Preparazione per l'installazione del server SnapCenter

SnapCenter Software 6.0

NetApp
January 31, 2025

Sommario

Preparazione per l'installazione del server SnapCenter

Requisiti di dominio e gruppo di lavoro

Il server SnapCenter può essere installato su sistemi che si trovano in un dominio o in un gruppo di lavoro. L'utente utilizzato per l'installazione deve disporre dei privilegi di amministratore sul computer in caso di gruppo di lavoro e dominio.

Per installare il server SnapCenter e i plug-in SnapCenter su host Windows, è necessario utilizzare uno dei seguenti elementi:

- **Dominio Active Directory**

  È necessario utilizzare un utente di dominio con diritti di amministratore locale. L'utente di 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 di domini multipli e trust tra domini, i domini tra foreste non sono supportati. La documentazione Microsoft sui domini e trust di Active Directory contiene ulteriori informazioni.

> Dopo aver installato il server SnapCenter, non modificare il dominio in cui si trova l'host SnapCenter. Se si rimuove l'host del server SnapCenter dal dominio in cui si trovava quando è stato installato il server SnapCenter e si tenta di disinstallare il server SnapCenter, l'operazione di disinstallazione non riesce.

Requisiti di spazio e dimensionamento

Prima di installare il server SnapCenter, è necessario conoscere i requisiti di spazio e dimensionamento. È inoltre necessario applicare gli aggiornamenti di sicurezza e di sistema disponibili.

Elemento	Requisiti dell'host Windows	Requisiti degli host Linux
Sistemi operativi	Microsoft Windows Sono supportate solo le versioni in inglese, tedesco, giapponese e cinese semplificato dei sistemi operativi. Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".	• Red Hat Enterprise Linux (RHEL) 8 e 9 • SUSE Linux Enterprise Server (SLES) 15 Per informazioni aggiornate sulle versioni supportate, vedere "Tool di matrice di interoperabilità NetApp".

Elemento	Requisiti dell'host Windows	Requisiti degli host Linux
Numero minimo di CPU	4 core	4 core
RAM minima	8 GB Il pool di buffer di MySQL Server utilizza il 20% della RAM totale.	8 GB
Spazio minimo su disco rigido per il software e i registri del server SnapCenter	7 GB Se il repository SnapCenter si trova nello stesso disco in cui è installato il server SnapCenter, si consiglia di utilizzare 15 GB.	15 GB
Spazio minimo su disco rigido per il repository SnapCenter	8 GB NOTA: Se il server SnapCenter si trova nello stesso disco in cui è installato il repository SnapCenter, si consiglia di utilizzare 15 GB.	Non applicabile

Elemento	Requisiti dell'host Windows	Requisiti degli host Linux
Pacchetti software richiesti	• Microsoft .NET Framework 4.7.2 o versione successiva • ASP.NET Core Hosting Bundle a partire dalla versione 8.0.5 e comprendente tutte le patch .NET 8 successive • PowerShell 7.4.2 o versione successiva Per . Per informazioni specifiche sulla risoluzione dei problemi, vedere "L'aggiornamento o l'installazione di SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet".	• ASP.NET Core Runtime che inizia con la versione 8.0.5 e include tutte le patch .NET 8 successive • PowerShell 7.4.2 o versione successiva • Nginx è un server web che può essere usato come proxy inverso • PAM-devel PAM (Plugggable Authentication Modules) è uno strumento di protezione del sistema che consente agli amministratori di sistema di impostare i criteri di autenticazione senza dover ricompilare i programmi che eseguono l'autenticazione.

Requisiti degli host SAN

Se l'host SnapCenter fa parte di un ambiente FC/iSCSI, potrebbe essere necessario installare software aggiuntivo sul sistema per consentire l'accesso allo storage ONTAP.

SnapCenter non include le utility host o un DSM. Se l'host SnapCenter fa parte di un ambiente SAN, potrebbe essere necessario installare e configurare il seguente software:

- Utility host

  Le utility host supportano FC e iSCSI e consentono di utilizzare MPIO sui server Windows. Per informazioni, vedere "Documentazione delle utility host".

- Microsoft DSM per Windows MPIO

  Questo software funziona con i driver MPIO di Windows per gestire percorsi multipli tra i computer host NetApp e Windows.

  Per le configurazioni ad alta disponibilità è necessario un DSM.

  Se si utilizza ONTAP DSM, è necessario eseguire la migrazione a Microsoft DSM. Per ulteriori informazioni, vedere "Come migrare da ONTAP DSM a Microsoft DSM".

Sistemi e applicazioni storage supportati

È necessario conoscere il sistema di storage, le applicazioni e i database supportati.

- SnapCenter supporta ONTAP 9.12.1 e versioni successive per la protezione dei dati.
- SnapCenter supporta Amazon FSX per NetApp ONTAP per proteggere i dati dalla versione della patch P1 del software SnapCenter 4.5.

  Se si utilizza Amazon FSX per NetApp ONTAP, assicurarsi che i plug-in host del server SnapCenter siano aggiornati alla versione 4.5 P1 o successiva per eseguire le operazioni di protezione dei dati.

  Supporta NVMe (non-volatile Memory Express) su TCP (Transport Control Protocol).

  Per informazioni su Amazon FSX per NetApp ONTAP, vedere "Documentazione di Amazon FSX per NetApp ONTAP".

- SnapCenter supporta la protezione di diverse applicazioni e database.

  Per informazioni dettagliate sulle applicazioni e i database supportati, vedere "Tool di matrice di interoperabilità NetApp".

- SnapCenter 4,9 P1 e versioni successive supporta la protezione dei carichi di lavoro Oracle e Microsoft SQL in ambienti VMware Cloud su Amazon Web Services (AWS) Software-Defined Data Center (SDDC).

  Per ulteriori informazioni, vedere "Proteggi i carichi di lavoro Oracle e MS SQL utilizzando NetApp SnapCenter in VMware Cloud su ambienti SDDC AWS".

Browser supportati

Il software SnapCenter può essere utilizzato su più browser.

- Chrome versione 125 e successive
- Microsoft Edge 110.0.1587.17 e versioni successive

Per informazioni aggiornate sulle versioni supportate, vedere : "Tool di matrice di interoperabilità NetApp".

Requisiti di connessione e porta

Prima di installare il server SnapCenter e i plug-in dell'applicazione o del database, assicurarsi che i requisiti di connessione e porte siano soddisfatti.

- Le applicazioni non possono condividere una porta.

  Ciascuna porta deve essere dedicata all'applicazione appropriata.

- Per le porte personalizzabili, è possibile selezionare una porta personalizzata durante l'installazione se non si desidera utilizzare la porta predefinita.

  È possibile modificare una porta del plug-in dopo l'installazione utilizzando la procedura guidata Modify host (Modifica host).

- Per le porte fisse, 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 quando si installa SnapCenter, è necessario aggiungere una regola firewall sull'host del plug-in per tale porta per il caricatore plug-in SnapCenter.

La tabella seguente elenca le diverse porte e i relativi valori predefiniti.

Tipo di porta	Porta predefinita
Porta SnapCenter	8146 (HTTPS), bidirezionale, personalizzabile, come nell'URL *https://server:8146* Utilizzato per la comunicazione tra il client SnapCenter (l'utente SnapCenter) e il server SnapCenter. Utilizzato anche per la comunicazione dagli host plug-in al server SnapCenter. Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Porta di comunicazione SMCore SnapCenter	8145 (HTTPS), bidirezionale, personalizzabile La porta viene utilizzata per la comunicazione tra il server SnapCenter e gli host in cui sono installati i plug-in SnapCenter. Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Porta del servizio di pianificazione	8154 (HTTPS) Questa porta viene utilizzata per orchestrare i flussi di lavoro dello scheduler SnapCenter per tutti i plug-in gestiti all'interno dell'host server SnapCenter in modo centralizzato. Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Porto di RabbitMQ	5672 (tcp) Questa è la porta predefinita su cui RabbitMQ ascolta e viene utilizzata per la comunicazione tra il servizio Scheduler e SnapCenter sul modello di editore-abbonato.

Tipo di porta	Porta predefinita
Porta MySQL	3306 (HTTPS), bidirezionale, personalizzabile La porta viene utilizzata per la comunicazione tra SnapCenter e il database del repository MySQL. È possibile creare connessioni protette dal server SnapCenter al server MySQL. "Scopri di più" Per personalizzare la porta, vedere "Installare il server SnapCenter utilizzando l'installazione guidata."
Host plug-in Windows	135, 445 (TCP) Oltre alle porte 135 e 445, dovrebbe essere aperto anche l'intervallo di porte dinamiche specificato da Microsoft. Le operazioni di installazione remota utilizzano il servizio WMI (Windows Management Instrumentation), che ricerca dinamicamente questo intervallo di porte. Per informazioni sull'intervallo di porte dinamiche supportato, consultare la sezione "Panoramica del servizio e requisiti della porta di rete per Windows" Le porte vengono utilizzate per la comunicazione tra il server SnapCenter e l'host su cui viene installato il plug-in. Per inviare i binari dei pacchetti plug-in agli host plug-in di Windows, le porte devono essere aperte solo sull'host plug-in e possono essere chiuse dopo l'installazione.
Host plug-in Linux o AIX	22 (SSH) Le porte vengono utilizzate per la comunicazione tra il server SnapCenter e l'host in cui viene installato il plug-in. Le porte vengono utilizzate da SnapCenter per copiare i binari dei pacchetti plug-in su host plug-in Linux o AIX e devono essere aperte o escluse dal firewall o da iptables.

Tipo di porta	Porta predefinita
Pacchetto plug-in SnapCenter per Windows, pacchetto plug-in SnapCenter per Linux o pacchetto plug-in SnapCenter per AIX	8145 (HTTPS), bidirezionale, personalizzabile La porta viene utilizzata per la comunicazione tra SMCore e gli host in cui è installato il pacchetto plug-in. Il percorso di comunicazione deve essere aperto anche tra la LIF di gestione SVM e il server SnapCenter. Per personalizzare la porta, vedere "Aggiungere host e installare il plug-in SnapCenter per Microsoft Windows" o. "Aggiungere host e installare il pacchetto di plug-in SnapCenter per Linux o AIX."
Plug-in SnapCenter per database Oracle	27216, personalizzabile La porta JDBC predefinita viene utilizzata dal plug-in per Oracle per la connessione al database Oracle. Per personalizzare la porta, vedere "Aggiungere host e installare il pacchetto di plug-in SnapCenter per Linux o AIX."
Plug-in SnapCenter per database Exchange	909, personalizzabile NET predefinito. La porta TCP viene utilizzata dal plug-in di Windows per la connessione ai call-back VSS di Exchange. Per personalizzare la porta, vedere "Aggiungere host e installare il plug-in per Exchange".
Plug-in supportati da NetApp per SnapCenter	9090 (HTTPS), fisso Si tratta di una porta interna che viene utilizzata solo sull'host plug-in personalizzato; non è richiesta alcuna eccezione firewall. La comunicazione tra il server SnapCenter e i plug-in personalizzati viene instradata attraverso la porta 8145.

Tipo di porta	Porta predefinita
Porta di comunicazione SVM o cluster ONTAP	443 (HTTPS), bidirezionale (HTTP), bidirezionale La porta viene utilizzata da SAL (Storage Abstraction Layer) per la comunicazione tra l'host che esegue il server SnapCenter e SVM. La porta viene attualmente utilizzata anche dagli host plug-in SAL on SnapCenter per Windows per la comunicazione tra l'host plug-in SnapCenter e SVM.
Plug-in SnapCenter per database SAP HANA vCode controllo ortografico	3instance_number13 o 3instance_number15, HTTP o HTTPS, bidirezionale e personalizzabile Per un singolo tenant MDC (Multitenant Database Container), il numero di porta termina con 13; per i non MDC, il numero di porta termina con 15. Ad esempio, 32013 è il numero della porta, ad esempio 20 e 31015 è il numero della porta, ad esempio 10. Per personalizzare la porta, vedere "Aggiungere host e installare pacchetti plug-in su host remoti."
Porta di comunicazione del controller di dominio	Consultare la documentazione Microsoft per identificare le porte che devono essere aperte nel firewall di un controller di dominio affinché l'autenticazione funzioni correttamente. È necessario aprire le porte richieste da Microsoft sul controller di dominio in modo che il server SnapCenter, gli host plug-in o altri client Windows possano autenticare gli utenti.

Per modificare i dettagli della porta, vedere "Modificare gli host dei plug-in".

Licenze SnapCenter

SnapCenter richiede diverse licenze per consentire la protezione dei dati di applicazioni, database, file system e macchine virtuali. Il tipo di licenze SnapCenter installate dipende dall'ambiente di storage e dalle funzionalità che si desidera utilizzare.

Licenza	Dove richiesto
Basato su controller standard SnapCenter	Richiesto per FAS, AFF, All SAN Array (ASA) La licenza standard SnapCenter è una licenza basata su controller ed è inclusa nell'ambito di ONTAP One. Se si dispone della licenza della suite SnapManager, si ottiene anche il diritto di licenza standard SnapCenter. Se si desidera installare SnapCenter in prova con FAS, AFF o ASA, è possibile ottenere una licenza di valutazione di ONTAP ONE contattando il rappresentante di vendita. Per informazioni sulle licenze incluse in ONTAP One, fare riferimento alla sezione "Licenze incluse con ONTAP ONE". SnapCenter è anche offerto come parte del bundle per la protezione dei dati. Se hai acquistato A400 o versioni successive, devi acquistare il bundle per la protezione dei dati.
SnapMirror o SnapVault	ONTAP Se la replica è attivata in SnapCenter, è necessario disporre di una licenza SnapMirror o SnapVault.
SnapRestore	Necessario per ripristinare e verificare i backup. Sui sistemi storage primari • Necessario sui sistemi di destinazione SnapVault per eseguire la verifica remota e il ripristino da un backup. • Necessario sui sistemi di destinazione SnapMirror per eseguire la verifica in remoto.
FlexClone	Necessario per clonare i database e le operazioni di verifica. Sui sistemi di storage primario e secondario • Necessario sui sistemi di destinazione SnapVault per creare cloni dal backup del vault secondario. • Necessario sui sistemi di destinazione SnapMirror per creare cloni dal backup SnapMirror secondario.

Licenza	Dove richiesto
Protocolli	• Licenza iSCSI o FC per LUN • Licenza CIFS per le condivisioni SMB • Licenza NFS per VMDK di tipo NFS • Licenza iSCSI o FC per VMFS tipo VMDK Necessario sui sistemi di destinazione SnapMirror per la distribuzione dei dati se un volume di origine non è disponibile.
Licenze standard SnapCenter (opzionali)	Destinazioni secondarie Si consiglia, ma non è necessario, di aggiungere le licenze standard di SnapCenter alle destinazioni secondarie. Se le licenze standard di SnapCenter non sono abilitate sulle destinazioni secondarie, non è possibile utilizzare SnapCenter per eseguire il backup delle risorse sulla destinazione secondaria dopo aver eseguito un'operazione di failover. Tuttavia, è necessaria una licenza FlexClone sulle destinazioni secondarie per eseguire operazioni di cloning e verifica.

Le licenze servizi file NAS SnapCenter e SnapCenter sono obsolete e non sono più disponibili. La licenza standard e la licenza basata sulla capacità non sono più richieste per Amazon FSX per NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP e Azure NetApp Files.

Installare una o più licenze SnapCenter. Per informazioni su come aggiungere licenze, vedere "Aggiunta di licenze SnapCenter basate su controller standard".

Licenze SMBR (Single Mailbox Recovery)

Se si utilizza il plug-in SnapCenter per Exchange per gestire i database e il ripristino di una singola casella postale (SMBR), è necessaria una licenza aggiuntiva per SMBR che deve essere acquistata separatamente in base alla casella postale dell'utente.

Il ripristino di una singola casella postale di NetApp® è giunto alla fine della disponibilità (EOA) il 12 maggio 2023. Per ulteriori informazioni, fare riferimento a "CPC-00507". NetApp continuerà a supportare i clienti che hanno acquistato capacità, manutenzione e supporto della casella postale attraverso i codici marketing introdotti il 24 giugno 2020, per tutta la durata del diritto al supporto.

Il servizio di ripristino di una singola casella postale di NetApp è un prodotto partner fornito da Ontrack. Ontrack PowerControl offre funzionalità simili a quelle del ripristino di una singola casella postale di NetApp. I clienti possono acquistare nuove licenze software Ontrack PowerControls e rinnovi di assistenza e manutenzione Ontrack PowerControls da Ontrack (fino al licensingteam@ontrack.com) per il ripristino granulare della mailbox dopo la data EOA del 12 maggio 2023.

Effettuare la registrazione per accedere al software SnapCenter

Puoi accedere al software SnapCenter se sei un nuovo utente di Amazon FSX per NetApp ONTAP o Azure NetApp Files e non hai un account NetApp esistente.

Prima di iniziare

- È necessario avere accesso all'ID e-mail aziendale.
- Se utilizzi Azure NetApp Files, dovresti avere l'ID dell'abbonamento ad Azure.
- Se utilizzi Amazon FSX per NetApp ONTAP, dovresti avere l'ID del file system del file system FSX per ONTAP.

A proposito di questa attività

La registrazione è soggetta a convalide di informazioni e può richiedere fino a un giorno per confermare e aggiornare il nuovo account NSS (NetApp Support Site) per accedere "completamente" dall'accesso "ospite".

Fasi

1. Fare clic https://mysupport.netapp.com/site/user/registration per effettuare la registrazione.
2. Inserisci il tuo ID email aziendale, completa la captcha, accetta l'informativa sulla privacy di NetApp e fai clic su **Invia**.
3. Autenticare la registrazione immettendo l'OTP inviato all'ID e-mail e fare clic su **continua**.
4. Nella pagina di completamento della registrazione, immettere i seguenti dettagli per completare la registrazione.
   a. Selezionare **cliente NetApp / utente finale**.
   b. Nel campo NUMERO DI SERIE, immettere una delle seguenti opzioni:
      - ID sottoscrizione di Azure se si utilizza Azure NetApp Files.
      - ID file system se stai utilizzando Amazon FSX per NetApp ONTAP.

> È possibile inoltrare un ticket all'indirizzo https://mysupport.netapp.com/site/help se si verificano problemi durante la registrazione o per conoscere lo stato.

Metodi di autenticazione per le credenziali

Le credenziali utilizzano metodi di autenticazione diversi a seconda dell'applicazione o dell'ambiente. Le credenziali autenticano gli utenti in modo che possano eseguire operazioni SnapCenter. È necessario creare un set di credenziali per l'installazione dei plug-in e un altro set per le operazioni di protezione dei dati.

Autenticazione di Windows

Il metodo di autenticazione di Windows esegue l'autenticazione con Active Directory. Per l'autenticazione di Windows, Active Directory viene configurato al di fuori di SnapCenter. SnapCenter esegue l'autenticazione senza alcuna configurazione aggiuntiva. È necessaria una credenziale Windows per eseguire attività come l'aggiunta di host, l'installazione di pacchetti plug-in e la pianificazione dei processi.

Autenticazione di dominio non attendibile

SnapCenter consente la creazione di credenziali Windows utilizzando utenti e gruppi appartenenti a domini non attendibili. Affinché l'autenticazione abbia esito positivo, è necessario registrare i domini non attendibili con SnapCenter.

Autenticazione del gruppo di lavoro locale

SnapCenter consente la creazione di credenziali Windows con utenti e gruppi di lavoro locali. L'autenticazione di Windows per gli utenti e i gruppi di lavoro locali non avviene al momento della creazione delle credenziali di Windows, ma viene posticipata fino a quando non vengono eseguite la registrazione dell'host e altre operazioni dell'host.

Autenticazione di SQL Server

Il metodo di autenticazione SQL esegue l'autenticazione con un'istanza di SQL Server. Ciò significa che un'istanza di SQL Server deve essere rilevata in SnapCenter. Pertanto, prima di aggiungere una credenziale SQL, è necessario aggiungere un host, installare pacchetti plug-in e aggiornare le risorse. È necessaria l'autenticazione di SQL Server per eseguire operazioni come la pianificazione su SQL Server o il rilevamento delle risorse.

Autenticazione Linux

Il metodo di autenticazione Linux esegue l'autenticazione su un host Linux. L'autenticazione Linux è necessaria durante la fase iniziale di aggiunta dell'host Linux e installazione del pacchetto di plug-in SnapCenter per Linux in remoto dall'interfaccia grafica di SnapCenter.

Autenticazione AIX

Il metodo di autenticazione AIX esegue l'autenticazione su un host AIX. È necessaria l'autenticazione AIX durante la fase iniziale di aggiunta dell'host AIX e installazione del pacchetto di plug-in SnapCenter per AIX in remoto dalla GUI di SnapCenter.

Autenticazione del database Oracle

Il metodo di autenticazione del database Oracle esegue l'autenticazione su un database Oracle. Se l'autenticazione del sistema operativo (OS) è disattivata sull'host del database, è necessaria un'autenticazione del database Oracle per eseguire operazioni sul database Oracle. Pertanto, prima di aggiungere una credenziale di database Oracle, è necessario creare un utente Oracle nel database Oracle con privilegi sysdba.

Autenticazione Oracle ASM

Il metodo di autenticazione Oracle ASM esegue l'autenticazione con un'istanza di Oracle Automatic Storage Management (ASM). Se viene richiesto di accedere all'istanza di Oracle ASM e se l'autenticazione del sistema operativo (OS) è disattivata sull'host del database, è necessaria un'autenticazione Oracle ASM. Pertanto, prima di aggiungere una credenziale Oracle ASM, è necessario creare un utente Oracle con privilegi sysasm nell'istanza di ASM.

Autenticazione del catalogo RMAN

Il metodo di autenticazione del catalogo RMAN viene autenticato nel database del catalogo Oracle Recovery Manager (RMAN). Se è stato configurato un meccanismo di catalogo esterno e il database è stato registrato

nel database del catalogo, è necessario aggiungere l'autenticazione del catalogo RMAN.

Connessioni e credenziali dello storage

Prima di eseguire operazioni di protezione dei dati, è necessario configurare le connessioni di storage e aggiungere le credenziali utilizzate dal server SnapCenter e dai plug-in SnapCenter.

- **Connessioni storage**

  Le connessioni storage consentono al server SnapCenter e ai plug-in SnapCenter di accedere allo storage ONTAP. L'impostazione di queste connessioni comporta anche la configurazione delle funzionalità di AutoSupport e del sistema di gestione degli eventi (EMS).

- **Credenziali**

  - Amministratore di dominio o qualsiasi membro del gruppo di amministratori

    Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori sul sistema in cui si sta installando il plug-in SnapCenter. I formati validi per il campo Nome utente sono:

    - *NetBIOS/nome utente*
    - *Dominio FQDN/nome utente*
    - *Nome utente@upn*
  - Amministratore locale (solo per gruppi di lavoro)

    Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale incorporato nel sistema in cui si sta installando il plug-in SnapCenter. È possibile specificare un account utente locale che appartiene al gruppo di amministratori locale se l'account utente dispone di privilegi elevati o se la funzione di controllo dell'accesso utente è disattivata nel sistema host.

  Il formato valido per il campo Nome utente è: *Nome utente*

  - Credenziali per singoli gruppi di risorse

    Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare almeno il gruppo di risorse e i privilegi di backup al nome utente.

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 anche possibile vedere "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 il `Set-SmMultiFactorAuthentication` cmdlet.
8. (Facoltativo) controllare lo stato e le impostazioni della configurazione MFA utilizzando il `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 alla "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 MFA e pulire i file di configurazione creati quando MFA è stato attivato utilizzando il `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 tramite 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, è necessario immettere l'autenticazione a secondo fattore (qualcosa che si ha e qualcosa che si è) per ottenere il token portante.

+ la validità del token portante è configurabile dal server ad FS per 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 SSO di ad FS, 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 il `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": 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	Ottieni
Corpo di risposta	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSHostName": "win-adfs-sc49.winscedom2.com" }

Informazioni sul copyright

Informazioni sul marchio commerciale