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

SnapCenter Software 4.7

NetApp
August 07, 2024

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-47/protect-scsql/reference_back_up_sql_server_database_or_instance_or_availability_group.html on August 07, 2024. Always check docs.netapp.com for the latest.

Inhalt

Sichern Sie die SQL Server-Datenbank, -Instanz oder -Verfügbarkeitsgruppe . . . 1
Backup-Workflow . . . 1
Bestimmen Sie, ob Ressourcen für ein Backup verfügbar sind . . . 2
Migrieren von Ressourcen auf ein NetApp Storage-System . . . 4
Erstellen von Backup-Richtlinien für SQL Server-Datenbanken . . . 6
Erstellen von Ressourcengruppen und Anhängen von Richtlinien für SQL Server . . . 15
Anforderungen für das Backup von SQL Ressourcen . . . 17
Backup von SQL-Ressourcen . . . 18
Sichern Sie SQL Server-Ressourcengruppen . . . 21
Monitoring von Backup-Vorgängen . . . 22
Erstellen Sie eine Storage-Systemverbindung und eine Zugangsdaten mit PowerShell Cmdlets . . . 23
Sichern Sie Ressourcen mit PowerShell cmdlets . . . 24
Abbrechen des SnapCenter-Plug-ins für Microsoft SQL Server-Backup-Vorgänge . . . 26
Sehen Sie sich SQL Server Backups und Klone auf der Seite Topologie an . . . 27
Entfernen Sie Backups mithilfe von PowerShell Cmdlets . . . 29
Reinigen Sie die Anzahl der sekundären Backups mit PowerShell cmdlets . . . 29

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

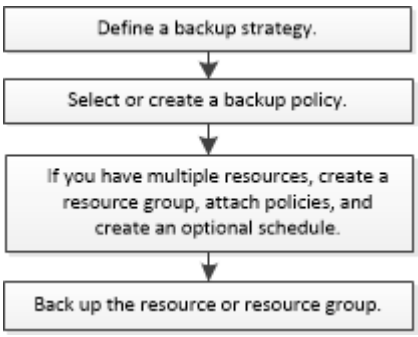
Backup-Workflow

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. Ausführliche Informationen zu PowerShell Cmdlets finden Sie in der Hilfe zu SnapCenter Cmdlet oder in der "SnapCenter Software Cmdlet Referenzhandbuch"

Wie SnapCenter Datenbanken sichert

SnapCenter nutzt Snapshot-Kopiertechnologie für das Backup der SQL Server Datenbanken, die sich auf LUNs oder VMDKs befinden. SnapCenter erstellt das Backup, indem Snapshot Kopien der Datenbanken erstellt werden.

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 mithilfe von Snapshot-Kopien gleichzeitig gesichert. Wenn die maximale Anzahl gleichzeitiger Backup-Datenbanken 35 beträgt und mehr als 35 Datenbanken in einem Storage Volume residieren, entspricht die Gesamtzahl der erstellten Snapshot-Kopien der Anzahl der Datenbanken, die durch 35 geteilt werden.

Sie können die maximale Anzahl von Datenbanken für jede Snapshot-Kopie in der Backup-Richtlinie konfigurieren.

Wenn SnapCenter eine Snapshot Kopie erstellt, wird das gesamte Storage-System-Volume in der Snapshot Kopie 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 nicht aus der Snapshot Kopie 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.

Was Sie brauchen

- 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 auf 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 die Datenbank auf Storage anderer Anbieter liegt, `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 Storage befindet und nicht geschützt ist, `Not protected` Wird in der Spalte **Gesamtstatus** angezeigt.
   - Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, wird auf der Benutzeroberfläche angezeigt `Backup not run` Meldung in der Spalte **Gesamtstatus**.
   - Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, und wenn das Backup für die Datenbank ausgelöst wird, wird die Benutzeroberfläche angezeigt `Backup succeeded` Meldung in der Spalte **Gesamtstatus**.

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.

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.

Was Sie brauchen

- 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 begrenzen und Sperren zu erhalten, anstatt eine interne Snapshot-Kopie der Datenbank zu verwenden.

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.

Was Sie brauchen

- 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 Snapshot Kopien in eine Spiegelung oder einen Vault replizieren, muss der SnapCenter Administrator Ihnen die Storage Virtual Machines (SVMs) sowohl für die Quell-Volumes als auch 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

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.

- 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 **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Name den Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Sicherungstyp die folgenden Schritte durch:

   a. Wählen Sie den Sicherungstyp:

Ihr Ziel ist	Tun Sie das…
Sichern Sie die Datenbankdateien und Transaktions-Logs und zur Verkürzung der Transaktions-Logs	i. Wählen Sie **Vollbackup und Log Backup** aus. ii. Geben Sie die maximale Anzahl an Datenbanken ein, die für jede Snapshot Kopie gesichert werden sollen. Sie müssen diesen Wert erhöhen, wenn Sie mehrere Backup-Vorgänge gleichzeitig ausführen möchten.
Sichern Sie die Datenbankdateien	i. Wählen Sie * Vollbackup* aus. ii. Geben Sie die maximale Anzahl an Datenbanken ein, die für jede Snapshot Kopie gesichert werden sollen. Der Standardwert ist 100 Sie müssen diesen Wert erhöhen, wenn Sie mehrere Backup-Vorgänge gleichzeitig ausführen möchten.
Sichern Sie die Transaktionsprotokolle	Wählen Sie **Backup protokollieren**.

b. 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.

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

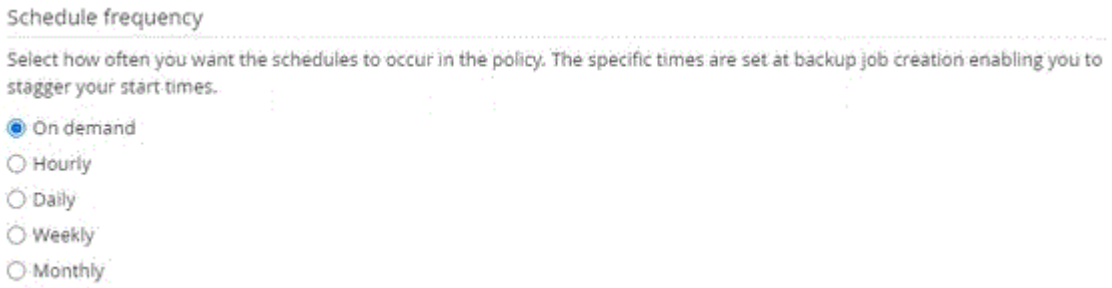
Für dieses Feld…	Tun Sie das…
Nur auf bevorzugtem Backup-Replikat sichern	Wählen Sie diese Option aus, um nur auf dem bevorzugten Backup-Replikat zu sichern. Über die für die AG im SQL Server konfigurierten Backup-Einstellungen wird das bevorzugte Backup-Replikat entschieden.
Wählen Sie Replikate für die Sicherung aus	Wählen Sie das primäre AG-Replikat oder das sekundäre AG-Replikat für das Backup aus.

Für dieses Feld…	Tun Sie das…
Backup-Priorität (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.

d. Wenn Sie das Backup planen möchten, das Sie mit dieser Richtlinie erstellen möchten, geben Sie den Terminplantyp an, indem Sie entweder **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

   Sie können einen Terminplantyp 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.

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

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

Ihr Ziel ist	Tun Sie das…
Aufbewahrung von nur einer bestimmten Anzahl von Snapshot Kopien	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.
Bewahren Sie die Backup-Kopien für eine bestimmte Anzahl von Tagen auf	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.

b. Führen Sie im Abschnitt **vollständige Backup-Aufbewahrungs-Einstellungen** für die Einstellungen für On Demand-Aufbewahrung die folgenden Aktionen aus:

Für dieses Feld…	Tun Sie das…
Gesamtzahl der zu Aufbewahrung erforderlichen Snapshot Kopien	Wenn Sie die Anzahl der Snapshot Kopien angeben möchten, die beibehalten werden sollen, wählen Sie **Snapshot-Kopien insgesamt, die beibehalten werden sollen** aus. Wenn die Anzahl der Snapshot Kopien die angegebene Anzahl überschreitet, werden die Snapshot Kopien mit den ältesten Kopien gelöscht, die zuerst gelöscht wurden. 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. Standardmäßig ist der Wert der Aufbewahrungsanzahl auf 2 festgelegt. Wenn Sie die Aufbewahrungsanzahl auf 1 festlegen, kann der Aufbewahrungsvorgang möglicherweise fehlschlagen, da die erste Snapshot Kopie die Referenzkopie für die SnapVault-Beziehung ist, bis eine neuere Snapshot Kopie auf das Ziel repliziert wird.
Behalten Sie Snapshot Kopien für bei	Wenn Sie die Anzahl der Tage angeben möchten, für die Sie die Snapshot Kopien behalten möchten, bevor Sie sie löschen, wählen Sie **Snapshot Kopien für** beibehalten aus.

c. 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.

Für dieses Feld…	Tun Sie das…
Gesamtzahl der zu Aufbewahrung erforderlichen Snapshot Kopien	Wenn Sie die Anzahl der Snapshot Kopien angeben möchten, die beibehalten werden sollen, wählen Sie **Snapshot-Kopien insgesamt, die beibehalten werden sollen** aus. Wenn die Anzahl der Snapshot Kopien die angegebene Anzahl überschreitet, werden die Snapshot Kopien mit den ältesten Kopien gelöscht, die zuerst gelöscht wurden. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 festlegen, kann der Aufbewahrungsvorgang möglicherweise fehlschlagen, da die erste Snapshot Kopie die Referenzkopie für die SnapVault-Beziehung ist, bis eine neuere Snapshot Kopie auf das Ziel repliziert wird.
Behalten Sie Snapshot Kopien für bei	Wenn Sie die Anzahl der Tage angeben möchten, für die Sie die Snapshot Kopien behalten möchten, bevor Sie sie löschen, wählen Sie **Snapshot Kopien für** beibehalten aus.

Die Aufbewahrung der Snapshot Kopie für dieses Protokoll ist standardmäßig auf 7 Tage festgelegt. Verwenden Sie Set-SmPolicy Cmdlet, um die Aufbewahrung von Snapshot-Protokollkopien zu ändern.

In diesem Beispiel wird die Aufbewahrung von Snapshot-Kopien für das Protokoll auf 2 festgelegt:

```
Set-SmPolicy -PolicyName 'newpol' -PolicyType 'Backup' -PluginPolicyType
'SCSQL' -sqlbackuptype 'FullBackupAndLogBackup' -RetentionSettings
@{BackupType='DATA';ScheduleType='Hourly';RetentionCount=2},@{BackupType
='LOG_SNAPSHOT';ScheduleType='None';RetentionCount=2},@{BackupType='LOG'
;ScheduleType='Hourly';RetentionCount=2} -scheduletype 'Hourly'
```

+ "SnapCenter behält Snapshot Kopien der Datenbank bei"

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

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Spiegelkopien von Backup-Sets auf einem anderen Volume (SnapMirror) zu erstellen.
Aktualisieren Sie die SnapVault nach dem Erstellen einer Snapshot Kopie	Wählen Sie diese Option aus, um die Disk-to-Disk-Backup-Replikation durchzuführen.
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Abhängig von dem ausgewählten Etikett der Snapshot Kopie wendet ONTAP die Aufbewahrungsrichtlinie für sekundäre Snapshot Kopien an, die mit dem Etikett übereinstimmt. ⓘ 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 bei Wiederholungszählung	Geben Sie die Anzahl der Replikationsversuche ein, die vor dem Anhalten des Prozesses auftreten sollen.

8. 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 konfigurieren, damit der sekundäre Storage die maximale Anzahl an Snapshot Kopien nicht erreicht.

9. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
   a. Wählen Sie im Abschnitt Überprüfung ausführen für folgende Backup-Pläne die Zeitplanhäufigkeit aus.
   b. Führen Sie im Abschnitt Optionen für die Datenbankkonsistenzprüfung die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Beschränkung der Integritätsstruktur auf die physische Struktur der Datenbank (PHYSICAL_ONLY)	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.
Alle Informationsmeldungen unterdrücken (KEINE INFOMSGS)	Wählen Sie * Alle Informationsmeldungen (NO_INFOMSGS)* aus, um alle Informationsmeldungen zu unterdrücken. Standardmäßig ausgewählt.
Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL_ERRORMSGS)	Wählen Sie **Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL_ERRORMSGS)** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen.
Nicht geclusterte Indizes (NOINDEX) nicht prüfen	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.
Beschränken Sie die Prüfungen, und erhalten Sie die Sperren anstelle einer internen Snapshot-Kopie der Datenbank (TABLOCK).	Wählen Sie **Limit the Checks und erhalten Sie die Sperren anstatt eine interne Datenbank Snapshot Kopie (TABLOCK)** zu verwenden, um die Prüfungen zu begrenzen und Sperren zu erhalten, anstatt eine interne Datenbank Snapshot Kopie zu verwenden.

c. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss bestätigen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.

d. 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.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **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.

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 Namen und ein Format für die benutzerdefinierte Snapshot Kopie ein. Beispiel: Custtext_resourcegruppe_Policy_hostname oder resourcegruppe_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie 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 Zeitpläne für ausgewählte Richtlinien konfigurieren auf + In der Spalte Zeitplan konfigurieren 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 Verifizierungszeitplan 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 Daten überprüfen und dann bearbeiten, indem Sie auf * klicken * Oder löschen Sie sie, indem Sie auf * klicken *.

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**.

Weitere 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. 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 * 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 **Custom Name Format for Snapshot copy** und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Namen der Snapshot Kopie verwenden möchten.

   Beispiel: Custtext_Policy_hostname oder Resource_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie 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 auf * klicken + * Um den Policy Wizard zu starten.

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

   b. Klicken Sie Auf + In der Spalte Zeitplan konfigurieren für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. In der Option * Pläne für Police hinzufügen* `policy_name` Konfigurieren Sie den Zeitplan, und klicken Sie dann auf **OK**.

      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 Verifizierungszeitplan 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**.

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

   d. Klicken Sie auf **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 klicken Sie dann auf **Fertig stellen**.

   Die Seite der Datenbanktopologie wird angezeigt.

8. Klicken Sie auf **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. Klicken Sie Auf **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 Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Nach Ihrer Beendigung

- 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, das `do_start method` Befehl startet den SnapCenter-VMware-Plug-in-Service. Aktualisieren Sie diesen Befehl auf

Folgendes: `Java -jar -Xmx8192M -Xms4096M`.

Weitere 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. 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 **Ressourcengruppe** aus.

   Sie können die Ressourcengruppe entweder durch Eingabe des Ressourcengruppennamens in das Suchfeld oder durch Klicken auf * durchsuchen* Und dann das Tag auswählen. Sie können dann auf * klicken* Zum Schließen des Filterfensters.

3. Wählen Sie auf der Seite Ressourcengruppen die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
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. Klicken Sie Auf **Backup**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Weitere 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
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- 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 Auf Filtern der Liste, sodass 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.

   Der Status des Backupjobs wird zwar angezeigt Wenn Sie auf die Jobdetails klicken, wird möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Backup-Vorgangs 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. Wenn Sie Plug-in für SQL Server oder Plug-in für Exchange Server verwenden, werden im Aktivitätsbereich auch Informationen über den erneuten Seeding 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 Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt.

   Wenn Sie auf einen der Vorgänge klicken, werden die Arbeitsdetails auf der Seite Jobdetails 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.

Was Sie brauchen

- 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 verweisen "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.

Was Sie brauchen

- 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 verweisen "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 Backup-Vorgang abbrechen, stoppt der SnapCenter-Server den Vorgang und entfernt alle Snapshot-Kopien aus dem Storage, falls das erstellte Backup nicht beim SnapCenter Server registriert ist. Wenn das Backup bereits beim SnapCenter Server registriert ist, wird die bereits erstellte Snapshot-Kopie nicht wieder zurückgeführt, auch wenn der Vorgang ausgelöst wird.

Was Sie brauchen

- 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.

Schritt

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitor-Seite	1. Klicken Sie im linken Navigationsbereich auf **Monitor** > **Jobs**. 2. Wählen Sie den Job aus und klicken Sie auf **Job abbrechen** .
Aktivitätsbereich	1. Klicken Sie nach dem Starten des Backup-Jobs auf Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt. 2. Wählen Sie den Vorgang aus. 3. Klicken Sie auf der Seite Jobdetails auf **Job abbrechen**.

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 den ausführen `Cancel-SmJob -JobID <int> -Force` Cmdlet zum gewaltsamen Beenden des Backup-Vorgangs.

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 mithilfe der SnapMirror Technologie auf dem sekundären Storage gespiegelt werden.

- Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault Technologie auf dem sekundären Storage 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.

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.
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 anschließend 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 verweisen "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 keine Snapshot-Kopien haben. Sie möchten dieses Cmdlet vielleicht verwenden, wenn die gesamten Snapshot Kopien, die in der Topologie zum Managen von Kopien angezeigt werden, nicht mit der Einstellung zum Speichern von sekundären Storage Snapshot Kopien 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 verweisen "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.

   Dieses Beispiel bereinigt die Anzahl der Backups für sekundäre Backups ohne Snapshot-Kopien:

```
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"):
```

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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