 랜섬웨어 복원력 관리자 역할을 부여할 수 있습니다.

사용자에게 접근 권한을 부여하기 전에 폴더와 프로젝트를 추가하세요. "폴더와 프로젝트를 추가하는 방법을 알아보세요."

NetApp Console 에서 액세스 권한이 부여되는 방식을 이해하십시오.

NetApp Console 역할 기반 접근 제어(RBAC) 모델을 사용하여 사용자 권한을 관리합니다. 구성원에게 개별적으로 또는 연합 그룹을 통해 미리 정의된 역할을 할당할 수 있습니다. 서비스 계정 및 연합 그룹에 역할을 추가하고 할당할 수 있습니다. 각 역할은 구성원이 관련 리소스에서 수행할 수 있는 작업을 정의합니다.

NetApp Console 에서 액세스 권한을 부여할 때 다음 사항에 유의하십시오.

- 모든 사용자는 리소스에 대한 액세스 권한을 부여받기 전에 먼저 NetApp Console 에 가입해야 합니다.
- 콘솔에서 각 사용자가 리소스에 액세스하려면 해당 사용자에게 명시적으로 역할을 할당해야 합니다. 이는 역할이 할당된 연합 그룹의 구성원인 경우에도 마찬가지입니다.
- 콘솔에서 직접 서비스 계정을 추가하고 역할을 할당할 수 있습니다.

역할 상속 사용

NetApp Console 에서 조직, 폴더 또는 프로젝트 수준에서 역할을 할당하면 선택한 범위 내의 모든 리소스가 해당

역할을 자동으로 상속받습니다. 예를 들어, 폴더 수준 역할은 해당 폴더에 포함된 모든 프로젝트에 적용되는 반면, 프로젝트 수준 역할은 해당 프로젝트 내의 모든 리소스에 적용됩니다.

조직 구성원 보기

조직의 리소스 계층 구조에서 다양한 수준에서 멤버에게 할당된 역할을 보면 멤버에게 어떤 리소스와 권한이 제공되는지 파악할 수 있습니다."역할을 사용하여 콘솔 리소스에 대한 액세스를 제어하는 방법을 알아보세요."

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.

   구성원 표에는 조직의 구성원이 나열됩니다.

3. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.

멤버에게 할당된 역할 보기

현재 그들에게 어떤 역할이 부여되었는지 확인할 수 있습니다.

폴더 또는 프로젝트 관리자 역할이 있는 경우 해당 페이지에는 조직의 모든 구성원이 표시됩니다. 하지만 권한이 있는 폴더와 프로젝트에 대해서만 멤버 권한을 보고 관리할 수 있습니다. "_폴더 또는 프로젝트 관리자_가 완료할 수 있는 작업에 대해 자세히 알아보세요." .

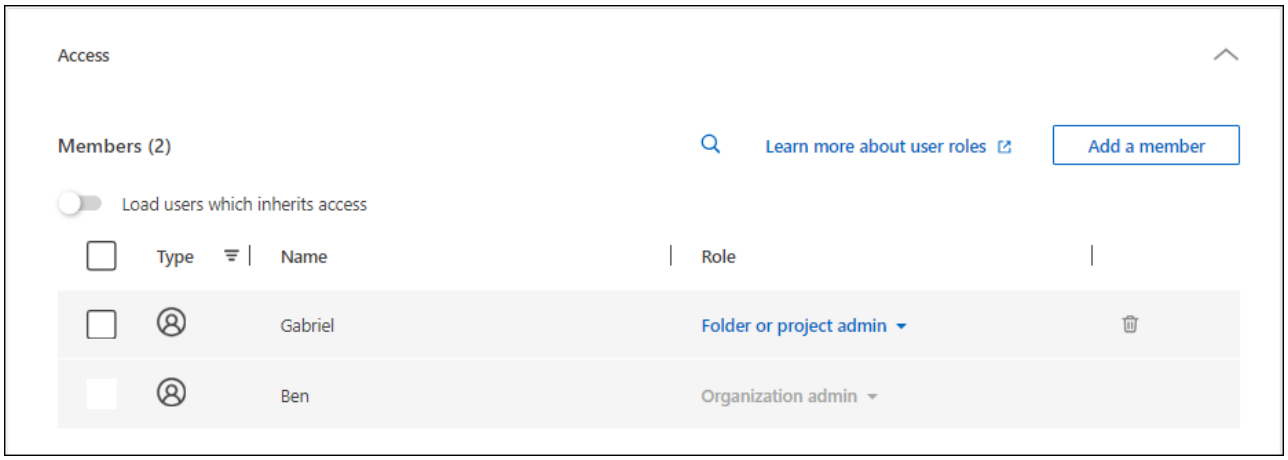
1. 회원 페이지에서 표에 있는 회원을 찾아 선택하세요. ••• 그런 다음 *세부 정보 보기*를 선택하세요.
2. 표에서 멤버에게 할당된 역할을 보고 싶은 조직, 폴더 또는 프로젝트에 해당하는 행을 확장하고 역할 열에서 *보기*를 선택합니다.

폴더 또는 프로젝트와 연관된 멤버 보기

특정 폴더 또는 프로젝트에 대한 접근 권한이 있는 구성원을 확인할 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *조직*을 선택하세요.
3. 조직 페이지에서 표의 프로젝트나 폴더로 이동하여 다음을 선택합니다. ••• 그런 다음 폴더 편집 또는 *프로젝트 편집*을 선택합니다.
   - 폴더나 프로젝트에 접근할 수 있는 멤버를 보려면 *접근*을 선택하세요.



멤버 접근 권한을 할당하거나 수정합니다.

사용자가 NetApp Console 에 가입하면 해당 사용자를 조직에 추가하고 리소스에 대한 액세스 권한을 부여하는 역할을 할당할 수 있습니다. "조직에 구성원을 추가하는 방법을 알아보세요."

필요에 따라 역할을 추가하거나 삭제하여 구성원의 접근 권한을 조정할 수 있습니다.

멤버에게 액세스 역할 추가

일반적으로 조직에 구성원을 추가할 때 역할을 할당하지만, 역할을 제거하거나 추가하여 언제든지 역할을 업데이트할 수 있습니다.

사용자에게 조직, 폴더 또는 프로젝트에 대한 액세스 역할을 할당할 수 있습니다.

구성원은 동일한 프로젝트 내에서 또는 서로 다른 프로젝트에서 여러 역할을 맡을 수 있습니다. 예를 들어, 소규모 조직에서는 사용 가능한 모든 접근 권한을 동일한 사용자에게 할당할 수 있는 반면, 대규모 조직에서는 사용자가 보다 전문화된 작업을 수행하도록 할 수 있습니다. 또는 조직 차원에서 한 사용자에게 랜섬웨어 복원력 관리자 역할을 부여할 수도 있습니다. 이 예시에서 사용자는 조직 내 모든 프로젝트에 대해 랜섬웨어 복원력 작업을 수행할 수 있습니다.

액세스 역할 전략은 NetApp 리소스를 구성한 방식과 일치해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. 사용자, 서비스 계정, 또는 연합 그룹 탭 중 하나를 선택하세요.
4. 작업 메뉴를 선택하세요 ••• 역할을 할당하려는 구성원 옆에 있는 *역할 추가*를 선택합니다.
5. 역할을 추가하려면 대화 상자의 단계를 완료하세요.
   - 조직, 폴더 또는 프로젝트 선택: 멤버에게 권한이 부여되어야 하는 리소스 계층 수준을 선택합니다.

     조직이나 폴더를 선택하면 해당 구성원은 해당 조직이나 폴더 내에 있는 모든 항목에 대한 권한을 갖게 됩니다.
   - 카테고리 선택: 역할 카테고리를 선택하세요. "액세스 역할에 대해 알아보세요" .
   - 역할 선택: 선택한 조직, 폴더 또는 프로젝트와 관련된 리소스에 대한 권한을 멤버에게 제공하는 역할을 선택합니다.

◦ 역할 추가: 조직 내 추가 폴더나 프로젝트에 대한 액세스 권한을 제공하려면 *역할 추가*를 선택하고 다른 폴더나 프로젝트 또는 역할 범주를 지정한 다음 역할 범주와 해당 역할을 선택합니다.

6. *새로운 역할 추가*를 선택하세요.

멤버의 할당된 역할 변경

멤버의 역할을 변경하여 접근 권한을 업데이트하세요.

사용자에게는 최소한 하나의 역할이 할당되어야 합니다. 사용자에게서 모든 역할을 제거할 수는 없습니다. 모든 역할을 제거해야 하는 경우 조직에서 해당 사용자를 삭제해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. 사용자, 서비스 계정, 또는 연합 그룹 탭 중 하나를 선택하세요.
4. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *세부정보 보기*를 선택하세요.
5. 표에서 멤버에게 할당된 역할을 변경하려는 조직, 폴더 또는 프로젝트에 해당하는 행을 확장하고 역할 열에서 *보기*를 선택하여 이 멤버에게 할당된 역할을 확인합니다.
6. 멤버의 기존 역할을 변경하거나 역할을 제거할 수 있습니다.
   a. 멤버의 역할을 변경하려면 변경하려는 역할 옆에 있는 *변경*을 선택하세요. 동일한 역할 범주 내에서만 역할을 변경할 수 있습니다. 예를 들어, 한 데이터 서비스 역할에서 다른 역할로 변경할 수 있습니다. 변경 사항을 확인하세요.
   b. 멤버의 역할을 해제하려면 다음을 선택하세요. 역할 옆에 있는 버튼을 클릭하면 해당 멤버에게서 해당 역할을 제거할 수 있습니다. 삭제를 확인하라는 메시지가 표시됩니다.

조직에서 구성원 제거

구성원이 조직을 떠나면 명단에서 제외하세요.

멤버를 제거하면 시스템에서 해당 멤버의 콘솔 권한은 취소되지만 콘솔 및 NetApp 지원 사이트 계정은 유지됩니다.

연합 회원

- 페더레이션된 사용자는 IdP에서 제거되면 NetApp Console 에 대한 액세스 권한을 자동으로 잃게 됩니다. 하지만 멤버 목록을 최신 상태로 유지하려면 콘솔 조직에서 해당 사용자를 제거해야 합니다.
- IdP에서 페더레이션 그룹에서 사용자를 제거하면 해당 그룹과 연결된 콘솔 액세스 권한을 잃게 됩니다. 하지만 콘솔에서 명시적으로 할당된 역할과 관련된 접근 권한은 여전히 유지됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. 사용자, 서비스 계정, 또는 연합 그룹 탭 중 하나를 선택하세요.
4. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *사용자 삭제*를 선택하세요.
5. 조직에서 해당 구성원을 제거할 것인지 확인하세요.

사용자 보안

멤버 보안 설정을 관리하여 NetApp Console 조직에 대한 사용자 액세스를 보호하십시오. 사용자 암호를 재설정하고, 다단계 인증(MFA)을 관리하고, 서비스 계정 자격 증명을 다시 생성할 수 있습니다.

필수 접근 권한 역할

최고 관리자, 조직 관리자 또는 폴더/프로젝트 관리자(해당 폴더 및 프로젝트를 관리하는 경우에 한함). 링크:reference-iam-predefined-roles.html[접근 권한 역할에 대해 알아보세요].

사용자 비밀번호 재설정 (로컬 사용자만 해당)

조직 관리자는 로컬 사용자의 비밀번호를 재설정할 수 없습니다. 하지만 사용자에게 직접 비밀번호를 재설정하도록 안내할 수는 있습니다.

콘솔 로그인 페이지에서 *비밀번호를 잊으셨습니까?*를 선택하여 비밀번호를 재설정하도록 사용자에게 안내합니다.

이 옵션은 연합 조직의 사용자에게는 제공되지 않습니다.

사용자의 다중 인증 요소(MFA) 관리

사용자가 MFA 장치에 대한 액세스 권한을 잃은 경우 MFA 구성을 제거하거나 비활성화할 수 있습니다.

다중 요소 인증은 로컬 사용자에게만 제공됩니다. 페더레이션 사용자는 MFA를 활성화할 수 없습니다.

사용자는 MFA를 제거한 후 로그인할 때 다시 설정해야 합니다. 사용자가 일시적으로 MFA 장치에 접근할 수 없게 된 경우, 저장된 복구 코드를 사용하여 로그인할 수 있습니다.

복구 코드가 없는 경우 MFA를 일시적으로 비활성화하여 로그인을 허용합니다. 사용자의 MFA를 비활성화하면 8시간 동안만 비활성화되고 그 후 자동으로 다시 활성화됩니다. 사용자는 해당 기간 동안 MFA 없이 한 번만 로그인할 수 있습니다. 8시간이 지나면 사용자는 MFA를 사용하여 로그인해야 합니다.

사용자의 다중 요소 인증을 관리하려면 영향을 받는 사용자와 동일한 도메인에 이메일 주소가 있어야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.

   구성원 표에는 조직의 구성원이 나열됩니다.

3. 회원 페이지에서 테이블의 회원으로 이동하여 다음을 선택합니다. ••• 그런 다음 *다중 인증 관리*를 선택하세요.
4. 사용자의 MFA 구성을 제거할지 또는 비활성화할지 선택합니다.

서비스 계정의 자격 증명을 다시 만듭니다.

서비스 자격 증명을 분실했거나 업데이트해야 하는 경우 새 자격 증명을 만들 수 있습니다.

새 자격 증명을 생성하면 이전 자격 증명이 삭제됩니다. 기존 계정 정보는 사용할 수 없습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *회원*을 선택하세요.
3. 멤버 테이블에서 서비스 계정으로 이동하여 다음을 선택합니다. ••• 그런 다음 *비밀 다시 만들기*를 선택하세요.
4. *다시 만들기*를 선택하세요.
5. 클라이언트 ID와 클라이언트 비밀번호를 다운로드하거나 복사하세요.

   콘솔에는 클라이언트 비밀 키가 한 번만 표시됩니다. 파일을 복사하거나 다운로드하여 안전한 곳에 보관하십시오.

NetApp Console 액세스 역할

NetApp Console 액세스 역할에 대해 알아보세요

NetApp Console 의 IAM(ID 및 액세스 관리)은 리소스 계층의 다양한 수준에서 조직 구성원에게 할당할 수 있는 미리 정의된 역할을 제공합니다. 이러한 역할을 할당하기 전에 각 역할에 포함된 권한을 이해해야 합니다. 역할은 플랫폼, 애플리케이션, 데이터 서비스라는 범주로 나뉩니다.

플랫폼 역할

플랫폼 역할은 역할 할당 및 사용자 관리를 포함한 NetApp Console 관리 권한을 부여합니다. 콘솔에는 여러 가지 플랫폼 역할이 있습니다.

플랫폼 역할	책임
"조직 관리자"	사용자에게 조직 내의 모든 프로젝트와 폴더에 대한 제한 없는 액세스를 허용하고, 모든 프로젝트나 폴더에 멤버를 추가하고, 명시적인 역할이 지정되지 않은 모든 작업을 수행하고 모든 데이터 서비스를 사용할 수 있도록 허용합니다. 이 역할을 가진 사용자는 폴더와 프로젝트를 만들고, 역할을 할당하고, 사용자를 추가하고, 적절한 자격 증명이 있는 경우 시스템을 관리하여 조직을 관리합니다. 이는 콘솔 에이전트를 생성할 수 있는 유일한 액세스 역할입니다.
"폴더 또는 프로젝트 관리자"	사용자에게 할당된 프로젝트와 폴더에 대한 제한 없는 액세스를 허용합니다. 자신이 관리하는 폴더나 프로젝트에 멤버를 추가할 수 있고, 할당된 폴더나 프로젝트 내의 리소스에 대한 모든 작업을 수행하고 모든 데이터 서비스나 애플리케이션을 사용할 수 있습니다. 폴더 또는 프로젝트 관리자는 콘솔 에이전트를 생성할 수 없습니다.
"연방 관리자"	사용자가 콘솔을 사용하여 페더레이션을 만들고 관리할 수 있으며, 이를 통해 SSO(Single Sign-On)가 가능합니다.
"연방 뷰어"	사용자가 콘솔을 사용하여 기존 페더레이션을 볼 수 있도록 합니다. 연합을 생성하거나 관리할 수 없습니다.
"파트너십 관리자"	사용자가 파트너십을 만들고 관리할 수 있습니다.
"파트너십 뷰어"	사용자가 기존 파트너십을 볼 수 있도록 합니다. 파트너십을 생성하거나 관리할 수 없습니다.

플랫폼 역할	책임
"슈퍼 관리자"	사용자에게 관리자 역할의 하위 집합을 제공합니다. 이 역할은 여러 사용자에게 콘솔 책임을 분산할 필요가 없는 소규모 조직을 위해 설계되었습니다.
"슈퍼 뷰어"	사용자에게 하위 집합의 뷰어 역할을 제공합니다. 이 역할은 여러 사용자에게 콘솔 책임을 분산할 필요가 없는 소규모 조직을 위해 설계되었습니다.

애플리케이션 역할

다음은 애플리케이션 카테고리의 역할 목록입니다. 각 역할은 지정된 범위 내에서 특정 권한을 부여합니다. 필요한 애플리케이션이나 플랫폼 역할이 없는 사용자는 해당 애플리케이션에 액세스할 수 없습니다.

신청 역할	책임
"Google Cloud NetApp Volumes 관리자"	Google Cloud NetApp Volumes 역할이 있는 사용자는 Google Cloud NetApp Volumes 검색하고 관리할 수 있습니다.
"Google Cloud NetApp Volumes 뷰어"	Google Cloud NetApp Volumes 사용자 역할이 있는 사용자는 Google Cloud NetApp Volumes 볼 수 있습니다.
"Keystone 관리자"	Keystone 관리자 역할이 있는 사용자는 서비스 요청을 생성할 수 있습니다. 사용자가 액세스하는 Keystone 테넌트 내에서 사용량, 리소스 및 관리자 세부 정보를 모니터링하고 볼 수 있습니다.
"Keystone 뷰어"	Keystone 뷰어 역할이 있는 사용자는 서비스 요청을 생성할 수 없습니다. 사용자가 액세스하는 Keystone 테넌트 내에서 소비량, 자산 및 관리 정보를 모니터링하고 볼 수 있습니다.
ONTAP Mediator 설정 역할	ONTAP Mediator 설정 역할이 있는 서비스 계정은 서비스 요청을 생성할 수 있습니다. 이 역할은 서비스 계정에서 인스턴스를 구성하는 데 필요합니다 ."ONTAP 클라우드 중재자" .
"운영 지원 분석가"	알림 및 모니터링 도구에 대한 액세스를 제공하고 지원 사례를 입력 및 관리하는 기능을 제공합니다.
"스토리지 관리자"	스토리지 상태 및 거버넌스 기능을 관리하고, 스토리지 리소스를 검색하고, 기존 시스템을 수정 및 삭제합니다.
"스토리지 뷰어"	저장소 상태 및 거버넌스 기능을 확인하고, 이전에 검색된 저장소 리소스를 확인합니다. 기존 스토리지 시스템을 검색, 수정 또는 삭제할 수 없습니다.
"시스템 건강 전문가"	저장소 및 상태, 거버넌스 기능을 관리합니다. 저장소 관리자의 모든 권한은 기존 시스템을 수정하거나 삭제할 수 없습니다.

데이터 서비스 역할

다음은 데이터 서비스 범주의 역할 목록입니다. 각 역할은 지정된 범위 내에서 특정 권한을 부여합니다. 필요한 데이터 서비스 역할이나 플랫폼 역할이 없는 사용자는 데이터 서비스에 액세스할 수 없습니다.

데이터 서비스 역할	책임
"백업 및 복구 슈퍼 관리자"	NetApp Backup and Recovery 에서 모든 작업을 수행합니다.
"백업 및 복구 관리자"	로컬 스냅샷에 백업을 수행하고, 보조 저장소에 복제하고, 개체 저장소에 백업합니다.
"백업 및 복구 복원 관리자"	백업 및 복구에서 작업 부하를 복원합니다.

데이터 서비스 역할	책임
"백업 및 복구 클론 관리자"	백업 및 복구에서 애플리케이션과 데이터를 복제합니다.
"백업 및 복구 뷰어"	백업 및 복구 정보를 확인합니다.
"재해 복구 관리자"	NetApp Disaster Recovery 서비스에서 모든 작업을 수행합니다.
"재해 복구 장애 조치 관리자"	장애 조치 및 마이그레이션을 수행합니다.
"재해 복구 애플리케이션 관리자"	복제 계획을 만들고, 복제 계획을 변경하고, 테스트 장애 조치를 시작합니다.
"재해 복구 뷰어"	정보만 보기.
분류 뷰어	사용자가 NetApp Data Classification 검사 결과를 볼 수 있습니다. 이 역할이 있는 사용자는 규정 준수 정보를 보고 액세스 권한이 있는 리소스에 대한 보고서를 생성할 수 있습니다. 이러한 사용자는 볼륨, 버킷 또는 데이터베이스 스키마의 스캐닝을 활성화하거나 비활성화할 수 없습니다. 분류에는 관리자 역할이 없습니다.
"랜섬웨어 복원력 관리자"	NetApp Ransomware Resilience 의 보호, 알림, 복구, 설정 및 보고서 탭에서 작업을 관리합니다.
"랜섬웨어 복원력 뷰어"	Ransomware Resilience에서 작업 부하 데이터를 보고, 알림 데이터를 보고, 복구 데이터를 다운로드하고, 보고서를 다운로드하세요.
"랜섬웨어 복원력 사용자 행동 관리자"	Ransomware Resilience에서 의심스러운 사용자 동작 탐지, 알림 및 모니터링을 구성, 관리하고 확인하세요.
"랜섬웨어 복원력 사용자 동작 뷰어"	랜섬웨어 복원력에서 의심스러운 사용자 행동 알림과 통찰력을 확인하세요.
SnapCenter 관리자	NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 클러스터의 스냅샷을 애플리케이션에 백업하는 기능을 제공합니다. 이 역할이 있는 멤버는 다음 작업을 완료할 수 있습니다. * 백업 및 복구 > 애플리케이션에서 모든 작업을 완료합니다. * 권한이 있는 프로젝트 및 폴더의 모든 시스템을 관리합니다. * 모든 NetApp Console 서비스를 사용합니다. SnapCenter 에는 뷰어 역할이 없습니다.

관련 링크

- "NetApp Console ID 및 액세스 관리에 대해 알아보세요"
- "NetApp Console IAM 시작하기"
- "NetApp Console 멤버 및 해당 권한 관리"
- "NetApp Console IAM에 대한 API에 대해 알아보세요"

NetApp Console 플랫폼 액세스 역할

사용자에게 플랫폼 역할을 할당하여 NetApp Console 관리, 역할 할당, 사용자 추가, 콘솔 에이전트 생성, 페더레이션 관리 권한을 부여합니다.

대규모 다국적 기업의 조직 역할에 대한 예

XYZ Corporation은 북미, 유럽, 아시아 태평양 등 지역별로 데이터 저장소 액세스를 구성하여 중앙 집중식 감독을 통해 지역적 제어를 제공합니다.

XYZ Corporation 콘솔의 *조직 관리자*는 각 지역에 대한 초기 조직과 별도 폴더를 만듭니다. 각 지역의 *폴더 또는 프로젝트 관리자*는 해당 지역의 폴더 내에서 프로젝트(관련 리소스 포함)를 구성합니다.

폴더 또는 프로젝트 관리자 역할을 맡은 지역 관리자는 리소스와 사용자를 추가하여 폴더를 적극적으로 관리합니다. 이러한 지역 관리자는 자신이 관리하는 폴더와 프로젝트를 추가, 제거 또는 이름을 바꿀 수도 있습니다. *조직 관리자*는 모든 새 리소스에 대한 권한을 상속받아 조직 전체의 저장소 사용량을 파악할 수 있습니다.

동일한 조직 내에서 한 명의 사용자에게 회사 IdP와의 조직 연합을 관리하는 연합 관리자 역할이 할당됩니다. 이 사용자는 연합 조직을 추가하거나 제거할 수 있지만, 조직 내의 사용자나 리소스를 관리할 수는 없습니다. 조직 관리자 *는 사용자에게 *연합 뷰어 역할을 할당하여 연합 상태를 확인하고 연합 조직을 볼 수 있도록 합니다.

다음 표는 각 콘솔 플랫폼 역할이 수행할 수 있는 작업을 나타냅니다.

조직 관리 역할

일	조직 관리자	폴더 또는 프로젝트 관리자
에이전트 생성	예	아니요
콘솔에서 시스템 생성, 수정 또는 삭제(시스템 추가 또는 검색)	예	예
폴더 및 프로젝트 생성, 삭제 포함	예	아니요
기존 폴더 및 프로젝트 이름 바꾸기	예	예
역할 할당 및 사용자 추가	예	예
리소스를 폴더 및 프로젝트와 연결	예	예
폴더 및 프로젝트와 에이전트 연결	예	아니요
폴더 및 프로젝트에서 에이전트 제거	예	아니요
에이전트 관리(인증서, 설정 등 편집)	예	아니요
관리 > 자격 증명에서 자격 증명을 관리합니다.	예	예
연합을 생성, 관리 및 보기	예	아니요
콘솔을 통해 지원을 등록하고 사례를 제출하세요.	예	예
명시적 액세스 역할과 연결되지 않은 데이터 서비스를 사용하세요.	예	예
감사 페이지 및 알림 보기	예	예

연방 역할

일	연방 관리자	연방 뷰어
연방을 만드세요	예	아니요
도메인 확인	예	아니요
페더레이션에 도메인 추가	예	아니요
페더레이션 비활성화 및 삭제	예	아니요
테스트 연합	예	아니요
연합 및 세부 정보 보기	예	예

파트너십 역할

일	파트너십 관리자	파트너십 뷰어
파트너십을 만들 수 있습니다	예	아니요
파트너 멤버에게 역할 할당	예	아니요
파트너십에 멤버를 추가할 수 있습니다	예	아니요
조직 파트너십 세부 정보를 볼 수 있습니다.	예	예

슈퍼 관리자 및 뷰어 역할

슈퍼 관리자 역할은 콘솔 기능, 저장소 및 데이터 서비스를 관리할 수 있는 전체 액세스 권한을 제공합니다. 이 역할은 행정과 거버넌스를 감독하는 사람에게 적합합니다. 이와 대조적으로, 슈퍼 뷰어 역할은 읽기 전용 액세스를 제공하므로 변경하지 않고도 가시성이 필요한 감사자나 이해 관계자에게 이상적입니다.

조직에서는 보안 위험을 최소화하고 최소 권한 원칙을 준수하기 위해 슈퍼 관리자 권한을 아껴서 사용해야 합니다. 대부분의 조직에서는 위험을 줄이고 감사 가능성을 높이기 위해 필요한 권한만 부여한 세분화된 역할을 할당해야 합니다.

슈퍼 역할에 대한 예

ABC Corporation은 데이터 서비스와 스토리지 관리를 위해 NetApp Console 활용하는 5명으로 구성된 소규모 팀을 보유하고 있습니다. 여러 역할을 분산하는 대신, 사용자 관리 및 리소스 구성을 포함한 모든 관리 작업을 처리하는 두 명의 상임 팀원에게 슈퍼 관리자 역할을 할당합니다. 나머지 3명의 팀원에게는 슈퍼 뷰어 역할이 할당되어 설정을 수정하지 않고도 저장소 상태와 데이터 서비스 상태를 모니터링할 수 있습니다.

역할	상속된 역할
슈퍼 관리자	• 조직 관리자 • 폴더 또는 프로젝트 관리자 • 연방 관리자 • 파트너십 관리자 • 랜섬웨어 복원력 관리자 • 재해 복구 관리 • 백업 슈퍼 관리자 • 스토리지 관리자 • Keystone 관리자 • Google Cloud NetApp Volumes 관리자

역할	상속된 역할
슈퍼 뷰어	• 조직 뷰어 • 연방 뷰어 • 파트너십 뷰어 • 랜섬웨어 복원력 뷰어 • 재해 복구 뷰어 • 백업 뷰어 • 스토리지 뷰어 • Keystone 뷰어 • Google Cloud NetApp Volumes 뷰어

애플리케이션 역할

NetApp Console 의 Google Cloud NetApp Volumes 역할

NetApp Console 에서 Google Cloud NetApp Volumes 에 대한 액세스 권한을 제공하기 위해 사용자에게 다음 역할을 할당할 수 있습니다.

Google Cloud NetApp Volumes 다음 역할을 사용합니다.

- * Google Cloud NetApp Volumes 관리자*: 콘솔에서 Google Cloud NetApp Volumes 검색하고 관리합니다.
- * Google Cloud NetApp Volumes 뷰어*: 콘솔에서 Google Cloud NetApp Volumes 확인합니다.

NetApp Console 의 Keystone 액세스 역할

Keystone 역할은 Keystone 대시보드에 대한 액세스를 제공하고 사용자가 Keystone 구독을 보고 관리할 수 있도록 합니다. Keystone 역할에는 Keystone 관리자와 Keystone 뷰어라는 두 가지가 있습니다. 두 역할의 주요 차이점은 Keystone 에서 수행할 수 있는 작업입니다. Keystone 관리자 역할은 서비스 요청을 만들거나 구독을 수정할 수 있는 유일한 역할입니다.

NetApp Console 의 Keystone 역할에 대한 예

XYZ Corporation에는 Keystone 구독 정보를 확인하는 여러 부서의 스토리지 엔지니어가 4명 있습니다. 이러한 모든 사용자는 Keystone 구독을 모니터링해야 하지만, 서비스 요청을 할 수 있는 사람은 팀 리더뿐입니다. 팀원 3명에게는 * Keystone 뷰어* 역할이 부여되고, 팀 리더에게는 * Keystone 관리자* 역할이 부여되어 회사의 서비스 요청에 대한 통제 지점이 마련됩니다.

다음 표는 각 Keystone 역할이 수행할 수 있는 작업을 나타냅니다.

특징과 동작	Keystone 관리자	Keystone 뷰어
다음 탭을 확인하세요: 구독, 자산, 모니터 및 관리	예	예

특징과 동작	**Keystone** 관리자	**Keystone** 뷰어
* Keystone 구독 페이지*:		
구독 보기	예	예
구독 수정 또는 갱신	예	아니요
* Keystone 자산 페이지*:		
자산 보기	예	예
자산 관리	예	아니요
* Keystone 알림 페이지*:		
알림 보기	예	예
알림 관리	예	아니요
나 자신에 대한 알림 만들기	예	예
* Licenses and subscriptions*:		
라이센스 및 구독을 볼 수 있습니다	예	예
* Keystone 보고서 페이지*:		
보고서 다운로드	예	예
보고서 관리	예	예
자신을 위한 보고서 만들기	예	예
서비스 요청:		
서비스 요청 생성	예	아니요
조직 내 모든 사용자가 생성한 서비스 요청 보기	예	예

NetApp Console 에 대한 운영 지원 분석가 액세스 역할

운영 지원 분석가 역할을 사용자에게 할당하면 해당 사용자에게 알림 및 모니터링 기능에 대한 접근 권한을 부여할 수 있습니다. 이 역할을 가진 사용자는 지원 사례를 열 수도 있습니다.

운영 지원 분석가

일	수행할 수 있습니다
설정 > 자격 증명에서 자신의 사용자 자격 증명을 관리하세요.	예
발견된 리소스 보기	예
콘솔을 통해 지원을 등록하고 사례를 제출하세요.	예
감사 페이지 및 알림 보기	예
알림 보기, 다운로드 및 구성	예

NetApp Console 의 스토리지 액세스 역할

NetApp Console 에서 스토리지 관리 기능에 액세스할 수 있도록 사용자에게 다음 역할을 할당할 수 있습니다. 사용자에게 저장소를 관리하는 관리자 역할이나 모니터링을 위한 뷰어 역할을 할당할 수 있습니다.

이러한 역할은 NetApp Console 파트너십 API에서 사용할 수 없습니다.

관리자는 다음과 같은 스토리지 리소스 및 기능에 대해 사용자에게 스토리지 역할을 할당할 수 있습니다.

저장 리소스:

- 온프레미스 ONTAP 클러스터
- StorageGRID
- E-시리즈

콘솔 서비스 및 기능:

- 디지털 어드바이저
- 소프트웨어 업데이트
- 수명주기 계획
- 지속 가능성

NetApp Console 의 스토리지 역할에 대한 예

다국적 기업인 XYZ Corporation은 스토리지 엔지니어와 스토리지 관리자로 구성된 대규모 팀을 보유하고 있습니다. 이를 통해 팀은 사용자 관리, 에이전트 생성, 라이선스 관리와 같은 핵심 콘솔 작업에 대한 액세스를 제한하는 동시에 해당 지역의 스토리지 자산을 관리할 수 있습니다.

12명으로 구성된 팀 내에서 두 명의 사용자에게 저장소 뷰어 역할이 부여됩니다. 이 역할을 통해 이들은 할당된 콘솔 프로젝트와 연관된 저장 리소스를 모니터링할 수 있습니다. 나머지 9명에게는 소프트웨어 업데이트를 관리하고, 콘솔을 통해 ONTAP 시스템 관리자에 액세스하고, 스토리지 리소스를 검색(시스템 추가)하는 기능이 포함된 스토리지 관리자 역할이 부여됩니다. 팀 내 한 사람에게 시스템 상태 전문가 역할이 부여되어 해당 지역의 스토리지 리소스 상태를 관리할 수 있지만, 시스템을 수정하거나 삭제할 수는 없습니다. 이 사람은 자신에게 할당된 프로젝트의 스토리지 리소스에 대한 소프트웨어 업데이트도 수행할 수 있습니다.

조직에는 사용자 관리, 에이전트 생성, 라이선스 관리를 포함하여 콘솔의 모든 측면을 관리할 수 있는 조직 관리자

역할이 있는 두 명의 추가 사용자가 있으며, 할당된 폴더와 프로젝트에 대한 콘솔 관리 작업을 수행할 수 있는 폴더 또는 프로젝트 관리자 역할이 있는 여러 사용자가 있습니다.

다음 표는 각 저장소 역할이 수행하는 작업을 보여줍니다.

특징과 동작	스토리지 관리자	시스템 건강 전문가	스토리지 뷰어
저장 관리:			
새로운 리소스 발견(시스템 생성)	예	예	아니요
발견된 시스템 보기	예	예	아니요
콘솔에서 시스템 삭제	예	아니요	아니요
시스템 수정	예	아니요	아니요
에이전트 생성	아니요	아니요	아니요
디지털 어드바이저			
모든 페이지 및 기능 보기	예	예	예
* Licenses and subscriptions*			
모든 페이지 및 기능 보기	아니요	아니요	아니요
소프트웨어 업데이트			
랜딩 페이지와 추천 보기	예	예	예
잠재적인 버전 권장 사항과 주요 이점을 검토하세요	예	예	예
클러스터에 대한 업데이트 세부 정보 보기	예	예	예
업데이트 전 점검을 실행하고 업그레이드 계획을 다운로드하세요	예	예	예
소프트웨어 업데이트 설치	예	예	아니요
수명주기 계획			
용량 계획 상태 검토	예	예	예
다음 작업(모범 사례, 계층)을 선택하세요	예	아니요	아니요
콜드 데이터를 클라우드 스토리지로 계층화하고 스토리지를 확보하세요	예	예	아니요
알림 설정	예	예	예

특징과 동작	스토리지 관리자	시스템 건강 전문가	스토리지 뷰어
지속가능성			
대시보드 및 권장 사항 보기	예	예	예
보고서 데이터 다운로드	예	예	예
탄소 감축 비율 편집	예	예	아니요
권장 사항 수정	예	예	아니요
권장 사항을 연기하다	예	예	아니요
시스템 관리자 접근			
자격 증명을 입력할 수 있습니다	예	예	아니요
신임장			
사용자 자격 증명	예	예	아니요

데이터 서비스 역할

NetApp Console 의 **NetApp Backup and Recovery** 역할

콘솔 내에서 NetApp Backup and Recovery 에 대한 액세스 권한을 제공하기 위해 사용자에게 다음 역할을 할당할 수 있습니다. 백업 및 복구 역할을 사용하면 조직 내에서 수행해야 하는 작업에 맞는 역할을 사용자에게 할당할 수 있는 유연성이 제공됩니다. 역할을 할당하는 방법은 귀하의 사업과 스토리지 관리 관행에 따라 달라집니다.

이 서비스는 NetApp Backup and Recovery 에 특정한 다음 역할을 사용합니다.

- 백업 및 복구 슈퍼 관리자: NetApp Backup and Recovery 에서 모든 작업을 수행합니다.
- 백업 및 복구 백업 관리자: NetApp Backup and Recovery 에서 로컬 스냅샷으로 백업을 수행하고, 보조 스토리지로 복제하고, 개체 스토리지로 백업 작업을 수행합니다.
- 백업 및 복구 복원 관리자: NetApp Backup and Recovery 사용하여 워크로드를 복원합니다.
- 백업 및 복구 복제 관리자: NetApp Backup and Recovery 사용하여 애플리케이션과 데이터를 복제합니다.
- 백업 및 복구 뷰어: NetApp Backup and Recovery 에서 정보를 볼 수 있지만, 어떤 작업도 수행할 수 없습니다.

모든 NetApp Console 액세스 역할에 대한 자세한 내용은 다음을 참조하세요. "콘솔 설정 및 관리 문서" .

일반적인 작업에 사용되는 역할

다음 표는 각 NetApp Backup and Recovery 역할이 모든 워크로드에 대해 수행할 수 있는 작업을 나타냅니다.

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 클론 관리자	백업 및 복구 뷰어
호스트 추가, 편집 또는 삭제	예	아니요	아니요	아니요	아니요
플러그인 설치	예	아니요	아니요	아니요	아니요
자격 증명 추가(호스트, 인스턴스, vCenter)	예	아니요	아니요	아니요	아니요
대시보드 및 모든 탭 보기	예	예	예	예	예
무료 체험 시작	예	아니요	아니요	아니요	아니요
워크로드 검색 시작	아니요	예	예	예	아니요
라이센스 정보 보기	예	예	예	예	예
라이센스 활성화	예	아니요	아니요	아니요	아니요
호스트 보기	예	예	예	예	예
일정:					
일정 활성화	예	예	예	예	아니요
일정을 중단하다	예	예	예	예	아니요
정책 및 보호:					
보호 계획 보기	예	예	예	예	예
보호 계획 생성, 수정 또는 삭제	예	예	아니요	아니요	아니요
작업 부하 복원	예	아니요	예	아니요	아니요
클론 생성, 분할 또는 삭제	예	아니요	아니요	예	아니요
정책 생성, 수정 또는 삭제	예	예	아니요	아니요	아니요
보고서:					
보고서 보기	예	예	예	예	예
보고서 만들기	예	예	예	예	아니요

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 클론 관리자	백업 및 복구 뷰어
보고서 삭제	예	아니요	아니요	아니요	아니요
* SnapCenter 에서 가져오기 및 호스트 관리*:					
가져온 SnapCenter 데이터 보기	예	예	예	예	예
SnapCenter 에서 데이터 가져오기	예	예	아니요	아니요	아니요
호스트 관리 (마이그레이션)	예	예	아니요	아니요	아니요
설정 구성:					
로그 디렉토리 구성	예	예	예	아니요	아니요
인스턴스 자격 증명 연결 또는 제거	예	예	예	아니요	아니요
버킷:					
버킷 보기	예	예	예	예	예
버킷 생성, 편집 또는 삭제	예	예	아니요	아니요	아니요

작업별 작업에 사용되는 역할

다음 표는 각 NetApp Backup and Recovery 역할이 특정 작업 부하에 대해 수행할 수 있는 작업을 나타냅니다.

쿠버네티스 워크로드

이 표는 각 NetApp Backup and Recovery 역할이 Kubernetes 워크로드에 대한 특정 작업에 대해 수행할 수 있는 작업을 나타냅니다.

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 뷰어
클러스터, 네임스페이스, 스토리지 클래스 및 API 리소스 보기	예	예	예	예
새로운 Kubernetes 클러스터 추가	예	예	아니요	아니요
클러스터 구성 업데이트	예	아니요	아니요	아니요
관리에서 클러스터 제거	예	아니요	아니요	아니요
신청서 보기	예	예	예	예

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 뷰어
새로운 애플리케이션을 만들고 정의합니다.	예	예	아니요	아니요
애플리케이션 구성 업데이트	예	예	아니요	아니요
관리에서 애플리케이션 제거	예	예	아니요	아니요
보호된 리소스 및 백업 상태 보기	예	예	예	예
백업을 생성하고 정책을 사용하여 애플리케이션을 보호합니다.	예	예	아니요	아니요
앱 보호 해제 및 백업 삭제	예	예	아니요	아니요
복구 지점 및 리소스 뷰어 결과 보기	예	예	예	예
복구 지점에서 애플리케이션 복원	예	아니요	예	아니요
Kubernetes 백업 정책 보기	예	예	예	예
Kubernetes 백업 정책 생성	예	예	예	아니요
백업 정책 업데이트	예	예	예	아니요
백업 정책 삭제	예	예	예	아니요
실행 후크 및 후크 소스 보기	예	예	예	예
실행 후크 및 후크 소스 생성	예	예	예	아니요
실행 후크 및 후크 소스 업데이트	예	예	예	아니요
실행 후크 및 후크 소스 삭제	예	예	예	아니요
실행 후크 템플릿 보기	예	예	예	예
실행 후크 템플릿 만들기	예	예	예	아니요
실행 후크 템플릿 업데이트	예	예	예	아니요
실행 후크 템플릿 삭제	예	예	예	아니요

특징과 동작	백업 및 복구 슈퍼 관리자	백업 및 복구 백업 관리자	백업 및 복구 복원 관리자	백업 및 복구 뷰어
작업 요약 및 분석 대시보드 보기	예	예	예	예
StorageGRID 버킷 및 스토리지 대상 보기	예	예	예	예

NetApp Console 의 **NetApp Disaster Recovery** 역할

콘솔 내에서 NetApp Disaster Recovery 에 대한 액세스 권한을 제공하기 위해 사용자에게 다음 역할을 할당할 수 있습니다. 재해 복구 역할을 통해 조직 내에서 수행해야 하는 작업에 맞는 역할을 사용자에게 할당할 수 있는 유연성이 제공됩니다. 역할을 할당하는 방법은 귀하의 사업과 스토리지 관리 관행에 따라 달라집니다.

재해 복구에는 다음과 같은 역할이 사용됩니다.

- 재해 복구 관리자: 모든 작업을 수행합니다.
- 재해 복구 장애 조치 관리자: 장애 조치 및 마이그레이션을 수행합니다.
- 재해 복구 애플리케이션 관리자: 복제 계획을 만듭니다. 복제 계획을 수정합니다. 테스트 장애 조치를 시작합니다.
- 재해 복구 뷰어: 정보만 봅니다.

다음 표는 각 역할이 수행할 수 있는 작업을 나타냅니다.

특징과 동작	재해 복구 관리	재해 복구 장애 조치 관리자	재해 복구 애플리케이션 관리자	재해 복구 뷰어
대시보드 및 모든 탭 보기	예	예	예	예
무료 체험 시작	예	아니요	아니요	아니요
워크로드 검색 시작	예	아니요	아니요	아니요
라이센스 정보 보기	예	예	예	예
라이센스 활성화	예	아니요	예	아니요
사이트 탭에서:				
사이트 보기	예	예	예	예
사이트 추가, 수정 또는 삭제	예	아니요	아니요	아니요
복제 계획 탭에서:				
복제 계획 보기	예	예	예	예

특징과 동작	재해 복구 관리	재해 복구 장애 조치 관리자	재해 복구 애플리케이션 관리자	재해 복구 뷰어
복제 계획 세부 정보 보기	예	예	예	예
복제 계획을 생성하거나 수정합니다.	예	예	예	아니요
보고서 만들기	예	아니요	아니요	아니요
스냅샷 보기	예	예	예	예
장애 조치 테스트 수행	예	예	예	아니요
장애 조치 수행	예	예	아니요	아니요
장애 복구 수행	예	예	아니요	아니요
마이그레이션 수행	예	예	아니요	아니요
리소스 그룹 탭에서:				
리소스 그룹 보기	예	예	예	예
리소스 그룹 생성, 수정 또는 삭제	예	아니요	예	아니요
작업 모니터링 탭에서:				
채용공고 보기	예	아니요	예	예
작업 취소	예	예	예	아니요

NetApp Console 의 랜섬웨어 복원력 액세스 역할

랜섬웨어 복원력 역할은 사용자에게 NetApp Ransomware Resilience 에 대한 액세스 권한을 제공합니다. 랜섬웨어 복원력은 다음과 같은 역할을 지원합니다.

기준 역할

- 랜섬웨어 복원력 관리자 - 랜섬웨어 복원력 설정 구성, 암호화 경고 조사 및 대응
- 랜섬웨어 복원력 뷰어 - 암호화 사고, 보고서 및 검색 설정 보기

사용자 행동 활동 역할"의심스러운 사용자 활동 감지" 알림은 파일 활동 이벤트와 같은 데이터에 대한 가시성을 제공합니다. 이러한 알림에는 파일 이름과 사용자가 수행한 파일 작업(예: 읽기, 쓰기, 삭제, 이름 바꾸기)이 포함됩니다. 이 데이터의 가시성을 제한하기 위해 이러한 역할을 가진 사용자만 이러한 알림을 관리하거나 볼 수 있습니다.

- 랜섬웨어 복원력 사용자 행동 관리 - 의심스러운 사용자 활동 감지를 활성화하고, 의심스러운 사용자 활동 알림을 조사하고 대응합니다.

- 랜섬웨어 복원력 사용자 동작 뷰어 - 의심스러운 사용자 활동 알림 보기

> 사용자 동작 역할은 독립된 역할이 아니며, 랜섬웨어 복원력 관리자 또는 뷰어 역할에 추가되도록 설계되었습니다. 자세한 내용은 다음을 참조하세요. 사용자 행동 역할.

각 역할에 대한 자세한 설명은 다음 표를 참조하세요.

기준 역할

다음 표에서는 랜섬웨어 복원력 관리자 및 뷰어 역할에서 사용할 수 있는 작업을 설명합니다.

특징과 동작	랜섬웨어 복원력 관리자	랜섬웨어 복원력 뷰어
대시보드 및 모든 탭 보기	예	예
대시보드에서 권장 사항 상태를 업데이트합니다.	예	아니요
무료 체험 시작	예	아니요
워크로드 검색 시작	예	아니요
워크로드 재발견 시작	예	아니요
보호 탭에서:		
암호화 정책에 대한 보호 계획을 추가, 수정 또는 삭제합니다.	예	아니요
작업 부하 보호	예	아니요
데이터 분류를 통해 민감한 데이터에 대한 노출을 식별하세요	예	아니요
보호 계획 및 세부 정보 목록	예	예
보호 그룹 목록	예	예
보호 그룹 세부 정보 보기	예	예
보호 그룹 생성, 편집 또는 삭제	예	아니요
데이터 다운로드	예	예
알림 탭에서:		
암호화 알림 및 알림 세부 정보 보기	예	예
암호화 사고 상태 편집	예	아니요

특징과 동작	랜섬웨어 복원력 관리자	랜섬웨어 복원력 뷰어
복구를 위한 암호화 경고 표시	예	아니요
암호화 사고 세부 정보 보기	예	예
암호화 사고를 기각하거나 해결합니다.	예	아니요
암호화 이벤트에서 영향을 받은 파일의 전체 목록을 가져옵니다.	예	아니요
암호화 이벤트 알림 데이터 다운로드	예	예
사용자 차단(Workload Security 에이전트 구성 포함)	예	아니요
복구 탭에서:		
암호화 이벤트에서 영향을 받은 파일 다운로드	예	아니요
암호화 이벤트에서 작업 부하 복원	예	아니요
암호화 이벤트에서 복구 데이터 다운로드	예	예
암호화 이벤트에서 보고서 다운로드	예	예
설정 탭에서:		
백업 대상 추가 또는 수정	예	아니요
백업 대상 나열	예	예
연결된 SIEM 대상 보기	예	예
SIEM 대상 추가 또는 수정	예	아니요
준비 훈련 구성	예	아니요
준비 훈련 시작, 재설정 또는 편집	예	아니요
준비 훈련 상태 검토	예	예
검색 구성 업데이트	예	아니요
검색 구성 보기	예	예
보고서 탭에서:		

특징과 동작	랜섬웨어 복원력 관리자	랜섬웨어 복원력 뷰어
보고서 다운로드	예	예

사용자 행동 역할

의심스러운 사용자 동작 설정을 구성하고 알림에 대응하려면 사용자에게 랜섬웨어 복원력 사용자 동작 관리자 역할이 있어야 합니다. 의심스러운 사용자 동작 알림만 보려면 사용자에게 랜섬웨어 복원력 사용자 동작 뷰어 역할이 있어야 합니다.

기존 Ransomware Resilience 관리자 또는 뷰어 권한이 있는 사용자에게는 사용자 동작 역할을 부여해야 합니다. "의심스러운 사용자 활동 설정 및 알림" . 예를 들어 랜섬웨어 복원력 관리자 역할이 있는 사용자는 사용자 활동 에이전트를 구성하고 사용자를 차단하거나 차단을 해제하기 위해 랜섬웨어 복원력 사용자 동작 관리자 역할을 받아야 합니다. 랜섬웨어 복원력 사용자 동작 관리자 역할은 랜섬웨어 복원력 뷰어에게 부여되어서는 안 됩니다.

의심스러운 사용자 활동 감지를 활성화하려면 콘솔 조직 관리자 역할이 있어야 합니다.

다음 표에서는 랜섬웨어 복원력 사용자 동작 관리자 및 뷰어 역할에서 사용할 수 있는 작업을 설명합니다.

특징과 동작	랜섬웨어 복원력 사용자 행동 관리자	랜섬웨어 복원력 사용자 동작 뷰어
설정 탭에서:		
사용자 활동 에이전트를 생성, 수정 또는 삭제합니다.	예	아니요
사용자 디렉토리 커넥터 생성 또는 삭제	예	아니요
데이터 수집기 일시 중지 또는 재개	예	아니요
데이터 침해 대비 훈련을 실행하세요	예	아니요
보호 탭에서:		
의심스러운 사용자 동작 정책에 대한 보호 계획을 추가, 수정 또는 삭제합니다.	예	아니요
알림 탭에서:		
사용자 활동 알림 및 알림 세부 정보 보기	예	예
사용자 활동 사고 상태 편집	예	아니요
복구를 위해 사용자 활동 알림을 표시합니다.	예	아니요
사용자 활동 사고 세부 정보 보기	예	예
사용자 활동 사고를 기각하거나 해결합니다.	예	아니요

특징과 동작	랜섬웨어 복원력 사용자 행동 관리자	랜섬웨어 복원력 사용자 동작 뷰어
의심스러운 사용자에 의해 영향을 받은 파일의 전체 목록을 가져옵니다.	예	예
사용자 활동 이벤트 알림 데이터 다운로드	예	예
사용자 차단 또는 차단 해제	예	아니요
복구 탭에서:		
사용자 활동 이벤트에 영향을 받은 파일 다운로드	예	아니요
사용자 활동 이벤트에서 작업 부하 복원	예	아니요
사용자 활동 이벤트에서 복구 데이터 다운로드	예	예
사용자 활동 이벤트에서 보고서 다운로드	예	예

신원 및 액세스 API

조직 및 프로젝트 ID

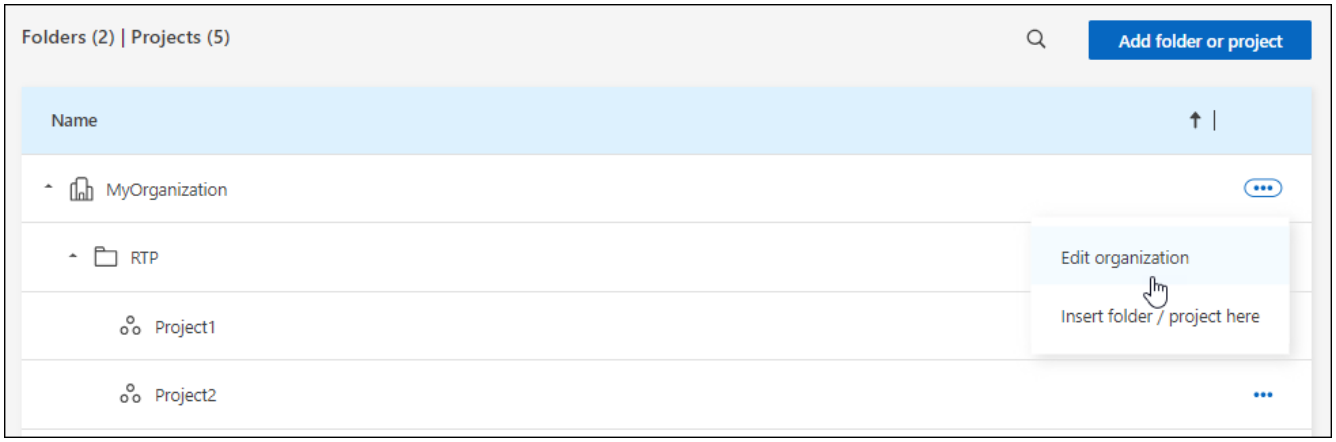
NetApp Console 조직에는 이름과 ID가 있습니다. 조직을 식별하는 데 도움이 되는 이름을 선택할 수 있습니다. 특정 통합을 위해 조직 ID를 검색해야 할 수도 있습니다.

조직 이름 변경

조직의 이름을 바꿀 수 있습니다. 조직 이상의 것을 지원하는 경우 도움이 됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *조직*을 선택하세요.
3. 조직 페이지에서 표의 첫 번째 행으로 이동하여 다음을 선택합니다. ••• 그런 다음 *조직 편집*을 선택하세요.



4. 새로운 조직 이름을 입력하고 *적용*을 선택하세요.

조직 **ID**를 얻으세요

조직 ID는 콘솔과의 특정 통합에 사용됩니다.

조직 페이지에서 조직 ID를 보고 필요에 따라 클립보드에 복사할 수 있습니다.

단계

1. 관리 **> ID** 및 액세스 > *조직*을 선택합니다.
2. 조직 페이지에서 요약 표시줄에 있는 조직 ID를 찾아 클립보드에 복사합니다. 나중에 사용하기 위해 저장할 수도 있고, 필요한 곳에 직접 복사해서 사용할 수도 있습니다.

프로젝트에 대한 **ID**를 얻으세요

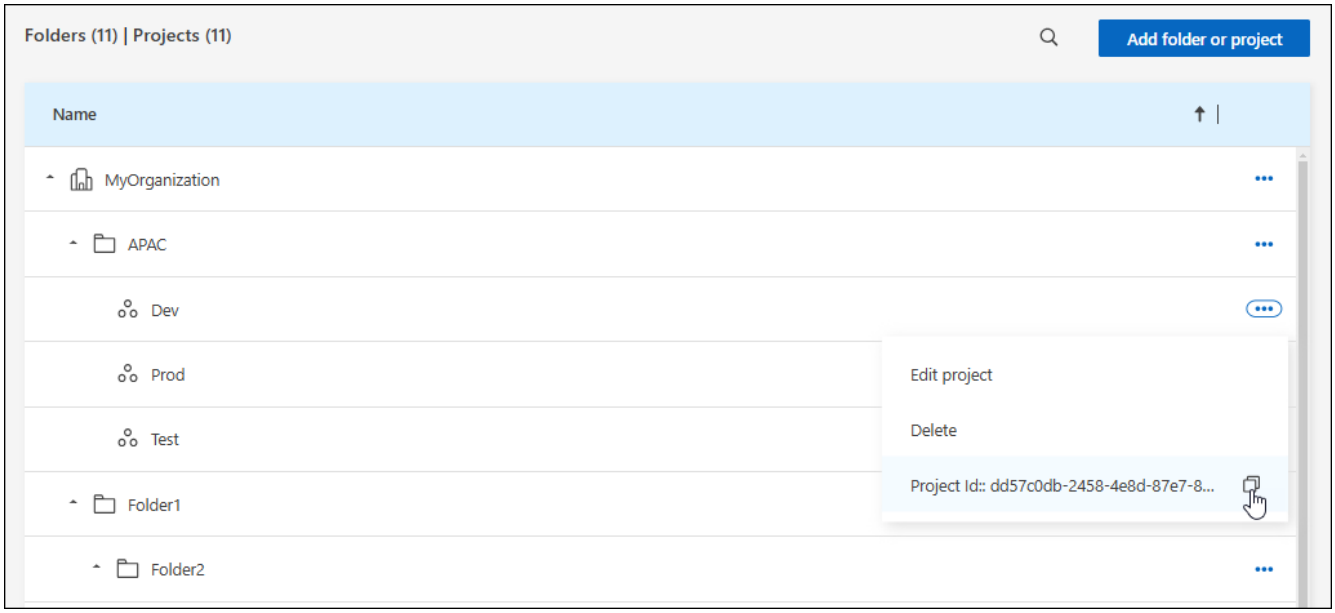
API를 사용하는 경우 프로젝트의 ID를 얻어야 합니다. 예를 들어, Cloud Volumes ONTAP 시스템을 생성할 때.

단계

1. 조직 페이지에서 표의 프로젝트로 이동하여 다음을 선택합니다. •••

   프로젝트 ID가 표시됩니다.

2. ID를 복사하려면 복사 버튼을 선택하세요.



관련 정보

- "ID 및 액세스 관리에 대해 알아보세요"
- "신원 및 액세스 시작하기"
- "ID 및 액세스를 위한 API에 대해 알아보세요"