Multi-Faktor-Authentifizierung (MFA)

SnapCenter Software 4.9

NetApp
September 26, 2025

Inhalt

Multi-Faktor-Authentifizierung (MFA)

Multi-Faktor-Authentifizierung (MFA) managen

Sie können die Multi-Faktor-Authentifizierung (MFA)-Funktion im Active Directory-Verbunddienst (AD FS) und im SnapCenter-Server verwalten.

Multi-Faktor-Authentifizierung (MFA) aktivieren

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

Über diese Aufgabe

- SnapCenter unterstützt SSO-basierte Anmeldungen, wenn andere Applikationen mit demselben AD FS konfiguriert werden. In bestimmten AD FS-Konfigurationen erfordert SnapCenter möglicherweise aus Sicherheitsgründen die Benutzerauthentifizierung in Abhängigkeit von der Persistenz der AD FS-Session.
- Die Informationen zu den Parametern, die mit dem Cmdlet verwendet werden können und deren Beschreibungen können durch Ausführen abgerufen werden `Get-Help command_name`. Alternativ können Sie auch sehen "SnapCenter Software Cmdlet Referenzhandbuch".

Bevor Sie beginnen

- Der Windows Active Directory Federation Service (AD FS) sollte in der jeweiligen Domäne ausgeführt werden.
- Sie sollten über einen AD FS-unterstützten Multi-Faktor-Authentifizierungsservice wie Azure MFA, Cisco Duo usw. verfügen.
- Der SnapCenter- und AD-FS-Server-Zeitstempel sollte unabhängig von der Zeitzone gleich sein.
- Beschaffung und Konfiguration des autorisierten CA-Zertifikats für den SnapCenter-Server.

  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 bei Upgrade, Reparatur oder Disaster Recovery (DR) in einer Standalone- oder Hochverfügbarkeitskonfiguration das selbstsignierte Zertifikat nicht wiederhergestellt wird, wodurch MFA neu konfiguriert werden kann.
  - Stellt IP-FQDN-Auflösungen sicher.

    Informationen zum CA-Zertifikat finden Sie unter "ZertifikatCSR-Datei erstellen".

Schritte

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

Der Parameter Path gibt den Pfad an, in dem die MFA-Metadatendatei im SnapCenter-Server-Host gespeichert werden soll.

6. Kopieren Sie die generierte Datei auf den AD FS-Host, um SnapCenter als Client-Einheit zu konfigurieren.
7. Aktivieren Sie MFA für SnapCenter-Server mithilfe von `Set-SmMultiFactorAuthentication` Cmdlet:
8. (Optional) Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mit `Get-SmMultiFactorAuthentication` Cmdlet:
9. Gehen Sie zur Microsoft Management Console (MMC), und führen Sie die folgenden Schritte aus:
   a. Klicken Sie Auf **Datei** > **Snapin Hinzufügen/Entfernen**.
   b. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
   c. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
   d. Klicken Sie Auf **Konsolenwurzel** > **Zertifikate – Lokaler Computer** > **Persönlich** > **Zertifikate**.
   e. Klicken Sie mit der rechten Maustaste auf das CA-Zertifikat, das an SnapCenter gebunden ist, und wählen Sie dann **Alle Aufgaben** > **Privater Schlüssel verwalten** aus.
   f. Führen Sie auf dem 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 **Locations** auf **OK**.
      iv. Geben Sie im Feld Objektname 'IIS_IUSRS' ein, und klicken Sie auf **Namen überprüfen** und klicken Sie auf **OK**.

      Wenn die Prüfung erfolgreich war, klicken Sie auf **OK**.
10. Öffnen Sie im AD FS-Host den AD FS-Managementassistenten, und führen Sie die folgenden Schritte aus:
    a. Klicken Sie mit der rechten Maustaste auf **vertraut auf Partei** > **Vertrauensbeschuss hinzufügen** > **Start**.
    b. Wählen Sie die zweite Option aus, und 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 eine Zugangskontrollrichtlinie nach Bedarf aus und klicken Sie auf **Weiter**.
    e. Wählen Sie die Einstellungen auf der nächsten Registerkarte standardmäßig aus.
    f. Klicken Sie Auf **Fertig Stellen**.

    SnapCenter wird jetzt als vertrauensanzeige-Partei mit dem angegebenen Anzeigenamen dargestellt.
11. Wählen Sie den Namen aus, und führen Sie die folgenden Schritte aus:
    a. Klicken Sie Auf **Richtlinie Zur Bearbeitung Von Forderungen**.
    b. Klicken Sie auf **Regel hinzufügen** und klicken Sie auf **Weiter**.
    c. Geben Sie einen Namen für die Antragsregel an.
    d. Wählen Sie **Active Directory** als Attributspeicher aus.
    e. Wählen Sie das Attribut als **Benutzer-Principal-Name** und den ausgehenden Antragsart als **Name-ID**

aus.

f. Klicken Sie Auf **Fertig Stellen**.

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 durch, um zu bestätigen, dass die Metadaten erfolgreich importiert wurden.
    a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauensbesteller und wählen Sie **Eigenschaften**.
    b. Stellen Sie sicher, dass die Felder Endpoints, Identifikatoren und Signatur ausgefüllt sind.
14. Schließen Sie alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um die vorhandenen oder aktiven Session-Cookies zu löschen, und melden Sie sich erneut an.

Die SnapCenter MFA-Funktion kann auch über REST-APIs aktiviert werden.

Informationen zur Fehlerbehebung finden Sie unter "Gleichzeitige Anmeldeversuche auf mehreren Registerkarten zeigen MFA-Fehler an".

AD FS MFA-Metadaten aktualisieren

Sie sollten die AD FS MFA-Metadaten in SnapCenter aktualisieren, sobald es Änderungen im AD FS-Server gibt, wie z. B. Upgrade, CA-Zertifikatverlängerung, DR usw.

Schritte

1. Laden Sie die AD FS Federation-Metadatendatei von herunter "https://<host FQDN>/FederationMetadaten/2007-06/FederationMetadata.XML“
2. Kopieren Sie die heruntergeladene Datei auf 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 Session-Cookies zu löschen, und melden Sie sich erneut an.

SnapCenter MFA-Metadaten aktualisieren

Sie sollten die SnapCenter MFA-Metadaten in AD FS immer dann aktualisieren, wenn es Änderungen am ADFS-Server gibt, wie Reparatur, CA-Zertifikatverlängerung, DR usw.

Schritte

1. Öffnen Sie im AD FS-Host den AD FS-Managementassistenten, und führen Sie die folgenden Schritte aus:
    a. Klicken Sie Auf **Treuhand-Party-Trusts**.
    b. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauensgesellschaft, das für

SnapCenter erstellt wurde, und klicken Sie auf **Löschen**.

Der benutzerdefinierte Name des Vertrauensverhältnisses wird angezeigt.

c. Multi-Faktor-Authentifizierung (MFA) aktivieren.

Siehe "Multi-Faktor-Authentifizierung aktivieren".

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

Multi-Faktor-Authentifizierung (MFA) deaktivieren

Schritte

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

Multi-Faktor-Authentifizierung (MFA) mit Rest-API, PowerShell und SCCLI managen

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

Richten Sie AD FS als OAuth/OIDC ein

Konfigurieren Sie AD FS mit dem Windows GUI Wizard

1. Navigieren Sie zu **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Navigieren Sie zu **ADFS** > **Anwendungsgruppen**.
   a. Klicken Sie mit der rechten Maustaste auf **Anwendungsgruppen**.
   b. Wählen Sie **Add Application Group** und geben Sie **Application Name** ein.
   c. Wählen Sie **Server-Anwendung**.
   d. Klicken Sie Auf **Weiter**.
3. Kopieren Sie Die Client-Kennung*.

   Dies ist die Client-ID. .. RückrufURL (SnapCenter-Server-URL) in Umleitung URL hinzufügen. .. Klicken Sie Auf **Weiter**.

4. Wählen Sie **gemeinsam genutzten Schlüssel generieren**.

   Kopieren Sie den geheimen Wert. Das ist das Geheimnis des Kunden. .. Klicken Sie Auf **Weiter**.

5. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.
   a. Klicken Sie auf der Seite **complete** auf **Close**.
6. Klicken Sie mit der rechten Maustaste auf die neu hinzugefügte **Application Group** und wählen Sie

Properties.

7. Wählen Sie aus den Anwendungseigenschaften **Anwendung hinzufügen**.
8. Klicken Sie auf **Anwendung hinzufügen**.

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

9. Geben Sie auf der Seite WebAPI konfigurieren die im vorherigen Schritt erstellte SnapCenter-Server-URL und die Clientkennung in den Abschnitt Kennung ein.
   a. Klicken Sie Auf **Hinzufügen**.
   b. Klicken Sie Auf **Weiter**.
10. Wählen Sie auf der Seite **Select Access Control Policy** die Kontrollrichtlinie entsprechend Ihrer Anforderung aus (z. B. „Permit everyone“ und „Require MFA“) und klicken Sie auf **Next**.
11. Auf der Seite **Configure Application permission** wird openid standardmäßig als Bereich ausgewählt, klicken Sie auf **Weiter**.
12. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.

    Klicken Sie auf der Seite **complete** auf **Close**.

13. Klicken Sie auf der Seite **Beispielanwendungseigenschaften** auf **OK**.
14. JWT-Token, das von einem Autorisierungsserver (AD FS) ausgegeben und von der Ressource verwendet werden soll.

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

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

    Konfigurieren Sie OpenID Connect so, dass ein Benutzername als Schadensfälle angegeben wird.

16. Öffnen Sie das Tool **AD FS Management** im Menü **Tools** oben rechts im Server Manager.
    a. Wählen Sie in der linken Seitenleiste den Ordner **Anwendungsgruppen** aus.
    b. Wählen Sie die Web-API aus und klicken Sie auf **EDIT**.
    c. Wechseln Sie zur Registerkarte „Emissionsumform“
17. Klicken Sie Auf **Regel Hinzufügen**.
    a. Wählen Sie in der Dropdown-Liste „Antragsregel“ die Option **LDAP-Attribute als Schadensfall senden** aus.
    b. Klicken Sie Auf **Weiter**.
18. Geben Sie den Namen **Claim rule** ein.
    a. Wählen Sie **Active Directory** in der Dropdown-Liste Attributspeicher aus.
    b. Wählen Sie **User-Principal-Name** in der Dropdown-Liste **LDAP Attribute** und **UPN** in der Dropdown-Liste O*utgoing Claim Type* aus.
    c. Klicken Sie Auf **Fertig Stellen**.

Erstellen Sie eine Anwendungsgruppe mit PowerShell Befehlen

Sie können die Anwendungsgruppe und die Web-API erstellen und den Umfang und die Ansprüche mit PowerShell Befehlen hinzufügen. Diese Befehle sind im automatisierten Skriptformat verfügbar. Weitere Informationen finden Sie im <link to KB article>.

1. Erstellen Sie die neue Anwendungsgruppe in AD FS mit der folgenden Kombination.

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

   `ClientRoleIdentifier` Name Ihrer Applikationsgruppe

   `redirectURL` Gültige URL für Umleitung nach Autorisierung

2. Erstellen Sie die AD FS Server-Anwendung und generieren Sie den Client-Schlüssel.

   ```
   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 den Client-Schlüssel aus der Ausgabe der folgenden Befehle, da sie nur einmal angezeigt wird.

   ```
   "client_id = $identifier"

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

5. Erteilen Sie der AD FS-Anwendung die allattallatallaims und openid-Berechtigungen.

   ```
   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 Transformer-Regeldatei aus.

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

7. Benennen Sie die Web-API-Anwendung und definieren Sie die zugehörigen Regeln für die Emissionstransformation mithilfe einer externen Datei.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Ablaufdatum des Zugriffstoken aktualisieren

Sie können die Ablaufzeit des Zugriffstoken mit dem PowerShell Befehl aktualisieren.

Über diese Aufgabe

- Ein Zugriffstoken kann nur für eine bestimmte Kombination von Benutzer, Client und Ressource verwendet werden. Zugriffstoken können nicht widerrufen werden und sind bis zu ihrem Ablauf gültig.
- Standardmäßig beträgt die Gültigkeitsdauer eines Zugriffstoken 60 Minuten. Diese minimale Verfallszeit ist ausreichend und skaliert. Sie müssen ausreichend Wert bieten, um fortlaufende geschäftskritische Aufgaben zu vermeiden.

Schritt

Verwenden Sie den folgenden Befehl im AD FS-Server, um die Ablaufzeit des Zugriffstoken für eine Anwendungsgruppe WebAPI zu aktualisieren.

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

Holen Sie sich das Inhabertoken von AD FS

Sie sollten die unten genannten Parameter in jedem REST-Client (wie Postman) ausfüllen und Sie werden aufgefordert, die Benutzeranmeldeinformationen einzugeben. Zusätzlich sollten Sie die zweite-Faktor-Authentifizierung eingeben (etwas, das Sie haben und etwas, das Sie sind), um den Träger-Token zu erhalten.

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

Feld	Wert

Zuteilungsart	Autorisierungscode
Rückruf-URL	Geben Sie die Basis-URL Ihrer Anwendung ein, wenn Sie keine Rückruf-URL haben.
Authentifizs-URL	[adfs-Domain-Name]/adfs/oauth2/Autorisieren
Zugriff auf Token-URL	[adfs-Domain-Name]/adfs/oauth2/Token
Client-ID	Geben Sie die AD FS-Client-ID ein
Kundengeheimnis	Geben Sie den AD FS-Client-Schlüssel ein
Umfang	OpenID
Clientauthentifizierung	Als Basis-AUTH-Kopfzeile senden
Ressource	Fügen Sie auf der Registerkarte **Advance Options** das Ressourcenfeld mit dem gleichen Wert wie die Callback-URL hinzu, das als „aud“-Wert im JWT-Token erscheint.

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

Sie können MFA in SnapCenter-Server mit 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 Trägertoken zur Authentifizierung des Benutzers zu verwenden.

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

Nach Ausführung des oben genannten Cmdlet wird eine Sitzung erstellt, damit der jeweilige Benutzer weitere SnapCenter Cmdlets ausführen kann.

SnapCenter MFA Rest API-Authentifizierung

Verwenden Sie das Trägertoken im Format *Authorization=Bearer <access token>* im REST-API-Client (wie Postman oder swagger) und geben Sie den Benutzer RoleName in der Kopfzeile 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 (Träger) 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 authentifizieren Sie es für nachfolgende Anfragen (SnapCenter Rest API), um einen Vorgang 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 zu erhalten.

   Wenn Sie auf die Schaltfläche klicken, um ein Zugriffstoken für eine Anwendung zu erhalten, werden Sie zur AD FS SSO-Seite weitergeleitet, auf der Sie Ihre AD-Anmeldeinformationen angeben und sich bei 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 Konfiguration).
   - Push: Genehmigen Sie die Push-Benachrichtigung, die an Ihr Telefon gesendet wird.
   - QR-Code: Verwenden Sie die mobile App AUTH Point, um den QR-Code zu scannen, und geben Sie dann den in der App angezeigten Verifizierungscode ein
   - Einmalpasswort: Geben Sie das Einmalpasswort für Ihr Token ein.
5. Nach erfolgreicher Authentifizierung wird ein Popup-Fenster geöffnet, das die Token Zugriff, ID und Aktualisieren enthält.

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

6. In der Rest-API sollten Sie das Zugriffstoken und den Rollennamen in der Kopfzeile übergeben.
7. SnapCenter validiert dieses Zugriffstoken aus AD FS.

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

8. Mit dem Benutzernamen und Rollennamen authentifiziert SnapCenter den Benutzer für eine API-Ausführung.

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

Aktivieren oder Deaktivieren der SnapCenter-MFA-Funktion für Rest-API, CLI und GUI

GUI

Schritte

1. Melden Sie sich beim SnapCenter-Server als SnapCenter-Administrator an.
2. Klicken Sie auf **Einstellungen** > **Globale Einstellungen** > **MultiFactorAuthentication(MFA) Settings**
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 zur Aktivierung von MFA für GUI, Rest API, PowerShell und SCCLI aus.

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

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

   Aktiviert MFA für SnapCenter-GUI, Rest-API, PowerShell und SCCLI, konfiguriert mit angegebenem 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 zur Aktivierung von MFA für GUI, Rest-API, PowerShell und SCCLI aus.

Parameter	Wert
Angeforderte URL	/API/4.9/settings/multifactorauthentifizierung
HTTP-Methode	Post

Text Anfordern	{ „IsGuiMFAEnabled“: Falsch, „IsRestApiMFAEnabled“: Wahr, „IsCliMFAEnabled“: False, „ADFSConfigFilePath“: „C:\\ADFS_metadata\\abc.XML“ }
Antwortkörper	{ „MFAConfiguration“: { „IsGuiMFAEnabled“: Falsch, „ADFSConfigFilePath“: „C:\\ADFS_metadata\\abc.XML“, „SCConfigFilePath“: Null, „IsRestApiMFAEnabled“: Wahr, „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/multifactorauthentifizierung
HTTP-Methode	Verstehen
Antwortkörper	{ „MFAConfiguration“: { „IsGuiMFAEnabled“: Falsch, „ADFSConfigFilePath“: „C:\\ADFS_metadata\\abc.XML“, „SCConfigFilePath“: Null, „IsRestApiMFAEnabled“: Wahr, „IsCliMFAEnabled“: False, „ADFSHostName“: „win-adfs-sc49.winscedom2.com“ } }