SAP HANA-Ressourcen sichern

SnapCenter Software 4.6

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/de-de/snapcenter-46/protect-hana/task_back_up_sap_hana_resources.html on January 18, 2024. Always check docs.netapp.com for the latest.

Inhalt

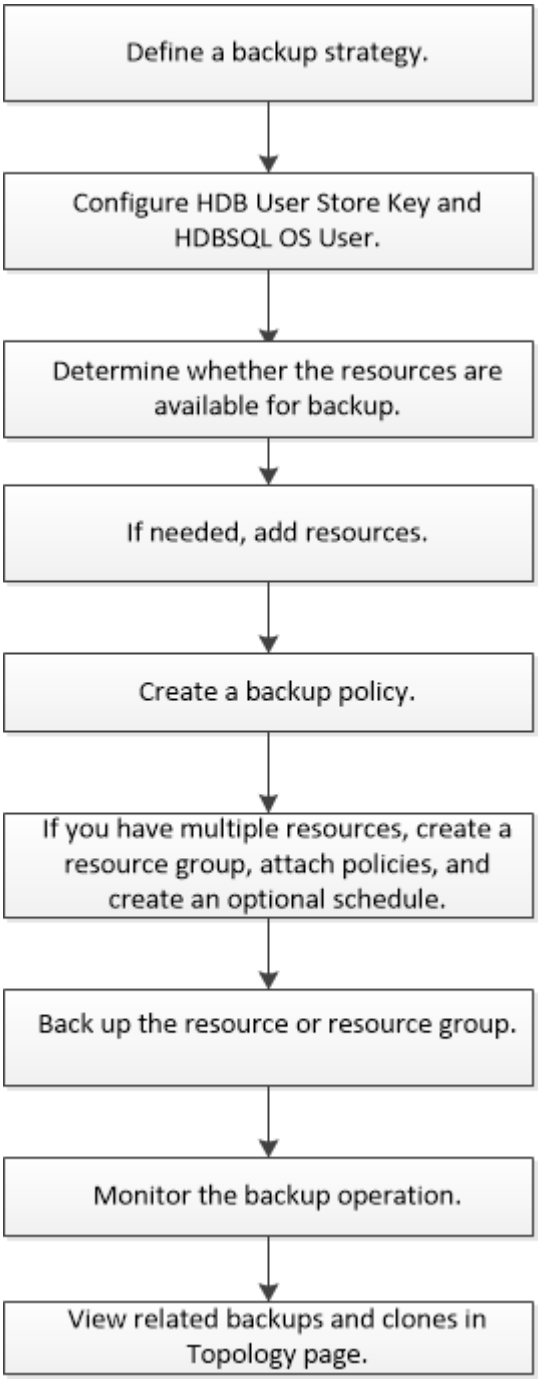
SAP HANA-Ressourcen sichern . . . 1
SAP HANA-Ressourcen sichern . . . 1
Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank . . . 2
Entdecken Sie Ressourcen und bereiten Sie mandantenfähige Datenbank-Container zur Datensicherung vor . . . 3
Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu . . . 5
Backup-Richtlinien für SAP HANA Datenbanken . . . 7
Erstellen von Ressourcengruppen und Anhängen von Richtlinien . . . 13
SAP HANA Datenbanken sichern . . . 17
Sichern von Ressourcengruppen . . . 20
Erstellen einer Storage-Systemverbindung und einer Zertifizierung mit PowerShell cmdlets für SAP HANA Datenbank . . . 21
Sichern Sie Datenbanken mit PowerShell Cmdlets . . . 23
Monitoring von Backup-Vorgängen . . . 26
Abbrechen der Backup-Vorgänge für SAP HANA . . . 28
Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an . . . 28

SAP HANA-Ressourcen sichern

SAP HANA-Ressourcen sichern

Sie können entweder ein Backup einer Ressource (Datenbank) oder einer Ressourcengruppe erstellen. Der Backup-Workflow umfasst die Planung, Identifizierung der Backup-Datenbanken, das Management von Backup-Richtlinien, das Erstellen von Ressourcengruppen und das Anhängen von Richtlinien, das Erstellen von Backups und das Monitoring der Betriebsprozesse.

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



Außerdem können Sie PowerShell Cmdlets manuell oder in Skripten verwenden, um Backup-, Wiederherstellungs- und Klonvorgänge durchzuführen. Die SnapCenter Cmdlet Hilfe und die Cmdlet Referenzinformationen enthalten weitere Informationen zu PowerShell Cmdlets.https://library.netapp.com/ecm/ecm_download_file/ECMLP2880726["SnapCenter Software Cmdlet Referenzhandbuch"^].

Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank

Sie müssen den HDB-Benutzerspeicherschlüssel und den HDBSQL OS-Benutzer konfigurieren, um Datenschutzvorgänge in SAP HANA-Datenbanken durchzuführen.

Was Sie brauchen

- Wenn in der SAP HANA-Datenbank nicht der HDB Secure User Store Key und der HDB SQL OS User konfiguriert sind, wird nur für die automatisch erkannten Ressourcen ein rotes Vorhängeschloss-Symbol angezeigt. Wenn sich während einer anschließenden Ermittlung der konfigurierte HDB Secure User Store Key als falsch herausstellte oder keinen Zugriff auf die Datenbank selbst bot, wird das rote Vorhängeschloss-Symbol erneut angezeigt.
- Sie müssen den HDB Secure User Store Key und den HDB SQL OS Benutzer so konfigurieren, dass sie die Datenbank schützen oder einer Ressourcengruppe hinzufügen können, um Datenschutzvorgänge durchzuführen.
- Sie müssen HDB SQL OS User konfigurieren, um auf die Systemdatenbank zugreifen zu können. Wenn HDB SQL OS User für den Zugriff auf nur die Mandantendatenbank konfiguriert ist, schlägt der Erkennungsvorgang fehl.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann SnapCenter-Plug-in für SAP HANA-Datenbank aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen den Ressourcentyp aus der Liste **Ansicht** aus.
3. (Optional) Klicken Sie Auf Und wählen Sie den Hostnamen aus.

   Sie können dann auf klicken Um den Filterbereich zu schließen.
4. Wählen Sie die Datenbank aus, und klicken Sie dann auf **Datenbank konfigurieren**.
5. Geben Sie im Abschnitt Datenbankeinstellungen konfigurieren den HDB-Schlüssel für sicheren Benutzerspeicher ein.

   > Der Plug-in-Hostname wird angezeigt und HDB SQL OS User wird automatisch in <sid>ADM eingetragen.

6. Klicken Sie auf **OK**.

Sie können die Datenbankkonfiguration auf der Seite Topology ändern.

Entdecken Sie Ressourcen und bereiten Sie mandantenfähige Datenbank-Container zur Datensicherung vor

Automatische Erkennung von Datenbanken

Ressourcen sind SAP HANA Datenbanken und nicht-Daten-Volumes auf dem Linux-Host, die von SnapCenter gemanagt werden. Diese Ressourcen können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge durchzuführen, nachdem die verfügbaren SAP HANA Datenbanken ermittelt wurden.

Was Sie brauchen

- Sie müssen bereits Aufgaben abgeschlossen haben, wie z. B. die Installation des SnapCenter-Servers, das Hinzufügen des HDB-Benutzerspeicherschlüssels, das Hinzufügen von Hosts und das Einrichten der Speichersystemverbindungen.
- Sie müssen den HDB Secure User Store Key und den HDB SQL OS-Benutzer auf dem Linux-Host konfiguriert haben.
  - Sie müssen den HDB-Benutzerspeicherschlüssel mit dem SID-Adm-Benutzer konfigurieren. Für HANA-Systeme mit A22 als SID muss beispielsweise der HDB User Store Key mit a22adm konfiguriert werden.
- Das SnapCenter Plug-in für SAP HANA Database unterstützt nicht das automatische Auffinden der Ressourcen in virtuellen RDM/VMDK-Umgebungen. Sie müssen Storage-Informationen für virtuelle Umgebungen bereitstellen und gleichzeitig Datenbanken manuell hinzufügen.

Über diese Aufgabe

Nach der Installation des Plug-ins werden alle Ressourcen auf diesem Linux-Host automatisch erkannt und auf der Seite Ressourcen angezeigt.

Die automatisch ermittelten Ressourcen können nicht geändert oder gelöscht werden.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das Plug-in für SAP HANA aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen den Ressourcentyp aus der Liste Ansicht aus.
3. (Optional) Klicken Sie Auf , und wählen Sie dann den Hostnamen aus.

   Sie können dann auf * klicken * Zum Schließen des Filterfensters.

4. Klicken Sie auf **Ressourcen aktualisieren**, um die auf dem Host verfügbaren Ressourcen zu ermitteln.

   Die Ressourcen werden zusammen mit Informationen wie Ressourcentyp, Hostname, zugeordnete Ressourcengruppen, Backup-Typ, Richtlinien und Gesamtstatus angezeigt.

   - Wenn sich die Datenbank auf einem NetApp Storage befindet und nicht geschützt ist, wird in der Spalte Status insgesamt nicht geschützt angezeigt.
   - Wenn sich die Datenbank auf einem NetApp Storage-System befindet und geschützt ist, und wenn kein Backup-Vorgang durchgeführt wird, wird in der Spalte Gesamtstatus der Eintrag Backup Not Run

angezeigt. Der Status ändert sich ansonsten auf „Sicherung fehlgeschlagen“ oder „Sicherung erfolgreich“, basierend auf dem letzten Backup-Status.

> Wenn in der SAP HANA-Datenbank kein HDB-sicherer Benutzerspeicherschlüssel konfiguriert ist, wird neben der Ressource ein rotes Vorhängeschloss-Symbol angezeigt. Wenn sich während einer anschließenden Ermittlung der konfigurierte HDB Secure User Store Key als falsch herausstellte oder keinen Zugriff auf die Datenbank selbst bot, wird das rote Vorhängeschloss-Symbol erneut angezeigt.

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

Nach Ihrer Beendigung

Sie müssen den HDB Secure User Store Key und den HDBSQL OS User so konfigurieren, dass sie die Datenbank schützen oder zur Ressourcengruppe hinzufügen können, um Datenschutzvorgänge durchzuführen.

"Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank"

Mandantenfähige Datenbank-Container werden für die Datensicherung vorbereitet

Bei direkt in SnapCenter registrierten SAP HANA Hosts wird das Installieren oder Upgrade des SnapCenter Plug-ins für SAP HANA Database eine automatische Ermittlung der Ressourcen auf dem Host auslösen. Nach der Installation oder dem Upgrade des Plug-ins werden für alle MDC-Ressourcen (Multi-Tenant-Datenbank-Container), die sich auf dem Plug-in-Host befand, automatisch eine andere MDC-Ressource mit einem anderen GUID-Format erkannt und in SnapCenter registriert. Die neue Ressource befindet sich im Status „`gesperrt`“.

Über diese Aufgabe

Wenn sich beispielsweise in SnapCenter 4.2 die E90-MDC-Ressource auf dem Plug-in-Host befand und manuell registriert wurde, wird nach dem Upgrade auf SnapCenter 4.3 eine weitere E90-MDC-Ressource mit einer anderen GUID erkannt und in SnapCenter registriert.

> Die Backups, die mit der Ressource von SnapCenter 4.2 und älteren Versionen verbunden sind, müssen bis zum Ablauf der Aufbewahrungsfrist aufbewahrt werden. Nach Ablauf des Aufbewahrungszeitraums können Sie die alte MDC-Ressource löschen und die neue automatisch erkannte MDC-Ressource weiterhin verwalten.

`Old MDC resource` Ist die MDC-Ressource für einen Plug-in-Host, der manuell in SnapCenter 4.2 oder früheren Versionen hinzugefügt wurde.

Führen Sie die folgenden Schritte durch, um die in SnapCenter 4.3 entdeckte neue Ressource für Datensicherungsvorgänge zu verwenden:

Schritte

1. Wählen Sie auf der Seite „Ressourcen“ die alte MDC-Ressource mit Backups aus, die der früheren

SnapCenter-Version hinzugefügt wurden, und legen Sie sie auf der Topologieseite in den „`maintBuße-Modus`“.

Wenn die Ressource Teil einer Ressourcengruppe ist, legen Sie die Ressourcengruppe in den „`mBetriebszustand`“.

2. Konfigurieren Sie die neue MDC-Ressource, die nach dem Upgrade auf SnapCenter 4.3 erkannt wurde, indem Sie die neue Ressource auf der Seite Ressourcen auswählen.

   „`Neue MDC-Ressource`“ ist die neu entdeckte MDC-Ressource, die erkannt wurde, nachdem der SnapCenter-Server und der Plug-in-Host auf 4.3 aktualisiert wurden. Die neue MDC-Ressource kann als Ressource mit demselben SID wie die alte MDC-Ressource, für einen bestimmten Host und mit einem roten Vorhängeschloss-Symbol daneben auf der Seite Ressourcen identifiziert werden.

3. Schützen Sie die neue MDC-Ressource, die nach dem Upgrade auf SnapCenter 4.3 erkannt wurde, indem Sie Schutzrichtlinien, Zeitpläne und Benachrichtigungseinstellungen auswählen.
4. Löschen Sie die Backups, die in SnapCenter 4.2 oder früheren Versionen basierend auf den Aufbewahrungseinstellungen erstellt wurden.
5. Löschen Sie die Ressourcengruppe auf der Seite Topologie.
6. Löschen Sie die alte MDC-Ressource von der Seite Ressourcen.

   Beispiel: Wenn die Aufbewahrungsdauer der primären Snapshot Kopien 7 Tage beträgt und die Aufbewahrung von sekundären Snapshot Kopien 45 Tage beträgt, nach 45 Tagen abgeschlossen sind und nachdem alle Backups gelöscht wurden, müssen Sie die Ressourcengruppe und die alte MDC-Ressource löschen.

Weitere Informationen

"Konfiguration des HDB-Benutzerspeicherschlüssels und des HDBSQL OS-Benutzers für die SAP HANA-Datenbank"

"Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an"

Fügen Sie dem Plug-in-Host manuell Ressourcen hinzu

Automatische Erkennung wird für bestimmte HANA-Instanzen nicht unterstützt. Sie müssen diese Ressourcen manuell hinzufügen.

Was Sie brauchen

- Sie müssen Aufgaben wie die Installation des SnapCenter-Servers, das Hinzufügen von Hosts, das Einrichten von Speichersystemverbindungen und das Hinzufügen des HDB-Benutzerspeicherschlüssels abgeschlossen haben.
- Für die SAP HANA Systemreplizierung wird empfohlen, alle Ressourcen dieses HANA-Systems in eine Ressourcengruppe hinzuzufügen und ein Ressourcengruppenbackup durchzuführen. So wird für ein nahtloses Backup im Takeover-Failback-Modus gesorgt.

"Erstellen von Ressourcengruppen und Anhängen von Richtlinien".

Über diese Aufgabe

Die automatische Erkennung wird für die folgenden Konfigurationen nicht unterstützt:

- RDM- und VMDK-Layouts

> Falls die oben genannten Ressourcen ermittelt werden, werden die Datensicherungsvorgänge von diesen Ressourcen nicht unterstützt.

- HANA Konfiguration für mehrere Hosts
- Mehrere Instanzen auf demselben Host
- Mehrschichtige Scale-out HANA System Replication
- Kaskadierte Replikationsumgebung im System Replication-Modus

Schritte

1. Wählen Sie im linken Navigationsbereich das SnapCenter-Plug-in für 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 bereitstellen“ die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Ressourcentyp	Geben Sie den Ressourcentyp ein. Ressourcentypen sind Single-Container, Multitenant Database Container (MDC) und Non-Data-Volume.
HANA-Systemname	Geben Sie den beschreibenden SAP HANA-Systemnamen ein. Diese Option ist nur verfügbar, wenn Sie einzelne Container- oder MDC-Ressourcentypen ausgewählt haben.
SID	Geben Sie die System-ID (SID) ein. Das installierte SAP HANA System wird durch eine einzige SID identifiziert.
Plug-in-Host	Wählen Sie den Plug-in-Host aus.
HDB Secure User Store Keys	Geben Sie den Schlüssel für die Verbindung zum SAP HANA-System ein. Der Schlüssel enthält die Anmeldeinformationen, um eine Verbindung zur Datenbank herzustellen. Für SAP HANA System Replication ist der sekundäre Benutzerschlüssel nicht validiert. Dies wird während der Übernahme verwendet.

Für dieses Feld…	Tun Sie das…
HDBSQL OS-Benutzer	Geben Sie den Benutzernamen ein, für den der HDB Secure User Store Key konfiguriert ist. Für Windows ist es erforderlich, dass der HDBSQL OS-Benutzer der SYSTEMBENUTZER ist. Daher müssen Sie den HDB Secure User Store Key für den SYSTEMBENUTZER konfigurieren.

4. Wählen Sie auf der Seite Speicher-Footprint angeben ein Speichersystem aus und wählen Sie ein oder mehrere Volumes, LUNs und qtrees aus, und klicken Sie dann auf **Speichern**.

   Optional: Klicken Sie auf das Symbol + Symbol, um weitere Volumes, LUNs und qtrees von anderen Speichersystemen hinzuzufügen.

5. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

   Die Datenbanken werden zusammen mit Informationen wie SID, Plug-in-Host, zugehörigen Ressourcengruppen und Richtlinien sowie dem Gesamtstatus angezeigt

Wenn Sie Benutzern Zugriff auf Ressourcen gewähren möchten, müssen Sie den Benutzern die Ressourcen zuweisen. Auf diese Weise können Benutzer die Aktionen ausführen, für die sie über Berechtigungen für die ihnen zugewiesenen Assets verfügen.

"Fügen Sie einen Benutzer oder eine Gruppe hinzu und weisen Sie Rollen und Assets zu"

Nach dem Hinzufügen der Datenbanken können Sie die Details der SAP HANA-Datenbank ändern.

Folgendes kann nicht geändert werden, wenn mit der SAP HANA-Ressource Backups verknüpft sind:

- Mandantenfähige Datenbank-Container (MDC): SID- oder HDBSQL Client (Plug-in)-Host
- Einzelner Container: SID- oder HDBSQL-Client (Plug-in)-Host
- Kein Datenvolumen: Ressourcenname, zugehöriger SID oder Plug-in-Host

Backup-Richtlinien für SAP HANA Datenbanken

Bevor Sie SnapCenter zum Sichern von SAP HANA-Datenbankressourcen verwenden, müssen Sie eine Backup-Richtlinie für die Ressource oder Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln.

Was Sie brauchen

- Sie müssen Ihre Backup-Strategie definiert haben.

  Weitere Informationen zur Definition einer Datensicherungsstrategie für SAP HANA Datenbanken finden Sie in den Informationen.

- Sie müssen auf die Datensicherung vorbereitet sein, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Einrichten von Verbindungen zu Storage-Systemen und das

Hinzufügen von Ressourcen ausführen.

- Der SnapCenter Administrator muss Ihnen die SVMs für die Quell- und Ziel-Volumes zuweisen, falls Sie Snapshot Kopien in eine Spiegelung oder einen Vault replizieren.

  Außerdem können Sie in der Richtlinie Replizierungs-, Skript- und Applikationseinstellungen festlegen. Diese Optionen sparen Zeit, wenn Sie die Richtlinie für eine andere Ressourcengruppe wiederverwenden möchten.

Über diese Aufgabe

- SAP HANA System Replication
  - Das primäre SAP HANA System ist gesichert, und alle Datensicherungsvorgänge können durchgeführt werden.
  - Sie können das sekundäre SAP HANA System schützen, aber die Backups können nicht erstellt werden.

    Nach dem Failover kann der gesamte Datensicherungsvorgang durchgeführt werden, wenn das sekundäre SAP HANA System zum primären SAP HANA System wird.

  Sie können kein Backup für SAP HANA Daten-Volume erstellen, aber SnapCenter schützt weiterhin die nicht-Daten-Volumes (NDV).

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 Einstellungen die folgenden Schritte aus:
   - Wählen Sie den Sicherungstyp:

Ihr Ziel ist	Tun Sie das…
Führen Sie eine Integritätsprüfung der Datenbank durch	Wählen Sie * File-Based Backup* Aus. Es werden nur aktive Mandanten gesichert.
Erstellen Sie mit Snapshot-Kopiertechnologie ein Backup	Wählen Sie **Snapshot-Basiert** Aus.

   - Geben Sie den Terminplantyp an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

     Sie können den Zeitplan (Startdatum, Enddatum und Häufigkeit) für den Backup-Vorgang beim Erstellen einer Ressourcengruppe angeben. So können Sie Ressourcengruppen erstellen, die dieselben Richtlinien und Backup-Häufigkeit verwenden, aber auch die Möglichkeit haben, den einzelnen Richtlinien unterschiedliche Backup-Zeitpläne zuzuweisen.

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

- (●) On demand
- ( ) Hourly
- ( ) Daily
- ( ) Weekly
- ( ) Monthly

> Wenn Sie für 2:00 Uhr geplant sind, wird der Zeitplan während der Sommerzeit (DST) nicht ausgelöst.

- Geben Sie im Abschnitt **Benutzerdefinierte Backup-Einstellungen** alle spezifischen Backup-Einstellungen an, die an das Plug-in Key-Value-Format übergeben werden müssen.

  Sie können mehrere wichtige Werte angeben, die an das Plug-in übergeben werden.

6. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite Sicherungstyp ausgewählten Terminplantyp an:

Ihr Ziel ist	Dann…
Aufbewahrung einer bestimmten Anzahl von Snapshot Kopien	Wählen Sie **Gesamtanzahl der zu behenden Snapshot-Kopien** aus, und geben Sie dann die Anzahl der Snapshot-Kopien an, die beibehalten werden sollen. Wenn die Anzahl der Snapshot Kopien die angegebene Anzahl überschreitet, werden die Snapshot Kopien mit den ältesten Kopien gelöscht, die zuerst gelöscht wurden. Der maximale Aufbewahrungswert ist 1018 für Ressourcen auf ONTAP 9.4 oder höher und 254 für Ressourcen unter ONTAP 9.3 oder einer früheren Version. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Wenn Sie Snapshot Backups auf Basis von Kopien aktivieren SnapVault möchten, müssen Sie die Aufbewahrungsanzahl auf 2 oder höher festlegen. Wenn Sie die Aufbewahrungsanzahl auf 1 festlegen, kann der Aufbewahrungsvorgang möglicherweise fehlschlagen, da die erste Snapshot Kopie die Referenzkopie für die SnapVault-Beziehung ist, bis eine neuere Snapshot Kopie auf das Ziel repliziert wird. Für die SAP HANA-Systemreplizierung wird empfohlen, alle Ressourcen des SAP HANA-Systems in einer Ressourcengruppe hinzuzufügen. So wird sichergestellt, dass die richtige Anzahl von Backups beibehalten wird.

Ihr Ziel ist	Dann…
Behalten Sie die Snapshot Kopien für eine bestimmte Anzahl von Tagen bei	Wählen Sie **Snapshot Kopien behalten für** aus, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshot Kopien behalten möchten, bevor Sie sie löschen.

7. Geben Sie für Snapshot-Copy-basierte Backups die Replikationseinstellungen auf der Seite Replikation an:

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Wenn die Sicherungsbeziehung in ONTAP vom Typ Mirror und Vault beträgt und wenn Sie nur diese Option auswählen, wird die auf dem primären Volume erstellte Snapshot Kopie nicht an das Ziel übertragen, sondern dort aufgeführt. Wenn diese Snapshot Kopie aus dem Ziel ausgewählt wird, um einen Wiederherstellungsvorgang durchzuführen, wird der sekundäre Speicherort für die ausgewählte Fehlermeldung „vaulted/mirrored Backup“ angezeigt.
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen.
Sekundäres Policy-Label	Wählen Sie eine Snapshot-Bezeichnung aus. Abhängig von dem ausgewählten Etikett der Snapshot Kopie wendet ONTAP die Aufbewahrungsrichtlinie für sekundäre Snapshot Kopien an, die mit dem Etikett übereinstimmt. Wenn Sie **Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, können Sie optional das Label für die sekundäre Richtlinie angeben. Wenn Sie jedoch **Update SnapVault nach dem Erstellen einer lokalen Snapshot Kopie** ausgewählt haben, sollten Sie das sekundäre Policy Label angeben.

Für dieses Feld…	Tun Sie das…
Anzahl der Wiederholversuche	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

> Sie sollten die SnapMirror Aufbewahrungsrichtlinie in ONTAP für den sekundären Storage konfigurieren, um zu vermeiden, dass die maximale Anzahl an Snapshot Kopien auf dem sekundären Storage erreicht wird.

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

Erstellen von Ressourcengruppen und Anhängen von 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.

Über diese Aufgabe

Zur Erstellung von SAP HANA System-Replikations-Backups wird empfohlen, alle Ressourcen des SAP HANA-Systems zu einer Ressourcengruppe hinzuzufügen. So wird für ein nahtloses Backup im Takeover-Failback-Modus gesorgt.

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 durch:

Für dieses Feld…	Tun Sie das…
Name	Geben Sie einen Namen für die Ressourcengruppe ein. Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

Für dieses Feld…	Tun Sie das…
Tags	Geben Sie eine oder mehrere Bezeichnungen ein, die Ihnen bei der späteren Suche nach der Ressourcengruppe helfen. Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.
Verwenden Sie für Snapshot-Kopie das benutzerdefinierte Namensformat	Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Namen der Snapshot Kopie verwenden möchten. Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.

4. Wählen Sie auf der Seite Ressourcen einen Hostnamen aus der Dropdown-Liste **Host** und Ressourcentyp aus der Dropdown-Liste **Ressourcentyp** aus.

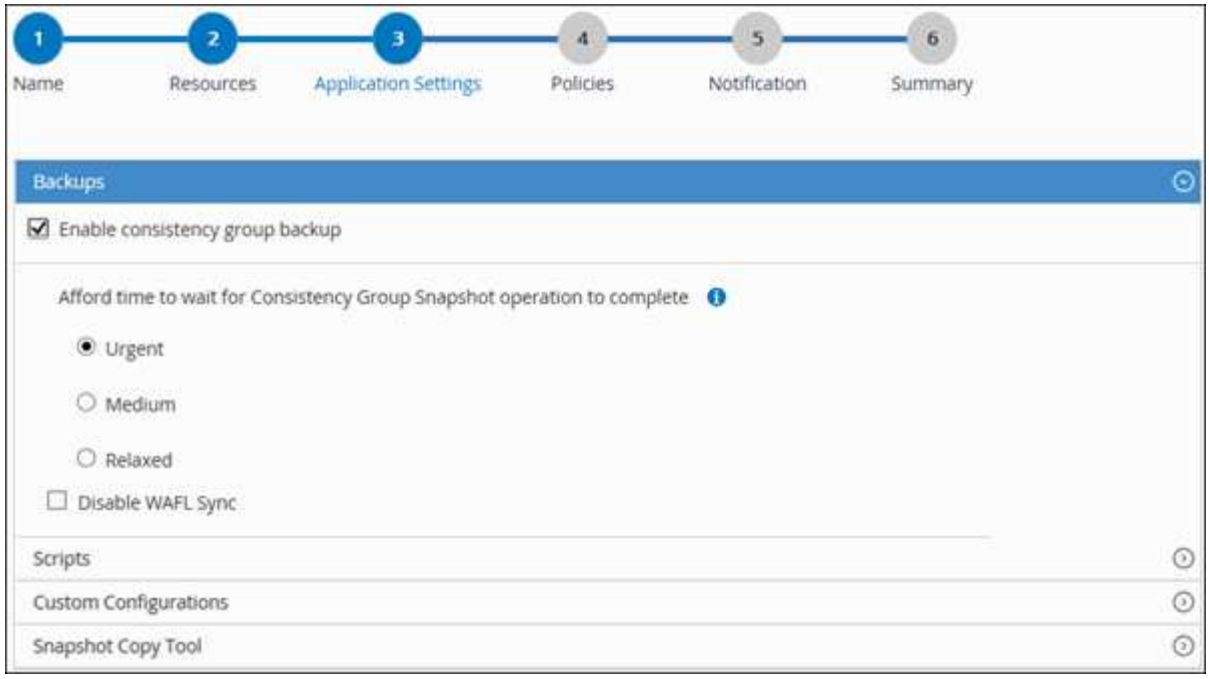
   Dadurch können Informationen auf dem Bildschirm gefiltert werden.

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. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   a. Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

      Aktivieren Sie das Backup von Konsistenzgruppen und führen Sie die folgenden Aufgaben aus:

Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der Snapshot-Vorgang der Konsistenzgruppe abgeschlossen ist	Wählen Sie **dringendst**, **Medium** oder **relaxed** aus, um die Wartezeit zum Abschluss des Snapshot-Kopiervorgangs anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

+ 

a. Klicken Sie auf den Pfeil **Scripts** und geben Sie die vor- und Post-Befehle für quiesce, Snapshot copy und unquiesce Operations ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.

b. Klicken Sie auf den Pfeil **Benutzerdefinierte Konfigurationen** und geben Sie die für alle Datenschutzvorgänge erforderlichen benutzerdefinierten Schlüsselwert-Paare mit dieser Ressource ein.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_ENABLE	(J/N)	Ermöglicht die Verwaltung des Archivprotokolls, die Archivprotokolle zu löschen.
ARCHIVE_LOG_RETENTION	Anzahl_Tage	Gibt die Anzahl der Tage an, die die Archivprotokolle aufbewahrt werden. Diese Einstellung muss gleich oder größer sein als NTAP_SNAPSHOT_ AUFBEWAHRUNG.
ARCHIVE_LOG_DIR	Change_info_Directory/logs	Gibt den Pfad zum Verzeichnis an, das die Archivprotokolle enthält.

Parameter	Einstellung	Beschreibung
ARCHIVE_LOG_EXT	Dateierweiterung	Gibt die Länge der Erweiterung der Archivprotokolldatei an. Wenn das Archivprotokoll beispielsweise log_Backup_0_0_0_0.16151855 1942 9 lautet und der Wert file_Extension 5 ist, bleibt die Erweiterung des Protokolls 5 Ziffern, also 16151.
ARCHIVE_LOG_RECURSIVE_ SE-BOGEN	(J/N)	Ermöglicht das Management von Archivprotokollen innerhalb von Unterverzeichnissen. Sie sollten diesen Parameter verwenden, wenn sich die Archivprotokolle unter Unterverzeichnissen befinden.

Die benutzerdefinierten Schlüsselwerterpaare werden für SAP HANA Linux-Plug-in-Systeme unterstützt und nicht für SAP HANA-Datenbanken unterstützt, die als zentrales Windows-Plug-in registriert sind.

c. Klicken Sie auf den Pfeil **Snapshot-Kopie-Tool**, um das Tool zum Erstellen von Snapshot-Kopien auszuwählen:

Ihre Situation	Dann…
SnapCenter, um das Plug-in für Windows zu nutzen und das Filesystem in einen konsistenten Zustand zu versetzen, bevor eine Snapshot Kopie erstellt wird. Für Linux-Ressourcen ist diese Option nicht anwendbar.	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus. Diese Option ist für das SnapCenter-Plug-in für SAP HANA Database nicht verfügbar.
SnapCenter zum Erstellen einer Snapshot Kopie auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
Geben Sie den Befehl ein, der auf dem Host ausgeführt werden soll, um Snapshot Kopien zu erstellen.	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, der auf dem Host ausgeführt werden soll, um eine Snapshot Kopie zu erstellen.

7. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

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

Die Richtlinien sind im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ aufgeführt.

b. Klicken Sie in der Spalte Zeitplan 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**.

   Hier ist Policy_Name der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte **angewendete Zeitpläne** aufgeführt.

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Der SMTP-Server muss unter **Einstellungen** > **Globale Einstellungen** konfiguriert sein.

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

SAP HANA Datenbanken sichern

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

Was Sie brauchen

- Sie müssen eine Sicherungsrichtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.
- Stellen Sie beim Backup-Vorgang auf Basis von Snapshot Kopien sicher, dass alle Mandantendatenbanken gültig und aktiv sind.
- Zur Erstellung von SAP HANA System-Replikations-Backups wird empfohlen, alle Ressourcen des SAP HANA-Systems zu einer Ressourcengruppe hinzuzufügen. So wird für ein nahtloses Backup im Takeover-Failback-Modus gesorgt.

  "Erstellen von Ressourcengruppen und Anhängen von Richtlinien".

  "Sichern von Ressourcengruppen"

- Wenn Sie ein dateibasiertes Backup erstellen möchten, wenn eine oder mehrere Mandanten-Datenbanken nicht verfügbar sind, setzen Sie DEN PARAMETER ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT in der HANA-Eigenschaftendatei mit AUF **JA** `Set-SmConfigSettings` Cmdlet:

  Die Informationen zu den Parametern, die mit dem Cmdlet verwendet werden können, und deren Beschreibungen können durch Ausführen von Get-Help *Command_Name* abgerufen werden. Alternativ

können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch"

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 **Ansicht** nach Ressourcentyp.

   Klicken Sie Auf , und wählen Sie dann den Host-Namen und den Ressourcentyp, um die Ressourcen zu filtern. Sie können dann auf klicken Um den Filterbereich zu schließen.

3. Klicken Sie auf die Ressource, die Sie sichern möchten.
4. 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 Namen der Snapshot-Kopie verwenden möchten.

   Beispiel: *Custext_Policy_hostname* oder *Resource_hostname*. Standardmäßig wird ein Zeitstempel an den Namen der Snapshot Kopie angehängt.

5. Gehen Sie auf der Seite Anwendungseinstellungen wie folgt vor:

   - Klicken Sie auf den Pfeil **Backups**, um zusätzliche Backup-Optionen festzulegen:

     Aktivieren Sie bei Bedarf das Backup der Konsistenzgruppe, und führen Sie die folgenden Aufgaben aus:

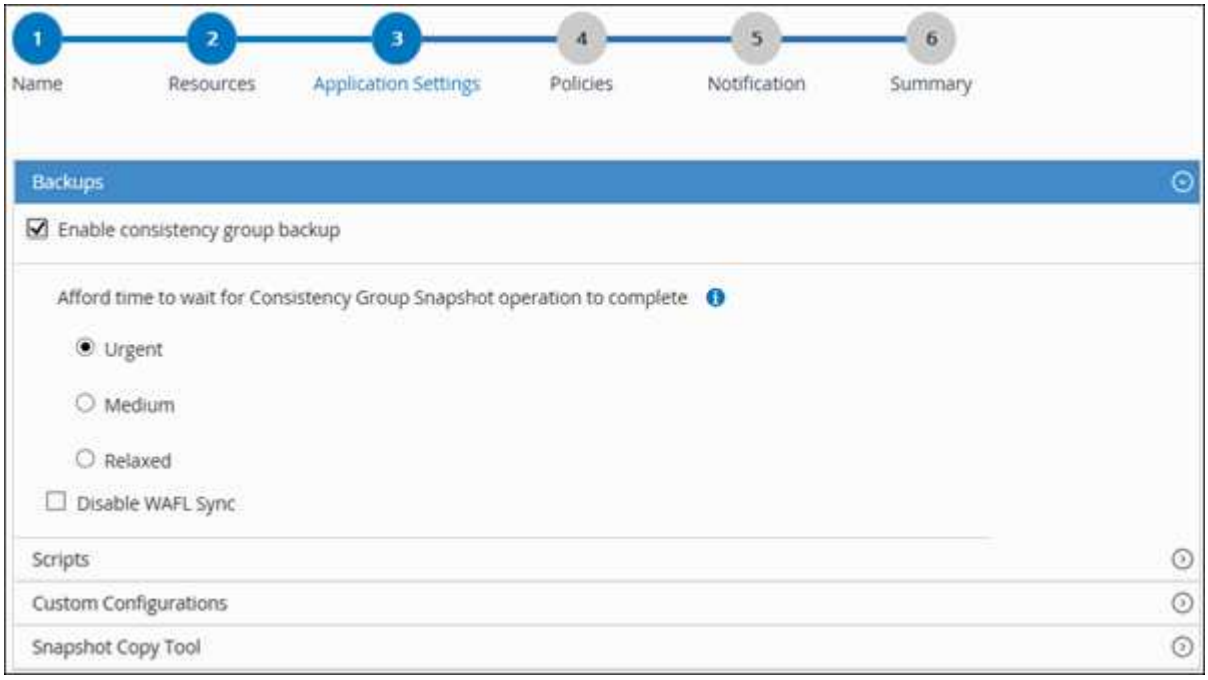
Für dieses Feld…	Tun Sie das…
Es dauert nicht lange, bis der „Consistency Group Snapshot“-Vorgang abgeschlossen ist	Wählen Sie **dringendst**, oder **Medium**, oder **relaxed** aus, um die Wartezeit bis zum Abschluss der Snapshot-Kopie anzugeben. Dringend = 5 Sekunden, Mittel = 7 Sekunden und entspannt = 20 Sekunden.
Deaktivieren Sie WAFL Sync	Wählen Sie diese Option aus, um zu vermeiden, einen WAFL Konsistenzpunkt zu erzwingen.

   - Klicken Sie auf den Pfeil **Scripts**, um vor- und Post-Befehle für quiesce, Snapshot copy und unquiesce-Vorgänge auszuführen.

     Sie können auch vor dem Beenden des Sicherungsvorgangs Vorbefehle ausführen. Prescripts und Postscripts werden auf dem SnapCenter Server ausgeführt.

   - Klicken Sie auf den Pfeil **Custom Configurations**und geben Sie dann die für alle Jobs mit dieser Ressource erforderlichen benutzerdefinierten Wertpaare ein.
   - Klicken Sie auf den Pfeil **Snapshot-Kopie-Tool**, um das Tool zum Erstellen von Snapshot-Kopien auszuwählen:

Ihre Situation	Dann…
SnapCenter zum Erstellen einer Snapshot Kopie auf Storage-Ebene	Wählen Sie **SnapCenter ohne Dateisystemkonsistenz** aus.
SnapCenter verwendet das Plug-in für Windows, um das Filesystem in einen konsistenten Zustand zu versetzen und anschließend eine Snapshot Kopie zu erstellen	Wählen Sie **SnapCenter mit Dateisystemkonsistenz** aus.
Geben Sie den Befehl ein, um eine Snapshot Kopie zu erstellen	Wählen Sie **other** aus, und geben Sie dann den Befehl ein, um eine Snapshot Kopie zu erstellen.



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

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

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

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

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

   c. Konfigurieren Sie im Dialogfeld Add Schedules for Policy_Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

   Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

7. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. SMTP muss auch unter **Einstellungen** > **Globale Einstellungen** konfiguriert werden.

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

   Die Seite „Ressourcen-Topologie“ wird angezeigt.

9. Klicken Sie auf **Jetzt sichern**.
10. Führen Sie auf der Seite Backup die folgenden Schritte aus:
    a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie für das Backup verwenden möchten.

       Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

    b. Klicken Sie Auf **Backup**.
11. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.
    - In MetroCluster-Konfigurationen kann SnapCenter nach einem Failover möglicherweise keine Sicherungsbeziehung 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 für VMware vSphere nicht groß genug ist, kann die Sicherung fehlschlagen.

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

Sichern von Ressourcengruppen

Eine Ressourcengruppe ist eine Sammlung von Ressourcen auf einem Host. Für alle in der Ressourcengruppe definierten Ressourcen wird ein Sicherungsvorgang in der Ressourcengruppe durchgeführt.

Was Sie brauchen

- Sie müssen eine Ressourcengruppe mit einer angehängten Richtlinie erstellt haben.
- Wenn Sie eine Ressource mit einer SnapMirror Beziehung mit einem sekundären Storage sichern möchten, sollte die dem Storage-Benutzer zugewiesene ONTAP-Rolle die Berechtigung „`snapmirror all`“ enthalten. Wenn Sie jedoch die Rolle „`vsadmin`“ verwenden, ist die Berechtigung „`snapmirror all`“ nicht erforderlich.

Über diese Aufgabe

Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn eine Ressourcengruppe über eine Richtlinie und einen konfigurierten Zeitplan verfügt, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

Schritte

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

   Sie können die Ressourcengruppe entweder durch Eingabe des Ressourcengruppennamens in das Suchfeld oder durch Klicken durchsuchen , Und dann das Tag auswählen. 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 Backup die folgenden Schritte aus:
   a. Wenn Sie der Ressourcengruppe mehrere Richtlinien zugeordnet haben, wählen Sie aus der Dropdown-Liste **Richtlinie** die Richtlinie aus, die Sie zum Sichern verwenden möchten.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Klicken Sie Auf **Backup**.
5. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Erstellen einer Storage-Systemverbindung und einer Zertifizierung mit PowerShell cmdlets für SAP HANA Datenbank

Sie müssen eine SVM-Verbindung (Storage Virtual Machine) und Zugangsdaten erstellen, bevor Sie PowerShell cmdlets verwenden können, um SAP HANA Datenbanken zu sichern, wiederherzustellen oder zu klonen.

Was Sie brauchen

- Sie sollten die PowerShell Umgebung auf die Ausführung der PowerShell Commandlets vorbereitet haben.
- Sie sollten die erforderlichen Berechtigungen in der Rolle „Infrastrukturadministrator“ besitzen, um Speicherverbindungen zu erstellen.
- Sie sollten sicherstellen, dass die Plug-in-Installationen nicht ausgeführt werden.

  Die Host-Plug-in-Installationen dürfen beim Hinzufügen einer Speichersystemverbindung nicht ausgeführt werden, da der Host-Cache möglicherweise nicht aktualisiert wird und der Datenbank-Status in der SnapCenter GUI unter „`not available for Backup`“ oder „`not on NetApp Storage`“ angezeigt werden kann.

- Speichersystemnamen sollten eindeutig sein.

  SnapCenter unterstützt nicht mehrere Storage-Systeme mit demselben Namen auf verschiedenen

Clustern. Jedes von SnapCenter unterstützte Storage-System sollte über einen eindeutigen Namen und eine eindeutige LIF-IP-Adresse für Daten verfügen.

Schritte

1. Initiieren Sie eine PowerShell-Verbindungssitzung mit dem Cmdlet Open-SmConnection.

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

2. Erstellen Sie mit dem Cmdlet "Add-SmStorageConnection" eine neue Verbindung zum Storage-System.

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

3. Erstellen Sie mit dem Cmdlet "Add-SmCredential" eine neue Anmeldeinformation.

   In diesem Beispiel wird das Erstellen einer neuen Anmeldeinformationen namens FinanceAdmin mit Windows-Anmeldeinformationen angezeigt:

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

4. Fügen Sie den SAP HANA-Kommunikationshost dem SnapCenter-Server hinzu.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. Installieren Sie das Paket und das SnapCenter-Plug-in für SAP HANA-Datenbank auf dem Host.

   Für Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
hana
```

   Für Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Legen Sie den Pfad zum HDBSQL-Client fest.

   Für Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

Für Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Sichern Sie Datenbanken mit PowerShell Cmdlets

Das Sichern einer Datenbank umfasst die Einrichtung einer Verbindung mit dem SnapCenter-Server, das Hinzufügen von Ressourcen, das Hinzufügen einer Richtlinie, das Erstellen einer Backup-Ressourcengruppen und das Sichern von Ressourcen.

Was Sie brauchen

- Sie müssen die PowerShell Umgebung vorbereitet haben, um die PowerShell Cmdlets auszuführen.
- Sie müssen die Speichersystemverbindung hinzugefügt und Anmeldedaten erstellt haben.

Schritte

1. Starten Sie eine Verbindungssitzung mit dem SnapCenter-Server für einen bestimmten Benutzer, indem Sie das Cmdlet "Open-SmConnection" verwenden.

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

   Die Eingabeaufforderung für Benutzername und Passwort wird angezeigt.

2. Mit dem Cmdlet "Add-SmResources" können Sie Ressourcen hinzufügen.

   Dieses Beispiel zeigt, wie eine SAP HANA-Datenbank des SingleContainer-Typs hinzugefügt wird:

   ```
   C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'
   -DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint
   (@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"})
   -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys 'HS10'
   -osdbuser 'h10adm' -filebackupprefix 'H10_'
   ```

In diesem Beispiel wird das Hinzufügen einer SAP HANA-Datenbank mit MultipleContainers-Typ beschrieben:

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType MultipleContainers
-StorageFootPrint
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.netapp.
com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType 'MultiTenant'
```

Dieses Beispiel zeigt, wie Sie eine Ressource erstellen, die nicht auf dem Datenvolumen ist:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Erstellen Sie mithilfe des Cmdlet "Add-SmPolicy" eine Backup-Richtlinie.

   In diesem Beispiel wird eine Backup-Richtlinie für ein auf Snapshot Kopien basierendes Backup erstellt:

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType Backup
-PluginPolicyType hana -BackupType SnapShotBasedBackup
```

   In diesem Beispiel wird eine Backup-Richtlinie für ein dateibasiertes Backup erstellt:

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. Schützen Sie die Ressource oder fügen Sie eine neue Ressourcengruppe zu SnapCenter mit dem Cmdlet "Add-SmResourceGroup" hinzu.

   Dieses Beispiel schützt eine einzelne Container-Ressource:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="SID"} -Description test
-usesnapcenterwithoutfilesystemconsistency
```

   Dieses Beispiel schützt eine Ressource mit mehreren Containern:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

In diesem Beispiel wird eine neue Ressourcengruppe mit der angegebenen Richtlinie und den angegebenen Ressourcen erstellt:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sccore
linux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

Dieses Beispiel erstellt eine Ressourcengruppe ohne Daten-Volume:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"="han
a"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"PluginName
"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="NonDataVolume\
S10\NonDataVolume";"PluginName"="hana"}) -Policies hanaprimary
```

5. Initiieren Sie einen neuen Sicherungsauftrag mit dem Cmdlet "New-SmBackup".

   Dieses Beispiel zeigt, wie eine Ressourcengruppe gesichert werden kann:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

   Dieses Beispiel sichert eine geschützte Ressource:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"} -Policy
hana_Filebased
```

6. Überwachen Sie den Job-Status (ausgeführt, abgeschlossen oder fehlgeschlagen) mit dem Cmdlet "Get-smJobSummaryReport".

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Überwachen Sie die Details zu Backup-Jobs wie Backup-ID, Backup-Name zum Wiederherstellen oder Klonen mit dem Cmdlet "Get-SmBackupReport".

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die verweisen "SnapCenter Software Cmdlet Referenzhandbuch".

Monitoring von Backup-Vorgängen

Monitoring von Backup-Vorgängen bei SAP HANA Datenbanken

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

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

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.
3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie Auf Filtern der Liste, sodass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

   Der Status des Backupjobs wird zwar angezeigt Wenn Sie auf die Jobdetails klicken, wird möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Backup-Vorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

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

Überwachen von Datensicherungsvorgängen in SAP HANA-Datenbanken im Bereich „Activity“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten Backup-Vorgängen angezeigt. Wenn Sie Plug-in für SQL Server oder Plug-in für Exchange Server verwenden, werden im Aktivitätsbereich auch Informationen über den erneuten Seeding angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie Auf Im Aktivitätsbereich werden die fünf letzten Vorgänge angezeigt.

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

Abbrechen der Backup-Vorgänge für SAP HANA

Sie können Backup-Vorgänge in der Warteschlange abbrechen.

Was Sie brauchen

- Sie müssen als SnapCenter-Administrator oder -Auftragseigentümer angemeldet sein, um Vorgänge abzubrechen.
- Sie können einen Sicherungsvorgang entweder über die Seite **Monitor** oder über den Bereich **Aktivität** abbrechen.
- Sie können einen laufenden Sicherungsvorgang nicht abbrechen.
- Sie können die SnapCenter GUI, PowerShell Commandlets oder CLI-Befehle verwenden, um die Backup-Vorgänge abzubrechen.
- Die Schaltfläche **Job abbrechen** ist für Vorgänge deaktiviert, die nicht abgebrochen werden können.
- Wenn Sie **Alle Mitglieder dieser Rolle sehen und auf anderen Mitgliedsobjekten** auf der Seite Benutzer\Gruppen arbeiten können, während Sie eine Rolle erstellen, können Sie die in der Warteschlange befindlichen Backup-Vorgänge anderer Mitglieder abbrechen, während Sie diese Rolle verwenden.

Schritte

1. Führen Sie eine der folgenden Aktionen aus:

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

Der Vorgang wird abgebrochen und die Ressource wird in den vorherigen Status zurückgesetzt.

Sehen Sie sich SAP HANA Datenbank-Backups und -Klone auf der Seite Topologie an

Bei der Vorbereitung von Backups und Klonen einer Ressource ist es unter Umständen hilfreich, eine grafische Darstellung aller Backups und Klone auf dem primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

In der Ansicht Kopien managen können Sie die folgenden Symbole überprüfen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Storage (Mirror-Kopien oder Vault-Kopien) verfügbar sind.

- Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
- Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapMirror Technologie auf dem sekundären Storage gespiegelt werden.
- Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault Technologie auf dem sekundären Storage repliziert werden.

  > Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

> Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

> Bei der SAP HANA Systemreplizierung werden die Restore- und Löschvorgänge unterstützt und für sekundäre Ressourcen wird der Klonvorgang unterstützt.

Auf der Seite Topology sehen Sie alle Backups und Klone, die für die ausgewählte Ressource oder Ressourcengruppe zur Verfügung stehen. Sie können die Details zu diesen Backups und Klonen anzeigen und diese dann zur Durchführung von Datensicherungsvorgängen auswählen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

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

4. Lesen Sie die **Übersichtskarte** durch, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Speicher verfügbar sind.

   Im Abschnitt **Summary Card** wird die Gesamtzahl der dateibasierten Backups, Snapshot-Kopien-Backups und Klone angezeigt.

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

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

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf die Datensicherungssymbole, um Restore-, Klon- und Löschvorgänge durchzuführen.

   > Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie anschließend auf .
8. Wenn Sie einen Klon aufteilen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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