SAML 인증 설정 관리

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager-910/config/reference_identity_provider_requirements_um.html on December 18, 2023. Always check docs.netapp.com for the latest.

목차

SAML 인증 설정 관리

원격 인증 설정을 구성한 후에는 SAML(Security Assertion Markup Language) 인증을 설정하여 원격 사용자가 Unified Manager 웹 UI에 액세스하기 전에 IDP(Secure Identity Provider)에 의해 인증되도록 할 수 있습니다.

SAML 인증이 활성화된 후에는 원격 사용자만 Unified Manager 그래픽 사용자 인터페이스에 액세스할 수 있습니다. 로컬 사용자 및 유지 관리 사용자는 UI에 액세스할 수 없습니다. 이 구성은 유지보수 콘솔에 액세스하는 사용자에게 영향을 주지 않습니다.

ID 공급자 요구 사항

ID 공급자(IDP)를 사용하여 모든 원격 사용자에 대해 SAML 인증을 수행하도록 Unified Manager를 구성하는 경우 Unified Manager에 성공적으로 연결되도록 몇 가지 필수 구성 설정을 알고 있어야 합니다.

IDP 서버에 Unified Manager URI 및 메타데이터를 입력해야 합니다. 이 정보는 Unified ManagerSAML 인증 페이지에서 복사할 수 있습니다. Unified Manager는 SAML(Security Assertion Markup Language) 표준의 서비스 공급자(SP)로 간주됩니다.

지원되는 암호화 표준

- AES(고급 암호화 표준): AES-128 및 AES-256
- 보안 해시 알고리즘(SHA): SHA-1 및 SHA-256

검증된 ID 공급자

- 시바볼레스
- ADFS(Active Directory Federation Services)

ADFS 구성 요구 사항

- Unified Manager가 이 기반 당사자 신뢰 항목에 대한 ADFS SAML 응답을 구문 분석하는 데 필요한 세 가지 청구 규칙을 다음 순서로 정의해야 합니다.

청구 규칙	값
SAM-계정-이름	이름 ID입니다
SAM-계정-이름	urn:OID: 0.9.2342.19200300.100.1.1
토큰 그룹 — 비정규화된 이름	urn:OID: 1.3.6.1.4.1.5923.1.5.1.1

- 인증 방법을 ""양식 인증""으로 설정해야 합니다. 그렇지 않을 경우 Unified Manager에서 로그아웃할 때 사용자에게 오류가 발생할 수 있습니다. 다음 단계를 수행하십시오.

a. ADFS 관리 콘솔을 엽니다.

b. 왼쪽 트리 뷰에서 Authentication Policies 폴더를 클릭합니다.

c. 오른쪽의 작업 에서 글로벌 기본 인증 정책 편집 을 클릭합니다.

d. 인트라넷 인증 방법을 기본값인 "Windows 인증" 대신 " 양식 인증"으로 설정합니다.

- 경우에 따라 Unified Manager 보안 인증서가 CA 서명되면 IDP를 통한 로그인이 거부됩니다. 이 문제를 해결하기 위한 두 가지 해결 방법이 있습니다.
  - 링크에 나와 있는 지침에 따라 연결된 CA 인증자에 대한 ADFS 서버의 해지 확인을 비활성화합니다.

    "신뢰할 수 있는 당사자 신뢰에 따라 해지 확인을 비활성화합니다"

  - CA 서버가 ADFS 서버 내에 상주하여 Unified Manager 서버 인증서 요청에 서명하도록 합니다.

기타 구성 요구 사항

- Unified Manager 시간 차이는 5분으로 설정되어 있으므로 IDP 서버와 Unified Manager 서버 간의 시간 차이는 5분 이내이거나 인증이 실패합니다.

SAML 인증을 사용하도록 설정합니다

SAML(Security Assertion Markup Language) 인증을 사용하면 원격 사용자가 Unified Manager 웹 UI에 액세스하기 전에 IDP(Secure Identity Provider)에서 인증을 받을 수 있습니다.

- 필요한 것 *
- 원격 인증을 구성하고 성공적으로 수행되었는지 확인해야 합니다.
- 애플리케이션 관리자 역할을 사용하여 하나 이상의 원격 사용자 또는 원격 그룹을 만들어야 합니다.
- IDP(Identity Provider)는 Unified Manager에서 지원해야 하며 구성해야 합니다.
- IDP URL 및 메타데이터가 있어야 합니다.
- IDP 서버에 대한 액세스 권한이 있어야 합니다.

Unified Manager에서 SAML 인증을 설정한 후에는 IDP가 Unified Manager 서버 호스트 정보로 구성될 때까지 사용자가 그래픽 사용자 인터페이스에 액세스할 수 없습니다. 따라서 구성 프로세스를 시작하기 전에 연결의 두 부분을 모두 완료할 수 있도록 준비해야 합니다. IDP는 Unified Manager를 구성하기 전이나 후에 구성할 수 있습니다.

SAML 인증이 활성화된 후에는 원격 사용자만 Unified Manager 그래픽 사용자 인터페이스에 액세스할 수 있습니다. 로컬 사용자 및 유지 관리 사용자는 UI에 액세스할 수 없습니다. 이 구성은 유지보수 콘솔, Unified Manager 명령 또는 ZAPI에 액세스하는 사용자에게는 영향을 주지 않습니다.

> 이 페이지에서 SAML 구성을 완료하면 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * SAML 인증 * 을 클릭합니다.
2. SAML 인증 활성화 * 확인란을 선택합니다.

IDP 연결을 구성하는 데 필요한 필드가 표시됩니다.

3. Unified Manager 서버를 IDP 서버에 연결하는 데 필요한 IDP URI 및 IDP 메타데이터를 입력합니다.

   IDP 서버에 Unified Manager 서버에서 직접 액세스할 수 있는 경우 IDP URI를 입력한 후 * Fetch IDP Metadata * 버튼을 클릭하여 IDP 메타데이터 필드를 자동으로 채울 수 있습니다.

4. Unified Manager 호스트 메타데이터 URI를 복사하거나 호스트 메타데이터를 XML 텍스트 파일에 저장합니다.

   이 정보를 사용하여 IDP 서버를 구성할 수 있습니다.

5. 저장 * 을 클릭합니다.

   구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

6. 확인 및 로그아웃 * 을 클릭하면 Unified Manager가 다시 시작됩니다.

다음에 권한이 있는 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 Unified Manager 로그인 페이지 대신 IDP 로그인 페이지에 자격 증명을 입력합니다.

아직 완료되지 않은 경우 IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.

> ID 공급자로 ADFS를 사용하는 경우 Unified Manager GUI는 ADFS 시간 제한을 적용하지 않으며 Unified Manager 세션 시간 제한에 도달할 때까지 계속 작동합니다. GUI 세션 시간 초과는 * 일반 * > * 기능 설정 * > * 비활성 시간 초과 * 를 클릭하여 변경할 수 있습니다.

SAML 인증에 사용되는 ID 공급자를 변경합니다

Unified Manager에서 원격 사용자를 인증하는 데 사용하는 IDP(ID 공급자)를 변경할 수 있습니다.

- 필요한 것 *
- IDP URL 및 메타데이터가 있어야 합니다.
- IDP에 대한 액세스 권한이 있어야 합니다.

Unified Manager를 구성하기 전이나 후에 새 IDP를 구성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * SAML 인증 * 을 클릭합니다.
2. Unified Manager 서버를 IDP에 연결하는 데 필요한 새 IDP URI 및 IDP 메타데이터를 입력합니다.

   IDP가 Unified Manager 서버에서 직접 액세스할 수 있는 경우 IDP URL을 입력한 후 * Fetch IDP Metadata * 버튼을 클릭하여 IDP 메타데이터 필드를 자동으로 채울 수 있습니다.

3. Unified Manager 메타데이터 URI를 복사하거나 메타데이터를 XML 텍스트 파일에 저장합니다.
4. 구성 저장 * 을 클릭합니다.

   구성을 변경할 것인지 확인하는 메시지 상자가 표시됩니다.

5. 확인 * 을 클릭합니다.

새 IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.

다음에 권한이 있는 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 이전 IDP 로그인 페이지 대신 새 IDP 로그인 페이지에 자격 증명을 입력합니다.

Unified Manager 보안 인증서 변경 후 **SAML** 인증 설정을 업데이트하는 중입니다

Unified Manager 서버에 설치된 HTTPS 보안 인증서를 변경하려면 SAML 인증 구성 설정을 업데이트해야 합니다. 호스트 시스템의 이름을 바꾸거나 호스트 시스템에 새 IP 주소를 할당하거나 시스템에 대한 보안 인증서를 수동으로 변경하면 인증서가 업데이트됩니다.

보안 인증서가 변경되고 Unified Manager 서버가 다시 시작되면 SAML 인증이 작동하지 않고 사용자가 Unified Manager 그래픽 인터페이스에 액세스할 수 없습니다. 사용자 인터페이스에 대한 액세스를 다시 활성화하려면 IDP 서버 및 Unified Manager 서버 모두에서 SAML 인증 설정을 업데이트해야 합니다.

단계

1. 유지보수 콘솔에 로그인합니다.
2. 주 메뉴 * 에서 * SAML 인증 비활성화 * 옵션에 대한 번호를 입력합니다.

   SAML 인증을 비활성화하고 Unified Manager를 다시 시작할지 확인하는 메시지가 표시됩니다.

3. 업데이트된 FQDN 또는 IP 주소를 사용하여 Unified Manager 사용자 인터페이스를 시작하고, 업데이트된 서버 인증서를 브라우저에 적용하고, 유지 관리 사용자 자격 증명을 사용하여 로그인합니다.
4. 설정/인증 * 페이지에서 * SAML 인증 * 탭을 선택하고 IDP 연결을 구성합니다.
5. Unified Manager 호스트 메타데이터 URI를 복사하거나 호스트 메타데이터를 XML 텍스트 파일에 저장합니다.
6. 저장 * 을 클릭합니다.

   구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

7. 확인 및 로그아웃 * 을 클릭하면 Unified Manager가 다시 시작됩니다.
8. IDP 서버에 액세스한 다음 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.

ID 공급자	구성 단계
고급	a. ADFS 관리 GUI에서 기존 기반 당사자 신뢰 항목을 삭제합니다. b. 업데이트된 Unified Manager 서버의 'saML_sp_metadata.xml'을 사용하여 새로운 신뢰할 수 있는 당사자 항목을 추가합니다. c. Unified Manager가 이 기반 당사자 신뢰 항목에 대한 ADFS SAML 응답을 구문 분석하는 데 필요한 세 가지 클레임 규칙을 정의합니다. d. ADFS Windows 서비스를 다시 시작합니다.
시바볼레스	a. Unified Manager 서버의 새 FQDN을 attribute-filter.xml과 reying-party.xml 파일로 업데이트합니다. b. Apache Tomcat 웹 서버를 다시 시작하고 포트 8005가 온라인 상태가 될 때까지 기다립니다.

9. Unified Manager에 로그인하고 IdP를 통해 SAML 인증이 예상대로 작동하는지 확인합니다.

SAML 인증을 사용하지 않도록 설정합니다

Unified Manager 웹 UI에 로그인하기 전에 IDP(Secure Identity Provider)를 통해 원격 사용자 인증을 중지하려면 SAML 인증을 사용하지 않도록 설정할 수 있습니다. SAML 인증이 비활성화된 경우 Active Directory 또는 LDAP와 같이 구성된 디렉토리 서비스 공급자가 로그온 인증을 수행합니다.

SAML 인증을 비활성화하면 로컬 사용자 및 유지 관리 사용자가 구성된 원격 사용자 외에 그래픽 사용자 인터페이스에 액세스할 수 있습니다.

그래픽 사용자 인터페이스에 액세스할 수 없는 경우 Unified Manager 유지보수 콘솔을 사용하여 SAML 인증을 비활성화할 수도 있습니다.

SAML 인증이 비활성화된 후 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * SAML 인증 * 을 클릭합니다.
2. SAML 인증 활성화 * 확인란의 선택을 취소합니다.
3. 저장 * 을 클릭합니다.

   구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

4. 확인 및 로그아웃 * 을 클릭하면 Unified Manager가 다시 시작됩니다.

다음 번에 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 IDP 로그인 페이지 대신 Unified Manager 로그인 페이지에 자격 증명을 입력합니다.

IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 삭제합니다.

유지 관리 콘솔에서 **SAML** 인증을 사용하지 않도록 설정합니다

Unified Manager GUI에 액세스할 수 없는 경우 유지보수 콘솔에서 SAML 인증을 비활성화해야 할 수 있습니다. 이는 구성이 잘못되거나 IDP에 액세스할 수 없는 경우에 발생할 수 있습니다.

- 필요한 것 *

유지보수 사용자로서 유지보수 콘솔에 액세스할 수 있어야 합니다.

SAML 인증이 비활성화된 경우 Active Directory 또는 LDAP와 같이 구성된 디렉토리 서비스 공급자가 로그온 인증을 수행합니다. 로컬 사용자 및 유지 관리 사용자는 구성된 원격 사용자 외에도 그래픽 사용자 인터페이스에 액세스할 수 있습니다.

UI의 설정/인증 페이지에서 SAML 인증을 비활성화할 수도 있습니다.

> SAML 인증이 비활성화된 후 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 유지보수 콘솔에 로그인합니다.
2. 주 메뉴 * 에서 * SAML 인증 비활성화 * 옵션에 대한 번호를 입력합니다.

   SAML 인증을 비활성화하고 Unified Manager를 다시 시작할지 확인하는 메시지가 표시됩니다.

3. y * 를 입력한 다음 Enter 키를 누르면 Unified Manager가 다시 시작됩니다.

다음 번에 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 IDP 로그인 페이지 대신 Unified Manager 로그인 페이지에 자격 증명을 입력합니다.

필요한 경우 IDP에 액세스하고 Unified Manager 서버 URL 및 메타데이터를 삭제합니다.

SAML 인증 페이지

SAML 인증 페이지를 사용하면 Unified Manager 웹 UI에 로그인하기 전에 IdP(Secure Identity Provider)를 통해 SAML을 사용하여 원격 사용자를 인증하도록 Unified Manager를 구성할 수 있습니다.

- SAML 구성을 생성하거나 수정하려면 애플리케이션 관리자 역할이 있어야 합니다.
- 원격 인증을 구성해야 합니다.
- 하나 이상의 원격 사용자 또는 원격 그룹을 구성해야 합니다.

원격 인증 및 원격 사용자를 구성한 후 SAML 인증 활성화 확인란을 선택하여 보안 ID 공급자를 사용하여 인증을 활성화할 수 있습니다.

- * IDP URI *

  Unified Manager 서버에서 IDP에 액세스하기 위한 URI입니다. URI의 예는 다음과 같습니다.

ADFS 예제 URI:

(https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml`)

Shibboleth 예제 URI:

(https://centos7.ntap2016.local/idp/shibboleth`)

- * IDP 메타데이터 *

  XML 형식의 IDP 메타데이터

  Unified Manager 서버에서 IDP URL에 액세스할 수 있는 경우 * Fetch IDP Metadata * 버튼을 클릭하여 이 필드를 채울 수 있습니다.

- * 호스트 시스템(FQDN) *

  설치 중에 정의된 Unified Manager 호스트 시스템의 FQDN입니다. 필요한 경우 이 값을 변경할 수 있습니다.

- * 호스트 URI *

  IDP에서 Unified Manager 호스트 시스템에 액세스하기 위한 URI입니다.

- * 호스트 메타데이터 *

  XML 형식의 호스트 시스템 메타데이터

저작권 정보

Copyright © 2023 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 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.