SAML을 사용합니다

SANtricity 11.7

NetApp
February 12, 2024

목차

SAML을 사용합니다

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.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- 스토리지 어레이에 있는 각 컨트롤러의 IP 주소 또는 도메인 이름을 알아야 합니다.
- 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

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

IDP 연결 정보를 스토리지 어레이에 제공하기 위해 IDP 메타데이터를 System Manager로 가져옵니다. 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. 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 멤버쉽을 스토리지 어레이의 사전 정의된 역할에 매핑해야 합니다.

시작하기 전에

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

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 상세정보

설정	설명
• 매핑 *	사용자 속성
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.	속성 값
매핑할 그룹의 속성 값을 지정합니다. 정규식이 지원됩니다. 이러한 특수 정규식 문자는 백슬래시로 이스케이프해야 합니다 (\ ) 정규식 패턴의 일부가 아닌 경우: \.[]{}() <> * +-=!?^$	
역할	필드를 클릭하고 속성에 매핑할 스토리지 시스템의 역할 중 하나를 선택합니다. 포함할 각 역할을 개별적으로 선택해야 합니다. Monitor 역할은 System Manager에 로그인하기 위한 다른 역할과 함께 필요합니다. 하나 이상의 그룹에 보안 관리자 역할도 필요합니다. 매핑된 역할에는 다음 권한이 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.

   Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에 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 사용자 인증을 위해 SAML 구성을 완료하는 것입니다. 이 프로세스 중에 SSO 로그인을 테스트하라는 메시지가 표시됩니다. SSO 로그인 테스트 프로세스는 이전 단계에서 설명합니다.

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.

- 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.

Confirm Enable SAML(SAML 활성화 확인) 대화 상자가 열립니다.

2. 유형 `enable`를 클릭한 다음 * 사용 * 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 상세정보

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 사용자에 대해서는 System Manager가 올바르게 작동하지 않습니다.

5. 선택적으로 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 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.