



# 액세스 관리

## SANtricity 11.5

NetApp  
February 12, 2024

# 목차

액세스 관리 .....	1
개념 .....	1
방법 .....	6
FAQ 를 참조하십시오 .....	26

# 액세스 관리

## 개념

### 액세스 관리 작동 방식

액세스 관리는 SANtricity 시스템 관리자에서 사용자 인증을 설정하는 방법입니다. 인증을 위해서는 사용자가 할당된 자격 증명을 사용하여 이러한 시스템에 로그인해야 합니다.

Access Management 구성 및 사용자 인증은 다음과 같이 작동합니다.

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 System Manager에 로그인합니다.



처음 로그인하는 경우 사용자 이름 admin이 자동으로 표시되며 변경할 수 없습니다. admin 사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

2. 관리자는 사용자 인터페이스에서 Access Management(액세스 관리)로 이동합니다. 스토리지 어레이는 RBAC(역할 기반 액세스 제어) 기능을 구현하는 로컬 사용자 역할을 사용하도록 사전 구성됩니다.
3. 관리자는 다음 인증 방법 중 하나 이상을 구성합니다.
  - \* 로컬 사용자 역할 \* — 스토리지 어레이에 적용된 RBAC 기능을 통해 인증이 관리됩니다. 로컬 사용자 역할에는 미리 정의된 사용자 프로필과 특정 액세스 권한이 있는 역할이 포함됩니다. 관리자는 이러한 로컬 사용자 역할을 단일 인증 방법으로 사용하거나 디렉터리 서비스와 함께 사용할 수 있습니다. 사용자 암호 설정 이외의 구성은 필요하지 않습니다.
  - \* 디렉터리 서비스 \* — 인증은 LDAP(Lightweight Directory Access Protocol) 서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스를 통해 관리됩니다. 관리자는 LDAP 서버에 연결한 다음 LDAP 사용자를 스토리지 배열에 포함된 로컬 사용자 역할에 매핑합니다.
  - \* SAML \* — 인증은 SAML(Security Assertion Markup Language) 2.0을 사용하여 ID 공급자(IDP)를 통해 관리됩니다. 관리자는 IdP 시스템과 스토리지 어레이 간의 통신을 설정한 다음 IdP 사용자를 스토리지 어레이에 포함된 로컬 사용자 역할에 매핑합니다.
4. 관리자는 사용자에게 System Manager에 대한 로그인 자격 증명을 제공합니다.
5. 사용자는 자격 증명을 입력하여 시스템에 로그인합니다.



SAML 및 SSO(Single Sign-On)로 인증이 관리되는 경우 시스템은 System Manager 로그인 대화 상자를 건너뛸 수 있습니다.

로그인 중에 시스템은 다음과 같은 백그라운드 작업을 수행합니다.

- 사용자 계정에 대해 사용자 이름과 암호를 인증합니다.
- 할당된 역할에 따라 사용자의 권한을 결정합니다.
- 사용자에게 사용자 인터페이스의 작업에 대한 액세스 권한을 제공합니다.
- 인터페이스의 오른쪽 위에 사용자 이름을 표시합니다.

## System Manager에서 사용 가능한 작업

작업에 대한 액세스 권한은 사용자가 할당한 역할에 따라 다르며, 여기에는 다음이 포함됩니다.

- \* 스토리지 관리자 \* — 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
- \* 보안 관리자 \* — 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
- \* 지원 관리자 \* — 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
- \* Monitor \* — 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용할 수 없는 작업은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다. 예를 들어 Monitor 역할을 가진 사용자는 볼륨에 대한 모든 정보를 볼 수 있지만 해당 볼륨을 수정하기 위한 기능에는 액세스할 수 없습니다. Copy Services \* 및 \* Add to Workload \* 와 같은 기능에 대한 탭은 회색으로 표시되고 보기/편집 설정만 사용할 수 있습니다.

## SANtricity 스토리지 관리자에 대한 사용자 액세스 권한

로컬 사용자 역할 및 디렉터리 서비스가 구성된 경우 사용자는 EMW(Enterprise Management Window)에서 다음 기능을 수행하기 전에 자격 증명을 입력해야 합니다.

- 스토리지 배열의 이름을 바꿉니다
- 컨트롤러 펌웨어 업그레이드 중
- 스토리지 배열 구성을 로드하는 중입니다
- 스크립트 실행
- 사용하지 않는 세션이 시간 초과된 경우 활성 작업을 수행하려고 합니다

스토리지에 대해 SAML이 구성된 경우 사용자는 EMW를 사용하여 해당 스토리지에 대한 스토리지를 검색 또는 관리할 수 없습니다.

## Access Management(액세스 관리) 용어

액세스 관리 용어가 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

기간	설명
Active Directory를 클릭합니다	AD(Active Directory)는 Windows 도메인 네트워크에 LDAP를 사용하는 Microsoft 디렉터리 서비스입니다.
바인딩	바인딩 작업은 클라이언트를 디렉터리 서버에 인증하는 데 사용됩니다. 일반적으로 바인딩에는 계정 및 암호 자격 증명이 필요하지만 일부 서버에서는 익명 바인딩 작업을 허용합니다.

기간	설명
CA	CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.
인증서	인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.
IDP	IDP(Identity Provider)는 사용자의 자격 증명을 요청하고 해당 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. IDP는 다중 요소 인증을 제공하고 Active Directory와 같은 사용자 데이터베이스를 사용하도록 구성할 수 있습니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다.
LDAP를 지원합니다	LDAP(Lightweight Directory Access Protocol)는 분산 디렉터리 정보 서비스에 액세스하고 유지 관리하기 위한 애플리케이션 프로토콜입니다. 이 프로토콜을 사용하면 다양한 응용 프로그램 및 서비스를 LDAP 서버에 연결하여 사용자의 유효성을 검사할 수 있습니다.
RBAC	역할 기반 액세스 제어(RBAC)는 개별 사용자의 역할에 따라 컴퓨터 또는 네트워크 리소스에 대한 액세스를 제어하는 방법입니다. RBAC 제어는 스토리지 어레이에 적용되고 사전 정의된 역할을 포함합니다.
SAML	SAML(Security Assertion Markup Language)은 두 개체 간의 인증 및 승인을 위한 XML 기반 표준입니다. SAML을 사용하면 다중 요소 인증을 수행할 수 있습니다. 사용자는 ID를 입증하기 위해 두 개 이상의 항목(예: 암호 및 지문)을 제공해야 합니다. 스토리지에 포함된 SAML 기능은 ID 어설션, 인증 및 권한 부여에 대해 SAML2.0을 준수합니다.
SP	서비스 공급자(SP)는 사용자 인증 및 액세스를 제어하는 시스템입니다. SAML로 액세스 관리를 구성하면 스토리지 어레이가 ID Provider에서 인증을 요청하는 서비스 공급자 역할을 합니다.
SSO	SSO(Single Sign-On)는 하나의 로그인 자격 증명 세트로 여러 응용 프로그램에 액세스할 수 있는 인증 서비스입니다.

## 매핑된 역할에 대한 권한

스토리지 어레이에 적용된 RBAC(역할 기반 액세스 제어) 기능에는 하나 이상의 역할이 매핑된 사전 정의된 사용자 프로필이 포함됩니다. 각 역할에는 SANtricity 시스템 관리자의 작업에 액세스할 수 있는 권한이 포함되어 있습니다.

사용자 프로필 및 매핑된 역할은 System Manager의 사용자 인터페이스에서 설정 [액세스 관리 > 로컬 사용자 역할] 메뉴에서 액세스할 수 있습니다.

역할은 다음과 같이 작업에 대한 사용자 액세스를 제공합니다.

- \* 스토리지 관리자 \* — 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
- \* 보안 관리자 \* — 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
- \* 지원 관리자 \* — 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
- \* Monitor \* — 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용자에게 특정 작업에 대한 권한이 없는 경우 해당 작업은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다.

## 로컬 사용자 역할을 사용하여 액세스 관리

액세스 관리의 경우 관리자는 스토리지 어레이에 적용된 RBAC(역할 기반 액세스 제어) 기능을 사용할 수 있습니다. 이러한 기능을 "로컬 사용자 역할"이라고 합니다.

### 구성 워크플로우

로컬 사용자 역할은 스토리지에 대해 사전 구성됩니다. 로컬 사용자 역할을 인증에 사용하려면 관리자가 다음을 수행할 수 있습니다.

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 SANtricity 시스템 관리자에 로그인합니다.



admin 사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

2. 관리자는 사용자 프로파일을 검토합니다. 사용자 프로필은 미리 정의되어 있으며 수정할 수 없습니다.
3. 필요에 따라 관리자는 각 사용자 프로필에 대해 새 암호를 할당합니다.
4. 사용자는 할당된 자격 증명을 사용하여 시스템에 로그인합니다.

### 관리

인증에 로컬 사용자 역할만 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

- 암호를 변경합니다.
- 암호의 최소 길이를 설정합니다.
- 사용자가 암호 없이 로그인할 수 있도록 허용합니다.

## 디렉토리 서비스를 통한 액세스 관리

액세스 관리의 경우 관리자는 LDAP(Lightweight Directory Access Protocol) 서버와 Microsoft의 Active Directory와 같은 디렉토리 서비스를 사용할 수 있습니다.

### 구성 워크플로우

네트워크에서 LDAP 서버 및 디렉토리 서비스를 사용하는 경우 구성은 다음과 같이 작동합니다.

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 SANtricity 시스템 관리자에 로그인합니다.



admin 사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

2. 관리자는 LDAP 서버에 대한 구성 설정을 입력합니다. 설정에는 도메인 이름, URL 및 바인딩 계정 정보가 포함됩니다.
3. LDAP 서버가 보안 프로토콜(LDAPS)을 사용하는 경우 관리자는 LDAP 서버와 스토리지 시스템 간의 인증을 위해 CA(인증 기관) 인증서 체인을 업로드합니다.
4. 서버 연결이 설정되면 관리자는 사용자 그룹을 스토리지 시스템의 역할에 매핑합니다. 이러한 역할은 미리 정의되어 있으며 수정할 수 없습니다.
5. 관리자는 LDAP 서버와 스토리지 시스템 간의 연결을 테스트합니다.
6. 사용자는 할당된 LDAP/Directory 서비스 자격 증명을 사용하여 시스템에 로그인합니다.

### 관리

인증을 위해 디렉토리 서비스를 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

- 디렉토리 서버를 추가합니다.
- 디렉토리 서버 설정을 편집합니다.
- LDAP 사용자를 로컬 사용자 역할에 매핑합니다.
- 디렉토리 서버를 제거합니다.

## SAML을 통한 액세스 관리

Access Management의 경우 관리자는 스토리지에 포함된 SAML(Security Assertion Markup Language) 2.0 기능을 사용할 수 있습니다.

### 구성 워크플로우

SAML 구성은 다음과 같이 작동합니다.

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 System Manager에 로그인합니다.



"admin" 사용자는 System Manager의 모든 기능에 액세스할 수 있습니다.

2. 관리자는 액세스 관리 아래의 \* SAML \* 탭으로 이동합니다.

3. 관리자는 ID 공급자(IDP)와의 통신을 구성합니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 스토리지 어레이와의 통신을 구성하기 위해 관리자는 IDP 시스템에서 IDP 메타데이터 파일을 다운로드한 다음 System Manager를 사용하여 파일을 스토리지 어레이에 업로드합니다.
4. 관리자는 서비스 공급자와 IDP 간의 신뢰 관계를 설정합니다. 서비스 공급자는 사용자 인증을 제어합니다. 이 경우 스토리지 배열의 컨트롤러는 서비스 공급자 역할을 합니다. 통신을 구성하기 위해 관리자는 System Manager를 사용하여 각 컨트롤러에 대한 서비스 공급자 메타데이터 파일을 내보냅니다. 그런 다음 관리자는 IDP 시스템에서 해당 메타데이터 파일을 IDP로 가져옵니다.



또한 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하는지 확인해야 합니다.

5. 관리자는 스토리지 어레이의 역할을 IDP에 정의된 사용자 속성에 매핑합니다. 이렇게 하려면 관리자가 System Manager를 사용하여 매핑을 생성합니다.
6. 관리자는 IDP URL에 대한 SSO 로그인을 테스트합니다. 이 테스트는 스토리지 배열 및 IDP가 통신할 수 있도록 보장합니다.



SAML이 활성화되면 사용자 인터페이스를 통해 이를 비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

7. System Manager에서 관리자는 스토리지 배열에 대해 SAML을 활성화합니다.
8. 사용자는 SSO 자격 증명을 사용하여 시스템에 로그인합니다.

## 관리

인증을 위해 SAML을 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

- 새 역할 매핑을 수정하거나 작성합니다
- 서비스 공급자 파일을 내보냅니다

## 액세스 제한

SAML이 활성화되면 다음 클라이언트가 스토리지 서비스 및 리소스에 액세스할 수 없습니다.

- 엔터프라이즈 관리 창(EMW)
- CLI(Command-Line Interface)
- SDK(소프트웨어 개발자 키트) 클라이언트
- 대역내 클라이언트
- HTTP 기본 인증 REST API 클라이언트
- 표준 REST API 끝점을 사용하여 로그인합니다

## 방법



## 로컬 사용자 역할을 봅니다

로컬 사용자 역할 탭에서 사용자 프로필의 매핑을 기본 역할에 표시할 수 있습니다. 이러한 매핑은 스토리지 어레이에서 적용되는 RBAC(역할 기반 액세스 제어)의 일부입니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

이 작업에 대해

사용자 프로파일과 매핑은 변경할 수 없습니다. 암호만 수정할 수 있습니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 로컬 사용자 역할 \* 탭을 선택합니다.

사용자 프로파일이 표에 표시됩니다.

- \* 루트 관리자 \* (admin) — 시스템의 모든 기능에 액세스할 수 있는 슈퍼 관리자. 이 사용자 프로필에는 모든 역할이 포함되어 있습니다.
- \* 스토리지 관리자 \* (스토리지) — 모든 스토리지 프로비저닝을 담당하는 관리자. 이 사용자 프로필에는 스토리지 관리자, 지원 관리자 및 모니터 역할이 포함됩니다.
- \* 보안 관리자 \* (보안) — 액세스 관리, 인증서 관리 및 보안 활성화 드라이브 기능을 비롯한 보안 구성을 담당하는 사용자입니다. 이 사용자 프로필에는 보안 관리 및 모니터 역할이 포함되어 있습니다.
- \* 지원 관리자 \* (지원) — 하드웨어 리소스, 오류 데이터 및 펌웨어 업그레이드를 담당하는 사용자입니다. 이 사용자 프로필에는 지원 관리자 및 모니터 역할이 포함되어 있습니다.
- \* 모니터 \* (모니터) — 시스템에 대한 읽기 전용 액세스 권한이 있는 사용자입니다. 이 사용자 프로필에는 Monitor 역할만 포함됩니다.

## 암호를 변경합니다

Access Management에서 각 사용자 프로필에 대한 사용자 암호를 변경할 수 있습니다.

시작하기 전에

- 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.
- 로컬 관리자 암호를 알아야 합니다.

이 작업에 대해

암호를 선택할 때는 다음 지침을 염두에 두십시오.

- 새 로컬 사용자 암호는 최소 암호(보기/편집 설정)에 대한 현재 설정을 충족하거나 초과해야 합니다.
- 암호는 대/소문자를 구분합니다.
- 후행 공백이 설정된 경우 암호에서 제거되지는 않습니다. 암호에 공백이 포함된 경우 해당 공백을 포함해야 합니다.
- 보안을 강화하려면 15자 이상의 영숫자 문자를 사용하고 암호를 자주 변경하십시오.



System Manager에서 암호를 변경하면 CLI(Command Line Interface)에서도 암호가 변경됩니다.  
또한 암호를 변경하면 사용자의 활성 세션이 종료됩니다.

#### 단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 로컬 사용자 역할 \* 탭을 선택합니다.
3. 테이블에서 사용자를 선택합니다.

암호 변경 \* 버튼을 사용할 수 있게 됩니다.

4. 암호 변경 \* 을 선택합니다.

암호 변경 \* 대화 상자가 열립니다.

5. 로컬 사용자 암호에 대해 최소 암호 길이를 설정하지 않은 경우 선택한 사용자가 스토리지 배열에 액세스하기 위해 암호를 입력하도록 확인란을 선택한 다음 선택한 사용자의 새 암호를 입력할 수 있습니다.
6. 로컬 관리자 암호를 입력한 다음 \* 변경 \* 을 클릭합니다.

#### 결과

사용자가 현재 로그인한 경우 암호 변경으로 인해 사용자의 활성 세션이 종료됩니다.

### 로컬 사용자 암호 설정을 변경합니다

스토리지 배열의 새 로컬 사용자 암호 또는 업데이트된 로컬 사용자 암호의 최소 길이를 설정할 수 있습니다. 또한 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스하도록 허용할 수 있습니다.

#### 시작하기 전에

- 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.

#### 이 작업에 대해

로컬 사용자 암호의 최소 길이를 설정할 때는 다음 지침을 염두에 두십시오.

- 설정을 변경해도 기존 로컬 사용자 암호에는 영향을 주지 않습니다.
- 로컬 사용자 암호에 필요한 최소 길이 설정은 0자에서 30자 사이여야 합니다.
- 새 로컬 사용자 암호는 현재 최소 길이 설정을 충족하거나 초과해야 합니다.
- 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스하도록 하려면 암호의 최소 길이를 설정하지 마십시오.

#### 단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 로컬 사용자 역할 \* 탭을 선택합니다.
3. 설정 보기/편집 \* 버튼을 선택합니다.

로컬 사용자 암호 설정 \* 대화 상자가 열립니다.

4. 다음 중 하나를 수행합니다.

- 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스할 수 있도록 하려면 "모든 로컬 사용자 암호를 최소 이상으로 요구" 확인란의 선택을 취소합니다.
- 모든 로컬 사용자 암호에 대해 최소 암호 길이를 설정하려면 "모든 로컬 사용자 암호를 최소 이상으로 요구" 확인란을 선택한 다음 spinner 상자를 사용하여 모든 로컬 사용자 암호에 필요한 최소 길이를 설정합니다.

새 로컬 사용자 암호는 현재 설정을 충족하거나 초과해야 합니다.

5. 저장 \* 을 클릭합니다.

## 디렉토리 서버를 추가합니다

액세스 관리에 대한 인증을 구성하려면 스토리지 어레이와 LDAP 서버 간의 통신을 설정한 다음 LDAP 사용자 그룹을 스토리지의 사전 정의된 역할에 매핑할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
- 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
- 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

이 작업에 대해

디렉토리 서버를 추가하는 과정은 2단계로 이루어집니다. 먼저 도메인 이름과 URL을 입력합니다. 서버에서 보안 프로토콜을 사용하는 경우 비표준 서명 기관에서 서명한 경우 인증을 위한 CA 인증서도 업로드해야 합니다. 바인딩 계정에 대한 자격 증명이 있는 경우 사용자 계정 이름 및 암호를 입력할 수도 있습니다. 그런 다음 LDAP 서버의 사용자 그룹을 스토리지의 사전 정의된 역할에 매핑합니다.



LDAP 서버를 추가하는 절차 중에는 레거시 관리 인터페이스가 비활성화됩니다. 기존 관리 인터페이스(symbol)는 스토리지 배열과 관리 클라이언트 간의 통신 방법입니다. 이 기능을 해제하면 스토리지 어레이와 관리 클라이언트에서 더욱 안전한 통신 방법(https를 통한 REST API)을 사용합니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 디렉터리 서비스 \* 탭에서 \* 디렉터리 서버 추가 \* 를 선택합니다.

디렉터리 서버 추가 \* 대화 상자가 열립니다.

3. 서버 설정 \* 탭에서 LDAP 서버의 자격 증명을 입력합니다.

필드 세부 정보

설정	설명
<ul style="list-style-type: none"> <li>구성 설정 *</li> </ul>	도메인
LDAP 서버의 도메인 이름을 입력합니다. 여러 도메인의 경우 심표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인( <i>username @domain</i> )에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.	서버 URL
LDAP 서버에 액세스하기 위한 URL을 'LDAP[s]://host:port' 형식으로 입력합니다.	인증서 업로드(선택 사항)
 이 필드는 LDAPS 프로토콜이 위의 서버 URL 필드에 지정된 경우에만 나타납니다.  찾아보기 * 를 클릭하고 업로드할 CA 인증서를 선택합니다. LDAP 서버를 인증하는 데 사용되는 신뢰할 수 있는 인증서 또는 인증서 체인입니다.	BIND ACCOUNT(선택 사항)
LDAP 서버에 대한 검색 쿼리 및 그룹 내에서 검색할 읽기 전용 사용자 계정을 입력합니다. LDAP 유형 형식으로 계정 이름을 입력합니다. 예를 들어 바인딩 사용자가 "bindacct"라고 하는 경우 "CN=bindacct, CN=Users, DC=CPoC, DC=local"과 같은 값을 입력할 수 있습니다.	바인딩 암호(선택 사항)
 이 필드는 위에 바인딩 계정을 입력할 때 나타납니다.  바인딩 계정의 암호를 입력합니다.	추가하기 전에 서버 연결을 테스트합니다
스토리지 배열이 입력한 LDAP 서버 구성과 통신할 수 있는지 확인하려면 이 확인란을 선택합니다. 이 테스트는 대화 상자 하단의 * 추가 * 를 클릭하면 발생합니다. 이 확인란을 선택하고 테스트에 실패하면 구성이 추가되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 추가할 수 있습니다.	<ul style="list-style-type: none"> <li>권한 설정**</li> </ul>
검색 기준 DN	사용자를 검색할 LDAP 컨텍스트를 일반적으로 'CN=Users,DC=copc,DC=local' 형식으로 입력합니다.

설정	설명
사용자 이름 특성입니다	인증을 위해 사용자 ID에 바인딩된 특성을 입력합니다. 예를 들어, 'sAMAccountName'을 입력합니다.
그룹 속성	그룹 대 역할 매핑에 사용되는 사용자의 그룹 속성 목록을 입력합니다. 예를 들어, memberOf , managedObjects 등이 있습니다.

- [역할 매핑]\*\* 탭을 클릭합니다.
- 미리 정의된 역할에 LDAP 그룹을 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.

#### 필드 세부 정보

설정	설명
• 매핑 *	그룹 DN
매핑할 LDAP 사용자 그룹의 그룹 DN(고유 이름)을 지정합니다.	역할



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에 대해서는 System Manager가 올바르게 작동하지 않습니다.

- 필요한 경우 \* 다른 매핑 추가 \* 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.
- 매핑을 마쳤으면 \* 추가 \* 를 클릭합니다.

시스템은 스토리지 시스템 및 LDAP 서버가 통신할 수 있도록 검증을 수행합니다. 오류 메시지가 나타나면 대화 상자에 입력한 자격 증명을 확인하고 필요한 경우 정보를 다시 입력합니다.

## 디렉토리 서버 설정 및 역할 매핑을 편집합니다

이전에 Access Management에서 디렉터리 서버를 구성한 경우 언제든지 해당 설정을 변경할 수 있습니다. 설정에는 서버 연결 정보와 그룹 대 역할 매핑이 포함됩니다.

### 시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- 디렉토리 서버를 정의해야 합니다.

### 단계

- 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.

2. 디렉터리 서비스 \* 탭을 선택합니다.
3. 둘 이상의 서버가 정의된 경우 테이블에서 편집할 서버를 선택합니다.
4. 설정 보기/편집 \* 을 선택합니다.

디렉터리 서버 설정 \* 대화 상자가 열립니다.

5. 서버 설정 \* 탭에서 원하는 설정을 변경합니다.

설정	설명
• 구성 설정 *	도메인
LDAP 서버의 도메인 이름입니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인( <i>username@domain</i> )에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.	서버 URL
LDAP 서버 접속에 대한 URL은 "LDAP[s]://host:port" 형식으로 되어 있습니다.	BIND ACCOUNT(선택 사항)
LDAP 서버에 대한 검색 쿼리 및 그룹 내 검색을 위한 읽기 전용 사용자 계정입니다.	바인딩 암호(선택 사항)
바인딩 계정의 암호입니다. (이 필드는 바인딩 계정을 입력할 때 나타납니다.)	저장하기 전에 서버 연결을 테스트합니다
스토리지 배열이 LDAP 서버 구성과 통신할 수 있는지 확인합니다. 이 테스트는 대화 상자 하단의 Save(저장)를 클릭한 후에 수행됩니다. 이 확인란을 선택하고 검사에 실패하면 구성이 변경되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 다시 편집할 수 있습니다.	• 권한 설정 *
검색 기준 DN	일반적으로 사용자를 검색할 LDAP 컨텍스트는 'CN=Users,DC=copc,DC=local' 형식입니다.
사용자 이름 특성입니다	인증을 위해 사용자 ID에 바인딩된 속성입니다. 예를 들어, 'sAMAccountName'을 입력합니다.
그룹 속성	그룹-역할 매핑에 사용되는 사용자의 그룹 속성 목록입니다. 예를 들어, memberOf , managedObjects 등이 있습니다.

6. 역할 매핑 \* 탭에서 원하는 매핑을 변경합니다.

설정	설명
• 매핑 *	그룹 DN
매핑할 LDAP 사용자 그룹의 도메인 이름입니다.	역할



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

7. 필요한 경우 \* 다른 매핑 추가 \* 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.

8. 저장 \* 을 클릭합니다.

#### 결과

이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

### 디렉토리 서버를 제거합니다

디렉토리 서버와 스토리지 시스템 간의 접속을 끊는 경우 Access Management 페이지에서 서버 정보를 제거할 수 있습니다. 새 서버를 구성한 다음 이전 서버를 제거하려는 경우 이 작업을 수행할 수 있습니다.

#### 시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

#### 이 작업에 대해

이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

#### 단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 디렉터리 서비스 \* 탭을 선택합니다.
3. 목록에서 삭제할 디렉터리 서버를 선택합니다.
4. 제거 \* 를 클릭합니다.

디렉터리 서버 제거 \* 대화 상자가 열립니다.

5. 필드에 remove를 입력한 다음 \* Remove \* 를 클릭합니다.

디렉터리 서버 구성 설정, 권한 설정 및 역할 매핑이 제거됩니다. 사용자는 더 이상 이 서버의 자격 증명으로 로그인할 수 없습니다.

### SAML을 구성합니다

액세스 관리에 대한 인증을 구성하려면 스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용할 수 있습니다. 이 구성은 ID 공급자와 스토리지 공급자 간의

## 연결을 설정합니다.

### 이 작업에 대해

IDP(Identity Provider)는 사용자의 자격 증명을 요청하고 해당 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. IDP는 다중 요소 인증을 제공하고 Active Directory와 같은 사용자 데이터베이스를 사용하도록 구성할 수 있습니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다. 서비스 공급자(SP)는 사용자 인증 및 액세스를 제어하는 시스템입니다. SAML로 액세스 관리를 구성하면 스토리지 어레이가 ID Provider에서 인증을 요청하는 서비스 공급자 역할을 합니다. IDP와 스토리지 어레이 간의 연결을 설정하려면 이 두 엔터티 간에 메타데이터 파일을 공유합니다. 다음으로 IDP 사용자 엔터티를 스토리지 어레이 역할에 매핑합니다. 마지막으로 SAML을 활성화하기 전에 연결 및 SSO 로그인을 테스트합니다.



- SAML 및 디렉토리 서비스 \* 디렉터리 서비스가 인증 방법으로 구성되어 있을 때 SAML을 설정하면 SAML이 System Manager의 디렉터리 서비스를 대체합니다. 나중에 SAML을 사용하지 않도록 설정하면 Directory Services 구성이 이전 구성으로 돌아갑니다.



- 편집 및 비활성화 \* SAML이 활성화되면 사용자 인터페이스를 통해 이를 \_비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

SAML 인증 구성은 다단계 절차입니다.

- 1단계: IDP 메타데이터 파일을 업로드합니다
- 2단계: 서비스 제공업체 파일 내보내기
- 3단계: 역할 매핑
- 4단계: SSO 로그인을 테스트합니다
- 5단계: SAML을 활성화합니다

**1단계: IDP 메타데이터 파일을 업로드합니다**

IDP 연결 정보를 스토리지 어레이에 제공하기 위해 IDP 메타데이터를 System Manager로 가져옵니다.

### 시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- IDP 관리자가 IDP 시스템을 구성했습니다.
- IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
- 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클럭이 동기화되도록 했습니다.
- IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 System Manager 액세스에 사용되는 로컬 시스템에서 사용할 수 있습니다.

### 이 작업에 대해

이 작업에서는 IDP의 메타데이터 파일을 System Manager로 업로드합니다. IDP 시스템은 인증 요청을 올바른 URL로 리디렉션하고 받은 응답을 검증하려면 이 메타데이터가 필요합니다. 두 개의 컨트롤러가 있더라도 스토리지 어레이에 대해 하나의 메타데이터 파일만 업로드하면 됩니다.



## 단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. SAML \* 탭을 선택합니다.

구성 단계의 개요가 페이지에 표시됩니다.

3. IdP(ID 공급자 가져오기) 파일 \* 링크를 클릭합니다.

ID 공급자 파일 가져오기 \* 대화 상자가 열립니다.

4. 로컬 시스템에 복사한 IDP 메타데이터 파일을 선택하여 업로드하려면 \* 찾아보기 \* 를 클릭합니다.

파일을 선택하면 IDP 엔티티 ID가 표시됩니다.

5. 가져오기 \* 를 클릭합니다.

## 2단계: 서비스 제공업체 파일 내보내기

IDP와 스토리지 어레이 간의 신뢰 관계를 설정하려면 서비스 공급자 메타데이터를 IDP로 가져옵니다.

### 시작하기 전에

- 스토리지 어레이에 있는 각 컨트롤러의 IP 주소 또는 도메인 이름을 알고 있습니다.

### 이 작업에 대해

이 작업에서는 컨트롤러에서 메타데이터를 내보냅니다(각 컨트롤러에 대해 파일 1개). IDP는 컨트롤러와 신뢰 관계를 설정하고 승인 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 서비스 공급자와 통신할 수 있도록 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

## 단계

1. Export Service Provider files \*(서비스 제공자 파일 내보내기 \*) 링크를 클릭합니다.

서비스 공급자 파일 내보내기 \* 대화 상자가 열립니다.

2. 컨트롤러 A \* 필드에 컨트롤러 IP 주소 또는 DNS 이름을 입력한 다음 \* 내보내기 \* 를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다. 스토리지 배열에 두 개의 컨트롤러가 포함된 경우, \* Controller B \* 필드의 두 번째 컨트롤러에 대해 이 단계를 반복합니다.

내보내기 를 클릭하면 서비스 공급자 메타데이터가 로컬 시스템에 다운로드됩니다. 파일이 저장된 위치를 기록해 둡니다.

3. 로컬 시스템에서 내보낸 서비스 공급자 메타데이터 파일을 찾습니다.

각 컨트롤러마다 XML 형식의 파일이 하나씩 있습니다.

4. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져와 트러스트 관계를 설정합니다. 파일을 직접 가져오거나 파일에서 컨트롤러 정보를 수동으로 입력할 수 있습니다.

### 3단계: 역할 매핑

사용자에게 System Manager에 대한 권한 부여 및 액세스 권한을 제공하려면 IDP 사용자 특성 및 그룹 멤버십을 스토리지 어레이의 사전 정의된 역할에 매핑해야 합니다.

시작하기 전에

- IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
- IDP 메타데이터 파일을 System Manager로 가져웁니다.
- 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.

이 작업에 대해

이 작업에서는 System Manager를 사용하여 IDP 그룹을 로컬 사용자 역할에 매핑합니다.

단계

1. System Manager 역할 매핑 링크를 클릭합니다.

역할 매핑 \* 대화 상자가 열립니다.

2. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.

필드 세부 정보

설정	설명
• 매핑 *	사용자 속성
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.	속성 값
매핑할 그룹의 속성 값을 지정합니다.	역할



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

3. 필요한 경우 \* 다른 매핑 추가 \* 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.



역할 매핑은 SAML이 활성화된 후에 수정할 수 있습니다.

4. 매핑을 마치면 \* 저장 \* 을 클릭합니다.

### 4단계: SSO 로그인을 테스트합니다

IDP 시스템 및 스토리지 어레이가 통신할 수 있도록 SSO 로그인을 선택적으로 테스트할 수 있습니다. 이 테스트는 SAML을 활성화하기 위한 마지막 단계에서도 수행됩니다.

시작하기 전에

- IDP 메타데이터 파일을 System Manager로 가져옵니다.
- 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.

#### 단계

1. Test SSO Login \* 링크를 선택합니다.

SSO 자격 증명을 입력하기 위한 대화 상자가 열립니다.

2. 보안 관리자 권한과 모니터 권한이 모두 있는 사용자의 로그인 자격 증명을 입력합니다.

시스템에서 로그인을 테스트하는 동안 대화 상자가 열립니다.

3. 테스트 성공 메시지를 찾습니다. 테스트가 성공적으로 완료되면 SAML 활성화를 위한 다음 단계로 이동합니다.

테스트가 성공적으로 완료되지 않으면 추가 정보와 함께 오류 메시지가 나타납니다. 다음을 확인합니다.

- 사용자는 보안 관리자 및 모니터 권한이 있는 그룹에 속합니다.
- IDP 서버에 대해 업로드한 메타데이터가 정확합니다.
- SP 메타데이터 파일의 컨트롤러 주소가 올바릅니다.

#### 5단계: SAML을 활성화합니다

마지막 단계는 SAML 사용자 인증을 활성화하는 것입니다.

#### 시작하기 전에

- IDP 메타데이터 파일을 System Manager로 가져옵니다.
- 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.
- 하나 이상의 Monitor 및 Security Admin 역할 매핑이 구성되어 있습니다.

#### 이 작업에 대해

이 작업은 사용자 인증을 위해 SAML 구성을 완료하는 방법을 설명합니다. 이 프로세스 중에 SSO 로그인을 테스트하라는 메시지가 표시됩니다. SSO 로그인 테스트 프로세스는 이전 단계에서 설명합니다.



- 편집 및 비활성화 \* SAML이 활성화되면 사용자 인터페이스를 통해 이를 \_비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

#### 단계

1. SAML \* 탭에서 \* SAML \* 활성화 링크를 선택합니다.

SAML \* 활성화 확인 대화 상자가 열립니다.

2. "enable"을 입력한 다음 \* Enable \* 을 클릭합니다.
3. SSO 로그인 테스트에 대한 사용자 자격 증명을 입력합니다.

#### 결과

시스템에서 SAML을 활성화하면 모든 활성 세션이 종료되고 SAML을 통해 사용자 인증이 시작됩니다.

## SAML 역할 매핑을 변경합니다

이전에 Access Management에 SAML을 구성한 경우 IDP 그룹과 스토리지 배열의 사전 정의된 역할 간의 역할 매핑을 변경할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
- SAML이 구성 및 활성화되었습니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. SAML \* 탭을 선택합니다.
3. 역할 매핑 \* 을 선택합니다.

역할 매핑 \* 대화 상자가 열립니다.

4. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.



SAML이 활성화되어 있는 동안에는 권한을 제거하지 않도록 주의하십시오. 그렇지 않으면 System Manager에 액세스할 수 없게 됩니다.

필드 세부 정보

설정	설명
• 매핑 *	사용자 속성
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.	속성 값
매핑할 그룹의 속성 값을 지정합니다.	역할



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

5. \* 선택 사항: \* 다른 매핑 추가 \* 를 클릭하여 추가 그룹-역할 매핑을 입력합니다.
6. 저장 \* 을 클릭합니다.

결과

이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

## SAML 서비스 공급자 파일을 내보냅니다

필요한 경우 스토리지 배열에 대한 서비스 공급자 메타데이터를 내보내고 해당 파일을 IdP(Identity Provider) 시스템으로 다시 가져올 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- SAML이 구성 및 활성화되었습니다.

이 작업에 대해

이 작업에서는 컨트롤러에서 메타데이터를 내보냅니다(각 컨트롤러에 대해 파일 1개). IDP는 컨트롤러와 신뢰 관계를 설정하고 인증 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 요청을 보내는 데 사용할 수 있는 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. SAML \* 탭을 선택합니다.
3. 내보내기 \* 를 선택합니다.

서비스 공급자 파일 내보내기 \* 대화 상자가 열립니다.

4. 각 컨트롤러에 대해 \* Export \* (내보내기 \*)를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다.



각 컨트롤러의 도메인 이름 필드는 읽기 전용입니다.

파일이 저장된 위치를 기록해 둡니다.

5. 로컬 시스템에서 내보낸 서비스 공급자 메타데이터 파일을 찾습니다.

각 컨트롤러마다 XML 형식의 파일이 하나씩 있습니다.

6. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져옵니다. 파일을 직접 가져오거나 해당 파일에서 컨트롤러 정보를 수동으로 입력할 수 있습니다.
7. 닫기 \* 를 클릭합니다.

## 감사 로그 활동을 봅니다

보안 관리자 권한이 있는 사용자는 감사 로그를 보고 사용자 작업, 인증 실패, 잘못된 로그인 시도 및 사용자 세션 수명을 모니터링할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.




2. Audit Log(감사 로그) \* 탭을 선택합니다.

◦ 감사 로그 \* 작업은 표 형식으로 표시되며 다음과 같은 정보 열이 포함되어 있습니다.

- \* 날짜/시간 \* — 스토리지 배열이 이벤트를 감지한 때의 타임스탬프(GMT).
- \* 사용자 이름 \* — 이벤트와 연결된 사용자 이름입니다. 스토리지 시스템에서 인증되지 않은 작업의 경우 "N/A"가 사용자 이름으로 나타납니다. 인증되지 않은 작업은 내부 프록시 또는 다른 메커니즘에 의해 트리거될 수 있습니다.
- \* 상태 코드 \* — 작업의 HTTP 상태 코드(200, 400 등) 및 이벤트와 관련된 설명 텍스트입니다.
- \* URL 액세스 \* — 전체 URL(호스트 포함) 및 쿼리 문자열
- \* 클라이언트 IP 주소 \* — 이벤트와 연결된 클라이언트의 IP 주소입니다.
- \* 소스 \* — 이벤트와 연결된 로깅 소스로, System Manager, CLI, 웹 서비스 또는 지원 셸이 될 수 있습니다.

3. 감사 로그 페이지의 선택 항목을 사용하여 이벤트를 보고 관리할 수 있습니다.

선택 세부 정보

선택	설명
이벤트 표시...	날짜 범위별로 표시되는 이벤트 제한(지난 24시간, 지난 7일, 지난 30일 또는 사용자 지정 날짜 범위)
필터	필드에 입력한 문자로 표시되는 이벤트를 제한합니다. 따옴표(" ")를 사용하여 정확히 일치하는 단어를 선택하거나, 또는 "를 입력하여 하나 이상의 단어를 반환하거나, 대시(--))를 입력하여 단어를 생략합니다.
새로 고침	페이지를 최신 이벤트로 업데이트하려면 * Refresh * 를 선택합니다.
설정 보기/편집	설정 보기/편집 * 을 선택하여 전체 로그 정책 및 기록할 작업 수준을 지정할 수 있는 대화 상자를 엽니다.
이벤트를 삭제합니다	페이지에서 이전 이벤트를 제거할 수 있는 대화 상자를 열려면 * 삭제 * 를 선택합니다.
열 표시/숨기기	<p>표시/숨기기 * 열 아이콘을 클릭합니다  테이블에 표시할 추가 열을 선택합니다. 추가 열은 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>• * Method * — HTTP 메서드(예: POST, GET, DELETE 등).</li> <li>• * CLI 명령 실행됨 * — Secure CLI 요청에 대해 실행되는 CLI 명령(문법)</li> <li>• * CLI return Status * — CLI 상태 코드 또는 클라이언트의 입력 파일 요청입니다.</li> <li>• * 기호 프로시저 * — 기호 프로시저가 실행됩니다.</li> <li>• * SSH 이벤트 유형 * — 로그인, 로그아웃 및 login_fail과 같은 SSH(Secure Shell) 이벤트 유형</li> <li>• * SSH 세션 PID * — SSH 세션의 프로세스 ID 번호입니다.</li> <li>• * SSH 세션 지속 시간 * — 사용자가 로그인한 시간(초)입니다.</li> </ul>
열 필터를 전환합니다	토글 * 아이콘을 클릭합니다  각 열의 필터링 필드를 엽니다. 열 필드에 문자를 입력하여 해당 문자로 표시되는 이벤트를 제한합니다. 필터링 필드를 닫으려면 아이콘을 다시 클릭합니다.
변경 내용을 취소합니다	실행 취소 * 아이콘을 클릭합니다  를 눌러 테이블을 기본 구성으로 되돌립니다.
내보내기	내보내기 * 를 클릭하여 테이블 데이터를 CSV(쉼표로 구분된 값) 파일에 저장합니다.

## 감사 로그 정책을 정의합니다

덮어쓰기 정책과 감사 로그에 기록된 이벤트 유형을 변경할 수 있습니다.

### 시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

### 이 작업에 대해

이 작업에서는 이전 이벤트를 덮어쓰는 정책과 이벤트 유형을 기록하는 정책을 비롯한 감사 로그 설정을 변경하는 방법에 대해 설명합니다.



### 단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. Audit Log(감사 로그) \* 탭을 선택합니다.
3. 설정 보기/편집 \* 을 선택합니다.

감사 로그 설정 \* 대화 상자가 열립니다.

4. 기록된 이벤트 유형 또는 덮어쓰기 정책을 변경합니다.



설정	설명
<p>정책 덮어쓰기</p>	<p>최대 용량에 도달할 때 이전 이벤트를 덮어쓰는 정책을 결정합니다.</p> <ul style="list-style-type: none"> <li>* 감사 로그가 가득 차면 감사 로그의 가장 오래된 이벤트를 덮어쓰도록 허용 * — 감사 로그가 50,000개 레코드에 도달할 때 이전 이벤트를 덮어씹니다.</li> <li>* 감사 로그 이벤트를 수동으로 삭제해야 함 * — 이벤트가 자동으로 삭제되지 않도록 지정합니다. 대신 설정된 백분율로 임계값 경고가 표시됩니다. 이벤트는 수동으로 삭제해야 합니다.</li> </ul> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 덮어쓰기 정책을 사용하지 않도록 설정하고 감사 로그 항목이 최대 한도에 도달하면 보안 관리자 권한이 없는 사용자는 System Manager에 액세스할 수 없습니다. 보안 관리자 권한이 없는 사용자에게 대한 시스템 액세스를 복원하려면 보안 관리자 역할에 할당된 사용자가 이전 이벤트 레코드를 삭제해야 합니다.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> 감사 로그 보관을 위해 syslog 서버가 구성된 경우 덮어쓰기 정책은 적용되지 않습니다.</p> </div>
<p>기록할 작업 수준입니다</p>	<p>기록할 이벤트 유형을 결정합니다.</p> <ul style="list-style-type: none"> <li>* 수정 이벤트만 기록 * — 사용자 작업이 시스템에서 변경을 수행하는 이벤트만 표시합니다.</li> <li>* 모든 수정 및 읽기 전용 이벤트 기록 * — 정보를 읽거나 다운로드하는 사용자 작업을 포함한 모든 이벤트를 표시합니다.</li> </ul>

5. 저장 \* 을 클릭합니다.

### 감사 로그에서 이벤트를 삭제합니다

이전 이벤트의 감사 로그를 지울 수 있으므로 이벤트 검색을 보다 쉽게 관리할 수 있습니다. 삭제 시 이전 이벤트를 CSV(쉼표로 구분된 값) 파일에 저장할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

이 작업에 대해

이 작업에서는 감사 로그에서 이전 이벤트를 제거하는 방법에 대해 설명합니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. Audit Log(감사 로그) \* 탭을 선택합니다.
3. 삭제 \* 를 선택합니다.

감사 로그 삭제 대화 상자가 열립니다.

4. 삭제할 가장 오래된 이벤트 수를 선택하거나 입력합니다.
5. 삭제된 이벤트를 CSV 파일로 내보내려면(권장) 확인란을 선택한 상태로 유지합니다. 다음 단계에서 \* 삭제 \* 를 클릭하면 파일 이름과 위치를 입력하라는 메시지가 표시됩니다. 그렇지 않으면 이벤트를 CSV 파일에 저장하지 않으려면 확인란을 클릭하여 선택을 취소합니다.
6. 삭제 \* 를 클릭합니다.

확인 대화 상자가 열립니다.

7. 필드에 삭제 를 입력한 다음 \* 삭제 \* 를 클릭합니다.

가장 오래된 이벤트는 감사 로그 페이지에서 제거됩니다.

## 감사 로그를 위해 **syslog** 서버를 구성합니다

감사 로그를 외부 syslog 서버에 보관하려는 경우 해당 서버와 스토리지 시스템 간의 통신을 구성할 수 있습니다. 연결이 설정되면 감사 로그가 syslog 서버에 자동으로 저장됩니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- syslog 서버 주소, 프로토콜 및 포트 번호를 사용할 수 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- 서버에서 보안 프로토콜(예: TLS)을 사용하는 경우 로컬 시스템에서 인증 기관(CA) 인증서를 사용할 수 있어야 합니다. CA 인증서는 서버와 클라이언트 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 감사 로그 \* 탭에서 \* Syslog 서버 구성 \* 을 선택합니다.

Syslog 서버 구성 \* 대화 상자가 열립니다.

3. 추가 \* 를 클릭합니다.

Add Syslog Server \* 대화 상자가 열립니다.

4. 서버에 대한 정보를 입력한 다음 \* 추가 \* 를 클릭합니다.

- 서버 주소 — 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
- 프로토콜 — 드롭다운 목록에서 프로토콜을 선택합니다(예: TLS, UDP 또는 TCP).
- 인증서 업로드(선택 사항) — TLS 프로토콜을 선택했지만 아직 서명된 CA 인증서를 업로드하지 않은 경우 찾아보기를 클릭하여 인증서 파일을 업로드합니다. 감사 로그는 신뢰할 수 있는 인증서가 없는 syslog 서버에 보관되지 않습니다.



나중에 인증서가 유효하지 않게 되면 TLS 핸드셰이크가 실패합니다. 따라서 오류 메시지가 감사 로그에 게시되고 메시지가 더 이상 syslog 서버로 전송되지 않습니다. 이 문제를 해결하려면 syslog 서버의 인증서를 수정한 다음 설정 [감사 로그 > Syslog 서버 구성 > 모두 테스트] 메뉴로 이동해야 합니다.

- Port — syslog 수신기의 포트 번호를 입력합니다. Add \* 를 클릭하면 \* Configure Syslog Servers \* 대화 상자가 열리고 구성된 syslog 서버가 페이지에 표시됩니다.

5. 스토리지 배열과의 서버 연결을 테스트하려면 \* Test All \* 을 선택합니다.

결과

구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.

## 감사 로그 레코드에 대한 **syslog** 서버 설정을 편집합니다

감사 로그 아카이빙에 사용되는 syslog 서버의 설정을 변경하고 서버에 대한 새 CA(인증 기관) 인증서를 업로드할 수도 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- syslog 서버 주소, 프로토콜 및 포트 번호를 사용할 수 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- 새 CA 인증서를 업로드하는 경우 로컬 시스템에서 인증서를 사용할 수 있어야 합니다.

단계

1. 메뉴: 설정 [Access Management](액세스 관리)를 선택합니다.
2. 감사 로그 \* 탭에서 \* Syslog 서버 구성 \* 을 선택합니다.

구성된 syslog 서버가 페이지에 표시됩니다.

3. 서버 정보를 편집하려면 서버 이름 오른쪽에 있는 \* Edit \* (연필) 아이콘을 선택한 후 다음 필드에서 원하는 대로 변경합니다.
  - 서버 주소 — 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
  - 프로토콜 — 드롭다운 목록에서 프로토콜을 선택합니다(예: TLS, UDP 또는 TCP).
  - Port — syslog 수신기의 포트 번호를 입력합니다.

4. 프로토콜을 보안 TLS 프로토콜(UDP 또는 TCP)으로 변경한 경우 \* 신뢰할 수 있는 인증서 가져오기 \* 를 클릭하여 CA 인증서를 업로드합니다.
5. 스토리지 배열과의 새 연결을 테스트하려면 \* Test All \* 을 선택합니다.

결과

구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.

## FAQ 를 참조하십시오

### 로그인할 수 없는 이유는 무엇입니까?

System Manager에 로그인할 때 오류가 발생하면 다음과 같은 가능한 원인을 검토하십시오.

다음 이유 중 하나로 System Manager에 로그인 오류가 발생할 수 있습니다.

- 잘못된 사용자 이름 또는 암호를 입력했습니다.
- 권한이 부족합니다.
- 디렉토리 서버(구성된 경우)를 사용할 수 없습니다. 이 경우 로컬 사용자 역할로 로그인을 시도하십시오.
- 여러 번 로그인을 시도했으나 실패하여 잠금 모드가 시작되었습니다. 다시 로그인하려면 10분 정도 기다립니다.
- 잠금 조건이 트리거되었고 감사 로그가 꽉 찰 수 있습니다. Access Management(액세스 관리)로 이동하여 감사 로그에서 이전 이벤트를 삭제합니다.
- SAML 인증이 활성화되었습니다. 로그인하려면 브라우저를 새로 고치십시오.

미러링 작업을 위해 원격 스토리지 어레이에 로그인 오류가 발생하는 원인은 다음과 같습니다.

- 잘못된 암호를 입력했습니다.
- 여러 번 로그인을 시도했으나 실패하여 잠금 모드가 시작되었습니다. 10분 정도 기다린 후 다시 로그인하십시오.
- 컨트롤러에 사용된 최대 클라이언트 연결 수에 도달했습니다. 여러 사용자 또는 클라이언트를 확인합니다.

### 디렉토리 서버를 추가하기 전에 알아야 할 사항은 무엇입니까?

Access Management에서 디렉터리 서버를 추가하기 전에 다음 요구 사항을 충족하는지 확인합니다.

- 사용자 그룹은 디렉터리 서비스에 정의되어 있어야 합니다.
- 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
- 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

### 스토리지 어레이 역할에 매핑하는 방법에 대해 알아야 할 내용은 무엇입니까?

그룹을 역할에 매핑하기 전에 다음 지침을 검토하십시오.

스토리지 시스템의 내장 RBAC(역할 기반 액세스 제어) 기능에는 다음과 같은 역할이 포함됩니다.

- \* 스토리지 관리자 \* — 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
- \* 보안 관리자 \* — 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
- \* 지원 관리자 \* — 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
- \* Monitor \* — 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

## 디렉터리 서비스

LDAP(Lightweight Directory Access Protocol) 서버 및 디렉터리 서비스를 사용하는 경우 다음 사항을 확인하십시오.

- 관리자가 디렉터리 서비스에 사용자 그룹을 정의했습니다.
- LDAP 사용자 그룹의 그룹 도메인 이름을 알고 있습니다.
- Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

## SAML

스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하는 경우 다음 사항을 확인하십시오.

- IDP(Identity Provider) 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
- 그룹 구성원 이름을 알고 있습니다.
- Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

## 이 변경의 영향을 받을 수 있는 외부 관리 도구는 무엇입니까?

관리 인터페이스 전환 또는 SAML 인증 방법 사용과 같이 System Manager에서 특정 변경 작업을 수행할 경우 일부 외부 도구와 기능의 사용이 제한될 수 있습니다.

### 관리 인터페이스

레거시 관리 인터페이스 설정이 활성화되어 있지 않으면 SANtricity SMI-S Provider 또는 OnCommand Insight(OCI)와 같은 기존 관리 인터페이스(기호)와 직접 통신하는 도구가 작동하지 않습니다. 또한 이 설정이 비활성화되어 있으면 레거시 CLI 명령을 사용하거나 미러링 작업을 수행할 수 없습니다.

자세한 내용은 기술 지원 부서에 문의하십시오.

### SAML 인증

SAML이 활성화되면 다음 클라이언트가 스토리지 서비스 및 리소스에 액세스할 수 없습니다.

- 엔터프라이즈 관리 창(EMW)
- CLI(Command-Line Interface)
- SDK(소프트웨어 개발자 키트) 클라이언트

- 대역내 클라이언트
- HTTP 기본 인증 REST API 클라이언트
- 표준 REST API 끝점을 사용하여 로그인합니다

자세한 내용은 기술 지원 부서에 문의하십시오.

## **SAML**을 구성 및 활성화하기 전에 알아야 할 내용은 무엇입니까?

인증을 위해 SAML(Security Assertion Markup Language) 기능을 구성 및 활성화하기 전에 다음 요구 사항을 충족하고 SAML 제한 사항을 이해해야 합니다.

### 요구 사항

시작하기 전에 다음 사항을 확인하십시오.

- ID 공급자(IDP)가 네트워크에 구성되어 있습니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다.
- IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹을 구성했습니다.
- IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
- 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클럭이 동기화되도록 했습니다.
- IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 System Manager 액세스에 사용되는 로컬 시스템에서 사용할 수 있습니다.
- 스토리지 어레이에 있는 각 컨트롤러의 IP 주소 또는 도메인 이름을 알고 있습니다.

### 제한 사항

위의 요구 사항 외에 다음과 같은 제한 사항을 이해해야 합니다.

- SAML이 활성화되면 사용자 인터페이스를 통해 이를 비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오. 최종 구성 단계에서 SAML을 활성화하기 전에 SSO 로그인을 테스트하는 것이 좋습니다. (SAML을 활성화하기 전에 SSO 로그인 테스트도 수행합니다.)
- 나중에 SAML을 사용하지 않도록 설정하면 이전 구성(로컬 사용자 역할 및/또는 디렉터리 서비스)이 자동으로 복원됩니다.
- 디렉터리 서비스가 현재 사용자 인증을 위해 구성된 경우 SAML은 해당 구성을 재정의합니다.
- SAML이 구성된 경우 다음 클라이언트가 스토리지 시스템 리소스에 액세스할 수 없습니다.
  - 엔터프라이즈 관리 창(EMW)
  - CLI(Command-Line Interface)
  - SDK(소프트웨어 개발자 키트) 클라이언트
  - 대역내 클라이언트
  - HTTP 기본 인증 REST API 클라이언트
  - 표준 REST API 끝점을 사용하여 로그인합니다

## 감사 로그에 기록되는 이벤트 유형은 무엇입니까?

감사 로그는 수정 이벤트 또는 수정 이벤트와 읽기 전용 이벤트를 모두 기록할 수 있습니다.

정책 설정에 따라 다음과 같은 유형의 이벤트가 표시됩니다.

- \* 수정 이벤트 \* — 시스템 변경(예: 스토리지 프로비저닝)이 포함된 System Manager 내 사용자 조치.
- \* 수정 및 읽기 전용 이벤트 \* — 볼륨 할당 보기와 같은 정보 보기 또는 다운로드와 관련된 이벤트뿐만 아니라 시스템에 대한 변경 사항을 포함하는 사용자 작업입니다.

## syslog 서버를 구성하기 전에 알아야 할 내용은 무엇입니까?

외부 syslog 서버에 감사 로그를 보관할 수 있습니다.

syslog 서버를 구성하기 전에 다음 지침을 염두에 두십시오.

- 서버 주소, 프로토콜 및 포트 번호를 알고 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- 서버에서 보안 프로토콜(예: TLS)을 사용하는 경우 로컬 시스템에서 인증 기관(CA) 인증서를 사용할 수 있어야 합니다. CA 인증서는 서버와 클라이언트 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다.
- 구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.
- View/Edit Settings(설정 보기/편집)에서 사용할 수 있는 \* Overwrite Policy \*(정책 덮어쓰기) 설정은 syslog 서버 구성을 사용하여 로그를 관리하는 방법에 영향을 주지 않습니다.
- 감사 로그는 RFC 5424 메시징 형식을 따릅니다.

## syslog 서버가 더 이상 감사 로그를 수신하지 않습니다. 어떻게 해야 합니까?

TLS 프로토콜을 사용하여 syslog 서버를 구성한 경우 어떤 이유로든 인증서가 유효하지 않으면 서버에서 메시지를 수신할 수 없습니다. 유효하지 않은 인증서에 대한 오류 메시지가 감사 로그에 게시됩니다.

이 문제를 해결하려면 먼저 syslog 서버의 인증서를 수정해야 합니다. 유효한 인증서 체인이 배치되면 설정 [감사 로그 > Syslog 서버 구성 > 모두 테스트] 메뉴로 이동합니다.

## 저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

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