사용자 접근 권한 및 보안 관리

NetApp Console setup and administration

NetApp
February 11, 2026

목차

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." .

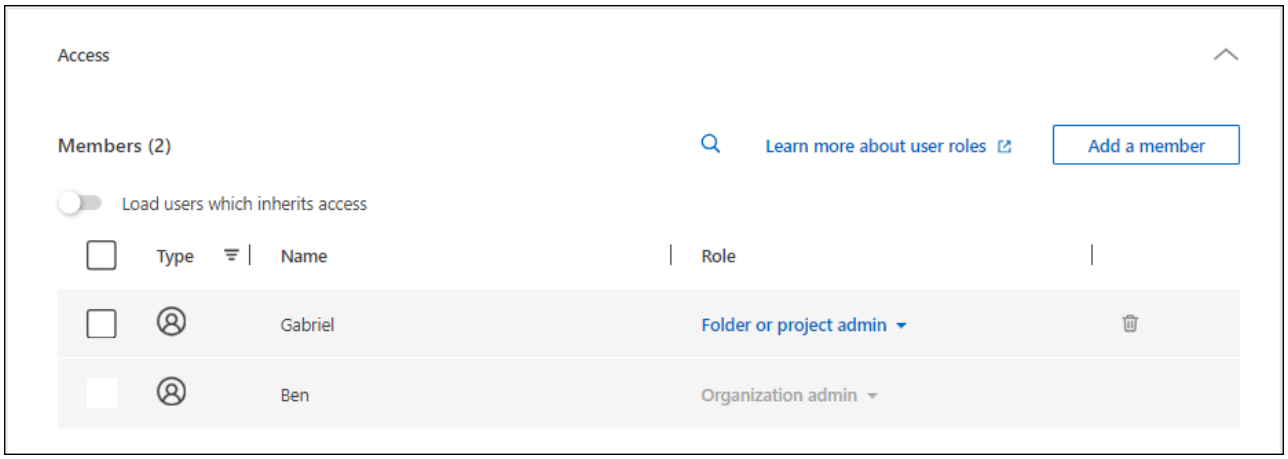
1. 회원 페이지에서 표에 있는 회원을 찾아 선택하세요. ••• 그런 다음 *세부 정보 보기*를 선택하세요.
2. 표에서 멤버에게 할당된 역할을 보고 싶은 조직, 폴더 또는 프로젝트에 해당하는 행을 확장하고 역할 열에서 *보기*를 선택합니다.

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.