



SnapCenter 서버 설치를 준비하세요

SnapCenter software

NetApp
November 06, 2025

목차

SnapCenter 서버 설치를 준비하세요	1
SnapCenter 서버 설치 요구 사항	1
Windows 호스트에 대한 도메인 및 작업 그룹 요구 사항	1
공간 및 크기 요구 사항	1
SAN 호스트 요구 사항	2
브라우저 요구 사항	3
포트 요구 사항	3
SnapCenter software 액세스하려면 등록하세요	7
다중 요소 인증(MFA)	7
다중 인증 요소(MFA) 관리	8
Rest API, PowerShell 및 SCCLI를 사용하여 다중 인증 요소(MFA) 관리	11
PowerShell, SCCLI 및 REST API를 사용하여 SnapCenter 서버에서 MFA 구성	15

SnapCenter 서버 설치를 준비하세요

SnapCenter 서버 설치 요구 사항

Windows나 Linux 호스트에 SnapCenter Server를 설치하기 전에 환경에 대한 모든 요구 사항이 충족되는지 검토하고 확인해야 합니다.

Windows 호스트에 대한 도메인 및 작업 그룹 요구 사항

SnapCenter 서버는 도메인이나 작업 그룹에 있는 Windows 호스트에 설치할 수 있습니다.

관리자 권한이 있는 사용자는 SnapCenter 서버를 설치할 수 있습니다.

- Active Directory 도메인: 로컬 관리자 권한이 있는 도메인 사용자를 사용해야 합니다. 도메인 사용자는 Windows 호스트의 로컬 관리자 그룹의 구성원이어야 합니다.
- 작업 그룹: 로컬 관리자 권한이 있는 로컬 계정을 사용해야 합니다.

도메인 트러스트, 다중 도메인 포리스트 및 크로스 도메인 트러스트는 지원되지만 크로스 포리스트 도메인은 지원되지 않습니다. Active Directory 도메인 및 트러스트에 대한 Microsoft 설명서에 자세한 내용이 포함되어 있습니다.



SnapCenter 서버를 설치한 후에는 SnapCenter 호스트가 있는 도메인을 변경해서는 안 됩니다. SnapCenter Server가 설치될 당시에 있던 도메인에서 SnapCenter Server 호스트를 제거한 다음 SnapCenter Server를 제거하려고 하면 제거 작업이 실패합니다.

공간 및 크기 요구 사항

공간과 크기 요구 사항을 잘 알고 있어야 합니다.

목	Windows 호스트 요구 사항	Linux 호스트 요구 사항
운영 체제	마이크로소프트 윈도우 운영 체제는 영어, 독일어, 일본어, 간체 중국어 버전만 지원됩니다. 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT ["NetApp 상호 운용성 매트릭스 도구"].	<ul style="list-style-type: none">• Red Hat Enterprise Linux(RHEL) 8 및 9• SUSE Linux Enterprise Server(SLES) 15 지원되는 버전에 대한 최신 정보는 다음을 참조하세요. https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT ["NetApp 상호 운용성 매트릭스 도구"].
최소 CPU 수	4개의 코어	4개의 코어

목	Windows 호스트 요구 사항	Linux 호스트 요구 사항
최소 RAM	8GB  MySQL 서버 버퍼 풀은 전체 RAM의 20%를 사용합니다.	8GB
SnapCenter 서버 소프트웨어 및 로그에 대한 최소 하드 드라이브 공간	7GB  SnapCenter 서버가 설치된 드라이브에 SnapCenter 저장소가 있는 경우 15GB를 권장합니다.	15GB
SnapCenter 저장소의 최소 하드 드라이브 공간	8GB  참고: SnapCenter 저장소가 설치된 드라이브에 SnapCenter 서버가 있는 경우 15GB를 권장합니다.	해당 없음
필수 소프트웨어 패키지	<ul style="list-style-type: none"> • ASP.NET Core Runtime 8.0.12(및 이후 모든 8.0.x 패치) 호스팅 번들 • PowerShell 7.4.2 이상 	<ul style="list-style-type: none"> • .NET Framework 8.0.12(및 이후의 모든 8.0.x 패치) • PowerShell 7.4.2 이상 • Nginx는 역방향 프록시로 사용할 수 있는 웹 서버입니다. • 팜-데벨 <p>PAM(Pluggable Authentication Modules)은 시스템 관리자가 인증을 수행하는 프로그램을 다시 컴파일하지 않고도 인증 정책을 설정할 수 있도록 해주는 시스템 보안 도구입니다.</p>



ASP.NET 코어는 Windows의 SnapCenter Server에 있는 임시 파일 시스템에 액세스하기 위해 IIS_IUSRS가 필요합니다.

SAN 호스트 요구 사항

SnapCenter에는 호스트 유틸리티나 DSM이 포함되어 있지 않습니다. SnapCenter 호스트가 SAN(FC/iSCSI) 환경의 일부인 경우 SnapCenter 서버 호스트에 추가 소프트웨어를 설치하고 구성해야 할 수도 있습니다.

- 호스트 유틸리티: 호스트 유틸리티는 FC와 iSCSI를 지원하며 Windows 서버에서 MPIO를 사용할 수 있게 해줍니다. "[자세히 알아보기](#)".
- Windows MPIO용 Microsoft DSM: 이 소프트웨어는 Windows MPIO 드라이버와 함께 작동하여 NetApp 과 Windows 호스트 컴퓨터 간의 여러 경로를 관리합니다. 고가용성 구성에는 DSM이 필요합니다.



ONTAP DSM을 사용하고 있다면 Microsoft DSM으로 마이그레이션해야 합니다. 자세한 내용은 다음을 참조하세요. "[ONTAP DSM에서 Microsoft DSM으로 마이그레이션하는 방법](#)".

브라우저 요구 사항

SnapCenter software Chrome 125 이상 및 Microsoft Edge 110.0.1587.17 이상을 지원합니다.

포트 요구 사항

SnapCenter software 다양한 구성 요소 간 통신을 위해 서로 다른 포트가 필요합니다.

- 애플리케이션은 포트를 공유할 수 없습니다.
- 사용자 정의 가능한 포트의 경우, 기본 포트를 사용하지 않으려면 설치 중에 사용자 정의 포트를 선택할 수 있습니다.
- 고정 포트의 경우 기본 포트 번호를 사용해야 합니다.
- 방화벽
 - 방화벽, 프록시 또는 기타 네트워크 장치는 연결을 방해해서는 안 됩니다.
 - SnapCenter 설치할 때 사용자 지정 포트를 지정하는 경우 SnapCenter 플러그인 로더의 해당 포트에 대한 방화벽 규칙을 Loader 호스트에 추가해야 합니다.

다음 표에는 다양한 포트와 기본값이 나열되어 있습니다.

포트 이름	포트 번호	규약	방향	설명
SnapCenter 웹 포트	8146	HTTPS	양방향	이 포트는 SnapCenter 클라이언트(SnapCenter 사용자)와 SnapCenter 서버 간 통신에 사용되며 플러그인 호스트에서 SnapCenter 서버로의 통신에도 사용됩니다. 포트 번호를 사용자 정의할 수 있습니다.

포트 이름	포트 번호	규약	방향	설명
SnapCenter SMCore 통신 포트	8145	HTTPS	양방향	이 포트는 SnapCenter 서버와 SnapCenter 플러그인이 설치된 호스트 간의 통신에 사용됩니다. 포트 번호를 사용자 정의할 수 있습니다.
스케줄러 서비스 포트	8154	HTTPS		이 포트는 SnapCenter 서버 호스트 내의 모든 관리 플러그인에 대한 SnapCenter 스케줄러 워크플로를 중앙 집중식으로 조율하는 데 사용됩니다. 포트 번호를 사용자 정의할 수 있습니다.
RabbitMQ 포트	5672	TCP		이는 RabbitMQ가 수신하는 기본 포트이며 Scheduler 서비스와 SnapCenter 간의 게시자-구독자 모델 통신에 사용됩니다.
MySQL 포트	3306	HTTPS		이 포트는 SnapCenter 저장소 데이터베이스와 통신하는 데 사용됩니다. SnapCenter 서버에서 MySQL 서버로 보안 연결을 생성할 수 있습니다. "자세히 알아보기"

포트 이름	포트 번호	규약	방향	설명
Windows 플러그인 호스트	135, 445	TCP		이 포트는 SnapCenter 서버와 플러그인이 설치되는 호스트 간의 통신에 사용됩니다. Microsoft에서 지정한 추가적인 동적 포트 범위도 열려 있어야 합니다.
Linux 또는 AIX 플러그인 호스트	22	SSH	단방향	이 포트는 SnapCenter 서버와 호스트 간의 통신에 사용되며, 서버에서 클라이언트 호스트로 시작됩니다.
Windows, Linux 또는 AIX용 SnapCenter 플러그인 패키지	8145	HTTPS	양방향	이 포트는 SMCORE와 플러그인 패키지가 설치된 호스트 간의 통신에 사용됩니다. 사용자 정의 가능. 포트 번호를 사용자 정의할 수 있습니다.
Oracle 데이터베이스용 SnapCenter 플러그인	27216			기본 JDBC 포트는 Oracle 플러그인이 Oracle 데이터베이스에 연결하는 데 사용됩니다.
Exchange 데이터베이스용 SnapCenter 플러그인	909			기본 NET.TCP 포트는 Windows 플러그인에서 Exchange VSS 콜백에 연결하는 데 사용됩니다.

포트 이름	포트 번호	규약	방향	설명
NetApp SnapCenter 위한 플러그인을 지원합니다.	9090	HTTPS		<p>이는 플러그인 호스트에서만 사용되는 내부 포트입니다. 방화벽 예외는 필요하지 않습니다.</p> <p>SnapCenter 서버와 플러그인 간의 통신은 포트 8145를 통해 라우팅됩니다.</p>
ONTAP 클러스터 또는 SVM 통신 포트	<ul style="list-style-type: none"> • 443(HTTPS) • 80(HTTP) 	<ul style="list-style-type: none"> • HTTPS • HTTP 	양방향	<p>이 포트는 SnapCenter Server를 실행하는 호스트와 SVM 간의 통신을 위해 SAL(Storage Abstraction Layer)에서 사용됩니다. 이 포트는 현재 SnapCenter for Windows 플러그인 호스트의 SAL에서도 사용되어 SnapCenter 플러그인 호스트와 SVM 간 통신에 사용됩니다.</p>
SAP HANA 데이터베이스용 SnapCenter 플러그인	<ul style="list-style-type: none"> • 3instance_number13 • 3instance_number15 	<ul style="list-style-type: none"> • HTTPS • HTTP 	양방향	<p>다중 테넌트 데이터베이스 컨테이너(MDC) 단일 테넌트의 경우 포트 번호는 13으로 끝납니다. MDC가 아닌 경우 포트 번호는 15로 끝납니다.</p> <p>포트 번호를 사용자 정의할 수 있습니다.</p>

포트 이름	포트 번호	규약	방향	설명
PostgreSQL용 SnapCenter 플러그인	5432			이 포트는 PostgreSQL 플러그인이 PostgreSQL 클러스터와 통신하는데 사용하는 기본 PostgreSQL 포트입니다. 포트 번호를 사용자 정의할 수 있습니다.

SnapCenter software 액세스하려면 등록하세요

Amazon FSx for NetApp ONTAP 또는 Azure NetApp Files 처음 사용하고 기존 NetApp 계정이 없는 경우 SnapCenter software 에 액세스하려면 등록해야 합니다.

시작하기 전에

- 회사 이메일 ID에 액세스할 수 있어야 합니다.
- Azure NetApp Files 사용하는 경우 Azure 구독 ID가 있어야 합니다.
- Amazon FSx for NetApp ONTAP 사용하는 경우 FSx for ONTAP 파일 시스템의 파일 시스템 ID가 있어야 합니다.

이 작업에 관하여

귀하의 등록은 정보 검증을 거쳐야 하며, 새로운 NetApp 지원 사이트(NSS) 계정을 게스트 액세스에서 전체 액세스로 확인 및 업그레이드하는 데 최대 하루가 걸릴 수 있습니다.

단계

1. 딸깍 하는 소리 <https://mysupport.netapp.com/site/user/registration> 등록을 위해.
2. 회사 이메일 ID를 입력하고, 캡차를 완료하고, NetApp의 개인정보 보호정책에 동의한 후 *제출*을 클릭하세요.
3. 이메일 ID로 전송된 OTP를 입력하여 등록을 인증하고 *계속*을 클릭하세요.
4. 등록 완료 페이지에서 다음 세부 정보를 입력하여 등록을 완료하세요.
 - a. * NetApp 고객/최종 사용자*를 선택하세요.
 - b. Azure NetApp Files 사용하는 경우 SERIAL NUMBER 필드에 Azure 구독 ID를 입력하고, Amazon FSx for NetApp ONTAP 사용하는 경우 파일 시스템 ID를 입력합니다.



티켓을 제출할 수 있습니다 <https://mysupport.netapp.com/site/help> 등록 중에 문제가 발생하거나 상태를 알고 싶은 경우.

다중 요소 인증(MFA)

다중 인증 요소(MFA) 관리

Active Directory Federation Service(AD FS) 서버와 SnapCenter 서버에서 다중 인증(MFA) 기능을 관리할 수 있습니다.

다중 요소 인증(MFA) 활성화

PowerShell 명령을 사용하여 SnapCenter Server에 대한 MFA 기능을 활성화할 수 있습니다.

이 작업에 관하여

- 다른 애플리케이션이 동일한 AD FS에 구성된 경우 SnapCenter SSO 기반 로그인을 지원합니다. 특정 AD FS 구성에서 SnapCenter AD FS 세션 지속성에 따라 보안상의 이유로 사용자 인증을 요구할 수 있습니다.
- cmdlet과 함께 사용할 수 있는 매개변수 및 해당 설명에 대한 정보는 다음을 실행하여 얻을 수 있습니다. `Get-Help command_name`. 또는 다음을 볼 수도 있습니다. "[SnapCenter 소프트웨어 Cmdlet 참조 가이드](#)".

시작하기 전에

- Windows Active Directory Federation Service(AD FS)가 해당 도메인에서 실행 중이어야 합니다.
- Azure MFA, Cisco Duo 등과 같이 AD FS에서 지원하는 다중 인증 서비스가 있어야 합니다.
- SnapCenter 와 AD FS 서버 타임스탬프는 시간대에 관계없이 동일해야 합니다.
- SnapCenter Server에 대한 공인 CA 인증서를 조달하고 구성합니다.

CA 인증서는 다음과 같은 이유로 필수입니다.

- 자체 서명된 인증서가 노드 수준에서 고유하기 때문에 ADFS-F5 통신이 중단되지 않도록 보장합니다.
- 독립 실행형 또는 고가용성 구성에서 업그레이드, 복구 또는 재해 복구(DR) 중에 자체 서명된 인증서가 다시 생성되지 않도록 하여 MFA 재구성을 방지합니다.
- IP-FQDN 확인을 보장합니다.

CA 인증서에 대한 정보는 다음을 참조하세요. "[CA 인증서 CSR 파일 생성](#)".

단계

1. Active Directory Federation Services(AD FS) 호스트에 연결합니다.
2. AD FS 페더레이션 메타데이터 파일을 다운로드합니다. "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>".
3. 다운로드한 파일을 SnapCenter 서버에 복사하여 MFA 기능을 활성화합니다.
4. PowerShell을 통해 SnapCenter 관리자 사용자로 SnapCenter 서버에 로그인합니다.
5. PowerShell 세션을 사용하여 `New-SmMultifactorAuthenticationMetadata -path cmdlet`을 사용하여 SnapCenter MFA 메타데이터 파일을 생성합니다.

경로 매개변수는 SnapCenter 서버 호스트에 MFA 메타데이터 파일을 저장할 경로를 지정합니다.

6. 생성된 파일을 AD FS 호스트에 복사하여 SnapCenter 클라이언트 엔터티로 구성합니다.
7. 다음을 사용하여 SnapCenter 서버에 대한 MFA를 활성화합니다. `Set-SmMultiFactorAuthentication cmdlet`.

8. (선택 사항) 다음을 사용하여 MFA 구성 상태 및 설정을 확인하세요. `Get-SmMultiFactorAuthentication cmdlet`.

9. Microsoft 관리 콘솔(MMC)로 이동하여 다음 단계를 수행합니다.

- a. 파일 > *스냅인 추가/제거*를 클릭합니다.
- b. 스냅인 추가/제거 창에서 *인증서*를 선택한 다음 *추가*를 클릭합니다.
- c. 인증서 스냅인 창에서 컴퓨터 계정 옵션을 선택한 다음 *마침*을 클릭합니다.
- d. 콘솔 루트 > 인증서 - 로컬 컴퓨터 > 개인 > *인증서*를 클릭합니다.
- e. SnapCenter 에 바인딩된 CA 인증서를 마우스 오른쪽 버튼으로 클릭한 다음 모든 작업 > *개인 키 관리*를 선택합니다.
- f. 권한 마법사에서 다음 단계를 수행하세요.
 - i. *추가*를 클릭하세요.
 - ii. *위치*를 클릭하고 해당 호스트(계층 구조의 최상위)를 선택합니다.
 - iii. 위치 팝업 창에서 *확인*을 클릭합니다.
 - iv. 개체 이름 필드에 'IIS_IUSRS'를 입력하고 *이름 확인*을 클릭한 다음 *확인*을 클릭합니다.

검사가 성공하면 *확인*을 클릭하세요.

10. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.

- a. 신뢰 당사자 트러스트*를 마우스 오른쪽 버튼으로 클릭하고 *신뢰 당사자 트러스트 추가 > *시작*을 클릭합니다.
- b. 두 번째 옵션을 선택하고 SnapCenter MFA 메타데이터 파일을 찾은 후 *다음*을 클릭합니다.
- c. 표시 이름을 지정하고 *다음*을 클릭합니다.
- d. 필요에 따라 액세스 제어 정책을 선택하고 *다음*을 클릭합니다.
- e. 다음 탭에서 설정을 기본값으로 선택하세요.
- f. *마침*을 클릭하세요.

SnapCenter 이제 제공된 표시 이름을 사용하는 신뢰 당사자로 반영됩니다.

11. 이름을 선택하고 다음 단계를 수행하세요.

- a. *청구 발행 정책 편집*을 클릭하세요.
- b. *규칙 추가*를 클릭하고 *다음*을 클릭합니다.
- c. 클레임 규칙의 이름을 지정합니다.
- d. 속성 저장소로 *Active Directory*를 선택합니다.
- e. 속성을 *User-Principal-Name*으로 선택하고, 나가는 클레임 유형을 *Name-ID*로 선택합니다.
- f. *마침*을 클릭하세요.

12. ADFS 서버에서 다음 PowerShell 명령을 실행합니다.

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-SigningCertificateRevocationCheck None
```

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'
```

-EncryptionCertificateRevocationCheck None

13. 메타데이터가 성공적으로 가져왔는지 확인하려면 다음 단계를 수행하세요.
 - a. 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *속성*을 선택합니다.
 - b. 엔드포인트, 식별자, 서명 필드가 채워져 있는지 확인하세요.
14. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성화된 세션 쿠키를 지우고 다시 로그인하세요.

SnapCenter MFA 기능은 REST API를 사용하여 활성화할 수도 있습니다.

문제 해결 정보는 다음을 참조하세요. "[여러 탭에서 동시 로그인 시도 시 MFA 오류가 표시됩니다.](#)".

AD FS MFA 메타데이터 업데이트

업그레이드, CA 인증서 갱신, DR 등 AD FS 서버에 수정 사항이 있을 때마다 SnapCenter 에서 AD FS MFA 메타데이터를 업데이트해야 합니다.

단계

1. AD FS 페더레이션 메타데이터 파일을 다운로드합니다. "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. 다운로드한 파일을 SnapCenter 서버에 복사하여 MFA 구성을 업데이트합니다.
3. 다음 cmdlet을 실행하여 SnapCenter 에서 AD FS 메타데이터를 업데이트합니다.

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성화된 세션 쿠키를 지우고 다시 로그인하세요.

SnapCenter MFA 메타데이터 업데이트

ADFS 서버에 복구, CA 인증서 갱신, DR 등 수정 사항이 있을 때마다 AD FS에서 SnapCenter MFA 메타데이터를 업데이트해야 합니다.

단계

1. AD FS 호스트에서 AD FS 관리 마법사를 열고 다음 단계를 수행합니다.
 - a. *신뢰 당사자 트러스트*를 선택하세요.
 - b. SnapCenter 에 대해 생성된 신뢰 당사자 트러스트를 마우스 오른쪽 버튼으로 클릭하고 *삭제*를 선택합니다.

신뢰 당사자 신뢰의 사용자 정의 이름이 표시됩니다.
 - c. 다중 요소 인증(MFA)을 활성화합니다.

보다 "[다중 요소 인증 활성화](#)".

2. 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성화된 세션 쿠키를 지우고 다시 로그인하세요.

다중 요소 인증(MFA) 비활성화

단계

1. MFA를 비활성화하고 MFA가 활성화되었을 때 생성된 구성 파일을 정리합니다. Set-

SmMultiFactorAuthentication cmdlet.

- 모든 브라우저 탭을 닫고 브라우저를 다시 열어 기존 또는 활성화된 세션 쿠키를 지우고 다시 로그인하세요.

Rest API, PowerShell 및 SCCLI를 사용하여 다중 인증 요소(MFA) 관리

MFA 로그인은 브라우저, REST API, PowerShell 및 SCCLI에서 지원됩니다. MFA는 AD FS ID 관리자를 통해 지원됩니다. GUI, REST API, PowerShell 및 SCCLI에서 MFA를 활성화, 비활성화하고 MFA를 구성할 수 있습니다.

AD FS를 OAuth/OIDC로 설정

Windows GUI 마법사를 사용하여 AD FS 구성

1. 서버 관리자 대시보드 > 도구 > *ADFS 관리*로 이동합니다.

2. **ADFS** > *응용 프로그램 그룹*으로 이동합니다.

- a. *응용 프로그램 그룹*을 마우스 오른쪽 버튼으로 클릭합니다.
- b. *애플리케이션 그룹 추가*를 선택하고 *애플리케이션 이름*을 입력합니다.
- c. *서버 애플리케이션*을 선택하세요.
- d. *다음*을 클릭하세요.

3. *클라이언트 식별자*를 복사하세요.

이것은 클라이언트 ID입니다. ... 리디렉트 URL에 콜백 URL(SnapCenter 서버 URL)을 추가합니다. ... *다음*을 클릭하세요.

4. *공유 비밀 생성*을 선택하세요.

비밀 값을 복사합니다. 이것은 고객의 비밀입니다. ... *다음*을 클릭하세요.

5. 요약 페이지에서 *다음*을 클릭합니다.

- a. 완료 페이지에서 *닫기*를 클릭합니다.

6. 새로 추가된 *응용 프로그램 그룹*을 마우스 오른쪽 버튼으로 클릭하고 *속성*을 선택합니다.

7. 앱 속성에서 *애플리케이션 추가*를 선택합니다.

8. *애플리케이션 추가*를 클릭하세요.

웹 API를 선택하고 *다음*을 클릭합니다.

9. 웹 API 구성 페이지에서 이전 단계에서 만든 SnapCenter 서버 URL과 클라이언트 식별자를 식별자 섹션에 입력합니다.

- a. *추가*를 클릭하세요.
- b. *다음*을 클릭하세요.

10. 액세스 제어 정책 선택 페이지에서 요구 사항에 따라 제어 정책을 선택합니다(예: 모든 사람 허용 및 MFA 요구) 그리고 *다음*을 클릭합니다.

11. 애플리케이션 권한 구성 페이지에서 기본적으로 openid가 범위로 선택되어 있으므로 *다음*을 클릭합니다.

12. 요약 페이지에서 *다음*을 클릭합니다.

완료 페이지에서 *닫기*를 클릭합니다.

13. 샘플 애플리케이션 속성 페이지에서 *확인*을 클릭합니다.

14. 권한 부여 서버(AD FS)에서 발행하고 리소스에서 사용하도록 의도된 JWT 토큰입니다.

이 토큰의 'aud' 또는 청중 클레임은 리소스 또는 웹 API의 식별자와 일치해야 합니다.

15. 선택한 WebAPI를 편집하고 콜백 URL(SnapCenter 서버 URL)과 클라이언트 식별자가 올바르게 추가되었는지 확인하세요.

OpenID Connect를 구성하여 사용자 이름을 클레임으로 제공합니다.

16. 서버 관리자의 오른쪽 상단에 있는 도구 메뉴 아래에 있는 **AD FS** 관리 도구를 엽니다.

a. 왼쪽 사이드바에서 애플리케이션 그룹 폴더를 선택합니다.

b. 웹 API를 선택하고 *편집*을 클릭합니다.

c. 발급 변환 규칙 탭으로 이동

17. *규칙 추가*를 클릭합니다.

a. 클레임 규칙 템플릿 드롭다운에서 *LDAP 속성을 클레임으로 보내기*를 선택합니다.

b. *다음*을 클릭하세요.

18. 청구 규칙 이름을 입력하세요.

a. 속성 저장소 드롭다운에서 *Active Directory*를 선택합니다.

b. **LDAP** 속성 드롭다운에서 사용자 주체 이름*을 선택하고 *송신 클레임 유형 드롭다운에서 *UPN*을 선택합니다.

c. *마침*을 클릭하세요.

PowerShell 명령을 사용하여 애플리케이션 그룹 만들기

PowerShell 명령을 사용하여 애플리케이션 그룹과 웹 API를 만들고 범위와 클레임을 추가할 수 있습니다. 이러한 명령은 자동화된 스크립트 형식으로 제공됩니다. 자세한 내용은 <KB 문서 링크>를 참조하세요.

1. 다음 명령을 사용하여 AD FS에서 새 애플리케이션 그룹을 만듭니다.

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier  
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

`ClientRoleIdentifier`귀하의 애플리케이션 그룹 이름

`redirectURL`승인 후 리디렉션을 위한 유효한 URL

2. AD FS 서버 애플리케이션을 만들고 클라이언트 비밀번호를 생성합니다.

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"  
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL  
-Identifier $identifier -GenerateClientSecret
```

3. ADFS 웹 API 애플리케이션을 만들고 사용해야 하는 정책 이름을 구성합니다.

```
$identifier = (New-Guid).Guid

Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"

-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 다음 명령의 출력에서 클라이언트 ID와 클라이언트 비밀번호를 얻으세요. 이는 한 번만 표시됩니다.

```
"client_id = $identifier"

"client_secret: "$($ADFSApp.ClientSecret)
```

5. AD FS 애플리케이션에 allatclaims 및 openid 권한을 부여합니다.

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==
"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 변환 규칙 파일을 작성합니다.

```
$transformrule |Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii $relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 외부 파일을 사용하여 웹 API 애플리케이션의 이름을 지정하고 발급 변환 규칙을 정의합니다.

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

액세스 토큰 만료 시간 업데이트

PowerShell 명령을 사용하여 액세스 토큰 만료 시간을 업데이트할 수 있습니다.

이 작업에 관하여

- 액세스 토큰은 사용자, 클라이언트, 리소스의 특정 조합에만 사용할 수 있습니다. 액세스 토큰은 취소할 수 없으며 만료일까지 유효합니다.
- 기본적으로 액세스 토큰의 만료 시간은 60분입니다. 이 최소 만료 시간은 충분하고 확장 가능합니다. 진행 중인 비즈니스에 중요한 작업을 피하기 위해 충분한 가치를 제공해야 합니다.

단계

애플리케이션 그룹 WebApi에 대한 액세스 토큰 만료 시간을 업데이트하려면 AD FS 서버에서 다음 명령을 사용합니다.

```
+ Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

AD FS에서 베어러 토큰 가져오기

REST 클라이언트(예: Postman)에서 아래에 언급된 매개변수를 입력하면 사용자 자격 증명을 입력하라는 메시지가 표시됩니다. 또한, 소지자 토큰을 받으려면 2차 인증(본인이 소유한 것 및 본인인 것)을 입력해야 합니다.

+ 베어러 토큰의 유효성은 애플리케이션별로 AD FS 서버에서 구성할 수 있으며 기본 유효 기간은 60분입니다.

필드	가치
보조금 유형	승인 코드
콜백 URL	콜백 URL이 없으면 애플리케이션의 기본 URL을 입력하세요.
인증 URL	[adfs-도메인-이름]/adfs/oauth2/authorize
액세스 토큰 URL	[adfs-도메인-이름]/adfs/oauth2/토큰
클라이언트 ID	AD FS 클라이언트 ID를 입력하세요
클라이언트 비밀번호	AD FS 클라이언트 비밀번호를 입력하세요
범위	오픈아이디
클라이언트 인증	기본 AUTH 헤더로 보내기
의지	고급 옵션 탭에서 JWT 토큰의 "aud" 값으로 제공되는 콜백 URL과 동일한 값을 가진 리소스 필드를 추가합니다.

PowerShell, SCCLI 및 REST API를 사용하여 SnapCenter 서버에서 MFA 구성

PowerShell, SCCLI 및 REST API를 사용하여 SnapCenter 서버에서 MFA를 구성할 수 있습니다.

SnapCenter MFA CLI 인증

PowerShell과 SCCLI에서 기존 cmdlet(Open-SmConnection)은 사용자를 인증하기 위해 전달자 토큰을 사용하기 위해 "AccessToken"이라는 필드가 하나 더 확장되었습니다.

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port <String>] [-RoleName <String>] [-AccessToken <string>]
```

위의 cmdlet을 실행한 후 해당 사용자가 추가 SnapCenter cmdlet을 실행할 수 있는 세션이 생성됩니다.

SnapCenter MFA REST API 인증

REST API 클라이언트(Postman이나 Swagger 등)에서 *Authorization=Bearer* <액세스 토큰> 형식의 베어러 토큰을 사용하고 헤더에 사용자 RoleName을 언급하면 SnapCenter 에서 성공적인 응답을 받을 수 있습니다.

MFA Rest API 워크플로

MFA가 AD FS로 구성된 경우 Rest API를 통해 SnapCenter 애플리케이션에 액세스하려면 액세스(베어러) 토큰을 사용하여 인증해야 합니다.

이 작업에 관하여

- Postman, Swagger UI 또는 FireCamp와 같은 REST 클라이언트를 사용할 수 있습니다.
- 액세스 토큰을 받아서 이후 요청(SnapCenter Rest API)을 인증하여 모든 작업을 수행합니다.

단계

AD FS MFA를 통해 인증하려면

1. 액세스 토큰을 가져오기 위해 AD FS 엔드포인트를 호출하도록 REST 클라이언트를 구성합니다.

애플리케이션에 대한 액세스 토큰을 받기 위해 버튼을 누르면 AD FS SSO 페이지로 리디렉션되며, 이 페이지에서 AD 자격 증명을 제공하고 MFA로 인증해야 합니다. 1. AD FS SSO 페이지에서 사용자 이름 텍스트 상자에 사용자 이름이나 이메일을 입력합니다.

+ 사용자 이름은 user@domain 또는 domain\user 형식이어야 합니다.

2. 비밀번호 텍스트 상자에 비밀번호를 입력하세요.
3. *로그인*을 클릭하세요.
4. 로그인 옵션 섹션에서 인증 옵션을 선택하고 인증합니다(구성에 따라 다름).
 - 푸시: 휴대폰으로 전송되는 푸시 알림을 승인합니다.
 - QR 코드: AUTH Point 모바일 앱을 사용하여 QR 코드를 스캔한 다음 앱에 표시된 확인 코드를 입력하세요.
 - 일회용 비밀번호: 토큰의 일회용 비밀번호를 입력하세요.

5. 인증에 성공하면 액세스 토큰, ID 토큰, 새로 고침 토큰이 포함된 팝업이 열립니다.

액세스 토큰을 복사하여 SnapCenter Rest API에서 사용하여 작업을 수행합니다.

6. Rest API에서는 헤더 섹션에 액세스 토큰과 역할 이름을 전달해야 합니다.

7. SnapCenter AD FS에서 이 액세스 토큰의 유효성을 검사합니다.

유효한 토큰이면 SnapCenter 이를 디코딩하여 사용자 이름을 가져옵니다.

8. SnapCenter 사용자 이름과 역할 이름을 사용하여 API 실행을 위해 사용자를 인증합니다.

인증에 성공하면 SnapCenter 결과를 반환하고, 그렇지 않으면 오류 메시지가 표시됩니다.

Rest API, CLI 및 GUI에 대한 SnapCenter MFA 기능 활성화 또는 비활성화

GUI

단계

1. SnapCenter 관리자로 SnapCenter 서버에 로그인합니다.
2. 설정 > 전역 설정 > *다중 인증(MFA) 설정*을 클릭합니다.
3. MFA 로그인을 활성화하거나 비활성화하려면 인터페이스(GUI/RST API/CLI)를 선택하세요.

PowerShell 인터페이스

단계

1. GUI, Rest API, PowerShell 및 SCCLI에 대해 MFA를 활성화하려면 PowerShell 또는 CLI 명령을 실행합니다.

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled  
-IsCliMFAEnabled -Path
```

경로 매개 변수는 AD FS MFA 메타데이터 xml 파일의 위치를 지정합니다.

지정된 AD FS 메타데이터 파일 경로로 구성된 SnapCenter GUI, Rest API, PowerShell 및 SCCLI에 대해 MFA를 활성화합니다.

2. 다음을 사용하여 MFA 구성 상태 및 설정을 확인하세요. `Get-SmMultiFactorAuthentication cmdlet`.

SCCLI 인터페이스

단계

1. # `sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true -IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path "C:\ADFS_metadata\abc.xml"`
2. # `sccli Get-SmMultiFactorAuthentication`

REST API

1. GUI, REST API, PowerShell 및 SCCLI에 대한 MFA를 활성화하기 위해 다음 게시물 API를 실행합니다.

매개변수	가치
요청된 URL	/api/4.9/설정/다중 인증
HTTP 메서드	우편
요청 본문	{ "IsGuiMFAEnabled": 거짓, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": 거짓, "ADFSConfigFilePath": "C:\ADFS_metadata\abc.xml" }
대응 기관	{ "MFAConfiguration": { "IsGuiMFAEnabled": 거짓, "ADFSConfigFilePath": "C:\ADFS_metadata\abc.xml", "SCConfigFilePath": 널, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": 거짓, "ADFSHostName": "win-ads-sc49.winscedom2.com" } }

2. 다음 API를 사용하여 MFA 구성 상태와 설정을 확인하세요.

매개변수	가치
요청된 URL	/api/4.9/설정/다중 인증
HTTP 메서드	얻다
대응 기관	{ "MFAConfiguration": { "IsGuiMFAEnabled": 거짓, "ADFSConfigFilePath": "C:\ADFS_metadata\abc.xml", "SCConfigFilePath": 널, "IsRestApiMFAEnabled": 참, "IsCliMFAEnabled": 거짓, "ADFSHostName": "win-ads-sc49.winscedom2.com" } }

저작권 정보

Copyright © 2025 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.