보안 및 규정 준수

NetApp Console setup and administration

NetApp
February 11, 2026

목차

보안 및 규정 준수

ID 페더레이션

NetApp Console 사용하여 ID 페더레이션을 사용하여 단일 로그인을 활성화합니다.

Single Sign-On(페더레이션)은 사용자가 회사 자격 증명을 사용하여 NetApp Console 에 로그인할 수 있도록 하여 로그인 프로세스를 간소화하고 보안을 강화합니다. ID 공급자(IdP) 또는 NetApp 지원 사이트를 통해 SSO(단일 로그인)를 활성화할 수 있습니다.

필수 역할

조직 관리자, 연합 관리자, 연합 뷰어."액세스 역할에 대해 자세히 알아보세요."

NetApp Support Site를 통한 Single Sign-On

NetApp 지원 사이트와 페더레이션하면 사용자는 동일한 자격 증명을 사용하여 콘솔, Active IQ Digital Advisor 및 기타 관련 앱에 로그인할 수 있습니다.

NetApp 지원 사이트와 페더레이션하는 경우 기업 ID 관리 공급자와 페더레이션할 수 없습니다. 귀하의 조직에 가장 적합한 것을 선택하세요.

단계

1. 다운로드하고 완료하세요 "NetApp 페더레이션 요청 양식" .
2. 양식에 명시된 이메일 주소로 양식을 제출해 주세요.

   NetApp 지원팀은 귀하의 요청을 검토하고 처리합니다.

ID 공급자를 사용한 Single Sign-On

콘솔에 대한 SSO(Single Sign-On)를 활성화하려면 ID 공급자와 페더레이션 연결을 설정할 수 있습니다. 이 프로세스에는 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성한 다음 콘솔에서 연결을 만드는 작업이 포함됩니다.

이전에 NetApp Cloud Central(콘솔의 외부 애플리케이션)을 사용하여 페더레이션을 구성한 경우, 콘솔 내에서 이를 관리하려면 페더레이션 페이지를 사용하여 페더레이션을 가져와야 합니다."연방을 가져오는 방법을 알아보세요."

지원되는 ID 공급자

NetApp 페더레이션을 위해 다음과 같은 프로토콜과 ID 공급자를 지원합니다.

프로토콜

- SAML(Security Assertion Markup Language) ID 공급자
- Active Directory 페더레이션 서비스(AD FS)

ID 공급자

- 마이크로소프트 엔트라 ID
- 핑페더레이트

NetApp Console 플로우와의 페더레이션

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성해야 합니다. 그런 다음 콘솔에서 ID 공급자의 구성을 사용하는 연결을 만들 수 있습니다.

귀하의 이메일 도메인이나 귀하가 소유한 다른 도메인과 연합할 수 있습니다. 이메일 도메인과 다른 도메인과 페더레이션하려면 먼저 해당 도메인을 소유하고 있는지 확인하세요.


도메인을 확인하세요(이메일 도메인을 사용하지 않는 경우)

이메일 도메인과 다른 도메인과 페더레이션하려면 해당 도메인의 소유자인지 확인하세요. 추가 단계 없이 이메일 도메인을 연합할 수 있습니다.


NetApp 서비스 공급자로 신뢰하도록 **IdP**를 구성하세요**.**

새로운 애플리케이션을 만들고 ACS URL, 엔터티 ID 또는 기타 자격 증명 정보와 같은 세부 정보를 제공하여 NetApp 신뢰하도록 ID 공급자를 구성합니다. 서비스 제공자 정보는 ID 제공자마다 다르므로 자세한 내용은 해당 ID 제공자의 설명서를 참조하세요. 이 단계를 완료하려면 IdP 관리자와 협력해야 합니다.


콘솔에서 페더레이션 연결을 만듭니다**.**

연결을 생성하려면 ID 공급자의 SAML 메타데이터 URL이나 파일을 제공하세요. 이 정보는 콘솔과 ID 공급자 간의 신뢰 관계를 설정하는 데 사용됩니다. 귀하가 제공하는 정보는 귀하가 사용하는 IdP에 따라 달라집니다. 예를 들어 Microsoft Entra ID를 사용하는 경우 클라이언트 ID, 비밀번호, 도메인을 제공해야 합니다.


콘솔에서 페더레이션을 테스트하세요

페더레이션 연결을 활성화하기 전에 테스트하세요. 콘솔의 페더레이션 페이지에서 테스트 옵션을 사용하여 테스트 사용자가 성공적으로 인증할 수 있는지 확인하세요. 테스트가 성공하면 연결을 활성화할 수 있습니다.


콘솔에서 연결을 활성화하세요

연결을 활성화하면 사용자는 회사 자격 증명을 사용하여 콘솔에 로그인할 수 있습니다.

시작하려면 해당 프로토콜이나 IdP에 대한 주제를 검토하세요.

- "AD FS를 사용하여 페더레이션 연결 설정"
- "Microsoft Entra ID를 사용하여 페더레이션 연결 설정"
- "PingFederate를 사용하여 페더레이션 연결 설정"
- "SAML ID 공급자와 페더레이션 연결 설정"

도메인 확인

페더레이션 연결에 대한 이메일 도메인을 확인하세요.

이메일 도메인과 다른 도메인과 페더레이션하려면 먼저 해당 도메인을 소유하고 있는지 확인해야 합니다. 페더레이션에는 검증된 도메인만 사용할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

도메인을 확인하려면 도메인의 DNS 설정에 TXT 레코드를 추가해야 합니다. 이 레코드는 사용자가 도메인을 소유하고 있음을 증명하는 데 사용되며 NetApp Console 페더레이션을 위해 도메인을 신뢰할 수 있도록 합니다. 이 단계를 완료하려면 IT 또는 네트워크 관리자와 협력해야 할 수도 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.
4. *도메인 소유권 확인*을 선택하세요.
5. 검증하려는 도메인을 입력하고 *계속*을 선택하세요.
6. 제공된 TXT 레코드를 복사하세요.
7. 도메인의 DNS 설정으로 이동하여 도메인의 TXT 레코드로 제공된 TXT 값을 구성합니다. 필요한 경우 IT 관리자나 네트워크 관리자와 협력하세요.
8. TXT 레코드를 추가한 후 콘솔로 돌아가서 *확인*을 선택하세요.

페더레이션 구성

NetApp Console Active Directory Federation Services(AD FS)와 페더레이션

NetApp Console NetApp Console 과 Active Directory Federation Services(AD FS)를 페더레이션합니다. 이를 통해 사용자는 회사 자격 증명을 사용하여 콘솔에 로그인할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

> 회사 IdP 또는 NetApp 지원 사이트와 연합할 수 있습니다. NetApp 둘 중 하나만 선택하는 것을 권장하지만, 둘 다 선택하는 것은 권장하지 않습니다.

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저, NetApp Console 서비스 공급자로 신뢰하도록 ID 공급자를 구성합니다. 그런 다음 ID 공급자의 구성을 사용하여 콘솔에서 연결을 만듭니다.

NetApp Console 에 대한 SSO(Single Sign-On)를 활성화하려면 AD FS 서버와 페더레이션을 설정할 수 있습니다. 이 프로세스에는 콘솔을 서비스 공급자로 신뢰하도록 AD FS를 구성한 다음 NetApp Console 에서 연결을 만드는 작업이 포함됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.
4. 도메인 세부 정보를 입력하세요:
   a. 검증된 도메인을 사용할지, 이메일 도메인을 사용할지 선택하세요. 이메일 도메인은 로그인한 계정과 연결된 도메인입니다.
   b. 구성 중인 페더레이션의 이름을 입력하세요.
   c. 검증된 도메인을 선택한 경우 목록에서 도메인을 선택하세요.
5. *다음*을 선택하세요.
6. 연결 방법으로 *프로토콜*을 선택한 다음 *Active Directory Federation Services(AD FS)*를 선택합니다.
7. *다음*을 선택하세요.
8. AD FS 서버에서 신뢰 당사자 트러스트를 만듭니다. PowerShell을 사용하거나 AD FS 서버에서 수동으로 구성할 수 있습니다. 신뢰 당사자 트러스트를 만드는 방법에 대한 자세한 내용은 AD FS 설명서를 참조하세요.
   a. 다음 스크립트를 사용하여 PowerShell을 사용하여 신뢰를 만듭니다.

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. 또는 AD FS 관리 콘솔에서 수동으로 신뢰를 만들 수 있습니다. 신뢰를 생성할 때 다음 NetApp Console 값을 사용하세요.
      - Relying Trust Identifier를 생성할 때 **YOUR_TENANT** 값을 사용하세요. `netapp-cloud-account`
      - *WS-Federation 지원 활성화*를 선택하는 경우 **YOUR_AUTH0_DOMAIN** 값을 사용하세요. `netapp-cloud-account.auth0.com`
   c. 신뢰를 생성한 후 AD FS 서버에서 메타데이터 URL을 복사하거나 페더레이션 메타데이터 파일을 다운로드합니다. 콘솔에서 연결을 완료하려면 이 URL이나 파일이 필요합니다.

   NetApp NetApp Console 최신 AD FS 구성을 자동으로 검색하도록 메타데이터 URL을 사용할 것을 권장합니다. 페더레이션 메타데이터 파일을 다운로드한 경우 AD FS 구성이 변경될 때마다 NetApp Console 에서 수동으로 업데이트해야 합니다.

9. 콘솔로 돌아가서 *다음*을 선택하여 연결을 만듭니다.
10. AD FS로 연결을 만듭니다.
    a. 이전 단계에서 AD FS 서버에서 복사한 *AD FS URL*을 입력하거나 AD FS 서버에서 다운로드한 페더레이션 메타데이터 파일을 업로드합니다.
11. *연결 만들기*를 선택합니다. 연결을 만드는 데 몇 초가 걸릴 수 있습니다.
12. *다음*을 선택하세요.

13. 연결을 테스트하려면 *연결 테스트*를 선택하세요. IdP 서버의 로그인 페이지로 이동됩니다. IdP 자격 증명으로 로그인하세요. 로그인 후 콘솔로 돌아가서 연결을 활성화하세요.

> 제한 모드에서 콘솔을 사용하는 경우, URL을 시크릿 브라우저 창이나 별도의 브라우저에 복사하여 IdP에 로그인하십시오.

14. 콘솔에서 *다음*을 선택하여 요약 페이지를 검토하십시오.
15. 알림을 설정하세요.

    7일 또는 30일 중에서 선택하세요. 이 시스템은 만료 알림을 이메일로 발송하고 콘솔에 표시하며, 해당 알림은 슈퍼 관리자, 조직 관리자, 페더레이션 관리자 및 페더레이션 뷰어 역할을 가진 모든 사용자에게 제공됩니다.

16. 연동 세부 정보를 검토한 다음 *연동 활성화*를 선택하십시오.
17. *마침*을 선택하여 과정을 완료하세요.

페더레이션을 활성화하면 사용자는 회사 자격 증명을 사용하여 NetApp Console 에 로그인합니다.

Microsoft Entra ID를 사용하여 **NetApp Console** 페더레이션

NetApp Console 에 대한 SSO(Single Sign-On)를 활성화하려면 Microsoft Entra ID IdP 공급자와 페더레이션하세요. 이를 통해 사용자는 회사 자격 증명을 사용하여 로그인할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

> 회사 IdP 또는 NetApp 지원 사이트와 연합할 수 있습니다. NetApp 둘 중 하나만 선택하는 것을 권장하지만, 둘 다 선택하는 것은 권장하지 않습니다.

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성해야 합니다. 그런 다음 콘솔에서 ID 공급자의 구성을 사용하는 연결을 만들 수 있습니다.

Microsoft Entra ID를 사용하여 페더레이션 연결을 설정하면 콘솔에 대한 SSO(Single Sign-On)를 사용할 수 있습니다. 이 프로세스에는 콘솔을 서비스 공급자로 신뢰하도록 Microsoft Entra ID를 구성한 다음 콘솔에서 연결을 만드는 작업이 포함됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.

도메인 세부 정보

1. 도메인 세부 정보를 입력하세요:
   a. 검증된 도메인을 사용할지, 이메일 도메인을 사용할지 선택하세요. 이메일 도메인은 로그인한 계정과 연결된 도메인입니다.

b. 구성 중인 페더레이션의 이름을 입력하세요.

c. 검증된 도메인을 선택한 경우 목록에서 도메인을 선택하세요.

2. *다음*을 선택하세요.

연결 방법

1. 연결 방법으로 *공급자*를 선택한 다음 *Microsoft Entra ID*를 선택하세요.
2. *다음*을 선택하세요.

구성 지침

1. NetApp 서비스 공급자로 신뢰하도록 Microsoft Entra ID를 구성하세요. 이 단계는 Microsoft Entra ID 서버에서 수행해야 합니다.

   a. 콘솔을 신뢰하려면 Microsoft Entra ID 앱을 등록할 때 다음 값을 사용하세요.

      - *리디렉션 URL*의 경우 다음을 사용하세요. `https://services.cloud.netapp.com`
      - *답변 URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/login/callback`

   b. Microsoft Entra ID 앱에 대한 클라이언트 비밀번호를 만듭니다. 페더레이션을 완료하려면 클라이언트 ID, 클라이언트 비밀번호, Entra ID 도메인 이름을 제공해야 합니다.

2. 콘솔로 돌아가서 *다음*을 선택하여 연결을 만듭니다.

연결 생성

1. Microsoft Entra ID로 연결 만들기

   a. 이전 단계에서 생성한 클라이언트 ID와 클라이언트 비밀번호를 입력하세요.

   b. Microsoft Entra ID 도메인 이름을 입력하세요.

2. *연결 만들기*를 선택하세요. 시스템은 몇 초 안에 연결을 생성합니다.

연결을 테스트하고 활성화합니다.

1. *다음*을 선택하세요.
2. 연결을 테스트하려면 *연결 테스트*를 선택하세요. IdP 서버의 로그인 페이지로 이동됩니다. IdP 자격 증명으로 로그인하세요. 로그인 후 콘솔로 돌아가서 연결을 활성화하세요.

   제한 모드에서 콘솔을 사용하는 경우, URL을 시크릿 브라우저 창이나 별도의 브라우저에 복사하여 IdP에 로그인하십시오.

3. 콘솔에서 *다음*을 선택하여 요약 페이지를 검토하십시오.
4. 알림을 설정하세요.

   7일 또는 30일 중에서 선택하세요. 이 시스템은 만료 알림을 이메일로 발송하고 콘솔에 표시하며, 해당 알림은 슈퍼 관리자, 조직 관리자, 페더레이션 관리자 및 페더레이션 뷰어 역할을 가진 모든 사용자에게 제공됩니다.

5. 연동 세부 정보를 검토한 다음 *연동 활성화*를 선택하십시오.

6. *마침*을 선택하여 과정을 완료하세요.

페더레이션을 활성화하면 사용자는 회사 자격 증명을 사용하여 NetApp Console 에 로그인합니다.

PingFederate를 사용하여 **NetApp Console** 페더레이션

PingFederate IdP 공급자와 페더레이션하여 NetApp Console 에 대한 SSO(Single Sign-On)를 활성화합니다. 이를 통해 사용자는 회사 자격 증명을 사용하여 로그인할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

회사 IdP 또는 NetApp 지원 사이트와 연합할 수 있습니다. NetApp 둘 중 하나만 선택하는 것을 권장하지만, 둘 다 선택하는 것은 권장하지 않습니다.

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성해야 합니다. 그런 다음 콘솔에서 ID 공급자의 구성을 사용하는 연결을 만들 수 있습니다.

PingFederate를 사용하여 페더레이션 연결을 설정하면 콘솔에 대한 SSO(Single Sign-On)를 활성화할 수 있습니다. 이 프로세스에는 PingFederate 서버가 콘솔을 서비스 공급자로 신뢰하도록 구성한 다음 콘솔에서 연결을 만드는 작업이 포함됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.
4. 도메인 세부 정보를 입력하세요:
   a. 검증된 도메인을 사용할지, 이메일 도메인을 사용할지 선택하세요. 이메일 도메인은 로그인한 계정과 연결된 도메인입니다.
   b. 구성 중인 페더레이션의 이름을 입력하세요.
   c. 검증된 도메인을 선택한 경우 목록에서 도메인을 선택하세요.
5. *다음*을 선택하세요.
6. 연결 방법으로 *공급자*를 선택한 다음 *PingFederate*를 선택하세요.
7. *다음*을 선택하세요.
8. NetApp 서비스 공급자로 신뢰하도록 PingFederate 서버를 구성합니다. 이 단계는 PingFederate 서버에서 수행해야 합니다.
   a. PingFederate가 NetApp Console 신뢰하도록 구성할 때 다음 값을 사용하세요.
      - 답변 **URL** 또는 *Assertion Consumer Service(ACS) URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/login/callback`
      - *로그아웃 URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/logout`
      - *대상/엔터티 ID*의 경우 다음을 사용하세요. `urn:auth0:netapp-cloud-account:<fed-`

`domain-name-saml>` 여기서 <fed-domain-name-pingfederate>는 페더레이션의 도메인 이름입니다. 예를 들어, 귀하의 도메인이 `example.com` , 대상/엔터티 ID는 다음과 같습니다. `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .

b. PingFederate 서버 URL을 복사합니다. 콘솔에서 연결을 생성하려면 이 URL이 필요합니다.

c. PingFederate 서버에서 X.509 인증서를 다운로드합니다. Base64로 인코딩된 PEM 형식(.pem, .crt, .cer)이어야 합니다.

9. 콘솔로 돌아가서 *다음*을 선택하여 연결을 만듭니다.
10. PingFederate로 연결을 만듭니다.
    a. 이전 단계에서 복사한 PingFederate 서버 URL을 입력하세요.
    b. X.509 서명 인증서를 업로드합니다. 인증서는 PEM, CER 또는 CRT 형식이어야 합니다.
11. *연결 만들기*를 선택하세요. 시스템은 몇 초 안에 연결을 생성합니다.
12. *다음*을 선택하세요.
13. 연결을 테스트하려면 *연결 테스트*를 선택하세요. IdP 서버의 로그인 페이지로 이동됩니다. IdP 자격 증명으로 로그인하세요. 로그인 후 콘솔로 돌아가서 연결을 활성화하세요.

    제한 모드에서 콘솔을 사용하는 경우, URL을 시크릿 브라우저 창이나 별도의 브라우저에 복사하여 IdP에 로그인하십시오.

14. 콘솔에서 *다음*을 선택하여 요약 페이지를 검토하십시오.
15. 알림을 설정하세요.

    7일 또는 30일 중에서 선택하세요. 이 시스템은 만료 알림을 이메일로 발송하고 콘솔에 표시하며, 해당 알림은 슈퍼 관리자, 조직 관리자, 페더레이션 관리자 및 페더레이션 뷰어 역할을 가진 모든 사용자에게 제공됩니다.

16. 연동 세부 정보를 검토한 다음 *연동 활성화*를 선택하십시오.
17. *마침*을 선택하여 과정을 완료하세요.

페더레이션을 활성화하면 사용자는 회사 자격 증명을 사용하여 NetApp Console 에 로그인합니다.

SAML ID 공급자와 페더레이션

SAML 2.0 IdP 공급자와 연합하여 NEtApp 콘솔에 대한 SSO(Single Sign-On)를 활성화합니다. 이를 통해 사용자는 회사 자격 증명을 사용하여 로그인할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

회사 IdP 또는 NetApp 지원 사이트와 연합할 수 있습니다. 두 나라 모두와 연합할 수는 없습니다.

NetApp 서비스 공급자가 시작하는(SP 가 시작하는) SSO만 지원합니다. 먼저 NetApp 서비스 공급자로 신뢰하도록 ID 공급자를 구성해야 합니다. 그런 다음 콘솔에서 ID 공급자의 구성을 사용하는 연결을 만들 수 있습니다.

SAML 2.0 공급자와 페더레이션 연결을 설정하면 콘솔에 대한 SSO(Single Sign-On)를 사용할 수 있습니다. 이 프로세스에는 서비스 공급자로서 NetApp 신뢰하도록 공급자를 구성한 다음 콘솔에서 연결을 만드는 작업이

포함됩니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. *새 페더레이션 구성*을 선택합니다.
4. 도메인 세부 정보를 입력하세요:
   a. 검증된 도메인을 사용할지, 이메일 도메인을 사용할지 선택하세요. 이메일 도메인은 로그인한 계정과 연결된 도메인입니다.
   b. 구성 중인 페더레이션의 이름을 입력하세요.
   c. 검증된 도메인을 선택한 경우 목록에서 도메인을 선택하세요.
5. *다음*을 선택하세요.
6. 연결 방법으로 *프로토콜*을 선택한 다음 *SAML ID 공급자*를 선택하세요.
7. *다음*을 선택하세요.
8. NetApp 서비스 공급자로 신뢰하도록 SAML ID 공급자를 구성합니다. 이 단계는 SAML 공급자 서버에서 수행해야 합니다.
   a. IdP에 속성이 있는지 확인하세요. `email` 사용자의 이메일 주소로 설정됩니다. 이는 콘솔이 사용자를 올바르게 식별하는 데 필요합니다.

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. 콘솔에 SAML 애플리케이션을 등록할 때 다음 값을 사용하세요.
   - 답변 **URL** 또는 *Assertion Consumer Service(ACS) URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/login/callback`
   - *로그아웃 URL*의 경우 다음을 사용하세요. `https://netapp-cloud-account.auth0.com/logout`
   - *대상/엔터티 ID*의 경우 다음을 사용하세요. `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` 여기서 <fed-domain-name-saml>은 페더레이션에 사용하려는 도메인 이름입니다. 예를 들어, 귀하의 도메인이 `example.com` , 대상/엔터티 ID는 다음과 같습니다. `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. 신뢰를 생성한 후 SAML 공급자 서버에서 다음 값을 복사합니다.
   - 로그인 URL

◦ 로그아웃 URL(선택 사항)

3. SAML 공급자 서버에서 X.509 인증서를 다운로드합니다. PEM, CER 또는 CRT 형식이어야 합니다.
   a. 콘솔로 돌아가서 *다음*을 선택하여 연결을 만듭니다.
   b. SAML로 연결을 생성합니다.
4. SAML 서버의 *로그인 URL*을 입력하세요.
5. SAML 공급자 서버에서 다운로드한 X.509 인증서를 업로드합니다.
6. 선택적으로 SAML 서버의 *로그아웃 URL*을 입력하세요.
   a. *연결 만들기*를 선택하세요. 시스템은 몇 초 안에 연결을 생성합니다.
   b. *다음*을 선택하세요.
   c. 연결을 테스트하려면 *연결 테스트*를 선택하세요. IdP 서버의 로그인 페이지로 이동됩니다. IdP 자격 증명으로 로그인하세요. 로그인 후 콘솔로 돌아가서 연결을 활성화하세요.

      제한 모드에서 콘솔을 사용하는 경우, URL을 시크릿 브라우저 창이나 별도의 브라우저에 복사하여 IdP에 로그인하십시오.

   d. 콘솔에서 *다음*을 선택하여 요약 페이지를 검토하십시오.
   e. 알림을 설정하세요.

      7일 또는 30일 중에서 선택하세요. 이 시스템은 만료 알림을 이메일로 발송하고 콘솔에 표시하며, 해당 알림은 슈퍼 관리자, 조직 관리자, 페더레이션 관리자 및 페더레이션 뷰어 역할을 가진 모든 사용자에게 제공됩니다.

   f. 연동 세부 정보를 검토한 다음 *연동 활성화*를 선택하십시오.
   g. *마침*을 선택하여 과정을 완료하세요.

페더레이션을 활성화하면 사용자는 회사 자격 증명을 사용하여 NetApp Console 에 로그인합니다.

연합 관리

NetApp Console 에서 페더레이션 관리

NetApp Console 에서 페더레이션을 관리할 수 있습니다. 이 기능을 비활성화하고, 만료된 자격 증명을 업데이트하고, 더 이상 필요하지 않으면 비활성화할 수 있습니다.

필수 역할

연합을 만들고 관리하려면 연합 관리자 역할이 필요합니다. 연방 뷰어는 연방 페이지를 볼 수 있습니다."액세스 역할에 대해 자세히 알아보세요."

기존 페더레이션에 추가적인 인증된 도메인을 추가할 수도 있습니다. 이를 통해 페더레이션 연결에 여러 도메인을 사용할 수 있습니다.

- NetApp Cloud Central을 사용하여 페더레이션을 구성한 경우 페더레이션 페이지를 통해 가져와서 콘솔에서 관리하세요."연방을 가져오는 방법을 알아보세요"
- 감사 페이지에서 페더레이션 활성화, 비활성화 및 업데이트와 같은 페더레이션 관리 이벤트를 확인할 수 있습니다. "NetApp Console 에서 작업 모니터링에 대해 자세히 알아보세요."

연합 활성화

연합을 생성했지만 활성화되지 않은 경우, 연합 페이지를 통해 활성화할 수 있습니다. 페더레이션을 활성화하면 페더레이션에 연결된 사용자가 회사 자격 증명을 사용하여 콘솔에 로그인할 수 있습니다. 연합을 활성화하기 전에 연합을 성공적으로 생성하고 테스트하세요.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 작업 메뉴를 선택하세요 ••• 활성화하려는 페더레이션 옆에 있는 *활성화*를 선택합니다.

기존 페더레이션에 검증된 도메인 추가

콘솔에서 기존 페더레이션에 검증된 도메인을 추가하여 동일한 ID 공급자(IdP)를 사용하는 여러 도메인을 사용할 수 있습니다.

페더레이션에 도메인을 추가하려면 먼저 콘솔에서 도메인을 확인해야 합니다. 아직 도메인을 확인하지 않은 경우 다음 단계에 따라 확인할 수 있습니다."콘솔에서 도메인을 확인하세요" .

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 작업 메뉴를 선택하세요⋮ 검증된 도메인을 추가하려는 페더레이션 옆에 있는 도메인 업데이트*를 선택합니다. *도메인 업데이트 대화 상자에는 이 페더레이션에 이미 연결된 도메인이 표시됩니다.
4. 사용 가능한 도메인 목록에서 확인된 도메인을 선택하세요.
5. *업데이트*를 선택하세요. 새로운 도메인 사용자는 30초 이내에 페더레이션 콘솔 액세스 권한을 얻을 수 있습니다.

만료되는 페더레이션 연결 업데이트

콘솔에서 페더레이션의 세부 정보를 업데이트할 수 있습니다. 예를 들어, 인증서나 클라이언트 비밀번호와 같은 자격 증명이 만료되면 페더레이션을 업데이트해야 합니다. 필요한 경우 알림 날짜를 업데이트하여 만료되기 전에 연결을 업데이트하도록 상기시켜줍니다.

로그인 문제를 방지하려면 IdP를 업데이트하기 전에 먼저 콘솔을 업데이트하세요. 프로세스 중에는 콘솔에 로그인 상태를 유지하세요.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 업데이트하려는 페더레이션 옆에 있는 작업 메뉴(세 개의 세로 점)를 선택하고 *페더레이션 업데이트*를 선택합니다.
4. 필요에 따라 연방의 세부 정보를 업데이트하세요.
5. *업데이트*를 선택하세요.

기존 연합 테스트

기존 연합의 연결을 테스트하여 제대로 작동하는지 확인합니다. 이를 통해 연합의 문제를 파악하고 해결하는 데 도움이

될 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 작업 메뉴를 선택하세요: 검증된 도메인을 추가하려는 페더레이션 옆에 있는 *연결 테스트*를 선택합니다.
4. *테스트*를 선택하세요. 시스템에서 회사 자격 증명을 사용하여 로그인하라는 메시지가 표시됩니다. 연결에 성공하면 NetApp Console 로 리디렉션됩니다. 연결에 실패하면 페더레이션에 문제가 있음을 나타내는 오류 메시지가 표시됩니다.
5. 완료*를 선택하면 *연방 탭으로 돌아갑니다.

페더레이션 비활성화

더 이상 연방이 필요하지 않으면 연방을 비활성화할 수 있습니다. 이렇게 하면 연합에 연결된 사용자가 회사 자격 증명을 사용하여 콘솔에 로그인하는 것을 방지할 수 있습니다. 필요한 경우 나중에 페더레이션을 다시 활성화할 수 있습니다.

IdP를 해제하거나 페더레이션을 중단하는 경우와 같이 페더레이션을 삭제하기 전에 페더레이션을 비활성화합니다. 나중에 필요할 경우 다시 활성화할 수 있습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. 작업 메뉴를 선택하세요: 검증된 도메인을 추가하려는 페더레이션 옆에 있는 *비활성화*를 선택합니다.

연합 삭제

더 이상 연합이 필요하지 않으면 삭제할 수 있습니다. 이렇게 하면 페더레이션이 제거되고 페더레이션에 연결된 사용자가 회사 자격 증명을 사용하여 콘솔에 로그인하는 것이 방지됩니다. 예를 들어, IdP가 폐기되거나 연합이 더 이상 필요하지 않은 경우입니다.

연합을 삭제한 후에는 복구할 수 없습니다. 새로운 연방을 만들어야 합니다.

삭제하려면 먼저 페더레이션을 비활성화해야 합니다. 연합을 삭제한 후에는 삭제를 취소할 수 없습니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연합*을 선택하면 *연합 페이지를 볼 수 있습니다.
3. 작업 메뉴를 선택하세요: 검증된 도메인을 추가하려는 페더레이션 옆에 있는 *삭제*를 선택합니다.

NetApp Console 로 페더레이션 가져오기

이전에 NetApp Cloud Central(NetApp Console 의 외부 애플리케이션)을 통해 페더레이션을 설정한 경우 페더레이션 페이지에서 기존 페더레이션 연결을 콘솔로 가져와서 새 인터페이스에서 관리할 수 있도록 하라는 메시지가 표시됩니다. 그러면 페더레이션 연결을 다시 만들지 않고도 최신 개선 사항을 활용할 수 있습니다.

기존 페더레이션을 가져온 후에는 페더레이션 페이지에서 페더레이션을 관리할 수 있습니다."연합 관리에 대해 자세히 알아보세요."

필수 역할

조직 관리자 또는 연방 관리자."액세스 역할에 대해 자세히 알아보세요."

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 연방 탭을 선택하세요.
3. *연합 가져오기*를 선택하세요.

ONTAP Advanced View(ONTAP System Manager)에 대한 ONTAP 권한 적용

기본적으로 콘솔 에이전트 자격 증명을 통해 사용자는 고급 보기(ONTAP 시스템 관리자)에 액세스할 수 있습니다. 대신 사용자에게 ONTAP 자격 증명을 입력하라는 메시지를 표시할 수 있습니다. 이를 통해 사용자 Cloud Volumes ONTAP 과 온프레미스 ONTAP 클러스터 모두에서 ONTAP 클러스터를 사용할 때 사용자의 ONTAP 권한이 적용됩니다.

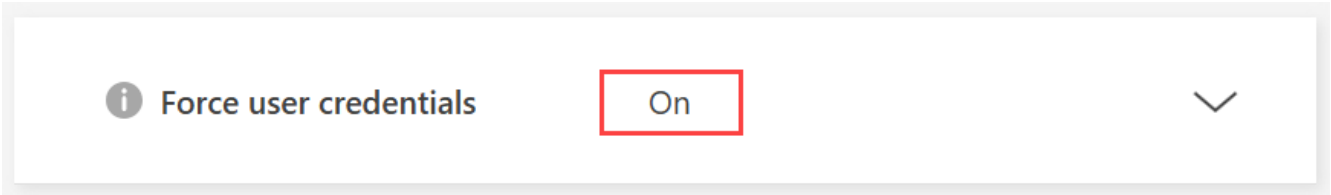
콘솔 에이전트 설정을 편집하려면 조직 관리자 역할이 있어야 합니다.

단계

1. *관리 > 에이전트*를 선택하세요.
2. 개요 페이지에서 콘솔 에이전트의 작업 메뉴를 선택하고 *에이전트 편집*을 선택합니다.

   편집하려면 콘솔 에이전트가 활성화되어 있어야 합니다.

3. 자격 증명 강제 적용 옵션을 확장합니다.
4. 자격 증명 강제 옵션을 활성화하려면 확인란을 선택한 다음 *저장*을 선택합니다.
5. 자격 증명 강제 옵션이 활성화되어 있는지 확인하세요.



NetApp Console 조직에 대해 읽기 전용 모드를 활성화합니다.

보안상의 예방 조치로 NetApp Console 조직에 대해 읽기 전용 모드를 활성화할 수 있습니다. 읽기 전용 모드에서는 사용자가 리소스와 설정을 볼 수는 있지만 변경할 수는 없습니다.

읽기 전용 모드에서는 관리자 권한을 가진 사용자가 변경을 하려면 수동으로 권한을 높여야 하므로 변경 사항이

의도적인 것임을 보장합니다.

필수 접근 권한 역할

최고 관리자 또는 조직 관리자.

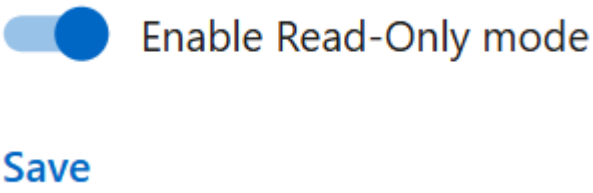
콘솔 조직에 대해 읽기 전용 모드를 활성화합니다.

콘솔 조직에 대한 변경을 제한하려면 읽기 전용 모드를 활성화하세요. 모든 사용자는 여전히 리소스를 볼 수 있습니다. 관리자 권한을 가진 사용자는 수동으로 권한을 높이지 않으면 콘솔에서 어떤 작업도 수행할 수 없습니다.

읽기 전용 모드가 활성화되면 사용자는 조직이 읽기 전용 모드임을 알리는 배너를 보게 됩니다. 사용자는 자신의 역할을 높이기 위해 사용자 설정으로 이동해야 합니다.

단계

1. *관리 > ID 및 액세스*를 선택합니다.
2. 조직 탭에서 읽기 전용 모드로 설정하려는 조직의 *조직 설정 편집*을 선택합니다.
3. 읽기 전용 모드 섹션에서 토글 스위치를 켜짐 위치로 이동하여 읽기 전용 모드를 활성화한 다음 *저장*을 선택합니다.



NetApp Console 에 최초 조직 관리자로 등록하세요.

회사에 NetApp Console 조직이 없는 경우 가입하여 조직을 생성하세요. 첫 번째 사용자는 관리자이며 계정과 권한을 관리합니다. 역할은 나중에 업데이트하고 관리자를 추가할 수 있습니다.

단계

1. 웹 브라우저를 열고 이동하세요 "NetApp Console"
2. NetApp 지원 사이트 계정이 있는 경우, 로그인 페이지에서 계정과 연결된 이메일 주소를 직접 입력하십시오.

   콘솔은 초기 로그인 과정에서 NetApp 지원 사이트 자격 증명을 사용하여 사용자를 등록합니다.

3. 콘솔 로그인을 만들어 가입하려면 *가입*을 선택하세요.
   a. 가입 페이지에서 필요한 정보를 입력하고 *다음*을 선택하세요.

      회원가입 양식에는 영문자만 입력할 수 있습니다.

   b. NetApp 에서 보낸 이메일이 받은 편지함에서 확인되었는지 확인하세요. 이메일 주소 확인 지침이 포함되어 있습니다.

      가입을 완료하려면 이메일 주소를 인증하세요.

4. 로그인 후 최종 사용자 라이선스 계약을 검토하고 동의하십시오.
5. 환영 페이지에서 조직을 생성하세요.
6. *시작하기*를 선택하세요.

+ 처음 관리자 권한을 획득한 경우, 안내에 따라 스토리지를 추가하고 콘솔 에이전트를 생성하는 등의 작업을 진행하세요. "콘솔 지원 사용법에 대해 알아보세요."

다음 단계

관리자로서 콘솔 지원 도구에 포함된 단계를 완료한 후에는 ID 및 액세스 전략을 계획하고, 조직에 사용자를 추가하고, 역할을 할당해야 합니다. "NetApp Console 의 ID 및 액세스 관리에 대해 알아보세요."

이미 조직이 있는 경우 **NetApp Console** 에 가입하거나 로그인하세요.

귀사에 이미 NetApp Console 조직이 있는 경우, 가입하거나 로그인하여 액세스하십시오. 가입 또는 로그인 방법은 회사에서 ID 페더레이션을 사용하는지 또는 NetApp 지원 사이트 자격 증명을 보유하고 있는지에 따라 다릅니다. 그렇지 않다면 NetApp Console 로그인 계정을 생성하십시오.

단계

1. 웹 브라우저를 열고 이동하세요 "NetApp Console"
2. NetApp 지원 사이트 계정이 있거나 회사에서 단일 로그인(SSO)을 설정한 경우 로그인 페이지에서 연결된 이메일 주소 또는 SSO 자격 증명을 입력하십시오. 안내에 따라 로그인을 완료하세요.

   두 경우 모두, 초기 로그인의 일부로 콘솔에 가입하게 됩니다.

3. 콘솔 로그인을 만들어 가입하려면 *가입*을 선택하세요.
   a. 가입 페이지에서 필요한 정보를 입력하고 *다음*을 선택하세요.

      회원가입 양식에는 영문자만 입력할 수 있습니다.

   b. NetApp 에서 보낸 이메일이 받은 편지함에서 확인되었는지 확인하세요. 이메일 주소 확인 지침이 포함되어 있습니다.

      가입을 완료하려면 이메일 주소를 인증하세요.

4. 로그인 후 최종 사용자 라이선스 계약을 검토하고 동의하십시오.
5. 시스템에서 조직을 생성하라는 메시지가 표시되면 대화 상자를 닫고 콘솔 관리자에게 알려 콘솔 조직에 추가하고 액세스 권한을 부여받으십시오. "조직 관리자에게 연락하는 방법을 알아보세요."

다음 단계

조직에 대한 액세스 권한이 부여되면 스토리지를 관리하고 할당된 데이터 서비스를 사용할 수 있습니다.