



# **Sichern von Exchange-Ressourcen**

## SnapCenter software

NetApp  
November 06, 2025

# Inhalt

Sichern von Exchange-Ressourcen .....	1
Sicherungsworkflow .....	1
Exchange-Datenbank und Backup-Verifizierung .....	1
Ermitteln, ob Exchange-Ressourcen für die Sicherung verfügbar sind .....	2
Erstellen von Sicherungsrichtlinien für Exchange Server-Datenbanken .....	3
Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Exchange-Server hinzu .....	11
Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell- Cmdlets für Exchange Server .....	14
Sichern Sie Exchange-Datenbanken .....	15
Sichern von Exchange-Ressourcengruppen .....	21
Überwachen von Sicherungsvorgängen .....	22
Überwachen von Vorgängen im Aktivitätsbereich .....	23
Abbrechen von Sicherungsvorgängen für die Exchange-Datenbank .....	23
Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“ .....	24

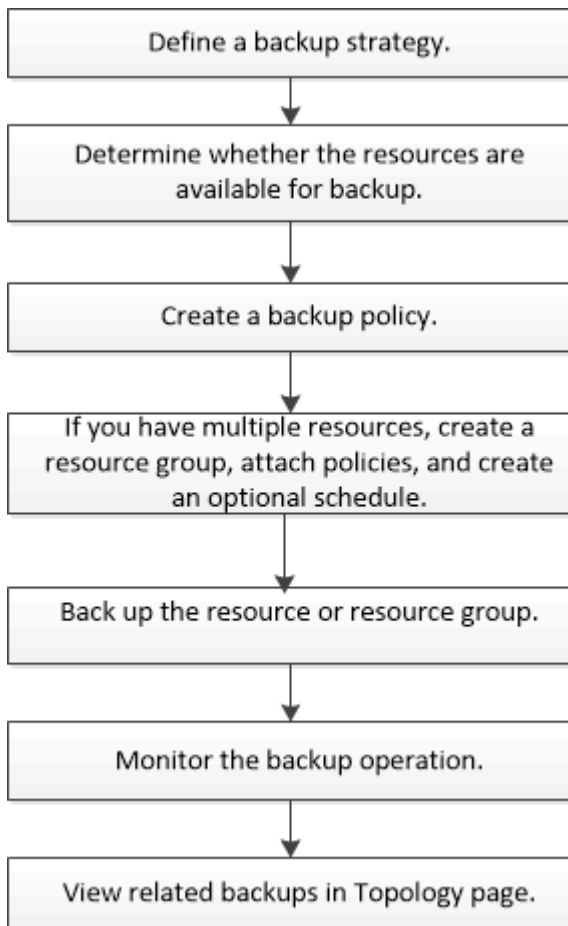
# Sichern von Exchange-Ressourcen

## Sicherungsworkflow

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

Sie können mehrere Sicherungen so planen, dass sie gleichzeitig auf mehreren Servern ausgeführt werden. Sicherungs- und Wiederherstellungsvorgänge können nicht gleichzeitig auf derselben Ressource ausgeführt werden. Aktive und passive Sicherungskopien auf demselben Volume werden nicht unterstützt.

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



## Exchange-Datenbank und Backup-Verifizierung

Das SnapCenter -Plug-in für Microsoft Exchange Server bietet keine Sicherungsüberprüfung. Sie können jedoch das mit Exchange bereitgestellte Tool „Eseutil“ verwenden, um Exchange-Datenbanken und -Sicherungen zu überprüfen.

Das Microsoft Exchange Eseutil-Tool ist ein Befehlszeilenprogramm, das in Ihrem Exchange-Server enthalten ist. Mit dem Dienstprogramm können Sie Konsistenzprüfungen durchführen, um die Integrität von Exchange-Datenbanken und -Sicherungen zu überprüfen.

**Best Practice:** Es ist nicht notwendig, Konsistenzprüfungen für Datenbanken durchzuführen, die Teil einer Database Availability Group (DAG)-Konfiguration mit mindestens zwei Replikaten sind.

Weitere Informationen finden Sie unter ["Microsoft Exchange Server-Dokumentation"](#).

## Ermitteln, ob Exchange-Ressourcen für die Sicherung verfügbar sind

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

### Bevor Sie beginnen

- Sie müssen bereits Aufgaben wie die Installation von SnapCenter Server, das Hinzufügen von Hosts, das Erstellen von Speichersystemverbindungen, das Hinzufügen von Anmeldeinformationen und die Installation des Plug-ins für Exchange abgeschlossen haben.
- Um die Funktionen der Single Mailbox Recovery-Software nutzen zu können, müssen Sie Ihre aktive Datenbank auf dem Exchange-Server lokalisiert haben, auf dem die Single Mailbox Recovery-Software installiert ist.
- Wenn sich Datenbanken auf VMware RDM LUNs befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren. Der ["SnapCenter Plug-in for VMware vSphere Dokumentation"](#) hat weitere Informationen.

### Informationen zu diesem Vorgang

- Sie können keine Datenbanken sichern, wenn die Option **Gesamtstatus** auf der Seite „Details“ auf „Nicht für Sicherung verfügbar“ eingestellt ist. Die Option **Gesamtstatus** wird auf „Nicht für Sicherung verfügbar“ gesetzt, wenn eine der folgenden Bedingungen zutrifft:
  - Datenbanken befinden sich nicht auf einer NetApp LUN.
  - Die Datenbanken befinden sich nicht im Normalzustand.

Datenbanken befinden sich nicht im Normalzustand, wenn sie sich im Status „Mounten“, „Unmounten“, „Reseed“ oder „Wiederherstellung ausstehend“ befinden.

- Wenn Sie über eine Database Availability Group (DAG) verfügen, können Sie alle Datenbanken in der Gruppe sichern, indem Sie den Sicherungsauftrag von der DAG aus ausführen.

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann **Microsoft Exchange Server** aus der Plug-In-Dropdownliste in der oberen linken Ecke der Ressourcenseite aus.
2. Wählen Sie auf der Seite „Ressourcen“ aus der Dropdownliste „Anzeigen“ die Option „**Datenbank**“, „**Datenbankverfügbarkeitsgruppe**“ oder „**Ressourcengruppe**“ aus.

Alle Datenbanken und DAGs werden mit ihren DAG- oder Hostnamen im FQDN-Format angezeigt, sodass Sie zwischen mehreren Datenbanken unterscheiden können.

Klicken  und wählen Sie den Hostnamen und den Exchange-Server aus, um die Ressourcen zu filtern.

Sie können dann auf  , um den Filterbereich zu schließen.

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

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



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

Die Ressourcen werden zusammen mit Informationen wie Ressourcenname, Name der Datenbankverfügbarkeitsgruppe, Server, auf dem die Datenbank derzeit aktiv ist, Server mit Kopien, Zeitpunkt der letzten Sicherung und Gesamtstatus angezeigt.

- Wenn sich die Datenbank auf einem Nicht- NetApp -Speicher befindet, wird in der Spalte „Gesamtstatus“ „Nicht für Sicherung verfügbar“ angezeigt.

Wenn sich in einer DAG die aktive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet und sich mindestens eine passive Datenbankkopie auf einem NetApp -Speicher befindet, wird in der Spalte **Gesamtstatus** „Nicht geschützt“ angezeigt.

Sie können keine Datenschutzvorgänge für eine Datenbank durchführen, die sich auf einem anderen Speichertyp als NetApp befindet.

- Wenn sich die Datenbank auf einem NetApp -Speicher befindet und nicht geschützt ist, wird in der Spalte **Gesamtstatus** „Nicht geschützt“ angezeigt.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist, zeigt die Benutzeroberfläche in der Spalte **Gesamtstatus** die Meldung „Sicherung nicht ausgeführt“ an.
- Wenn sich die Datenbank auf einem NetApp Speichersystem befindet und geschützt ist und die Sicherung für die Datenbank ausgelöst wird, zeigt die Benutzeroberfläche in der Spalte **Gesamtstatus** die Meldung „Sicherung erfolgreich“ an.

## Erstellen von Sicherungsrichtlinien für Exchange Server-Datenbanken

Sie können eine Sicherungsrichtlinie für die Exchange-Ressourcen oder für die Ressourcengruppen erstellen, bevor Sie SnapCenter zum Sichern von Microsoft Exchange Server-Ressourcen verwenden, oder Sie können eine Sicherungsrichtlinie erstellen, wenn Sie eine Ressourcengruppe erstellen oder eine einzelne Ressource sichern.

### Bevor Sie beginnen

- Sie müssen Ihre Datenschutzstrategie definiert haben.

Einzelheiten finden Sie in den Informationen zum Definieren einer Datenschutzstrategie für Exchange-Datenbanken.

- Sie müssen sich auf den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Identifizieren von Ressourcen und das Erstellen von Speichersystemverbindungen abgeschlossen haben.

- Sie müssen die Exchange Server-Ressourcen aktualisiert (erkannt) haben.
- Wenn Sie Snapshots auf einen Spiegel oder Tresor replizieren, muss der SnapCenter Administrator Ihnen die virtuellen Speichermaschinen (SVMs) sowohl für die Quell- als auch für die Zielvolumes zugewiesen haben.
- Wenn Sie die PowerShell-Skripte in Prescripts und Postscripts ausführen möchten, sollten Sie den Wert des `usePowershellProcessforScripts` Parameter auf `true` im `web.config` Datei.

Der Standardwert ist „false“.

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

### Informationen zu diesem Vorgang

- Eine Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten und aufbewahren und wie häufig die Ressource oder Ressourcengruppe gesichert wird. Darüber hinaus können Sie Skripteeinstellungen festlegen. Das Angeben von Optionen in einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.
- Die vollständige Aufbewahrung von Backups ist an eine bestimmte Richtlinie gebunden. Eine Datenbank oder Ressource, die Richtlinie A mit einer vollständigen Sicherungsaufbewahrung von 4 verwendet, behält 4 vollständige Sicherungen bei und hat keine Auswirkungen auf Richtlinie B für dieselbe Datenbank oder Ressource, die möglicherweise eine Aufbewahrung von 3 hat, um 3 vollständige Sicherungen beizubehalten.
- Die Aufbewahrung von Protokollsicherungen ist richtlinienübergreifend wirksam und gilt für alle Protokollsicherungen einer Datenbank oder Ressource. Wenn also eine vollständige Sicherung mit Richtlinie B durchgeführt wird, wirkt sich die Protokollaufbewahrungseinstellung auf Protokollsicherungen aus, die mit Richtlinie A auf derselben Datenbank oder Ressource erstellt wurden. Ebenso wirkt sich die Protokollaufbewahrungseinstellung für Richtlinie A auf Protokollsicherungen aus, die von Richtlinie B in derselben Datenbank erstellt wurden.
- Der `SCRIPTS_PATH` wird mithilfe des Schlüssels „PredefinedWindowsScriptsDirectory“ definiert, der sich in der Datei „SMCoreServiceHost.exe.Config“ des Plug-In-Hosts befindet.

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

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

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

**Best Practice:** Am besten konfigurieren Sie die sekundäre Aufbewahrungsrichtlinie basierend auf der Anzahl der vollständigen und Protokollsicherungen, die Sie insgesamt aufbewahren möchten. Wenn Sie sekundäre Aufbewahrungsrichtlinien konfigurieren, bedenken Sie, dass bei Datenbanken und Protokollen, die sich auf unterschiedlichen Volumes befinden, jede Sicherung drei Snapshots haben kann, und dass bei Datenbanken und Protokollen, die sich auf demselben Volume befinden, jede Sicherung zwei Snapshots haben kann.


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

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

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

## 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 die Details ein.
5. Führen Sie auf der Seite „Sicherungstyp und Replikation“ die folgenden Schritte aus:
  - a. Wählen Sie den Sicherungstyp:

Wenn Sie wollen...	Machen Sie Folgendes...
Sichern Sie die Datenbankdateien und die erforderlichen Transaktionsprotokolle	<p>Wählen Sie <b>Vollständige Sicherung und Protokollsicherung</b>.</p> <p>Datenbanken werden mit Protokollkürzung gesichert und alle Protokolle werden gesichert, einschließlich der gekürzten Protokolle.</p> <div>  <p>Dies ist der empfohlene Sicherungstyp.</p> </div>
Sichern Sie die Datenbankdateien und die nicht festgeschriebenen Transaktionsprotokolle	<p>Wählen Sie <b>Vollständige Sicherung</b>.</p> <p>Datenbanken werden mit Protokollkürzung gesichert, gekürzte Protokolle werden nicht gesichert.</p>
Sichern Sie alle Transaktionsprotokolle	<p>Wählen Sie <b>Protokollsicherung</b>.</p> <p>Alle Transaktionsprotokolle auf dem aktiven Dateisystem werden gesichert und es erfolgt keine Protokollkürzung.</p> <p>Auf derselben Festplatte wie das Live-Protokoll wird ein <i>scebackupinfo</i>-Verzeichnis erstellt. Dieses Verzeichnis enthält den Zeiger auf die inkrementellen Änderungen für die Exchange-Datenbank und ist nicht gleichbedeutend mit den vollständigen Protokolldateien.</p>

Wenn Sie wollen...	Machen Sie Folgendes...
Sichern Sie alle Datenbankdateien und Transaktionsprotokolle, ohne die Transaktionsprotokolldateien zu kürzen	<p>Wählen Sie <b>Backup kopieren</b>.</p> <p>Alle Datenbanken und alle Protokolle werden gesichert und es erfolgt keine Protokollkürzung. Normalerweise verwenden Sie diesen Sicherungstyp zum erneuten Seeding eines Replikats oder zum Testen oder Diagnostizieren eines Problems.</p>



Sie sollten den für Protokollsicherungen erforderlichen Speicherplatz auf Grundlage der vollständigen Sicherungsaufbewahrung und nicht auf Grundlage der minutengenauen (UTM) Aufbewahrung definieren.



Erstellen Sie beim Umgang mit Exchange-Volumes (LUNs) separate Tresorrichtlinien für Protokolle und Datenbanken und legen Sie die Aufbewahrungsdauer (Keep) für die Protokollrichtlinie für jedes Label auf die doppelte Zahl fest wie für die Datenbankrichtlinie, wobei Sie dieselben Labels verwenden. Weitere Informationen finden Sie unter ["SnapCenter für Exchange-Backups speichert nur die Hälfte der Snapshots auf dem Vault-Zielprotokollvolume"](#)

b. Wählen Sie im Abschnitt „Einstellungen der Datenbankverfügbarkeitsgruppe“ eine Aktion aus:

Für dieses Feld...	Machen Sie Folgendes...
Sichern aktiver Kopien	<p>Wählen Sie diese Option, um nur die aktiven Kopien der ausgewählten Datenbank zu sichern.</p> <p>Bei Datenbankverfügbarkeitsgruppen (DAGs) sichert diese Option nur aktive Kopien aller Datenbanken in der DAG.</p> <p>Passive Kopien werden nicht gesichert.</p>
Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen	<p>Wählen Sie diese Option, um alle Kopien der Datenbanken auf den ausgewählten Servern (aktiv und passiv) zu sichern.</p> <p>Bei DAGs sichert diese Option sowohl aktive als auch passive Kopien aller Datenbanken auf den ausgewählten Servern.</p>



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

c. Wählen Sie im Abschnitt „Häufigkeit planen“ einen oder mehrere der Häufigkeitstypen aus: **Auf Anfrage, Stündlich, Täglich, Wöchentlich** und **Monatlich**.



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




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

a. Wählen Sie die Richtlinienbezeichnung aus.



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

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

Für dieses Feld...	Machen Sie Folgendes...
Aktualisieren Sie SnapMirror nach dem Erstellen eines lokalen Snapshots	<p>Wählen Sie diese Option, um Spiegelkopien von Sicherungssätzen auf einem anderen Volume (SnapMirror) aufzubewahren.</p> <p>Während der sekundären Replikation lädt die Ablaufzeit des SnapLock die Ablaufzeit des primären SnapLock .</p> <p>Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.</p> <div>  <p>Die Nur-Primär-Richtlinie kann nicht verwendet werden, wenn SnapMirror Active Sync für Exchange ONTAP -Volumes eingerichtet ist. SnapCenter lässt dies nicht zu. Sie sollten die Option „Spiegeln“ aktivieren.</p> </div> <p>Durch Klicken auf die Schaltfläche <b>Aktualisieren</b> auf der Seite „Topologie“ werden die Ablaufzeiten des sekundären und primären SnapLock aktualisiert, die von ONTAP abgerufen werden.</p> <p>Sehen <a href="#">"Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“"</a> .</p>
Aktualisieren Sie SnapVault nach dem Erstellen eines lokalen Snapshots	Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen.

Für dieses Feld...	Machen Sie Folgendes...
Fehleranzahl der Wiederholungsversuche	Geben Sie die Anzahl der Replikationsversuche ein, die durchgeführt werden sollen, bevor der Prozess angehalten wird.



Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Speicher konfigurieren, um zu vermeiden, dass das maximale Limit für Snapshots auf dem sekundären Speicher erreicht wird.

#### 6. Konfigurieren Sie auf der Seite „Aufbewahrung“ die Aufbewahrungseinstellungen.

Die angezeigten Optionen hängen vom Sicherungstyp und der Häufigkeit ab, die Sie zuvor ausgewählt haben.



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



Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault -Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 setzen, schlägt der Aufbewahrungsvorgang möglicherweise fehl, da der erste Snapshot der Referenz-Snapshot für die SnapVault -Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.

- a. Wählen Sie im Abschnitt „Aufbewahrungseinstellungen für Protokollsicherungen“ eine der folgenden Optionen aus:

Wenn Sie wollen...	Machen Sie Folgendes...
<p>Behalten Sie nur eine bestimmte Anzahl von Protokollsicherungen</p>	<p>Wählen Sie <b>Anzahl der vollständigen Sicherungen, für die Protokolle aufbewahrt werden</b> und geben Sie die Anzahl der vollständigen Sicherungen an, für die Sie eine minutengenaue Wiederherstellung wünschen.</p> <p>Die minutengenaue Aufbewahrung (UTM) gilt für Protokollsicherungen, die über eine vollständige oder Protokollsicherung erstellt wurden. Wenn beispielsweise die UTM-Aufbewahrungseinstellungen so konfiguriert sind, dass die Protokollsicherungen der letzten 5 vollständigen Sicherungen aufbewahrt werden, werden die Protokollsicherungen der letzten 5 vollständigen Sicherungen aufbewahrt.</p> <p>Die im Rahmen von Voll- und Log-Backups erstellten Log-Ordner werden im Rahmen von UTM automatisch gelöscht. Sie können die Protokollordner nicht manuell löschen. Wenn beispielsweise die Aufbewahrungseinstellung für die vollständige oder vollständige und Protokollsicherung auf 1 Monat und die UTM-Aufbewahrung auf 10 Tage eingestellt ist, wird der im Rahmen dieser Sicherungen erstellte Protokollordner gemäß UTM gelöscht. Infolgedessen sind nur 10-Tage-Protokollordner vorhanden und alle anderen Sicherungen sind für die Wiederherstellung zu einem bestimmten Zeitpunkt markiert.</p> <p>Sie können den UTM-Aufbewahrungswert auf 0 setzen, wenn Sie keine minutengenaue Wiederherstellung durchführen möchten. Dadurch wird die Wiederherstellung zu einem bestimmten Zeitpunkt ermöglicht.</p> <p><b>Best Practice:</b> Es ist am besten, wenn die Einstellung der Einstellung für „Gesamtanzahl der Snapshots (vollständige Sicherungen)“ im Abschnitt „Einstellungen für die Aufbewahrung vollständiger Sicherungen“ entspricht. Dadurch wird sichergestellt, dass die Protokolldateien für jede vollständige Sicherung erhalten bleiben.</p>

Wenn Sie wollen...	Machen Sie Folgendes...
Bewahren Sie die Sicherungskopien für eine bestimmte Anzahl von Tagen auf	<p>Wählen Sie die Option <b>Protokollsicherungen bis zuletzt aufbewahren</b> und geben Sie die Anzahl der Tage an, für die die Protokollsicherungskopien aufbewahrt werden sollen.</p> <p>Die Protokollsicherungen werden bis zur Anzahl der Tage der vollständigen Sicherungen aufbewahrt.</p>
Snapshot-Sperrzeitraum	<p>Wählen Sie <b>Sperrzeitraum für Snapshot-Kopie</b> und wählen Sie Tage, Monate oder Jahre aus.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p>

Wenn Sie als Sicherungstyp **Protokollsicherung** ausgewählt haben, werden Protokollsicherungen als Teil der aktuellen Aufbewahrungseinstellungen für vollständige Sicherungen aufbewahrt.

- b. Wählen Sie im Abschnitt „Aufbewahrungseinstellungen für vollständige Sicherungen“ eine der folgenden Optionen für On-Demand-Sicherungen und dann eine für vollständige Sicherungen aus:

Für dieses Feld...	Machen Sie Folgendes...
Behalten Sie nur eine bestimmte Anzahl von Snapshots	<p>Wenn Sie die Anzahl der aufzubewahrenden Vollsicherungen angeben möchten, wählen Sie die Option <b>Gesamtzahl der aufzubewahrenden Snapshot-Kopien</b> und geben Sie die Anzahl der aufzubewahrenden Snapshots (Vollsicherungen) an.</p> <p>Wenn die Anzahl der vollständigen Sicherungen die angegebene Zahl überschreitet, werden die vollständigen Sicherungen, die die angegebene Zahl überschreiten, gelöscht, wobei die ältesten Kopien zuerst gelöscht werden.</p>
Vollständige Backups für eine bestimmte Anzahl von Tagen aufbewahren	Wählen Sie die Option <b>Snapshot-Kopien aufbewahren für</b> und geben Sie die Anzahl der Tage an, die Snapshots (vollständige Backups) aufbewahrt werden sollen.
Sperrzeitraum für primäre Snapshots	<p>Wählen Sie <b>Sperrzeitraum für primäre Snapshot-Kopie</b> und wählen Sie Tage, Monate oder Jahre aus.</p> <p>Die Aufbewahrungsdauer von SnapLock sollte weniger als 100 Jahre betragen.</p>

Für dieses Feld...	Machen Sie Folgendes...
Sperrzeitraum für sekundäre Snapshots	Wählen Sie <b>Sperrzeitraum für sekundäre Snapshot-Kopie</b> und wählen Sie Tage, Monate oder Jahre aus.

Wenn Sie auf einem Host in einer DAG-Konfiguration eine Datenbank mit nur Protokollsicherungen und ohne vollständige Sicherungen haben, werden die Protokollsicherungen auf folgende Weise aufbewahrt:

- Standardmäßig sucht SnapCenter die älteste vollständige Sicherung für diese Datenbank auf allen anderen Hosts im DAG und löscht alle Protokollsicherungen auf diesem Host, die vor der vollständigen Sicherung erstellt wurden.
- Sie können das oben genannte Standardaufbewahrungsverhalten für eine Datenbank auf einem Host in einem DAG mit ausschließlich Protokollsicherungen überschreiben, indem Sie den Schlüssel **MaxLogBackupOnlyCountWithoutFullBackup** in der Datei *C:\Program Files\NetApp\SnapCenter\WebApp\web.config* hinzufügen.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

Im Beispiel bedeutet der Wert 10, dass Sie bis zu 10 Protokollsicherungen auf dem Host aufbewahren.

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

- Zu den Prescript-Sicherungsargumenten gehören „\$Database“ und „\$ServerInstance“.
- Zu den Postscript-Sicherungsargumenten gehören „\$Database“, „\$ServerInstance“, „\$BackupName“, „\$LogDirectory“ und „\$LogSnapshot“.

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



Der Prescripts- oder Postscripts-Pfad sollte keine Laufwerke oder Freigaben enthalten. Der Pfad sollte relativ zum SCRIPTS\_PATH sein.

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

## Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Exchange-Server hinzu

Für jeden Datenschutzjob ist eine Ressourcengruppe erforderlich. Sie müssen der Ressourcengruppe außerdem eine oder mehrere Richtlinien zuordnen, um die Art des Datenschutzauftrags, den Sie ausführen möchten, und den Schutzzeitplan zu definieren.

### Informationen zu diesem Vorgang

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

Bei Bedarf können Sie diesen Pfad ändern und den SMcore-Dienst neu starten. Aus Sicherheitsgründen wird empfohlen, den Standardpfad zu verwenden.

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

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

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


## Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Microsoft Exchange Server-Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ in der Liste „Ansicht“ die Option „Datenbank“ aus.



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

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

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

Für dieses Feld...	Machen Sie Folgendes...
Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden	<p>Optional: Geben Sie einen benutzerdefinierten Snapshot-Namen und ein benutzerdefiniertes Format ein.</p> <p>Beispiel:  <code>customtext_resourcegroup_policy_hostname</code> oder <code>resourcegroup_hostname</code>. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.</p>

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

- a. Wählen Sie den Ressourcentyp und die Datenbankverfügbarkeitsgruppe aus Dropdown-Listen aus, um die Liste der verfügbaren Ressourcen zu filtern.



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

In den Abschnitten „Verfügbare Ressourcen“ und „Ausgewählte Ressourcen“ wird der Datenbankname mit dem FQDN des Hosts angezeigt. Dieser FQDN zeigt nur an, dass die Datenbank auf diesem bestimmten Host aktiv ist und möglicherweise keine Sicherung auf diesem Host durchführt. Sie sollten aus der Serverauswahloption einen oder mehrere Sicherungsserver auswählen, auf denen Sie eine Sicherung durchführen möchten, falls Sie in der Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben.

- b. Geben Sie den Namen der Ressource in das Suchtextfeld ein oder scrollen Sie, um eine Ressource zu finden.
- c. Um Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben, führen Sie einen der folgenden Schritte aus:
  - Wählen Sie **Alle Ressourcen auf demselben Speichervolume automatisch auswählen**, um alle Ressourcen auf demselben Volume in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.
  - Wählen Sie die Ressourcen aus dem Abschnitt „Verfügbare Ressourcen“ aus und klicken Sie dann auf den Rechtspfeil, um sie in den Abschnitt „Ausgewählte Ressourcen“ zu verschieben.

Ressourcengruppen von SnapCenter für Microsoft Exchange Server können nicht mehr als 30 Datenbanken pro Snapshot haben. Wenn in einer Ressourcengruppe mehr als 30 Datenbanken vorhanden sind, wird für die zusätzlichen Datenbanken ein zweiter Snapshot erstellt. Daher werden unter dem Hauptsicherungsjob zwei Unterjobs erstellt. Bei Sicherungen mit sekundärer Replikation kann es während der Ausführung einer SnapMirror oder SnapVault -Aktualisierung zu Szenarien kommen, in denen sich die Aktualisierung für beide Unteraufträge überschneidet. Der Hauptsicherungsauftrag wird für immer weiter ausgeführt, auch wenn die Protokolle anzeigen, dass der Auftrag abgeschlossen ist.

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

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




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



Wenn eine Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** enthält, wird eine Serverauswahloption angezeigt, um einen oder mehrere Server auszuwählen. Die Serverauswahloption listet nur den Server auf, auf dem sich die ausgewählte Datenbank im NetApp -Speicher befindet.

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

- b. Klicken Sie im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ auf  \* **in der Spalte \*Zeitpläne konfigurieren** für die Richtlinie, für die Sie den Zeitplan konfigurieren möchten.
- c. Konfigurieren Sie im Dialogfeld „Zeitpläne für Richtlinie *Richtliniennamen* hinzufügen“ den Zeitplan, indem Sie das Startdatum, das Ablaufdatum und die Häufigkeit angeben, und klicken Sie dann auf **OK**.

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

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

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. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

Für die E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder über die GUI oder den PowerShell-Befehl angeben haben. `Set-SmSmtServer` .

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

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

## Erstellen einer Speichersystemverbindung und einer Anmeldeinformation mithilfe von PowerShell-Cmdlets für Exchange Server

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

### Bevor Sie beginnen

- Sie sollten die PowerShell-Umgebung für die Ausführung der PowerShell-Cmdlets vorbereitet haben.
- Sie sollten über die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ verfügen, um Speicherverbindungen zu erstellen.

- Sie sollten sicherstellen, dass die Plug-In-Installationen nicht im Gange sind.

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

- Speichersystemnamen sollten eindeutig sein.

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

## Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mithilfe des `Open-SmConnection` Cmdlet.

Dieses Beispiel öffnet eine PowerShell-Sitzung:

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

2. Erstellen Sie eine neue Verbindung zum Speichersystem, indem Sie das `Add-SmStorageConnection` Cmdlet.

In diesem Beispiel wird eine neue Speichersystemverbindung erstellt:

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

3. Erstellen Sie ein neues Ausführen-als-Konto mithilfe des `Add-Credential` Cmdlet.

In diesem Beispiel wird ein neues „Ausführen als“-Konto mit dem Namen „ExchangeAdmin“ und Windows-Anmeldeinformationen erstellt:

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

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von `Get-Help command_name`. Alternativ können Sie auch auf die [Referenzhandbuch für SnapCenter -Software-Cmdlets](#) .

## Sichern Sie Exchange-Datenbanken

Wenn eine Datenbank nicht Teil einer Ressourcengruppe ist, können Sie die Datenbank oder die Datenbankverfügbarkeitsgruppe auf der Seite „Ressourcen“ sichern.

**Bevor Sie beginnen**

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Sie müssen das vom Sicherungsvorgang verwendete Aggregat der von der Datenbank verwendeten SVM zugewiesen haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Wenn Sie eine Sicherung einer Datenbank oder einer Datenbankverfügbarkeitsgruppe durchführen möchten, die über eine aktive/passive Datenbankkopie auf einem NetApp und Nicht- NetApp -Speicher verfügt, und Sie in der Richtlinie die Option **Aktive Kopien sichern** oder **Kopien auf Servern sichern, die während der Erstellungszeit des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben, wechseln die Sicherungsaufträge in den Warnzustand. Die Sicherung ist für die aktive/passive Datenbankkopie auf NetApp -Speicher erfolgreich, für die aktive/passive Datenbankkopie auf Nicht-NetApp -Speicher schlägt die Sicherung fehl.

**Best Practice:** Führen Sie nicht gleichzeitig Backups von aktiven und passiven Datenbanken durch. Es kann zu einem Race Condition kommen und eine der Sicherungen kann fehlschlagen.

## SnapCenter -Benutzeroberfläche



### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das **Microsoft Exchange Server-Plug-In** aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ entweder „Datenbank“ oder „Datenbankverfügbarkeitsgruppe“ aus der Liste „Anzeigen“ aus.

Auf der Seite „Ressourcen“ wird  Das Symbol zeigt an, dass sich die Datenbank auf einem Nicht-NetApp -Speicher befindet.



Wenn sich in einer DAG eine aktive Datenbankkopie auf einem Nicht- NetApp -Speicher befindet und mindestens eine passive Datenbankkopie auf einem NetApp -Speicher liegt, können Sie die Datenbank schützen.

Klicken Sie auf  \* und wählen Sie dann den Hostnamen und den Datenbanktyp aus, um die Ressourcen zu filtern. Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

- Wenn Sie eine Datenbank sichern möchten, klicken Sie auf den Datenbanknamen.
    - i. Wenn die Topologieansicht angezeigt wird, klicken Sie auf **Schützen**.
    - ii. Wenn der Assistent „Datenbank – Ressource schützen“ angezeigt wird, fahren Sie mit Schritt 3 fort.
  - Wenn Sie eine Datenbankverfügbarkeitsgruppe sichern möchten, klicken Sie auf den Namen der Datenbankverfügbarkeitsgruppe.
3. Wenn Sie einen benutzerdefinierten Snapshot-Namen angeben möchten, aktivieren Sie auf der Seite „Ressourcen“ das Kontrollkästchen **Benutzerdefiniertes Namensformat für Snapshot-Kopie verwenden** und geben Sie dann ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

Beispiel: *customtext\_policy\_hostname* oder *resource\_hostname*. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

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

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



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



Wenn eine Richtlinie die Option **Sicherungskopien auf Servern, die bei der Erstellung des Sicherungsauftrags ausgewählt werden sollen** enthält, wird eine Serverauswahloption angezeigt, um einen oder mehrere Server auszuwählen. Die Serverauswahloption listet nur den Server auf, auf dem sich die ausgewählte Datenbank auf einem NetApp -Speicher befindet.

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

- b.

Klicken Sie auf \*  \* in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen

Zeitplan konfigurieren möchten.

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

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

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

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

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



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

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

Die Seite „Datenbanktopologie“ wird angezeigt.

7. Klicken Sie auf **Jetzt sichern**.

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

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

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

- b. Klicken Sie auf **Sichern**.

9. Überwachen Sie den Fortschritt der Sicherung, indem Sie im Aktivitätsbereich unten auf der Seite auf den Auftrag doppelklicken, um die Seite mit den Auftragsdetails anzuzeigen.

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

Weitere Informationen finden Sie unter: ["SnapMirror oder SnapVault -Beziehung kann nach MetroCluster Failover nicht erkannt werden"](#)

- Wenn Sie Anwendungsdaten auf VMDKs sichern und die Java-Heap-Größe für das SnapCenter Plug-in for VMware vSphere nicht groß genug ist, schlägt die Sicherung möglicherweise fehl.

Um die Java-Heap-Größe zu erhöhen, suchen Sie die Skriptdatei `/opt/netapp/init_scripts/scvservice`. In diesem Skript startet der Befehl `do_start method` den SnapCenter VMware-Plug-in-Dienst. Aktualisieren Sie diesen Befehl wie folgt: `Java -jar -Xmx8192M -Xms4096M`

## PowerShell-Cmdlets

### Schritte

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

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

Die Eingabeaufforderung für Benutzername und Kennwort wird angezeigt.

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

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit einem vollständigen Backup und einem Protokoll-Backup vom Exchange-Sicherungstyp erstellt:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies
```

In diesem Beispiel wird eine neue Sicherungsrichtlinie mit einem stündlichen vollständigen Backup und einem Protokoll-Backup vom Exchange-Sicherungstyp erstellt:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly  
-RetentionSettings  
&{'BackupType'='DATA'; 'ScheduleType'='Hourly'; 'RetentionCount'='10'}
```

In diesem Beispiel wird eine neue Sicherungsrichtlinie erstellt, um nur Exchange-Protokolle zu sichern:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup  
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

## 3. Ermitteln Sie Hostressourcen mithilfe des Cmdlets „Get-SmResources“.

Dieses Beispiel ermittelt die Ressourcen für das Microsoft Exchange Server-Plug-In auf dem angegebenen Host:

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

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

In diesem Beispiel wird eine neue Exchange Server-Datenbanksicherungsressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

In diesem Beispiel wird eine neue Backup-Ressourcengruppe für die Exchange Database Availability Group (DAG) mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database Availability Group";"Names"="DAGSCE0102"}
```

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

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

In diesem Beispiel wird eine neue Sicherung auf einem sekundären Speicher erstellt:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

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

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

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

In diesem Beispiel wird ein Auftragszusammenfassungsbericht für eine bestimmte Auftrags-ID angezeigt:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie

durch Ausführen von *Get-Help command\_name*. Alternativ siehe ["Referenzhandbuch für SnapCenter -Software-Cmdlets"](#).

## Sichern von Exchange-Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host oder Exchange DAG und die Ressourcengruppe kann entweder einen ganzen DAG oder einzelne Datenbanken umfassen. Sie können die Ressourcengruppen von der Seite „Ressourcen“ aus sichern.

### Bevor Sie beginnen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Sie müssen das vom Sicherungsvorgang verwendete Aggregat der von der Datenbank verwendeten Storage Virtual Machine (SVM) zugewiesen haben.
- Wenn Sie eine Ressource sichern möchten, die über eine SnapMirror -Beziehung mit einem sekundären Speicher verfügt, sollte die dem Speicherbenutzer zugewiesene Rolle das Privileg „snapmirror all“ enthalten. Wenn Sie jedoch die Rolle „vsadmin“ verwenden, ist das Privileg „snapmirror all“ nicht erforderlich.
- Wenn eine Ressourcengruppe über mehrere Datenbanken von verschiedenen Hosts verfügt, kann es sein, dass der Sicherungsvorgang auf einigen Hosts aufgrund von Netzwerkproblemen verspätet beginnt. Sie sollten den Wert von konfigurieren `MaxRetryForUninitializedHosts` in `web.config` mithilfe der `Set-SmConfigSettings` PowerShell-Cmdlet.
- Wenn Sie in einer Ressourcengruppe eine Datenbank oder Datenbankverfügbarkeitsgruppe einschließen, die über eine aktive/passive Datenbankkopie auf einem NetApp und Nicht- NetApp -Speicher verfügt, und Sie in der Richtlinie die Option **Aktive Kopien sichern** oder **Kopien auf Servern sichern, die während der Erstellungszeit des Sicherungsauftrags ausgewählt werden sollen** ausgewählt haben, wechseln die Sicherungsaufträge in den Warnzustand.



Die Sicherung ist für die aktive/passive Datenbankkopie auf NetApp -Speicher erfolgreich, für die aktive/passive Datenbankkopie auf Nicht- NetApp -Speicher schlägt die Sicherung fehl.

### Informationen zu diesem Vorgang

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

### Schritte

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

Sie können die Ressourcengruppe suchen, indem Sie entweder den Namen der Ressourcengruppe in das Suchfeld eingeben oder auf \* klicken.  \* und wählen Sie dann das Tag aus. Sie können dann auf \* klicken.  \*, um den Filterbereich zu schließen.

3. Wählen Sie auf der Seite „Ressourcengruppen“ die Ressourcengruppe aus, die Sie sichern möchten, und klicken Sie dann auf **Jetzt sichern**.
4. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:

- a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdownliste **Richtlinie** die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

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

- b. Klicken Sie auf **Sichern**.







5. Überwachen Sie den Fortschritt der Sicherung, indem Sie im Aktivitätsbereich unten auf der Seite auf den Auftrag doppelklicken, um die Seite mit den Auftragsdetails anzuzeigen.

## Überwachen von Sicherungsvorgängen


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

### Informationen zu diesem Vorgang


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

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

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite „Überwachen“ auf **Jobs**.
3. Führen Sie auf der Seite „Jobs“ die folgenden Schritte aus:
  - a. Klicken  um die Liste so zu filtern, dass nur Sicherungsvorgänge aufgelistet werden.
  - b. Geben Sie das Start- und Enddatum an.
  - c. Wählen Sie aus der Dropdownliste **Typ** die Option **Backup** aus.
  - d. Wählen Sie aus der Dropdown-Liste **Status** den Sicherungsstatus aus.
  - e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.



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

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


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

## Überwachen von Vorgängen im Aktivitätsbereich

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

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

### Schritte

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

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

## Abbrechen von Sicherungsvorgängen für die Exchange-Datenbank


Sie können Sicherungsvorgänge in der Warteschlange abbrechen.

### Was Sie brauchen

- Sie müssen als SnapCenter -Administrator oder Auftragseigentümer angemeldet sein, um Vorgänge abzuberechnen.
- Sie können einen Sicherungsvorgang entweder auf der Seite **Überwachen** oder im Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die Sicherungsvorgänge über die SnapCenter -GUI, PowerShell-Cmdlets oder CLI-Befehle abbrechen.
- Die Schaltfläche **Auftrag abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie beim Erstellen einer Rolle auf der Seite „Benutzer/Gruppen“ die Option **Alle Mitglieder dieser Rolle können die Objekte anderer Mitglieder sehen und bearbeiten** ausgewählt haben, können Sie die in die Warteschlange gestellten Sicherungsvorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

### Schritte

1. Führen Sie eine der folgenden Aktionen aus:

Von der...	Aktion
Monitorseite	a. Klicken Sie im linken Navigationsbereich auf <b>Monitor &gt; Jobs</b> . b. Wählen Sie den Vorgang aus und klicken Sie dann auf <b>Auftrag abbrechen</b> .
Aktivitätsbereich	a. Klicken Sie nach dem Starten des Sicherungsvorgangs auf *  * im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen. b. Wählen Sie den Vorgang aus. c. Klicken Sie auf der Seite „Auftragsdetails“ auf <b>Auftrag abbrechen</b> .

Der Vorgang wird abgebrochen und die Ressource in den vorherigen Zustand zurückversetzt.




## Anzeigen von Exchange-Sicherungen auf der Seite „Topologie“

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

### Informationen zu diesem Vorgang

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

Sie können das folgende Symbol in der Ansicht „Kopien verwalten“ überprüfen, um festzustellen, ob die Sicherungen auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Tresorkopien).




-  zeigt die Anzahl der Sicherungen an, die auf dem primären Speicher verfügbar sind.
-  zeigt die Anzahl der Sicherungen an, die mithilfe der SnapMirror -Technologie auf dem sekundären Speicher gespiegelt werden.
-  zeigt die Anzahl der Sicherungen an, die mithilfe der SnapVault -Technologie auf dem sekundären Speicher repliziert werden.

- Die angezeigte Anzahl der Backups umfasst die aus dem sekundären Speicher gelöschten Backups.

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

**Best Practice:** Um sicherzustellen, dass die richtige Anzahl replizierter Sicherungen angezeigt wird, empfehlen wir Ihnen, die Topologie zu aktualisieren.

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

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

### Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Wählen Sie auf der Seite „Ressourcen“ die Datenbank, die Ressource oder die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource entweder aus der Datenbankdetailansicht oder aus der Ressourcengruppendetailansicht aus.

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

4. Im Abschnitt „Zusammenfassungskarte“ finden Sie eine Übersicht über die Anzahl der auf dem primären und sekundären Speicher verfügbaren Sicherungen.

Im Abschnitt „Zusammenfassungskarte“ werden die Gesamtzahl der Sicherungen und die Gesamtzahl der Protokollsicherungen angezeigt.

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

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

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

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

- Für SnapMirror Active Sync und nur für ONTAP 9.14.1 sollten Async Mirror- oder Async MirrorVault-Beziehungen zum neuen primären Ziel nach dem Failover manuell konfiguriert werden. Ab ONTAP 9.15.1 wird Async Mirror oder Async MirrorVault nach dem Failover automatisch auf das neue primäre Ziel konfiguriert.
- Nach dem Failover sollte ein Backup für SnapCenter erstellt werden, um über das Failover informiert

zu sein. Sie können erst auf **Aktualisieren** klicken, nachdem eine Sicherung erstellt wurde.

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

Die Details der Sicherungen werden in einem Tabellenformat angezeigt.

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



Sie können Sicherungen, die sich auf dem sekundären Speicher befinden, weder umbenennen noch löschen. Das Löschen von Snapshots wird durch die ONTAP Aufbewahrungseinstellungen geregelt.

## 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, BEISPIELHAFT 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.