개념
SANtricity 11.8

NetApp
December 16, 2024

목차

개념

액세스 관리 작동 방식

Access Management를 사용하여 Unified Manager에서 사용자 인증을 설정합니다.

구성 워크플로우

Access Management 구성은 다음과 같이 작동합니다.

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

   처음 로그인하는 경우 사용자 이름이 `admin` 자동으로 표시되며 변경할 수 없습니다. `admin`사용자는 시스템의 모든 기능에 액세스할 수 있습니다. 암호는 처음 로그인할 때 설정해야 합니다.

2. 관리자는 미리 구성된 로컬 사용자 역할이 포함된 사용자 인터페이스에서 Access Management로 이동합니다. 이러한 역할은 RBAC(역할 기반 액세스 제어) 기능 구현입니다.
3. 관리자는 다음 인증 방법 중 하나 이상을 구성합니다.
   - * 로컬 사용자 역할 * — 인증은 RBAC 기능을 통해 관리됩니다. 로컬 사용자 역할에는 특정 액세스 권한을 가진 사전 정의된 사용자 및 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. 관리자가 LDAP 서버에 연결한 다음 LDAP 사용자를 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 Unified Manager에 대한 로그인 자격 증명을 제공합니다.
5. 사용자는 자격 증명을 입력하여 시스템에 로그인합니다. 로그인 중에 시스템은 다음과 같은 백그라운드 작업을 수행합니다.
   - 사용자 계정에 대해 사용자 이름과 암호를 인증합니다.
   - 할당된 역할에 따라 사용자의 권한을 결정합니다.
   - 사용자에게 사용자 인터페이스의 기능에 대한 액세스 권한을 제공합니다.
   - 상단 배너에 사용자 이름을 표시합니다.

기능은 **Unified Manager**에서 사용할 수 있습니다

기능에 대한 액세스는 사용자가 할당한 역할에 따라 달라집니다. 여기에는 다음이 포함됩니다.

- * 스토리지 관리자 * — 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
- * 보안 관리자 * — 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.

- * 지원 관리자 * — 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 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 기능은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다.

Access Management(액세스 관리) 용어

Unified Manager에 액세스 관리 용어가 어떻게 적용되는지 알아보십시오.

기간	설명
Active Directory를 클릭합니다	AD(Active Directory)는 Windows 도메인 네트워크에 LDAP를 사용하는 Microsoft 디렉터리 서비스입니다.
바인딩	바인딩 작업은 클라이언트를 디렉토리 서버에 인증하는 데 사용됩니다. 일반적으로 바인딩에는 계정 및 암호 자격 증명이 필요하지만 일부 서버에서는 익명 바인딩 작업을 허용합니다.
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.
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. Unified Manager에는 사전 정의된 역할이 포함되어 있습니다.
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. 스토리지의 내장된 SAML 기능은 ID 어설션, 인증 및 권한 부여에 대해 SAML2.0을 준수합니다.
SSO	SSO(Single Sign-On)는 하나의 로그인 자격 증명 세트로 여러 응용 프로그램에 액세스할 수 있는 인증 서비스입니다.

기간	설명
웹 서비스 프록시	표준 HTTPS 메커니즘을 통해 액세스를 제공하는 웹 서비스 프록시를 사용하면 관리자가 스토리지 시스템에 대한 관리 서비스를 구성할 수 있습니다. 프록시는 Windows 또는 Linux 호스트에 설치할 수 있습니다. Unified Manager 인터페이스는 웹 서비스 프록시에서 사용할 수 있습니다.

매핑된 역할에 대한 권한

RBAC(역할 기반 액세스 제어) 기능에는 하나 이상의 역할이 매핑된 사전 정의된 사용자가 포함됩니다. 각 역할에는 Unified Manager의 작업에 액세스할 수 있는 권한이 포함됩니다.

역할은 다음과 같이 작업에 대한 사용자 액세스를 제공합니다.

- * 스토리지 관리자 * — 스토리지의 스토리지 객체에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
- * 보안 관리자 * — 액세스 관리 및 인증서 관리에서 보안 구성에 액세스합니다.
- * 지원 관리자 * — 스토리지 배열, 오류 데이터 및 MEL 이벤트의 모든 하드웨어 리소스에 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 기능에 대한 권한이 없는 경우 해당 기능을 선택할 수 없거나 사용자 인터페이스에 표시되지 않습니다.

로컬 사용자 역할을 사용하여 액세스 관리

관리자는 Unified Manager에서 적용된 RBAC(역할 기반 액세스 제어) 기능을 사용할 수 있습니다. 이러한 기능을 "로컬 사용자 역할"이라고 합니다.

구성 워크플로우

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

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 Unified Manager에 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

관리자는 LDAP(Lightweight Directory Access Protocol) 서버와 Microsoft의 Active Directory와 같은 디렉터리 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 Unified Manager에 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 웹 서비스 프록시가 설치된 호스트 시스템 간의 인증을 위해 CA(인증 기관) 인증서 체인을 업로드합니다.
4. 서버 연결이 설정되면 관리자는 사용자 그룹을 로컬 사용자 역할에 매핑합니다. 이러한 역할은 미리 정의되어 있으며 수정할 수 없습니다.
5. 관리자는 LDAP 서버와 웹 서비스 프록시 간의 연결을 테스트합니다.
6. 사용자는 할당된 LDAP/Directory 서비스 자격 증명을 사용하여 시스템에 로그인합니다.

관리

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

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 Unified 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 시스템과의 통신을 구성하기 위해 관리자는 IDP 시스템에서 IDP 메타데이터 파일을 다운로드한 다음 Unified 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. 관리자는 Unified Manager를 사용하여 컨트롤러의 서비스 공급자 메타데이터 파일을 내보내어 통신을 구성합니다. 그런 다음 관리자는 IDP 시스템에서 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. 이를 위해 관리자는 Unified 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. Unified Manager에서 관리자는 스토리지 어레이에 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 활성화된 경우 사용자는 기존 Storage Manager 인터페이스에서 해당 스토리지에 대한 스토리지를 검색 또는 관리할 수 없습니다.

또한 다음 클라이언트는 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