Autenticazione a più fattori (MFA)

SnapCenter Software 4.9

NetApp
March 20, 2024

Sommario

Autenticazione a più fattori (MFA)

Gestire l’autenticazione a più fattori (MFA)

È possibile gestire la funzionalità di autenticazione multifattore (MFA) nel server del servizio di federazione Active Directory (ad FS) e nel server SnapCenter.

Attiva autenticazione a più fattori (MFA)

È possibile attivare la funzionalità MFA per il server SnapCenter utilizzando i comandi PowerShell.

A proposito di questa attività

- SnapCenter supporta gli accessi basati su SSO quando altre applicazioni sono configurate nello stesso ad FS. In alcune configurazioni di ad FS, SnapCenter potrebbe richiedere l’autenticazione dell’utente per motivi di sicurezza, a seconda della persistenza della sessione di ad FS.
- Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name`. In alternativa, è possibile vedere anche "Guida di riferimento al cmdlet del software SnapCenter".

Prima di iniziare

- Windows Active Directory Federation Service (ad FS) deve essere attivo e in esecuzione nel rispettivo dominio.
- È necessario disporre di un servizio di autenticazione multifattore supportato da ad FS, ad esempio Azure MFA, Cisco Duo e così via.
- L’indicatore di data e ora del server SnapCenter e ad FS deve essere lo stesso indipendentemente dal fuso orario.
- Procurarsi e configurare il certificato CA autorizzato per il server SnapCenter.

  Il certificato CA è obbligatorio per i seguenti motivi:

  - Garantisce che le comunicazioni ADFS-F5 non si interrangano perché i certificati autofirmati sono univoci a livello di nodo.
  - Garantisce che durante l’upgrade, la riparazione o il disaster recovery (DR) in una configurazione standalone o ad alta disponibilità, il certificato autofirmato non venga ricreato, evitando così la riconfigurazione MFA.
  - Garantisce risoluzioni IP-FQDN.

    Per informazioni sul certificato CA, vedere "Generare il file CSR del certificato CA".

Fasi

1. Connettersi all’host Active Directory Federation Services (ad FS).
2. Scaricare il file di metadati della federazione ad FS da "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copiare il file scaricato sul server SnapCenter per attivare la funzione MFA.
4. Accedere al server SnapCenter come utente amministratore di SnapCenter tramite PowerShell.
5. Utilizzando la sessione PowerShell, generare il file di metadati MFA di SnapCenter utilizzando il cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

Il parametro path specifica il percorso per salvare il file di metadati MFA nell'host del server SnapCenter.

6. Copiare il file generato nell'host ad FS per configurare SnapCenter come entità client.
7. Attivare MFA per il server SnapCenter utilizzando `Set-SmMultiFactorAuthentication` cmdlet.
8. (Facoltativo) controllare lo stato e le impostazioni della configurazione MFA utilizzando `Get-SmMultiFactorAuthentication` cmdlet.
9. Accedere alla console di gestione Microsoft (MMC) ed effettuare le seguenti operazioni:
   a. Fare clic su **file** > **Aggiungi/Rimuovi Snapin**.
   b. Nella finestra Aggiungi o Rimuovi snap-in, selezionare **certificati**, quindi fare clic su **Aggiungi**.
   c. Nella finestra dello snap-in certificati, selezionare l'opzione **account computer**, quindi fare clic su **fine**.
   d. Fare clic su **Directory principale console** > **certificati – computer locale** > **personale** > **certificati**.
   e. Fare clic con il pulsante destro del mouse sul certificato CA associato a SnapCenter, quindi selezionare **tutte le attività** > **Gestisci chiavi private**.
   f. Nella procedura guidata delle autorizzazioni, attenersi alla seguente procedura:
      i. Fare clic su **Aggiungi**.
      ii. Fare clic su **Locations** (posizioni) e selezionare l'host desiderato (in cima alla gerarchia).
      iii. Fare clic su **OK** nella finestra a comparsa **Locations**.
      iv. Nel campo Object name (Nome oggetto), immettere 'IIS_IUSRS', fare clic su **Check Names** (Controlla nomi) e fare clic su **OK**.

      Se il controllo ha esito positivo, fare clic su **OK**.
10. Nell'host ad FS, aprire la procedura guidata di gestione di ad FS ed eseguire le seguenti operazioni:
    a. Fare clic con il pulsante destro del mouse su **Trust di parte affidabile** > **Aggiungi Trust di parte affidabile** > **Start**.
    b. Selezionare la seconda opzione, sfogliare il file di metadati MFA di SnapCenter e fare clic su **Avanti**.
    c. Specificare un nome visualizzato e fare clic su **Avanti**.
    d. Scegliere un criterio di controllo degli accessi come richiesto e fare clic su **Avanti**.
    e. Selezionare le impostazioni predefinite nella scheda successiva.
    f. Fare clic su **fine**.

    SnapCenter si riflette ora come parte di base con il nome visualizzato fornito.
11. Selezionare il nome ed effettuare le seguenti operazioni:
    a. Fare clic su **Edit Claim Issuance Policy** (Modifica policy di emissione richieste
    b. Fare clic su **Add Rule** (Aggiungi regola) e fare clic su **Next** (Avanti).
    c. Specificare un nome per la regola di richiesta di rimborso.
    d. Selezionare **Active Directory** come archivio di attributi.
    e. Selezionare l'attributo **User-Principal-Name** e il tipo di richiesta di rimborso in uscita come **Name-ID**.
    f. Fare clic su **fine**.
12. Eseguire i seguenti comandi PowerShell sul server ADFS.

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

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

13. Attenersi alla seguente procedura per confermare che i metadati sono stati importati correttamente.
    a. Fare clic con il pulsante destro del mouse sul trust della parte che si basa e selezionare **Proprietà**.
    b. Assicurarsi che i campi Endpoint, Identifier e Firma siano compilati.
14. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

La funzionalità MFA di SnapCenter può anche essere attivata utilizzando API REST.

Per informazioni sulla risoluzione dei problemi, fare riferimento a. "I tentativi di accesso simultanei in più schede mostrano un errore MFA".

Aggiornare i metadati di ad FS MFA

È necessario aggiornare i metadati MFA di ad FS in SnapCenter ogni volta che si verifica una modifica nel server di ad FS, ad esempio aggiornamento, rinnovo del certificato CA, DR e così via.

Fasi

1. Scaricare il file di metadati della federazione ad FS da "https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copiare il file scaricato sul server SnapCenter per aggiornare la configurazione MFA.
3. Aggiornare i metadati di ad FS in SnapCenter eseguendo il seguente cmdlet:

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

4. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Aggiornare i metadati MFA di SnapCenter

È necessario aggiornare i metadati MFA di SnapCenter in ad FS ogni volta che si verifica una modifica nel server ADFS, ad esempio riparazione, rinnovo del certificato CA, DR e così via.

Fasi

1. Nell'host ad FS, aprire la procedura guidata di gestione di ad FS ed eseguire le seguenti operazioni:
    a. Fare clic su **Trust di parte**.
    b. Fare clic con il pulsante destro del mouse sul trust della parte di base creato per SnapCenter e fare clic su **Elimina**.

    Viene visualizzato il nome definito dall'utente del trust della parte che si basa.

    c. Attivare l'autenticazione a più fattori (MFA).

    Vedere "Abilitare l'autenticazione a più fattori".

2. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Disattiva autenticazione a più fattori (MFA)

Fasi

1. Disattivare l'MFA e pulire i file di configurazione creati al momento dell'attivazione dell'MFA utilizzando `Set-SmMultiFactorAuthentication` cmdlet.
2. Chiudere tutte le schede del browser e riaprire un browser per eliminare i cookie di sessione esistenti o attivi, quindi eseguire nuovamente l'accesso.

Gestisci l'autenticazione a più fattori (MFA) utilizzando REST API, PowerShell e SCCLI

L'accesso MFA è supportato da browser, REST API, PowerShell e SCCLI. MFA è supportato da un Identity Manager di ad FS. È possibile attivare MFA, disattivare MFA e configurare MFA da GUI, REST API, PowerShell e SCCLI.

Impostare ad FS come OAuth/OIDC

Configurare ad FS utilizzando la GUI di Windows

1. Accedere a **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Accedere a **ADFS** > **gruppi di applicazioni**.
   a. Fare clic con il pulsante destro del mouse su **gruppi di applicazioni**.
   b. Selezionare **Add Application group** (Aggiungi gruppo di applicazioni) e immettere **Application Name** (Nome applicazione).
   c. Selezionare **applicazione server**.
   d. Fare clic su **Avanti**.
3. Copia **identificatore del client**.

   ID client. .. Aggiungere l'URL di richiamata (URL del server SnapCenter) nell'URL di reindirizzamento. .. Fare clic su **Avanti**.

4. Selezionare **generate shared secret**.

   Copiare il valore segreto. Questo è il segreto del cliente. .. Fare clic su **Avanti**.

5. Nella pagina **Riepilogo**, fare clic su **Avanti**.
   a. Nella pagina **complete**, fare clic su **Close** (Chiudi).
6. Fare clic con il pulsante destro del mouse sul nuovo **Application Group** e selezionare **Properties**.
7. Selezionare **Aggiungi applicazione** da Proprietà applicazione.
8. Fare clic su **Aggiungi applicazione**.

   Selezionare API Web e fare clic su **Avanti**.

9. Nella pagina Configura API web, inserire l'URL del server SnapCenter e l'identificativo client creati nel

passaggio precedente nella sezione identificativo.

a. Fare clic su **Aggiungi**.

b. Fare clic su **Avanti**.

10. Nella pagina **Choose Access Control Policy** (Scegli policy di controllo dell'accesso), selezionare la policy di controllo in base ai requisiti (ad esempio, Permit Everyone and Request MFA) e fare clic su **Next** (Avanti).
11. Nella pagina **Configure Application Permission** (Configura autorizzazione applicazione), per impostazione predefinita openid è selezionato come ambito, fare clic su **Next** (Avanti).
12. Nella pagina **Riepilogo**, fare clic su **Avanti**.

    Nella pagina **complete**, fare clic su **Close** (Chiudi).

13. Nella pagina **Proprietà applicazione di esempio**, fare clic su **OK**.
14. Token JWT emesso da un server di autorizzazione (ad FS) e destinato ad essere utilizzato dalla risorsa.

    La richiesta "aud" o di pubblico di questo token deve corrispondere all'identificatore della risorsa o dell'API Web.

15. Modificare l'API Web selezionata e verificare che l'URL di richiamata (URL del server SnapCenter) e l'identificatore del client siano stati aggiunti correttamente.

    Configurare OpenID Connect in modo da fornire un nome utente come rivendicato.

16. Aprire lo strumento **ad FS Management** situato nel menu **Tools** in alto a destra di Server Manager.
    a. Selezionare la cartella **Application Groups** dalla barra laterale sinistra.
    b. Selezionare l'API Web e fare clic su **EDIT**.
    c. Accedere alla scheda Issuance Transform Rules (regole di trasformazione emissione)
17. Fare clic su **Add Rule** (Aggiungi regola).
    a. Selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) nell'elenco a discesa Claim Rule template (
    b. Fare clic su **Avanti**.
18. Inserire il nome **Claim rule**.
    a. Selezionare **Active Directory** nell'elenco a discesa dell'archivio degli attributi.
    b. Selezionare **User-Principal-Name** nel menu a discesa **LDAP Attribute** e **UPN** nel menu a discesa o*utgoing Claim Type*.
    c. Fare clic su **fine**.

Creare un gruppo di applicazioni utilizzando i comandi PowerShell

È possibile creare il gruppo di applicazioni, l'API Web e aggiungere l'ambito e le attestazioni utilizzando i comandi PowerShell. Questi comandi sono disponibili in formato script automatizzato. Per ulteriori informazioni, vedere <link to KB article>.

1. Creare il nuovo gruppo di applicazioni in ad FS utilizzando la seguente comand.

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

`ClientRoleIdentifier` nome del gruppo di applicazioni

`redirectURL` URL valido per il reindirizzamento dopo l'autorizzazione

2. Creare l'applicazione server di ad FS e generare il segreto del client.

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

3. Creare l'applicazione API Web ADFS e configurare il nome del criterio da utilizzare.

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

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

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

4. Ottenere l'ID client e il client secret dall'output dei seguenti comandi perché vengono visualizzati una sola volta.

```
"client_id = $identifier"

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

5. Concedere all'applicazione ad FS le autorizzazioni Allatclaims e 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. Annotare il file di regole di trasformazione.

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

7. Assegnare un nome all'applicazione API Web e definirne le regole di conversione mediante un file esterno.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Aggiornare il tempo di scadenza del token di accesso

È possibile aggiornare il tempo di scadenza del token di accesso utilizzando il comando PowerShell.

A proposito di questa attività

- Un token di accesso può essere utilizzato solo per una combinazione specifica di utente, client e risorsa. I token di accesso non possono essere revocati e sono validi fino alla scadenza.
- Per impostazione predefinita, la scadenza di un token di accesso è di 60 minuti. Questo tempo di scadenza minimo è sufficiente e scalabile. Devi fornire un valore sufficiente per evitare qualsiasi lavoro business-critical in corso.

Passo

Per aggiornare il tempo di scadenza del token di accesso per un gruppo di applicazioni WebAPI, utilizzare il seguente comando nel server ad FS.

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

Ottenere il token del bearer da ad FS

Inserire i parametri indicati di seguito in qualsiasi client REST (come Postman) e richiedere di inserire le credenziali dell'utente. Inoltre, per ottenere il token del bearer, è necessario immettere l'autenticazione del secondo fattore (qualcosa che si possiede e qualcosa che si è).

+ La validità del token bearer è configurabile dal server ad FS per ogni applicazione e il periodo di validità predefinito è di 60 minuti.

Campo	Valore
Tipo di concessione	Codice di autorizzazione
URL di richiamata	Se non si dispone di un URL di richiamata, immettere l'URL di base dell'applicazione.
URL di autenticazione	[adfs-domain-name]/adfs/oauth2/authorize
URL token di accesso	[adfs-domain-name]/adfs/oauth2/token
ID client	Inserire l'ID del client ad FS

Segreto del client	Inserire il segreto del client ad FS
Scopo	OpenID
Autenticazione del client	Invia come intestazione AUTH di base
Risorsa	Nella scheda **Opzioni avanzate**, aggiungere il campo risorsa con lo stesso valore dell'URL di richiamata, che viene fornito come valore "aud" nel token JWT.

Configurare MFA nel server SnapCenter utilizzando PowerShell, SCCLI e REST API

È possibile configurare MFA nel server SnapCenter utilizzando PowerShell, SCCLI e REST API.

Autenticazione SnapCenter MFA CLI

In PowerShell e SCCLI, il cmdlet esistente (Open-SmConnection) viene esteso con un altro campo chiamato "AccessToken" per utilizzare il token bearer per autenticare l'utente.

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

Una volta eseguito il cmdlet sopra indicato, viene creata una sessione per consentire al rispettivo utente di eseguire ulteriori cmdlet SnapCenter.

Autenticazione API REST MFA SnapCenter

Utilizzare il token bearer nel formato *Authorization=bearer <access token>* nel client API REST (come Postman o swagger) e citare il nome del ruolo dell'utente nell'intestazione per ottenere una risposta corretta da SnapCenter.

Flusso di lavoro API REST MFA

Quando MFA è configurato con ad FS, è necessario eseguire l'autenticazione utilizzando un token di accesso (bearer) per accedere all'applicazione SnapCenter da qualsiasi API REST.

A proposito di questa attività

- Puoi utilizzare qualsiasi client REST come Postman, Swagger UI o FireCamp.
- Ottenere un token di accesso e utilizzarlo per autenticare le richieste successive (API REST SnapCenter) per eseguire qualsiasi operazione.

Fasi

Per l'autenticazione tramite ad FS MFA

1. Configurare il client REST per chiamare l'endpoint ad FS per ottenere il token di accesso.

Quando si preme il pulsante per ottenere un token di accesso per un'applicazione, si viene reindirizzati alla pagina SSO di ad FS, dove è necessario fornire le credenziali ad e autenticare con MFA. 1. Nella pagina ad FS SSO, digitare il nome utente o l'indirizzo e-mail nella casella di testo Nome utente.

+ I nomi utente devono essere formattati come utente@dominio o dominio utente.

2. Digitare la password nella casella di testo Password.
3. Fare clic su **Log in** (Accedi).
4. Nella sezione **Opzioni di accesso**, selezionare un'opzione di autenticazione e autenticare (a seconda della configurazione).
   - Push: Consente di approvare la notifica push inviata al telefono.
   - Codice QR: Utilizza l'app mobile AUTH Point per eseguire la scansione del codice QR, quindi digita il codice di verifica visualizzato nell'app
   - Password monouso: Digitare la password monouso per il token.
5. Una volta completata l'autenticazione, viene visualizzata una finestra a comparsa contenente Access, ID e Refresh Token.

   Copiare il token di accesso e utilizzarlo nell'API REST di SnapCenter per eseguire l'operazione.

6. Nell'API REST, passare il token di accesso e il nome del ruolo nella sezione dell'intestazione.
7. SnapCenter convalida questo token di accesso da ad FS.

   Se si tratta di un token valido, SnapCenter lo decodifica e ottiene il nome utente.

8. Utilizzando il nome utente e il nome ruolo, SnapCenter autentica l'utente per un'esecuzione API.

   Se l'autenticazione ha esito positivo, SnapCenter restituisce il risultato, altrimenti viene visualizzato un messaggio di errore.

Attivare o disattivare la funzionalità MFA di SnapCenter per API REST, CLI e GUI

GUI

Fasi

1. Accedere al server SnapCenter come amministratore SnapCenter.
2. Fare clic su **Impostazioni** > **Impostazioni globali** > **Impostazioni MultiFactorAuthentication(MFA)**
3. Selezionare l'interfaccia (GUI/RST API/CLI) per attivare o disattivare l'accesso MFA.

Interfaccia PowerShell

Fasi

1. Eseguire i comandi PowerShell o CLI per abilitare MFA per GUI, REST API, PowerShell e SCCLI.

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

   Il parametro path specifica la posizione del file xml di metadati di ad FS MFA.

Abilita MFA per GUI SnapCenter, API REST, PowerShell e SCCLI configurati con il percorso file di metadati ad FS specificato.

2. Controllare lo stato e le impostazioni della configurazione MFA utilizzando `Get-SmMultiFactorAuthentication` cmdlet.

INTERFACCIA SCCLI

Fasi

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

API REST

1. Eseguire la seguente API post per abilitare MFA per GUI, REST API, PowerShell e SCCLI.

Parametro	Valore
URL richiesto	/api/4.9/settings/autenticazione multifattoriale
Metodo HTTP	Post
Corpo della richiesta	{ "IsGuiMFAEnabled": Falso, "IsRestApiMFAEnabled": Vero, "IsCliMFAEnabled": Falso, "ADFSConfigFilePath": "C: ADFS_metadata.abc.xml" }
Corpo di risposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": Falso, "ADFSConfigFilePath": "C: ADFS_metadata abc.xml", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": Vero, "IsCliMFAEnabled": Falso, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }

2. Controllare lo stato e le impostazioni della configurazione MFA utilizzando la seguente API.

Parametro	Valore
URL richiesto	/api/4.9/settings/autenticazione multifattoriale
Metodo HTTP	Ottieni

Corpo di risposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": Falso, "ADFSConfigFilePath": "C: ADFS_metadata abc.xml", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": Vero, "IsCliMFAEnabled": Falso, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } }