



Vorbereiten der Installation des SnapCenter -Servers

SnapCenter software

NetApp
November 06, 2025

Inhalt

Vorbereiten der Installation des SnapCenter -Servers	1
Voraussetzungen für die Installation von SnapCenter Server	1
Domänen- und Arbeitsgruppenanforderungen für Windows-Host	1
Platz- und Größenanforderungen	1
SAN-Hostanforderungen	3
Browseranforderungen	3
Portanforderungen	3
Registrieren Sie sich, um auf die SnapCenter software zuzugreifen	8
Multi-Faktor-Authentifizierung (MFA)	9
Verwalten der Multi-Faktor-Authentifizierung (MFA)	9
Verwalten Sie die Multi-Faktor-Authentifizierung (MFA) mit Rest API, PowerShell und SCCLI	12
Konfigurieren Sie MFA in SnapCenter Server mit PowerShell, SCCLI und REST-API	16

Vorbereiten der Installation des SnapCenter -Servers

Voraussetzungen für die Installation von SnapCenter Server

Bevor Sie SnapCenter Server auf einem Windows- oder Linux-Host installieren, sollten Sie überprüfen und sicherstellen, dass alle Anforderungen für Ihre Umgebung erfüllt sind.

Domänen- und Arbeitsgruppenanforderungen für Windows-Host

Der SnapCenter -Server kann auf einem Windows-Host installiert werden, der sich entweder in einer Domäne oder in einer Arbeitsgruppe befindet.

Der Benutzer mit Administratorrechten darf den SnapCenter -Server installieren.

- Active Directory-Domäne: Sie müssen einen Domänenbenutzer mit lokalen Administratorrechten verwenden. Der Domänenbenutzer muss Mitglied der lokalen Administratorgruppe auf dem Windows-Host sein.
- Arbeitsgruppen: Sie müssen ein lokales Konto mit lokalen Administratorrechten verwenden.

Während Domänenvertrauensstellungen, Mehrdomäengesamtstrukturen und domänenübergreifende Vertrauensstellungen unterstützt werden, werden gesamtstrukturübergreifende Domänen nicht unterstützt. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu Active Directory-Domänen und -Vertrauensstellungen.

 Nach der Installation des SnapCenter -Servers sollten Sie die Domäne, in der sich der SnapCenter Host befindet, nicht ändern. Wenn Sie den SnapCenter Server-Host aus der Domäne entfernen, in der er sich bei der Installation des SnapCenter Servers befand, und dann versuchen, den SnapCenter Server zu deinstallieren, schlägt der Deinstallationsvorgang fehl.

Platz- und Größenanforderungen

Sie sollten mit den Platz- und Größenanforderungen vertraut sein.

Artikel	Windows-Hostanforderungen	Linux-Hostanforderungen
Betriebssysteme	<p>Microsoft Windows</p> <p>Es werden nur die Betriebssystemversionen Englisch, Deutsch, Japanisch und vereinfachtes Chinesisch unterstützt.</p> <p>Aktuelle Informationen zu unterstützten Versionen finden Sie unter https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT['NetApp Interoperabilitätsmatrix-Tool'].</p>	<ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL) 8 und 9• SUSE Linux Enterprise Server (SLES) 15 <p>Aktuelle Informationen zu unterstützten Versionen finden Sie unter https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT['NetApp Interoperabilitätsmatrix-Tool'].</p>

Artikel	Windows-Hostanforderungen	Linux-Hostanforderungen
Minimale CPU-Anzahl	4 Kerne	4 Kerne
Mindest-RAM	<p>8 GB</p> <p> Der Pufferpool des MySQL-Servers verwendet 20 Prozent des gesamten RAM.</p>	8 GB
Mindestfestplattenspeicherplatz für die SnapCenter Server-Software und -Protokolle	<p>7 GB</p> <p> Wenn sich das SnapCenter Repository auf demselben Laufwerk befindet, auf dem SnapCenter Server installiert ist, werden 15 GB empfohlen.</p>	15 GB
Mindestfestplattenspeicherplatz für das SnapCenter -Repository	<p>8 GB</p> <p> HINWEIS: Wenn sich der SnapCenter -Server auf demselben Laufwerk befindet, auf dem das SnapCenter Repository installiert ist, werden 15 GB empfohlen.</p>	Nicht zutreffend

Artikel	Windows-Hostanforderungen	Linux-Hostanforderungen
Erforderliche Softwarepakete	<ul style="list-style-type: none"> ASP.NET Core Runtime 8.0.12 (und alle nachfolgenden 8.0.x-Patches) Hosting-Paket PowerShell 7.4.2 oder höher 	<ul style="list-style-type: none"> .NET Framework 8.0.12 (und alle nachfolgenden 8.0.x-Patches) PowerShell 7.4.2 oder höher Nginx ist ein Webserver, der als Reverse-Proxy verwendet werden kann Pam-devel <p>PAM (Pluggable Authentication Modules) ist ein Systemsicherheitstool, mit dem Systemadministratoren Authentifizierungsrichtlinien festlegen können, ohne Programme, die die Authentifizierung durchführen, neu kompilieren zu müssen.</p>



ASP.NET Core benötigt IIS_IUSRS, um auf das temporäre Dateisystem im SnapCenter Server unter Windows zuzugreifen.

SAN-Hostanforderungen

SnapCenter enthält keine Host-Dienstprogramme oder ein DSM. Wenn der SnapCenter Host Teil einer SAN-Umgebung (FC/iSCSI) ist, müssen Sie möglicherweise zusätzliche Software auf dem SnapCenter -Server -Host installieren und konfigurieren.

- Host-Dienstprogramme: Die Host-Dienstprogramme unterstützen FC und iSCSI und ermöglichen Ihnen die Verwendung von MPIO auf Ihren Windows-Servern. ["Weitere Informationen"](#) .
- Microsoft DSM für Windows MPIO: Diese Software arbeitet mit Windows MPIO-Treibern, um mehrere Pfade zwischen NetApp und Windows-Hostcomputern zu verwalten. Für Hochverfügbarkeitskonfigurationen ist ein DSM erforderlich.



Wenn Sie ONTAP DSM verwendet haben, sollten Sie zu Microsoft DSM migrieren. Weitere Informationen finden Sie unter ["So migrieren Sie von ONTAP DSM zu Microsoft DSM"](#) .

Browseranforderungen

Die SnapCenter software unterstützt Chrome 125 und höher sowie Microsoft Edge 110.0.1587.17 und höher.

Portanforderungen

Die SnapCenter software benötigt unterschiedliche Ports für die Kommunikation zwischen verschiedenen Komponenten.

- Anwendungen können keinen Port gemeinsam nutzen.

- Für anpassbare Ports können Sie während der Installation einen benutzerdefinierten Port auswählen, wenn Sie den Standardport nicht verwenden möchten.
- Bei festen Ports sollten Sie die Standard-Portnummer akzeptieren.
- Firewalls
 - Firewalls, Proxys oder andere Netzwerkgeräte sollten die Verbindungen nicht stören.
 - Wenn Sie bei der Installation von SnapCenter einen benutzerdefinierten Port angeben, sollten Sie für den SnapCenter Plug-in Loader eine Firewall-Regel auf dem Plug-in-Host für diesen Port hinzufügen.

In der folgenden Tabelle sind die verschiedenen Ports und ihre Standardwerte aufgeführt.

Portname	Portnummern	Protokoll	Richtung	Beschreibung
SnapCenter -Webport	8146	HTTPS	Bidirektional	<p>Dieser Port wird für die Kommunikation zwischen dem SnapCenter Client (dem SnapCenter -Benutzer) und dem SnapCenter -Server verwendet und wird auch für die Kommunikation von den Plug-In-Hosts zum SnapCenter -Server verwendet.</p> <p>Sie können die Portnummer anpassen.</p>
SnapCenter SMCore- Kommunikationsport	8145	HTTPS	Bidirektional	<p>Dieser Port wird für die Kommunikation zwischen dem SnapCenter Server und den Hosts verwendet, auf denen die SnapCenter Plug-Ins installiert sind.</p> <p>Sie können die Portnummer anpassen.</p>

Portname	Portnummern	Protokoll	Richtung	Beschreibung
Scheduler-Dienstport	8154	HTTPS		<p>Dieser Port wird verwendet, um die SnapCenter -Scheduler -Workflows für alle verwalteten Plug-Ins innerhalb des SnapCenter -Serverhosts zentral zu orchestrieren.</p> <p>Sie können die Portnummer anpassen.</p>
RabbitMQ-Port	5672	TCP		<p>Dies ist der Standardport, auf dem RabbitMQ lauscht, und er wird für die Publisher-Subscriber-Modellkommunikation zwischen dem Scheduler-Dienst und SnapCenter verwendet.</p>
MySQL-Port	3306	HTTPS		<p>Der Port wird für die Kommunikation mit der SnapCenter -Repository -Datenbank verwendet. Sie können sichere Verbindungen vom SnapCenter -Server zum MySQL-Server erstellen. "Mehr erfahren"</p>

Portname	Portnummern	Protokoll	Richtung	Beschreibung
Windows-Plug-In-Hosts	135, 445	TCP		Dieser Port wird für die Kommunikation zwischen dem SnapCenter -Server und dem Host verwendet, auf dem das Plug-In installiert wird. Der zusätzliche dynamische Portbereich, der von Microsoft angegeben wird, sollte ebenfalls offen sein.
Linux- oder AIX-Plug-in-Hosts	22	SSH	Unidirektional	Dieser Port wird für die Kommunikation zwischen dem SnapCenter -Server und dem Host verwendet und vom Server zum Client-Host initiiert.
SnapCenter Plug-In-Paket für Windows, Linux oder AIX	8145	HTTPS	Bidirektional	Dieser Port wird für die Kommunikation zwischen SMCore und Hosts verwendet, auf denen das Plug-In-Paket installiert ist. Anpassbar. Sie können die Portnummer anpassen.
SnapCenter -Plug-in für Oracle-Datenbank	27216			Der Standard-JDBC-Port wird vom Plug-In für Oracle zum Herstellen einer Verbindung mit der Oracle-Datenbank verwendet.

Portname	Portnummern	Protokoll	Richtung	Beschreibung
SnapCenter -Plug-in für Exchange-Datenbank	909			Der Standard-NET.TCP-Port wird vom Plug-In für Windows zum Herstellen einer Verbindung mit den Exchange-VSS-Rückrufen verwendet.
Von NetApp unterstützte Plug-ins für SnapCenter	9090	HTTPS		<p>Dies ist ein interner Port, der nur auf dem Plug-In-Host verwendet wird. Es ist keine Firewall-Ausnahme erforderlich.</p> <p>Die Kommunikation zwischen dem SnapCenter -Server und den Plug-Ins wird über Port 8145 geleitet.</p>
ONTAP Cluster oder SVM-Kommunikationsport	<ul style="list-style-type: none"> • 443 (HTTPS) • 80 (HTTP) 	<ul style="list-style-type: none"> • HTTPS • HTTP 	Bidirektional	Der Port wird vom SAL (Storage Abstraction Layer) für die Kommunikation zwischen dem Host, auf dem SnapCenter Server ausgeführt wird, und SVM verwendet. Der Port wird derzeit auch vom SAL auf SnapCenter für Windows-Plug-in-Hosts für die Kommunikation zwischen dem SnapCenter -Plug-in-Host und SVM verwendet.

Portname	Portnummern	Protokoll	Richtung	Beschreibung
SnapCenter Plug-in für SAP HANA-Datenbank	<ul style="list-style-type: none"> 3instance_number13 3instance_number15 	<ul style="list-style-type: none"> HTTPS HTTP 	Bidirektional	<p>Bei einem Multitenant-Datenbankcontainer (MDC) mit einem einzelnen Mandanten endet die Portnummer mit 13; bei Nicht-MDC endet die Portnummer mit 15.</p> <p>Sie können die Portnummer anpassen.</p>
SnapCenter Plug-in für PostgreSQL	5432			<p>Dieser Port ist der PostgreSQL-Standardport, der vom Plug-In für PostgreSQL für die Kommunikation mit dem PostgreSQL-Cluster verwendet wird.</p> <p>Sie können die Portnummer anpassen.</p>

Registrieren Sie sich, um auf die SnapCenter software zuzugreifen

Sie sollten sich für den Zugriff auf die SnapCenter software registrieren, wenn Sie neu bei Amazon FSx for NetApp ONTAP oder Azure NetApp Files sind und kein bestehendes NetApp Konto haben.

Bevor Sie beginnen

- Sie sollten Zugriff auf die Unternehmens-E-Mail-ID haben.
- Wenn Sie Azure NetApp Files verwenden, sollten Sie über die Azure-Abonnement-ID verfügen.
- Wenn Sie Amazon FSx for NetApp ONTAP verwenden, sollten Sie die Dateisystem-ID Ihres FSx für ONTAP -Dateisystems haben.

Informationen zu diesem Vorgang

Ihre Registrierung unterliegt der Validierung Ihrer Informationen und es kann bis zu einem Tag dauern, bis das neue NetApp Support Site (NSS)-Konto bestätigt und vom **Gast**-Zugriff auf **vollständigen** Zugriff aktualisiert wird.

Schritte

1. Klicken <https://mysupport.netapp.com/site/user/registration> zur Registrierung.
2. Geben Sie Ihre Unternehmens-E-Mail-ID ein, füllen Sie das Captcha aus, akzeptieren Sie die Datenschutzrichtlinie von NetApp und klicken Sie auf **Senden**.
3. Authentifizieren Sie die Registrierung, indem Sie das an Ihre E-Mail-ID gesendete OTP eingeben und auf **Weiter** klicken.
4. Geben Sie auf der Seite zum Abschluss der Registrierung die folgenden Details ein, um die Registrierung abzuschließen.
 - a. Wählen Sie * NetApp -Kunde/Endbenutzer*.
 - b. Geben Sie im Feld SERIENNUMMER entweder die Azure-Abonnement-ID ein, wenn Sie Azure NetApp Files verwenden, oder die Dateisystem-ID, wenn Sie Amazon FSx for NetApp ONTAP verwenden.



Sie können ein Ticket erstellen unter <https://mysupport.netapp.com/site/help> wenn Sie während der Registrierung auf ein Problem stoßen oder den Status erfahren möchten.

Multi-Faktor-Authentifizierung (MFA)

Verwalten der Multi-Faktor-Authentifizierung (MFA)

Sie können die Multi-Faktor-Authentifizierungsfunktion (MFA) im Active Directory Federation Service (AD FS)-Server und im SnapCenter Server verwalten.

Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA).

Sie können die MFA-Funktionalität für SnapCenter Server mithilfe von PowerShell-Befehlen aktivieren.

Informationen zu diesem Vorgang

- SnapCenter unterstützt SSO-basierte Anmeldungen, wenn andere Anwendungen im selben AD FS konfiguriert sind. In bestimmten AD FS-Konfigurationen erfordert SnapCenter möglicherweise aus Sicherheitsgründen eine Benutzeroauthentifizierung, abhängig von der Persistenz der AD FS-Sitzung.
- Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von `Get-Help command_name`. Alternativ können Sie auch sehen "["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#)" .

Bevor Sie beginnen

- Der Windows Active Directory Federation Service (AD FS) sollte in der jeweiligen Domäne aktiv und betriebsbereit sein.
- Sie sollten über einen von AD FS unterstützten Multi-Faktor-Authentifizierungsdienst wie Azure MFA, Cisco Duo usw. verfügen.
- Der Zeitstempel des SnapCenter und AD FS-Servers sollte unabhängig von der Zeitzone identisch sein.
- Beschaffen und konfigurieren Sie das autorisierte CA-Zertifikat für SnapCenter Server.

Ein CA-Zertifikat ist aus folgenden Gründen obligatorisch:

- Stellt sicher, dass die ADFS-F5-Kommunikation nicht unterbrochen wird, da die selbstsignierten Zertifikate auf Knotenebene eindeutig sind.
- Stellt sicher, dass während eines Upgrades, einer Reparatur oder einer Notfallwiederherstellung (DR)

in einer eigenständigen oder Hochverfügbarkeitskonfiguration das selbstsignierte Zertifikat nicht neu erstellt wird, wodurch eine MFA-Neukonfiguration vermieden wird.

- Stellt IP-FQDN-Auflösungen sicher.

Informationen zum CA-Zertifikat finden Sie unter "[CA-Zertifikat-CSR-Datei generieren](#)".

Schritte

1. Stellen Sie eine Verbindung zum Active Directory Federation Services (AD FS)-Host her.
2. Laden Sie die AD FS-Verbundmetadatendatei herunter von "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>".
3. Kopieren Sie die heruntergeladene Datei auf den SnapCenter -Server, um die MFA-Funktion zu aktivieren.
4. Melden Sie sich über PowerShell als SnapCenter -Administratorbenutzer beim SnapCenter -Server an.
5. Generieren Sie mithilfe der PowerShell-Sitzung die SnapCenter MFA-Metadatendatei mit dem Cmdlet `New-SmMultifactorAuthenticationMetadata -path`.

Der Pfadparameter gibt den Pfad zum Speichern der MFA-Metadatendatei im SnapCenter Server-Host an.

6. Kopieren Sie die generierte Datei auf den AD FS-Host, um SnapCenter als Cliententität zu konfigurieren.
7. Aktivieren Sie MFA für SnapCenter Server mithilfe des `Set-SmMultiFactorAuthentication` Cmdlet.
8. (Optional) Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe von `Get-SmMultiFactorAuthentication` Cmdlet.
9. Gehen Sie zur Microsoft-Verwaltungskonsole (MMC) und führen Sie die folgenden Schritte aus:
 - a. Klicken Sie auf **Datei** > **Snap-In hinzufügen/entfernen**.
 - b. Wählen Sie im Fenster „Snap-Ins hinzufügen oder entfernen“ **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
 - c. Wählen Sie im Zertifikat-Snap-In-Fenster die Option **Computerkonto** und klicken Sie dann auf **Fertig**.
 - d. Klicken Sie auf **Konsolenstamm** > **Zertifikate – Lokaler Computer** > **Persönlich** > **Zertifikate**.
 - e. Klicken Sie mit der rechten Maustaste auf das an SnapCenter gebundene CA-Zertifikat und wählen Sie dann **Alle Aufgaben** > **Private Schlüssel verwalten**.
 - f. Führen Sie im Berechtigungsassistenten die folgenden Schritte aus:
 - i. Klicken Sie auf **Hinzufügen**.
 - ii. Klicken Sie auf **Standorte** und wählen Sie den betreffenden Host (oben in der Hierarchie) aus.
 - iii. Klicken Sie im Popup-Fenster **Standorte** auf **OK**.
 - iv. Geben Sie im Feld „Objektname“ „IIS_IUSRS“ ein, klicken Sie auf **Namen überprüfen** und dann auf **OK**.

Wenn die Prüfung erfolgreich war, klicken Sie auf **OK**.

10. Öffnen Sie im AD FS-Host den AD FS-Verwaltungsassistenten und führen Sie die folgenden Schritte aus:
 - a. Klicken Sie mit der rechten Maustaste auf **Vertrauensstellungen der vertrauenden Partei** > **Vertrauensstellung der vertrauenden Partei hinzufügen** > **Start**.
 - b. Wählen Sie die zweite Option, durchsuchen Sie die SnapCenter MFA-Metadatendatei und klicken Sie auf **Weiter**.
 - c. Geben Sie einen Anzeigenamen an und klicken Sie auf **Weiter**.

- d. Wählen Sie nach Bedarf eine Zugriffskontrollrichtlinie aus und klicken Sie auf **Weiter**.
- e. Wählen Sie im nächsten Reiter die Standardeinstellungen aus.
- f. Klicken Sie auf **Fertig**.

SnapCenter wird jetzt mit dem angegebenen Anzeigenamen als vertrauende Partei angezeigt.

11. Wählen Sie den Namen aus und führen Sie die folgenden Schritte aus:
 - a. Klicken Sie auf **Richtlinie zur Anspruchsausstellung bearbeiten**.
 - b. Klicken Sie auf **Regel hinzufügen** und dann auf **Weiter**.
 - c. Geben Sie einen Namen für die Anspruchsregel an.
 - d. Wählen Sie **Active Directory** als Attributspeicher aus.
 - e. Wählen Sie das Attribut als **User-Principal-Name** und den ausgehenden Anspruchstyp als **Name-ID**.
 - f. Klicken Sie auf **Fertig**.
12. Führen Sie die folgenden PowerShell-Befehle auf dem ADFS-Server aus.

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

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

13. Führen Sie die folgenden Schritte aus, um zu bestätigen, dass die Metadaten erfolgreich importiert wurden.
 - a. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Seite und wählen Sie **Eigenschaften**.
 - b. Stellen Sie sicher, dass die Felder „Endpunkte“, „Kennungen“ und „Signatur“ ausgefüllt sind.
14. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Sitzungscookies zu löschen, und melden Sie sich erneut an.

Die SnapCenter MFA-Funktionalität kann auch mithilfe von REST-APIs aktiviert werden.

Informationen zur Fehlerbehebung finden Sie unter "[Gleichzeitige Anmeldeversuche in mehreren Registerkarten zeigen einen MFA-Fehler](#)".

Aktualisieren der AD FS MFA-Metadaten

Sie sollten die AD FS MFA-Metadaten in SnapCenter aktualisieren, wenn es Änderungen am AD FS-Server gibt, z. B. Upgrade, Erneuerung des CA-Zertifikats, DR usw.

Schritte

1. Laden Sie die AD FS-Verbundmetadatendatei herunter von "<https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. Kopieren Sie die heruntergeladene Datei auf den SnapCenter -Server, um die MFA-Konfiguration zu aktualisieren.
3. Aktualisieren Sie die AD FS-Metadaten in SnapCenter , indem Sie das folgende Cmdlet ausführen:

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

4. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Sitzungscookies zu löschen, und melden Sie sich erneut an.

Aktualisieren Sie die SnapCenter MFA-Metadaten

Sie sollten die SnapCenter MFA-Metadaten in AD FS aktualisieren, wenn am ADFS-Server Änderungen vorgenommen werden, z. B. Reparaturen, Erneuerung des CA-Zertifikats, DR usw.

Schritte

1. Öffnen Sie im AD FS-Host den AD FS-Verwaltungsassistenten und führen Sie die folgenden Schritte aus:
 - a. Wählen Sie **Vertrauensstellungen der vertrauenden Partei** aus.
 - b. Klicken Sie mit der rechten Maustaste auf die Vertrauensstellung der vertrauenden Partei, die für SnapCenter erstellt wurde, und wählen Sie **Löschen**.

Der benutzerdefinierte Name des Relying Party Trust wird angezeigt.

- c. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA).

Sehen ["Aktivieren Sie die Multi-Faktor-Authentifizierung"](#).

2. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Sitzungscookies zu löschen, und melden Sie sich erneut an.

Deaktivieren Sie die Multi-Faktor-Authentifizierung (MFA).

Schritte

1. Deaktivieren Sie MFA und bereinigen Sie die Konfigurationsdateien, die beim Aktivieren von MFA erstellt wurden, mithilfe des `Set-SmMultiFactorAuthentication` Cmdlet.
2. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Sitzungscookies zu löschen, und melden Sie sich erneut an.

Verwalten Sie die Multi-Faktor-Authentifizierung (MFA) mit Rest API, PowerShell und SCCLI

Die MFA-Anmeldung wird über Browser, REST-API, PowerShell und SCCLI unterstützt. MFA wird durch einen AD FS-Identitätsmanager unterstützt. Sie können MFA aktivieren, deaktivieren und MFA über GUI, REST-API, PowerShell und SCCLI konfigurieren.

AD FS als OAuth/OIDC einrichten

AD FS mit dem Windows-GUI-Assistenten konfigurieren

1. Navigieren Sie zu **Server Manager Dashboard > Tools > ADFS-Verwaltung**.
2. Navigieren Sie zu **ADFS > Anwendungsgruppen**.
 - a. Klicken Sie mit der rechten Maustaste auf **Anwendungsgruppen**.
 - b. Wählen Sie **Anwendungsgruppe hinzufügen** und geben Sie **Anwendungsname** ein.
 - c. Wählen Sie **Serveranwendung**.
 - d. Klicken Sie auf **Weiter**.
3. Kopieren Sie **Client-ID**.

Dies ist die Client-ID. ... Fügen Sie der Umleitungs-URL eine Rückruf-URL (SnapCenter -Server-URL) hinzu. ... Klicken Sie auf **Weiter**.

4. Wählen Sie **Gemeinsames Geheimnis generieren**.

Kopieren Sie den geheimen Wert. Dies ist das Geheimnis des Kunden. ... Klicken Sie auf **Weiter**.

5. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.

a. Klicken Sie auf der Seite **Abgeschlossen** auf **Schließen**.

6. Klicken Sie mit der rechten Maustaste auf die neu hinzugefügte **Anwendungsgruppe** und wählen Sie **Eigenschaften**.

7. Wählen Sie in den App-Eigenschaften **Anwendung hinzufügen** aus.

8. Klicken Sie auf **Anwendung hinzufügen**.

Wählen Sie Web-API und klicken Sie auf **Weiter**.

9. Geben Sie auf der Seite „Web-API konfigurieren“ die im vorherigen Schritt erstellte SnapCenter -Server -URL und Client-ID in den Abschnitt „ID“ ein.

a. Klicken Sie auf **Hinzufügen**.

b. Klicken Sie auf **Weiter**.

10. Wählen Sie auf der Seite **Zugriffskontrollrichtlinie auswählen** die Kontrollrichtlinie entsprechend Ihren Anforderungen aus (z. B. „Jeden zulassen“ und „MFA erforderlich“) und klicken Sie auf **Weiter**.

11. Klicken Sie auf der Seite **Anwendungsberechtigung konfigurieren** standardmäßig auf „openid“ als Bereich. Klicken Sie auf **Weiter**.

12. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.

Klicken Sie auf der Seite **Abgeschlossen** auf **Schließen**.

13. Klicken Sie auf der Seite **Beispielanwendungseigenschaften** auf **OK**.

14. Von einem Autorisierungsserver (AD FS) ausgestelltes und von der Ressource zu verwendendes JWT-Token.

Der „aud“- oder Zielgruppenanspruch dieses Tokens muss mit der Kennung der Ressource oder Web-API übereinstimmen.

15. Bearbeiten Sie die ausgewählte WebAPI und überprüfen Sie, ob die Rückruf-URL (SnapCenter -Server -URL) und die Client-ID korrekt hinzugefügt wurden.

Konfigurieren Sie OpenID Connect, um einen Benutzernamen als Ansprüche bereitzustellen.

16. Öffnen Sie das Tool **AD FS-Verwaltung**, das sich im Menü **Tools** oben rechts im Server-Manager befindet.

a. Wählen Sie in der linken Seitenleiste den Ordner **Anwendungsgruppen** aus.

b. Wählen Sie die Web-API aus und klicken Sie auf **BEARBEITEN**.

c. Zur Registerkarte „Ausgabetransformationsregeln“

17. Klicken Sie auf **Regel hinzufügen**.

a. Wählen Sie im Dropdownmenü „Anspruchsregelvorlage“ die Option „LDAP-Attribute als Ansprüche senden“ aus.

- b. Klicken Sie auf **Weiter**.
18. Geben Sie den Namen der **Anspruchsregel** ein.
- Wählen Sie im Dropdown-Menü „Attributspeicher“ **Active Directory** aus.
 - Wählen Sie **User-Principal-Name** im Dropdown-Menü **LDAP-Attribut** und **UPN** im Dropdown-Menü **Ausgehender Anspruchstyp**.
 - Klicken Sie auf **Fertig**.

Erstellen einer Anwendungsgruppe mit PowerShell-Befehlen

Sie können die Anwendungsgruppe und die Web-API erstellen und den Bereich und die Ansprüche mithilfe von PowerShell-Befehlen hinzufügen. Diese Befehle sind im automatisierten Skriptformat verfügbar. Weitere Informationen finden Sie unter <Link zum KB-Artikel>.

1. Erstellen Sie die neue Anwendungsgruppe in AD FS mit dem folgenden Befehl.

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier  
-ApplicationGroupIdentifier $ClientRoleIdentifier  
'ClientRoleIdentifier`Name Ihrer Anwendungsgruppe  
'redirectURL`gültige URL zur Weiterleitung nach Autorisierung
```

2. Erstellen Sie die AD FS-Serveranwendung und generieren Sie das Clientgeheimnis.

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

3. Erstellen Sie die ADFS-Web-API-Anwendung und konfigurieren Sie den Richtliniennamen, den sie verwenden soll.

```
$Identifier = (New-Guid).Guid  
  
Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier  
-Name "App Web API"  
  
-Identifier $Identifier -AccessControlPolicyName "Permit everyone"
```

4. Holen Sie sich die Client-ID und das Client-Geheimnis aus der Ausgabe der folgenden Befehle, da diese nur einmal angezeigt werden.

```
"client_id = $Identifier"  
  
"client_secret: $($ADFSApp.ClientSecret)
```

5. Erteilen Sie der AD FS-Anwendung die Berechtigungen „allatclaims“ und „openid“.

```
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. Schreiben Sie die Datei mit den Transformationsregeln.

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

7. Benennen Sie die Web-API-Anwendung und definieren Sie ihre Ausgabetransformationsregeln mithilfe einer externen Datei.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile
$relativePath
```

Ablaufzeit des Zugriffstokens aktualisieren

Sie können die Ablaufzeit des Zugriffstokens mit dem PowerShell-Befehl aktualisieren.

Über diese Aufgabe

- Ein Zugriffstoken kann nur für eine bestimmte Kombination aus Benutzer, Client und Ressource verwendet werden. Zugriffstoken können nicht widerrufen werden und sind bis zu ihrem Ablauf gültig.
- Standardmäßig beträgt die Ablaufzeit eines Zugriffstokens 60 Minuten. Diese minimale Ablaufzeit ist ausreichend und skaliert. Sie müssen einen ausreichenden Wert bereitstellen, um die Ausführung geschäftskritischer Jobs zu vermeiden.

Schritt

Um die Ablaufzeit des Zugriffstokens für eine Anwendungsgruppen-WebAPI zu aktualisieren, verwenden Sie den folgenden Befehl im AD FS-Server.

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

Abrufen des Bearertokens von AD FS

Sie sollten die unten genannten Parameter in einem beliebigen REST-Client (wie Postman) eingeben und werden aufgefordert, die Benutzeranmeldeinformationen einzugeben. Zusätzlich sollten Sie die Zwei-Faktor-Authentifizierung (etwas, das Sie haben und etwas, das Sie sind) eingeben, um das Inhabertoken zu erhalten.

+ Die Gültigkeit des Bearer-Tokens kann vom AD FS-Server pro Anwendung konfiguriert werden und die Standardgültigkeitsdauer beträgt 60 Minuten.

Feld	Wert
Zuschussart	Autorisierungscode
Rückruf-URL	Geben Sie die Basis-URL Ihrer Anwendung ein, wenn Sie keine Rückruf-URL haben.
Authentifizierungs-URL	[ADFS-Domänenname]/adfs/oauth2/authorize
Zugriffstoken-URL	[ADFS-Domänenname]/adfs/oauth2/token
Client-ID	Geben Sie die AD FS-Client-ID ein
Clientgeheimnis	Geben Sie den geheimen AD FS-Clientschlüssel ein.
Umfang	OpenID
Client-Authentifizierung	Als Basic AUTH Header senden
Ressource	Fügen Sie auf der Registerkarte Erweiterte Optionen das Feld „Ressource“ mit demselben Wert wie die Rückruf-URL hinzu, die als „aud“-Wert im JWT-Token enthalten ist.

Konfigurieren Sie MFA in SnapCenter Server mit PowerShell, SCCLI und REST-API

Sie können MFA in SnapCenter Server mithilfe von PowerShell, SCCLI und REST API konfigurieren.

SnapCenter MFA CLI-Authentifizierung

In PowerShell und SCCLI wird das vorhandene Cmdlet (Open-SmConnection) um ein weiteres Feld namens „AccessToken“ erweitert, um das Bearer-Token zur Authentifizierung des Benutzers zu verwenden.

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

Nachdem das obige Cmdlet ausgeführt wurde, wird für den jeweiligen Benutzer eine Sitzung erstellt, um weitere SnapCenter -Cmdlets auszuführen.

SnapCenter MFA Rest API-Authentifizierung

Verwenden Sie das Bearer-Token im Format *Authorization=Bearer <Zugriffstoken>* im REST-API-Client (wie Postman oder Swagger) und geben Sie den Rollennamen des Benutzers im Header an, um eine erfolgreiche Antwort von SnapCenter zu erhalten.

MFA Rest API-Workflow

Wenn MFA mit AD FS konfiguriert ist, sollten Sie sich mit einem Zugriffstoken (Bearer-Token) authentifizieren, um über eine beliebige Rest-API auf die SnapCenter -Anwendung zuzugreifen.

Über diese Aufgabe

- Sie können jeden REST-Client wie Postman, Swagger UI oder FireCamp verwenden.
- Holen Sie sich ein Zugriffstoken und verwenden Sie es zur Authentifizierung nachfolgender Anfragen (SnapCenter Rest API), um beliebige Vorgänge auszuführen.

Schritte

Zur Authentifizierung über AD FS MFA

1. Konfigurieren Sie den REST-Client so, dass er den AD FS-Endpunkt aufruft, um das Zugriffstoken abzurufen.

Wenn Sie auf die Schaltfläche klicken, um ein Zugriffstoken für eine Anwendung zu erhalten, werden Sie zur AD FS-SSO-Seite weitergeleitet, wo Sie Ihre AD-Anmeldeinformationen angeben und sich mit MFA authentifizieren müssen. 1. Geben Sie auf der AD FS-SSO-Seite Ihren Benutzernamen oder Ihre E-Mail-Adresse in das Textfeld „Benutzername“ ein.

+ Benutzernamen müssen als Benutzer@Domäne oder Domäne\Benutzer formatiert sein.

2. Geben Sie im Textfeld „Kennwort“ Ihr Kennwort ein.
3. Klicken Sie auf **Anmelden**.
4. Wählen Sie im Abschnitt **Anmeldeoptionen** eine Authentifizierungsoption aus und authentifizieren Sie sich (je nach Ihrer Konfiguration).
 - Push: Genehmigen Sie die Push-Benachrichtigung, die an Ihr Telefon gesendet wird.
 - QR-Code: Scannen Sie den QR-Code mit der mobilen AUTH Point-App und geben Sie anschließend den in der App angezeigten Bestätigungscode ein.
 - Einmalkennwort: Geben Sie das Einmalkennwort für Ihr Token ein.
5. Nach erfolgreicher Authentifizierung öffnet sich ein Popup, das den Zugriff, die ID und das Aktualisierungstoken enthält.

Kopieren Sie das Zugriffstoken und verwenden Sie es in der SnapCenter Rest API, um den Vorgang auszuführen.

6. In der Rest-API sollten Sie das Zugriffstoken und den Rollennamen im Header-Abschnitt übergeben.
7. SnapCenter validiert dieses Zugriffstoken von AD FS.

Wenn es sich um ein gültiges Token handelt, dekodiert SnapCenter es und erhält den Benutzernamen.

8. Mithilfe des Benutzernamens und des Rollennamens authentifiziert SnapCenter den Benutzer für eine API-Ausführung.

Wenn die Authentifizierung erfolgreich ist, gibt SnapCenter das Ergebnis zurück, andernfalls wird eine Fehlermeldung angezeigt.

Aktivieren oder deaktivieren Sie die SnapCenter MFA-Funktionalität für Rest API, CLI und GUI

GUI

Schritte

1. Melden Sie sich als SnapCenter -Administrator beim SnapCenter -Server an.
2. Klicken Sie auf **Einstellungen > Globale Einstellungen > MultiFactorAuthentication(MFA)-Einstellungen**
3. Wählen Sie die Schnittstelle (GUI/RST API/CLI) aus, um die MFA-Anmeldung zu aktivieren oder zu deaktivieren.

PowerShell-Schnittstelle

Schritte

1. Führen Sie die PowerShell- oder CLI-Befehle aus, um MFA für GUI, Rest API, PowerShell und SCCLI zu aktivieren.

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

Der Pfadparameter gibt den Speicherort der XML-Datei mit den AD FS MFA-Metadaten an.

Aktiviert MFA für SnapCenter GUI, Rest API, PowerShell und SCCLI, konfiguriert mit dem angegebenen AD FS-Metadatendateipfad.

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe des `Get-SmMultiFactorAuthentication` Cmdlet.

SCCLI-Schnittstelle

Schritte

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

REST-APIs

1. Führen Sie die folgende Post-API aus, um MFA für GUI, Rest-API, PowerShell und SCCLI zu aktivieren.

Parameter	Wert
Angeforderte URL	/api/4.9/settings/multifactorauthentication
HTTP-Methode	Post

Anforderungstext	<pre>{ "IsGuiMFAEnabled": false, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }</pre>
Antworttext	<pre>{ "MFAConfiguration": { "IsGuiMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }</pre>

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe der folgenden API.

Parameter	Wert
Angeforderte URL	/api/4.9/settings/multifactorauthentication
HTTP-Methode	Erhalten
Antworttext	<pre>{ "MFAConfiguration": { "IsGuiMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }</pre>

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.