Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe

SnapCenter Software 5.0

NetApp
July 18, 2024

Inhalt

Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe

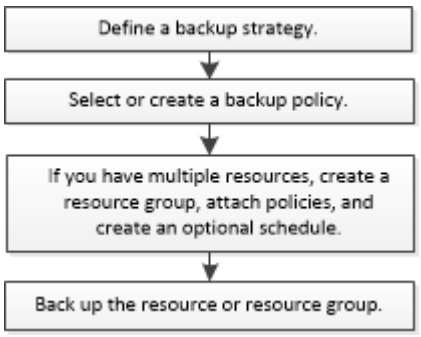
Backup-Workflow

Wenn Sie das SnapCenter Plug-in für Microsoft SQL Server in Ihrer Umgebung installieren, können Sie mit SnapCenter die SQL Server Ressourcen sichern.

Sie können mehrere Backups so planen, dass sie gleichzeitig über mehrere Server ausgeführt werden.

Backup- und Restore-Vorgänge können nicht gleichzeitig auf derselben Ressource durchgeführt werden.

Der folgende Workflow zeigt die Reihenfolge, in der Sie die Backup-Vorgänge durchführen müssen:



Die Optionen „Jetzt sichern“, „Wiederherstellen“, „Backups verwalten“ und „Klonen“ auf der Seite „Ressourcen“ werden deaktiviert, wenn Sie eine nicht von NetApp stammende LUN, eine beschädigte Datenbank oder eine wiederhergestellte Datenbank auswählen.

Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup, Wiederherstellung, Wiederherstellung, Verifizierung und Klonvorgänge durchzuführen. Detaillierte Informationen zu PowerShell Cmdlets finden Sie in der SnapCenter Cmdlet-Hilfe oder im "SnapCenter Software Cmdlet Referenzhandbuch"

Wie SnapCenter Datenbanken sichert

SnapCenter verwendet Snapshot Technologie, um die SQL Server Datenbanken auf LUNs oder VMDKs zu sichern. SnapCenter erstellt das Backup durch Erstellen von Snapshots der Datenbanken.

Wenn Sie auf der Seite Ressourcen eine Datenbank für ein vollständiges Datenbank-Backup auswählen, wählt SnapCenter automatisch alle anderen Datenbanken aus, die sich auf demselben Storage Volume befinden. Wenn die LUN oder VMDK nur eine einzige Datenbank speichert, können Sie die Datenbank einzeln löschen oder erneut auswählen. Wenn die LUN oder VMDK mehrere Datenbanken enthält, müssen Sie die Datenbanken als Gruppe löschen oder neu auswählen.

Alle Datenbanken, die sich auf einem einzelnen Volume befinden, werden gleichzeitig mithilfe von Snapshots gesichert. Wenn die maximale Anzahl gleichzeitiger Backup-Datenbanken 35 ist und sich mehr als 35 Datenbanken auf einem Speicher-Volume befinden, dann entspricht die Gesamtzahl der erstellten Snapshots der Anzahl der Datenbanken geteilt durch 35.

Sie können die maximale Anzahl an Datenbanken für jeden Snapshot in der Backup-Richtlinie konfigurieren.

Wenn SnapCenter einen Snapshot erstellt, wird im Snapshot das gesamte Storage-System-Volume erfasst. Das Backup ist jedoch nur für den SQL-Hostserver gültig, für den das Backup erstellt wurde.

Wenn sich Daten von anderen SQL Host-Servern auf demselben Volume befinden, können diese Daten vom Snapshot nicht wiederhergestellt werden.

Weitere Informationen

"Sichern Sie Ressourcen mit PowerShell cmdlets"

"Fehler beim Quiesce oder Gruppieren von Ressourcen"

Bestimmen Sie, ob Ressourcen für ein Backup verfügbar sind

Ressourcen sind die Datenbanken, Applikationsinstanzen, Verfügbarkeitsgruppen und ähnliche Komponenten, die von den installierten Plug-ins gewartet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, sodass Sie Datensicherungsjobs ausführen können. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Sie zur Verfügung haben. Das ermitteln der verfügbaren Ressourcen überprüft außerdem, ob die Plug-in-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. das Installieren von SnapCenter-Servern, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen.
- Um die Microsoft SQL-Datenbanken zu ermitteln, sollte eine der folgenden Bedingungen erfüllt sein.
  - Der Benutzer, der zum Hinzufügen des Plug-in-Hosts zum SnapCenter Server verwendet wurde, sollte über die erforderlichen Berechtigungen (Sysadmin) auf dem Microsoft SQL Server verfügen.
  - Wenn die oben genannte Bedingung nicht erfüllt ist, sollten Sie im SnapCenter-Server den Benutzer konfigurieren, der über die erforderlichen Berechtigungen (sysadmin) auf dem Microsoft SQL-Server verfügt. Der Benutzer sollte auf der Ebene der Microsoft SQL Server-Instanz konfiguriert werden und der Benutzer kann ein SQL- oder Windows-Benutzer sein.
- Um die Microsoft SQL-Datenbanken in einem Windows-Cluster zu ermitteln, müssen Sie den TCP/IP-Port (Failover Cluster Instance) für die Failover-Cluster-Instanz (FCI) freigeben.
- Wenn Datenbanken auf VMware RDM-LUNs oder VMDKs vorhanden sind, müssen Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit SnapCenter registrieren.

  Weitere Informationen finden Sie unter "Implementieren Sie das SnapCenter Plug-in für VMware vSphere"
- Wenn der Host mit gMSA hinzugefügt wird und der gMSA über Login- und System Admin-Berechtigungen verfügt, wird das gMSA verwendet, um eine Verbindung zur SQL-Instanz herzustellen.

Über diese Aufgabe

Datenbanken können nicht gesichert werden, wenn die Option **Gesamtstatus** auf der Seite Details auf nicht verfügbar für Backups eingestellt ist. Die Option **Gesamtstatus** ist für die Sicherung auf nicht verfügbar

eingestellt, wenn eine der folgenden Optionen zutrifft:

- Datenbanken sind nicht auf einer NetApp LUN.
- Datenbanken befinden sich nicht im normalen Zustand.

  Datenbanken befinden sich nicht im normalen Zustand, wenn sie offline sind, sie wiederherstellen, ausstehende Wiederherstellung, Verdacht usw.

- Datenbanken verfügen über unzureichende Berechtigungen.

  Wenn ein Benutzer beispielsweise nur Zugriff auf die Datenbank hat, können Dateien und Eigenschaften der Datenbank nicht identifiziert werden und können daher nicht gesichert werden.

SnapCenter kann nur die primäre Datenbank sichern, wenn Sie eine Verfügbarkeitsgruppe auf der SQL Server Standard Edition haben.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Dropdown-Liste **Ansicht** * oder **Instanz** oder **Verfügbarkeitsgruppe** aus.

   Klicken Sie auf , und wählen Sie den Hostnamen und die SQL Server-Instanz aus, um die Ressourcen zu filtern. Sie können dann klicken , um den Filterbereich zu schließen.

3. Klicken Sie Auf **Ressourcen Aktualisieren**.

   Die neu hinzugefügten, umbenannten oder gelöschten Ressourcen werden in den SnapCenter-Serverbestand aktualisiert.

   Sie müssen die Ressourcen aktualisieren, wenn die Datenbanken außerhalb von SnapCenter umbenannt werden.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Host- oder Cluster-Name, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich die Datenbank auf einem nicht-NetApp-Speicher befindet, `Not available for backup` wird in der Spalte **Gesamtstatus** angezeigt.

     Sie können keine Datensicherungsvorgänge für eine Datenbank ausführen, die sich auf einem Storage-System anderer Anbieter befindet.

   - Wenn sich die Datenbank auf einem NetApp-Speicher befindet und nicht geschützt ist, `Not protected` wird in der Spalte **Gesamtstatus** angezeigt.
   - Wenn sich die Datenbank auf einem NetApp-Speichersystem befindet und geschützt ist, zeigt die Benutzeroberfläche `Backup not run` eine Meldung in der Spalte **Gesamtstatus** an.
   - Wenn sich die Datenbank auf einem NetApp-Speichersystem befindet und geschützt ist und das Backup für die Datenbank ausgelöst wird, wird auf der Benutzeroberfläche die Meldung in der Spalte **Gesamtstatus** angezeigt `Backup succeeded` .

Wenn Sie beim Einrichten der Anmeldeinformationen eine SQL-Authentifizierung aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Vorhängeschloss-Symbol angezeigt. Wenn das Vorhängeschloss-Symbol angezeigt wird, müssen Sie die Instanz oder die Datenbankanmeldeinformationen angeben, damit die Instanz oder Datenbank einer Ressourcengruppe erfolgreich hinzugefügt werden kann.

1. Nachdem der SnapCenter-Administrator einem RBAC-Benutzer die Ressourcen zuweist, muss sich der RBAC-Benutzer anmelden und auf **Ressourcen aktualisieren** klicken, um die neuesten **Gesamtstatus** der Ressourcen anzuzeigen.

Migrieren von Ressourcen auf ein NetApp Storage-System

Nachdem Sie Ihr NetApp Storage-System mit dem SnapCenter Plug-in für Microsoft Windows bereitgestellt haben, können Sie Ihre Ressourcen auf das NetApp Storage-System oder von einer NetApp LUN zu einer anderen NetApp LUN migrieren. Hierzu stehen entweder die SnapCenter Graphical User Interface (GUI) oder die PowerShell Commandlets zur Verfügung.

Bevor Sie beginnen

- Sie müssen dem SnapCenter-Server Storage-Systeme hinzugefügt haben.
- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.

Die meisten Felder auf diesen Assistentenseiten sind selbsterklärend. In den folgenden Informationen werden einige der Felder beschrieben, für die Sie möglicherweise eine Anleitung benötigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Dropdown-Liste **Ansicht** die Option **Datenbank** oder **Instanz** aus.
3. Wählen Sie entweder die Datenbank oder die Instanz aus der Liste aus und klicken Sie auf **Migrieren**.
4. Führen Sie auf der Seite Ressourcen die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Datenbankname (optional)	Wenn Sie eine Instanz für die Migration ausgewählt haben, müssen Sie die Datenbanken dieser Instanz aus der Dropdown-Liste **Databases** auswählen.
Wählen Sie Reiseziele	Wählen Sie den Zielspeicherort für Daten- und Protokolldateien aus. Die Daten- und Log-Dateien werden in den Daten- bzw. Log-Ordner unter dem ausgewählten NetApp-Laufwerk verschoben. Wenn kein Ordner in der Ordnerstruktur vorhanden ist, wird ein Ordner erstellt und die Ressource migriert.

Für dieses Feld…	Tun Sie das…
Details zur Datenbankdatei anzeigen (optional)	Wählen Sie diese Option aus, wenn Sie mehrere Dateien einer einzigen Datenbank migrieren möchten. Diese Option wird nicht angezeigt, wenn Sie die Ressource **Instanz** auswählen.
Optionen	Wählen Sie **Kopie der migrierten Datenbank am ursprünglichen Speicherort löschen**, um die Kopie der Datenbank aus der Quelle zu löschen. Optional: **UPDATE-STATISTIKEN auf Tabellen AUSFÜHREN, bevor Sie die Datenbank entfernen**.

5. Führen Sie auf der Seite Verifizieren die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Optionen Zur Datenbankkonsistenzprüfung	Wählen Sie **vorher ausführen** aus, um die Integrität der Datenbank vor der Migration zu überprüfen. Wählen Sie **nach** ausführen, um die Integrität der Datenbank nach der Migration zu überprüfen.

Für dieses Feld…	Tun Sie das…
DBCC CHECKDB Optionen	• Wählen Sie die Option **PHYSICAL_ONLY**, um die Integritätsprüfung auf die physische Struktur der Datenbank zu begrenzen und um zerrissene Seiten, Prüfsummenfehler und häufige Hardwarefehler zu erkennen, die die Datenbank beeinträchtigen. • Wählen Sie die Option **NO_INFOMSGS**, um alle Informationsmeldungen zu unterdrücken. • Wählen Sie die Option **ALL_ERRORMSGS** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen. • Wählen Sie die Option **NOINDEX** aus, wenn Sie keine nicht geclusterten Indizes überprüfen möchten. Die SQL Server-Datenbank verwendet Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen. Sie können diese Option auswählen, um die Ausführungszeit zu verkürzen. • Wählen Sie die Option **TABLOCK**, um die Prüfungen zu beschränken und Sperren anstelle eines internen Datenbank-Snapshots zu erhalten.

6. Überprüfen Sie die Zusammenfassung, und klicken Sie dann auf **Fertig stellen**.

Erstellen von Backup-Richtlinien für SQL Server-Datenbanken

Sie können eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, bevor Sie SnapCenter zum Sichern von SQL Server-Ressourcen verwenden. Alternativ können Sie beim Erstellen einer Ressourcengruppen oder beim Sichern einer einzelnen Ressource eine Backup-Richtlinie erstellen.

Bevor Sie beginnen

- Sie müssen Ihre Datensicherungsstrategie definiert haben.
- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, die Identifizierung von Ressourcen und das Erstellen von Verbindungen zum Storage-System abschließen.
- Sie müssen das Host-Protokollverzeichnis für die Protokollsicherung konfiguriert haben.

- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.
- Wenn Sie Snapshots auf eine Spiegelung oder einen Vault replizieren, muss der SnapCenter Administrator Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch für die Ziel-Volumes zugewiesen haben.

  Informationen darüber, wie Administratoren Benutzern Ressourcen zuweisen, finden Sie in den SnapCenter Installationsinformationen.

- Wenn Sie die PowerShell-Skripte in Prescripts und Postscripts ausführen möchten, sollten Sie den Wert des Parameters usePowershellProcessforScripts in der Datei Web.config auf true setzen.

  Der Standardwert ist false.

- Weitere Informationen zu Voraussetzungen und Einschränkungen finden Sie unter SnapMirror Business Continuity (SM-BC). "Objektbeschränkungen für SnapMirror Business Continuity"

Über diese Aufgabe

- Eine Backup-Richtlinie ist eine Reihe von Regeln, die festlegen, wie Backups gemanagt und aufbewahrt werden und wie oft die Ressourcen- oder Ressourcengruppe gesichert wird. Außerdem können Sie Replizierungs- und Skript-Einstellungen festlegen. Durch das Festlegen von Optionen in einer Richtlinie wird Zeit eingespart, wenn die Richtlinie für eine andere Ressourcengruppe wiederverwendet werden soll.

  DER SCRIPTS_PATH wird mit dem PredefinedWindowsScriptDirectory-Schlüssel definiert, der sich in der SMCoreServiceHost.exe.Config-Datei des Plug-in-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMCore Service neu starten. Es wird empfohlen, den Standardpfad für die Sicherheit zu verwenden.

  Der Wert des Schlüssels kann von Swagger über die API angezeigt werden: API /4.7/configsettings

  Sie können die GET API verwenden, um den Wert der Taste anzuzeigen. SET-API wird nicht unterstützt.

- SnapLock

  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.

    Wenn Sie eine Snapshot-Sperrfrist festlegen, wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.

    Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

  Die primären SnapLock-Einstellungen werden in der SnapCenter Backup Policy gemanagt, und die sekundären SnapLock-Einstellungen werden von ONTAP gemanagt.

Schritt: Richtliniennamen Erstellen

1. Wählen Sie im linken Navigationsbereich **Einstellungen**.
2. Wählen Sie auf der Seite Einstellungen die Option **Richtlinien** aus.

3. Wählen Sie **Neu**.
4. Geben Sie auf der Seite **Name** den Namen und die Beschreibung der Richtlinie ein.

Schritt 2: Konfigurieren von Backup-Optionen

1. Wählen Sie Ihren Sicherungstyp aus

Vollständige Sicherung und Protokollsicherung

Sichern Sie die Datenbankdateien und Transaktionsprotokolle und verkürzen Sie die Transaktionsprotokolle.

1. Wählen Sie **Vollbackup und Log Backup** aus.
2. Geben Sie die maximale Anzahl an Datenbanken ein, die für jeden Snapshot gesichert werden sollen.

Sie müssen diesen Wert erhöhen, wenn Sie mehrere Backup-Vorgänge gleichzeitig ausführen möchten.

Vollständiges Backup

Sichern Sie die Datenbankdateien.

1. Wählen Sie * Vollbackup* aus.
2. Geben Sie die maximale Anzahl an Datenbanken ein, die für jeden Snapshot gesichert werden sollen. Der Standardwert ist 100

Sie müssen diesen Wert erhöhen, wenn Sie mehrere Backup-Vorgänge gleichzeitig ausführen möchten.

Backup Protokollieren

Sichern Sie die Transaktionsprotokolle. . Wählen Sie **Backup protokollieren**.

Backup Nur Kopieren

1. Wenn Sie Ihre Ressourcen mithilfe einer anderen Backup-Anwendung sichern, wählen Sie **nur Backup kopieren**.

Wenn die Transaktionsprotokolle intakt bleiben, kann jede Backup-Anwendung die Datenbanken wiederherstellen. In der Regel sollten Sie die Option nur kopieren unter anderen Umständen nicht verwenden.

Microsoft SQL unterstützt nicht die Option **nur kopieren Backup** zusammen mit der Option **Vollbackup und Log Backup** für sekundären Speicher.

1. Führen Sie im Abschnitt Einstellungen für Verfügbarkeitsgruppen die folgenden Aktionen durch:

   a. Nur Backup auf bevorzugtem Backup-Replikat.

      Wählen Sie diese Option aus, um nur auf dem bevorzugten Backup-Replikat zu sichern. Über die für die AG im SQL Server konfigurierten Backup-Einstellungen wird das bevorzugte Backup-Replikat entschieden.

b. Wählen Sie Replikate für das Backup aus.

   Wählen Sie das primäre AG-Replikat oder das sekundäre AG-Replikat für das Backup aus.

c. Backup-Priorität auswählen (minimale und maximale Backup-Priorität)

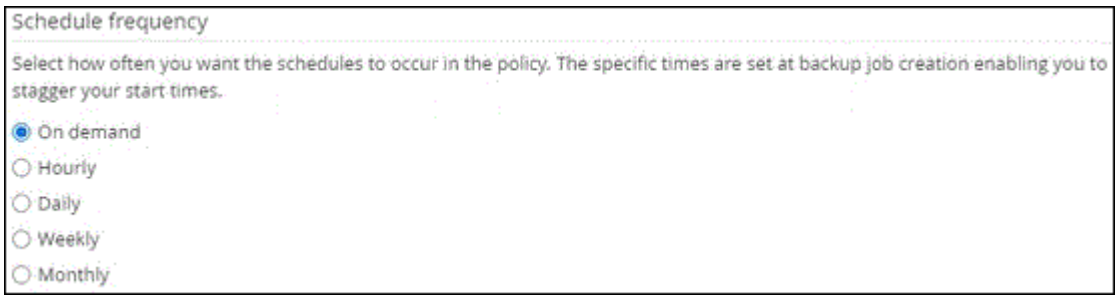
   Geben Sie eine Mindestanzahl der Backup-Prioritäten und eine Nummer der maximalen Backup-Priorität an, die das AG-Replikat für das Backup entscheidet. Sie können beispielsweise eine Mindestpriorität von 10 und eine maximale Priorität von 50 haben. In diesem Fall werden alle AG-Replikate mit einer Priorität von mehr als 10 und weniger als 50 für Backups in Betracht gezogen.

   Standardmäßig ist die Mindestpriorität 1 und die maximale Priorität 100.

Bei Cluster-Konfigurationen werden die Backups entsprechend den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Node des Clusters aufbewahrt. Wenn sich der Owner-Knoten der AG ändert, werden die Backups gemäß den Aufbewahrungseinstellungen erstellt und die Backups des vorherigen Owner-Knotens beibehalten. Die Aufbewahrung für AG ist nur auf Node-Ebene anwendbar.

2. Planen Sie die Backup-Häufigkeit für diese Richtlinie. Geben Sie den Zeitplantyp an, indem Sie entweder **On Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

   Sie können nur einen Plantyp für eine Richtlinie auswählen.



Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang festlegen, während Sie eine Ressourcengruppe erstellen. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien- und Backup-Häufigkeit verwenden, aber Sie können jeder Richtlinie verschiedene Backup-Zeitpläne zuweisen.

Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

Schritt 3: Konfigurieren der Aufbewahrungseinstellungen

Führen Sie auf der Seite Aufbewahrung je nach dem auf der Seite Backup-Typ ausgewählten Backup-Typ eine oder mehrere der folgenden Aktionen durch:

1. Führen Sie in den Aufbewahrungseinstellungen für den Abschnitt „minutengenaue Wiederherstellung“ eine der folgenden Aktionen aus:

Bestimmte Anzahl von Kopien

Bewahren Sie nur eine bestimmte Anzahl von Snapshots auf.

1. Wählen Sie die Option **Protokoll-Backups aufbewahren, die für die letzte <Zahl> Tage** gelten, und geben Sie die Anzahl der zu beheldenden Tage an. Wenn Sie diesem Limit nahe kommen, können Sie ältere Kopien löschen.

Bestimmte Anzahl von Tagen

Bewahren Sie die Backup-Kopien für eine bestimmte Anzahl von Tagen auf.

1. Wählen Sie die Option **Protokoll-Backups aufbewahren, die für die letzten <number> Tage voller Backups** gelten, und geben Sie die Anzahl der Tage an, um die Backup-Kopien des Protokolls zu behalten.

1. Führen Sie im Abschnitt **vollständige Backup-Aufbewahrungs-Einstellungen** für die Einstellungen für On Demand-Aufbewahrung die folgenden Aktionen aus:
   a. Geben Sie die Gesamtzahl der zu erbehalt enden Snapshots an
      i. Um die Anzahl der zu befolgenden Snapshots anzugeben, wählen Sie **Gesamtanzahl der zu befolgenden Snapshot-Kopien** aus.
      ii. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht.

Standardmäßig ist der Wert der Aufbewahrungsanzahl auf 2 festgelegt. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt.

1. Dauer der Aufbewahrung von Snapshots
   a. Wenn Sie die Anzahl der Tage angeben möchten, für die Sie die Snapshots vor dem Löschen behalten möchten, wählen Sie **Snapshot-Kopien beibehalten für**.
2. Wenn Sie die Sperrfrist für Snapshots angeben möchten, wählen Sie **Sperrfrist für Snapshot-Kopie** und wählen Sie Tage, Monate oder Jahre aus.

   Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

3. Geben Sie im Abschnitt **vollständige Backup-Aufbewahrungseinstellungen** für die Einstellungen für die stündliche, tägliche, wöchentliche und monatliche Aufbewahrung die Aufbewahrungseinstellungen für den Terminplantyp an, der auf der Seite Backup-Typ ausgewählt wurde.
   a. Geben Sie die Gesamtzahl der zu erbehalt enden Snapshots an
      i. Um die Anzahl der zu befolgenden Snapshots anzugeben, wählen Sie **Gesamtanzahl der zu befolgenden Snapshot-Kopien** aus. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht.

Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

1. Dauer der Aufbewahrung von Snapshots
   a. Um die Anzahl der Tage anzugeben, für die Sie die Snapshots vor dem Löschen behalten möchten, wählen Sie **Snapshot Kopien beibehalten für**.
2. Wenn Sie die Sperrfrist für Snapshots angeben möchten, wählen Sie **Sperrfrist für Snapshot-Kopie** und wählen Sie Tage, Monate oder Jahre aus.

   Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

   Die Snapshot-Protokollaufbewahrung ist standardmäßig auf 7 Tage eingestellt. Verwenden Sie das Cmdlet "Set-SmPolicy", um die Snapshot Aufbewahrung des Protokolls zu ändern.

Dieses Beispiel setzt die Snapshot-Protokollaufbewahrung auf 2:

Beispiel 1. Beispiel Anzeigen

```
Set-SmPolicy -PolicyName 'newpol' -PolicyTyp 'Backup' -PluginPolicyTyp 'SCSQL' -sqlbackuptyp
'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='hourly';RetentionCount=2},@{2}@{2}
BackupType='LOG';ScheduleType='hourly'
```

"SnapCenter behält Snapshot Kopien der Datenbank bei"

Schritt 4: Konfigurieren der Replikationseinstellungen

1. Geben Sie auf der Seite „Replikation“ die Replikation auf das sekundäre Speichersystem an:

SnapMirror aktualisieren

Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie.

1. Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume (SnapMirror) zu erstellen.

   Diese Option sollte für SnapMirror Business Continuity (SM-BC) oder für SnapMirror Sync (SM-S) aktiviert sein.

   Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden.

   Siehe "Sehen Sie sich SQL Server Backups und Klone auf der Seite Topologie an".

Aktualisieren Sie SnapVault

Aktualisieren Sie SnapVault nach dem Erstellen einer Snapshot Kopie.

1. Wählen Sie diese Option aus, um die Disk-to-Disk-Backup-Replikation durchzuführen.

   Während der sekundären Replizierung wird mit der SnapLock-Ablaufzeit die primäre SnapLock-Ablaufzeit geladen. Durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie wird die sekundäre und primäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen werden.

   Wenn SnapLock nur auf dem sekundären aus ONTAP, dem sogenannten SnapLock-Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche * Aktualisieren* auf der Seite Topologie die Sperrfrist auf dem sekundären, das von ONTAP abgerufen wird, aktualisiert.

   Weitere Informationen zu SnapLock Vault finden Sie unter "Speichern von Snapshot-Kopien in WORM-KOPIEN auf einem Vault-Ziel"

   Siehe "Sehen Sie sich SQL Server Backups und Klone auf der Seite Topologie an".

Sekundäre Richtlinienbezeichnung

1. Wählen Sie eine Snapshot-Bezeichnung aus.

Je nach der ausgewählten Snapshot-Beschriftung wendet ONTAP die sekundäre Snapshot-Aufbewahrungsrichtlinie an, die der Markierung entspricht.

> Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.

Fehler Anzahl Der Wiederholungen

1. Geben Sie die Anzahl der Replikationsversuche ein, die vor dem Anhalten des Prozesses auftreten sollen.

Schritt 5: Konfigurieren der Skripteinstellungen

1. Geben Sie auf der Seite Skript den Pfad und die Argumente des Vorskripts bzw. des Postskripts ein, die vor bzw. nach dem Backup ausgeführt werden sollen.

   Sie können beispielsweise ein Skript ausführen, um SNMP-Traps zu aktualisieren, Warnmeldungen zu automatisieren und Protokolle zu senden.

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

   Sie müssen die SnapMirror Aufbewahrungsrichtlinie in ONTAP so konfigurieren, dass der sekundäre Storage nicht die maximale Snapshot-Grenze erreicht.

Schritt 6: Konfigurieren Sie die Überprüfungseinstellungen

Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

1. Wählen Sie im Abschnitt Überprüfung ausführen für folgende Backup-Pläne die Zeitplanhäufigkeit aus.
2. Führen Sie im Abschnitt Optionen für die Datenbankkonsistenzprüfung die folgenden Aktionen durch:
   a. Beschränkung der Integritätsstruktur auf die physische Struktur der Datenbank (PHYSICAL_ONLY)
      i. Wählen Sie **Beschränkung der Integritätsstruktur auf physische Struktur der Datenbank (PHYSICAL_ONLY)** aus, um die Integritätsprüfung auf die physische Struktur der Datenbank zu begrenzen und um gerissene Seiten, Prüfsummenfehler und häufige Hardwarefehler zu erkennen, die die Datenbank beeinträchtigen.
   b. Alle Informationsmeldungen unterdrücken (KEINE INFOMSGS)
      i. Wählen Sie * Alle Informationsmeldungen (NO_INFOMSGS)* aus, um alle Informationsmeldungen zu unterdrücken. Standardmäßig ausgewählt.
   c. Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL_ERRORMSGS)
      i. Wählen Sie **Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL_ERRORMSGS)** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen.
   d. Nicht geclusterte Indizes (NOINDEX) nicht prüfen
      i. Wählen Sie * nicht gruppierte Indizes (NOINDEX)* aus, wenn Sie keine nicht geclusterten Indizes überprüfen möchten. Die SQL Server-Datenbank verwendet Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.
   e. Begrenzen Sie die Überprüfungen und erhalten Sie die Sperren anstelle eines internen Datenbank-Snapshot (TABLOCK)
      i. Wählen Sie **Schränken Sie die Prüfungen ein und erhalten Sie die Sperren anstatt eine interne Datenbank Snapshot Kopie (TABLOCK)** zu verwenden, um die Überprüfungen zu begrenzen und Sperren anstelle eines internen Datenbank-Snapshots zu erhalten.
3. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss bestätigen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.
4. Geben Sie im Abschnitt **Verification Script settings** den Pfad und die Argumente des Vorskripts bzw. Postscript ein, die vor oder nach dem Verifizierungsvorgang ausgeführt werden sollen.

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

Schritt 7: Zusammenfassung überprüfen

1. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für SQL Server

Eine Ressourcengruppe ist ein Container, dem Sie Ressourcen hinzufügen, die Sie gemeinsam sichern und schützen möchten. Mit einer Ressourcengruppen können Sie alle Daten sichern, die einer bestimmten Anwendung zugeordnet sind. Für jeden Datenschutzauftrag ist eine Ressourcengruppen erforderlich. Sie müssen der Ressourcengruppe auch eine oder mehrere Richtlinien zuordnen, um den Typ des Datensicherungsauftrags zu definieren, den Sie ausführen möchten.

Sie können Ressourcen einzeln schützen, ohne eine neue Ressourcengruppe zu erstellen. Sie können Backups auf der geschützten Ressource erstellen.

Über diese Aufgabe

- Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- Das Hinzufügen neuer Datenbanken ohne SM-BC zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SM-BC enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Datenbanken zu einer vorhandenen Ressourcengruppe im Failover-Modus von SM-BC wird nicht unterstützt. Sie können der Ressourcengruppe nur im regulären oder Failback-Status Ressourcen hinzufügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Datenbank** aus.

   Wenn Sie kürzlich eine Ressource zu SnapCenter hinzugefügt haben, klicken Sie auf **Ressourcen aktualisieren**, um die neu hinzugefügte Ressource anzuzeigen.

3. Klicken Sie Auf **Neue Ressourcengruppe**.
4. Führen Sie auf der Seite Name die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie den Namen der Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

5. Führen Sie auf der Seite Ressourcen die folgenden Schritte aus:
   a. Wählen Sie den Hostnamen, den Ressourcentyp und die SQL Server-Instanz aus Dropdown-Listen aus, um die Liste der Ressourcen zu filtern.

      Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

   b. So verschieben Sie Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** in den Abschnitt Ausgewählte Ressourcen:
      - Wählen Sie **Automatische Auswahl aller Ressourcen auf demselben Speichervolumen**, um alle Ressourcen auf demselben Volume in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.
      - Wählen Sie die Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den Pfeil nach rechts, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:
   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie auf * * klicken + .

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

   b. Klicken Sie im Abschnitt Configure Schedules for Selected Policies auf * * + in der Spalte Configure Schedules für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.

c. Konfigurieren Sie den Zeitplan im Dialogfeld Add Schedules for Policy_Name_, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben und dann auf **OK** klicken.

   Sie müssen dies für jede in der Richtlinie angegebene Frequenz tun. Die konfigurierten Zeitpläne werden in der Spalte angewendete Zeitpläne im Abschnitt **Zeitpläne für ausgewählte Richtlinien konfigurieren** aufgelistet.

d. Wählen Sie den Microsoft SQL Server Scheduler aus.

   Sie müssen auch eine Planer-Instanz auswählen, die der Planungsrichtlinie zugeordnet werden soll.

   Wenn Sie den Microsoft SQL Server Scheduler nicht auswählen, ist der Standard Microsoft Windows Scheduler.

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden. Sie sollten die Zeitpläne nicht ändern und den Backupjob umbenennen, der in Windows Scheduler oder SQL Server Agent erstellt wurde.

7. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

   a. Wählen Sie den Verifikationsserver aus der Dropdown-Liste **Überprüfungsserver** aus.

      Die Liste enthält alle SQL Server, die in SnapCenter hinzugefügt wurden. Sie können mehrere Verifizierungsserver auswählen (lokaler Host oder Remote-Host).

      Die Version des Verifizierungsservers sollte mit der Version und Edition des SQL-Servers übereinstimmen, der die primäre Datenbank hostet.

   a. Klicken Sie auf **Lokatoren laden**, um die SnapMirror und SnapVault Volumes zu laden, um eine Überprüfung auf dem sekundären Speicher durchzuführen.

   b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und klicken Sie dann auf * * + .

   c. Führen Sie im Dialogfeld Add Verification Schedules Policy_Name die folgenden Aktionen durch:

Ihr Ziel ist	Tun Sie das…
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen**.

   d. Klicken Sie auf **OK**.

      Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt. Sie können die Informationen überprüfen und dann bearbeiten, indem Sie auf * * *  klicken oder durch Klicken auf * * * löschen ✖ .

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail

angeben. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

> Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

Anforderungen für das Backup von SQL Ressourcen

Bevor Sie eine SQL-Ressource sichern, müssen Sie sicherstellen, dass mehrere Anforderungen erfüllt sind.

- Sie müssen eine Ressource von einem nicht-NetApp Storage-System in ein NetApp Storage-System migriert haben.
- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung zu einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Der von einem Active Directory (AD)-Benutzer initiierte Backup-Vorgang schlägt fehl, wenn die SQL-Instanz-Anmeldeinformationen nicht dem AD-Benutzer oder der AD-Gruppe zugewiesen sind. Sie müssen die SQL-Instanz-Anmeldeinformationen AD-Benutzer oder -Gruppe über die Seite **Einstellungen** > **Benutzerzugriff** zuweisen.
- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn eine Ressourcengruppe mehrere Datenbanken von verschiedenen Hosts enthält, kann der Backup-Vorgang auf einigen Hosts aufgrund von Netzwerkproblemen spät ausgelöst werden. Sie sollten den Wert von FMaxRetryForUninitializedHosts in Web.config mit dem Cmdlet Set-SmConfigSettings PS konfigurieren.

Backup von SQL-Ressourcen

Wenn eine Ressource noch nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

Über diese Aufgabe

- Für die Authentifizierung von Windows-Anmeldeinformationen müssen Sie die Anmeldeinformationen einrichten, bevor Sie die Plug-ins installieren.
- Für die Authentifizierung der SQL Server-Instanz müssen Sie die Anmeldeinformationen nach der Installation der Plug-ins hinzufügen.
- Für die gMSA-Authentifizierung müssen Sie gMSA beim Registrieren des Hosts mit SnapCenter auf der Seite **Add Host** oder **Modify Host** einrichten, um den gMSA zu aktivieren und zu verwenden.
- Wenn der Host mit gMSA hinzugefügt wird und der gMSA über Login- und System Admin-Berechtigungen verfügt, wird das gMSA verwendet, um eine Verbindung zur SQL-Instanz herzustellen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen * Datenbank* oder **Instanz** oder **Verfügbarkeitsgruppe** aus der Dropdown-Liste **Ansicht** aus.

   a. Wählen Sie die Datenbank, die Instanz oder die Verfügbarkeitsgruppe aus, die Sie sichern möchten.

      Wenn Sie eine Sicherungskopie einer Instanz erstellen, sind die Informationen zum letzten Sicherungsstatus oder zum Zeitstempel dieser Instanz auf der Seite Ressourcen nicht verfügbar.

   In der Topologieansicht lässt sich nicht unterscheiden, ob der Backup-Status, der Zeitstempel oder das Backup für eine Instanz oder eine Datenbank gilt.

3. Aktivieren Sie auf der Seite „Ressourcen“ das Kontrollkästchen **benutzerdefiniertes Namensformat für Snapshot-Kopie**, und geben Sie dann ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

   Beispiel: Custtext_Policy_hostname oder Resource_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

4. Führen Sie auf der Seite Richtlinien die folgenden Aufgaben aus:

   a. Wählen Sie im Abschnitt Richtlinien eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine Richtlinie erstellen, indem Sie * * auswählen  , um den Richtlinien-Assistenten zu starten.

      Im Abschnitt * Zeitpläne für ausgewählte Richtlinien konfigurieren* werden die ausgewählten Richtlinien aufgelistet.

   b. Wählen Sie * *  in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Dialogfeld **Add Schedules for Policy** `policy_name` den Zeitplan und wählen Sie dann **OK** aus.

      Hier `policy_name` ist der Name der Richtlinie, die Sie ausgewählt haben.

   Die konfigurierten Zeitpläne sind in der Spalte **angewendete Zeitpläne** aufgeführt.

   a. Wählen Sie den Microsoft SQL Server Scheduler verwenden* aus, und wählen Sie dann die Planerinstanz aus der Dropdown-Liste **Scheduler Instance** aus, die mit der Planungsrichtlinie verknüpft ist.

5. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

   a. Wählen Sie den Verifikationsserver aus der Dropdown-Liste **Überprüfungsserver** aus.

      Sie können mehrere Verifizierungsserver auswählen (lokaler Host oder Remote-Host).

   Die Version des Verifizierungsservers sollte gleich oder höher sein als die Version der Edition des SQL-Servers, der die primäre Datenbank hostet.

a. Wählen Sie **sekundäre Lokatoren laden, um Backups auf dem sekundären Speichersystem zu überprüfen**, um Ihre Backups auf dem sekundären Speichersystem zu überprüfen.

b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und wählen Sie dann * * aus.

c. Führen Sie im Dialogfeld Add Verification Schedules_Policy_Name_ die folgenden Aktionen durch:

Ihr Ziel ist	Tun Sie das…
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen**.

Wenn der Verifikationsserver keine Speicherverbindung hat, schlägt der Verifizierungsvorgang mit Fehler fehl: Datenträger konnte nicht bereitgestellt werden.

d. Wählen Sie **OK**.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

7. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.

Die Seite der Datenbanktopologie wird angezeigt.

8. Wählen Sie **Jetzt sichern**.
9. Führen Sie auf der Seite Backup die folgenden Schritte aus:

a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie für das Backup verwenden möchten.

Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

b. Wählen Sie zur Überprüfung Ihres Backups **nach dem Backup**.

c. Wählen Sie **Backup**.

Sie sollten den im Windows Scheduler oder SQL Server Agent erstellten Sicherungsauftrag nicht umbenennen.

Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

Es wird eine implizite Ressourcengruppe erstellt. Sie können dies anzeigen, indem Sie auf der Seite „Benutzerzugriff“ den jeweiligen Benutzer oder die jeweilige Gruppe auswählen. Der implizite Gruppentyp lautet „`Ressource`“.

10. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Nachdem Sie fertig sind

- In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung erkennen.

  "SnapMirror oder SnapVault-Beziehung kann nach MetroCluster Failover nicht erkannt werden"

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java Heap-Größe für das SnapCenter-Plug-in für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen. Um die Java-Heap-Größe zu erhöhen, suchen Sie nach der Skriptdatei /opt/netapp/init_scvservice. In diesem Skript startet der `do_start method` Befehl den SnapCenter VMware Plug-in-Service. Aktualisieren Sie diesen Befehl auf Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

"Sichern Sie Ressourcen mit PowerShell cmdlets"

"Backup-Vorgänge schlagen wegen der Verzögerung im TCP_TIMEOUT bei MySQL-Verbindungsfehler fehl"

"Das Backup schlägt mit dem Windows Scheduler-Fehler fehl"

"Fehler beim Quiesce oder Gruppieren von Ressourcen"

Sichern Sie SQL Server-Ressourcengruppen

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe durchsuchen, indem Sie den Namen der Ressourcengruppe in das Suchfeld eingeben, oder indem Sie * *[Filtersymbol]auswählen und dann das Tag auswählen. Sie können dann * * auswählen[Filtersymbol], um das Filterfenster zu schließen.

3. Wählen Sie auf der Seite Ressourcengruppen die Ressourcengruppe aus, die Sie sichern möchten, und wählen Sie dann **Jetzt sichern** aus.
4. Führen Sie auf der Seite Backup die folgenden Schritte aus:

a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

   Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

b. Wählen Sie nach dem Backup **Verify** aus, um das On-Demand-Backup zu überprüfen.

   Die Option **Verify** in der Richtlinie gilt nur für geplante Jobs.

c. Wählen Sie **Backup**.

5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor** > **Jobs** auswählen.

Verwandte Informationen

"Erstellen von Backup-Richtlinien für SQL Server-Datenbanken"

"Erstellen von Ressourcengruppen und Anhängen von Richtlinien für SQL Server"

"Sichern Sie Ressourcen mit PowerShell cmdlets"

"Backup-Vorgänge schlagen wegen der Verzögerung im TCP_TIMEOUT bei MySQL-Verbindungsfehler fehl"

"Das Backup schlägt mit dem Windows Scheduler-Fehler fehl"

Monitoring von Backup-Vorgängen

Überwachen Sie die Backup-Vorgänge für SQL-Ressourcen auf der Seite SnapCenter-Jobs

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Jobs angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.

3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

   Obwohl der Status des Sicherungsauftrags angezeigt wird, wird beim Klicken auf Jobdetails möglicherweise angezeigt , dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Überwachen Sie Datenschutzvorgänge für SQL-Ressourcen im Bereich „Aktivität“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten Backup-Vorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf den Bereich „Aktivität“, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Job-Details** aufgeführt.

Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um Datensicherungsvorgänge durchzuführen.

Bevor Sie beginnen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige Management-LIF-IP-Adresse verfügen.

Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mit dem Cmdlet Open-SmConnection.

   In diesem Beispiel wird eine PowerShell Sitzung geöffnet:

   ```
   PS C:\> Open-SmConnection
   ```

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel werden neue Anmeldeinformationen mit dem Namen FinanceAdmin mit Windows-Anmeldeinformationen erstellt:

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Sichern Sie Ressourcen mit PowerShell cmdlets

Sie können die PowerShell Commandlets zum Sichern von SQL Server-Datenbanken oder Windows-Dateisystemen verwenden. Dazu gehört die Sicherung einer SQL Server-Datenbank oder eines Windows-Dateisystems, einschließlich der Herstellung einer Verbindung mit dem SnapCenter-Server, der Ermittlung der SQL Server-Datenbankinstanzen oder Windows-Dateisysteme, das Hinzufügen einer Richtlinie, das Erstellen einer Backup-Ressourcengruppe, das Sichern und das Überprüfen des Backups.

Bevor Sie beginnen

- Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.
- Sie müssen die Speichersystemverbindung hinzugefügt und Anmeldedaten erstellt haben.
- Sie müssen Hosts hinzugefügt und Ressourcen erkannt haben.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

   ```
   Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
   ```

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   Dieses Beispiel erstellt eine neue Backup-Richtlinie mit einem SQL Backup-Typ von FullBackup:

   ```
   PS C:\> Add-SmPolicy -PolicyName TESTPolicy
   -PluginPolicyType SCSQL -PolicyType Backup
   -SqlBackupType FullBackup -Verbose
   ```

   In diesem Beispiel wird eine neue Backup-Richtlinie mit einem Backup-Typ von CrashConsistent für Windows File-Systeme erstellt:

   ```
   PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
   -PluginPolicyType SCW -PolicyType Backup
   -ScwBackupType CrashConsistent -Verbose
   ```

3. Ermitteln Sie Host-Ressourcen mit dem Cmdlet "Get-SmResources".

   Dieses Beispiel ermittelt die Ressourcen für das Microsoft SQL Plug-in auf dem angegebenen Host:

   ```
   C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
   -PluginCode SCSQL
   ```

   In diesem Beispiel werden Ressourcen für Windows File-Systeme auf dem angegebenen Host ermittelt:

   ```
   C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
   -PluginCode SCW
   ```

4. Fügen Sie mit dem Cmdlet "Add-SmResourceGroup" eine neue Ressourcengruppe zu SnapCenter hinzu.

   In diesem Beispiel wird eine neue Ressourcengruppe für die Sicherung von SQL-Datenbanken mit der

angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

Dieses Beispiel erstellt eine neue Windows Dateisystem-Backup-Ressourcengruppe mit der angegebenen Richtlinie und Ressourcen:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Zeigen Sie den Status des Backup-Jobs mit dem Cmdlet "Get-SmBackupReport" an.

   In diesem Beispiel wird ein Job-Summary-Bericht aller Jobs angezeigt, die am angegebenen Datum ausgeführt wurden:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Abbrechen des SnapCenter-Plug-ins für Microsoft SQL Server-Backup-Vorgänge

Sie können laufende, in die Warteschlange eingereihte oder nicht reaktionsfähige Backup-Vorgänge abbrechen. Wenn Sie einen Sicherungsvorgang abbrechen, stoppt der SnapCenter-Server den Vorgang und entfernt alle Snapshots aus dem Speicher, wenn das erstellte Backup nicht beim SnapCenter-Server registriert ist. Wenn das Backup bereits beim SnapCenter-Server registriert ist, wird ein Rollback des bereits erstellten Snapshots selbst dann nicht durchgeführt, wenn der Abbruch ausgelöst wurde.

Bevor Sie beginnen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um

Wiederherstellungsvorgänge abzubrechen.

- Sie können nur das Protokoll oder die vollständigen Backup-Vorgänge abbrechen, die in die Warteschlange gestellt werden oder ausgeführt werden.
- Sie können den Vorgang nicht abbrechen, nachdem die Überprüfung gestartet wurde.

  Wenn Sie den Vorgang vor der Überprüfung abbrechen, wird der Vorgang abgebrochen und der Verifizierungsvorgang wird nicht durchgeführt.

- Sie können einen Sicherungsvorgang entweder über die Seite Überwachen oder über den Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter GUI können Sie PowerShell cmdlets verwenden, um Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Wählen Sie im linken Navigationsbereich **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und wählen Sie **Job abbrechen** .
Aktivitätsbereich	1. Wählen Sie nach dem Starten des Backupjobs im Aktivitätsbereich die Option aus , um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Wählen Sie auf der Seite Job-Details die Option **Job abbrechen** aus.

Ergebnis

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt. Wenn der Vorgang, den Sie abgebrochen haben, im Status Abbrechen oder Ausführen nicht reagiert, sollten Sie das Cmdlet ausführen `Cancel-SmJob -JobID <int> -Force` , um den Sicherungsvorgang gewaltsam anzuhalten.

Sehen Sie sich SQL Server Backups und Klone auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

Sie können die folgenden Symbole in der Ansicht **Kopien verwalten** anzeigen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Vault-Kopien).

-  Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapMirror-Technologie gespiegelt werden.
-  Zeigt die Anzahl der Backups und Klone an, die auf dem sekundären Speicher mithilfe der SnapVault-Technologie repliziert werden.
  - Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden.

    Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

Wenn Sie eine sekundäre Beziehung als SnapMirror Business Continuity (SM-BC) haben, werden die folgenden zusätzlichen Symbole angezeigt:

-  Impliziert, dass der Replikatstandort hochgefahren ist.
-  Bedeutet, dass der Replikatstandort ausgefallen ist.
-  Impliziert, dass die sekundäre Spiegel- oder Vault-Beziehung nicht wiederhergestellt wurde.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

   Wenn die ausgewählte Ressource eine geklonte Datenbank ist, schützen Sie die geklonte Datenbank, wird die Quelle des Klons auf der Seite Topologie angezeigt. Klicken Sie auf **Details**, um das zum Klonen

verwendete Backup anzuzeigen.

Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Prüfen Sie die Übersichtskarte, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Storage verfügbar sind.

   Im Abschnitt **Übersichtskarte** wird die Gesamtzahl der Backups und Klone angezeigt.

   Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

   Wenn ein SnapLock-fähiges Backup durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die primäre und sekundäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen wird. Ein wöchentlicher Zeitplan aktualisiert auch die primäre und sekundäre SnapLock-Ablaufzeit, die von ONTAP abgerufen wird.

   Wenn die Applikationsressource über mehrere Volumes verteilt ist, ist die SnapLock-Ablaufzeit für das Backup die längste SnapLock-Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock-Ablaufzeit wird von ONTAP abgerufen.

   Wenn Sie für SnapMirror Business Continuity (SM-BC) auf die Schaltfläche * Aktualisieren* klicken, wird das SnapCenter-Backup-Inventar aktualisiert, indem Sie ONTAP sowohl für primäre als auch für Replikatstandorte abfragen. Ein wöchentlicher Zeitplan führt diese Aktivität auch für alle Datenbanken durch, die eine SM-BC-Beziehung enthalten.

   - Bei SM-BC sollten die Beziehungen zwischen Async Mirror, Vault und MirrorVault zum neuen primären Ziel nach dem Failover manuell konfiguriert werden.
   - Nach dem Failover sollte ein Backup erstellt werden, damit SnapCenter den Failover erkennt. Sie können erst dann auf **Refresh** klicken, wenn ein Backup erstellt wurde.

5. Klicken Sie in der Ansicht **Kopien verwalten** auf **Backups** oder **Klone** auf dem primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf die Datensicherungssymbole, um Vorgänge zum Wiederherstellen, Klonen, Umbenennen und Löschen durchzuführen.

   Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen.

7. Wählen Sie einen Klon aus der Tabelle aus und klicken Sie auf **Clone Split**.
8. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .

Entfernen Sie Backups mithilfe von PowerShell Cmdlets

Mit dem Cmdlet "Remove-SmBackup" können Sie Backups löschen, wenn Sie diese nicht mehr für andere Datenschutzvorgänge benötigen.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Löschen Sie ein oder mehrere Backups mit dem Cmdlet "Remove-SmBackup".

   In diesem Beispiel werden zwei Backups mithilfe der Backup-IDs gelöscht:

```
Remove-SmBackup -BackupIds 3,4
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```

Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets

Sie können das Cmdlet "Remove-SmBackup" verwenden, um die Anzahl der Backups für sekundäre Backups zu bereinigen, die keinen Snapshot haben. Sie können dieses Cmdlet verwenden, wenn die in der Topologie zum Verwalten von Kopien angezeigten Snapshots insgesamt nicht mit der Einstellung für die Aufbewahrung von sekundären SpeicherSnapshot übereinstimmen.

Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Bereinigen Sie die Anzahl der sekundären Backups mit dem Parameter -CleanupSecondaryBackups.

   In diesem Beispiel wird die Anzahl der Backups für sekundäre Backups ohne Snapshots bereinigt:

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"):
```