



인증 관리

OnCommand Unified Manager 9.5

NetApp

December 20, 2023

목차

인증 관리	1
원격 인증 활성화 중	1
원격 인증에서 중첩 그룹을 해제합니다	2
인증 서비스 설정 중	3
인증 서버 추가	4
인증 서버의 구성을 테스트하는 중입니다	5
인증 서버 편집	6
인증 서버를 삭제하는 중입니다	6
Active Directory 또는 OpenLDAP를 사용한 인증	7
SAML 인증을 사용하도록 설정합니다	7
ID 공급자 요구 사항	9
SAML 인증에 사용되는 ID 공급자를 변경합니다	10
SAML 인증을 사용하지 않도록 설정합니다	11
인증 창 및 대화 상자에 대한 설명입니다	12

인증 관리

Unified Manager 서버에서 LDAP 또는 Active Directory를 사용하여 인증을 설정하고 서버와 함께 작동하도록 구성하여 원격 사용자를 인증할 수 있습니다.

또한 SAML 인증을 설정하면 원격 사용자가 Unified Manager 웹 UI에 로그인하기 전에 IDP(Secure Identity Provider)를 통해 인증되도록 할 수 있습니다.

원격 인증 활성화 중

Unified Manager 서버가 인증 서버와 통신할 수 있도록 원격 인증을 설정할 수 있습니다. 인증 서버 사용자는 Unified Manager 그래픽 인터페이스에 액세스하여 스토리지 객체와 데이터를 관리할 수 있습니다.

시작하기 전에

OnCommand 관리자 역할이 있어야 합니다.



Unified Manager 서버는 인증 서버에 직접 연결되어 있어야 합니다. SSSD(System Security Services Daemon) 또는 NSLCD(Name Service LDAP Caching Daemon)와 같은 로컬 LDAP 클라이언트를 비활성화해야 합니다.

이 작업에 대해


Open LDAP 또는 Active Directory를 사용하여 원격 인증을 설정할 수 있습니다. 원격 인증이 비활성화되어 있으면 원격 사용자가 Unified Manager에 액세스할 수 없습니다.

원격 인증은 LDAP 및 LDAPS(Secure LDAP)를 통해 지원됩니다. Unified Manager에서는 비보안 통신의 기본 포트는 389를 사용하고 보안 통신의 기본 포트는 636을 사용합니다.



사용자를 인증하는 데 사용되는 인증서는 X.509 형식을 따라야 합니다.

단계

1. 도구 모음에서 * 를 클릭합니다  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정/인증 * 페이지에서 * 원격 인증 활성화 * 를 선택합니다.
3. Authentication Service* 필드에서 서비스 유형을 선택하고 인증 서비스를 구성합니다.

인증 유형...	다음 정보를 입력합니다...
Active Directory를 클릭합니다	<ul style="list-style-type: none"> 인증 서버 관리자 이름은 다음 형식 중 하나입니다. <ul style="list-style-type: none"> ◦ domainname**username ◦ username@domainname ◦ Bind Distinguished Name (적절한 LDAP 표기법 사용) 관리자 암호입니다 기본 고유 이름(적절한 LDAP 표기법 사용)
LDAP를 엽니다	<ul style="list-style-type: none"> 적절한 LDAP 표시법으로 고유 이름 바인딩 암호를 바인딩합니다 기본 고유 이름입니다

Active Directory 사용자의 인증에 오랜 시간이 걸리거나 시간이 걸리는 경우 인증 서버가 응답하는 데 시간이 오래 걸릴 수 있습니다. Unified Manager에서 중첩된 그룹에 대한 지원을 사용하지 않도록 설정하면 인증 시간이 줄어들 수 있습니다.

인증 서버에 대해 보안 연결 사용 옵션을 선택하면 Unified Manager는 SSL(Secure Sockets Layer) 프로토콜을 사용하여 인증 서버와 통신합니다.

- 인증 서버를 추가하고 인증을 테스트합니다.
- 저장 후 닫기 * 를 클릭합니다.

원격 인증에서 중첩 그룹을 해제합니다

원격 인증이 활성화된 경우 그룹 구성원이 아닌 개별 사용자만 Unified Manager에 원격으로 인증할 수 있도록 중첩된 그룹 인증을 비활성화할 수 있습니다. Active Directory 인증 응답 시간을 향상시키려면 중첩된 그룹을 사용하지 않도록 설정할 수 있습니다.

시작하기 전에

- OnCommand 관리자 역할이 있어야 합니다.
- 중첩된 그룹을 사용하지 않도록 설정하는 것은 Active Directory를 사용하는 경우에만 적용됩니다.

이 작업에 대해

Unified Manager에서 중첩된 그룹에 대한 지원을 사용하지 않도록 설정하면 인증 시간이 줄어들 수 있습니다. 중첩된 그룹 지원이 비활성화되어 있고 원격 그룹이 Unified Manager에 추가된 경우, 개별 사용자는 Unified Manager에 인증할 원격 그룹의 구성원이어야 합니다.

단계

- 도구 모음에서 * 를 클릭합니다  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.

2. 설정/인증 * 페이지에서 * 중첩 그룹 조회 비활성화 * 상자를 선택합니다.

3. 저장 * 을 클릭합니다.


인증 서비스 설정 중

인증 서비스를 사용하면 Unified Manager에 대한 액세스를 제공하기 전에 인증 서버에서 원격 사용자 또는 원격 그룹을 인증할 수 있습니다. 사전 정의된 인증 서비스(예: Active Directory 또는 OpenLDAP)를 사용하거나 고유한 인증 메커니즘을 구성하여 사용자를 인증할 수 있습니다.

시작하기 전에

- 원격 인증을 활성화해야 합니다.
- OnCommand 관리자 역할이 있어야 합니다.

단계

1. 도구 모음에서 * 를 클릭합니다  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정 * 옵션 페이지에서 * 관리 서버 * > * 인증 * 을 클릭합니다.
3. 다음 인증 서비스 중 하나를 선택합니다.

다음을 선택한 경우...	다음을 수행하십시오.
Active Directory를 클릭합니다	<ol style="list-style-type: none"> a. 관리자 이름과 암호를 입력합니다. b. 인증 서버의 기본 고유 이름을 지정합니다. <p>예를 들어 인증 서버의 도메인 이름이 <code>ou@domain.com</code> 이면 기본 고유 이름은 <code>입니다 cn=ou,dc=domain,dc=com.</code></p>
OpenLDAP를 클릭합니다	<ol style="list-style-type: none"> a. 바인딩 고유 이름 및 바인딩 암호를 입력합니다. b. 인증 서버의 기본 고유 이름을 지정합니다. <p>예를 들어 인증 서버의 도메인 이름이 <code>ou@domain.com</code> 이면 기본 고유 이름은 <code>입니다 cn=ou,dc=domain,dc=com.</code></p>

다음을 선택한 경우...	다음을 수행하십시오.
기타	<p>a. 바인딩 고유 이름 및 바인딩 암호를 입력합니다.</p> <p>b. 인증 서버의 기본 고유 이름을 지정합니다.</p> <p>예를 들어 인증 서버의 도메인 이름이 <code>ou@domain.com</code> 이면 기본 고유 이름은 <code>입니다 cn=ou,dc=domain,dc=com.</code></p> <p>c. 인증 서버에서 지원하는 LDAP 프로토콜 버전을 지정합니다.</p> <p>d. 사용자 이름, 그룹 구성원 자격, 사용자 그룹 및 구성원 특성을 입력합니다.</p>



인증 서비스를 수정하려면 기존 인증 서버를 삭제한 다음 새 인증 서버를 추가해야 합니다.

4. 저장 후 닫기 * 를 클릭합니다.

인증 서버 추가

인증 서버를 추가하고 관리 서버에서 원격 인증을 설정하여 인증 서버 내의 원격 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다.


시작하기 전에


- 다음 정보를 사용할 수 있어야 합니다.
 - 인증 서버의 호스트 이름 또는 IP 주소입니다
 - 인증 서버의 포트 번호입니다
- 관리 서버가 인증 서버의 원격 사용자 또는 그룹을 인증할 수 있도록 원격 인증을 활성화하고 인증 서비스를 구성해야 합니다.
- OnCommand 관리자 역할이 있어야 합니다.

이 작업에 대해

추가하려는 인증 서버가 동일한 데이터베이스를 사용하는 고가용성(HA) 쌍의 일부인 경우 파트너 인증 서버를 추가할 수도 있습니다. 이렇게 하면 인증 서버 중 하나에 연결할 수 없을 때 관리 서버가 파트너와 통신할 수 있습니다.

단계

1. 도구 모음에서 * 를 클릭합니다  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정/인증 * 페이지에서 * 관리 서버 * > * 인증 * 을 클릭합니다.
3. 보안 연결 인증 사용 * 옵션을 활성화 또는 비활성화합니다.

원하는 작업	다음을 수행하십시오.
활성화	<p>a. 원격 인증 활성화 확인란에서 * 보안 연결 사용 * 옵션을 선택합니다.</p> <p>b. Authentication Servers 영역에서 * Add * 를 클릭합니다.</p> <p>c. Add Authentication Server 대화 상자에서 서버의 인증 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.</p> <p>d. 호스트 권한 부여 대화 상자에서 인증서 보기를 클릭합니다.</p> <p>e. 인증서 보기 대화 상자에서 인증서 정보를 확인한 다음 * 닫기 * 를 클릭합니다.</p> <p>f. 호스트 권한 부여 대화 상자에서 * 예 * 를 클릭합니다.</p> <div style="border: 1px solid gray; padding: 10px; margin-top: 20px;">  <p>보안 연결 인증 사용 * 옵션을 활성화하면 Unified Manager가 인증 서버와 통신하고 인증서를 표시합니다. Unified Manager는 보안 통신을 위한 기본 포트로 636을 사용하고 비보안 통신을 위한 포트 번호 389를 사용합니다.</p> </div>
비활성화합니다	<p>a. 원격 인증 활성화 확인란에서 * 보안 연결 사용 * 옵션을 선택 취소합니다.</p> <p>b. Authentication Servers 영역에서 * Add * 를 클릭합니다.</p> <p>c. Add Authentication Server 대화 상자에서 서버의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)와 포트 세부 정보를 지정합니다.</p> <p>d. 추가 * 를 클릭합니다.</p>

추가한 인증 서버가 Servers 영역에 표시됩니다.

4. 테스트 인증을 수행하여 추가한 인증 서버에서 사용자를 인증할 수 있는지 확인합니다.

인증 서버의 구성을 테스트하는 중입니다

관리 서버가 인증 서버와 통신할 수 있는지 확인하기 위해 인증 서버 구성을 검증할 수 있습니다. 인증 서버에서 원격 사용자 또는 원격 그룹을 검색하고 구성된 설정을 사용하여 인증하여 구성을 확인할 수 있습니다.


시작하기 전에

- Unified Manager 서버가 원격 사용자 또는 원격 그룹을 인증할 수 있도록 원격 인증을 설정하고 인증 서비스를 구성해야 합니다.
- 관리 서버가 이러한 서버에서 원격 사용자 또는 원격 그룹을 검색하고 인증할 수 있도록 인증 서버를 추가해야 합니다.
- OnCommand 관리자 역할이 있어야 합니다.

이 작업에 대해

인증 서비스가 Active Directory로 설정되어 있고 인증 서버의 기본 그룹에 속하는 원격 사용자의 인증을 확인하는 경우 기본 그룹에 대한 정보가 인증 결과에 표시되지 않습니다.

단계

1. 도구 모음에서 * 를 클릭합니다  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정/인증 * 페이지에서 * 인증 테스트 * 를 클릭합니다.
3. Test User * (사용자 테스트 *) 대화 상자에서 원격 사용자의 사용자 이름 및 암호 또는 원격 그룹의 사용자 이름을 지정한 다음 * Test * (테스트 *)를 클릭합니다.

원격 그룹을 인증하는 경우 암호를 입력하지 않아야 합니다.


인증 서버 편집

Unified Manager 서버가 인증 서버와 통신하는 데 사용하는 포트를 변경할 수 있습니다.

시작하기 전에

OnCommand 관리자 역할이 있어야 합니다.

단계

1. 도구 모음에서 * 를 클릭합니다  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정/인증 * 페이지에서 * 중첩 그룹 조회 비활성화 * 상자를 선택합니다.
3. Authentication Servers * 영역에서 편집할 인증 서버를 선택한 다음 * Edit * 를 클릭합니다.
4. 인증 서버 편집 * 대화 상자에서 포트 세부 정보를 편집합니다.
5. 저장 * 을 클릭합니다.

인증 서버를 삭제하는 중입니다

Unified Manager 서버가 인증 서버와 통신하지 못하도록 하려면 인증 서버를 삭제할 수 있습니다. 예를 들어 관리 서버가 통신하는 인증 서버를 변경하려는 경우 인증 서버를 삭제하고 새 인증 서버를 추가할 수 있습니다.


시작하기 전에

OnCommand 관리자 역할이 있어야 합니다.

이 작업에 대해

인증 서버를 삭제하면 인증 서버의 원격 사용자 또는 그룹이 Unified Manager에 더 이상 액세스할 수 없습니다.

단계

1. 도구 모음에서 * 를 클릭합니다  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정/인증 * 페이지에서 삭제할 인증 서버를 하나 이상 선택한 다음 * 삭제 * 를 클릭합니다.
3. 예 * 를 클릭하여 삭제 요청을 확인합니다.

보안 연결 사용 * 옵션을 활성화하면 인증 서버와 연관된 인증서가 인증 서버와 함께 삭제됩니다.

Active Directory 또는 OpenLDAP를 사용한 인증

관리 서버에서 원격 인증을 사용하도록 설정하고 인증 서버 내의 사용자가 액세스할 수 있도록 관리 서버가 인증 서버와 통신하도록 구성할 수 있습니다. 관리 서버에서 원격 인증을 사용하도록 설정하고 관리 서버가 인증 서버와 통신하도록 구성할 수 있습니다 인증 서버 내의 사용자가 Unified Manager에 액세스할 수 있습니다.

다음 미리 정의된 인증 서비스 중 하나를 사용하거나 고유한 인증 서비스를 지정할 수 있습니다.

- Microsoft Active Directory를 클릭합니다



Microsoft Lightweight Directory Services는 사용할 수 없습니다.

- OpenLDAP를 클릭합니다

필요한 인증 서비스를 선택하고 적절한 인증 서버를 추가하여 인증 서버의 원격 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다. 원격 사용자 또는 그룹에 대한 자격 증명은 인증 서버에서 관리합니다. 관리 서버는 LDAP(Lightweight Directory Access Protocol)를 사용하여 구성된 인증 서버 내에서 원격 사용자를 인증합니다.

Unified Manager에서 만든 로컬 사용자의 경우 관리 서버에서 사용자 이름과 암호 데이터베이스를 자체적으로 유지 관리합니다. 관리 서버는 인증을 수행하고 Active Directory 또는 OpenLDAP를 인증에 사용하지 않습니다.

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.

시작하기 전에

- 원격 인증을 구성하고 성공적으로 수행되었는지 확인해야 합니다.
- OnCommand 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.

이 작업에 대해


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. 도구 모음에서 * 를 클릭합니다.  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정/인증 * 페이지에서 * SAML 인증 * 탭을 선택합니다.
3. SAML 인증 활성화 * 확인란을 선택합니다.

IDP 연결을 구성하는 데 필요한 필드가 표시됩니다.

4. 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.

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

이 정보를 사용하여 IDP 서버를 구성할 수 있습니다.

6. 저장 * 을 클릭합니다.

구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

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

결과

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

작업을 마친 후

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. Unified Manager가 Windows, Red Hat 또는 CentOS에 배포되면 다음 Unified Manager CLI 명령을 사용하여 GUI 세션 시간 초과를 변경할 수 있습니다. `um option set absolute.session.timeout=00:15:00`이 명령은 Unified Manager GUI 세션 시간 초과를 15분으로 설정합니다.

ID 공급자 요구 사항

ID 공급자(IDP)를 사용하여 모든 원격 사용자에게 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 Manager SAML 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 Internet Explorer를 사용할 때 Unified Manager에서 로그아웃할 때 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.
<http://www.torivar.com/2016/03/22/adfs-3-0-disable-revocation-check-windows-2012-r2/>
 - 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.
- 사용자가 Internet Explorer를 사용하여 Unified Manager에 액세스하려고 하면 다음 메시지가 표시될 수 있습니다.
* 웹 사이트에서 페이지를 표시할 수 없습니다 *. 이 경우, 이러한 사용자는 * 도구 * > * 인터넷 옵션 * > * 고급 * 에서 "HTTP 오류 메시지 표시" 옵션을 선택 해제하십시오.

SAML 인증에 사용되는 ID 공급자를 변경합니다

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


시작하기 전에

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

이 작업에 대해

Unified Manager를 구성하기 전이나 후에 새 IDP를 구성할 수 있습니다.

단계

1. 도구 모음에서 * 를 클릭합니다  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정/인증 * 페이지에서 * SAML 인증 * 탭을 선택합니다.
3. 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.

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

구성을 변경할 것인지 확인하는 메시지 상자가 표시됩니다.

6. 확인 * 을 클릭합니다.

작업을 마친 후

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.

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 로그인 인증을 수행합니다.

이 작업에 대해


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. 도구 모음에서 * 를 클릭합니다.  를 누른 다음 왼쪽 설정 메뉴에서 * 인증 * 을 누릅니다.
2. 설정/인증 * 페이지에서 * SAML 인증 * 탭을 선택합니다.
3. SAML 인증 활성화 * 확인란의 선택을 취소합니다.
4. 저장 * 을 클릭합니다.

구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

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

결과

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

작업을 마친 후

IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 삭제합니다.

인증 창 및 대화 상자에 대한 설명입니다

설정/인증 페이지에서 LDAP 인증을 활성화할 수 있습니다.

설정/인증 페이지

설정/인증 페이지를 사용하여 Unified Manager 웹 UI에 로그인하려는 원격 사용자를 인증하도록 Unified Manager를 구성할 수 있습니다.

원격 인증 페이지를 사용하면 Unified Manager가 인증 서버와 통신하여 원격 사용자를 인증하도록 구성할 수 있습니다.

SAML 인증 페이지를 사용하면 Unified Manager가 IDP(Secure Identity Provider)와 통신하여 원격 사용자를 인증하도록 구성할 수 있습니다.

원격 인증 페이지

원격 인증 페이지를 사용하여 Unified Manager 웹 UI에 로그인하려는 원격 사용자를 인증하도록 Unified Manager를 인증 서버와 통신하도록 구성할 수 있습니다.

OnCommand 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

원격 인증 활성화 확인란을 선택한 후 인증 서버를 사용하여 원격 인증을 활성화할 수 있습니다.

- * 인증 서비스 *

Active Directory, OpenLDAP 등의 디렉터리 서비스 공급자에서 사용자를 인증하도록 관리 서버를 구성하거나 고유한 인증 메커니즘을 지정할 수 있습니다. 원격 인증을 설정한 경우에만 인증 서비스를 지정할 수 있습니다.

- * Active Directory *

- 관리자 이름

인증 서버의 관리자 이름을 지정합니다.

- 암호

인증 서버에 액세스할 암호를 지정합니다.

- 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 [ou@domain.com](#) 이면 기본 고유 이름은 `cn=ou,dc=domain,dc=com`.

- 중첩된 그룹 조회를 비활성화합니다

중첩 그룹 조회 옵션을 사용할지 여부를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩된 그룹에 대한 지원을 비활성화하여 인증 속도를 높일 수 있습니다.

- 보안 연결을 사용합니다

인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.

◦ * OpenLDAP *

▪ 고유 이름 바인딩

인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인딩 고유 이름을 지정합니다.

▪ 바인딩 암호

인증 서버에 액세스할 암호를 지정합니다.

▪ 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 [ou@domain.com](#) 이면 기본 고유 이름은 `입니다 cn=ou, dc=domain, dc=com.`

▪ 보안 연결을 사용합니다

보안 LDAP가 LDAPS 인증 서버와 통신하는 데 사용됨을 지정합니다.

◦ 기타 *

▪ 고유 이름 바인딩

구성한 인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인딩 고유 이름을 지정합니다.

▪ 바인딩 암호

인증 서버에 액세스할 암호를 지정합니다.

▪ 기본 고유 이름

인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 [ou@domain.com](#) 이면 기본 고유 이름은 `입니다 cn=ou, dc=domain, dc=com.`

▪ 프로토콜 버전

인증 서버에서 지원하는 LDAP(Lightweight Directory Access Protocol) 버전을 지정합니다. 프로토콜 버전을 자동으로 감지할지 또는 버전을 2나 3으로 설정할지 지정할 수 있습니다.

▪ 사용자 이름 특성

관리 서버에서 인증할 사용자 로그인 이름이 포함된 인증 서버의 속성 이름을 지정합니다.

▪ 그룹 구성원 자격 특성

사용자의 인증 서버에 지정된 속성 및 값을 기반으로 관리 서버 그룹 구성원 자격을 원격 사용자에게 할당하는 값을 지정합니다.

▪ UGID

원격 사용자가 인증 서버에 `groupOfUniqueNames` 개체의 구성원으로 포함된 경우 이 옵션을 사용하면 해당 `groupOfUniqueNames` 개체의 지정된 속성에 따라 관리 서버 그룹 구성원을 원격 사용자에게 할당할 수 있습니다.

- 중첩된 그룹 조회를 비활성화합니다

중첩 그룹 조회 옵션을 사용할지 여부를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩된 그룹에 대한 지원을 비활성화하여 인증 속도를 높일 수 있습니다.

- 회원

인증 서버가 그룹의 개별 구성원에 대한 정보를 저장하는 데 사용하는 속성 이름을 지정합니다.

- 사용자 객체 클래스

원격 인증 서버에 있는 사용자의 객체 클래스를 지정합니다.

- 그룹 객체 클래스

원격 인증 서버에 있는 모든 그룹의 객체 클래스를 지정합니다.

- 보안 연결을 사용합니다

인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.



인증 서비스를 수정하려면 기존 인증 서버를 삭제하고 새 인증 서버를 추가해야 합니다.

Authentication Servers 영역

인증 서버 영역에는 관리 서버가 원격 사용자를 찾고 인증하기 위해 통신하는 인증 서버가 표시됩니다. 원격 사용자 또는 그룹에 대한 자격 증명은 인증 서버에서 관리합니다.

- * 명령 버튼 *

인증 서버를 추가, 편집 또는 삭제할 수 있습니다.

- 추가

인증 서버를 추가할 수 있습니다.

추가하려는 인증 서버가 같은 데이터베이스를 사용하는 고가용성 쌍의 일부인 경우 파트너 인증 서버를 추가할 수도 있습니다. 이렇게 하면 인증 서버 중 하나에 연결할 수 없을 때 관리 서버가 파트너와 통신할 수 있습니다.

- 편집

선택한 인증 서버에 대한 설정을 편집할 수 있습니다.

- 삭제

선택한 인증 서버를 삭제합니다.

- * 이름 또는 IP 주소 *

관리 서버에서 사용자를 인증하는 데 사용되는 인증 서버의 호스트 이름 또는 IP 주소를 표시합니다.

- * 포트 *

인증 서버의 포트 번호를 표시합니다.

- * 인증 테스트 *

이 단추는 원격 사용자 또는 그룹을 인증하여 인증 서버 구성을 확인합니다.

테스트하는 동안 사용자 이름만 지정하면 관리 서버가 인증 서버에서 원격 사용자를 검색하지만 사용자를 인증하지는 않습니다. 사용자 이름과 암호를 모두 지정하면 관리 서버가 원격 사용자를 검색하고 인증합니다.

원격 인증이 비활성화되어 있으면 인증을 테스트할 수 없습니다.

SAML 인증 페이지

SAML 인증 페이지를 사용하면 Unified Manager 웹 UI에 로그인하기 전에 SAML을 사용하여 원격 사용자를 인증하도록 Unified Manager를 구성할 수 있습니다.

- SAML 구성을 생성하거나 수정하려면 OnCommand 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 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.