Konzepte

SnapCenter Software 5.0

NetApp
July 18, 2024

Inhalt

Konzepte

Übersicht über SnapCenter

SnapCenter Software ist eine einfache, zentralisierte und skalierbare Plattform, die applikationskonsistenten Datenschutz für Applikationen, Datenbanken, Host-Filesysteme und VMs bietet, die auf ONTAP Systemen in der Hybrid Cloud ausgeführt werden.

SnapCenter bietet mithilfe von NetApp Snapshot, SnapRestore, FlexClone, SnapMirror und SnapVault Technologien folgende Vorteile:

- Schnelle, platzsparende, applikationskonsistente festplattenbasierte Backups
- Rasante, granulare Wiederherstellung und applikationskonsistente Recoverys
- Schnelles, platzsparendes Klonen

SnapCenter enthält sowohl SnapCenter Server als auch individuelle schlanke Plug-ins. Sie können die Implementierung von Plug-ins für Remote-Applikations-Hosts automatisieren, Backup-, Verifizierungs- und Klonvorgänge planen und alle Datensicherungsvorgänge überwachen.

Es gibt folgende Möglichkeiten für die Implementierung von SnapCenter:

- Lokal, um Folgendes zu schützen:
  - Daten auf primären ONTAP FAS-, AFF- oder All-SAN-Array- (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
- Lokal in einer Hybrid Cloud zur Sicherung folgender Komponenten:
  - Daten auf primären ONTAP FAS, AFF oder ASA Systemen, die auf Cloud Volumes ONTAP repliziert werden
  - Daten auf primären und sekundären ONTAP FAS-, AFF- oder ASA-Systemen, gesichert auf Objekt- und Archiv-Storage in der Cloud (mithilfe der BlueXP Backup- und Recovery-Integration)
- 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)

SnapCenter umfasst folgende Kernfunktionen:

- Zentralisierte, applikationskonsistente Datensicherung

  Datensicherung wird unterstützt für Microsoft Exchange Server, Microsoft SQL Server, Oracle Datenbanken auf Linux oder AIX, SAP HANA Datenbank und Windows Host Dateisysteme auf ONTAP Systemen.

  Datensicherung wird auch für andere standardmäßige oder benutzerdefinierte Applikationen und Datenbanken unterstützt, indem ein Framework für die Erstellung benutzerdefinierter SnapCenter Plug-ins

bereitgestellt wird. Dadurch wird die Datensicherung für andere Applikationen und Datenbanken über dieselbe zentrale Konsole ermöglicht. Durch die Nutzung dieses Frameworks hat NetApp benutzerdefinierte SnapCenter Plug-ins für IBM DB2, MongoDB, MySQL usw. im NetApp Automation Store veröffentlicht.

"NetApp Storage Automation Store"

- Richtlinienbasierte Backups

  Richtlinienbasierte Backups nutzen die NetApp Snapshot Technologie, um schnelle, platzsparende, applikationskonsistente, festplattenbasierte Backups zu erstellen. Optional können Sie den Schutz dieser Backups auf dem sekundären Storage durch Updates vorhandener Sicherungsbeziehungen automatisieren.

- Backups mehrerer Ressourcen

  Sie können mehrere Ressourcen (Applikationen, Datenbanken oder Host-Filesysteme) desselben Typs gleichzeitig mithilfe von SnapCenter Ressourcengruppen 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, applikationskonsistentes Klonen und damit eine beschleunigte Software-Entwicklung. Sie können Klone auf jedem beliebigen Ziel in der Hybrid Cloud erstellen.

- Grafische Benutzeroberfläche (GUI) zum Einzelmanagement

  Die SnapCenter Benutzeroberfläche bietet eine einheitliche, zentrale Benutzeroberfläche für das Management von Backups und Klonen einer Ressource in jedem beliebigen Ziel in der Hybrid Cloud.

- REST-APIs, Windows Commandlets und UNIX Befehle

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

  Weitere Informationen zu REST-APIs finden Sie unter "ÜBERSICHT ÜBER DIE REST-API".

  Weitere Informationen zu Windows-Cmdlets finden Sie unter "SnapCenter Software Cmdlet Referenzhandbuch".

  Weitere Informationen zu UNIX-Befehlen finden Sie unter "SnapCenter Software Command Reference Guide".

- Zentrale Datensicherungs-Konsole und Berichterstellung
- Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) für Sicherheit und Delegierung.
- Repository-Datenbank mit Hochverfügbarkeit

  SnapCenter bietet eine integrierte Repository-Datenbank mit Hochverfügbarkeit zum Speichern aller Backup-Metadaten.

- Automatisierte Push-Installation von Plug-ins

  Sie können einen Remote-Push von SnapCenter-Plug-ins vom SnapCenter Server Host an Applikations-Hosts automatisieren.

- Hochverfügbarkeit

  Hochverfügbarkeit für SnapCenter wird über externen Load Balancer (F5) eingerichtet. Im selben Datacenter werden bis zu zwei Nodes unterstützt.

- Disaster Recovery (DR)

  Bei einem Ausfall wie z. B. einer Ressourcenbeschädigung oder einem Server-Absturz können Sie den SnapCenter Server wiederherstellen.

- SnapLock

  SnapLock ist eine hochperformante Compliance-Lösung für Unternehmen, die mit WORM-Storage (Write Once, Read Many) Dateien aus gesetzlichen und Governance-Gründen in unveränderter Form aufbewahren.

  Weitere Informationen zu SnapLock finden Sie unter "Was ist SnapLock"

- SnapMirror Business Continuity (SM-BC)

  SnapMirror Business Continuity (SM-BC) sorgt dafür, dass die Business Services auch bei einem vollständigen Standortausfall weiterlaufen und Applikationen mithilfe einer sekundären Kopie einen transparenten Failover unterstützen. Zum Auslösen eines Failovers mit SM-BC sind weder manuelle Eingriffe noch zusätzliche Skripte erforderlich.

  Die für diese Funktion unterstützten Plug-ins sind das SnapCenter Plug-in für SQL Server, das SnapCenter Plug-in für Windows und das SnapCenter Plug-in für Oracle Database.

  Weitere Informationen zu SM-BC finden Sie unter "SnapMirror Business Continuity (SM-BC)"

  Stellen Sie für SM-BC sicher, dass Sie die verschiedenen Hardware-, Software- und Systemkonfigurationsanforderungen erfüllt haben. Weitere Informationen finden Sie unter "Voraussetzungen"

- Synchrones Spiegeln

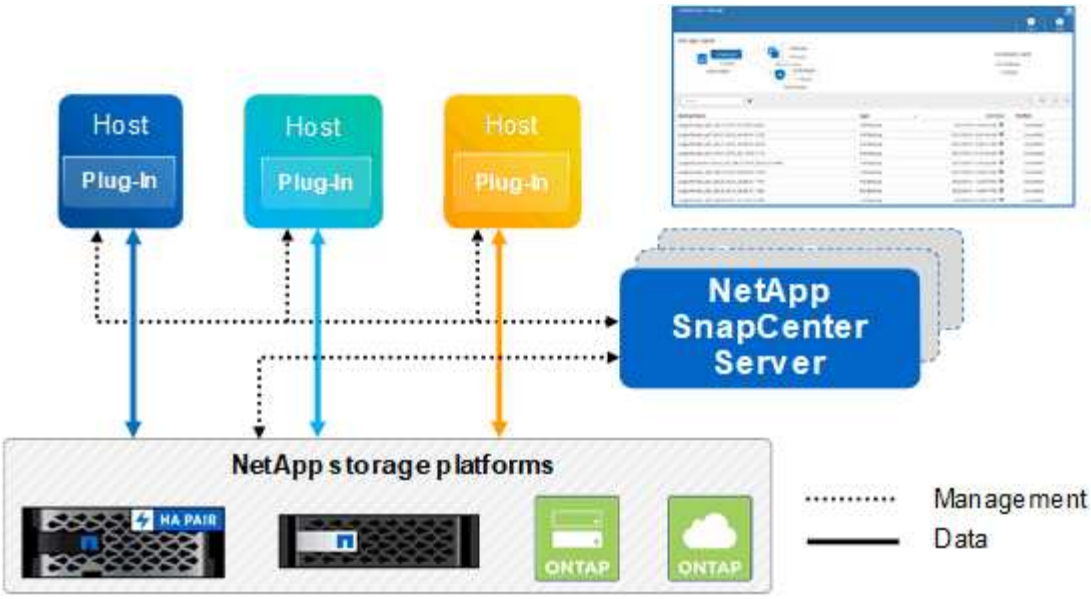
  Die Funktion für die synchrone Spiegelung ermöglicht eine Online-Datenreplizierung in Echtzeit zwischen Speicherarrays über Remote-Entfernungen.

  Weitere Informationen zur Sync-Spiegelung finden Sie unter "Übersicht über synchrones Spiegeln"

Architektur von SnapCenter

Die SnapCenter Plattform basiert auf einer mehrstufigen Architektur, die einen zentralen Management Server (SnapCenter Server) und einen SnapCenter Plug-in-Host umfasst.

SnapCenter unterstützt standortübergreifende Datacenter. Der SnapCenter-Server und der Plug-in-Host können sich an verschiedenen geografischen Standorten befinden.



Komponenten von SnapCenter

SnapCenter besteht aus SnapCenter Server und SnapCenter Plug-ins. Sie sollten nur die geeigneten Plug-ins für die Daten installieren, die Sie schützen möchten.

- SnapCenter Server
- Das SnapCenter Plug-ins-Paket für Windows enthält die folgenden Plug-ins:
  - SnapCenter Plug-in für Microsoft SQL Server
  - SnapCenter Plug-in für Microsoft Windows
  - SnapCenter Plug-in für Microsoft Exchange Server
  - SnapCenter-Plug-in für SAP HANA Database
- Das SnapCenter Plug-ins-Paket für Linux umfasst die folgenden Plug-ins:
  - SnapCenter Plug-in für Oracle Database
  - SnapCenter-Plug-in für SAP HANA Database
  - SnapCenter Plug-in für UNIX Filesysteme
- Das SnapCenter Plug-ins-Paket für AIX enthält die folgenden Plug-ins:
  - SnapCenter Plug-in für Oracle Database
  - SnapCenter Plug-in für UNIX Filesysteme
- Benutzerdefinierte SnapCenter Plug-ins

  Benutzerdefinierte Plug-ins werden von der Community unterstützt und können von der heruntergeladen werden "NetApp Storage Automation Store".

Das SnapCenter Plug-in für VMware vSphere, vormals NetApp Data Broker, ist eine eigenständige virtuelle Appliance, die SnapCenter Datensicherungsvorgänge auf virtualisierten Datenbanken und Filesystemen unterstützt.

SnapCenter Server

Der SnapCenter Server umfasst einen Webserver, eine zentralisierte HTML5-basierte Benutzeroberfläche, PowerShell Commandlets, REST-APIs und das SnapCenter Repository.

SnapCenter ermöglicht Hochverfügbarkeit und horizontale Skalierung über mehrere SnapCenter-Server hinweg in einer einzigen Benutzeroberfläche. Eine Hochverfügbarkeit ist über einen externen Load Balancer (F5) möglich. Bei größeren Umgebungen mit Tausenden von Hosts kann das Hinzufügen mehrerer SnapCenter Server zum Lastausgleich beitragen.

- Wenn Sie das SnapCenter-Plug-ins-Paket für Windows verwenden, wird der Host-Agent auf dem SnapCenter-Server und dem Windows-Plug-in-Host ausgeführt. Der Host-Agent führt die Zeitpläne nativ auf dem Remote-Windows-Host aus, oder für Microsoft SQL Server wird der Zeitplan auf der lokalen SQL-Instanz ausgeführt.

  Der SnapCenter-Server kommuniziert mit den Windows-Plug-ins über den Host-Agent.

- Wenn Sie das SnapCenter-Plug-ins-Paket für Linux oder das SnapCenter-Plug-ins-Paket für AIX verwenden, werden auf dem SnapCenter-Server Zeitpläne als Windows-Aufgabenpläne ausgeführt.
  - Für das SnapCenter-Plug-in für Oracle Database kommuniziert der Host-Agent, der auf dem SnapCenter Server-Host ausgeführt wird, mit dem SnapCenter-Plug-in-Loader (SPL), der auf dem Linux- oder AIX-Host ausgeführt wird, um verschiedene Datensicherungsvorgänge auszuführen.
  - Für das SnapCenter-Plug-in für SAP HANA-Datenbanken und benutzerdefinierte SnapCenter-Plug-ins kommuniziert der SnapCenter-Server mit diesen Plug-ins über den SCCore-Agent, der auf dem Host ausgeführt wird.

Der SnapCenter-Server und die Plug-ins kommunizieren mit dem Host-Agent über HTTPS. Informationen zu den Vorgängen von SnapCenter werden im SnapCenter Repository gespeichert.

SnapCenter unterstützt ungemeinsamen Namespace für Windows Hosts. Wenn Sie Probleme bei der Verwendung von ungemeinsamen Namespace haben, lesen Sie "SnapCenter kann bei Verwendung von nicht gemeinsamem Namespace keine Ressourcen erkennen".

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
Plug-in für SQL Server	Plug-ins-Paket für Windows	Plug-in für Windows	SQL Server Host	Windows
Plug-in für Windows	Plug-ins-Paket für Windows		Windows Host	Windows
Plug-in für Exchange	Plug-ins-Paket für Windows	Plug-in für Windows	Exchange Server Host	Windows

Plug-in-Name	Im Installationspaket enthalten	Weitere Plug-ins sind erforderlich	Auf dem Host installiert	Unterstützte Plattformen
Plug-in für Oracle Database	Plug-ins-Paket für Linux und Plug-ins-Paket für AIX	Plug-in für UNIX	Oracle Host	Linux oder AIX
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
Benutzerdefinierte Plug-ins	"NetApp Storage Automation Store"	Plug-in für Windows für File-System-Backups	Benutzerdefinierter Applikations-Host	Linux oder Windows

Das SnapCenter Plug-in für VMware vSphere unterstützt absturzkonsistente und VM-konsistente Backup- und Restore-Prozesse für Virtual Machines (VMs), Datastores und Virtual Machine Disks (VMDKs). Zudem unterstützt es die applikationsspezifischen Plug-ins von SnapCenter, um applikationskonsistente Backup- und Restore-Vorgänge für virtualisierte Datenbanken und Filesysteme zu sichern.

Für Nutzer von SnapCenter 4.1.1 enthält die Dokumentation zum SnapCenter Plug-in für VMware vSphere 4.1.1 Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen. Für Nutzer von SnapCenter 4.2.x, die NetApp Data Broker 1.0 und 1.0.1, enthält Dokumentation Informationen zum Schutz von virtualisierten Datenbanken und Dateisystemen mithilfe des SnapCenter Plug-ins für VMware vSphere, das durch die Linux-basierte NetApp Data Broker Virtual Appliance (Open Virtual Appliance Format) bereitgestellt wird. Für Benutzer, die SnapCenter 4.3 oder höher verwenden, enthält das "Dokumentation zum SnapCenter Plug-in für VMware vSphere" Informationen zum Schutz virtualisierter Datenbanken und Dateisysteme mithilfe des Linux-basierten SnapCenter-Plug-ins für die virtuelle VMware vSphere-Appliance (Open Virtual Appliance Format).

SnapCenter Plug-in für Microsoft SQL Server Funktionen

- Automatisiert applikationsspezifische Backup-, Restore- und Klonvorgänge für Microsoft SQL Server Datenbanken in einer SnapCenter Umgebung.
- Unterstützt Microsoft SQL Server Datenbanken auf VMDK und RDM (Raw Device Mapping) LUNs bei der Bereitstellung des SnapCenter Plug-ins für VMware vSphere sowie bei der Registrierung des Plug-ins bei SnapCenter
- Unterstützt nur die Provisionierung von SMB-Freigaben. Für das Backup von SQL Server-Datenbanken auf SMB-Freigaben wird keine Unterstützung geboten.
- Unterstützt den Import von Backups von SnapManager für Microsoft SQL Server in SnapCenter.

SnapCenter Plug-in für Microsoft Windows Funktionen

- Ermöglicht die applikationsgerechte Datensicherung für andere Plug-ins, die auf Windows Hosts in Ihrer SnapCenter Umgebung laufen
- Automatisiert applikationsspezifische Backup-, Restore- und Klonvorgänge für Microsoft Filesysteme in Ihrer SnapCenter Umgebung

- Unterstützt Storage-Bereitstellung, Snapshot-Konsistenz und Speicherplatzrückgewinnung für Windows Hosts

> Das Plug-in für Windows stellt SMB-Freigaben und Windows-Filesysteme auf physischen und RDM-LUNs bereit, unterstützt jedoch keine Backup-Vorgänge für Windows File-Systeme auf SMB-Shares.

SnapCenter Plug-in für Microsoft Exchange Server Funktionen

- Automatisiert applikationsspezifische Backup- und Restore-Vorgänge für Microsoft Exchange Server Datenbanken und Datenbankverfügbarkeitsgruppen (Database Availability Groups, DAGs) in Ihrer SnapCenter Umgebung
- Unterstützung virtualisierter Exchange Server auf RDM LUNs bei der Bereitstellung des SnapCenter Plug-in für VMware vSphere und Registrierung des Plug-ins bei SnapCenter

SnapCenter Plug-in für Oracle Database Funktionen

- Automatisierung applikationsspezifischer Backups, Restores, Recoverys, Überprüfung, Mounten, Unmounten und Klonen für Oracle Datenbanken in Ihrer SnapCenter Umgebung
- Unterstützung von Oracle-Datenbanken für SAP, aber die Integration von SAP BR*Tools ist nicht möglich

SnapCenter Plug-in für UNIX Funktionen

- Ermöglicht das Plug-in für Oracle Database die Durchführung von Datensicherungsvorgängen auf Oracle Datenbanken, indem es den zugrunde liegenden Host Storage Stack auf Linux oder AIX Systemen unterstützt
- Unterstützt NFS-Protokolle (Network File System) und SAN (Storage Area Network) auf einem Storage-System, auf dem ONTAP ausgeführt wird
- Bei Linux Systemen werden Oracle-Datenbanken auf VMDK und RDM-LUNs unterstützt, wenn Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.
- Unterstützt Mount Guard für AIX auf SAN-Dateisystemen und LVM-Layout.
- Unterstützt Enhanced Journaled File System (JFS2) mit Inline-Protokollierung auf SAN-Dateisystemen und LVM-Layout nur für AIX-Systeme.

  ES werden NATIVE SAN-Geräte, Dateisysteme und LVM-Layouts unterstützt, die auf SAN-Geräten basieren.

- Automatisierung von applikationsorientierten Backup-, Restore- und Klonvorgängen für UNIX File-Systeme in der SnapCenter-Umgebung

SnapCenter Plug-in für SAP HANA Database Funktionen

- Automatisiert applikationsspezifische Backups, Restores und das Klonen von SAP HANA Datenbanken in einer SnapCenter Umgebung

Benutzerdefinierte SnapCenter Plug-ins-Funktionen

- Unterstützung benutzerdefinierter Plug-ins zum Management von Applikationen oder Datenbanken, die nicht von anderen SnapCenter Plug-ins unterstützt werden Benutzerdefinierte Plug-ins werden im Rahmen der SnapCenter Installation nicht bereitgestellt.

- Unterstützt die Erstellung von Spiegelkopien von Backup-Sätzen auf einem anderen Volume und die Disk-to-Disk Backup-Replizierung.
- Unterstützt sowohl Windows als auch Linux Umgebungen. In Windows Umgebungen können benutzerdefinierte Applikationen über benutzerdefinierte Plug-ins optional mit dem SnapCenter Plug-in für Microsoft Windows ausgeführt werden, um dateibasierte Backups zu erstellen.

Benutzerdefinierte Plug-in-Beispiele für MySQL, DB2 und MongoDB für SnapCenter-Software können von der heruntergeladen werden "NetApp Storage Automation Store".

Individuelle MySQL, DB2 und MongoDB Plug-ins werden nur durch die NetApp Communitys unterstützt.

NetApp unterstützt die Möglichkeit zur Erstellung und Verwendung benutzerdefinierter Plug-ins. Die von Ihnen erstellten benutzerdefinierten Plug-ins werden von NetApp jedoch nicht unterstützt.

Weitere Informationen finden Sie unter "Entwickeln Sie ein Plug-in für Ihre Applikation"

SnapCenter Repository

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

Die MySQL-Server-Repository-Datenbank wird standardmäßig bei der Installation des SnapCenter-Servers installiert. Wenn MySQL Server bereits installiert ist und Sie eine Neuinstallation von SnapCenter Server durchführen, sollten Sie MySQL Server deinstallieren.

SnapCenter unterstützt MySQL Server 5.7.25 oder höher als die SnapCenter Repository-Datenbank. Wenn Sie eine frühere Version von MySQL Server mit einer früheren Version von SnapCenter verwendet haben, wird der MySQL Server beim SnapCenter Upgrade auf 5.7.25 oder höher aktualisiert.

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

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.
- SnapCenter verwendet Sicherheitsalgorithmen, die dem Federal Information Processing Standard (FIPS) entsprechen.

- SnapCenter unterstützt die Verwendung der vom Kunden bereitgestellten autorisierten CA-Zertifikate.
- SnapCenter 4.1.1 oder höher unterstützt TLS 1.2 (Transport Layer Security) für die Kommunikation mit ONTAP. Sie können TLS 1.2 auch für die Kommunikation zwischen Clients und Servern verwenden.

  Ab 5.0 unterstützt SnapCenter (TLS) 1.3 für die Kommunikation mit ONTAP.

- SnapCenter unterstützt einen bestimmten Satz von SSL-Cipher-Suites, um die Sicherheit der Netzwerkkommunikation zu gewährleisten.

  Weitere Informationen finden Sie unter "So konfigurieren Sie die unterstützte SSL Cipher Suite".

- 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 unter 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 oder mehr falschen Anmeldeversuchen vorübergehend deaktiviert.
- Unterstützt CA-Zertifikatauthentifizierung 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 zum Aktivieren von MFA finden Sie unter "Multi-Faktor-Authentifizierung aktivieren".

Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter

RBAC-Typen

Mit der rollenbasierten Zugriffssteuerung (RBAC) und den ONTAP Berechtigungen von SnapCenter können SnapCenter Administratoren die Kontrolle über SnapCenter Ressourcen an verschiedene Benutzer oder Benutzergruppen delegieren. Dank dieses zentral gemanagten Zugriffs können Applikationsadministratoren innerhalb delegierter Umgebungen sicher arbeiten.

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

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

SnapCenter verwendet folgende Arten der rollenbasierten Zugriffssteuerung:

- RBAC von SnapCenter
- SnapCenter Plug-in RBAC (für einige Plug-ins)
- RBAC auf Applikationsebene
- ONTAP-Berechtigungen

RBAC von SnapCenter

Rollen und Berechtigungen

SnapCenter wird mit vordefinierten Rollen ausgeliefert, deren Berechtigungen bereits zugewiesen sind. Sie können diesen Rollen Benutzer oder Benutzergruppen zuweisen. Sie können auch neue Rollen erstellen und Berechtigungen und Benutzer verwalten.

Zuweisen von Berechtigungen für Benutzer oder Gruppen

Sie können Benutzern oder Gruppen Berechtigungen zuweisen, um auf SnapCenter-Objekte wie Hosts, Speicherverbindungen und Ressourcengruppen zuzugreifen. Sie können die Berechtigungen der SnapCenterAdmin-Rolle nicht ändern.

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.

> Wenn Sie eine benutzerdefinierte Rolle erstellen, muss sie alle Berechtigungen der SnapCenter-Administratorrolle enthalten. Wenn Sie nur einige der Berechtigungen kopieren, z. B. Host add oder Host remove, können Sie diese Vorgänge nicht ausführen.

Authentifizierung

Benutzer müssen bei der Anmeldung über die grafische Benutzeroberfläche (GUI) oder PowerShell Commandlets über die Authentifizierung sorgen. Wenn Benutzer Mitglieder mehrerer Rollen sind, werden sie nach der Eingabe von Anmeldedaten aufgefordert, die gewünschte Rolle anzugeben. Benutzer müssen außerdem eine Authentifizierung zur Ausführung der APIs bereitstellen.

RBAC auf Applikationsebene

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

Wenn Sie beispielsweise Snapshot- und Datensicherungsvorgänge in einer SQL Server-Umgebung durchführen möchten, müssen Sie Anmeldedaten mit den richtigen Windows- oder SQL-Anmeldedaten festlegen. Der SnapCenter-Server authentifiziert die Anmeldeinformationen, die auf beiden Methoden festgelegt sind. Wenn Sie Snapshot- und Datensicherungsvorgänge in einer Windows-Dateisystemumgebung auf ONTAP-Speicher ausführen möchten, muss die SnapCenter-Administratorrolle über Administratorrechte auf dem Windows-Host verfügen.

Wenn Sie Datensicherungsvorgänge in einer Oracle-Datenbank durchführen möchten und wenn die Betriebssystemauthentifizierung im Datenbank-Host deaktiviert ist, müssen Sie die Anmeldedaten mit der Oracle-Datenbank oder den Oracle-ASM-Anmeldeinformationen festlegen. Der SnapCenter-Server authentifiziert die Anmeldeinformationen, die mit einer dieser Methoden festgelegt wurden, je nach Operation.

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 Data ONTAP RBAC.

Weitere Informationen finden Sie unter "SnapCenter Plug-in für VMware vSphere RBAC"

ONTAP-Berechtigungen

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

Informationen zum Erstellen des Kontos und Zuweisen von Berechtigungen finden Sie unter "Erstellen einer ONTAP-Cluster-Rolle mit minimalen Berechtigungen"

RBAC-Berechtigungen und -Rollen

Mit der rollenbasierten Zugriffssteuerung (Role Based Access Control, RBAC) von SnapCenter können Sie Rollen erstellen und diesen Rollen Berechtigungen zuweisen und dann den Rollen Benutzer oder Benutzergruppen zuweisen. So können SnapCenter Administratoren eine zentral verwaltete Umgebung erstellen, während Applikationsadministratoren die Datensicherung managen können. SnapCenter wird mit vordefinierten Rollen und Berechtigungen ausgeliefert.

SnapCenter Rollen

SnapCenter wird mit den folgenden vordefinierten Rollen ausgeliefert. Sie können diesen Rollen Benutzer und Gruppen zuweisen oder neue Rollen erstellen.

Wenn Sie einem Benutzer eine Rolle zuweisen, werden auf der Seite „Jobs“ nur Aufträge angezeigt, die für diesen Benutzer relevant sind, es sei denn, Sie haben die Rolle „SnapCenter-Admin“ zugewiesen.

- Administrator für App Backup und Klonen
- Backup und Clone Viewer
- Infrastrukturadministrator
- SnapCenterAdmin

SnapCenter Plug-in für VMware vSphere Rollen

Für das Management der VM-konsistenten Datensicherung von VMs, VMDKs und Datastores werden in vCenter die folgenden Rollen vom SnapCenter Plug-in für VMware vSphere erstellt:

- SCV Administrator
- SCV-Ansicht
- SCV-Backup
- SCV-Wiederherstellung
- Wiederherstellung der SCV-Gastdatei

Weitere Informationen finden Sie unter "RBAC-Typen für SnapCenter Plug-in für VMware vSphere Benutzer"

Best Practice: NetApp empfiehlt, eine ONTAP-Rolle für das SnapCenter Plug-in für VMware vSphere Operationen zu erstellen und diese alle erforderlichen Berechtigungen zuzuweisen.

SnapCenter-Berechtigungen

SnapCenter bietet folgende Berechtigungen:

- Ressourcengruppe
- Richtlinie
- Backup
- Host
- Storage-Anbindung
- Klonen
- Bereitstellung (nur für Microsoft SQL Datenbank)
- Dashboard
- Berichte An
- Wiederherstellen
  - Vollständige Volume-Wiederherstellung (nur bei benutzerdefinierten Plug-ins)
- Ressource

  Für nicht-Administratoren sind vom Administrator Plug-in-Berechtigungen erforderlich, um eine Ressourcenerkennung durchzuführen.

- Plug-in Installieren oder Deinstallieren

  Wenn Sie die Berechtigungen für die Plug-in-Installation aktivieren, müssen Sie auch die Host-Berechtigung ändern, um Lese- und Updates zu aktivieren.

- Migration
- Mount (nur für Oracle Database)
- Unmount (nur für Oracle Database)
- Job-Überwachung

  Mit der Berechtigung Job Monitor können Mitglieder verschiedener Rollen die Vorgänge für alle Objekte anzeigen, denen sie zugewiesen sind.

Vordefinierte SnapCenter-Rollen und -Berechtigungen

Im Lieferumfang von SnapCenter sind vordefinierte Rollen enthalten, von denen jede bereits aktiviert ist. Beim Einrichten und Verwalten der rollenbasierten Zugriffssteuerung können Sie entweder die vordefinierten Rollen verwenden oder neue erstellen.

SnapCenter umfasst die folgenden vordefinierten Rollen:

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

Wenn Sie einem Benutzer einer Rolle hinzufügen, müssen Sie entweder die Berechtigung StorageConnection zuweisen, um die Kommunikation mit der Storage Virtual Machine (SVM) zu aktivieren, oder dem Benutzer eine SVM zuweisen, damit die Berechtigung zur Verwendung der SVM aktiviert wird. Mit der Berechtigung für

Speicherverbindungen können Benutzer SVM-Verbindungen erstellen.

Ein Benutzer mit der Rolle „SnapCenter-Admin“ kann beispielsweise SVM-Verbindungen erstellen und einem Benutzer mit der Rolle „App-Backup“ und „Clone Admin“ zuweisen. Dieser besitzt standardmäßig keine Berechtigung, SVM-Verbindungen zu erstellen oder zu bearbeiten. Ohne SVM-Verbindung können Benutzer Backup-, Klon- oder Restore-Vorgänge nicht abschließen.

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	Aktualisieren	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
Klonen	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

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	Löschen
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
Job-Überwachung	Ja.	Keine Angabe	Keine Angabe	Keine Angabe	Keine Angabe

Backup und Clone Viewer-Rolle

Die Rolle Backup und Clone Viewer verfügt über eine schreibgeschützte Ansicht aller Berechtigungen. In dieser Rolle sind auch Berechtigungen für Erkennung, Berichterstellung und Zugriff auf das Dashboard aktiviert.

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	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
Klonen	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

Berechtigungen	Aktiviert	Erstellen	Lesen	Aktualisieren	Löschen
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
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	Aktualisieren	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.
Klonen	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

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

SnapCenter Disaster Recovery

Mithilfe der Disaster Recovery-Funktion von SnapCenter können Sie den SnapCenter Server im Falle von Ausfällen wie einer Beschädigung von Ressourcen oder einem Serverabsturz wiederherstellen. Sie können SnapCenter Repositorys, Serverzeitpläne und Serverkonfigurationskomponenten wiederherstellen. Sie können auch das SnapCenter Plug-in für SQL Server und das SnapCenter Plug-in für SQL Server Storage wiederherstellen.

In diesem Abschnitt werden die beiden Arten der Disaster Recovery (DR) in SnapCenter beschrieben:

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 FÜR das Backup des SnapCenter Servers REST-APIs. Siehe "REST-API-Workflows für Disaster Recovery von SnapCenter Server".

- Die Konfigurationsdatei für die Audit-Einstellungen wird nicht im DR-Backup gesichert und auch nicht auf dem DR-Server nach dem Wiederherstellungsvorgang. Sie sollten die Einstellungen für das Überwachungsprotokoll manuell wiederholen.

SnapCenter Plug-in und Storage DR

DR wird nur für das SnapCenter Plug-in für SQL Server unterstützt. Wenn das SnapCenter-Plug-in für SQL Server ausfällt, wechseln Sie zu einem anderen SQL-Host und stellen Sie die Daten mit wenigen Schritten wieder her. Siehe "Disaster Recovery eines SnapCenter Plug-ins für SQL Server".

SnapCenter nutzt ONTAP SnapMirror Technologie zur Datenreplizierung. Er kann zur DR an einem sekundären Standort repliziert und synchron gehalten werden. Ein Failover kann durch die Unterbrechung der Replizierungsbeziehung in SnapMirror initiiert werden. Während Failback kann die Synchronisierung umgekehrt werden und Daten vom DR-Standort zurück zum primären Standort repliziert werden.

Ressourcen, Ressourcengruppen und Richtlinien

Bevor Sie SnapCenter verwenden, ist es hilfreich, grundlegende Konzepte im Zusammenhang mit Backup-, Klon- und Restore-Vorgängen zu verstehen, die durchgeführt werden sollen. Sie interagieren mit Ressourcen, Ressourcengruppen und Richtlinien für verschiedene Vorgänge.

- **Ressourcen** sind normalerweise Datenbanken, Windows-Dateisysteme oder File Shares, die Sie mit SnapCenter sichern oder klonen.

  Je nach Umgebung können es sich jedoch um Ressourcen wie Datenbankinstanzen, Microsoft SQL Server Availability Groups, Oracle Datenbanken, Oracle RAC Datenbanken, Windows File-Systeme oder eine Gruppe benutzerdefinierter Applikationen handeln.

- Eine **Ressourcengruppe** ist eine Sammlung von Ressourcen auf einem Host oder Cluster. Die Ressourcengruppe kann auch Ressourcen von mehreren Hosts und mehreren Clustern enthalten.

  Wenn Sie einen Vorgang für eine Ressourcengruppe ausführen, führen Sie diesen Vorgang für alle Ressourcen aus, die in der Ressourcengruppe gemäß dem von Ihnen für die Ressourcengruppe festgelegten Zeitplan definiert sind.

  Sie können nach Bedarf eine einzelne Ressource oder eine Ressourcengruppe sichern. Sie können auch geplante Backups für einzelne Ressourcen und Ressourcengruppen konfigurieren.

  Wenn Sie einen Host einer Gruppe gemeinsam genutzter Ressourcen in den Wartungsmodus versetzen und Pläne mit derselben gemeinsam genutzten Ressourcengruppe verknüpft sind, werden alle geplanten Vorgänge für alle anderen Hosts der gemeinsam genutzten Ressourcengruppe ausgesetzt.

  Sie sollten ein Datenbank-Plug-in zum Sichern von Datenbanken, ein Filesystem-Plug-in zum Backup von Filesystemen und das SnapCenter Plug-in für VMware vSphere zum Sichern von VMs und Datastores verwenden.

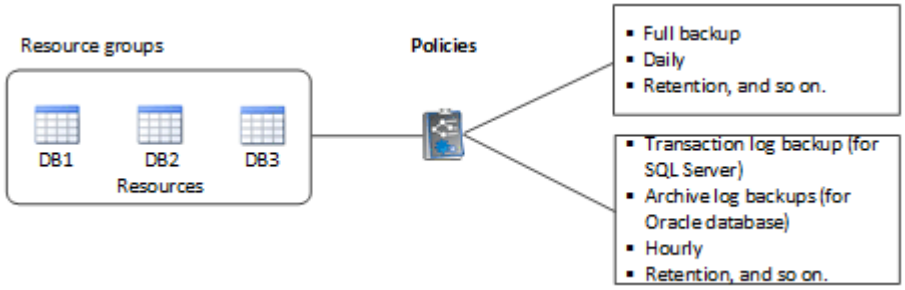
- **Richtlinien** Geben Sie die Backup-Häufigkeit, die Aufbewahrung von Kopien, die Replikation, Skripte und andere Merkmale von Datenschutzvorgängen an.

  Wenn Sie eine Ressourcengruppe erstellen, wählen Sie eine oder mehrere Richtlinien für diese Gruppe aus. Sie können auch eine Richtlinie auswählen, wenn Sie ein Backup nach Bedarf ausführen.

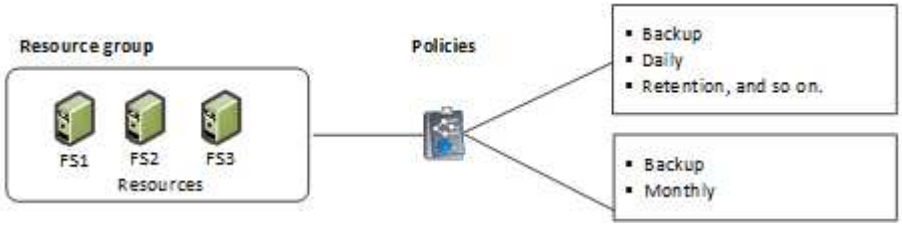
Denken Sie an eine Ressourcengruppe, die definiert *was* Sie schützen möchten und wann Sie sie in Bezug auf Tag und Zeit schützen möchten. Denken Sie an eine Politik, die definiert *wie* Sie sie schützen möchten. Wenn Sie beispielsweise alle Datenbanken sichern oder alle Dateisysteme eines Hosts sichern, können Sie eine Ressourcengruppe erstellen, die alle Datenbanken oder alle Dateisysteme des Hosts enthält. Sie können dann zwei Richtlinien an die Ressourcengruppe anhängen: Eine Tagesrichtlinie und eine Stundenpolitik.

Wenn Sie die Ressourcengruppe erstellen und die Richtlinien anhängen, können Sie die Ressourcengruppe so konfigurieren, dass sie täglich ein vollständiges Backup durchführt, und einen anderen Zeitplan, der stündlich Protokoll-Backups durchführt.

Das folgende Bild veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



Die folgende Abbildung veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Windows File-Systeme:



Vorschriften und Postskripte

Im Rahmen Ihrer Datensicherungsabläufe können Sie benutzerdefinierte Prescripts und Postskripte verwenden. Diese Skripte ermöglichen die Automatisierung entweder vor oder nach Ihrem Datensicherungsauftrag. Sie können z. B. ein Skript einschließen, das Sie automatisch über Fehler oder Warnungen bei Datenschutzaufstellungsfehlern benachrichtigt. Bevor Sie Ihre Prescripts und Postscripts einrichten, sollten Sie einige der Anforderungen zur Erstellung dieser Skripte kennen.

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 im Rahmen des SnapCenter Betriebs ausgeführten Prescripts und Postskripte auf nicht virtualisierten und virtualisierten Storage-Systemen 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 Sicherungsauftrag gestartet wird, ordnet die Richtlinie das Skript automatisch den gesicherten 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.

SnapCenter-Automatisierung mit REST-APIs

MITHILFE VON REST-APIs lassen sich verschiedene SnapCenter-Managementvorgänge ausführen. REST-APIs sind über die Swagger Webseite zugänglich. Sie können auf die Swagger-Webseite zugreifen, um die REST-API-Dokumentation anzuzeigen und einen API-Aufruf manuell zu tätigen. Mit REST-APIs

können Sie Ihren SnapCenter Server oder Ihren SnapCenter vSphere Host managen.

DIE REST-APIs für…	Befinden sich in…
SnapCenter Server	\Https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/
SnapCenter Plug-in für VMware vSphere	\Https://<OVA_IP_address_or_host_name>:<scv_plugin_port>/API/swagger-ui.HTML#

Weitere Informationen zu SnapCenter REST-APIs finden Sie unter "Übersicht ÜBER REST-APIs"

Weitere Informationen zum SnapCenter-Plug-in für VMware vSphere REST-APIs finden Sie unter "SnapCenter Plug-in für VMware vSphere REST-APIs"