Erste Schritte

SnapCenter software

NetApp
November 06, 2025

Inhalt

Erste Schritte

Erfahren Sie mehr über die SnapCenter software

SnapCenter -Übersicht

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, anwendungskonsistente, 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, die sich auf primären ONTAP FAS, AFF oder ASA Systemen befinden und auf sekundäre ONTAP FAS, AFF oder ASA Systeme repliziert werden
  - Daten, die sich auf primären ONTAP Select Systemen befinden
  - Daten, die sich auf primären und sekundären ONTAP FAS, AFF oder ASA -Systemen befinden und durch den lokalen StorageGRID Objektspeicher geschützt sind
  - Daten, die sich auf primären und sekundären ONTAP ASA r2-Systemen befinden
- Vor Ort in einer Hybrid Cloud zum Schutz der folgenden Elemente:
  - Daten, die sich auf primären ONTAP FAS, AFF oder ASA Systemen befinden und 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 öffentlichen Cloud zum Schutz der folgenden Elemente:
  - Daten, die sich auf primären Systemen von Cloud Volumes ONTAP (früher ONTAP Cloud) befinden
  - Daten, die sich auf Amazon FSX für ONTAP befinden
  - Daten, die sich auf primären Azure NetApp Files (Oracle, Microsoft SQL und SAP HANA) befinden

Hauptmerkmale

SnapCenter bietet die folgenden Hauptfunktionen:

- Zentralisierter, anwendungskonsistenter Datenschutz verschiedener Anwendungen

Der Datenschutz wird für Microsoft Exchange Server, Microsoft SQL Server, Oracle-Datenbanken unter Linux oder AIX, SAP HANA-Datenbanken, IBM Db2, PostgreSQL, MySQL und Windows-Host-Dateisysteme unterstützt, die auf ONTAP Systemen ausgeführt werden. SnapCenter unterstützt auch den Schutz von Anwendungen wie MongoDB, Storage, MaxDB, Sybase ASE, 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.

- Wiederherstellung und Wiederherstellung

  SnapCenter ermöglicht schnelle, granulare Wiederherstellungen von Backups und anwendungskonsistente, zeitbasierte Wiederherstellung. Sie können von jedem Ziel in der Hybrid Cloud wiederherstellen.

- 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-Cmdlets, UNIX-Befehle

  SnapCenter bietet REST-APIs für die meisten Funktionen zur Integration mit jeder Orchestrierungssoftware sowie zur Verwendung von Windows PowerShell-Cmdlets und der Befehlszeilenschnittstelle.

- Zentralisiertes Datenschutz-Dashboard und Reporting
- Rollenbasierte Zugriffskontrolle (RBAC) für Sicherheit und Delegation
- Eine integrierte Repository-Datenbank mit hoher Verfügbarkeit zum Speichern aller Backup-Metadaten
- Automatisierte Push-Installation von Plug-Ins
- Hohe Verfügbarkeit
- Notfallwiederherstellung (DR)
- SnapLock "Weitere Informationen"
- SnapMirror Active Sync (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC])
- Synchrone Spiegelung "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 umfasst 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 Anwendungen 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 zentralisierte HTML5-basierte Benutzeroberfläche, PowerShell-Cmdlets, REST-APIs und das SnapCenter Repository.

SnapCenter speichert Informationen zu seinen Vorgängen im SnapCenter -Repository.

SnapCenter -Plug-Ins

Jedes SnapCenter Plug-in unterstützt bestimmte Umgebungen, Datenbanken und Anwendungen.

Plug-in-Name	Im Installationspaket enthalten	Erfordert andere Plug-Ins	Auf dem Host installiert	Unterstützte Plattform
SnapCenter -Plug-In für Microsoft SQL Server	Plug-In-Paket für Windows	Plug-in für Windows	SQL Server-Host	Windows
SnapCenter -Plug-in für Windows	Plug-In-Paket für Windows		Windows-Host	Windows
SnapCenter -Plug-in für Microsoft Exchange Server	Plug-In-Paket für Windows	Plug-in für Windows	Exchange Server-Host	Windows
SnapCentre-Plug-in für Oracle-Datenbank	Plug-In-Paket für Linux und Plug-In-Paket für AIX	Plug-in für UNIX	Oracle-Host	Linux oder AIX
SnapCenter Plug-in für SAP HANA-Datenbank	Plug-In-Paket für Linux und Plug-In-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-In-Paket für Linux und Plug-In-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	Db2-Host	Linux, AIX oder Windows
SnapCenter -Plug-in für PostgreSQL	Plug-In-Paket für Linux und Plug-In-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	PostgreSQL-Host	Linux oder Windows
SnaoCenter-Plug-in für MySQL	Plug-In-Paket für Linux und Plug-In-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	MySQL-Host	Linux oder Windows

Plug-in-Name	Im Installationspaket enthalten	Erfordert andere Plug-Ins	Auf dem Host installiert	Unterstützte Plattform
SnapCenter -Plug-in für MongoDB	Plug-In-Paket für Linux und Plug-In-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	MongoDB-Host	Linux oder Windows
SnapCenter -Plug-in für ORASCPM (Oracle-Anwendungen)	Plug-In-Paket für Linux und Plug-In-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	Oracle-Host	Linux oder Windows
SnapCenter Plug-In für SAP ASE	Plug-In-Paket für Linux und Plug-In-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	SAP-Host	Linux oder Windows
SnapCenter -Plug-in für SAP MaxDB	Plug-In-Paket für Linux und Plug-In-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	SAP MaxDB-Host	Linux oder Windows
SnapCenter -Plug-in für Speicher-Plug-in	Plug-In-Paket für Linux und Plug-In-Paket für Windows	Plug-in für UNIX oder Plug-in für Windows	Speicherhost	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 "SnapCenter Plug-in for VMware vSphere Dokumentation" .

SnapCenter -Repository

Das SnapCenter Repository, manchmal auch als NSM-Datenbank bezeichnet, speichert Informationen und Metadaten für jeden SnapCenter Vorgang.

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 die folgenden Informationen und Metadaten:

- Metadaten sichern, klonen, wiederherstellen und überprüfen
- Berichts-, Job- und Ereignisinformationen

- Host- und Plug-in-Informationen
- Rollen-, Benutzer- und Berechtigungsdetails
- Informationen zur Speichersystemverbindung

Sicherheitsfunktionen in SnapCenter

SnapCenter verwendet strenge Sicherheits- und Authentifizierungsfunktionen, damit Ihre Daten geschützt bleiben.

SnapCenter umfasst die folgenden Sicherheitsfunktionen:

- Die gesamte Kommunikation mit SnapCenter erfolgt über HTTP über SSL (HTTPS).
- Alle Anmeldeinformationen in SnapCenter sind durch die Verschlüsselung Advanced Encryption Standard (AES) geschützt.
- Unterstützt Sicherheitsalgorithmen, die dem Federal Information Processing Standard (FIPS) entsprechen.
- Unterstützt die Verwendung der vom Kunden bereitgestellten autorisierten CA-Zertifikate.
- Unterstützt Transport Layer Security (TLS) 1.3 für die Kommunikation mit ONTAP. Sie können TLS 1.2 auch für die Kommunikation zwischen Clients und Servern verwenden.
- Unterstützt einen bestimmten Satz von SSL-Verschlüsselungssammlungen, um Sicherheit bei der Netzwerkkommunikation zu gewährleisten. "Mehr erfahren" .
- SnapCenter wird innerhalb der Firewall Ihres Unternehmens installiert, um den Zugriff auf den SnapCenter -Server und die Kommunikation zwischen dem SnapCenter -Server und den Plug-Ins zu ermöglichen.
- Für den Zugriff auf die SnapCenter -API und -Operationen werden mit AES-Verschlüsselung verschlüsselte Token verwendet, die nach 24 Stunden ablaufen.
- SnapCenter lässt sich in Windows Active Directory integrieren, um die Anmeldung und die rollenbasierte Zugriffskontrolle (RBAC) zu ermöglichen, die die Zugriffsberechtigungen regelt.
- IPsec wird mit SnapCenter auf ONTAP für Windows- und Linux-Hostmaschinen unterstützt. "Mehr erfahren" .
- SnapCenter PowerShell-Cmdlets sind sitzungsgesichert.
- Nach einer standardmäßigen Inaktivitätszeit von 15 Minuten warnt Sie SnapCenter , dass Sie in 5 Minuten abgemeldet werden.

  Nach 20 Minuten Inaktivität meldet SnapCenter Sie ab und Sie müssen sich erneut anmelden. Sie können den Abmeldezeitraum ändern.

- Nach 5 falschen Anmeldeversuchen wird die Anmeldung vorübergehend deaktiviert.
- Unterstützt die CA-Zertifikatauthentifizierung zwischen SnapCenter Server und ONTAP. "Mehr erfahren" .
- Integrity Verifier wird dem SnapCenter -Server und den Plug-Ins hinzugefügt und validiert alle mitgelieferten Binärdateien während Neuinstallations- und Upgradevorgängen.

CA-Zertifikatübersicht

Das SnapCenter Server-Installationsprogramm aktiviert während der Installation die zentrale SSL-Zertifikatunterstützung. Um die sichere Kommunikation zwischen dem Server und dem Plug-in zu verbessern, unterstützt SnapCenter die Verwendung der vom Kunden bereitgestellten autorisierten CA-Zertifikate.

Sie sollten CA-Zertifikate nach der Installation des SnapCenter -Servers und der entsprechenden Plug-Ins

bereitstellen. Weitere Informationen finden Sie unter "CA-Zertifikat-CSR-Datei generieren" .

Sie können auch ein CA-Zertifikat für das SnapCenter -Plug-In für VMware vSphere bereitstellen. Weitere Informationen finden Sie unter "Zertifikate erstellen und importieren" .

Zweiwege-SSL-Kommunikation

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

Übersicht über die zertifikatbasierte Authentifizierung

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

Multi-Faktor-Authentifizierung (MFA)

MFA verwendet einen Identitätsanbieter (IdP) eines Drittanbieters über die Security Assertion Markup Language (SAML), um Benutzersitzungen zu verwalten. Diese Funktion verbessert die Authentifizierungssicherheit durch die Möglichkeit, neben dem vorhandenen Benutzernamen und Kennwort mehrere Faktoren wie TOTP, Biometrie, Push-Benachrichtigungen usw. zu verwenden. Darüber hinaus ermöglicht es dem Kunden, seine eigenen Benutzeridentitätsanbieter zu verwenden, um eine einheitliche Benutzeranmeldung (SSO) für sein gesamtes Portfolio zu erhalten.

MFA ist nur für die Anmeldung bei der SnapCenter Server-Benutzeroberfläche anwendbar. Die Anmeldungen werden über die IdP Active Directory Federation Services (AD FS) authentifiziert. Sie können bei AD FS verschiedene Authentifizierungsfaktoren konfigurieren. SnapCenter ist der Dienstanbieter und Sie sollten SnapCenter als vertrauende Partei in AD FS konfigurieren. Um MFA in SnapCenter zu aktivieren, benötigen Sie die AD FS-Metadaten.

Informationen zum Aktivieren von MFA finden Sie unter"Aktivieren Sie die Multi-Faktor-Authentifizierung" .

Rollenbasierte Zugriffskontrolle in SnapCenter

Die rollenbasierte Zugriffskontrolle (RBAC) und ONTAP Berechtigungen von SnapCenter ermöglichen es SnapCenter Administratoren, die Kontrolle über SnapCenter -Ressourcen an verschiedene Benutzer oder Benutzergruppen zu delegieren. Dieser zentral verwaltete Zugriff ermöglicht Anwendungsadministratoren, sicher in delegierten Umgebungen zu arbeiten.

Sie können jederzeit Rollen erstellen und ändern und Benutzern Ressourcenzugriff gewähren. Wenn Sie SnapCenter jedoch zum ersten Mal einrichten, sollten Sie zumindest Active Directory-Benutzer oder -Gruppen zu Rollen hinzufügen und diesen Benutzern oder Gruppen dann Ressourcenzugriff gewähren.

> Sie können SnapCenter nicht zum Erstellen von Benutzer- oder Gruppenkonten verwenden. Sie sollten Benutzer- oder Gruppenkonten im Active Directory des Betriebssystems oder der Datenbank erstellen.

Arten von RBAC in SnapCenter

SnapCenter verwendet die folgenden Arten der rollenbasierten Zugriffskontrolle:

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

SnapCenter RBAC

SnapCenter verfügt über vordefinierte Rollen und Sie können diesen Rollen Benutzer oder Benutzergruppen zuweisen. Die vordefinierten Rollen sind:

- SnapCenter -Administratorrolle
- Rolle „App-Backup und -Klon-Administrator“
- Rolle „Backup- und Klon-Viewer“
- Rolle des Infrastrukturadministrators

Wenn Sie einem Benutzer eine Rolle zuweisen, werden auf der Seite „Jobs“ nur die für diesen Benutzer relevanten Jobs angezeigt, es sei denn, Sie haben ihm die Rolle „SnapCenterAdmin“ zugewiesen.

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

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

> Wenn Sie eine benutzerdefinierte Rolle erstellen, muss diese alle Berechtigungen der SnapCenterAdmin-Rolle enthalten. Wenn Sie nur einige der Berechtigungen kopieren, beispielsweise „Host hinzufügen“ oder „Host entfernen“, können Sie diese Vorgänge nicht ausführen.

Benutzer müssen sich bei der Anmeldung über die grafische Benutzeroberfläche (GUI) oder mithilfe von PowerShell-Cmdlets authentifizieren. Wenn Benutzer Mitglieder mehrerer Rollen sind, werden sie nach der Eingabe der Anmeldeinformationen aufgefordert, die Rolle anzugeben, die sie verwenden möchten. Benutzer müssen sich außerdem authentifizieren, um die APIs auszuführen.

RBAC auf Anwendungsebene

SnapCenter verwendet Anmeldeinformationen, um zu überprüfen, ob autorisierte SnapCenter Benutzer auch über Berechtigungen auf Anwendungsebene verfügen.

Wenn Sie beispielsweise Datenschutzvorgänge in einer SQL Server-Umgebung durchführen möchten, müssen Sie die Anmeldeinformationen mit den richtigen Windows- oder SQL-Anmeldeinformationen festlegen. Der SnapCenter -Server authentifiziert die festgelegten Anmeldeinformationen mit einer der beiden Methoden. 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 im 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 for VMware vSphere RBAC

Wenn Sie das SnapCenter VMware-Plug-In für VM-konsistenten Datenschutz verwenden, bietet der vCenter Server eine zusätzliche RBAC-Ebene. Das SnapCenter VMware-Plug-in unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC. "Weitere Informationen"

Best Practice: 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"

Den vordefinierten SnapCenter -Rollen zugewiesene Berechtigungen

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

Beispielsweise kann ein Benutzer mit der SnapCenter -Administratorrolle SVM-Verbindungen erstellen und sie einem Benutzer mit der Rolle „App Backup and Clone Admin“ zuweisen, der standardmäßig nicht über die Berechtigung zum Erstellen oder Bearbeiten von SVM-Verbindungen verfügt. Ohne eine SVM-Verbindung können Benutzer keine Sicherungs-, Klon- oder Wiederherstellungsvorgänge durchführen.

SnapCenter -Administratorrolle

Für die 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.

Rolle „App-Backup und -Klon-Administrator“

Die Rolle „App-Backup- und -Klon-Administrator“ verfügt über die erforderlichen Berechtigungen zum Ausführen administrativer Aktionen für Anwendungs-Backups und klonbezogene Aufgaben. Diese Rolle verfügt nicht über Berechtigungen für Hostverwaltung, Bereitstellung, Speicherverbindungsverwaltung oder Remoteinstallation.

Berechtigungen	Ermöglicht	Erstellen	Lesen	Aktualisieren	Löschen
Ressourcengruppe	Nicht zutreffend	Ja	Ja	Ja	Ja
Politik	Nicht zutreffend	Ja	Ja	Ja	Ja
Sicherung	Nicht zutreffend	Ja	Ja	Ja	Ja
Gastgeber	Nicht zutreffend	Ja	Ja	Ja	Ja

Berechtigungen	Ermöglicht	Erstellen	Lesen	Aktualisieren	Löschen
Speicherverbindung	Nicht zutreffend	Nein	Ja	Nein	Nein
Klonen	Nicht zutreffend	Ja	Ja	Ja	Ja
Bestimmung	Nicht zutreffend	Nein	Ja	Nein	Nein
Dashboard	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Berichte	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Wiederherstellen	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Ressource	Ja	Ja	Ja	Ja	Ja
Plug-in installieren/deinstallieren	Nein	Nicht zutreffend		Nicht zutreffend	Nicht zutreffend
Migration	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Montieren	Ja	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Aushängen	Ja	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Vollständige Volume-Wiederherstellung	Nein	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Sekundärschutz	Nein	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Job-Monitor	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Rolle „Backup- und Klon-Viewer“

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

Berechtigungen	Ermöglicht	Erstellen	Lesen	Aktualisieren	Löschen
Ressourcengruppe	Nicht zutreffend	Nein	Ja	Nein	Nein

Berechtigungen	Ermöglicht	Erstellen	Lesen	Aktualisieren	Löschen
Politik	Nicht zutreffend	Nein	Ja	Nein	Nein
Sicherung	Nicht zutreffend	Nein	Ja	Nein	Nein
Gastgeber	Nicht zutreffend	Nein	Ja	Nein	Nein
Speicherverbindung	Nicht zutreffend	Nein	Ja	Nein	Nein
Klonen	Nicht zutreffend	Nein	Ja	Nein	Nein
Bestimmung	Nicht zutreffend	Nein	Ja	Nein	Nein
Dashboard	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Berichte	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Wiederherstellen	Nein	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Ressource	Nein	Nein	Ja	Ja	Nein
Plug-in installieren/deinstallieren	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Migration	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Montieren	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Aushängen	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Vollständige Volume-Wiederherstellung	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Sekundärschutz	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Job-Monitor	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Rolle des Infrastrukturadministrators

Die Rolle „Infrastrukturadministrator“ verfügt über Berechtigungen für Hostverwaltung, Speicherverwaltung, Bereitstellung, Ressourcengruppen, Remote-Installationsberichte und Zugriff auf das Dashboard.

Berechtigungen	Ermöglicht	Erstellen	Lesen	Aktualisieren	Löschen
Ressourcengruppe	Nicht zutreffend	Ja	Ja	Ja	Ja
Politik	Nicht zutreffend	Nein	Ja	Ja	Ja
Sicherung	Nicht zutreffend	Ja	Ja	Ja	Ja
Gastgeber	Nicht zutreffend	Ja	Ja	Ja	Ja
Speicherverbindung	Nicht zutreffend	Ja	Ja	Ja	Ja
Klonen	Nicht zutreffend	Nein	Ja	Nein	Nein
Bestimmung	Nicht zutreffend	Ja	Ja	Ja	Ja
Dashboard	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Berichte	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Wiederherstellen	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Ressource	Ja	Ja	Ja	Ja	Ja
Plug-in installieren/deinstallieren	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Migration	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Montieren	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Aushängen	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Vollständige Volume-Wiederherstellung	Nein	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Sekundärschutz	Nein	Nein	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Job-Monitor	Ja	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Notfallwiederherstellung in SnapCenter

Mit der Disaster Recovery-Funktion (DR) von SnapCenter können Sie sich von Katastrophen wie Ressourcenbeschädigungen oder Serverabstürzen erholen. Es hilft bei der Wiederherstellung des SnapCenter Repositorys, der Serverpläne, der Konfigurationskomponenten und des SnapCenter -Plug-ins für SQL Server und seines Speichers.

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

SnapCenter Server DR

- SnapCenter Server-Daten werden gesichert und können wiederhergestellt werden, ohne dass dem SnapCenter Server ein Plug-In hinzugefügt oder von diesem verwaltet werden muss.
- Der sekundäre SnapCenter -Server sollte im selben Installationsverzeichnis und auf demselben Port wie der primäre SnapCenter -Server installiert werden.
- Schließen Sie für die Multi-Faktor-Authentifizierung (MFA) während der SnapCenter Server-DR alle Browser-Registerkarten und öffnen Sie einen Browser erneut, um sich erneut anzumelden. Dadurch werden die vorhandenen oder aktiven Sitzungscookies gelöscht und die richtigen Konfigurationsdaten aktualisiert.
- Die Notfallwiederherstellungsfunktion von SnapCenter verwendet REST-APIs zum Sichern des SnapCenter -Servers. Sehen "REST-API-Workflows für die Notfallwiederherstellung von SnapCenter Server" .
- Die Konfigurationsdatei mit den Überwachungseinstellungen wird weder im DR-Backup noch auf dem DR-Server nach dem Wiederherstellungsvorgang gesichert. Sie sollten die Audit-Protokolleinstellungen manuell wiederholen.

SnapCenter Plug-in und Storage DR

DR ist nur für das SnapCenter -Plug-in für SQL Server verfügbar. Wenn das Plug-In ausgefallen ist, wechseln Sie zu einem anderen SQL-Host und stellen Sie die Daten mithilfe einiger Schritte wieder her. Sehen "Notfallwiederherstellung des SnapCenter -Plug-ins für SQL Server" .

SnapCenter verwendet ONTAP SnapMirror zum Replizieren von Daten, was für DR verwendet werden kann, indem die Daten an einem sekundären Standort synchronisiert bleiben. Um ein Failover einzuleiten, unterbrechen Sie die SnapMirror -Replikation. Kehren Sie während des Fallbacks die Synchronisierung um, um Daten vom DR-Standort zurück zum primären Standort zu replizieren.

Von SnapCenter benötigte Lizenzen

SnapCenter erfordert mehrere Lizenzen, um den Datenschutz von Anwendungen, Datenbanken, Dateisystemen und virtuellen Maschinen zu ermöglichen. Die Art der SnapCenter -Lizenzen, die Sie installieren, hängt von Ihrer Speicherumgebung und den Funktionen ab, die Sie verwenden möchten.

Lizenz	Wo erforderlich
SnapCenter Standard-Controller-basiert	Erforderlich für FAS, AFF, ASA Die SnapCenter Standard-Lizenz ist eine Controller-basierte Lizenz und ist Teil von NetApp ONTAP One. Wenn Sie über die SnapManager Suite-Lizenz verfügen, erhalten Sie auch die SnapCenter Standard-Lizenzberechtigung. Wenn Sie SnapCenter auf Testbasis mit FAS, AFF oder ASA -Speicher installieren möchten, können Sie eine Evaluierungslizenz für NetApp ONTAP One erhalten, indem Sie sich an den Vertriebsmitarbeiter wenden. Informationen zu den in NetApp ONTAP One enthaltenen Lizenzen finden Sie unter "In NetApp ONTAP One enthaltene Lizenzen" . SnapCenter wird auch als Teil eines Datenschutzpakets angeboten. Wenn Sie A400 oder höher gekauft haben, sollten Sie das Datenschutzpaket erwerben.
SnapMirror oder SnapVault	ONTAP Wenn die Replikation in SnapCenter aktiviert ist, ist entweder eine SnapMirror oder eine SnapVault -Lizenz erforderlich.
SnapRestore	Erforderlich zum Wiederherstellen und Überprüfen von Sicherungen. Auf primären Speichersystemen • Erforderlich auf SnapVault -Zielsystemen, um eine Remote-Überprüfung durchzuführen und aus einer Sicherung wiederherzustellen. • Erforderlich auf SnapMirror Zielsystemen, um eine Remote-Verifizierung durchzuführen.

Lizenz	Wo erforderlich
FlexClone	Erforderlich zum Klonen von Datenbanken und für Überprüfungsvorgänge. Auf primären und sekundären Speichersystemen • Erforderlich auf SnapVault -Zielsystemen, um Klone aus der sekundären Tresorsicherung zu erstellen. • Erforderlich auf SnapMirror Zielsystemen, um Klone aus sekundären SnapMirror Backups zu erstellen.
Protokolllizenzen	• iSCSI- oder FC-Lizenz für LUNs • CIFS-Lizenz für SMB-Freigaben • NFS-Lizenz für VMDKs vom Typ NFS • iSCSI- oder FC-Lizenz für VMDKs vom Typ VMFS Erforderlich auf SnapMirror Zielsystemen, um Daten bereitzustellen, wenn kein Quellvolume verfügbar ist.
SnapCenter Standard-Lizenzen (optional)	Sekundärziele Es wird empfohlen, ist aber nicht erforderlich, dass Sie SnapCenter Standard-Lizenzen zu sekundären Zielen hinzufügen. Wenn SnapCenter Standard-Lizenzen auf sekundären Zielen nicht aktiviert sind, können Sie SnapCenter nach der Durchführung eines Failover-Vorgangs nicht zum Sichern von Ressourcen auf dem sekundären Ziel verwenden. Auf sekundären Zielen ist jedoch eine FlexClone -Lizenz erforderlich, um Klon- und Überprüfungsvorgänge durchzuführen.

Lizenz	Wo erforderlich
Single Mailbox Recovery (SMBR)-Lizenzen	Wenn Sie das SnapCenter -Plug-in für Exchange zum Verwalten von Microsoft Exchange Server-Datenbanken und Single Mailbox Recovery (SMBR) verwenden, benötigen Sie eine zusätzliche Lizenz für SMBR, die je nach Benutzerpostfach separat erworben werden muss. Die Verfügbarkeit von NetApp® Single Mailbox Recovery (EOA) endet am 12. Mai 2023. Weitere Informationen finden Sie unter"CPC-00507" . NetApp wird Kunden, die Postfachkapazität, Wartung und Support über die am 24. Juni 2020 eingeführten Marketing-Teilenummern erworben haben, für die Dauer des Supportanspruchs weiterhin unterstützen. NetApp Single Mailbox Recovery ist ein Partnerprodukt von Ontrack. Ontrack PowerControls bietet ähnliche Funktionen wie NetApp Single Mailbox Recovery. Kunden können neue Ontrack PowerControls-Softwarelizenzen sowie Wartungs- und Supportverlängerungen für Ontrack PowerControls von Ontrack (über licensingteam@ontrack.com) für eine detaillierte Postfachwiederherstellung nach dem EOA-Datum (12. Mai 2023) erwerben.

Die Lizenzen für SnapCenter Advanced und SnapCenter NAS File Services sind veraltet und nicht mehr verfügbar. Die Standardlizenz und die kapazitätsbasierte Lizenz sind für Amazon FSx for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP und Azure NetApp Files nicht mehr erforderlich.

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

SnapMirror Active Sync in SnapCenter

SnapMirror Active Sync ermöglicht die Weiterführung des Betriebs von Geschäftsdiensten auch bei einem vollständigen Site-Ausfall und unterstützt Anwendungen bei einem transparenten Failover mithilfe einer sekundären Kopie. Um mit SnapMirror Active Sync ein Failover auszulösen, sind weder manuelle Eingriffe noch zusätzliche Skripts erforderlich.

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

Stellen Sie für die aktive Synchronisierung von SnapMirror sicher, dass Sie die verschiedenen Hardware-, Software- und Systemkonfigurationsanforderungen erfüllt haben. Weitere Informationen finden Sie unter "Voraussetzungen"

Die für diese Funktion unterstützten Plug-ins sind SnapCenter Plug-in für SQL Server, SnapCenter Plug-in für Windows, SnapCenter Plug-in für Oracle-Datenbanken, SnapCenter Plug-in für SAP HANA-Datenbanken,

SnapCenter Plug-in für Microsoft Exchange Server und SnapCenter Plug-in für Unix.

Um die Host-Initiator-Nähe in SnapCenter zu unterstützen, sollte der Wert, entweder Quelle oder Ziel, in ONTAP festgelegt werden.

Die in SnapCenter nicht unterstützten Anwendungsfälle:

- Wenn Sie die vorhandenen asymmetrischen SnapMirror Active Sync-Workloads in symmetrische umwandeln, indem Sie die Richtlinie für die SnapMirror Active Sync-Beziehungen in ONTAP von *automatedfailover* in *automatedfailoverduplex* ändern, wird dies in SnapCenter nicht unterstützt.
- Wenn Sicherungen einer Ressourcengruppe vorhanden sind (bereits in SnapCenter geschützt) und dann die Speicherrichtlinie für die SnapMirror -Active-Sync-Beziehungen von *automatedfailover* in *automatedfailoverduplex* in ONTAP geändert wird, wird dies in SnapCenter nicht unterstützt.

Schlüsselbegriffe des Datenschutzes

Machen Sie sich vor der Verwendung von SnapCenter mit den wichtigsten Konzepten für Sicherung, Klonen und Wiederherstellen vertraut.

Ressourcen

Zu den Ressourcen gehören Datenbanken, Windows-Dateisysteme oder Dateifreigaben, die mit SnapCenter gesichert oder geklont wurden. Abhängig von Ihrer Umgebung können Ressourcen auch Datenbankinstanzen, SQL Server-Verfügbarkeitsgruppen, Oracle-Datenbanken, RAC-Datenbanken oder benutzerdefinierte Anwendungsgruppen sein.

Ressourcengruppe

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Cluster, möglicherweise von mehreren Hosts und Clustern. An einer Ressourcengruppe ausgeführte Vorgänge gelten für alle darin enthaltenen Ressourcen basierend auf dem angegebenen Zeitplan. 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 bestimmte Ressourcen zu sichern: Datenbank-Plug-ins für Datenbanken, Dateisystem-Plug-ins für Dateisysteme und das SnapCenter Plug-in for VMware vSphere für VMs und Datenspeicher.

Richtlinien

Richtlinien legen die Sicherungshäufigkeit, die Aufbewahrung von Kopien, Replikation, Skripts und andere Merkmale von Datenschutzvorgängen fest.

Beim Erstellen einer Ressourcengruppe oder beim Durchführen einer On-Demand-Sicherung können eine oder mehrere Richtlinien ausgewählt werden.

Eine Ressourcengruppe definiert, was geschützt werden muss und wann es hinsichtlich Tag und Uhrzeit geschützt werden soll. Eine Richtlinie beschreibt, wie der Schutz umgesetzt wird. Wenn beispielsweise eine Sicherung aller Datenbanken oder Dateisysteme eines Hosts erforderlich ist, kann eine Ressourcengruppe erstellt werden, die alle Datenbanken oder Dateisysteme auf dem Host umfasst. Der Ressourcengruppe könnten dann zwei Richtlinien zugeordnet werden: eine Tagesrichtlinie und eine Stundenrichtlinie.

Beim Erstellen der Ressourcengruppe und Anhängen der Richtlinien ist es möglich, sie so zu konfigurieren, dass täglich eine vollständige Sicherung und stündlich ein weiterer Zeitplan für Protokollsicherungen durchgeführt wird.

Bei Datenschutzvorgängen können benutzerdefinierte Prescripts und Postscripts verwendet werden. Diese Skripte ermöglichen eine Automatisierung entweder vor oder nach dem Datenschutzjob. Beispielsweise könnte ein Skript automatisch über Fehler oder Warnungen bei Datenschutzaufträgen informieren. Bevor Sie Präskripte und Postskripte einrichten, ist es wichtig, die Anforderungen zum Erstellen dieser Skripte zu verstehen.

Verwendung von Präskripten und Postskripten

Benutzerdefinierte Prescripts und Postscripts können Ihre Datenschutzaufgaben vor oder nach dem Job automatisieren. Sie können beispielsweise ein Skript hinzufügen, das Sie über Jobfehler oder Warnungen benachrichtigt. Stellen Sie vor der Einrichtung sicher, dass Sie die Anforderungen für diese Skripte verstehen.

Unterstützte Skripttypen

Die folgenden Skripttypen werden für Windows unterstützt:

- Batchdateien
- PowerShell-Skripts
- Perl-Skripte

Für UNIX werden die folgenden Skripttypen unterstützt:

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

> Neben der Standard-Bash-Shell werden auch andere Shells wie SH-Shell, K-Shell und C-Shell unterstützt.

Skriptpfad

Alle Prescripts und Postscripts, die als Teil von SnapCenter -Vorgängen auf nicht virtualisierten und virtualisierten Speichersystemen ausgeführt werden, werden auf dem Plug-In-Host ausgeführt.

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

> Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben 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.

Wo Skripte angegeben werden

Skripte werden in Sicherungsrichtlinien angegeben. Wenn ein Sicherungsauftrag gestartet wird, verknüpft die Richtlinie das Skript automatisch mit den zu sichernden Ressourcen. Wenn Sie eine Sicherungsrichtlinie

erstellen, können Sie die Prescript- und Postscript-Argumente angeben.

Sie können nicht mehrere Skripte angeben.

Skript-Timeouts

Das Timeout ist standardmäßig auf 60 Sekunden eingestellt. Sie können den Timeout-Wert ändern.

Skriptausgabe

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

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

Von SnapCenter unterstützte Speichersysteme und Anwendungen

Sie sollten die von SnapCenter unterstützten Speichersysteme, Anwendungen und Datenbanken kennen.

Unterstützte Speichersysteme

- NetApp ONTAP 9.12.1 und höher
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

  Unterstützt Non-Volatile Memory Express (NVMe) über Transport Control Protocol (TCP).

  Informationen zu Amazon FSx for NetApp ONTAP finden Sie unter "Amazon FSx for NetApp ONTAP -Dokumentation" .

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

Unterstützte Anwendungen und Datenbanken

SnapCenter unterstützt den Schutz verschiedener Anwendungen und Datenbanken. Ausführliche Informationen zu den unterstützten Anwendungen und Datenbanken finden Sie unter "NetApp Interoperabilitätsmatrix-Tool" .

SnapCenter unterstützt den Schutz von Oracle- und Microsoft SQL-Workloads in VMware Cloud auf Amazon Web Services (AWS) Software-Defined Data Center (SDDC)-Umgebungen. "Weitere Informationen" .

Authentifizierungsmethoden für SnapCenter -Anmeldeinformationen

Für Anmeldeinformationen werden je nach Anwendung oder Umgebung unterschiedliche Authentifizierungsmethoden verwendet. Anmeldeinformationen authentifizieren Benutzer, damit sie SnapCenter -Vorgänge ausführen können. Sie sollten einen Satz Anmeldeinformationen für die Installation von Plug-Ins und einen anderen für Datenschutzvorgänge erstellen.

Windows-Authentifizierung

Die Windows-Authentifizierungsmethode authentifiziert sich gegenüber Active Directory. Für die Windows-Authentifizierung wird Active Directory außerhalb von SnapCenter eingerichtet. SnapCenter authentifiziert ohne zusätzliche Konfiguration. Sie benötigen Windows-Anmeldeinformationen, um Hosts hinzuzufügen, Plug-In-Pakete zu installieren und Jobs zu planen.

Nicht vertrauenswürdige Domänenauthentifizierung

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

Lokale Arbeitsgruppenauthentifizierung

SnapCenter ermöglicht die Erstellung von Windows-Anmeldeinformationen mit lokalen Arbeitsgruppenbenutzern und -gruppen. Die Windows-Authentifizierung für lokale Arbeitsgruppenbenutzer und -gruppen erfolgt nicht während der Erstellung der Windows-Anmeldeinformationen, sondern wird verschoben, bis die Hostregistrierung und andere Hostvorgänge durchgeführt werden.

SQL Server-Authentifizierung

Die SQL-Authentifizierungsmethode authentifiziert sich gegenüber einer SQL Server-Instanz. Dies bedeutet, dass in SnapCenter eine SQL Server-Instanz 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 die Planung auf SQL Server oder die Ermittlung von Ressourcen durchzuführen.

Linux-Authentifizierung

Die Linux-Authentifizierungsmethode authentifiziert sich gegenüber einem Linux-Host. Sie benötigen eine Linux-Authentifizierung während des ersten Schritts, bei dem Sie den Linux-Host hinzufügen und das SnapCenter Plug-Ins-Paket für Linux remote über die SnapCenter -GUI installieren.

AIX-Authentifizierung

Die AIX-Authentifizierungsmethode authentifiziert gegenüber einem AIX-Host. Sie benötigen eine AIX-Authentifizierung während des ersten Schritts, bei dem Sie den AIX-Host hinzufügen und das SnapCenter Plug-Ins-Paket für AIX remote über die SnapCenter -GUI installieren.

Oracle-Datenbankauthentifizierung

Die Oracle-Datenbankauthentifizierungsmethode authentifiziert gegenüber einer Oracle-Datenbank. Sie benötigen eine Oracle-Datenbankauthentifizierung, um Vorgänge an der Oracle-Datenbank auszuführen, wenn die Betriebssystemauthentifizierung (OS) auf dem Datenbankhost deaktiviert ist. Bevor Sie Anmeldeinformationen für eine Oracle-Datenbank hinzufügen, sollten Sie daher einen Oracle-Benutzer mit Sysdba-Berechtigungen in der Oracle-Datenbank erstellen.

Oracle ASM-Authentifizierung

Die Oracle ASM-Authentifizierungsmethode authentifiziert sich gegenüber einer Oracle Automatic Storage Management (ASM)-Instanz. Die Oracle ASM-Authentifizierung ist erforderlich, wenn Sie auf eine Oracle ASM-Instanz zugreifen müssen und die Betriebssystemauthentifizierung auf dem Datenbankhost deaktiviert ist. Erstellen Sie vor dem Hinzufügen einer Oracle ASM-Anmeldeinformation einen Oracle-Benutzer mit

Systemberechtigungen in der ASM-Instanz.

RMAN-Katalogauthentifizierung

Die RMAN-Katalogauthentifizierungsmethode authentifiziert sich gegenüber der Oracle Recovery Manager (RMAN)-Katalogdatenbank. Wenn Sie einen externen Katalogmechanismus konfiguriert und Ihre Datenbank bei der Katalogdatenbank registriert haben, müssen Sie die RMAN-Katalogauthentifizierung hinzufügen.

Unterstützte SnapCenter -Vorgänge für ASA r2-Systeme

ASA r2-Speichersysteme werden ab SnapCenter 6.1 unterstützt. "Erfahren Sie mehr über ASA r2-Systeme"

SnapCenter nutzt REST-APIs, um alle Vorgänge auf ASA r2-Systemen auszuführen, die ZAPIs nicht unterstützen.

Von SnapCenter für ASA r2-Systeme unterstützte Vorgänge

- Erstellen primärer Backups von Anwendungen über VMDK
- Übertragen von Konsistenzgruppen-Snapshots auf ein sekundäres Speichersystem
- Wiederherstellen der Backups von primären und sekundären Speichersystemen auf dem ursprünglichen Host oder dem alternativen Host
  - In-Place-Wiederherstellung von primären und sekundären Speichersystemen mit VMware vMotion
  - Verbinden und Kopieren und Wiederherstellen von primären und sekundären Speichersystemen
- Klonen der Backups auf den ursprünglichen Host oder auf den alternativen Host

SnapCenter kann ONTAP Konsistenzgruppen erkennen oder erstellen. Es kann außerdem SnapMirror -Beziehungen zum Zielcluster für sekundären Schutz bereitstellen und initialisieren.

Informationen zum Aktivieren des sekundären Schutzes auf ASA R2-Systemen für Ihre Anwendung finden Sie unter:

- "Aktivieren Sie den sekundären Schutz für Microsoft SQL Server-Ressourcen"
- "Aktivieren Sie den sekundären Schutz für SAP HANA-Ressourcen"
- "Aktivieren Sie den sekundären Schutz für Oracle-Ressourcen"
- "Aktivieren Sie den sekundären Schutz für Windows-Dateisysteme"
- "Aktivieren Sie den sekundären Schutz für IBM Db2-Ressourcen"
- "Aktivieren Sie den sekundären Schutz für PostgreSQL-Ressourcen"
- "Aktivieren Sie den sekundären Schutz für MySQL-Ressourcen"
- "Aktivieren Sie den sekundären Schutz für Unix-Dateisysteme"

Vorgänge, die von SnapCenter für ASA r2-Systeme nicht unterstützt werden

- Raw Device Mapping (RDM)
- Anwendungsvolumes für Oracle
- SAP HANA NDV
- LockVault

- Manipulationssichere Schnappschüsse
- FlexGroup -Volumina
- Hierarchische Konsistenzgruppe
- Migration von ASA, AFF oder FAS Speichersystemen zu ASA r2-Speichersystemen
- Schutz von Datenbanken mit einer Mischung aus ASA, AFF oder FAS -Ressourcen und ASA r2-Ressourcen
- Umbenennen von Snapshots
- Sekundäre Bereitstellung des Protokollverzeichnisses des SQL-Plugin-Hosts

Schnellstart für die SnapCenter software

Die Kurzanleitung beschreibt die grundlegenden Schritte zur Installation und Konfiguration der SnapCenter software.

1 Vorbereiten der Installation von SnapCenter Server

Sie sollten sicherstellen, dass alle Anforderungen zur Installation des SnapCenter -Servers erfüllt sind.

- "Anforderungen"
- "Registrieren Sie sich, um auf die SnapCenter software zuzugreifen"
- "Aktivieren Sie die Multifaktor-Authentifizierung"

2 Installieren Sie SnapCenter Server

Der SnapCenter -Server kann entweder auf Windows- oder Linux-Hosts installiert werden. Laden Sie das SnapCenter Server-Installationspaket von der "NetApp Support Site" und führen Sie das Installationsprogramm aus.

- "Installieren Sie den SnapCenter -Server unter Windows"
- "Installieren Sie SnapCenter Server unter Linux"

3 SnapCenter Server konfigurieren

Nach der Installation des SnapCenter -Servers sollten Sie ihn entsprechend Ihrer Umgebung konfigurieren.

4 Installieren Sie das Plug-In für Ihre Anwendung

Stellen Sie sicher, dass alle Voraussetzungen für die Installation des anwendungsspezifischen Plug-ins je nach verwendeter Anwendung erfüllt sind, und fahren Sie dann mit der Installation des jeweiligen Plug-ins fort.

5 Schützen Sie Ihre Anwendung

Nach der erfolgreichen Installation des SnapCenter -Servers und der erforderlichen Plug-Ins können Sie mit der Erstellung von Anwendungssicherungen beginnen. Diese Backups können später bei Bedarf zur Wiederherstellung und zum Klonen verwendet werden.