Prepararsi all'installazione di SnapCenter Server

SnapCenter software

NetApp
November 06, 2025

Sommario

Prepararsi all’installazione di SnapCenter Server

Requisiti per installare SnapCenter Server

Prima di installare SnapCenter Server su un host Windows o Linux, è necessario verificare e assicurarsi che tutti i requisiti per l’ambiente siano soddisfatti.

Requisiti di dominio e gruppo di lavoro per l’host Windows

SnapCenter Server può essere installato su un host Windows appartenente a un dominio o a un gruppo di lavoro.

L’utente con privilegi di amministratore è autorizzato a installare il server SnapCenter .

- Dominio Active Directory: è necessario utilizzare un utente di dominio con diritti di amministratore locale. L’utente del dominio deve essere membro del gruppo Administrator locale sull’host Windows.
- Gruppi di lavoro: è necessario utilizzare un account locale con diritti di amministratore locale.

Sebbene siano supportati trust di dominio, foreste multidominio e trust tra domini, i domini tra foreste non sono supportati. Per ulteriori informazioni, consultare la documentazione Microsoft sui domini e i trust di Active Directory.

Dopo aver installato SnapCenter Server, non modificare il dominio in cui si trova l’host SnapCenter . Se si rimuove l’host di SnapCenter Server dal dominio in cui si trovava al momento dell’installazione di SnapCenter Server e poi si tenta di disinstallare SnapCenter Server, l’operazione di disinstallazione non riesce.

Requisiti di spazio e dimensioni

Dovresti conoscere i requisiti di spazio e dimensioni.

Articolo	Requisiti host Windows	Requisiti host Linux
Sistemi operativi	Microsoft Windows Sono supportate solo le versioni in inglese, tedesco, giapponese e cinese semplificato dei sistemi operativi. Per le informazioni più recenti sulle versioni supportate, vederehttps://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["Strumento matrice di interoperabilità NetApp"^] .	• Red Hat Enterprise Linux (RHEL) 8 e 9 • SUSE Linux Enterprise Server (SLES) 15 Per le informazioni più recenti sulle versioni supportate, vederehttps://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["Strumento matrice di interoperabilità NetApp"^] .
Numero minimo di CPU	4 core	4 core

Articolo	Requisiti host Windows	Requisiti host Linux
RAM minima	8 GB Il buffer pool di MySQL Server utilizza il 20 percento della RAM totale.	8 GB
Spazio minimo sul disco rigido per il software e i registri di SnapCenter Server	7 GB Se il repository SnapCenter si trova nella stessa unità in cui è installato SnapCenter Server, si consiglia di disporre di 15 GB.	15 GB
Spazio minimo su disco rigido per il repository SnapCenter	8 GB NOTA: se SnapCenter Server si trova nella stessa unità in cui è installato il repository SnapCenter , si consiglia di disporre di 15 GB.	Non applicabile
Pacchetti software richiesti	• Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) • PowerShell 7.4.2 o versione successiva Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet" .	• .NET Framework 8.0.12 (e tutte le successive patch 8.0.x) • PowerShell 7.4.2 o versione successiva • Nginx è un server web che può essere utilizzato come proxy inverso • Pam-devel PAM (Pluggable Authentication Modules) è uno strumento di sicurezza del sistema che consente agli amministratori di sistema di impostare criteri di autenticazione senza dover ricompilare i programmi che eseguono l'autenticazione.

ASP.NET Core necessita di IIS_IUSRS per accedere al file system temporaneo in SnapCenter Server su Windows.

Requisiti dell'host SAN

SnapCenter non include utilità host o un DSM. Se l'host SnapCenter fa parte di un ambiente SAN (FC/iSCSI), potrebbe essere necessario installare e configurare software aggiuntivo sull'host SnapCenter Server.

- Utilità host: le utilità host supportano FC e iSCSI e consentono di utilizzare MPIO sui server Windows. "Saperne di più" .
- Microsoft DSM per Windows MPIO: questo software funziona con i driver Windows MPIO per gestire più percorsi tra NetApp e computer host Windows. Per le configurazioni ad alta disponibilità è necessario un DSM.

Se utilizzavi ONTAP DSM, dovresti migrare a Microsoft DSM. Per ulteriori informazioni, vedere "Come migrare da ONTAP DSM a Microsoft DSM" .

Requisiti del browser

Il SnapCenter software supporta Chrome 125 e versioni successive e Microsoft Edge 110.0.1587.17 e versioni successive.

Requisiti portuali

Il SnapCenter software richiede porte diverse per la comunicazione tra i diversi componenti.

- Le applicazioni non possono condividere una porta.
- Per le porte personalizzabili, è possibile selezionare una porta personalizzata durante l'installazione se non si desidera utilizzare la porta predefinita.
- Per le porte fisse, dovresti accettare il numero di porta predefinito.
- Firewall
  - Firewall, proxy o altri dispositivi di rete non devono interferire con le connessioni.
  - Se si specifica una porta personalizzata durante l'installazione SnapCenter, è necessario aggiungere una regola firewall sull'host del plug-in per quella porta per SnapCenter Plug-in Loader.

Nella tabella seguente sono elencate le diverse porte e i relativi valori predefiniti.

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Porta web SnapCenter	8146	HTTPS	Bidirezionale	Questa porta viene utilizzata per la comunicazione tra il client SnapCenter (l'utente SnapCenter) e il server SnapCenter e viene utilizzata anche per la comunicazione dagli host del plug-in al server SnapCenter . È possibile personalizzare il numero di porta.
Porta di comunicazione SnapCenter SMCore	8145	HTTPS	Bidirezionale	Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e gli host in cui sono installati i plug-in SnapCenter . È possibile personalizzare il numero di porta.
Porta del servizio di pianificazione	8154	HTTPS		Questa porta viene utilizzata per orchestrare in modo centralizzato i flussi di lavoro dello scheduler di SnapCenter per tutti i plug-in gestiti all'interno dell'host del server SnapCenter . È possibile personalizzare il numero di porta.

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Porta RabbitMQ	5672	TCP		Questa è la porta predefinita su cui RabbitMQ è in ascolto e viene utilizzata per la comunicazione del modello publisher-subscriber tra il servizio Scheduler e SnapCenter.
Porta MySQL	3306	HTTPS		La porta viene utilizzata per comunicare con il database del repository SnapCenter . È possibile creare connessioni protette dal server SnapCenter al server MySQL."Saperne di più"
Host plug-in di Windows	135, 445	TCP		Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e l'host su cui viene installato il plug-in. Dovrebbe essere aperto anche un intervallo di porte dinamiche aggiuntivo specificato da Microsoft.
Host plug-in Linux o AIX	22	SSH	Unidirezionale	Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e l'host, avviata dal server all'host client.

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Pacchetto di plug-in SnapCenter per Windows, Linux o AIX	8145	HTTPS	Bidirezionale	Questa porta viene utilizzata per la comunicazione tra SMCore e gli host in cui è installato il pacchetto plug-in. Personalizzabile. È possibile personalizzare il numero di porta.
Plug-in SnapCenter per Oracle Database	27216			La porta JDBC predefinita viene utilizzata dal plug-in per Oracle per la connessione al database Oracle.
Plug-in SnapCenter per database Exchange	909			La porta NET.TCP predefinita viene utilizzata dal plug-in per Windows per la connessione ai callback di Exchange VSS.
Plug-in supportati da NetApp per SnapCenter	9090	HTTPS		Si tratta di una porta interna utilizzata solo sull'host del plug-in; non è richiesta alcuna eccezione del firewall. La comunicazione tra SnapCenter Server e i plug-in avviene tramite la porta 8145.

Nome della porta	Numeri di porta	Protocollo	Direzione	Descrizione
Cluster ONTAP o porta di comunicazione SVM	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	Bidirezionale	La porta viene utilizzata dal SAL (Storage Abstraction Layer) per la comunicazione tra l'host che esegue SnapCenter Server e SVM. Attualmente la porta è utilizzata anche dal SAL sugli host del plug-in SnapCenter per Windows per la comunicazione tra l'host del plug-in SnapCenter e SVM.
Plug-in SnapCenter per database SAP HANA	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	Bidirezionale	Per un contenitore di database multi-tenant (MDC) con un solo tenant, il numero di porta termina con 13; per un contenitore non MDC, il numero di porta termina con 15. È possibile personalizzare il numero di porta.
Plug-in SnapCenter per PostgreSQL	5432			Questa porta è la porta PostgreSQL predefinita utilizzata per la comunicazione tra il plug-in per PostgreSQL e il cluster PostgreSQL. È possibile personalizzare il numero di porta.

Registrati per accedere al SnapCenter software

Se non hai familiarità con Amazon FSx for NetApp ONTAP o Azure NetApp Files e non hai un account NetApp esistente, devi registrarti per accedere al SnapCenter software.

Prima di iniziare

- Dovresti avere accesso all'ID e-mail aziendale.
- Se si utilizza Azure NetApp Files, è necessario disporre dell'ID di sottoscrizione di Azure.
- Se si utilizza Amazon FSx for NetApp ONTAP, è necessario disporre dell'ID del file system FSx per ONTAP .

Informazioni su questo compito

La registrazione è soggetta a convalida delle informazioni e potrebbe volerci fino a un giorno per confermare e aggiornare il nuovo account NetApp Support Site (NSS) dall'accesso **ospite** all'accesso **completo**.

Passi

1. Clic https://mysupport.netapp.com/site/user/registration per la registrazione.
2. Inserisci il tuo ID e-mail aziendale, completa il captcha, accetta l'informativa sulla privacy di NetApp e fai clic su **Invia**.
3. Autentica la registrazione inserendo l'OTP inviato al tuo indirizzo e-mail e clicca su **Continua**.
4. Nella pagina di completamento della registrazione, inserisci i seguenti dati per completare la registrazione.
   a. Seleziona **Cliente NetApp /Utente finale**.
   b. Nel campo NUMERO DI SERIE, immettere l'ID della sottoscrizione di Azure se si utilizza Azure NetApp Files oppure l'ID del file system se si utilizza Amazon FSx for NetApp ONTAP.

Puoi sollevare un biglietto a https://mysupport.netapp.com/site/help se riscontri problemi durante la registrazione o per conoscerne lo stato.

Autenticazione a più fattori (MFA)

Gestire l'autenticazione a più fattori (MFA)

È possibile gestire la funzionalità di autenticazione a più fattori (MFA) nel server Active Directory Federation Service (AD FS) e nel server SnapCenter .

Abilita l'autenticazione a più fattori (MFA)

È possibile abilitare la funzionalità MFA per SnapCenter Server utilizzando i comandi di PowerShell.

Informazioni su questo compito

- 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 AD FS.
- Le informazioni riguardanti i parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name` . In alternativa, puoi anche vedere "Guida di riferimento ai cmdlet del software SnapCenter" .

Prima di iniziare

- Windows Active Directory Federation Service (AD FS) deve essere attivo e funzionante nel rispettivo dominio.
- Dovresti disporre di un servizio di autenticazione a più fattori supportato da AD FS, come Azure MFA, Cisco Duo e così via.

- Il timestamp SnapCenter e del server AD FS deve essere lo stesso, indipendentemente dal fuso orario.
- Ottenere e configurare il certificato CA autorizzato per SnapCenter Server.

  Il certificato CA è obbligatorio per i seguenti motivi:

  - Garantisce che le comunicazioni ADFS-F5 non vengano interrotte perché i certificati autofirmati sono univoci a livello di nodo.
  - Garantisce che durante l'aggiornamento, la riparazione o il ripristino di emergenza (DR) in una configurazione autonoma o ad alta disponibilità, il certificato autofirmato non venga ricreato, evitando così la riconfigurazione MFA.
  - Garantisce le risoluzioni IP-FQDN.

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

Passi

1. Connettersi all'host Active Directory Federation Services (AD FS).
2. Scarica il file dei metadati della federazione AD FS da"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copiare il file scaricato su SnapCenter Server per abilitare la funzionalità MFA.
4. Accedere a SnapCenter Server come utente amministratore SnapCenter tramite PowerShell.
5. Utilizzando la sessione di PowerShell, generare il file di metadati SnapCenter MFA utilizzando il cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   Il parametro path specifica il percorso in cui 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. Abilita MFA per SnapCenter Server 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 eseguire i seguenti passaggi:
   a. Fare clic su **File** > **Aggiungi/Rimuovi snap-in**.
   b. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
   c. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
   d. Fare clic su **Console Root** > **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 per le autorizzazioni, eseguire i seguenti passaggi:
      i. Fare clic su **Aggiungi**.
      ii. Fare clic su **Posizioni** e selezionare l'host interessato (in cima alla gerarchia).
      iii. Fare clic su **OK** nella finestra pop-up **Posizioni**.
      iv. Nel campo del nome dell'oggetto, immettere 'IIS_IUSRS' e fare clic su **Controlla nomi**, quindi 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 AD FS ed eseguire i seguenti passaggi:
    a. Fare clic con il pulsante destro del mouse su **Trust della parte affidabile** > **Aggiungi trust della parte affidabile** > **Avvia**.
    b. Selezionare la seconda opzione, sfogliare il file dei metadati SnapCenter MFA e fare clic su **Avanti**.
    c. Specificare un nome visualizzato e fare clic su **Avanti**.
    d. Selezionare una policy di controllo degli accessi in base alle proprie esigenze e fare clic su **Avanti**.
    e. Selezionare le impostazioni predefinite nella scheda successiva.
    f. Fare clic su **Fine**.

    SnapCenter viene ora visualizzato come relying party con il nome visualizzato fornito.

11. Selezionare il nome ed eseguire i seguenti passaggi:
    a. Fare clic su **Modifica politica di emissione reclami**.
    b. Fare clic su **Aggiungi regola** e quindi su **Avanti**.
    c. Specificare un nome per la regola di rivendicazione.
    d. Selezionare **Active Directory** come archivio attributi.
    e. Selezionare l'attributo come **User-Principal-Name** e il tipo di claim 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. Per confermare che i metadati siano stati importati correttamente, procedere come segue.
    a. Fare clic con il pulsante destro del mouse sul trust della parte affidabile e selezionare **Proprietà**.
    b. Assicurarsi che i campi Endpoint, Identificatori e Firma siano compilati.
14. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

La funzionalità SnapCenter MFA può essere abilitata anche tramite API REST.

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

Aggiorna i metadati AD FS MFA

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

Passi

1. Scarica il file dei metadati della federazione AD FS da"https://<host Nome di dominio completo>/FederationMetadata/2007-06/FederationMetadata.xml"

2. Copiare il file scaricato su SnapCenter Server per aggiornare la configurazione MFA.
3. Aggiornare i metadati 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 il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

Aggiorna i metadati SnapCenter MFA

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

Passi

1. Nell'host AD FS, aprire la procedura guidata di gestione AD FS ed eseguire i seguenti passaggi:
   a. Selezionare **Trust della parte affidante**.
   b. Fare clic con il pulsante destro del mouse sul trust della relying party creato per SnapCenter e selezionare **Elimina**.

      Verrà visualizzato il nome definito dall'utente del trust della parte affidabile.

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

      Vedere "Abilita l'autenticazione a più fattori" .
2. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

Disabilitare l'autenticazione a più fattori (MFA)

Passi

1. Disabilitare MFA e pulire i file di configurazione creati quando MFA è stato abilitato utilizzando `Set-SmMultiFactorAuthentication` cmdlet.
2. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

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

L'accesso MFA è supportato da browser, REST API, PowerShell e SCCLI. L'MFA è supportato tramite un gestore di identità AD FS. È possibile abilitare MFA, disabilitare MFA e configurare MFA da GUI, REST API, PowerShell e SCCLI.

Imposta AD FS come OAuth/OIDC

Configurare AD FS utilizzando la procedura guidata GUI di Windows

1. Passare a **Dashboard di Server Manager** > **Strumenti** > **Gestione ADFS**.
2. Passare a **ADFS** > **Gruppi di applicazioni**.
   a. Fare clic con il tasto destro del mouse su **Gruppi di applicazioni**.

b. Selezionare **Aggiungi gruppo di applicazioni** e immettere **Nome applicazione**.

c. Selezionare **Applicazione server**.

d. Fare clic su **Avanti**.

3. Copia **Identificatore cliente**.

   Questo è l'ID cliente. .. Aggiungere l'URL di callback (URL del server SnapCenter) nell'URL di reindirizzamento. .. Fare clic su **Avanti**.

4. Seleziona **Genera segreto condiviso**.

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

5. Nella pagina **Riepilogo**, fare clic su **Avanti**.

   a. Nella pagina **Completa**, fare clic su **Chiudi**.

6. Fare clic con il pulsante destro del mouse sul **Gruppo applicazioni** appena aggiunto e selezionare **Proprietà**.

7. Selezionare **Aggiungi applicazione** da Proprietà app.

8. Fare clic su **Aggiungi applicazione**.

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

9. Nella pagina Configura API Web, immettere l'URL del server SnapCenter e l'identificatore client creati nel passaggio precedente nella sezione Identificatore.

   a. Fare clic su **Aggiungi**.

   b. Fare clic su **Avanti**.

10. Nella pagina **Scegli criterio di controllo degli accessi**, seleziona il criterio di controllo in base alle tue esigenze (ad esempio, Consenti a tutti e richiedi MFA) e fai clic su **Avanti**.

11. Nella pagina **Configura autorizzazione applicazione**, per impostazione predefinita openid è selezionato come ambito, fare clic su **Avanti**.

12. Nella pagina **Riepilogo**, fare clic su **Avanti**.

    Nella pagina **Completa**, fare clic su **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 a essere utilizzato dalla risorsa.

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

15. Modifica la WebAPI selezionata e verifica che l'URL di callback (URL del server SnapCenter) e l'identificatore client siano stati aggiunti correttamente.

    Configurare OpenID Connect per fornire un nome utente come claim.

16. Aprire lo strumento **Gestione AD FS** che si trova nel menu **Strumenti** in alto a destra di Server Manager.

    a. Selezionare la cartella **Gruppi di applicazioni** dalla barra laterale sinistra.

    b. Selezionare l'API Web e fare clic su **MODIFICA**.

c. Vai alla scheda Regole di trasformazione dell'emissione

17. Fare clic su **Aggiungi regola**.
    a. Selezionare **Invia attributi LDAP come claim** nel menu a discesa Modello regola claim.
    b. Fare clic su **Avanti**.
18. Inserisci il nome della **Regola di rivendicazione**.
    a. Selezionare **Active Directory** nel menu a discesa Archivio 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 di PowerShell

È possibile creare il gruppo di applicazioni, l'API Web e aggiungere l'ambito e le attestazioni utilizzando i comandi di PowerShell. Questi comandi sono disponibili in formato script automatizzato. Per maggiori informazioni vedere <link all'articolo della Knowledge Base>.

1. Creare il nuovo gruppo di applicazioni in AD FS utilizzando il seguente comando.

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

   `ClientRoleIdentifier`nome del tuo gruppo di applicazioni

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

2. Creare l'applicazione server AD FS e generare il segreto client.

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

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

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

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

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

4. Ottieni l'ID client e il segreto client dall'output dei seguenti comandi perché vengono mostrati solo una 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. Scrivere il file delle regole di trasformazione.

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

7. Assegna un nome all'applicazione Web API e definisci le sue regole di trasformazione del rilascio utilizzando un file esterno.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Aggiorna il tempo di scadenza del token di accesso

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

Informazioni su questo compito

- 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 loro scadenza.
- Per impostazione predefinita, il tempo di scadenza di un token di accesso è di 60 minuti. Questo tempo di scadenza minimo è sufficiente e proporzionato. È necessario fornire un valore sufficiente per evitare lavori critici per l'azienda in corso.

Fare un passo

Per aggiornare la 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>"`

Ottieni il token portatore da AD FS

Dovresti compilare i parametri menzionati di seguito in qualsiasi client REST (come Postman) e ti verrà chiesto di inserire le credenziali utente. Inoltre, dovresti inserire l'autenticazione a due fattori (qualcosa che hai e qualcosa che sei) per ottenere il token portatore.

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

Campo	Valore
Tipo di sovvenzione	Codice di autorizzazione
URL di richiamata	Se non si dispone di un URL di callback, immettere l'URL di base dell'applicazione.
URL di autorizzazione	[nome-dominio-adfs]/adfs/oauth2/authorize
URL del token di accesso	[nome-dominio-adfs]/adfs/oauth2/token
ID cliente	Inserisci l'ID client AD FS
Segreto del cliente	Inserisci il segreto del client AD FS
Ambito	OpenID
Autenticazione del client	Invia come intestazione AUTH di base
Risorsa	Nella scheda **Opzioni avanzate**, aggiungi il campo Risorsa con lo stesso valore dell'URL di callback, che viene fornito come valore "aud" nel token JWT.

Configurare MFA in SnapCenter Server utilizzando PowerShell, SCCLI e REST API

È possibile configurare MFA in SnapCenter Server utilizzando PowerShell, SCCLI e REST API.

Autenticazione SnapCenter MFA CLI

In PowerShell e SCCLI, il cmdlet esistente (Open-SmConnection) è esteso con un ulteriore campo denominato "AccessToken" per utilizzare il token di connessione per autenticare l'utente.

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

Dopo l'esecuzione del cmdlet sopra indicato, viene creata una sessione per consentire all'utente interessato di eseguire ulteriori cmdlet SnapCenter .

Autenticazione API REST MFA SnapCenter

Utilizzare il token del portatore nel formato *Authorization=Bearer <token di accesso>* nel client REST API (come Postman o Swagger) e menzionare l'utente RoleName nell'intestazione per ottenere una risposta positiva da SnapCenter.

Flusso di lavoro dell'API REST MFA

Quando MFA è configurato con AD FS, è necessario autenticarsi utilizzando un token di accesso (bearer) per accedere all'applicazione SnapCenter tramite qualsiasi API REST.

Informazioni su questo compito

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

Passi

Per autenticarsi tramite AD FS MFA

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

   Quando fai clic sul pulsante per ottenere un token di accesso per un'applicazione, verrai reindirizzato alla pagina AD FS SSO, dove dovrai fornire le tue credenziali AD ed eseguire l'autenticazione con MFA. 1. Nella pagina AD FS SSO, digita il tuo nome utente o indirizzo email nella casella di testo Nome utente.

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

2. Nella casella di testo Password, digita la tua password.
3. Fare clic su **Accedi**.
4. Dalla sezione **Opzioni di accesso**, seleziona un'opzione di autenticazione ed esegui l'autenticazione (a seconda della configurazione).
   - Push: approva la notifica push inviata al tuo telefono.
   - Codice QR: usa l'app mobile AUTH Point per scansionare il codice QR, quindi digita il codice di verifica mostrato nell'app
   - Password monouso: digita la password monouso per il tuo token.
5. Dopo l'autenticazione avvenuta con successo, si aprirà una finestra popup contenente il token di accesso, l'ID e il token di aggiornamento.

   Copia il token di accesso e utilizzalo nell'API Rest SnapCenter per eseguire l'operazione.

6. Nell'API REST, dovresti 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 del ruolo, SnapCenter autentica l'utente per l'esecuzione dell'API.

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

Abilita o disabilita la funzionalità SnapCenter MFA per REST API, CLI e GUI

Interfaccia grafica

Passi

1. Accedi al server SnapCenter come amministratore SnapCenter .
2. Fare clic su **Impostazioni** > **Impostazioni globali** > **Impostazioni di autenticazione a più fattori (MFA)**
3. Selezionare l'interfaccia (GUI/RST API/CLI) per abilitare o disabilitare l'accesso MFA.

Interfaccia PowerShell

Passi

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 dei metadati AD FS MFA.

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

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

Interfaccia SCCLI

Passi

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	Inviare
Corpo della richiesta	{ "IsGuiMFAEnabled": false, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" }

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