



Konfigurationsinformationen sichern

SnapCenter Software 4.8

NetApp
January 18, 2024

Inhalt

- Konfigurationsinformationen sichern 1
 - Unterstützte Oracle Database Konfigurationen für Backups 1
 - Arten von Backups, die für Oracle-Datenbanken unterstützt werden 1
 - Wie SnapCenter Oracle Datenbanken erkennt 2
 - Bevorzugte Knoten im RAC-Setup 4
 - So katalogisieren Sie Backups mit Oracle Recovery Manager 5
 - Vordefinierte Umgebungsvariablen für Backup-spezifische Prescript und Postscript 6
 - Optionen zur Backup-Aufbewahrung 12
 - Backup-Pläne 12
 - Konventionen bei Backup-Namen 13

Konfigurationsinformationen sichern

Unterstützte Oracle Database Konfigurationen für Backups

SnapCenter unterstützt das Backup verschiedener Oracle Database Konfigurationen.

- Oracle Standalone
- Oracle Real Application Clusters (RAC)
- Oracle Standalone Legacy
- Oracle Standalone Container-Datenbank (CDB)
- Oracle Data Guard Standby

Sie können nur Offline-Mount-Backups von Data Guard Standby-Datenbanken erstellen. Offline-Shutdown-Backup, Backup nur für Archivprotokolle und vollständiges Backup werden nicht unterstützt.

- Oracle Active Data Guard Standby

Sie können nur Online-Backups von Active Data Guard Standby-Datenbanken erstellen. Backup nur für Archivprotokolle und vollständige Backups werden nicht unterstützt.

Vor dem Erstellen eines Backups von Data Guard Standby oder der Active Data Guard Standby Datenbank wird der Managed Recovery-Prozess (MRP) angehalten und nach dem Erstellen des Backups wird MRP gestartet.

- Automatisches Storage-Management (ASM)
 - ASM Standalone und ASM RAC auf Virtual Machine Disk (VMDK)

Unter allen für Oracle-Datenbanken unterstützten Wiederherstellungsmethoden können Sie nur eine Verbindung-und-Kopie-Wiederherstellung von ASM RAC-Datenbanken auf VMDK durchführen.

- ASM Standalone und ASM RAC on Raw Device Mapping (RDM)
Sie können Backup-, Wiederherstellungs- und Klonvorgänge für Oracle-Datenbanken auf ASM mit oder ohne ASMLib durchführen.
- Oracle ASM Filtertreiber (ASMFDF)

PDB-Migration und PDB-Klonvorgänge werden nicht unterstützt.

- Oracle Flex ASM

Aktuelle Informationen zu unterstützten Oracle-Versionen finden Sie unter "[NetApp Interoperabilitäts-Matrix-Tool](#)".

Arten von Backups, die für Oracle-Datenbanken unterstützt werden

Der Sicherungstyp gibt den Sicherungstyp an, den Sie erstellen möchten. SnapCenter unterstützt Online- und Offline-Backups für Oracle Datenbanken.

Online-Backup

Ein Backup, das erstellt wird, wenn sich die Datenbank im Online-Status befindet, wird als Online-Backup bezeichnet. Auch als Hot Backup bezeichnet, ermöglicht ein Online-Backup die Erstellung eines Backups der Datenbank, ohne dass es heruntergefahren werden muss.

Im Rahmen des Online-Backups können Sie eine Sicherung der folgenden Dateien erstellen:

- Nur Datendateien und Kontrolldateien
- Nur Archivprotokolldateien (in diesem Szenario wird die Datenbank nicht in den Backup-Modus versetzt)
- Vollständige Datenbank, die Datendateien, Kontrolldateien und Archivprotokolldateien umfasst

Offline-Backup

Ein Backup, das erstellt wird, wenn sich die Datenbank entweder im gemounteten oder Herunterfahrzustand befindet, wird als Offline-Backup bezeichnet. Ein Offline-Backup wird auch als Cold Backup bezeichnet. Sie können nur Datendateien und Steuerdateien in Offline-Backups einbeziehen. Sie können entweder einen Offline-Mount- oder Offline-Shutdown-Backup erstellen.

- Wenn Sie ein Offline-Mount-Backup erstellen, müssen Sie sicherstellen, dass sich die Datenbank in einem gemounteten Zustand befindet.

Wenn sich die Datenbank in einem anderen Zustand befindet, schlägt der Backup-Vorgang fehl.

- Beim Erstellen einer Offline-Shutdown-Sicherung kann sich die Datenbank in einem beliebigen Zustand befinden.

Der Datenbankstatus wird in den erforderlichen Zustand geändert, um ein Backup zu erstellen. Nach dem Erstellen des Backups wird der Datenbankzustand in den ursprünglichen Zustand zurückgesetzt.

Wie SnapCenter Oracle Datenbanken erkennt

Bei den Ressourcen handelt es sich um Oracle-Datenbanken auf dem Host, die von SnapCenter verwaltet werden. Diese Datenbanken können Ressourcengruppen hinzugefügt werden, um Datensicherungsvorgänge auszuführen, nachdem Sie die verfügbaren Datenbanken ermittelt haben.

In den folgenden Abschnitten wird der Prozess beschrieben, den SnapCenter zur Ermittlung verschiedener Typen und Versionen von Oracle-Datenbanken verwendet.

Für Oracle-Versionen 11g_ bis 12c__R1

RAC-Datenbank

Die RAC-Datenbanken werden nur anhand von `/etc/oratab`-Einträgen ermittelt. Sie sollten die Datenbankeinträge in der Datei `/etc/oratab` haben.

Standalone

Die eigenständigen Datenbanken werden nur anhand von `/etc/oratab`-Einträgen ermittelt.

ASM

Der ASM-Instanzeintrag sollte in der Datei `/etc/oratab` verfügbar sein.

RAC 1-Knoten

Die RAC One Node-Datenbanken werden nur anhand von /etc/oratab-Einträgen ermittelt. Die Datenbanken sollten entweder im nomount-, Mount- oder Open-Zustand sein. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Der RAC One Node Datenbankstatus wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt und Backups mit der Datenbank verknüpft sind.

Wenn die Datenbank verschoben wird, sollten Sie die folgenden Schritte ausführen:

1. Fügen Sie den umgelagerten Datenbankeintrag manuell in der Datei /etc/oratab auf dem Knoten Failed-over RAC hinzu.
2. Aktualisieren Sie die Ressourcen manuell.
3. Wählen Sie auf der Ressourcen-Seite die RAC One Node-Datenbank aus, und klicken Sie dann auf Datenbankeinstellungen.
4. Konfigurieren Sie die Datenbank so, dass die bevorzugten Cluster-Knoten auf den RAC-Knoten eingestellt werden, der derzeit die Datenbank hostet.
5. Führen Sie die SnapCenter Vorgänge aus.
6. Wenn Sie eine Datenbank von einem Knoten auf einen anderen Knoten verschoben haben und der Eintrag Oratab im früheren Knoten nicht gelöscht wird, löschen Sie den Oratab-Eintrag manuell, um zu vermeiden, dass dieselbe Datenbank zweimal angezeigt wird.

Für Oracle Versionen 12cR2 bis 18c

RAC-Datenbank

Die RAC-Datenbanken werden mit dem Befehl srvctl config ermittelt. Sie sollten die Datenbankeinträge in der Datei /etc/oratab haben.

Standalone

Die eigenständigen Datenbanken werden anhand der Einträge in der Datei /etc/oratab und der Ausgabe des Befehls srvctl config ermittelt.

ASM

Der ASM-Instanzeintrag muss sich nicht in der Datei /etc/oratab befinden.

RAC 1-Knoten

Die RAC One Node-Datenbanken werden nur mit dem Befehl srvctl config ermittelt. Die Datenbanken sollten entweder im nomount-, Mount- oder Open-Zustand sein. Der RAC One Node Datenbankstatus wird als umbenannt oder gelöscht markiert, wenn die Datenbank bereits erkannt und Backups mit der Datenbank verknüpft sind.

Wenn die Datenbank verschoben wird, sollten Sie die folgenden Schritte ausführen: . Aktualisieren Sie die Ressourcen manuell. . Wählen Sie auf der Ressourcen-Seite die RAC One Node-Datenbank aus, und klicken Sie dann auf Datenbankeinstellungen. . Konfigurieren Sie die Datenbank so, dass die bevorzugten Cluster-Knoten auf den RAC-Knoten eingestellt werden, der derzeit die Datenbank hostet. . Führen Sie die SnapCenter Vorgänge aus.



Wenn in der Datei /etc/oratab Oracle 12cR2 und 18c-Datenbankeinträge vorhanden sind und dieselbe Datenbank beim Befehl `srvctl config` registriert ist, beseitigt SnapCenter die doppelten Datenbankeinträge. Wenn veraltete Datenbankeinträge vorhanden sind, wird die Datenbank erkannt, die Datenbank ist jedoch nicht erreichbar und der Status ist offline.

Bevorzugte Knoten im RAC-Setup

In Oracle Real Application Clusters (RAC)-Setup können Sie die bevorzugten Knoten angeben, die SnapCenter für die Durchführung des Backup-Vorgangs verwendet. Wenn Sie den bevorzugten Node nicht angeben, weist SnapCenter automatisch einen Node als bevorzugten Node zu und auf diesem Node wird das Backup erstellt.

Die bevorzugten Knoten können einer oder alle Cluster-Knoten sein, wo die RAC-Datenbankinstanzen vorhanden sind. Der Sicherungsvorgang wird nur auf diesen bevorzugten Knoten in der Reihenfolge der Präferenz ausgelöst.

Beispiel

Die RAC-Datenbank `cdbrac` hat drei Instanzen: `Cdbrac1` auf `node1`, `cdbrac2` auf `node2` und `cdbrac3` auf `node3`.

Die Instanzen `node1` und `node2` werden als bevorzugte Nodes konfiguriert, wobei `node2` die erste Präferenz und `node1` als zweite Präferenz. Wenn Sie einen Sicherungsvorgang ausführen, wird in `node2` der erste Vorgang versucht, da er der erste bevorzugte Node ist.

Wenn `node2` nicht in dem Status zum Sichern ist, was aus mehreren Gründen, wie z. B. dem Plug-in-Agent, auf dem Host nicht ausgeführt werden kann, ist die Datenbankinstanz auf dem Host nicht im erforderlichen Zustand für den angegebenen Backup-Typ, Oder die Datenbankinstanz auf `node2` in einer FlexASM-Konfiguration wird nicht von der lokalen ASM-Instanz bereitgestellt; dann wird der Vorgang auf `node1` versucht.

Das `node3` wird nicht für das Backup verwendet, da es sich nicht auf der Liste der bevorzugten Nodes befindet.

Flex ASM-Einrichtung

In einem Flex ASM-Setup werden Leaf-Knoten nicht als bevorzugte Knoten aufgeführt, wenn die Kardinalität kleiner als die Anzahl der Knoten im RAC-Cluster ist. Wenn sich Änderungen an den Flex ASM-Cluster-Knotenrollen ergeben, sollten Sie manuell ermitteln, damit die bevorzugten Nodes aktualisiert werden.

Erforderlicher Datenbankstatus

Die RAC-Datenbankinstanzen auf den bevorzugten Nodes müssen den erforderlichen Status aufweisen, damit das Backup erfolgreich abgeschlossen werden kann:

- Eine der RAC-Datenbankinstanzen in den konfigurierten bevorzugten Knoten muss sich im offenen Zustand befinden, um ein Online-Backup zu erstellen.
- Eine der RAC-Datenbankinstanzen in den konfigurierten bevorzugten Knoten muss sich im Mount-Status befinden, und alle anderen Instanzen, einschließlich anderer bevorzugter Knoten, müssen sich im Mount-Status oder niedriger befinden, um ein Offline-Mount-Backup zu erstellen.
- Instanzen von RAC Datenbanken können in jedem Zustand sein. Sie müssen jedoch die bevorzugten Nodes angeben, um ein Offline-Herunterfahren-Backup zu erstellen.

So katalogisieren Sie Backups mit Oracle Recovery Manager

Sie können die Backups von Oracle-Datenbanken mit Oracle Recovery Manager (RMAN) katalogisieren, um die Backup-Informationen im Oracle RMAN-Repository zu speichern.

Die katalogisierten Backups können später für Wiederherstellungen auf Blockebene oder für zeitpunktgenaue Recovery-Vorgänge in Tablespace verwendet werden. Wenn Sie diese katalogisierten Backups nicht benötigen, können Sie die Kataloginformationen entfernen.

Die Datenbank muss im gemounteten oder höheren Zustand für die Katalogisierung enthalten sein. Sie können Katalogisierung von Daten-Backups, Archivierungs-Log-Backups und vollständigen Backups durchführen. Wenn die Katalogisierung für ein Backup einer Ressourcengruppe mit mehreren Datenbanken aktiviert ist, wird für jede Datenbank eine Katalogisierung durchgeführt. Bei Oracle RAC-Datenbanken wird die Katalogisierung auf dem bevorzugten Knoten durchgeführt, auf dem die Datenbank mindestens gemounted ist.

Wenn Sie Backups einer RAC-Datenbank katalogisieren möchten, stellen Sie sicher, dass für diese Datenbank kein anderer Job ausgeführt wird. Wenn ein anderer Job ausgeführt wird, schlägt der Katalogisierung fehl, anstatt sich in die Warteschlange zu stellen.

Externe Katalogdatenbank

Standardmäßig wird die Kontrolldatei der Zieldatenbank zur Katalogisierung verwendet. Wenn Sie eine externe Katalogdatenbank hinzufügen möchten, können Sie diese konfigurieren, indem Sie die Anmeldeinformationen und den TNS-Namen (Transparent Network Substrat) des externen Katalogs mithilfe des Datenbankeinstellungs-Assistenten von der grafischen Benutzeroberfläche von SnapCenter (GUI) angeben. Sie können die externe Katalogdatenbank auch über die CLI konfigurieren, indem Sie den Befehl `Configure-SmOracleDatabase` mit den Optionen `-OracleRmanCatalogCredentialName` und `-OracleRmanCatalogTnsName` ausführen.

RMAN-Befehl

Wenn Sie die Katalogisierung-Option aktiviert haben und gleichzeitig eine Oracle-Backup-Richtlinie über die SnapCenter-GUI erstellen, werden die Backups über Oracle RMAN als Teil des Backup-Vorgangs katalogisiert. Sie können auch eine verzögerte Katalogisierung von Backups durchführen, indem Sie das ausführen `Catalog-SmBackupWithOracleRMAN` Befehl.

Nach der Katalogisierung der Backups können Sie das ausführen `Get-SmBackupDetails` Befehl zum Abrufen der katalogisierten Backup-Informationen wie dem Tag für katalogisierte Datendateien, dem Katalogpfad der Steuerdatei und den katalogisierten Protokollspeicherorten des Archivs.

Benennungsformat

Wenn der Name der ASM-Festplattengruppe größer oder gleich 16 Zeichen ist, ab SnapCenter 3.0, lautet das für die Datensicherung verwendete Namensformat `SC_HASHCODEofDISKGROUP_DBSID_BACKUPID`. Wenn der Name der Laufwerksgruppe jedoch weniger als 16 Zeichen beträgt, ist das für das Backup verwendete Namensformat `DISKGROUPNAME_DBSID_BACKUPID`, das gleiche Format wie in SnapCenter 2.0.

Die `HASHCODEofDISKGROUP` ist eine automatisch generierte Nummer (2 bis 10 Stellen), die für jede ASM-Laufwerksgruppe eindeutig ist.

Crosscheck-Operationen

Sie können crosschecks durchführen, um veraltete RMAN Repository-Informationen über Backups zu aktualisieren, deren Repository-Datensätze nicht ihrem physischen Status entsprechen. Wenn ein Benutzer zum Beispiel archivierte Protokolle mit einem Betriebssystembefehl von der Festplatte entfernt, zeigt die Steuerdatei immer noch an, dass sich die Protokolle auf der Festplatte befinden, wenn sie sich tatsächlich nicht befinden.

Mit der crosscheck-Operation können Sie die Steuerdatei mit den Informationen aktualisieren. Sie können crosscheck aktivieren, indem Sie den Befehl `set-SmConfigSettings` ausführen und den Wert `TRUE` dem PARAMETER `ENABLE_CROSSCHECK` zuweisen. Der Standardwert ist `FALSE`.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

Kataloginformationen entfernen

Sie können die Kataloginformationen entfernen, indem Sie den Befehl `Uncatalog-SmBackupWithOracleRMAN` ausführen. Sie können die Kataloginformationen nicht mithilfe der SnapCenter-GUI entfernen. Die Informationen eines katalogisierten Backups werden jedoch beim Löschen des Backups oder beim Löschen der mit diesem katalogisierten Backup verknüpften Aufbewahrungs- und Ressourcengruppe entfernt.



Wenn Sie eine Löschung des SnapCenter-Hosts erzwingen, werden die Informationen der mit diesem Host verbundenen katalogisierten Backups nicht entfernt. Sie müssen die Informationen aller katalogisierten Backups für diesen Host entfernen, bevor Sie die Löschung des Hosts erzwingen.

Wenn die Katalogisierung und Entkatalogisieren fehlschlägt, weil die Betriebsdauer den für DEN PARAMETER `ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT` angegebenen Zeitwert überschritten hat, sollten Sie den Wert des Parameters ändern, indem Sie den folgenden Befehl ausführen:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Nachdem Sie den Wert des Parameters geändert haben, starten Sie den SnapCenter-Plug-in-Loader-Dienst (SPL) neu, indem Sie den folgenden Befehl ausführen:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

Die Informationen zu den Parametern, die mit dem Befehl und deren Beschreibungen verwendet werden können, können durch Ausführen von `get-Help Command_Name` abgerufen werden. Alternativ können Sie auf die verweisen "[SnapCenter Software Command Reference Guide](#)".

Vordefinierte Umgebungsvariablen für Backup-spezifische Prescript und Postscript

Mit SnapCenter können Sie die vordefinierten Umgebungsvariablen verwenden, wenn Sie während der Erstellung von Backup-Richtlinien das Prescript und das Postscript ausführen. Diese Funktion wird mit Ausnahme von VMDK für alle Oracle-Konfigurationen unterstützt.

SnapCenter definiert die Werte der Parameter, auf die in der Umgebung, in der die Shell-Skripte ausgeführt werden, direkt zugegriffen werden kann. Bei der Ausführung der Skripte müssen Sie die Werte dieser Parameter nicht manuell angeben.

Unterstützte vordefinierte Umgebungsvariablen für das Erstellen von Backup-Richtlinien

- **SC_JOB_ID** gibt die Job-ID des Vorgangs an.

Beispiel: 256

- **SC_ORACLE_SID** gibt die Systemkennung der Datenbank an.

Wenn der Vorgang mehrere Datenbanken umfasst, enthält der Parameter Datenbanknamen, die per Pipe getrennt sind.

Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

Beispiel: NFSB32 NFSB31

- **SC_HOST** gibt den Hostnamen der Datenbank an.

Bei RAC ist der Hostname der Name des Hosts, auf dem das Backup durchgeführt wird.

Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

Beispiel: scsmohost2.gdl.englobe.netapp.com

- **SC_OS_USER** gibt den Betriebssystembesitzer der Datenbank an.

Die Daten werden als <db1>@<osser1><db2>@<osser2> formatiert.

Beispiel: NFSB31@oracle NFSB32@oracle

- **SC_OS_GROUP** gibt die Betriebssystemgruppe der Datenbank an.

Die Daten werden als <db1>@<osgroup1><db2>@<osgroerp2> formatiert.

Beispiel: NFSB31@Installation von NFSB32@oinstall

- **SC_BACKUP_TYPE** gibt den Sicherungstyp an (online voll, online Daten, Online log, offline Shutdown, offline Mount)

Beispiele:

- Für vollständige Backups: ONLINEFULL
- Backup nur Daten: OnLINEDATA
- Für nur-Protokoll-Sicherung: ONLINELOG

- **SC_BACKUP_NAME** gibt den Namen des Backups an.

Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

Beispiel: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0

LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1 AV@RG2_scspr2417819002_07-20-

2021_12.16.48.9267

- **SC_BACKUP_ID** gibt die Backup-ID an.

Dieser Parameter wird für Anwendungs-Volumes ausgefüllt.

BEISPIEL: DATEN@203 LOG@@205 V/207

- **SC_ORACLE_HOME** gibt den Pfad des Oracle Home-Verzeichnisses an.

Beispiel: NFSB32@/ora01/App/oracle/Produkt/18.1.0/db_1 natürlich
NFSB31@/ora01/App/oracle/Product/18.1.0/db_1

- **SC_BACKUP_RETENTION** gibt den in der Richtlinie definierten Aufbewahrungszeitraum an.

Beispiele:

- Für vollständige Sicherung: Stündliche DATEN@TAGE:3 natürlich LOG@ANZAHL:4
- Nur für On-Demand-Datensicherung: OnDemand Daten@COUNT:2
- Nur für On-Demand-Log-Backup: OnDemand-LOG@COUNT:2

- **SC_RESOURCE_GROUP_NAME** gibt den Namen der Ressourcengruppe an.

Beispiel: RG1

- **SC_BACKUP_POLICY_NAME** gibt den Namen der Backup Policy an.

Beispiel: Backup_Policy

- **SC_AV_NAME** gibt die Namen der Anwendungsvolumes an.

Beispiel: AV1 natürlich AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** gibt die Speicherzuordnung von SVM zu Volume für das Verzeichnis der Datendateien an. Er wird der Name des übergeordneten Volume für luns und qtrees sein.

Die Daten werden als <db1>@<SVM1:Volume1><db2>@<SVM2:Volume2> formatiert.

Beispiele:

- Für 2 Datenbanken in derselben Ressourcengruppe:
NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA
NFSB31@Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
- Für eine einzelne Datenbank mit Datendateien, die über mehrere Volumes verteilt sind:
Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** gibt die Speicherzuordnung von SVM zu Volume für das Log-Dateiverzeichnis an. Er wird der Name des übergeordneten Volume für luns und qtrees sein.

Beispiele:

- Für einzelne Datenbankinstanz: Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
- Für mehrere Datenbankinstanzen: NFSB31@Buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
NFSB32@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO

- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** gibt die Liste der Snapshots an, die den Namen des Speichersystems und den Namen des Volumes enthalten.

Beispiele:

- Für einzelne Datenbankinstanz:
Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07 02.28.26.3973-21-2021_1_1
- Für mehrere Datenbankinstanzen:
NFSB32@@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,Buck:/vol/scspr2417819002_NFS_CDB_2021_07 02.28.26.3973 2021_21_SB1-17002_SB002_SB71_21_SB71BG_07 02.28.26.3973 2021_21_SB002_SB71B2B2BG_07 02.28.26.3973_SB002_SB002_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB002_SB1.01_SB1.01_SB002_SB002_SB1.01_SB002_SB71.01_SB71.01_SB1.01_SB002_SB002_SB1.01_SB1.01_

- **SC_PRIMARY_SNAPSHOT_NAMES** gibt die Namen der primären Snapshots an, die während des Backups erstellt wurden.

Beispiele:

- Für einzelne Datenbankinstanz: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- Für mehrere Datenbankinstanzen: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1 NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- Für Snapshots der Konsistenzgruppe, die 2 Volumes umfassen: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350

- **SC_PRIMARY_MOUNT_POINTS** gibt die Details des Mount-Punkts an, die Teil des Backups sind.

Zu den Details gehört das Verzeichnis, auf dem Volumes angehängt sind und nicht das unmittelbare übergeordnete Objekt der zu sicherenden Datei. Bei einer ASM-Konfiguration ist dies der Name der Laufwerksgruppe.

Die Daten werden als <db1>@<mountpoint1,mountpoint2><db2>@<mountpoint1,mountpoint2> formatiert.

Beispiele:

- Für einzelne Datenbankinstanz: /Mnt/nfsdb3_Data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1
- Für mehrere Datenbankinstanzen:
NFSB31@/mnt/nfsdb31_Data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1
NFSB32@/mnt/nfsdb32_Data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
- FÜR ASM: +DATA2DG,+LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** gibt die Namen der Snapshots an, die während der Sicherung der einzelnen Mount-Punkte erstellt wurden.

Beispiele:

- Für einzelne Datenbank-Instanz: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfb32_Data, RG2_scspr2417819002_07-21-

2021_02.28.26.3973_1:/mnt/nfsb31_log

- Für mehrere Datenbankinstanzen: NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_Data, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb31_Data, RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/b32_nfslog

- **SC_ARCHIVELOGS_LOCATIONS** gibt den Speicherort des Archiv-Log-Verzeichnisses an.

Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Archivprotokolldateien. Wenn die Archivprotokolle an mehreren Orten abgelegt werden, werden alle Speicherorte erfasst. Dazu gehören auch die FRA-Szenarien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

Beispiele:

- Für einzelne Datenbank auf NFS: /Mnt/nfsdb2_log
- Für mehrere Datenbanken auf NFS und für die NFSB31 Datenbank-Archiv-Logs, die in zwei verschiedenen Speicherorten platziert sind: NFSB31@/mnt/nsdb31_log1,/mnt/nfsdb31_log2 natürlich NFSB32@/mnt/nfsdb32_log
- FÜR ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

- **SC_REDO_LOGS_LOCATIONS** gibt den Speicherort des Verzeichnisses der Wiederherstellungsprotokolle an.

Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Redo-Log-Dateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

Beispiele:

- Für einzelne Datenbank auf NFS: /Mnt/nfsdb2_Data/newdb1
- Für mehrere Datenbanken auf NFS: NFSB31@/mnt/nfsdb31_Data/newdb31 NFSB32@/mnt/nfsdb32_Data/newdb32
- FÜR ASM: +LOG2DG/ASMDB2/ONLINELOG

- **SC_CONTROL_FILES_LOCATIONS** gibt den Speicherort des Steuerdateien-Verzeichnisses an.

Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Steuerdateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

Beispiele:

- Für einzelne Datenbank auf NFS: /Mnt/nfsdb2_Data/Fra/newdb1,/mnt/nfsdb2_Data/newdb1
- Für mehrere Datenbanken auf NFS:
NFSB31@/mnt/nfsdb31_Data/Fra/newdb31,/mnt/nfsdb31_Data/newdb31
NFSB32@/mnt/nfsdb32_Data/Fra/newdb32,/mnt/nfsdb32_Data/newdb32
- FÜR ASM: +LOG2DG/ASMDB2/CONTROLFILE

- **SC_DATA_FILES_LOCATIONS"** gibt den Speicherort des Verzeichnisses der Datendateien an.

Die Verzeichnisnamen sind das unmittelbare übergeordnete Element der Datendateien. Wenn Softlinks für das Verzeichnis verwendet werden, wird das gleiche ausgefüllt.

Beispiele:

NFSB32@@Buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21 07
02.28.26.3973 2021 21-
2021_02.28.26.3973_0,Buck:/vol/scsprin2417819002_NFS_CDB_NF32_REDO_2021 21 07
02.28.26.3973_21_SB001.01_SB1-
172_SB002_SB1.01_SB002_SB1.02_SB1.02_SB1.01_SB002_SB1.02_SB1.01_SB1.01_SB1.01_SB002_
SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB1.01_SB002_SB1.01_SB002_SB002_SB002_SB00
BG_SB002_07 02.28.26.3973 2021_SB1.01_SB1.01

Optionen zur Backup-Aufbewahrung

Sie können entweder die Anzahl der Tage festlegen, für die Backup-Kopien aufbewahrt werden sollen, oder die Anzahl der Backup-Kopien angeben, die aufbewahrt werden sollen, bis zu einem ONTAP von maximal 255 Kopien. Beispielsweise muss Ihr Unternehmen unter Umständen Backup-Kopien von 10 Tagen oder 130 Backup-Kopien aufbewahren.

Beim Erstellen einer Richtlinie können Sie die Aufbewahrungsoptionen für den Backup-Typ und den Zeitplantyp angeben.

Wenn Sie die SnapMirror Replizierung einrichten, wird die Aufbewahrungsrichtlinie auf dem Ziel-Volume gespiegelt.

SnapCenter löscht die zurückbehaltenen Backups mit Beschriftungen, die dem Zeitplantyp entsprechen. Wenn der Zeitplantyp für die Ressource oder Ressourcengruppe geändert wurde, verbleiben Backups mit dem alten Etikett des Zeitplantyps möglicherweise weiterhin im System.



Für die langfristige Aufbewahrung von Backup-Kopien sollten Sie SnapVault-Backup verwenden.

Backup-Pläne

Die Sicherungshäufigkeit (Planungstyp) wird in den Richtlinien angegeben. In der Konfiguration der Ressourcengruppe wird ein Backup-Zeitplan angegeben. Der wichtigste Faktor bei der Ermittlung der Backup-Häufigkeit oder des Zeitplans ist die Änderungsrate für die Ressource und die Bedeutung der Daten. Sie können eine stark genutzte Ressource unter Umständen jede Stunde sichern, während Sie selten genutzte Ressourcen einmal am Tag sichern können. Weitere Faktoren sind die Bedeutung der Ressource für Ihr Unternehmen, das Service Level Agreement (SLA) und das Recovery Point Objective (RPO).

Ein SLA definiert das erwartete Service-Level und löst zahlreiche Service-bezogene Probleme, einschließlich Verfügbarkeit und Performance des Service. Ein RPO definiert die Strategie für das Alter der Dateien, die aus dem Backup-Storage wiederhergestellt werden müssen, damit die normalen Vorgänge nach einem Ausfall fortgesetzt werden können. SLA und RPO tragen zur Datensicherungsstrategie bei.

Selbst bei einer stark ausgelasteten Ressource ist es nicht mehr als ein oder zwei Mal pro Tag erforderlich, ein komplettes Backup auszuführen. So könnten beispielsweise regelmäßige Transaktions-Log-Backups ausreichen, um sicherzustellen, dass Sie die Backups haben, die Sie benötigen. Je öfter Sie Ihre Datenbanken sichern, desto weniger Transaktions-Logs benötigt SnapCenter zum Zeitpunkt der Wiederherstellung, was zu

schnelleren Restore-Vorgängen führen kann.

Backup-Zeitpläne haben zwei Teile:

- Sicherungshäufigkeit

Die Backup-Häufigkeit (wie oft Backups durchgeführt werden sollen), die für einige Plug-ins als *Schedule Type* bezeichnet wird, ist Teil einer Richtlinienkonfiguration. Sie können stündlich, täglich, wöchentlich oder monatlich als Sicherungshäufigkeit für die Richtlinie auswählen. Wenn Sie keine dieser Frequenzen auswählen, ist die erstellte Richtlinie eine reine On-Demand-Richtlinie. Sie können auf Richtlinien zugreifen, indem Sie auf **Einstellungen** > **Richtlinien** klicken.

- Backup-Pläne

Backup-Zeitpläne (genau, wann Backups durchgeführt werden sollen) sind Teil der Konfiguration einer Ressourcengruppe. Wenn Sie beispielsweise eine Ressourcengruppe haben, die eine Richtlinie für wöchentliche Backups konfiguriert hat, können Sie den Zeitplan so konfigurieren, dass er jeden Donnerstag um 10:00 Uhr gesichert wird. Sie können auf Ressourcengruppenpläne zugreifen, indem Sie auf **Ressourcen** > **Ressourcengruppen** klicken.

Konventionen bei Backup-Namen

Sie können entweder die standardmäßige Namenskonvention für Snapshot Kopien verwenden oder eine individuelle Namenskonvention verwenden. Die standardmäßige Backup-Namenskonvention fügt einen Zeitstempel zu den Namen von Snapshot Kopien hinzu, der Ihnen hilft, zu identifizieren, wann die Kopien erstellt wurden.

Die Snapshot Kopie verwendet die folgende standardmäßige Namenskonvention:

```
resourcegroupname_hostname_timestamp
```

Sie sollten Ihre Backup-Ressourcengruppen logisch benennen, wie im folgenden Beispiel:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In diesem Beispiel haben die Syntaxelemente folgende Bedeutungen:

- *Dts1* ist der Name der Ressourcengruppe.
- *Mach1x88* ist der Hostname.
- *03-12-2015_23.17.26* ist das Datum und der Zeitstempel.

Alternativ können Sie das Namensformat für die Snapshot-Kopie angeben und Ressourcen oder Ressourcengruppen schützen, indem Sie **Verwenden Sie benutzerdefiniertes Namensformat für die Snapshot-Kopie** wählen. Beispiel: `Custtext_resourcegruppe_Policy_hostname` oder `resourcegruppe_hostname`. Standardmäßig wird dem Namen der Snapshot Kopie das Suffix mit dem Zeitstempel hinzugefügt.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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.