Erfahren Sie mehr über SnapCenter Software

SnapCenter software

NetApp
January 09, 2026

Inhalt

Erfahren Sie mehr über SnapCenter Software

Übersicht über SnapCenter

Die SnapCenter software ist eine einfache, zentralisierte und skalierbare Plattform für anwendungskonsistenten Datenschutz. Es schützt Anwendungen, Datenbanken, Host-Dateisysteme und VMs auf ONTAP -Systemen in der Hybrid Cloud.

SnapCenter verwendet die Technologien NetApp Snapshot, SnapRestore, FlexClone, SnapMirror und SnapVault , um Folgendes bereitzustellen:

- Schnelle, platzsparende, applikationskonsistente festplattenbasierte Backups
- Schnelle, detaillierte Wiederherstellung und anwendungskonsistente Wiederherstellung
- Schnelles, platzsparendes Klonen

SnapCenter umfasst SnapCenter Server und leichte Plug-Ins. Sie können die Plug-In-Bereitstellung auf Remote-Anwendungshosts automatisieren, Sicherungs-, Überprüfungs- und Klonvorgänge planen und Datenschutzvorgänge überwachen.

Sie können SnapCenter zum Schutz Ihrer Daten entweder vor Ort oder in einer öffentlichen Cloud installieren.

- Vor Ort zum Schutz der folgenden Punkte:
  - Daten auf primären ONTAP FAS, AFF oder ASA Systemen, die auf sekundäre ONTAP FAS, AFF oder ASA Systeme repliziert werden
  - Daten auf primären ONTAP Select Systemen
  - Daten auf primären und sekundären ONTAP FAS, AFF oder ASA Systemen, die auf lokalem StorageGRID Objekt-Storage gesichert sind
  - Daten auf primären und sekundären ONTAP ASA r2-Systemen
- Vor Ort in einer Hybrid Cloud zum Schutz der folgenden Elemente:
  - Daten auf primären ONTAP FAS, AFF oder ASA Systemen, die auf Cloud Volumes ONTAP repliziert werden
  - Daten, die sich auf primären und sekundären ONTAP FAS, AFF oder ASA -Systemen befinden und mithilfe der NetApp -Backup- und Recovery-Integration in Objekt- und Archivspeicher in der Cloud geschützt sind
- In einer Public Cloud zur Sicherung folgender Komponenten:
  - Daten auf primären Cloud Volumes ONTAP Systemen (früher ONTAP Cloud)
  - Daten auf Amazon FSX für ONTAP
  - Daten auf primärem Azure NetApp Files (Oracle, Microsoft SQL und SAP HANA)

Wichtige Funktionen

SnapCenter bietet folgende Kernfunktionen:

- Zentralisierte, applikationskonsistente Datensicherung unterschiedlicher Applikationen

  Datensicherung wird für Microsoft Exchange Server, Microsoft SQL Server, Oracle Datenbanken auf Linux

oder AIX, SAP HANA Datenbanken, IBM DB2, PostgreSQL, MySQL und Windows Host Dateisysteme auf ONTAP Systemen unterstützt. SnapCenter unterstützt auch den Schutz von Anwendungen wie MongoDB, Storage, MaxDB, Sybase ASE und ORASCPM.

- Richtlinienbasierte Backups

  Richtlinienbasierte Backups nutzen die NetApp Snapshot-Technologie, um schnelle, platzsparende, anwendungskonsistente, festplattenbasierte Backups zu erstellen. Sie können auch einen automatischen Schutz dieser Sicherungen auf einem sekundären Speicher einrichten, indem Sie vorhandene Schutzbeziehungen aktualisieren.

- Backups für mehrere Ressourcen

  Mithilfe von SnapCenter -Ressourcengruppen können Sie mehrere Ressourcen (Anwendungen, Datenbanken oder Hostdateisysteme) desselben Typs gleichzeitig sichern.

- Restore und Recovery

  SnapCenter ermöglicht schnelle, granulare Restores von Backups sowie applikationskonsistente, zeitbasierte Recoverys. Die Wiederherstellung ist von jedem Ziel in der Hybrid Cloud aus möglich.

- Klonen

  SnapCenter ermöglicht schnelles, platzsparendes und anwendungskonsistentes Klonen. Sie können auf jedem Ziel in der Hybrid Cloud klonen.

- Grafische Benutzeroberfläche für die Einzelbenutzerverwaltung

  SnapCenter bietet eine einzige Schnittstelle zum Verwalten von Backups und Klonen in jedem Hybrid Cloud-Ziel.

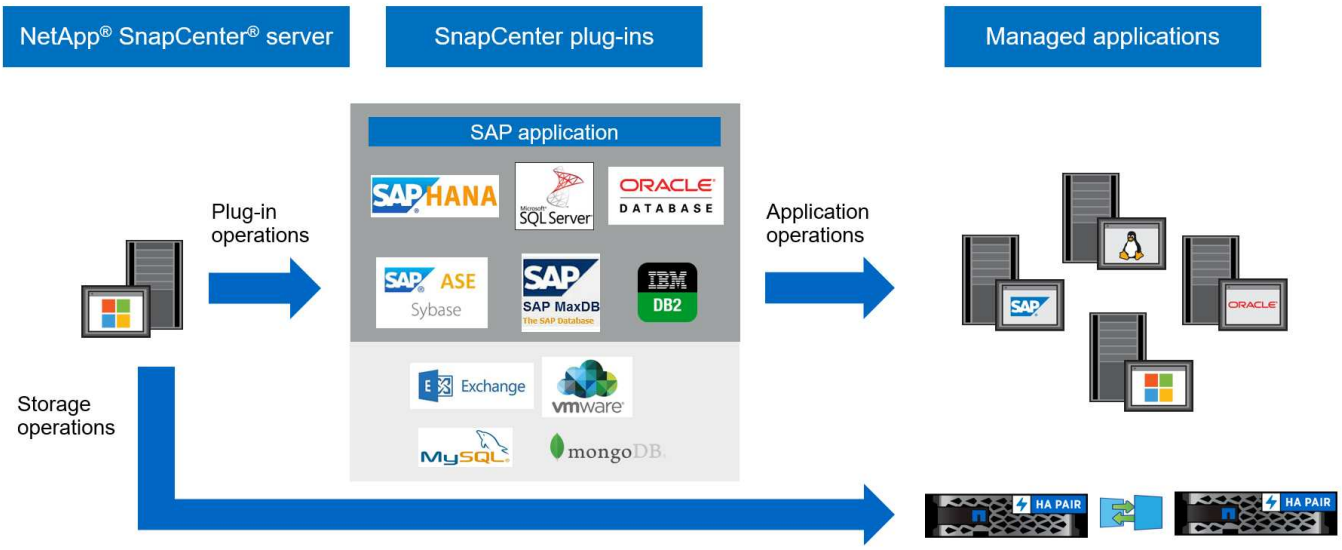
- REST-APIs, Windows Commandlets und UNIX Befehle

  SnapCenter bietet REST-APIs für die meisten Funktionen zur Integration in jede Orchestrierungs-Software sowie zur Verwendung von Windows PowerShell Cmdlets und Befehlszeilenschnittstelle.

- Zentrales Dashboard und Reporting zur Datensicherung
- Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) für Sicherheit und Delegierung
- Eine integrierte Repository-Datenbank mit hoher Verfügbarkeit zum Speichern aller Backup-Metadaten
- Automatisierte Push-Installation von Plug-ins
- Hochverfügbarkeit
- Disaster Recovery (DR)
- SnapLock "Weitere Informationen"
- SnapMirror Active Sync (zunächst veröffentlicht als SnapMirror Business Continuity [SM-BC])
- Synchrones Spiegeln "Weitere Informationen"

SnapCenter Architektur und Komponenten

SnapCenter verwendet ein mehrschichtiges Design mit einem zentralen Verwaltungsserver und Plug-in-Hosts. Die Server- und Plug-In-Hosts können sich an verschiedenen Standorten befinden.



SnapCenter enthält den SnapCenter-Server, das SnapCenter-Plug-in-Paket für Windows und das SnapCenter-Plug-in-Paket für Linux. Jedes Paket enthält Plug-ins für verschiedene Applikationen und Infrastrukturkomponenten.

SnapCenter Server

Der SnapCenter-Server unterstützt die Betriebssysteme Microsoft Windows und Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). Der SnapCenter-Server umfasst einen Webserver, eine zentrale HTML5-basierte Benutzeroberfläche, PowerShell Commandlets, REST-APIs und das SnapCenter-Repository.

SnapCenter speichert Informationen zu seinen Vorgängen im SnapCenter -Repository.

SnapCenter Plug-ins

Jedes SnapCenter-Plug-in unterstützt spezifische Umgebungen, Datenbanken und Applikationen.

Plug-in-Name	Im Installationspaket enthalten	Weitere Plug-ins sind erforderlich	Auf dem Host installiert	Unterstützte Plattformen
SnapCenter Plug-in für Microsoft SQL Server	Plug-ins-Paket für Windows	Plug-in für Windows	SQL Server Host	Windows
SnapCenter Plug-in für Windows	Plug-ins-Paket für Windows		Windows Host	Windows
SnapCenter Plug-in für Microsoft Exchange Server	Plug-ins-Paket für Windows	Plug-in für Windows	Exchange Server Host	Windows
SnapCenter Plug-in für Oracle Database	Plug-ins-Paket für Linux und Plug-ins Package für AIX	Plug-in für UNIX	Oracle Host	Linux oder AIX

Plug-in-Name	Im Installationspaket enthalten	Weitere Plug-ins sind erforderlich	Auf dem Host installiert	Unterstützte Plattformen
SnapCenter Plug-in für SAP HANA Database	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	HDBSQL-Client-Host	Linux oder Windows
SnapCenter Plug-in für IBM DB2	Plug-ins-Paket für Linux und Plug-ins Package für Windows	Plug-in für UNIX oder Plug-in für Windows	DB2-Host	Linux, AIX oder Windows
SnapCenter Plug-in für PostgreSQL	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	PostgreSQL-Host	Linux oder Windows
SnaoCenter Plug-in für MySQL	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	MySQL-Host	Linux oder Windows
SnapCenter Plug-in für MongoDB	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	MongoDB Host	Linux oder Windows
SnapCenter Plug-in für ORASCPM (Oracle Applikationen)	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	Oracle Host	Linux oder Windows
SnapCenter Plug-in für SAP ASE	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	SAP-Host	Linux oder Windows
SnapCenter Plug-in für SAP MaxDB	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	SAP MaxDB-Host	Linux oder Windows
SnapCenter Plug-in für Storage Plug-in	Plug-ins-Paket für Linux und Plug-ins-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	Storage Host	Linux oder Windows

Das SnapCenter Plug-in for VMware vSphere unterstützt absturzkonsistente und VM-konsistente Sicherungs- und Wiederherstellungsvorgänge für virtuelle Maschinen (VMs), Datenspeicher und Virtual Machine Disks (VMDKs). Es unterstützt außerdem anwendungskonsistente Sicherungs- und Wiederherstellungsvorgänge für virtualisierte Datenbanken und Dateisysteme.

Um Datenbanken, Dateisysteme, VMs oder Datenspeicher auf VMs zu schützen, stellen Sie das SnapCenter Plug-in for VMware vSphere Geräte bereit. Weitere Informationen finden Sie unter "Dokumentation zum SnapCenter Plug-in für VMware vSphere" .

SnapCenter Repository

Das SnapCenter-Repository, auch als NSM-Datenbank bezeichnet, speichert Informationen und Metadaten für jede SnapCenter-Operation.

Bei der SnapCenter Server-Installation wird standardmäßig die MySQL Server-Repository-Datenbank installiert. Wenn Sie MySQL Server bereits installiert haben und eine Neuinstallation von SnapCenter Server durchführen möchten, müssen Sie MySQL Server deinstallieren.

SnapCenter unterstützt MySQL Server 8.0.37 oder höher als SnapCenter -Repository-Datenbank. Wenn Sie eine frühere Version von MySQL Server mit einer früheren Version von SnapCenter verwenden, aktualisiert der SnapCenter -Upgradeprozess MySQL Server auf Version 8.0.37 oder höher.

Das SnapCenter Repository speichert folgende Informationen und Metadaten:

- Metadaten für Backup, Klonen, Wiederherstellung und Verifizierung
- Reporting-, Job- und Ereignisinformationen
- Host- und Plug-in-Informationen
- Rollen-, Benutzer- und Berechtigungsdetails
- Informationen zur Storage-Systemverbindung

Sicherheitsfunktionen in SnapCenter

SnapCenter setzt strenge Sicherheits- und Authentifizierungsfunktionen ein, damit Ihre Daten sicher bleiben.

SnapCenter umfasst die folgenden Sicherheitsfunktionen:

- Die gesamte Kommunikation zu SnapCenter verwendet HTTP über SSL (HTTPS).
- Alle Anmeldedaten in SnapCenter werden mit AES-Verschlüsselung (Advanced Encryption Standard) geschützt.
- Unterstützt Sicherheitsalgorithmen, die den Federal Information Processing Standard (FIPS) erfüllen.
- Unterstützt die Verwendung der vom Kunden bereitgestellten autorisierten Zertifizierungsstellenzertifikate.
- Unterstützt TLS 1.3 (Transport Layer Security) für die Kommunikation mit ONTAP. Sie können TLS 1.2 auch für die Kommunikation zwischen Clients und Servern verwenden.
- Unterstützt bestimmte SSL-Cipher-Suites für Sicherheit in der Netzwerkkommunikation. "Weitere Informationen .".
- SnapCenter wird innerhalb der Firewall Ihres Unternehmens installiert, um den Zugriff auf den SnapCenter Server zu ermöglichen und die Kommunikation zwischen dem SnapCenter Server und den Plug-ins zu ermöglichen.
- Für den SnapCenter-API- und -Betriebszugriff werden Tokens verwendet, die mit AES-Verschlüsselung verschlüsselt sind und nach 24 Stunden ablaufen.
- SnapCenter lässt sich zur Anmeldung und zur rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) in Windows Active Directory integrieren und ermöglicht die Zugriffsberechtigungen.
- IPsec wird mit SnapCenter auf ONTAP für Windows- und Linux-Hostcomputer unterstützt. "Weitere Informationen .".
- SnapCenter PowerShell Commandlets sind über die Sitzungen gesichert.

- Nach einer Standardlaufzeit von 15 Minuten Inaktivität warnt Sie SnapCenter, dass Sie in 5 Minuten abgemeldet werden.

  Nach 20 Minuten Inaktivität meldet SnapCenter Sie aus, und Sie müssen sich erneut anmelden. Sie können den Ausloggen Zeitraum ändern.

- Die Anmeldung ist nach 5 falschen Anmeldeversuchen vorübergehend deaktiviert.
- Unterstützt die Authentifizierung von CA-Zertifikaten zwischen SnapCenter Server und ONTAP. "Weitere Informationen .".
- Integritätsprüfung wird dem SnapCenter-Server und den Plug-ins hinzugefügt und validiert alle im Lieferumfang enthaltenen Binärdateien bei Neuinstallationen und Upgrades.

ÜBERSICHT ÜBER DAS CA-Zertifikat

Das Installationsprogramm von SnapCenter Server ermöglicht die zentralisierte Unterstützung von SSL-Zertifikaten während der Installation. Um die sichere Kommunikation zwischen Server und Plug-in zu verbessern, unterstützt SnapCenter die Verwendung der vom Kunden bereitgestellten autorisierten CA-Zertifikate.

Sie sollten CA-Zertifikate bereitstellen, nachdem Sie den SnapCenter-Server und die entsprechenden Plug-ins installiert haben. Weitere Informationen finden Sie unter "ZertifikatCSR-Datei erstellen".

Sie können auch ein CA-Zertifikat für SnapCenter-Plug-in für VMware vSphere implementieren. Weitere Informationen finden Sie unter "Erstellen und Importieren von Zertifikaten".

Bidirektionale SSL-Kommunikation

Die bidirektionale SSL-Kommunikation sichert die gegenseitige Kommunikation zwischen dem SnapCenter-Server und den Plug-ins.

Übersicht über die zertifikatbasierte Authentifizierung

Die zertifikatbasierte Authentifizierung überprüft die Authentizität der jeweiligen Benutzer, die versuchen, auf den SnapCenter-Plug-in-Host zuzugreifen. Der Benutzer sollte das SnapCenter-Serverzertifikat ohne privaten Schlüssel exportieren und in den vertrauenswürdigen Speicher des Plug-in-Hosts importieren. Die zertifikatbasierte Authentifizierung funktioniert nur, wenn die bidirektionale SSL-Funktion aktiviert ist.

Multi-Faktor-Authentifizierung (MFA)

MFA verwendet für das Management von Benutzersitzungen einen Identitätsanbieter (IdP) über die Security Assertion Markup Language (SAML) eines Drittanbieters. Diese Funktionalität verbessert die Authentifizierungssicherheit, da sie neben dem vorhandenen Benutzernamen und Passwort mehrere Faktoren wie TOTP, Biometrie, Push-Benachrichtigungen usw. verwenden kann. Zudem können Kunden mithilfe von IT-Providern ihre eigenen Benutzeridentitätsanbieter nutzen, um einheitliche SSO (Benutzeranmeldung) in ihrem gesamten Portfolio zu erhalten.

MFA ist nur für die Benutzerschnittstelle von SnapCenter Server anwendbar. Die Anmeldungen werden über die IdP Active Directory Federation Services (AD FS) authentifiziert. Sie können verschiedene Authentifizierungsfaktoren bei AD FS konfigurieren. SnapCenter ist der Service-Provider, und Sie sollten SnapCenter als eine abhängige Partei in AD FS konfigurieren. Um MFA in SnapCenter zu aktivieren, sind die AD FS-Metadaten erforderlich.

Informationen zur Aktivierung von MFA finden Sie unter "Multi-Faktor-Authentifizierung aktivieren".

Rollenbasierte Zugriffssteuerung in SnapCenter

Mit der rollenbasierten Zugriffskontrolle (RBAC) und den ONTAP Berechtigungen von SnapCenter können SnapCenter -Administratoren Benutzern oder Gruppen Ressourcenzugriff zuweisen. Dieser zentral verwaltete Zugriff ermöglicht Anwendungsadministratoren, sicher in bestimmten Umgebungen zu arbeiten.

Sie sollten Rollen erstellen oder ändern und Benutzern Ressourcenzugriff gewähren. Wenn Sie SnapCenter zum ersten Mal einrichten, fügen Sie Active Directory-Benutzer oder -Gruppen zu Rollen hinzu und weisen Sie diesen Benutzern oder Gruppen Ressourcen zu.

SnapCenter erstellt keine Benutzer- oder Gruppenkonten. Erstellen Sie Benutzer- oder Gruppenkonten im Active Directory des Betriebssystems oder der Datenbank.

Typen der RBAC in SnapCenter

SnapCenter unterstützt die folgenden Arten der rollenbasierten Zugriffskontrolle:

- SnapCenter RBAC
- RBAC auf Applikationsebene
- SnapCenter Plug-in für VMware vSphere RBAC
- ONTAP-Berechtigungen

SnapCenter RBAC

SnapCenter verfügt über vordefinierte Rollen und Sie können diesen Rollen Benutzer oder Gruppen zuweisen.

- SnapCenter Administratorrolle
- Administratorrolle für App Backup und Klonen
- Backup und Clone Viewer-Rolle
- Rolle für den Infrastrukturadministrator

Wenn Sie einem Benutzer eine Rolle zuweisen, zeigt SnapCenter die für diesen Benutzer relevanten Jobs auf der Seite „Jobs“ an, es sei denn, der Benutzer verfügt über die Rolle „SnapCenterAdmin“.

Sie können auch neue Rollen erstellen und Berechtigungen und Benutzer verwalten. Sie können Benutzern oder Gruppen Berechtigungen zuweisen, um auf SnapCenter-Objekte wie Hosts, Speicherverbindungen und Ressourcengruppen zuzugreifen.

Sie können Benutzern und Gruppen innerhalb derselben Gesamtstruktur und Benutzern, die zu verschiedenen Wäldern gehören, RBAC-Berechtigungen zuweisen. Sie können Benutzern, die zu verschachtelten Gruppen gehören, keine RBAC-Berechtigungen zuweisen.

Achten Sie beim Erstellen einer benutzerdefinierten Rolle darauf, dass diese alle Berechtigungen der SnapCenterAdmin-Rolle enthält. Wenn Sie nur einige Berechtigungen kopieren, verhindert SnapCenter , dass Sie alle Vorgänge ausführen.

Benutzer müssen sich bei der Anmeldung über die Benutzeroberfläche oder PowerShell-Cmdlets authentifizieren. Wenn Benutzer mehrere Rollen haben, wählen sie nach der Anmeldung eine Rolle aus. Auch

zum Ausführen von APIs ist eine Authentifizierung erforderlich.

RBAC auf Applikationsebene

SnapCenter verwendet die Zugangsdaten, um sicherzustellen, dass autorisierte SnapCenter Benutzer auch über Berechtigungen auf Applikationsebene verfügen.

Um beispielsweise Datenschutzvorgänge in einer SQL Server-Umgebung durchzuführen, legen Sie die richtigen Windows- oder SQL-Anmeldeinformationen fest. Wenn Sie Datenschutzvorgänge in einer Windows-Dateisystemumgebung auf ONTAP -Speicher durchführen möchten, muss die SnapCenter Administratorrolle über Administratorrechte auf dem Windows-Host verfügen.

Wenn Sie Datenschutzvorgänge für eine Oracle-Datenbank durchführen möchten und die Betriebssystemauthentifizierung auf dem Datenbankhost deaktiviert ist, müssen Sie die Anmeldeinformationen mit den Anmeldeinformationen der Oracle-Datenbank oder von Oracle ASM festlegen. Der SnapCenter -Server authentifiziert die festgelegten Anmeldeinformationen je nach Vorgang mit einer dieser Methoden.

SnapCenter Plug-in für VMware vSphere RBAC

Wenn Sie das SnapCenter VMware Plug-in für die VM-konsistente Datensicherung nutzen, bietet der vCenter Server zusätzliche RBAC-Level. Das SnapCenter VMware Plug-in unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC. "Weitere Informationen"

HINWEIS: NetApp empfiehlt, dass Sie eine ONTAP Rolle für SnapCenter Plug-in for VMware vSphere Vorgänge erstellen und ihr alle erforderlichen Berechtigungen zuweisen.

ONTAP-Berechtigungen

Sie sollten ein vsadmin-Konto mit den erforderlichen Berechtigungen für den Zugriff auf das Speichersystem erstellen."Weitere Informationen"

Berechtigungen, die den vordefinierten SnapCenter-Rollen zugewiesen sind

Wenn Sie einen Benutzer zu einer Rolle hinzufügen, weisen Sie ihm entweder die Berechtigung „StorageConnection“ zu, um die Kommunikation mit der Storage Virtual Machine (SVM) zu ermöglichen, oder weisen Sie dem Benutzer eine SVM zu, um ihm die Berechtigung zur Verwendung der SVM zu erteilen. Mit der Berechtigung „Speicherverbindung“ können Benutzer SVM-Verbindungen erstellen.

Beispielsweise kann ein SnapCenter Administrator SVM-Verbindungen erstellen und sie App Backup- und Clone-Administratorbenutzern zuweisen, die keine SVM-Verbindungen erstellen oder bearbeiten können. Ohne eine SVM-Verbindung können Benutzer keine Sicherungs-, Klon- oder Wiederherstellungsvorgänge durchführen.

SnapCenter Administratorrolle

In der SnapCenter-Administratorrolle sind alle Berechtigungen aktiviert. Sie können die Berechtigungen für diese Rolle nicht ändern. Sie können der Rolle Benutzer und Gruppen hinzufügen oder sie entfernen.

Administratorrolle für App Backup und Klonen

Die Rolle „App Backup“ und „Clone Admin“ verfügt über die erforderlichen Berechtigungen zur Durchführung administrativer Aktionen für Applikations-Backups und klonbezogene Aufgaben. Diese Rolle verfügt nicht über Berechtigungen für Host-Management, Bereitstellung, Storage-Verbindungs-Management oder Remote-Installation.

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisierung	Löschen
Ressourcengruppe	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Richtlinie	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Backup	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Host	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Storage-Anbindung	Keine Angabe	Nein	Ja.	Nein	Nein
Klon	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Bereitstellung	Keine Angabe	Nein	Ja.	Nein	Nein
Dashboard	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Berichte An	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Wiederherstellen	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Ressource	Ja.	Ja.	Ja.	Ja.	Ja.
Plug-in Installation/Deinstallation	Nein	Keine Angabe		Keine Angabe	Keine Angabe
Migration	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Montieren	Ja.	Ja.	Keine Angabe	Keine Angabe	Keine Angabe
Unmounten	Ja.	Ja.	Keine Angabe	Keine Angabe	Keine Angabe
Vollständige Volume-Wiederherstellung	Nein	Nein	Keine Angabe	Keine Angabe	Keine Angabe
Zweitschutz	Nein	Nein	Keine Angabe	Keine Angabe	Keine Angabe
Job-Überwachung	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Backup und Clone Viewer-Rolle

Die Rolle „Backup- und Klon-Viewer“ verfügt über die schreibgeschützte Ansicht aller Berechtigungen. Für diese Rolle sind außerdem Berechtigungen für die Erkennung, Berichterstellung und den Zugriff auf das Dashboard aktiviert.

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisierung	Löschen
Ressourcengruppe	Keine Angabe	Nein	Ja.	Nein	Nein
Richtlinie	Keine Angabe	Nein	Ja.	Nein	Nein
Backup	Keine Angabe	Nein	Ja.	Nein	Nein
Host	Keine Angabe	Nein	Ja.	Nein	Nein
Storage-Anbindung	Keine Angabe	Nein	Ja.	Nein	Nein
Klon	Keine Angabe	Nein	Ja.	Nein	Nein
Bereitstellung	Keine Angabe	Nein	Ja.	Nein	Nein
Dashboard	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Berichte An	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Wiederherstellen	Nein	Nein	Keine Angabe	Keine Angabe	Keine Angabe
Ressource	Nein	Nein	Ja.	Ja.	Nein
Plug-in Installation/Deinstallation	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Migration	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Montieren	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Unmounten	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Vollständige Volume-Wiederherstellung	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisierung	Löschen
Zweitschutz	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Job-Überwachung	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Rolle für den Infrastrukturadministrator

Die Rolle „Infrastrukturadministrator“ hat Berechtigungen für Host-Management, Storage-Management, Bereitstellung, Ressourcengruppen, Remote-Installationsberichte, Zugriff auf das Dashboard.

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisierung	Löschen
Ressourcengruppe	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Richtlinie	Keine Angabe	Nein	Ja.	Ja.	Ja.
Backup	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Host	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Storage-Anbindung	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Klon	Keine Angabe	Nein	Ja.	Nein	Nein
Bereitstellung	Keine Angabe	Ja.	Ja.	Ja.	Ja.
Dashboard	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Berichte An	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Wiederherstellen	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Ressource	Ja.	Ja.	Ja.	Ja.	Ja.
Plug-in Installation/Deinstallation	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Migration	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Montieren	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisierung	Löschen
Unmounten	Nein	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe
Vollständige Volume-Wiederherstellung	Nein	Nein	Keine Angabe	Keine Angabe	Keine Angabe
Zweitschutz	Nein	Nein	Keine Angabe	Keine Angabe	Keine Angabe
Job-Überwachung	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Disaster Recovery in SnapCenter

Die Disaster Recovery-Funktion (DR) von SnapCenter ermöglicht Ihnen das Recovery nach Ausfällen, z. B. nach Beschädigung von Ressourcen oder Server-Abstürzen. Es hilft, das SnapCenter-Repository, Serverzeitpläne, Konfigurationskomponenten und das SnapCenter-Plug-in für SQL Server und seinen Speicher wiederherzustellen.

In diesem Abschnitt werden die beiden Arten von DR in SnapCenter erläutert:

DR mit SnapCenter Servern

- Die Daten des SnapCenter Servers werden gesichert und können ohne Plug-in wiederhergestellt werden, das dem SnapCenter Server hinzugefügt oder durch ihn gemanagt wird.
- Der sekundäre SnapCenter Server sollte auf demselben Installationsverzeichnis und auf demselben Port wie der primäre SnapCenter-Server installiert sein.
- Für die Multi-Faktor-Authentifizierung (MFA) schließen Sie während der SnapCenter-Server-Wiederherstellung alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um sich erneut anzumelden. Dadurch werden die vorhandenen oder aktiven Sitzungscookies gelöscht und die korrekten Konfigurationsdaten aktualisiert.
- Die Disaster Recovery-Funktion von SnapCenter verwendet REST-APIs, um einen SnapCenter-Server zu sichern. Siehe "REST-API-Workflows für Disaster Recovery von SnapCenter Server".
- Die Konfigurationsdatei für Überwachungseinstellungen wird nach dem Wiederherstellungsvorgang weder im DR-Backup noch auf dem DR-Server gesichert. Sie sollten die Einstellungen für das Überwachungsprotokoll manuell wiederholen.

SnapCenter Plug-in und Storage DR

DR ist nur für das SnapCenter Plug-in für SQL Server verfügbar. Wenn das Plug-in ausfällt, wechseln Sie zu einem anderen SQL-Host, und stellen Sie die Daten mithilfe einiger Schritte wieder her. Siehe "Disaster Recovery eines SnapCenter Plug-ins für SQL Server".

SnapCenter verwendet ONTAP SnapMirror zur Replizierung von Daten. Diese können für DR verwendet werden, indem die Daten am sekundären Standort synchronisiert werden. Brechen Sie die SnapMirror-Replizierung ab, um ein Failover zu initiieren. Bei einem Fallback ist die Synchronisierung rückgängig zu

machen, um Daten vom DR-Standort zurück zum primären Standort zu replizieren.

Von SnapCenter benötigte 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, ASA Bei der SnapCenter Standardlizenz handelt es sich um eine Controller-basierte Lizenz, die als Teil von NetApp ONTAP One enthalten ist. Wenn Sie die Lizenz für die SnapManager Suite besitzen, erhalten Sie auch die Standardlizenz von SnapCenter. Wenn Sie SnapCenter als Testlizenz mit FAS, AFF oder ASA Storage installieren möchten, erhalten Sie bei Ihrem Vertriebsmitarbeiter eine Evaluierungslizenz für NetApp ONTAP One. Informationen zu Lizenzen, die in NetApp ONTAP One enthalten sind, finden Sie unter "In NetApp ONTAP One enthaltene Lizenzen". SnapCenter ist auch als Teil des Datensicherungs-Bundles verfügbar. Wenn Sie A400 oder höher erworben haben, sollten Sie ein Datensicherungs-Bundle erwerben.
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.
Protokolllizenzen	• 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.

Lizenz	Bei Bedarf
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.

Lizenzen für SnapCenter Advanced- und SnapCenter-NAS-Fileservices sind veraltet und sind nicht mehr verfügbar. Für Amazon FSX for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP und Azure NetApp Files sind die Standardlizenz und die kapazitätsbasierte Lizenz nicht mehr erforderlich.

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

Aktive SnapMirror-Synchronisierung in SnapCenter

SnapMirror Active Sync ermöglicht Business Services auch bei einem vollständigen Standortausfall den Betrieb weiter und unterstützt Applikationen bei einem transparenten Failover mithilfe einer sekundären Kopie. Es sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich, um einen Failover mit SnapMirror Active Sync auszulösen.

Weitere Informationen zu SnapMirror Active Sync finden Sie unter "Übersicht über SnapMirror Active Sync".

Stellen Sie für die aktive SnapMirror Synchronisierung sicher, dass Sie die verschiedenen Anforderungen an Hardware, Software und Systemkonfiguration erfüllt haben. Weitere Informationen finden Sie unter "Voraussetzungen"

Folgende Plug-ins werden für diese Funktion unterstützt: SnapCenter Plug-in für SQL Server, SnapCenter

Plug-in für Windows, SnapCenter Plug-in für Oracle Database, SnapCenter Plug-in für SAP HANA Database, SnapCenter Plug-in für Microsoft Exchange Server und SnapCenter Plug-in für Unix.

Nach der Installation des SnapCenter -Servers und der Plug-Ins sollten Sie die REST-API für SnapCenter aktivieren, um SnapMirror -Active-Sync-Beziehungen zu erkennen.

- Bearbeiten Sie auf dem SnapCenter -Serverhost die Datei *C:\Programme\ NetApp\SMCore\SMCoreServiceHost.dll.config*, um den Wert des Parameters *IsRestEnabledForStorageConnection* auf *true* zu ändern, und starten Sie dann den SnapCenter SMCore-Dienst neu.
- Auf den Windows-Plug-In-Hosts:
  - Bearbeiten Sie die Datei *C:\Program Files\ NetApp\ SnapCenter\SMCore\SMCoreServiceHost.dll.config*, um den Wert des Parameters *IsRestEnabledForStorageConnection* auf *true* zu ändern.
  - Bearbeiten Sie die Datei *C:\Programme\ NetApp\ SnapCenter\SMCore\SnapDriveService.dll.config*, um den Wert des Parameters *IsRestEnabledForStorageConnection* in *true* zu ändern.
  - Starten Sie den SnapCenter SMCore-Dienst neu.

Um die Nähe des Host-Initiators in SnapCenter zu unterstützen, sollte dieser Wert entweder als Quelle oder als Ziel in ONTAP festgelegt werden.

Die in SnapCenter nicht unterstützten Anwendungsfälle:

- Wenn Sie vorhandene asymmetrische SnapMirror Workloads mit aktiver Synchronisierung in symmetrisch konvertieren, indem Sie die Richtlinie für die aktiven SnapMirror Synchronisierungsbeziehungen von *automatisiertFailover* zu *automatisiertFailover* in ONTAP ändern, wird dies auch nicht in SnapCenter unterstützt.
- Wenn Backups einer Ressourcengruppe (bereits in SnapCenter geschützt) vorhanden sind und dann die Storage-Richtlinie auf den aktiven Synchronisierungsbeziehungen von SnapMirror von *automatisiertFailover* auf *automatisiertFailover* in ONTAP geändert wird, wird dies auch nicht in SnapCenter unterstützt.

Schlüsselkonzepte der Datensicherung

Bevor Sie SnapCenter verwenden, sollten Sie sich über die Schlüsselkonzepte für Backup, Klonen und Wiederherstellung informieren.

Ressourcen

Zu den Ressourcen zählen Datenbanken, Windows Filesysteme oder Dateifreigaben, die mit SnapCenter gesichert oder geklont wurden. Je nach Umgebung können außerdem Datenbankinstanzen, SQL Server-Verfügbarkeitsgruppen, Oracle-Datenbanken, RAC-Datenbanken oder benutzerdefinierte Applikationsgruppen sein.

Ressourcengruppe

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster, möglicherweise von mehreren Hosts und Clustern. Vorgänge, die für eine Ressourcengruppe ausgeführt werden, werden auf Basis des angegebenen Zeitplans auf alle zugehörigen Ressourcen angewendet. Sie können On-Demand- oder geplante Backups für einzelne Ressourcen oder Gruppen durchführen.

Wenn ein Host in einer gemeinsam genutzten Ressourcengruppe in den Wartungsmodus wechselt, werden alle geplanten Vorgänge für diese Gruppe auf allen Hosts ausgesetzt.

Verwenden Sie relevante Plug-ins, um spezifische Ressourcen zu sichern: Datenbank-Plug-ins für Datenbanken, Filesystem-Plug-ins für Filesysteme und SnapCenter Plug-in für VMware vSphere für VMs und Datastores.

Richtlinien

Mithilfe von Richtlinien werden die Backup-Häufigkeit, die Aufbewahrung von Kopien, Replizierung, Skripte und andere Merkmale von Datensicherungsvorgängen festgelegt.

Eine oder mehrere Richtlinien können beim Erstellen einer Ressourcengruppe oder beim Durchführen eines On-Demand-Backups ausgewählt werden.

Eine Ressourcengruppe definiert, was geschützt werden muss und wann sie Tag und Uhrzeit geschützt werden soll. Eine Richtlinie beschreibt, wie der Schutz durchgeführt wird. Wenn beispielsweise ein Backup aller Datenbanken oder Dateisysteme eines Hosts erforderlich ist, kann eine Ressourcengruppe mit allen Datenbanken oder Dateisystemen im Host erstellt werden. Der Ressourcengruppe könnten dann zwei Richtlinien zugeordnet werden: Eine tägliche Richtlinie und eine stündliche Richtlinie.

Beim Erstellen der Ressourcengruppe und Anhängen der Richtlinien ist es möglich, sie so zu konfigurieren, dass täglich ein vollständiges Backup durchgeführt wird und ein weiterer Zeitplan für stündliche Protokollsicherungen erstellt wird.

Für Datensicherungsvorgänge können benutzerdefinierte Verordnungen und Postskripte verwendet werden. Diese Skripte ermöglichen eine Automatisierung vor oder nach der Datensicherung. Ein Skript könnte beispielsweise automatisch über Ausfälle oder Warnungen von Datenschutzaufschlägen informieren. Vor dem Einrichten von Verordnungen und Postskripten ist es von entscheidender Bedeutung, die Anforderungen für die Erstellung dieser Skripts zu verstehen.

Konsistenzgruppe (CG)

Eine Konsistenzgruppe ist eine Sammlung von Volumes, die als eine Einheit verwaltet werden. CGs werden zur Gewährleistung der Datenkonsistenz über Speichereinheiten und Datenträger hinweg synchronisiert. In ONTAP bieten sie eine einfache Verwaltung und eine Schutzgarantie für eine Anwendungs-Workload, die sich über mehrere Volumes erstreckt. Erfahren Sie mehr über "Konsistenzgruppen" .

Verwendung von Verordnungen und Postskripten

Benutzerdefinierte Verordnungen und Postskripte können Ihre Datensicherungsaufgaben vor oder nach dem Job automatisieren. Sie können beispielsweise ein Skript hinzufügen, um Sie über Auftragsfehler oder Warnungen zu informieren. Bevor Sie sie einrichten, müssen Sie die Anforderungen für diese Skripte verstehen.

Unterstützte Skripttypen

Die folgenden Skripttypen werden für Windows unterstützt:

- Batch-Dateien
- PowerShell Skripte
- Perl-Skripte

Für UNIX werden die folgenden Skripttypen unterstützt:

- Perl-Skripte
- Python-Skripte
- Shell-Skripte

Zusammen mit Standard-Bash-Shell werden auch andere Shells wie sh-Shell, k-shell und c-shell unterstützt.

Skriptpfad

Alle Verordnungen und Postskripte, die als Teil der SnapCenter-Vorgänge auf nicht virtualisierten und nicht virtualisierten Storage-Systemen ausgeführt werden, werden auf dem Plug-in-Host ausgeführt.

- Die Windows-Skripte sollten sich auf dem Plug-in-Host befinden.

Der Pfad für Prescripts oder Postscripts darf keine Laufwerke oder Shares enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

- Die UNIX-Skripte sollten sich auf dem Plug-in-Host befinden.

Der Skriptpfad wird zum Zeitpunkt der Ausführung validiert.

Angeben von Skripten

Skripte werden in den Backup-Richtlinien angegeben. Wenn ein Backup-Job gestartet wird, ordnet die Policy das Skript automatisch den zu sichernden Ressourcen zu. Wenn Sie eine Sicherungsrichtlinie erstellen, können Sie die Vorschrift- und die Postscript-Argumente angeben.

Sie können nicht mehrere Skripte angeben.

Skript-Timeouts

Die Zeitüberschreitung ist standardmäßig auf 60 Sekunden eingestellt. Sie können den Zeitüberschreitungswert ändern.

Skriptausgabe

Das Standardverzeichnis für die Windows-Druckschriften und Postscripts-Ausgabedateien ist Windows\System32.

Es gibt keinen Standardspeicherort für UNIX Prescripts und Postscripts. Sie können die Ausgabedatei an einen beliebigen bevorzugten Speicherort weiterleiten.

Storage-Systeme und Applikationen unterstützt von SnapCenter

Sie sollten die Storage-Systeme, Applikationen und Datenbanken kennen, die von SnapCenter unterstützt werden.

Unterstützte Storage-Systeme

- NetApp ONTAP 9.12.1 und höher
- Azure NetApp Dateien
- Amazon FSX für NetApp ONTAP

  Amazon FSx for NetApp ONTAP unterstützt Non-Volatile Memory Express (NVMe) über Transport Control Protocol (TCP).

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

- NetApp ASA r2-Systeme, auf denen NetApp ONTAP 9.16.1 und höher ausgeführt wird

  Sie sollten ONTAP 9.17.1 verwenden, wenn Sie SnapCenter Server 6.2 und SnapCenter -Plug-Ins 6.2 verwenden.

Unterstützte Applikationen und Datenbanken

SnapCenter unterstützt den Schutz verschiedener Anwendungen und Datenbanken.

SnapCenter 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".

Authentifizierungsmethoden für SnapCenter-Anmeldeinformationen

Anmeldeinformationen verwenden je nach Anwendung oder Umgebung unterschiedliche Authentifizierungsmethoden. Anmeldedaten authentifizieren Benutzer, sodass sie SnapCenter-Vorgänge ausführen können. Sie sollten einen Satz von Anmeldeinformationen für die Installation von Plug-ins und einen anderen für Datensicherungsvorgänge 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-Anmeldeinformationen, um Hosts hinzuzufügen, Plug-in-Pakete zu installieren und Jobs zu planen.

Nicht vertrauenswürdige Domänenauthentifizierung

Mit SnapCenter können Benutzer und Gruppen, die zu nicht vertrauenswürdigen Domänen gehören, Windows-Anmeldeinformationen erstellen. 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 erfolgt nicht

während der Erstellung von Windows-Anmeldeinformationen, sondern wird verschoben, bis die Hostregistrierung und andere Hostvorgänge ausgeführt 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 eine SQL Server-Authentifizierung, um Vorgänge wie das Planen auf SQL Server oder das Erkennen von Ressourcen auszuführen.

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 einer Oracle-Datenbankanmeldeinformationen einen Oracle-Benutzer in der Oracle-Datenbank mit sysdba Privileges erstellen.

Oracle ASM Authentifizierung

Die Oracle ASM-Authentifizierungsmethode authentifiziert sich anhand einer Oracle Automatic Storage Management (ASM)-Instanz. Die Oracle ASM-Authentifizierung ist erforderlich, wenn Sie auf eine Oracle ASM-Instanz zugreifen müssen und die OS-Authentifizierung auf dem Datenbank-Host deaktiviert ist. Erstellen Sie vor dem Hinzufügen einer Oracle ASM-Anmeldeinformationen einen Oracle-Benutzer mit System-Privileges in der ASM-Instanz.

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.