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

SnapCenter software

NetApp
November 06, 2025

Inhalt

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

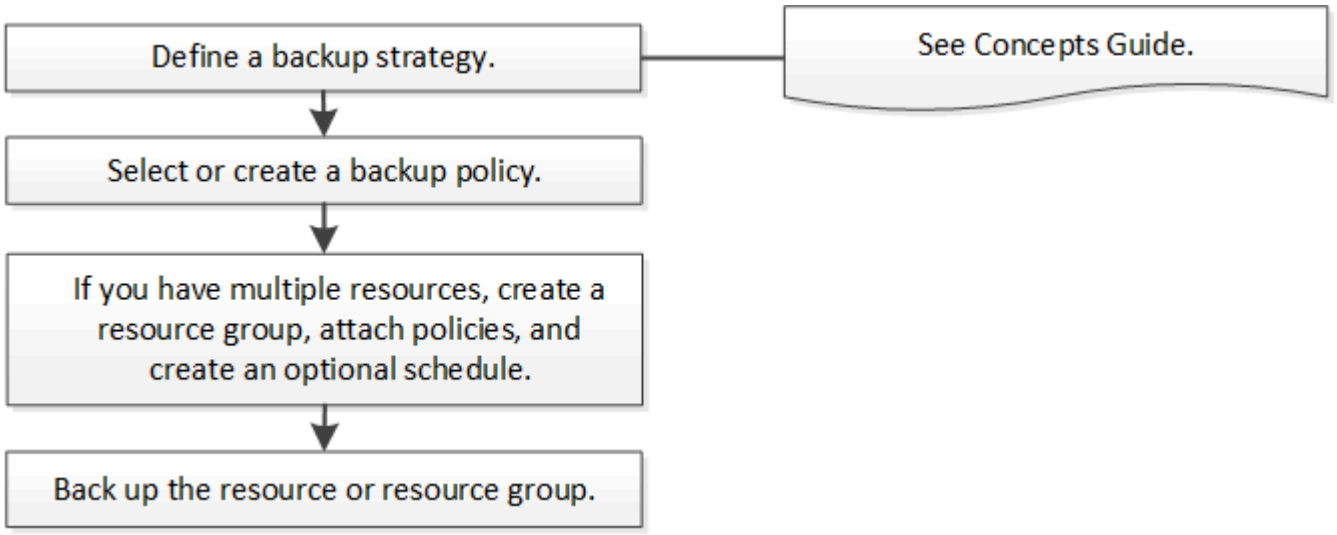
Sicherungsworkflow

Wenn Sie das SnapCenter -Plug-in für Microsoft SQL Server in Ihrer Umgebung installieren, können Sie SnapCenter zum Sichern der SQL Server-Ressourcen verwenden.

Sie können mehrere Sicherungen so planen, dass sie gleichzeitig auf mehreren Servern ausgeführt werden.

Sicherungs- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressource ausgeführt werden.

Der folgende Arbeitsablauf zeigt die Reihenfolge, in der Sie die Sicherungsvorgänge durchführen müssen:



Die Optionen „Jetzt sichern“, „Wiederherstellen“, „Sicherungen verwalten“ und „Klonen“ auf der Seite „Ressourcen“ sind deaktiviert, wenn Sie eine Nicht- NetApp -LUN, eine beschädigte Datenbank oder eine Datenbank auswählen, die wiederhergestellt wird.

Sie können PowerShell-Cmdlets auch manuell oder in Skripts verwenden, um Sicherungs-, Wiederherstellungs-, Überprüfungs- und Klonvorgänge durchzuführen. Ausführliche Informationen zu PowerShell-Cmdlets finden Sie in der SnapCenter -Cmdlet-Hilfe oder im "Referenzhandbuch für SnapCenter -Software-Cmdlets"

So sichert SnapCenter Datenbanken

SnapCenter verwendet Snapshot-Technologie, um die SQL Server-Datenbanken zu sichern, die sich auf LUNs oder VMDKs befinden. SnapCenter erstellt das Backup, indem es Snapshots der Datenbanken erstellt.

Wenn Sie auf der Seite „Ressourcen“ eine Datenbank für eine vollständige Datenbanksicherung auswählen, wählt SnapCenter automatisch alle anderen Datenbanken aus, die sich auf demselben Speichervolume 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 erneut auswählen.

Alle Datenbanken, die sich auf einem einzelnen Volume befinden, werden gleichzeitig mithilfe von Snapshots gesichert. Wenn die maximale Anzahl gleichzeitiger Sicherungsdatenbanken 35 beträgt und sich mehr als 35 Datenbanken in einem Speichervolume befinden, entspricht die Gesamtzahl der erstellten Snapshots der Anzahl der Datenbanken geteilt durch 35.

Sie können die maximale Anzahl von Datenbanken für jeden Snapshot in der Sicherungsrichtlinie konfigurieren.

Wenn SnapCenter einen Snapshot erstellt, wird das gesamte Speichersystemvolume im Snapshot erfasst. Allerdings ist die Sicherung nur für den SQL-Hostserver gültig, für den die Sicherung erstellt wurde.

Wenn sich Daten von anderen SQL-Hostservern auf demselben Volume befinden, können diese Daten nicht aus dem Snapshot wiederhergestellt werden.

Weitere Informationen finden

"Vorgänge zum Stilllegen oder Gruppieren von Ressourcen schlagen fehl"

Ermitteln, ob Ressourcen für die Sicherung verfügbar sind

Ressourcen sind die Datenbanken, Anwendungsinstanzen, Verfügbarkeitsgruppen und ähnliche Komponenten, die von den von Ihnen installierten Plug-Ins verwaltet werden. Sie können diese Ressourcen zu Ressourcengruppen hinzufügen, um Datenschutzaufgaben auszuführen. Zunächst müssen Sie jedoch ermitteln, welche Ressourcen Ihnen zur Verfügung stehen. Durch die Ermittlung der verfügbaren Ressourcen wird auch überprüft, ob die Plug-In-Installation erfolgreich abgeschlossen wurde.

Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation von SnapCenter Server, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen und das Hinzufügen von Anmeldeinformationen abgeschlossen haben.
- Um die Microsoft SQL-Datenbanken zu erkennen, muss 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 obige 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 kann ein SQL- oder Windows-Benutzer sein.
- Um die Microsoft SQL-Datenbanken in einem Windows-Cluster zu erkennen, müssen Sie den TCP/IP-Port der Failover Cluster Instance (FCI) entsperren.
- Wenn sich Datenbanken auf VMware RDM LUNs oder VMDKs befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren.

  Weitere Informationen finden Sie unter "Bereitstellen des SnapCenter Plug-in for VMware vSphere"
- Wenn der Host mit gMSA hinzugefügt wird und das gMSA über Anmelde- und Systemadministratorrechte verfügt, wird das gMSA zum Herstellen einer Verbindung mit der SQL-Instanz verwendet.

Informationen zu diesem Vorgang

Sie können keine Datenbanken sichern, wenn die Option **Gesamtstatus** auf der Seite „Details“ auf „Nicht für Sicherung verfügbar“ eingestellt ist. Die Option **Gesamtstatus** wird auf „Nicht für Sicherung verfügbar“ gesetzt, wenn eine der folgenden Bedingungen zutrifft:

- Datenbanken befinden sich nicht auf einer NetApp LUN.
- Die Datenbanken befinden sich nicht im Normalzustand.

  Datenbanken befinden sich nicht im Normalzustand, wenn sie offline sind, wiederhergestellt werden, die Wiederherstellung aussteht, verdächtig ist usw.

- Datenbanken verfügen über unzureichende Berechtigungen.

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

SnapCenter kann nur die primäre Datenbank sichern, wenn Sie über eine Verfügbarkeitsgruppenkonfiguration auf SQL Server Standard Edition verfügen.

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“ aus der Dropdown-Liste „Ansicht“ die Option „Datenbank“ oder „Instanz“ oder „Verfügbarkeitsgruppe“ aus.

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

3. Klicken Sie auf **Ressourcen aktualisieren**.

   Die neu hinzugefügten, umbenannten oder gelöschten Ressourcen werden im SnapCenter Server-Inventar aktualisiert.

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

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Host- oder Clustername, zugehörigen Ressourcengruppen, Sicherungstyp, 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 Datenschutzvorgänge für eine Datenbank durchführen, die sich auf einem Nicht NetApp -Speicher befindet.

   - Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, `Not protected` wird in der Spalte **Gesamtstatus** angezeigt.
   - Wenn die Datenbank auf einem NetApp -Speichersystem liegt und geschützt ist, zeigt die Benutzeroberfläche `Backup not run` Meldung in der Spalte **Gesamtstatus**.
   - Wenn die Datenbank auf einem NetApp Speichersystem liegt und geschützt ist und die Sicherung für die Datenbank ausgelöst wird, zeigt die Benutzeroberfläche `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 Vorhängeschlosssymbol angezeigt. Wenn das Vorhängeschlosssymbol angezeigt wird, müssen Sie die Anmeldeinformationen der Instanz oder Datenbank angeben, um die Instanz oder Datenbank erfolgreich zu einer Ressourcengruppe hinzuzufügen.

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

Migrieren Sie Ressourcen zum NetApp Speichersystem

Nachdem Sie Ihr NetApp Speichersystem mit dem SnapCenter -Plug-in für Microsoft Windows bereitgestellt haben, können Sie Ihre Ressourcen entweder mithilfe der grafischen Benutzeroberfläche (GUI) von SnapCenter oder mithilfe der PowerShell-Cmdlets zum NetApp -Speichersystem oder von einer NetApp -LUN zu einer anderen NetApp -LUN migrieren.

Bevor Sie beginnen

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

Die meisten Felder auf diesen Assistentenseiten sind selbsterklärend. Die folgenden Informationen beschreiben einige der Felder, für die Sie möglicherweise Anleitungen 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“ aus der Dropdown-Liste „Anzeigen“ 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 aus:

Für dieses Feld…	Machen Sie Folgendes…
Datenbankname (optional)	Wenn Sie eine Instanz für die Migration ausgewählt haben, müssen Sie die Datenbanken dieser Instanz aus der Dropdown-Liste **Datenbanken** auswählen.
Ziele auswählen	Wählen Sie den Zielspeicherort für Daten- und Protokolldateien. Die Daten- und Protokolldateien werden in den Ordner „Daten“ bzw. „Protokoll“ unter dem ausgewählten NetApp Laufwerk verschoben. Wenn ein Ordner in der Ordnerstruktur nicht vorhanden ist, wird ein Ordner erstellt und die Ressource migriert.

Für dieses Feld…	Machen Sie Folgendes…
Datenbankdateidetails anzeigen (optional)	Wählen Sie diese Option, wenn Sie mehrere Dateien einer einzelnen 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: **FÜHREN SIE UPDATE STATISTICS für Tabellen aus, bevor Sie die Datenbank trennen**.

5. Führen Sie auf der Seite „Überprüfen“ die folgenden Aktionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Optionen zur Datenbankkonsistenzprüfung	Wählen Sie **Vorher ausführen**, um die Integrität der Datenbank vor der Migration zu überprüfen. Wählen Sie **Ausführen nach**, um die Integrität der Datenbank nach der Migration zu überprüfen.

Für dieses Feld…	Machen Sie Folgendes…
DBCC CHECKDB-Optionen	• Wählen Sie die Option **PHYSICAL_ONLY**, um die Integritätsprüfung auf die physische Struktur der Datenbank zu beschränken und beschädigte Seiten, Prüfsummenfehler und allgemeine Hardwarefehler zu erkennen, die sich auf die Datenbank auswirken. • Wählen Sie die Option **NO_INFOMSGS**, um alle Informationsmeldungen zu unterdrücken. • Wählen Sie die Option **ALL_ERRORMSGS**, um alle gemeldeten Fehler pro Objekt anzuzeigen. • Wählen Sie die Option **NOINDEX**, wenn Sie nicht gruppierte Indizes nicht überprüfen möchten. Die SQL Server-Datenbank verwendet den 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 einzuschränken und Sperren zu erhalten, anstatt einen internen Datenbank-Snapshot zu verwenden.

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

Erstellen von Sicherungsrichtlinien 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, oder Sie können eine Sicherungsrichtlinie erstellen, wenn Sie eine Ressourcengruppe erstellen oder eine einzelne Ressource sichern.

Bevor Sie beginnen

- Sie müssen Ihre Datenschutzstrategie definiert haben.
- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Identifizieren von Ressourcen und das Erstellen von Speichersystemverbindungen abgeschlossen haben.
- Sie müssen das Host-Protokollverzeichnis für die Protokollsicherung konfiguriert haben.
- Sie müssen die SQL Server-Ressourcen aktualisiert (erkannt) haben.

- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss der SnapCenter Administrator Ihnen die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.

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

- 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“.

- Überprüfen Sie die spezifischen Voraussetzungen und Einschränkungen der SnapMirror Active Sync. Weitere Informationen finden Sie unter "Objektlimits für SnapMirror Active Sync" .

Informationen zu diesem Vorgang

- Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten und aufbewahren und wie häufig die Ressource oder Ressourcengruppe gesichert wird. Darüber hinaus können Sie Replikations- und Skripteinstellungen angeben. Das Angeben von Optionen in einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

  Der SCRIPTS_PATH wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

  Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad 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 des Schlüssels anzuzeigen. SET-API wird nicht unterstützt.

- SnapLock

  - Wenn die Option „Sicherungskopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock -Aufbewahrungsdauer kleiner oder gleich der angegebenen Aufbewahrungsdauer in Tagen sein.

    Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots verhindert, bis die Aufbewahrungsfrist abgelaufen ist. Dies kann dazu führen, dass mehr Snapshots aufbewahrt werden als in der Richtlinie angegeben.

  Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

Schritt 1: Richtliniennamen erstellen

1. Wählen Sie im linken Navigationsbereich **Einstellungen** aus.
2. Wählen Sie auf der Seite „Einstellungen“ **Richtlinien** aus.
3. Wählen Sie **Neu**.
4. Geben Sie auf der Seite **Name** den Richtliniennamen und die Details ein.

Schritt 2: Richtlinienoptionen konfigurieren

1. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
   a. Wählen Sie Ihren Speichertyp aus.
   b. Wählen Sie Ihren Richtlinienumfang aus.

Vollständige Sicherung und Protokollsicherung

Sichern Sie die Datenbankdateien und Transaktionsprotokolle und kürzen Sie die Transaktionsprotokolle.

i. Wählen Sie **Vollständige Sicherung und Protokollsicherung**.
ii. Geben Sie die maximale Anzahl der Datenbanken ein, die für jeden Snapshot gesichert werden sollen.

> Sie müssen diesen Wert erhöhen, wenn Sie mehrere Sicherungsvorgänge gleichzeitig ausführen möchten.

Vollständige Sicherung

Sichern Sie die Datenbankdateien.

i. Wählen Sie **Vollständige Sicherung**.
ii. Geben Sie die maximale Anzahl der Datenbanken ein, die für jeden Snapshot gesichert werden sollen. Der Standardwert ist 100

> Sie müssen diesen Wert erhöhen, wenn Sie mehrere Sicherungsvorgänge gleichzeitig ausführen möchten.

Protokollsicherung

i. Sichern Sie die Transaktionsprotokolle.
ii. Wählen Sie **Protokollsicherung**.

Nur Kopie-Backup

i. Wenn Sie Ihre Ressourcen mithilfe einer anderen Sicherungsanwendung sichern, wählen Sie **Nur Sicherung kopieren**.

Wenn die Transaktionsprotokolle intakt bleiben, kann jede Sicherungsanwendung die Datenbanken wiederherstellen. Normalerweise sollten Sie die Option „Nur kopieren“ unter keinen anderen Umständen verwenden.

> Microsoft SQL unterstützt die Option **Nur Kopie-Sicherung** zusammen mit der Option **Vollständige Sicherung und Protokollsicherung** für sekundären Speicher nicht.

Schritt 3: Konfigurieren der Verfügbarkeitsgruppeneinstellungen

1. Führen Sie im Abschnitt „Einstellungen der Verfügbarkeitsgruppe“ die folgenden Aktionen aus:

a. Sicherung nur auf bevorzugter Sicherungsreplik.

   Wählen Sie diese Option, um nur auf der bevorzugten Sicherungsreplik zu sichern. Das bevorzugte Sicherungsreplikat wird durch die für die AG im SQL Server konfigurierten Sicherungseinstellungen bestimmt.

b. Wählen Sie Replikate für die Sicherung aus.

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

c. Wählen Sie die Sicherungspriorität (minimale und maximale Sicherungspriorität)

   Geben Sie eine minimale und eine maximale Sicherungsprioritätszahl an, die das AG-Replikat für die Sicherung bestimmen. Sie können beispielsweise eine Mindestpriorität von 10 und eine Höchstpriorität von 50 festlegen. In diesem Fall werden alle AG-Replikate mit einer Priorität über 10 und unter 50 für die Sicherung berücksichtigt.

   Standardmäßig beträgt die Mindestpriorität 1 und die Höchstpriorität 100.

In Clusterkonfigurationen werden die Sicherungen gemäß den in der Richtlinie festgelegten Aufbewahrungseinstellungen auf jedem Knoten des Clusters aufbewahrt. Wenn sich der Besitzerknoten der AG ändert, werden die Sicherungen gemäß den Aufbewahrungseinstellungen erstellt und die Sicherungen des vorherigen Besitzerknotens bleiben erhalten. Die Aufbewahrung für AG gilt nur auf Knotenebene.

Schritt 4: Konfigurieren der Snapshot- und Replikationseinstellungen

1. Führen Sie auf der Seite „Snapshot und Replikation“ die folgenden Schritte aus:

   a. Geben Sie den Zeitplantyp an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.

      Sie können für eine Richtlinie nur einen Zeitplantyp auswählen.

      Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Sicherungsvorgang beim Erstellen einer Ressourcengruppe angeben. Auf diese Weise können Sie Ressourcengruppen erstellen, die dieselbe Richtlinie und Sicherungshäufigkeit verwenden, aber jeder Richtlinie unterschiedliche Sicherungspläne zuweisen.

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

Schritt 5: Konfigurieren Sie aktuelle Aufbewahrungseinstellungen

1. Führen Sie im Abschnitt „Aktuelle Aufbewahrungseinstellungen“ je nach dem auf der Seite „Sicherungstyp“ ausgewählten Sicherungstyp eine oder mehrere der folgenden Aktionen aus:

Spezifische Anzahl von Kopien

Behalten Sie nur eine bestimmte Anzahl von Snapshots.

1. Wählen Sie die Option **Protokollsicherungen der letzten <Anzahl> Tage aufbewahren** und geben Sie die Anzahl der Tage an, die aufbewahrt werden sollen. Wenn Sie sich diesem Limit nähern, möchten Sie möglicherweise ältere Kopien löschen.

Bestimmte Anzahl von Tagen

Bewahren Sie die Sicherungskopien für eine bestimmte Anzahl von Tagen auf.

1. Wählen Sie die Option **Protokollsicherungen der letzten <Anzahl> Tage vollständiger Sicherungen aufbewahren** und geben Sie die Anzahl der Tage an, die die Protokollsicherungskopien aufbewahrt werden sollen.

Schritt 6: Snapshot-Einstellungen konfigurieren

1. Führen Sie für die Aufbewahrungseinstellungen für vollständige Sicherungen die folgenden Aktionen aus:

   a. Geben Sie die Gesamtzahl der aufzubewahrenden Snapshots an

      i. Um die Anzahl der aufzubewahrenden Snapshots anzugeben, wählen Sie **Aufzubewahrende Kopien**.

      ii. Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.

   Standardmäßig ist der Wert für die Aufbewahrungsanzahl auf 2 eingestellt. Wenn Sie die Aufbewahrungsanzahl auf 1 setzen, schlägt der Aufbewahrungsvorgang möglicherweise fehl, da der erste Snapshot der Referenz-Snapshot für die SnapVault -Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der zugrunde liegenden NetApp ONTAP Version unterstützt wird.

2. Aufbewahrungsdauer von Snapshots

   a. Wenn Sie die Anzahl der Tage angeben möchten, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden, wählen Sie **Kopien aufbewahren für**.

3. Wählen Sie **Sperrzeitraum für Snapshot-Kopien** und geben Sie die Dauer in Tagen, Monaten oder Jahren an.

   Die Aufbewahrungsdauer von Snaplock sollte weniger als 100 Jahre betragen.

4. Wählen Sie eine Richtlinienbezeichnung aus.

Sie können primären Snapshots SnapMirror Labels für die Remote-Replikation zuweisen, sodass die primären Snapshots den Snapshot-Replikationsvorgang von SnapCenter auf sekundäre ONTAP -Systeme auslagern können. Dies kann erfolgen, ohne die Option SnapMirror oder SnapVault auf der Richtlinienseite zu aktivieren.

Schritt 7: Konfigurieren sekundärer Replikationsoptionen

1. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

SnapMirror aktualisieren

Aktualisieren Sie SnapMirror, nachdem Sie eine lokale Snapshot-Kopie erstellt haben.

1. Wählen Sie diese Option, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume (SnapMirror) zu erstellen.

   Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.

   Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.

   Sehen "Anzeigen von SQL Server-Sicherungen und -Klonen auf der Seite „Topologie“" .

SnapVault aktualisieren

Aktualisieren Sie SnapVault , nachdem Sie eine Snapshot-Kopie erstellt haben.

1. Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen.

   Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock . Durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.

   Wenn SnapLock nur auf dem sekundären Server von ONTAP , bekannt als SnapLock Vault, konfiguriert ist, wird durch Klicken auf die Schaltfläche **Aktualisieren** auf der Seite „Topologie“ die Sperrdauer auf dem sekundären Server aktualisiert, die von ONTAP abgerufen wird.

   Weitere Informationen zu SnapLock Vault finden Sie unter "Übertragen Sie Snapshot-Kopien in WORM auf einem Tresorziel"

   Sehen "Anzeigen von SQL Server-Sicherungen und -Klonen auf der Seite „Topologie“" .

Fehlerwiederholungsanzahl

1. Geben Sie die Anzahl der Replikationsversuche ein, die durchgeführt werden sollen, bevor der Prozess angehalten wird.

Schritt 8: Skripteinstellungen konfigurieren

1. Geben Sie auf der Seite „Skript“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Sicherungsvorgang ausgeführt werden soll.

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

   Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

Sie müssen die SnapMirror Aufbewahrungsrichtlinie in ONTAP so konfigurieren, dass der sekundäre Speicher die maximale Anzahl an Snapshots nicht erreicht.

Schritt 9: Konfigurieren der Überprüfungseinstellungen

Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

1. Wählen Sie im Abschnitt „Überprüfung für folgende Sicherungszeitpläne ausführen“ die Zeitplanhäufigkeit aus.
2. Führen Sie im Abschnitt „Optionen zur Datenbankkonsistenzprüfung“ die folgenden Aktionen aus:
   a. Beschränken Sie die Integritätsstruktur auf die physische Struktur der Datenbank (PHYSICAL_ONLY).
      i. Wählen Sie **Integritätsstruktur auf die physische Struktur der Datenbank beschränken (NUR_PHYSIKALISCH)** aus, um die Integritätsprüfung auf die physische Struktur der Datenbank zu beschränken und zerrissene Seiten, Prüfsummenfehler und allgemeine Hardwarefehler zu erkennen, die sich auf die Datenbank auswirken.
   b. Alle Informationsmeldungen unterdrücken (NO INFOMSGS)
      i. Wählen Sie **Alle Informationsmeldungen unterdrücken (NO_INFOMSGS)**, 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)**, um alle gemeldeten Fehler pro Objekt anzuzeigen.
   d. Nicht gruppierte Indizes nicht prüfen (NOINDEX)
      i. Wählen Sie **Nicht gruppierte Indizes nicht prüfen (NOINDEX)** aus, wenn Sie keine nicht gruppierten Indizes prüfen möchten. Die SQL Server-Datenbank verwendet den Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.
   e. Begrenzen Sie die Prüfungen und erhalten Sie die Sperren, anstatt einen internen Datenbank-Snapshot (TABLOCK) zu verwenden.
      i. Wählen Sie **Beschränken Sie die Prüfungen und erhalten Sie die Sperren, anstatt eine interne Datenbank-Snapshot-Kopie zu verwenden (TABLOCK)** aus, um die Prüfungen zu begrenzen und Sperren zu erhalten, anstatt einen internen Datenbank-Snapshot zu verwenden.
3. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss überprüfen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.
4. Geben Sie im Abschnitt **Einstellungen des Überprüfungsskripts** den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Überprüfungsvorgang ausgeführt werden soll.

Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS_PATH sein.

Schritt 10: Zusammenfassung der Überprüfung

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

Erstellen von Ressourcengruppen und Anfügen von Richtlinien für SQL Server

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

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

Informationen zu diesem Vorgang

- Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.
- Das Hinzufügen neuer Datenbanken ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Datenbanken zu einer vorhandenen Ressourcengruppe im Failover-Modus von SnapMirror Active Sync wird nicht unterstützt. Sie können der Ressourcengruppe nur im regulären oder Failback-Zustand 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 SnapCenter kürzlich eine Ressource 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 aus:

Für dieses Feld…	Machen Sie Folgendes…
Name	Geben Sie den Namen der Ressourcengruppe ein. Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.
Schlagwörter	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

Für dieses Feld…	Machen Sie Folgendes…
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein. Beispiel: customtext_resourcegroup_policy_hostname oder resourcegroup_hostname. Standardmäßig wird dem 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 den Dropdown-Listen aus, um die Liste der Ressourcen zu filtern.

      Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

   b. Um Ressourcen aus dem Abschnitt **Verfügbare Ressourcen** in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben, führen Sie einen der folgenden Schritte aus:
      - Wählen Sie **Alle Ressourcen auf demselben Speichervolume automatisch auswählen**, 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 Rechtspfeil, 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 Dropdownliste aus.

      Sie können auch eine Richtlinie 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 „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.
   c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **OK**.

      Sie müssen dies für jede in der Richtlinie aufgeführte Frequenz tun. Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgelistet.

   d. Wählen Sie den Microsoft SQL Server-Scheduler aus.

      Sie müssen außerdem eine Scheduler-Instanz auswählen, die mit der Planungsrichtlinie verknüpft werden soll.

      Wenn Sie den Microsoft SQL Server-Scheduler nicht auswählen, wird standardmäßig der Microsoft Windows-Scheduler verwendet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden. Sie sollten die Zeitpläne nicht ändern und den im Windows-Scheduler oder SQL Server-Agent erstellten Sicherungsauftrag nicht umbenennen.

7. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

   a. Wählen Sie den Verifizierungsserver aus der Dropdown-Liste **Verifizierungsserver** aus.

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

      Die Version des Überprüfungsservers sollte mit der Version und Edition des SQL-Servers übereinstimmen, auf dem die primäre Datenbank gehostet wird.

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

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

   c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen“ (Richtlinienname) die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planen Sie eine Überprüfung	Wählen Sie **Geplante Überprüfung ausführen**.

   d. Klicken Sie auf **OK**.

      Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet. Sie können die Überprüfung und anschließend die Bearbeitung durchführen, indem Sie auf * klicken. * oder durch Klicken auf * löschen ✖ *.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

   Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl „Set-SmSmtpServer“ angegeben haben.

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

Ähnliche Informationen

"Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken"

Erstellen Sie Ressourcengruppen und aktivieren Sie den sekundären Schutz für Microsoft SQL Server-Ressourcen auf ASA r2-Systemen

Sie sollten die Ressourcengruppe erstellen, um die Ressourcen hinzuzufügen, die sich auf ASA R2-Systemen befinden. Sie können den sekundären Schutz auch beim Erstellen der Ressourcengruppe bereitstellen.

Bevor Sie beginnen

- Sie sollten sicherstellen, dass Sie nicht sowohl ONTAP 9.x-Ressourcen als auch ASA r2-Ressourcen zur gleichen Ressourcengruppe hinzufügen.
- Sie sollten sicherstellen, dass Sie keine Datenbank mit ONTAP 9.x-Ressourcen und ASA r2-Ressourcen haben.

Informationen zu diesem Vorgang

- Der sekundäre Schutz ist nur verfügbar, wenn dem angemeldeten Benutzer die Rolle zugewiesen ist, für die die Funktion **SecondaryProtection** aktiviert ist.
- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nachdem die primäre und sekundäre Konsistenzgruppe erstellt wurden, wird der Wartungsmodus der Ressourcengruppe beendet.
- SnapCenter unterstützt keinen sekundären Schutz für eine Klonressource.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-In aus der Liste aus.
2. Klicken Sie auf der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:
   a. Geben Sie im Feld „Name“ einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.

   b. Geben Sie im Feld „Tag“ eine oder mehrere Bezeichnungen ein, um die spätere Suche nach der Ressourcengruppe zu erleichtern.

      Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

   c. Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

      Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

   d. Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

      Sie sollten genau dasselbe Ziel verwenden, das in der Anwendung festgelegt wurde, gegebenenfalls einschließlich Präfix.

4. Wählen Sie auf der Seite „Ressourcen“ den Datenbank-Hostnamen aus der Dropdown-Liste **Host** aus.

Die Ressourcen werden nur dann im Abschnitt „Verfügbare Ressourcen“ aufgeführt, wenn die Ressource erfolgreich erkannt wurde. Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

5. Wählen Sie die ASA r2-Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ aus und verschieben Sie sie in den Abschnitt „Ausgewählte Ressourcen“.
6. Wählen Sie auf der Seite „Anwendungseinstellungen“ die Sicherungsoption aus.
7. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

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

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

   b. Klicken + in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

      Dabei ist *Richtlinienname* der Name der von Ihnen ausgewählten Richtlinie.

      Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

   Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

8. Wenn der sekundäre Schutz für die von Ihnen ausgewählte Richtlinie aktiviert ist, wird die Seite „Sekundärer Schutz“ angezeigt und Sie müssen die folgenden Schritte ausführen:

   a. Wählen Sie den Typ der Replikationsrichtlinie aus.

      Die synchrone Replikationsrichtlinie wird nicht unterstützt.

   b. Geben Sie das Konsistenzgruppensuffix an, das Sie verwenden möchten.

   c. Wählen Sie aus den Dropdown-Menüs „Zielcluster“ und „Ziel-SVM“ den Peering-Cluster und die SVM aus, die Sie verwenden möchten.

      Das Cluster- und SVM-Peering wird von SnapCenter nicht unterstützt. Sie sollten System Manager oder ONTAP CLIs verwenden, um Cluster- und SVM-Peering durchzuführen.

Wenn die Ressourcen bereits außerhalb von SnapCenter geschützt sind, werden diese Ressourcen im Abschnitt „Sekundär geschützte Ressourcen“ angezeigt.

1. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

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

b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren.

c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen“ (Richtlinienname) die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planen Sie eine Überprüfung	Wählen Sie **Geplante Überprüfung ausführen** und wählen Sie dann den Zeitplantyp aus der Dropdownliste aus.

d. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Sicherungen auf dem sekundären Speichersystem zu überprüfen.

e. Klicken Sie auf **OK**.

Die konfigurierten Überprüfungszeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

2. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

ⓘ Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl „Set-SmSmtpServer“ angegeben haben.

3. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Voraussetzungen für die Sicherung 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 -Speichersystem auf ein NetApp -Speichersystem migriert haben.
- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror -Beziehung zu einem sekundären Speicher sichern möchten, sollte die dem Speicherbenutzer zugewiesene ONTAP -Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Der von einem Active Directory (AD)-Benutzer initiierte Sicherungsvorgang schlägt fehl, wenn die Anmeldeinformationen der SQL-Instanz nicht dem AD-Benutzer oder der AD-Gruppe zugewiesen sind. Sie

müssen die Anmeldeinformationen der SQL-Instanz dem AD-Benutzer oder der AD-Gruppe auf der Seite **Einstellungen** > **Benutzerzugriff** zuweisen.

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn eine Ressourcengruppe über mehrere Datenbanken von verschiedenen Hosts verfügt, kann es sein, dass der Sicherungsvorgang auf einigen Hosts aufgrund von Netzwerkproblemen verspätet ausgelöst wird. Sie sollten den Wert von FMaxRetryForUninitializedHosts in web.config mithilfe des PS-Cmdlets Set-SmConfigSettings konfigurieren.

Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets

Sie müssen eine Verbindung zur Storage Virtual Machine (SVM) und Anmeldeinformationen erstellen, bevor Sie PowerShell-Cmdlets zum Ausführen von Datenschutzvorgängen verwenden.

Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

  Während des Hinzufügens einer Speichersystemverbindung dürfen keine Host-Plug-In-Installationen ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbankstatus in der SnapCenter -GUI möglicherweise als „Nicht für Sicherung verfügbar“ oder „Nicht auf NetApp -Speicher“ angezeigt wird.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Speichersysteme mit demselben Namen auf verschiedenen Clustern. Jedes von SnapCenter unterstützte Speichersystem sollte einen eindeutigen Namen und eine eindeutige Verwaltungs-LIF-IP-Adresse haben.

Schritte

1. Initiieren Sie eine PowerShell Core-Verbindungssitzung mithilfe des Cmdlets Open-SmConnection.

   Dieses Beispiel öffnet eine PowerShell-Sitzung:

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

2. Erstellen Sie mithilfe des Cmdlets Add-SmStorageConnection eine neue Verbindung zum Speichersystem.

   In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

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

3. Erstellen Sie mithilfe des Cmdlets Add-SmCredential neue Anmeldeinformationen.

   In diesem Beispiel wird eine neue Anmeldeinformation mit dem Namen „FinanceAdmin“ mit Windows-Anmeldeinformationen erstellt:

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

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Sichern von SQL-Ressourcen

Wenn eine Ressource noch nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus sichern.

Informationen zu diesem Vorgang

- Um den Sicherungsvorgang zu optimieren, sollten Sie einen Reverse-Lookup-Datensatz der Windows-Clusternamen und IP-Adressen im DNS-Server erstellen.
- Für die Authentifizierung mit Windows-Anmeldeinformationen müssen Sie Ihre 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 einrichten, während Sie den Host bei SnapCenter auf der Seite **Host hinzufügen** oder **Host ändern** registrieren, um gMSA zu aktivieren und zu verwenden.
- Wenn der Host mit gMSA hinzugefügt wird und das gMSA über Anmelde- und Systemadministratorrechte verfügt, darf das gMSA eine Verbindung zur SQL-Instanz herstellen.
  - SnapCenter überprüft, ob die Authentifizierung für SQL-Instanzen konfiguriert ist. Wenn die Authentifizierung konfiguriert ist, wird mit diesen Anmeldeinformationen auf die SQL-Instanz zugegriffen.
  - Wenn die Authentifizierung nicht konfiguriert ist, verwenden Sie gMSA, um zu prüfen, ob das SQL-Plug-In derzeit ausgeführt wird. Wenn das Plug-In aktiv ist, wird es verwendet, um eine Verbindung zur SQL-Instanz herzustellen.
  - Der Zugriff auf die SQL-Instanz erfolgt über die Windows-Anmeldeinformationsauthentifizierung, wenn weder die Authentifizierung für SQL-Instanzen konfiguriert ist noch das Plug-In betriebsbereit ist.

SnapCenter -Benutzeroberfläche

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ aus der Dropdown-Liste „Anzeigen“ die Option „Datenbank“ oder „Instanz“ oder „Verfügbarkeitsgruppe“ aus.

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

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

   In der Topologieansicht können Sie nicht unterscheiden, ob es sich bei dem Sicherungsstatus, dem Zeitstempel oder der Sicherung um eine Instanz oder eine Datenbank handelt.

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

   Beispielsweise customtext_policy_hostname oder resource_hostname. Standardmäßig wird dem 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 Dropdownliste aus.

      Sie können eine Richtlinie erstellen, indem Sie * auswählen.  * um den Richtlinienassistenten zu starten.

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

   b. Wählen *  * in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

   c. Im Fenster **Zeitpläne für Richtlinie hinzufügen** `policy_name` Dialogfeld, konfigurieren Sie den Zeitplan und wählen Sie dann **OK**.

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

   Die konfigurierten Zeitpläne werden in der Spalte **Angewandte Zeitpläne** aufgelistet.

   a. Wählen Sie **Microsoft SQL Server-Scheduler verwenden** und wählen Sie dann aus der Dropdown-Liste **Scheduler-Instanz** die Scheduler-Instanz aus, die der Planungsrichtlinie zugeordnet ist.

5. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:

   a. Wählen Sie den Verifizierungsserver aus der Dropdown-Liste **Verifizierungsserver** 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, auf dem die primäre Datenbank gehostet wird.

a. Wählen Sie **Sekundäre Locatoren 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 Überprüfungszeitplan konfigurieren möchten, und wählen Sie dann * + *.

c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen *Richtlinienname*“ die folgenden Aktionen aus:

Wenn Sie wollen…	Machen Sie Folgendes…
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planen Sie eine Überprüfung	Wählen Sie **Geplante Überprüfung ausführen**.

Wenn der Überprüfungsserver keine Speicherverbindung hat, schlägt der Überprüfungsvorgang mit folgendem Fehler fehl: „Datenträger konnte nicht eingebunden werden.“

d. Wählen Sie **OK**.

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl „Set-SmSmtpServer“ angegeben haben.

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

Die Seite „Datenbanktopologie“ wird angezeigt.

8. Wählen Sie **Jetzt sichern**.

9. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

b. Wählen Sie **Nach Sicherung überprüfen**, um Ihre Sicherung zu überprüfen.

c. Wählen Sie **Backup**.

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

Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

Es wird eine implizite Ressourcengruppe erstellt. Sie können dies anzeigen, indem Sie den entsprechenden Benutzer oder die entsprechende Gruppe auf der Seite „Benutzerzugriff“ auswählen. Der implizite Ressourcengruppentyp ist „Ressource“.

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

Nach Abschluss

- In MetroCluster -Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Schutzbeziehung 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 for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl. Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei /opt/netapp/init_scripts/scvservice. In diesem Skript `do_start method` Der Befehl startet den SnapCenter VMware-Plug-In-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M.`

Ähnliche Informationen

"Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken"

"Sicherungsvorgänge schlagen aufgrund der Verzögerung im TCP_TIMEOUT mit einem MySQL-Verbindungsfehler fehl"

"Die Sicherung schlägt mit einem Windows-Planerfehler fehl"

"Vorgänge zum Stilllegen oder Gruppieren von Ressourcen schlagen fehl"

PowerShell-Cmdlets

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

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

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

2. Erstellen Sie eine Sicherungsrichtlinie mithilfe des Cmdlets Add-SmPolicy.

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit dem SQL-Sicherungstyp „FullBackup“ erstellt:

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

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit dem Sicherungstyp „CrashConsistent“ für das Windows-Dateisystem erstellt:

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

3. Ermitteln Sie Hostressourcen mithilfe des Cmdlets „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
```

   Dieses Beispiel ermittelt die Ressourcen für Windows-Dateisysteme auf dem angegebenen Host:

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

4. Fügen Sie SnapCenter mithilfe des Cmdlets Add-SmResourceGroup eine neue Ressourcengruppe hinzu.

   In diesem Beispiel wird eine neue SQL-Datenbank-Sicherungsressourcengruppe 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"
```

   In diesem Beispiel wird eine neue Ressourcengruppe zur Sicherung des Windows-Dateisystems mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

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

5. Starten Sie einen neuen Sicherungsauftrag mithilfe des Cmdlets New-SmBackup.

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

6. Zeigen Sie den Status des Sicherungsauftrags mithilfe des Cmdlets Get-SmBackupReport an.

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

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

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Sichern von SQL Server-Ressourcengruppen

Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden die Sicherungen automatisch gemäß dem Zeitplan durchgeführt.

Schritte

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

   Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder indem Sie und wählen Sie dann das Tag aus. Sie können dann auswählen , um den Filterbereich 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 „Sichern“ die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

      Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

   b. Wählen Sie nach der Sicherung „Überprüfen“ aus, um die On-Demand-Sicherung zu überprüfen.

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

   c. Wählen Sie **Backup**.

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

Ähnliche Informationen

"Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken"

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

"Sicherungsvorgänge schlagen aufgrund der Verzögerung im TCP_TIMEOUT mit einem MySQL-Verbindungsfehler fehl"

"Die Sicherung schlägt mit einem Windows-Planerfehler fehl"

Überwachen Sie Sicherungsvorgänge für SQL-Ressourcen auf der Seite „SnapCenter -Aufträge“.

Sie können den Fortschritt verschiedener Sicherungsvorgänge mithilfe der SnapCenterJobs-Seite überwachen. Möglicherweise möchten Sie den Fortschritt überprüfen, um festzustellen, wann der Vorgang abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

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

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange
- Abgesagt

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 um die Liste so zu filtern, dass nur Sicherungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdownliste **Typ** die Option **Backup** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.

Obwohl der Status des Sicherungsauftrags angezeigt wird ✔ Wenn Sie auf die Auftragsdetails klicken, sehen Sie möglicherweise, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt werden oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.

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

Überwachen von Datenschutzvorgängen für SQL-Ressourcen im Aktivitätsbereich

Im Aktivitätsbereich werden die fünf zuletzt ausgeführten Vorgänge angezeigt. Im Aktivitätsbereich wird auch angezeigt, wann der Vorgang gestartet wurde und welchen Status er hat.

Im Aktivitätsbereich werden Informationen zu Sicherungs-, Wiederherstellungs-, Klon- und geplanten Sicherungsvorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Klicken im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Auftragsdetails** aufgelistet.

Abbrechen des SnapCenter -Plug-ins für Microsoft SQL Server-Sicherungsvorgänge

Sie können Sicherungsvorgänge abbrechen, die ausgeführt werden, in der Warteschlange stehen oder nicht reagieren. Wenn Sie einen Sicherungsvorgang abbrechen, stoppt der SnapCenter Server den Vorgang und entfernt alle Snapshots aus dem Speicher, wenn die erstellte Sicherung nicht beim SnapCenter -Server registriert ist. Wenn die Sicherung bereits beim SnapCenter Server registriert ist, wird der bereits erstellte Snapshot auch nach dem Auslösen des Abbruchs nicht zurückgesetzt.

Bevor Sie beginnen

- Sie müssen als SnapCenter Administrator oder Auftragseigentümer angemeldet sein, um Wiederherstellungsvorgänge abzubrechen.
- Sie können nur Protokoll- oder vollständige Sicherungsvorgänge abbrechen, die sich in der Warteschlange befinden oder ausgeführt werden.
- Sie können den Vorgang nicht mehr abbrechen, nachdem die Überprüfung begonnen hat.

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

- Sie können einen Sicherungsvorgang entweder auf der Seite „Überwachen“ oder im Aktivitätsbereich abbrechen.
- Zusätzlich zur Verwendung der SnapCenter -GUI können Sie PowerShell-Cmdlets verwenden, um

Vorgänge abzubrechen.

- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer\Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

Führen Sie eine der folgenden Aktionen aus:

Von der…	Aktion
Monitorseite	1. Wählen Sie im linken Navigationsbereich **Monitor** > **Jobs** aus. 2. Wählen Sie den Auftrag aus und wählen Sie **Auftrag abbrechen**.
Aktivitätsbereich	1. Nachdem Sie den Sicherungsauftrag gestartet haben, wählen Sie im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. 2. Wählen Sie den Vorgang aus. 3. Wählen Sie auf der Seite „Auftragsdetails“ die Option „Auftrag abbrechen“ aus.

Ergebnis

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt. Wenn der Vorgang, den Sie abgebrochen haben, im Status „Abbrechen“ oder „Ausführen“ nicht reagiert, sollten Sie den `Cancel-SmJob -JobID <int> -Force` Cmdlet, um den Sicherungsvorgang zwangsweise zu beenden.

Anzeigen von SQL Server-Sicherungen und -Klonen auf der Seite „Topologie“

Wenn Sie die Sicherung oder das Klonen einer Ressource vorbereiten, kann es hilfreich sein, eine grafische Darstellung aller Sicherungen und Klone auf dem primären und sekundären Speicher anzuzeigen.

Informationen zu diesem Vorgang

Auf der Seite „Topologie“ können Sie alle Sicherungen und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen und Klone anzeigen und sie dann auswählen, um Datenschutzvorgänge durchzuführen.

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

-  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 Speicher gespiegelt werden.
-  zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault -Technologie auf dem sekundären Speicher repliziert werden.
  - Die angezeigte Anzahl der Backups umfasst die aus dem sekundären Speicher gelöschten Backups.

    Wenn Sie beispielsweise 6 Sicherungen mit einer Richtlinie zum Aufbewahren von nur 4 Sicherungen erstellt haben, wird die Anzahl der angezeigten Sicherungen mit 6 angegeben.

Klone einer Sicherung eines versionsflexiblen Spiegels auf einem Volume vom Typ „Mirror-Vault“ werden in der Topologieansicht angezeigt, die Anzahl der Spiegelsicherungen in der Topologieansicht umfasst jedoch nicht die versionsflexible Sicherung.

Wenn Sie eine sekundäre Beziehung als SnapMirror Active Sync haben (ursprünglich veröffentlicht als SnapMirror Business Continuity [SM-BC]), können Sie die folgenden zusätzlichen Symbole sehen:

-  Die Replikationssite ist aktiv.
-  Die Replikationssite ist ausgefallen.
-  Die sekundäre Spiegel- oder Tresorbeziehung wurde nicht wiederhergestellt.

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 die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource entweder aus der Ressourcendetailansicht oder aus der Ressourcengruppendetailansicht aus.

   Wenn es sich bei der ausgewählten Ressource um eine geklonte Datenbank handelt, schützen Sie die geklonte Datenbank. Die Quelle des Klons wird 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. Überprüfen Sie die Karte „Zusammenfassung“, um eine Übersicht über die Anzahl der auf dem primären und sekundären Speicher verfügbaren Sicherungen und Klone anzuzeigen.

   Der Abschnitt **Zusammenfassungskarte** zeigt die Gesamtzahl der Backups und Klone an.

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

   Wenn eine SnapLock -fähige Sicherung durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock aktualisiert.

Ein wöchentlicher Zeitplan aktualisiert auch die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock .

Wenn die Anwendungsressource auf mehrere Volumes verteilt ist, entspricht die SnapLock -Ablaufzeit für die Sicherung der längsten SnapLock -Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock -Ablaufzeit wird von ONTAP abgerufen.

Bei der aktiven Synchronisierung von SnapMirror wird durch Klicken auf die Schaltfläche **Aktualisieren** das SnapCenter -Sicherungsinventar aktualisiert, indem ONTAP sowohl nach primären als auch nach Replikationsstandorten abgefragt wird. Ein wöchentlicher Zeitplan führt diese Aktivität auch für alle Datenbanken aus, die eine aktive Synchronisierungsbeziehung mit SnapMirror enthalten.

- Für SnapMirror Active Sync und nur für ONTAP 9.14.1 sollten Async Mirror- oder Async MirrorVault-Beziehungen zum neuen primären Ziel nach dem Failover manuell konfiguriert werden. Ab ONTAP 9.15.1 wird Async Mirror oder Async MirrorVault automatisch auf das neue primäre Ziel konfiguriert.
- Nach dem Failover sollte ein Backup für SnapCenter erstellt werden, um über das Failover informiert zu sein. Sie können erst auf **Aktualisieren** klicken, nachdem eine Sicherung erstellt wurde.

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

   Die Details der Backups und Klone werden in einem Tabellenformat angezeigt.

6. Wählen Sie die Sicherung aus der Tabelle aus und klicken Sie dann auf die Datenschutzsymbole, um Wiederherstellungs-, Klon-, Umbenennungs- und Löschvorgänge durchzuführen.

   Sie können Sicherungen, die sich auf dem sekundären Speicher befinden, weder umbenennen noch löschen.

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

Bereinigen der Anzahl sekundärer Sicherungen mithilfe von PowerShell-Cmdlets

Sie können das Cmdlet „Remove-SmBackup“ verwenden, um die Sicherungsanzahl für sekundäre Sicherungen ohne Snapshot zu bereinigen. Sie können dieses Cmdlet verwenden, wenn die Gesamtzahl der in der Topologie „Kopien verwalten“ angezeigten Snapshots nicht mit der Snapshot-Aufbewahrungseinstellung des sekundären Speichers übereinstimmt.

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

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Schritte

1. Initiieren Sie mithilfe des Cmdlets Open-SmConnection eine Verbindungssitzung mit dem SnapCenter -Server für einen angegebenen Benutzer.

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

2. Bereinigen Sie die Anzahl sekundärer Sicherungen mit dem Parameter -CleanupSecondaryBackups.

   In diesem Beispiel wird die Sicherungsanzahl für sekundäre Sicherungen 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"):
```