Bereiten Sie sich auf die Installation des SnapCenter-Servers vor

SnapCenter Software 5.0

NetApp
July 18, 2024

Inhalt

Bereiten Sie sich auf die Installation des SnapCenter-Servers vor

Anforderungen an Domäne und Arbeitsgruppe

Der SnapCenter-Server kann auf Systemen installiert werden, die sich entweder in einer Domäne oder in einer Arbeitsgruppe befinden. Der für die Installation verwendete Benutzer muss bei Arbeitsgruppen und Domänen über Administratorrechte auf dem Computer verfügen.

Für die Installation von SnapCenter Server und SnapCenter Plug-ins auf Windows Hosts sollten Sie einen der folgenden Schritte verwenden:

- **Active Directory-Domäne**

  Sie müssen einen Domänenbenutzer mit lokalen Administratorrechten verwenden. Der Domänenbenutzer muss Mitglied der lokalen Administratorgruppe auf dem Windows-Host sein.

- **Arbeitsgruppen**

  Sie müssen ein lokales Konto mit lokalen Administratorrechten verwenden.

Obwohl Domänen-Trusts, Multi-Domain-Wälder und domänenübergreifende Trusts unterstützt werden, werden forstübergreifende Domänen nicht unterstützt. Die Microsoft-Dokumentation zu Active Directory-Domänen und Trusts enthält weitere Informationen.

> Nach der Installation des SnapCenter-Servers sollten Sie nicht die Domäne ändern, in der sich der SnapCenter-Host befindet. Wenn Sie den SnapCenter-Server-Host aus der Domäne entfernen, in der sich der SnapCenter-Server installiert hatte, und dann versuchen Sie, SnapCenter-Server zu deinstallieren, schlägt der Deinstallationsvorgang fehl.

Platz- und Größenanforderungen

Vor der Installation des SnapCenter Servers sollten Sie mit den Platz- und Größenanforderungen vertraut sein. Sie sollten auch die verfügbaren System- und Sicherheitsupdates anwenden.

Element	Anforderungen
Betriebssysteme	Microsoft Windows Es werden nur englische, deutsche, japanische und vereinfachte chinesische Versionen der Betriebssysteme unterstützt. Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

Element	Anforderungen
Minimale CPU-Anzahl	4 Kerne
Mind. RAM	8 GB Der MySQL Server Pufferpool nutzt 20 Prozent des gesamten RAM.
Minimaler Festplattenspeicher für die SnapCenter-Serversoftware und Protokolle	4 GB Wenn sich das SnapCenter-Repository auf demselben Laufwerk befindet, auf dem SnapCenter-Server installiert ist, wird empfohlen, 10 GB zu verwenden.
Minimaler Festplattenspeicher für das SnapCenter-Repository	6 GB HINWEIS: Wenn der SnapCenter-Server auf demselben Laufwerk installiert ist, auf dem das SnapCenter-Repository installiert ist, wird empfohlen, 10 GB zu verwenden.
Erforderliche Softwarepakete	• Microsoft .NET Framework 4.7.2 oder höher • Windows Management Framework (WMF) 4.0 oder höher • PowerShell 4.0 oder höher Für . NETZSPEZIFISCHE Informationen zur Fehlerbehebung, siehe "SnapCenter-Upgrade oder -Installation schlägt bei Legacy-Systemen ohne Internetverbindung fehl".

SAN-Host-Anforderungen

Wenn Ihr SnapCenter Host Teil einer FC-/iSCSI-Umgebung ist, müssen Sie möglicherweise zusätzliche Software auf dem System installieren, um den Zugriff auf ONTAP Storage zu ermöglichen.

SnapCenter umfasst keine Host Utilities oder DSM. Wenn Ihr SnapCenter Host Teil einer SAN-Umgebung ist, müssen Sie eventuell die folgende Software installieren und konfigurieren:

- Host Utilities

  Die Host Utilities unterstützen FC und iSCSI, und es ermöglicht Ihnen die Verwendung von MPIO auf Ihren Windows Servern. Weitere Informationen finden Sie unter "Host Utilities-Dokumentation".

- Microsoft DSM für Windows MPIO

  Diese Software arbeitet mit Windows MPIO-Treibern für das Management mehrerer Pfade zwischen NetApp und Windows Host-Computern zusammen.

  DSM ist für Hochverfügbarkeitskonfigurationen erforderlich.

  Wenn Sie ONTAP DSM verwenden, sollten Sie zu Microsoft DSM migrieren. Weitere Informationen finden Sie unter "So migrieren Sie von ONTAP DSM zu Microsoft DSM".

Unterstützte Storage-Systeme und Applikationen

Sie sollten die unterstützten Storage-Systeme, Applikationen und Datenbanken kennen.

- SnapCenter unterstützt ONTAP 8.3.0 und neuere Versionen für den Schutz Ihrer Daten.
- SnapCenter unterstützt Amazon FSX für NetApp ONTAP, um Ihre Daten vor der SnapCenter Software 4.5 P1-Patch-Veröffentlichung zu schützen.

  Wenn Sie Amazon FSX für NetApp ONTAP verwenden, stellen Sie sicher, dass die SnapCenter Server Host-Plug-ins auf 4.5 P1 oder höher aktualisiert werden, um Datensicherungsprozesse zu auszuführen.

  Weitere Informationen zu Amazon FSX for NetApp ONTAP finden Sie unter "Dokumentation zu Amazon FSX für NetApp ONTAP".

- SnapCenter unterstützt den Schutz verschiedener Applikationen und Datenbanken.

  Ausführliche Informationen zu den unterstützten Anwendungen und Datenbanken finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

- SnapCenter 4.9 P1 und höher unterstützt den Schutz von Oracle- und Microsoft-SQL-Workloads in VMware Cloud auf AWS-Umgebungen (Software-Defined Data Center) von Amazon Web Services.

  Weitere Informationen finden Sie unter "Schützen Sie Oracle- und MS-SQL-Workloads mithilfe von NetApp SnapCenter in VMware Cloud auf AWS SDDC-Umgebungen".

Unterstützte Browser

SnapCenter-Software kann auf mehreren Browsern verwendet werden.

- Chrom

  Wenn sie v66 verwenden, kann das SnapCenter GUI möglicherweise nicht gestartet werden.

- Internet Explorer

  Die SnapCenter UI wird nicht richtig geladen, wenn Sie IE 10 oder frühere Versionen verwenden. Sie sollten ein Upgrade auf IE 11 durchführen.

  - Es wird nur die Standardsicherheit unterstützt.

    Wenn Sie Änderungen an den Sicherheitseinstellungen von Internet Explorer vornehmen, treten erhebliche Probleme bei der Anzeige des Browsers auf.

    - Die Kompatibilitätsansicht für Internet Explorer muss deaktiviert sein.
- Microsoft Edge

Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperabilitäts-Matrix-Tool".

Verbindungs- und Portanforderungen

Stellen Sie sicher, dass die Verbindungs- und Ports-Anforderungen erfüllt sind, bevor Sie die SnapCenter Server- und Applikations- oder Datenbank-Plug-ins installieren.

- Anwendungen können einen Port nicht gemeinsam nutzen.

  Jeder Port muss der entsprechenden Applikation zugeordnet sein.

- Bei anpassbaren Ports können Sie während der Installation einen benutzerdefinierten Port auswählen, wenn Sie den Standardport nicht verwenden möchten.

  Sie können einen Plug-in-Port nach der Installation mithilfe des Assistenten zum Ändern von Hosts ändern.

- Für feste Ports sollten Sie die Standard-Port-Nummer akzeptieren.
- Firewalls
    - Firewalls, Proxys oder andere Netzwerkgeräte sollten keine Verbindung stören.
    - Wenn Sie bei der Installation von SnapCenter einen benutzerdefinierten Port angeben, sollten Sie auf dem Plug-in-Host eine Firewall-Regel für diesen Port für den SnapCenter-Plug-in-Loader hinzufügen.

In der folgenden Tabelle werden die verschiedenen Ports und ihre Standardwerte aufgeführt.

Typ des Ports	Standardport
SnapCenter-Port	8146 (HTTPS), bidirektional, anpassbar, wie in der URL *https://server:8146* Wird für die Kommunikation zwischen dem SnapCenter-Client (dem SnapCenter-Benutzer) und dem SnapCenter-Server verwendet. Wird auch zur Kommunikation von den Plug-in-Hosts mit dem SnapCenter-Server verwendet. Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."
SnapCenter SMCore-Kommunikations-Port	8145 (HTTPS), bidirektional, anpassbar Der Port wird für die Kommunikation zwischen dem SnapCenter-Server und den Hosts verwendet, auf denen die SnapCenter-Plug-ins installiert sind. Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."

Typ des Ports	Standardport
MySQL-Anschluss	3306 (HTTPS), bidirektional Der Port wird für die Kommunikation zwischen SnapCenter und der MySQL Repository Datenbank verwendet. Sie können sichere Verbindungen vom SnapCenter-Server zum MySQL-Server erstellen. "Weitere Informationen ." Informationen zum Anpassen des Ports finden Sie unter "Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."
Windows Plug-in-Hosts	135, 445 (TCP) Neben den Ports 135 und 445 sollte auch der von Microsoft festgelegte dynamische Portbereich geöffnet sein. Remote-Installationsvorgänge verwenden den Windows Management Instrumentation (WMI)-Dienst, der diesen Portbereich dynamisch durchsucht. Informationen zum unterstützten dynamischen Portbereich finden Sie unter "Serviceübersicht und Netzwerkanschlussanforderungen für Windows" Die Ports dienen zur Kommunikation zwischen dem SnapCenter-Server und dem Host, auf dem das Plug-in installiert wird. Um Plug-in-Binärdateien auf Windows-Plug-in-Hosts zu übertragen, müssen die Ports nur auf dem Plug-in-Host geöffnet sein, und sie können nach der Installation geschlossen werden.
Linux- oder AIX-Plug-in-Hosts	22 (SSH) Die Ports dienen zur Kommunikation zwischen dem SnapCenter-Server und dem Host, auf dem das Plug-in installiert wird. Die Ports werden von SnapCenter verwendet, um Plug-in-Paketbinärdateien auf Linux- oder AIX-Plug-in-Hosts zu kopieren. Sie sollten von der Firewall oder von iptables geöffnet oder ausgeschlossen sein.

Typ des Ports	Standardport
SnapCenter-Plug-ins-Paket für Windows, SnapCenter-Plug-ins-Paket für Linux oder SnapCenter-Plug-ins-Paket für AIX	8145 (HTTPS), bidirektional, anpassbar Der Port wird für die Kommunikation zwischen SMCore und Hosts verwendet, auf denen das Plug-ins-Paket installiert ist. Der Kommunikationspfad muss auch zwischen der SVM-Management-LIF und dem SnapCenter-Server offen sein. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für Microsoft Windows" oder "Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX."
SnapCenter Plug-in für Oracle Database	27216, anpassbar Der Standard-JDBC-Port wird vom Plug-in für Oracle für die Verbindung mit der Oracle-Datenbank verwendet. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX."
Benutzerdefinierte Plug-ins für SnapCenter	9090 (HTTPS), fest Dies ist ein interner Port, der nur auf dem benutzerdefinierten Plug-in-Host verwendet wird. Es ist keine Firewall-Ausnahme erforderlich. Die Kommunikation zwischen dem SnapCenter-Server und benutzerdefinierten Plug-ins wird über Port 8145 geleitet.
ONTAP-Cluster oder SVM-Kommunikations-Port	443 (HTTPS), bidirectional80 (HTTP), bidirektional Der Port wird von der SAL (Storage Abstraction Layer) für die Kommunikation zwischen dem Host verwendet, auf dem SnapCenter-Server und SVM ausgeführt wird. Der Port wird zur Kommunikation zwischen dem SnapCenter Plug-in-Host und der SVM derzeit auch von der SAL on SnapCenter für Windows Plug-in-Hosts verwendet.

Typ des Ports	Standardport
SnapCenter-Plug-in für SAP HANA-Datenbank vCode Zauber-Checkerports	3instance_number13 or 3instance_number15, HTTP oder HTTPS, bidirektional und anpassbar Bei einem einzelnen Mandanten mit mandantenfähigen Datenbank-Containern (MDC) endet die Port-Nummer mit 13. Für einen nicht-MDC-Server endet die Port-Nummer mit 15. Beispielsweise ist 32013 die Portnummer für die Instanz 20 und 31015 die Portnummer für Instanz 10. Informationen zum Anpassen des Ports finden Sie unter "Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts."
Kommunikations-Port des Domänencontrollers	In der Microsoft-Dokumentation finden Sie Informationen zu den Ports, die in der Firewall auf einem Domänencontroller geöffnet werden sollen, damit die Authentifizierung ordnungsgemäß funktioniert. Es ist erforderlich, die erforderlichen Microsoft-Ports auf dem Domänen-Controller zu öffnen, damit der SnapCenter-Server, Plug-in-Hosts oder andere Windows-Client die Benutzer authentifizieren kann.

Informationen zum Ändern der Portdetails finden Sie unter "Ändern Sie die Plug-in-Hosts".

SnapCenter-Lizenzen

Für die Datensicherung von Applikationen, Datenbanken, Filesystemen und Virtual Machines benötigt SnapCenter mehrere Lizenzen. Die Art der installierten SnapCenter Lizenzen hängt von Ihrer Storage-Umgebung und den gewünschten Funktionen ab.

Lizenz	Bei Bedarf
SnapCenter Standard Controller-basiert	Erforderlich für FAS, AFF, All-SAN-Array (ASA) Bei der SnapCenter Standard Lizenz handelt es sich um eine Controller-basierte Lizenz und ist im Rahmen des Premium Bundle enthalten. Wenn Sie die Lizenz für die SnapManager Suite besitzen, erhalten Sie auch die Standardlizenz von SnapCenter. Wenn Sie SnapCenter Testversionen mit FAS, AFF oder ASA Storage installieren möchten, erhalten Sie eine Evaluierungslizenz für Premium-Pakete. Wenden Sie sich hierzu an den Vertriebsmitarbeiter. SnapCenter ist auch als Teil des Datensicherungs-Bundles verfügbar. Wenn Sie A400 oder höher erworben haben, sollten Sie ein Datensicherungs-Bundle erwerben.
Kapazitätsbasierte SnapCenter Lösung	Erforderlich für ONTAP Select und Cloud Volumes ONTAP Als Cloud Volumes ONTAP- oder ONTAP Select-Kunde müssen Sie eine kapazitätsbasierte Lizenz pro TB erwerben, die auf den von SnapCenter gemanagten Daten basiert. Standardmäßig liefert SnapCenter eine integrierte kapazitätsbasierte SnapCenter-Testlizenz mit 90 TB und 100 Tagen im Umfang von TB aus. Weitere Informationen erhalten Sie von dem Vertriebsmitarbeiter.
SnapMirror oder SnapVault	ONTAP Wenn die Replizierung in SnapCenter aktiviert ist, ist entweder eine SnapMirror oder eine SnapVault Lizenz erforderlich.
SnapRestore	Für die Wiederherstellung und Überprüfung von Backups erforderlich. Auf primären Storage-Systemen • Erforderlich auf SnapVault Zielsystemen, um eine Remote-Verifizierung und die Wiederherstellung aus einem Backup durchzuführen. • Erforderlich auf SnapMirror Zielsystemen für die Remote-Verifizierung

Lizenz	Bei Bedarf
FlexClone	Die für das Klonen von Datenbanken und Verifizierungsvorgängen erforderlich sind. Auf primären und sekundären Storage-Systemen • Erforderlich auf SnapVault Zielsystemen, um Klone aus dem sekundären Vault Backup zu erstellen. • Erforderlich auf SnapMirror Zielsystemen, um Klone aus dem sekundären SnapMirror Backup zu erstellen.
Protokolle	• ISCSI- oder FC-Lizenz für LUNs • CIFS-Lizenz für SMB-Freigaben • NFS-Lizenz für NFS-Typ VMDKs • ISCSI- oder FC-Lizenz für VMFS-VMDKs des Typs VMDK Ist auf SnapMirror Zielsystemen erforderlich, um Daten bereitzustellen, wenn ein Quell-Volume nicht verfügbar ist.
SnapCenter-Standardlizenzen (optional)	Sekundäre Ziele Es wird empfohlen, aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen hinzufügen. Wenn SnapCenter Standardlizenzen nicht für sekundäre Ziele aktiviert sind, können Sie nach einem Failover-Vorgang SnapCenter nicht für ein Backup von Ressourcen auf dem sekundären Ziel verwenden. Allerdings ist eine FlexClone Lizenz für sekundäre Ziele erforderlich, um Klon- und Verifizierungsvorgänge durchzuführen.

Lizenzen für SnapCenter Advanced- und SnapCenter-NAS-Fileservices sind veraltet und sind nicht mehr verfügbar.

Sie sollten eine oder mehrere SnapCenter Lizenzen installieren. Informationen zum Hinzufügen von Lizenzen finden Sie unter "Controller-basierte SnapCenter Standard-Lizenzen hinzufügen" oder "Hinzufügen von kapazitätsbasierten SnapCenter Standard-Lizenzen".

Single Mailbox Recovery-Lizenzen (SMBR

Wenn Sie für das Management von Microsoft Exchange Server Datenbanken und Single Mailbox Recovery (SMBR) mit dem SnapCenter Plug-in für Exchange arbeiten, benötigen Sie eine zusätzliche Lizenz für SMBR, die separat in Abhängigkeit von der Benutzer-Mailbox erworben werden muss.

Die Einstellung der Verfügbarkeit für NetApp Single Mailbox Recovery (EOA) steht am 12. Mai 2023 fest. Weitere Informationen finden Sie unter "CPC-00507". NetApp unterstützt Kunden, die für den Zeitraum der Support-Berechtigung Mailbox-Kapazität, Wartung und Support erworben haben, weiterhin über die am 24. Juni 2020 eingeführten Marketing-Teilenummern.

NetApp Single Mailbox Recovery ist ein Partnerprodukt von Ontrack. OnTrack PowerControls bietet ähnliche Funktionen wie NetApp Single Mailbox Recovery. Kunden können von Ontrack (bis licensingteam@ontrack.com) neue Ontrack PowerControls Softwarelizenzen und Ontrack PowerControls Wartungs- und Supportverlängerungen für eine granulare Mailbox-Recovery nach dem EOA-Datum vom 12. Mai 2023 beziehen.

Authentifizierungsmethoden für Ihre Anmeldedaten

Je nach Anwendung oder Umgebung verwenden Anmeldeinformationen unterschiedliche Authentifizierungsmethoden. Anmeldedaten authentifizieren Benutzer, sodass sie SnapCenter-Vorgänge ausführen können. Zum Installieren von Plug-ins und einem anderen Satz für Datensicherungsvorgänge sollten Sie einen Satz von Anmeldeinformationen erstellen.

Windows Authentifizierung

Die Windows-Authentifizierungsmethode authentifiziert sich gegen Active Directory. Für die Windows-Authentifizierung wird Active Directory außerhalb von SnapCenter eingerichtet. SnapCenter authentifiziert sich ohne zusätzliche Konfiguration. Sie benötigen Windows-Anmeldedaten, um Aufgaben wie das Hinzufügen von Hosts, die Installation von Plug-in-Paketen und die Planung von Jobs auszuführen.

Nicht vertrauenswürdige Domänenauthentifizierung

SnapCenter ermöglicht die Erstellung von Windows-Anmeldeinformationen unter Verwendung von Benutzern und Gruppen, die zu nicht vertrauenswürdigen Domänen gehören. Damit die Authentifizierung erfolgreich ist, sollten Sie die nicht vertrauenswürdigen Domains bei SnapCenter registrieren.

Authentifizierung für lokale Arbeitsgruppen

SnapCenter ermöglicht die Erstellung von Windows-Anmeldeinformationen für Benutzer und Gruppen lokaler Arbeitsgruppen. Die Windows-Authentifizierung für Benutzer und Gruppen lokaler Arbeitsgruppen findet zum Zeitpunkt der Erstellung von Windows-Anmeldeinformationen nicht statt, wird jedoch verschoben, bis die Hostregistrierung und andere Hostvorgänge durchgeführt werden.

SQL Server-Authentifizierung

Die SQL-Authentifizierungsmethode authentifiziert sich anhand einer SQL Server-Instanz. Das bedeutet, dass eine SQL Server-Instanz in SnapCenter erkannt werden muss. Daher müssen Sie vor dem Hinzufügen von SQL-Anmeldeinformationen einen Host hinzufügen, Plug-in-Pakete installieren und Ressourcen aktualisieren. Sie benötigen die SQL Server-Authentifizierung für Vorgänge wie die Planung auf SQL Server oder die Ermittlung von Ressourcen.

Linux-Authentifizierung

Die Linux-Authentifizierungsmethode authentifiziert sich bei einem Linux-Host. Sie benötigen die Linux-Authentifizierung während des ersten Schritts des Hinzufügens des Linux-Hosts und der Remote-Installation des SnapCenter-Plug-ins-Pakets für Linux über die SnapCenter-Benutzeroberfläche.

AIX-Authentifizierung

Die AIX-Authentifizierungsmethode authentifiziert sich gegen einen AIX-Host. Sie benötigen eine AIX-Authentifizierung während des ersten Schritts, in dem Sie den AIX-Host hinzufügen und das SnapCenter Plug-ins Paket für AIX Remote von der SnapCenter-Benutzeroberfläche aus installieren.

Oracle-Datenbankauthentifizierung

Die Oracle-Datenbankauthentifizierung authentifiziert sich anhand einer Oracle-Datenbank. Sie benötigen eine Oracle-Datenbankauthentifizierung, um Vorgänge in der Oracle-Datenbank auszuführen, wenn die Betriebssystemauthentifizierung auf dem Datenbank-Host deaktiviert ist. Daher sollten Sie vor dem Hinzufügen von Oracle-Datenbankberechtigungen einen Oracle-Benutzer in der Oracle-Datenbank mit sysdba-Berechtigungen erstellen.

Oracle ASM Authentifizierung

Die Oracle ASM-Authentifizierungsmethode authentifiziert sich anhand einer Oracle Automatic Storage Management (ASM)-Instanz. Wenn Sie auf die Oracle ASM-Instanz zugreifen müssen und wenn die Betriebssystemauthentifizierung auf dem Datenbank-Host deaktiviert ist, benötigen Sie eine Oracle ASM-Authentifizierung. Daher sollten Sie vor dem Hinzufügen einer Oracle ASM-Berechtigung einen Oracle-Benutzer mit sysasm-Berechtigungen in der ASM-Instanz erstellen.

RMAN-Katalogauthentifizierung

Die Authentifizierungsmethode des RMAN-Katalogs authentifiziert sich mit der Oracle Recovery Manager (RMAN)-Katalogdatenbank. Wenn Sie einen externen Katalogmechanismus konfiguriert und Ihre Datenbank in der Katalogdatenbank registriert haben, müssen Sie die RMAN-Katalogauthentifizierung hinzufügen.

Storage-Verbindungen und Anmeldedaten

Vor Durchführung von Datensicherungsvorgängen sollten Sie die Speicherverbindungen einrichten und die Zugangsdaten hinzufügen, die der SnapCenter-Server und die SnapCenter-Plug-ins verwenden werden.

- **Speicherverbindungen**

  Über die Speicherverbindungen können SnapCenter-Server und SnapCenter-Plug-ins auf den ONTAP-Speicher zugreifen. Zum Einrichten dieser Verbindungen gehört auch die Konfiguration von Funktionen für das AutoSupport- und Ereignismanagement-System (EMS).

- **Anmeldeinformationen**

  - Domänenadministrator oder ein beliebiges Mitglied der Administratorgruppe

    Geben Sie den Domänenadministrator oder ein Mitglied der Administratorgruppe auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Gültige Formate für das Feld Benutzername sind:

- *NetBIOS\Benutzername*
- *Domain FQDN\Benutzername*
- *Benutzername@upn*

◦ Lokaler Administrator (nur für Arbeitsgruppen)

Geben Sie bei Systemen, die zu einer Arbeitsgruppe gehören, den integrierten lokalen Administrator auf dem System an, auf dem Sie das SnapCenter-Plug-in installieren. Sie können ein lokales Benutzerkonto angeben, das zur lokalen Administratorgruppe gehört, wenn das Benutzerkonto über erweiterte Berechtigungen verfügt oder die Funktion Benutzerzugriffssteuerung auf dem Hostsystem deaktiviert ist.

Das zulässige Format für das Feld Benutzername lautet: *Username*

◦ Anmeldedaten für einzelne Ressourcengruppen

Wenn Sie Anmeldedaten für einzelne Ressourcengruppen einrichten und der Benutzername nicht über vollständige Administratorrechte verfügt, müssen Sie dem Benutzernamen mindestens die Ressourcengruppe und die Sicherungsberechtigungen zuweisen.

Multi-Faktor-Authentifizierung (MFA)

Multi-Faktor-Authentifizierung (MFA) managen

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

Multi-Faktor-Authentifizierung (MFA) aktivieren

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

Über diese Aufgabe

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

Bevor Sie beginnen

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

CA-Zertifikat ist aus folgenden Gründen obligatorisch:

◦ Stellt sicher, dass die ADFS-F5-Kommunikation nicht unterbrochen wird, da die selbstsignierten

Zertifikate auf Knotenebene eindeutig sind.

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

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

Schritte

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

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

      Wenn die Prüfung erfolgreich war, klicken Sie auf **OK**.
10. Öffnen Sie im AD FS-Host den AD FS-Managementassistenten, und führen Sie die folgenden Schritte aus:
    a. Klicken Sie mit der rechten Maustaste auf **vertraut auf Partei** > **Vertrauensbeschuss hinzufügen** > **Start**.

b. Wählen Sie die zweite Option aus, und durchsuchen Sie die SnapCenter MFA-Metadatendatei und klicken Sie auf **Weiter**.

c. Geben Sie einen Anzeigenamen an und klicken Sie auf **Weiter**.

d. Wählen Sie eine Zugangskontrollrichtlinie nach Bedarf aus und klicken Sie auf **Weiter**.

e. Wählen Sie die Einstellungen auf der nächsten Registerkarte standardmäßig aus.

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

SnapCenter wird jetzt als vertrauensanzeige-Partei mit dem angegebenen Anzeigenamen dargestellt.

11. Wählen Sie den Namen aus, und führen Sie die folgenden Schritte aus:

a. Klicken Sie Auf **Richtlinie Zur Bearbeitung Von Forderungen**.

b. Klicken Sie auf **Regel hinzufügen** und klicken Sie auf **Weiter**.

c. Geben Sie einen Namen für die Antragsregel an.

d. Wählen Sie **Active Directory** als Attributspeicher aus.

e. Wählen Sie das Attribut als **Benutzer-Principal-Name** und den ausgehenden Antragsart als **Name-ID** aus.

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

12. Führen Sie die folgenden PowerShell-Befehle auf dem ADFS-Server aus.

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

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

13. Führen Sie die folgenden Schritte durch, um zu bestätigen, dass die Metadaten erfolgreich importiert wurden.

a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauensbesteller und wählen Sie **Eigenschaften**.

b. Stellen Sie sicher, dass die Felder Endpoints, Identifikatoren und Signatur ausgefüllt sind.

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

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

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

AD FS MFA-Metadaten aktualisieren

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

Schritte

1. Laden Sie die AD FS-Verbundmetadaten-Datei von FQDN>/FederationMetadata/2007-06/FederationMetadata.XML herunter "https://<host .“
2. Kopieren Sie die heruntergeladene Datei auf SnapCenter-Server, um die MFA-Konfiguration zu

aktualisieren.

3. Aktualisieren Sie die AD FS Metadaten in SnapCenter, indem Sie das folgende Cmdlet ausführen:

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

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

SnapCenter MFA-Metadaten aktualisieren

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

Schritte

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

      Der benutzerdefinierte Name des Vertrauensverhältnisses wird angezeigt.

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

      Siehe "Multi-Faktor-Authentifizierung aktivieren".

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

Multi-Faktor-Authentifizierung (MFA) deaktivieren

Schritte

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

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

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

Richten Sie AD FS als OAuth/OIDC ein

Konfigurieren Sie AD FS mit dem Windows GUI Wizard

1. Navigieren Sie zu **Server Manager Dashboard** > **Tools** > **ADFS Management**.
2. Navigieren Sie zu **ADFS** > **Anwendungsgruppen**.
   a. Klicken Sie mit der rechten Maustaste auf **Anwendungsgruppen**.
   b. Wählen Sie **Add Application Group** und geben Sie **Application Name** ein.

c. Wählen Sie **Server-Anwendung**.

d. Klicken Sie Auf **Weiter**.

3. Kopieren Sie Die Client-Kennung*.

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

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

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

5. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.

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

6. Klicken Sie mit der rechten Maustaste auf die neu hinzugefügte **Application Group** und wählen Sie **Properties**.
7. Wählen Sie aus den Anwendungseigenschaften **Anwendung hinzufügen**.
8. Klicken Sie auf **Anwendung hinzufügen**.

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

9. Geben Sie auf der Seite WebAPI konfigurieren die im vorherigen Schritt erstellte SnapCenter-Server-URL und die Clientkennung in den Abschnitt Kennung ein.

   a. Klicken Sie Auf **Hinzufügen**.

   b. Klicken Sie Auf **Weiter**.

10. Wählen Sie auf der Seite **Select Access Control Policy** die Kontrollrichtlinie entsprechend Ihrer Anforderung aus (z. B. „Permit everyone“ und „Require MFA“) und klicken Sie auf **Next**.
11. Auf der Seite **Configure Application permission** wird openid standardmäßig als Bereich ausgewählt, klicken Sie auf **Weiter**.
12. Klicken Sie auf der Seite **Zusammenfassung** auf **Weiter**.

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

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

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

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

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

16. Öffnen Sie das Tool **AD FS Management** im Menü **Tools** oben rechts im Server Manager.

    a. Wählen Sie in der linken Seitenleiste den Ordner **Anwendungsgruppen** aus.

    b. Wählen Sie die Web-API aus und klicken Sie auf **EDIT**.

    c. Wechseln Sie zur Registerkarte „Emissionsumform“

17. Klicken Sie Auf **Regel Hinzufügen**.
    a. Wählen Sie in der Dropdown-Liste „Antragsregel“ die Option **LDAP-Attribute als Schadensfall senden** aus.
    b. Klicken Sie Auf **Weiter**.
18. Geben Sie den Namen **Claim rule** ein.
    a. Wählen Sie **Active Directory** in der Dropdown-Liste Attributspeicher aus.
    b. Wählen Sie **User-Principal-Name** in der Dropdown-Liste **LDAP Attribute** und **UPN** in der Dropdown-Liste O*utgoing Claim Type* aus.
    c. Klicken Sie Auf **Fertig Stellen**.

Erstellen Sie eine Anwendungsgruppe mit PowerShell Befehlen

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

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

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

   `ClientRoleIdentifier` Name Ihrer Applikationsgruppe

   `redirectURL` Gültige URL für Umleitung nach Autorisierung

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

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

3. Erstellen Sie die ADFS-Web-API-Anwendung und konfigurieren Sie den Richtliniennamen, den sie verwenden soll.

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

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

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

4. Holen Sie sich die Client-ID und den Client-Schlüssel aus der Ausgabe der folgenden Befehle, da sie nur einmal angezeigt wird.

   ```
   "client_id = $identifier"

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

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

   ```
   Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
   ```

```
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. Schreiben Sie die Transformer-Regeldatei aus.

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

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

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

Ablaufdatum des Zugriffstoken aktualisieren

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

Über diese Aufgabe

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

Schritt

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

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

Holen Sie sich das Inhabertoken von AD FS

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

+ die Gültigkeit des Inhabertoken ist vom AD FS-Server pro Anwendung konfigurierbar und die Standardgültigkeitsdauer beträgt 60 Minuten.

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

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

Sie können MFA in SnapCenter-Server mit PowerShell, SCCLI und REST-API konfigurieren.

SnapCenter MFA CLI-Authentifizierung

In PowerShell und SCCLI wird das vorhandene Cmdlet (Open-SmConnection) um ein weiteres Feld namens "AccessToken" erweitert, um das Trägertoken zur Authentifizierung des Benutzers zu verwenden.

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

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

SnapCenter MFA Rest API-Authentifizierung

Verwenden Sie das Trägertoken im Format *Authorization=Bearer <access token>* im REST-API-Client (wie Postman oder swagger) und geben Sie den Benutzer RoleName in der Kopfzeile an, um eine erfolgreiche Antwort von SnapCenter zu erhalten.

MFA-Rest-API-Workflow

Wenn MFA mit AD FS konfiguriert ist, sollten Sie sich mit einem Zugriffstoken (Träger) authentifizieren, um über eine beliebige Rest-API auf die SnapCenter-Anwendung zuzugreifen.

Über diese Aufgabe

- Sie können jeden REST-Client wie Postman, Swagger UI oder FireCamp verwenden.
- Holen Sie sich ein Zugriffstoken und authentifizieren Sie es für nachfolgende Anfragen (SnapCenter Rest API), um einen Vorgang auszuführen.

Schritte

Zur Authentifizierung über AD FS MFA

1. Konfigurieren Sie den REST-Client so, dass er den AD FS-Endpunkt aufruft, um das Zugriffstoken zu erhalten.

   Wenn Sie auf die Schaltfläche klicken, um ein Zugriffstoken für eine Anwendung zu erhalten, werden Sie zur AD FS SSO-Seite weitergeleitet, auf der Sie Ihre AD-Anmeldeinformationen angeben und sich bei MFA authentifizieren müssen. 1. Geben Sie auf der AD FS SSO-Seite Ihren Benutzernamen oder Ihre E-Mail-Adresse in das Textfeld Benutzername ein.

   + Benutzernamen müssen als Benutzer@Domain oder Domain\user formatiert werden.

2. Geben Sie im Textfeld Kennwort Ihr Kennwort ein.
3. Klicken Sie auf **Anmelden**.
4. Wählen Sie im Abschnitt **Anmeldeoptionen** eine Authentifizierungsoption aus und authentifizieren Sie sich (je nach Konfiguration).
   - Push: Genehmigen Sie die Push-Benachrichtigung, die an Ihr Telefon gesendet wird.
   - QR-Code: Verwenden Sie die mobile App AUTH Point, um den QR-Code zu scannen, und geben Sie dann den in der App angezeigten Verifizierungscode ein
   - Einmalpasswort: Geben Sie das Einmalpasswort für Ihr Token ein.
5. Nach erfolgreicher Authentifizierung wird ein Popup-Fenster geöffnet, das die Token Zugriff, ID und Aktualisieren enthält.

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

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

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

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

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

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

GUI

Schritte

1. Melden Sie sich beim SnapCenter-Server als SnapCenter-Administrator an.
2. Klicken Sie auf **Einstellungen** > **Globale Einstellungen** > **MultiFactorAuthentication(MFA) Settings**
3. Wählen Sie die Schnittstelle (GUI/RST API/CLI) aus, um die MFA-Anmeldung zu aktivieren oder zu deaktivieren.

PowerShell-Schnittstelle

Schritte

1. Führen Sie die PowerShell- oder CLI-Befehle zur Aktivierung von MFA für GUI, Rest API, PowerShell und SCCLI aus.

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

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

   Aktiviert MFA für SnapCenter-GUI, Rest-API, PowerShell und SCCLI, konfiguriert mit angegebenem AD FS-Metadatendateipfad.

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mit dem `Get-SmMultiFactorAuthentication` Cmdlet.

SCCLI-Schnittstelle

Schritte

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

REST-APIs

1. Führen Sie die folgende Post-API zur Aktivierung von MFA für GUI, Rest-API, PowerShell und SCCLI aus.

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

Text Anfordern	{ "IsGuiMFAEnabled": False, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.XML" }
Antwortkörper	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.XML", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, „ADFSHostName“: „win-adfs-sc49.winscedom2.com“ } }

2. Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mithilfe der folgenden API.

Parameter	Wert
Angeforderte URL	/API/4.9/settings/multifactorauthentifizierung
HTTP-Methode	Verstehen
Antwortkörper	{ "MFAConfiguration": { "IsGuiMFAEnabled": False, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.XML", "SCConfigFilePath": Null, "IsRestApiMFAEnabled": True, "IsCliMFAEnabled": False, „ADFSHostName“: „win-adfs-sc49.winscedom2.com“ } }