



Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden

SnapCenter software

NetApp
November 06, 2025

This PDF was generated from <https://docs.netapp.com/de-de/snapcenter-61/protect-azure/protect-applications-azure-netapp-files.html> on November 06, 2025. Always check docs.netapp.com for the latest.

Inhalt

Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden	1
Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden	1
Einschränkungen	1
Installieren Sie SnapCenter und erstellen Sie Anmeldeinformationen	1
Installieren von SnapCenter auf einer virtuellen Azure-Maschine	1
Erstellen der Azure-Anmeldeinformationen in SnapCenter	3
Konfigurieren des Azure-Speicherkontos	4
Erstellen Sie die Anmeldeinformationen zum Hinzufügen des Plug-In-Hosts	4
Schützen Sie SAP HANA-Datenbanken	5
Hosts hinzufügen und SnapCenter Plug-In für SAP HANA-Datenbank installieren	5
SAP HANA-Datenbank hinzufügen	6
Erstellen von Sicherungsrichtlinien für SAP HANA-Datenbanken	7
Erstellen von Ressourcengruppen und Anfügen von SAP HANA-Sicherungsrichtlinien	7
Sichern von SAP HANA-Datenbanken, die auf Azure NetApp Files ausgeführt werden	8
Sichern von SAP HANA-Ressourcengruppen	9
Wiederherstellen und Wiederherstellen von SAP HANA-Datenbanken	10
Klonen Sie die SAP HANA-Datenbanksicherung	11
Schützen Sie Microsoft SQL Server-Datenbanken	12
Hosts hinzufügen und SnapCenter Plug-In für SQL Server-Datenbank installieren	12
Erstellen von Sicherungsrichtlinien für SQL Server-Datenbanken	13
Erstellen von Ressourcengruppen und Anfügen von SQL-Sicherungsrichtlinien	14
Sichern von SQL Server-Datenbanken, die auf Azure NetApp Files ausgeführt werden	15
Sichern von SQL Server-Ressourcengruppen	16
Wiederherstellen und Wiederherstellen von SQL Server-Datenbanken	17
Klonen Sie die SQL Server-Datenbanksicherung	18
Schützen Sie Oracle-Datenbanken	20
Hosts hinzufügen und SnapCenter Plug-In für Oracle-Datenbank installieren	20
Erstellen von Sicherungsrichtlinien für Oracle-Datenbanken	21
Erstellen Sie Ressourcengruppen und fügen Sie Oracle-Sicherungsrichtlinien hinzu	21
Sichern von Oracle-Datenbanken, die auf Azure NetApp Files ausgeführt werden	23
Sichern von Oracle-Ressourcengruppen	23
Wiederherstellen und Wiederherstellen von Oracle-Datenbanken	24
Klonen Sie die Oracle-Datenbanksicherung	27

Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden

Schützen von Anwendungen, die auf Azure NetApp Files ausgeführt werden

SnapCenter unterstützt den Schutz Ihrer Anwendungen wie Oracle, SQL und SAP HANA, die sich auf Azure NetApp Files befinden. Ab Version 6.0.1 unterstützt SnapCenter die Azure NetApp Files -Sicherungsfunktion, die die Datenschutzfunktionen von Azure NetApp Files erweitert, indem sie eine vollständig verwaltete Sicherungslösung für langfristige Wiederherstellung, Archivierung und Compliance bietet.

Azure NetApp Files ist eine Premium-Speicherlösung, deren langfristige Aufbewahrung von Backups teuer sein kann. Um die Kosten zu optimieren, können Sie die Sicherungen vom Azure NetApp Files -Speicher in einen Azure-Objektspeicher verschieben. Ab SnapCenter 6.0.1 können Sie Anwendungen, die sich auf Azure NetApp Files befinden, in Azure Blob Storage (Objektspeicher) sichern und klonen. Sie können zwei Kopien Ihrer Daten aufbewahren: Volume-Snapshot-Kopien im Azure NetApp Files -Speicher für die kurzfristige Wiederherstellung und eine weitere Kopie im Azure Blob Storage für die langfristige Wiederherstellung.

Wenn eine Richtlinie mit Azure NetApp Files -Sicherung aktiviert und einer Ressource zugeordnet ist, übernimmt SnapCenter die Erstellung von Volume-Snapshots und deren Sicherung in Azure Blob Storage. SnapCenter erstellt den Backup-Tresor und aktiviert die Sicherung für das Volume. Wenn Sie die Sicherung für das Volume aktiviert haben, verwendet SnapCenter den vorhandenen Tresor.

Einschränkungen

- Objektspeicherfunktionen für FAS, ASA oder AFF ONTAP und Amazon FSx for NetApp ONTAP Speichersysteme werden nicht unterstützt.
- Mount- und Katalog-Workflows von Oracle und SAP HANA werden für Objektspeicher-Backups nicht unterstützt, für Snapshots jedoch schon.
- Oracle PDB-Klone werden für Objektspeichersicherungen nicht unterstützt, für Snapshots jedoch schon.
- Die Sicherungsüberprüfung aus dem Objektspeicher, die REST-API-Unterstützung, die Verwaltung des Klon-Lebenszyklus aus dem Objektspeicher und die Berichtsfunktionen für Objektspeicher-Sicherungen werden nicht unterstützt.
- Die Wiederherstellung von Sicherungen auf Azure Blob Storage in Azure NetApp Files wird nicht unterstützt. Alternativ können Sie die Klonoption verwenden.
- Klonaufteilung wird nicht unterstützt.

Installieren Sie SnapCenter und erstellen Sie Anmeldeinformationen

Installieren von SnapCenter auf einer virtuellen Azure-Maschine

Sie können die SnapCenter software von der NetApp -Support-Site herunterladen und die Software auf der virtuellen Azure-Maschine installieren.

Bevor Sie beginnen

- Stellen Sie sicher, dass die virtuelle Azure Windows-Maschine die Anforderungen für die Installation von SnapCenter Server erfüllt. Weitere Informationen finden Sie unter "[Voraussetzungen für die Installation von SnapCenter Server](#)".
- Wenn Sie Azure NetApp Files noch nicht kennen und noch kein NetApp -Konto haben, stellen Sie sicher, dass Sie sich registriert haben, damit Sie auf die SnapCenter -Software zugreifen können. Weitere Informationen finden Sie unter "[Registrieren Sie sich, um auf die SnapCenter software zuzugreifen](#)".

Schritte

1. Laden Sie das SnapCenter Server-Installationspaket herunter von "[NetApp Support Site](#)".
2. Starten Sie die Installation des SnapCenter -Servers, indem Sie auf die heruntergeladene EXE-Datei doppelklicken.

Nachdem Sie die Installation gestartet haben, werden alle Vorprüfungen durchgeführt und wenn die Mindestanforderungen nicht erfüllt sind, werden entsprechende Fehler- oder Warnmeldungen angezeigt. Sie können die Warnmeldungen ignorieren und mit der Installation fortfahren. Fehler sollten jedoch behoben sein.

3. Überprüfen Sie die vorab ausgefüllten Werte, die für die Installation des SnapCenter -Servers erforderlich sind, und ändern Sie sie bei Bedarf.

Sie müssen das Kennwort für die MySQL Server-Repository-Datenbank nicht angeben. Während der Installation des SnapCenter -Servers wird das Kennwort automatisch generiert.



Das Sonderzeichen „%“ wird im benutzerdefinierten Pfad für die Repository-Datenbank nicht unterstützt. Wenn Sie „%“ in den Pfad aufnehmen, schlägt die Installation fehl.

4. Klicken Sie auf **Jetzt installieren**.

Sollten Sie ungültige Werte angegeben haben, werden entsprechende Fehlermeldungen angezeigt. Sie sollten die Werte erneut eingeben und dann die Installation starten.



Wenn Sie auf die Schaltfläche **Abbrechen** klicken, wird der ausgeführte Schritt abgeschlossen und anschließend der Rollback-Vorgang gestartet. Der SnapCenter -Server wird vollständig vom Host entfernt.

Wenn Sie jedoch auf **Abbrechen** klicken, während die Vorgänge „Neustart der SnapCenter Server-Site“ oder „Warten auf den Start des SnapCenter Servers“ ausgeführt werden, wird die Installation fortgesetzt, ohne den Vorgang abubrechen.

Registrieren Sie das Produkt, um den Support zu aktivieren

Wenn Sie neu bei NetApp sind und noch kein NetApp -Konto haben, sollten Sie das Produkt registrieren, um Support zu erhalten.

Schritte

1. Navigieren Sie nach der Installation von SnapCenter zu **Hilfe > Info**.
2. Notieren Sie sich im Dialogfeld „Über SnapCenter“ die SnapCenter Instanz, eine 20-stellige Nummer, die mit 971 beginnt.
3. Klicken <https://register.netapp.com>.

4. Klicken Sie auf **Ich bin kein registrierter NetApp -Kunde**.
5. Geben Sie Ihre Daten ein, um sich zu registrieren.
6. Lassen Sie das Feld „NetApp -Referenz-SN“ leer.
7. Wählen Sie * SnapCenter* aus der Dropdown-Liste „Produktlinie“ aus.
8. Wählen Sie den Abrechnungsanbieter aus.
9. Geben Sie die 20-stellige SnapCenter Instanz-ID ein.
10. Klicken Sie auf **Senden**.

Erstellen der Azure-Anmeldeinformationen in SnapCenter

Sie sollten die Azure-Anmeldeinformationen in SnapCenter erstellen, um auf das Azure NetApp -Konto zuzugreifen.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie den Dienstprinzipal in Azure erstellt haben.
- Stellen Sie sicher, dass Sie über die Mandanten-ID, die Client-ID und den geheimen Schlüssel verfügen, die mit dem Dienstprinzipal verknüpft sind.
 - Die Mandanten-ID finden Sie im Azure-Portal auf der Übersichtsseite für die Entra-ID.
 - Die Client-ID wird auch als Anwendungs-ID für den Enterprise-App-/Service-Principal bezeichnet. Dies finden Sie im Azure-Portal auf der Übersichtsseite für die Unternehmensanwendung, die Sie als Dienstprinzipal für SnapCenter erstellt haben.
 - Der geheime Clientschlüssel wird auch als geheimer Wert bezeichnet. Sie können dieses Clientgeheimnis im Azure-Portal erstellen, indem Sie unter Entra ID zu **App-Registrierungen** navigieren. Nachdem Sie die von Ihnen erstellte Enterprise-App ausgewählt haben, navigieren Sie zu **Zertifikate und Geheimnisse** und dann zu **Neues Client-Geheimnis**.



Auf den geheimen Wert kann nur zugegriffen werden, wenn er erstellt wurde. Sie können später nicht mehr darauf zugreifen.

- Dem Dienstprinzipal müssen Berechtigungen erteilt werden. Die Rolle des Mitwirkenden ermöglicht dem Dienstprinzipal, erforderliche Aktionen in Azure auszuführen. Dies kann über die Zugriffssteuerungsseite (IAM) auf der Abonnementseite gewährt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die folgenden Informationen an, die zum Erstellen der Anmeldeinformationen erforderlich sind.

Für dieses Feld...	Machen Sie Folgendes...
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldeinformationen ein.

Für dieses Feld...	Machen Sie Folgendes...
Authentifizierungsmodus	Wählen Sie Azure-Anmeldeinformationen aus der Dropdownliste aus.
Mandanten-ID	Geben Sie die Mandanten-ID ein.
Client-ID	Geben Sie die Client-ID ein.
Geheimer Clientschlüssel	Geben Sie den geheimen Clientschlüssel ein.

5. Klicken Sie auf **OK**.

Konfigurieren des Azure-Speicherkontos

Sie sollten das Azure-Speicherkonto in SnapCenter konfigurieren.

Das Azure-Speicherkonto enthält Details zur Abonnement-ID, den Azure-Anmeldeinformationen und dem Azure NetApp -Konto.



Die Standardlizenzen und die kapazitätsbasierte Lizenz sind für Azure NetApp Files nicht erforderlich.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Speichersysteme**.
2. Wählen Sie auf der Seite „Speichersysteme“ * Azure NetApp Files* aus und klicken Sie auf **Neu**.
3. Wählen Sie die Anmeldeinformationen, die Abonnement-ID und das NetApp -Konto aus den jeweiligen Dropdown-Listen aus.
4. Klicken Sie auf **Senden**.

Erstellen Sie die Anmeldeinformationen zum Hinzufügen des Plug-In-Hosts

SnapCenter verwendet Anmeldeinformationen, um Benutzer für SnapCenter -Vorgänge zu authentifizieren.

Sie sollten Anmeldeinformationen für die Installation von SnapCenter Plug-Ins und zusätzliche Anmeldeinformationen für die Durchführung von Datenschutzvorgängen erstellen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**.
4. Geben Sie auf der Seite „Anmeldeinformationen“ die folgenden Informationen an, die zum Erstellen der Anmeldeinformationen erforderlich sind.

Für dieses Feld...	Machen Sie Folgendes...
Anmeldeinformationsname	Geben Sie einen Namen für die Anmeldeinformationen ein.
Authentifizierungsmodus	Wählen Sie den Authentifizierungsmodus aus der Dropdown-Liste aus.
Authentifizierungstyp	Wählen Sie entweder Passwortbasiert oder SSH-Schlüsselbasiert (nur für Linux-Host).
Benutzername	Geben Sie den Benutzernamen an.
Passwort	Wenn Sie die kennwortbasierte Authentifizierung ausgewählt haben, geben Sie das Kennwort an.
Privater SSH-Schlüssel	Wenn Sie die SSH-Schlüssel-basierte Authentifizierung ausgewählt haben, geben Sie den privaten Schlüssel an.
Verwenden Sie Sudo-Berechtigungen	Aktivieren Sie das Kontrollkästchen „Sudo-Berechtigungen verwenden“, wenn Sie Anmeldeinformationen für einen Nicht-Root-Benutzer erstellen.  Dies gilt nur für Linux-Benutzer.

5. Klicken Sie auf **OK**.

Schützen Sie SAP HANA-Datenbanken

Hosts hinzufügen und SnapCenter Plug-In für SAP HANA-Datenbank installieren

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen und dann die Plug-In-Pakete zu installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

Bevor Sie beginnen

- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.
- Wenn Sie die Installation auf dem zentralen Host durchführen, stellen Sie sicher, dass die SAP HANA-Clientsoftware auf diesem Host installiert ist, und öffnen Sie die erforderlichen Ports auf dem SAP HANA-Datenbankhost, um die HDB-SQL-Abfragen remote auszuführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Aktionen aus:
 - a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
 - b. Geben Sie im Feld „Hostname“ den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.
 - c. Geben Sie im Feld „Anmeldeinformationen“ die von Ihnen erstellten Anmeldeinformationen ein.
5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie auf **Weitere Optionen** und geben Sie die Details an.
7. Klicken Sie auf **Senden**.
8. Wenn der Hosttyp Linux ist, überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.

9. Überwachen Sie den Installationsfortschritt.

SAP HANA-Datenbank hinzufügen

Sie sollten die SAP HANA-Datenbank manuell hinzufügen.

Informationen zu diesem Vorgang

Ressourcen müssen manuell hinzugefügt werden, wenn das Plug-in auf einem zentralen Server installiert ist. Wenn das SAP HANA-Plug-In auf dem HANA-Datenbankhost installiert ist, wird das HANA-System automatisch erkannt.



Die automatische Erkennung wird für die HANA-Multihostkonfiguration nicht unterstützt. Sie muss nur über ein zentrales Plug-In hinzugefügt werden.

Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter -Plug-in für die SAP HANA-Datenbank aus der Dropdown-Liste aus und klicken Sie dann auf **Ressourcen**.
2. Klicken Sie auf der Seite „Ressourcen“ auf **SAP HANA-Datenbank hinzufügen**.
3. Führen Sie auf der Seite „Ressourcendetails angeben“ die folgenden Aktionen aus:
 - a. Geben Sie den Ressourcentyp entweder als Einzelcontainer, Multitenant-Datenbankcontainer oder Nicht-Datenvolume ein.
 - b. Geben Sie den SAP HANA-Systemnamen ein.
 - c. Geben Sie die System-ID (SID) ein.
 - d. Wählen Sie den Plug-In-Host aus.
 - e. Geben Sie den Schlüssel ein, um eine Verbindung zum SAP HANA-System herzustellen.
 - f. Geben Sie den Benutzernamen ein, für den der HDB Secure User Store Key konfiguriert ist.
4. Wählen Sie auf der Seite „Speicherbedarf angeben“ als Speichertyp „Azure NetApp Files“ aus.
 - a. Wählen Sie das Azure NetApp Konto aus.

- b. Wählen Sie den Kapazitätspool und die zugehörigen Volumes aus.
- c. Klicken Sie auf **Speichern**.
5. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Erstellen von Sicherungsrichtlinien für SAP HANA-Datenbanken

Bevor Sie SnapCenter zum Sichern von SAP HANA-Datenbankressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten.

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 Richtliniennamen und eine Beschreibung ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
 - a. Wählen Sie als Speichertyp * Azure NetApp Files* aus.
 - b. Wählen Sie **Dateibasiert**, wenn Sie eine Integritätsprüfung der Datenbank durchführen möchten.
 - c. Wählen Sie **Snapshot-basiert**, wenn Sie ein Backup mithilfe der Snapshot-Technologie erstellen möchten.
6. Führen Sie auf der Seite „Snapshot und Sicherung“ die folgenden Schritte aus:
 - a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
 - b. Geben Sie die Aufbewahrungseinstellungen an.
 - c. Wenn Sie die Azure NetApp Files -Sicherung aktivieren möchten, wählen Sie **Sicherung aktivieren** und geben Sie die Aufbewahrungseinstellungen an.
7. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**.

Erstellen von Ressourcengruppen und Anfügen von SAP HANA-Sicherungsrichtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten.

Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft 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.

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 der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Name	Geben Sie einen Namen für die Ressourcengruppe ein.
Schlagwörter	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.
5. 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.
 - b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf *  * für die Richtlinie, die Sie konfigurieren möchten.
 - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.
7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
8. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Sichern von SAP HANA-Datenbanken, die auf Azure NetApp Files ausgeführt werden

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

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Ressourcenseite die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.
3. Wählen Sie die Ressource aus, die Sie sichern möchten.
4. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.
5. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:
 - a. Wählen Sie den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen.

- b. Wählen Sie den Pfeil **Skripts** aus, um Vor- und Nachbefehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge auszuführen.
- c. Wählen Sie den Pfeil **Benutzerdefinierte Konfigurationen** aus und geben Sie dann die benutzerdefinierten Wertepaare ein, die für alle Jobs erforderlich sind, die diese Ressource verwenden.
- d. Wählen Sie **Snapshot Copy Tool > SnapCenter ohne Dateisystemkonsistenz**, um Snapshots zu erstellen.

Die Option **Dateisystemkonsistenz** ist nur für Anwendungen anwendbar, die auf Windows-Hosts ausgeführt werden.

6. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

- a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
- b. Wählen *  * in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamenname* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

policy_name ist der Name der von Ihnen ausgewählten Richtlinie.

7. 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. SMTP muss auch unter **Einstellungen > Globale Einstellungen** konfiguriert werden.

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

9. Wählen Sie **Jetzt sichern**.

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

- a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, 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.

11. Wählen Sie **Backup**.

12. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

Sichern von SAP HANA-Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

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.

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 der Ressourcengruppe mehrere Richtlinien zugeordnet sind, 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 **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

Wiederherstellen und Wiederherstellen von SAP HANA-Datenbanken

Sie können Daten aus den Sicherungen wiederherstellen und wiederherstellen.

Informationen zu diesem Vorgang

Wenn bei automatisch erkannten HANA-Systemen die Option **Vollständige Ressource** ausgewählt ist, erfolgt die Wiederherstellung mithilfe der Snapshot-Wiederherstellungstechnologie für einzelne Dateien. Wenn das Kontrollkästchen **Schnelle Wiederherstellung** aktiviert ist, wird die Volume Revert-Technologie verwendet.

Für manuell hinzugefügte Ressourcen wird immer die Volume Revert-Technologie verwendet.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.
3. Wählen Sie die Ressource aus oder wählen Sie eine Ressourcengruppe und dann eine Ressource in dieser Gruppe aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder aus dem primären oder sekundären (gespiegelten oder im Tresor gespeicherten) Speichersystem aus.
5. Wählen Sie in der Tabelle „Primäre Sicherung(en)“ die Sicherung aus, aus der Sie wiederherstellen möchten, und klicken Sie dann auf *  *.
6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ die Option **Vollständige Ressource** aus.

Alle konfigurierten Datenvolumes der SAP HANA-Datenbank werden wiederhergestellt.

7. Führen Sie für automatisch erkannte HANA-Systeme auf der Seite „Wiederherstellungsbereich“ die folgenden Aktionen aus:
 - a. Wählen Sie **Auf den aktuellsten Stand wiederherstellen**, wenn Sie die Wiederherstellung so nah wie möglich an die aktuelle Zeit heranführen möchten.
 - b. Wählen Sie **Bis zu einem bestimmten Zeitpunkt wiederherstellen**, wenn Sie bis zum angegebenen Zeitpunkt wiederherstellen möchten.
 - c. Wählen Sie **Aus angegebener Datensicherung wiederherstellen**, wenn Sie eine Wiederherstellung aus einer bestimmten Datensicherung durchführen möchten.

- d. Wählen Sie **Keine Wiederherstellung**, wenn Sie jetzt keine Wiederherstellung wünschen.
- e. Geben Sie die Speicherorte für die Protokollsicherung an.
- f. Geben Sie den Speicherort des Sicherungskatalogs an.
8. Geben Sie auf der Seite „Pre Ops“ die Befehle „Pre Restore“ und „Unmount“ ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
9. Geben Sie auf der Seite „Post Ops“ die Befehle „Mount“ und „Post Restore“ ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
10. 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. SMTP muss auch auf der Seite **Einstellungen > Globale Einstellungen** konfiguriert werden.

11. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

Klonen Sie die SAP HANA-Datenbanksicherung

Sie können SnapCenter verwenden, um eine SAP HANA-Datenbank mithilfe der Sicherung der Datenbank zu klonen. Bei den erstellten Klonen handelt es sich um dicke Klone, die im übergeordneten Kapazitätspool erstellt werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Filtern Sie auf der Seite „Ressourcen“ die Ressourcen aus der Dropdown-Liste **Anzeigen** basierend auf dem Ressourcentyp.
3. Wählen Sie die Ressource oder Ressourcengruppe aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** vom primären Speichersystem aus.
5. Wählen Sie die Datensicherung aus der Tabelle aus und klicken Sie anschließend auf .
6. Führen Sie auf der Seite „Standort“ die folgenden Aktionen aus:
 - a. Wählen Sie den Host aus, auf dem das SAP HANA-Plug-In zur Verwaltung des geklonten HANA-Systems installiert ist.

Es kann sich um einen zentralen Plug-In-Host oder einen HANA-Systemhost handeln.



Wenn das HANA-Plug-In auf einem zentralen Host installiert ist, der HANA-Datenbanken auf anderen Hosts verwaltet, überspringt SnapCenter beim Erstellen oder Löschen von Klonen absichtlich Host-seitige Vorgänge (Mounten oder Unmounten des Dateisystems), da der Zielsystem ein zentraler Host ist. Sie sollten benutzerdefinierte Skripte vor oder nach dem Klonen verwenden, um Mount- und Unmount-Vorgänge durchzuführen.

- a. Geben Sie die SAP HANA-SID ein, um aus den vorhandenen Sicherungen zu klonen.
- b. Geben Sie die IP-Adressen oder Hostnamen ein, auf die die geklonten Volumes exportiert werden.

- c. Wenn die ANF-Volumes der SAP HANA-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie das QOS für die geklonten Volumes an.

Wenn die QOS für die geklonten Volumes nicht angegeben ist, wird die QOS des Quellvolumes verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

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

- a. Geben Sie die Befehle für „Pre-Clone“ oder „Post-Clone“ ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
- b. Geben Sie den Mount-Befehl ein, um ein Dateisystem auf einem Host zu mounten.

Wenn das HANA-Quellsystem automatisch erkannt wird und das Plug-In für den Klonzielhost auf dem SAP HANA-Host installiert ist, trennt SnapCenter automatisch die Bereitstellung der vorhandenen HANA-Datenvolumes auf dem Klonzielhost und stellt die neu geklonten HANA-Datenvolumes bereit.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.



Clone Split ist für ANF-Klone deaktiviert, da der ANF-Klon bereits ein unabhängiges Volume ist, das aus dem ausgewählten Snapshot erstellt wurde.

Schützen Sie Microsoft SQL Server-Datenbanken

Hosts hinzufügen und SnapCenter Plug-In für SQL Server-Datenbank installieren

SnapCenter unterstützt den Datenschutz von SQL-Instanzen auf SMB-Freigaben auf Azure NetApp Files. Die eigenständigen und Verfügbarkeitsgruppenkonfigurationen (AG) werden unterstützt.

Sie müssen die SnapCenter -Seite „Host hinzufügen“ verwenden, um Hosts hinzuzufügen, und dann das Plug-In-Paket installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

Bevor Sie beginnen

- Sie müssen ein Benutzer sein, dem eine Rolle mit den Berechtigungen zum Installieren und Deinstallieren von Plug-Ins zugewiesen ist, beispielsweise die SnapCenter Administratorrolle.
- Wenn Sie beim Installieren eines Plug-Ins auf einem Windows-Host Anmeldeinformationen angeben, die nicht integriert sind, oder wenn der Benutzer zu einem lokalen Arbeitsgruppenbenutzer gehört, müssen Sie die Benutzerkontensteuerung auf dem Host deaktivieren.

Schritte

1. Wählen Sie im linken Navigationsbereich **Hosts** aus.
2. Stellen Sie sicher, dass oben die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Wählen Sie **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Schritte aus:

- a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
- b. Geben Sie im Feld „Hostname“ den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.
- c. Geben Sie im Feld „Anmeldeinformationen“ die von Ihnen erstellten Anmeldeinformationen ein.
5. Wählen Sie im Abschnitt **Zu installierende Plug-ins auswählen** die zu installierenden Plug-ins aus.
6. (Optional) Klicken Sie auf **Weitere Optionen** und geben Sie die Details an.
7. Wählen Sie **Senden**.
8. Wählen Sie **Protokollverzeichnis konfigurieren**, geben Sie auf der Seite „Host-Protokollverzeichnis konfigurieren“ den SMB-Pfad des Host-Protokollverzeichnisses ein und klicken Sie auf **Speichern**.
9. Klicken Sie auf **Senden** und überwachen Sie den Installationsfortschritt.

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.

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 Richtliniennamen und eine Beschreibung ein.
5. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
 - a. Wählen Sie als Speichertyp * Azure NetApp Files* aus.
 - b. Wählen Sie den Sicherungstyp aus.
 - i. Wählen Sie **Vollständige Sicherung und Protokollsicherung**, wenn Sie Datenbankdateien und Transaktionsprotokolle sichern möchten.
 - ii. Wählen Sie **Vollständige Sicherung**, wenn Sie nur die Datenbankdateien sichern möchten.
 - iii. Wählen Sie **Protokollsicherung**, wenn Sie nur die Transaktionsprotokolle sichern möchten.
 - iv. Wählen Sie **Nur Backup kopieren**, wenn Sie Ihre Ressourcen mithilfe einer anderen Anwendung sichern möchten.
 - c. Führen Sie im Abschnitt „Einstellungen der Verfügbarkeitsgruppe“ die folgenden Aktionen aus:
 - i. Wählen Sie „Auf bevorzugter Sicherungsreplik sichern“, wenn Sie nur auf der Replik sichern möchten.
 - ii. Wählen Sie das primäre AG-Replikat oder das sekundäre AG-Replikat für die Sicherung aus.
 - iii. Wählen Sie die Sicherungspriorität aus.
6. Führen Sie auf der Seite „Snapshot und Sicherung“ die folgenden Schritte aus:
 - a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
 - b. Geben Sie die Aufbewahrungseinstellungen je nach ausgewähltem Sicherungstyp an.
 - c. Wenn Sie die Azure NetApp Files -Sicherung aktivieren möchten, wählen Sie **Sicherung aktivieren**

und geben Sie die Aufbewahrungseinstellungen an.

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

- a. Wählen Sie im Abschnitt „Überprüfung für folgende Sicherungszeitpläne ausführen“ die Zeitplanhäufigkeit aus.
- b. Führen Sie im Abschnitt „Optionen zur Datenbankkonsistenzprüfung“ die folgenden Aktionen aus:
 - 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.
 - ii. Wählen Sie **Alle Informationsmeldungen unterdrücken (NO_INFOMSGS)**, um alle Informationsmeldungen zu unterdrücken.

Standardmäßig ausgewählt.

- iii. Wählen Sie **Alle gemeldeten Fehlermeldungen pro Objekt anzeigen (ALL_ERRORMSGs)**, um alle gemeldeten Fehler pro Objekt anzuzeigen.
- iv. 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.

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

8. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**.

Erstellen von Ressourcengruppen und Anfügen von SQL-Sicherungsrichtlinien

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen, die Sie sichern und schützen möchten.

Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft 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.

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 der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Name	Geben Sie einen Namen für die Ressourcengruppe ein.
Schlagwörter	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.
5. 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.
 - b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf *  * für die Richtlinie, die Sie konfigurieren möchten.
 - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.
 - d. Wählen Sie den Microsoft SQL Server-Scheduler aus.
7. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
 - a. Wählen Sie den Verifizierungsserver aus.
 - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf *  *.
 - c. Wählen Sie entweder **Überprüfung nach Sicherung ausführen** oder **Geplante Überprüfung ausführen**.
 - d. Klicken Sie auf **OK**.
8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Sichern von SQL Server-Datenbanken, die auf Azure NetApp Files ausgeführt werden

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

Bevor Sie beginnen

Sie sollten einen Lastenausgleich erstellen, wenn dem Azure Windows-Failovercluster keine Cluster-IP zugewiesen ist oder er von SnapCenter aus nicht erreichbar ist. Die IP des Load Balancers sollte konfiguriert

und vom SnapCenter -Server aus erreichbar sein.

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 Ressourcenseite aus der Dropdownliste „Anzeigen“ die Option „Datenbank“, „Instanz“ oder „Verfügbarkeitsgruppe“ aus.
3. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.
4. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:
 - a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
 - b. Wählen *  * in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
 - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.

policy_name ist der Name der von Ihnen ausgewählten Richtlinie.
 - d. 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.
 - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf *  *.
 - c. Wählen Sie entweder **Überprüfung nach Sicherung ausführen** oder **Geplante Überprüfung ausführen**.
 - d. Klicken Sie auf OK.
6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
8. Wählen Sie **Jetzt sichern**.
9. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
 - a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.
 - b. Wählen Sie **Nach Sicherung überprüfen**.
 - c. Wählen Sie **Backup**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

Sichern von SQL Server-Ressourcengruppen

Sie können Ressourcengruppen sichern, die aus mehreren Ressourcen bestehen. Ein Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe

definierten Ressourcen ausgeführt.

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.
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 der Ressourcengruppe mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.
 - b. Wählen Sie nach der Sicherung „Überprüfen“ aus, um die On-Demand-Sicherung zu überprüfen.
 - c. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

Wiederherstellen und Wiederherstellen von SQL Server-Datenbanken

Sie können SnapCenter verwenden, um gesicherte SQL Server-Datenbanken wiederherzustellen. Die Datenbankwiederherstellung ist ein mehrphasiger Prozess, bei dem alle Daten und Protokollseiten aus einer angegebenen SQL Server-Sicherung in eine angegebene Datenbank kopiert werden.

Informationen zu diesem Vorgang

Sie sollten sicherstellen, dass die Zielinanz für die Wiederherstellung mit einem Active Directory-Benutzer konfiguriert ist, der zur Active Directory-Domäne SMB AD gehört und über die Berechtigung verfügt, die Dateiberechtigungen entsprechend festzulegen. Sie sollten die Anmeldeinformationen in SnapCenter auf Instanzebene konfigurieren.

Die SQL-Authentifizierung für die Zielinanz wird für SMB-Konfigurationen nicht unterstützt. Die Zielinanz sollte in SnapCenter mit dem Active Directory-Benutzer konfiguriert werden, der über die erforderlichen Berechtigungen verfügt.

Wenn das Dienstkonto der SnapCenter Plug-in-Dienste kein Active Directory-Benutzer ist, wird beim Durchführen der Wiederherstellung auf einem alternativen Host der Benutzer benötigt, der die vollständige Kontrolle über die Quellvolumes hat, damit dieser seine Identität annehmen und den erforderlichen Vorgang ausführen kann.

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“ entweder „**Datenbank**“ oder „**Ressourcengruppe**“ aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ die Option „**Backups** vom Speichersystem“ aus.
5. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf das  Symbol.
6. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:

- a. Wählen Sie **Datenbank auf demselben Host wiederherstellen, auf dem die Sicherung erstellt wurde**, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Sicherungen erstellt wurden.
 - b. Wählen Sie **Datenbank auf einem anderen Host wiederherstellen**, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem die Sicherungen erstellt werden.
7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:
- a. Wählen Sie **Keine**, wenn Sie nur die vollständige Sicherung ohne Protokolle wiederherstellen müssen.
 - b. Wählen Sie den minutengenauen Wiederherstellungsvorgang „Alle Protokollsicherungen“ aus, um alle verfügbaren Protokollsicherungen nach der vollständigen Sicherung wiederherzustellen.
 - c. Wählen Sie **Nach Protokollsicherungen** aus, um einen Wiederherstellungsvorgang zu einem bestimmten Zeitpunkt durchzuführen, bei dem die Datenbank basierend auf Sicherungsprotokollen bis zum Sicherungsprotokoll mit dem ausgewählten Datum wiederhergestellt wird.
 - d. Wählen Sie **Bis zu einem bestimmten Datum bis** aus, um das Datum und die Uhrzeit anzugeben, nach denen Transaktionsprotokolle nicht mehr auf die wiederhergestellte Datenbank angewendet werden.
 - e. Wenn Sie **Alle Protokollsicherungen**, **Nach Protokollsicherungen** oder **Nach bestimmtem Datum bis** ausgewählt haben und sich die Protokolle an einem benutzerdefinierten Speicherort befinden, wählen Sie **Benutzerdefiniertes Protokollverzeichnis verwenden** und geben Sie dann den Protokollspeicherort an.
8. Geben Sie auf der Seite „Pre-Ops“ und „Post-Ops“ die erforderlichen Details an.
9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Überwachen > Jobs**.

Klonen Sie die SQL Server-Datenbanksicherung

Sie können SnapCenter verwenden, um eine SQL-Datenbank mithilfe der Sicherung der Datenbank zu klonen. Bei den erstellten Klonen handelt es sich um dicke Klone, die im übergeordneten Kapazitätspool erstellt werden.

Informationen zu diesem Vorgang

Sie sollten sicherstellen, dass die Ziellinstanz für den Klon mit einem Active Directory-Benutzer konfiguriert ist, der zur Active Directory-Domäne SMB AD gehört und über die Berechtigung verfügt, die Dateiberechtigungen entsprechend festzulegen. Sie sollten die Anmeldeinformationen in SnapCenter auf Instanzebene konfigurieren.

Die SQL-Authentifizierung für die Ziellinstanz wird für SMB-Konfigurationen nicht unterstützt. Die Ziellinstanz sollte in SnapCenter mit dem Active Directory-Benutzer konfiguriert werden, der über die erforderlichen Berechtigungen verfügt.

Wenn das Dienstkonto der SnapCenter Plug-in-Dienste kein Active Directory-Benutzer ist, wird beim Klonen der Benutzer benötigt, der die vollständige Kontrolle über die Quellvolumes hat, damit seine Identität angenommen werden kann und der erforderliche Vorgang ausgeführt werden kann.

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“ entweder „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Kopien verwalten** die Sicherung vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus und wählen Sie dann *  *.
6. Geben Sie auf der Seite **Klonoptionen** alle erforderlichen Details ein.
7. Wählen Sie auf der Seite „Speicherort“ einen Speicherort aus, um einen Klon zu erstellen.

Wenn die ANF-Volumes der SQL Server-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie die QOS für die geklonten Volumes an.

Wenn die QOS für die geklonten Volumes nicht angegeben ist, wird die QOS des Quellvolumes verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

8. Wählen Sie auf der Seite „Protokolle“ eine der folgenden Optionen aus:
 - a. Wählen Sie **Keine**, wenn Sie nur die vollständige Sicherung ohne Protokolle klonen möchten.
 - b. Wählen Sie **Alle Protokollsicherungen** aus, wenn Sie alle verfügbaren Protokollsicherungen mit Datum nach der vollständigen Sicherung klonen möchten.
 - c. Wählen Sie **Nach Protokollsicherungen bis**, wenn Sie die Datenbank basierend auf den Sicherungsprotokollen klonen möchten, die bis zum Sicherungsprotokoll mit dem ausgewählten Datum erstellt wurden.
 - d. Wählen Sie **Nach bestimmtem Datum bis** aus, wenn Sie die Transaktionsprotokolle nach dem angegebenen Datum und der angegebenen Uhrzeit nicht mehr anwenden möchten.
9. Geben Sie auf der Seite **Skript** das Skript-Timeout, den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Klonvorgang ausgeführt werden soll.
10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
11. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

Klon-Lebenszyklus durchführen

Mit SnapCenter können Sie Klone aus einer Ressourcengruppe oder Datenbank erstellen. Sie können entweder einen On-Demand-Klon durchführen oder wiederkehrende Klonvorgänge einer Ressourcengruppe oder Datenbank planen. Wenn Sie regelmäßig ein Backup klonen, können Sie den Klon zum Entwickeln von Anwendungen, Auffüllen von Daten oder Wiederherstellen von Daten verwenden.

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“ entweder „Datenbank“ oder „Ressourcengruppe“ aus der Liste „Anzeigen“ aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Kopien verwalten** die Sicherung vom primären Speichersystem aus.

5. Wählen Sie die Sicherung aus und wählen Sie dann *  *.
6. Geben Sie auf der Seite **Klonooptionen** alle erforderlichen Details ein.
7. Wählen Sie auf der Seite „Speicherort“ einen Speicherort aus, um einen Klon zu erstellen.

Wenn die ANF-Volumes der SQL Server-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie die QOS für die geklonten Volumes an.

Wenn die QOS für die geklonten Volumes nicht angegeben ist, wird die QOS des Quellvolumes verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

8. Geben Sie auf der Seite **Skript** das Skript-Timeout, den Pfad und die Argumente des Präskripts oder Postskripts ein, das vor bzw. nach dem Klonvorgang ausgeführt werden soll.
9. Führen Sie auf der Seite „Planen“ eine der folgenden Aktionen aus:
 - Wählen Sie **Jetzt ausführen**, wenn Sie den Klonauftrag sofort ausführen möchten.
 - Wählen Sie **Zeitplan konfigurieren** aus, wenn Sie festlegen möchten, wie häufig der Klonvorgang erfolgen soll, wann der Klonzeitplan beginnen soll, an welchem Tag der Klonvorgang erfolgen soll, wann der Zeitplan ablaufen soll und ob die Klone nach Ablauf des Zeitplans gelöscht werden müssen.
10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
11. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

Schützen Sie Oracle-Datenbanken

Hosts hinzufügen und SnapCenter Plug-In für Oracle-Datenbank installieren

Sie können auf der Seite „Host hinzufügen“ Hosts hinzufügen und dann das SnapCenter Plug-ins-Paket für Linux oder das SnapCenter Plug-ins-Paket für AIX installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

Sie können einen Host hinzufügen und Plug-In-Pakete entweder für einen einzelnen Host oder für einen Cluster installieren. Wenn Sie das Plug-in auf einem Cluster (Oracle RAC) installieren, wird das Plug-in auf allen Knoten des Clusters installiert. Für Oracle RAC One Node sollten Sie das Plug-in sowohl auf aktiven als auch auf passiven Knoten installieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Aktionen aus:
 - a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
 - b. Geben Sie im Feld „Hostname“ den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des Hosts ein.
 - c. Geben Sie im Feld „Anmeldeinformationen“ die von Ihnen erstellten Anmeldeinformationen ein.
5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die zu installierenden Plug-ins aus.

6. (Optional) Klicken Sie auf **Weitere Optionen** und geben Sie die Details an.
7. Klicken Sie auf **Senden**.
8. Überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

In einer Cluster-Konfiguration sollten Sie den Fingerabdruck jedes Knotens im Cluster überprüfen.

9. Überwachen Sie den Installationsfortschritt.

Erstellen von Sicherungsrichtlinien für Oracle-Datenbanken

Bevor Sie SnapCenter zum Sichern von Oracle-Datenbankressourcen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, die Sie sichern möchten.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Wählen Sie „Oracle-Datenbank“ aus der Dropdownliste aus.
4. Klicken Sie auf **Neu**.
5. Geben Sie auf der Seite „Name“ den Richtliniennamen und eine Beschreibung ein.
6. Führen Sie auf der Seite „Richtlinientyp“ die folgenden Schritte aus:
 - a. Wählen Sie als Speichertyp * Azure NetApp Files* aus.
 - b. Wählen Sie als Sicherungstyp entweder Online- oder Offline-Sicherung aus.
 - c. Wenn Sie die Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren möchten, wählen Sie **Sicherung mit Oracle Recovery Manager (RMAN) katalogisieren**.
 - d. Wenn Sie Archivprotokolle nach der Sicherung bereinigen möchten, wählen Sie **Archivprotokolle nach der Sicherung bereinigen**.
 - e. Geben Sie die Einstellungen zum Löschen des Archivprotokolls an.
7. Führen Sie auf der Seite „Snapshot und Sicherung“ die folgenden Schritte aus:
 - a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
 - b. Geben Sie die Aufbewahrungseinstellungen an.
 - c. Wenn Sie die Azure NetApp Files -Sicherung aktivieren möchten, wählen Sie **Sicherung aktivieren** und geben Sie die Aufbewahrungseinstellungen an.
8. Geben Sie auf der Seite „Skript“ den Pfad und die Argumente des Präskripts oder Postskripts ein, das Sie vor bzw. nach dem Sicherungsvorgang ausführen möchten.
9. Wählen Sie auf der Seite „Überprüfung“ den Sicherungszeitplan aus, für den Sie den Überprüfungsvorgang durchführen möchten, und geben Sie den Pfad und die Argumente des Präskripts oder Postskripts ein, das Sie vor bzw. nach dem Überprüfungsvorgang ausführen möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**.

Erstellen Sie Ressourcengruppen und fügen Sie Oracle-Sicherungsrichtlinien hinzu

Eine Ressourcengruppe ist der Container, zu dem Sie Ressourcen hinzufügen müssen,

die Sie sichern und schützen möchten.

Mit einer Ressourcengruppe können Sie alle Daten, die mit einer bestimmten Anwendung verknüpft 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.

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 der Seite „Ressourcen“ auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite „Name“ die folgenden Aktionen aus:

Für dieses Feld...	Machen Sie Folgendes...
Name	Geben Sie einen Namen für die Ressourcengruppe ein.
Schlagwörter	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen später bei der Suche nach der Ressourcengruppe helfen.
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.
Ziel der Archivprotokolldatei	Geben Sie die Ziele der Archivprotokolldateien an.

4. Wählen Sie auf der Seite „Ressourcen“ einen Hostnamen aus der Dropdownliste **Host** und einen Ressourcentyp aus der Dropdownliste **Ressourcentyp** aus.
5. 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.
 - b. Klicken Sie in der Spalte „Zeitpläne konfigurieren“ auf *  * für die Richtlinie, die Sie konfigurieren möchten.
 - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.
7. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
 - a. Wählen Sie den Verifizierungsserver aus.
 - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf *  .
 - c. Wählen Sie entweder **Überprüfung nach Sicherung ausführen** oder **Geplante Überprüfung ausführen**.
 - d. Klicken Sie auf **OK**.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.

Sichern von Oracle-Datenbanken, die auf Azure NetApp Files ausgeführt werden

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

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 Ressourcenseite in der Dropdownliste „Ansicht“ die Option „Datenbank“ aus.
3. Wählen Sie auf der Ressourcenseite **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** aus und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.
4. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:
 - a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.
 - b. Wählen *  * in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.
 - c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan und wählen Sie dann **OK** aus.
5. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
 - a. Wählen Sie den Verifizierungsserver aus.
 - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungszeitplan konfigurieren möchten, und klicken Sie dann auf *  *.
 - c. Wählen Sie entweder **Überprüfung nach Sicherung ausführen** oder **Geplante Überprüfung ausführen**.
 - d. Klicken Sie auf OK.
6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
8. Wählen Sie **Jetzt sichern**.
9. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
 - a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.
 - b. Klicken Sie auf **Sichern**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

Sichern von Oracle-Ressourcengruppen

Sie können Ressourcengruppen sichern, die aus mehreren Ressourcen bestehen. Ein

Sicherungsvorgang für die Ressourcengruppe wird für alle in der Ressourcengruppe definierten Ressourcen ausgeführt.

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.
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 der Ressourcengruppe mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.
 - b. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen** > **Jobs** auswählen.

Wiederherstellen und Wiederherstellen von Oracle-Datenbanken

Im Falle eines Datenverlusts können Sie mit SnapCenter Daten aus einem oder mehreren Backups auf Ihrem aktiven Dateisystem wiederherstellen und anschließend die Datenbank wiederherstellen.

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“ entweder **Datenbank** oder **Ressourcengruppe** aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** vom primären Speichersystem aus.
5. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf *  *.
6. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:
 - a. Wählen Sie RAC, wenn Sie eine Sicherung einer Datenbank in einer RAC-Umgebung ausgewählt haben.
 - b. Führen Sie die folgenden Aktionen aus:
 - i. Wählen Sie **Alle Datendateien**, wenn Sie nur die Datenbankdateien wiederherstellen möchten.
 - ii. Wählen Sie **Tablespaces**, wenn Sie nur die Tablespaces wiederherstellen möchten.
 - iii. Wählen Sie **Redo-Log-Dateien**, wenn Sie die Redo-Log-Dateien der Data Guard-Standby- oder Active Data Guard-Standby-Datenbanken wiederherstellen möchten.
 - iv. Wählen Sie **Pluggable Databases** und geben Sie die PDBs an, die Sie wiederherstellen möchten.
 - v. Wählen Sie **Pluggable Database (PDB)-Tablespaces** aus und geben Sie dann die PDB und die Tablespaces dieser PDB an, die Sie wiederherstellen möchten.
 - vi. Wählen Sie **Datenbank auf demselben Host wiederherstellen, auf dem die Sicherung erstellt wurde**, wenn Sie die Datenbank auf demselben SQL-Server wiederherstellen möchten, auf dem die Sicherungen erstellt wurden.

- vii. Wählen Sie **Datenbank auf einem anderen Host wiederherstellen**, wenn die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederhergestellt werden soll, auf dem die Sicherungen erstellt werden.
 - viii. Wählen Sie **Datenbankstatus ändern, falls für Wiederherstellung und Recovery erforderlich** aus, um den Status der Datenbank in den für die Durchführung von Wiederherstellungs- und Recovery-Vorgängen erforderlichen Status zu ändern.
 - ix. Wählen Sie **In-Place-Wiederherstellung erzwingen**, wenn Sie eine In-Place-Wiederherstellung in Szenarien durchführen möchten, in denen nach der Sicherung neue Datendateien hinzugefügt werden oder wenn LUNs zu einer LVM-Datenträgergruppe hinzugefügt, gelöscht oder neu erstellt werden.
7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:
 - a. Wählen Sie **Alle Protokolle**, wenn Sie die letzte Transaktion wiederherstellen möchten.
 - b. Wählen Sie **Bis SCN (System Change Number)**, wenn Sie zu einer bestimmten SCN wiederherstellen möchten.
 - c. Wählen Sie **Datum und Uhrzeit**, wenn Sie die Wiederherstellung auf ein bestimmtes Datum und eine bestimmte Uhrzeit durchführen möchten.
 - d. Wählen Sie **Keine Wiederherstellung**, wenn Sie keine Wiederherstellung wünschen.
 - e. Wählen Sie **Externe Archivprotokollspeicherorte angeben**, wenn Sie den Speicherort der externen Archivprotokolldateien angeben möchten.
 8. Geben Sie auf der Seite „Pre-Ops“ und „Post-Ops“ die erforderlichen Details an.
 9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
 10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
 11. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen > Jobs** klicken.

Wiederherstellen und Wiederherstellen von Tablespaces mithilfe der Point-in-Time-Wiederherstellung

Sie können eine Teilmenge beschädigter oder gelöschter Tablespaces wiederherstellen, ohne dass dies Auswirkungen auf die anderen Tablespaces in der Datenbank hat. SnapCenter verwendet RMAN, um eine Point-in-Time-Wiederherstellung (PITR) der Tablespaces durchzuführen.

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“ entweder **„Datenbank“** oder **„Ressourcengruppe“** aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstanz (Multitenant)“ aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus dem Speichersystem aus.

Wenn das Backup nicht katalogisiert ist, sollten Sie das Backup auswählen und auf **Katalog** klicken.

5. Wählen Sie das katalogisierte Backup aus und klicken Sie dann auf *  *.
6. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:
 - a. Wählen Sie **RAC**, wenn Sie eine Sicherung einer Datenbank in einer RAC-Umgebung ausgewählt haben.

- b. Wählen Sie **Tablespaces**, wenn Sie nur die Tablespaces wiederherstellen möchten.
 - c. Wählen Sie **Datenbankstatus ändern, falls für Wiederherstellung und Recovery erforderlich** aus, um den Status der Datenbank in den für die Durchführung von Wiederherstellungs- und Recovery-Vorgängen erforderlichen Status zu ändern.
7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:
 - a. Wählen Sie **Bis SCN (System Change Number)**, wenn Sie zu einer bestimmten SCN wiederherstellen möchten.
 - b. Wählen Sie **Datum und Uhrzeit**, wenn Sie die Wiederherstellung auf ein bestimmtes Datum und eine bestimmte Uhrzeit durchführen möchten.
 8. Geben Sie auf der Seite „Pre-Ops“ und „Post-Ops“ die erforderlichen Details an.
 9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
 10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
 11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Überwachen > Jobs**.

Wiederherstellen und Wiederherstellen einer steckbaren Datenbank mithilfe der Point-in-Time-Wiederherstellung

Sie können eine Pluggable Database (PDB), die beschädigt oder gelöscht wurde, wiederherstellen, ohne dass dies Auswirkungen auf die anderen PDBs in der Containerdatenbank (CDB) hat. SnapCenter verwendet RMAN, um eine Point-in-Time-Wiederherstellung (PITR) der PDB durchzuführen.

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“ entweder **„Datenbank“** oder **„Ressourcengruppe“** aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstanz (Multitenant)“ aus.
4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** aus dem Speichersystem aus.

Wenn das Backup nicht katalogisiert ist, sollten Sie das Backup auswählen und auf **Katalog** klicken.

5. Wählen Sie das katalogisierte Backup aus und klicken Sie dann auf *  *.
6. Führen Sie auf der Seite „Wiederherstellungsbereich“ die folgenden Aufgaben aus:
 - a. Wählen Sie **RAC**, wenn Sie eine Sicherung einer Datenbank in einer RAC-Umgebung ausgewählt haben.
 - b. Führen Sie eine der folgenden Aktionen aus, je nachdem, ob Sie die PDB oder Tablespaces in einer PDB wiederherstellen möchten:
 - Wählen Sie **Pluggable Databases (PDBs)**, wenn Sie eine PDB wiederherstellen möchten.
 - Wählen Sie **Pluggable Database (PDB)-Tablespaces** aus, wenn Sie Tablespaces in einer PDB wiederherstellen möchten.
7. Wählen Sie auf der Seite „Wiederherstellungsbereich“ eine der folgenden Optionen aus:
 - a. Wählen Sie **Bis SCN (System Change Number)**, wenn Sie zu einer bestimmten SCN wiederherstellen möchten.

- b. Wählen Sie **Datum und Uhrzeit**, wenn Sie die Wiederherstellung auf ein bestimmtes Datum und eine bestimmte Uhrzeit durchführen möchten.
8. Geben Sie auf der Seite „Pre-Ops“ und „Post-Ops“ die erforderlichen Details an.
9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig**.
11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Überwachen > Jobs**.

Klonen Sie die Oracle-Datenbanksicherung

Sie können SnapCenter verwenden, um eine Oracle-Datenbank mithilfe der Sicherung der Datenbank zu klonen. Bei den erstellten Klonen handelt es sich um dicke Klone, die im übergeordneten Kapazitätspool erstellt werden.

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“ entweder **„Datenbank“** oder **„Ressourcengruppe“** aus.
3. Wählen Sie die Datenbank aus.
4. Wählen Sie auf der Ansichtsseite „Kopien verwalten“ die Sicherung vom primären Speichersystem aus.
5. Wählen Sie die Datensicherung aus und klicken Sie dann auf *  *.
6. Wählen Sie auf der Seite „Name“ aus, ob Sie eine Datenbank (CDB oder nicht CDB) oder eine Pluggable-Datenbank (PDB) klonen möchten.
7. Geben Sie auf der Seite „Standorte“ die erforderlichen Details an.

Wenn die ANF-Volumes der Oracle-Datenbank in einem manuellen QOS-Kapazitätspool konfiguriert sind, geben Sie das QOS für die geklonten Volumes an.

Wenn die QOS für die geklonten Volumes nicht angegeben ist, wird die QOS des Quellvolumes verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

8. Führen Sie auf der Seite „Anmeldeinformationen“ einen der folgenden Schritte aus:
 - a. Wählen Sie unter Anmeldeinformationsname für Sys-Benutzer die Anmeldeinformationen aus, die zum Definieren des Sys-Benutzerkennworts der Klondatenbank verwendet werden sollen.
 - b. Wählen Sie für den Anmeldeinformationsnamen der ASM-Instanz **Keine** aus, wenn die Betriebssystemauthentifizierung für die Verbindung mit der ASM-Instanz auf dem Klonhost aktiviert ist.

Andernfalls wählen Sie die Oracle ASM-Anmeldeinformationen aus, die entweder mit dem Benutzer „sys“ oder einem Benutzer mit der für den Klonhost geltenden Berechtigung „sysasm“ konfiguriert sind.

9. Geben Sie auf der Seite „Pre-Ops“ den Pfad und die Argumente der Prescripts an und ändern Sie im Abschnitt „Datenbankparametereinstellungen“ die Werte der vorab ausgefüllten Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.
10. Auf der Seite „Post-Ops“ sind standardmäßig **„Datenbank wiederherstellen“** und **„Bis Abbrechen“** ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.

- a. Wenn Sie „Bis Abbrechen“ auswählen, führt SnapCenter die Wiederherstellung durch, indem es die neueste Protokollsicherung mit der ununterbrochenen Sequenz von Archivprotokollen nach der zum Klonen ausgewählten Datensicherung bereitstellt.
- b. Wenn Sie **Datum und Uhrzeit** auswählen, stellt SnapCenter die Datenbank bis zu einem angegebenen Datum und einer angegebenen Uhrzeit wieder her.
- c. Wenn Sie **Bis SCN** auswählen, stellt SnapCenter die Datenbank bis zu einem angegebenen SCN wieder her.
- d. Wenn Sie **Externe Archivprotokollspeicherorte angeben** auswählen, ermittelt und mountet SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit.
- e. Standardmäßig ist das Kontrollkästchen **Neue DBID erstellen** aktiviert, um eine eindeutige Nummer (DBID) für die geklonte Datenbank zu generieren, die sie von der Quelldatenbank unterscheidet.

Deaktivieren Sie das Kontrollkästchen, wenn Sie der geklonten Datenbank die DBID der Quelldatenbank zuweisen möchten. Wenn Sie in diesem Szenario die geklonte Datenbank beim externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.

- f. Aktivieren Sie das Kontrollkästchen **Temporäre Datei für temporären Tablespace erstellen**, wenn Sie eine temporäre Datei für den standardmäßigen temporären Tablespace der geklonten Datenbank erstellen möchten.
 - g. Fügen Sie unter **Geben Sie SQL-Einträge ein, die beim Erstellen des Klons angewendet werden sollen** die SQL-Einträge hinzu, die beim Erstellen des Klons angewendet werden sollen.
 - h. Geben Sie unter **Geben Sie die nach dem Klonvorgang auszuführenden Skripts ein** den Pfad und die Argumente des Postskripts an, das Sie nach dem Klonvorgang ausführen möchten.
11. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
 12. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
 13. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen > Jobs** auswählen.

Klonen einer steckbaren Datenbank

Sie können eine Pluggable Database (PDB) auf eine andere oder dieselbe Ziel-CDB auf demselben Host oder einem alternativen Host klonen. Sie können die geklonte PDB auch zu einem gewünschten SCN oder Datum und einer gewünschten Uhrzeit wiederherstellen.

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“ entweder **„Datenbank“** oder **„Ressourcengruppe“** aus.
3. Wählen Sie die Datenbank vom Typ „Einzelinstantz (Multitenant)“ aus.
4. Wählen Sie auf der Ansichtsseite „Kopien verwalten“ die Sicherung vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus und klicken Sie dann auf *  *.
6. Wählen Sie auf der Seite „Name“ **PDB-Klon** aus und geben Sie die anderen Details an.
7. Geben Sie auf der Seite „Standorte“ die erforderlichen Details an.

8. Geben Sie auf der Seite „Pre-Ops“ den Pfad und die Argumente der Prescripts an und ändern Sie im Abschnitt „Datenbankparametereinstellungen“ die Werte der vorab ausgefüllten Datenbankparameter, die zum Initialisieren der Datenbank verwendet werden.
9. Auf der Seite „Post-Ops“ ist standardmäßig **„Bis Abbrechen“** ausgewählt, um die Wiederherstellung der geklonten Datenbank durchzuführen.
 - a. Wenn Sie „Bis Abbrechen“ auswählen, führt SnapCenter die Wiederherstellung durch, indem es die neueste Protokollsicherung mit der ununterbrochenen Sequenz von Archivprotokollen nach der zum Klonen ausgewählten Datensicherung bereitstellt.
 - b. Wenn Sie **Datum und Uhrzeit** auswählen, stellt SnapCenter die Datenbank bis zu einem angegebenen Datum und einer angegebenen Uhrzeit wieder her.
 - c. Wenn Sie **Externe Archivprotokollspeicherorte angeben** auswählen, ermittelt und mountet SnapCenter die optimale Anzahl von Protokollsicherungen basierend auf der angegebenen SCN oder dem ausgewählten Datum und der ausgewählten Uhrzeit.
 - d. Standardmäßig ist das Kontrollkästchen **Neue DBID erstellen** aktiviert, um eine eindeutige Nummer (DBID) für die geklonte Datenbank zu generieren, die sie von der Quelldatenbank unterscheidet.

 Deaktivieren Sie das Kontrollkästchen, wenn Sie der geklonten Datenbank die DBID der Quelldatenbank zuweisen möchten. Wenn Sie in diesem Szenario die geklonte Datenbank beim externen RMAN-Katalog registrieren möchten, in dem die Quelldatenbank bereits registriert ist, schlägt der Vorgang fehl.
 - e. Aktivieren Sie das Kontrollkästchen **Temporäre Datei für temporären Tablespace erstellen**, wenn Sie eine temporäre Datei für den standardmäßigen temporären Tablespace der geklonten Datenbank erstellen möchten.
 - f. Fügen Sie unter **Geben Sie SQL-Einträge ein, die beim Erstellen des Klons angewendet werden sollen** die SQL-Einträge hinzu, die beim Erstellen des Klons angewendet werden sollen.
 - g. Geben Sie unter **Geben Sie die nach dem Klonvorgang auszuführenden Skripts ein** den Pfad und die Argumente des Postskripts an, das Sie nach dem Klonvorgang ausführen möchten.
10. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.
11. Überprüfen Sie die Zusammenfassung und wählen Sie dann **Fertig**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Überwachen > Jobs** auswählen.

Copyright-Informationen

Copyright © 2025 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 IRGEND EINER 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.