



# **Microsoft SQL Server Datenbanken schützen**

SnapCenter software

NetApp  
January 09, 2026

# Inhalt

- Microsoft SQL Server Datenbanken schützen ..... 1
  - Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für die SQL Server-Datenbank..... 1
  - Erstellen von Backup-Richtlinien für SQL Server-Datenbanken ..... 1
  - Erstellen von Ressourcengruppen und Anhängen von SQL-Backup-Richtlinien..... 3
  - Sichern Sie auf Azure NetApp Files laufende SQL Server Datenbanken ..... 4
  - Sichern Sie SQL Server-Ressourcengruppen ..... 5
  - Stellen Sie SQL Server Datenbanken wieder her ..... 5
  - Klonen Sie das SQL Server Datenbank-Backup ..... 7
    - Führen Sie Den Klon-Lebenszyklus Durch ..... 8

# Microsoft SQL Server Datenbanken schützen

## Fügen Sie Hosts hinzu und installieren Sie das SnapCenter Plug-in für die SQL Server-Datenbank

SnapCenter unterstützt die Datensicherung von SQL-Instanzen auf SMB-Freigaben auf Azure NetApp Files. Die Standalone- und Verfügbarkeitsgruppen-Konfigurationen werden unterstützt.

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

### Bevor Sie beginnen

- Sie müssen ein Benutzer sein, der einer Rolle zugewiesen ist, die über die Berechtigungen für die Plug-in-Installation und -Deinstallation verfügt, wie z. B. die Rolle „SnapCenter-Administrator“.
- Wenn Sie ein Plug-in auf einem Windows-Host installieren, wenn Sie keine Anmeldedaten angeben oder der Benutzer zu einem lokalen Workgroup-Benutzer gehört, müssen Sie UAC auf dem Host deaktivieren.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Hosts** aus.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Wählen Sie **Hinzufügen**.
4. Gehen Sie auf der Seite Hosts wie folgt vor:
  - a. Wählen Sie im Feld Hosttyp den Hosttyp aus.
  - b. Geben Sie im Feld Hostname den vollständig qualifizierten 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 **Plug-ins zur Installation 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 **Configure log Directory** und geben Sie auf der Seite Configure Host log Directory den SMB-Pfad des Host-Protokollverzeichnisses ein, und klicken Sie auf **Save**.
9. Klicken Sie auf **Absenden** und überwachen Sie den Installationsfortschritt.

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

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

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Klicken Sie Auf **Neu**.
4. Geben Sie auf der Seite Name den Namen und die Beschreibung der Richtlinie ein.
5. Führen Sie auf der Seite Richtlinientyp die folgenden Schritte durch:
  - a. Wählen Sie **Azure NetApp Files** als Speichertyp aus.
  - b. Wählen Sie den Sicherungstyp aus.
    - i. Wählen Sie **Full Backup and Log Backup** aus, wenn Sie Datenbankdateien und Transaktionsprotokolle sichern möchten.
    - ii. Wählen Sie **Full Backup**, wenn Sie nur die Datenbankdateien sichern möchten.
    - iii. Wählen Sie **Log Backup**, wenn Sie nur die Transaktionsprotokolle sichern möchten.
    - iv. Wählen Sie **nur Backup kopieren**, wenn Sie Ihre Ressourcen mit einer anderen Anwendung sichern möchten.
  - c. Führen Sie im Abschnitt Einstellungen für Verfügbarkeitsgruppen die folgenden Aktionen durch:
    - i. Wählen Sie auf bevorzugtem Backup-Replikat sichern, wenn Sie nur auf dem Replikat sichern möchten.
    - ii. Wählen Sie das primäre AG-Replikat oder das sekundäre AG-Replikat für das Backup aus.
    - iii. Wählen Sie die Backup-Priorität aus.
6. Führen Sie auf der Seite Snapshot und Backup die folgenden Schritte durch:
  - a. Wählen Sie die Häufigkeit der geplanten Sicherung aus.
  - b. Legen Sie die Aufbewahrungseinstellungen abhängig vom ausgewählten Sicherungstyp fest.
  - 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 Überprüfung die folgenden Schritte aus:
  - a. Wählen Sie im Abschnitt Überprüfung ausführen für folgende Backup-Pläne die Zeitplanhäufigkeit aus.
  - b. Führen Sie im Abschnitt Optionen für die Datenbankkonsistenzprüfung die folgenden Aktionen durch:
    - i. Wählen Sie **Beschränkung der Integritätsstruktur auf physische Struktur der Datenbank (PHYSICAL\_ONLY)** aus, um die Integritätsprüfung auf die physische Struktur der Datenbank zu begrenzen und um gerissene Seiten, Prüfsummenfehler und häufige Hardwarefehler zu erkennen, die die Datenbank beeinträchtigen.
    - 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)** aus, um alle gemeldeten Fehler pro Objekt anzuzeigen.
    - iv. Wählen Sie \* nicht gruppierte Indizes (NOINDEX)\* aus, wenn Sie keine nicht geclusterten Indizes überprüfen möchten.

Die SQL Server-Datenbank verwendet Microsoft SQL Server Database Consistency Checker (DBCC), um die logische und physische Integrität der Objekte in der Datenbank zu überprüfen.

- v. Wählen Sie **Schränken Sie die Prüfungen ein und erhalten Sie die Sperren anstatt eine interne Datenbank Snapshot Kopie (TABLOCK)** zu verwenden, um die Überprüfungen zu begrenzen und Sperren anstelle eines internen Datenbank-Snapshots zu erhalten.
  - c. Wählen Sie im Abschnitt **Protokollsicherung** die Option **Protokollsicherung nach Abschluss bestätigen** aus, um die Protokollsicherung nach Abschluss zu überprüfen.
  - d. Geben Sie im Abschnitt **Verification Script settings** den Pfad und die Argumente des Vorskripts bzw. Postscript ein, die vor oder nach dem Verifizierungsvorgang ausgeführt werden sollen.
8. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig stellen**.

## Erstellen von Ressourcengruppen und Anhängen von SQL-Backup-Richtlinien

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

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


### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plugin aus der Liste aus.
2. Klicken Sie auf der Seite Ressourcen auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite Name die folgenden Aktionen durch:

Für dieses Feld...	Tun Sie das...
Name	Geben Sie einen Namen für die Ressourcengruppe ein.
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.
5. Wählen Sie die Ressourcen im Abschnitt **Verfügbare Ressourcen** aus und klicken Sie dann auf den rechten Pfeil, um sie in den Abschnitt **Ausgewählte Ressourcen** zu verschieben.
6. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:
  - a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.
  - b. Klicken Sie in der Spalte Zeitpläne konfigurieren auf \* \*  für die Richtlinie, die Sie konfigurieren

möchten.

- c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy\_Policy\_Name\_ den Zeitplan, und klicken Sie dann auf **OK**.
  - d. Wählen Sie den Microsoft SQL Server Scheduler aus.
7. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
- a. Wählen Sie den Überprüfungsserver aus.
  - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und klicken Sie dann auf \*\*  .
  - c. Wählen Sie entweder **Verifizierung nach Backup ausführen** oder **geplante Verifizierung ausführen**.
  - d. Klicken Sie auf **OK**.
8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.


## Sichern Sie auf Azure NetApp Files laufende SQL Server Datenbanken

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


### Bevor Sie beginnen

Sie sollten einen Load Balancer erstellen, wenn dem Azure Windows-Failover-Cluster keine Cluster-IP zugewiesen ist oder wenn er nicht über SnapCenter erreichbar ist. Die IP des Load Balancer sollte konfiguriert und vom SnapCenter-Server aus erreichbar sein.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plugin aus der Liste aus.
2. Wählen Sie auf der Seite Ressource aus der Dropdown-Liste Ansicht die Option **Datenbank, Instanz** oder **Verfügbarkeitsgruppe** aus.
3. Wählen Sie auf der Seite Ressource **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 Dropdown-Liste aus.
  - b. Wählen Sie \*\*  in der Spalte Configure Schedules für die Richtlinie aus, für die Sie einen Zeitplan konfigurieren möchten.
  - c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy\_Policy\_Name den Zeitplan, und wählen Sie dann **OK** aus.  
  
*Policy\_Name* ist der Name der von Ihnen ausgewählten Richtlinie.
  - d. Wählen Sie **Use Microsoft SQL Server Scheduler** aus, und wählen Sie dann die Scheduler-Instanz

aus der Dropdown-Liste **Scheduler-Instanz** aus, die mit der Planungsrichtlinie verknüpft ist.

5. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
  - a. Wählen Sie den Überprüfungsserver aus.
  - b. Wählen Sie die Richtlinie aus, für die Sie Ihren Überprüfungsplan konfigurieren möchten, und klicken Sie dann auf **\*\***  .
  - c. Wählen Sie entweder **Verifizierung nach Backup ausführen** oder **geplante Verifizierung ausführen**.
  - d. Klicken Sie auf OK.
6. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
7. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
8. Wählen Sie **Jetzt sichern**.
9. Führen Sie auf der Seite Backup die folgenden Schritte aus:
  - a. Wenn der Ressource mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdown-Liste **Policy** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.
  - b. Wählen Sie **nach Sicherung prüfen**.
  - c. Wählen Sie **Backup**.
10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor > Jobs** klicken.

## Sichern Sie SQL Server-Ressourcengruppen

Sie können die Ressourcengruppen sichern, die aus mehreren Ressourcen bestehen. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plugin aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** 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 Backup die folgenden Schritte aus:
  - a. Wenn der Ressourcengruppe mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdown-Liste **Policy** die Richtlinie aus, die Sie für das Backup verwenden möchten.
  - b. Wählen Sie nach dem Backup **Verify** aus, um das On-Demand-Backup zu überprüfen.
  - c. Wählen Sie **Backup**.
5. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor > Jobs** auswählen.

## Stellen Sie SQL Server Datenbanken wieder her


Mit SnapCenter können Sie SQL Server-Datenbanken wiederherstellen. Die Wiederherstellung einer Datenbank ist ein mehrphasiger Prozess, bei dem alle Daten

und Protokollseiten aus einer bestimmten SQL-Server-Sicherung in eine bestimmte Datenbank kopiert werden.

### Bevor Sie beginnen

- Konfigurieren Sie die Zielinstanz mit einem Active Directory-Benutzer, der zur SMB Active Directory-Domäne gehört und über die Berechtigung verfügt, die Dateiberechtigungen entsprechend festzulegen.
- Konfigurieren Sie die Anmeldeinformationen auf SnapCenter Instanzebene.
- Wenn sich die SQL-Datenbank auf einer CIFS-Freigabe befindet, müssen das RunAS-Konto und das SQL-Dienstkonto (Domänenkonto) des Plug-in-Hosts Teil der Konfiguration sein. `BUILTIN\Administrators` Gruppe des CIFS-Servers in ONTAP.
- SMB-Konfigurationen unterstützen keine SQL-Authentifizierung für die Zielinstanz. Konfigurieren Sie die Zielinstanz in SnapCenter mit einem Active Directory-Benutzer, der über die erforderlichen Berechtigungen verfügt.
- Wenn es sich bei dem SnapCenter Plug-in-Dienstkonto nicht um einen Active Directory-Benutzer handelt, stellen Sie sicher, dass beim Wiederherstellen auf einem alternativen Host ein Benutzer mit vollständiger Kontrolle über die Quellvolumes verfügbar ist.

### 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 **Datenbank** oder **Ressourcengruppe** aus der Liste Ansicht aus.
3. Wählen Sie die Datenbank oder die Ressourcengruppe aus der Liste aus.
4. Wählen Sie in der Ansicht Manage Copies die Option **Backups** aus dem Speichersystem aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf das  Symbol.
6. Wählen Sie auf der Seite „Bereich wiederherstellen“ eine der folgenden Optionen aus:
  - a. Wählen Sie **Datenbank auf demselben Host wiederherstellen, auf dem die Sicherung erstellt wurde**, um die Datenbank auf demselben SQL-Server wiederherzustellen.
  - b. Wählen Sie **Datenbank auf einem alternativen Host wiederherstellen**, wenn Sie die Datenbank auf einem anderen SQL-Server auf demselben oder einem anderen Host wiederherstellen möchten, auf dem die Sicherungen erstellt werden.
7. Wählen Sie auf der Seite „Recovery Scope“ eine der folgenden Optionen aus:
  - a. Wählen Sie **Keine** aus, wenn Sie nur das vollständige Backup ohne Protokolle wiederherstellen müssen.
  - b. Wählen Sie **Alle Protokollsicherungen** Up-to-the-minute Backup Restore Operation, um alle verfügbaren Protokollsicherungen nach dem vollständigen Backup wiederherzustellen.
  - c. Wählen Sie **nach Log-Backups**, um einen Point-in-Time-Wiederherstellungsvorgang durchzuführen, der die Datenbank basierend auf Backup-Protokollen bis zum ausgewählten Datum wiederherstellt.
  - d. Wählen Sie **nach einem bestimmten Datum bis**, um Datum und Uhrzeit anzugeben, nach denen Transaktionsprotokolle nicht auf die wiederhergestellte Datenbank angewendet werden.
  - e. Wenn Sie **Alle Log-Backups, durch Log-Backups oder nach einem bestimmten Datum bis** ausgewählt haben und sich die Protokolle an einem benutzerdefinierten Speicherort befinden, wählen Sie **Benutzerdefiniertes Log-Verzeichnis verwenden** und geben Sie dann den Speicherort an.
8. Geben Sie auf der Seite Pre-Ops und Post Ops die erforderlichen Details an.



9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
11. Überwachen Sie den Wiederherstellungsprozess mithilfe der Seite **Monitor > Jobs**.

## Klonen Sie das SQL Server Datenbank-Backup

Sie können SnapCenter verwenden, um eine SQL-Datenbank mithilfe des Backups der Datenbank zu klonen. Die erstellten Klone sind Thick Clones und werden im übergeordneten Kapazitätspool erstellt.


### Über diese Aufgabe

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

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

Wenn das Dienstkonto für die SnapCenter-Plug-in-Dienste kein Active Directory-Benutzer ist, ist während des Klonens der Benutzer erforderlich, der die volle Kontrolle über die Quell-Volumes hat, damit er initiiert werden kann und den erforderlichen Vorgang ausführen kann.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Manage Copies** das Backup vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus, und wählen Sie dann \* aus  \*.
6. Geben Sie auf der Seite **Clone Options** alle erforderlichen Details an.
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 keine QOS für die geklonten Volumes angegeben wird, wird die QOS des Quell-Volume 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 **None**, wenn Sie nur die vollständige Sicherung ohne Protokolle klonen möchten.
  - b. Wählen Sie **Alle Protokollsicherungen** aus, wenn Sie alle verfügbaren Protokollsicherungen klonen möchten, die nach dem vollständigen Backup datiert wurden.
  - c. Wählen Sie **by log Backups until** aus, wenn Sie die Datenbank auf Basis der Backup-Protokolle


klonen möchten, die bis zum Backup-Protokoll mit dem ausgewählten Datum erstellt wurden.

- d. Wählen Sie **nach spezifischem Datum bis** aus, wenn Sie die Transaktionsprotokolle nicht nach dem angegebenen Datum und der angegebenen Uhrzeit anwenden möchten.
9. Geben Sie auf der Seite **Script** das Skript-Timeout, den Pfad und die Argumente des Prescript oder Postscript ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
11. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor > Jobs** auswählen.

## Führen Sie Den Klon-Lebenszyklus Durch

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 ein Backup regelmäßig klonen, können Sie mit dem Klon Applikationen entwickeln, Daten ausfüllen oder Daten wiederherstellen.

### Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** aus, und wählen Sie dann das entsprechende Plugin aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen die Option **Datenbank** oder **Ressourcengruppe** aus der Liste **Ansicht** aus.
3. Wählen Sie die Datenbank oder Ressourcengruppe aus.
4. Wählen Sie auf der Ansichtsseite **Manage Copies** das Backup vom primären Speichersystem aus.
5. Wählen Sie die Sicherung aus, und wählen Sie dann \* aus \*.
6. Geben Sie auf der Seite **Clone Options** alle erforderlichen Details an.
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 keine QOS für die geklonten Volumes angegeben wird, wird die QOS des Quell-Volume verwendet. Wenn der automatische QOS-Kapazitätspool verwendet wird, wird der angegebene QOS-Wert ignoriert.

8. Geben Sie auf der Seite **Script** das Skript-Timeout, den Pfad und die Argumente des Prescript oder Postscript ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.
9. Führen Sie auf der Seite Zeitplan eine der folgenden Aktionen durch:
  - Wählen Sie **Jetzt ausführen** aus, wenn Sie den Klon-Job sofort ausführen möchten.
  - Wählen Sie **Configure schedule** aus, wenn Sie bestimmen möchten, wie häufig der Klonvorgang stattfinden soll, wann der Klonzeitplan starten soll, an welchem Tag der Klonvorgang stattfinden soll, wann der Zeitplan abläuft und ob die Klone nach Ablauf des Zeitplans gelöscht werden müssen.
10. Wählen Sie auf der Seite **Benachrichtigung** aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.
11. Überprüfen Sie die Zusammenfassung, und wählen Sie dann **Fertig stellen**.
12. Überwachen Sie den Vorgangsfortschritt, indem Sie **Monitor > Jobs** auswählen.

## Copyright-Informationen

Copyright © 2026 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.