Multi-Faktor-Authentifizierung (MFA)

SnapCenter software

NetApp
November 06, 2025

Inhalt

Multi-Faktor-Authentifizierung (MFA) . . . 1
- Verwalten der Multi-Faktor-Authentifizierung (MFA) . . . 1
  - Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA). . . . 1
  - Aktualisieren der AD FS MFA-Metadaten . . . 3
  - Aktualisieren Sie die SnapCenter MFA-Metadaten . . . 3
  - Deaktivieren Sie die Multi-Faktor-Authentifizierung (MFA). . . . 4
- Verwalten Sie die Multi-Faktor-Authentifizierung (MFA) mit Rest API, PowerShell und SCCLI . . . 4
  - AD FS als OAuth/OIDC einrichten . . . 4
  - Erstellen einer Anwendungsgruppe mit PowerShell-Befehlen . . . 5
  - Ablaufzeit des Zugriffstokens aktualisieren . . . 7
  - Abrufen des Bearertokens von AD FS . . . 7
- Konfigurieren Sie MFA in SnapCenter Server mit PowerShell, SCCLI und REST-API . . . 8
  - SnapCenter MFA CLI-Authentifizierung . . . 8
  - SnapCenter MFA Rest API-Authentifizierung . . . 8
  - MFA Rest API-Workflow . . . 8
  - Aktivieren oder deaktivieren Sie die SnapCenter MFA-Funktionalität für Rest API, CLI und GUI . . . 9

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 Benutzerauthentifizierung, 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.
    a. Wählen Sie im Dropdown-Menü „Attributspeicher“ **Active Directory** aus.
    b. Wählen Sie **User-Principal-Name** im Dropdown-Menü **LDAP-Attribut** und **UPN** im Dropdown-Menü **Ausgehender Anspruchstyp**.
    c. 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	{ "IsGuiMFAEnabled": false, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }
Antworttext	{ "MFAConfiguration": { "IsGuiMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

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