사용자 및 접근 권한 관리

NetApp Console local deployment

NetApp
August 10, 2026

목차

사용자 및 접근 권한 관리

NetApp Console 로컬 배포에서 멤버 액세스 관리

NetApp Console 로컬 배포 환경에서 스토리지 엔지니어가 액세스할 수 있는 모든 항목 확인, 다른 지역에 새 역할 추가, 책임이 변경될 때 해당 사용자의 액세스 권한 제거 등 여러 폴더 또는 플릿에 걸쳐 사용자의 역할을 검토하거나 변경할 수 있습니다.

필수 액세스 역할

최고 관리자, 조직 관리자 또는 폴더/플릿 관리자(자신이 관리하는 폴더 및 플릿에 한함). "액세스 역할에 대해 알아보기".

사용자의 필요에 따라 두 가지 방법으로 액세스 권한을 확인하고 관리할 수 있습니다. 조직 내 모든 장비에 걸쳐 특정 사용자가 보유한 역할을 확인하려면 **Members** 페이지를 사용하십시오.

특정 플릿에 액세스할 수 있는 사람을 확인하려면 해당 플릿에 배정된 구성원을 검토하십시오. "플리트 액세스 할당 관리".

새 멤버, 서비스 계정 또는 디렉터리 사용자를 추가하고 첫 번째 역할을 할당하려면 온보딩 작업을 사용하십시오. "멤버 추가 및 역할 할당".

NetApp Console에서 액세스 권한이 부여되는 방식 이해

NetApp Console은 역할 기반 액세스 제어(RBAC)를 사용하여 멤버 권한을 관리합니다. 멤버에게 필요한 액세스 범위에 따라 조직, 폴더 또는 플릿 수준에서 미리 정의된 역할을 할당할 수 있습니다.

역할 상속 사용

조직 또는 폴더 수준에서 할당한 역할은 그 아래의 하위 범위로 상속되므로, 상속된 역할 할당은 원래 역할을 부여했던 상위 범위에서 변경해야 합니다.

"NetApp Console 로컬 배포에서 역할 상속에 대해 알아보십시오.".

멤버에게 할당된 역할 보기

변경 사항을 적용하기 전에 구성원이 어떤 역할을 어떤 범위 내에서 맡고 있는지 정확히 확인하십시오. 예를 들어, 팀원이 이미 `Production-EU-West` 플릿에서 Storage admin 역할을 보유하고 있는지 확인하십시오.

폴더 또는 플릿 관리자 역할을 가진 경우, 해당 페이지에는 조직의 모든 구성원이 표시됩니다. 하지만 권한을 보고 관리할 수 있는 대상은 본인이 관리하는 폴더와 플릿뿐입니다. "NetApp Console 로컬 배포에서 폴더 또는 플릿 관리자 작업에 대해 알아봅니다.".

1. **Members** 페이지에서 표의 구성원으로 이동하여 ••• 을 선택한 다음 **View details** 를 선택합니다.
2. 표에서 구성원의 할당된 역할을 보려는 조직, 폴더 또는 플릿에 해당하는 행을 확장하고 * 역할 * 열에서 * 보기 * 를 선택합니다.

멤버 액세스 권한 할당 또는 수정

구성원의 책임이 변경될 때마다 액세스 권한을 조정할 수 있습니다. 예를 들어, 팀원이 두 번째 지역의 백업 업무를 맡게

되면 기존 스토리지 역할은 그대로 두고 해당 지역의 플릿에 Backup and Recovery 관리자 역할을 추가할 수 있습니다.

새 멤버를 추가하고 첫 번째 역할을 할당해야 하는 경우 "멤버 추가 및 역할 할당"을 참조하십시오.

기존 멤버에게 액세스 역할 추가

구성원의 책임이 확장될 경우 조직, 폴더 또는 플릿 수준에서 추가 역할을 부여하십시오. 예를 들어 Storage admin에게 조직 수준에서 Backup and recovery admin 역할을 부여하면 기존 스토리지 권한을 유지하면서 모든 플릿에서 백업 및 복구 작업을 관리할 수 있습니다.

조직, 폴더 또는 플릿에 대한 액세스 역할을 구성원에게 할당할 수 있습니다.

구성원은 동일한 플릿 내에서 또는 서로 다른 플릿에서 여러 역할을 가질 수 있습니다. 예를 들어, 소규모 조직에서는 사용 가능한 모든 액세스 역할을 동일한 사용자에게 할당할 수 있는 반면, 대규모 조직에서는 사용자가 보다 전문화된 작업을 수행하도록 할 수 있습니다. 또는 조직 수준에서 한 사용자에게 랜섬웨어 복원력 관리자 역할을 할당할 수도 있습니다. 이 경우 해당 사용자는 조직 내 모든 플릿에서 랜섬웨어 복원력 관련 작업을 수행할 수 있습니다.

액세스 역할 전략은 NetApp 리소스를 구성한 방식과 일치해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *구성원*을 선택합니다.
3. 사용자, 디렉토리 사용자 또는 서비스 계정 멤버 탭 중 하나를 선택하십시오.
4. 역할을 부여하려는 구성원 옆에 있는 작업 메뉴 ⋯를 선택하고 *역할 추가*를 선택합니다.
5. 역할을 추가하려면 대화 상자의 단계를 완료하십시오.
   - 조직, 폴더 또는 플릿 선택: 구성원이 권한을 가져야 하는 리소스 계층 구조의 수준을 선택합니다.

     조직 또는 폴더를 선택하면 해당 구성원은 조직 또는 폴더 내의 모든 항목에 대한 권한을 갖게 됩니다.
   - 카테고리를 선택하세요: 역할 카테고리를 선택하세요. "액세스 역할에 대해 알아보기".
   - 역할 선택: 선택한 조직, 폴더 또는 플릿과 연결된 리소스에 대한 권한을 구성원에게 부여하는 역할을 선택하십시오.
   - 역할 추가: 조직 내의 다른 폴더 또는 플릿에 대한 액세스 권한을 부여하려면 *역할 추가*를 선택하고 다른 폴더, 플릿 또는 역할 범주를 지정한 다음 역할 범주와 해당 역할을 선택합니다.
6. *새 역할 추가*를 선택합니다.

멤버에게 할당된 역할 변경

구성원의 책임이 변경될 경우 기존 역할을 다른 역할로 교체하십시오. 예를 들어, `Production-US-East`플릿의 Storage viewer가 Storage admin 역할이 필요한 경우입니다.

모든 사용자는 최소 하나 이상의 역할을 보유해야 합니다. 사용자에게서 모든 역할을 한 번에 제거할 수는 없습니다. 모든 역할을 제거해야 하는 경우, 조직에서 해당 사용자를 삭제하십시오.

단계

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

3. 사용자, 디렉토리 사용자 또는 서비스 계정 멤버 탭 중 하나를 선택하십시오.
4. **Members** 페이지에서 표의 구성원으로 이동하여 ••• 을 선택한 다음 **View details** 를 선택합니다.
5. 표에서 구성원의 역할을 변경하려는 조직, 폴더 또는 플릿에 해당하는 행을 확장하고 역할 열에서 *보기*를 선택하여 해당 구성원에게 할당된 역할을 확인하십시오.
6. 기존 멤버의 역할을 변경하거나 역할을 삭제할 수 있습니다.
   a. 멤버의 역할을 변경하려면 변경하려는 역할 옆에 있는 *변경*을 선택합니다. 역할은 동일한 역할 범주 내에서만 변경할 수 있습니다. 예를 들어, 데이터 서비스 역할 간에 변경할 수 있습니다. 변경 사항을 확인합니다.
   b. 멤버의 역할을 해제하려면 해당 역할 옆의 🗑을 선택하여 멤버의 역할을 해제하십시오. 제거를 확인하는 메시지가 표시됩니다.

조직에서 구성원 제거

구성원이 조직을 떠나거나 Console 액세스가 더 이상 필요하지 않게 되는 방식으로 역할이 변경되면 해당 구성원을 제거하십시오. 예를 들어, 계약직 직원의 계약이 종료되거나 직원이 Console 조직 외부의 팀으로 이동하는 경우입니다.

디렉터리 사용자

디렉터리에서 사용자를 제거하면 해당 사용자의 인증이 차단됩니다. 또한 Console 조직에서도 해당 사용자를 제거하여 구성원 목록을 정확하게 유지하고 Console 로컬 배포 시 할당된 모든 역할을 제거해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. *구성원*을 선택합니다.
3. 사용자, 디렉토리 사용자 또는 서비스 계정 멤버 탭 중 하나를 선택하십시오.
4. 구성원 페이지에서 표의 구성원으로 이동하여 •••을 선택한 다음 *사용자 삭제*를 선택합니다.
5. 해당 구성원을 조직에서 삭제하시겠습니까?

NetApp Console 로컬 배포에서 플릿 액세스 할당 보기 또는 변경

NetApp Console 로컬 배포에서 폴더 및 스토리지 플릿에 대한 멤버 액세스 할당을 감사하거나 변경할 수 있습니다. 폴더 및 플릿 관리자는 일반적으로 자신이 관리하는 범위만 표시되는 이 보기에서 작업합니다.

필수 액세스 역할

최고 관리자, 조직 관리자, 폴더 관리자 또는 플릿 관리자. "액세스 역할에 대해 알아보기".

또는 여러 폴더나 그룹에 걸쳐 특정 멤버의 모든 역할을 관리할 수도 있습니다. "구성원 액세스 관리".

폴더 및 플릿 액세스 작동 방식

콘솔 로컬 배포는 역할 기반 액세스 제어(RBAC)를 사용합니다. 폴더 수준에서 할당한 역할은 해당 폴더 내의 모든 플릿 및 하위 폴더에 적용되며, 플릿 수준에서 할당한 역할은 해당 플릿의 리소스에만 적용됩니다. "NetApp Console 로컬 배포에서 역할 상속에 대해 알아보십시오.".

구성원이 폴더 또는 조직으로부터 역할을 상속받은 경우, 플릿 수준에서 해당 역할을 변경할 수 없습니다. 상속된 액세스 권한을 변경하려면 상위 범위에서 역할을 변경해야 합니다.

폴더 또는 플릿에 할당된 구성원 보기

특정 폴더 또는 플릿을 관리할 수 있는 사용자를 정확히 검토하십시오. 예를 들어, 새 프로덕션 ONTAP 클러스터를 `Production-US-East`플릿에 연결하기 전에 플릿의 액세스 탭을 열어 액세스 권한이 있는 사용자를 확인하십시오.

단계

1. 관리 > *ID 및 액세스*를 선택합니다.
2. *Organization*을 선택합니다.
3. 조직 페이지에서 표의 폴더 또는 플릿으로 이동하고 ••• 을 선택한 다음 폴더 편집 또는 *플릿 편집*을 선택합니다.
4. 폴더 또는 플릿에 액세스할 수 있는 구성원을 보려면 *액세스*를 선택합니다.

폴더 또는 플릿에서 멤버 액세스 권한 수정

이미 조직에 속한 구성원의 역할을 특정 폴더 또는 플릿에 맞춰 조정할 수 있습니다. 예를 들어, 팀원이 개발 플릿에서 프로덕션 플릿으로 이동할 때 다른 플릿의 액세스 권한에는 영향을 주지 않고 프로덕션 플릿에서 해당 구성원의 Storage viewer 권한을 Storage admin 권한으로 승격시킬 수 있습니다.

새 멤버를 추가하고 첫 번째 역할을 할당하려면 온보딩 작업을 사용하십시오. "멤버 추가 및 역할 할당".

단계

1. 조직 페이지에서 표의 폴더 또는 플릿으로 이동하고 ••• 을 선택한 다음 폴더 편집 또는 *플릿 편집*을 선택합니다.
2. *액세스*를 선택하여 액세스 권한이 있는 구성원 목록을 확인합니다.
3. 멤버 액세스 수정:
   - 멤버 역할 변경: 조직 관리자 이외의 역할을 가진 멤버의 경우, 기존 역할을 선택하고 새 역할을 선택하십시오. 변경 사항은 이 범위에만 적용되며, 상위 범위에서 상속된 역할은 여기에 표시되지 않습니다.
   - 이 범위에서 멤버 액세스 제거: 이 폴더 또는 플릿에 직접 역할이 정의된 멤버의 경우, 해당 역할을 제거하여 이 범위에서의 액세스 권한을 취소합니다. 이렇게 해도 해당 멤버가 조직에서 제거되거나 다른 범위에서 가진 역할에는 영향을 미치지 않습니다.

     "조직에서 구성원 제거".
4. *적용*을 선택합니다.

NetApp Console 로컬 배포에서 멤버 보안 관리

NetApp Console 로컬 배포 조직에 대한 사용자 액세스를 안전하게 보호하려면 멤버 보안 설정을 관리하세요. 로컬 사용자가 직접 암호를 변경하도록 안내하고, 로컬 사용자의 다단계 인증(MFA)을 관리하고, 서비스 계정 자격 증명을 다시 생성할 수 있습니다.

필수 액세스 역할

최고 관리자, 조직 관리자, 폴더 관리자 또는 플릿 관리자. "액세스 역할에 대해 알아보기".

사용자 비밀번호 재설정 (로컬 사용자만 해당)

관리자는 로컬 사용자 암호를 직접 재설정할 수 없습니다.

로컬 사용자가 콘솔 로컬 배포 로그인 페이지에서 *Forgot password?*를 선택하여 비밀번호를 재설정하도록 안내하십시오.

이 옵션은 디렉터리 사용자에게는 제공되지 않습니다.

로컬 사용자의 다단계 인증(MFA) 관리

로컬 사용자가 MFA 장치에 대한 액세스 권한을 잃어버린 경우, 해당 사용자의 MFA 구성을 제거하거나 비활성화할 수 있습니다.

다중 요소 인증은 로컬 사용자에게만 제공됩니다. 디렉터리 사용자는 Console 로컬 배포를 통해 다중 요소 인증을 활성화할 수 없습니다.

다음 지침을 참고하여 적절한 조치를 선택하십시오.

- 사용자가 MFA 장치에 일시적으로 액세스할 수 없는 경우 *사용 안 함*을 선택합니다. MFA를 비활성화하면 8시간 동안 MFA 없이 한 번 로그인할 수 있으며, 이후 MFA가 자동으로 다시 활성화됩니다.
- 사용자가 MFA를 완전히 재설정해야 하는 경우 *제거*를 선택합니다. MFA를 제거하면 사용자는 MFA를 다시 설정할 때까지 MFA 없이 로그인할 수 있습니다.

사용자가 복구 코드를 저장해 둔 경우 해당 코드를 사용하여 로그인할 수 있습니다. 복구 코드가 없는 사용자의 경우, MFA를 비활성화하여 사용자가 로그인하고 액세스 권한을 복구할 수 있도록 하십시오.

로컬 사용자의 다단계 인증을 관리하려면 해당 사용자와 동일한 도메인의 이메일 주소가 있어야 합니다.

단계

1. 관리 > *ID 및 액세스*를 선택합니다.
2. *구성원*을 선택합니다.
3. 멤버 페이지에서 표에 있는 멤버로 이동하여 ••• 을 선택한 다음 *다단계 인증 관리*를 선택합니다.
4. 사용자의 MFA 구성을 제거할지 비활성화할지 선택합니다.

완료한 후

감사 로그를 검토하여 누가 언제 MFA 액세스 권한을 변경했는지, 그리고 변경 작업이 성공했는지 여부를 확인하십시오. "NetApp Console 로컬 배포 활동을 감사하는 방법을 알아보십시오.".

서비스 계정의 자격 증명을 다시 생성합니다.

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

새 자격 증명을 생성하면 이전 자격 증명은 삭제됩니다. 이전 자격 증명은 더 이상 사용할 수 없습니다.

단계

1. 관리 > *ID 및 액세스*를 선택합니다.

2. *구성원*을 선택합니다.
3. 멤버 테이블에서 서비스 계정으로 이동하여 ⋯을 선택한 다음 *비밀번호 다시 생성*을 선택합니다.
4. *다시 만들기*를 선택합니다.
5. 클라이언트 ID와 클라이언트 시크릿을 다운로드하거나 복사합니다.

   콘솔 로컬 배포 환경에서는 클라이언트 비밀 키가 한 번만 표시됩니다. 클라이언트 비밀 키를 복사하거나 다운로드하여 안전하게 보관하십시오.