NetApp Console 사용

NetApp Console setup and administration

NetApp
January 23, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/console-setup-admin/task-logging-in.html on January 23, 2026. Always check docs.netapp.com for the latest.

목차

NetApp Console 사용

NetApp Console 에 로그인하세요

NetApp Console 에 로그인하는 방법은 사용하는 배포 모드에 따라 달라집니다.

24시간이 지나거나 브라우저를 닫으면 자동으로 로그아웃됩니다.

"콘솔 배포 모드에 대해 알아보세요" .

표준 모드

NetApp Console 에 가입한 후 웹 기반 콘솔에서 로그인하여 데이터 및 스토리지 인프라 관리를 시작할 수 있습니다.

이 작업에 관하여

다음 옵션 중 하나를 사용하여 NetApp Console 에 로그인할 수 있습니다.

- 기존 NetApp 지원 사이트(NSS) 자격 증명
- 이메일 주소와 비밀번호를 사용하는 NetApp Console 계정
- 연합 연결

  단일 로그인을 사용하면 회사 디렉토리의 자격 증명(연방 ID)을 사용하여 로그인할 수 있습니다. "ID 연합을 설정하는 방법을 알아보세요" .

단계

1. 웹 브라우저를 열고 이동하세요 "NetApp Console"
2. 로그인 페이지에서 로그인에 사용된 이메일 주소를 입력하세요.
3. 로그인과 관련된 인증 방법에 따라 자격 증명을 입력하라는 메시지가 표시됩니다.
   - NetApp 클라우드 자격 증명: 비밀번호를 입력하세요
   - 연합 사용자: 연합 ID 자격 증명을 입력하세요.
   - NetApp 지원 사이트 계정: NetApp 지원 사이트 자격 증명을 입력하세요.

결과

이제 로그인하여 하이브리드 멀티클라우드 인프라를 관리할 수 있습니다.

제한 모드

제한 모드에서 콘솔을 사용하는 경우 에이전트에서 로컬로 실행되는 사용자 인터페이스에서 콘솔에 로그인해야 합니다.

이 작업에 관하여

제한 모드에서는 콘솔에서 다음 옵션 중 하나를 사용하여 로그인할 수 있습니다.

- 이메일 주소와 비밀번호를 사용하여 NetApp Console 로그인합니다.
- 연합 연결

  단일 로그인을 사용하면 회사 디렉토리의 자격 증명(연방 ID)을 사용하여 로그인할 수 있습니다. "ID 페더레이션을 사용하는 방법을 알아보세요" .

단계

1. 웹 브라우저를 열고 에이전트가 설치된 IP 주소를 입력하세요.
2. 사용자 이름과 비밀번호를 입력하여 로그인하세요.

여러 콘솔 에이전트와 함께 작업

여러 개의 콘솔 에이전트를 사용하는 경우 콘솔에서 해당 콘솔 에이전트 간에 직접 전환하여 연결된 시스템을 볼 수 있습니다.

콘솔 에이전트 간 전환

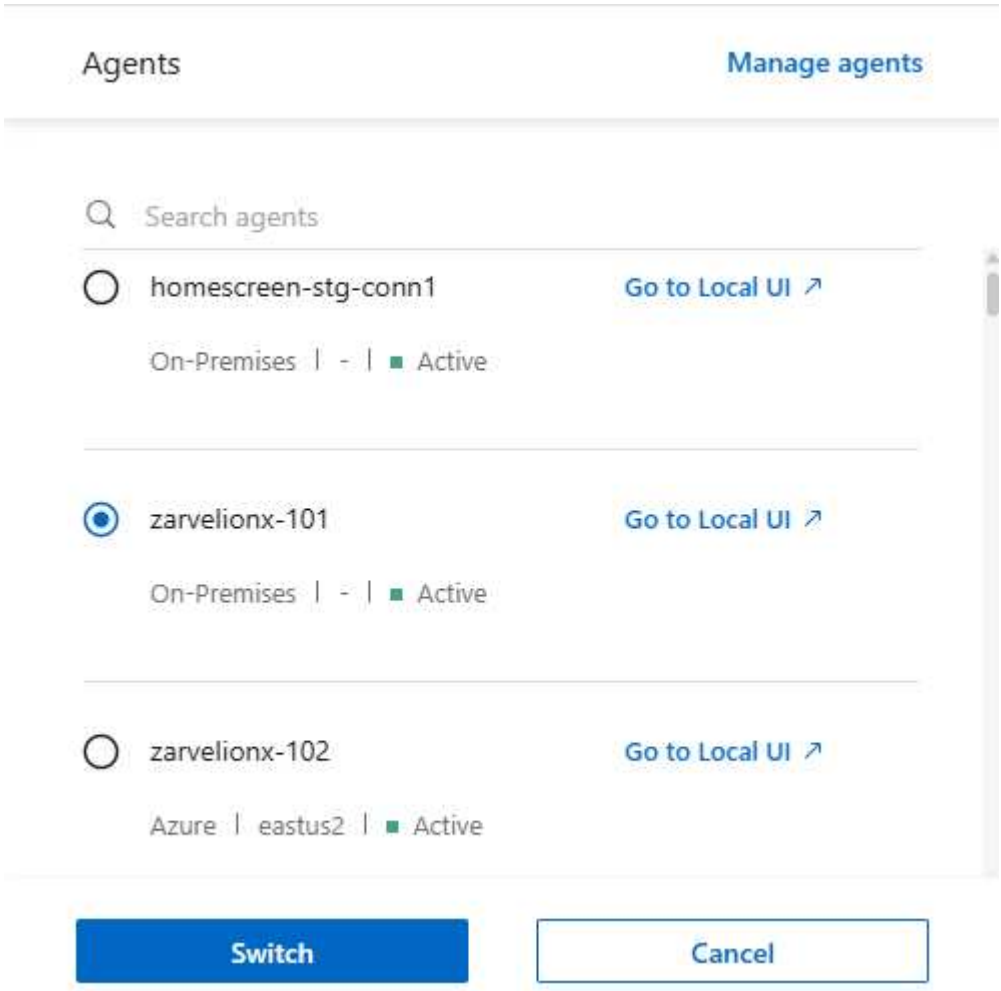
여러 개의 콘솔 에이전트가 있는 경우 에이전트 간에 전환하여 특정 에이전트와 연결된 시스템을 볼 수 있습니다.

예를 들어, 멀티 클라우드 환경에서는 AWS에 한 에이전트가 있고 Google Cloud에 다른 에이전트가 있을 수 있습니다. 각 클라우드 환경에서 Cloud Volumes ONTAP 시스템을 관리하려면 이러한 에이전트 간에 전환하세요.

에이전트의 로컬 UI에서 NetApp Console 볼 때 이 옵션을 사용할 수 없습니다.

단계

1. 콘솔 에이전트 아이콘을 선택하세요( )을 클릭하면 사용 가능한 에이전트 목록을 볼 수 있습니다.



결과

콘솔이 새로 고쳐지고 선택한 에이전트와 관련된 시스템이 표시됩니다.

NetApp Console 홈페이지에서 메트릭 보기

저장소의 상태를 모니터링하면 저장소 보호에 문제가 있는 경우 이를 인지하고 이를 해결하기 위한 조치를 취할 수 있습니다. NetApp Console 홈페이지를 사용하면 NetApp Backup and Recovery 에서 수행한 백업 및 복원 상태를 볼 수 있으며, NetApp Ransomware Resilience 에서 표시된 대로 랜섬웨어 공격 위험이 있거나 보호되는 워크로드 수를 볼 수 있습니다. 개별 클러스터와 Cloud Volumes ONTAP 의 스토리지 용량, ONTAP 알림, 클러스터 또는 Cloud Volumes ONTAP 시스템당 스토리지 성능 용량, 보유한 다양한 유형의 라이선스 등을 검토할 수 있습니다.

홈페이지의 모든 창에는 조직 수준의 데이터가 표시됩니다. 저장소 용량 및 저장소 성능 창에는 사용자가 IAM 권한에 따라 액세스할 수 있는 프로젝트와 연결된 시스템이 표시됩니다.

시스템은 홈페이지의 데이터를 5분마다 새로 고칩니다. 캐싱으로 인해 이 페이지의 데이터가 최대 15분 동안 실제 값과 다를 수 있습니다.

홈페이지에서 정확한 지표를 얻으려면 적절한 크기와 구성의 콘솔 에이전트가 필요합니다.

필수 NetApp Console 역할

홈페이지의 각 창에는 서로 다른 사용자 역할이 필요합니다.

- 저장 용량 창: NetApp Console 시스템 페이지를 볼 수 있는 기능
- * ONTAP 알림 창*: 폴더 또는 프로젝트 관리자, 운영 지원 분석가, 조직 관리자, 조직 뷰어, 슈퍼 관리자, 슈퍼 뷰어
- 스토리지 성능 용량 창: NetApp Console 시스템 페이지를 볼 수 있는 기능
- * Licenses and subscriptions 창*: 폴더 또는 프로젝트 관리자, 조직 관리자, 조직 뷰어, 슈퍼 관리자, 슈퍼 뷰어
- 랜섬웨어 복원력 창: 폴더 또는 프로젝트 관리자, 조직 관리자, 랜섬웨어 복원력 관리자, 랜섬웨어 복원력 뷰어, 슈퍼 관리자, 슈퍼 뷰어
- 백업 및 복구 창: 백업 및 복구 백업 관리자, 백업 및 복구 슈퍼 관리자, 백업 및 복구 백업 뷰어, 백업 및 복구 복제 관리자, 폴더 또는 프로젝트 관리자, 조직 관리자, 백업 및 복구 복원 관리자, 슈퍼 관리자, 슈퍼 뷰어

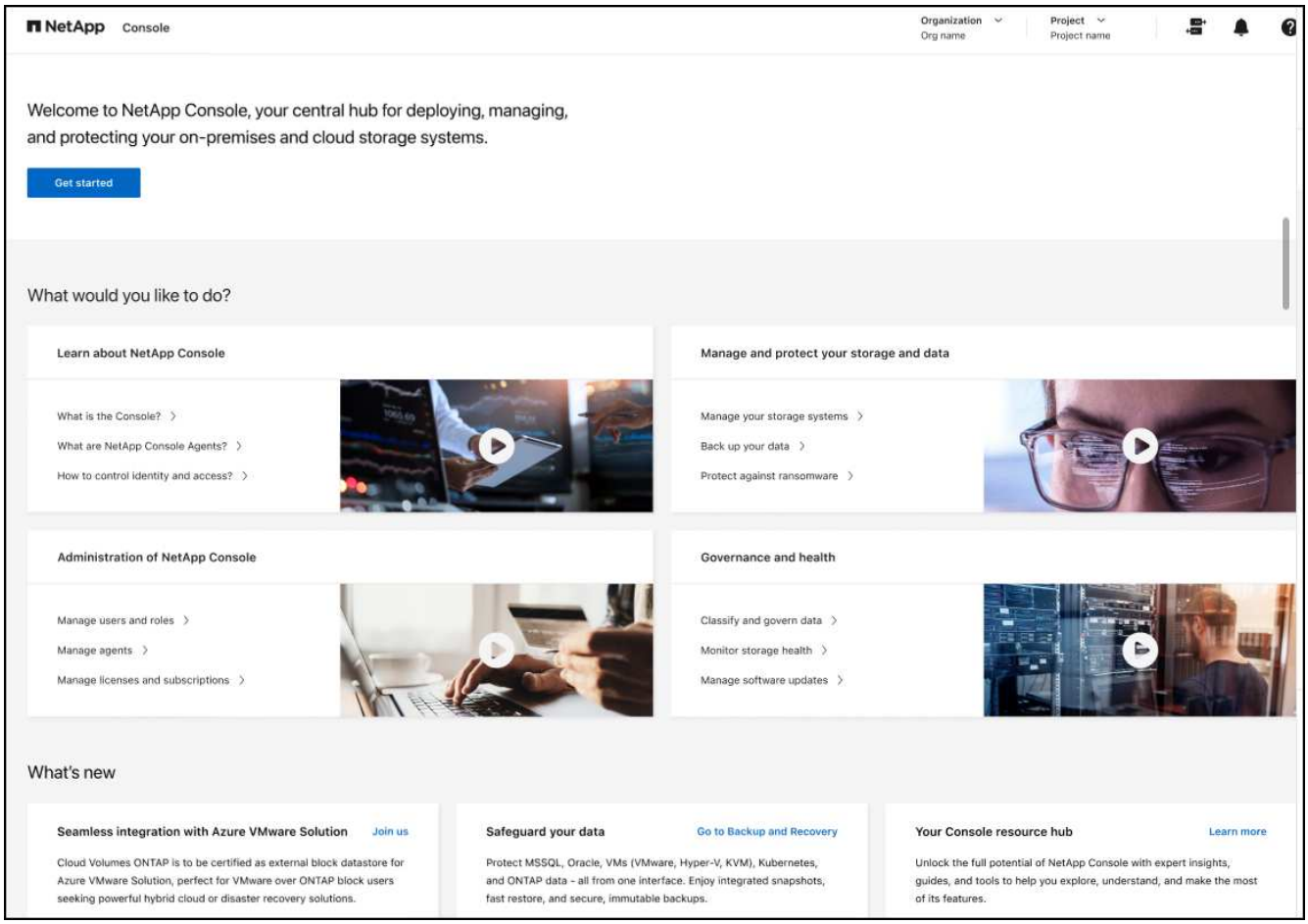
창에 액세스할 권한이 없는 경우 해당 창에는 해당 창을 사용할 권한이 없다는 메시지가 표시됩니다.

"NetApp Console 액세스 역할에 대해 알아보세요." .

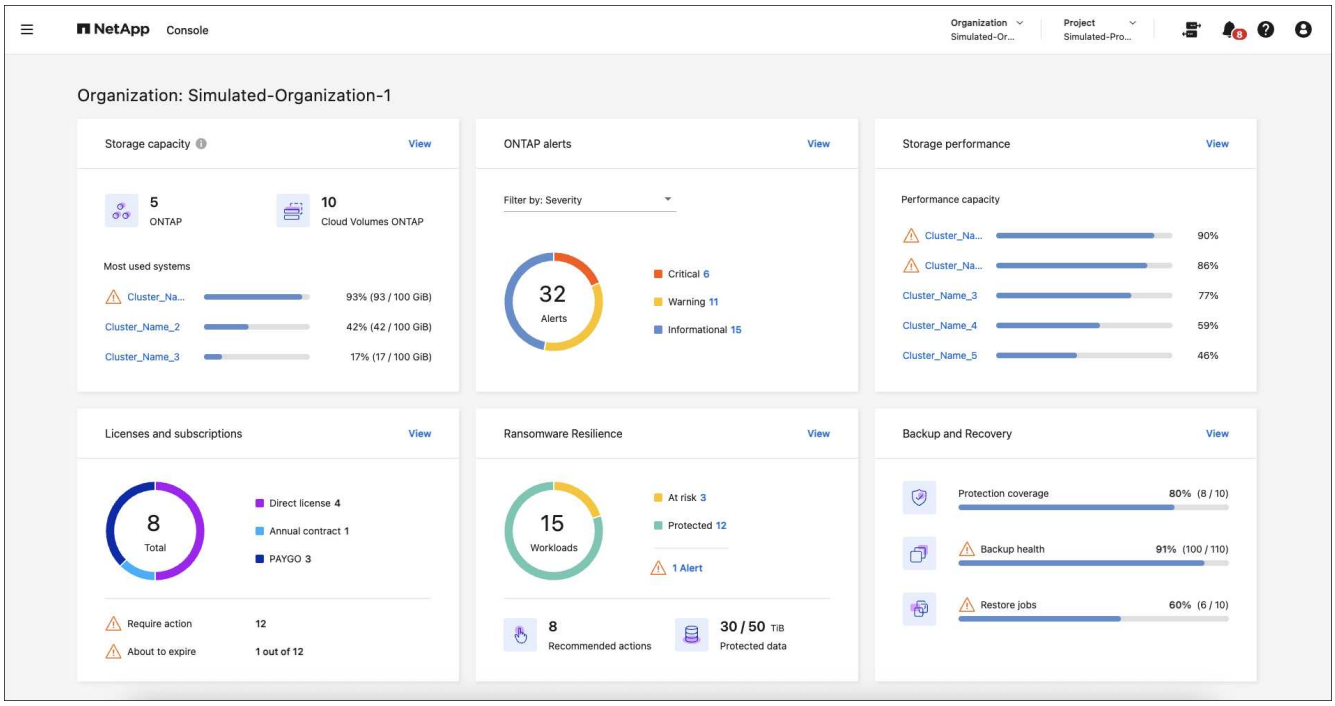
단계

1. NetApp Console 메뉴에서 *홈*을 선택합니다.

   조직 관리자 역할이 있고 에이전트나 스토리지 시스템이 설정되어 있지 않으면 홈페이지에 시작 정보가 표시됩니다.



NetApp Console 이미 설정한 경우, 하나 이상의 콘솔 에이전트가 활성화되어 있고 해당 에이전트에 하나 이상의 클러스터 또는 Cloud Volumes ONTAP 시스템이 추가되어 있으면 홈페이지에 스토리지 환경에 대한 메트릭이 표시됩니다.



홈페이지에 메트릭이 표시되도록 설정

다음 조건이 충족되면 홈페이지에서 지표를 볼 수 있습니다.

- NetApp Console 의 SaaS 인스턴스에 로그인했습니다.
- 기존 스토리지 리소스(에이전트 및 클러스터 또는 Cloud Volumes ONTAP 시스템)가 있는 조직에 속해 있습니다.
- 최소한 하나의 콘솔 에이전트가 활성화되어 있습니다.
- 해당 에이전트에 하나 이상의 클러스터 또는 Cloud Volumes ONTAP 시스템이 추가되었습니다.

홈페이지에 지표가 나타나도록 하려면 다음 작업을 완료하세요.

- 최소한 하나의 콘솔 에이전트를 활성화합니다.
- 해당 에이전트를 사용하여 하나 이상의 클러스터 또는 하나의 Cloud Volumes ONTAP 추가합니다.

전체 저장 용량 보기

스토리지 용량 창은 ONTAP 클러스터와 Cloud Volumes ONTAP 시스템에 대한 다음 정보를 제공합니다.

- 콘솔에서 발견된 ONTAP 시스템 수
- 콘솔에서 발견된 Cloud Volumes ONTAP 시스템 수
- 클러스터당 용량 사용량

클러스터 또는 Cloud Volumes ONTAP 시스템의 순서는 사용된 용량에 따라 결정됩니다. 가장 용량이 큰 클러스터나 시스템이 먼저 나타나므로 쉽게 식별할 수 있습니다.

경고 표시기는 클러스터 용량이 80%에 도달했음을 나타내며, 데이터는 5분마다 업데이트됩니다.

> 여러 프로젝트가 있는 경우 시스템 페이지와 비교하여 저장소 용량 창에 다른 데이터가 표시될 수 있습니다. 시스템 페이지는 프로젝트 수준에 따른 정보를 표시하는 반면, 스토리지 용량 창은 조직 수준의 정보를 표시하기 때문입니다. 또한, 성능 최적화를 위해 데이터가 최대 15분 동안 캐시되므로 이 창의 데이터는 최대 15분 동안 실제 값과 다를 수 있습니다.

단계

1. NetApp Console 메뉴에서 스토리지 용량 창을 검토합니다.
2. 저장 용량 창에서 *보기*를 선택하여 콘솔 시스템 페이지로 이동합니다.
3. 시스템 페이지에서 보려는 클러스터가 포함된 프로젝트를 선택합니다.
4. 시스템 페이지에서 클러스터를 선택하면 해당 클러스터에 대한 자세한 내용을 볼 수 있습니다.

ONTAP 알림 보기

NetApp 온프레미스 ONTAP 환경에서 발생하는 문제나 잠재적 위험을 확인하세요. EMS가 아닌 알림과 EMS 알림을 볼 수 있습니다.

데이터는 5분마다 업데이트됩니다.

다음과 같은 심각도의 ONTAP 알림을 볼 수 있습니다.

- 비판적인
- 경고
- 정보 제공

다음 영향 지역에 대한 ONTAP 알림을 확인할 수 있습니다.

- 용량
- 성능
- 보호
- 유효성
- 보안

캐싱을 사용하면 성능이 최적화되지만, 이 창의 데이터가 최대 15분 동안 실제 값과 달라질 수 있습니다.

지원 시스템

- 온프레미스 ONTAP NAS 또는 SAN 시스템이 지원됩니다.
- Cloud Volumes ONTAP 시스템은 지원되지 않습니다.

지원되는 데이터 소스

ONTAP 에서 발생하는 특정 이벤트에 대한 알림을 확인합니다. 이는 EMS와 지표 기반 알림의 조합입니다.

ONTAP 알림에 대한 자세한 내용은 다음을 참조하세요. "ONTAP 알림 정보" .

귀하가 볼 수 있는 알림 목록은 다음을 참조하세요. "ONTAP 스토리지의 잠재적 위험 보기" .

단계

1. NetApp Console 메뉴에서 ONTAP 알림 창을 검토합니다.
2. 선택적으로 심각도 수준을 선택하여 알림을 필터링하거나 필터를 변경하여 영향 영역을 기준으로 알림을 표시합니다.
3. ONTAP 알림 창에서 *보기*를 선택하여 콘솔 알림 페이지로 이동합니다.

스토리지 성능 용량 보기

클러스터 또는 Cloud Volumes ONTAP 시스템당 사용되는 스토리지 성능 용량을 검토하여 성능 용량, 대기 시간 및 IOPS가 워크로드에 어떤 영향을 미치는지 확인하세요. 예를 들어, 중요한 워크로드에 대한 지연 시간을 최소화하고 IOPS와 처리량을 극대화하기 위해 워크로드를 전환해야 할 수도 있습니다.

시스템은 클러스터와 시스템을 성능 용량별로 정렬하고, 가장 높은 용량을 먼저 나열하여 쉽게 식별할 수 있도록 합니다.

캐싱을 사용하면 성능이 최적화되지만, 이 창의 데이터가 최대 15분 동안 실제 값과 달라질 수 있습니다.

단계

1. NetApp Console 메뉴에서 스토리지 성능 창을 검토합니다.

2. 저장소 성능 창에서 *보기*를 선택하면 성능 페이지로 이동합니다. 이 페이지에는 모든 클러스터와 Cloud Volumes ONTAP 시스템의 성능, 용량, IOPS, 지연 시간 데이터가 나열되어 있습니다.
3. 시스템 관리자에서 세부 정보를 보려면 클러스터를 선택하세요.

귀하가 보유한 라이센스 및 구독을 확인하세요

Licenses and subscriptions 창에서 다음 정보를 검토하세요.

- 귀하가 보유한 라이선스 및 구독의 총 수입니다.
- 귀하가 보유한 각 유형의 라이선스 및 구독 수(직접 라이선스, 연간 계약 또는 PAYGO).
- 활성화되어 있거나 조치가 필요하거나 만료가 임박한 라이선스 및 구독의 수입니다.
- 시스템은 조치가 필요하거나 만료가 임박한 라이선스 유형 옆에 표시기를 표시합니다.

데이터는 5분마다 새로 고쳐집니다.

캐싱을 사용하면 성능이 최적화되지만, 이 창의 데이터가 최대 15분 동안 실제 값과 달라질 수 있습니다.

단계

1. NetApp Console 메뉴에서 Licenses and subscriptions 창을 검토합니다.
2. Licenses and subscriptions 창에서 *보기*를 선택하여 콘솔 Licenses and subscriptions 페이지로 이동합니다.

랜섬웨어 복원력 상태 보기

워크로드가 랜섬웨어 공격의 위험에 처해 있는지, 아니면 NetApp Ransomware Resilience 데이터 서비스로 보호되는지 알아보세요. 보호되는 총 데이터 양을 검토하고, 권장되는 작업 수를 보고, 랜섬웨어 보호와 관련된 알림 수를 볼 수 있습니다.

데이터는 5분마다 새로 고쳐지며 NetApp Ransomware Resilience 대시보드에 표시된 데이터와 일치합니다.

"NetApp Ransomware Resilience 에 대해 알아보세요" .

단계

1. NetApp Console 메뉴에서 랜섬웨어 복원력 창을 검토합니다.
2. 랜섬웨어 복원력 창에서 다음 중 하나를 수행하세요.
    - *보기*를 선택하여 NetApp Ransomware Resilience 보드로 이동합니다. 자세한 내용은 다음을 참조하세요. "NetApp Ransomware Resilience 보드를 사용하여 워크로드 상태를 모니터링합니다." .
    - NetApp Ransomware Resilience 보드에서 "권장 작업"을 검토하세요. 자세한 내용은 다음을 참조하세요. "NetApp Ransomware Resilience 대시보드에서 보호 권장 사항을 검토하세요." .
    - NetApp Ransomware Resilience 알림 페이지에서 알림을 검토하려면 알림 링크를 선택하세요. 자세한 내용은 다음을 참조하세요. "NetApp Ransomware Resilience 사용하여 감지된 랜섬웨어 알림을 처리하세요" .

백업 및 복구 상태 보기

NetApp Backup and Recovery 에서 백업 및 복원의 전반적인 상태를 검토합니다. 보호된 리소스와 보호되지 않은 리소스의 수를 볼 수 있습니다. 또한 작업 부하를 보호하기 위해 백업 및 복원 작업의 비율도 확인할 수 있습니다.

백분율이 높을수록 데이터 보호가 향상되었음을 나타냅니다.

데이터는 5분마다 새로 고쳐집니다.

캐싱을 사용하면 성능이 최적화되지만, 이 창의 데이터가 최대 15분 동안 실제 값과 달라질 수 있습니다.

단계

1. NetApp Console 메뉴에서 백업 및 복구 창을 검토합니다.
2. *보기*를 선택하여 NetApp Backup and Recovery 보드로 이동합니다. 자세한 내용은 다음을 참조하세요. "NetApp Backup and Recovery 설명서" .

NetApp Console 사용자 설정 관리

비밀번호 변경, 다중 인증(MFA) 활성화, 콘솔 관리자 확인 등 콘솔 프로필을 수정할 수 있습니다.

콘솔 내에서 각 사용자는 사용자와 설정에 대한 정보가 포함된 프로필을 갖습니다. 프로필 설정을 보고 편집할 수 있습니다.

표시 이름 변경

콘솔에서 다른 사용자에게 자신을 식별하는 데 사용되는 표시 이름을 변경할 수 있습니다. 사용자 이름이나 이메일 주소는 변경할 수 없습니다.

단계

1. 콘솔의 오른쪽 상단에 있는 프로필 아이콘을 선택하면 사용자 설정 패널을 볼 수 있습니다.
2. 이름 옆에 있는 편집 아이콘을 선택하세요.
3. 이름 필드에 새로운 표시 이름을 입력합니다.

읽기 전용 모드에서 당신의 역할을 강화하세요

경우에 따라 조직 관리자가 조직을 읽기 전용 모드로 설정할 수 있습니다. 관리자 권한이 있는 경우 변경을 하려면 권한을 높여야 합니다. 이는 변경 사항이 의도적이고 승인된 것임을 보장합니다.

권한을 높이면 현재 세션이 만료될 때까지 콘솔에서 변경 작업을 수행할 수 있습니다.

작업이 끝나면 콘솔에서 로그아웃하거나 슬라이더를 원래 위치로 되돌려 읽기 전용 모드로 돌아가십시오. 시스템은 세션이 만료되면 관리자 권한을 제거합니다.

단계

1. 콘솔의 오른쪽 상단에 있는 프로필 아이콘을 선택하면 사용자 설정 패널을 볼 수 있습니다.
2. 읽기 전용 모드 상태로 설정하려면 슬라이더를 '높음' 위치로 이동한 후 변경 사항을 확인하십시오.

다중 요소 인증 구성

보안을 강화하기 위해 두 번째 검증 방법을 요구하여 다중 인증 요소(MFA)를 구성합니다.

외부 ID 공급자 또는 NetApp 지원 사이트를 통해 단일 로그인(SSO)을 사용하는 사용자는 다단계 인증(MFA)을 활성화할 수 없습니다. 이 두 가지 조건 중 하나라도 충족되면 프로필 설정에서 MFA를 활성화하는 옵션이 표시되지 않습니다.

사용자 계정이 API 액세스에 사용되는 경우 MFA를 활성화하지 마세요. 다중 요소 인증이 사용자 계정에 활성화되면 API 액세스가 중단됩니다. 모든 API 액세스에 서비스 계정을 사용하세요.

시작하기 전에

- Google Authenticator나 Microsoft Authenticator와 같은 인증 앱을 이미 기기에 다운로드했어야 합니다.
- MFA를 설정하려면 비밀번호가 필요합니다.

> 인증 앱에 액세스할 수 없거나 복구 코드를 분실한 경우 콘솔 관리자에게 문의하여 도움을 받으세요.

단계

1. 콘솔의 오른쪽 상단에 있는 프로필 아이콘을 선택하면 사용자 설정 패널을 볼 수 있습니다.
2. 다중 인증 요소 헤더 옆에 있는 *구성*을 선택합니다.
3. 메시지에 따라 계정에 MFA를 설정하세요.
4. 완료되면 복구 코드를 저장하라는 메시지가 표시됩니다. 코드를 복사하거나 코드가 포함된 텍스트 파일을 다운로드하세요. 이 코드를 안전한 곳에 보관하세요. 인증 앱에 대한 액세스 권한을 잃은 경우 복구 코드가 필요합니다.

   MFA를 설정한 후에는 로그인할 때마다 인증 앱에서 일회용 코드를 입력하라는 메시지가 콘솔에 표시됩니다.

MFA 복구 코드를 다시 생성하세요

복구 코드는 한 번만 사용할 수 있습니다. 기존 계정을 사용하거나 분실한 경우 새 계정을 만드세요.

단계

1. 콘솔의 오른쪽 상단에 있는 프로필 아이콘을 선택하면 사용자 설정 패널을 볼 수 있습니다.
2. 선택하다 ••• 다중 인증 요소 헤더 옆에 있습니다.
3. *복구 코드 재생성*을 선택하세요.
4. 생성된 복구 코드를 복사하여 안전한 곳에 저장하세요.

MFA 구성을 삭제하세요

작업이 끝나면 콘솔에서 로그아웃하거나 슬라이더를 원래 위치로 되돌려 읽기 전용 모드로 돌아가십시오. 시스템은 세션이 만료되면 관리자 권한을 제거합니다.

> 인증 앱이나 복구 코드에 액세스할 수 없는 경우 조직 관리자에게 문의하여 MFA 구성을 재설정해야 합니다.

단계

1. 콘솔의 오른쪽 상단에 있는 프로필 아이콘을 선택하면 사용자 설정 패널을 볼 수 있습니다.
2. 선택하다 ••• 다중 인증 요소 헤더 옆에 있습니다.
3. *삭제*를 선택하세요.

조직 관리자에게 문의하세요

조직 관리자에게 문의해야 하는 경우 콘솔에서 직접 이메일을 보낼 수 있습니다. 관리자는 조직 내의 사용자 계정과 권한을 관리합니다.

관리자에게 연락 기능을 사용하려면 브라우저에 기본 이메일 애플리케이션을 구성해야 합니다.

단계

1. 콘솔의 오른쪽 상단에 있는 프로필 아이콘을 선택하면 사용자 설정 패널을 볼 수 있습니다.
2. 조직 관리자에게 이메일을 보내려면 *관리자에게 연락*을 선택하세요.
3. 사용할 이메일 애플리케이션을 선택하세요.
4. 이메일을 작성하고 *보내기*를 선택하세요.

다크 모드(다크 테마) 구성

콘솔을 다크 모드로 표시하도록 설정할 수 있습니다.

단계

1. 콘솔의 오른쪽 상단에 있는 프로필 아이콘을 선택하면 사용자 설정 패널을 볼 수 있습니다.
2. 어두운 테마 슬라이더를 움직여 활성화하세요.

저작권 정보

Copyright © 2026 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.