



# **Bereiten Sie sich auf die Installation des SnapCenter-Servers vor**

## **SnapCenter Software 4.8**

NetApp  
January 18, 2024

# Inhalt

- Bereiten Sie sich auf die Installation des SnapCenter-Servers vor ..... 1
  - Anforderungen an Domäne und Arbeitsgruppe ..... 1
  - Platz- und Größenanforderungen ..... 1
  - SAN-Host-Anforderungen ..... 2
  - Unterstützte Storage-Systeme und Applikationen ..... 3
  - Unterstützte Browser ..... 3
  - Verbindungs- und Portanforderungen ..... 4
  - SnapCenter-Lizenzen ..... 7
  - Authentifizierungsmethoden für Ihre Anmeldedaten ..... 10
  - Storage-Verbindungen und Anmeldedaten ..... 11
  - Multi-Faktor-Authentifizierung (MFA) managen ..... 12

# 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	<p>Microsoft Windows</p> <p>Es werden nur englische, deutsche, japanische und vereinfachte chinesische Versionen der Betriebssysteme unterstützt.</p> <p>Aktuelle Informationen zu unterstützten Versionen finden Sie unter "<a href="#">NetApp Interoperabilitäts-Matrix-Tool</a>".</p>

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	<ul style="list-style-type: none"> <li>• Microsoft .NET Framework 4.7.2 oder höher</li> <li>• Windows Management Framework (WMF) 4.0 oder höher</li> <li>• PowerShell 4.0 oder höher</li> </ul> <p>Informationen zur .NET-spezifischen Fehlerbehebung finden Sie unter "<a href="#">SnapCenter-Upgrade oder -Installation schlägt bei Legacy-Systemen ohne Internetverbindung fehl</a>".</p> <p>Aktuelle Informationen zu unterstützten Versionen finden Sie unter "<a href="#">NetApp Interoperabilitäts-Matrix-Tool</a>".</p>

## 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.

Informationen zu Amazon FSX für 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"](#).

## 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	<p>8146 (HTTPS), bidirektional, anpassbar, wie in der URL <code>https://server:8146</code></p> <p>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.</p> <p>Informationen zum Anpassen des Ports finden Sie unter <a href="#">"Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."</a></p>
SnapCenter SMCORE-Kommunikations-Port	<p>8145 (HTTPS), bidirektional, anpassbar</p> <p>Der Port wird für die Kommunikation zwischen dem SnapCenter-Server und den Hosts verwendet, auf denen die SnapCenter-Plug-ins installiert sind.</p> <p>Informationen zum Anpassen des Ports finden Sie unter <a href="#">"Installieren Sie den SnapCenter-Server mithilfe des Installationsassistenten."</a></p>

Typ des Ports	Standardport
MySQL-Anschluss	<p>3306 (HTTPS), bidirektional</p> <p>Der Port wird für die Kommunikation zwischen SnapCenter und der MySQL Repository Datenbank verwendet.</p> <p>Sie können sichere Verbindungen vom SnapCenter-Server zum MySQL-Server erstellen. <a href="#">"Weitere Informationen ."</a></p>
Windows Plug-in-Hosts	<p>135, 445 (TCP)</p> <p>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.</p> <p>Informationen zum unterstützten dynamischen Portbereich finden Sie unter <a href="#">"Serviceübersicht und Netzwerkanschlussanforderungen für Windows"</a></p> <p>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.</p>
Linux- oder AIX-Plug-in-Hosts	<p>22 (SSH)</p> <p>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.</p>

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 <a href="#">"Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für Microsoft Windows"</a> Oder <a href="#">"Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX."</a>
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 <a href="#">"Fügen Sie Hosts hinzu, und installieren Sie das SnapCenter-Plug-ins-Paket für Linux oder AIX."</a>
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	<p data-bbox="813 153 1487 222">3instance_number13 or 3instance_number15, HTTP oder HTTPS, bidirektional und anpassbar</p> <p data-bbox="813 254 1487 390">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.</p> <p data-bbox="813 422 1487 491">Beispielsweise ist 32013 die Portnummer für die Instanz 20 und 31015 die Portnummer für Instanz 10.</p> <p data-bbox="813 522 1487 625">Informationen zum Anpassen des Ports finden Sie unter <a href="#">"Fügen Sie Hosts hinzu und installieren Sie Plug-in-Pakete auf Remote-Hosts."</a></p>
Kommunikations-Port des Domänencontrollers	<p data-bbox="813 678 1487 842">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.</p> <p data-bbox="813 873 1487 1010">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.</p>

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	<p>Erforderlich für FAS und AFF</p> <p>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 auf Testbasis mit FAS oder AFF Storage installieren möchten, wenden Sie sich an den Vertriebsmitarbeiter, um eine Evaluierungslizenz für das Premium Bundle zu erhalten.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 20px;">  <p>SnapCenter ist auch als Teil des Datensicherungs-Bundles verfügbar. Wenn Sie A400 oder höher erworben haben, sollten Sie ein Datensicherungs-Bundle erwerben.</p> </div>
Kapazitätsbasierte SnapCenter Lösung	<p>Erforderlich für ONTAP Select und Cloud Volumes ONTAP</p> <p>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.</p>
SnapMirror oder SnapVault	<p>ONTAP</p> <p>Wenn die Replizierung in SnapCenter aktiviert ist, ist entweder eine SnapMirror oder eine SnapVault Lizenz erforderlich.</p>
SnapRestore	<p>Für die Wiederherstellung und Überprüfung von Backups erforderlich.</p> <p>Auf primären Storage-Systemen</p> <ul style="list-style-type: none"> <li>• Erforderlich auf SnapVault Zielsystemen, um eine Remote-Verifizierung und die Wiederherstellung aus einem Backup durchzuführen.</li> <li>• Erforderlich auf SnapMirror Zielsystemen für die Remote-Verifizierung</li> </ul>

Lizenz	Bei Bedarf
FlexClone	<p>Die für das Klonen von Datenbanken und Verifizierungsvorgängen erforderlich sind.</p> <p>Auf primären und sekundären Storage-Systemen</p> <ul style="list-style-type: none"> <li>• Erforderlich auf SnapVault Zielsystemen, um Klone aus dem sekundären Vault Backup zu erstellen.</li> <li>• Erforderlich auf SnapMirror Zielsystemen, um Klone aus dem sekundären SnapMirror Backup zu erstellen.</li> </ul>
Protokolle	<ul style="list-style-type: none"> <li>• ISCSI- oder FC-Lizenz für LUNs</li> <li>• CIFS-Lizenz für SMB-Freigaben</li> <li>• NFS-Lizenz für NFS-Typ VMDKs</li> <li>• ISCSI- oder FC-Lizenz für VMFS-VMDKs des Typs VMDK</li> </ul> <p>Ist auf SnapMirror Zielsystemen erforderlich, um Daten bereitzustellen, wenn ein Quell-Volume nicht verfügbar ist.</p>
SnapCenter-Standardlizenzen (optional)	<p>Sekundäre Ziele</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>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.</p> </div>



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](mailto: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 Administratorengruppe gehört, wenn das Benutzerkonto über erhöhte Berechtigungen verfügt oder die Benutzerzugriffssteuerungsfunktion 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) managen

In diesem Thema wird beschrieben, wie die Multi-Faktor-Authentifizierung (MFA) im Active Directory-Verbunddienst (AD FS) und SnapCenter-Server verwaltet wird.

### Multi-Faktor-Authentifizierung (MFA) aktivieren

In diesem Thema wird beschrieben, wie die MFA-Funktionalität im Active Directory-Verbunddienst (AD FS)-Server und SnapCenter-Server aktiviert wird.

#### 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](#)".

#### Was Sie benötigen

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

CA-Zertifikat ist aus folgenden Gründen obligatorisch:

- Stellt sicher, dass die ADFS-F5-Kommunikation nicht unterbrochen wird, da die selbstsignierten Zertifikate auf Knotenebene eindeutig sind.

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

Informationen zum CA-Zertifikat finden Sie unter ["ZertifikatCSR-Datei erstellen"](#).

## Schritte

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

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

6. Kopieren Sie die generierte Datei auf den AD FS-Host, um SnapCenter als Client-Einheit zu konfigurieren.
7. Aktivieren Sie MFA für SnapCenter-Server mithilfe von *Set-SmMultiFactorAuthentication -Enable -Path* Cmdlet:

Der Parameter PATH gibt den Speicherort der XML-Metadatendatei AD FS MFA an, die in Schritt 3 auf den SnapCenter-Server kopiert wurde.

8. (Optional) Überprüfen Sie den MFA-Konfigurationsstatus und die Einstellungen mit *Get-SmMultiFactorAuthentication* Cmdlet:
9. Gehen Sie zur Microsoft Management Console (MMC), und führen Sie die folgenden Schritte aus:
  - a. Klicken Sie Auf **Datei > Snapin Hinzufügen/Entfernen**.
  - b. Wählen Sie im Fenster Snap-ins hinzufügen oder entfernen die Option **Zertifikate** und klicken Sie dann auf **Hinzufügen**.
  - c. Wählen Sie im Snap-in-Fenster Zertifikate die Option **Computerkonto** aus und klicken Sie dann auf **Fertig stellen**.
  - d. Klicken Sie Auf **Konsolenwurzel > Zertifikate – Lokaler Computer > Persönlich > Zertifikate**.
  - e. Klicken Sie mit der rechten Maustaste auf das CA-Zertifikat, das an SnapCenter gebunden ist, und wählen Sie dann **Alle Aufgaben > Privater Schlüssel verwalten** aus.
  - f. Führen Sie auf dem Berechtigungsassistenten die folgenden Schritte aus:
    - i. Klicken Sie Auf **Hinzufügen**.
    - ii. Klicken Sie auf **Standorte** und wählen Sie den betreffenden Host (oben in der Hierarchie) aus.
    - iii. Klicken Sie im Popup-Fenster **Locations** auf **OK**.
    - iv. Geben Sie im Feld Objektname 'IIS\_IUSRS' ein, und klicken Sie auf **Namen überprüfen** und klicken Sie auf **OK**.

Wenn die Prüfung erfolgreich war, klicken Sie auf **OK**.

10. Öffnen Sie im AD FS-Host den AD FS-Managementassistenten, und führen Sie die folgenden Schritte aus:
  - a. Klicken Sie mit der rechten Maustaste auf **vertraut auf Partei > Vertrauensbeschluss hinzufügen > Start**.
  - b. Wählen Sie die zweite Option aus, und durchsuchen Sie die SnapCenter MFA-Metadaten-Datei und klicken Sie auf **Weiter**.
  - c. Geben Sie einen Anzeigenamen an und klicken Sie auf **Weiter**.
  - d. Wählen Sie eine Zugangskontrollrichtlinie nach Bedarf aus und klicken Sie auf **Weiter**.
  - e. Wählen Sie die Einstellungen auf der nächsten Registerkarte standardmäßig aus.
  - f. Klicken Sie auf **Fertig Stellen**.

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

11. Wählen Sie den Namen aus, und führen Sie die folgenden Schritte aus:
  - a. Klicken Sie auf **Richtlinie Zur Bearbeitung Von Forderungen**.
  - b. Klicken Sie auf **Regel hinzufügen** und klicken Sie auf **Weiter**.
  - c. Geben Sie einen Namen für die Antragsregel an.
  - d. Wählen Sie **Active Directory** als Attributspeicher aus.
  - e. Wählen Sie das Attribut als **Benutzer-Principal-Name** und den ausgehenden Antragsart als **Name-ID** aus.
  - f. Klicken Sie auf **Fertig Stellen**.
12. Führen Sie die folgenden PowerShell-Befehle auf dem ADFS-Server aus.

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

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

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

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

Informationen zur Fehlerbehebung finden Sie unter ["Gleichzeitige Anmeldeversuche auf mehreren Registerkarten zeigen MFA-Fehler an"](#).

## AD FS MFA-Metadaten aktualisieren

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

### Schritte



1. Laden Sie die AD FS Federation-Metadatendatei von herunter "<https://<host FQDN>/FederationMetadaten/2007-06/FederationMetadata.XML>"
2. Kopieren Sie die heruntergeladene Datei auf SnapCenter-Server, um die MFA-Konfiguration zu aktualisieren.
3. Aktualisieren Sie die AD FS Metadaten in SnapCenter, indem Sie das folgende Cmdlet ausführen:

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

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

## SnapCenter MFA-Metadaten aktualisieren

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

### Schritte

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

Der benutzerdefinierte Name des Vertrauensverhältnisses wird angezeigt.

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

Siehe "[Multi-Faktor-Authentifizierung aktivieren](#)".

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

## Multi-Faktor-Authentifizierung (MFA) deaktivieren

### Schritte

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

## Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.