



Datenbanken

NetApp Solutions

NetApp
May 10, 2024

Inhalt

- NetApp Lösungen für Enterprise Database 1
 - Oracle Datenbank 1
 - Microsoft SQL Server 493
 - Open Source-Datenbanken 591
 - SnapCenter für Datenbanken 601
 - Toolkits für DB-Automatisierung 838
 - DB-Sizing-Toolkits 857

NetApp Lösungen für Enterprise Database

Oracle Datenbank

AWS Cloud

TR-4986: Vereinfachte, automatisierte Oracle-Implementierung auf Amazon FSX ONTAP mit iSCSI

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Amazon FSX for NetApp ONTAP ist ein Storage-Service, mit dem Sie vollständig gemanagte NetApp ONTAP-Filesysteme in der AWS-Cloud starten und ausführen können. Es vereint die bekannten Funktionen, Performance, Funktionen und APIs von NetApp-Dateisystemen mit der Agilität, Skalierbarkeit und Einfachheit eines vollständig gemanagten AWS-Service. So können Sie sicher sein, dass Sie den anspruchsvollsten Datenbank-Workload wie Oracle in der AWS Cloud ausführen.

Diese Dokumentation zeigt die vereinfachte Implementierung von Oracle-Datenbanken in einem Amazon FSX ONTAP-Filesystem mithilfe von Ansible-Automatisierung. Die Oracle-Datenbank wird in einer eigenständigen Neustartkonfiguration mit iSCSI-Protokoll für den Datenzugriff und Oracle ASM für das Management von Datenbank-Storage-Laufwerken bereitgestellt. Er bietet auch Informationen zum Backup, zur Wiederherstellung und zum Klonen von Oracle-Datenbanken mithilfe der UI-Lösung von NetApp SnapCenter, um einen Storage-effizienten Datenbankbetrieb in der AWS-Cloud zu ermöglichen.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Automatisierte Implementierung von Oracle-Datenbanken auf dem Dateisystem Amazon FSX ONTAP
- Sicherung und Wiederherstellung von Oracle-Datenbanken auf dem Amazon FSX ONTAP-Dateisystem mit dem NetApp SnapCenter-Tool
- Oracle-Datenbank-Klon für Entwicklung/Test oder andere Anwendungsfälle auf dem Amazon FSX ONTAP Filesystem mit dem NetApp SnapCenter Tool

Zielgruppe

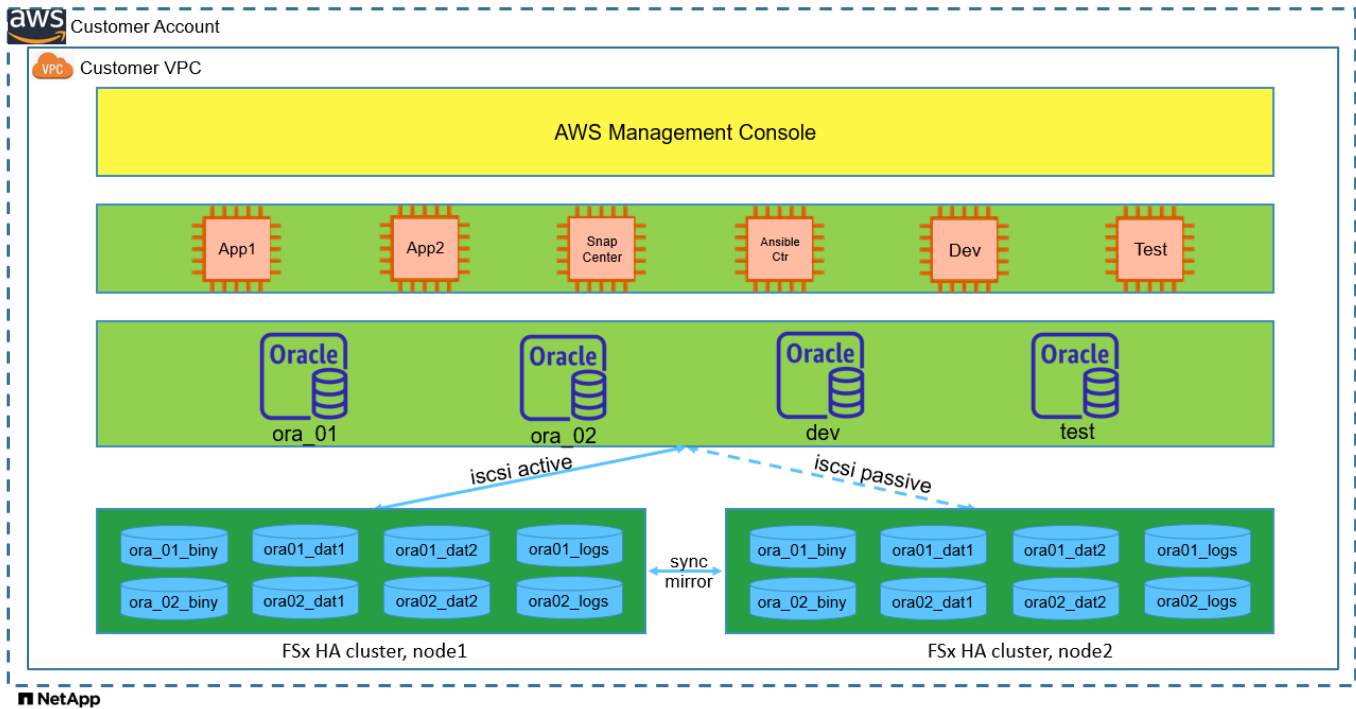
Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle auf Amazon FSX ONTAP Dateisystem implementieren möchte.
- Ein Datenbanklösungsarchitekt, der Oracle-Workloads auf Amazon FSX ONTAP-Filesystemen testen möchte.
- Ein Storage-Administrator, der eine Oracle Datenbank auf dem Amazon FSX ONTAP Filesystem implementieren und managen möchte.
- Einen Anwendungseigentümer, der eine Oracle-Datenbank auf dem Dateisystem Amazon FSX ONTAP einrichten möchte.

Test- und Validierungsumgebung der Lösung

Die Lösung wurde in einer Testumgebung getestet und validiert. Siehe Abschnitt [\[Key Factors for Deployment Consideration\]](#) Finden Sie weitere Informationen.

Simplified, automated Oracle deployment on Amazon FSx ONTAP with iSCSI



Hardware- und Softwarekomponenten

Hardware		
Amazon FSX ONTAP-Storage	Aktuelle Version von AWS angeboten	Ein FSX HA-Cluster in der gleichen VPC und Verfügbarkeitszone
EC2 Instanz für Computing	t2.xlarge/4vCPU/16G	Zwei EC2 T2 xlarge EC2 Instanzen zur gleichzeitigen Implementierung
Software		
Redhat Linux	RHEL-8.6, 4.18.0-372.9.1.el8.x86_64-Kernel	Bereitstellung der RedHat Subscription für Tests
Windows Server	2022 Standard, 10.0.20348 Build 20348	Hosting von SnapCenter-Servern
Oracle Grid Infrastructure	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
SnapCenter Server	Version 4.9P1	Workgroup-Bereitstellung

Öffnen Sie JDK	Version java-1.8.0-openjdk.x86_64	Anforderungen für SnapCenter Plugin auf DB VMs
----------------	-----------------------------------	--

Konfiguration der Oracle-Datenbank in der Laborumgebung

Server	* Datenbank*	DB-Speicher
ora_01	NTAP1(NTAP1_PDB1,NTAP1_PDB2,NTAP1_PDB3)	ISCSI-luns auf Amazon FSX ONTAP-Dateisystem
ora_02	NTAP2(NTAP2_PDB1,NTAP2_PDB2,NTAP2_PDB3)	ISCSI-luns auf Amazon FSX ONTAP-Dateisystem

Wichtige Faktoren für die Implementierung

- **Speicherlayout der Oracle-Datenbank.** in dieser automatisierten Oracle-Bereitstellung stellen wir vier Datenbankvolumes bereit, um Oracle-Binärdaten, -Daten und -Protokolle standardmäßig zu hosten. Eine einzelne lun in einem Volume wird Oracle-Binärdaten zugewiesen. Dann erstellen wir zwei ASM-Festplattengruppen aus Daten und Protokoll-luns. Innerhalb der +DATA asm-Festplattengruppe stellen wir zwei Daten-Volumes mit zwei luns in einem Volumen bereit. Innerhalb der +LOGS asm-Datenträgergruppe erstellen wir zwei luns in einem Logvolumen. Mehrere luns in einem ONTAP Volume bieten im Allgemeinen eine bessere Performance.
- **Implementierung mehrerer DB-Server.** die Automatisierungslösung kann eine Oracle-Container-Datenbank auf mehreren DB-Servern in einem einzelnen Ansible-Playbook bereitstellen. Unabhängig von der Anzahl der DB-Server bleibt die Playbook-Ausführung gleich. Sie können mehrere Container-Datenbanken auf einer einzelnen EC2-Instanz mit unterschiedlichen Datenbankinstanzkennungen (Oracle SID) implementieren. Stellen Sie jedoch sicher, dass auf dem Host ausreichend Speicher zur Unterstützung der bereitgestellten Datenbanken vorhanden ist.
- **ISCSI Konfiguration.** der EC2 Instance Datenbank Server verbindet sich mit FSX Speicher mit dem iSCSI Protokoll. EC2-Instanzen werden normalerweise mit einer einzelnen Netzwerkschnittstelle oder ENI implementiert. Die einzelne NIC-Schnittstelle überträgt sowohl den iSCSI- als auch den Anwendungsdatenverkehr. Es ist wichtig, die Spitzenanforderungen an den I/O-Durchsatz der Oracle-Datenbank abzuschätzen, indem der Oracle AWR-Bericht sorgfältig analysiert wird, um die richtige EC2-Compute-Instanz zu wählen, die sowohl die Anforderungen an den Anwendungs- als auch den iSCSI-Datendurchsatz erfüllt. Zudem beschränkt AWS EC2 jeden TCP-Flow im Allgemeinen auf 5 Gbit/s. Jeder iSCSI-Pfad bietet eine Bandbreite von 5 Gbit/s (625 Mbit/s), und möglicherweise sind mehrere iSCSI-Verbindungen erforderlich, um höhere Durchsatzanforderungen zu unterstützen.
- **Oracle ASM-Redundanzebene, die für jede von Ihnen erstellte Oracle ASM-Datenträgergruppe verwendet werden soll.** Da der Amazon FSX ONTAP HA für den Datenschutz auf Clusterplattenebene aktiviert ist, sollten Sie verwenden `External Redundancy`, Das bedeutet, dass die Option Oracle ASM nicht erlaubt, den Inhalt der Datenträgergruppe zu spiegeln.
- **Datenbanksicherung.** NetApp bietet eine SnapCenter Software Suite für Datenbank-Backup, -Wiederherstellung und -Klonen mit einer benutzerfreundlichen Benutzeroberfläche. NetApp empfiehlt die Implementierung eines solchen Management Tools, damit Snapshot Backups (unter einer Minute), schnelle Datenbank-Restores (in Minuten) und Datenbankklone möglich sind.

Lösungsimplementierung

Die folgenden Abschnitte enthalten schrittweise Verfahren für die automatisierte Bereitstellung und den Schutz von Oracle 19c auf dem Amazon FSX ONTAP-Dateisystem mit direkt gemounteten Datenbank-luns über iSCSI zu EC2-Instanz-VM in einem einzelnen Knoten Starten Sie die Konfiguration mit Oracle ASM als Datenbank-

Volume-Manager neu.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wurde ein AWS Konto eingerichtet, und die erforderlichen VPC und Netzwerksegmente wurden in Ihrem AWS Konto erstellt.
2. Implementieren Sie über die AWS EC2 Konsole EC2 Linux Instanzen als Oracle DB Server. Aktivieren Sie die SSH-Authentifizierung für privaten/öffentlichen Schlüssel für ec2-Benutzer. Details zur Umgebungs-Einrichtung finden Sie im Architekturdiagramm im vorherigen Abschnitt. Sehen Sie sich auch die an ["Benutzerhandbuch für Linux-Instanzen"](#) Finden Sie weitere Informationen.
3. Provisionieren Sie über die AWS FSX-Konsole ein Filesystem von Amazon FSX ONTAP, das die Anforderungen erfüllt. Lesen Sie die Dokumentation ["Erstellen von FSX für ONTAP-Dateisysteme"](#) Schritt-für-Schritt-Anleitungen.
4. Die Schritte 2 und 3 können mit dem folgenden Terraform Automatisierungs-Toolkit durchgeführt werden, das eine EC2-Instanz mit dem Namen erstellt `ora_01` Und ein FSX Dateisystem mit dem Namen `fsx_01`. Überprüfen Sie die Anweisung sorgfältig, und ändern Sie die Variablen vor der Ausführung entsprechend Ihrer Umgebung. Sie können die Vorlage ganz einfach an Ihre eigenen Implementierungsanforderungen anpassen.

```
git clone https://github.com/NetApp-
Automation/na_aws_fsx_ec2_deploy.git
```

5. Stellen Sie eine EC2 Linux-Instanz als Ansible-Controller-Node mit der neuesten Version von Ansible und Git bereit. Details finden Sie unter folgendem Link: ["Erste Schritte mit der Automatisierung von NetApp Lösungen"](#) In Abschnitt -
Setup the Ansible Control Node for CLI deployments on RHEL / CentOS Oder
Setup the Ansible Control Node for CLI deployments on Ubuntu / Debian.
6. Stellen Sie einen Windows-Server bereit, um das UI-Tool NetApp SnapCenter mit der neuesten Version auszuführen. Details finden Sie unter folgendem Link: ["Installieren Sie den SnapCenter-Server"](#)
7. Klonen Sie eine Kopie des NetApp Toolkit zur Implementierungsautomatisierung für iSCSI.

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-
bb/na_oracle_deploy_iscsi.git
```

8. Stellen Sie die folgenden Oracle 19c-Installationsdateien im Verzeichnis EC2-Instanzen `/tmp/Archive` auf.

```
installer_archives:
- "LINUX.X64_193000_grid_home.zip"
- "p34762026_190000_Linux-x86-64.zip"
- "LINUX.X64_193000_db_home.zip"
- "p34765931_190000_Linux-x86-64.zip"
- "p6880880_190000_Linux-x86-64.zip"
```



Stellen Sie sicher, dass Sie mindestens 50G im Oracle VM Root-Volume zugewiesen haben, um ausreichend Speicherplatz für die Erstellung von Oracle Installationsdateien zu haben.

9. Sehen Sie sich das folgende Video an:

[Vereinfachte und automatisierte Oracle-Implementierung auf Amazon FSX ONTAP mit iSCSI](#)

Automatisierungsparameter-Dateien

In dem Playbook „Ansible“ werden die Installations- und Konfigurationsaufgaben von Datenbanken mit vordefinierten Parametern ausgeführt. Für diese Oracle-Automatisierungslösung gibt es drei benutzerdefinierte Parameterdateien, die vor der Ausführung des Playbooks Benutzereingaben erfordern.

- Hosts: Legen Sie Ziele fest, für die das Automatisierungs-Playbook ausgeführt wird.
- vars/vars.yml - die globale Variablendatei, die Variablen definiert, die für alle Ziele gelten.
- Host_VARS/Host_Name.yml - die lokale Variablendatei, die Variablen definiert, die nur auf ein benanntes Ziel angewendet werden. In unserem Anwendungsbeispiel handelt es sich um die Oracle DB-Server.

Zusätzlich zu diesen benutzerdefinierten Variablendateien gibt es mehrere standardmäßige Variablendateien, die Standardparameter enthalten, die nicht geändert werden müssen, sofern dies nicht erforderlich ist. In den folgenden Abschnitten wird die Konfiguration der benutzerdefinierten Variablendateien erläutert.

Konfiguration von Parameterdateien

1. Ansible Ziel hosts Dateikonfiguration:

```
# Enter Amazon FSx ONTAP management IP address
[ontap]
172.16.9.32

# Enter name for ec2 instance (not default IP address naming) to be
# deployed one by one, follow by ec2 instance IP address, and ssh
# private key of ec2-user for the instance.
[oracle]
ora_01 ansible_host=10.61.180.21 ansible_ssh_private_key_file
=ora_01.pem
ora_02 ansible_host=10.61.180.23 ansible_ssh_private_key_file
=ora_02.pem
```

2. Weltweit vars/vars.yml Dateikonfiguration

```
#####
#####
#####          Oracle 19c deployment global user
configurable variables          #####
#####          Consolidate all variables from ONTAP, linux
and oracle          #####
#####
#####
#####          ONTAP env specific config variables
#####
#####
#####
#####
#####
#####
#####          Linux env specific config variables
#####
```

```
# Enter the supported ONTAP platform: on-prem, aws-fsx.
ontap_platform: aws-fsx
```

```
# Enter ONTAP cluster management user credentials
username: "fsxadmin"
password: "xxxxxxxx"
```

```
#####
#####

# Enter RHEL subscription to enable repo
redhat_sub_username: xxxxxxxx
redhat_sub_password: "xxxxxxx"

#####
#####
###           Oracle DB env specific config variables
###
#####
#####

# Enter Database domain name
db_domain: solutions.netapp.com

# Enter initial password for all required Oracle passwords. Change
them after installation.
initial_pwd_all: xxxxxxxx
```

3. Lokaler DB-Server host_vars/host_name.yml Konfiguration wie ora_01.yml, ora_02.yml ...

```
# User configurable Oracle host specific parameters

# Enter container database SID. By default, a container DB is
created with 3 PDBs within the CDB
oracle_sid: NTAP1

# Enter database shared memory size or SGA. CDB is created with SGA
at 75% of memory_limit, MB. The grand total of SGA should not exceed
75% available RAM on node.
memory_limit: 8192
```

Ausführung des Playbook

Das Automatisierungs-Toolkit enthält insgesamt sechs Playbooks. Jede führt unterschiedliche Aufgabenblöcke aus und erfüllt unterschiedliche Zwecke.

```
0-all_playbook.yml - execute playbooks from 1-4 in one playbook run.
1-ansible_requirements.yml - set up Ansible controller with required
libs and collections.
2-linux_config.yml - execute Linux kernel configuration on Oracle DB
servers.
3-ontap_config.yml - configure ONTAP svm/volumes/luns for Oracle
database and grant DB server access to luns.
4-oracle_config.yml - install and configure Oracle on DB servers for
grid infrastructure and create a container database.
5-destroy.yml - optional to undo the environment to dismantle all.
```

Es gibt drei Optionen, um Playbooks mit den folgenden Befehlen auszuführen.

1. Führen Sie alle Playbooks für die Implementierung in einem kombinierten Durchlauf aus.

```
ansible-playbook -i hosts 0-all_playbook.yml -u ec2-user -e
@vars/vars.yml
```

2. Führen Sie Playbooks einzeln mit der Zahlenfolge von 1 bis 4 aus.

```
ansible-playbook -i hosts 1-ansible_requirements.yml -u ec2-user -e
@vars/vars.yml
```

```
ansible-playbook -i hosts 2-linux_config.yml -u ec2-user -e
@vars/vars.yml
```

```
ansible-playbook -i hosts 3-ontap_config.yml -u ec2-user -e
@vars/vars.yml
```

```
ansible-playbook -i hosts 4-oracle_config.yml -u ec2-user -e
@vars/vars.yml
```

3. Führen Sie 0-all_Playbook.yml mit einem Tag aus.

```
ansible-playbook -i hosts 0-all_playbook.yml -u ec2-user -e  
@vars/vars.yml -t ansible_requirements
```

```
ansible-playbook -i hosts 0-all_playbook.yml -u ec2-user -e  
@vars/vars.yml -t linux_config
```

```
ansible-playbook -i hosts 0-all_playbook.yml -u ec2-user -e  
@vars/vars.yml -t ontap_config
```

```
ansible-playbook -i hosts 0-all_playbook.yml -u ec2-user -e  
@vars/vars.yml -t oracle_config
```

4. Die Umgebung rückgängig machen

```
ansible-playbook -i hosts 5-destroy.yml -u ec2-user -e  
@vars/vars.yml
```

Validierung nach der Ausführung

Melden Sie sich nach der Ausführung des Playbooks als oracle-Benutzer beim oracle DB-Server an, um zu überprüfen, ob die Grid-Infrastruktur und die Datenbank von Oracle erfolgreich erstellt wurden. Im Folgenden sehen Sie ein Beispiel für die Validierung von Oracle-Datenbanken auf Host ora_01.

1. Oracle Container-Datenbank auf EC2-Instanz validieren

```
[admin@ansiblect1 na_oracle_deploy_iscsi]$ ssh -i ora_01.pem ec2-
user@172.30.15.40
Last login: Fri Dec  8 17:14:21 2023 from 10.61.180.18
[ec2-user@ip-172-30-15-40 ~]$ uname -a
Linux ip-172-30-15-40.ec2.internal 4.18.0-372.9.1.el8.x86_64 #1 SMP
Fri Apr 15 22:12:19 EDT 2022 x86_64 x86_64 x86_64 GNU/Linux

[ec2-user@ip-172-30-15-40 ~]$ sudo su
[root@ip-172-30-15-40 ec2-user]# su - oracle
Last login: Fri Dec  8 16:25:52 UTC 2023 on pts/0
[oracle@ip-172-30-15-40 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Dec 8 18:18:20 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> select name, open_mode, log_mode from v$database;

NAME          OPEN_MODE          LOG_MODE
-----
NTAP1         READ WRITE        ARCHIVELOG

SQL> show pdbs

          CON_ID CON_NAME          OPEN MODE RESTRICTED
-----
          2 PDB$SEED          READ ONLY NO
          3 NTAP1_PDB1          READ WRITE NO
          4 NTAP1_PDB2          READ WRITE NO
          5 NTAP1_PDB3          READ WRITE NO

SQL> select name from v$datafile;

NAME
```

```
-----  
+DATA/NTAP1/DATAFILE/system.257.1155055419  
+DATA/NTAP1/DATAFILE/sysaux.258.1155055463  
+DATA/NTAP1/DATAFILE/undotbs1.259.1155055489  
+DATA/NTAP1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/system.266.115  
5056241  
+DATA/NTAP1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/sysaux.267.115  
5056241  
+DATA/NTAP1/DATAFILE/users.260.1155055489  
+DATA/NTAP1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/undotbs1.268.1  
155056241  
+DATA/NTAP1/0C03AAFA7C6FD2E5E063280F1EACFBE0/DATAFILE/system.272.115  
5057059  
+DATA/NTAP1/0C03AAFA7C6FD2E5E063280F1EACFBE0/DATAFILE/sysaux.273.115  
5057059  
+DATA/NTAP1/0C03AAFA7C6FD2E5E063280F1EACFBE0/DATAFILE/undotbs1.271.1  
155057059  
+DATA/NTAP1/0C03AAFA7C6FD2E5E063280F1EACFBE0/DATAFILE/users.275.1155  
057075
```

NAME

```
-----  
+DATA/NTAP1/0C03AC0089ACD352E063280F1EAC12BD/DATAFILE/system.277.115  
5057075  
+DATA/NTAP1/0C03AC0089ACD352E063280F1EAC12BD/DATAFILE/sysaux.278.115  
5057075  
+DATA/NTAP1/0C03AC0089ACD352E063280F1EAC12BD/DATAFILE/undotbs1.276.1  
155057075  
+DATA/NTAP1/0C03AC0089ACD352E063280F1EAC12BD/DATAFILE/users.280.1155  
057091  
+DATA/NTAP1/0C03ACEABA54D386E063280F1EACE573/DATAFILE/system.282.115  
5057091  
+DATA/NTAP1/0C03ACEABA54D386E063280F1EACE573/DATAFILE/sysaux.283.115  
5057091  
+DATA/NTAP1/0C03ACEABA54D386E063280F1EACE573/DATAFILE/undotbs1.281.1  
155057091  
+DATA/NTAP1/0C03ACEABA54D386E063280F1EACE573/DATAFILE/users.285.1155  
057105
```

19 rows selected.

```
SQL> select name from v$controlfile;
```

NAME

```
-----  
+DATA/NTAP1/CONTROLFILE/current.261.1155055529  
+LOGS/NTAP1/CONTROLFILE/current.256.1155055529
```

```
SQL> select member from v$logfile;
```

```
MEMBER  
-----
```

```
-----  
+DATA/NTAP1/ONLINELOG/group_3.264.1155055531  
+LOGS/NTAP1/ONLINELOG/group_3.259.1155055539  
+DATA/NTAP1/ONLINELOG/group_2.263.1155055531  
+LOGS/NTAP1/ONLINELOG/group_2.257.1155055539  
+DATA/NTAP1/ONLINELOG/group_1.262.1155055531  
+LOGS/NTAP1/ONLINELOG/group_1.258.1155055539
```

```
6 rows selected.
```

```
SQL> exit
```

```
Disconnected from Oracle Database 19c Enterprise Edition Release  
19.0.0.0.0 - Production  
Version 19.18.0.0.0
```

2. Oracle Listener validieren

```
[oracle@ip-172-30-15-40 ~]$ lsnrctl status listener
```

```
LSNRCTL for Linux: Version 19.0.0.0.0 - Production on 08-DEC-2023  
18:20:24
```

```
Copyright (c) 1991, 2022, Oracle. All rights reserved.
```

```
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=ip-172-30-  
15-40.ec2.internal) (PORT=1521)))
```

```
STATUS of the LISTENER
```

```
-----  
Alias                LISTENER  
Version              TNSLSNR for Linux: Version 19.0.0.0.0 -  
Production  
Start Date           08-DEC-2023 16:26:09  
Uptime                0 days 1 hr. 54 min. 14 sec  
Trace Level          off  
Security              ON: Local OS Authentication  
SNMP                  OFF  
Listener Parameter File
```

```

/u01/app/oracle/product/19.0.0/grid/network/admin/listener.ora
Listener Log File          /u01/app/oracle/diag/tnslsnr/ip-172-30-15-
40/listener/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=ip-172-30-15-
40.ec2.internal) (PORT=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc) (KEY=EXTPROC1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcps) (HOST=ip-172-30-15-
40.ec2.internal) (PORT=5500)) (Security=(my_wallet_directory=/u01/app/
oracle/product/19.0.0/NTAP1/admin/NTAP1/xdb_wallet)) (Presentation=HT
TP) (Session=RAW))
Services Summary...
Service "+ASM" has 1 instance(s).
  Instance "+ASM", status READY, has 1 handler(s) for this
service...
Service "+ASM_DATA" has 1 instance(s).
  Instance "+ASM", status READY, has 1 handler(s) for this
service...
Service "+ASM_LOGS" has 1 instance(s).
  Instance "+ASM", status READY, has 1 handler(s) for this
service...
Service "0c03aafa7c6fd2e5e063280f1eacfb0.solutions.netapp.com" has
1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "0c03ac0089acd352e063280f1eac12bd.solutions.netapp.com" has
1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "0c03aceaba54d386e063280f1eace573.solutions.netapp.com" has
1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "NTAP1.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "NTAP1XDB.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "ntap1_pdb1.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "ntap1_pdb2.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "ntap1_pdb3.solutions.netapp.com" has 1 instance(s).

```

Instance "NTAP1", status READY, has 1 handler(s) for this service...

The command completed successfully

3. Die Grid-Infrastruktur und die erstellten Ressourcen validieren

```
[oracle@ip-172-30-15-40 ~]$ asm
[oracle@ip-172-30-15-40 ~]$ crsctl check has
CRS-4638: Oracle High Availability Services is online
[oracle@ip-172-30-15-40 ~]$ crsctl stat res -t
-----
-----
Name          Target  State          Server          State
details
-----
-----
Local Resources
-----
-----
ora.DATA.dg          ONLINE  ONLINE         ip-172-30-15-40  STABLE
ora.LISTENER.lsnr    ONLINE  ONLINE         ip-172-30-15-40  STABLE
ora.LOGS.dg          ONLINE  ONLINE         ip-172-30-15-40  STABLE
ora.asm              ONLINE  ONLINE         ip-172-30-15-40  Started,STABLE
ora.ons              OFFLINE  OFFLINE        ip-172-30-15-40  STABLE
-----
-----
Cluster Resources
-----
-----
ora.cssd
  1          ONLINE  ONLINE         ip-172-30-15-40  STABLE
ora.diskmon
  1          OFFLINE OFFLINE        ip-172-30-15-40  STABLE
ora.driver.afd
  1          ONLINE  ONLINE         ip-172-30-15-40  STABLE
ora.evmd
  1          ONLINE  ONLINE         ip-172-30-15-40  STABLE
ora.ntap1.db
  1          ONLINE  ONLINE         ip-172-30-15-40
```

```
Open,HOME=/u01/app/o
```

```
racle/product/19.0.0
```

```
/NTAP1, STABLE
```

```
-----  
-----
```

4. Validierung von Oracle ASM.

```
[oracle@ip-172-30-15-40 ~]$ asmcmd  
ASMCMD> lsdg  
State      Type      Rebal  Sector  Logical_Sector  Block      AU  
Total_MB  Free_MB  Req_mir_free_MB  Usable_file_MB  Offline_disks  
Voting_files  Name  
MOUNTED  EXTERN  N      512     512     4096    4194304  
163840   155376      0      155376  
N  DATA/  
MOUNTED  EXTERN  N      512     512     4096    4194304  
81920    80972      0      80972  
N  LOGS/  
ASMCMDB> lsdsk  
Path  
AFD:ORA_01_DAT1_01  
AFD:ORA_01_DAT1_03  
AFD:ORA_01_DAT2_02  
AFD:ORA_01_DAT2_04  
AFD:ORA_01_LOGS_01  
AFD:ORA_01_LOGS_02  
ASMCMDB> afd_state  
ASMCMDB-9526: The AFD state is 'LOADED' and filtering is 'ENABLED' on  
host 'ip-172-30-15-40.ec2.internal'  
ASMCMDB> exit
```

5. Melden Sie sich bei Oracle Enterprise Manager Express an, um die Datenbank zu validieren.

Not secure | <https://172.30.15.40:5500/em/login>

ORACLE ENTERPRISE MANAGER DATABASE EXPRESS

Username

Password

Container Name

[Log in](#)

ORACLE

Copyright 2013, 2020, Oracle and/or its affiliates. All rights reserved.

Not secure | <https://172.30.15.40:5500/em/shell>

ORACLE Enterprise Manager Database Express

NTAP1 (19.18.0.0.0) Performance Storage

Database Home

Time Zone: Browser (GMT-00:00) 1 min Auto-Refresh Refresh

Status

Up Time 1 hours, 21 minutes, 12 seconds

Type **Single Instance (NTAP1)**

CDB (3 PDB(s))

Version 19.18.0.0.0 Enterprise Edition

Platform Name Linux x86 64-bit

Thread 1

Archiver Started

Last Backup Time N/A

Incident(s) 5

Performance

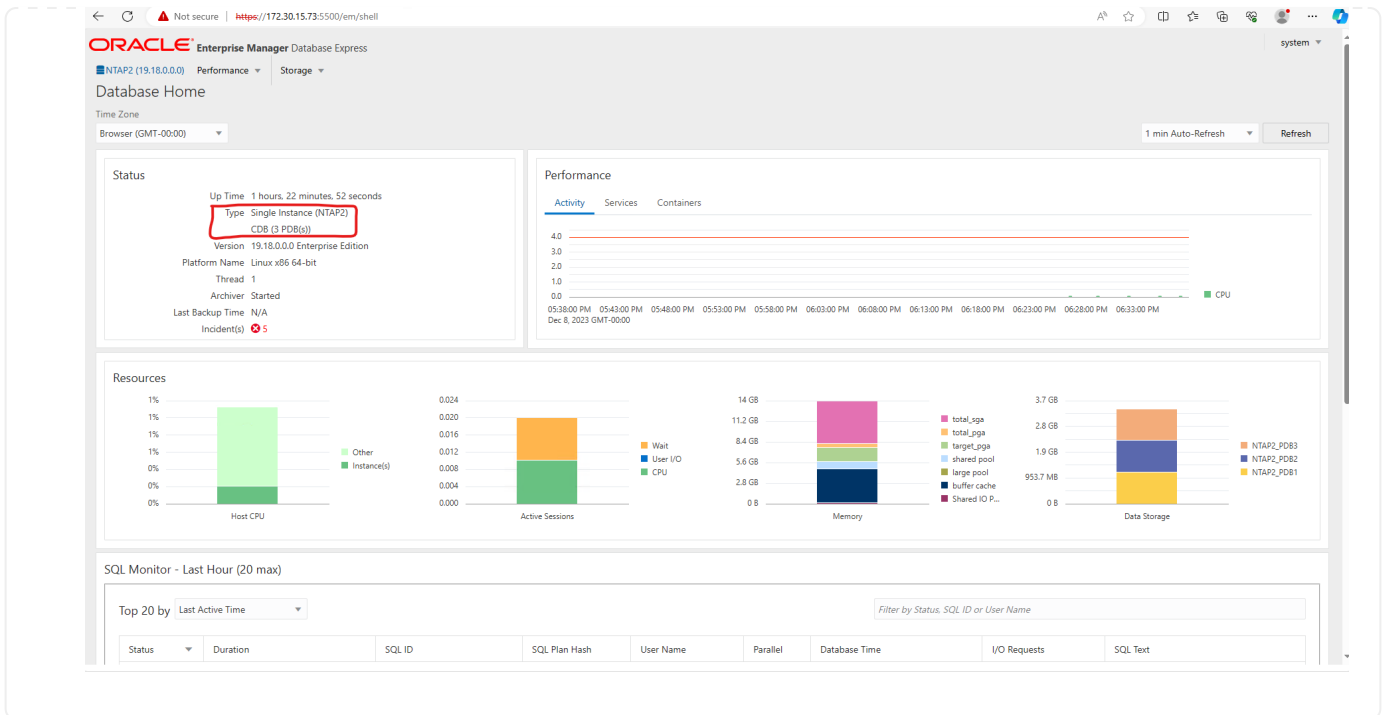
Activity Services Containers

Resources

SQL Monitor - Last Hour (20 max)

Top 20 by Last Active Time Filter by Status: SQL ID or User Name

Status	Duration	SQL ID	SQL Plan Hash	User Name	Parallel	Database Time	I/O Requests	SQL Text
--------	----------	--------	---------------	-----------	----------	---------------	--------------	----------



Backup, Wiederherstellung und Klonen von Oracle mit SnapCenter

Siehe TR-4979 "[Vereinfachtes, automatisiertes Oracle in VMware Cloud on AWS mit Gast-Mounted FSX ONTAP](#)" Abschnitt Oracle backup, restore, and clone with SnapCenter Bietet Details zur Einrichtung von SnapCenter und zur Ausführung von Datenbank-Backup-, Wiederherstellungs- und Klon-Workflows.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- Amazon FSX für NetApp ONTAP

["https://aws.amazon.com/fsx/netapp-ontap/"](https://aws.amazon.com/fsx/netapp-ontap/)

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

- Installieren der Oracle Grid-Infrastruktur für einen eigenständigen Server mit einer neuen Datenbankinstallation

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3)

- Installieren und Konfigurieren von Oracle Database mithilfe von Antwortdateien

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7)

- Verwenden Sie Red hat Enterprise Linux 8.2 mit ONTAP

["https://docs.netapp.com/us-en/ontap-sanhost/hu_rhel_82.html#all-san-array-configurations"](https://docs.netapp.com/us-en/ontap-sanhost/hu_rhel_82.html#all-san-array-configurations)

TR-4979: Vereinfachtes, selbstverwaltetes Oracle in VMware Cloud on AWS mit Gast-Mounted FSX ONTAP

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Unternehmen nutzen bereits seit Jahrzehnten Oracle auf VMware in privaten Datacentern. VMware Cloud (VMC) für AWS stellt eine Push-Button-Lösung bereit, um die softwaredefinierte Datacenter-Software (SDDC) der Enterprise-Klasse von VMware in die dedizierte, flexible Bare-Metal-Infrastruktur der AWS Cloud zu integrieren. AWS FSX ONTAP bietet Premium-Speicher für VMC SDDC und eine Data Fabric, mit der Kunden geschäftskritische Anwendungen wie Oracle in privaten, öffentlichen und hybriden Cloud-Umgebungen auf vSphere®-Basis mit optimiertem Zugriff auf AWS-Services ausführen können. Unabhängig davon, ob es sich um einen vorhandenen oder neuen Oracle-Workload handelt, bietet VMC on AWS eine vertraute, vereinfachte und selbst gemanagte Oracle-Umgebung auf VMware mit allen Vorteilen der AWS-Cloud und ermöglicht gleichzeitig das gesamte Plattformmanagement und die Optimierung auf VMware.

In dieser Dokumentation wird die Bereitstellung und der Schutz einer Oracle-Datenbank in einer VMC-Umgebung mit Amazon FSX ONTAP als primärem Datenbank-Storage demonstriert. Die Oracle-Datenbank kann in VMC im FSX Storage als direkte LUNs mit Gastzugriff auf VM oder über NFS bereitgestellte VMware VMDK-Datenspeicher-Festplatten bereitgestellt werden. Der Schwerpunkt dieses technischen Berichts liegt auf der Implementierung der Oracle-Datenbank als direkter, über Gäste eingebauter FSX Storage auf VMs im VMC-Cluster mit dem iSCSI-Protokoll und Oracle ASM. Wir zeigen außerdem, wie das UI-Tool NetApp SnapCenter zum Sichern, Wiederherstellen und Klonen einer Oracle Datenbank für Entwicklungs- und Testzwecke oder andere Anwendungsfälle für den Storage-effizienten Datenbankbetrieb in der VMC auf AWS verwendet wird.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Oracle-Datenbankimplementierung in VMC auf AWS mit Amazon FSX ONTAP als primärem Datenbank-Storage
- Backup und Wiederherstellung von Oracle-Datenbanken in VMC auf AWS mit dem Tool NetApp SnapCenter
- Klon einer Oracle-Datenbank für Entwicklung/Test oder andere Anwendungsfälle in VMC auf AWS mit dem Tool NetApp SnapCenter

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

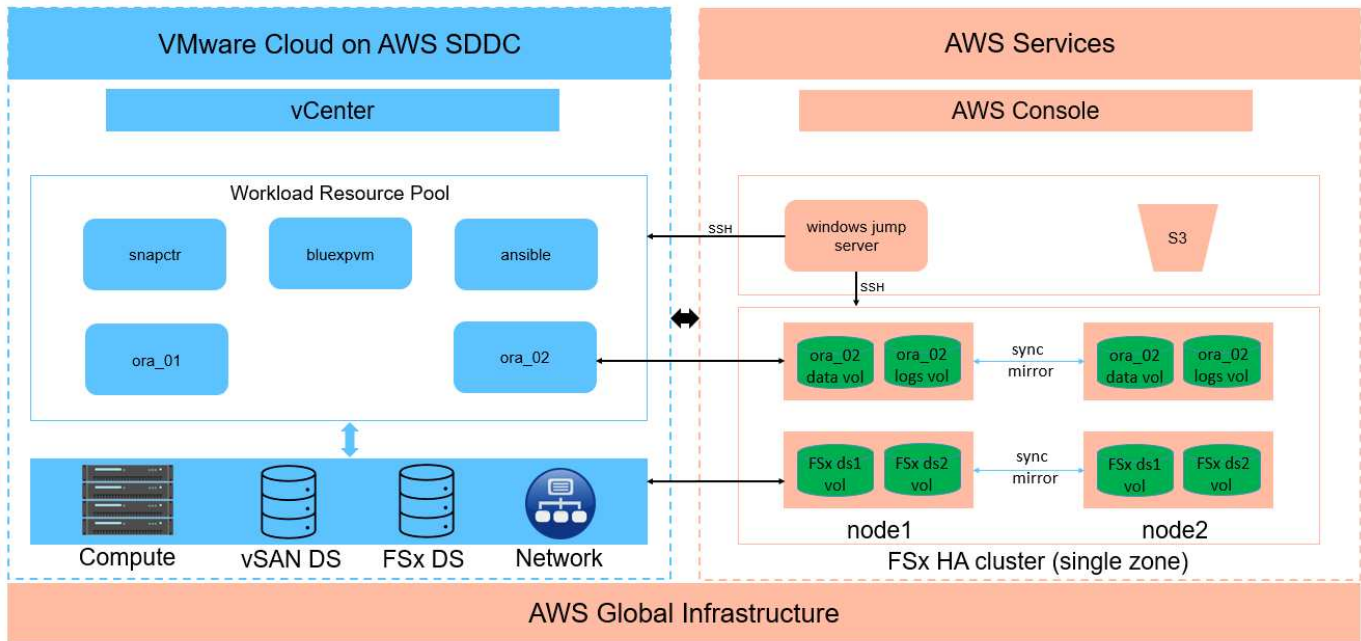
- Ein DBA, der Oracle in VMC auf AWS mit Amazon FSX ONTAP implementieren möchte
- Ein Lösungsarchitekt für Datenbanken, der Oracle-Workloads in VMC in der AWS-Cloud testen möchte
- Ein Storage-Administrator, der eine in VMC auf AWS mit Amazon FSX ONTAP implementierte Oracle-Datenbank implementieren und managen möchte
- Ein Applikationseigentümer, der eine Oracle-Datenbank in VMC in der AWS-Cloud einrichten möchte

Test- und Validierungsumgebung der Lösung

Das Testen und Validieren dieser Lösung wurde in einer Lab-Umgebung mit VMC auf AWS durchgeführt, die möglicherweise nicht mit der endgültigen Implementierungsumgebung übereinstimmt. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind

Oracle Database Deployment in VMware Cloud on AWS SDDC with Amazon FSx ONTAP



NetApp

Hardware- und Softwarekomponenten

Hardware		
FSX ONTAP-Storage	Aktuelle Version von AWS angeboten	Ein FSX ONTAP HA-Cluster in der gleichen VPC und Verfügbarkeitszone wie VMC
VMC SDDC-Cluster	Amazon EC2 i3.Metal Single Node/Intel Xeon E5-2686 CPU, 36 Cores/512 GB RAM	10.37 TB vSAN Storage
Software		
Redhat Linux	RHEL-8.6, 4.18.0-372.9.1.el8.x86_64-Kernel	Bereitstellung der RedHat Subscription für Tests
Windows Server	2022 Standard, 10.0.20348 Build 20348	Hosting von SnapCenter-Servern
Oracle Grid Infrastructure	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet

Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
SnapCenter Server	Version 4.9P1	Workgroup-Bereitstellung
BlueXP Backup und Recovery für VMs	Version 1.0	Bereitgestellt als eine ova vSphere Plugin VM
VMware vSphere	Version 8.0.1.00300	VMware Tools, Version: 11365 - Linux, 12352 - Windows
Öffnen Sie JDK	Version java-1.8.0-openjdk.x86_64	Anforderungen für SnapCenter Plugin auf DB VMs

Konfiguration der Oracle-Datenbank in VMC auf AWS

Server	* Datenbank*	DB-Speicher
ora_01	Cdb1(cdb1_pdb1,cdb1_pdb2,cdb1_pdb3)	VMDK-Datenspeicher auf FSX ONTAP
ora_01	Cdb2(cdb2_pdb)	VMDK-Datenspeicher auf FSX ONTAP
ora_02	Cdb3(cdb3_pdb1,cdb3_pdb2,cdb3_pdb3)	Direkte über Gäste montierte FSX ONTAP
ora_02	Cdb4(cdb4_pdb)	Direkte über Gäste montierte FSX ONTAP

Wichtige Faktoren für die Implementierung

- **FSX zu VMC-Konnektivität.** Wenn Sie Ihr SDDC auf VMware Cloud auf AWS bereitstellen, wird es innerhalb eines AWS-Kontos und einer VPC erstellt, die Ihrer Organisation zugewiesen ist und von VMware verwaltet wird. Sie müssen das SDDC auch mit einem AWS-Konto, dem AWS-Kundenkonto, verbinden. Über diese Verbindung kann Ihr SDDC auf die AWS-Services zugreifen, die zu Ihrem Kundenkonto gehören. FSX for ONTAP ist ein in Ihrem Kundenkonto bereitgestellter AWS-Service. Sobald das VMC SDDC mit Ihrem Kundenkonto verbunden ist, ist FSX Storage für die VMs im VMC SDDC für direkte Gastmontage verfügbar.
- **FSX Storage HA Cluster Single- oder Multi-Zone-Implementierung.** bei diesen Tests und Validierungen haben wir einen FSX HA-Cluster in einer einzelnen AWS Verfügbarkeitszone implementiert. NetApp empfiehlt außerdem die Implementierung von FSX für NetApp ONTAP und VMware Cloud on AWS in derselben Verfügbarkeitszone, um eine bessere Performance zu erzielen und Datentransfergebühren zwischen Verfügbarkeitszonen zu vermeiden.
- **FSX Storage-Cluster-Sizing.** ein Amazon FSX for ONTAP Storage-Dateisystem bietet bis zu 160,000 RAW SSD IOPS, einen Durchsatz von bis zu 4 Gbit/s und eine maximale Kapazität von 192 tib. Sie können das Cluster jedoch in Bezug auf die bereitgestellten IOPS, den Durchsatz und die Storage-Grenze (mindestens 1,024 gib) dimensionieren, basierend auf Ihren tatsächlichen Anforderungen zum Zeitpunkt der Implementierung. Die Kapazität lässt sich spontan dynamisch anpassen, ohne dass die Applikationsverfügbarkeit beeinträchtigt wird.

- **Oracle Daten- und Protokolllayout.** in unseren Tests und Validierungen haben wir jeweils zwei ASM-Datenträgergruppen für Daten und Logs eingesetzt. Innerhalb der +DATA asm-Festplattengruppe haben wir vier LUNs in einem Daten-Volume bereitgestellt. Innerhalb der +LOGS asm-Datenträgergruppe haben wir zwei LUNs in einem Logvolumen bereitgestellt. Im Allgemeinen bieten mehrere in einem Amazon FSX für ONTAP Volume bereitgestellte LUNs eine bessere Performance.
- **iSCSI-Konfiguration.** die Datenbank-VMs im VMC SDDC verbinden sich mit FSX Speicher mit dem iSCSI-Protokoll. Es ist wichtig, die höchste I/O-Durchsatzanforderung der Oracle-Datenbank zu ermitteln, indem der Oracle AWR-Bericht sorgfältig analysiert wird, um die Anforderungen an den Anwendungs- und iSCSI-Datenverkehr und den Durchsatz zu ermitteln. NetApp empfiehlt außerdem, beiden FSX iSCSI-Endpunkten vier iSCSI-Verbindungen mit einer ordnungsgemäß konfigurierten Multipath-Konfiguration zuzuweisen.
- **Oracle ASM-Redundanzebene, die für jede von Ihnen erstellte Oracle ASM-Datenträgergruppe verwendet werden kann.** Da FSX ONTAP den Speicher bereits auf der FSX-Clusterebene spiegelt, sollten Sie externe Redundanz verwenden, was bedeutet, dass die Option Oracle ASM nicht erlaubt, den Inhalt der Datenträgergruppe zu spiegeln.
- **Datenbanksicherung.** NetApp bietet eine SnapCenter Software Suite für Datenbank-Backup, -Wiederherstellung und -Klonen mit einer benutzerfreundlichen Benutzeroberfläche. NetApp empfiehlt die Implementierung eines solchen Management Tools, damit Snapshot Backups (unter einer Minute), schnelle Datenbank-Restores (in Minuten) und Datenbankklone möglich sind.

Lösungsimplementierung

Die folgenden Abschnitte enthalten Schritt-für-Schritt-Verfahren für die Implementierung von Oracle 19c in VMC auf AWS mit direkt eingebautem FSX ONTAP-Storage auf DB-VM in einem einzelnen Knoten Neustarten der Konfiguration mit Oracle ASM als Datenbank-Volume-Manager.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wurde ein softwaredefiniertes Datacenter (SDDC) erstellt, das VMware Cloud auf AWS nutzt. Eine detaillierte Anleitung zum Erstellen eines SDDC in VMC finden Sie in der VMware-Dokumentation ["Erste Schritte mit VMware Cloud on AWS"](#)
2. Es wurde ein AWS Konto eingerichtet, und die erforderlichen VPC und Netzwerksegmente wurden in Ihrem AWS Konto erstellt. Das AWS Konto ist mit Ihrem VMC SDDC verknüpft.
3. Implementieren Sie über die AWS EC2 Konsole einen Amazon FSX for ONTAP Storage HA-Cluster, um die Oracle Database Volumes zu hosten. Wenn Sie mit der Bereitstellung von FSX-Speicher nicht vertraut sind, lesen Sie die Dokumentation ["Erstellen von FSX für ONTAP-Datensysteme"](#) Schritt-für-Schritt-Anleitungen.
4. Der oben genannte Schritt kann mit dem folgenden Terraform Automatisierungs-Toolkit durchgeführt werden, das eine EC2-Instanz als Jump-Host für SDDC beim VMC-Zugriff über SSH und ein FSX Filesystem erstellt. Lesen Sie die Anweisungen sorgfältig durch, und ändern Sie die Variablen vor der Ausführung entsprechend Ihrer Umgebung.

```
git clone https://github.com/NetApp-  
Automation/na_aws_fsx_ec2_deploy.git
```

5. Erstellen Sie VMs im VMware SDDC auf AWS, um Ihre Oracle-Umgebung zu hosten und in VMC bereitzustellen. In unserer Demonstration haben wir zwei Linux VMs als Oracle DB Server, einen Windows Server für den SnapCenter Server und einen optionalen Linux-Server als Ansible Controller für die automatisierte Oracle-Installation oder -Konfiguration erstellt, falls gewünscht. Im Folgenden sehen Sie eine Momentaufnahme der Lab-Umgebung für die Lösungsvalidierung.

6. Optional bietet NetApp auch mehrere Automatisierungs-Toolkits zur Ausführung von Oracle-Bereitstellung und -Konfiguration, falls zutreffend. Siehe ["Toolkits für DB-Automatisierung"](#) Finden Sie weitere Informationen.



Stellen Sie sicher, dass Sie mindestens 50G im Oracle VM Root-Volume zugewiesen haben, damit ausreichend Speicherplatz für das Stage von Oracle Installationsdateien zur Verfügung steht.

DB VM-Kernel-Konfiguration

Melden Sie sich bei den bereitgestellten Voraussetzungen als Admin-Benutzer über SSH bei der Oracle VM an und sudo beim Root-Benutzer, um den Linux-Kernel für die Oracle-Installation zu konfigurieren. Oracle-Installationsdateien können in einem AWS S3-Bucket bereitgestellt und in die VM übertragen werden.

1. Erstellen Sie ein Staging-Verzeichnis `/tmp/archive` Und legen Sie die fest `777` Berechtigung.

```
mkdir /tmp/archive
```

```
chmod 777 /tmp/archive
```

2. Laden Sie die Oracle-Binärinstallationsdateien und andere erforderliche rpm-Dateien herunter, und stellen Sie sie auf den bereit `/tmp/archive` Verzeichnis.

Siehe die folgende Liste der Installationsdateien, die in aufgeführt sind `/tmp/archive` Auf der DB VM.

```
[admin@ora_02 ~]$ ls -l /tmp/archive/
total 10539364
-rw-rw-r--. 1 admin admin      19112 Oct  4 17:04 compat-
libcap1-1.10-7.el7.x86_64.rpm
-rw-rw-r--. 1 admin admin    3059705302 Oct  4 17:10
LINUX.X64_193000_db_home.zip
-rw-rw-r--. 1 admin admin    2889184573 Oct  4 17:11
LINUX.X64_193000_grid_home.zip
-rw-rw-r--. 1 admin admin     589145 Oct  4 17:04
netapp_linux_unified_host_utilities-7-1.x86_64.rpm
-rw-rw-r--. 1 admin admin     31828 Oct  4 17:04 oracle-
database-preinstall-19c-1.0-2.el8.x86_64.rpm
-rw-rw-r--. 1 admin admin    2872741741 Oct  4 17:12
p34762026_190000_Linux-x86-64.zip
-rw-rw-r--. 1 admin admin    1843577895 Oct  4 17:13
p34765931_190000_Linux-x86-64.zip
-rw-rw-r--. 1 admin admin    124347218 Oct  4 17:13
p6880880_190000_Linux-x86-64.zip
-rw-rw-r--. 1 admin admin     257136 Oct  4 17:04
policycoreutils-python-utils-2.9-9.el8.noarch.rpm
[admin@ora_02 ~]$
```

3. Installieren Sie Oracle 19c RPM, das die meisten Anforderungen an die Kernel-Konfiguration erfüllt.

```
yum install /tmp/archive/oracle-database-preinstall-19c-1.0-2.el8.x86_64.rpm
```

4. Laden Sie die fehlenden Dateien herunter, und installieren Sie sie `compat-libcap1` Unter Linux 8.

```
yum install /tmp/archive/compat-libcap1-1.10-7.el7.x86_64.rpm
```

5. Laden Sie von NetApp die NetApp Host Utilities herunter und installieren Sie sie.

```
yum install /tmp/archive/netapp_linux_unified_host_utilities-7-1.x86_64.rpm
```

6. Installieren `policycoreutils-python-utils`.

```
yum install /tmp/archive/policycoreutils-python-utils-2.9-9.el8.noarch.rpm
```

7. Installieren Sie Open JDK Version 1.8.

```
yum install java-1.8.0-openjdk.x86_64
```

8. Installieren Sie `iSCSI-Initiator-Utils`.

```
yum install iscsi-initiator-utils
```

9. Installieren Sie `sg3_utils`.

```
yum install sg3_utils
```

10. Installieren Sie `device-Mapper-Multipath`.

```
yum install device-mapper-multipath
```

11. Deaktivieren Sie transparente hugepages im aktuellen System.

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled
```



```
echo never > /sys/kernel/mm/transparent_hugepage/defrag
```

12. Fügen Sie die folgenden Zeilen hinzu `/etc/rc.local` Zu deaktivieren `transparent_hugepage` Nach dem Neustart.

```
vi /etc/rc.local
```

```
# Disable transparent hugepages
if test -f /sys/kernel/mm/transparent_hugepage/enabled;
then
    echo never > /sys/kernel/mm/transparent_hugepage/enabled
fi
if test -f /sys/kernel/mm/transparent_hugepage/defrag;
then
    echo never > /sys/kernel/mm/transparent_hugepage/defrag
fi
```

13. Deaktivieren sie selinux, indem Sie ändern `SELINUX=enforcing` Bis `SELINUX=disabled`. Sie müssen den Host neu starten, damit die Änderung wirksam wird.

```
vi /etc/sysconfig/selinux
```

14. Fügen Sie die folgenden Zeilen zu hinzu `limit.conf` Um die Dateibeschreibungsgrenze und die Stapelgröße festzulegen.

```
vi /etc/security/limits.conf
```

```
*          hard    nofile      65536
*          soft    stack       10240
```

15. Fügen Sie Swap-Speicherplatz zur DB VM hinzu, wenn kein Swap-Speicherplatz mit diesem Befehl konfiguriert ist: ["Wie weisen ich Speicher zu, um durch Verwendung einer Auslagerungsdatei als Auslagerungsspeicher in einer Amazon EC2 Instanz zu arbeiten?"](#) Die genaue Menge des zu addieren Speicherplatzes hängt von der Größe des RAM bis zu 16G ab.
16. Ändern `node.session.timeo.replacement_timeout` Im `iscsi.conf` Konfigurationsdatei von 120 bis 5 Sekunden.

```
vi /etc/iscsi/iscsid.conf
```

17. Aktivieren und starten Sie den iSCSI-Service auf der EC2-Instanz.

```
systemctl enable iscsid
```

```
systemctl start iscsid
```

18. Rufen Sie die iSCSI-Initiatoradresse ab, die für die Datenbank-LUN-Zuordnung verwendet werden soll.

```
cat /etc/iscsi/initiatorname.iscsi
```

19. Fügen Sie die asm-Gruppen für asm-Verwaltungsbenutzer (oracle) hinzu.

```
groupadd asmadmin
```

```
groupadd asmdba
```

```
groupadd asmoper
```

20. Ändern Sie den oracle-Benutzer, um asm-Gruppen als sekundäre Gruppen hinzuzufügen (der oracle-Benutzer sollte nach der RPM-Installation von Oracle vor der Installation erstellt worden sein).

```
usermod -a -G asmadmin oracle
```

```
usermod -a -G asmdba oracle
```

```
usermod -a -G asmoper oracle
```

21. Stoppen und deaktivieren Sie die Linux-Firewall, wenn sie aktiv ist.

```
systemctl stop firewalld
```

```
systemctl disable firewalld
```

22. Aktivieren Sie passwortloses Sudo für Admin-Benutzer durch Entkommentieren # %wheel

ALL=(ALL) NOPASSWD: ALL Zeile in Datei /etc/sudoers. Ändern Sie die Dateiberechtigung, um die Bearbeitung vorzunehmen.

```
chmod 640 /etc/sudoers
```

```
vi /etc/sudoers
```

```
chmod 440 /etc/sudoers
```

23. EC2-Instanz neu booten

Bereitstellung und Zuordnung von FSX ONTAP-LUNs zur DB-VM

Stellen Sie drei Volumes über die Befehlszeile bereit, indem Sie sich beim FSX Cluster als fsxadmin-Benutzer über ssh und FSX Cluster-Management-IP anmelden. Erstellen Sie LUNs innerhalb der Volumes, um die Binärdateien, Daten und Protokolldateien der Oracle-Datenbank zu hosten.

1. Melden Sie sich über SSH als Benutzer von fsxadmin am FSX-Cluster an.

```
ssh fsxadmin@10.49.0.74
```

2. Führen Sie den folgenden Befehl aus, um ein Volume für die Oracle-Binärdatei zu erstellen.

```
vol create -volume ora_02_biny -aggregate aggr1 -size 50G -state  
online -type RW -snapshot-policy none -tiering-policy snapshot-only
```

3. Führen Sie den folgenden Befehl aus, um ein Volume für Oracle-Daten zu erstellen.

```
vol create -volume ora_02_data -aggregate aggr1 -size 100G -state  
online -type RW -snapshot-policy none -tiering-policy snapshot-only
```

4. Führen Sie den folgenden Befehl aus, um ein Volume für Oracle-Protokolle zu erstellen.

```
vol create -volume ora_02_logs -aggregate aggr1 -size 100G -state  
online -type RW -snapshot-policy none -tiering-policy snapshot-only
```

5. Validieren der erstellten Volumes

```
vol show ora*
```

Ausgabe vom Befehl:

```
FsxId0c00cec8dad373fd1::> vol show ora*  
Vserver   Volume           Aggregate      State         Type         Size  
Available Used%  
-----  
nim       ora_02_biny     aggr1         online        RW           50GB  
22.98GB  51%  
nim       ora_02_data     aggr1         online        RW           100GB  
18.53GB  80%  
nim       ora_02_logs     aggr1         online        RW           50GB  
7.98GB   83%
```

6. Erstellen Sie eine binäre LUN innerhalb des Datenbank-Binärsvolumens.

```
lun create -path /vol/ora_02_biny/ora_02_biny_01 -size 40G -ostype linux
```

7. Erstellen Sie Daten-LUNs im Datenbank-Daten-Volumen.

```
lun create -path /vol/ora_02_data/ora_02_data_01 -size 20G -ostype linux
```

```
lun create -path /vol/ora_02_data/ora_02_data_02 -size 20G -ostype linux
```

```
lun create -path /vol/ora_02_data/ora_02_data_03 -size 20G -ostype linux
```

```
lun create -path /vol/ora_02_data/ora_02_data_04 -size 20G -ostype linux
```

8. Erstellen Sie Protokoll-LUNs im Datenbank-Protokoll-Volumen.

```
lun create -path /vol/ora_02_logs/ora_02_logs_01 -size 40G -ostype linux
```

```
lun create -path /vol/ora_02_logs/ora_02_logs_02 -size 40G -ostype linux
```

9. Erstellen Sie eine Initiatorgruppe für die EC2-Instanz, wobei der Initiator aus Schritt 14 der obigen EC2-Kernel-Konfiguration abgerufen wird.

```
igroup create -igroup ora_02 -protocol iscsi -ostype linux  
-initiator iqn.1994-05.com.redhat:f65fed7641c2
```

10. Ordnen Sie die LUNs der oben erstellten Initiatorgruppe zu. Erhöhen Sie die LUN-ID für jede zusätzliche LUN sequenziell.

```

lun map -path /vol/ora_02_biny/ora_02_biny_01 -igroup ora_02
-vserver svm_ora -lun-id 0
lun map -path /vol/ora_02_data/ora_02_data_01 -igroup ora_02
-vserver svm_ora -lun-id 1
lun map -path /vol/ora_02_data/ora_02_data_02 -igroup ora_02
-vserver svm_ora -lun-id 2
lun map -path /vol/ora_02_data/ora_02_data_03 -igroup ora_02
-vserver svm_ora -lun-id 3
lun map -path /vol/ora_02_data/ora_02_data_04 -igroup ora_02
-vserver svm_ora -lun-id 4
lun map -path /vol/ora_02_logs/ora_02_logs_01 -igroup ora_02
-vserver svm_ora -lun-id 5
lun map -path /vol/ora_02_logs/ora_02_logs_02 -igroup ora_02
-vserver svm_ora -lun-id 6

```

11. Überprüfen Sie die LUN-Zuordnung.

```
mapping show
```

Es wird erwartet, dass dies wieder zutrifft:

```

FsxId0c00cec8dad373fd1::> mapping show
(lun mapping show)
Vserver      Path                                          Igroup    LUN ID
Protocol
-----
-----
nim          /vol/ora_02_biny/ora_02_u01_01             ora_02     0
iscsi
nim          /vol/ora_02_data/ora_02_u02_01             ora_02     1
iscsi
nim          /vol/ora_02_data/ora_02_u02_02             ora_02     2
iscsi
nim          /vol/ora_02_data/ora_02_u02_03             ora_02     3
iscsi
nim          /vol/ora_02_data/ora_02_u02_04             ora_02     4
iscsi
nim          /vol/ora_02_logs/ora_02_u03_01             ora_02     5
iscsi
nim          /vol/ora_02_logs/ora_02_u03_02             ora_02     6
iscsi

```


Importieren und richten Sie nun den FSX ONTAP-Speicher für die Oracle Grid-Infrastruktur und Datenbankinstallation auf der VMC-Datenbank-VM ein.

1. Loggen Sie sich bei der DB VM über SSH als Admin-Benutzer mit Putty vom Windows Jump-Server ein.
2. FSX iSCSI-Endpunkte werden mithilfe einer der beiden SVM iSCSI-IP-Adressen ermittelt. Ändern Sie Ihre umgebungsspezifische Portaladresse.

```
sudo iscsiadm iscsiadm --mode discovery --op update --type  
sendtargets --portal 10.49.0.12
```

3. Erstellen Sie iSCSI-Sitzungen, indem Sie sich bei jedem Ziel anmelden.

```
sudo iscsiadm --mode node -l all
```

Die erwartete Ausgabe des Befehls ist:

```
[ec2-user@ip-172-30-15-58 ~]$ sudo iscsiadm --mode node -l all  
Logging in to [iface: default, target: iqn.1992-  
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3, portal:  
10.49.0.12,3260]  
Logging in to [iface: default, target: iqn.1992-  
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3, portal:  
10.49.0.186,3260]  
Login to [iface: default, target: iqn.1992-  
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3, portal:  
10.49.0.12,3260] successful.  
Login to [iface: default, target: iqn.1992-  
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3, portal:  
10.49.0.186,3260] successful.
```

4. Zeigen Sie eine Liste aktiver iSCSI-Sitzungen an und validieren Sie sie.

```
sudo iscsiadm --mode session
```

Geben Sie die iSCSI-Sitzungen wieder.


```
[ec2-user@ip-172-30-15-58 ~]$ sudo iscsiadm --mode session  
tcp: [1] 10.49.0.186:3260,1028 iqn.1992-  
08.com.netapp:sn.545a38bf06ac11ee8503e395ab90d704:vs.3 (non-flash)  
tcp: [2] 10.49.0.12:3260,1029 iqn.1992-  
08.com.netapp:sn.545a38bf06ac11ee8503e395ab90d704:vs.3 (non-flash)
```

5. Vergewissern Sie sich, dass die LUNs in den Host importiert wurden.

```
sudo sanlun lun show
```

Dadurch wird eine Liste der Oracle LUNs aus FSX zurückgegeben.

```

[admin@ora_02 ~]$ sudo sanlun lun show
controller(7mode/E-Series)/
device          host          lun
vserver(cDOT/FlashRay)  lun-pathname
filename        adapter      protocol  size  product
-----
nim              /vol/ora_02_logs/ora_02_u03_02
/dev/sdo         host34       iSCSI     20g   cDOT
nim              /vol/ora_02_logs/ora_02_u03_01
/dev/sdn         host34       iSCSI     20g   cDOT
nim              /vol/ora_02_data/ora_02_u02_04
/dev/sdm         host34       iSCSI     20g   cDOT
nim              /vol/ora_02_data/ora_02_u02_03
/dev/sdl         host34       iSCSI     20g   cDOT
nim              /vol/ora_02_data/ora_02_u02_02
/dev/sdk         host34       iSCSI     20g   cDOT
nim              /vol/ora_02_data/ora_02_u02_01
/dev/sdj         host34       iSCSI     20g   cDOT
nim              /vol/ora_02_biny/ora_02_u01_01
/dev/sdi         host34       iSCSI     40g   cDOT
nim              /vol/ora_02_logs/ora_02_u03_02
/dev/sdh         host33       iSCSI     20g   cDOT
nim              /vol/ora_02_logs/ora_02_u03_01
/dev/sdg         host33       iSCSI     20g   cDOT
nim              /vol/ora_02_data/ora_02_u02_04
/dev/sdf         host33       iSCSI     20g   cDOT
nim              /vol/ora_02_data/ora_02_u02_03
/dev/sde         host33       iSCSI     20g   cDOT
nim              /vol/ora_02_data/ora_02_u02_02
/dev/sdd         host33       iSCSI     20g   cDOT
nim              /vol/ora_02_data/ora_02_u02_01
/dev/sdc         host33       iSCSI     20g   cDOT
nim              /vol/ora_02_biny/ora_02_u01_01
/dev/sdb         host33       iSCSI     40g   cDOT

```

6. Konfigurieren Sie die `multipath.conf` Datei mit folgenden Standard- und Blacklist-Einträgen.

```
sudo vi /etc/multipath.conf
```

Folgende Einträge hinzufügen:

```

defaults {
    find_multipaths yes
    user_friendly_names yes
}

blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st) [0-9]*"
    devnode "^hd[a-z]"
    devnode "^cciss.*"
}

```

7. Starten Sie den Multipath Service.

```
sudo systemctl start multipathd
```

Jetzt werden Multipath-Geräte in der angezeigt `/dev/mapper` Verzeichnis.

```

[ec2-user@ip-172-30-15-58 ~]$ ls -l /dev/mapper
total 0
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e68512d -> ../dm-0
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685141 -> ../dm-1
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685142 -> ../dm-2
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685143 -> ../dm-3
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685144 -> ../dm-4
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685145 -> ../dm-5
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685146 -> ../dm-6
crw----- 1 root root 10, 236 Mar 21 18:19 control

```

8. Melden Sie sich beim FSX ONTAP-Cluster als Benutzer von fsxadmin über SSH an, um die Seriennummer für jede LUN ab 6c574xxx abzurufen..., die HEX-Nummer beginnt mit 3600a0980, das ist die AWS-Anbieter-ID.

```
lun show -fields serial-hex
```

Und wie folgt zurückkehren:

```
FsxId02ad7bf3476b741df::> lun show -fields serial-hex
vserver path                               serial-hex
-----
svm_ora /vol/ora_02_biny/ora_02_biny_01 6c574235472455534e68512d
svm_ora /vol/ora_02_data/ora_02_data_01 6c574235472455534e685141
svm_ora /vol/ora_02_data/ora_02_data_02 6c574235472455534e685142
svm_ora /vol/ora_02_data/ora_02_data_03 6c574235472455534e685143
svm_ora /vol/ora_02_data/ora_02_data_04 6c574235472455534e685144
svm_ora /vol/ora_02_logs/ora_02_logs_01 6c574235472455534e685145
svm_ora /vol/ora_02_logs/ora_02_logs_02 6c574235472455534e685146
7 entries were displayed.
```

9. Aktualisieren Sie die `/dev/multipath.conf` Datei, um einen benutzerfreundlichen Namen für das Multipath-Gerät hinzuzufügen.

```
sudo vi /etc/multipath.conf
```

Mit folgenden Einträgen:

```

multipaths {
    multipath {
        wwid          3600a09806c574235472455534e68512d
        alias         ora_02_biny_01
    }
    multipath {
        wwid          3600a09806c574235472455534e685141
        alias         ora_02_data_01
    }
    multipath {
        wwid          3600a09806c574235472455534e685142
        alias         ora_02_data_02
    }
    multipath {
        wwid          3600a09806c574235472455534e685143
        alias         ora_02_data_03
    }
    multipath {
        wwid          3600a09806c574235472455534e685144
        alias         ora_02_data_04
    }
    multipath {
        wwid          3600a09806c574235472455534e685145
        alias         ora_02_logs_01
    }
    multipath {
        wwid          3600a09806c574235472455534e685146
        alias         ora_02_logs_02
    }
}

```

10. Starten Sie den Multipath-Dienst neu, um zu überprüfen, ob die Geräte unter `/dev/mapper` Haben sich zu LUN-Namen und zu Serial-Hex-IDs geändert.

```
sudo systemctl restart multipathd
```

Prüfen `/dev/mapper` So kehren Sie wie folgt zurück:

```
[ec2-user@ip-172-30-15-58 ~]$ ls -l /dev/mapper
total 0
crw----- 1 root root 10, 236 Mar 21 18:19 control
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_02_biny_01 -> ../dm-
0
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_02_data_01 -> ../dm-
1
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_02_data_02 -> ../dm-
2
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_02_data_03 -> ../dm-
3
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_02_data_04 -> ../dm-
4
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_02_logs_01 -> ../dm-
5
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_02_logs_02 -> ../dm-
6
```

11. Partitionieren Sie die binäre LUN mit einer einzigen primären Partition.

```
sudo fdisk /dev/mapper/ora_02_biny_01
```

12. Formatieren Sie die partitionierte binäre LUN mit einem XFS-Dateisystem.

```
sudo mkfs.xfs /dev/mapper/ora_02_biny_01p1
```

13. Mounten Sie die binäre LUN in /u01.

```
sudo mkdir /u01
```

```
sudo mount -t xfs /dev/mapper/ora_02_biny_01p1 /u01
```

14. Ändern /u01 Mount Point Ownership für den oracle-Benutzer und die zugehörige primäre Gruppe.

```
sudo chown oracle:oinstall /u01
```

15. Suchen Sie die UUI der binären LUN.

```
sudo blkid /dev/mapper/ora_02_biny_01p1
```

16. Hinzufügen eines Mount-Punkts zu `/etc/fstab`.

```
sudo vi /etc/fstab
```

Fügen Sie die folgende Zeile hinzu.

```
UUID=d89fb1c9-4f89-4de4-b4d9-17754036d11d    /u01    xfs
defaults,nofail 0                2
```

17. Fügen Sie als Root-Benutzer die udev-Regel für Oracle-Geräte hinzu.

```
vi /etc/udev/rules.d/99-oracle-asmdevices.rules
```

Folgende Einträge einbeziehen:

```
ENV{DM_NAME}=="ora*", GROUP:="oinstall", OWNER:="oracle",
MODE:="660"
```

18. Laden Sie als root-Benutzer die udev-Regeln neu.

```
udevadm control --reload-rules
```

19. Lösen Sie als Root-Benutzer die udev-Regeln aus.

```
udevadm trigger
```

20. Laden Sie als root-Benutzer multipathd neu.

```
systemctl restart multipathd
```

21. Booten Sie den EC2-Instanzhost neu.

Installation der Oracle Grid-Infrastruktur

1. Loggen Sie sich als Admin-Benutzer über SSH bei der DB VM ein und aktivieren Sie die Passwort-Authentifizierung durch Entkommentieren `PasswordAuthentication yes` Und dann kommentiert `PasswordAuthentication no`.

```
sudo vi /etc/ssh/sshd_config
```

2. Starten Sie den sshd-Dienst neu.

```
sudo systemctl restart sshd
```

3. Setzen Sie das Oracle-Benutzerpasswort zurück.

```
sudo passwd oracle
```

4. Melden Sie sich als Oracle Restart Software Owner User (oracle) an. Erstellen Sie ein Oracle-Verzeichnis wie folgt:

```
mkdir -p /u01/app/oracle
```

```
mkdir -p /u01/app/oraInventory
```

5. Ändern Sie die Verzeichnisberechtigungseinstellung.

```
chmod -R 775 /u01/app
```

6. Erstellen Sie ein Grid-Home-Verzeichnis, und ändern Sie es.

```
mkdir -p /u01/app/oracle/product/19.0.0/grid
```

```
cd /u01/app/oracle/product/19.0.0/grid
```

7. Entpacken Sie die Grid-Installationsdateien.

```
unzip -q /tmp/archive/LINUX.X64_193000_grid_home.zip
```

8. Löschen Sie von der Startseite des Rasters aus die OPatch Verzeichnis.


```
rm -rf OPatch
```

9. Entpacken Sie die Datei von Grid Home aus `p6880880_190000_Linux-x86-64.zip`.

```
unzip -q /tmp/archive/p6880880_190000_Linux-x86-64.zip
```

10. Von der Startseite des Rasters aus, überarbeiten `cv/admin/cvu_config`, Entkommentieren und ersetzen `CV_ASSUME_DISTID=OEL5` Mit `CV_ASSUME_DISTID=OL7`.

```
vi cv/admin/cvu_config
```

11. Bereiten Sie ein vor `gridsetup.rsp` Datei für die automatische Installation und legen Sie die `rsp`-Datei im ab `/tmp/archive` Verzeichnis. Die `rsp`-Datei sollte die Abschnitte A, B und G mit den folgenden Informationen abdecken:

```
INVENTORY_LOCATION=/u01/app/oraInventory
oracle.install.option=HA_CONFIG
ORACLE_BASE=/u01/app/oracle
oracle.install.asm.OSDBA=asmdba
oracle.install.asm.OSOPER=asmoper
oracle.install.asm.OSASM=asmadmin
oracle.install.asm.SYSASMPassword="SetPWD"
oracle.install.asm.diskGroup.name=DATA
oracle.install.asm.diskGroup.redundancy=EXTERNAL
oracle.install.asm.diskGroup.AUSize=4
oracle.install.asm.diskGroup.disks=/dev/mapper/ora_02_data_01,/dev/mapper/ora_02_data_02,/dev/mapper/ora_02_data_03,/dev/mapper/ora_02_data_04
oracle.install.asm.diskGroup.diskDiscoveryString=/dev/mapper/*
oracle.install.asm.monitorPassword="SetPWD"
oracle.install.asm.configureAFD=true
```

12. Melden Sie sich bei der EC2-Instanz als Root-Benutzer an und legen Sie fest `ORACLE_HOME` Und `ORACLE_BASE`.

```
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/
```

```
export ORACLE_BASE=/tmp
```

```
cd /u01/app/oracle/product/19.0.0/grid/bin
```

13. Initialisieren Sie die Festplattengeräte für die Verwendung mit dem Oracle ASM-Filtertreiber.

```
./asmcmd afd_label DATA01 /dev/mapper/ora_02_data_01 --init
```

```
./asmcmd afd_label DATA02 /dev/mapper/ora_02_data_02 --init
```

```
./asmcmd afd_label DATA03 /dev/mapper/ora_02_data_03 --init
```

```
./asmcmd afd_label DATA04 /dev/mapper/ora_02_data_04 --init
```

```
./asmcmd afd_label LOGS01 /dev/mapper/ora_02_logs_01 --init
```

```
./asmcmd afd_label LOGS02 /dev/mapper/ora_02_logs_02 --init
```

14. Installieren cvuqdisk-1.0.10-1.rpm.

```
rpm -ivh /u01/app/oracle/product/19.0.0/grid/cv/rpm/cvuqdisk-1.0.10-1.rpm
```

15. Nicht Festgelegt \$ORACLE_BASE.

```
unset ORACLE_BASE
```

16. Melden Sie sich als Oracle-Benutzer bei der EC2-Instanz an und extrahieren Sie den Patch in /tmp/archive Ordner.

```
unzip -q /tmp/archive/p34762026_190000_Linux-x86-64.zip -d /tmp/archive
```

17. Starten Sie von Grid Home /u01/App/oracle/Product/19.0.0/GRID aus und als oracle-Benutzer gridSetup.sh Für die Installation der Netzinfrastruktur.

```
./gridSetup.sh -applyRU /tmp/archive/34762026/ -silent  
-responseFile /tmp/archive/gridsetup.rsp
```

18. Führen Sie als root-Benutzer folgende(n) Skript(e) aus:

```
/u01/app/oraInventory/orainstRoot.sh
```

```
/u01/app/oracle/product/19.0.0/grid/root.sh
```

19. Laden Sie als root-Benutzer den multipathd neu.

```
systemctl restart multipathd
```

20. Führen Sie als Oracle-Benutzer den folgenden Befehl aus, um die Konfiguration abzuschließen:

```
/u01/app/oracle/product/19.0.0/grid/gridSetup.sh -executeConfigTools  
-responseFile /tmp/archive/gridsetup.rsp -silent
```

21. Erstellen Sie als Oracle-Benutzer die PROTOKOLLDATENTRÄGER-Gruppe.

```
bin/asmca -silent -sysAsmPassword 'yourPWD' -asmsnmpPassword  
'yourPWD' -createDiskGroup -diskGroupName LOGS -disk 'AFD:LOGS*'  
-redundancy EXTERNAL -au_size 4
```

22. Validieren Sie als Oracle-Benutzer nach der Installation die Grid-Services.

```
bin/crsctl stat res -t
```

```
[oracle@ora_02 grid]$ bin/crsctl stat res -t
```

```
-----  
-----  
Name          Target  State          Server          State  
details  
-----  
-----  
Local Resources  
-----  
-----  
ora.DATA.dg  
          ONLINE  ONLINE          ora_02          STABLE  
ora.LISTENER.lsnr  
          ONLINE  INTERMEDIATE   ora_02          Not All  
Endpoints Re  
gistered, STABLE  
ora.LOGS.dg  
          ONLINE  ONLINE          ora_02          STABLE  
ora.asm  
          ONLINE  ONLINE          ora_02  
Started, STABLE  
ora.ons  
          OFFLINE OFFLINE          ora_02          STABLE  
-----  
-----  
Cluster Resources  
-----  
-----  
ora.cssd  
   1      ONLINE  ONLINE          ora_02          STABLE  
ora.diskmon  
   1      OFFLINE OFFLINE          STABLE  
ora.driver.afd  
   1      ONLINE  ONLINE          ora_02          STABLE  
ora.evmd  
   1      ONLINE  ONLINE          ora_02          STABLE  
-----  
-----
```

23. Überprüfen Sie den Status des ASM-Filtertreibers.

```

[oracle@ora_02 grid]$ export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/grid
[oracle@ora_02 grid]$ export ORACLE_SID=+ASM
[oracle@ora_02 grid]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ora_02 grid]$ asmcmd
ASMCMDS> lsdg
State      Type      Rebal  Sector  Logical_Sector  Block      AU
Total_MB  Free_MB  Req_mir_free_MB  Usable_file_MB  Offline_disks
Voting_files  Name
MOUNTED  EXTERN  N      512     512     4096    4194304
81920    81780      0      81780      0
N  DATA/
MOUNTED  EXTERN  N      512     512     4096    4194304
40960    40852      0      40852      0
N  LOGS/
ASMCMDS> afd_state
ASMCMDS-9526: The AFD state is 'LOADED' and filtering is 'ENABLED' on
host 'ora_02'
ASMCMDS> exit
[oracle@ora_02 grid]$

```

24. Überprüfen Sie den HA-Service-Status.

```

[oracle@ora_02 bin]$ ./crsctl check has
CRS-4638: Oracle High Availability Services is online

```

Installation der Oracle Database

1. Melden Sie sich als Oracle-Benutzer an, und heben Sie die Einstellung auf `$ORACLE_HOME` Und `$ORACLE_SID` Wenn es eingestellt ist.

```
unset ORACLE_HOME
```

```
unset ORACLE_SID
```

2. Erstellen Sie das Oracle DB Home-Verzeichnis, und ändern Sie es in das Verzeichnis.

```
mkdir /u01/app/oracle/product/19.0.0/cdb3
```

```
cd /u01/app/oracle/product/19.0.0/cdb3
```

3. Entpacken Sie die Oracle DB-Installationsdateien.

```
unzip -q /tmp/archive/LINUX.X64_193000_db_home.zip
```

4. Löschen Sie von der DB-Startseite aus die `OPatch` Verzeichnis.

```
rm -rf OPatch
```

5. Entzippen Sie die Datei von DB Home aus `p6880880_190000_Linux-x86-64.zip`.

```
unzip -q /tmp/archive/p6880880_190000_Linux-x86-64.zip
```

6. Überarbeiten Sie von der DB-Startseite aus `cv/admin/cvu_config` Und entkommentieren und ersetzen `CV_ASSUME_DISTID=OEL5` Mit `CV_ASSUME_DISTID=OL7`.

```
vi cv/admin/cvu_config
```

7. Von `/tmp/archive` Das DB 19.18 RU-Patch entpacken.

```
unzip -q /tmp/archive/p34765931_190000_Linux-x86-64.zip -d  
/tmp/archive
```

8. Bereiten Sie die automatische DB-Installationsdatei in vor `/tmp/archive/dbinstall.rsp` Verzeichnis mit folgenden Werten:

```
oracle.install.option=INSTALL_DB_SWONLY
UNIX_GROUP_NAME=oinstall
INVENTORY_LOCATION=/u01/app/oraInventory
ORACLE_HOME=/u01/app/oracle/product/19.0.0/cdb3
ORACLE_BASE=/u01/app/oracle
oracle.install.db.InstallEdition=EE
oracle.install.db.OSDBA_GROUP=dba
oracle.install.db.OSOPER_GROUP=oper
oracle.install.db.OSBACKUPDBA_GROUP=oper
oracle.install.db.OSDGDBA_GROUP=dba
oracle.install.db.OSKMDBA_GROUP=dba
oracle.install.db.OSRACDBA_GROUP=dba
oracle.install.db.rootconfig.executeRootScript=false
```

9. Führen Sie von cdb3 Home /u01/App/oracle/Product/19.0.0/cdb3 aus, und führen Sie die Installation der Datenbank ohne Software aus.

```
./runInstaller -applyRU /tmp/archive/34765931/ -silent
-ignorePrereqFailure -responseFile /tmp/archive/dbinstall.rsp
```

10. Führen Sie als Root-Benutzer den aus `root.sh` Skript nach der reinen Software-Installation.

```
/u01/app/oracle/product/19.0.0/db1/root.sh
```

11. Erstellen Sie als oracle-Benutzer den `dbca.rsp` Datei mit folgenden Einträgen:

```
gdbName=cdb3.demo.netapp.com
sid=cdb3
createAsContainerDatabase=true
numberOfPDBs=3
pdbName=cdb3_pdb
useLocalUndoForPDBs=true
pdbAdminPassword="yourPWD"
templateName=General_Purpose.dbc
sysPassword="yourPWD"
systemPassword="yourPWD"
dbsnmpPassword="yourPWD"
datafileDestination=+DATA
recoveryAreaDestination=+LOGS
storageType=ASM
diskGroupName=DATA
characterSet=AL32UTF8
nationalCharacterSet=AL16UTF16
listeners=LISTENER
databaseType=MULTIPURPOSE
automaticMemoryManagement=false
totalMemory=8192
```

12. Starten Sie als oracle-Benutzer die DB-Erstellung mit dbca.

```
bin/dbca -silent -createDatabase -responseFile /tmp/archive/dbca.rsp
```

Ausgabe:


```

Prepare for db operation
7% complete
Registering database with Oracle Restart
11% complete
Copying database files
33% complete
Creating and starting Oracle instance
35% complete
38% complete
42% complete
45% complete
48% complete
Completing Database Creation
53% complete
55% complete
56% complete
Creating Pluggable Databases
60% complete
64% complete
69% complete
78% complete
Executing Post Configuration Actions
100% complete
Database creation complete. For details check the logfiles at:
  /u01/app/oracle/cfgtoollogs/dbca/cdb3.
Database Information:
Global Database Name:cdb3.vmc.netapp.com
System Identifier(SID):cdb3
Look at the log file "/u01/app/oracle/cfgtoollogs/dbca/cdb3/cdb3.log"
for further details.

```

1. Wiederholen Sie die gleichen Schritte aus Schritt 2, um eine Container-Datenbank cdb4 in einem separaten ORACLE_HOME /u01/App/oracle/Product/19.0.0/cdb4 mit einer einzelnen PDB zu erstellen.
2. Validieren Sie als Oracle-Benutzer Oracle Restart HA-Services nach der DB-Erstellung, dass alle Datenbanken (cdb3, cdb4) mit HA-Diensten registriert sind.

```
/u01/app/oracle/product/19.0.0/grid/crsctl stat res -t
```

Ausgabe:

```
[oracle@ora_02 bin]$ ./crsctl stat res -t
```


Name	Target	State	Server	State
details				

Local Resources				

ora.DATA.dg	ONLINE	ONLINE	ora_02	STABLE
ora.LISTENER.lsnr	ONLINE	INTERMEDIATE	ora_02	Not All
Endpoints Re				
gistered, STABLE				
ora.LOGS.dg	ONLINE	ONLINE	ora_02	STABLE
ora.asm	ONLINE	ONLINE	ora_02	
Started, STABLE				
ora.ons	OFFLINE	OFFLINE	ora_02	STABLE

Cluster Resources				

ora.cdb3.db				
1	ONLINE	ONLINE	ora_02	
Open, HOME=/u01/app/o				
racle/product/19.0.0				
/cdb3, STABLE				
ora.cdb4.db				
1	ONLINE	ONLINE	ora_02	
Open, HOME=/u01/app/o				
racle/product/19.0.0				
/cdb4, STABLE				
ora.cssd				
1	ONLINE	ONLINE	ora_02	STABLE
ora.diskmon				
1	OFFLINE	OFFLINE		STABLE
ora.driver.afd				
1	ONLINE	ONLINE	ora_02	STABLE

```
ora.evmd
      1          ONLINE  ONLINE          ora_02          STABLE
-----
-----
```

3. Legen Sie den Oracle-Benutzer fest `.bash_profile`.

```
vi ~/.bash_profile
```

Folgende Einträge hinzufügen:

```
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db3
export ORACLE_SID=db3
export PATH=$PATH:$ORACLE_HOME/bin
alias asm='export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/grid;export
ORACLE_SID=+ASM;export PATH=$PATH:$ORACLE_HOME/bin'
alias cdb3='export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/cdb3;export
ORACLE_SID=cdb3;export PATH=$PATH:$ORACLE_HOME/bin'
alias cdb4='export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/cdb4;export
ORACLE_SID=cdb4;export PATH=$PATH:$ORACLE_HOME/bin'
```

4. Validieren Sie die für `cdb3` erstellte CDB/PDB.

```
cdb3
```

```
[oracle@ora_02 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Mon Oct 9 08:19:20 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> select name, open_mode from v$database;
```

```

NAME          OPEN_MODE
-----
CDB3          READ WRITE

```

```
SQL> show pdbs
```

```

CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
2 PDB$SEED                                READ ONLY  NO
3 CDB3_PDB1                                READ WRITE NO
4 CDB3_PDB2                                READ WRITE NO
5 CDB3_PDB3                                READ WRITE NO

```

```
SQL>
```

```
SQL> select name from v$datafile;
```

```

NAME
-----
+DATA/CDB3/DATAFILE/system.257.1149420273
+DATA/CDB3/DATAFILE/sysaux.258.1149420317
+DATA/CDB3/DATAFILE/undotbs1.259.1149420343
+DATA/CDB3/86B637B62FE07A65E053F706E80A27CA/DATAFILE/system.266.1149
421085
+DATA/CDB3/86B637B62FE07A65E053F706E80A27CA/DATAFILE/sysaux.267.1149
421085
+DATA/CDB3/DATAFILE/users.260.1149420343
+DATA/CDB3/86B637B62FE07A65E053F706E80A27CA/DATAFILE/undotbs1.268.11
49421085
+DATA/CDB3/06FB206DF15ADEE8E065025056B66295/DATAFILE/system.272.1149
422017
+DATA/CDB3/06FB206DF15ADEE8E065025056B66295/DATAFILE/sysaux.273.1149
422017
+DATA/CDB3/06FB206DF15ADEE8E065025056B66295/DATAFILE/undotbs1.271.11
49422017
+DATA/CDB3/06FB206DF15ADEE8E065025056B66295/DATAFILE/users.275.11494
22033

```

```

NAME
-----
+DATA/CDB3/06FB21766256DF9AE065025056B66295/DATAFILE/system.277.1149
422033
+DATA/CDB3/06FB21766256DF9AE065025056B66295/DATAFILE/sysaux.278.1149
422033

```

```

+DATA/CDB3/06FB21766256DF9AE065025056B66295/DATAFILE/undotbs1.276.11
49422033
+DATA/CDB3/06FB21766256DF9AE065025056B66295/DATAFILE/users.280.11494
22049
+DATA/CDB3/06FB22629AC1DFD7E065025056B66295/DATAFILE/system.282.1149
422049
+DATA/CDB3/06FB22629AC1DFD7E065025056B66295/DATAFILE/sysaux.283.1149
422049
+DATA/CDB3/06FB22629AC1DFD7E065025056B66295/DATAFILE/undotbs1.281.11
49422049
+DATA/CDB3/06FB22629AC1DFD7E065025056B66295/DATAFILE/users.285.11494
22063

```

19 rows selected.

SQL>

5. Validieren Sie die für cdb4 erstellte CDB/PDB.

```

cdb4

```

```

[oracle@ora_02 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Mon Oct 9 08:20:26 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> select name, open_mode from v$databases;

NAME          OPEN_MODE
-----
CDB4          READ WRITE

SQL> show pdbs

          CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----

```

```
2 PDB$SEED          READ ONLY NO
3 CDB4_PDB          READ WRITE NO
```

```
SQL>
```

```
SQL> select name from v$datafile;
```

```
NAME
```

```
-----
-----
+DATA/CDB4/DATAFILE/system.286.1149424943
+DATA/CDB4/DATAFILE/sysaux.287.1149424989
+DATA/CDB4/DATAFILE/undotbs1.288.1149425015
+DATA/CDB4/86B637B62FE07A65E053F706E80A27CA/DATAFILE/system.295.1149
425765
+DATA/CDB4/86B637B62FE07A65E053F706E80A27CA/DATAFILE/sysaux.296.1149
425765
+DATA/CDB4/DATAFILE/users.289.1149425015
+DATA/CDB4/86B637B62FE07A65E053F706E80A27CA/DATAFILE/undotbs1.297.11
49425765
+DATA/CDB4/06FC3070D5E12C23E065025056B66295/DATAFILE/system.301.1149
426581
+DATA/CDB4/06FC3070D5E12C23E065025056B66295/DATAFILE/sysaux.302.1149
426581
+DATA/CDB4/06FC3070D5E12C23E065025056B66295/DATAFILE/undotbs1.300.11
49426581
+DATA/CDB4/06FC3070D5E12C23E065025056B66295/DATAFILE/users.304.11494
26597
```

```
11 rows selected.
```

6. Melden Sie sich bei jeder cdb als sysdba mit sqlplus an und stellen Sie die Größe des DB-Wiederherstellungsziels auf die Größe der +LOGS-Datenträgergruppe für beide cdb's ein.

```
alter system set db_recovery_file_dest_size = 40G scope=both;
```

7. Melden Sie sich bei jeder cdb als sysdba mit sqlplus an und aktivieren Sie den Archivprotokollmodus mit folgenden Befehlssätzen nacheinander.

```
sqlplus /as sysdba
```

```
shutdown immediate;
```

```
startup mount;
```

```
alter database archivelog;
```

```
alter database open;
```

Damit ist die Neustartbereitstellung auf einem Amazon FSX für ONTAP-Speicher und einer VMC DB-VM für Oracle 19c Version 19.18 abgeschlossen. Falls gewünscht, empfiehlt NetApp, die Oracle Steuerdatei und die Online-Protokolldateien in die +LOGS-Datenträgergruppe zu verschieben.

Backup, Wiederherstellung und Klonen von Oracle mit SnapCenter

SnapCenter-Einrichtung

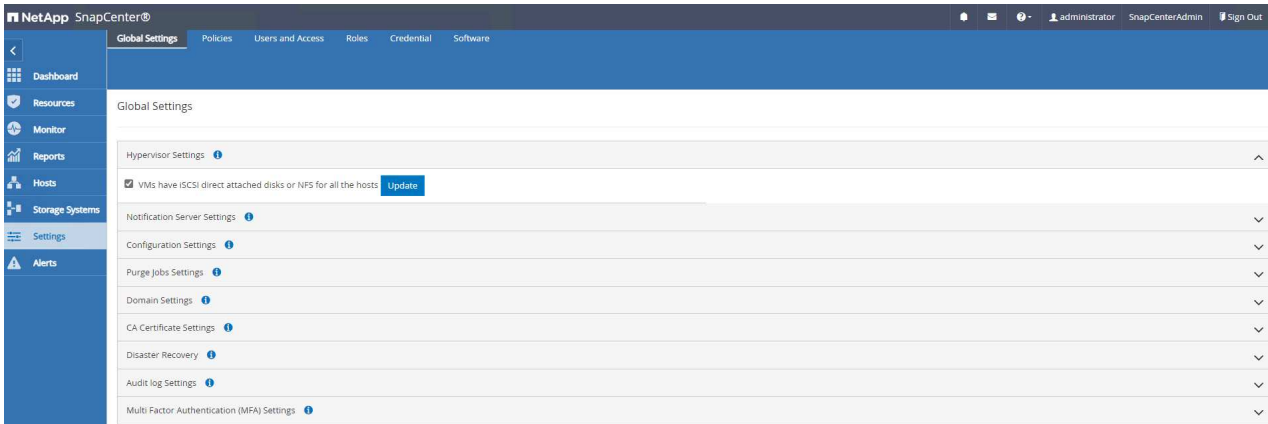
SnapCenter setzt auf ein Host-seitiges Plug-in für Datenbank-VM, um applikationsorientierte Management-Aktivitäten für die Datensicherung durchzuführen. Detaillierte Informationen zu NetApp SnapCenter Plug-in für Oracle finden Sie in dieser Dokumentation "[Welche Möglichkeiten bietet das Plug-in für Oracle Database](#)". Im Folgenden finden Sie allgemeine Schritte zur Einrichtung von SnapCenter für Oracle-Datenbank-Backup, -Recovery und -Klonen.

1. Laden Sie die aktuelle Version der SnapCenter Software von der NetApp Support-Website herunter: "[NetApp Support-Downloads](#)".
2. Installieren Sie als Administrator das neueste java JDK von "[Holen Sie sich Java für Desktop-Anwendungen](#)" Auf Windows-Host des SnapCenter-Servers.

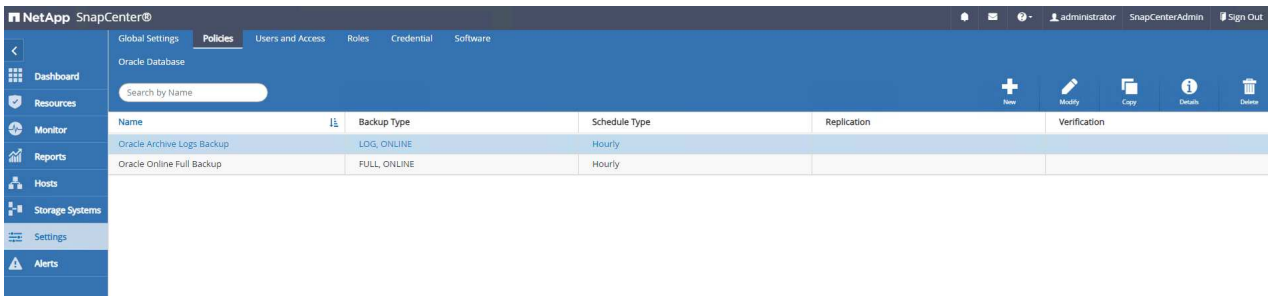


Wenn Windows-Server in einer Domänenumgebung bereitgestellt wird, fügen Sie der lokalen Administratorgruppe des SnapCenter-Servers einen Domänenbenutzer hinzu, und führen Sie die SnapCenter-Installation mit dem Domänenbenutzer aus.

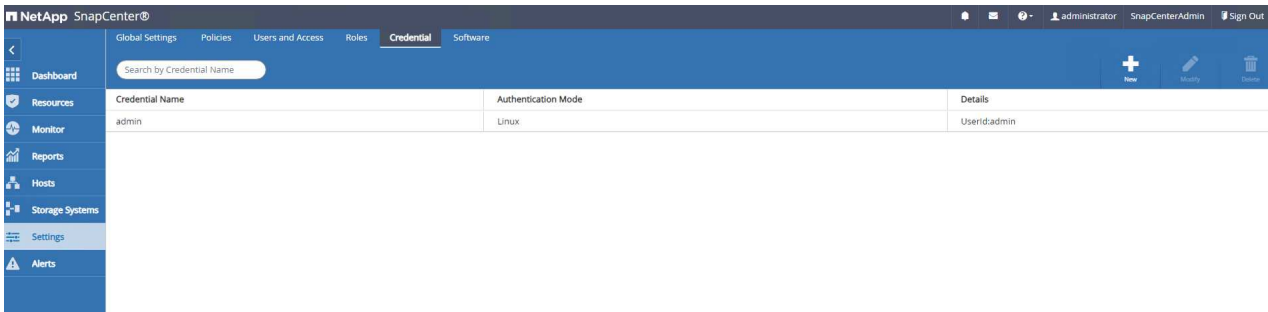
3. Melden Sie sich bei der SnapCenter-Benutzeroberfläche über HTTPS-Port 8846 als Installationsbenutzer an, um SnapCenter für Oracle zu konfigurieren.
4. Aktualisierung Hypervisor Settings In globalen Einstellungen.



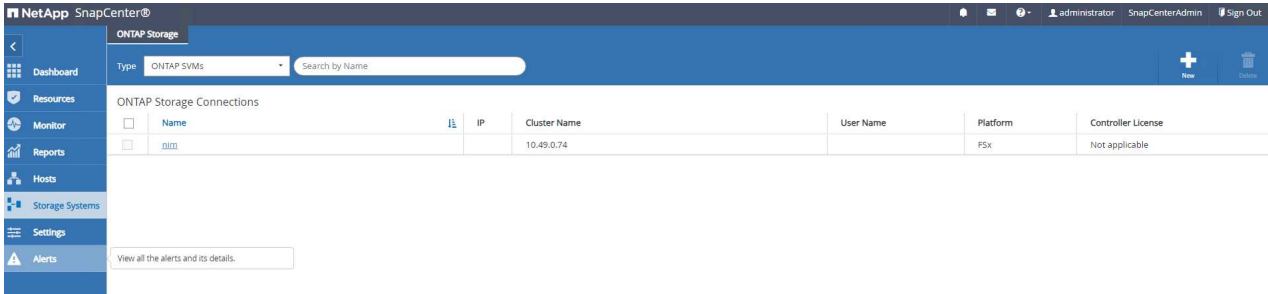
5. Erstellen Sie Backup-Richtlinien für Oracle Datenbanken. Im Idealfall erstellen Sie eine separate Backup-Richtlinie für Archivprotokolle, um häufigere Backups zu ermöglichen, um Datenverlust bei einem Ausfall zu minimieren.



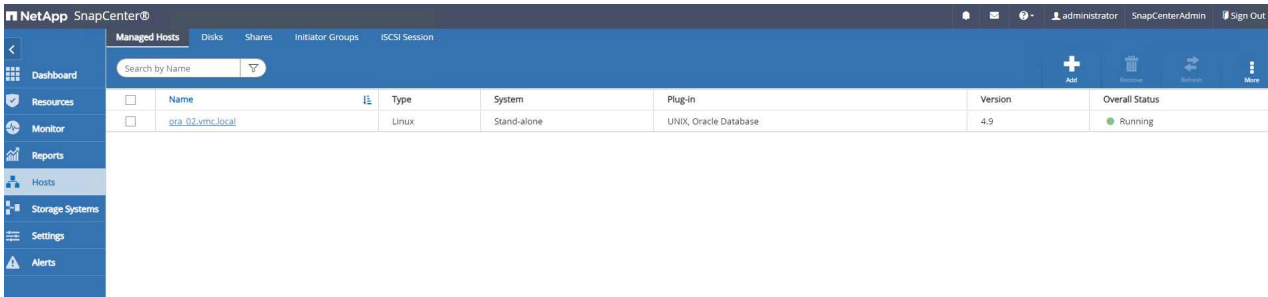
6. Hinzufügen eines Datenbanksservers `Credential` Für SnapCenter-Zugriff auf DB VM. Die Anmeldeinformationen sollten über Sudo-Berechtigung auf einer Linux-VM oder Administratorberechtigung auf einer Windows-VM verfügen.



7. Fügen Sie FSX ONTAP Storage-Cluster zu hinzu `Storage Systems` Mit Cluster-Management-IP und Authentifizierung über `fsxadmin` Benutzer-ID.



8. Fügen Sie die Oracle-Datenbank-VM in VMC zu hinzu `Hosts` Mit Serveranmeldeinformationen, die im vorherigen Schritt 6 erstellt wurden.

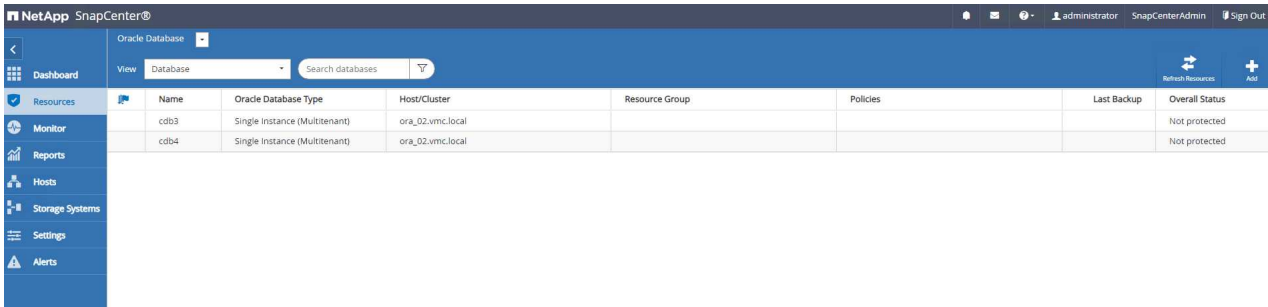


Stellen Sie sicher, dass der Name des SnapCenter-Servers in die IP-Adresse der DB VM aufgelöst werden kann und der Name der DB VM auf die IP-Adresse des SnapCenter-Servers aufgelöst werden kann.

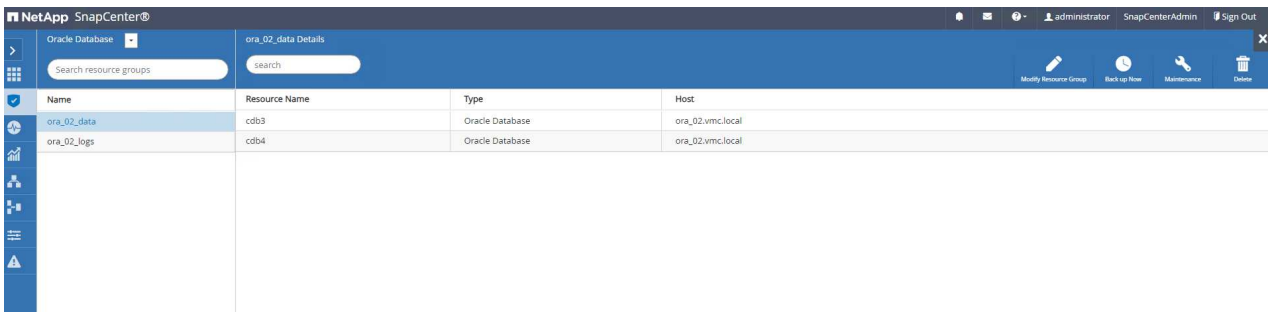
Datenbank-Backup

SnapCenter nutzt FSX ONTAP-Volumen-Snapshot für viel schnelleres Datenbank-Backup, -Wiederherstellung oder -Klonen im Vergleich zu herkömmlichen RMAN-basierten Methoden. Die Snapshots sind anwendungskonsistent, da die Datenbank vor einem Snapshot in den Oracle-Backup-Modus versetzt wird.

1. Von Resources Registerkarte werden alle Datenbanken auf der VM automatisch erkannt, nachdem die VM zu SnapCenter hinzugefügt wurde. Zunächst wird der Datenbankstatus als angezeigt `Not protected`.




2. Erstellen einer Ressourcengruppe zur Sicherung der Datenbank in einer logischen Gruppierung, z. B. durch DB-VM usw. In diesem Beispiel haben wir eine ora_02_Data-Gruppe erstellt, um ein vollständiges Online-Datenbank-Backup für alle Datenbanken auf VM ora_02 durchzuführen. Die Ressourcengruppe ora_02_log führt die Sicherung archivierter Protokolle nur auf der VM durch. Das Erstellen einer Ressourcengruppe definiert außerdem einen Zeitplan für die Ausführung des Backups.




3. Das Backup von Ressourcengruppen kann auch manuell durch Klicken auf ausgelöst werden `Back up Now` Und das Backup mit der in der Ressourcengruppe definierten Richtlinie ausführen.

Add schedules for policy Oracle Online Full Backup ✕

Hourly

Start date 

Expires on 

Repeat every hours mins

i The schedules are triggered in the SnapCenter Server time zone. ✕

4. Der Backupjob kann am überwacht werden Monitor Klicken Sie auf den laufenden Job.

Job Details

Backup of Resource Group 'ora_01_data' with policy 'Oracle Online Full Backup'

- ✓ ▾ Backup of Resource Group 'ora_01_data' with policy 'Oracle Online Full Backup'
 - ✓ ▾ ora_01.vmc.local
 - ✓ ▶ Prescripts
 - ✓ ▶ Preparing for Oracle Database Backup
 - ✓ ▶ Preparing for File-System Backup
 - ✓ ▶ Backup datafiles and control files
 - ✓ ▶ Backup archive logs
 - ✓ ▶ Finalizing Oracle Database Backup
 - ✓ ▶ Finalizing File-System Backup
 - ✓ ▶ Postscripts
 - ✓ ▶ Data Collection
 - ✓ ▶ Send EMS Messages

Task Name: ora_01.vmc.local Start Time: 10/07/2023 8:53:24 AM End Time: 10/07/2023 8:54:33 AM

View Logs Cancel job Close

5. Nach einer erfolgreichen Sicherung zeigt der Datenbankstatus den Jobstatus und die letzte Sicherungszeit an.

NetApp SnapCenter®

Administrator SnapCenterAdmin Sign Out

Dashboard View: Database Search databases

Resources	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
Monitor	cdb1	Single Instance (Multitenant)	ora_01.vmc.local	ora_01_data ora_01_logs	Oracle Archive Logs Backup Oracle Online Full Backup	10/07/2023 12:00:25 PM	Backup succeeded
Reports	cdb2	Single Instance (Multitenant)	ora_01.vmc.local	ora_01_data ora_01_logs	Oracle Archive Logs Backup Oracle Online Full Backup	10/07/2023 12:00:25 PM	Backup succeeded
Hosts	cdb3	Single Instance (Multitenant)	ora_02.vmc.local	ora_02_data ora_02_logs	Oracle Archive Logs Backup Oracle Online Full Backup	10/07/2023 8:05:25 AM	Backup succeeded
Storage Systems	cdb4	Single Instance (Multitenant)	ora_02.vmc.local	ora_02_data ora_02_logs	Oracle Archive Logs Backup Oracle Online Full Backup	10/07/2023 8:05:25 AM	Backup succeeded

Settings Alerts

6. Klicken Sie auf die Datenbank, um die Backup-Sätze für jede Datenbank anzuzeigen.

The screenshot shows the NetApp SnapCenter interface for Oracle Database backup management. The main view is for the 'cdb3 Topology'. On the left, there is a search bar and a list of databases: cdb1, cdb2, cdb3 (selected), and cdb4. The 'Manage Copies' section shows 22 Backups and 0 Clones. A 'Summary Card' displays the following statistics: 22 Backups, 8 Data Backups, 14 Log Backups, and 0 Clones. Below this is a table of 'Primary Backup(s)' with the following data:

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora_02_10-07-2023_08.05.02.4105_1	1	Log	10/07/2023 8:05:26 AM	Not Applicable	False	Not Cataloged	2928738
ora_02_10-07-2023_07.50.02.4250_1	1	Log	10/07/2023 7:50:27 AM	Not Applicable	False	Not Cataloged	2927731
ora_02_10-07-2023_07.45.02.4192_1	1	Log	10/07/2023 7:45:49 AM	Not Applicable	False	Not Cataloged	2927497
ora_02_10-07-2023_07.45.02.4192_0	1	Data	10/07/2023 7:45:31 AM	Unverified	False	Not Cataloged	2927446
ora_02_10-07-2023_07.35.02.3846_1	1	Log	10/07/2023 7:35:25 AM	Not Applicable	False	Not Cataloged	2926747
ora_02_10-07-2023_07.20.02.3803_1	1	Log	10/07/2023 7:20:25 AM	Not Applicable	False	Not Cataloged	2925995
ora_02_10-07-2023_07.05.02.3948_1	1	Log	10/07/2023 7:05:26 AM	Not Applicable	False	Not Cataloged	2924987
ora_02_10-07-2023_06.50.02.3786_1	1	Log	10/07/2023 6:50:26 AM	Not Applicable	False	Not Cataloged	2923925

Datenbank-Recovery

SnapCenter bietet verschiedene Wiederherstellungs- und Recovery-Optionen für Oracle Datenbanken aus dem Snapshot-Backup. In diesem Beispiel zeigen wir eine Point-in-Time-Wiederherstellung, um eine Tabelle versehentlich wiederherzustellen. Auf VM ora_02, zwei Datenbanken cdb3, cdb4 teilen sich die gleichen +DATEN und +LOGS-Plattengruppen. Die Datenbankwiederherstellung für eine Datenbank hat keine Auswirkung auf die Verfügbarkeit der anderen Datenbank.

1. Erstellen Sie zunächst eine Testtabelle, und fügen Sie eine Zeile in die Tabelle ein, um eine Point-in-Time-Wiederherstellung zu validieren.

```
[oracle@ora_02 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Oct 6 14:15:21 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> select name, open_mode from v$database;

NAME          OPEN_MODE
-----
CDB3          READ WRITE

SQL> show pdbs

          CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
          2 PDB$SEED                                READ ONLY  NO
          3 CDB3_PDB1                                READ WRITE NO
          4 CDB3_PDB2                                READ WRITE NO
          5 CDB3_PDB3                                READ WRITE NO

SQL>

SQL> alter session set container=cdb3_pdb1;

Session altered.

SQL> create table test (id integer, dt timestamp, event
varchar(100));
```

Table created.

```
SQL> insert into test values(1, sysdate, 'test oracle recovery on
guest mounted fsx storage to VMC guest vm ora_02');
```

1 row created.

```
SQL> commit;
```

Commit complete.

```
SQL> select * from test;
```

```
          ID
-----
DT
-----
EVENT
-----
          1
06-OCT-23 03.18.24.000000 PM
test oracle recovery on guest mounted fsx storage to VMC guest vm
ora_02
```

```
SQL> select current_timestamp from dual;
```

```
CURRENT_TIMESTAMP
-----
06-OCT-23 03.18.53.996678 PM -07:00
```

2. Wir führen ein manuelles Snapshot Backup aus dem SnapCenter. Legen Sie dann die Tabelle ab.

```

SQL> drop table test;

Table dropped.

SQL> commit;

Commit complete.

SQL> select current_timestamp from dual;

CURRENT_TIMESTAMP
-----
06-OCT-23 03.26.30.169456 PM -07:00

SQL> select * from test;
select * from test
          *
ERROR at line 1:
ORA-00942: table or view does not exist

```

- Notieren Sie sich die SCN-Nummer des Protokollbackups, wenn Sie den Backup-Satz aus dem letzten Schritt erstellt haben. Klicken Sie auf **Restore** Um den Wiederherstellungs-Workflow zu starten.

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora_02_10-06-2023_14.22.59.0383_1	1	Log		10/06/2023 2:23:43 PM	Not Applicable	False	Not Cataloged	2795205
ora_02_10-06-2023_14.22.59.0383_0	1	Data		10/06/2023 2:23:27 PM	Unverified	False	Not Cataloged	2795113
ora_02_10-06-2023_14.20.01.8472_1	1	Log		10/06/2023 2:20:24 PM	Not Applicable	False	Not Cataloged	2794928
ora_02_10-06-2023_14.05.01.8346_1	1	Log		10/06/2023 2:05:24 PM	Not Applicable	False	Not Cataloged	2793950
ora_02_10-06-2023_13.52.09.1111_1	1	Log		10/06/2023 1:52:59 PM	Not Applicable	False	Not Cataloged	2792888
ora_02_10-06-2023_13.52.09.1111_0	1	Data		10/06/2023 1:52:43 PM	Unverified	False	Not Cataloged	2792838

- Wählen Sie den Wiederherstellungsbereich aus.

Restore cdb3

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Restore Scope ⓘ

All Datafiles

Pluggable databases (PDBs)

Pluggable database (PDB) tablespaces

Control files

Database State

Change database state if needed for restore and recovery

Restore Mode ⓘ

Force in place restore

If this check box is not selected and if any of the in place restore criteria is not met, restore will be performed using the connect and copy method. The connect and copy restore method might take time based on the files being restored.

Previous Next

5. Wählen Sie den Wiederherstellungsumfang bis zum Protokoll-SCN aus dem letzten vollständigen Datenbankbackup aus.

Restore cdb3

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Choose Recovery Scope

All Logs i

Until SCN (System Change Number)

SCN i

Date and Time

No recovery

Specify external archive log files locations + - i

i After the operation is complete, it is recommended to create a full backup of the Oracle database. x

Previous **Next**

6. Geben Sie alle optionalen Pre-Skripte an, die ausgeführt werden sollen.

Restore cdb3 x

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps**
- 4 PostOps
- 5 Notification
- 6 Summary

Specify optional scripts to run before performing a restore job ⓘ

Prescript full path

Arguments

Script timeout

7. Geben Sie ein beliebiges optionales After-Script an, das ausgeführt werden soll.

Restore cdb3 x

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Specify optional scripts to run after performing a restore job ⓘ

Postscript full path

Arguments

Open the database or container database in READ-WRITE mode after recovery

8. Senden Sie bei Bedarf einen Jobbericht.

Restore cdb3 x

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification**
- 6 Summary

Provide email settings ⓘ

Email preference:

From:

To:

Subject:

Attach job report

9. Überprüfen Sie die Zusammenfassung, und klicken Sie auf `Finish` Um die Wiederherstellung und Wiederherstellung zu starten.

Restore cdb3
✕

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary

Summary

Backup name	ora_02_10-06-2023_14.22.59.0383_0
Backup date	10/06/2023 2:23:27 PM
Restore scope	All DataFiles
Recovery scope	Until SCN 2795205
Auxiliary destination	
Options	Change database state if necessary , Open the database or container database in READ-WRITE mode after recovery
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

Previous
Finish

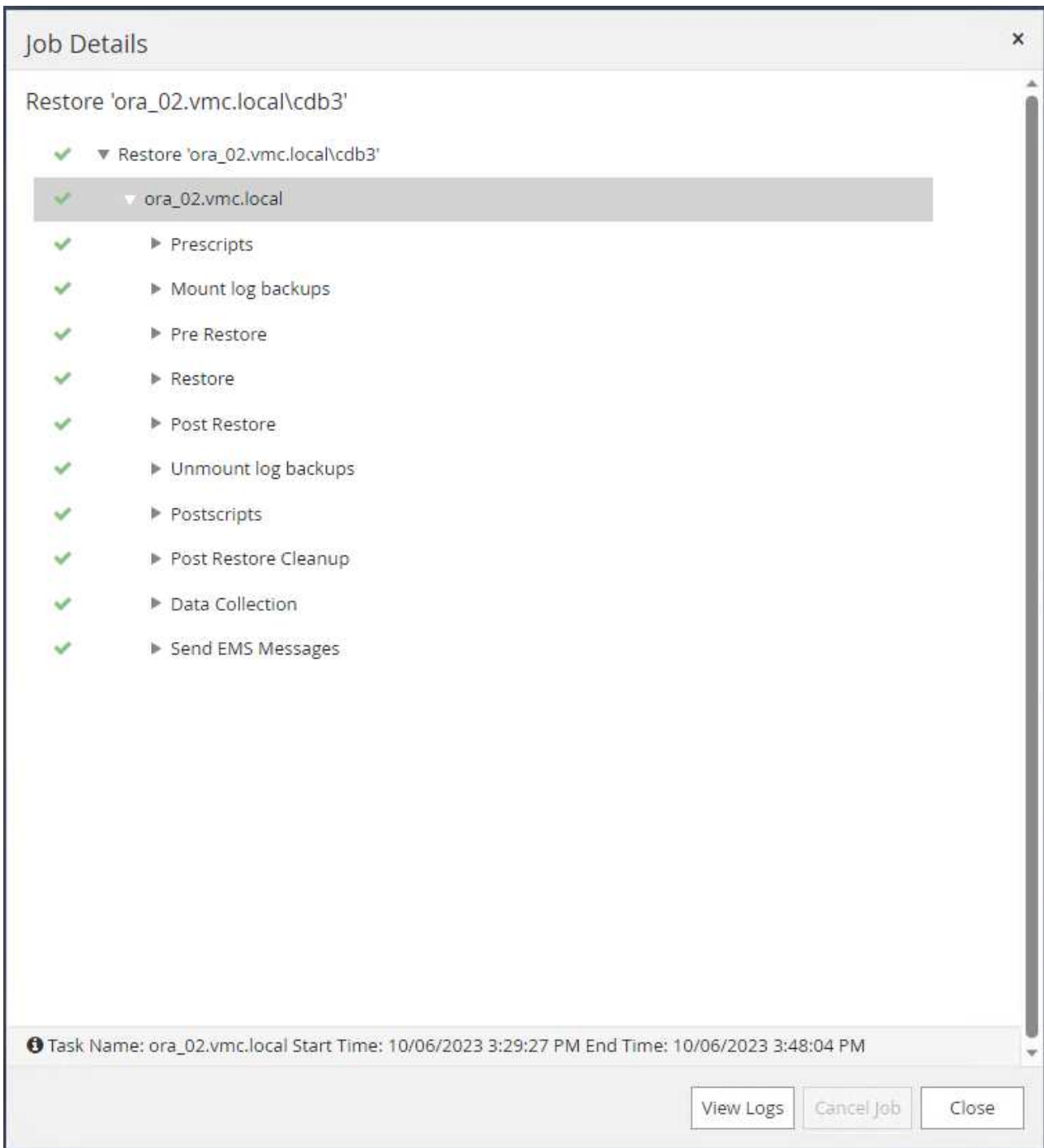
10. Von Oracle Restart Grid control, beobachten wir, dass cdb3 ist in der Wiederherstellung und Recovery cdb4 ist online und verfügbar.

```

[oracle@ora_02 bin]$ ./crsctl stat res -t
-----
Name                Target  State        Server        State details
-----
Local Resources
-----
ora.DATA.dg         ONLINE  ONLINE       ora_02        STABLE
ora.LISTENER.lsnr   ONLINE  INTERMEDIATE ora_02        Not All Endpoints Re
registered, STABLE
ora.LOGS.dg         ONLINE  ONLINE       ora_02        STABLE
ora.LOGS_CDB3_22.dg ONLINE  ONLINE       ora_02        STABLE
ora.asm             ONLINE  ONLINE       ora_02        Started, STABLE
ora.ons             OFFLINE OFFLINE       ora_02        STABLE
-----
Cluster Resources
-----
ora.cdb3.db
  1                 ONLINE  INTERMEDIATE ora_02        Dismounted, Mount Ini
tiated, HOME=/u01/app
/oracle/product/19.0
.0/cdb3, STABLE
ora.cdb4.db
  1                 ONLINE  ONLINE       ora_02        Open, HOME=/u01/app/o
racle/product/19.0.0
/cdb4, STABLE
ora.cssd
  1                 ONLINE  ONLINE       ora_02        STABLE
ora.diskmon
  1                 OFFLINE OFFLINE       STABLE
ora.driver.afd
  1                 ONLINE  ONLINE       ora_02        STABLE
ora.evmd
  1                 ONLINE  ONLINE       ora_02        STABLE
-----
[oracle@ora_02 bin]$ █

```

11. Von Monitor Öffnen Sie den Job, um die Details zu überprüfen.



- Überprüfen Sie in DB VM ora_02, ob die verlorene Tabelle nach einer erfolgreichen Recovery wiederhergestellt wurde.

```
[oracle@ora_02 bin]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Fri Oct 6 17:01:28 2023  
Version 19.18.0.0.0
```

```
Copyright (c) 1982, 2022, Oracle. All rights reserved.
```



```
Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0
```

```
SQL> select name, open_mode from v$database;
```

```
NAME          OPEN_MODE
-----
CDB3          READ WRITE
```

```
SQL> show pdbs
```

```
CON_ID CON_NAME          OPEN MODE  RESTRICTED
-----
2 PDB$SEED          READ ONLY  NO
3 CDB3_PDB1        READ WRITE NO
4 CDB3_PDB2        READ WRITE NO
5 CDB3_PDB3        READ WRITE NO
```

```
SQL> alter session set container=CDB3_PDB1;
```

```
Session altered.
```

```
SQL> select * from test;
```

```
          ID
-----
DT
-----
EVENT
-----
          1
06-OCT-23 03.18.24.000000 PM
test oracle recovery on guest mounted fsx storage to VMC guest vm
ora_02
```

```
SQL> select current_timestamp from dual;
```

```
CURRENT_TIMESTAMP
-----
06-OCT-23 05.02.20.382702 PM -07:00
```

```
SQL>
```


In diesem Beispiel wird mit denselben Backup-Sets eine Datenbank auf derselben VM in einem anderen ORACLE_HOME geklont. Die Verfahren gelten auch für das Klonen einer Datenbank aus dem Backup auf separate VM in VMC, falls erforderlich.

1. Öffnen Sie die Datenbank cdb3-Backup-Liste. Klicken Sie bei einem beliebigen Daten-Backup auf **Clone** Um den Workflow für Datenbankklone zu starten.

The screenshot shows the NetApp SnapCenter interface for an Oracle Database. The main content area displays a table of backup records for the database cdb3. The table has columns for Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. One record is highlighted in blue.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora_02_10-06-2023_17.20.01.9983_1	1	Log	10/06/2023 5:20:23 PM	Not Applicable	False	Not Cataloged	2814539
ora_02_10-06-2023_17.05.01.9656_1	1	Log	10/06/2023 5:05:24 PM	Not Applicable	False	Not Cataloged	2813819
ora_02_10-06-2023_16.50.01.9670_1	1	Log	10/06/2023 4:50:25 PM	Not Applicable	False	Not Cataloged	2812382
ora_02_10-06-2023_16.45.02.2685_1	1	Log	10/06/2023 4:45:45 PM	Not Applicable	False	Not Cataloged	2812040
ora_02_10-06-2023_16.45.02.2685_0	1	Data	10/06/2023 4:45:30 PM	Unverified	False	Not Cataloged	2811991
ora_02_10-06-2023_16.35.01.9959_1	1	Log	10/06/2023 4:35:22 PM	Not Applicable	False	Not Cataloged	2811534

2. Benennen Sie die SID der Klondatenbank.

Clone from cdb3 x

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Complete Database Clone

Clone SID:

Exclude PDBs:

PDB Clone

3. Wählen Sie eine VM in VMC als Ziel-Datenbank-Host aus. Auf dem Host sollte eine identische Oracle-Version installiert und konfiguriert worden sein.

x
Clone from cdb3

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Select the host to create a clone

Clone host

Datafile locations i

Reset

Control files i

x +

x Reset

Redo logs i

Group	Size	Unit	Number of files			
▶ RedoGroup 1	x	200	MB	2	+	+ Reset
▶ RedoGroup 2	x	200	MB	2	+	
▶ RedoGroup 3	x	200	MB	2	+	

Previous
Next

4. Wählen Sie ORACLE_HOME, Benutzer und Gruppe auf dem Zielhost aus. Standardmäßig Anmeldedaten beibehalten.

Clone from cdb3

1 Name

2 Locations

3 **Credentials**

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user: None + ⓘ

ASM instance Credential name: None + ⓘ

Database port: 1521

ASM Port: 1521

Oracle Home Settings ⓘ

Oracle Home: /u01/app/oracle/product/19.0.0/cdb4

Oracle OS User: oracle

Oracle OS Group: oinstall

Previous Next

5. Ändern Sie die Parameter der Klondatenbank, um die Konfigurations- oder Ressourcenanforderungen für die Klondatenbank zu erfüllen.

Clone from cdb3
✕

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Specify scripts to run before clone operation ?

Prescript full path

Arguments

Script timeout secs

Database Parameter settings

processes	320	✕	▲
remote_login_passwordfile	EXCLUSIVE	✕	+
sga_target	2048M	✕	▼
undo_tablespace	UNDOTBS1	✕	▼

6. Wählen Sie den Wiederherstellungsumfang aus. `Until Cancel` Stellt den Klon bis zur letzten verfügbaren Protokolldatei im Backup-Set wieder her.

Clone from cdb3

1 Name
2 Locations
3 Credentials
4 PreOps
5 PostOps
6 Notification
7 Summary

Recover Database

Until Cancel ⓘ
 Date and Time ⓘ
Date-time format: MM/DD/YYYY hh:mm:ss
 Until SCN (System Change Number) ⓘ

Specify external archive log locations ⓘ

Create new DBID ⓘ
 Create tempfile for temporary tablespace ⓘ
 Enter SQL queries to apply when clone is created
 Enter scripts to run after clone operation ⓘ

Previous Next

7. Überprüfen Sie die Zusammenfassung, und starten Sie den Klonjob.

Clone from cdb3

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

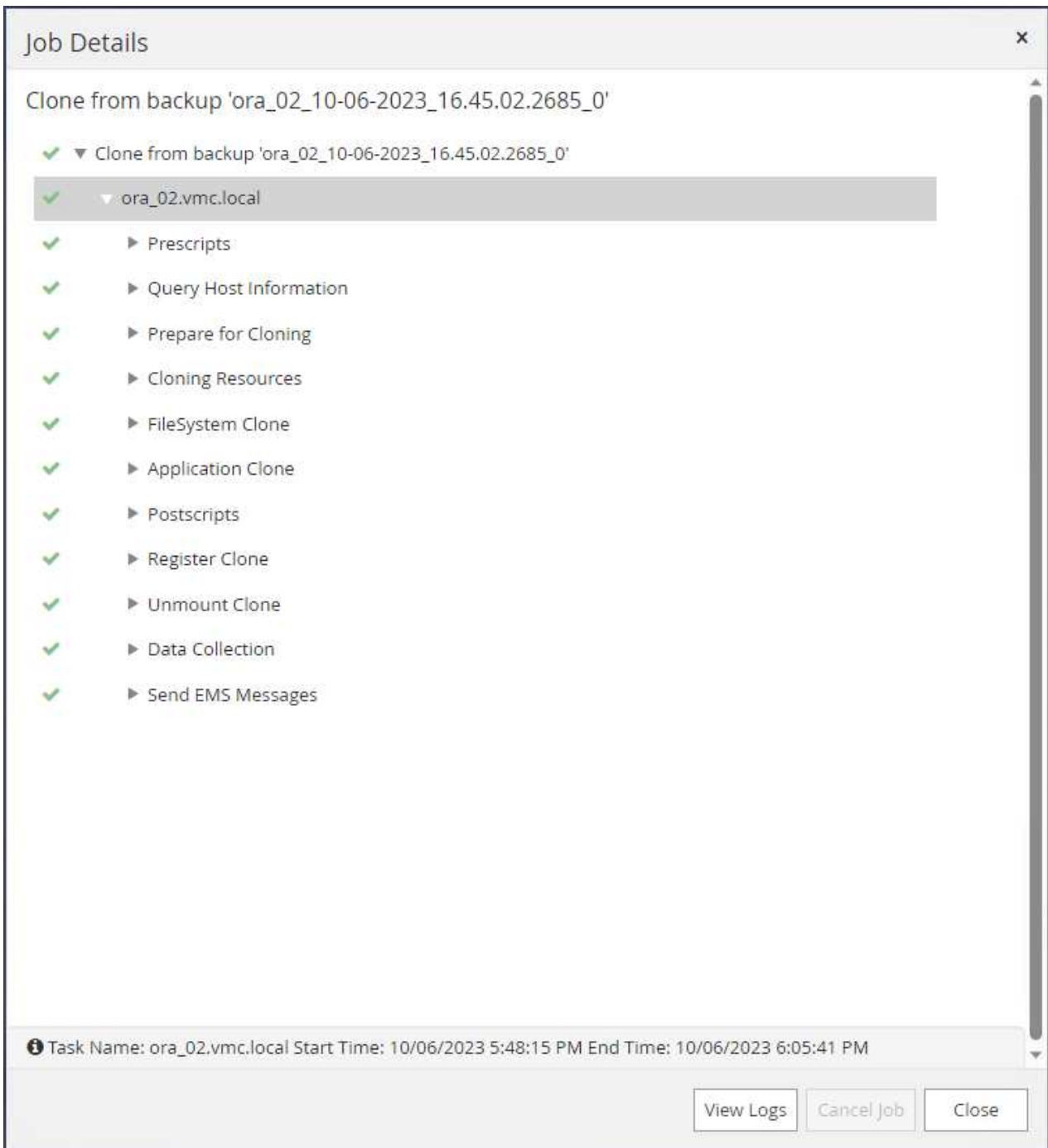
7 Summary

Summary

Clone from backup	ora_02_10-06-2023_16.45.02.2685_0
Clone SID	cdb3tst
Clone server	ora_01.vmc.local
Exclude PDBs	none
Oracle home	/u01/app/oracle/product/19.0.0/cdb2
Oracle OS user	oracle
Oracle OS group	oinstall
Datafile mountpaths	+SC_2090922_cdb3tst
Control files	+SC_2090922_cdb3tst/cdb3tst/control/control01.ctl +SC_2090922_cdb3tst/cdb3tst/control/control02.ctl
Redo groups	RedoGroup =1 TotalSize =200 Path =+SC_2090922_cdb3tst/cdb3tst/redo01_01.log RedoGroup =1 TotalSize =200 Path =+SC_2090922_cdb3tst/cdb3tst/redo01_02.log RedoGroup =2 TotalSize =200 Path =+SC_2090922_cdb3tst/cdb3tst/redo02_01.log RedoGroup =2 TotalSize =200 Path =+SC_2090922_cdb3tst/cdb3tst/redo02_02.log RedoGroup =3 TotalSize =200 Path =+SC_2090922_cdb3tst/cdb3tst/redo03_01.log RedoGroup =3 TotalSize =200 Path =+SC_2090922_cdb3tst/cdb3tst/redo03_02.log
Recovery scope	Until Cancel
Prescript full path	none
Prescript arguments	
Postscript full path	none
Postscript arguments	
Send email	No

Previous Finish

8. Überwachen Sie die Ausführung des Klonjobs von Monitor Registerkarte.



9. Geklonte Datenbank wird sofort in SnapCenter registriert.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb1	Single Instance (Multitenant)	ora_01.vmc.local				Not protected
cdb2	Single Instance (Multitenant)	ora_01.vmc.local				Not protected
cdb3	Single Instance (Multitenant)	ora_02.vmc.local	ora_02_data ora_02_logs	Oracle Archive Logs Backup Oracle Online Full Backup	10/06/2023 6:20:23 PM	Backup succeeded
cdb3st	Single Instance (Multitenant)	ora_02.vmc.local				Not protected
cdb4	Single Instance (Multitenant)	ora_02.vmc.local	ora_02_data ora_02_logs	Oracle Archive Logs Backup Oracle Online Full Backup	10/06/2023 6:20:23 PM	Backup succeeded

10. Ab DB VM ora_02 wird die geklonte Datenbank auch in der Oracle Restart Grid Control registriert, und die verlorene Testtabelle wird wie unten gezeigt in der geklonten Datenbank cdb3tst wiederhergestellt.

```
[oracle@ora_02 ~]$ /u01/app/oracle/product/19.0.0/grid/bin/crsctl
stat res -t
-----
-----
Name          Target  State          Server          State
details
-----
-----
Local Resources
-----
-----
ora.DATA.dg
          ONLINE  ONLINE         ora_02          STABLE
ora.LISTENER.lsnr
          ONLINE  INTERMEDIATE  ora_02          Not All
Endpoints Re
gistered, STABLE
ora.LOGS.dg
          ONLINE  ONLINE         ora_02          STABLE
ora.SC_2090922_CDB3TST.dg
          ONLINE  ONLINE         ora_02          STABLE
ora.asm
          ONLINE  ONLINE         ora_02
Started, STABLE
ora.ons
          OFFLINE OFFLINE        ora_02          STABLE
-----
-----
Cluster Resources
-----
-----
ora.cdb3.db
      1      ONLINE  ONLINE         ora_02
Open, HOME=/u01/app/o
racle/product/19.0.0
/cdb3, STABLE
ora.cdb3tst.db
      1      ONLINE  ONLINE         ora_02
Open, HOME=/u01/app/o
```

```
racle/product/19.0.0
```

```
/cdb4, STABLE
```

```
ora.cdb4.db
```

```
1 ONLINE ONLINE ora_02
```

```
Open, HOME=/u01/app/o
```

```
racle/product/19.0.0
```

```
/cdb4, STABLE
```

```
ora.cssd
```

```
1 ONLINE ONLINE ora_02 STABLE
```

```
ora.diskmon
```

```
1 OFFLINE OFFLINE STABLE
```

```
ora.driver.afd
```

```
1 ONLINE ONLINE ora_02 STABLE
```

```
ora.evmd
```

```
1 ONLINE ONLINE ora_02 STABLE
```

```
-----  
-----
```

```
[oracle@ora_02 ~]$ export
```

```
ORACLE_HOME=/u01/app/oracle/product/19.0.0/cdb4
```

```
[oracle@ora_02 ~]$ export ORACLE_SID=cdb3tst
```

```
[oracle@ora_02 ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Sat Oct 7 08:04:51 2023  
Version 19.18.0.0.0
```

```
Copyright (c) 1982, 2022, Oracle. All rights reserved.
```

```
Connected to:
```

```
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
```

```
Production
```

```
Version 19.18.0.0.0
```

```
SQL> select name, open_mode from v$database;
```

```
NAME OPEN_MODE
```

```
-----
```

```
CDB3TST READ WRITE
```

```
SQL> show pdbs
```

```
CON_ID CON_NAME
```

```
OPEN MODE RESTRICTED
```

```

2 PDB$SEED                READ ONLY NO
3 CDB3_PDB1               READ WRITE NO
4 CDB3_PDB2               READ WRITE NO
5 CDB3_PDB3               READ WRITE NO
SQL> alter session set container=CDB3_PDB1;

Session altered.

SQL> select * from test;

          ID
-----
DT
-----
EVENT
-----
          1
06-OCT-23 03.18.24.000000 PM
test oracle recovery on guest mounted fsx storage to VMC guest vm
ora_02

SQL>

```

Hiermit sind die Backups, Wiederherstellungen und Klonvorgänge von SnapCenter der Oracle-Datenbank im VMC SDDC auf AWS abgeschlossen.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- VMware Cloud on AWS Dokumentation

["https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html"](https://docs.vmware.com/en/VMware-Cloud-on-AWS/index.html)

- Installieren der Oracle Grid-Infrastruktur für einen eigenständigen Server mit einer neuen Datenbankinstallation

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3)

- Installieren und Konfigurieren von Oracle Database mithilfe von Antwortdateien

["https://docs.oracle.com/en/database/oracle/oracle-database/19/adb/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7"](https://docs.oracle.com/en/database/oracle/oracle-database/19/adb/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7)

- Amazon FSX für NetApp ONTAP

["https://aws.amazon.com/fsx/netapp-ontap/"](https://aws.amazon.com/fsx/netapp-ontap/)

TR-4981: Kostenreduzierung mit Oracle Active Data Guard und Amazon FSX ONTAP

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Oracle Data Guard gewährleistet Hochverfügbarkeit, Datensicherung und Disaster Recovery für Unternehmensdaten in einer primären Datenbank und einer Standby-Datenbankreplikationskonfiguration. Oracle Active Data Guard ermöglicht Benutzern den Zugriff auf Standby-Datenbanken, während die Datenreplikation von der primären Datenbank auf Standby-Datenbanken aktiv ist. Data Guard ist ein Bestandteil der Oracle Database Enterprise Edition. Eine separate Lizenzierung ist nicht erforderlich. Active Data Guard hingegen ist eine Oracle Database Enterprise Edition-Option, die daher eine separate Lizenzierung erfordert. Mehrere Standby-Datenbanken können in der Active Data Guard-Einrichtung eine Datenreplikation von einer primären Datenbank empfangen. Für jede zusätzliche Standby-Datenbank ist jedoch eine Active Data Guard Lizenz und zusätzlicher Storage als Größe der primären Datenbank erforderlich. Die Betriebskosten summieren sich schnell.

Wenn Sie die Kosten für den Betrieb Ihrer Oracle-Datenbank senken möchten und einen Active Data Guard in AWS einrichten möchten, sollten Sie eine Alternative in Betracht ziehen. Verwenden Sie anstelle von Active Data Guard Data Guard zur Replikation von der primären Datenbank auf eine einzige physische Standby-Datenbank auf Amazon FSX ONTAP Storage. Anschließend können mehrere Kopien dieser Standby-Datenbank geklont und für Lese-/Schreibzugriff für viele andere Anwendungsfälle wie Berichte, Entwicklung, Tests usw. geöffnet werden. Die Nettoergebnisse stellen Funktionen von Active Data Guard effektiv bereit, wobei die Active Data Guard Lizenz sowie zusätzliche Storage-Kosten für jede zusätzliche Standby-Datenbank entfallen. In dieser Dokumentation zeigen wir, wie Sie einen Oracle Data Guard mit Ihrer vorhandenen primären Datenbank in AWS einrichten und die physische Standby-Datenbank auf dem Amazon FSX ONTAP-Storage platzieren. Die Standby-Datenbank wird nach Bedarf über Snapshot gesichert und für Lese-/Schreibzugriff geklont.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Oracle Data Guard zwischen einer primären Datenbank auf jedem Storage in AWS bis Standby-Datenbank auf Amazon FSX ONTAP Storage
- Klonen der Standby-Datenbank während der Schließung zur Datenreplikation für Anwendungsfälle wie Berichterstellung, Entwicklung, Test usw.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

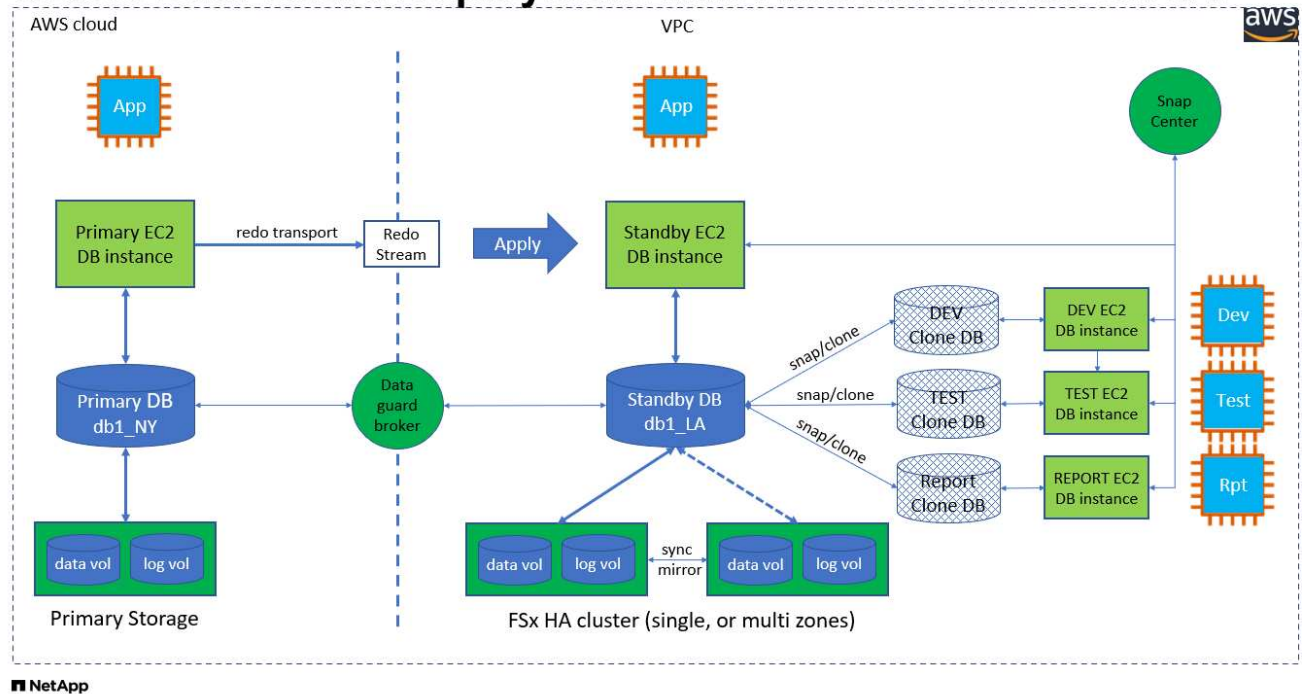
- Ein DBA, der Oracle Active Data Guard in AWS für Hochverfügbarkeit, Datensicherung und Disaster Recovery einrichtet.
- Ein Datenbanklösungsarchitekt, der an der Oracle Active Data Guard-Konfiguration in der AWS-Cloud interessiert ist.
- Ein Storage-Administrator, der den AWS FSX ONTAP Storage, der Oracle Data Guard unterstützt, managt.
- Ein Applikationseigentümer, der Oracle Data Guard in AWS FSX/EC2-Umgebung einrichten möchte.

Test- und Validierungsumgebung der Lösung

Das Testen und Validieren dieser Lösung wurde in einer AWS FSX ONTAP und EC2 Lab-Umgebung durchgeführt, die möglicherweise nicht mit der endgültigen Implementierungsumgebung übereinstimmt. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind

Oracle Data Guard Deployment with Amazon FSx for ONTAP



Hardware- und Softwarekomponenten

Hardware		
FSX ONTAP-Storage	Aktuelle Version von AWS angeboten	Ein FSX HA-Cluster in der gleichen VPC und Verfügbarkeitszone
EC2 Instanz für Computing	t2.xlarge/4vCPU/16G	Drei EC2 T2 xlarge EC2-Instanzen, eine als primärer DB-Server, eine als Standby-DB-Server und die dritte als Klon-DB-Server
Software		
Redhat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Bereitstellung der RedHat Subscription für Tests
Oracle Grid Infrastructure	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet

Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
---------------	---------------------	--

Konfiguration von Oracle Data Guard mit hypothetischer Einrichtung von NY zu LA DR

* Datenbank*	DB_UNIQUE_NAME	Oracle Net Service Name
Primär	db1_NY	db1_NY.demo.netapp.com
Physikalischer Standby	db1_LA	db1_LA.demo.netapp.com

Wichtige Faktoren für die Implementierung

- Funktionsweise von Oracle Standby Database FlexClone.** AWS FSX ONTAP FlexClone stellt freigegebene Kopien derselben Standby-Datenbank-Volumes bereit, die beschreibbar sind. Die Kopien der Volumes sind tatsächlich Zeiger, die zurück zu den ursprünglichen Datenblöcken verweisen, bis ein neuer Schreibvorgang des Klons initiiert wird. ONTAP weist dann neuen Speicherblöcken für die neuen Schreibvorgänge zu. Alle Lese-I/O-Vorgänge werden durch die ursprünglichen Datenblöcke verarbeitet, die bei der aktiven Replizierung zur Verfügung stehen. Der Klon ist somit sehr Storage-effizient und kann für viele andere Anwendungsfälle mit minimaler und inkrementeller neuer Storage-Zuweisung für neue Schreib-I/Os verwendet werden. Dies führt zu enormen Einsparungen bei den Storage-Kosten, indem der Platzbedarf für Active Data Guard Storage deutlich verringert wird. NetApp empfiehlt, FlexClone-Aktivitäten bei einem Datenbank-Wechsel vom primären Storage auf Standby FSX-Storage zu minimieren, um die Oracle-Performance auf hohem Niveau aufrechtzuerhalten.
- Oracle Software-Anforderungen.** im Allgemeinen muss eine physische Standby-Datenbank die gleiche Database Home-Version wie die primäre Datenbank haben, einschließlich Patch Set Exceptions (PSEs), Critical Patch Updates (CPUs), und Patch-Set-Updates (PSUs), es sei denn, es wird ein Oracle Data Guard Standby-First Patch Apply-Prozess durchgeführt (wie in My Oracle Support Note 1265700.1 unter beschrieben "support.oracle.com")
- Überlegungen zur Struktur des Standby-Datenbankverzeichnisses.** Wenn möglich, sollten die Datendateien, Protokolldateien und Kontrolldateien auf den primären und Standby-Systemen dieselben Namen und Pfadnamen haben und die Namenskonventionen für die optimale flexible Architektur (OFA) verwenden. Die Archivverzeichnisse in der Standby-Datenbank sollten auch zwischen Standorten identisch sein, einschließlich Größe und Struktur. Diese Strategie erlaubt es anderen Vorgängen wie Backups, Switchover und Failover, dieselben Schritte auszuführen, wodurch die Wartungskomplexität verringert wird.
- Protokollierungsmodus erzwingen.** um sich vor nicht eingeloggtten direkten Schreibvorgängen in der primären Datenbank zu schützen, die nicht an die Standby-Datenbank weitergegeben werden kann, aktivieren Sie die Option PROTOKOLLIERUNG an der primären Datenbank ERZWINGEN, bevor Sie Datendatei-Backups für die Standby-Erstellung durchführen.
- Database Storage Management.** aus Gründen der Benutzerfreundlichkeit empfiehlt Oracle, dass Sie Oracle Automatic Storage Management (Oracle ASM) und Oracle Managed Files (OMF) in einer Oracle Data Guard-Konfiguration symmetrisch auf der primären und Standby-Datenbank(en) einrichten.
- EC2 Compute-Instanzen.** in diesen Tests und Validierungen haben wir eine AWS EC2 t2.xlarge-Instanz als Compute-Instanz der Oracle-Datenbank verwendet. NetApp empfiehlt, in der Produktionsumgebung eine EC2-Instanz vom Typ M5 als Computing-Instanz für Oracle zu verwenden, da sie für Datenbank-Workloads optimiert ist. Sie müssen die Größe der EC2-Instanz entsprechend der Anzahl der vCPUs und der Menge des RAM anpassen, basierend auf den tatsächlichen Workload-Anforderungen.
- FSX Storage HA Cluster Single- oder Multi-Zone-Implementierung.** bei diesen Tests und Validierungen haben wir einen FSX HA-Cluster in einer einzelnen AWS Verfügbarkeitszone implementiert. Für die

Implementierung in der Produktion empfiehlt NetApp die Implementierung eines FSX HA-Paars in zwei verschiedenen Verfügbarkeitszonen. Ein FSX Cluster wird jeweils in einem HA-Paar bereitgestellt, das synchron in einem Paar aktiv/Passiv-Filesysteme gespiegelt ist, um Redundanz auf Storage-Ebene zu gewährleisten. Die Implementierung mit mehreren Zonen verbessert die Hochverfügbarkeit bei einem Ausfall in einer einzelnen AWS Zone noch weiter.

- **FSX Storage-Cluster-Sizing.** ein Amazon FSX for ONTAP Storage-Dateisystem bietet bis zu 160,000 RAW SSD IOPS, einen Durchsatz von bis zu 4 Gbit/s und eine maximale Kapazität von 192 tib. Sie können das Cluster jedoch in Bezug auf die bereitgestellten IOPS, den Durchsatz und die Storage-Grenze (mindestens 1,024 gib) anpassen, basierend auf Ihren tatsächlichen Anforderungen zum Zeitpunkt der Implementierung. Die Kapazität lässt sich spontan dynamisch anpassen, ohne dass die Applikationsverfügbarkeit beeinträchtigt wird.

Lösungsimplementierung

Es wird angenommen, dass Sie bereits Ihre primäre Oracle-Datenbank in einer VPC in der AWS EC2-Umgebung als Ausgangspunkt für die Einrichtung von Data Guard implementiert haben. Die primäre Datenbank wird mithilfe von Oracle ASM für das Storage-Management bereitgestellt. Zwei ASM-Datenträgergruppen - +DATEN und +PROTOKOLLE werden für Oracle-Datendateien, Log-Dateien und Steuerdatei usw. erstellt. Weitere Informationen zur Oracle-Implementierung in AWS mit ASM erhalten Sie in den folgenden technischen Berichten.

- ["Oracle Database Deployment on EC2 und FSX Best Practices"](#)
- ["Implementierung und Schutz von Oracle Database in AWS FSX/EC2 mit iSCSI/ASM"](#)
- ["Oracle 19c im Standalone-Neustart auf AWS FSX/EC2 mit NFS/ASM"](#)

Ihre primäre Oracle-Datenbank kann entweder auf einem FSX ONTAP oder einem beliebigen Storage innerhalb des AWS EC2 Ecosystems ausgeführt werden. Der folgende Abschnitt enthält schrittweise Bereitstellungsverfahren für das Einrichten von Oracle Data Guard zwischen einer primären EC2 DB-Instanz mit ASM-Speicher auf einer Standby-EC2-DB-Instanz mit ASM-Speicher.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wurde ein AWS Konto eingerichtet, und die erforderlichen VPC und Netzwerksegmente wurden in Ihrem AWS Konto erstellt.
2. Über die AWS EC2-Konsole müssen Sie mindestens drei EC2 Linux-Instanzen implementieren, eine als primäre Oracle DB-Instanz, eine als Standby Oracle DB-Instanz und eine Clone-Ziel-DB-Instanz für Berichterstellung, Entwicklung und Test usw. Weitere Details zur Umgebungs-Einrichtung finden Sie im Architekturdiagramm im vorherigen Abschnitt. Sehen Sie sich auch die AWS-Übersicht an "[Benutzerhandbuch für Linux-Instanzen](#)" Finden Sie weitere Informationen.
3. Implementieren Sie über die AWS EC2 Konsole Amazon FSX for ONTAP Storage HA-Cluster, um Oracle Volumes zu hosten, die die Oracle-Standby-Datenbank speichern. Wenn Sie mit der Bereitstellung von FSX-Speicher nicht vertraut sind, lesen Sie die Dokumentation "[Erstellen von FSX für ONTAP-Dateisysteme](#)" Schritt-für-Schritt-Anleitungen.
4. Die Schritte 2 und 3 können mit dem folgenden Terraform Automatisierungs-Toolkit durchgeführt werden, das eine EC2-Instanz mit dem Namen `ora_01` und ein FSX Dateisystem mit dem Namen `fsx_01` erstellt. Überprüfen Sie die Anweisung sorgfältig, und ändern Sie die Variablen vor der Ausführung entsprechend Ihrer Umgebung. Sie können die Vorlage ganz einfach an Ihre eigenen Implementierungsanforderungen anpassen.

```
git clone https://github.com/NetApp-  
Automation/na_aws_fsx_ec2_deploy.git
```



Stellen Sie sicher, dass Sie mindestens 50G im Root-Volume der EC2-Instanz zugewiesen haben, damit genügend Speicherplatz für die Bereitstellung der Oracle Installationsdateien zur Verfügung steht.

Bereiten Sie die primäre Datenbank für Data Guard vor

In dieser Demonstration haben wir eine primäre Oracle-Datenbank namens db1 auf der primären EC2 DB-Instanz mit zwei ASM-Datenträgergruppen in Standalone Restart-Konfiguration mit Datendateien in ASM-Datenträgergruppe +DATEN und Flash-Recovery-Bereich in ASM-Datenträgergruppe +LOGS eingerichtet. Im Folgenden werden die detaillierten Verfahren zum Einrichten der primären Datenbank für Data Guard erläutert. Alle Schritte sollten als Datenbankeigentümer - oracle-Benutzer ausgeführt werden.

1. Konfiguration der primären Datenbank db1 auf der primären EC2 DB-Instanz ip-172-30-15-45. Die ASM-Laufwerksgruppen können sich auf jedem beliebigen Storage innerhalb der EC2-Umgebung befinden.

```
[oracle@ip-172-30-15-45 ~]$ cat /etc/oratab

# This file is used by ORACLE utilities.  It is created by root.sh
# and updated by either Database Configuration Assistant while
# creating
# a database or ASM Configuration Assistant while creating ASM
# instance.

# A colon, ':', is used as the field terminator.  A new line
# terminates
# the entry.  Lines beginning with a pound sign, '#', are comments.
#
# Entries are of the form:
#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:
#
# The first and second fields are the system identifier and home
# directory of the database respectively.  The third field indicates
# to the dbstart utility that the database should , "Y", or should
# not,
# "N", be brought up at system boot time.
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
+ASM:/u01/app/oracle/product/19.0.0/grid:N
db1:/u01/app/oracle/product/19.0.0/db1:N

[oracle@ip-172-30-15-45 ~]$
/u01/app/oracle/product/19.0.0/grid/bin/crsctl stat res -t
-----
-----
Name          Target  State          Server          State
details
-----
-----
Local Resources
```

```

-----
ora.DATA.dg
      ONLINE  ONLINE      ip-172-30-15-45      STABLE
ora.LISTENER.lsnr
      ONLINE  ONLINE      ip-172-30-15-45      STABLE
ora.LOGS.dg
      ONLINE  ONLINE      ip-172-30-15-45      STABLE
ora.asm
      ONLINE  ONLINE      ip-172-30-15-45
Started, STABLE
ora.ons
      OFFLINE OFFLINE      ip-172-30-15-45      STABLE
-----
Cluster Resources
-----
ora.cssd
  1      ONLINE  ONLINE      ip-172-30-15-45      STABLE
ora.dbf1.db
  1      ONLINE  ONLINE      ip-172-30-15-45
Open, HOME=/u01/app/o
racle/product/19.0.0
/dbf1, STABLE
ora.diskmon
  1      OFFLINE OFFLINE      STABLE
ora.driver.afd
  1      ONLINE  ONLINE      ip-172-30-15-45      STABLE
ora.evmd
  1      ONLINE  ONLINE      ip-172-30-15-45      STABLE
-----
-----

```

2. Aktivieren Sie von sqlplus die erzwungene Anmeldung auf dem primären Standort.

```
alter database force logging;
```

3. Aktivieren Sie von sqlplus Flashback auf primär. Flashback ermöglicht die einfache Wiederherstellung der primären Datenbank als Standby nach einem Failover.

```
alter database flashback on;
```

4. Konfigurieren der Authentifizierung für den Wiederherstelltransport mit Oracle-Passwortdatei - Erstellen Sie eine pwd-Datei auf dem primären System mit dem Dienstprogramm orapwd, falls nicht festgelegt, und kopieren Sie sie in das Verzeichnis ORACLE_HOME/dbs der Standby-Datenbank.
5. Erstellen Sie Standby-Wiederherstellungsprotokolle in der primären Datenbank mit der Größe der aktuellen Online-Protokolldatei. Protokollgruppen sind eine mehr als eine Online-Protokolldateigruppe. Die primäre Datenbank kann dann schnell in die Standby-Rolle überführen und bei Bedarf mit dem Empfang von Wiederherstellungsdaten beginnen.

```
alter database add standby logfile thread 1 size 200M;
```

Validate after standby logs addition:

```
SQL> select group#, type, member from v$logfile;
```

GROUP#	TYPE	MEMBER
3	ONLINE	+DATA/DB1/ONLINELOG/group_3.264.1145821513
2	ONLINE	+DATA/DB1/ONLINELOG/group_2.263.1145821513
1	ONLINE	+DATA/DB1/ONLINELOG/group_1.262.1145821513
4	STANDBY	+DATA/DB1/ONLINELOG/group_4.286.1146082751
4	STANDBY	+LOGS/DB1/ONLINELOG/group_4.258.1146082753
5	STANDBY	+DATA/DB1/ONLINELOG/group_5.287.1146082819
5	STANDBY	+LOGS/DB1/ONLINELOG/group_5.260.1146082821
6	STANDBY	+DATA/DB1/ONLINELOG/group_6.288.1146082825
6	STANDBY	+LOGS/DB1/ONLINELOG/group_6.261.1146082827
7	STANDBY	+DATA/DB1/ONLINELOG/group_7.289.1146082835
7	STANDBY	+LOGS/DB1/ONLINELOG/group_7.262.1146082835

11 rows selected.

6. Erstellen Sie aus sqlplus ein pfile aus spfile zur Bearbeitung.

```
create pfile='/home/oracle/initdb1.ora' from spfile;
```

7. Überarbeiten Sie die pfile und fügen Sie die folgenden Parameter hinzu.

```
DB_NAME=db1
DB_UNIQUE_NAME=db1_NY
LOG_ARCHIVE_CONFIG='DG_CONFIG=(db1_NY,db1_LA) '
LOG_ARCHIVE_DEST_1='LOCATION=USE_DB_RECOVERY_FILE_DEST
VALID_FOR=(ALL_LOGFILES,ALL_ROLES) DB_UNIQUE_NAME=db1_NY '
LOG_ARCHIVE_DEST_2='SERVICE=db1_LA ASYNC
VALID_FOR=(ONLINE_LOGFILES,PRIMARY_ROLE) DB_UNIQUE_NAME=db1_LA '
REMOTE_LOGIN_PASSWORDFILE=EXCLUSIVE
FAL_SERVER=db1_LA
STANDBY_FILE_MANAGEMENT=AUTO
```

8. Erstellen Sie in sqlplus spfile im ASM +DATA-Verzeichnis aus überarbeitetem pfile im Verzeichnis /Home/oracle.

```
create spfile='+DATA' from pfile='/home/oracle/initdb1.ora';
```

9. Suchen Sie die neu erstellte spfile unter +DATA Disk Group (ggf. mit dem Dienstprogramm asmcmd). Verwenden Sie srvctl, um das Raster zu ändern, um die Datenbank von neuem spfile zu starten, wie unten gezeigt.

```

[oracle@ip-172-30-15-45 db1]$ srvctl config database -d db1
Database unique name: db1
Database name: db1
Oracle home: /u01/app/oracle/product/19.0.0/db1
Oracle user: oracle
Spfile: +DATA/DB1/PARAMETERFILE/spfile.270.1145822903
Password file:
Domain: demo.netapp.com
Start options: open
Stop options: immediate
Database role: PRIMARY
Management policy: AUTOMATIC
Disk Groups: DATA
Services:
OSDBA group:
OSOPER group:
Database instance: db1
[oracle@ip-172-30-15-45 db1]$ srvctl modify database -d db1 -spfile
+DATA/DB1/PARAMETERFILE/spfiledb1.ora
[oracle@ip-172-30-15-45 db1]$ srvctl config database -d db1
Database unique name: db1
Database name: db1
Oracle home: /u01/app/oracle/product/19.0.0/db1
Oracle user: oracle
Spfile: +DATA/DB1/PARAMETERFILE/spfiledb1.ora
Password file:
Domain: demo.netapp.com
Start options: open
Stop options: immediate
Database role: PRIMARY
Management policy: AUTOMATIC
Disk Groups: DATA
Services:
OSDBA group:
OSOPER group:
Database instance: db1

```

10. Ändern Sie tnsnames.ora, um db_Unique_Name für die Namensauflösung hinzuzufügen.

```

# tnsnames.ora Network Configuration File:
/u01/app/oracle/product/19.0.0/db1/network/admin/tnsnames.ora
# Generated by Oracle configuration tools.

db1_NY =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = ip-172-30-15-
45.ec2.internal) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = db1)
    )
  )

db1_LA =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = ip-172-30-15-
67.ec2.internal) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = db1)
    )
  )

LISTENER_DB1 =
  (ADDRESS = (PROTOCOL = TCP) (HOST = ip-172-30-15-
45.ec2.internal) (PORT = 1521))

```

11. Fügen Sie der Datei Listener.ora den Namen des Data Guard-Dienstes db1_NY_DGMGRL.demo.netapp für die primäre Datenbank hinzu.


```
#Backup file is /u01/app/oracle/crsdata/ip-172-30-15-45/output/listener.ora.bak.ip-172-30-15-45.oracle line added by Agent
# listener.ora Network Configuration File:
/u01/app/oracle/product/19.0.0/grid/network/admin/listener.ora
# Generated by Oracle configuration tools.
```

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = ip-172-30-15-45.ec2.internal) (PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
    )
  )
```

```
SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = db1_NY_DGMGRL.demo.netapp.com)
      (ORACLE_HOME = /u01/app/oracle/product/19.0.0/db1)
      (SID_NAME = db1)
    )
  )
```

```
ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER=ON # line added by Agent
VALID_NODE_CHECKING_REGISTRATION_LISTENER=ON # line added by Agent
```

1. Fahren Sie die Datenbank mit `srvctl` herunter und starten Sie sie neu, und überprüfen Sie, ob die Data-Guard-Parameter jetzt aktiv sind.

```
srvctl stop database -d db1
```

```
srvctl start database -d db1
```

Damit ist die Einrichtung der primären Datenbank für Data Guard abgeschlossen.

Bereiten Sie die Standby-Datenbank vor und aktivieren Sie Data Guard

Für Oracle Data Guard sind eine Betriebssystemkernelkonfiguration und Oracle Software-Stacks einschließlich Patch-Sets auf der EC2-Standby-DB-Instanz erforderlich, die mit der primären EC2-DB-Instanz übereinstimmen. Um das Management und die Einfachheit zu vereinfachen, sollte die Konfiguration des Datenbank-Storage der EC2-Instanz im Standby-Modus auch mit der primären EC2-DB-Instanz übereinstimmen, z. B. Name, Anzahl und Größe der ASM-Festplattengruppen. Im Folgenden finden Sie detaillierte Verfahren zum Einrichten der Standby-EC2-DB-Instanz für Data Guard. Alle Befehle sollten als oracle-Benutzer-ID ausgeführt werden.

1. Prüfen Sie zunächst die Konfiguration der primären Datenbank auf der primären EC2 Instanz. In dieser Demonstration haben wir eine primäre Oracle-Datenbank namens db1 auf der primären EC2-DB-Instanz mit zwei ASM-Datenträgergruppen +DATA und +LOGS in Standalone-Restart-Konfiguration eingerichtet. Die primären ASM-Festplattengruppen können sich auf jedem beliebigen Storage innerhalb des EC2-Ecosystems befinden.
2. Befolgen Sie die Anweisungen in der Dokumentation "[TR-4965: Oracle Database Deployment and Protection in AWS FSX/EC2 with iSCSI/ASM](#)" Grid und Oracle auf EC2 Standby-DB-Instanz installieren und konfigurieren, um mit der primären Datenbank abzugleichen. Der Datenbank-Storage sollte bereitgestellt und der Standby-EC2-DB-Instanz von FSX ONTAP mit derselben Speicherkapazität wie die primäre EC2-DB-Instanz zugewiesen werden.



Stoppen Sie bei Schritt 10 in Oracle database installation Abschnitt. Die Standby-Datenbank wird mit der DBCA-Datenbankduplizierungsfunktion aus der primären Datenbank instanziiert.

3. Sobald die Oracle Software installiert und konfiguriert ist, kopieren Sie aus dem im Standby-Modus für ORACLE_HOME festgelegten dbs-Verzeichnis das oracle-Passwort von der primären Datenbank.

```
scp
oracle@172.30.15.45:/u01/app/oracle/product/19.0.0/db1/dbs/orapwdb1
.
```

4. Erstellen Sie die Datei tnsnames.ora mit folgenden Einträgen.

```
# tnsnames.ora Network Configuration File:
/u01/app/oracle/product/19.0.0/db1/network/admin/tnsnames.ora
# Generated by Oracle configuration tools.

db1_NY =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = ip-172-30-15-
45.ec2.internal) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = db1)
    )
  )

db1_LA =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST = ip-172-30-15-
67.ec2.internal) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = db1)
    )
  )
```

5. Fügen Sie den Namen des DB Data Guard-Service zur Listener.ora-Datei hinzu.

```

#Backup file is /u01/app/oracle/crsdata/ip-172-30-15-
67/output/listener.ora.bak.ip-172-30-15-67.oracle line added by
Agent
# listener.ora Network Configuration File:
/u01/app/oracle/product/19.0.0/grid/network/admin/listener.ora
# Generated by Oracle configuration tools.

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST = ip-172-30-15-
67.ec2.internal) (PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
    )
  )

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = db1_LA_DGMGRL.demo.netapp.com)
      (ORACLE_HOME = /u01/app/oracle/product/19.0.0/db1)
      (SID_NAME = db1)
    )
  )

ENABLE_GLOBAL_DYNAMIC_ENDPOINT_LISTENER=ON # line added
by Agent
VALID_NODE_CHECKING_REGISTRATION_LISTENER=ON # line added
by Agent

```

6. Legen Sie oracle-Startseite und -Pfad fest.

```
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
```

```
export PATH=$PATH:$ORACLE_HOME/bin
```

7. Verwenden Sie dbca, um die Standby-Datenbank von der primären Datenbank db1 zu instanzieren.

```

[oracle@ip-172-30-15-67 bin]$ dbca -silent -createDuplicateDB
-gdbName db1 -primaryDBConnectionString ip-172-30-15-
45.ec2.internal:1521/db1_NY.demo.netapp.com -sid db1 -initParams
fal_server=db1_NY -createAsStandby -dbUniqueName db1_LA
Enter SYS user password:

Prepare for db operation
22% complete
Listener config step
44% complete
Auxiliary instance creation
67% complete
RMAN duplicate
89% complete
Post duplicate database operations
100% complete

Look at the log file
"/u01/app/oracle/cfgtoollogs/dbca/db1_LA/db1_LA.log" for further
details.

```

8. Duplizierte Standby-Datenbank validieren Neu duplizierte Standby-Datenbank zunächst im SCHREIBGESCHÜTZTEN Modus geöffnet.

```

[oracle@ip-172-30-15-67 bin]$ export ORACLE_SID=db1
[oracle@ip-172-30-15-67 bin]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Aug 30 18:25:46
2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> select name, open_mode from v$database;

NAME          OPEN_MODE
-----
DB1           READ ONLY

```

```
SQL> show parameter name
```

NAME	TYPE	VALUE
-----	-----	

cdb_cluster_name	string	
cell_offloadgroup_name	string	
db_file_name_convert	string	
db_name	string	db1
db_unique_name	string	db1_LA
global_names	boolean	FALSE
instance_name	string	db1
lock_name_space	string	
log_file_name_convert	string	
pdb_file_name_convert	string	
processor_group_name	string	

NAME	TYPE	VALUE
-----	-----	

service_names	string	
db1_LA.demo.netapp.com		

```
SQL>
```

```
SQL> show parameter log_archive_config
```

NAME	TYPE	VALUE
-----	-----	

log_archive_config	string	
DG_CONFIG=(db1_NY,db1_LA)		

```
SQL> show parameter fal_server
```

NAME	TYPE	VALUE
-----	-----	

fal_server	string	db1_NY

```
SQL> select name from v$datafile;
```

NAME

+DATA/DB1_LA/DATAFILE/system.261.1146248215
+DATA/DB1_LA/DATAFILE/sysaux.262.1146248231
+DATA/DB1_LA/DATAFILE/undotbs1.263.1146248247
+DATA/DB1_LA/03C5C01A66EE9797E0632D0F1EAC5F59/DATAFILE/system.264.11

```
46248253
+DATA/DB1_LA/03C5C01A66EE9797E0632D0F1EAC5F59/DATAFILE/sysaux.265.11
46248261
+DATA/DB1_LA/DATAFILE/users.266.1146248267
+DATA/DB1_LA/03C5C01A66EE9797E0632D0F1EAC5F59/DATAFILE/undotbs1.267.
1146248269
+DATA/DB1_LA/03C5EFD07C41A1FAE0632D0F1EAC9BD8/DATAFILE/system.268.11
46248271
+DATA/DB1_LA/03C5EFD07C41A1FAE0632D0F1EAC9BD8/DATAFILE/sysaux.269.11
46248279
+DATA/DB1_LA/03C5EFD07C41A1FAE0632D0F1EAC9BD8/DATAFILE/undotbs1.270.
1146248285
+DATA/DB1_LA/03C5EFD07C41A1FAE0632D0F1EAC9BD8/DATAFILE/users.271.114
6248293
```

NAME

```
-----
-----
+DATA/DB1_LA/03C5F0DDF35CA2B6E0632D0F1EAC8B6B/DATAFILE/system.272.11
46248295
+DATA/DB1_LA/03C5F0DDF35CA2B6E0632D0F1EAC8B6B/DATAFILE/sysaux.273.11
46248301
+DATA/DB1_LA/03C5F0DDF35CA2B6E0632D0F1EAC8B6B/DATAFILE/undotbs1.274.
1146248309
+DATA/DB1_LA/03C5F0DDF35CA2B6E0632D0F1EAC8B6B/DATAFILE/users.275.114
6248315
+DATA/DB1_LA/03C5F1C9B142A2F1E0632D0F1EACF21A/DATAFILE/system.276.11
46248317
+DATA/DB1_LA/03C5F1C9B142A2F1E0632D0F1EACF21A/DATAFILE/sysaux.277.11
46248323
+DATA/DB1_LA/03C5F1C9B142A2F1E0632D0F1EACF21A/DATAFILE/undotbs1.278.
1146248331
+DATA/DB1_LA/03C5F1C9B142A2F1E0632D0F1EACF21A/DATAFILE/users.279.114
6248337
```

19 rows selected.

```
SQL> select name from v$controlfile;
```

NAME

```
-----
-----
+DATA/DB1_LA/CONTROLFILE/current.260.1146248209
+LOGS/DB1_LA/CONTROLFILE/current.257.1146248209
```

```
SQL> select name from v$tempfile;
```

```
NAME
```

```
-----  
-----  
+DATA/DB1_LA/TEMPFILE/temp.287.1146248371  
+DATA/DB1_LA/03C5C01A66EE9797E0632D0F1EAC5F59/TEMPFILE/temp.288.1146  
248375  
+DATA/DB1_LA/03C5EFD07C41A1FAE0632D0F1EAC9BD8/TEMPFILE/temp.290.1146  
248463  
+DATA/DB1_LA/03C5F0DDF35CA2B6E0632D0F1EAC8B6B/TEMPFILE/temp.291.1146  
248463  
+DATA/DB1_LA/03C5F1C9B142A2F1E0632D0F1EACF21A/TEMPFILE/temp.292.1146  
248463
```

```
SQL> select group#, type, member from v$logfile order by 2, 1;
```

```
GROUP# TYPE MEMBER  
-----  
-----  
1 ONLINE +LOGS/DB1_LA/ONLINELOG/group_1.259.1146248349  
1 ONLINE +DATA/DB1_LA/ONLINELOG/group_1.280.1146248347  
2 ONLINE +DATA/DB1_LA/ONLINELOG/group_2.281.1146248351  
2 ONLINE +LOGS/DB1_LA/ONLINELOG/group_2.258.1146248353  
3 ONLINE +DATA/DB1_LA/ONLINELOG/group_3.282.1146248355  
3 ONLINE +LOGS/DB1_LA/ONLINELOG/group_3.260.1146248355  
4 STANDBY +DATA/DB1_LA/ONLINELOG/group_4.283.1146248357  
4 STANDBY +LOGS/DB1_LA/ONLINELOG/group_4.261.1146248359  
5 STANDBY +DATA/DB1_LA/ONLINELOG/group_5.284.1146248361  
5 STANDBY +LOGS/DB1_LA/ONLINELOG/group_5.262.1146248363  
6 STANDBY +LOGS/DB1_LA/ONLINELOG/group_6.263.1146248365  
6 STANDBY +DATA/DB1_LA/ONLINELOG/group_6.285.1146248365  
7 STANDBY +LOGS/DB1_LA/ONLINELOG/group_7.264.1146248369  
7 STANDBY +DATA/DB1_LA/ONLINELOG/group_7.286.1146248367
```

```
14 rows selected.
```

```
SQL> select name, open_mode from v$database;
```

```
NAME OPEN_MODE  
-----  
DB1 READ ONLY
```

9. Starten Sie die Standby-Datenbank in neu mount Stufen Sie den folgenden Befehl ein, um die von der Standby-Datenbank gemanagte Recovery zu aktivieren.


```
alter database recover managed standby database disconnect from
session;
```

```
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup mount;
ORACLE instance started.
```

```
Total System Global Area 8053062944 bytes
Fixed Size                  9182496 bytes
Variable Size               1291845632 bytes
Database Buffers            6744440832 bytes
Redo Buffers                 7593984 bytes
```

```
Database mounted.
```

```
SQL> alter database recover managed standby database disconnect from
session;
```

```
Database altered.
```

10. Überprüfen Sie den Wiederherstellungsstatus der Standby-Datenbank. Beachten Sie die recovery logmerger In APPLYING_LOG Aktion.

```
SQL> SELECT ROLE, THREAD#, SEQUENCE#, ACTION FROM
V$DATAGUARD_PROCESS;
```

ROLE	THREAD#	SEQUENCE#	ACTION
recovery apply slave	0	0	IDLE
recovery apply slave	0	0	IDLE
recovery apply slave	0	0	IDLE
recovery apply slave	0	0	IDLE
recovery logmerger	1	30	APPLYING_LOG
RFS ping	1	30	IDLE
RFS async	1	30	IDLE
archive redo	0	0	IDLE
archive redo	0	0	IDLE
archive redo	0	0	IDLE
gap manager	0	0	IDLE

ROLE	THREAD#	SEQUENCE#	ACTION
managed recovery	0	0	IDLE
redo transport monitor	0	0	IDLE
log writer	0	0	IDLE
archive local	0	0	IDLE
redo transport timer	0	0	IDLE

```
16 rows selected.
```

```
SQL>
```

Damit ist die Data Guard-Schutzeinrichtung für db1 von primär bis Standby abgeschlossen, wobei die verwaltete Standby-Wiederherstellung aktiviert ist.

Data Guard Broker Einrichten

Oracle Data Guard Broker ist ein verteiltes Management-Framework, das die Erstellung, Wartung und Überwachung von Oracle Data Guard Konfigurationen automatisiert und zentralisiert. Im folgenden Abschnitt wird erläutert, wie Data Guard Broker für die Verwaltung der Data Guard-Umgebung eingerichtet wird.

1. Starten Sie Data Guard Broker sowohl auf primären als auch auf Standby-Datenbanken mit folgendem Befehl über sqlplus.

```
alter system set dg_broker_start=true scope=both;
```

2. Stellen Sie von der primären Datenbank eine Verbindung zu Data Guard Broker als SYSDBA her.

```
[oracle@ip-172-30-15-45 db1]$ dgmgrl sys@db1_NY
DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Aug 30
19:34:14 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights
reserved.

Welcome to DGMGRL, type "help" for information.
Password:
Connected to "db1_NY"
Connected as SYSDBA.
```

3. Erstellen und Aktivieren der Data Guard Broker-Konfiguration.

```
DGMGRL> create configuration dg_config as primary database is db1_NY
connect identifier is db1_NY;
Configuration "dg_config" created with primary database "db1_ny"
DGMGRL> add database db1_LA as connect identifier is db1_LA;
Database "db1_la" added
DGMGRL> enable configuration;
Enabled.
DGMGRL> show configuration;

Configuration - dg_config

Protection Mode: MaxPerformance
Members:
db1_ny - Primary database
db1_la - Physical standby database

Fast-Start Failover: Disabled

Configuration Status:
SUCCESS (status updated 28 seconds ago)
```

4. Überprüfung des Datenbankstatus im Data Guard Broker Management Framework

```
DGMGRL> show database db1_ny;
```

```
Database - db1_ny
```

```
Role:                PRIMARY
Intended State:      TRANSPORT-ON
Instance(s):        db1
```

```
Database Status:
SUCCESS
```

```
DGMGRL> show database db1_la;
```

```
Database - db1_la
```

```
Role:                PHYSICAL STANDBY
Intended State:      APPLY-ON
Transport Lag:       0 seconds (computed 1 second ago)
Apply Lag:           0 seconds (computed 1 second ago)
Average Apply Rate: 2.00 KByte/s
Real Time Query:    OFF
Instance(s):        db1
```

```
Database Status:
SUCCESS
```

```
DGMGRL>
```

Im Falle eines Ausfalls kann Data Guard Broker verwendet werden, um umgehend ein Failover der primären Datenbank in den Standby-Modus durchzuführen.

Clone Standby-Datenbank für andere Anwendungsfälle

Der Hauptvorteil des Staging von Standby-Datenbank auf AWS FSX ONTAP in Data Guard besteht darin, dass mit FlexCloned viele andere Anwendungsfälle mit minimaler zusätzlicher Storage-Investition bedient werden können. Im folgenden Abschnitt zeigen wir, wie man für andere Zwecke wie ENTWICKLUNG, TEST, BERICHT usw. ein Snapshot von den gemounteten und unter Recovery-Standby-Datenbank-Volumes auf FSX ONTAP erstellt und klonet. mit dem Tool NetApp SnapCenter.

Im Folgenden werden allgemeine Verfahren zum Klonen einer LESE-/SCHREIBDATENBANK aus der verwalteten physischen Standby-Datenbank in Data Guard unter Verwendung von SnapCenter beschrieben. Detaillierte Anweisungen zum Einrichten und Konfigurieren von SnapCenter finden Sie unter "[Hybrid-Cloud-Datenbanklösungen mit SnapCenter](#)" Relevant Oracle Sektionen.

1. Wir beginnen damit, eine Testtabelle zu erstellen und eine Zeile in die Testtabelle der primären Datenbank einzufügen. Wir werden dann validieren, wenn die Transaktion in den Standby-Modus und schließlich den Klon durchlaufen wird.

```
[oracle@ip-172-30-15-45 db1]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Aug 31 16:35:53
2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> alter session set container=db1_pdb1;

Session altered.

SQL> create table test(
  2 id integer,
  3 dt timestamp,
  4 event varchar(100));

Table created.

SQL> insert into test values(1, sysdate, 'a test transaction on
primary database db1 and ec2 db host: ip-172-30-15-
45.ec2.internal');

1 row created.

SQL> commit;
```

```
Commit complete.
```

```
SQL> select * from test;
```

```
          ID
-----
DT
-----
EVENT
-----
          1
31-AUG-23 04.49.29.000000 PM
a test transaction on primary database db1 and ec2 db host: ip-172-
30-15-45.ec2.
internal
```

```
SQL> select instance_name, host_name from v$instance;
```

```
INSTANCE_NAME
-----
HOST_NAME
-----
db1
ip-172-30-15-45.ec2.internal
```

2. FSX Storage-Cluster hinzufügen zu `Storage Systems In SnapCenter` mit FSX Clustermanagement-IP und `fsxadmin`-Zugangsdaten.
3. AWS ec2-User zu hinzufügen `Credential In Settings`.
4. Fügen Sie Standby EC2 DB-Instanz hinzu und klonen Sie EC2 DB-Instanz zu `Hosts`.



Für die EC2 DB-Kloninstanz sollten ähnliche Oracle-Software-Stacks installiert und konfiguriert sein. In unserem Testfall wurden die Grid-Infrastruktur und Oracle 19C installiert und konfiguriert, aber es wurde keine Datenbank erstellt.

5. Erstellen einer Backup-Richtlinie, die auf das Offline-/Mounten eines vollständigen Datenbank-Backups zugeschnitten ist
6. Wenden Sie die Sicherungsrichtlinie an, um die Standby-Datenbank in zu schützen `Resources Registerkarte`.

7. Klicken Sie auf Datenbanknamen, um die Seite Datenbank-Backups zu öffnen. Wählen Sie ein Backup aus, das für den Datenbankklon verwendet werden soll, und klicken Sie auf `Clone` Um den Clone-Workflow zu starten.
8. Wählen Sie `Complete Database Clone` Und benennen Sie die Clone-Instanz-SID.
9. Wählen Sie den Clone-Host aus, der die geklonte Datenbank aus der Standby-DB hostet. Akzeptieren Sie die Standardeinstellung für Datendateien, Steuerdateien und Wiederherstellungsprotokolle. Auf dem Clone-Host werden zwei ASM-Laufwerksgruppen erstellt, die den Laufwerksgruppen in der Standby-Datenbank entsprechen.
10. Für die OS-basierte Authentifizierung sind keine Datenbankmeldeinformationen erforderlich. Stimmen Sie die Oracle Home-Einstellung mit den Einstellungen in der EC2 Clone-Datenbankinstanz ab.
11. Ändern Sie ggf. die Parameter der Klondatenbank und geben Sie ggf. Skripte an, die vor dem Clonen ausgeführt werden sollen.
12. Geben Sie SQL ein, um nach dem Klon auszuführen. In der Demo führten wir Befehle aus, um den Datenbank-Archivmodus für eine Entwicklungs-/Test-/Berichtsdatenbank zu deaktivieren.
13. Konfigurieren Sie bei Bedarf die E-Mail-Benachrichtigung.
14. Überprüfen Sie die Zusammenfassung, und klicken Sie auf `Finish` Um den Klon zu starten.
15. Überwachen Sie den Klonjob in `Monitor` Registerkarte. Wir beobachteten, dass es etwa 8 Minuten dauerte, um eine Datenbank mit einer Größe von 300 GB an Datenbank-Volumes zu klonen.
16. Validierung der Klondatenbank von SnapCenter, die sofort bei registriert wird `Resources` Nach dem Klonvorgang rechts abwählen.
17. Abfrage der Klondatenbank von EC2-Instanz des Klons. Wir validierten, dass die Testtransaktion, die in der primären Datenbank auftrat, bis zur Klondatenbank durchläuft war.

```
[oracle@ip-172-30-15-126 ~]$ export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/dev
[oracle@ip-172-30-15-126 ~]$ export ORACLE_SID=db1dev
[oracle@ip-172-30-15-126 ~]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ip-172-30-15-126 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Sep 6 16:41:41 2023
Version 19.18.0.0.0
```


Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production

Version 19.18.0.0.0

SQL> select name, open_mode, log_mode from v\$database;

NAME	OPEN_MODE	LOG_MODE
DB1DEV	READ WRITE	NOARCHIVELOG

SQL> select instance_name, host_name from v\$instance;

INSTANCE_NAME	HOST_NAME
db1dev	ip-172-30-15-126.ec2.internal

SQL> alter session set container=db1_pdb1;

Session altered.

SQL> select * from test;

ID	DT	EVENT
1	31-AUG-23 04.49.29.000000 PM	a test transaction on primary database db1 and ec2 db host: ip-172-30-15-45.ec2. internal

SQL>

Damit ist der Klon und die Validierung einer neuen Oracle-Datenbank aus der Standby-Datenbank in Data Guard auf FSX Storage für ENTWICKLUNG, TESTS, BERICHTE oder andere Anwendungsfälle abgeschlossen. Mehrere Oracle Datenbanken können in derselben Standby-Datenbank in Data Guard geklont werden.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- Data Guard-Konzepte und -Administration

["https://docs.oracle.com/en/database/oracle/oracle-database/19/sbydb/index.html#Oracle%C2%AE-Data-Guard"](https://docs.oracle.com/en/database/oracle/oracle-database/19/sbydb/index.html#Oracle%C2%AE-Data-Guard)

- WP-7357: Oracle Database Deployment on EC2 und FSX Best Practices

["Einführung"](#)

- Amazon FSX für NetApp ONTAP

["https://aws.amazon.com/fsx/netapp-ontap/"](https://aws.amazon.com/fsx/netapp-ontap/)

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

TR-4973: Schnelle Wiederherstellung und Klonen von Oracle VLDB mit Incremental Merge auf AWS FSX ONTAP

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Die Wiederherstellung einer sehr großen Datenbank (VLDB) in Oracle mit dem Backup-Tool Oracle Recovery Manager (RMAN) kann eine große Herausforderung darstellen. Der Datenbankwiederherstellungsprozess von Backup-Medien im Fehlerfall kann zeitaufwändig sein, wodurch die Datenbank-Recovery verzögert wird und möglicherweise Ihr Service Level Agreement (SLA) erheblich beeinträchtigt wird. Ab Version 10g hat Oracle jedoch eine RMAN-Funktion eingeführt, mit der Benutzer Kopien der Oracle-Datenbankdateien auf zusätzlichem Festplattenspeicher auf dem DB-Server-Host erstellen können. Diese Image-Kopien können mit RMAN täglich inkrementell aktualisiert werden. Bei einem Ausfall kann der Datenbankadministrator (DBA) die Oracle-Datenbank schnell von den fehlerhaften Medien auf die Image-Kopie umschalten, sodass keine vollständige Wiederherstellung der Datenbankmedien erforderlich ist. Das Ergebnis ist ein deutlich verbesserter SLA, der allerdings mit der Verdopplung des erforderlichen Datenbank-Storage verbunden ist.

Wenn Sie SLA für Ihre VLDB bevorzugen und erwägen, die Oracle-Datenbank in eine Public Cloud wie AWS zu verschieben, können Sie eine ähnliche Datenbankschutzstruktur mit Ressourcen wie AWS FSX ONTAP für die Bereitstellung Ihrer Standby-Datenbank-Image-Kopie einrichten. In dieser Dokumentation zeigen wir, wie ein NFS-Dateisystem aus AWS FSX ONTAP bereitgestellt und exportiert wird, um auf einem Oracle Datenbankserver gemountet zu werden, damit eine Standby-Datenbankkopie für eine schnelle Recovery bei einem Ausfall des primären Storage bereitgestellt wird.

Besser noch, wir zeigen auch, wie Sie mit NetApp FlexClone eine Kopie desselben Staging-NFS-Filesystems für andere Anwendungsfälle erstellen können, wie z. B. das Einrichten einer Entwicklungs-/Test-Oracle Umgebung mit derselben Standby-Datenbank-Image-Kopie ohne zusätzliche Storage-Investition.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Eine inkrementelle Zusammenführung der Oracle VLDB-Image-Kopie über RMAN auf NFS-Mount Point auf dem AWS FSX ONTAP-Speicher.
- Schnelle Wiederherstellung eines Oracle VLDB durch Umschalten auf Datenbank-Image-Kopie auf FSX ONTAP-Speicher im Falle eines Ausfalls.
- Clone FSX ONTAP NFS-Dateisystem-Volume Speichern einer Oracle VLDB-Image-Kopie für das Einrichten einer anderen Datenbankinstanz für andere Anwendungsfälle verwendet werden.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

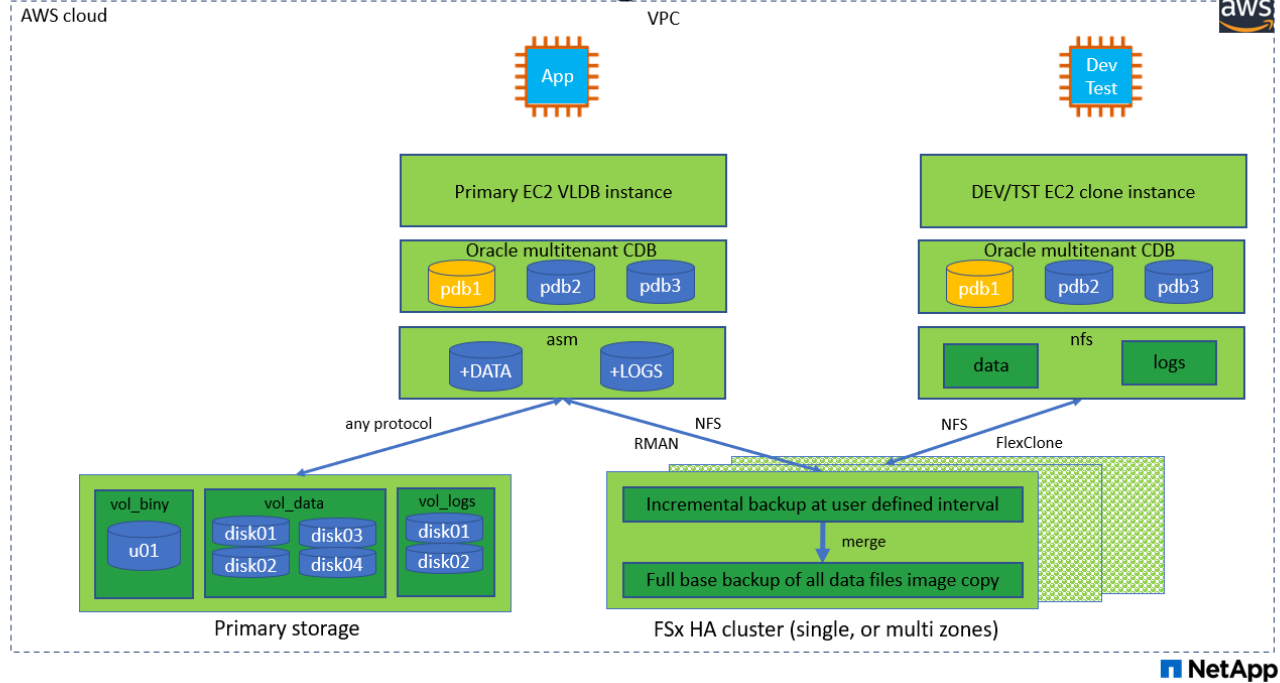
- Ein DBA, der die inkrementelle Zusammenführung von Oracle VLDB-Bildkopien über RMAN in AWS für eine schnellere Datenbank-Recovery einrichtet.
- Ein Datenbanklösungsarchitekt, der Oracle-Workloads in der AWS Public Cloud testet.
- Ein Storage-Administrator managt die auf AWS FSX ONTAP Storage implementierten Oracle-Datenbanken.
- Ein Applikationseigentümer, der Oracle Datenbanken in der AWS FSX/EC2-Umgebung einrichten möchte.

Test- und Validierungsumgebung der Lösung

Das Testen und Validieren dieser Lösung wurde in einer AWS FSX ONTAP- und EC2-Umgebung durchgeführt, die möglicherweise nicht mit der endgültigen Implementierungsumgebung übereinstimmt. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind

Oracle VLDB Incremental Merge via RMAN on AWS FSxN



Hardware- und Softwarekomponenten

Hardware		
FSX ONTAP-Storage	Aktuelle Version von AWS angeboten	Ein FSX HA-Cluster in der gleichen VPC und Verfügbarkeitszone
EC2 Instanz für Computing	t2.xlarge/4vCPU/16G	Zwei EC2 T2 xlarge EC2-Instanzen, eine als primärer DB-Server und die andere als Klon-DB-Server
Software		
Redhat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Bereitstellung der RedHat Subscription für Tests
Oracle Grid Infrastructure	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip

Wichtige Faktoren für die Implementierung

- **Oracle VLDB Speicherlayout für RMAN Incremental Merge.** in unseren Tests und Validierungen wird das NFS-Volumen für Oracle Incremental Backup und Merge von einem einzigen FSX Dateisystem

zugewiesen, das 4 Gbps Durchsatz, 160,000 Raw SSD IOPS und 192 tib Kapazitätslimit hat. Für die Bereitstellung über diese Schwellenwerte können mehrere FSX-Filesysteme parallel mit mehreren NFS-Mount-Punkten verkettet werden, um eine höhere Kapazität zu bieten.

- **Oracle Wiederherstellbarkeit mit RMAN Incremental Merge.** das inkrementelle RMAN Backup und Merge wird in der Regel in einer benutzerdefinierten Frequenz basierend auf Ihren RTO- und RPO-Zielen ausgeführt. Bei einem vollständigen Verlust des primären Storage und/oder archivierter Protokolle kann es zu Datenverlusten kommen. Die Oracle-Datenbank kann bis zum letzten inkrementellen Backup wiederhergestellt werden, das über die FSX Datenbank-Backup-Image-Kopie verfügbar ist. Um den Datenverlust zu minimieren, kann der Oracle Flash Recovery-Bereich auf FSX NFS-Bereitstellungspunkt eingerichtet werden, und archivierte Protokolle werden zusammen mit Datenbank-Image-Kopie auf FSX NFS-Mount gesichert.
- **Ausführung von Oracle VLDB aus FSX NFS-Dateisystem.** im Gegensatz zu anderen Massenspeichern für Datenbank-Backup, AWS FSX ONTAP ist ein Cloud-fähiger Produktionsspeicher, der ein hohes Maß an Performance und Speichereffizienz bietet. Sobald Oracle VLDB vom Primär-Storage zur Image-Kopie im FSX ONTAP NFS-Dateisystem umschaltet, kann die Datenbank-Performance auf hohem Niveau beibehalten werden, während der Ausfall des primären Speichers behoben wird. Sie können sicher sein, dass die Benutzererfahrung bei primären Storage-Ausfällen nicht beeinträchtigt wird.
- **FlexClone Oracle VLDB Image-Kopie von NFS-Volume für andere Anwendungsfälle.** AWS FSX ONTAP FlexClone bietet gemeinsam genutzte Kopien desselben NFS-Daten-Volumes, die beschreibbar sind. Somit können sie für viele andere Anwendungsfälle verwendet werden, wobei die Integrität der Bereitstellung von Oracle VLDB-Image-Kopien auch dann erhalten bleibt, wenn die Oracle-Datenbank gewechselt wird. Dies führt zu enormen Einsparungen bei den Storage-Kosten, da der Platzbedarf für VLDB deutlich reduziert wird. NetApp empfiehlt, die FlexClone-Aktivitäten zu minimieren, wenn die Datenbank zum Kopieren des primären Storage und des Datenbank-Images wechselt, um die Oracle-Performance auf hohem Niveau zu erhalten.
- **EC2 Compute-Instanzen.** in diesen Tests und Validierungen haben wir eine AWS EC2 t2.xlarge-Instanz als Compute-Instanz der Oracle-Datenbank verwendet. NetApp empfiehlt, in der Produktionsumgebung eine EC2-Instanz vom Typ M5 als Computing-Instanz für Oracle zu verwenden, da sie für Datenbank-Workloads optimiert ist. Sie müssen die Größe der EC2-Instanz entsprechend der Anzahl der vCPUs und der Menge des RAM anpassen, basierend auf den tatsächlichen Workload-Anforderungen.
- **FSX Storage HA Cluster Single- oder Multi-Zone-Implementierung.** bei diesen Tests und Validierungen haben wir einen FSX HA-Cluster in einer einzelnen AWS Verfügbarkeitszone implementiert. Für die Implementierung in der Produktion empfiehlt NetApp die Implementierung eines FSX HA-Paars in zwei verschiedenen Verfügbarkeitszonen. Ein FSX HA-Cluster wird in einem HA-Paar bereitgestellt, das in einem Paar aktiv/Passiv-Filesysteme gespiegelt wird, um Redundanz auf Storage-Ebene bereitzustellen. Die Implementierung mit mehreren Zonen verbessert die Hochverfügbarkeit bei einem Ausfall in einer einzelnen AWS Zone noch weiter.
- **FSX Storage-Cluster-Sizing.** ein Amazon FSX for ONTAP Storage-Dateisystem bietet bis zu 160,000 RAW SSD IOPS, einen Durchsatz von bis zu 4 Gbit/s und eine maximale Kapazität von 192 tib. Sie können das Cluster jedoch in Bezug auf die bereitgestellten IOPS, den Durchsatz und die Storage-Grenze (mindestens 1,024 gib) anpassen, basierend auf Ihren tatsächlichen Anforderungen zum Zeitpunkt der Implementierung. Die Kapazität lässt sich spontan dynamisch anpassen, ohne dass die Applikationsverfügbarkeit beeinträchtigt wird.
- **DNFS-Konfiguration.** dNFS ist in den Oracle-Kernel integriert und ist dafür bekannt, die Performance von Oracle-Datenbanken drastisch zu steigern, wenn Oracle auf NFS-Speicher bereitgestellt wird. DNFS ist in Oracle-Binärdatei verpackt, ist aber nicht standardmäßig aktiviert. Sie sollte für jede Oracle Database-Bereitstellung auf NFS aktiviert werden. Für die Bereitstellung mehrerer FSX Dateisysteme für eine VLDB sollte dNFS Multi-Path zu verschiedenen FSX NFS-Dateisystemen ordnungsgemäß konfiguriert werden.

Lösungsimplementierung

Es wird vorausgesetzt, dass Sie bereits Ihre Oracle VLDB in der AWS EC2-Umgebung innerhalb einer VPC implementiert haben. Wenn Sie Hilfe zur Oracle-Implementierung in AWS benötigen, lesen Sie bitte die folgenden technischen Berichte, um Hilfe zu erhalten.

- ["Oracle Database Deployment on EC2 und FSX Best Practices"](#)
- ["Implementierung und Schutz von Oracle Database in AWS FSX/EC2 mit iSCSI/ASM"](#)
- ["Oracle 19c im Standalone-Neustart auf AWS FSX/EC2 mit NFS/ASM"](#)

Ihre Oracle VLDB kann entweder auf einem FSX ONTAP oder einem anderen Speicher der Wahl innerhalb des AWS EC2 Ökosystems ausgeführt werden. Der folgende Abschnitt enthält schrittweise Bereitstellungsverfahren zum Einrichten der inkrementellen Zusammenführung von RMAN mit einer Image-Kopie einer Oracle VLDB, die in einem NFS-Mount vom AWS FSX ONTAP-Speicher bereitgestellt wird.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wurde ein AWS Konto eingerichtet, und die erforderlichen VPC und Netzwerksegmente wurden in Ihrem AWS Konto erstellt.
2. Über die AWS EC2-Konsole müssen Sie zwei EC2 Linux-Instanzen implementieren, eine als primärer Oracle DB Server und einen optionalen alternativen Clone-Ziel-DB-Server. Im Architekturdiagramm im vorherigen Abschnitt finden Sie weitere Details zum Umgebungs-Setup. Sehen Sie sich auch die an ["Benutzerhandbuch für Linux-Instanzen"](#) Finden Sie weitere Informationen.
3. Implementieren Sie über die AWS EC2 Konsole Amazon FSX for ONTAP Storage HA-Cluster, um NFS-Volumes zu hosten, die die Standby-Image-Kopie der Oracle Datenbank speichern. Wenn Sie mit der Bereitstellung von FSX-Speicher nicht vertraut sind, lesen Sie die Dokumentation ["Erstellen von FSX für ONTAP-Dateisysteme"](#) Schritt-für-Schritt-Anleitungen.
4. Die Schritte 2 und 3 können mit dem folgenden Terraform Automatisierungs-Toolkit durchgeführt werden, das eine EC2-Instanz mit dem Namen erstellt `ora_01` Und ein FSX Dateisystem mit dem Namen `fsx_01`. Überprüfen Sie die Anweisung sorgfältig, und ändern Sie die Variablen vor der Ausführung entsprechend Ihrer Umgebung. Sie können die Vorlage ganz einfach an Ihre eigenen Implementierungsanforderungen anpassen.

```
git clone https://github.com/NetApp-  
Automation/na_aws_fsx_ec2_deploy.git
```



Stellen Sie sicher, dass Sie mindestens 50G im Root-Volume der EC2-Instanz zugewiesen haben, damit genügend Speicherplatz für die Bereitstellung der Oracle Installationsdateien zur Verfügung steht.

NFS-Volume bereitstellen und exportieren, das an EC2 DB Instanz-Host gemountet werden soll

In dieser Demonstration zeigen wir, wie man ein NFS-Volumen von der Kommandozeile bereitstellt, indem man sich bei einem FSX Cluster über ssh als fsxadmin Benutzer über FSX Cluster Management IP anmeldet. Alternativ kann das Volume auch über die AWS FSX Konsole zugewiesen werden. Wiederholen Sie die Verfahren auf anderen FSX-Dateisystemen, wenn mehr als ein FSX Dateisystem eingerichtet sind, um die Größe der Datenbank aufzunehmen.

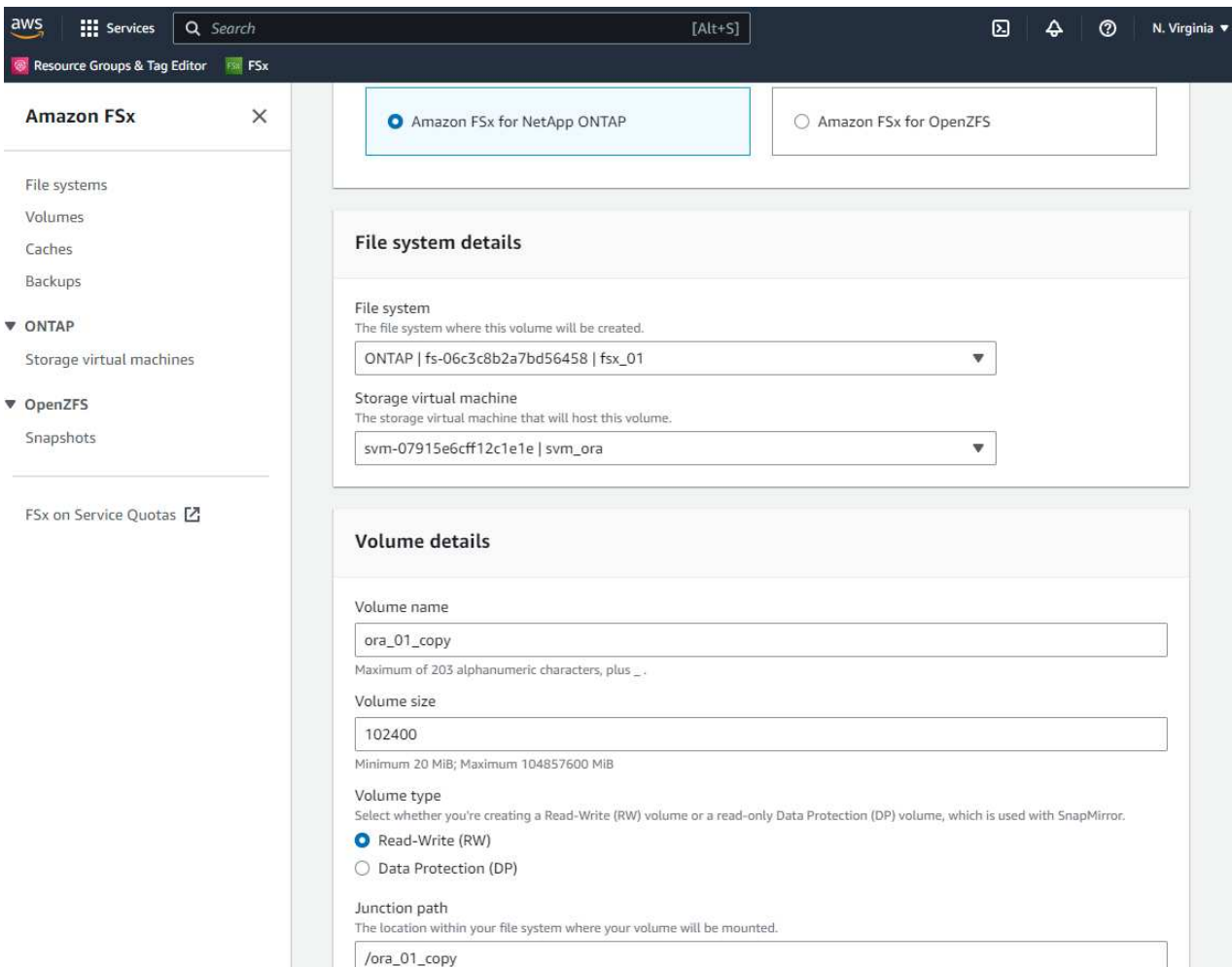
1. Stellen Sie zunächst NFS-Volume über CLI bereit, indem Sie sich am FSX-Cluster über SSH als fsxadmin-Benutzer anmelden. Ändern Sie Ihre FSX Cluster-Management-IP-Adresse, die von der AWS FSX ONTAP UI-Konsole abgerufen werden kann.

```
ssh fsxadmin@172.30.15.53
```

2. Erstellen Sie ein NFS-Volume in der gleichen Größe wie Ihr primärer Speicher, um die primären Datendateien der Oracle VLDB-Datenbank zu speichern.

```
vol create -volume ora_01_copy -aggregate aggr1 -size 100G -state  
online -type RW -junction-path /ora_01_copy -snapshot-policy none  
-tiering-policy snapshot-only
```

3. Alternativ kann das Volume über die Benutzeroberfläche der AWS FSX Konsole mit Optionen bereitgestellt werden: Storage-Effizienz Enabled, Sicherheitsstil Unix , Snapshot-Richtlinie None`Und Storage Tiering `Snapshot Only Wie unten gezeigt.



- Erstellen Sie eine angepasste Snapshot-Richtlinie für oracle-Datenbanken mit einem täglichen Zeitplan und einer Aufbewahrung von 30 Tagen. Sie sollten die Richtlinie hinsichtlich Snapshot-Häufigkeit und Aufbewahrungsfenster an Ihre spezifischen Anforderungen anpassen.

```
snapshot policy create -policy oracle -enabled true -schedule1 daily
-count1 30
```

Wenden Sie die Richtlinie auf das bereitgestellte NFS-Volume für das inkrementelle RMAN-Backup und -Zusammenführen an.

```
vol modify -volume ora_01_copy -snapshot-policy oracle
```

- Melden Sie sich bei EC2-Instanz als ec2-user an und erstellen Sie ein Verzeichnis /nfsfxn. Erstellen Sie zusätzliche Mount-Point-Verzeichnisse für zusätzliche FSX-Dateisysteme.

```
sudo mkdir /nfsfsxn
```

- FSX ONTAP-NFS-Volume auf EC2-DB-Instanz-Host mounten. Ändern Sie zu Ihrer FSX virtuellen Server NFS-LIF-Adresse. Die NFS-LIF-Adresse kann von der FSX ONTAP UI Konsole abgerufen

werden.

```
sudo mount 172.30.15.19:/ora_01_copy /nfsfsxn -o  
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=262144,ws  
ize=262144,noi  
tr
```

7. Ändern Sie Mount Point Ownership in oracle:oisntall, ändern Sie ggf. Ihren oracle-Benutzernamen und die primäre Gruppe.

```
sudo chown oracle:oinstall /nfsfsxn
```

Einrichtung der inkrementellen Zusammenführung von Oracle RMAN mit Image Copy auf FSX

RMAN Incremental Merge Aktualisieren Sie die Staging-Datenbank-Datendateien-Image-Kopie kontinuierlich bei jedem inkrementellen Backup/Merge-Intervall. Die Image-Kopie der Datenbanksicherung ist so aktuell wie die Häufigkeit, in der Sie die inkrementelle Sicherung/Zusammenführung durchführen. Berücksichtigen Sie also die Datenbankleistung, Ihre RTO- und RPO-Ziele bei der Entscheidung über die Häufigkeit der inkrementellen Backups und Merge von RMAN.

1. Melden Sie sich bei der primären EC2-Instanz des DB-Servers als oracle-Benutzer an
2. Erstellen Sie ein oracopy-Verzeichnis unter Mount Point /nfsfsxn, um oracle-Datendateien-Image-Kopien und das archlog-Verzeichnis für den Oracle Flash-Recovery-Bereich zu speichern.

```
mkdir /nfsfsxn/oracopy
```

```
mkdir /nfsfsxn/archlog
```

3. Melden Sie sich bei der Oracle-Datenbank über sqlplus an, aktivieren Sie die Nachverfolgung von Blockänderungen für schnellere inkrementelle Backups und ändern Sie den Oracle Flash-Recovery-Bereich in den FSxN-Mount-Bereich, wenn er sich derzeit im Primärspeicher befindet. Auf diese Weise können die RMAN-Standardsteuerdatei/die SPFile-automatischen Backups und archivierte Protokolle zum Recovery auf dem FSxN-NFS-Mount gesichert werden.

```
sqlplus / as sysdba
```

Führen Sie an der Eingabeaufforderung sqlplus folgenden Befehl aus.

```
alter database enable block change tracking using file  
'/nfsfsxn/oracopy/bct_db1.ctf'
```

```
alter system set db_recovery_file_dest='/nfsfsxn/archlog/'  
scope=both;
```

4. Erstellen Sie ein RMAN-Backup und ein inkrementelles Merge-Skript. Das Skript weist mehrere Kanäle für die parallele Sicherung und Zusammenführung von RMAN zu. Bei der ersten Ausführung würde die erste vollständige Basisplan-Image-Kopie erzeugt. In einem vollständigen Durchlauf löscht es zunächst veraltete Backups, die sich außerhalb des Aufbewahrungsfensters befinden, um den Staging-Bereich sauber zu halten. Es schaltet dann die aktuelle Protokolldatei vor dem Zusammenführen und Sichern um. Das inkrementelle Backup folgt der Zusammenführung, sodass die Kopie des Datenbank-Images den aktuellen Datenbankstatus um einen Sicherungs-/Mergezyklus zurückverfolgt. Die Merge- und Backup-Reihenfolge kann rückgängig gemacht werden, um die Wiederherstellung nach Belieben des Benutzers zu beschleunigen. Das RMAN-Skript kann in ein einfaches Shell-Skript integriert werden, das von crontab auf dem primären DB-Server ausgeführt wird. Stellen Sie sicher, dass die automatische Sicherung der Steuerdatei in der RMAN-Einstellung aktiviert ist.

```
vi /home/oracle/rman_bkup_merge.cmd
```

Add following lines:

```
RUN
```

```
{  
  allocate channel c1 device type disk format '/nfsfsxn/oracopy/%U';  
  allocate channel c2 device type disk format '/nfsfsxn/oracopy/%U';  
  allocate channel c3 device type disk format '/nfsfsxn/oracopy/%U';  
  allocate channel c4 device type disk format '/nfsfsxn/oracopy/%U';  
  delete obsolete;  
  sql 'alter system archive log current';  
  recover copy of database with tag 'OraCopyBKUPonFSxN_level_0';  
  backup incremental level 1 copies=1 for recover of copy with tag  
'OraCopyBKUPonFSxN_level_0' database;  
}
```

5. Melden Sie sich am EC2 DB-Server lokal als oracle-Benutzer mit oder ohne RMAN-Katalog bei RMAN an. In dieser Demo stellen wir keine Verbindung zu einem RMAN-Katalog her.

```
rman target / nocatalog;
```

output:

```
[oracle@ip-172-30-15-99 ~]$ rman target / nocatalog;
```

```
Recovery Manager: Release 19.0.0.0.0 - Production on Wed May 24  
17:44:49 2023  
Version 19.18.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights  
reserved.
```

```
connected to target database: DB1 (DBID=1730530050)  
using target database control file instead of recovery catalog
```

```
RMAN>
```

6. Führen Sie an der Eingabeaufforderung von RMAN das Skript aus. Bei der ersten Ausführung wird eine Kopie des Basisgrads der Datenbank erstellt, und die nachfolgenden Ausführungen werden zusammengeführt und die Basisgrafkopie schrittweise aktualisiert. Im Folgenden wird beschrieben, wie das Skript und die typische Ausgabe ausgeführt werden. Legen Sie die Anzahl der Kanäle fest, die den CPU-Kernen auf dem Host entsprechen.

```
RMAN> @/home/oracle/rman_bkup_merge.cmd
```

```

RMAN> RUN
2> {
3>  allocate channel c1 device type disk format
   '/nfsfsxn/oracopy/%U';
4>  allocate channel c2 device type disk format
   '/nfsfsxn/oracopy/%U';
5>  allocate channel c3 device type disk format
   '/nfsfsxn/oracopy/%U';
6>  allocate channel c4 device type disk format
   '/nfsfsxn/oracopy/%U';
7>  delete obsolete;
8>  sql 'alter system archive log current';
9>  recover copy of database with tag 'OraCopyBKUPonFSxN_level_0';
10> backup incremental level 1 copies=1 for recover of copy with
tag 'OraCopyBKUPonFSxN_level_0' database;
11> }

allocated channel: c1
channel c1: SID=411 device type=DISK

allocated channel: c2
channel c2: SID=146 device type=DISK

allocated channel: c3
channel c3: SID=402 device type=DISK

allocated channel: c4
channel c4: SID=37 device type=DISK

Starting recover at 17-MAY-23
no copy of datafile 1 found to recover
no copy of datafile 3 found to recover
no copy of datafile 4 found to recover
no copy of datafile 5 found to recover
no copy of datafile 6 found to recover
no copy of datafile 7 found to recover
.
.
Finished recover at 17-MAY-23

Starting backup at 17-MAY-23
channel c1: starting incremental level 1 datafile backup set
channel c1: specifying datafile(s) in backup set
input datafile file number=00022
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.287.113

```

```
7018311
input datafile file number=00026
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.291.113
7018481
input datafile file number=00030
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.295.113
7018787
input datafile file number=00011
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/undotbs1.27
1.1136668041
input datafile file number=00035
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.300.113
7019181
channel c1: starting piece 1 at 17-MAY-23
channel c2: starting incremental level 1 datafile backup set
channel c2: specifying datafile(s) in backup set
input datafile file number=00023
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.288.113
7018359
input datafile file number=00027
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.292.113
7018523
input datafile file number=00031
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.296.113
7018837
input datafile file number=00009
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/system.272.
1136668041
input datafile file number=00034
name=+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.299.113
7019117
.
.
Finished backup at 17-MAY-23

Starting Control File and SPFILE Autobackup at 17-MAY-23
piece
handle=+LOGS/DB1/AUTOBACKUP/2023_05_17/s_1137095435.367.1137095435
comment=NONE
Finished Control File and SPFILE Autobackup at 17-MAY-23
released channel: c1
released channel: c2
released channel: c3
released channel: c4

RMAN> **end-of-file**
```

7. Führen Sie nach dem Backup eine Datenbank-Image-Kopie auf, um zu beobachten, dass im FSX ONTAP NFS-Bereitstellungspunkt eine Datenbank-Image-Kopie erstellt wurde.

```

RMAN> list copy of database tag 'OraCopyBKUPonFSxN_level_0';

List of Datafile Copies
=====

Key          File S Completion Time Ckp SCN      Ckp Time      Sparse
-----
19           1    A 17-MAY-23      3009819      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
      SYSTEM_FNO-1_0h1sd7ae
      Tag: ORACOPYBKUPONFSXN_LEVEL_0

20           3    A 17-MAY-23      3009826      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
      SYSAUX_FNO-3_0i1sd7at
      Tag: ORACOPYBKUPONFSXN_LEVEL_0

21           4    A 17-MAY-23      3009830      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
      UNDOTBS1_FNO-4_0j1sd7b4
      Tag: ORACOPYBKUPONFSXN_LEVEL_0

27           5    A 17-MAY-23      2383520      12-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
      SYSTEM_FNO-5_0p1sd7cf
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 2, PDB Name: PDB$SEED

26           6    A 17-MAY-23      2383520      12-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
      SYSAUX_FNO-6_0o1sd7c8
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 2, PDB Name: PDB$SEED

34           7    A 17-MAY-23      3009907      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
      7_101sd7dl
      Tag: ORACOPYBKUPONFSXN_LEVEL_0

33           8    A 17-MAY-23      2383520      12-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
      UNDOTBS1_FNO-8_0v1sd7di
      Tag: ORACOPYBKUPONFSXN_LEVEL_0

```

Container ID: 2, PDB Name: PDB\$SEED

```
28      9      A 17-MAY-23      3009871      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-9_0q1sd7cm
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 3, PDB Name: DB1_PDB1

22      10     A 17-MAY-23      3009849      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSAUX_FNO-10_0k1sd7bb
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 3, PDB Name: DB1_PDB1

25      11     A 17-MAY-23      3009862      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-11_0n1sd7c1
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 3, PDB Name: DB1_PDB1

35      12     A 17-MAY-23      3009909      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
12_111sd7dm
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 3, PDB Name: DB1_PDB1

29      13     A 17-MAY-23      3009876      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-13_0r1sd7ct
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 4, PDB Name: DB1_PDB2

23      14     A 17-MAY-23      3009854      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSAUX_FNO-14_0l1sd7bi
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 4, PDB Name: DB1_PDB2

31      15     A 17-MAY-23      3009900      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-15_0t1sd7db
      Tag: ORACOPYBKUPONFSXN_LEVEL_0
      Container ID: 4, PDB Name: DB1_PDB2

36      16     A 17-MAY-23      3009911      17-MAY-23      NO
      Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
```

```

16_121sd7dn
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 4, PDB Name: DB1_PDB2

30      17      A 17-MAY-23      3009895      17-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-17_0s1sd7d4
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 5, PDB Name: DB1_PDB3

24      18      A 17-MAY-23      3009858      17-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSAUX_FNO-18_0m1sd7bq
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 5, PDB Name: DB1_PDB3

32      19      A 17-MAY-23      3009903      17-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-19_0u1sd7de
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 5, PDB Name: DB1_PDB3

37      20      A 17-MAY-23      3009914      17-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
20_131sd7do
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 5, PDB Name: DB1_PDB3

4       21      A 17-MAY-23      3009019      17-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
21_021sd6pv
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 3, PDB Name: DB1_PDB1

5       22      A 17-MAY-23      3009419      17-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
22_031sd6r2
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 3, PDB Name: DB1_PDB1

6       23      A 17-MAY-23      3009460      17-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
23_041sd6s5
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 3, PDB Name: DB1_PDB1

```


7	24	A	17-MAY-23	3009473	17-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
24_051sd6t9						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
8	25	A	17-MAY-23	3009502	17-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
25_061sd6uc						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
9	26	A	17-MAY-23	3009548	17-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
26_071sd6vf						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
10	27	A	17-MAY-23	3009576	17-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
27_081sd70i						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
11	28	A	17-MAY-23	3009590	17-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
28_091sd71l						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
12	29	A	17-MAY-23	3009619	17-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
29_0a1sd72o						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
13	30	A	17-MAY-23	3009648	17-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
30_0b1sd73r						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
14	31	A	17-MAY-23	3009671	17-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
31_0c1sd74u						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						

```

Container ID: 3, PDB Name: DB1_PDB1

15      32      A 17-MAY-23      3009729      17-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
32_0d1sd762
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

16      33      A 17-MAY-23      3009743      17-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
33_0e1sd775
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

17      34      A 17-MAY-23      3009771      17-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
34_0f1sd788
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

18      35      A 17-MAY-23      3009805      17-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
35_0g1sd79b
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

```

RMAN>

8. Melden Sie das Schema von der Oracle RMAN-Eingabeaufforderung, um zu beobachten, dass sich die aktuellen aktiven Datenbankdatendateien in der primären Speichergruppe ASM +DATA befinden.

```

RMAN> report schema;

Report of database schema for database with db_unique_name DB1

List of Permanent Datafiles
=====
File Size(MB) Tablespace          RB segs Datafile Name
-----
1      1060      SYSTEM          YES
+DATA/DB1/DATAFILE/system.257.1136666315
3      810       SYSAUX          NO
+DATA/DB1/DATAFILE/sysaux.258.1136666361
4      675       UNDOTBS1        YES
+DATA/DB1/DATAFILE/undotbs1.259.1136666385

```

```

5      400      PDB$SEED:SYSTEM      NO
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/system.266.11366
67165
6      460      PDB$SEED:SYSAUX      NO
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/sysaux.267.11366
67165
7      5        USERS      NO
+DATA/DB1/DATAFILE/users.260.1136666387
8      230      PDB$SEED:UNDOTBS1      NO
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/undotbs1.268.113
6667165
9      400      DB1_PDB1:SYSTEM      YES
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/system.272.11366
68041
10     490      DB1_PDB1:SYSAUX      NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/sysaux.273.11366
68041
11     465      DB1_PDB1:UNDOTBS1      YES
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/undotbs1.271.113
6668041
12     5        DB1_PDB1:USERS      NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/users.275.113666
8057
13     400      DB1_PDB2:SYSTEM      YES
+DATA/DB1/FB867EA89ECF81C0E053630F1EACB901/DATAFILE/system.277.11366
68057
14     470      DB1_PDB2:SYSAUX      NO
+DATA/DB1/FB867EA89ECF81C0E053630F1EACB901/DATAFILE/sysaux.278.11366
68057
15     235      DB1_PDB2:UNDOTBS1      YES
+DATA/DB1/FB867EA89ECF81C0E053630F1EACB901/DATAFILE/undotbs1.276.113
6668057
16     5        DB1_PDB2:USERS      NO
+DATA/DB1/FB867EA89ECF81C0E053630F1EACB901/DATAFILE/users.280.113666
8071
17     400      DB1_PDB3:SYSTEM      YES
+DATA/DB1/FB867F8A4D4F821CE053630F1EAC69CC/DATAFILE/system.282.11366
68073
18     470      DB1_PDB3:SYSAUX      NO
+DATA/DB1/FB867F8A4D4F821CE053630F1EAC69CC/DATAFILE/sysaux.283.11366
68073
19     235      DB1_PDB3:UNDOTBS1      YES
+DATA/DB1/FB867F8A4D4F821CE053630F1EAC69CC/DATAFILE/undotbs1.281.113
6668073
20     5        DB1_PDB3:USERS      NO
+DATA/DB1/FB867F8A4D4F821CE053630F1EAC69CC/DATAFILE/users.285.113666

```

8087

21 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.286.11370182
39
22 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.287.11370183
11
23 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.288.11370183
59
24 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.289.11370184
05
25 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.290.11370184
43
26 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.291.11370184
81
27 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.292.11370185
23
28 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.293.11370187
07
29 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.294.11370187
45
30 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.295.11370187
87
31 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.296.11370188
37
32 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.297.11370189
35
33 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.298.11370190
77
34 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.299.11370191
17
35 4096 DB1_PDB1:SOE NO
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/DATAFILE/soe.300.11370191
81

List of Temporary Files

=====

File	Size (MB)	Tablespace	Maxsize (MB)	Tempfile Name
1	123	TEMP	32767	+DATA/DB1/TEMPFILE/temp.265.1136666447
2	123	PDB\$SEED:TEMP	32767	+DATA/DB1/FB864A929AEB79B9E053630F1EAC7046/TEMPFILE/temp.269.1136667185
3	10240	DB1_PDB1:TEMP	32767	+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/TEMPFILE/temp.274.1136668051
4	123	DB1_PDB2:TEMP	32767	+DATA/DB1/FB867EA89ECF81C0E053630F1EACB901/TEMPFILE/temp.279.1136668067
5	123	DB1_PDB3:TEMP	32767	+DATA/DB1/FB867F8A4D4F821CE053630F1EAC69CC/TEMPFILE/temp.284.1136668081

RMAN>

9. Validieren der Datenbank-Image-Kopie vom NFS-Bereitstellungspunkt des Betriebssystems

```
[oracle@ip-172-30-15-99 ~]$ ls -l /nfsfsxn/oracopy/
total 70585148
-rw-r----- 1 oracle asm 4294975488 May 17 18:09 data_D-DB1_I-
1730530050_TS-SOE_FNO-21_021sd6pv
-rw-r----- 1 oracle asm 4294975488 May 17 18:10 data_D-DB1_I-
1730530050_TS-SOE_FNO-22_031sd6r2
-rw-r----- 1 oracle asm 4294975488 May 17 18:10 data_D-DB1_I-
1730530050_TS-SOE_FNO-23_041sd6s5
-rw-r----- 1 oracle asm 4294975488 May 17 18:11 data_D-DB1_I-
1730530050_TS-SOE_FNO-24_051sd6t9
-rw-r----- 1 oracle asm 4294975488 May 17 18:11 data_D-DB1_I-
1730530050_TS-SOE_FNO-25_061sd6uc
-rw-r----- 1 oracle asm 4294975488 May 17 18:12 data_D-DB1_I-
1730530050_TS-SOE_FNO-26_071sd6vf
-rw-r----- 1 oracle asm 4294975488 May 17 18:13 data_D-DB1_I-
1730530050_TS-SOE_FNO-27_081sd70i
-rw-r----- 1 oracle asm 4294975488 May 17 18:13 data_D-DB1_I-
1730530050_TS-SOE_FNO-28_091sd71l
-rw-r----- 1 oracle asm 4294975488 May 17 18:14 data_D-DB1_I-
1730530050_TS-SOE_FNO-29_0a1sd72o
-rw-r----- 1 oracle asm 4294975488 May 17 18:14 data_D-DB1_I-
```

```

1730530050_TS-SOE_FNO-30_0b1sd73r
-rw-r----- 1 oracle asm 4294975488 May 17 18:15 data_D-DB1_I-
1730530050_TS-SOE_FNO-31_0c1sd74u
-rw-r----- 1 oracle asm 4294975488 May 17 18:16 data_D-DB1_I-
1730530050_TS-SOE_FNO-32_0d1sd762
-rw-r----- 1 oracle asm 4294975488 May 17 18:16 data_D-DB1_I-
1730530050_TS-SOE_FNO-33_0e1sd775
-rw-r----- 1 oracle asm 4294975488 May 17 18:17 data_D-DB1_I-
1730530050_TS-SOE_FNO-34_0f1sd788
-rw-r----- 1 oracle asm 4294975488 May 17 18:17 data_D-DB1_I-
1730530050_TS-SOE_FNO-35_0g1sd79b
-rw-r----- 1 oracle asm 513810432 May 17 18:18 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-10_0k1sd7bb
-rw-r----- 1 oracle asm 492838912 May 17 18:18 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-14_0l1sd7bi
-rw-r----- 1 oracle asm 492838912 May 17 18:18 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-18_0m1sd7bq
-rw-r----- 1 oracle asm 849354752 May 17 18:18 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-3_0i1sd7at
-rw-r----- 1 oracle asm 482353152 May 17 18:18 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-6_0o1sd7c8
-rw-r----- 1 oracle asm 1111498752 May 17 18:18 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-1_0h1sd7ae
-rw-r----- 1 oracle asm 419438592 May 17 18:19 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-13_0r1sd7ct
-rw-r----- 1 oracle asm 419438592 May 17 18:19 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-17_0s1sd7d4
-rw-r----- 1 oracle asm 419438592 May 17 18:19 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-5_0p1sd7cf
-rw-r----- 1 oracle asm 419438592 May 17 18:19 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-9_0q1sd7cm
-rw-r----- 1 oracle asm 487596032 May 17 18:18 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-11_0n1sd7c1
-rw-r----- 1 oracle asm 246423552 May 17 18:19 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-15_0t1sd7db
-rw-r----- 1 oracle asm 246423552 May 17 18:19 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-19_0u1sd7de
-rw-r----- 1 oracle asm 707796992 May 17 18:18 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-4_0j1sd7b4
-rw-r----- 1 oracle asm 241180672 May 17 18:19 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-8_0v1sd7di
-rw-r----- 1 oracle asm 5251072 May 17 18:19 data_D-DB1_I-
1730530050_TS-USERS_FNO-12_1l1sd7dm
-rw-r----- 1 oracle asm 5251072 May 17 18:19 data_D-DB1_I-
1730530050_TS-USERS_FNO-16_1t1sd7dn
-rw-r----- 1 oracle asm 5251072 May 17 18:19 data_D-DB1_I-

```

```
1730530050_TS-USERS_FNO-20_131sd7do  
-rw-r----- 1 oracle asm      5251072 May 17 18:19 data_D-DB1_I-  
1730530050_TS-USERS_FNO-7_101sd7d1
```

Damit ist die Einrichtung der Backup- und Merge-Sicherung für das Standby-Image der Oracle-Datenbank abgeschlossen.

Wechseln Sie zur schnellen Wiederherstellung von Oracle DB zu Image Copy

Im Falle eines Fehlers aufgrund eines Problems mit dem primären Storage, wie z. B. Datenverlust oder -Beschädigung, kann die Datenbank im FSX ONTAP NFS-Mount schnell auf die Image-Kopie umgeschaltet und ohne Datenbank-Wiederherstellung in den aktuellen Zustand zurückversetzt werden. Durch die Eliminierung der Medienwiederherstellung wird die Datenbank-Recovery für ein VLDB erheblich beschleunigt. In diesem Anwendungsfall wird davon ausgegangen, dass die Host-Instanz der Datenbank intakt ist und dass die Datenbanksteuerungsdatei sowie archivierte und aktuelle Protokolle für die Recovery verfügbar sind.

1. Melden Sie sich beim EC2-DB-Server-Host als oracle-Benutzer an und erstellen Sie vor dem Wechsel eine Testtabelle.

```
[ec2-user@ip-172-30-15-99 ~]$ sudo su
[root@ip-172-30-15-99 ec2-user]# su - oracle
Last login: Thu May 18 14:22:34 UTC 2023
[oracle@ip-172-30-15-99 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 18 14:30:36
2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> show pdbs

          CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
          2 PDB$SEED                                READ ONLY  NO
          3 DB1_PDB1                                READ WRITE NO
          4 DB1_PDB2                                READ WRITE NO
          5 DB1_PDB3                                READ WRITE NO

SQL> alter session set container=db1_pdb1;

Session altered.

SQL> create table test (id integer, dt timestamp, event
varchar(100));

Table created.

SQL> insert into test values(1, sysdate, 'test oracle incremental
merge switch to copy');
```



```

1 row created.

SQL> commit;

Commit complete.

SQL> select * from test;

          ID
-----
DT
-----
EVENT
-----
          1
18-MAY-23 02.35.37.000000 PM
test oracle incremental merge switch to copy

SQL>

```

2. Simulieren Sie einen Fehler, indem Sie die Datenbank herunterfahren und dann oracle in der Bereitstellungsphase starten.

```

SQL> shutdown abort;
ORACLE instance shut down.
SQL> startup mount;
ORACLE instance started.

Total System Global Area 1.2885E+10 bytes
Fixed Size                  9177880 bytes
Variable Size              1778384896 bytes
Database Buffers          1.1073E+10 bytes
Redo Buffers                24375296 bytes
Database mounted.
SQL>

```

3. Stellen Sie als oracle-Benutzer eine Verbindung zur Oracle-Datenbank über RMAN her, um die Datenbank zum Kopieren zu wechseln.

```

RMAN> switch database to copy;

```

datafile 1 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-1_0h1sd7ae"
datafile 3 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-3_0i1sd7at"
datafile 4 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-4_0j1sd7b4"
datafile 5 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-5_0p1sd7cf"
datafile 6 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-6_0o1sd7c8"
datafile 7 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-7_101sd7d1"
datafile 8 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-8_0v1sd7di"
datafile 9 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-9_0q1sd7cm"
datafile 10 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-10_0k1sd7bb"
datafile 11 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-11_0n1sd7c1"
datafile 12 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-12_111sd7dm"
datafile 13 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-13_0r1sd7ct"
datafile 14 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-14_0l1sd7bi"
datafile 15 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-15_0t1sd7db"
datafile 16 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-16_121sd7dn"
datafile 17 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-17_0s1sd7d4"
datafile 18 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-18_0m1sd7bq"
datafile 19 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-19_0u1sd7de"
datafile 20 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-20_131sd7do"
datafile 21 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-21_021sd6pv"
datafile 22 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-22_031sd6r2"
datafile 23 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-23_041sd6s5"
datafile 24 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-24_051sd6t9"

```
datafile 25 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-25_061sd6uc"  
datafile 26 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-26_071sd6vf"  
datafile 27 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-27_081sd70i"  
datafile 28 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-28_091sd71l"  
datafile 29 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-29_0a1sd72o"  
datafile 30 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-30_0b1sd73r"  
datafile 31 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-31_0c1sd74u"  
datafile 32 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-32_0d1sd762"  
datafile 33 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-33_0e1sd775"  
datafile 34 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-34_0f1sd788"  
datafile 35 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-35_0g1sd79b"
```

4. Stellen Sie die Datenbank wieder her und öffnen Sie sie, um sie vom letzten inkrementellen Backup auf den aktuellen Stand zu bringen.

```
RMAN> recover database;  
  
Starting recover at 18-MAY-23  
allocated channel: ORA_DISK_1  
channel ORA_DISK_1: SID=392 device type=DISK  
channel ORA_DISK_1: starting incremental datafile backup set restore  
channel ORA_DISK_1: specifying datafile(s) to restore from backup  
set  
destination for restore of datafile 00009: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-9_0q1sd7cm  
destination for restore of datafile 00023: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-23_041sd6s5  
destination for restore of datafile 00027: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-27_081sd70i  
destination for restore of datafile 00031: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-31_0c1sd74u  
destination for restore of datafile 00034: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-34_0f1sd788  
channel ORA_DISK_1: reading from backup piece  
/nfsfsxn/oracopy/321sfous_98_1_1
```

```

channel ORA_DISK_1: piece handle=/nfsfsxn/oracopy/321sfous_98_1_1
tag=ORACOPYBKUPONFSXN_LEVEL_0
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup
set
destination for restore of datafile 00010: /nfsfsxn/oracopy/data_D-
DB1_I-1730530050_TS-SYSAUX_FNO-10_0k1sd7bb
destination for restore of datafile 00021: /nfsfsxn/oracopy/data_D-
DB1_I-1730530050_TS-SOE_FNO-21_021sd6pv
destination for restore of datafile 00025: /nfsfsxn/oracopy/data_D-
DB1_I-1730530050_TS-SOE_FNO-25_061sd6uc
.
.
.
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup
set
destination for restore of datafile 00016: /nfsfsxn/oracopy/data_D-
DB1_I-1730530050_TS-USERS_FNO-16_121sd7dn
channel ORA_DISK_1: reading from backup piece
/nfsfsxn/oracopy/3i1sfov0_114_1_1
channel ORA_DISK_1: piece handle=/nfsfsxn/oracopy/3i1sfov0_114_1_1
tag=ORACOPYBKUPONFSXN_LEVEL_0
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup
set
destination for restore of datafile 00020: /nfsfsxn/oracopy/data_D-
DB1_I-1730530050_TS-USERS_FNO-20_131sd7do
channel ORA_DISK_1: reading from backup piece
/nfsfsxn/oracopy/3j1sfov0_115_1_1
channel ORA_DISK_1: piece handle=/nfsfsxn/oracopy/3j1sfov0_115_1_1
tag=ORACOPYBKUPONFSXN_LEVEL_0
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01

starting media recovery
media recovery complete, elapsed time: 00:00:01

Finished recover at 18-MAY-23

RMAN> alter database open;

```

```
Statement processed
```

```
RMAN>
```

5. Überprüfen Sie die Datenbankstruktur von sqlplus nach der Wiederherstellung, um zu beobachten, dass alle Datenbankdatendateien mit Ausnahme von Kontrolle, Temp und aktuellen Log-Dateien sind nun umgeschaltet, um auf FSX ONTAP NFS-Dateisystem kopieren.

```
SQL> select name from v$datafile
       2 union
       3 select name from v$tempfile
       4 union
       5 select name from v$controlfile
       6 union
       7 select member from v$logfile;
```

```
NAME
```

```
-----
-----
+DATA/DB1/CONTROLFILE/current.261.1136666435
+DATA/DB1/FB864A929AEB79B9E053630F1EAC7046/TEMPFILE/temp.269.1136667
185
+DATA/DB1/FB867DA8C68C816EE053630F1EAC2BCF/TEMPFILE/temp.274.1136668
051
+DATA/DB1/FB867EA89ECF81C0E053630F1EACB901/TEMPFILE/temp.279.1136668
067
+DATA/DB1/FB867F8A4D4F821CE053630F1EAC69CC/TEMPFILE/temp.284.1136668
081
+DATA/DB1/ONLINELOG/group_1.262.1136666437
+DATA/DB1/ONLINELOG/group_2.263.1136666437
+DATA/DB1/ONLINELOG/group_3.264.1136666437
+DATA/DB1/TEMPFILE/temp.265.1136666447
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-21_021sd6pv
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-22_031sd6r2
```

```
NAME
```

```
-----
-----
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-23_041sd6s5
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-24_051sd6t9
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-25_061sd6uc
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-26_071sd6vf
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-27_081sd70i
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-28_091sd711
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-29_0a1sd72o
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-30_0b1sd73r
```

```
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-31_0c1sd74u  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-32_0d1sd762  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-33_0e1sd775
```

NAME

```
-----  
-----  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-34_0f1sd788  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-35_0g1sd79b  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-10_0k1sd7bb  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-14_0l1sd7bi  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-18_0m1sd7bq  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-3_0i1sd7at  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-6_0o1sd7c8  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-13_0r1sd7ct  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-17_0s1sd7d4  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-1_0h1sd7ae  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-5_0p1sd7cf
```

NAME

```
-----  
-----  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-9_0q1sd7cm  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-11_0n1sd7c1  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-15_0t1sd7db  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-19_0u1sd7de  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-4_0j1sd7b4  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-8_0v1sd7di  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-12_1l1sd7dm  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-16_121sd7dn  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-20_131sd7do  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-7_101sd7dl
```

43 rows selected.

SQL>

6. Überprüfen Sie in SQL plus den Inhalt der Testtabelle, die wir vor dem Wechsel zum Kopieren eingefügt haben

```

SQL> show pdbs

      CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
      2 PDB$SEED                                     READ ONLY  NO
      3 DB1_PDB1                                     READ WRITE NO
      4 DB1_PDB2                                     READ WRITE NO
      5 DB1_PDB3                                     READ WRITE NO
SQL> alter session set container=db1_pdb1;

Session altered.

SQL> select * from test;

      ID
-----
DT
-----
EVENT
-----
      1
18-MAY-23 02.35.37.000000 PM
test oracle incremental merge switch to copy

SQL>

```

7. Sie könnten die Oracle-Datenbank im FSX-NFS-Mount für einen längeren Zeitraum ohne Performance-Einbußen ausführen, da FSX ONTAP redundanter, hochperformanter Storage auf Produktionsniveau ist. Wenn das Problem mit dem primären Storage behoben ist, können Sie darauf zurückwechseln, indem Sie die inkrementellen Backup-Merge-Prozesse mit minimalen Ausfallzeiten umkehren.

Oracle DB Recovery von Image-Kopie auf verschiedenen EC2 DB-Instanz-Host

Bei einem Ausfall des primären Storage und des EC2 DB-Instanz-Hosts kann die Recovery nicht vom ursprünglichen Server aus durchgeführt werden. Glücklicherweise haben Sie noch eine Backup-Image-Kopie der Oracle-Datenbank auf dem redundanten FSxN NFS-Dateisystem. Sie können schnell eine weitere identische EC2 DB-Instanz bereitstellen und die Image-Kopie Ihres VLDB auf dem neuen EC2 DB-Host über NFS mounten, um Recovery auszuführen. In diesem Abschnitt werden die dazu erforderlichen Schritte Schritt für Schritt erläutert.

1. Fügen Sie eine Zeile in die Testtabelle ein, die wir zuvor für die Wiederherstellung der Oracle-Datenbank auf eine alternative Hostvalidierung erstellt haben.

```
[oracle@ip-172-30-15-99 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Tue May 30 17:21:05
2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> show pdbs

          CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
          2 PDB$SEED                                READ ONLY  NO
          3 DB1_PDB1                                READ WRITE NO
          4 DB1_PDB2                                READ WRITE NO
          5 DB1_PDB3                                READ WRITE NO
SQL> alter session set container=db1_pdb1;

Session altered.

SQL> insert into test values(2, sysdate, 'test recovery on a new EC2
instance host with image copy on FSxN');

1 row created.

SQL> commit;

Commit complete.

SQL> select * from test;
```



```

          ID
-----
DT
-----
EVENT
-----

          1
18-MAY-23 02.35.37.000000 PM
test oracle incremental merge switch to copy

          2
30-MAY-23 05.23.11.000000 PM
test recovery on a new EC2 instance host with image copy on FSxN

SQL>

```

2. Führen Sie als oracle-Benutzer ein inkrementelles RMAN-Backup aus und führen Sie die Transaktion zusammen, um das Backup-Set auf dem FSxN-NFS-Mount zu löschen.

```

[oracle@ip-172-30-15-99 ~]$ rman target / nocatalog

Recovery Manager: Release 19.0.0.0.0 - Production on Tue May 30
17:26:03 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights
reserved.

connected to target database: DB1 (DBID=1730530050)
using target database control file instead of recovery catalog

RMAN> @rman_bkup_merge.cmd

```

3. Fahren Sie den primären EC2 DB-Instanzhost herunter, um einen Totalausfall des Storage und des DB-Server-Hosts zu simulieren.
4. Einführung einer neuen EC2 DB-Instanz Host ora_02 mit gleichem Betriebssystem und derselben Version über die AWS EC2-Konsole Konfigurieren Sie das Kernal des Betriebssystems mit denselben Patches wie den Host des primären EC2-DB-Servers, Oracle Preinstall RPM und fügen Sie dem Host auch Swap-Speicherplatz hinzu. Installieren Sie die gleiche Version und Patches von Oracle wie auf dem primären EC2 DB-Server-Host mit rein softwarebasierter Option. Diese Aufgaben können mit dem NetApp Automatisierungs-Toolkit automatisiert werden, das unter den unten stehenden Links verfügbar ist.

Toolkit: ["na_oracle19c_Deploy"](#)

Dokumentation: ["Automated Deployment of Oracle19c for ONTAP on NFS"](#)

- Konfigurieren Sie die Oracle-Umgebung ähnlich wie die primäre EC2-Datenbankinstanz Host ora_01, z. B. oratab, oralnst.loc und Oracle User .bash_profile. Es empfiehlt sich, diese Dateien auf dem FSxN NFS-Mount-Punkt zu sichern.
- Die Backup-Image-Kopie der Oracle Datenbank im FSxN NFS-Mount wird auf einem FSX-Cluster gespeichert, das AWS Verfügbarkeitszonen umfasst, um Redundanz, hohe Verfügbarkeit und hohe Performance zu ermöglichen. Das NFS-Dateisystem kann einfach auf einem neuen Server montiert werden, soweit das Netzwerk erreichbar ist. Mit den folgenden Verfahren wird die Image-Kopie eines Oracle VLDB-Backups für die Recovery auf den neu zur Verfügung gestellten EC2 DB-Instanz-Host gemountet.

Erstellen Sie als ec2-User den Mount-Punkt.

```
sudo mkdir /nfsfsxn
```

Mounten Sie als ec2-User das NFS-Volume, das die Oracle VLDB Backup-Image-Kopie gespeichert hat.

```
sudo mount 172.30.15.19:/ora_01_copy /nfsfsxn -o
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsiz=262144,wsiz=262144,noi
tr
```

- Validieren Sie die Backup-Image-Kopie der Oracle-Datenbank auf FSxN NFS-Bereitstellungspunkt.

```
[ec2-user@ip-172-30-15-124 ~]$ ls -ltr /nfsfsxn/oracopy
total 78940700
-rw-r-----. 1 oracle 54331 482353152 May 26 18:45 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-6_4m1t508t
-rw-r-----. 1 oracle 54331 419438592 May 26 18:45 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-5_4q1t509n
-rw-r-----. 1 oracle 54331 241180672 May 26 18:45 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-8_4t1t50a6
-rw-r-----. 1 oracle 54331 450560 May 30 15:29 6b1tf6b8_203_1_1
-rw-r-----. 1 oracle 54331 663552 May 30 15:29 6c1tf6b8_204_1_1
-rw-r-----. 1 oracle 54331 122880 May 30 15:29 6d1tf6b8_205_1_1
-rw-r-----. 1 oracle 54331 507904 May 30 15:29 6e1tf6b8_206_1_1
-rw-r-----. 1 oracle 54331 4259840 May 30 15:29 6f1tf6b9_207_1_1
-rw-r-----. 1 oracle 54331 9060352 May 30 15:29 6h1tf6b9_209_1_1
-rw-r-----. 1 oracle 54331 442368 May 30 15:29 6i1tf6b9_210_1_1
-rw-r-----. 1 oracle 54331 475136 May 30 15:29 6j1tf6bb_211_1_1
-rw-r-----. 1 oracle 54331 48660480 May 30 15:29 6g1tf6b9_208_1_1
-rw-r-----. 1 oracle 54331 589824 May 30 15:29 6l1tf6bb_213_1_1
-rw-r-----. 1 oracle 54331 606208 May 30 15:29 6m1tf6bb_214_1_1
-rw-r-----. 1 oracle 54331 368640 May 30 15:29 6o1tf6bb_216_1_1
```

```

-rw-r-----. 1 oracle 54331      368640 May 30 15:29 6p1tf6bc_217_1_1
-rw-r-----. 1 oracle 54331      57344 May 30 15:29 6r1tf6bc_219_1_1
-rw-r-----. 1 oracle 54331      57344 May 30 15:29 6s1tf6bc_220_1_1
-rw-r-----. 1 oracle 54331      57344 May 30 15:29 6t1tf6bc_221_1_1
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-23_3q1t4ut3
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-21_3o1t4ut2
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-27_461t4vt7
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-25_3s1t4v1a
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-22_3p1t4ut3
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-31_4a1t5015
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-29_481t4vt7
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-34_4d1t5058
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-26_451t4vt7
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-24_3r1t4ut3
-rw-r-----. 1 oracle 54331 555753472 May 30 17:26 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-10_4i1t5083
-rw-r-----. 1 oracle 54331 429924352 May 30 17:26 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-9_4n1t509m
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-30_491t5014
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-28_471t4vt7
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-35_4e1t5059
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-32_4b1t501u
-rw-r-----. 1 oracle 54331 487596032 May 30 17:26 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-11_411t508t
-rw-r-----. 1 oracle 54331 4294975488 May 30 17:26 data_D-DB1_I-
1730530050_TS-SOE_FNO-33_4c1t501v
-rw-r-----. 1 oracle 54331 5251072 May 30 17:26 data_D-DB1_I-
1730530050_TS-USERS_FNO-12_4v1t50aa
-rw-r-----. 1 oracle 54331 1121984512 May 30 17:26 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-1_4f1t506m
-rw-r-----. 1 oracle 54331 707796992 May 30 17:26 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-4_4h1t5083

```

```

-rw-r-----. 1 oracle 54331 534781952 May 30 17:26 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-14_4j1t508s
-rw-r-----. 1 oracle 54331 429924352 May 30 17:26 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-13_4o1t509m
-rw-r-----. 1 oracle 54331 429924352 May 30 17:26 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-17_4p1t509m
-rw-r-----. 1 oracle 54331 534781952 May 30 17:26 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-18_4k1t508t
-rw-r-----. 1 oracle 54331 1027612672 May 30 17:26 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-3_4g1t506m
-rw-r-----. 1 oracle 54331 5251072 May 30 17:26 data_D-DB1_I-
1730530050_TS-USERS_FNO-7_4u1t50a6
-rw-r-----. 1 oracle 54331 246423552 May 30 17:26 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-15_4r1t50a6
-rw-r-----. 1 oracle 54331 5251072 May 30 17:26 data_D-DB1_I-
1730530050_TS-USERS_FNO-16_501t50ad
-rw-r-----. 1 oracle 54331 246423552 May 30 17:26 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-19_4s1t50a6
-rw-r-----. 1 oracle 54331 5251072 May 30 17:26 data_D-DB1_I-
1730530050_TS-USERS_FNO-20_511t50ad
-rw-r-----. 1 oracle 54331 2318712832 May 30 17:32 721tfd6b_226_1_1
-rw-r-----. 1 oracle 54331 1813143552 May 30 17:33 701tfd6a_224_1_1
-rw-r-----. 1 oracle 54331 966656 May 30 17:33 731tfdic_227_1_1
-rw-r-----. 1 oracle 54331 5980160 May 30 17:33 751tfdij_229_1_1
-rw-r-----. 1 oracle 54331 458752 May 30 17:33 761tfdin_230_1_1
-rw-r-----. 1 oracle 54331 458752 May 30 17:33 771tfdiq_231_1_1
-rw-r-----. 1 oracle 54331 11091968 May 30 17:33 741tfdij_228_1_1
-rw-r-----. 1 oracle 54331 401408 May 30 17:33 791tfdit_233_1_1
-rw-r-----. 1 oracle 54331 2070708224 May 30 17:33 6v1tfd6a_223_1_1
-rw-r-----. 1 oracle 54331 376832 May 30 17:33 7a1tfdit_234_1_1
-rw-r-----. 1 oracle 54331 1874903040 May 30 17:33 711tfd6b_225_1_1
-rw-r-----. 1 oracle 54331 303104 May 30 17:33 7c1tfdiu_236_1_1
-rw-r-----. 1 oracle 54331 319488 May 30 17:33 7d1tfdi_237_1_1
-rw-r-----. 1 oracle 54331 57344 May 30 17:33 7f1tfdi_239_1_1
-rw-r-----. 1 oracle 54331 57344 May 30 17:33 7g1tfdi_240_1_1
-rw-r-----. 1 oracle 54331 57344 May 30 17:33 7h1tfdi_241_1_1
-rw-r--r--. 1 oracle 54331 12720 May 30 17:33 db1_ctl.sql
-rw-r-----. 1 oracle 54331 11600384 May 30 17:54 bct_db1.ctf

```

8. Überprüfen Sie die verfügbaren archivierten Oracle-Protokolle auf dem FSxN-NFS-Mount für die Wiederherstellung, und notieren Sie sich die letzte Protokollsequenznummer. In diesem Fall ist es 175. Unser Wiederherstellungspunkt liegt bei der Protokollierung der Sequenznummer 176.

```

[ec2-user@ip-172-30-15-124 ~]$ ls -ltr
/nfsfsxn/archlog/DB1/archivelog/2023_05_30
total 5714400

```

```
-r--r----- . 1 oracle 54331      321024 May 30 14:59
ol_mf_1_140__003t9mvn_.arc
-r--r----- . 1 oracle 54331      48996352 May 30 15:29
ol_mf_1_141__01t9qf6r_.arc
-r--r----- . 1 oracle 54331    167477248 May 30 15:44
ol_mf_1_142__02n3x2qb_.arc
-r--r----- . 1 oracle 54331    165684736 May 30 15:46
ol_mf_1_143__02rotwyb_.arc
-r--r----- . 1 oracle 54331    165636608 May 30 15:49
ol_mf_1_144__02x563wh_.arc
-r--r----- . 1 oracle 54331    168408064 May 30 15:51
ol_mf_1_145__031kg2co_.arc
-r--r----- . 1 oracle 54331    169446400 May 30 15:54
ol_mf_1_146__035xpcdt_.arc
-r--r----- . 1 oracle 54331    167595520 May 30 15:56
ol_mf_1_147__03bds8qf_.arc
-r--r----- . 1 oracle 54331    169270272 May 30 15:59
ol_mf_1_148__03gyt7rx_.arc
-r--r----- . 1 oracle 54331    170712576 May 30 16:01
ol_mf_1_149__03mfxl7v_.arc
-r--r----- . 1 oracle 54331    170744832 May 30 16:04
ol_mf_1_150__03qzz0ty_.arc
-r--r----- . 1 oracle 54331    169380864 May 30 16:06
ol_mf_1_151__03wgxdry_.arc
-r--r----- . 1 oracle 54331    169833984 May 30 16:09
ol_mf_1_152__040y85v3_.arc
-r--r----- . 1 oracle 54331    165134336 May 30 16:20
ol_mf_1_153__04ox946w_.arc
-r--r----- . 1 oracle 54331    169929216 May 30 16:22
ol_mf_1_154__04rbv7n8_.arc
-r--r----- . 1 oracle 54331    171903488 May 30 16:23
ol_mf_1_155__04tvlyvn_.arc
-r--r----- . 1 oracle 54331    179061248 May 30 16:25
ol_mf_1_156__04xgfjtl_.arc
-r--r----- . 1 oracle 54331    173593088 May 30 16:26
ol_mf_1_157__04zyg8hw_.arc
-r--r----- . 1 oracle 54331    175999488 May 30 16:27
ol_mf_1_158__052gp9mt_.arc
-r--r----- . 1 oracle 54331    179092992 May 30 16:29
ol_mf_1_159__0551wk7s_.arc
-r--r----- . 1 oracle 54331    175524352 May 30 16:30
ol_mf_1_160__057l46my_.arc
-r--r----- . 1 oracle 54331    173949440 May 30 16:32
ol_mf_1_161__05b2dmwp_.arc
-r--r----- . 1 oracle 54331    184166912 May 30 16:33
ol_mf_1_162__05drbj8n_.arc
```

```

-r--r-----. 1 oracle 54331 173026816 May 30 16:35
o1_mf_1_163__05h8lm1h_.arc
-r--r-----. 1 oracle 54331 174286336 May 30 16:36
o1_mf_1_164__05krsqmh_.arc
-r--r-----. 1 oracle 54331 166092288 May 30 16:37
o1_mf_1_165__05n378pw_.arc
-r--r-----. 1 oracle 54331 177640960 May 30 16:39
o1_mf_1_166__05pmg741_.arc
-r--r-----. 1 oracle 54331 173972992 May 30 16:40
o1_mf_1_167__05s3o01r_.arc
-r--r-----. 1 oracle 54331 178474496 May 30 16:41
o1_mf_1_168__05vmwt34_.arc
-r--r-----. 1 oracle 54331 177694208 May 30 16:43
o1_mf_1_169__05y45qdd_.arc
-r--r-----. 1 oracle 54331 170814976 May 30 16:44
o1_mf_1_170__060kgh33_.arc
-r--r-----. 1 oracle 54331 177325056 May 30 16:46
o1_mf_1_171__063ltvgv_.arc
-r--r-----. 1 oracle 54331 164455424 May 30 16:47
o1_mf_1_172__065d94fq_.arc
-r--r-----. 1 oracle 54331 178252288 May 30 16:48
o1_mf_1_173__067wnwy8_.arc
-r--r-----. 1 oracle 54331 170579456 May 30 16:50
o1_mf_1_174__06b9zdh8_.arc
-r--r-----. 1 oracle 54331 93928960 May 30 17:26
o1_mf_1_175__08c7jc2b_.arc
[ec2-user@ip-172-30-15-124 ~]$

```

9. Setzen Sie als oracle Benutzer DIE Variable ORACLE_HOME auf die aktuelle Oracle Installation auf der neuen EC2-Instanz DB Host ora_02, ORACLE_SID auf die primäre Oracle-Instanz SID. In diesem Fall ist es db1.
10. Erstellen Sie als oracle-Benutzer eine allgemeine Oracle-Init-Datei im Oracle_HOME/dbs-Verzeichnis mit einer Konfiguration der richtigen Administratorverzeichnisse. Vor allem aber Oracle flash recovery area Zeigen Sie auf den FSxN NFS-Mount-Pfad, wie in der primären Oracle VLDB-Instanz definiert. flash recovery area Die Konfiguration wird in Abschnitt demonstriert Setup Oracle RMAN incremental merge to image copy on FSx. Legen Sie die Oracle-Steuerdatei auf FSX ONTAP NFS-Dateisystem fest.

```
vi $ORACLE_HOME/dbs/initdb1.ora
```

Mit folgenden Beispieleinträgen:

```
*.audit_file_dest='/u01/app/oracle/admin/db1/adump'  
*.audit_trail='db'  
*.compatible='19.0.0'  
*.control_files=('/nfsfsxn/oracopy/db1.ctl')  
*.db_block_size=8192  
*.db_create_file_dest='/nfsfsxn/oracopy/'  
*.db_domain='demo.netapp.com'  
*.db_name='db1'  
*.db_recovery_file_dest_size=85899345920  
*.db_recovery_file_dest='/nfsfsxn/archlog/'  
*.diagnostic_dest='/u01/app/oracle'  
*.dispatchers='(PROTOCOL=TCP) (SERVICE=db1XDB)'  
*.enable_pluggable_database=true  
*.local_listener='LISTENER'  
*.nls_language='AMERICAN'  
*.nls_territory='AMERICA'  
*.open_cursors=300  
*.pga_aggregate_target=1024m  
*.processes=320  
*.remote_login_passwordfile='EXCLUSIVE'  
*.sga_target=10240m  
*.undo_tablespace='UNDOTBS1'
```

Die oben genannte init-Datei sollte im Falle einer Abweichung durch eine wiederhergestellte Backup-init-Datei vom primären Oracle DB-Server ersetzt werden.

11. Starten Sie als oracle-Benutzer RMAN, um die Oracle Recovery auf einem neuen EC2 DB Instance-Host auszuführen.

```
[oracle@ip-172-30-15-124 dbs]$ rman target / nocatalog;
```

```
Recovery Manager: Release 19.0.0.0.0 - Production on Wed May 31  
00:56:07 2023  
Version 19.18.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights  
reserved.
```

```
connected to target database (not started)
```

```
RMAN> startup nomount;
```

```
Oracle instance started
```

```
Total System Global Area 12884900632 bytes
```

```
Fixed Size 9177880 bytes
```

```
Variable Size 1778384896 bytes
```

```
Database Buffers 11072962560 bytes
```

```
Redo Buffers 24375296 bytes
```

12. Datenbank-ID festlegen. Die Datenbank-ID kann vom Oracle-Dateinamen der Bildkopie am FSX NFS-Bereitstellungspunkt abgerufen werden.

```
RMAN> set dbid = 1730530050;
```

```
executing command: SET DBID
```

13. Stellen Sie die controlfile aus dem automatischen Backup wieder her. Wenn Oracle controlfile und spfile autobackup aktiviert sind, werden sie in jedem inkrementellen Backup- und Merge-Zyklus gesichert. Die letzte Sicherung wird wiederhergestellt, wenn mehrere Kopien verfügbar sind.


```

RMAN> restore controlfile from autobackup;

Starting restore at 31-MAY-23
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=2 device type=DISK

recovery area destination: /nfsfsxn/archlog
database name (or database unique name) used for search: DB1
channel ORA_DISK_1: AUTOBACKUP
/nfsfsxn/archlog/DB1/autobackup/2023_05_30/o1_mf_s_1138210401__08qlx
rrr_.bkp found in the recovery area
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20230531
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20230530
channel ORA_DISK_1: restoring control file from AUTOBACKUP
/nfsfsxn/archlog/DB1/autobackup/2023_05_30/o1_mf_s_1138210401__08qlx
rrr_.bkp
channel ORA_DISK_1: control file restore from AUTOBACKUP complete
output file name=/nfsfsxn/oracopy/db1.ct1
Finished restore at 31-MAY-23

```

14. Wiederherstellen der init-Datei aus spfile in einen /tmp-Ordner für die Aktualisierung der Parameterdatei später, um mit der primären DB-Instanz zu übereinstimmen.

```

RMAN> restore spfile to pfile '/tmp/archive/initdb1.ora' from
autobackup;

Starting restore at 31-MAY-23
using channel ORA_DISK_1

recovery area destination: /nfsfsxn/archlog
database name (or database unique name) used for search: DB1
channel ORA_DISK_1: AUTOBACKUP
/nfsfsxn/archlog/DB1/autobackup/2023_05_30/o1_mf_s_1138210401__08qlx
rrr_.bkp found in the recovery area
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20230531
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20230530
channel ORA_DISK_1: restoring spfile from AUTOBACKUP
/nfsfsxn/archlog/DB1/autobackup/2023_05_30/o1_mf_s_1138210401__08qlx
rrr_.bkp
channel ORA_DISK_1: SPFILE restore from AUTOBACKUP complete
Finished restore at 31-MAY-23

```

15. Mounten Sie die Steuerdatei und validieren Sie die Image-Kopie des Datenbank-Backup.

```
RMAN> alter database mount;
```

```
released channel: ORA_DISK_1  
Statement processed
```

```
RMAN> list copy of database tag 'OraCopyBKUPonFSxN_level_0';
```

```
List of Datafile Copies
```

```
=====
```

Key	File S	Completion Time	Ckp SCN	Ckp Time	Sparse
316	1 A	30-MAY-23	4120170	30-MAY-23	NO
	Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-1_4f1t506m				
	Tag: ORACOPYBKUPONFSXN_LEVEL_0				
322	3 A	30-MAY-23	4120175	30-MAY-23	NO
	Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-3_4g1t506m				
	Tag: ORACOPYBKUPONFSXN_LEVEL_0				
317	4 A	30-MAY-23	4120179	30-MAY-23	NO
	Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-4_4h1t5083				
	Tag: ORACOPYBKUPONFSXN_LEVEL_0				
221	5 A	26-MAY-23	2383520	12-MAY-23	NO
	Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-5_4q1t509n				
	Tag: ORACOPYBKUPONFSXN_LEVEL_0				
	Container ID: 2, PDB Name: PDB\$SEED				
216	6 A	26-MAY-23	2383520	12-MAY-23	NO
	Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-6_4m1t508t				
	Tag: ORACOPYBKUPONFSXN_LEVEL_0				
	Container ID: 2, PDB Name: PDB\$SEED				
323	7 A	30-MAY-23	4120207	30-MAY-23	NO
	Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-7_4u1t50a6				
	Tag: ORACOPYBKUPONFSXN_LEVEL_0				
227	8 A	26-MAY-23	2383520	12-MAY-23	NO
	Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-8_4t1t50a6				

```

Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 2, PDB Name: PDB$SEED

308      9      A 30-MAY-23      4120158      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-9_4nlt509m
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

307      10     A 30-MAY-23      4120166      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYS_AUX_FNO-10_4ilt5083
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

313      11     A 30-MAY-23      4120154      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-11_4l1t508t
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

315      12     A 30-MAY-23      4120162      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
12_4v1t50aa
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

319      13     A 30-MAY-23      4120191      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-13_4olt509m
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 4, PDB Name: DB1_PDB2

318      14     A 30-MAY-23      4120183      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYS_AUX_FNO-14_4j1t508s
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 4, PDB Name: DB1_PDB2

324      15     A 30-MAY-23      4120199      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-15_4r1t50a6
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 4, PDB Name: DB1_PDB2

325      16     A 30-MAY-23      4120211      30-MAY-23      NO

```

```

Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
16_501t50ad
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 4, PDB Name: DB1_PDB2

320    17    A 30-MAY-23      4120195      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-17_4p1t509m
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 5, PDB Name: DB1_PDB3

321    18    A 30-MAY-23      4120187      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYS_AUX_FNO-18_4k1t508t
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 5, PDB Name: DB1_PDB3

326    19    A 30-MAY-23      4120203      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-19_4s1t50a6
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 5, PDB Name: DB1_PDB3

327    20    A 30-MAY-23      4120216      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
20_511t50ad
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 5, PDB Name: DB1_PDB3

298    21    A 30-MAY-23      4120166      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
21_3o1t4ut2
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

302    22    A 30-MAY-23      4120154      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
22_3p1t4ut3
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

297    23    A 30-MAY-23      4120158      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
23_3q1t4ut3
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

```

306	24	A	30-MAY-23	4120162	30-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
24_3r1t4ut3						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
300	25	A	30-MAY-23	4120166	30-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
25_3s1t4v1a						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
305	26	A	30-MAY-23	4120154	30-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
26_451t4vt7						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
299	27	A	30-MAY-23	4120158	30-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
27_461t4vt7						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
310	28	A	30-MAY-23	4120162	30-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
28_471t4vt7						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
303	29	A	30-MAY-23	4120166	30-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
29_481t4vt7						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
309	30	A	30-MAY-23	4120154	30-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
30_491t5014						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
301	31	A	30-MAY-23	4120158	30-MAY-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
31_4a1t5015						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						

```

Container ID: 3, PDB Name: DB1_PDB1

312      32      A 30-MAY-23      4120162      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
32_4b1t501u
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

314      33      A 30-MAY-23      4120162      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
33_4c1t501v
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

304      34      A 30-MAY-23      4120158      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
34_4d1t5058
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

311      35      A 30-MAY-23      4120154      30-MAY-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
35_4e1t5059
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

```

16. Wechseln Sie zwischen Datenbank und Kopie, um die Recovery ohne Datenbank-Wiederherstellung auszuführen.

```

RMAN> switch database to copy;

Starting implicit crosscheck backup at 31-MAY-23
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=11 device type=DISK
Crosschecked 33 objects
Finished implicit crosscheck backup at 31-MAY-23

Starting implicit crosscheck copy at 31-MAY-23
using channel ORA_DISK_1
Crosschecked 68 objects
Finished implicit crosscheck copy at 31-MAY-23

searching for all files in the recovery area
cataloging files...
cataloging done

```

List of Cataloged Files

=====

File Name:

/nfsfsxn/archlog/DB1/autobackup/2023_05_30/o1_mf_s_1138210401__08qlx
rrr_.bkp

datafile 1 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-1_4f1t506m"
datafile 3 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-3_4g1t506m"
datafile 4 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-4_4h1t5083"
datafile 5 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-5_4q1t509n"
datafile 6 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-6_4m1t508t"
datafile 7 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-7_4u1t50a6"
datafile 8 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-8_4t1t50a6"
datafile 9 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-9_4n1t509m"
datafile 10 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-10_4i1t5083"
datafile 11 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-11_4l1t508t"
datafile 12 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-12_4v1t50aa"
datafile 13 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-13_4o1t509m"
datafile 14 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-14_4j1t508s"
datafile 15 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-15_4r1t50a6"
datafile 16 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-16_501t50ad"
datafile 17 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-17_4p1t509m"
datafile 18 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-18_4k1t508t"
datafile 19 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-19_4s1t50a6"
datafile 20 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-20_511t50ad"
datafile 21 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-21_3o1t4ut2"

```
datafile 22 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-22_3p1t4ut3"
datafile 23 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-23_3q1t4ut3"
datafile 24 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-24_3r1t4ut3"
datafile 25 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-25_3s1t4v1a"
datafile 26 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-26_451t4vt7"
datafile 27 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-27_461t4vt7"
datafile 28 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-28_471t4vt7"
datafile 29 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-29_481t4vt7"
datafile 30 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-30_491t5014"
datafile 31 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-31_4a1t5015"
datafile 32 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-32_4b1t501u"
datafile 33 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-33_4c1t501v"
datafile 34 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-34_4d1t5058"
datafile 35 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-35_4e1t5059"
```

17. Führen Sie die Oracle Recovery bis zum letzten verfügbaren Archivprotokoll im Flash-Recovery-Bereich aus.

```
RMAN> run {
2> set until sequence=176;
3> recover database;
4> }

executing command: SET until clause

Starting recover at 31-MAY-23
using channel ORA_DISK_1

starting media recovery

archived log for thread 1 with sequence 142 is already on disk as
file
```



```
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_142__02n3x2qb_.ar
c
archived log for thread 1 with sequence 143 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_143__02rotwyb_.ar
c
archived log for thread 1 with sequence 144 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_144__02x563wh_.ar
c
archived log for thread 1 with sequence 145 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_145__031kg2co_.ar
c
archived log for thread 1 with sequence 146 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_146__035xpcdt_.ar
c
archived log for thread 1 with sequence 147 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_147__03bds8qf_.ar
c
archived log for thread 1 with sequence 148 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_148__03gyt7rx_.ar
c
archived log for thread 1 with sequence 149 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_149__03mfxl7v_.ar
c
archived log for thread 1 with sequence 150 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_150__03qzz0ty_.ar
c
archived log for thread 1 with sequence 151 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_151__03wgxdry_.ar
c
archived log for thread 1 with sequence 152 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_152__040y85v3_.ar
c
archived log for thread 1 with sequence 153 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_153__04ox946w_.ar
c
```

archived log for thread 1 with sequence 154 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_154__04rbv7n8_.ar
c
archived log for thread 1 with sequence 155 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_155__04tvlyvn_.ar
c
archived log for thread 1 with sequence 156 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_156__04xgfjtl_.ar
c
archived log for thread 1 with sequence 157 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_157__04zyg8hw_.ar
c
archived log for thread 1 with sequence 158 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_158__052gp9mt_.ar
c
archived log for thread 1 with sequence 159 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_159__0551wk7s_.ar
c
archived log for thread 1 with sequence 160 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_160__057146my_.ar
c
archived log for thread 1 with sequence 161 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_161__05b2dmwp_.ar
c
archived log for thread 1 with sequence 162 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_162__05drbj8n_.ar
c
archived log for thread 1 with sequence 163 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_163__05h8lm1h_.ar
c
archived log for thread 1 with sequence 164 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_164__05krsqmh_.ar
c
archived log for thread 1 with sequence 165 is already on disk as
file

```
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_165__05n378pw_.ar
c
archived log for thread 1 with sequence 166 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_166__05pmg741_.ar
c
archived log for thread 1 with sequence 167 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_167__05s3o01r_.ar
c
archived log for thread 1 with sequence 168 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_168__05vmwt34_.ar
c
archived log for thread 1 with sequence 169 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_169__05y45qdd_.ar
c
archived log for thread 1 with sequence 170 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_170__060kgh33_.ar
c
archived log for thread 1 with sequence 171 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_171__0631tvgv_.ar
c
archived log for thread 1 with sequence 172 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_172__065d94fq_.ar
c
archived log for thread 1 with sequence 173 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_173__067wnwy8_.ar
c
archived log for thread 1 with sequence 174 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_174__06b9zdh8_.ar
c
archived log for thread 1 with sequence 175 is already on disk as
file
/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_175__08c7jc2b_.ar
c
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_142__02n3x2q
b_.arc thread=1 sequence=142
archived log file
```

name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_143__02rotwy
b_.arc thread=1 sequence=143
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_144__02x563w
h_.arc thread=1 sequence=144
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_145__031kg2c
o_.arc thread=1 sequence=145
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_146__035xpcd
t_.arc thread=1 sequence=146
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_147__03bds8q
f_.arc thread=1 sequence=147
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_148__03gyt7r
x_.arc thread=1 sequence=148
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_149__03mfxl7
v_.arc thread=1 sequence=149
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_150__03qzz0t
y_.arc thread=1 sequence=150
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_151__03wgxdr
y_.arc thread=1 sequence=151
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_152__040y85v
3_.arc thread=1 sequence=152
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_153__04ox946
w_.arc thread=1 sequence=153
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_154__04rbv7n
8_.arc thread=1 sequence=154
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_155__04tv1yv
n_.arc thread=1 sequence=155
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_156__04xgfjt
l_.arc thread=1 sequence=156
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_157__04zyg8h
w_.arc thread=1 sequence=157
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_158__052gp9m

```
t_.arc thread=1 sequence=158
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_159__0551wk7
s_.arc thread=1 sequence=159
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_160__057146m
y_.arc thread=1 sequence=160
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_161__05b2dmw
p_.arc thread=1 sequence=161
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_162__05drbj8
n_.arc thread=1 sequence=162
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_163__05h81m1
h_.arc thread=1 sequence=163
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_164__05krsqm
h_.arc thread=1 sequence=164
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_165__05n378p
w_.arc thread=1 sequence=165
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_166__05pmg74
l_.arc thread=1 sequence=166
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_167__05s3o01
r_.arc thread=1 sequence=167
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_168__05vmwt3
4_.arc thread=1 sequence=168
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_169__05y45qd
d_.arc thread=1 sequence=169
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_170__060kgh3
3_.arc thread=1 sequence=170
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_171__0631tvq
v_.arc thread=1 sequence=171
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_172__065d94f
q_.arc thread=1 sequence=172
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_173__067wnwy
8_.arc thread=1 sequence=173
```

```
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_174__06b9zdh
8_.arc thread=1 sequence=174
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_05_30/o1_mf_1_175__08c7jc2
b_.arc thread=1 sequence=175
media recovery complete, elapsed time: 00:48:34
Finished recover at 31-MAY-23
```



Für eine schnellere Recovery sollten Sie parallele Sitzungen mit dem Parameter `Recovery_parallelism` aktivieren oder den Grad der Parallelität im Wiederherstellungsbefehl für die Datenbankwiederherstellung angeben: `RECOVER DATABASE PARALLEL (DEGREE d INSTANCES DEFAULT)`; . Im Allgemeinen sollte der Grad der Parallelität der Anzahl der CPU-Kerne auf dem Host entsprechen.

18. Beenden Sie RMAN, melden Sie sich mit sqlplus als oracle-Benutzer an, um die Datenbank zu öffnen und das Protokoll nach einer unvollständigen Recovery zurückzusetzen.

```
SQL> select name, open_mode from v$database;
```

```
NAME          OPEN_MODE
-----
DB1           MOUNTED
```

```
SQL> select member from v$logfile;
```

```
MEMBER
-----
+DATA/DB1/ONLINELOG/group_3.264.1136666437
+DATA/DB1/ONLINELOG/group_2.263.1136666437
+DATA/DB1/ONLINELOG/group_1.262.1136666437
```

```
SQL> alter database rename file
'+DATA/DB1/ONLINELOG/group_1.262.1136666437' to
'/nfsfsxn/oracopy/redo01.log';
```

Database altered.

```
SQL> alter database rename file
'+DATA/DB1/ONLINELOG/group_2.263.1136666437' to
'/nfsfsxn/oracopy/redo02.log';
```

Database altered.

```
SQL> alter database rename file
'+DATA/DB1/ONLINELOG/group_3.264.1136666437' to
'/nfsfsxn/oracopy/redo03.log';
```

Database altered.

```
SQL> alter database open resetlogs;
```

Database altered.

19. Überprüfen Sie die Datenbank, die auf einem neuen Host wiederhergestellt wurde, der die Zeile enthält, die vor dem Ausfall der primären Datenbank eingefügt wurde.

```

SQL> show pdbs

      CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
      2 PDB$SEED                                     READ ONLY  NO
      3 DB1_PDB1                                     READ WRITE NO
      4 DB1_PDB2                                     READ WRITE NO
      5 DB1_PDB3                                     READ WRITE NO
SQL> alter session set container=db1_pdb1;

Session altered.

SQL> select * from test;

      ID DT
EVENT
-----
-----
-----
-----
-----
      1 18-MAY-23 02.35.37.000000 PM
test oracle incremental merge switch to copy
      2 30-MAY-23 05.23.11.000000 PM
test recovery on a new EC2 instance host with image copy on FSxN

```

20. Andere Aufgaben nach der Wiederherstellung

Add FSxN NFS mount to fstab so that the NFS file system will be mounted when EC2 instance host rebooted.

As EC2 user, vi /etc/fstab and add following entry:

```

172.30.15.19:/ora_01_copy          /nfsfsxn          nfs
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=262144,wsiz=262144,noi
tr 0          0

```

Update the Oracle init file from primary database init file backup that is restored to /tmp/archive and create spfile as needed.

Damit ist die Wiederherstellung der Oracle VLDB-Datenbank von der Backup-Image-Kopie auf dem FSxN NFS-Dateisystem auf einen neuen EC2 DB-Instanzhost abgeschlossen.

Klonen der Oracle Standby-Image-Kopie für andere Anwendungsfälle

Ein weiterer Vorteil der Verwendung von AWS FSX ONTAP für das Staging von Oracle VLDB-Bildkopie ist, dass es FlexCloned sein kann, um viele andere Zwecke mit minimaler zusätzlicher Speicherinvestition zu dienen. Im folgenden Anwendungsfall zeigen wir, wie das Staging-NFS-Volume auf FSX ONTAP für andere Oracle Anwendungsfälle wie ENTWICKLUNG, UAT usw. erstellt und geklont wird

1. Wir beginnen damit, eine Zeile in dieselbe Testtabelle einzufügen, die wir zuvor erstellt haben.

```
SQL> insert into test values (3, sysdate, 'test clone on a new EC2 instance host with image copy on FSxN');
```

```
1 row created.
```

```
SQL> select * from test;
```

```
          ID
-----
DT
-----
EVENT
-----
          1
18-MAY-23 02.35.37.000000 PM
test oracle incremental merge switch to copy

          2
30-MAY-23 05.23.11.000000 PM
test recovery on a new EC2 instance host with image copy on FSxN

          ID
-----
DT
-----
EVENT
-----

          3
05-JUN-23 03.19.46.000000 PM
test clone on a new EC2 instance host with image copy on FSxN

SQL>
```

2. Erstellen Sie ein RMAN-Backup und führen Sie die FSX ONTAP-Datenbank-Image-Kopie zusammen, so dass die Transaktion im Backup-Set auf FSX NFS-Mount erfasst, aber nicht in Kopie zusammengeführt wird, bis geklonte Datenbank wiederhergestellt wird.

```
RMAN> @/home/oracle/rman_bkup_merge.cmd
```

3. Loggen Sie sich beim FSX Cluster über ssh als fsxadmin Benutzer ein, um die Schnappschüsse zu beobachten, die durch geplante Backup Policy erstellt wurden - oracle und nehmen Sie einen einmalig Schnappschuss, so dass es die Transaktion, die wir in Schritt 1 festgelegt haben, einschließen wird.

```
FsxId06c3c8b2a7bd56458::> vol snapshot create -vserver svm_ora
-volume ora_01_copy -snapshot one-off.2023-06-05-1137 -foreground
true
```

```
FsxId06c3c8b2a7bd56458::> snapshot show
```

```
---Blocks---
```

```
Vserver Volume Snapshot Size
Total% Used%
```

```
-----
```

```
svm_ora ora_01_copy
          daily.2023-06-02_0010 3.59GB
2% 5%
          daily.2023-06-03_0010 1.10GB
1% 1%
          daily.2023-06-04_0010 608KB
0% 0%
          daily.2023-06-05_0010 3.81GB
2% 5%
          one-off.2023-06-05-1137 168KB
0% 0%
          svm_ora_root
          weekly.2023-05-28_0015 1.86MB
0% 78%
          daily.2023-06-04_0010 152KB
0% 22%
          weekly.2023-06-04_0015 1.24MB
0% 70%
          daily.2023-06-05_0010 196KB
0% 27%
          hourly.2023-06-05_1005 156KB
0% 22%
          hourly.2023-06-05_1105 156KB
0% 22%
          hourly.2023-06-05_1205 156KB
0% 22%
          hourly.2023-06-05_1305 156KB
0% 22%
          hourly.2023-06-05_1405 1.87MB
0% 78%
          hourly.2023-06-05_1505 148KB
0% 22%
```

```
15 entries were displayed.
```

4. Klonen Sie aus dem einmaligen Snapshot, um zum Einrichten einer neuen DB1-Kloninstanz auf einem alternativen EC2 Oracle-Host verwendet zu werden. Sie haben die Möglichkeit, von allen verfügbaren täglichen Snapshots für Volume ora_01_copy zu klonen.

```
FsxId06c3c8b2a7bd56458::> vol clone create -flexclone db1_20230605of
-type RW -parent-vserver svm_ora -parent-volume ora_01_copy
-junction-path /db1_20230605of -junction-active true -parent
-snapshot one-off.2023-06-05-1137
[Job 464] Job succeeded: Successful

FsxId06c3c8b2a7bd56458::>

FsxId06c3c8b2a7bd56458::> vol show db1*
Vserver   Volume           Aggregate      State      Type      Size
Available Used%
-----
-----
svm_ora   db1_20230605of
          aggr1            online        RW         200GB
116.6GB  38%

FsxId06c3c8b2a7bd56458::>
```

5. Deaktivieren Sie die Snapshot-Richtlinie für das geklonte Volume, da sie die Snapshot-Richtlinie des übergeordneten Volumes übernimmt, es sei denn, Sie möchten das geklonte Volume schützen und lassen Sie es dann in Ruhe.

```
FsxId06c3c8b2a7bd56458::> vol modify -volume db1_20230605of
-snapshot-policy none

Warning: You are changing the Snapshot policy on volume
"db1_20230605of" to "none". Snapshot copies on this volume that do
not match any of the prefixes of the new Snapshot policy will not be
deleted. However, when the new Snapshot policy
          takes effect, depending on the new retention count, any
existing Snapshot copies that continue to use the same prefixes
might be deleted. See the 'volume modify' man page for more
information.
Do you want to continue? {y|n}: y
Volume modify successful on volume db1_20230605of of Vserver
svm_ora.

FsxId06c3c8b2a7bd56458::>
```

6. Melden Sie sich bei einer neuen EC2 Linux-Instanz an. Die Oracle Software ist dabei mit derselben

Version und Patch-Ebene wie Ihre primäre Oracle EC2 Instanz vorinstalliert und mounten Sie das geklonte Volume.

```
[ec2-user@ip-172-30-15-124 ~]$ sudo mkdir /nfsfsxn
[ec2-user@ip-172-30-15-124 ~]$ sudo mount -t nfs
172.30.15.19:/db1_20230605of /nfsfsxn -o
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsiz=262144,wsiz=262144,noi
tr
```

7. Validieren Sie die inkrementellen Backup-Sätze der Datenbank, Image-Kopien und die verfügbaren archivierten Protokolle im FSX NFS-Mount.

```
[ec2-user@ip-172-30-15-124 ~]$ ls -ltr /nfsfsxn/oracopy
total 79450332
-rw-r----- 1 oracle 54331 482353152 Jun  1 19:02 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-6_891tkrhr
-rw-r----- 1 oracle 54331 419438592 Jun  1 19:03 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-5_8d1tkril
-rw-r----- 1 oracle 54331 241180672 Jun  1 19:03 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-8_8g1tkrj7
-rw-r----- 1 oracle 54331 912506880 Jun  1 20:21 8n1tkvv2_279_1_1
-rw-r----- 1 oracle 54331 925696 Jun  1 20:21 8q1tl05i_282_1_1
-rw-r----- 1 oracle 54331 1169014784 Jun  1 20:21 8p1tkvv2_281_1_1
-rw-r----- 1 oracle 54331 6455296 Jun  1 20:21 8r1tl05m_283_1_1
-rw-r----- 1 oracle 54331 139264 Jun  1 20:21 8t1tl05t_285_1_1
-rw-r----- 1 oracle 54331 3514368 Jun  1 20:21 8s1tl05t_284_1_1
-rw-r----- 1 oracle 54331 139264 Jun  1 20:21 8u1tl060_286_1_1
-rw-r----- 1 oracle 54331 425984 Jun  1 20:21 901tl062_288_1_1
-rw-r----- 1 oracle 54331 344064 Jun  1 20:21 911tl062_289_1_1
-rw-r----- 1 oracle 54331 245760 Jun  1 20:21 931tl063_291_1_1
-rw-r----- 1 oracle 54331 237568 Jun  1 20:21 941tl064_292_1_1
-rw-r----- 1 oracle 54331 57344 Jun  1 20:21 961tl065_294_1_1
-rw-r----- 1 oracle 54331 57344 Jun  1 20:21 971tl066_295_1_1
-rw-r----- 1 oracle 54331 57344 Jun  1 20:21 981tl067_296_1_1
-rw-r----- 1 oracle 54331 1040760832 Jun  1 20:23 8m1tkvv2_278_1_1
-rw-r----- 1 oracle 54331 932847616 Jun  1 20:24 8o1tkvv2_280_1_1
-rw-r----- 1 oracle 54331 1121984512 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-1_821tkrb8
-rw-r----- 1 oracle 54331 1027612672 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-3_831tkrd9
-rw-r----- 1 oracle 54331 429924352 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-9_8a1tkrhr
-rw-r----- 1 oracle 54331 707796992 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-4_851tkrgf
-rw-r----- 1 oracle 54331 534781952 Jun  5 15:21 data_D-DB1_I-
```

```

1730530050_TS-SYSAUX_FNO-14_871tkrhr
-rw-r----- 1 oracle 54331 534781952 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-18_881tkrhr
-rw-r----- 1 oracle 54331 429924352 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-13_8b1tkril
-rw-r----- 1 oracle 54331 429924352 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-SYSTEM_FNO-17_8c1tkril
-rw-r----- 1 oracle 54331 246423552 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-15_8e1tkril
-rw-r----- 1 oracle 54331 246423552 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-19_8f1tkrj4
-rw-r----- 1 oracle 54331 5251072 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-USERS_FNO-7_8h1tkrj9
-rw-r----- 1 oracle 54331 5251072 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-USERS_FNO-16_8j1tkrja
-rw-r----- 1 oracle 54331 5251072 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-USERS_FNO-20_8k1tkrjb
-rw-r----- 1 oracle 54331 5251072 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-USERS_FNO-12_8i1tkrj9
-rw-r----- 1 oracle 54331 555753472 Jun  5 15:21 data_D-DB1_I-
1730530050_TS-SYSAUX_FNO-10_861tkrgo
-rw-r----- 1 oracle 54331 796925952 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-UNDOTBS1_FNO-11_841tkrf2
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-21_7j1tkqk6
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-34_801tkram
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-29_7r1tkr32
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-25_7n1tkqrh
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-31_7t1tkr3i
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-33_7v1tkra6
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-23_7l1tkqk6
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-27_7p1tkqrq
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-35_811tkrap
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-32_7u1tkr42
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-22_7k1tkqk6
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-

```

```

1730530050_TS-SOE_FNO-24_7m1tkqk6
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-28_7q1tkqs1
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-30_7s1tkr3a
-rw-r----- 1 oracle 54331 4294975488 Jun  5 15:22 data_D-DB1_I-
1730530050_TS-SOE_FNO-26_7o1tkqrj
-rw-r----- 1 oracle 54331 1241432064 Jun  5 15:30 9d1tv06n_301_1_1
-rw-r----- 1 oracle 54331 1019805696 Jun  5 15:31 9a1tv06m_298_1_1
-rw-r----- 1 oracle 54331      4612096 Jun  5 15:31 9e1tv01d_302_1_1
-rw-r----- 1 oracle 54331   967163904 Jun  5 15:31 9b1tv06n_299_1_1
-rw-r----- 1 oracle 54331   31563776 Jun  5 15:31 9g1tv01t_304_1_1
-rw-r----- 1 oracle 54331    319488 Jun  5 15:31 9h1tv01t_305_1_1
-rw-r----- 1 oracle 54331    335872 Jun  5 15:31 9i1tv0m0_306_1_1
-rw-r----- 1 oracle 54331    565248 Jun  5 15:31 9k1tv0m1_308_1_1
-rw-r----- 1 oracle 54331    581632 Jun  5 15:31 9l1tv0m5_309_1_1
-rw-r----- 1 oracle 54331   54345728 Jun  5 15:31 9f1tv01t_303_1_1
-rw-r----- 1 oracle 54331    368640 Jun  5 15:31 9n1tv0m5_311_1_1
-rw-r----- 1 oracle 54331    385024 Jun  5 15:31 9o1tv0m6_312_1_1
-rw-r----- 1 oracle 54331  985858048 Jun  5 15:31 9c1tv06n_300_1_1
-rw-r----- 1 oracle 54331    57344 Jun  5 15:31 9q1tv0m7_314_1_1
-rw-r----- 1 oracle 54331    57344 Jun  5 15:31 9r1tv0m8_315_1_1
-rw-r----- 1 oracle 54331    57344 Jun  5 15:31 9s1tv0m9_316_1_1
-rw-r--r-- 1 oracle 54331    12720 Jun  5 15:31 db1_ct1.sql
-rw-r----- 1 oracle 54331  11600384 Jun  5 15:48 bct_db1.ctf
[ec2-user@ip-172-30-15-124 ~]$

```

```

[oracle@ip-172-30-15-124 ~]$ ls -l
/nfsfsxn/archlog/DB1/archivelog/2023_06_05
total 2008864
-rw-r----- 1 oracle 54331      729088 Jun  5 14:38
o1_mf_1_190_17vwwvt9_.arc
-rw-r----- 1 oracle 54331 166651904 Jun  5 14:44
o1_mf_1_191_17vx6vmg_.arc
-rw-r----- 1 oracle 54331 167406080 Jun  5 14:47
o1_mf_1_192_17vxctms_.arc
-rw-r----- 1 oracle 54331 166868992 Jun  5 14:49
o1_mf_1_193_17vxjjps_.arc
-rw-r----- 1 oracle 54331 166087168 Jun  5 14:52
o1_mf_1_194_17vxnxrh_.arc
-rw-r----- 1 oracle 54331 175210496 Jun  5 14:54
o1_mf_1_195_17vxswv5_.arc
-rw-r----- 1 oracle 54331 167078400 Jun  5 14:57
o1_mf_1_196_17vxy1wp_.arc
-rw-r----- 1 oracle 54331 169701888 Jun  5 14:59
o1_mf_1_197_17vy3cyw_.arc

```



```
-rw-r----- 1 oracle 54331 167845376 Jun  5 15:02
o1_mf_1_198_17vy8245_.arc
-rw-r----- 1 oracle 54331 170763776 Jun  5 15:05
o1_mf_1_199_17vydv4c_.arc
-rw-r----- 1 oracle 54331 193853440 Jun  5 15:07
o1_mf_1_200_17vykf23_.arc
-rw-r----- 1 oracle 54331 165523968 Jun  5 15:09
o1_mf_1_201_17vyp1dh_.arc
-rw-r----- 1 oracle 54331 161117184 Jun  5 15:12
o1_mf_1_202_17vyvrm5_.arc
-rw-r----- 1 oracle 54331 10098176 Jun  5 15:21
o1_mf_1_203_17vzdfwm_.arc
```

8. Die Recovery-Prozesse ähneln jetzt dem vorherigen Nutzungsfall der Wiederherstellung zu einer neuen EC2 DB-Instanz nach einem Ausfall: oracle-Umgebung (oratab, Oracle_HOME, Oracle_SID) auf die primäre Produktionsinstanz einstellen Erstellen Sie eine init-Datei einschließlich db_Recovery_File_dest_size und db_Recovery_File_dest, die auf ein Flash-Wiederherstellungsverzeichnis auf FSX NFS-Mount verweisen. Dann lanuch RMAN Recovery ausführen. Im Folgenden finden Sie die Schritte und die Ausgabe des Befehls.

```
[oracle@ip-172-30-15-124 dbs]$ rman target / nocatalog

Recovery Manager: Release 19.0.0.0.0 - Production on Wed Jun 7
14:44:33 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights
reserved.

connected to target database (not started)

RMAN> startup nomount;

Oracle instance started

Total System Global Area      10737418000 bytes

Fixed Size                     9174800 bytes
Variable Size                  1577058304 bytes
Database Buffers               9126805504 bytes
Redo Buffers                    24379392 bytes

RMAN> set dbid = 1730530050;

executing command: SET DBID
```

```
RMAN> restore controlfile from autobackup;
```

```
Starting restore at 07-JUN-23
```

```
allocated channel: ORA_DISK_1
```

```
channel ORA_DISK_1: SID=2 device type=DISK
```

```
recovery area destination: /nfsfsxn/archlog/
```

```
database name (or database unique name) used for search: DB1
```

```
channel ORA_DISK_1: AUTOBACKUP
```

```
/nfsfsxn/archlog/DB1/autobackup/2023_06_05/o1_mf_s_1138721482_17vzyb  
vq_.bkp found in the recovery area
```

```
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20230607
```

```
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20230606
```

```
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20230605
```

```
channel ORA_DISK_1: restoring control file from AUTOBACKUP
```

```
/nfsfsxn/archlog/DB1/autobackup/2023_06_05/o1_mf_s_1138721482_17vzyb  
vq_.bkp
```

```
channel ORA_DISK_1: control file restore from AUTOBACKUP complete
```

```
output file name=/nfsfsxn/oracopy/db1.ctl
```

```
Finished restore at 07-JUN-23
```

```
RMAN> alter database mount;
```

```
released channel: ORA_DISK_1
```

```
Statement processed
```

```
RMAN> list incarnation;
```

```
List of Database Incarnations
```

DB Key	Inc Key	DB Name	DB ID	STATUS	Reset SCN	Reset Time
1	1	DB1	1730530050	PARENT	1	17-APR-19
2	2	DB1	1730530050	CURRENT	1920977	12-MAY-23

```
RMAN> list copy of database tag 'OraCopyBKUPonFSxN_level_0';
```

```
List of Datafile Copies
```

```
=====
```

Key	File S	Completion Time	Ckp SCN	Ckp Time	Sparse
362	1	A 05-JUN-23	8319160	01-JUN-23	NO

```
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
```

```

SYSTEM_FNO-1_821tkrb8
    Tag: ORACOPYBKUPONFSXN_LEVEL_0

363      3      A 05-JUN-23      8319165      01-JUN-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYS_AUX_FNO-3_831tkrd9
    Tag: ORACOPYBKUPONFSXN_LEVEL_0

365      4      A 05-JUN-23      8319171      01-JUN-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-4_851tkrgf
    Tag: ORACOPYBKUPONFSXN_LEVEL_0

355      5      A 01-JUN-23      2383520      12-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-5_8d1tkril
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 2, PDB Name: PDB$SEED

349      6      A 01-JUN-23      2383520      12-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYS_AUX_FNO-6_891tkrhr
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 2, PDB Name: PDB$SEED

372      7      A 05-JUN-23      8319201      01-JUN-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
7_8h1tkrj9
    Tag: ORACOPYBKUPONFSXN_LEVEL_0

361      8      A 01-JUN-23      2383520      12-MAY-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-8_8g1tkrj7
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 2, PDB Name: PDB$SEED

364      9      A 05-JUN-23      8318717      01-JUN-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-9_8altkrhr
    Tag: ORACOPYBKUPONFSXN_LEVEL_0
    Container ID: 3, PDB Name: DB1_PDB1

376      10     A 05-JUN-23      8318714      01-JUN-23      NO
    Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYS_AUX_FNO-10_861tkrgo
    Tag: ORACOPYBKUPONFSXN_LEVEL_0

```

```

Container ID: 3, PDB Name: DB1_PDB1

377      11      A 05-JUN-23      8318720      01-JUN-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-11_841tkrf2
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

375      12      A 05-JUN-23      8318719      01-JUN-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
12_8i1tkrj9
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

368      13      A 05-JUN-23      8319184      01-JUN-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-13_8b1tkril
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 4, PDB Name: DB1_PDB2

366      14      A 05-JUN-23      8319175      01-JUN-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSAUX_FNO-14_871tkrhr
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 4, PDB Name: DB1_PDB2

370      15      A 05-JUN-23      8319193      01-JUN-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-15_8e1tkril
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 4, PDB Name: DB1_PDB2

373      16      A 05-JUN-23      8319206      01-JUN-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
16_8j1tkrja
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 4, PDB Name: DB1_PDB2

369      17      A 05-JUN-23      8319188      01-JUN-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
SYSTEM_FNO-17_8c1tkril
Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 5, PDB Name: DB1_PDB3

367      18      A 05-JUN-23      8319180      01-JUN-23      NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-

```

SYSAUX_FNO-18_881tkrhr

Tag: ORACOPYBKUPONFSXN_LEVEL_0

Container ID: 5, PDB Name: DB1_PDB3

371 19 A 05-JUN-23 8319197 01-JUN-23 NO

Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-
UNDOTBS1_FNO-19_8f1tkrj4

Tag: ORACOPYBKUPONFSXN_LEVEL_0

Container ID: 5, PDB Name: DB1_PDB3

374 20 A 05-JUN-23 8319210 01-JUN-23 NO

Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-
20_8k1tkrjb

Tag: ORACOPYBKUPONFSXN_LEVEL_0

Container ID: 5, PDB Name: DB1_PDB3

378 21 A 05-JUN-23 8318720 01-JUN-23 NO

Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
21_7j1tkqk6

Tag: ORACOPYBKUPONFSXN_LEVEL_0

Container ID: 3, PDB Name: DB1_PDB1

388 22 A 05-JUN-23 8318714 01-JUN-23 NO

Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
22_7k1tkqk6

Tag: ORACOPYBKUPONFSXN_LEVEL_0

Container ID: 3, PDB Name: DB1_PDB1

384 23 A 05-JUN-23 8318717 01-JUN-23 NO

Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
23_7l1tkqk6

Tag: ORACOPYBKUPONFSXN_LEVEL_0

Container ID: 3, PDB Name: DB1_PDB1

389 24 A 05-JUN-23 8318719 01-JUN-23 NO

Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
24_7m1tkqk6

Tag: ORACOPYBKUPONFSXN_LEVEL_0

Container ID: 3, PDB Name: DB1_PDB1

381 25 A 05-JUN-23 8318720 01-JUN-23 NO

Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-
25_7n1tkqrh

Tag: ORACOPYBKUPONFSXN_LEVEL_0

Container ID: 3, PDB Name: DB1_PDB1

392	26	A	05-JUN-23	8318714	01-JUN-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
26_7o1tkqrj						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
385	27	A	05-JUN-23	8318717	01-JUN-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
27_7p1tkqrq						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
390	28	A	05-JUN-23	8318719	01-JUN-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
28_7q1tkqsl						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
380	29	A	05-JUN-23	8318720	01-JUN-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
29_7r1tkr32						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
391	30	A	05-JUN-23	8318714	01-JUN-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
30_7s1tkr3a						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
382	31	A	05-JUN-23	8318717	01-JUN-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
31_7t1tkr3i						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
387	32	A	05-JUN-23	8318719	01-JUN-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
32_7u1tkr42						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						
Container ID: 3, PDB Name: DB1_PDB1						
383	33	A	05-JUN-23	8318719	01-JUN-23	NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-						
33_7v1tkra6						
Tag: ORACOPYBKUPONFSXN_LEVEL_0						

Container ID: 3, PDB Name: DB1_PDB1

379 34 A 05-JUN-23 8318717 01-JUN-23 NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-34_801tkram

Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

386 35 A 05-JUN-23 8318714 01-JUN-23 NO
Name: /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-35_811tkrap

Tag: ORACOPYBKUPONFSXN_LEVEL_0
Container ID: 3, PDB Name: DB1_PDB1

RMAN> switch database to copy;

datafile 1 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-1_821tkrb8"

datafile 3 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-3_831tkrd9"

datafile 4 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-4_851tkrgf"

datafile 5 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-5_8d1tkril"

datafile 6 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-6_891tkrhr"

datafile 7 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-7_8h1tkrj9"

datafile 8 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-8_8g1tkrj7"

datafile 9 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-9_8a1tkrhr"

datafile 10 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-10_861tkrgo"

datafile 11 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-11_841tkrf2"

datafile 12 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-12_8i1tkrj9"

datafile 13 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-13_8b1tkril"

datafile 14 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-14_871tkrhr"

datafile 15 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-15_8e1tkril"

datafile 16 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-16_8j1tkrja"

```
datafile 17 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-17_8cltkril"  
datafile 18 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-18_88ltkrhr"  
datafile 19 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-19_8fltkrj4"  
datafile 20 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-20_8kltkrjb"  
datafile 21 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-21_7jltkqk6"  
datafile 22 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-22_7kltkqk6"  
datafile 23 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-23_7l1tkqk6"  
datafile 24 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-24_7mltkqk6"  
datafile 25 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-25_7nltkqrh"  
datafile 26 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-26_7oltkqrj"  
datafile 27 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-27_7pltkqrq"  
datafile 28 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-28_7qltkqs1"  
datafile 29 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-29_7rltkr32"  
datafile 30 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-30_7sltkr3a"  
datafile 31 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-31_7tltkr3i"  
datafile 32 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-32_7ultkr42"  
datafile 33 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-33_7vltkra6"  
datafile 34 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-34_80ltkram"  
datafile 35 switched to datafile copy "/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-35_8l1tkrap"
```

```
RMAN> run {  
2> set until sequence 204;  
3> recover database;  
4> }
```

```
executing command: SET until clause
```


Starting recover at 07-JUN-23

using channel ORA_DISK_1

starting media recovery

archived log for thread 1 with sequence 190 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_190_17vwvvt9_.arc

archived log for thread 1 with sequence 191 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_191_17vx6vmg_.arc

archived log for thread 1 with sequence 192 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_192_17vxctms_.arc

archived log for thread 1 with sequence 193 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_193_17vxjjps_.arc

archived log for thread 1 with sequence 194 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_194_17vxnrxrh_.arc

archived log for thread 1 with sequence 195 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_195_17vxswv5_.arc

archived log for thread 1 with sequence 196 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_196_17vxyllwp_.arc

archived log for thread 1 with sequence 197 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_197_17vy3cyw_.arc

archived log for thread 1 with sequence 198 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_198_17vy8245_.arc

archived log for thread 1 with sequence 199 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_199_17vydv4c_.arc

archived log for thread 1 with sequence 200 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_200_17vykf23_.arc

archived log for thread 1 with sequence 201 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_201_17vyp1dh_.arc

archived log for thread 1 with sequence 202 is already on disk as
file

/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_202_17vyvrm5_.arc

archived log for thread 1 with sequence 203 is already on disk as
file

```
/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_203_17vzdfwm_.arc
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_190_17vwvvt9
_.arc thread=1 sequence=190
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_191_17vx6vmg
_.arc thread=1 sequence=191
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_192_17vxctms
_.arc thread=1 sequence=192
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_193_17vxjjps
_.arc thread=1 sequence=193
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_194_17vxnxrh
_.arc thread=1 sequence=194
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_195_17vxswv5
_.arc thread=1 sequence=195
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_196_17vxyllwp
_.arc thread=1 sequence=196
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_197_17vy3cyw
_.arc thread=1 sequence=197
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_198_17vy8245
_.arc thread=1 sequence=198
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_199_17vydv4c
_.arc thread=1 sequence=199
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_200_17vykf23
_.arc thread=1 sequence=200
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_201_17vyp1dh
_.arc thread=1 sequence=201
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_202_17vyvrm5
_.arc thread=1 sequence=202
archived log file
name=/nfsfsxn/archlog/DB1/archivelog/2023_06_05/o1_mf_1_203_17vzdfwm
_.arc thread=1 sequence=203
media recovery complete, elapsed time: 00:19:30
Finished recover at 07-JUN-23
```

```
RMAN> exit
```

```
Recovery Manager complete.
```

```
[oracle@ip-172-30-15-124 dbs]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Wed Jun 7 15:58:12 2023  
Version 19.18.0.0.0
```

```
Copyright (c) 1982, 2022, Oracle. All rights reserved.
```

```
Connected to:
```

```
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -  
Production
```

```
Version 19.18.0.0.0
```

```
SQL> select member from v$logfile;
```

```
MEMBER
```

```
-----  
-----
```

```
+DATA/DB1/ONLINELOG/group_3.264.1136666437
```

```
+DATA/DB1/ONLINELOG/group_2.263.1136666437
```

```
+DATA/DB1/ONLINELOG/group_1.262.1136666437
```

```
SQL> alter database rename file
```

```
'+DATA/DB1/ONLINELOG/group_1.262.1136666437' to
```

```
 '/nfsfsxn/oracopy/redo01.log';
```

```
Database altered.
```

```
SQL> alter database rename file
```

```
'+DATA/DB1/ONLINELOG/group_2.263.1136666437' to
```

```
 '/nfsfsxn/oracopy/redo02.log';
```

```
Database altered.
```

```
SQL> alter database rename file
```

```
'+DATA/DB1/ONLINELOG/group_3.264.1136666437' to
```

```
 '/nfsfsxn/oracopy/redo03.log';
```

```
Database altered.
```

```
SQL> alter database noarchivelog;
```

```
Database altered.
```

```
SQL> alter database open resetlogs;
```

```
Database altered.
```

```
SQL> set lin 200;
```

```
SQL> select name from v$datafile
2 union
3 select name from v$controlfile
4 union
5 select name from v$tempfile
6 union
7 select member from v$logfile;
```

```
NAME
```

```
-----
-----
/nfsfsxn/oracopy/DB1/FB864A929AEB79B9E053630F1EAC7046/datafile/o1_mf
_temp_l81bhz6g_.tmp
/nfsfsxn/oracopy/DB1/FB867DA8C68C816EE053630F1EAC2BCF/datafile/o1_mf
_temp_l81bj16t_.tmp
/nfsfsxn/oracopy/DB1/FB867EA89ECF81C0E053630F1EACB901/datafile/o1_mf
_temp_l81bj135_.tmp
/nfsfsxn/oracopy/DB1/FB867F8A4D4F821CE053630F1EAC69CC/datafile/o1_mf
_temp_l81bj13g_.tmp
/nfsfsxn/oracopy/DB1/datafile/o1_mf_temp_l81bhwjg_.tmp
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-21_7j1tkqk6
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-22_7k1tkqk6
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-23_7l1tkqk6
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-24_7m1tkqk6
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-25_7n1tkqrh
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-26_7o1tkqrj
```

```
NAME
```

```
-----
-----
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-27_7p1tkqrq
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-28_7q1tkqs1
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-29_7r1tkr32
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-30_7s1tkr3a
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-31_7t1tkr3i
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-32_7u1tkr42
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-33_7v1tkra6
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-34_801tkram
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-35_811tkrap
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-10_861tkrgo
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-14_871tkrhr
```

NAME

```
-----  
-----  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-18_881tkrhr  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-3_831tkrd9  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-6_891tkrhr  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-13_8b1tkril  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-17_8c1tkril  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-1_821tkrb8  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-5_8d1tkril  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-9_8a1tkrhr  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-11_841tkrf2  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-15_8e1tkril  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-19_8f1tkrj4
```

NAME

```
-----  
-----  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-4_851tkrgf  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-8_8g1tkrj7  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-12_8i1tkrj9  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-16_8j1tkrja  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-20_8k1tkrjb  
/nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-7_8h1tkrj9  
/nfsfsxn/oracopy/db1.ctl  
/nfsfsxn/oracopy/redo01.log  
/nfsfsxn/oracopy/redo02.log  
/nfsfsxn/oracopy/redo03.log
```

43 rows selected.

SQL> show pdbs;

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	DB1_PDB1	READ WRITE	NO
4	DB1_PDB2	READ WRITE	NO
5	DB1_PDB3	READ WRITE	NO

SQL> alter session set container=db1_pdb1;

Session altered.

SQL> select * from test;

```

          ID DT
EVENT
-----
-----
-----
          1 18-MAY-23 02.35.37.000000 PM
test oracle incremental merge switch to copy
          2 30-MAY-23 05.23.11.000000 PM
test recovery on a new EC2 instance host with image copy on FSxN
          3 05-JUN-23 03.19.46.000000 PM
test clone on a new EC2 instance host with image copy on FSxN

SQL>

```

9. Benennen Sie die geklonte Datenbankinstanz um und ändern Sie die Datenbank-ID mit dem Dienstprogramm Oracle nid. Der Status der Datenbankinstanz muss in sein mount Um den Befehl auszuführen.

```

SQL> select name, open_mode, log_mode from v$database;

NAME          OPEN_MODE          LOG_MODE
-----
DB1           READ WRITE        NOARCHIVELOG

SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.

SQL> startup mount;
ORACLE instance started.

Total System Global Area 1.0737E+10 bytes
Fixed Size                 9174800 bytes
Variable Size             1577058304 bytes
Database Buffers          9126805504 bytes
Redo Buffers              24379392 bytes
Database mounted.
SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release
19.0.0.0.0 - Production
Version 19.18.0.0.0
[oracle@ip-172-30-15-124 dbs]$ nid target=/ dbname=db1tst

DBNEWID: Release 19.0.0.0.0 - Production on Wed Jun 7 16:15:14 2023

```

Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights reserved.

Connected to database DB1 (DBID=1730530050)

Connected to server version 19.18.0

Control Files in database:

/nfsfsxn/oracopy/db1.ctl

Change database ID and database name DB1 to DB1TST? (Y/[N]) => Y

Proceeding with operation

Changing database ID from 1730530050 to 3054879890

Changing database name from DB1 to DB1TST

Control File /nfsfsxn/oracopy/db1.ctl - modified

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-1_821tkrb - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-3_831tkrd - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-4_851tkrg - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-5_8d1tkri - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-6_891tkrh - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-7_8h1tkrj - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-8_8g1tkrj - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-9_8a1tkrh - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-10_861tkrg - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-11_841tkrf - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-12_8i1tkrj - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-13_8b1tkri - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-14_871tkrh - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-UNDOTBS1_FNO-15_8e1tkri - dbid changed, wrote new name

Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-

16_8j1tkrj - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSTEM_FNO-

17_8cltkri - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SYSAUX_FNO-

18_881tkrh - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-

UNDOTBS1_FNO-19_8f1tkrj - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-USERS_FNO-

20_8k1tkrj - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

21_7j1tkqk - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

22_7k1tkqk - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

23_7l1tkqk - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

24_7m1tkqk - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

25_7n1tkqr - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

26_7o1tkqr - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

27_7p1tkqr - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

28_7q1tkqs - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

29_7r1tkr3 - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

30_7s1tkr3 - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

31_7t1tkr3 - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

32_7u1tkr4 - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

33_7v1tkra - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

34_801tkra - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/data_D-DB1_I-1730530050_TS-SOE_FNO-

35_811tkra - dbid changed, wrote new name
 Datafile /nfsfsxn/oracopy/DB1/datafile/o1_mf_temp_l81bhwjg_.tm -
 dbid changed, wrote new name
 Datafile
 /nfsfsxn/oracopy/DB1/FB864A929AEB79B9E053630F1EAC7046/datafile/o1_mf
 _temp_l81bhzh6g_.tm - dbid changed, wrote new name
 Datafile
 /nfsfsxn/oracopy/DB1/FB867DA8C68C816EE053630F1EAC2BCF/datafile/o1_mf


```
_temp_l81bj16t_.tm - dbid changed, wrote new name
  Datafile
/nfsfsxn/oracopy/DB1/FB867EA89ECF81C0E053630F1EACB901/datafile/o1_mf
_temp_l81bj135_.tm - dbid changed, wrote new name
  Datafile
/nfsfsxn/oracopy/DB1/FB867F8A4D4F821CE053630F1EAC69CC/datafile/o1_mf
_temp_l81bj13g_.tm - dbid changed, wrote new name
  Control File /nfsfsxn/oracopy/db1.ctl - dbid changed, wrote new
name
  Instance shut down

Database name changed to DB1TST.
Modify parameter file and generate a new password file before
restarting.
Database ID for database DB1TST changed to 3054879890.
All previous backups and archived redo logs for this database are
unusable.
Database is not aware of previous backups and archived logs in
Recovery Area.
Database has been shutdown, open database with RESETLOGS option.
Succesfully changed database name and ID.
DBNEWID - Completed succesfully.
```

10. Ändern Sie die Konfiguration der Oracle-Datenbankumgebung in einen neuen Datenbanknamen oder eine neue Instanz-ID in Oratab, init-Datei, und erstellen Sie die erforderlichen Administratorverzeichnisse, die mit der neuen Instanz-ID übereinstimmen. Starten Sie dann die Instanz mit der Option Resetlogs.

```
SQL> startup mount;
ORACLE instance started.
```

```
Total System Global Area 1.0737E+10 bytes
Fixed Size                  9174800 bytes
Variable Size               1577058304 bytes
Database Buffers           9126805504 bytes
Redo Buffers                 24379392 bytes
Database mounted.
```

```
SQL> alter database open resetlogs;
```

```
Database altered.
```

```
SQL> select name, open_mode, log_mode from v$database;
```

NAME	OPEN_MODE	LOG_MODE
DB1TST	READ WRITE	NOARCHIVELOG

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	DB1_PDB1	MOUNTED	
4	DB1_PDB2	MOUNTED	
5	DB1_PDB3	MOUNTED	

```
SQL> alter pluggable database all open;
```

```
Pluggable database altered.
```

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	DB1_PDB1	READ WRITE	NO
4	DB1_PDB2	READ WRITE	NO
5	DB1_PDB3	READ WRITE	NO

```
SQL>
```

Damit ist der Klon einer neuen Oracle Instanz abgeschlossen. Diese stammt aus dem Staging von Datenbankkopie im FSX NFS-Mount für ENTWICKLUNG, Anwenderakzeptanz oder andere Anwendungsfälle. Mehrere Oracle-Instanzen können aus derselben Staging-Image-Kopie geklont werden.



Wenn Sie auf einen Fehler kommen `RMAN-06571: datafile 1 does not have recoverable copy` Wenn Sie die Datenbank in die Kopie wechseln, überprüfen Sie die Inkarnation der Datenbank, die mit der primären Produktions-DB übereinstimmt. Falls erforderlich, setzen Sie die Inkarnation zurück, um sie mit dem primären RMAN-Befehl zu vergleichen `reset database to incarnation n;`

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- RMAN: Zusammengeführte inkrementelle Backup-Strategien (Doc-ID 745798.1)

["https://support.oracle.com/knowledge/Oracle%20Database%20Products/745798_1.html"](https://support.oracle.com/knowledge/Oracle%20Database%20Products/745798_1.html)

- RMAN Backup und Recovery Benutzerhandbuch

["https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/getting-started-rman.html"](https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/getting-started-rman.html)

- Amazon FSX für NetApp ONTAP

["https://aws.amazon.com/fsx/netapp-ontap/"](https://aws.amazon.com/fsx/netapp-ontap/)

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL14422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL14422!3!467723097970!e!!g!!aws%20ec2

TR-4974: Oracle 19c im Standalone Restart auf AWS FSX/EC2 mit NFS/ASM

Allen Cao, Niyaz Mohamed, NetApp

Zweck

ASM (Automatic Storage Management) ist ein beliebter Oracle Storage Volume Manager, der in vielen Oracle-Installationen eingesetzt wird. Es ist außerdem die von Oracle empfohlene Storage-Managementlösung. Sie stellt eine Alternative zu herkömmlichen Volume Managern und Filesystemen dar. Seit Oracle Version 11g wurde ASM mit Grid-Infrastruktur anstatt mit einer Datenbank verpackt. Um Oracle ASM für das Storage-Management ohne RAC zu nutzen, müssen Sie daher die Oracle Grid-Infrastruktur auf einem eigenständigen Server installieren, der auch als Oracle Restart bezeichnet wird. Dies führt zweifellos zu einer größeren Komplexität in einer ansonsten einfacheren Oracle-Datenbankimplementierung. Wie der Name jedoch andeutet, werden bei der Bereitstellung von Oracle im Restart-Modus ausgefallene Oracle-Dienste nach einem Host-Neustart ohne Benutzereingriff neu gestartet, was ein gewisses Maß an Hochverfügbarkeit oder HA-Funktionalität bietet.

Oracle ASM wird allgemein in FC-, iSCSI-Storage-Protokollen und luns als Roh-Storage-Geräten eingesetzt. Die Konfiguration von ASM auf NFS-Protokoll und NFS-Dateisystem wird jedoch auch von Oracle unterstützt. In dieser Dokumentation zeigen wir, wie eine Oracle 19c-Datenbank mit dem NFS-Protokoll und Oracle ASM in einer Amazon FSX für ONTAP Storage-Umgebung mit EC2 Computing-Instanzen implementiert wird. Wir zeigen Ihnen auch, wie Sie den NetApp SnapCenter-Service über die NetApp BlueXP Konsole nutzen können, um Ihre Oracle Datenbank für Entwicklung/Tests zu sichern, wiederherzustellen und zu klonen. Andere

Anwendungsfälle für den Storage-effizienten Datenbankbetrieb in der AWS Public Cloud zeigen wir Ihnen auch, wie.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Oracle Database-Implementierung in Amazon FSx for ONTAP Storage und EC2-Computing-Instanzen mit NFS/ASM
- Test und Validierung eines Oracle-Workloads in der Public AWS Cloud mit NFS/ASM
- Testen und Validieren der in AWS bereitgestellten Funktionen zum Neustart von Oracle-Datenbanken

Zielgruppe

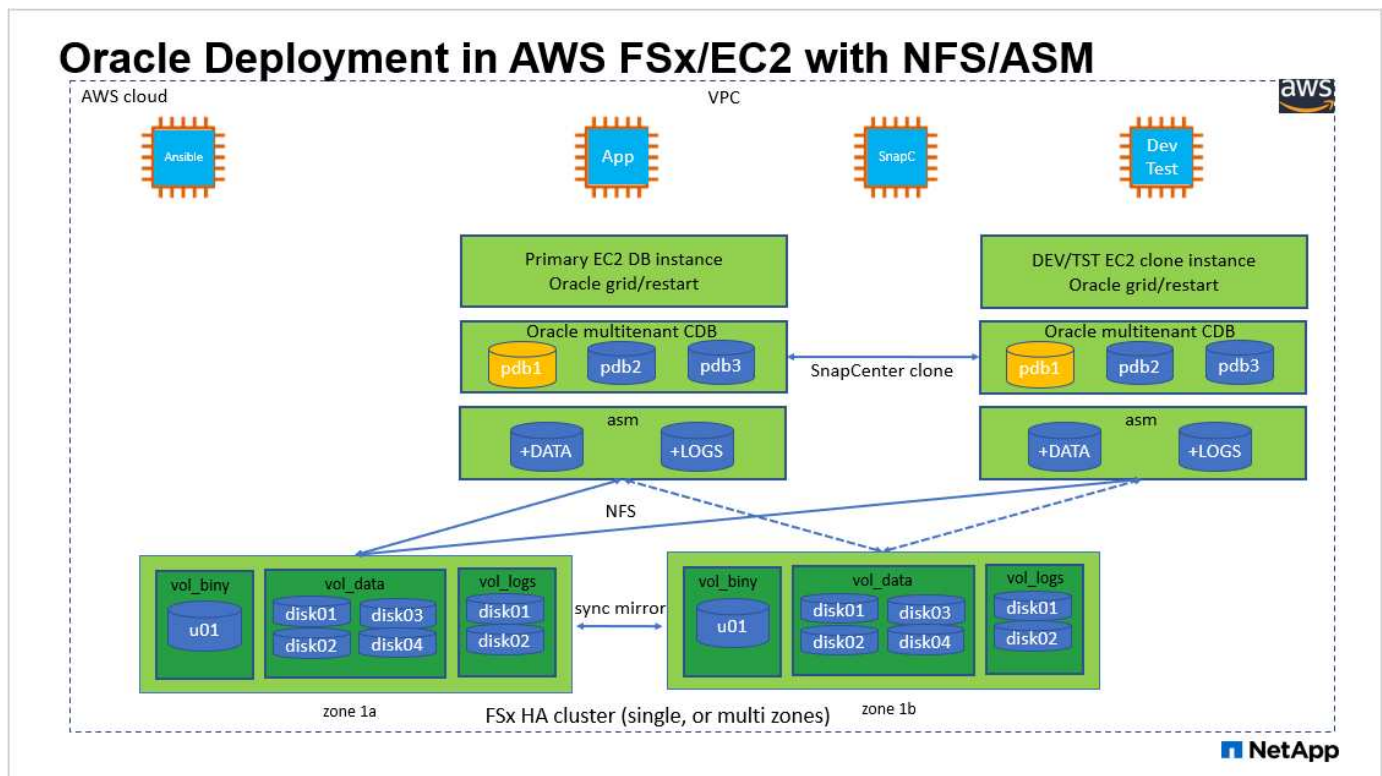
Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle in einer AWS Public Cloud mit NFS/ASM implementieren möchte.
- Ein Solution Architect für Datenbanken, der Oracle-Workloads in der AWS-Public Cloud testen möchte.
- Storage-Administrator, der eine in AWS FSX Storage implementierte Oracle-Datenbank implementieren und managen möchte.
- Der Applikationseigentümer, der eine Oracle Database in AWS FSX/EC2 einrichten möchte.

Test- und Validierungsumgebung der Lösung

Tests und Validierungen dieser Lösung wurden in einer AWS FSX- und EC2-Umgebung durchgeführt, die möglicherweise nicht mit der endgültigen Implementierungsumgebung übereinstimmt. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind



Hardware- und Softwarekomponenten

Hardware		
FSX ONTAP-Storage	Aktuelle Version von AWS angeboten	Ein FSX HA-Cluster in der gleichen VPC und Verfügbarkeitszone
EC2 Instanz für Computing	t2.xlarge/4vCPU/16G	Zwei EC2 T2 xlarge EC2-Instanzen, eine als primärer DB-Server und die andere als Klon-DB-Server
Software		
Redhat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Bereitstellung der RedHat Subscription für Tests
Oracle Grid Infrastructure	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
SnapCenter-Service	Version	v2.3.1.2324

Wichtige Faktoren für die Implementierung

- **EC2 Compute-Instanzen.** in diesen Tests und Validierungen haben wir einen Instanztyp AWS EC2 t2.xlarge für die Compute-Instanz der Oracle-Datenbank verwendet. NetApp empfiehlt, in der Produktionsumgebung eine EC2-Instanz vom Typ M5 als Computing-Instanz für Oracle zu verwenden, da sie für Datenbank-Workloads optimiert ist. Sie müssen die Größe der EC2-Instanz entsprechend der Anzahl der vCPUs und der Menge des RAM anpassen, basierend auf den tatsächlichen Workload-Anforderungen.
- **FSX Storage HA Cluster Single- oder Multi-Zone-Implementierung.** bei diesen Tests und Validierungen haben wir einen FSX HA-Cluster in einer einzelnen AWS Verfügbarkeitszone implementiert. Für die Implementierung in der Produktion empfiehlt NetApp die Implementierung eines FSX HA-Paars in zwei verschiedenen Verfügbarkeitszonen. Ein FSX HA-Cluster wird in einem HA-Paar bereitgestellt, das in einem Paar aktiv/Passiv-Filesysteme gespiegelt wird, um Redundanz auf Storage-Ebene bereitzustellen. Die Implementierung mit mehreren Zonen verbessert die Hochverfügbarkeit bei einem Ausfall in einer einzelnen AWS Zone noch weiter.
- **FSX Storage-Cluster-Sizing.** ein Amazon FSX for ONTAP Storage-Dateisystem bietet bis zu 160,000 RAW SSD IOPS, einen Durchsatz von bis zu 4 Gbit/s und eine maximale Kapazität von 192 tib. Sie können das Cluster jedoch in Bezug auf die bereitgestellten IOPS, den Durchsatz und die Storage-Grenze (mindestens 1,024 gib) anpassen, basierend auf Ihren tatsächlichen Anforderungen zum Zeitpunkt der Implementierung. Die Kapazität lässt sich spontan dynamisch anpassen, ohne dass die Applikationsverfügbarkeit beeinträchtigt wird.
- **Oracle Daten- und Protokolllayout.** in unseren Tests und Validierungen haben wir jeweils zwei ASM-Datenträgergruppen für Daten und Logs eingesetzt. Innerhalb der +DATA asm-Datenträgergruppe haben wir vier Platten in einem Daten NFS File System Mount-Punkt bereitgestellt. Innerhalb der +LOGS asm-Datenträgergruppe haben wir zwei Platten in einem logs NFS-Dateisystem Mount-Punkt bereitgestellt. Bei

großen Datenbankimplementierungen können ASM-Festplattengruppen so aufgebaut werden, dass sie mehrere FSX Dateisysteme mit ASM-NFS-Festplatten umfassen, die über mehrere NFS-Mount-Punkte verteilt sind, die auf FSX-Dateisystemen verankert sind. Diese spezielle Einrichtung wurde speziell dafür entwickelt, den Datenbankdurchsatz mit mehr als 4 GB/s und 160,000 SSD-Brutto-IOPS zu erreichen.

- **DNFS-Konfiguration.** dNFS ist in den Oracle-Kernel integriert und ist dafür bekannt, die Performance von Oracle-Datenbanken drastisch zu steigern, wenn Oracle auf NFS-Speicher bereitgestellt wird. DNFS ist in Oracle-Binärdatei verpackt, ist aber nicht standardmäßig aktiviert. Sie sollte für jede Oracle Database-Bereitstellung auf NFS aktiviert werden. Bei der Bereitstellung mehrerer FSX-Dateisysteme für große Datenbanken sollte dNFS-Multi-Path ordnungsgemäß konfiguriert werden.
- **Oracle ASM-Redundanzebene, die für jede Oracle ASM-Datenträgergruppe verwendet werden soll, die Sie erstellen.** Da FSX den Speicher bereits auf der FSX-Clusterebene spiegelt, sollten Sie dies tun **ONLY** Verwenden Sie die Option Externe Redundanz. Dies bedeutet, dass Oracle ASM den Inhalt der Laufwerksgruppe nicht spiegeln kann. Dies ist besonders wichtig, da die Speicherung von NFS für Oracle-Datenbankdaten **EINE HARTE NFS-Mount-Option** erfordert, die für das Spiegeln von ASM-Inhalten auf Oracle-Ebene **NICHT** wünschenswert ist.
- **Datenbank-Backup.** NetApp bietet eine SaaS-Version des SnapCenter Softwareservice zum Sichern, Wiederherstellen und Klonen von Datenbanken in der Cloud, die über die NetApp BlueXP Konsolen-UI verfügbar ist. NetApp empfiehlt die Implementierung eines solchen Service, um schnelle Snapshot Backups (unter einer Minute), schnelle Datenbank-Restores (wenige Minuten) und Datenbankklone zu erreichen.

Lösungsimplementierung

Im folgenden Abschnitt werden schrittweise Bereitstellungsverfahren beschrieben.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wurde ein AWS Konto eingerichtet, und die erforderlichen VPC und Netzwerksegmente wurden in Ihrem AWS Konto erstellt.
2. Über die AWS EC2-Konsole müssen Sie zwei EC2 Linux-Instanzen implementieren, eine als primärer Oracle DB Server und einen optionalen alternativen Clone-Ziel-DB-Server. Im Architekturdiagramm im vorherigen Abschnitt finden Sie weitere Details zum Umgebungs-Setup. Sehen Sie sich auch die an "[Benutzerhandbuch für Linux-Instanzen](#)" Finden Sie weitere Informationen.
3. Über die AWS EC2-Konsole implementieren Sie Amazon FSX for ONTAP Storage HA-Cluster, um die Oracle Database Volumes zu hosten. Wenn Sie mit der Bereitstellung von FSX-Speicher nicht vertraut sind, lesen Sie die Dokumentation "[Erstellen von FSX für ONTAP-Dateisysteme](#)" Schritt-für-Schritt-Anleitungen.
4. Die Schritte 2 und 3 können mit dem folgenden Terraform Automatisierungs-Toolkit durchgeführt werden, das eine EC2-Instanz mit dem Namen erstellt `ora_01` Und ein FSX Dateisystem mit dem Namen `fsx_01`. Überprüfen Sie die Anweisung sorgfältig, und ändern Sie die Variablen vor der Ausführung entsprechend Ihrer Umgebung.

```
git clone https://github.com/NetApp-  
Automation/na_aws_fsx_ec2_deploy.git
```



Stellen Sie sicher, dass Sie mindestens 50G im Root-Volume der EC2-Instanz zugewiesen haben, damit genügend Speicherplatz für die Bereitstellung der Oracle Installationsdateien zur Verfügung steht.

Konfiguration des EC2-Instance-Kernels

Melden Sie sich bei den bereitgestellten Voraussetzungen als ec2-User bei der EC2-Instanz an und sudo to root-Benutzer, um den Linux-Kernel für die Oracle-Installation zu konfigurieren.

1. Erstellen Sie ein Staging-Verzeichnis `/tmp/archive` Und legen Sie die fest `777` Berechtigung.

```
mkdir /tmp/archive  
  
chmod 777 /tmp/archive
```

2. Laden Sie die Oracle-Binärinstallationsdateien und andere erforderliche rpm-Dateien herunter, und stellen Sie sie auf den bereit `/tmp/archive` Verzeichnis.

Siehe die folgende Liste der Installationsdateien, die in aufgeführt sind `/tmp/archive` Auf der EC2-Instanz.

```
[ec2-user@ip-172-30-15-58 ~]$ ls -l /tmp/archive  
total 10537316  
-rw-rw-r--. 1 ec2-user ec2-user      19112 Mar 21 15:57 compat-  
libcap1-1.10-7.el7.x86_64.rpm  
-rw-rw-r--  1 ec2-user ec2-user 3059705302 Mar 21 22:01  
LINUX.X64_193000_db_home.zip  
-rw-rw-r--  1 ec2-user ec2-user 2889184573 Mar 21 21:09  
LINUX.X64_193000_grid_home.zip  
-rw-rw-r--. 1 ec2-user ec2-user      589145 Mar 21 15:56  
netapp_linux_unified_host_utilities-7-1.x86_64.rpm  
-rw-rw-r--. 1 ec2-user ec2-user      31828 Mar 21 15:55 oracle-  
database-preinstall-19c-1.0-2.el8.x86_64.rpm  
-rw-rw-r--  1 ec2-user ec2-user 2872741741 Mar 21 22:31  
p34762026_190000_Linux-x86-64.zip  
-rw-rw-r--  1 ec2-user ec2-user 1843577895 Mar 21 22:32  
p34765931_190000_Linux-x86-64.zip  
-rw-rw-r--  1 ec2-user ec2-user  124347218 Mar 21 22:33  
p6880880_190000_Linux-x86-64.zip  
-rw-r--r--  1 ec2-user ec2-user    257136 Mar 22 16:25  
policycoreutils-python-utils-2.9-9.el8.noarch.rpm
```

3. Installieren Sie Oracle 19c RPM, das die meisten Anforderungen an die Kernel-Konfiguration erfüllt.

```
yum install /tmp/archive/oracle-database-preinstall-19c-1.0-  
2.el8.x86_64.rpm
```

4. Laden Sie die fehlenden Dateien herunter, und installieren Sie sie `compat-libcap1` Unter Linux 8.


```
yum install /tmp/archive/compat-libcap1-1.10-7.el7.x86_64.rpm
```

5. Laden Sie von NetApp die NetApp Host Utilities herunter und installieren Sie sie.

```
yum install /tmp/archive/netapp_linux_unified_host_utilities-7-1.x86_64.rpm
```

6. Installieren `policycoreutils-python-utils`, Die in der EC2-Instanz nicht verfügbar ist.

```
yum install /tmp/archive/policycoreutils-python-utils-2.9-9.el8.noarch.rpm
```

7. Installieren Sie Open JDK Version 1.8.

```
yum install java-1.8.0-openjdk.x86_64
```

8. installieren sie `nfs-utils`.

```
yum install nfs-utils
```

9. Deaktivieren Sie transparente hugepages im aktuellen System.

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled  
echo never > /sys/kernel/mm/transparent_hugepage/defrag
```

Fügen Sie die folgenden Zeilen hinzu `/etc/rc.local` Zu deaktivieren `transparent_hugepage`
Nach dem Neustart:

```
# Disable transparent hugepages  
if test -f /sys/kernel/mm/transparent_hugepage/enabled;  
then  
    echo never > /sys/kernel/mm/transparent_hugepage/enabled  
fi  
if test -f /sys/kernel/mm/transparent_hugepage/defrag;  
then  
    echo never > /sys/kernel/mm/transparent_hugepage/defrag  
fi
```

10. Deaktivieren sie `selinux`, indem Sie ändern `SELINUX=enforcing` Bis `SELINUX=disabled`. Sie müssen den Host neu starten, damit die Änderung wirksam wird.

```
vi /etc/sysconfig/selinux
```

11. Fügen Sie die folgenden Zeilen zu hinzu `limits.conf` So legen Sie die Dateibeschränkungsgrenze und die Stapelgröße ohne Anführungszeichen fest " " .

```
vi /etc/security/limits.conf
**          hard    nofile      65536"
**          soft    stack       10240"
```

12. Fügen Sie der EC2-Instanz Swap-Speicherplatz hinzu, indem Sie diese Anweisung befolgen: "[Wie weisen ich Speicher zu, um durch Verwendung einer Auslagerungsdatei als Auslagerungsspeicher in einer Amazon EC2 Instanz zu arbeiten?](#)" Die genaue Menge des zu addieren Speicherplatzes hängt von der Größe des RAM bis zu 16G ab.
13. Fügen Sie die ASM-Gruppe hinzu, die für die asm-Sysasm-Gruppe verwendet werden soll

```
groupadd asm
```

14. Ändern Sie den oracle-Benutzer, um ASM als sekundäre Gruppe hinzuzufügen (der oracle-Benutzer sollte nach der RPM-Installation von Oracle vor der Installation erstellt worden sein).

```
usermod -a -G asm oracle
```

15. EC2-Instanz neu booten

Bereitstellen und Exportieren von NFS-Volumes, die auf den EC2-Instanz-Host gemountet werden sollen

Stellen Sie drei Volumes über die Befehlszeile bereit, indem Sie sich beim FSX Cluster über ssh anmelden als fsxadmin-Benutzer mit FSX Cluster Management IP, um die binären, Daten- und Protokolldateien der Oracle-Datenbank zu hosten.

1. Melden Sie sich über SSH als Benutzer von fsxadmin am FSX-Cluster an.

```
ssh fsxadmin@172.30.15.53
```

2. Führen Sie den folgenden Befehl aus, um ein Volume für die Oracle-Binärdatei zu erstellen.

```
vol create -volume ora_01_biny -aggregate aggr1 -size 50G -state  
online -type RW -junction-path /ora_01_biny -snapshot-policy none  
-tiering-policy snapshot-only
```

3. Führen Sie den folgenden Befehl aus, um ein Volume für Oracle-Daten zu erstellen.

```
vol create -volume ora_01_data -aggregate aggr1 -size 100G -state  
online -type RW -junction-path /ora_01_data -snapshot-policy none  
-tiering-policy snapshot-only
```

4. Führen Sie den folgenden Befehl aus, um ein Volume für Oracle-Protokolle zu erstellen.

```
vol create -volume ora_01_logs -aggregate aggr1 -size 100G -state  
online -type RW -junction-path /ora_01_logs -snapshot-policy none  
-tiering-policy snapshot-only
```

5. Erstellte DB-Volumes validieren

```
vol show
```

Es wird erwartet, dass dies wieder zutrifft:

```

FsxId02ad7bf3476b741df::> vol show
(vol show)
FsxId06c3c8b2a7bd56458::> vol show
Vserver   Volume           Aggregate   State      Type      Size
Available Used%
-----
svm_ora   ora_01_biny      aggr1      online     RW        50GB
47.50GB   0%
svm_ora   ora_01_data      aggr1      online     RW        100GB
95.00GB   0%
svm_ora   ora_01_logs      aggr1      online     RW        100GB
95.00GB   0%
svm_ora   svm_ora_root     aggr1      online     RW        1GB
972.1MB   0%
4 entries were displayed.

```

Konfiguration des Datenbank-Storage

Importieren und richten Sie nun den FSX Storage für die Oracle Grid-Infrastruktur und die Datenbankinstallation auf dem EC2-Instanzhost ein.

1. Melden Sie sich über SSH als ec2-Benutzer mit Ihrem SSH-Schlüssel und der IP-Adresse der EC2-Instanz an.

```
ssh -i ora_01.pem ec2-user@172.30.15.58
```

2. Erstellen Sie das Verzeichnis /u01, um das Binärdateisystem von Oracle zu mounten

```
sudo mkdir /u01
```

3. Mounten Sie das binäre Volume in /u01, Geändert zu Ihrer FSX NFS LIF IP-Adresse. Wenn Sie FSX Cluster über das Automatisierungs-Toolkit von NetApp implementiert haben, wird die NFS-LIF-IP-Adresse des virtuellen Storage-Servers in der Ausgabe am Ende der Ausführung der Ressourcenbereitstellung aufgeführt. Andernfalls kann es von der AWS FSX Konsolen-UI abgerufen werden.

```
sudo mount -t nfs 172.30.15.19:/ora_01_biny /u01 -o  
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536
```

4. Ändern /u01 Mount Point Ownership für den Oracle-Benutzer und die zugehörige primäre Gruppe.

```
sudo chown oracle:oinstall /u01
```

5. Erstellen Sie das Verzeichnis /oradata, um das Oracle-Datendateisystem zu mounten

```
sudo mkdir /oradata
```

6. Mounten Sie das Daten-Volume auf /oradata, Geändert zu Ihrer FSX NFS LIF IP-Adresse

```
sudo mount -t nfs 172.30.15.19:/ora_01_data /oradata -o  
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536
```

7. Ändern /oradata Mount Point Ownership für den Oracle-Benutzer und die zugehörige primäre Gruppe.

```
sudo chown oracle:oinstall /oradata
```

8. Erstellen Sie das Verzeichnis /oralogs, um das Dateisystem Oracle logs zu mounten

```
sudo mkdir /oralogs
```

9. Mounten Sie das Protokoll-Volume in /oralogs, Geändert zu Ihrer FSX NFS LIF IP-Adresse

```
sudo mount -t nfs 172.30.15.19:/ora_01_logs /oralogs -o  
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536
```

10. Ändern /oralogs Mount Point Ownership für den Oracle-Benutzer und die zugehörige primäre Gruppe.

```
sudo chown oracle:oinstall /oralogs
```

11. Hinzufügen eines Mount-Punkts zu /etc/fstab.

```
sudo vi /etc/fstab
```

Fügen Sie die folgende Zeile hinzu.

```
172.30.15.19:/ora_01_biny      /u01          nfs  
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536  0  
0  
172.30.15.19:/ora_01_data     /oradata      nfs  
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536  0  
0  
172.30.15.19:/ora_01_logs     /oralogs      nfs  
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536  0  
0
```

12. Erstellen sie für oracle-Benutzer asm-Ordner, um asm-Festplattendateien zu speichern

```
sudo su  
su - oracle  
mkdir /oradata/asm  
mkdir /oralogs/asm
```

13. Erstellen Sie als oracle-Benutzer asm-Datenfestplattendateien, und ändern Sie die Anzahl so, dass sie mit der Größe der Festplatte mit der Blockgröße übereinstimmt.

```
dd if=/dev/zero of=/oradata/asm/nfs_data_disk01 bs=1M count=20480
oflag=direct
dd if=/dev/zero of=/oradata/asm/nfs_data_disk02 bs=1M count=20480
oflag=direct
dd if=/dev/zero of=/oradata/asm/nfs_data_disk03 bs=1M count=20480
oflag=direct
dd if=/dev/zero of=/oradata/asm/nfs_data_disk04 bs=1M count=20480
oflag=direct
```

14. Ändern Sie als Root-Benutzer die Berechtigung für die Datenplattendatei auf 640

```
chmod 640 /oradata/asm/*
```

15. ERSTELLEN SIE ALS oracle-Benutzer asm-Protokolldateien, und ändern Sie die Anzahl, um sie der Größe der Festplatte mit der Blockgröße anzupassen.

```
dd if=/dev/zero of=/oralogs/asm/nfs_logs_disk01 bs=1M count=40960
oflag=direct
dd if=/dev/zero of=/oralogs/asm/nfs_logs_disk02 bs=1M count=40960
oflag=direct
```

16. Ändern Sie als Root-Benutzer die Berechtigung für die Protokolldatenträger in 640

```
chmod 640 /oralogs/asm/*
```

17. Booten Sie den EC2-Instanzhost neu.

Installation der Oracle Grid-Infrastruktur

1. Melden Sie sich als ec2-Benutzer über SSH bei der EC2-Instanz an und aktivieren Sie die Passwortauthentifizierung durch Entkommentieren `PasswordAuthentication yes` Und dann kommentiert `PasswordAuthentication no`.

```
sudo vi /etc/ssh/sshd_config
```

2. Starten Sie den sshd-Dienst neu.

```
sudo systemctl restart sshd
```

3. Setzen Sie das Oracle-Benutzerpasswort zurück.

```
sudo passwd oracle
```

4. Melden Sie sich als Oracle Restart Software Owner User (oracle) an. Erstellen Sie ein Oracle-Verzeichnis wie folgt:

```
mkdir -p /u01/app/oracle  
mkdir -p /u01/app/oraInventory
```

5. Ändern Sie die Verzeichnisberechtigungseinstellung.

```
chmod -R 775 /u01/app
```

6. Erstellen Sie ein Grid-Home-Verzeichnis, und ändern Sie es.

```
mkdir -p /u01/app/oracle/product/19.0.0/grid  
cd /u01/app/oracle/product/19.0.0/grid
```

7. Entpacken Sie die Grid-Installationsdateien.

```
unzip -q /tmp/archive/LINUX.X64_193000_grid_home.zip
```

8. Löschen Sie von der Startseite des Rasters aus die OPatch Verzeichnis.

```
rm -rf OPatch
```

9. Kopieren Sie von der Grid Home-Funktion `p6880880_190000_Linux-x86-64.zip` An `GRID_Home`, und entpacken Sie sie.


```
cp /tmp/archive/p6880880_190000_Linux-x86-64.zip .
unzip p6880880_190000_Linux-x86-64.zip
```

10. Von der Startseite des Rasters aus, überarbeiten `cv/admin/cvu_config`, Entkommentieren und ersetzen `CV_ASSUME_DISTID=OEL5` Mit `CV_ASSUME_DISTID=OL7`.

```
vi cv/admin/cvu_config
```

11. Bereiten Sie ein vor `gridsetup.rsp` Datei für die automatische Installation und legen Sie die `rsp`-Datei im ab `/tmp/archive` Verzeichnis. Die `rsp`-Datei sollte die Abschnitte A, B und G mit den folgenden Informationen abdecken:

```
INVENTORY_LOCATION=/u01/app/oraInventory
oracle.install.option=HA_CONFIG
ORACLE_BASE=/u01/app/oracle
oracle.install.asm.OSDBA=dba
oracle.install.asm.OSOPER=oper
oracle.install.asm.OSASM=asm
oracle.install.asm.SYSASMPassword="SetPWD"
oracle.install.asm.diskGroup.name=DATA
oracle.install.asm.diskGroup.redundancy=EXTERNAL
oracle.install.asm.diskGroup.AUSize=4
oracle.install.asm.diskGroup.disks=/oradata/asm/*,/orlogs/asm/*
oracle.install.asm.diskGroup.diskDiscoveryString=/oradata/asm/nfs_data_
ta_disk01,/oradata/asm/nfs_data_disk02,/oradata/asm/nfs_data_disk03,
/oradata/asm/nfs_data_disk04
oracle.install.asm.monitorPassword="SetPWD"
oracle.install.asm.configureAFD=false
```

12. Melden Sie sich als Root-Benutzer bei der EC2-Instanz an.

13. Installieren `cvuqdisk-1.0.10-1.rpm`.

```
rpm -ivh /u01/app/oracle/product/19.0.0/grid/cv/rpm/cvuqdisk-1.0.10-
1.rpm
```

14. Melden Sie sich als Oracle-Benutzer bei der EC2-Instanz an und extrahieren Sie den Patch in `/tmp/archive` Ordner.

```
unzip p34762026_190000_Linux-x86-64.zip
```

15. Starten Sie von Grid Home `/u01/App/oracle/Product/19.0.0/GRID` aus und als oracle-Benutzer

gridSetup.sh Für die Installation der Netzinfrastruktur.

```
./gridSetup.sh -applyRU /tmp/archive/34762026/ -silent  
-responseFile /tmp/archive/gridsetup.rsp
```

Ignorieren Sie die Warnungen über falsche Gruppen für die Netzinfrastruktur. Wir verwenden einen einzigen Oracle-Benutzer, um Oracle Restart zu verwalten. Das wird also erwartet.

16. Führen Sie als root-Benutzer folgende(n) Skript(e) aus:

```
/u01/app/oraInventory/orainstRoot.sh  
  
/u01/app/oracle/product/19.0.0/grid/root.sh
```

17. Führen Sie als Oracle-Benutzer den folgenden Befehl aus, um die Konfiguration abzuschließen:

```
/u01/app/oracle/product/19.0.0/grid/gridSetup.sh -executeConfigTools  
-responseFile /tmp/archive/gridsetup.rsp -silent
```

18. Erstellen Sie als Oracle-Benutzer die PROTOKOLLDATENTRÄGER-Gruppe.

```
bin/asmca -silent -sysAsmPassword 'yourPWD' -asmsnmpPassword  
'yourPWD' -createDiskGroup -diskGroupName LOGS -disk  
'/orlogs/asm/nfs_logs_disk*' -redundancy EXTERNAL -au_size 4
```

19. Validieren Sie als Oracle-Benutzer nach der Installation die Grid-Services.

```

bin/crsctl stat res -t
+
Name                Target  State      Server
State details
Local Resources
ora.DATA.dg         ONLINE ONLINE     ip-172-30-15-58
STABLE
ora.LISTENER.lsnr   ONLINE ONLINE     ip-172-30-15-58
STABLE
ora.LOGS.dg         ONLINE ONLINE     ip-172-30-15-58
STABLE
ora.asm             ONLINE ONLINE     ip-172-30-15-58
Started,STABLE
ora.ons             OFFLINE OFFLINE    ip-172-30-15-58
STABLE
Cluster Resources
ora.cssd            ONLINE ONLINE     ip-172-30-15-58
STABLE
ora.diskmon         OFFLINE OFFLINE
STABLE
ora.driver.afd      ONLINE ONLINE     ip-172-30-15-58
STABLE
ora.evmd            ONLINE ONLINE     ip-172-30-15-58
STABLE

```

Installation der Oracle Database

1. Melden Sie sich als Oracle-Benutzer an, und heben Sie die Einstellung auf \$ORACLE_HOME Und \$ORACLE_SID Wenn es eingestellt ist.

```
unset ORACLE_HOME
unset ORACLE_SID
```

2. Erstellen Sie das Oracle DB Home-Verzeichnis, und ändern Sie es.

```
mkdir /u01/app/oracle/product/19.0.0/db1
cd /u01/app/oracle/product/19.0.0/db1
```

3. Entpacken Sie die Oracle DB-Installationsdateien.

```
unzip -q /tmp/archive/LINUX.X64_193000_db_home.zip
```

4. Löschen Sie von der DB-Startseite aus die OPatch Verzeichnis.

```
rm -rf OPatch
```

5. Kopieren Sie von der DB-Startseite aus p6880880_190000_Linux-x86-64.zip Bis `grid_home` Und dann entpacken Sie es.

```
cp /tmp/archive/p6880880_190000_Linux-x86-64.zip .
unzip p6880880_190000_Linux-x86-64.zip
```

6. Überarbeiten Sie von der DB-Startseite aus cv/admin/cvu_config`Und entkommentieren und ersetzen `CV_ASSUME_DISTID=OEL5 Mit CV_ASSUME_DISTID=OL7.

```
vi cv/admin/cvu_config
```

7. Von /tmp/archive Das DB 19.18 RU-Patch entpacken.

```
unzip p34765931_190000_Linux-x86-64.zip
```

8. Bereiten Sie die automatische DB-Installationsdatei in vor /tmp/archive/dbinstall.rsp Verzeichnis mit folgenden Werten:

```
oracle.install.option=INSTALL_DB_SWONLY
UNIX_GROUP_NAME=oinstall
INVENTORY_LOCATION=/u01/app/oraInventory
ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
ORACLE_BASE=/u01/app/oracle
oracle.install.db.InstallEdition=EE
oracle.install.db.OSDBA_GROUP=dba
oracle.install.db.OSOPER_GROUP=oper
oracle.install.db.OSBACKUPDBA_GROUP=oper
oracle.install.db.OSDGDBA_GROUP=dba
oracle.install.db.OSKMDBA_GROUP=dba
oracle.install.db.OSRACDBA_GROUP=dba
oracle.install.db.rootconfig.executeRootScript=false
```

9. Führen Sie von db1 Home /u01/App/oracle/Product/19.0.0/db1 aus die automatische, rein softwarebasierte DB-Installation aus.

```
./runInstaller -applyRU /tmp/archive/34765931/ -silent
-ignorePrereqFailure -responseFile /tmp/archive/dbinstall.rsp
```

10. Führen Sie als Root-Benutzer den aus `root.sh` Skript nach der Installation nur für Software.

```
/u01/app/oracle/product/19.0.0/db1/root.sh
```

11. Erstellen Sie als Oracle-Benutzer den `dbca.rsp` Datei mit folgenden Einträgen:

```
gdbName=db1.demo.netapp.com
sid=db1
createAsContainerDatabase=true
numberOfPDBs=3
pdbName=db1_pdb
useLocalUndoForPDBs=true
pdbAdminPassword="yourPWD"
templateName=General_Purpose.dbc
sysPassword="yourPWD"
systemPassword="yourPWD"
dbsnmpPassword="yourPWD"
storageType=ASM
diskGroupName=DATA
characterSet=AL32UTF8
nationalCharacterSet=AL16UTF16
listeners=LISTENER
databaseType=MULTIPURPOSE
automaticMemoryManagement=false
totalMemory=8192
```



Legen Sie den Gesamtspeicher auf der Grundlage des verfügbaren Speichers im EC2-Instanzhost fest. Oracle weist 75 % der `totalMemory` Zu DB-Instanz-SGA oder Puffer-Cache.

12. Als Oracle-Benutzer, lauch DB-Erstellung mit dbca.

```
bin/dbca -silent -createDatabase -responseFile /tmp/archive/dbca.rsp
```

output:

Prepare for db operation

7% complete

Registering database with Oracle Restart

11% complete

Copying database files

33% complete

Creating and starting Oracle instance

35% complete

38% complete

42% complete

45% complete

48% complete

Completing Database Creation

53% complete

55% complete

56% complete

Creating Pluggable Databases

60% complete

64% complete

69% complete

78% complete

Executing Post Configuration Actions

100% complete

Database creation complete. For details check the logfiles at:

/u01/app/oracle/cfgtoollogs/dbca/db1.

Database Information:

Global Database Name:db1.demo.netapp.com

System Identifier(SID):db1

Look at the log file "/u01/app/oracle/cfgtoollogs/dbca/db1/db1.log"
for further details.

13. Validieren Sie als Oracle-Benutzer Oracle Neustart der HA-Services nach der DB-Erstellung.

```

[oracle@ip-172-30-15-58 db1]$ ../grid/bin/crsctl stat res -t
-----
-----
Name          Target  State          Server          State
details
-----
-----
Local Resources
-----
-----
ora.DATA.dg
          ONLINE  ONLINE         ip-172-30-15-58      STABLE
ora.LISTENER.lsnr
          ONLINE  ONLINE         ip-172-30-15-58      STABLE
ora.LOGS.dg
          ONLINE  ONLINE         ip-172-30-15-58      STABLE
ora.asm
          ONLINE  ONLINE         ip-172-30-15-58
Started,STABLE
ora.ons
          OFFLINE OFFLINE         ip-172-30-15-58      STABLE
-----
-----
Cluster Resources
-----
-----
ora.cssd
   1      ONLINE  ONLINE         ip-172-30-15-58      STABLE
ora.dbf.db
   1      ONLINE  ONLINE         ip-172-30-15-58
Open,HOME=/u01/app/o
racle/product/19.0.0
/db1,STABLE
ora.diskmon
   1      OFFLINE OFFLINE
ora.evmd
   1      ONLINE  ONLINE         ip-172-30-15-58      STABLE
-----
-----
[oracle@ip-172-30-15-58 db1]$

```

14. Legen Sie den Oracle-Benutzer fest `.bash_profile`.


```
vi ~/.bash_profile
```

15. Folgende Einträge hinzufügen:

```
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
export ORACLE_SID=db1
export PATH=$PATH:$ORACLE_HOME/bin
alias asm='export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/grid;export
ORACLE_SID=+ASM;export PATH=$PATH:$ORACLE_HOME/bin'
```

16. Überprüfen Sie die erstellte CDB/PDB.

```
. ~/.bash_profile

sqlplus / as sysdba

SQL> select name, open_mode from v$database;

NAME          OPEN_MODE

DB1           READ WRITE

SQL> select name from v$datafile;

NAME

+DATA/DB1/DATAFILE/system.256.1132176177
+DATA/DB1/DATAFILE/sysaux.257.1132176221
+DATA/DB1/DATAFILE/undotbs1.258.1132176247
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/system.265.11321
77009
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/sysaux.266.11321
77009
+DATA/DB1/DATAFILE/users.259.1132176247
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/undotbs1.267.113
2177009
+DATA/DB1/F7852758DCD6B800E0533A0F1EAC1DC6/DATAFILE/system.271.11321
77853
+DATA/DB1/F7852758DCD6B800E0533A0F1EAC1DC6/DATAFILE/sysaux.272.11321
77853
+DATA/DB1/F7852758DCD6B800E0533A0F1EAC1DC6/DATAFILE/undotbs1.270.113
2177853
+DATA/DB1/F7852758DCD6B800E0533A0F1EAC1DC6/DATAFILE/users.274.113217
```

```
7871
```

```
NAME
```

```
+DATA/DB1/F785288BBCD1BA78E0533A0F1EACCD6F/DATAFILE/system.276.11321
77871
+DATA/DB1/F785288BBCD1BA78E0533A0F1EACCD6F/DATAFILE/sysaux.277.11321
77871
+DATA/DB1/F785288BBCD1BA78E0533A0F1EACCD6F/DATAFILE/undotbs1.275.113
2177871
+DATA/DB1/F785288BBCD1BA78E0533A0F1EACCD6F/DATAFILE/users.279.113217
7889
+DATA/DB1/F78529A14DD8BB18E0533A0F1EACB8ED/DATAFILE/system.281.11321
77889
+DATA/DB1/F78529A14DD8BB18E0533A0F1EACB8ED/DATAFILE/sysaux.282.11321
77889
+DATA/DB1/F78529A14DD8BB18E0533A0F1EACB8ED/DATAFILE/undotbs1.280.113
2177889
+DATA/DB1/F78529A14DD8BB18E0533A0F1EACB8ED/DATAFILE/users.284.113217
7907
```

```
19 rows selected.
```

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	DB1_PDB1	READ WRITE	NO
4	DB1_PDB2	READ WRITE	NO
5	DB1_PDB3	READ WRITE	NO

```
SQL>
```

17. Wechseln Sie als oracle-Benutzer zu Oracle Database Home Directory /u01/App/oracle/Product/19.0.0/db1, und aktivieren Sie dNFS

```
cd /u01/app/oracle/product/19.0.0/db1

mkdir rdbms/lib/odm

cp lib/libnfsodm19.so rdbms/lib/odm/
```

18. Konfigurieren Sie die oranfstab-Datei in ORACLE_HOME

```
vi $ORACLE_HOME/dbs/oranfstab

add following entries:

server: fsx_01
local: 172.30.15.58 path: 172.30.15.19
nfs_version: nfsv3
export: /ora_01_biny mount: /u01
export: /ora_01_data mount: /oradata
export: /ora_01_logs mount: /oralogs
```

19. Melden Sie sich als oracle-Benutzer bei der Datenbank von sqlplus an und legen Sie die Größe und den Speicherort der DB-Wiederherstellung auf die +LOGS-Laufwerksgruppe fest.

```
. ~/.bash_profile

sqlplus / as sysdba

alter system set db_recovery_file_dest_size = 80G scope=both;

alter system set db_recovery_file_dest = '+LOGS' scope=both;
```

20. Aktivieren Sie den Archivprotokollmodus, und starten Sie die Oracle DB-Instanz neu

```
shutdown immediate;

startup mount;

alter database archivelog;

alter database open;

alter system switch logfile;
```

21. Überprüfen Sie den DB-Protokollmodus und dNFS nach dem Neustart der Instanz

```
SQL> select name, log_mode from v$database;
```

```
NAME          LOG_MODE
-----
DB1           ARCHIVELOG
```

```
SQL> select svrname, dirname from v$dnfs_servers;
```

```
SVRNAME
-----
DIRNAME
-----
fsx_01
/ora_01_data

fsx_01
/ora_01_biny

fsx_01
/ora_01_logs
```

22. Validierung von Oracle ASM

```
[oracle@ip-172-30-15-58 db1]$ asm
[oracle@ip-172-30-15-58 db1]$ sqlplus / as sysasm

SQL*Plus: Release 19.0.0.0.0 - Production on Tue May 9 20:39:39 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> set lin 200
SQL> col path form a30
SQL> select name, path, header_status, mount_status, state from
v$asm_disk;

NAME          PATH
```

```

HEADER_STATU MOUNT_S STATE
-----
-----
DATA_0002          /oradata/asm/nfs_data_disk01  MEMBER
  CACHED  NORMAL
DATA_0000          /oradata/asm/nfs_data_disk02  MEMBER
  CACHED  NORMAL
DATA_0001          /oradata/asm/nfs_data_disk03  MEMBER
  CACHED  NORMAL
DATA_0003          /oradata/asm/nfs_data_disk04  MEMBER
  CACHED  NORMAL
LOGS_0000          /orlogs/asm/nfs_logs_disk01   MEMBER
  CACHED  NORMAL
LOGS_0001          /orlogs/asm/nfs_logs_disk02   MEMBER
  CACHED  NORMAL

```

6 rows selected.

```
SQL> select name, state, ALLOCATION_UNIT_SIZE, TOTAL_MB, FREE_MB
from v$asm_diskgroup;
```

```

NAME                                STATE      ALLOCATION_UNIT_SIZE
TOTAL_MB      FREE_MB
-----
DATA                                MOUNTED    4194304
81920          73536
LOGS                                MOUNTED    4194304
81920          81640

```

This completes Oracle 19c version 19.18 Restart deployment on an Amazon FSx for ONTAP and EC2 compute instance with NFS/ASM. If desired, NetApp recommends relocating the Oracle control file and online log files to the +LOGS disk group.

Automatische Bereitstellungsoption

NetApp veröffentlicht ein vollständig automatisiertes Toolkit für die Lösungsbereitstellung mit Ansible, um die Implementierung dieser Lösung zu erleichtern. Bitte überprüfen Sie die Verfügbarkeit des Toolkits. Nach der Veröffentlichung wird hier ein Link gepostet.

Backup, Wiederherstellung und Klonen von Oracle Datenbanken mit SnapCenter Services

Derzeit wird Oracle-Datenbanken mit NFS- und ASM-Speicheroption nur von dem herkömmlichen UI-Tool SnapCenter Server unterstützt, siehe ["Hybrid-Cloud-Datenbanklösungen mit SnapCenter"](#) Weitere

Informationen zum Backup, zur Wiederherstellung und zum Klonen von Oracle-Datenbanken erhalten Sie in der Benutzeroberfläche von NetApp SnapCenter.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- Installieren der Oracle Grid-Infrastruktur für einen eigenständigen Server mit einer neuen Datenbankinstallation

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3)

- Installieren und Konfigurieren von Oracle Database mithilfe von Antwortdateien

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7)

- Amazon FSX für NetApp ONTAP

["https://aws.amazon.com/fsx/netapp-ontap/"](https://aws.amazon.com/fsx/netapp-ontap/)

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

TR-4965: Oracle Database Deployment and Protection in AWS FSX/EC2 with iSCSI/ASM

Allen Cao, Niyaz Mohamed, NetApp

Zweck

ASM (Automatic Storage Management) ist ein beliebter Oracle Storage Volume Manager, der in vielen Oracle-Installationen eingesetzt wird. Es ist außerdem die von Oracle empfohlene Storage-Managementlösung. Sie stellt eine Alternative zu herkömmlichen Volume Managern und Filesystemen dar. Seit Oracle Version 11g ist ASM nicht mehr eine Datenbank, sondern eine Grid-Infrastruktur. Um Oracle ASM für das Storage-Management ohne RAC zu nutzen, müssen Sie daher die Oracle Grid-Infrastruktur auf einem eigenständigen Server installieren, der auch als Oracle Restart bezeichnet wird. Dies führt zweifellos zu einer größeren Komplexität bei der Implementierung von Oracle-Datenbanken. Wie der Name jedoch andeutet, werden ausgefallene Oracle-Dienste, wenn Oracle im Neustart-Modus bereitgestellt wird, automatisch von der Grid-Infrastruktur oder nach einem Host-Neustart ohne Benutzereingriff neu gestartet, was ein gewisses Maß an Hochverfügbarkeit oder HA-Funktionalität bietet.

In dieser Dokumentation zeigen wir, wie eine Oracle Datenbank mit dem iSCSI-Protokoll und Oracle ASM in einer Amazon FSX für ONTAP Storage-Umgebung mit EC2 Computing-Instanzen implementiert wird. Wir zeigen Ihnen auch, wie Sie den NetApp SnapCenter-Service über die NetApp BlueXP Konsole nutzen können, um Ihre Oracle Datenbank für Entwicklung/Tests zu sichern, wiederherzustellen und zu klonen. Andere Anwendungsfälle für den Storage-effizienten Datenbankbetrieb in der AWS Public Cloud zeigen wir Ihnen auch, wie.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Oracle Database-Implementierung in Amazon FSX for ONTAP Storage und EC2-Computing-Instanzen mit iSCSI/ASM
- Testen und Validieren eines Oracle-Workloads in der Public AWS Cloud mit iSCSI/ASM
- Testen und Validieren der in AWS bereitgestellten Funktionen zum Neustart von Oracle-Datenbanken

Zielgruppe

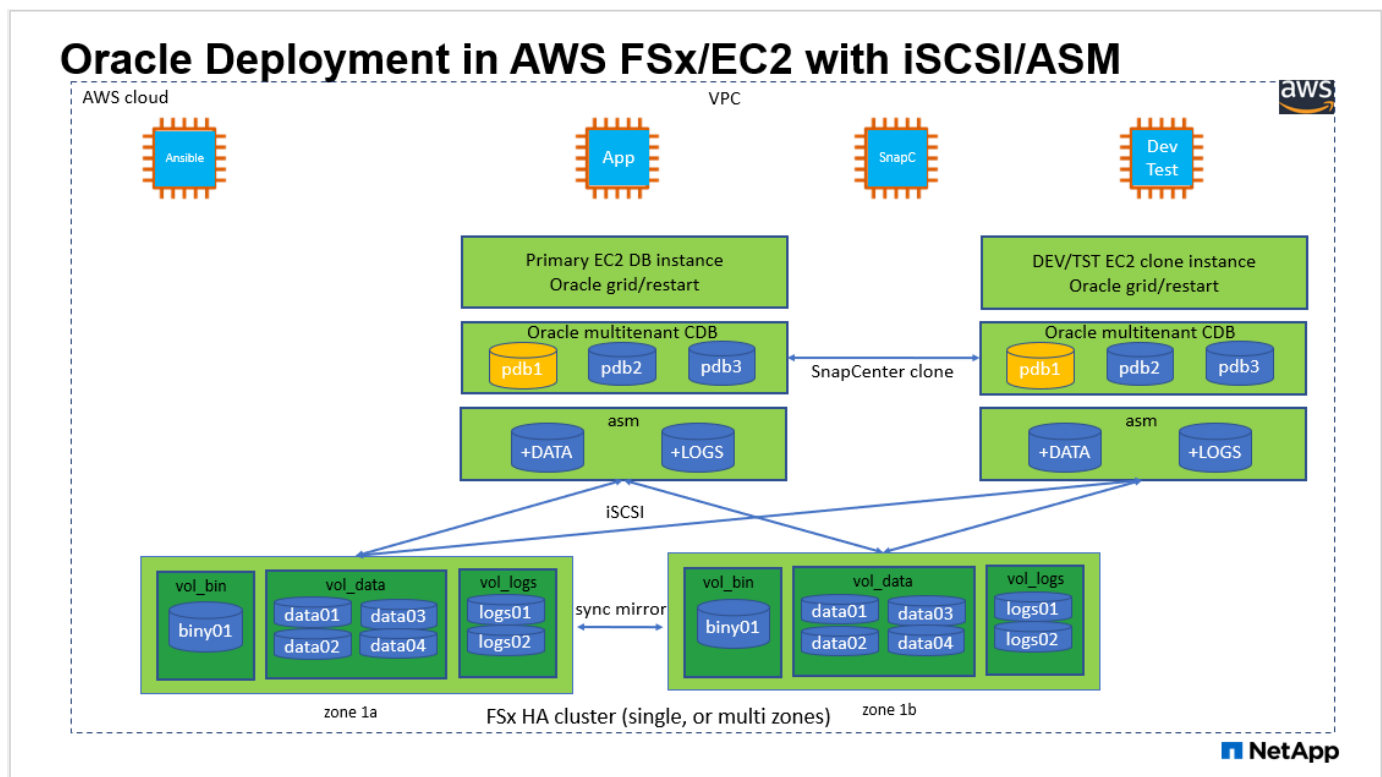
Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle in einer AWS Public Cloud mit iSCSI/ASM implementieren möchte.
- Ein Solution Architect für Datenbanken, der Oracle-Workloads in der AWS-Public Cloud testen möchte.
- Storage-Administrator, der eine in AWS FSX Storage implementierte Oracle-Datenbank implementieren und managen möchte.
- Der Applikationseigentümer, der eine Oracle Database in AWS FSX/EC2 einrichten möchte.

Test- und Validierungsumgebung der Lösung

Tests und Validierungen dieser Lösung wurden in einer AWS FSX- und EC2-Umgebung durchgeführt, die möglicherweise nicht mit der endgültigen Implementierungsumgebung übereinstimmt. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind



Hardware- und Softwarekomponenten

Hardware

FSX ONTAP-Storage	Aktuelle Version von AWS angeboten	Ein FSX HA-Cluster in der gleichen VPC und Verfügbarkeitszone
EC2 Instanz für Computing	t2.xlarge/4vCPU/16G	Zwei EC2 T2 xlarge EC2-Instanzen, eine als primärer DB-Server und die andere als Klon-DB-Server
Software		
Redhat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Bereitstellung der RedHat Subscription für Tests
Oracle Grid Infrastructure	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
SnapCenter-Service	Version	v2.3.1.2324

Wichtige Faktoren für die Implementierung

- **EC2 Compute-Instanzen.** in diesen Tests und Validierungen haben wir einen Instanztyp AWS EC2 t2.xlarge für die Compute-Instanz der Oracle-Datenbank verwendet. NetApp empfiehlt, in der Produktionsumgebung eine EC2-Instanz vom Typ M5 als Computing-Instanz für Oracle zu verwenden, da sie für Datenbank-Workloads optimiert ist. Sie müssen die Größe der EC2-Instanz entsprechend der Anzahl der vCPUs und der Menge des RAM anpassen, basierend auf den tatsächlichen Workload-Anforderungen.
- **FSX Storage HA Cluster Single- oder Multi-Zone-Implementierung.** bei diesen Tests und Validierungen haben wir einen FSX HA-Cluster in einer einzelnen AWS Verfügbarkeitszone implementiert. Für die Implementierung in der Produktion empfiehlt NetApp die Implementierung eines FSX HA-Paars in zwei verschiedenen Verfügbarkeitszonen. Ein FSX HA-Cluster wird in einem HA-Paar bereitgestellt, das in einem Paar aktiv/Passiv-Filesysteme gespiegelt wird, um Redundanz auf Storage-Ebene bereitzustellen. Die Implementierung mit mehreren Zonen verbessert die Hochverfügbarkeit bei einem Ausfall in einer einzelnen AWS Zone noch weiter.
- **FSX Storage-Cluster-Sizing.** ein Amazon FSX for ONTAP Storage-Dateisystem bietet bis zu 160,000 RAW SSD IOPS, einen Durchsatz von bis zu 4 Gbit/s und eine maximale Kapazität von 192 tib. Sie können das Cluster jedoch in Bezug auf die bereitgestellten IOPS, den Durchsatz und die Storage-Grenze (mindestens 1,024 gib) anpassen, basierend auf Ihren tatsächlichen Anforderungen zum Zeitpunkt der Implementierung. Die Kapazität lässt sich spontan dynamisch anpassen, ohne dass die Applikationsverfügbarkeit beeinträchtigt wird.
- **Oracle Daten- und Protokolllayout.** in unseren Tests und Validierungen haben wir jeweils zwei ASM-Datenträgergruppen für Daten und Logs eingesetzt. Innerhalb der +DATA asm-Festplattengruppe haben wir vier LUNs in einem Daten-Volumen bereitgestellt. Innerhalb der +LOGS asm-Datenträgergruppe haben wir zwei LUNs in einem logs Volumen bereitgestellt. Im Allgemeinen bieten mehrere in einem Amazon FSX für ONTAP Volume bereitgestellte LUNs eine bessere Performance.
- **ISCSI Konfiguration.** der EC2 Instance Datenbank Server verbindet sich mit FSX Speicher mit dem iSCSI Protokoll. EC2-Instanzen werden normalerweise mit einer einzelnen Netzwerkschnittstelle oder ENI

implementiert. Die einzelne NIC-Schnittstelle überträgt sowohl den iSCSI- als auch den Anwendungsdatenverkehr. Es ist wichtig, die Spitzenanforderungen für den I/O-Durchsatz der Oracle-Datenbank abzuschätzen, indem der Oracle AWR-Bericht sorgfältig analysiert wird, um eine geeignete EC2-Compute-Instanz zu wählen, die sowohl die Anforderungen an den Anwendungs- als auch den iSCSI-Datendurchsatz erfüllt. NetApp empfiehlt außerdem, beiden FSX iSCSI-Endpunkten vier iSCSI-Verbindungen mit einer ordnungsgemäß konfigurierten Multipath-Konfiguration zuzuweisen.

- **Oracle ASM-Redundanzebene, die für jede von Ihnen erstellte Oracle ASM-Laufwerksgruppe verwendet wird.** Da FSX den Speicher bereits auf der FSX-Clusterebene spiegelt, sollten Sie External Redundancy verwenden, was bedeutet, dass die Option Oracle ASM nicht erlaubt, den Inhalt der Laufwerksgruppe zu spiegeln.
- **Datenbank-Backup.** NetApp bietet eine SaaS-Version des SnapCenter Softwareservice zum Sichern, Wiederherstellen und Klonen von Datenbanken in der Cloud, die über die NetApp BlueXP Konsolen-UI verfügbar ist. NetApp empfiehlt die Implementierung eines solchen Service, um schnelle Snapshot Backups (unter einer Minute), schnelle Datenbank-Restores (wenige Minuten) und Datenbankklone zu erreichen.

Lösungsimplementierung

Im folgenden Abschnitt werden schrittweise Bereitstellungsverfahren beschrieben.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wurde ein AWS Konto eingerichtet, und die erforderlichen VPC und Netzwerksegmente wurden in Ihrem AWS Konto erstellt.
2. Über die AWS EC2-Konsole müssen Sie zwei EC2 Linux-Instanzen implementieren, eine als primärer Oracle DB Server und einen optionalen alternativen Clone-Ziel-DB-Server. Im Architekturdiagramm im vorherigen Abschnitt finden Sie weitere Details zum Umgebungs-Setup. Sehen Sie sich auch die an "[Benutzerhandbuch für Linux-Instanzen](#)". Finden Sie weitere Informationen.
3. Über die AWS EC2-Konsole implementieren Sie Amazon FSX for ONTAP Storage HA-Cluster, um die Oracle Database Volumes zu hosten. Wenn Sie mit der Bereitstellung von FSX-Speicher nicht vertraut sind, lesen Sie die Dokumentation "[Erstellen von FSX für ONTAP-Dateisysteme](#)" Schritt-für-Schritt-Anleitungen.
4. Die Schritte 2 und 3 können mit dem folgenden Terraform Automatisierungs-Toolkit durchgeführt werden, das eine EC2-Instanz mit dem Namen `ora_01` und ein FSX Dateisystem mit dem Namen `fsx_01` erstellt. Überprüfen Sie die Anweisung sorgfältig, und ändern Sie die Variablen vor der Ausführung entsprechend Ihrer Umgebung.

```
git clone https://github.com/NetApp-
Automation/na_aws_fsx_ec2_deploy.git
```



Stellen Sie sicher, dass Sie mindestens 50G im Root-Volume der EC2-Instanz zugewiesen haben, damit genügend Speicherplatz für die Bereitstellung der Oracle Installationsdateien zur Verfügung steht.

Konfiguration des EC2-Instance-Kernels

Melden Sie sich bei den bereitgestellten Voraussetzungen als ec2-User bei der EC2-Instanz an und sudo to root-Benutzer, um den Linux-Kernel für die Oracle-Installation zu konfigurieren.

1. Erstellen Sie ein Staging-Verzeichnis `/tmp/archive` Und legen Sie die fest `777` Berechtigung.

```
mkdir /tmp/archive  
  
chmod 777 /tmp/archive
```

2. Laden Sie die Oracle-Binärinstallationsdateien und andere erforderliche rpm-Dateien herunter, und stellen Sie sie auf den bereit `/tmp/archive` Verzeichnis.

Siehe die folgende Liste der Installationsdateien, die in aufgeführt sind `/tmp/archive` Auf der EC2-Instanz.

```
[ec2-user@ip-172-30-15-58 ~]$ ls -l /tmp/archive  
total 10537316  
-rw-rw-r--. 1 ec2-user ec2-user      19112 Mar 21 15:57 compat-  
libcap1-1.10-7.el7.x86_64.rpm  
-rw-rw-r--  1 ec2-user ec2-user 3059705302 Mar 21 22:01  
LINUX.X64_193000_db_home.zip  
-rw-rw-r--  1 ec2-user ec2-user 2889184573 Mar 21 21:09  
LINUX.X64_193000_grid_home.zip  
-rw-rw-r--. 1 ec2-user ec2-user      589145 Mar 21 15:56  
netapp_linux_unified_host_utilities-7-1.x86_64.rpm  
-rw-rw-r--. 1 ec2-user ec2-user      31828 Mar 21 15:55 oracle-  
database-preinstall-19c-1.0-2.el8.x86_64.rpm  
-rw-rw-r--  1 ec2-user ec2-user 2872741741 Mar 21 22:31  
p34762026_190000_Linux-x86-64.zip  
-rw-rw-r--  1 ec2-user ec2-user 1843577895 Mar 21 22:32  
p34765931_190000_Linux-x86-64.zip  
-rw-rw-r--  1 ec2-user ec2-user  124347218 Mar 21 22:33  
p6880880_190000_Linux-x86-64.zip  
-rw-r--r--  1 ec2-user ec2-user    257136 Mar 22 16:25  
policycoreutils-python-utils-2.9-9.el8.noarch.rpm
```

3. Installieren Sie Oracle 19c RPM, das die meisten Anforderungen an die Kernel-Konfiguration erfüllt.

```
yum install /tmp/archive/oracle-database-preinstall-19c-1.0-  
2.el8.x86_64.rpm
```

4. Laden Sie die fehlenden Dateien herunter, und installieren Sie sie `compat-libcap1` Unter Linux 8.

```
yum install /tmp/archive/compat-libcap1-1.10-7.el7.x86_64.rpm
```

5. Laden Sie von NetApp die NetApp Host Utilities herunter und installieren Sie sie.

```
yum install /tmp/archive/netapp_linux_unified_host_utilities-7-1.x86_64.rpm
```

6. Installieren `policycoreutils-python-utils`, Die in der EC2-Instanz nicht verfügbar ist.

```
yum install /tmp/archive/policycoreutils-python-utils-2.9-9.el8.noarch.rpm
```

7. Installieren Sie Open JDK Version 1.8.

```
yum install java-1.8.0-openjdk.x86_64
```

8. Installieren Sie `iscsi-Initiator-Utils`.

```
yum install iscsi-initiator-utils
```

9. Installieren `sg3_utils`.

```
yum install sg3_utils
```

10. Installieren `device-mapper-multipath`.

```
yum install device-mapper-multipath
```

11. Deaktivieren Sie transparente hugepages im aktuellen System.

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled  
echo never > /sys/kernel/mm/transparent_hugepage/defrag
```

Fügen Sie die folgenden Zeilen in hinzu `/etc/rc.local` Zu deaktivieren `transparent_hugepage` Nach dem Neustart:

```
# Disable transparent hugepages
    if test -f /sys/kernel/mm/transparent_hugepage/enabled;
then
    echo never > /sys/kernel/mm/transparent_hugepage/enabled
fi
    if test -f /sys/kernel/mm/transparent_hugepage/defrag;
then
    echo never > /sys/kernel/mm/transparent_hugepage/defrag
fi
```

12. Deaktivieren sie selinux, indem Sie ändern SELINUX=enforcing Bis SELINUX=disabled. Sie müssen den Host neu starten, damit die Änderung wirksam wird.

```
vi /etc/sysconfig/selinux
```

13. Fügen Sie die folgenden Zeilen zu hinzu limit.conf So legen Sie die Dateibeschreibungsgrenze und die Stapelgröße ohne Anführungszeichen fest " ".

```
vi /etc/security/limits.conf
**          hard    nofile          65536"
**          soft    stack           10240"
```

14. Fügen Sie der EC2-Instanz Swap-Speicherplatz hinzu, indem Sie diese Anweisung befolgen: ["Wie weisen ich Speicher zu, um durch Verwendung einer Auslagerungsdatei als Auslagerungsspeicher in einer Amazon EC2 Instanz zu arbeiten?"](#) Die genaue Menge des zu addieren Speicherplatzes hängt von der Größe des RAM bis zu 16G ab.
15. Ändern node.session.timeo.replacement_timeout Im iscsi.conf Konfigurationsdatei von 120 bis 5 Sekunden.

```
vi /etc/iscsi/iscsid.conf
```

16. Aktivieren und starten Sie den iSCSI-Service auf der EC2-Instanz.

```
systemctl enable iscsid
systemctl start iscsid
```

17. Rufen Sie die iSCSI-Initiatoradresse ab, die für die Datenbank-LUN-Zuordnung verwendet werden soll.

```
cat /etc/iscsi/initiatorname.iscsi
```

18. Fügen Sie die ASM-Gruppe hinzu, die für die asm-Sysasm-Gruppe verwendet werden soll.

```
groupadd asm
```

19. Ändern Sie den oracle-Benutzer, um ASM als sekundäre Gruppe hinzuzufügen (der oracle-Benutzer sollte nach der RPM-Installation von Oracle vor der Installation erstellt worden sein).

```
usermod -a -G asm oracle
```

20. Stoppen und deaktivieren Sie die Linux-Firewall, wenn sie aktiv ist.

```
systemctl stop firewalld  
systemctl disable firewalld
```

21. EC2-Instanz neu booten

Bereitstellung und Zuordnung von Datenbank-Volumes und LUNs zum EC2-Instanz-Host

Stellen Sie drei Volumes über die Befehlszeile bereit, indem Sie sich beim FSX Cluster über ssh anmelden als fsxadmin-Benutzer mit FSX Cluster Management IP, um die binären, Daten- und Protokolldateien der Oracle-Datenbank zu hosten.

1. Melden Sie sich über SSH als Benutzer von fsxadmin am FSX-Cluster an.

```
ssh fsxadmin@172.30.15.53
```

2. Führen Sie den folgenden Befehl aus, um ein Volume für die Oracle-Binärdatei zu erstellen.

```
vol create -volume ora_01_biny -aggregate aggr1 -size 50G -state  
online -type RW -snapshot-policy none -tiering-policy snapshot-only
```

3. Führen Sie den folgenden Befehl aus, um ein Volume für Oracle-Daten zu erstellen.

```
vol create -volume ora_01_data -aggregate aggr1 -size 100G -state  
online -type RW -snapshot-policy none -tiering-policy snapshot-only
```

4. Führen Sie den folgenden Befehl aus, um ein Volume für Oracle-Protokolle zu erstellen.

```
vol create -volume ora_01_logs -aggregate aggr1 -size 100G -state  
online -type RW -snapshot-policy none -tiering-policy snapshot-only
```

5. Erstellen Sie eine binäre LUN innerhalb des Datenbank-Binärvolumes.

```
lun create -path /vol/ora_01_biny/ora_01_biny_01 -size 40G -ostype  
linux
```

6. Erstellen Sie Daten-LUNs im Datenbank-Daten-Volume.

```
lun create -path /vol/ora_01_data/ora_01_data_01 -size 20G -ostype  
linux  
  
lun create -path /vol/ora_01_data/ora_01_data_02 -size 20G -ostype  
linux  
  
lun create -path /vol/ora_01_data/ora_01_data_03 -size 20G -ostype  
linux  
  
lun create -path /vol/ora_01_data/ora_01_data_04 -size 20G -ostype  
linux
```

7. Erstellen Sie Protokoll-LUNs im Datenbank-Protokoll-Volumen.

```
lun create -path /vol/ora_01_logs/ora_01_logs_01 -size 40G -ostype linux  
lun create -path /vol/ora_01_logs/ora_01_logs_02 -size 40G -ostype linux
```

8. Erstellen Sie eine Initiatorgruppe für die EC2-Instanz, wobei der Initiator aus Schritt 14 der obigen EC2-Kernel-Konfiguration abgerufen wird.

```
igroup create -igroup ora_01 -protocol iscsi -ostype linux  
-initiator iqn.1994-05.com.redhat:f65fed7641c2
```

9. Ordnen Sie die LUNs der oben erstellten Initiatorgruppe zu. Für jede zusätzliche LUN innerhalb eines Volumens wird die LUN-ID sequenziell inkrementiert.

```
lun map -path /vol/ora_01_biny/ora_01_biny_01 -igroup ora_01  
-vserver svm_ora -lun-id 0  
lun map -path /vol/ora_01_data/ora_01_data_01 -igroup ora_01  
-vserver svm_ora -lun-id 1  
lun map -path /vol/ora_01_data/ora_01_data_02 -igroup ora_01  
-vserver svm_ora -lun-id 2  
lun map -path /vol/ora_01_data/ora_01_data_03 -igroup ora_01  
-vserver svm_ora -lun-id 3  
lun map -path /vol/ora_01_data/ora_01_data_04 -igroup ora_01  
-vserver svm_ora -lun-id 4  
lun map -path /vol/ora_01_logs/ora_01_logs_01 -igroup ora_01  
-vserver svm_ora -lun-id 5  
lun map -path /vol/ora_01_logs/ora_01_logs_02 -igroup ora_01  
-vserver svm_ora -lun-id 6
```

10. Überprüfen Sie die LUN-Zuordnung.

```
mapping show
```

Es wird erwartet, dass dies wieder zutrifft:


```
FsxId02ad7bf3476b741df::> mapping show
```

```
(lun mapping show)
```

Vserver Protocol	Path	Igroup	LUN ID
svm_ora iscsi	/vol/ora_01_biny/ora_01_biny_01	ora_01	0
svm_ora iscsi	/vol/ora_01_data/ora_01_data_01	ora_01	1
svm_ora iscsi	/vol/ora_01_data/ora_01_data_02	ora_01	2
svm_ora iscsi	/vol/ora_01_data/ora_01_data_03	ora_01	3
svm_ora iscsi	/vol/ora_01_data/ora_01_data_04	ora_01	4
svm_ora iscsi	/vol/ora_01_logs/ora_01_logs_01	ora_01	5
svm_ora iscsi	/vol/ora_01_logs/ora_01_logs_02	ora_01	6

Konfiguration des Datenbank-Storage

Importieren und richten Sie nun den FSX Storage für die Oracle Grid-Infrastruktur und die Datenbankinstallation auf dem EC2-Instanzhost ein.

1. Melden Sie sich über SSH als ec2-Benutzer mit Ihrem SSH-Schlüssel und der IP-Adresse der EC2-Instanz an.

```
ssh -i ora_01.pem ec2-user@172.30.15.58
```

2. FSX iSCSI-Endpunkte werden mithilfe einer der beiden SVM iSCSI-IP-Adressen ermittelt. Ändern Sie dann Ihre umgebungsspezifische Portaladresse.

```
sudo iscsiadm iscsiadm --mode discovery --op update --type  
sendtargets --portal 172.30.15.51
```

3. Erstellen Sie iSCSI-Sitzungen, indem Sie sich bei jedem Ziel anmelden.

```
sudo iscsiadm --mode node -l all
```

Die erwartete Ausgabe des Befehls ist:

```
[ec2-user@ip-172-30-15-58 ~]$ sudo iscsiadm --mode node -l all  
Logging in to [iface: default, target: iqn.1992-  
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3, portal:  
172.30.15.51,3260]  
Logging in to [iface: default, target: iqn.1992-  
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3, portal:  
172.30.15.13,3260]  
Login to [iface: default, target: iqn.1992-  
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3, portal:  
172.30.15.51,3260] successful.  
Login to [iface: default, target: iqn.1992-  
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3, portal:  
172.30.15.13,3260] successful.
```

4. Zeigen Sie eine Liste aktiver iSCSI-Sitzungen an und validieren Sie sie.

```
sudo iscsiadm --mode session
```

Geben Sie die iSCSI-Sitzungen wieder.

```
[ec2-user@ip-172-30-15-58 ~]$ sudo iscsiadm --mode session
tcp: [1] 172.30.15.51:3260,1028 iqn.1992-
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3 (non-flash)
tcp: [2] 172.30.15.13:3260,1029 iqn.1992-
08.com.netapp:sn.1f795e65c74911edb785affbf0a2b26e:vs.3 (non-flash)
```

5. Vergewissern Sie sich, dass die LUNs in den Host importiert wurden.

```
sudo sanlun lun show
```

Dadurch wird eine Liste der Oracle LUNs aus FSX zurückgegeben.

```

[ec2-user@ip-172-30-15-58 ~]$ sudo sanlun lun show
controller(7mode/E-Series)/                               device
host                lun
vservers(cDOT/FlashRay)    lun-pathname
filename             adapter  protocol  size    product

svm_ora              /vol/ora_01_logs/ora_01_logs_02
/dev/sdn             host3    iSCSI    40g    cDOT
svm_ora              /vol/ora_01_logs/ora_01_logs_01
/dev/sdm             host3    iSCSI    40g    cDOT
svm_ora              /vol/ora_01_data/ora_01_data_03
/dev/sdk             host3    iSCSI    20g    cDOT
svm_ora              /vol/ora_01_data/ora_01_data_04
/dev/sdl             host3    iSCSI    20g    cDOT
svm_ora              /vol/ora_01_data/ora_01_data_01
/dev/sdi             host3    iSCSI    20g    cDOT
svm_ora              /vol/ora_01_data/ora_01_data_02
/dev/sdj             host3    iSCSI    20g    cDOT
svm_ora              /vol/ora_01_biny/ora_01_biny_01
/dev/sdh             host3    iSCSI    40g    cDOT
svm_ora              /vol/ora_01_logs/ora_01_logs_02
/dev/sdg             host2    iSCSI    40g    cDOT
svm_ora              /vol/ora_01_logs/ora_01_logs_01
/dev/sdf             host2    iSCSI    40g    cDOT
svm_ora              /vol/ora_01_data/ora_01_data_04
/dev/sde             host2    iSCSI    20g    cDOT
svm_ora              /vol/ora_01_data/ora_01_data_02
/dev/sdc             host2    iSCSI    20g    cDOT
svm_ora              /vol/ora_01_data/ora_01_data_03
/dev/sdd             host2    iSCSI    20g    cDOT
svm_ora              /vol/ora_01_data/ora_01_data_01
/dev/sdb             host2    iSCSI    20g    cDOT
svm_ora              /vol/ora_01_biny/ora_01_biny_01
/dev/sda             host2    iSCSI    40g    cDOT

```

6. Konfigurieren Sie die `multipath.conf` Datei mit folgenden Standard- und Blacklist-Einträgen.

```
sudo vi /etc/multipath.conf

defaults {
    find_multipaths yes
    user_friendly_names yes
}

blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st) [0-9]*"
    devnode "^hd[a-z]"
    devnode "^cciss.*"
}
```

7. Starten Sie den Multipath Service.

```
sudo systemctl start multipathd
```

Jetzt werden Multipath-Geräte in der angezeigt `/dev/mapper` Verzeichnis.

```
[ec2-user@ip-172-30-15-58 ~]$ ls -l /dev/mapper
total 0
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e68512d -> ../dm-0
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685141 -> ../dm-1
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685142 -> ../dm-2
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685143 -> ../dm-3
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685144 -> ../dm-4
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685145 -> ../dm-5
lrwxrwxrwx 1 root root          7 Mar 21 20:13
3600a09806c574235472455534e685146 -> ../dm-6
crw----- 1 root root 10, 236 Mar 21 18:19 control
```

8. Melden Sie sich beim FSX Cluster als Benutzer von `fsxadmin` über SSH an, um die Seriennummer für jede LUN abzurufen, die mit `6c574xxx` beginnt..., die HEX-Nummer beginnt mit `3600a0980`, was AWS-Hersteller-ID ist.

```
lun show -fields serial-hex
```

Und wie folgt zurückkehren:

```
FsxId02ad7bf3476b741df::> lun show -fields serial-hex
vserver path                               serial-hex
-----
svm_ora /vol/ora_01_biny/ora_01_biny_01 6c574235472455534e68512d
svm_ora /vol/ora_01_data/ora_01_data_01 6c574235472455534e685141
svm_ora /vol/ora_01_data/ora_01_data_02 6c574235472455534e685142
svm_ora /vol/ora_01_data/ora_01_data_03 6c574235472455534e685143
svm_ora /vol/ora_01_data/ora_01_data_04 6c574235472455534e685144
svm_ora /vol/ora_01_logs/ora_01_logs_01 6c574235472455534e685145
svm_ora /vol/ora_01_logs/ora_01_logs_02 6c574235472455534e685146
7 entries were displayed.
```

9. Aktualisieren Sie die `/dev/multipath.conf` Datei, um einen benutzerfreundlichen Namen für das Multipath-Gerät hinzuzufügen.

```
sudo vi /etc/multipath.conf
```

Mit folgenden Einträgen:

```

multipaths {
    multipath {
        wwid          3600a09806c574235472455534e68512d
        alias         ora_01_biny_01
    }
    multipath {
        wwid          3600a09806c574235472455534e685141
        alias         ora_01_data_01
    }
    multipath {
        wwid          3600a09806c574235472455534e685142
        alias         ora_01_data_02
    }
    multipath {
        wwid          3600a09806c574235472455534e685143
        alias         ora_01_data_03
    }
    multipath {
        wwid          3600a09806c574235472455534e685144
        alias         ora_01_data_04
    }
    multipath {
        wwid          3600a09806c574235472455534e685145
        alias         ora_01_logs_01
    }
    multipath {
        wwid          3600a09806c574235472455534e685146
        alias         ora_01_logs_02
    }
}

```

10. Starten Sie den Multipath-Dienst neu, um zu überprüfen, ob die Geräte unter `/dev/mapper` Haben sich zu LUN-Namen und zu Serial-Hex-IDs geändert.

```
sudo systemctl restart multipathd
```

Prüfen `/dev/mapper` So kehren Sie wie folgt zurück:

```
[ec2-user@ip-172-30-15-58 ~]$ ls -l /dev/mapper
total 0
crw----- 1 root root 10, 236 Mar 21 18:19 control
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_01_biny_01 -> ../dm-
0
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_01_data_01 -> ../dm-
1
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_01_data_02 -> ../dm-
2
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_01_data_03 -> ../dm-
3
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_01_data_04 -> ../dm-
4
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_01_logs_01 -> ../dm-
5
lrwxrwxrwx 1 root root      7 Mar 21 20:41 ora_01_logs_02 -> ../dm-
6
```

11. Partitionieren Sie die binäre LUN mit einer einzigen primären Partition.

```
sudo fdisk /dev/mapper/ora_01_biny_01
```

12. Formatieren Sie die partitionierte binäre LUN mit einem XFS-Dateisystem.

```
sudo mkfs.xfs /dev/mapper/ora_01_biny_01p1
```

13. Mounten Sie die binäre LUN in /u01.

```
sudo mount -t xfs /dev/mapper/ora_01_biny_01p1 /u01
```

14. Ändern /u01 Mount Point Ownership für den Oracle-Benutzer und die ihm zugesagte primäre Gruppe.

```
sudo chown oracle:oinstall /u01
```

15. Suchen Sie die UUID der binären LUN.

```
sudo blkid /dev/mapper/ora_01_biny_01p1
```

16. Hinzufügen eines Mount-Punkts zu /etc/fstab.


```
sudo vi /etc/fstab
```

Fügen Sie die folgende Zeile hinzu.

```
UUID=d89fb1c9-4f89-4de4-b4d9-17754036d11d      /u01      xfs
defaults,nofail 0                2
```



Es ist wichtig, die Binärdatei nur mit der UUID und mit der Nofail-Option zu mounten, um mögliche Probleme mit der Root-Sperre während des Neustarts von EC2-Instanzen zu vermeiden.

17. Fügen Sie als Root-Benutzer die udev-Regel für Oracle-Geräte hinzu.

```
vi /etc/udev/rules.d/99-oracle-asmdevices.rules
```

Folgende Einträge einbeziehen:

```
ENV{DM_NAME}=="ora*", GROUP:="oinstall", OWNER:="oracle",
MODE:="660"
```

18. Laden Sie als root-Benutzer die udev-Regeln neu.

```
udevadm control --reload-rules
```

19. Lösen Sie als Root-Benutzer die udev-Regeln aus.

```
udevadm trigger
```

20. Laden Sie als root-Benutzer multipathd neu.

```
systemctl restart multipathd
```

21. Booten Sie den EC2-Instanzhost neu.

Installation der Oracle Grid-Infrastruktur

1. Melden Sie sich als ec2-Benutzer über SSH bei der EC2-Instanz an und aktivieren Sie die Passwortauthentifizierung durch Entkommentieren `PasswordAuthentication yes` Und dann kommentiert `PasswordAuthentication no`.

```
sudo vi /etc/ssh/sshd_config
```

2. Starten Sie den sshd-Dienst neu.

```
sudo systemctl restart sshd
```

3. Setzen Sie das Oracle-Benutzerpasswort zurück.

```
sudo passwd oracle
```

4. Melden Sie sich als Oracle Restart Software Owner User (oracle) an. Erstellen Sie ein Oracle-Verzeichnis wie folgt:

```
mkdir -p /u01/app/oracle  
mkdir -p /u01/app/oraInventory
```

5. Ändern Sie die Verzeichnisberechtigungseinstellung.

```
chmod -R 775 /u01/app
```

6. Erstellen Sie ein Grid-Home-Verzeichnis, und ändern Sie es.

```
mkdir -p /u01/app/oracle/product/19.0.0/grid  
cd /u01/app/oracle/product/19.0.0/grid
```

7. Entpacken Sie die Grid-Installationsdateien.

```
unzip -q /tmp/archive/LINUX.X64_193000_grid_home.zip
```

8. Löschen Sie von der Startseite des Rasters aus die OPatch Verzeichnis.

```
rm -rf OPatch
```

9. Entpacken Sie die Datei von Grid Home aus `p6880880_190000_Linux-x86-64.zip`.

```
unzip -q /tmp/archive/p6880880_190000_Linux-x86-64.zip
```

10. Von der Startseite des Rasters aus, überarbeiten `cv/admin/cvu_config`, Entkommentieren und ersetzen `CV_ASSUME_DISTID=OEL5` Mit `CV_ASSUME_DISTID=OL7`.

```
vi cv/admin/cvu_config
```

11. Bereiten Sie ein vor `gridsetup.rsp` Datei für die automatische Installation und legen Sie die `rsp`-Datei im ab `/tmp/archive` Verzeichnis. Die `rsp`-Datei sollte die Abschnitte A, B und G mit den folgenden Informationen abdecken:

```
INVENTORY_LOCATION=/u01/app/oraInventory
oracle.install.option=HA_CONFIG
ORACLE_BASE=/u01/app/oracle
oracle.install.asm.OSDBA=dba
oracle.install.asm.OSOPER=oper
oracle.install.asm.OSASM=asm
oracle.install.asm.SYSASMPassword="SetPWD"
oracle.install.asm.diskGroup.name=DATA
oracle.install.asm.diskGroup.redundancy=EXTERNAL
oracle.install.asm.diskGroup.AUSize=4
oracle.install.asm.diskGroup.disks=/dev/mapper/ora_01_data_01,/dev/mapper/ora_01_data_02,/dev/mapper/ora_01_data_03,/dev/mapper/ora_01_data_04
oracle.install.asm.diskGroup.diskDiscoveryString=/dev/mapper/*
oracle.install.asm.monitorPassword="SetPWD"
oracle.install.asm.configureAFD=true
```

12. Melden Sie sich bei der EC2-Instanz als Root-Benutzer an und legen Sie fest `ORACLE_HOME` Und `ORACLE_BASE`.

```
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/grid
export ORACLE_BASE=/tmp
cd /u01/app/oracle/product/19.0.0/grid/bin
```

13. Stellen Sie Festplattengeräte für die Verwendung mit dem Oracle ASM-Filtertreiber bereit.

```
./asmcmd afd_label DATA01 /dev/mapper/ora_01_data_01 --init  
./asmcmd afd_label DATA02 /dev/mapper/ora_01_data_02 --init  
./asmcmd afd_label DATA03 /dev/mapper/ora_01_data_03 --init  
./asmcmd afd_label DATA04 /dev/mapper/ora_01_data_04 --init  
./asmcmd afd_label LOGS01 /dev/mapper/ora_01_logs_01 --init  
./asmcmd afd_label LOGS02 /dev/mapper/ora_01_logs_02 --init
```

14. Installieren cvuqdisk-1.0.10-1.rpm.

```
rpm -ivh /u01/app/oracle/product/19.0.0/grid/cv/rpm/cvuqdisk-1.0.10-1.rpm
```

15. Nicht Festgelegt \$ORACLE_BASE.

```
unset ORACLE_BASE
```

16. Melden Sie sich als Oracle-Benutzer bei der EC2-Instanz an und extrahieren Sie den Patch in /tmp/archive Ordner.

```
unzip /tmp/archive/p34762026_190000_Linux-x86-64.zip -d /tmp/archive
```

17. Starten Sie von Grid Home /u01/App/oracle/Product/19.0.0/GRID aus und als oracle-Benutzer gridSetup.sh Für die Installation der Netzinfrastruktur.

```
./gridSetup.sh -applyRU /tmp/archive/34762026/ -silent  
-responseFile /tmp/archive/gridsetup.rsp
```

Ignorieren Sie die Warnungen über falsche Gruppen für die Netzinfrastruktur. Wir verwenden einen einzigen Oracle-Benutzer, um Oracle Restart zu verwalten. Das wird also erwartet.

18. Führen Sie als root-Benutzer folgende(n) Skript(e) aus:

```
/u01/app/oraInventory/orainstRoot.sh  
  
/u01/app/oracle/product/19.0.0/grid/root.sh
```

19. Laden Sie als root-Benutzer den multipathd neu.

```
systemctl restart multipathd
```

20. Führen Sie als Oracle-Benutzer den folgenden Befehl aus, um die Konfiguration abzuschließen:

```
/u01/app/oracle/product/19.0.0/grid/gridSetup.sh -executeConfigTools  
-responseFile /tmp/archive/gridsetup.rsp -silent
```

21. Erstellen Sie als Oracle-Benutzer die PROTOKOLLDATENTRÄGER-Gruppe.

```
bin/asmca -silent -sysAsmPassword 'yourPWD' -asmsnmpPassword  
'yourPWD' -createDiskGroup -diskGroupName LOGS -disk 'AFD:LOGS*'  
-redundancy EXTERNAL -au_size 4
```

22. Validieren Sie als Oracle-Benutzer nach der Installation die Grid-Services.

```
bin/crsctl stat res -t  
+  
Name                Target  State          Server  
State details  
Local Resources  
ora.DATA.dg         ONLINE  ONLINE        ip-172-30-15-58  
STABLE  
ora.LISTENER.lsnr   ONLINE  ONLINE        ip-172-30-15-58  
STABLE  
ora.LOGS.dg         ONLINE  ONLINE        ip-172-30-15-58  
STABLE  
ora.asm             ONLINE  ONLINE        ip-172-30-15-58  
Started,STABLE  
ora.ons             OFFLINE OFFLINE        ip-172-30-15-58  
STABLE  
Cluster Resources  
ora.cssd            ONLINE  ONLINE        ip-172-30-15-58  
STABLE  
ora.diskmon         OFFLINE OFFLINE  
STABLE  
ora.driver.afd      ONLINE  ONLINE        ip-172-30-15-58  
STABLE  
ora.evmd            ONLINE  ONLINE        ip-172-30-15-58  
STABLE
```

23. Überprüfen Sie den Status des ASM-Filtertreibers.

```
[oracle@ip-172-30-15-58 grid]$ export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/grid
[oracle@ip-172-30-15-58 grid]$ export ORACLE_SID=+ASM
[oracle@ip-172-30-15-58 grid]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ip-172-30-15-58 grid]$ asmcmd
ASMCMDS> lsdg
State      Type      Rebal  Sector  Logical_Sector  Block      AU
Total_MB  Free_MB  Req_mir_free_MB  Usable_file_MB  Offline_disks
Voting_files  Name
MOUNTED   EXTERN  N       512     512     4096    1048576
81920    81847      0       0       81847      0
N  DATA/
MOUNTED   EXTERN  N       512     512     4096    1048576
81920    81853      0       0       81853      0
N  LOGS/
ASMCMDS> afd_state
ASMCMDS-9526: The AFD state is 'LOADED' and filtering is 'ENABLED' on
host 'ip-172-30-15-58.ec2.internal'
```

Installation der Oracle Database

1. Melden Sie sich als Oracle-Benutzer an, und heben Sie die Einstellung auf \$ORACLE_HOME Und \$ORACLE_SID Wenn es eingestellt ist.

```
unset ORACLE_HOME
unset ORACLE_SID
```

2. Erstellen Sie das Oracle DB Home-Verzeichnis, und ändern Sie es.

```
mkdir /u01/app/oracle/product/19.0.0/db1
cd /u01/app/oracle/product/19.0.0/db1
```

3. Entpacken Sie die Oracle DB-Installationsdateien.

```
unzip -q /tmp/archive/LINUX.X64_193000_db_home.zip
```

4. Löschen Sie von der DB-Startseite aus die OPatch Verzeichnis.

```
rm -rf OPatch
```

5. Entzippen Sie die Datei von DB Home aus p6880880_190000_Linux-x86-64.zip.

```
unzip -q /tmp/archive/p6880880_190000_Linux-x86-64.zip
```

6. Überarbeiten Sie von der DB-Startseite aus cv/admin/cvu_config`Und entkommentieren und ersetzen `CV_ASSUME_DISTID=OEL5 Mit CV_ASSUME_DISTID=OL7.

```
vi cv/admin/cvu_config
```

7. Von /tmp/archive Das DB 19.18 RU-Patch entpacken.

```
unzip p34765931_190000_Linux-x86-64.zip
```

8. Bereiten Sie die automatische DB-Installationsdatei in vor /tmp/archive/dbinstall.rsp Verzeichnis mit folgenden Werten:

```
oracle.install.option=INSTALL_DB_SWONLY
UNIX_GROUP_NAME=oinstall
INVENTORY_LOCATION=/u01/app/oraInventory
ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
ORACLE_BASE=/u01/app/oracle
oracle.install.db.InstallEdition=EE
oracle.install.db.OSDBA_GROUP=dba
oracle.install.db.OSOPER_GROUP=oper
oracle.install.db.OSBACKUPDBA_GROUP=oper
oracle.install.db.OSDGDBA_GROUP=dba
oracle.install.db.OSKMDBA_GROUP=dba
oracle.install.db.OSRACDBA_GROUP=dba
oracle.install.db.rootconfig.executeRootScript=false
```

9. Führen Sie von db1 Home /u01/App/oracle/Product/19.0.0/db1 aus die automatische, rein softwarebasierte DB-Installation aus.

```
./runInstaller -applyRU /tmp/archive/34765931/ -silent
-ignorePrereqFailure -responseFile /tmp/archive/dbinstall.rsp
```

10. Führen Sie als Root-Benutzer den aus `root.sh` Skript nach der Installation nur für Software.

```
/u01/app/oracle/product/19.0.0/db1/root.sh
```

11. Erstellen Sie als Oracle-Benutzer den `dbca.rsp` Datei mit folgenden Einträgen:


```
gdbName=db1.demo.netapp.com
sid=db1
createAsContainerDatabase=true
numberOfPDBs=3
pdbName=db1_pdb
useLocalUndoForPDBs=true
pdbAdminPassword="yourPWD"
templateName=General_Purpose.dbc
sysPassword="yourPWD"
systemPassword="yourPWD"
dbsnmpPassword="yourPWD"
datafileDestination=+DATA
recoveryAreaDestination=+LOGS
storageType=ASM
diskGroupName=DATA
characterSet=AL32UTF8
nationalCharacterSet=AL16UTF16
listeners=LISTENER
databaseType=MULTIPURPOSE
automaticMemoryManagement=false
totalMemory=8192
```

12. Als Oracle-Benutzer, lauch DB-Erstellung mit dbca.

```
bin/dbca -silent -createDatabase -responseFile /tmp/archive/dbca.rsp
```

output:

Prepare for db operation

7% complete

Registering database with Oracle Restart

11% complete

Copying database files

33% complete

Creating and starting Oracle instance

35% complete

38% complete

42% complete

45% complete

48% complete

Completing Database Creation

53% complete

55% complete

56% complete

Creating Pluggable Databases

60% complete

64% complete

69% complete

78% complete

Executing Post Configuration Actions

100% complete

Database creation complete. For details check the logfiles at:

/u01/app/oracle/cfgtoollogs/dbca/db1.

Database Information:

Global Database Name:db1.demo.netapp.com

System Identifier(SID):db1

Look at the log file "/u01/app/oracle/cfgtoollogs/dbca/db1/db1.log"
for further details.

13. Validieren Sie als Oracle-Benutzer Oracle Neustart der HA-Services nach der DB-Erstellung.

```
[oracle@ip-172-30-15-58 db1]$ ../grid/bin/crsctl stat res -t
```

Name	Target	State	Server	State
Local Resources				
ora.DATA.dg	ONLINE	ONLINE	ip-172-30-15-58	STABLE
ora.LISTENER.lsnr	ONLINE	ONLINE	ip-172-30-15-58	STABLE
ora.LOGS.dg	ONLINE	ONLINE	ip-172-30-15-58	STABLE
ora.asm	ONLINE	ONLINE	ip-172-30-15-58	Started,STABLE
ora.ons	OFFLINE	OFFLINE	ip-172-30-15-58	STABLE
Cluster Resources				
ora.cssd	ONLINE	ONLINE	ip-172-30-15-58	STABLE
ora.dbf.db	ONLINE	ONLINE	ip-172-30-15-58	Open,HOME=/u01/app/oracle/product/19.0.0/db1,STABLE
ora.diskmon	OFFLINE	OFFLINE		STABLE
ora.driver.afd	ONLINE	ONLINE	ip-172-30-15-58	STABLE
ora.evmd	ONLINE	ONLINE	ip-172-30-15-58	STABLE

14. Legen Sie den Oracle-Benutzer fest `.bash_profile`.

```
vi ~/.bash_profile
```

15. Folgende Einträge hinzufügen:

```
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
export ORACLE_SID=db1
export PATH=$PATH:$ORACLE_HOME/bin
alias asm='export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/grid;export
ORACLE_SID=+ASM;export PATH=$PATH:$ORACLE_HOME/bin'
```

16. Überprüfen Sie die erstellte CDB/PDB.

```
/home/oracle/.bash_profile

sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```

```
NAME          OPEN_MODE
```

```
DB1           READ WRITE
```

```
SQL> select name from v$datafile;
```

```
NAME
```

```
+DATA/DB1/DATAFILE/system.256.1132176177
```

```
+DATA/DB1/DATAFILE/sysaux.257.1132176221
```

```
+DATA/DB1/DATAFILE/undotbs1.258.1132176247
```

```
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/system.265.1132177009
```

```
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/sysaux.266.1132177009
```

```
+DATA/DB1/DATAFILE/users.259.1132176247
```

```
+DATA/DB1/86B637B62FE07A65E053F706E80A27CA/DATAFILE/undotbs1.267.1132177009
```

```
+DATA/DB1/F7852758DCD6B800E0533A0F1EAC1DC6/DATAFILE/system.271.1132177853
```

```
+DATA/DB1/F7852758DCD6B800E0533A0F1EAC1DC6/DATAFILE/sysaux.272.1132177853
```

```
+DATA/DB1/F7852758DCD6B800E0533A0F1EAC1DC6/DATAFILE/undotbs1.270.1132177853
```

```
+DATA/DB1/F7852758DCD6B800E0533A0F1EAC1DC6/DATAFILE/users.274.1132177871
```

```
NAME
```

```
+DATA/DB1/F785288BBCD1BA78E0533A0F1EACCD6F/DATAFILE/system.276.1132177871
```

```
+DATA/DB1/F785288BBCD1BA78E0533A0F1EACCD6F/DATAFILE/sysaux.277.1132177871
```

```
+DATA/DB1/F785288BBCD1BA78E0533A0F1EACCD6F/DATAFILE/undotbs1.275.1132177871
```

```
+DATA/DB1/F785288BBCD1BA78E0533A0F1EACCD6F/DATAFILE/users.279.1132177889
```

```
+DATA/DB1/F78529A14DD8BB18E0533A0F1EACB8ED/DATAFILE/system.281.1132177889
```

```
+DATA/DB1/F78529A14DD8BB18E0533A0F1EACB8ED/DATAFILE/sysaux.282.1132177889
```

```
+DATA/DB1/F78529A14DD8BB18E0533A0F1EACB8ED/DATAFILE/undotbs1.280.1132177889
```

```
+DATA/DB1/F78529A14DD8BB18E0533A0F1EACB8ED/DATAFILE/users.284.113217  
7907
```

```
19 rows selected.
```

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	DB1_PDB1	READ WRITE	NO
4	DB1_PDB2	READ WRITE	NO
5	DB1_PDB3	READ WRITE	NO

```
SQL>
```

17. Stellen Sie die Größe des DB-Wiederherstellungsziels auf die Größe der +LOGS-Datenträgergruppe ein.

```
alter system set db_recovery_file_dest_size = 80G scope=both;
```

18. Melden Sie sich mit sqlplus bei der Datenbank an und aktivieren Sie den Archivprotokollmodus.

```
sqlplus /as sysdba.  
  
shutdown immediate;  
  
startup mount;  
  
alter database archivelog;  
  
alter database open;
```

Damit ist die Neustartbereitstellung von Oracle 19c Version 19.18 auf einer Amazon FSX for ONTAP- und EC2-Compute-Instanz abgeschlossen. Falls gewünscht, empfiehlt NetApp, die Oracle Steuerdatei und die Online-Protokolldateien in die +LOGS-Datenträgergruppe zu verschieben.

Automatische Bereitstellungsoption

Siehe ["TR-4986: Vereinfachte, automatisierte Oracle-Implementierung auf Amazon FSX ONTAP mit iSCSI"](#)
Entsprechende Details.

Backup, Wiederherstellung und Klonen von Oracle Datenbanken mit SnapCenter Services

Siehe ["SnapCenter-Services für Oracle"](#) Weitere Informationen zu Backup, Wiederherstellung und Klonen von Oracle Datenbanken erhalten Sie über die NetApp BlueXP Konsole.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- Installieren der Oracle Grid-Infrastruktur für einen eigenständigen Server mit einer neuen Datenbankinstallation

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3)

- Installieren und Konfigurieren von Oracle Database mithilfe von Antwortdateien

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7)

- Amazon FSX für NetApp ONTAP

["https://aws.amazon.com/fsx/netapp-ontap/"](https://aws.amazon.com/fsx/netapp-ontap/)

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

Oracle Database Deployment auf AWS EC2 und FSX Best Practices

WP-7357: Einführung zu Oracle Database Deployment auf EC2 und FSX Best Practices

Allen Cao, Niyaz Mohamed, Jeffrey Steiner, NetApp

Viele geschäftskritische Oracle Datenbanken der Enterprise-Klasse werden nach wie vor lokal gehostet, und viele Unternehmen möchten diese Oracle Datenbanken in eine Public Cloud migrieren. Häufig sind diese Oracle-Datenbanken Applikationsorientierung vorhanden und benötigen daher benutzerspezifische Konfigurationen. Diese Funktionen fehlen bei vielen Public-Cloud-Angeboten für Datenbanken als Service. Aus diesem Grund erfordert die aktuelle Datenbanklandschaft eine Public-Cloud-basierte Oracle Datenbanklösung, die auf einem hochperformanten, skalierbaren Computing- und Storage-Service aufbaut und individuelle Anforderungen erfüllt. AWS EC2 Computing-Instanzen und der AWS FSX Storage-Service sind möglicherweise die fehlenden Bestandteile dieses Puzzles, das Sie zum Erstellen und Migrieren Ihrer geschäftskritischen Oracle Datenbank-Workloads in eine Public Cloud nutzen können.

Amazon Elastic Compute Cloud (Amazon EC2) ist ein Web-Service, der eine sichere, anpassbare Computing-Kapazität in der Cloud bietet. Es wurde entwickelt, um Unternehmen das webbasierte Cloud-Computing zu erleichtern. Über die einfache Amazon EC2 Web-Service-Schnittstelle erhalten und konfigurieren Sie Kapazitäten mit minimalem Reibungsaufwand. Es bietet Ihnen die vollständige Kontrolle über Ihre Computing-Ressourcen und ermöglicht Ihnen, auf Amazon bewährten Computing-Umgebung laufen.

Amazon FSX für ONTAP ist ein AWS Storage-Service, der branchenführende NetApp ONTAP Block- und File-Storage verwendet, der NFS, SMB und iSCSI aufdeckt. Dank einer derart leistungsstarken Storage Engine war es noch nie einfacher, geschäftskritische Oracle Datenbankapplikationen mit Reaktionszeiten von unter einer Millisekunde, einem Durchsatz von mehreren GBit/s und mehr als 100,000 IOPS pro Datenbankinstanz in AWS zu verschieben. Der FSX Storage-Service verfügt außerdem über native Replizierungsfunktionen, mit denen Sie Ihre Oracle Datenbanken problemlos zu AWS migrieren oder Ihre geschäftskritische Oracle Datenbank zu einer sekundären AWS Verfügbarkeitszone für HA oder DR zu replizieren.

Ziel dieser Dokumentation ist es, Schritt-für-Schritt-Prozesse, Verfahren und Best Practice-Anleitungen zur Implementierung und Konfiguration einer Oracle Datenbank mit FSX Storage und einer EC2 Instanz zu liefern, die eine Performance ähnlich wie ein lokales System bietet. NetApp stellt zudem ein Automatisierungs-Toolkit bereit, das die meisten Aufgaben für die Implementierung, Konfiguration und das Management Ihres Oracle Datenbank-Workloads in der AWS Public Cloud automatisiert.

In folgendem Video erfahren Sie mehr über die Lösung und den Anwendungsfall:

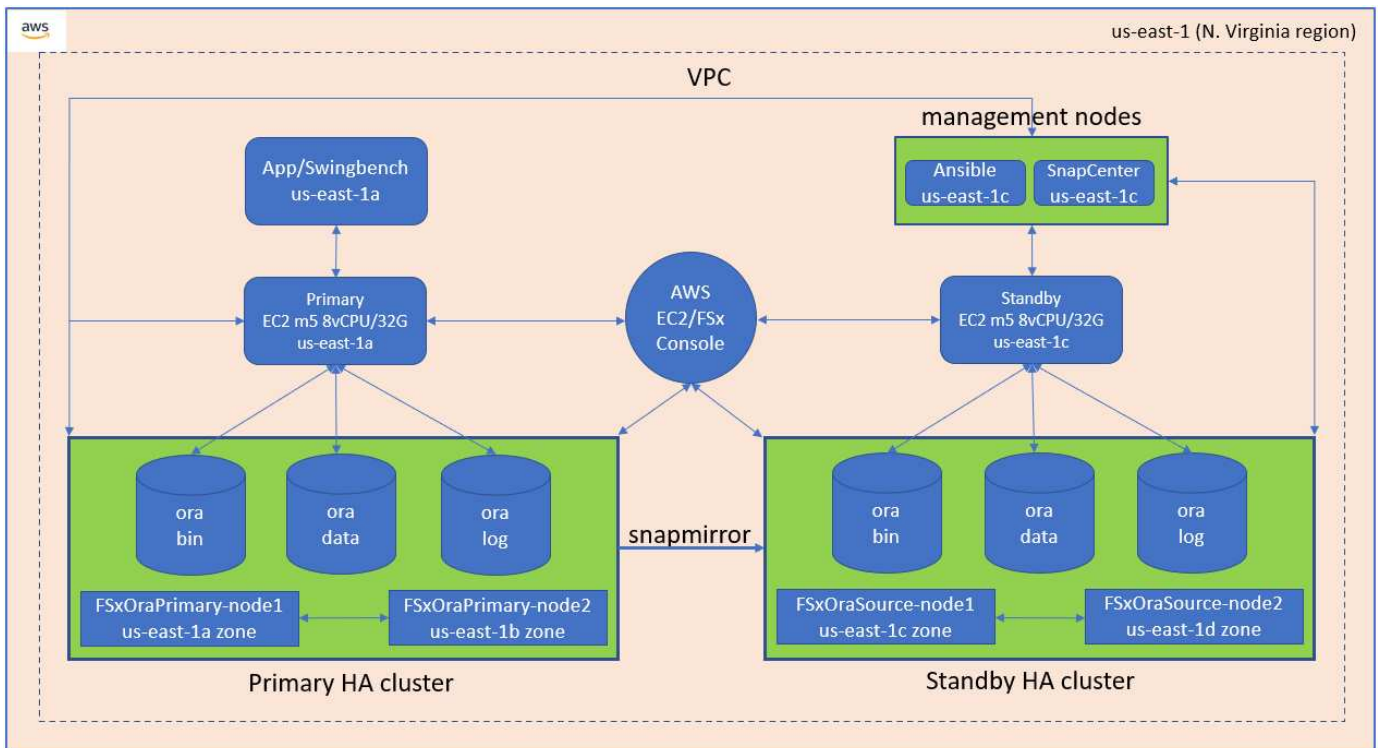
["Modernisieren Sie Ihre Oracle-Datenbank mit Hybrid Cloud in AWS und FSX ONTAP, Part1 – Anwendungsfall und Lösungsarchitektur"](#)

Lösungsarchitektur

Das folgende Architekturdiagramm zeigt eine hochverfügbare Implementierung von Oracle Datenbanken auf einer AWS EC2 Instanz mit dem FSX Storage-Service. Ein ähnliches Bereitstellungsschema, jedoch mit Standby in einer anderen Region kann für das Disaster Recovery eingerichtet werden.

In der Umgebung wird die Oracle Computing-Instanz über eine AWS EC2 Instance Console implementiert. Über die Konsole stehen mehrere EC2-Instanztypen zur Verfügung. NetApp empfiehlt die Implementierung eines datenbankorientierten EC2 Instanztyps wie ein m5 Ami Image mit RedHat Enterprise Linux 8 und bis zu 10 Gps Netzwerkbandbreite.

Oracle Datenbank-Storage auf FSX Volumes hingegen wird mit der AWS FSX Konsole oder der CLI bereitgestellt. Die Oracle-Binärdateien, Daten oder Log-Volumes werden anschließend präsentiert und auf einem Linux-Host der EC2 Instanz gemountet. Jeder Daten- oder Protokoll-Volume kann abhängig vom verwendeten Storage-Protokoll mehrere LUNs zugewiesen sein.



Ein FSX Storage-Cluster verfügt über doppelte Redundanz, sodass sowohl der primäre als auch der Standby-Storage-Cluster in zwei verschiedenen Verfügbarkeitszonen implementiert werden können. Datenbank-Volumes werden von einem primären FSX-Cluster auf ein Standby-FSX-Cluster in einem vom Benutzer konfigurierbaren Intervall für alle Oracle Binär-, Daten- und Protokoll-Volumes repliziert.

Diese hochverfügbare Oracle-Umgebung wird über einen Ansible-Controller-Node sowie einen SnapCenter-Backup-Server und ein UI-Tool verwaltet. Oracle-Installation, -Konfiguration und -Replizierung werden mithilfe von Playbook-basierten Ansible-Tool-Kits automatisiert. Jedes Update auf dem Kernel-Betriebssystem der Oracle EC2 Instanz oder Oracle Patching kann parallel ausgeführt werden, um den Primär- und Standby-Modus synchron zu halten. So kann die Erstautomatisierung auch problemlos erweitert werden, um bei Bedarf einige sich wiederholende tägliche Oracle Aufgaben durchzuführen.

SnapCenter stellt Workflows für zeitpunktgenaue Oracle Database Recovery oder für das Datenbankklonen in den primären oder Standby-Zonen bereit, falls erforderlich. Über die Benutzeroberfläche von SnapCenter können Sie das Backup und die Replizierung von Oracle Datenbanken auf Standby FSX Storage konfigurieren, um für Hochverfügbarkeit oder Disaster Recovery entsprechend Ihrer RTO- oder RPO-Vorgaben zu sorgen.

Die Lösung stellt einen alternativen Prozess bereit, der Funktionen bietet, die denen von Oracle RAC und Data Guard Deployment ähnlich sind.

Für die Implementierung von Oracle Database sind Faktoren zu berücksichtigen

Eine Public Cloud bietet eine große Auswahl an Computing- und Storage-Ressourcen. Der Einsatz der richtigen Computing-Instanz und der richtigen Storage Engine ist ein guter Ausgangspunkt für die Datenbankimplementierung. Wählen Sie außerdem Computing- und Storage-Konfigurationen aus, die für Oracle Datenbanken optimiert sind.

In den folgenden Abschnitten werden die wichtigsten Aspekte bei der Implementierung von Oracle Datenbanken in einer AWS Public Cloud auf einer EC2 Instanz mit FSX Storage beschrieben.

VM-Performance

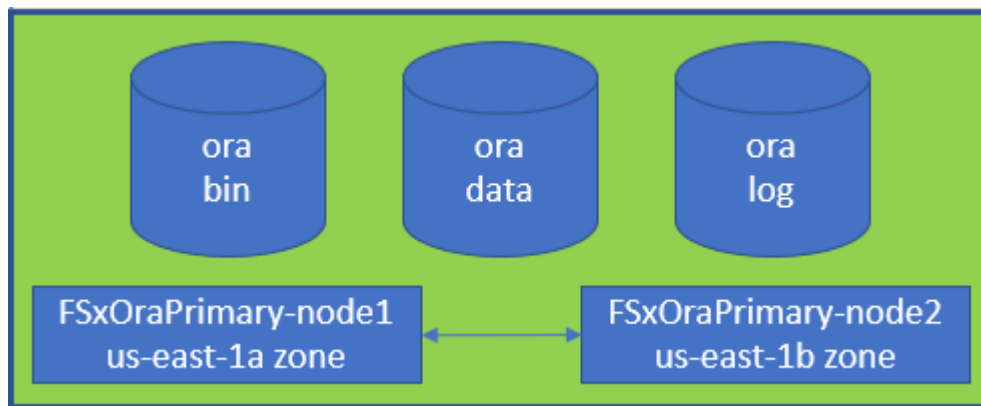
Für die optimale Performance einer relationalen Datenbank in einer Public Cloud ist die Auswahl der richtigen VM-Größe wichtig. Um eine bessere Performance zu erzielen, empfiehlt NetApp die Verwendung einer EC2 M5 Series Instanz für die Oracle Implementierung, die für Datenbank-Workloads optimiert ist. Derselbe Instanztyp wird auch verwendet, um eine RDS-Instanz für Oracle von AWS zu versorgen.

- Wählen Sie basierend auf Workload-Merkmalen die richtige vCPU- und RAM-Kombination aus.
- Fügen Sie Swap-Speicherplatz zu einer VM hinzu. Die Standard-Implementierung der EC2-Instanz erstellt keinen Swap-Speicherplatz, der nicht optimal für eine Datenbank ist.

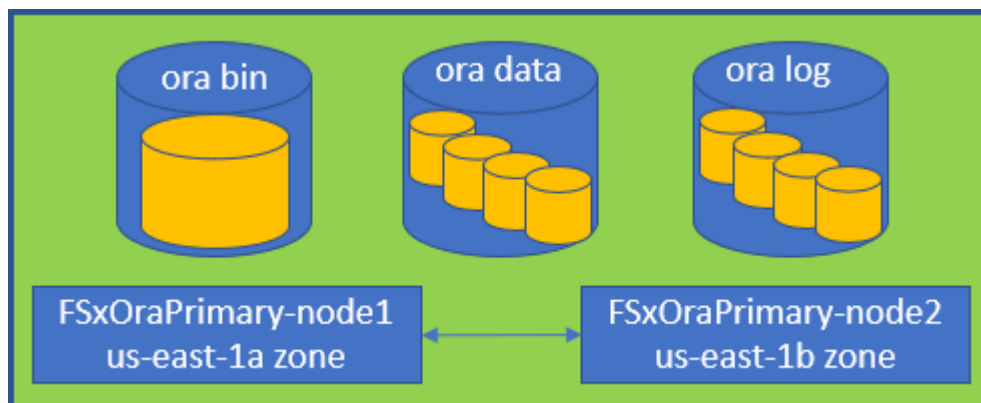
Storage-Layout und -Einstellungen

NetApp empfiehlt das folgende Storage Layout:

- Für NFS-Storage besteht das empfohlene Volume-Layout aus drei Volumes: Eines für die Oracle-Binärdatei, eines für Oracle-Daten und einer doppelten Kontrolldatei und eines für das aktive Protokoll, archiviertes Protokoll und die Kontrolldatei von Oracle.



- Für iSCSI-Storage empfiehlt sich das Volume-Layout aus drei Volumes: Eines für die Oracle-Binärdatei, eines für Oracle-Daten und einer doppelten Kontrolldatei und eines für das aktive Protokoll, Archivprotokoll und die Kontrolldatei von Oracle. Allerdings sollte jede Daten- und Protokoll-Volume idealerweise vier LUNs enthalten. Die LUNs sind idealerweise auf den HA Cluster Nodes ausgeglichen.



- Für Storage-IOPS und -Durchsatz können Sie den Schwellenwert für bereitgestellte IOPS und Durchsatz für den FSX Storage-Cluster festlegen. Die Parameter können spontan angepasst werden, wann sich der Workload ändert.
 - Die automatische IOPS-Einstellung beträgt drei IOPS pro gib der zugewiesenen Storage-Kapazität

oder den benutzerdefinierten Storage bis zu 80,000.

- Der Durchsatz wird wie folgt erhöht: 128, 256, 512, 1024, 2045 Mbps.

Überprüfen Sie die "[Amazon FSX für die Performance von NetApp ONTAP](#)" Dokumentation bei der Größenbestimmung von Durchsatz und IOPS.

NFS-Konfiguration

Linux, das gängigste Betriebssystem, umfasst native NFS-Funktionen. Oracle bietet den direkten NFS-Client (dNFS), der nativ in Oracle integriert ist. Oracle unterstützt NFSv3 seit über 20 Jahren. DNFS wird mit NFSv3 mit allen Versionen von Oracle unterstützt. NFSv4 wird von allen Betriebssystemen unterstützt, die dem NFSv4-Standard entsprechen. DNFS-Unterstützung für NFSv4 erfordert Oracle 12.1.0.2 oder höher. Für NFSv4.1 ist besondere Unterstützung des Betriebssystems erforderlich. Das NetApp Interoperabilitäts-Matrix-Tool (IMT) enthält weitere Informationen zu unterstützten Betriebssystemen. DNFS-Unterstützung für NFSv4.1 erfordert Oracle Version 19.3.0.0 oder höher.

Die automatisierte Oracle-Implementierung mit dem NetApp Automatisierungs-Toolkit konfiguriert dNFS auf NFSv3 automatisch.

Weitere Faktoren, die berücksichtigt werden sollten:

- TCP-Slot-Tabellen entsprechen dem NFS-Äquivalent zur Warteschlangentiefe des Host-Bus-Adapters (HBA). Diese Tabellen steuern die Anzahl der NFS-Vorgänge, die zu einem beliebigen Zeitpunkt ausstehen können. Der Standardwert ist normalerweise 16, was für eine optimale Performance viel zu niedrig ist. Das entgegengesetzte Problem tritt auf neueren Linux-Kerneln auf, die automatisch die Begrenzung der TCP-Slot-Tabelle auf ein Niveau erhöhen können, das den NFS-Server mit Anforderungen sättigt.

Um eine optimale Performance zu erzielen und Performance-Probleme zu vermeiden, passen Sie die Kernel-Parameter an, die die TCP-Slot-Tabellen steuern, auf 128 an.

```
sysctl -a | grep tcp.*.slot_table
```

- Die folgende Tabelle enthält die empfohlenen NFS-Mount-Optionen für Linux NFSv3 – Single-Instance.

File Type	Mount Options
<ul style="list-style-type: none">• Control files• Data files• Redo logs	<code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536</code>
<ul style="list-style-type: none">• ORACLE_HOME• ORACLE_BASE	<code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536</code>



Überprüfen Sie vor der Verwendung von dNFS, ob die in Oracle Doc 1495104.1 beschriebenen Patches installiert sind. Die NetApp Support-Matrix für NFSv3 und NFSv4 enthält keine spezifischen Betriebssysteme. Alle Betriebssysteme, die der RFC entsprechen, werden unterstützt. Wenn Sie die Online-IMT nach Unterstützung für NFSv3 oder NFSv4 suchen, wählen Sie kein bestimmtes Betriebssystem aus, da keine Treffer angezeigt werden. Alle Betriebssysteme werden implizit von der allgemeinen Richtlinie unterstützt.

Hochverfügbarkeit

Wie in der Lösungsarchitektur angegeben, wird HA auf der Replizierung auf Storage-Ebene aufgebaut. Somit sind Start und Verfügbarkeit von Oracle davon abhängig, wie schnell Computing- und Storage-Ressourcen aufgerufen und wiederhergestellt werden können. Die folgenden wichtigen Faktoren sind wichtig:

- Eine Standby-Computing-Instanz ist bereit und mit dem primären über das parallele Ansible-Update zu beiden Hosts synchronisiert.
- Replizieren Sie das Binärvolumen aus dem primären Standby-Modus, damit Sie Oracle in letzter Minute nicht installieren und herausfinden müssen, was installiert und gepatcht werden muss.
- Die Replizierungsfrequenz bestimmt, wie schnell die Oracle-Datenbank wiederhergestellt werden kann, damit der Service verfügbar ist. Zwischen der Replizierungshäufigkeit und dem Storage-Verbrauch besteht ein Kompromiss.
- Nutzen Sie die Automatisierung, um das Recovery zu beschleunigen und den Wechsel auf Standby schnell und frei von menschlichen Fehlern zu machen. NetApp stellt zu diesem Zweck ein Automatisierungstoolkit zur Verfügung.

Schritt-für-Schritt-Anweisungen zur Oracle-Implementierung auf AWS EC2 und FSX

In diesem Abschnitt werden die Implementierungsverfahren für die Implementierung von Oracle RDS Custom Database mit FSX Storage beschrieben.

Implementieren Sie eine EC2 Linux-Instanz für Oracle über die EC2-Konsole

Für neue AWS-Lösungen müssen Sie zunächst eine AWS-Umgebung einrichten. Die Registerkarte Dokumentation auf der Landing Page der AWS-Website enthält EC2-Anweisungslinks zur Implementierung einer Linux-EC2-Instanz, die zum Hosten Ihrer Oracle-Datenbank über die AWS-EC2-Konsole verwendet werden kann. Der folgende Abschnitt enthält eine Zusammenfassung dieser Schritte. Weitere Informationen finden Sie in der zugehörigen AWS EC2-spezifischen Dokumentation.

Einrichten der AWS EC2-Umgebung

Sie müssen ein AWS-Konto erstellen, um die erforderlichen Ressourcen bereitzustellen, um Ihre Oracle Umgebung auf dem EC2 und FSX Service auszuführen. Die folgende AWS-Dokumentation enthält die erforderlichen Details:

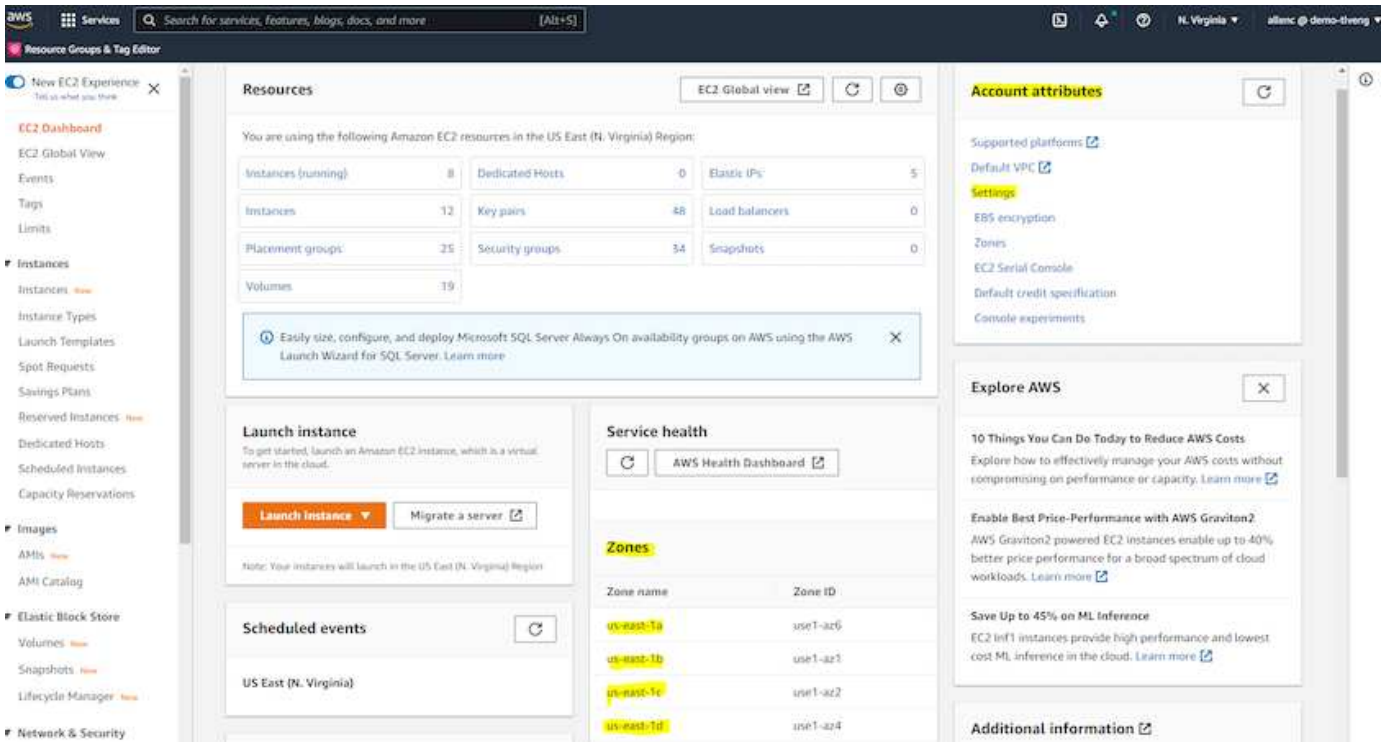
- ["Einrichten zur Verwendung von Amazon EC2"](#)

Hauptthemen:

- Melden Sie sich für AWS an.
- Erstellen Sie ein Schlüsselpaar.
- Erstellen Sie eine Sicherheitsgruppe.

Aktivierung mehrerer Verfügbarkeitszonen in AWS-Kontoattributen

Für eine Oracle-Hochverfügbarkeitskonfiguration, wie im Architekturdiagramm gezeigt, müssen Sie mindestens vier Verfügbarkeitszonen in einer Region aktivieren. Die verschiedenen Verfügbarkeitszonen können auch in verschiedenen Regionen aufgestellt werden, um die für das Disaster Recovery erforderlichen Entfernungen zu erfüllen.



Erstellen und Verbinden mit einer EC2-Instanz zum Hosten von Oracle-Datenbank

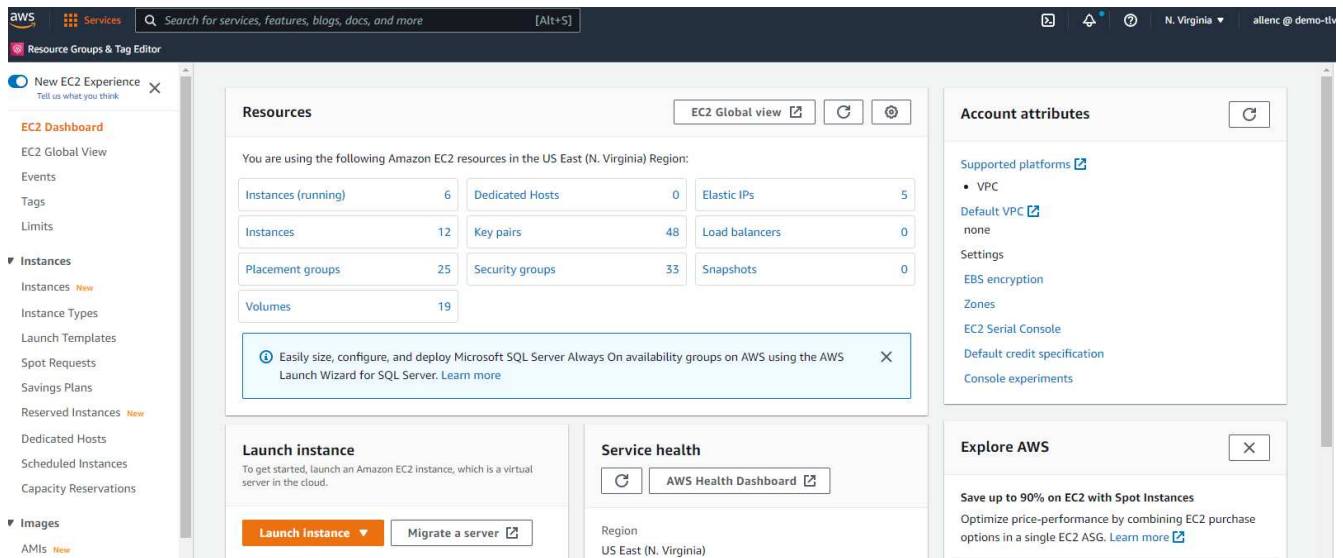
Siehe Lernprogramm "[Erste Schritte mit Amazon EC2 Linux Instanzen](#)" Für Schritt-für-Schritt-Anweisungen und Best Practices bei der Implementierung.

Hauptthemen:

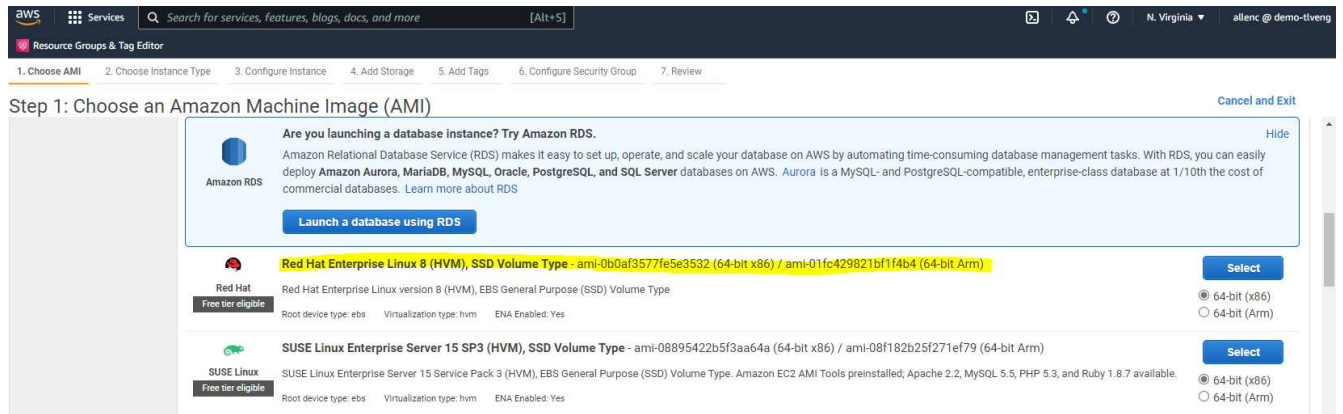
- Überblick.
- Voraussetzungen.
- Schritt 1: Eine Instanz starten.
- Schritt 2: Stellen Sie eine Verbindung zu Ihrer Instanz her.
- Schritt 3: Reinigen Sie Ihre Instanz.

Die folgenden Screenshots zeigen die Bereitstellung einer m5-Typ Linux-Instanz mit der EC2-Konsole für die Ausführung von Oracle.

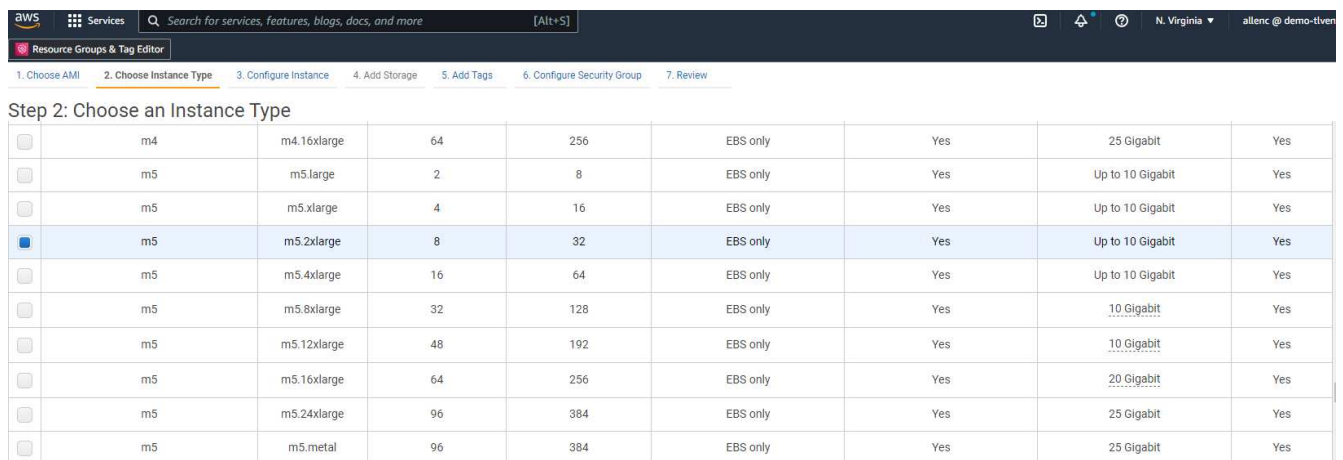
1. Klicken Sie im EC2-Dashboard auf die gelbe Schaltfläche Instanz starten, um den Implementierungs-Workflow für EC2 Instanzen zu starten.



- Wählen Sie in Schritt 1 „Red hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0b0af3577fe5e3532 (64-bit x86) / ami-01fc429821bf1f4b4 (64-bit ARM)“ aus.



- Wählen Sie in Schritt 2 einen m5-Instanztyp mit der entsprechenden CPU- und Speicherzuweisung basierend auf Ihrem Oracle-Datenbank-Workload aus. Klicken Sie Auf „Weiter: Instanzdetails Konfigurieren“.



- Wählen Sie in Schritt 3 die VPC und das Subnetz aus, in dem die Instanz platziert werden soll, und aktivieren Sie die öffentliche IP-Zuweisung. Klicken Sie Auf „Next: Add Storage“ (Weiter).

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia allenc @ demo-tiveng

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option Request Spot instances

Network vpc-0474064fc537e5182 Create new VPC
No default VPC found. Create a new default VPC.

Subnet subnet-08c952541f4ab282d us-east-1a Create new subnet
250 IP Addresses available

Auto-assign Public IP Enable

Hostname type Use subnet setting (IP name)

DNS Hostname Enable IP name IPv4 (A record) DNS requests
 Enable resource-based IPv4 (A record) DNS requests
 Enable resource-based IPv6 (AAAA record) DNS requests

Placement group Add instance to placement group

Capacity Reservation Open

Domain join directory No directory Create new directory

IAM role None Create new IAM role

Cancel Previous Review and Launch Next: Add Storage

5. Weisen Sie in Schritt 4 genügend Speicherplatz für die Root-Festplatte zu. Möglicherweise benötigen Sie den Speicherplatz, um einen Swap hinzuzufügen. Standardmäßig weist EC2-Instanz keinen Swap-Speicherplatz zu, was nicht optimal für die Ausführung von Oracle ist.

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia allenc @ demo-tiveng

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-03a3ad00558b4d17c	50	General Purpose SSD (gp2)	150 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Add New Volume

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Shared file systems
You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

Add file system

Cancel Previous Review and Launch Next: Add Tags

6. Fügen Sie in Schritt 5 bei Bedarf ein Tag für die Instanzidentifikation hinzu.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webservers. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum) Value (256 characters maximum) Instances Volumes Network Interfaces

This resource currently has no tags.

Choose the Add tag button or click to add a Name tag. Make sure your IAM policy includes permissions to create tags.

Add Tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

7. Wählen Sie in Schritt 6 eine vorhandene Sicherheitsgruppe aus oder erstellen Sie eine neue mit der gewünschten ein- und ausgehenden Richtlinie für die Instanz.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-0d746a0908b897c48	AviOCCM03112021OCCM1635951256631-OCCMSecurityGroup-B3QFHUJRLUVW	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-07b0625cd544aee16	AviOCCM0311OCCM1635943382952-OCCMSecurityGroup-1L8D4QX2SC945	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-0618122caef6c50e9	AviOCCM1103OCCM1635944222133-OCCMSecurityGroup-DX5PHX6CKVKC	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-0d63ea8c78987e660	AviOCCM1209OCCM1631452667252-OCCMSecurityGroup-T5KVZ1Q4SH48	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-0aed9f8836b48c52d	AviOCCMFSxOCCM1638110371156-OCCMSecurityGroup-N0ENZJW3TVYB	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-083a6ea5c912375	connector1OCCM1631455604110-OCCMSecurityGroup-1790QV45PH3ZW	NetApp OCCM Instance External Security Group	Copy to new
<input checked="" type="checkbox"/> sg-08148ca915189ac87	default	default VPC security group	Copy to new
<input type="checkbox"/> sg-07f6c527620e3bb22	fsx02OCCM163339531669-OCCMSecurityGroup-1XZYCSWM15NP7	NetApp OCCM Instance External Security Group	Copy to new
<input type="checkbox"/> sg-0f359d2ba38db749f	SG-Version10-OCE6MEs-NetAppExternalSecurityGroup-N8B50KGTK58U	ONTAP Cloud firewall rules for management and data interface	Copy to new

Inbound rules for sg-08148ca915189ac87 (Selected security groups: sg-08148ca915189ac87)

Type	Protocol	Port Range	Source	Description
All traffic	All	All	192.168.1.0/24	
All traffic	All	All	sg-08148ca915189ac87 (default)	

Cancel Previous Review and Launch

8. Überprüfen Sie in Schritt 7 die Zusammenfassung der Instanzkonfiguration, und klicken Sie auf Starten, um die Instanzbereitstellung zu starten. Sie werden aufgefordert, ein Schlüsselpaar zu erstellen oder ein Schlüsselpaar für den Zugriff auf die Instanz auszuwählen.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details Edit AMI

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0b0af3577fe5e3532
 Free tier eligible Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type
 Root Device Type: ebs Virtualization type: hvm

Instance Type Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m5.2xlarge	-	8	32	EBS only	Yes	Up to 10 Gigabit

Security Groups Edit security groups

Security Group ID	Name	Description
sg-08148ca915189ac87	default	default VPC security group

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
All traffic	All	All	192.168.1.0/24	
All traffic	All	All	sg-08148ca915189ac87 (default)	

Instance Details Edit instance details

Storage Edit storage

Cancel Previous Launch

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Choose an existing key pair ▼

Select a key pair

accesststkey | RSA ▼

I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Cancel Launch Instances

- Melden Sie sich über ein SSH-Schlüsselpaar bei der EC2-Instanz an. Nehmen Sie ggf. Änderungen an Ihrem Schlüsselnamen und Ihrer Instanz-IP-Adresse vor.

```
ssh -i ora-dblv2.pem ec2-user@54.80.114.77
```

Sie müssen zwei EC2-Instanzen als primäre und Standby-Oracle-Server in ihrer festgelegten

Verfügbarkeitszone erstellen, wie im Architekturdiagramm dargestellt.

Stellen Sie FSX für ONTAP File-Systeme für Oracle Datenbank-Storage bereit

Die Implementierung der EC2-Instanz weist ein EBS Root Volume für das Betriebssystem zu. FSX für ONTAP stellt Oracle Datenbank-Storage-Volumes bereit, einschließlich der Oracle Binär-, Daten- und Protokoll-Volumes. Die FSX-Storage-NFS-Volumes können entweder über die AWS FSX Konsole oder über die Oracle-Installation bereitgestellt werden und durch Konfigurationsautomatisierung, die die Volumes dem Benutzer in einer Automatisierungsparameter-Datei zuweist.

Erstellen von FSX für ONTAP-Dateisysteme

Habe auf diese Dokumentation verwiesen "[Verwalten von FSX für ONTAP-Dateisysteme](#)" Zur Erstellung von FSX für ONTAP-Dateisysteme.

Wichtige Überlegungen:

- SSD-Storage-Kapazität: Mindestens 1024 gib, maximal 192 tib.
- Provisionierter SSD-IOPS: Maximal 80,000 SSD-IOPS pro Filesystem, basierend auf Workload-Anforderungen.
- Durchsatzkapazität.
- Legen Sie das Administratorpasswort fsxadmin/vsadmin fest. Erforderlich für FSX-Konfigurationsautomatisierung
- Backup und Wartung. Automatische tägliche Backups deaktivieren; Datenbank-Storage-Backups werden durch SnapCenter-Planung durchgeführt.
- Rufen Sie die SVM Management-IP-Adresse und protokollspezifische Zugriffadressen auf der SVM Detailseite ab. Erforderlich für FSX-Konfigurationsautomatisierung

The screenshot shows the AWS Management Console interface for an Amazon FSx for ONTAP file system. The main content area is titled "fsx (svm-005c6edf027866ca4)". It contains two sections: "Summary" and "Endpoints".

Summary:

SVM ID	svm-005c6edf027866ca4	Creation time	2022-01-24T18:02:24-05:00	Active Directory	-
SVM name	fsx	Lifecycle state	Created		
UUID	1a07ea1f-7d6e-11ec-97a9-7df96ee2a64a	Subtype	DEFAULT		
File system ID	fs-0a51a3f08922224d5				
Resource ARN	arn:aws:fsx:us-east-1:759995470648:storage-virtual-machine/fs-0a51a3f08922224d5/svm-005c6edf027866ca4				

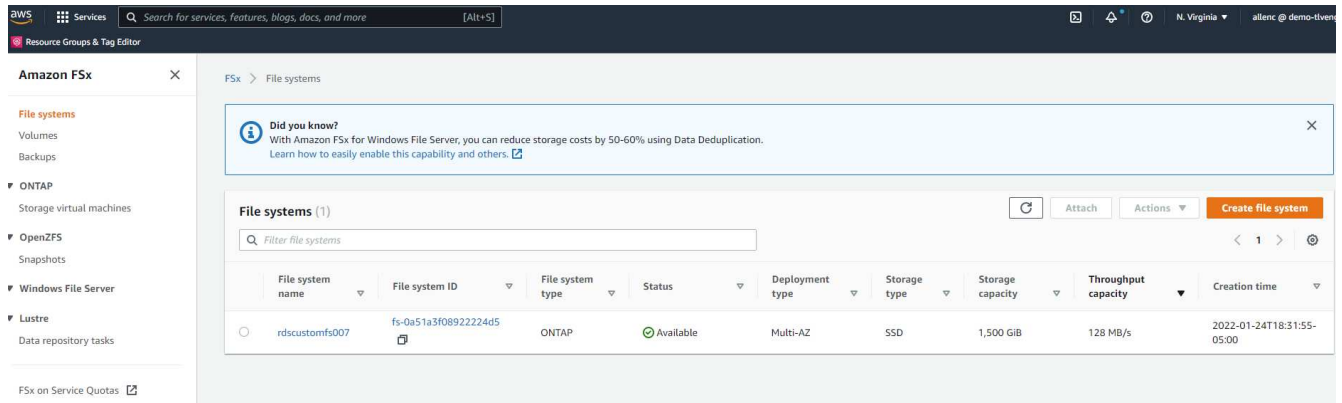
Endpoints:

Management DNS name	svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com	Management IP address	198.19.255.68
NFS DNS name	svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com	NFS IP address	198.19.255.68
iSCSI DNS name	iscsi.svm-005c6edf027866ca4.fs-0a51a3f08922224d5.fsx.us-east-1.amazonaws.com	iSCSI IP addresses	10.0.1.200, 10.0.0.86

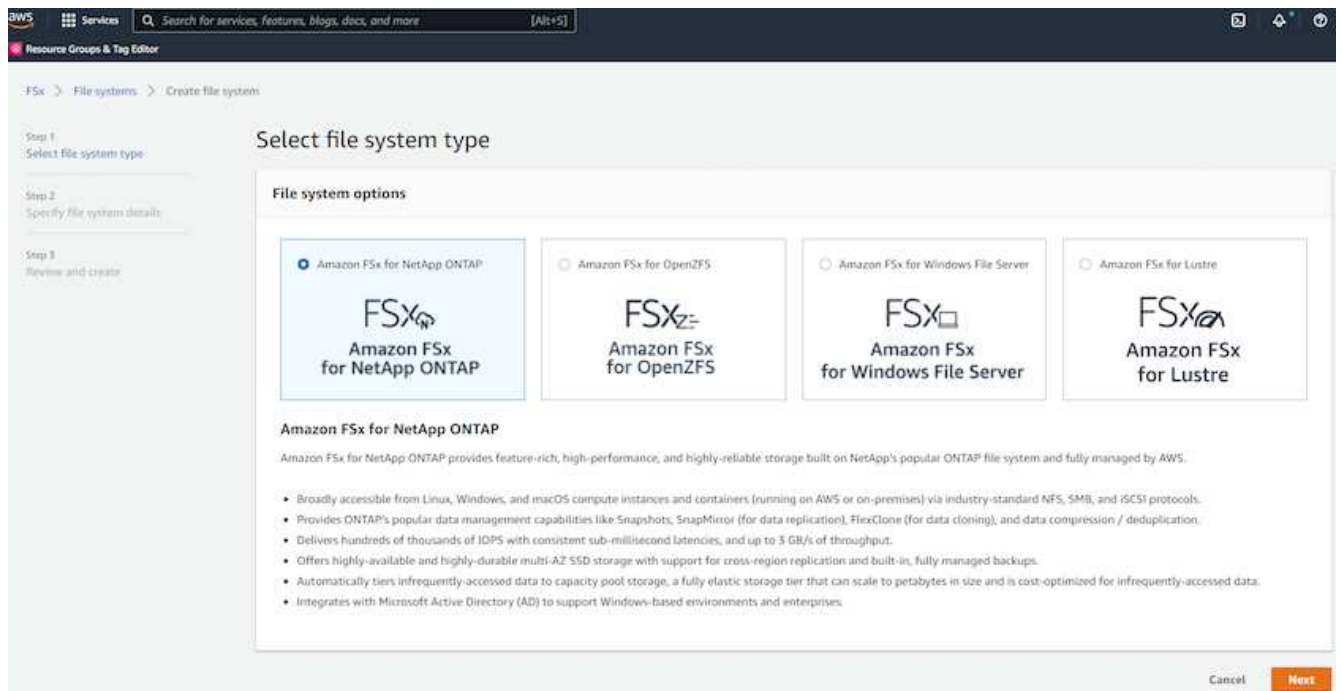
Sehen Sie sich die folgenden Schritt-für-Schritt-Anweisungen zum Einrichten eines primären oder Standby HA FSX-Clusters an.

1. Klicken Sie auf der FSX-Konsole auf Dateisystem erstellen, um den FSX-Bereitstellungsprozess zu

starten.



2. Wählen Sie Amazon FSX für NetApp ONTAP aus. Klicken Sie anschließend auf Weiter.



3. Wählen Sie Standard Erstellen und benennen Sie unter Dateisystemdetails Ihr Dateisystem, Multi-AZ HA. Wählen Sie je nach Datenbank-Workload entweder automatisch oder vom Benutzer bereitgestellte IOPS bis zu 80,000 SSD-IOPS. FSX Storage verfügt über bis zu 2 tib NVMe-Caching im Backend, das noch höhere gemessene IOPS liefern kann.

File system details

File system name - optional [Info](#)

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . _ : /

Deployment type [Info](#)

Multi-AZ

Single-AZ

SSD storage capacity [Info](#)

Minimum 1024 GiB; Maximum 192 TiB.

Provisioned SSD IOPS

Amazon FSx provides 3 IOPS per GiB of storage capacity. You can also provision additional SSD IOPS as needed.

Automatic (3 IOPS per GiB of SSD storage)

User-provisioned

Maximum 80,000 IOPS

Throughput capacity [Info](#)

The sustained speed at which the file server hosting your file system can serve data. The file server can also burst to higher speeds for periods of time.

Recommended throughput capacity

128 MB/s

Specify throughput capacity

Throughput capacity

4. Wählen Sie im Abschnitt Netzwerk & Sicherheit die VPC, die Sicherheitsgruppe und die Subnetze aus. Diese sollten vor der Bereitstellung von FSX erstellt werden. Platzieren Sie die FSX-Storage-Nodes auf Basis der Rolle des FSX-Clusters (primär oder Standby) in die entsprechenden Zonen.

Network & security

Virtual Private Cloud (VPC) [Info](#)

Specify the VPC from which your file system is accessible.

vpc-0474064fc537e5182 ▼

VPC Security Groups [Info](#)

Specify VPC Security Groups to associate with your file system's network interfaces.

Choose VPC security group(s) ▼

sg-08148ca915189ac87 (default) ✕

Preferred subnet [Info](#)

Specify the preferred subnet for your file system.

subnet-08c952541f4ab282d (us-east-1a) ▼

Standby subnet

subnet-0a84d6eeeb0f4e5c0 (us-east-1b) ▼

VPC route tables

Specify the VPC route tables associated with your file system.

VPC's default route table

Select one or more VPC route tables

Endpoint IP address range

Specify the IP address range in which the endpoints to access your file system will be created

No preference

Select an IP address range

5. Akzeptieren Sie im Abschnitt Sicherheit & Verschlüsselung die Standardeinstellung, und geben Sie das fsxadmin-Passwort ein.

Security & encryption

Encryption key [Info](#)
 AWS Key Management Service (KMS) encryption key that protects your file system data at rest.

aws/fsx (default) ▼

Description	Account	KMS key ID
Default master key that protects my FSx resources when no other key is defined	759995470648	5b31feff-6759-4306-a852-9c99a743982a

File system administrative password
 Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

Don't specify a password
 Specify a password

Password

Confirm password

6. Geben Sie den SVM-Namen und das vsadmin-Passwort ein.

Default storage virtual machine configuration

Storage virtual machine name

SVM administrative password
 Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

Don't specify a password
 Specify a password

Password

Confirm password

Active Directory
 Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.

Do not join an Active Directory
 Join an Active Directory

7. Behalten Sie die Volume-Konfiguration leer. Sie müssen derzeit kein Volume erstellen.

Default volume configuration

Volume name

Maximum of 203 alphanumeric characters, plus _.

Junction path

The location within your file system where your volume will be mounted.

Volume size

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

Enabled (recommended)

Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

▶ Backup and maintenance - optional

▶ Tags - optional

Cancel Back Next

8. Prüfen Sie die Seite Zusammenfassung, und klicken Sie auf Dateisystem erstellen, um die Bereitstellung des FSX-Dateisystems abzuschließen.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

Step 1 Select file system type

Step 2 Specify file system details

Step 3 Review and create

Create file system

Summary
Verify the following attributes before proceeding

Attribute	Value	Editable after creation
File system type	Amazon FSx for NetApp ONTAP	
File system name	aws_ora_prod	✓
Deployment type	Multi-AZ	
Storage type	SSD	
SSD storage capacity	1,024 GiB	✓
Minimum SSD IOPS	40000 IOPS	✓
Throughput capacity	512 MB/s	✓
Virtual Private Cloud (VPC)	vpc-0474064fc537e5182	
VPC Security Groups	sg-08148ca915189ac87	✓
Preferred subnet	subnet-08c952541f4ab282d	
Standby subnet	subnet-0a84d6eeeb0f4e5c0	
VPC route tables	VPC's default route table	
Endpoint IP address range	No preference	
KMS key ID	arn:aws:kms:us-east-1:759995470648:key/5b31feff-6759-4306-a852-9c99a743982a	
Daily automatic backup window	No preference	✓
Automatic backup	7 day(s)	✓

Bereitstellung von Datenbank-Volumes für Oracle Database

Siehe "[Management von FSX für ONTAP-Volumes – Erstellen eines Volumes](#)" Entsprechende Details.

Wichtige Überlegungen:

- Dimensionierung der Datenbank-Volumes entsprechend.
- Deaktivieren der Kapazitäts-Pool Tiering-Richtlinie für eine Performance-Konfiguration
- Oracle dNFS für NFS Storage Volumes aktivieren.
- Multipath-Einrichtung für iSCSI-Storage-Volumes

Erstellen Sie Datenbank-Volume über die FSX Konsole

Über die AWS FSX-Konsole können Sie drei Volumes für Oracle-Datenbank-File-Storage erstellen: Eines für die Oracle-Binärdatei, eines für die Oracle-Daten und eines für das Oracle-Protokoll. Stellen Sie sicher, dass die Volume-Benennung mit dem Oracle Host-Namen (definiert in der Hosts-Datei im Automatisierungs-Toolkit) übereinstimmt, um die ordnungsgemäße Identifizierung zu finden. In diesem Beispiel verwenden wir db1 als Oracle-Hostname von EC2 anstelle eines typischen IP-Adressenbasierten Hostnamens für eine EC2-Instanz.

Create volume



File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007

Storage virtual machine

svm-005c6edf027866ca4 | fsx

Volume name

db1_bin

Maximum of 203 alphanumeric characters, plus _ .

Junction path

/db1_bin

The location within your file system where your volume will be mounted.

Volume size

51200

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

Enabled (recommended)

Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None

Cancel

Confirm

Create volume



File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007



Storage virtual machine

svm-005c6edf027866ca4 | fsx



Volume name

db1_data

Maximum of 203 alphanumeric characters, plus _ .

Junction path

/db1_data

The location within your file system where your volume will be mounted.

Volume size

512000

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

- Enabled (recommended)
- Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None



Cancel

Confirm

Create volume
✕

File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007 ▼

Storage virtual machine

svm-005c6edf027866ca4 | fsx ▼

Volume name

db1_log

Maximum of 203 alphanumeric characters, plus _.

Junction path

/db1_log

The location within your file system where your volume will be mounted.

Volume size

256000

Minimum 20 MiB; Maximum 104857600 MiB

Storage efficiency

Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.

Enabled (recommended)

 Disabled

Capacity pool tiering policy

You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.

None ▼

Cancel
Confirm



Das Erstellen von iSCSI-LUNs wird derzeit nicht von der FSX-Konsole unterstützt. Für die Implementierung von iSCSI-LUNs bei Oracle können die Volumes und LUNs mithilfe von Automatisierung für ONTAP mit dem NetApp Automatisierungs-Toolkit erstellt werden.

Installation und Konfiguration von Oracle auf einer EC2-Instanz mit FSX Datenbank-Volumes

Das Automatisierungsteam von NetApp stellt ein Automatisierungs-Kit bereit, um Oracle Installation und Konfiguration auf EC2 Instanzen gemäß den Best Practices auszuführen. Die aktuelle Version des Automatisierungs-Kits unterstützt Oracle 19c on NFS mit dem Standard RU Patch 19.8. Das Automationskit kann bei Bedarf problemlos an andere RU-Patches angepasst werden.

Ansible-Controller vorbereiten, um die Automatisierung auszuführen

Befolgen Sie die Anweisungen im Abschnitt „[Erstellen und Verbinden mit einer EC2-Instanz zum Hosten von Oracle-Datenbank](#)“, Bezeichnet, um eine kleine EC2 Linux-Instanz zum Ausführen des Ansible-Controllers bereitzustellen. Anstatt RedHat zu verwenden, sollte Amazon Linux t2.Large mit 2vCPU und 8G RAM ausreichend sein.

Rufen Sie das NetApp Oracle Deployment Automation Toolkit ab

Melden Sie sich bei der EC2-Ansible-Controller-Instanz an, die von Schritt 1 als ec2-Benutzer bereitgestellt wird, und führen Sie das aus, wenn sie das ec2-User-Home-Verzeichnis verwenden `git clone` Befehl zum Klonen einer Kopie des Automatisierungscodes.

```
git clone https://github.com/NetApp-Automation/na_oracle19c_deploy.git
```

```
git clone https://github.com/NetApp-  
Automation/na_rds_fsx_oranfs_config.git
```

Führen Sie die automatisierte Oracle 19c-Implementierung mit dem Automatisierungs-Toolkit aus

Siehe diese detaillierte Anweisung "[CLI-Implementierung einer Oracle 19c Datenbank](#)" Um Oracle 19c mit CLI-Automatisierung zu implementieren. Die Befehlsyntax für die Ausführung des Playbook-Befehls ändert sich klein, da Sie ein SSH-Schlüsselpaar anstelle eines Passworts für die Host-Zugriffs-Authentifizierung verwenden. Die folgende Liste enthält eine allgemeine Zusammenfassung:

1. Standardmäßig verwendet eine EC2-Instanz ein SSH-Schlüsselpaar für die Zugriffsauthentisierung. Über Ansible-Root-Verzeichnisse zur Controller-Automatisierung `/home/ec2-user/na_oracle19c_deploy`, und `/home/ec2-user/na_rds_fsx_oranfs_config` Erstellen Sie eine Kopie des SSH-Schlüssels `accesststkey.pem` Für den im Schritt implementierten Oracle Host „[Erstellen und Verbinden mit einer EC2-Instanz zum Hosten von Oracle-Datenbank](#).“
2. Melden Sie sich als ec2-User beim DB-Host der EC2-Instanz an, und installieren Sie die python3-Bibliothek.

```
sudo yum install python3
```

3. Erstellen Sie einen 16G-Swap-Speicherplatz vom Root-Festplattenlaufwerk. Standardmäßig erstellt eine EC2-Instanz keinen Swap-Speicherplatz. Folgen Sie der folgenden AWS Dokumentation: "[Wie weisen ich Speicher zu, um durch Verwendung einer Auslagerungsdatei als Auslagerungsspeicher in einer Amazon EC2 Instanz zu arbeiten?](#)".
4. Zurück zum Ansible-Controller (`cd /home/ec2-user/na_rds_fsx_oranfs_config`), und führen Sie das Pre-Clone-Playbook mit den entsprechenden Anforderungen und aus `linux_config` tags:

```
ansible-playbook -i hosts rds_preclone_config.yml -u ec2-user --private  
-key accesststkey.pem -e @vars/fsx_vars.yml -t requirements_config
```

```
ansible-playbook -i hosts rds_preclone_config.yml -u ec2-user --private-key accesststkey.pem -e @vars/fsx_vars.yml -t linux_config
```

5. Wechseln Sie zum `/home/ec2-user/na_oracle19c_deploy-master` Lesen Sie die README-Datei, und füllen Sie den globalen Ordner aus `vars.yml` Datei mit den relevanten globalen Parametern.
6. Füllen Sie das aus `host_name.yml` Datei mit den entsprechenden Parametern im `host_vars` Verzeichnis.
7. Führen Sie das Playbook für Linux aus, und drücken Sie die Eingabetaste, wenn Sie zur Eingabe des vsadmin-Passworts aufgefordert werden.

```
ansible-playbook -i hosts all_playbook.yml -u ec2-user --private-key accesststkey.pem -t linux_config -e @vars/vars.yml
```

8. Führen Sie das Playbook für Oracle aus, und drücken Sie die Eingabetaste, wenn Sie zur Eingabe des vsadmin-Passworts aufgefordert werden.

```
ansible-playbook -i hosts all_playbook.yml -u ec2-user --private-key accesststkey.pem -t oracle_config -e @vars/vars.yml
```

Ändern Sie ggf. das Berechtigungsbit für die SSH-Schlüsseldatei in 400. Ändern Sie den Oracle-Host (`ansible_host` im `host_vars` Datei) IP-Adresse an die öffentliche Adresse Ihrer EC2 Instanz.

Einrichten von SnapMirror zwischen primärem und Standby FSX HA-Cluster

Für Hochverfügbarkeit und Disaster Recovery kann SnapMirror Replizierung zwischen dem primären und Standby FSX Storage-Cluster eingerichtet werden. Im Gegensatz zu anderen Cloud-Storage-Services ermöglicht FSX Benutzern die Steuerung und das Management der Storage-Replizierung mit der gewünschten Häufigkeit und dem Replizierungsdurchsatz. Außerdem können Benutzer HA/DR ohne Auswirkungen auf die Verfügbarkeit testen.

Die folgenden Schritte zeigen, wie die Replikation zwischen einem primären und Standby FSX-Storage-Cluster eingerichtet wird.

1. Primären und Standby-Cluster-Peering einrichten. Melden Sie sich als `fsxadmin`-Benutzer im primären Cluster an, und führen Sie den folgenden Befehl aus. Bei dieser gegenseitigen Erstellung wird der Befehl `create` sowohl auf dem primären Cluster als auch auf dem Standby-Cluster ausgeführt. Austausch `standby_cluster_name` Mit dem entsprechenden Namen für Ihre Umgebung einfügen.

```
cluster peer create -peer-addr  
standby_cluster_name,inter_cluster_ip_address -username fsxadmin  
-initial-allowed-vserver-peers *
```

2. Einrichten von Vserver Peering zwischen dem primären und dem Standby-Cluster Melden Sie sich als `vsadmin`-Benutzer im primären Cluster an, und führen Sie den folgenden Befehl aus. Austausch `primary_vserver_name`, `standby_vserver_name`, `standby_cluster_name` Den entsprechenden

Namen für Ihre Umgebung bereit.

```
vserver peer create -vserver primary_vserver_name -peer-vserver
standby_vserver_name -peer-cluster standby_cluster_name -applications
snapmirror
```

3. Überprüfen Sie, ob die Cluster- und vserver-Peerings korrekt eingerichtet sind.

```
FsxId00164454fac5591e6::> cluster peer show
Peer Cluster Name          Cluster Serial Number Availability Authentication
-----
FsxId0b6a95149d07aa82e    1-80-000011           Available      ok

FsxId00164454fac5591e6::> vserver peer show
Vserver      Peer      Peer      Peer Cluster      Peering      Remote
Vserver      Vserver   State     Peer Cluster      Applications  Vserver
-----
svm_FSxOraSource
      svm_FSxOraTarget
            peered      FsxId0b6a95149d07aa82e
                                snapmirror      svm_FSxOraTarget

FsxId00164454fac5591e6::>
```

4. Erstellung von Ziel-NFS-Volumes im Standby-FSX Cluster für jedes Quell-Volumen im primären FSX-Cluster Ersetzen Sie den für Ihre Umgebung geeigneten Volume-Namen.

```
vol create -volume dr_db1_bin -aggregate aggr1 -size 50G -state online
-policy default -type DP
```

```
vol create -volume dr_db1_data -aggregate aggr1 -size 500G -state online
-policy default -type DP
```

```
vol create -volume dr_db1_log -aggregate aggr1 -size 250G -state online
-policy default -type DP
```

5. Sie können auch iSCSI Volumes und LUNs für die Oracle-Binärdatei, Oracle Daten und das Oracle-Protokoll erstellen, wenn das iSCSI-Protokoll für den Datenzugriff verwendet wird. Lassen Sie ungefähr 10% freien Platz in den Volumes für Schnappschüsse.

```
vol create -volume dr_db1_bin -aggregate aggr1 -size 50G -state online
-policy default -unix-permissions ---rwxr-xr-x -type RW
```

```
lun create -path /vol/dr_db1_bin/dr_db1_bin_01 -size 45G -ostype linux
```

```
vol create -volume dr_db1_data -aggregate aggr1 -size 500G -state online  
-policy default -unix-permissions ---rwxr-xr-x -type RW
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_01 -size 100G -ostype  
linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_02 -size 100G -ostype  
linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_03 -size 100G -ostype  
linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_04 -size 100G -ostype  
linux
```

```
vol create -Volume dr_db1_log -aggregate aggr1 -size 250G -State online -Policy Standard -unix  
-Berechtigungen ---rwxr-xr-x -type RW
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_01 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_02 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_03 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_04 -size 45G -ostype linux
```

6. Erstellen Sie bei iSCSI LUNs eine Zuordnung für den Oracle-Host-Initiator für jede LUN, wobei die binäre LUN als Beispiel verwendet wird. Ersetzen Sie die Initiatorgruppe durch einen entsprechenden Namen für Ihre Umgebung und erhöhen Sie die LUN-id für jede zusätzliche LUN.

```
lun mapping create -path /vol/dr_db1_bin/dr_db1_bin_01 -igroup ip-10-0-  
1-136 -lun-id 0
```

```
lun mapping create -path /vol/dr_db1_data/dr_db1_data_01 -igroup ip-10-0-1-136 -lun-id 1
```

7. Erstellen einer SnapMirror Beziehung zwischen dem primären und dem Standby-Datenbank-Volume Ersetzen Sie den entsprechenden SVM-Namen für Ihre Umgebung.s

```
snapmirror create -source-path svm_FSxOraSource:db1_bin -destination -path svm_FSxOraTarget:dr_db1_bin -vserver svm_FSxOraTarget -throttle unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

```
snapmirror create -source-path svm_FSxOraSource:db1_data -destination -path svm_FSxOraTarget:dr_db1_data -vserver svm_FSxOraTarget -throttle unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

```
snapmirror create -source-path svm_FSxOraSource:db1_log -destination -path svm_FSxOraTarget:dr_db1_log -vserver svm_FSxOraTarget -throttle unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

Die SnapMirror Einrichtung kann mit einem NetApp Automation Toolkit für NFS-Datenbank-Volumes automatisiert werden. Das Toolkit kann auf der öffentlichen NetApp GitHub Website heruntergeladen werden.

```
git clone https://github.com/NetApp-Automation/na_ora_hadr_failover_resync.git
```

Lesen Sie die README-Anweisungen sorgfältig durch, bevor Sie die Einrichtung und Failover-Tests durchführen.



Bei der Replizierung der Oracle Binary vom primären zu einem Standby-Cluster können sich Auswirkungen auf die Oracle Lizenz ergeben. Weitere Informationen erhalten Sie bei Ihrem Oracle-Lizenzvertreter. Als Alternative könnte Oracle zum Zeitpunkt der Recovery und des Failover installiert und konfiguriert werden.

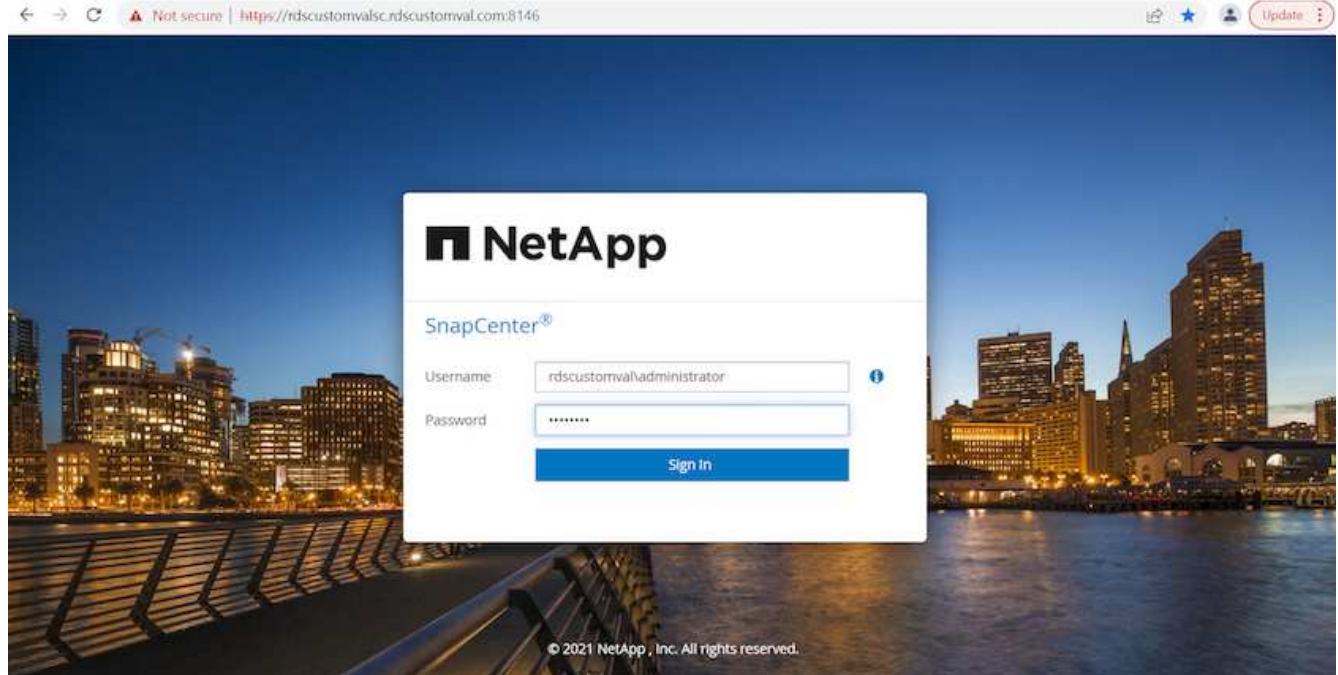
SnapCenter Deployment

SnapCenter Installation

Folgen "[Installieren des SnapCenter-Servers](#)" So installieren Sie den SnapCenter-Server: In dieser Dokumentation wird die Installation eines eigenständigen SnapCenter-Servers erläutert. Eine SaaS-Version von SnapCenter ist derzeit in der Beta-Überprüfung und könnte in Kürze verfügbar sein. Wenden Sie sich bei Bedarf an Ihren NetApp Vertriebsmitarbeiter, um Informationen zur Verfügbarkeit zu erhalten.

Konfiguration des SnapCenter Plug-ins für den EC2 Oracle Host

1. Melden Sie sich nach der automatisierten SnapCenter-Installation als administrativer Benutzer für den Windows-Host an, auf dem der SnapCenter-Server installiert ist.



2. Klicken Sie im linken Menü auf Einstellungen und dann Credential und New, um ec2-User-Anmeldeinformationen für die SnapCenter-Plugin-Installation hinzuzufügen.

Credential Name	Authentication Mode	Details
244rdscustomdb	SQL	UserId:admin
42rdscustomdb	SQL	UserId:admin
admin	SQL	UserId:admin
administrator	Windows	UserId:administrator
ec2-user	Linux	UserId:ec2-user
onpremSQL	Windows	UserId:rdscustomval/administrator
rdscdb2	Windows	UserId:administrator
rdscdb244	Windows	UserId:administrator
rdssql	Windows	UserId:administrator
tst244	SQL	UserId:admin
tstcredfordemo	Windows	UserId:administrator

3. Setzen Sie das ec2-User-Passwort zurück und aktivieren Sie die SSH-Passwort-Authentifizierung, indem Sie den bearbeiten `/etc/ssh/sshd_config` Datei auf dem EC2 Instance Host.
4. Vergewissern Sie sich, dass das Kontrollkästchen „Sudo-Berechtigungen verwenden“ aktiviert ist. Im vorherigen Schritt setzen Sie einfach das ec2-User-Passwort zurück.

Credential ✕

Credential Name

Authentication Mode ▼

Username ⓘ

Password

Use sudo privileges ⓘ

5. Fügen Sie zur Namensauflösung den SnapCenter-Servernamen und die IP-Adresse zur Host-Datei der EC2-Instanz hinzu.

```

[ec2-user@ip-10-0-0-151 ~]$ sudo vi /etc/hosts
[ec2-user@ip-10-0-0-151 ~]$ cat /etc/hosts
127.0.0.1    localhost localhost.localdomain localhost4
localhost4.localdomain4
::1        localhost localhost.localdomain localhost6
localhost6.localdomain6
10.0.1.233  rdscustomvalsc.rdscustomval.com rdscustomvalsc
```

6. Fügen Sie auf dem Windows-Host des SnapCenter-Servers der Windows-Hostdatei die Host-IP-Adresse der EC2-Instanz hinzu C:\Windows\System32\drivers\etc\hosts.

```

10.0.0.151    ip-10-0-0-151.ec2.internal
```

7. Wählen Sie im linken Menü Hosts > Managed Hosts aus und klicken Sie dann auf Hinzufügen, um den EC2 Instance Host zu SnapCenter hinzuzufügen.

Name	Type	System	Plug-in	Version	Overall Status
RDSAMAZ-VJ0DQK0	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Host down
rdscustommssql1.rdscustomval.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

Aktivieren Sie Oracle Database, und klicken Sie vor dem Senden auf More Options.

Host Type: Linux

Host Name: 10.0.0.151

Credentials: ec2-user

Select Plug-ins to Install SnapCenter Plug-ins Package 4.5 P2 for Linux

- Oracle Database
- SAP HANA

[More Options](#): Port, Install Path, Custom Plug-Ins...

Submit Cancel

Aktivieren Sie Prüfungen Vor Der Installation Überspringen. Bestätigen Sie die Überprüfung der Vorinstallation überspringen, und klicken Sie dann auf nach Speichern senden.

More Options ✕

Port i

Installation Path i

Skip preinstall checks

Custom Plug-ins

Choose a File

No plug-ins found.

Sie werden mit Fingerabdruck bestätigen aufgefordert und dann auf Bestätigen und Senden klicken.

Confirm Fingerprint ✕

Authenticity of the host cannot be determined i

Host name	Fingerprint	Valid
ip-10-0-0-151.ec2.internal	ssh-rsa 2048 97:6F:3C:7D:38:42:F6:54:B7:AF:E3:61:61:BA:2E:6F	

Nach erfolgreicher Plugin-Konfiguration wird der Gesamtstatus des verwalteten Hosts als aktiv angezeigt.

Managed Hosts									
Search by Name		Disks		Shares		Initiator Groups		iSCSI Session	
<input type="checkbox"/>	Name	Type	System	Plug-in	Version			Overall Status	
<input type="checkbox"/>	ip-10-0-0-151.ec2.internal	Linux	Stand-alone	UNIX, Oracle Database	4.5			● Running	

Konfigurieren der Backup-Richtlinie für Oracle-Datenbank

Siehe diesen Abschnitt "[Backup-Richtlinie für Datenbanken in SnapCenter einrichten](#)" Weitere Informationen zur Konfiguration der Backup-Richtlinie für Oracle Datenbanken finden Sie unter.

Im Allgemeinen müssen Sie eine Politik für das vollständige Snapshot-Backup der Oracle-Datenbank und eine Politik für das Oracle Archiv-Log-only Snapshot-Backup erstellen.



Sie können Oracle Archivprotokoll-Beschneidung in der Backup-Richtlinie aktivieren, um den Protokollarchiv-Speicherplatz zu steuern. Aktivieren Sie „Update SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie“ in der „Select secondary Replication Option“, da Sie die Replizierung zu einem Standby-Standort für HA oder DR benötigen.

Konfigurieren Sie Backup und Planung von Oracle Datenbanken

Das Datenbank-Backup in SnapCenter ist benutzerkonfigurierbar und kann entweder einzeln oder als Gruppe in einer Ressourcengruppe eingerichtet werden. Das Backup-Intervall hängt von den RTO- und RPO-Zielen ab. NetApp empfiehlt, alle paar Stunden ein komplettes Datenbank-Backup auszuführen und das Protokoll-Backup mit einer höheren Frequenz, z. B. 10-15 Minuten, zu archivieren, um eine schnelle Recovery zu ermöglichen.

Weitere Informationen finden Sie im Abschnitt Oracle von ["Backup-Richtlinie zum Schutz der Datenbank implementieren"](#) Für detaillierte Schritt-für-Schritt-Prozesse zur Implementierung der im Abschnitt erstellten Backup-Richtlinie [Konfigurieren der Backup-Richtlinie für Oracle-Datenbank](#) Und für die Backup-Jobplanung.

Das folgende Bild zeigt ein Beispiel für die Ressourcengruppen, die zum Backup einer Oracle-Datenbank eingerichtet wurden.

The screenshot shows the NetApp SnapCenter interface. The main content area displays a table of Oracle Database resources. The table has columns for Name, Oracle Database Type, Host/Cluster, Resource Group, Policies, Last Backup, and Overall Status. One resource is listed with the name 'ORCL', type 'Single Instance', host 'ip-100-0-151.ec2.internal', and resource group 'Orcl Full Backup' and 'Orcl Inc Backup'. The policies are 'Oracle full backup' and 'Oracle log backup'. The last backup was performed on 03/24/2022 at 8:40:08 PM, and the overall status is 'Backup succeeded'.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
ORCL	Single Instance	ip-100-0-151.ec2.internal	Orcl Full Backup Orcl Inc Backup	Oracle full backup Oracle log backup	03/24/2022 8:40:08 PM	Backup succeeded

EC2 und FSX Oracle Datenbankmanagement

Neben der AWS EC2 und FSX Managementkonsole werden der Ansible-Steuerungsknoten und das SnapCenter UI-Tool für das Datenbankmanagement in dieser Oracle-Umgebung implementiert.

Ein Ansible-Steuerungsknoten kann zum Management der Oracle Umgebungskonfiguration verwendet werden. Dabei stehen parallele Updates zur Verfügung, durch die primäre und Standby-Instanzen für Kernel- oder Patch-Updates synchronisiert werden. Failover, Resynchronisierung und Failback können mit dem NetApp Automation Toolkit automatisiert werden, um eine schnelle Wiederherstellung und Verfügbarkeit von Applikationen mit Ansible zu ermöglichen. Einige wiederholbare Aufgaben zum Datenbankmanagement können mithilfe eines Playbooks zur Reduzierung menschlicher Fehler ausgeführt werden.

Das SnapCenter UI Tool kann Datenbank-Snapshot-Backups, zeitpunktgenaue Recovery, Klonen von Datenbanken usw. mit dem SnapCenter Plug-in für Oracle Datenbanken durchführen. Weitere Informationen zu Oracle-Plugin-Funktionen finden Sie im ["SnapCenter Plug-in für Oracle Database – Übersicht"](#).

Die folgenden Abschnitte erläutern, wie die wichtigsten Funktionen des Oracle Datenbankmanagements über die Benutzeroberfläche von SnapCenter erfüllt werden:

- Datenbank-Snapshot-Backups
- Zeitpunktgenaue Datenbank-Wiederherstellung

- Erstellen von Datenbankklonen

Beim Klonen von Datenbanken wird ein Replikat einer primären Datenbank auf einem separaten EC2 Host zur Datenwiederherstellung im Falle eines logischen Datenfehlers oder einer Beschädigung erstellt. Klone können auch für Applikationstests, Fehlerbehebung, Patch-Validierung usw. verwendet werden.

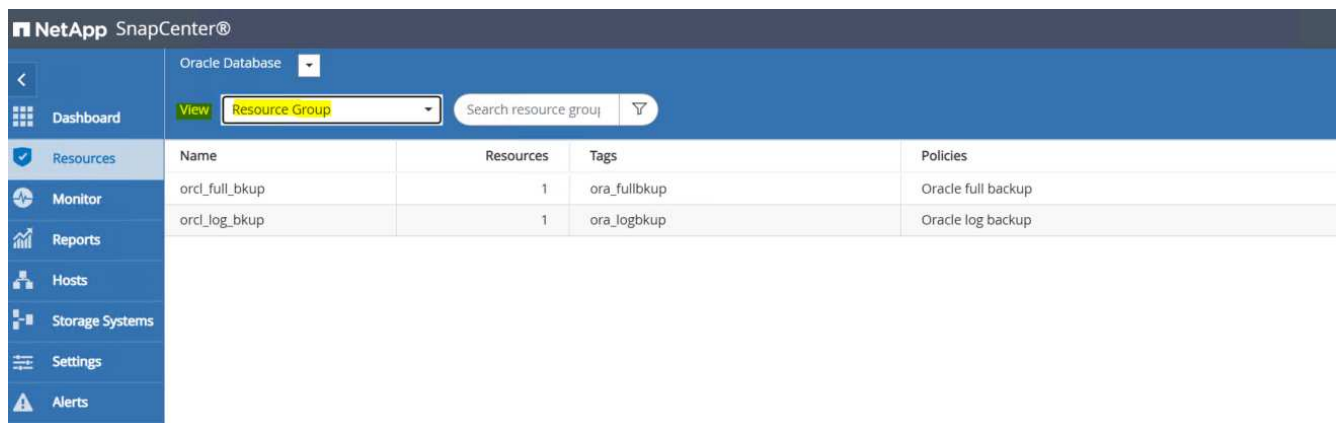
Erstellen eines Snapshots

Eine EC2/FSX Oracle-Datenbank wird regelmäßig in vom Benutzer konfigurierten Intervallen gesichert. Ein Benutzer kann jederzeit auch ein einmalig durchzuführenden Snapshot Backup durchführen. Dies gilt sowohl für Volldatenbank-Snapshot-Backups als auch für Archiv-Log-only Snapshot-Backups.

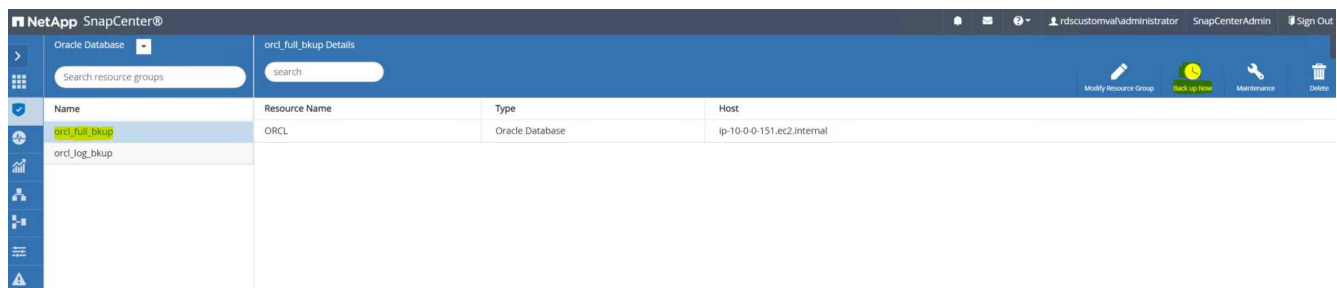
Erstellen eines vollständigen Datenbank-Snapshots

Ein vollständiger Datenbank-Snapshot umfasst alle Oracle Dateien, einschließlich Datendateien, Steuerdateien und Archivprotokolldateien.

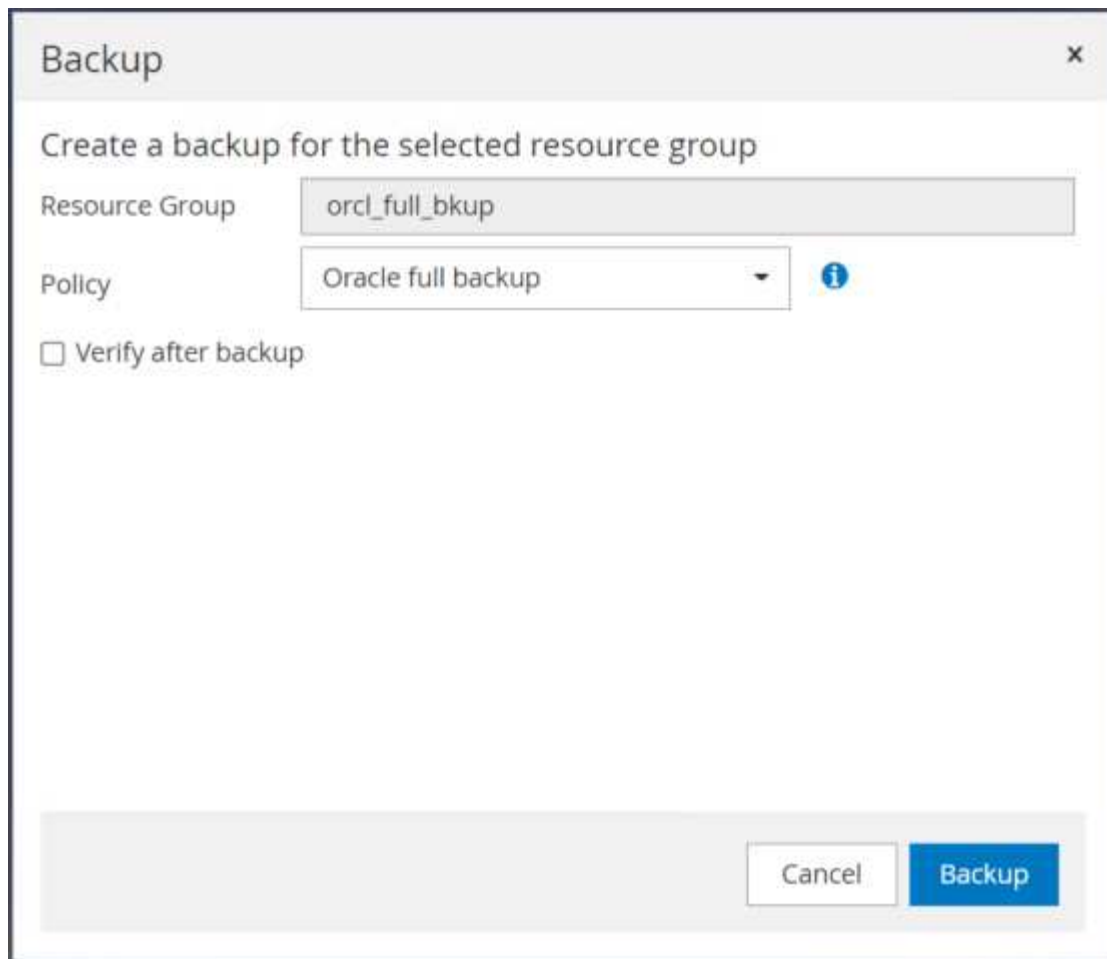
1. Melden Sie sich in der Benutzeroberfläche von SnapCenter an und klicken Sie im Menü auf der linken Seite auf „Ressourcen“. Wechseln Sie im Dropdown-Menü Ansicht in die Ansicht Ressourcengruppe.



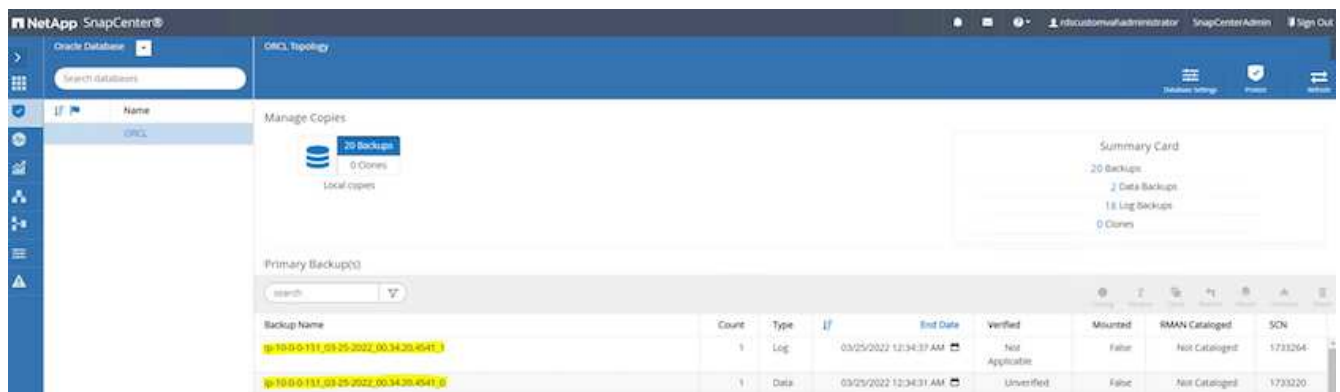
2. Klicken Sie auf den Namen der vollständigen Backup-Ressource, und klicken Sie dann auf das Symbol Jetzt sichern, um ein Add-hoc-Backup zu starten.



3. Klicken Sie auf Backup und bestätigen Sie dann das Backup, um eine vollständige Datenbank-Sicherung zu starten.



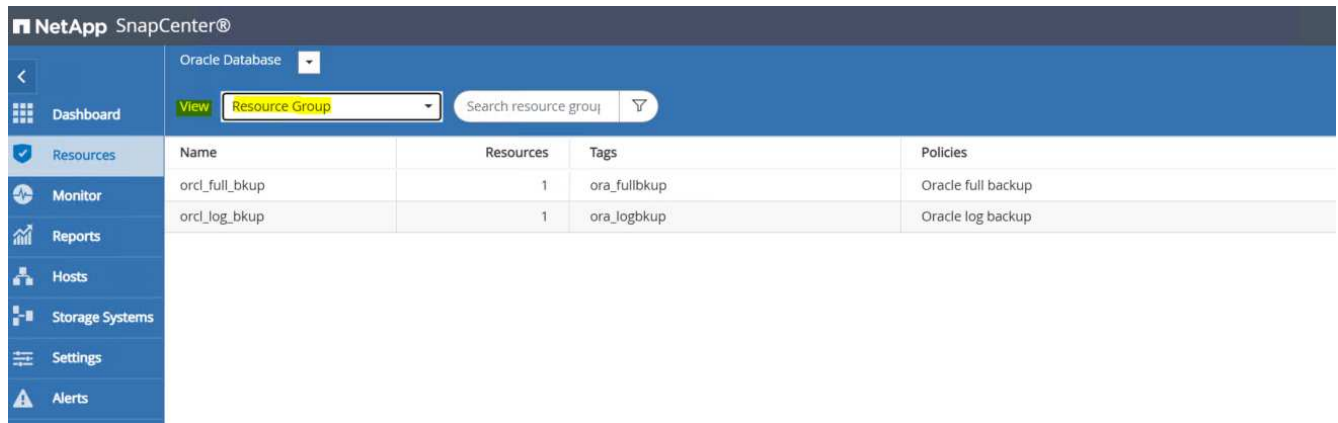
Öffnen Sie in der Ansicht „Ressource“ für die Datenbank die Seite „verwaltete Backupkopien für die Datenbank“, um zu überprüfen, ob die einmalige Sicherung erfolgreich abgeschlossen wurde. Ein vollständiges Datenbank-Backup erstellt zwei Snapshots: Einen für das Daten-Volume und einen für das Log-Volume.



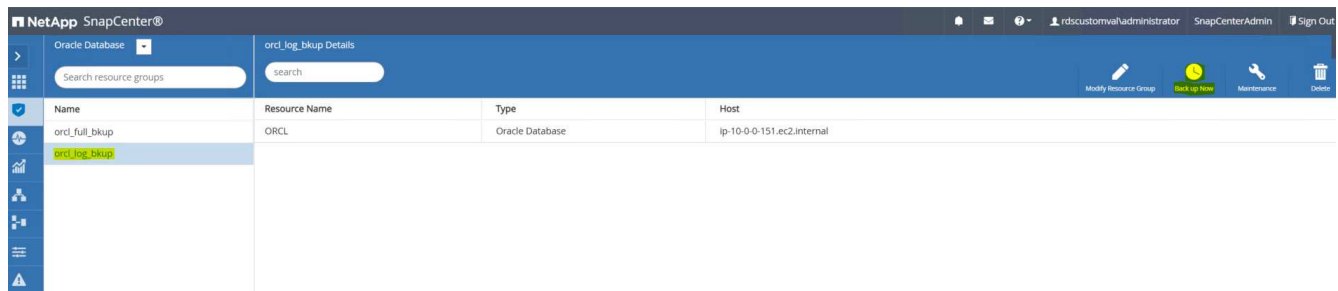
Erstellen eines Snapshot für Archivprotokolle

Ein Snapshot für das Archivprotokoll wird nur für das Oracle Archiv-Log-Volume erstellt.

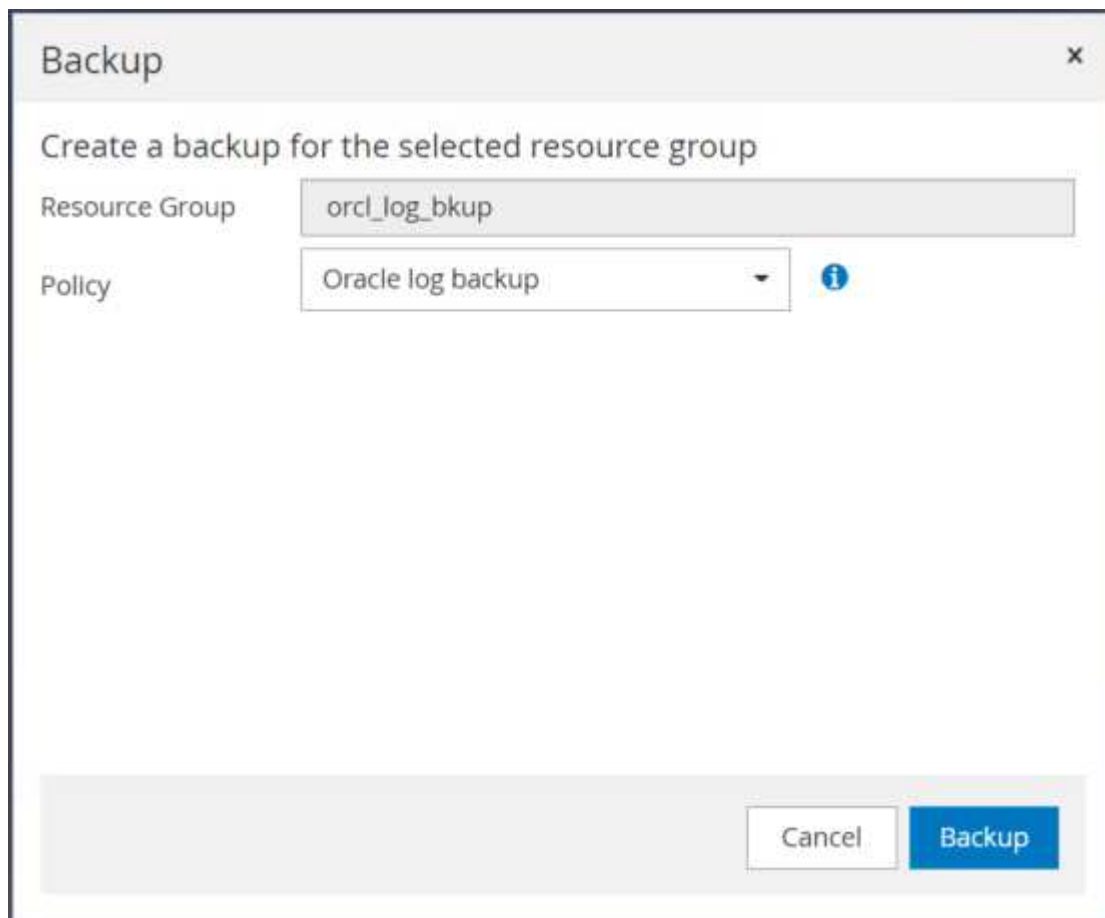
1. Melden Sie sich in der Benutzeroberfläche von SnapCenter an und klicken Sie in der Menüleiste links auf die Registerkarte „Ressourcen“. Wechseln Sie im Dropdown-Menü Ansicht in die Ansicht Ressourcengruppe.



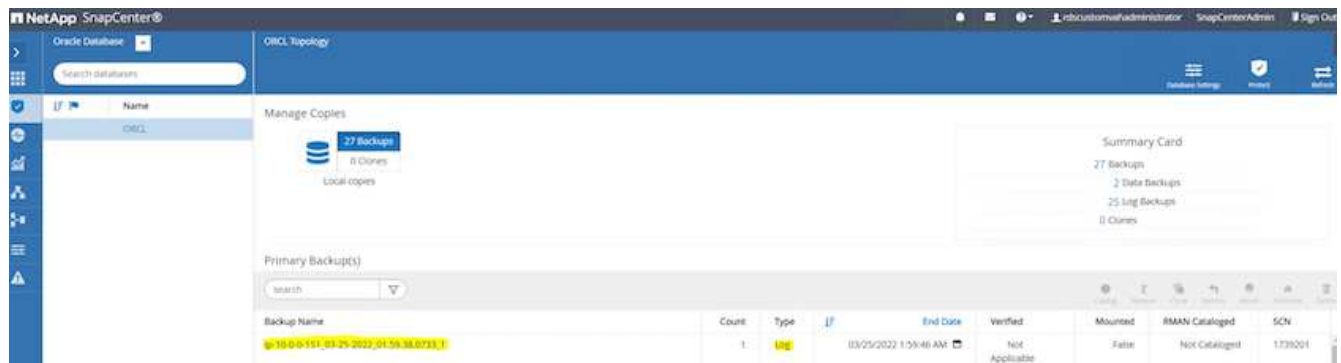
2. Klicken Sie auf den Namen der Backup-Ressource protokollieren und klicken Sie dann auf das Symbol Jetzt sichern, um eine zusätzliche Sicherung für Archivprotokolle zu starten.



3. Klicken Sie auf Backup und bestätigen Sie dann das Backup, um eine Archiv-Log-Sicherung zu starten.



Öffnen Sie in der Ansicht „Ressource“ für die Datenbank die Seite „verwaltete Backupkopien für die Datenbank“, um zu überprüfen, ob die Sicherungskopie für das einmalige Archivprotokoll erfolgreich abgeschlossen wurde. Ein Backup des Archivprotokolls erstellt einen Snapshot für das Protokollvolumen.



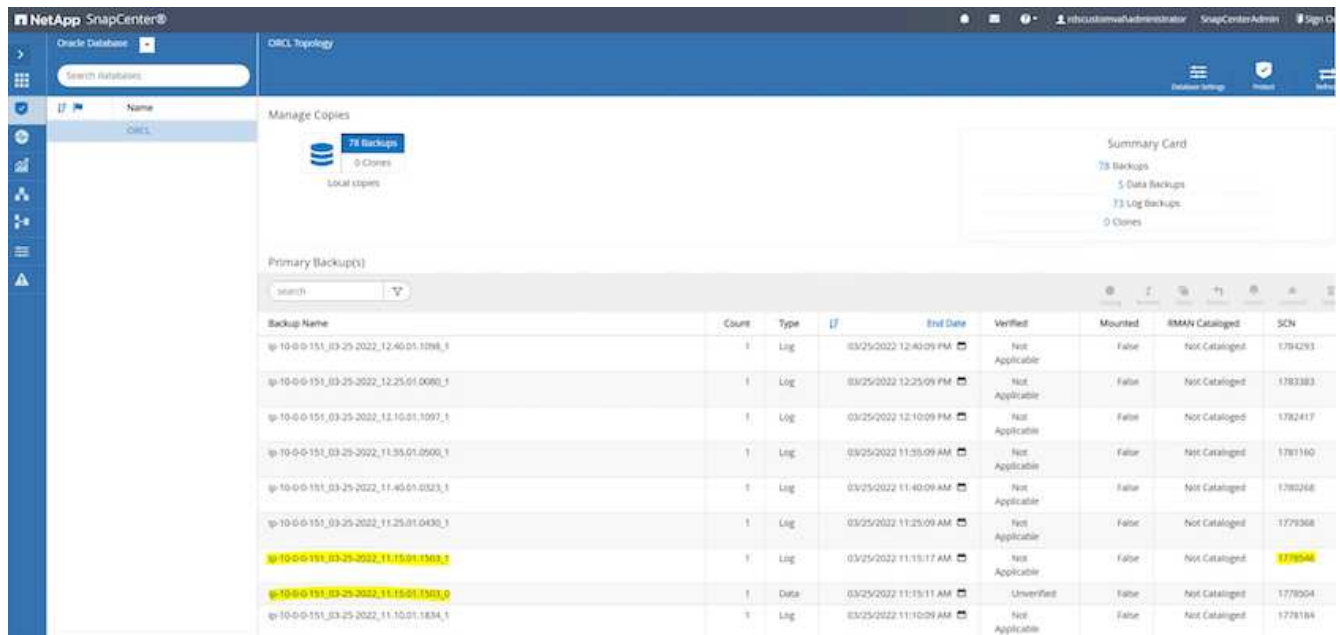
Wiederherstellung zu einem bestimmten Zeitpunkt

Eine zeitpunktgenaue SnapCenter Wiederherstellung wird auf demselben EC2 Instanzhost ausgeführt. Führen Sie die folgenden Schritte aus, um die Wiederherstellung durchzuführen:

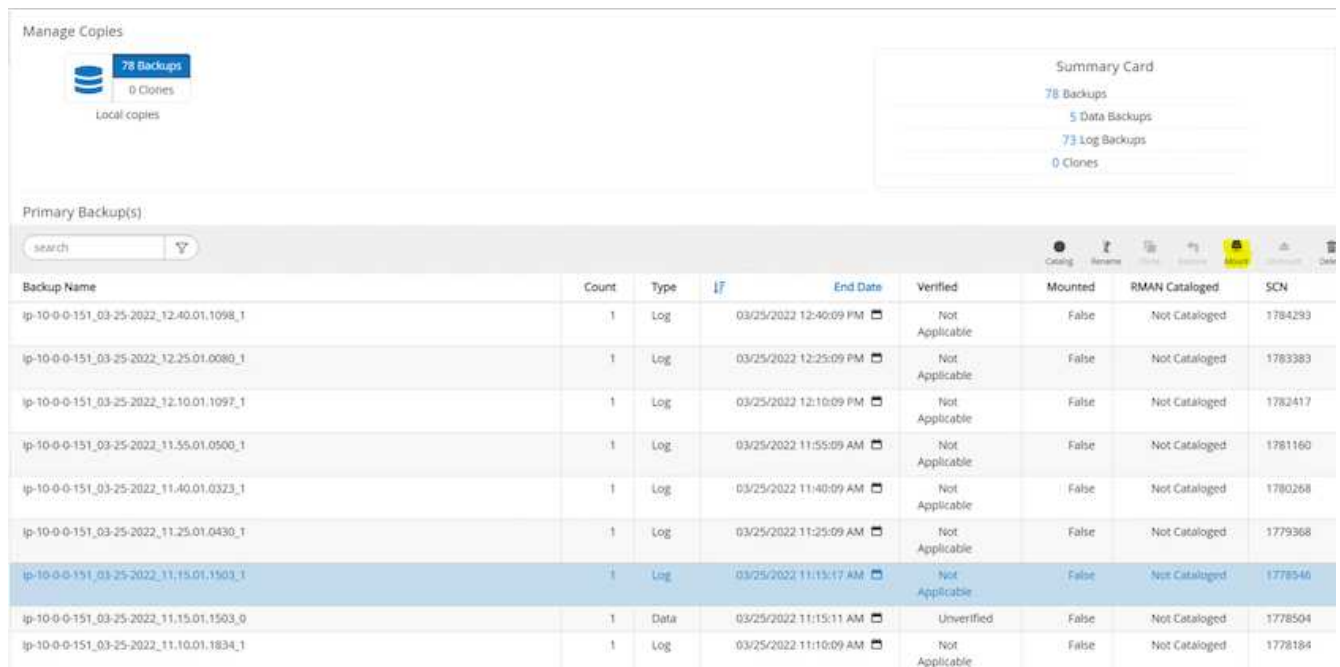
1. Klicken Sie auf der Registerkarte SnapCenter-Ressourcen > Datenbank auf den Datenbanknamen, um das Datenbank-Backup zu öffnen.



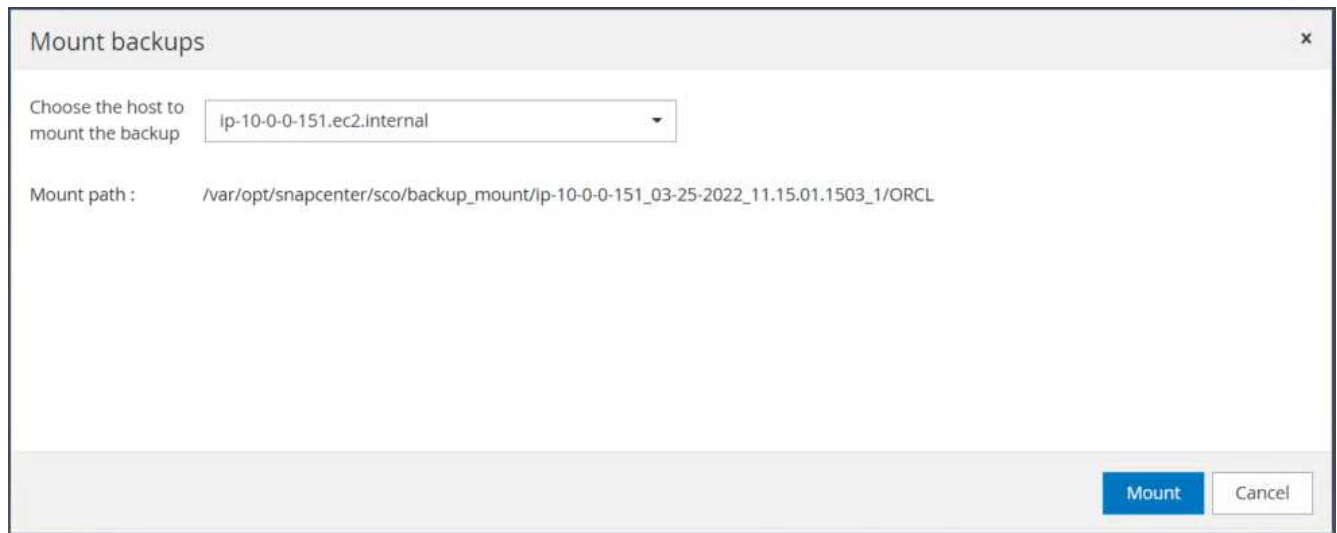
2. Wählen Sie die Datenbank-Backup-Kopie und den gewünschten Zeitpunkt für die Wiederherstellung aus. Markieren Sie auch die entsprechende SCN-Nummer für den Point-in-Time. Die Point-in-Time-Wiederherstellung kann entweder mit der Zeit oder mit dem SCN durchgeführt werden.



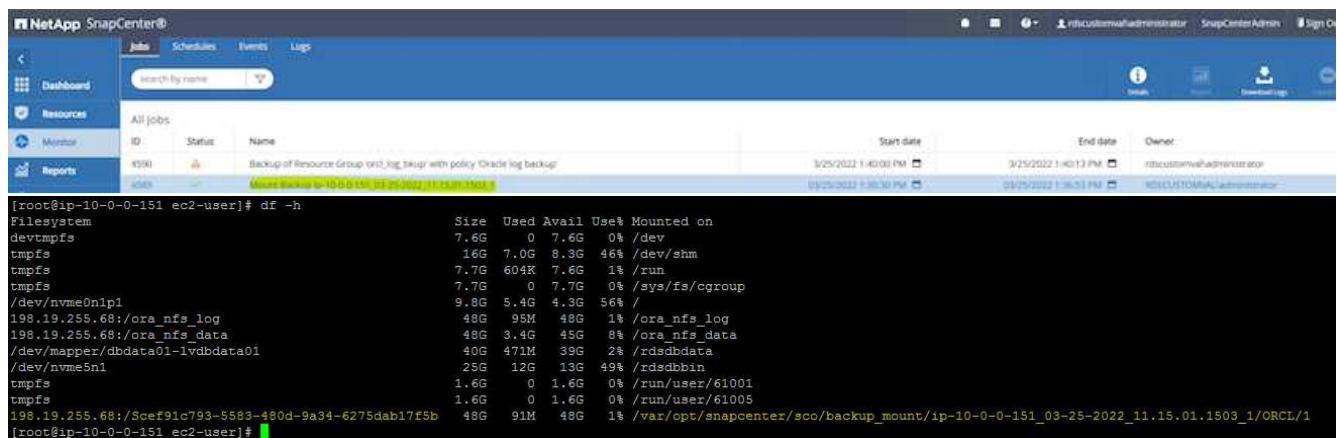
3. Markieren Sie den Snapshot des Protokollvolumens, und klicken Sie auf die Schaltfläche Mount, um das Volume zu mounten.



4. Wählen Sie die primäre EC2-Instanz, um das Protokoll-Volumen zu mounten.



5. Vergewissern Sie sich, dass der Mount-Job erfolgreich abgeschlossen wurde. Überprüfen Sie auch auf dem EC2 Instance-Host, um das gemountete Protokoll-Volumen und auch den Mount Point-Pfad zu sehen.



6. Kopieren Sie die Archivprotokolle vom gemounteten Protokollvolumen in das aktuelle Archivprotokollverzeichnis.

```
[ec2-user@ip-10-0-0-151 ~]$ cp /var/opt/snapcenter/sco/backup_mount/ip-10-0-0-151_03-25-2022_11.15.01.1503_1/ORCL/1/db/ORCL_A/arch/*.arc /ora_nfs_log/db/ORCL_A/arch/
```

7. Kehren Sie zur Registerkarte SnapCenter-Ressourcen > Seite Datenbank-Backup zurück, markieren Sie die Daten-Snapshot-Kopie und klicken Sie auf die Schaltfläche Wiederherstellen, um den Workflow zur Datenbankwiederherstellung zu starten.

Manage Copies

80 Backups

0 Clones

Local copies

Summary Card

80 Backups

5 Data Backups

75 Log Backups

0 Clones

Primary Backup(s)

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
lp-10-0-0-151_03-25-2022_12.10.01.1097_1	1	Log	03/25/2022 12:10:09 PM	Not Applicable	False	Not Cataloged	1782417
lp-10-0-0-151_03-25-2022_11.55.01.0500_1	1	Log	03/25/2022 11:55:09 AM	Not Applicable	False	Not Cataloged	1781160
lp-10-0-0-151_03-25-2022_11.40.01.0323_1	1	Log	03/25/2022 11:40:09 AM	Not Applicable	False	Not Cataloged	1780268
lp-10-0-0-151_03-25-2022_11.25.01.0430_1	1	Log	03/25/2022 11:25:09 AM	Not Applicable	False	Not Cataloged	1779368
lp-10-0-0-151_03-25-2022_11.15.01.1503_1	1	Log	03/25/2022 11:15:17 AM	Not Applicable	True	Not Cataloged	1778546
lp-10-0-0-151_03-25-2022_11.15.01.1503_0	1	Data	03/25/2022 11:15:11 AM	Unverified	False	Not Cataloged	1778504
lp-10-0-0-151_03-25-2022_11.10.01.1834_1	1	Log	03/25/2022 11:10:09 AM	Not Applicable	False	Not Cataloged	1778184

8. Überprüfen Sie „Alle Datendateien“ und „Datenbankstatus ändern, falls erforderlich für Restore und Recovery“, und klicken Sie auf Weiter.

Restore ORCL

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary

Restore Scope ⓘ

All Datafiles

Tablespaces

Control files

Database State

Change database state if needed for restore and recovery

Restore Mode ⓘ

Force in place restore

If this check box is not selected and if any of the in place restore criteria is not met, restore will be performed using the connect and copy method. The connect and copy restore method might take time based on the files being restored.

Previous Next

9. Wählen Sie einen gewünschten Wiederherstellungsumfang mit SCN oder Time aus. Statt die gemounteten Archivprotokolle wie in Schritt 6 gezeigt in das aktuelle Logverzeichnis zu kopieren, kann der gemountete Archiv-Log-Pfad in "Geben Sie externe Archiv-Log-Dateien Speicherorte" zur Wiederherstellung aufgelistet werden.

Restore ORCL

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Choose Recovery Scope

All Logs

Until SCN (System Change Number)

SCN

Date and Time

No recovery

Specify external archive log files locations

Previous Next

10. Geben Sie bei Bedarf ein optionales Preskript an.

Restore ORCL x

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Specify optional scripts to run before performing a restore job ⓘ

Prescript full path

Arguments

Script timeout

11. Geben Sie ggf. ein optionales Nachskript an, das ausgeführt werden soll. Überprüfen Sie die geöffnete Datenbank nach der Wiederherstellung.

Restore ORCL x

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps**
- 5 Notification
- 6 Summary

Specify optional scripts to run after performing a restore job ⓘ

Postscript full path

Arguments

Open the database or container database in READ-WRITE mode after recovery

12. Geben Sie einen SMTP-Server und eine E-Mail-Adresse an, wenn eine Jobbenachrichtigung erforderlich ist.

Restore ORCL x

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification**
- 6 Summary

Provide email settings ⓘ

Email preference:

From:

To:

Subject:

Attach job report

13. Stellen Sie die Jobübersicht wieder her. Klicken Sie auf Fertig stellen, um den Wiederherstellungsauftrag zu starten.

Restore ORCL
✕

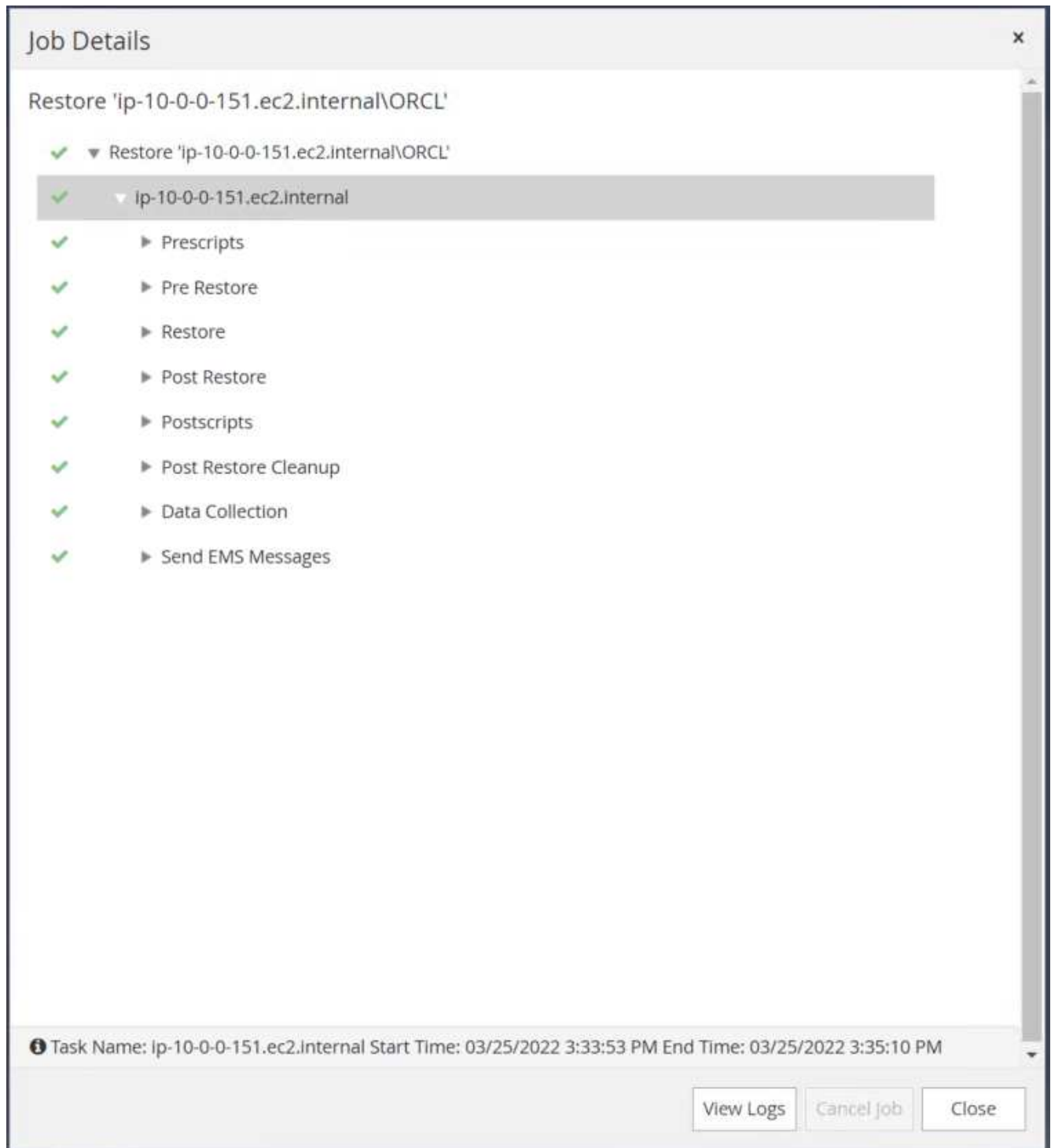
- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary

Summary

Backup name	ip-10-0-0-151_03-25-2022_11.15.01.1503_0
Backup date	03/25/2022 11:15:11 AM
Restore scope	All DataFiles
Recovery scope	Until SCN 1778546
Auxiliary destination	
Options	Change database state if necessary , Open the database or container database in READ-WRITE mode after recovery
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

Previous
Finish

14. Validieren Sie die Wiederherstellung aus SnapCenter.



15. Validieren Sie die Wiederherstellung über den EC2 Instance Host.

```

-bash-4.2$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Mar 25 15:44:08 2022
Version 19.8.0.0.0

Copyright (c) 1982, 2020, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL> select name, RESETLOGS_CHANGE#, RESETLOGS_TIME, open_mode from v$database;

NAME          RESETLOGS_CHANGE# RESETLOGS_TIME OPEN_MODE
-----
ORCL          1778547 25-MAR-22 READ WRITE

SQL>

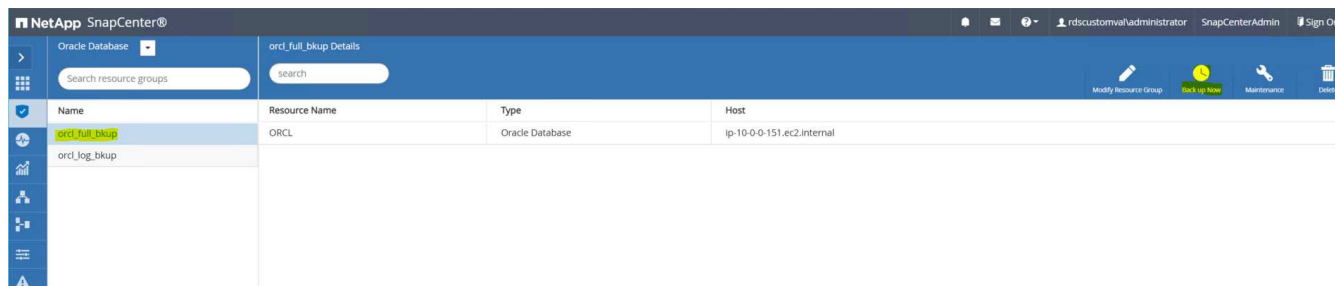
```

16. Um die Bereitstellung des Wiederherstellungsprotokollvolumens aufzuheben, kehren Sie die Schritte in Schritt 4 um.

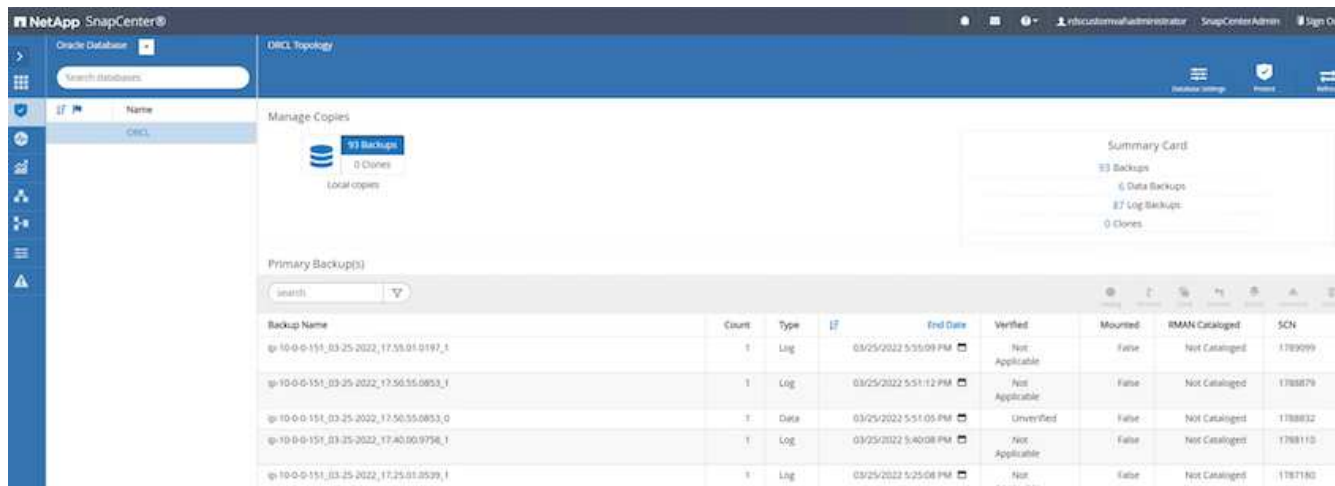
Erstellen eines Datenbankklons

Der folgende Abschnitt zeigt, wie der Workflow für SnapCenter-Klone zum Erstellen eines Datenbankklons aus einer primären Datenbank auf eine Standby-EC2-Instanz verwendet wird.

1. Erstellen Sie mit der vollständigen Backup-Ressourcengruppe ein vollständiges Snapshot-Backup der primären Datenbank von SnapCenter.



2. Öffnen Sie auf der Registerkarte SnapCenter-Ressource > Datenbank die Seite Datenbank-Backup-Verwaltung für die primäre Datenbank, aus der das Replikat erstellt werden soll.



3. Mounten Sie den in Schritt 4 erstellte Protokoll-Volume-Snapshot zum Standby-EC2-Instanz-Host.

The screenshot displays the OCI console interface for managing backups. At the top, there's a 'Manage Copies' section with a '95 Backups' indicator and '0 Clones' under 'Local copies'. A 'Summary Card' on the right shows '95 Backups', '6 Data Backups', '89 Log Backups', and '0 Clones'. Below this is a table of 'Primary Backup(s)' with columns for Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. One backup is highlighted in blue.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ip-10-0-0-151_03-25-2022_18.55.01.0309_1	1	Log	03/25/2022 6:55:09 PM	Not Applicable	False	Not Cataloged	1892563
ip-10-0-0-151_03-25-2022_18.40.00.9602_1	1	Log	03/25/2022 6:40:23 PM	Not Applicable	False	Not Cataloged	1891375
ip-10-0-0-151_03-25-2022_17.55.01.0197_1	1	Log	03/25/2022 5:55:09 PM	Not Applicable	False	Not Cataloged	1789099
ip-10-0-0-151_03-25-2022_17.50.55.0853_1	1	Log	03/25/2022 5:51:12 PM	Not Applicable	False	Not Cataloged	1788679
ip-10-0-0-151_03-25-2022_17.50.55.0853_0	1	Data	03/25/2022 5:51:05 PM	Unverified	False	Not Cataloged	1788832
ip-10-0-0-151_03-25-2022_17.40.00.9758_1	1	Log	03/25/2022 5:40:08 PM	Not	False	Not Cataloged	1788110

Below the table, a 'Mount backups' dialog box is open. It prompts the user to 'Choose the host to mount the backup' with a dropdown menu showing 'ip-10-0-0-47.ec2.internal'. The 'Mount path' is displayed as '/var/opt/snapcenter/sco/backup_mount/ip-10-0-0-151_03-25-2022_17.50.55.0853_1/ORCL'. At the bottom right of the dialog are 'Mount' and 'Cancel' buttons.

4. Markieren Sie die für das Replikat zu klonenden Snapshot Kopie und klicken Sie auf die Schaltfläche Klonen, um das Klonverfahren zu starten.

ORCL Topology

Database Settings Protect Refresh

Manage Copies

93 Backups
0 Clones
Local copies

Summary Card

93 Backups
6 Data Backups
87 Log Backups
0 Clones

Primary Backup(s)

search

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
ip-10-0-0-151_03-25-2022_17:55:01.0197_1	1	Log		03/25/2022 5:55:09 PM	Not Applicable	False	Not Cataloged	1789099
ip-10-0-0-151_03-25-2022_17:50:55.0853_1	1	Log		03/25/2022 5:51:12 PM	Not Applicable	False	Not Cataloged	1788879
ip-10-0-0-151_03-25-2022_17:50:55.0853_0	1	Data		03/25/2022 5:51:03 PM	Unverified	False	Not Cataloged	1788832
ip-10-0-0-151_03-25-2022_17:40:00.9758_1	1	Log		03/25/2022 5:40:08 PM	Not Applicable	False	Not Cataloged	1788110
ip-10-0-0-151_03-25-2022_17:25:01.0539_1	1	Log		03/25/2022 5:25:08 PM	Not Applicable	False	Not Cataloged	1787180

- Ändern Sie den Namen der Replikatkopie, damit sie sich vom Namen der primären Datenbank unterscheidet. Klicken Sie Auf Weiter.

Clone from ORCL

1 Name

Provide clone database SID

Clone SID

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Previous Next

- Ändern Sie den Klon-Host auf den Standby-EC2-Host, akzeptieren Sie die Standardbenennung und

klicken Sie auf Weiter.

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Select the host to create a clone

Clone host: ip-10-0-0-47.ec2.internal

Datafile locations ⓘ

/ora_nfs_data_ORCLREAD [Reset]

Control files ⓘ

/ora_nfs_data_ORCLREAD/ORCLREAD/control/control01.ctl [Reset]

Redo logs ⓘ

Group	Size	Unit	Number of files
RedoGroup 1	128	MB	1
/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo04.log [Reset]			
RedoGroup 2	128	MB	1

[Previous] [Next]

7. Ändern Sie Ihre Oracle-Starteinstellungen auf die für den Oracle-Zielservers-Host konfigurierten Einstellungen, und klicken Sie auf Weiter.

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user: None + i

Database port: 1521

Oracle Home Settings i

Oracle Home: /rdsdbbin/oracle

Oracle OS User: rdsdb

Oracle OS Group: database

Previous Next

8. Geben Sie einen Wiederherstellungspunkt mit entweder Time oder dem SCN und dem angehängten Archivprotokollpfad an.

Clone from ORCL
✕

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Recover Database

Until Cancel i

Date and Time i

i

Date-time format: MM/DD/YYYY hh:mm:ss

Until SCN (System Change Number)

Specify external archive log locations i

Create new DBID i
 Create tempfile for temporary tablespace i
 Enter SQL queries to apply when clone is created i
 Enter scripts to run after clone operation i

Previous

Next

9. Senden Sie bei Bedarf die SMTP-E-Mail-Einstellungen.

305

Clone from ORCL x

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Provide email settings i

Email preference Never

From From email

To Email to

Subject Notification

Attach job report

Previous Next

10. Klonen Sie die Jobübersicht, und klicken Sie auf Fertig stellen, um den Klonauftrag zu starten.

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

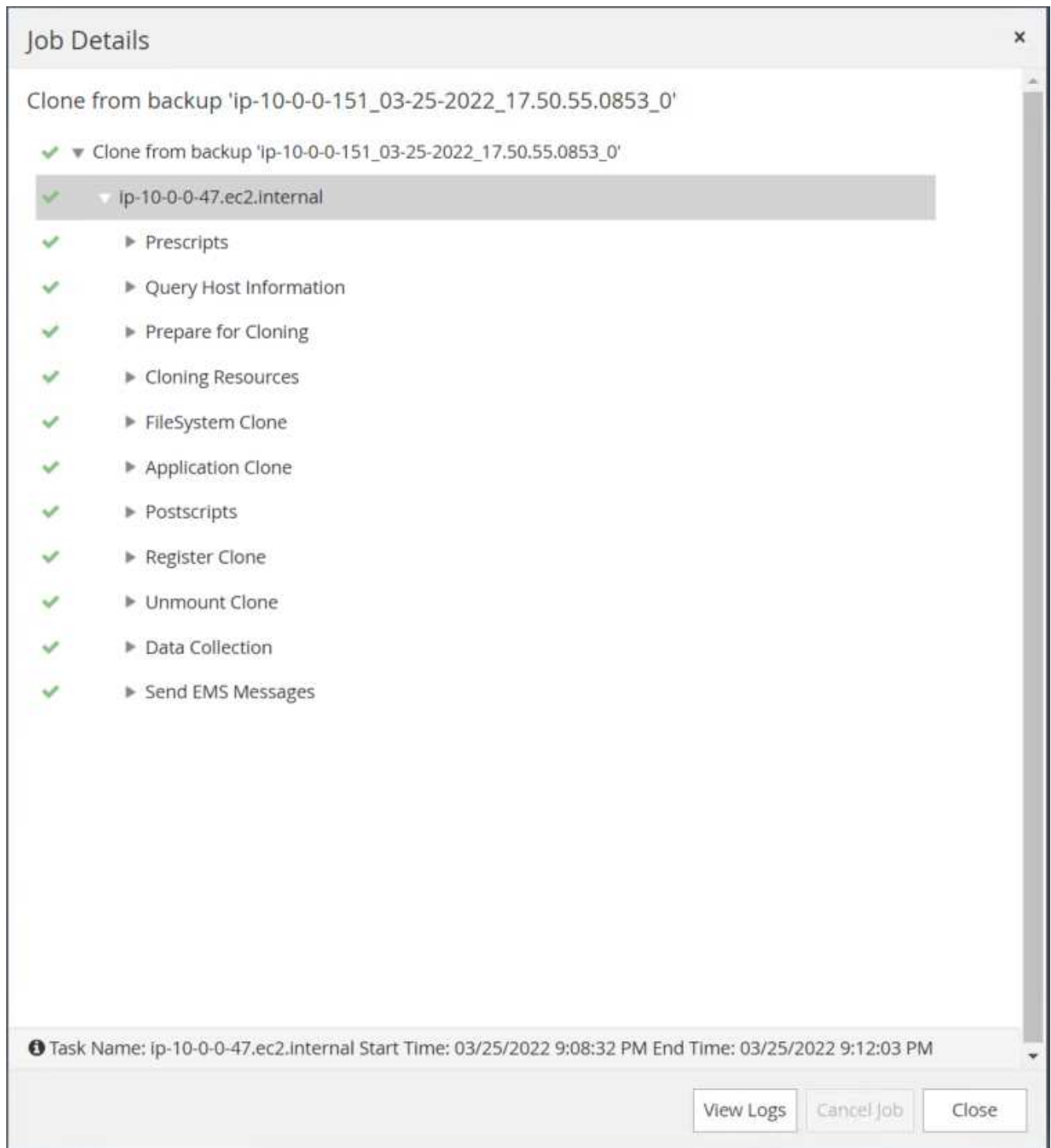
7 Summary

Summary

Clone from backup	ip-10-0-0-151_03-25-2022_17:50:55.0853_0
Clone SID	ORCLREAD
Clone server	ip-10-0-0-47.ec2.internal
Oracle home	/rdsdbbin/oracle
Oracle OS user	rdsdb
Oracle OS group	database
Datafile mountpaths	/ora_nfs_data_ORCLREAD
Control files	/ora_nfs_data_ORCLREAD/ORCLREAD/control/control01.ctl
Redo groups	RedoGroup =1 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo04.log RedoGroup =2 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo03.log RedoGroup =3 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo02.log RedoGroup =4 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo01.log
Recovery scope	Until SCN 1788879
Prescript full path	none
Prescript arguments	
Postscript full path	none
Postscript arguments	
Send email	No

Previous Finish

11. Überprüfen Sie das Klon-Jobprotokoll, indem Sie das Klon-Jobprotokoll überprüfen.



Die geklonte Datenbank ist sofort in SnapCenter registriert.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
ORCL	Single Instance	ip-10-0-0-151.ec2.internal	orcl_full_backup orcl_log_backup	Oracle full backup Oracle log backup	03/25/2022 9:10:09 PM	Backup succeeded
ORCLREAD	Single Instance	ip-10-0-0-47.ec2.internal				Not protected

12. Deaktivieren Sie den Oracle Archivprotokollmodus. Melden Sie sich als oracle-Benutzer bei der EC2-Instanz an und führen Sie den folgenden Befehl aus:

```
sqlplus / as sysdba
```

```
shutdown immediate;
```

```
startup mount;
```

```
alter database noarchivelog;
```

```
alter database open;
```



Anstelle primärer Oracle Backup-Kopien kann ein Klon auch aus replizierten sekundären Backup-Kopien auf dem FSX Ziel-Cluster erstellt werden. Dies gilt gleichermaßen.

HA-Failover auf Standby und Resynchronisierung

Der Standby Oracle HA Cluster bietet Hochverfügbarkeit bei einem Ausfall am primären Standort, entweder in der Rechenschicht oder auf der Storage-Ebene. Ein wesentlicher Vorteil der Lösung besteht darin, dass Anwender die Infrastruktur jederzeit und beliebig oft testen und validieren können. Failover kann vom Benutzer simuliert oder durch wirklichen Ausfall ausgelöst werden. Die Failover-Prozesse sind identisch und können für ein schnelles Applikations-Recovery automatisiert werden.

Siehe folgende Liste der Failover-Verfahren:

1. Führen Sie bei einem simulierten Failover ein Protokoll-Snapshot-Backup aus, um die neuesten Transaktionen auf den Standby-Standort zu leeren, wie im Abschnitt dargestellt [Erstellen eines Snapshot für Archivprotokolle](#). Bei einem durch einen tatsächlichen Ausfall ausgelösten Failover werden die letzten wiederherstellbaren Daten auf den Standby-Standort repliziert, wobei das letzte erfolgreiche Backup des geplanten Protokoll-Volumes erfolgt.
2. SnapMirror zwischen primärem und Standby FSX-Cluster unterbrechen
3. Mounten Sie die replizierten Standby-Datenbank-Volumes auf dem Standby-EC2 Instance-Host.
4. Verknüpfen Sie die Oracle-Binärdatei neu, wenn die replizierte Oracle-Binärdatei für die Oracle-Wiederherstellung verwendet wird.
5. Stellen Sie die Standby-Oracle-Datenbank auf das letzte verfügbare Archivprotokoll wieder her.
6. Öffnen Sie die Standby-Oracle-Datenbank für den Anwendungs- und Benutzerzugriff.
7. Bei einem tatsächlichen Ausfall des primären Standorts übernimmt die Standby-Oracle-Datenbank nun die Rolle des neuen primären Standorts und Datenbank-Volumes können dazu verwendet werden, den ausgefallenen primären Standort als neuen Standby-Standort mit der Reverse SnapMirror Methode wiederherzustellen.

8. Wenn ein simulierter Ausfall des primären Standorts im Rahmen des Tests oder der Validierung auftritt, fahren Sie nach Abschluss der Testdurchführung die Standby-Oracle-Datenbank herunter. Heben Sie dann die Standby-Datenbank-Volumes vom Standby-EC2-Instance-Host auf und synchronisieren Sie die Replikation vom primären Standort zum Standby-Standort neu.

Diese Verfahren können mit dem NetApp Automation Toolkit durchgeführt werden, das auf der öffentlichen NetApp GitHub Website heruntergeladen werden kann.

```
git clone https://github.com/NetApp-  
Automation/na_ora_hadr_failover_resync.git
```

Lesen Sie die README-Anweisung sorgfältig, bevor Sie die Einrichtung und Failover-Tests durchführen.

Datenbankmigration von lokalen Systemen in die Public Cloud

Die Migration der Datenbank stellt auf jeden Fall eine Herausforderung dar. Die Migration einer Oracle Datenbank von On-Premises-Systemen in die Cloud ist keine Ausnahme.

In den folgenden Abschnitten werden die wichtigsten Faktoren aufgeführt, die Sie bei der Migration von Oracle Datenbanken in die AWS Public Cloud mit AWS EC2 Computing- und FSX Storage-Plattform berücksichtigen sollten.

ONTAP Storage ist vor Ort verfügbar

Wenn die lokale Oracle Datenbank sich auf einem ONTAP Storage Array befindet, lässt sich die Replizierung für die Datenbankmigration dank der in AWS FSX ONTAP Storage integrierten NetApp SnapMirror Technologie einfacher einrichten. Der Migrationsprozess kann über die NetApp BlueXP Konsole orchestriert werden.

1. Erstellung einer EC2 Ziel-Computing-Instanz, die zur lokalen Instanz passt
2. Stellen Sie passende Datenbank-Volumes gleicher Größe über die FSX-Konsole bereit.
3. Mounten Sie die FSX-Datenbank-Volumes in die EC2-Instanz.
4. Einrichten der SnapMirror Replizierung zwischen den lokalen Datenbank-Volumes und den FSX Ziel-Datenbank-Volumes Die erste Synchronisierung benötigt möglicherweise etwas Zeit, um die primären Quelldaten zu verschieben, aber die folgenden inkrementellen Updates sind viel schneller.
5. Beenden Sie zum Zeitpunkt der Umschaltung die primäre Applikation, um alle Transaktionen zu beenden. Führen Sie über die Oracle sqlplus CLI-Schnittstelle einen Oracle Online-Protokollschalter aus und erlauben Sie SnapMirror Sync, das letzte archivierte Protokoll auf das Ziel-Volume zu übertragen.
6. Untergliedern Sie die gespiegelten Volumes, führen Sie Oracle Recovery am Ziel aus und bringen Sie die Datenbank für den Service auf.
7. Weisen Sie Applikationen auf die Oracle Datenbank in der Cloud zu.

Im folgenden Video wird gezeigt, wie eine Oracle Datenbank mithilfe der NetApp BlueXP Konsole und SnapMirror Replizierung von On-Premises zu AWS FSX/EC2 migriert wird.

[Migrieren Sie lokale Oracle DB zu AWS](#)

ONTAP Storage ist vor Ort nicht verfügbar

Wenn die lokale Oracle Datenbank auf Storage anderer Anbieter als ONTAP gehostet wird, basiert die Datenbankmigration auf dem Restore einer Backup-Kopie einer Oracle Datenbank. Sie müssen das

Archivprotokoll wiedergeben, um es vor dem Umschalten aktuell zu machen.

AWS S3 kann als Staging-Storage-Bereich für das Verschieben und Migrieren von Datenbanken verwendet werden. Für diese Methode sind die folgenden übergeordneten Schritte zu beachten:

1. Bereitstellung einer neuen, übereinstimmenden EC2 Instanz, die mit der lokalen Instanz vergleichbar ist
2. Stellen Sie gleich große Datenbank-Volumes vom FSX Storage bereit und mounten Sie die Volumes auf die EC2 Instanz.
3. Erstellen einer Oracle Backup-Kopie auf Festplattenebene
4. Die Backup-Kopie kann in AWS S3 Storage verschoben werden.
5. Stellen Sie die Oracle-Kontrolldatei wieder her und stellen Sie die Datenbank wieder her, indem Sie Daten und das Archivprotokoll aus dem S3-Storage ziehen.
6. Synchronisieren der Oracle Zieldatenbank mit der lokalen Quelldatenbank
7. Fahren Sie beim Switchover die Applikation und die Oracle Quelldatenbank herunter. Kopieren Sie die letzten paar Archivprotokolle und wenden Sie sie auf die Oracle Zieldatenbank an, um sie auf den neuesten Stand zu bringen.
8. Starten Sie die Zieldatenbank für den Benutzerzugriff.
9. Umleiten der Applikation zur Zieldatenbank, um die Umschaltung abzuschließen.

Migrieren Sie lokale Oracle Datenbanken mithilfe von PDB-Verschiebungen mit maximaler Verfügbarkeit zu AWS FSX/EC2

Dieser Migrationsansatz eignet sich am besten für Oracle Datenbanken, die bereits im mandantenfähigen PDB/CDB-Modell implementiert sind. ONTAP-Storage steht vor Ort nicht zur Verfügung. Bei der Methode zur Verschiebung der PDB wird mithilfe der Oracle PDB-Technologie Hot-Clone-Datenbanken zwischen einer Quell-CDB und einer Ziel-CDB verschoben. Gleichzeitig werden Serviceunterbrechungen minimiert.

Erstellen Sie zunächst CDB in der AWS FSX/EC2 mit ausreichend Storage, um PDBs zu hosten und von lokalen Standorten aus zu migrieren. Mehrere on-Premises-PDBs können nacheinander umgezogen werden.

1. Wenn die lokale Datenbank in einer einzelnen Instanz statt im mandantenfähigen PDB/CDB-Modell implementiert wird, befolgen Sie die Anweisungen in ["Konvertieren einer einzelnen nicht-CDB-Instanz in eine PDB in einer mandantenfähigen CDB"](#) Um die einzelne Instanz in mandantenfähige PDB/CDB zu konvertieren. Folgen Sie dann dem nächsten Schritt, um die konvertierte PDB zu CDB in AWS FSX/EC2 zu migrieren.
2. Wenn die lokale Datenbank bereits im mandantenfähigen PDB/CDB-Modell implementiert ist, befolgen Sie die Anweisungen in ["Migrieren Sie lokale Oracle-Datenbanken in die Cloud mit PDB-Verschiebung"](#) Für die Durchführung der Migration.

Im folgenden Video wird gezeigt, wie eine Oracle Database (PDB) mithilfe von PDB-Verschiebungen mit maximaler Verfügbarkeit auf FSX/EC2 migriert werden kann.

["Migrieren Sie die lokale Oracle PDB zu AWS CDB mit maximaler Verfügbarkeit"](#)



Obwohl die Anweisungen in Schritt 1 und 2 im Kontext der Public Cloud von Azure dargestellt werden, gelten die Verfahren für die AWS Cloud ohne Änderungen.

Das NetApp Solutions Automation Team bietet ein Migrations-Toolkit, das die Migration von Oracle Datenbanken vor Ort in die AWS Cloud erleichtert. Verwenden Sie den folgenden Befehl, um das Oracle Database Migration Toolkit für die PDB-Verschiebung herunterzuladen.

```
git clone https://github.com/NetApp-Automation/na_ora_aws_migration.git
```

Azure Cloud

TR-4990: Schnelle Wiederherstellung von Oracle VLDB mit Incremental Merge auf ANF

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Die Wiederherstellung einer sehr großen Datenbank (VLDB) in Oracle mit dem Backup-Tool Oracle Recovery Manager (RMAN) kann eine große Herausforderung darstellen. Der Datenbankwiederherstellungsprozess von Backup-Medien im Fehlerfall kann zeitaufwändig sein, wodurch die Datenbank-Recovery verzögert wird und möglicherweise Ihr Service Level Agreement (SLA) erheblich beeinträchtigt wird. Ab Version 10g hat Oracle jedoch eine RMAN-Funktion eingeführt, mit der Benutzer Kopien der Oracle-Datenbankdateien auf zusätzlichem Festplattenspeicher auf dem DB-Server-Host erstellen können. Diese Image-Kopien können mit RMAN täglich inkrementell aktualisiert werden. Bei einem Ausfall kann der Datenbankadministrator (DBA) die Oracle-Datenbank schnell von den fehlerhaften Medien auf die Image-Kopie umschalten, sodass keine vollständige Wiederherstellung der Datenbankmedien erforderlich ist. Das Ergebnis ist ein deutlich verbesserter SLA, der allerdings mit der Verdopplung des erforderlichen Datenbank-Storage verbunden ist.

Wenn Sie SLA für Ihre VLDB bevorzugen und die Migration der Oracle-Datenbank in eine Public Cloud wie Azure erwägen, können Sie eine ähnliche Datenbankschutzstruktur mit Ressourcen wie Microsoft Azure NetApp Files (ANF) für die Bereitstellung Ihrer Standby-Datenbankbildkopie einrichten. In dieser Dokumentation zeigen wir, wie ein NFS-Filesystem aus dem ANF-Kapazitätspool bereitgestellt und exportiert wird, um auf einem Oracle Datenbankserver gemountet zu werden und eine Standby-Datenbankkopie für eine schnelle Recovery bei einem Ausfall des Primärspeichers zu erstellen.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Eine inkrementelle Zusammenführung von Oracle VLDB-Image-Kopien über RMAN auf NFS-Mount-Punkt außerhalb des Microsoft ANF-Kapazitätspool-Speichers.
- Schnelle Recovery einer Oracle VLDB im Falle eines Fehlers auf derselben VM des Azure-Datenbankservers.
- Schnelle Recovery einer Oracle VLDB im Falle eines Ausfalls auf einer Standby-VM des Azure-Datenbankservers.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

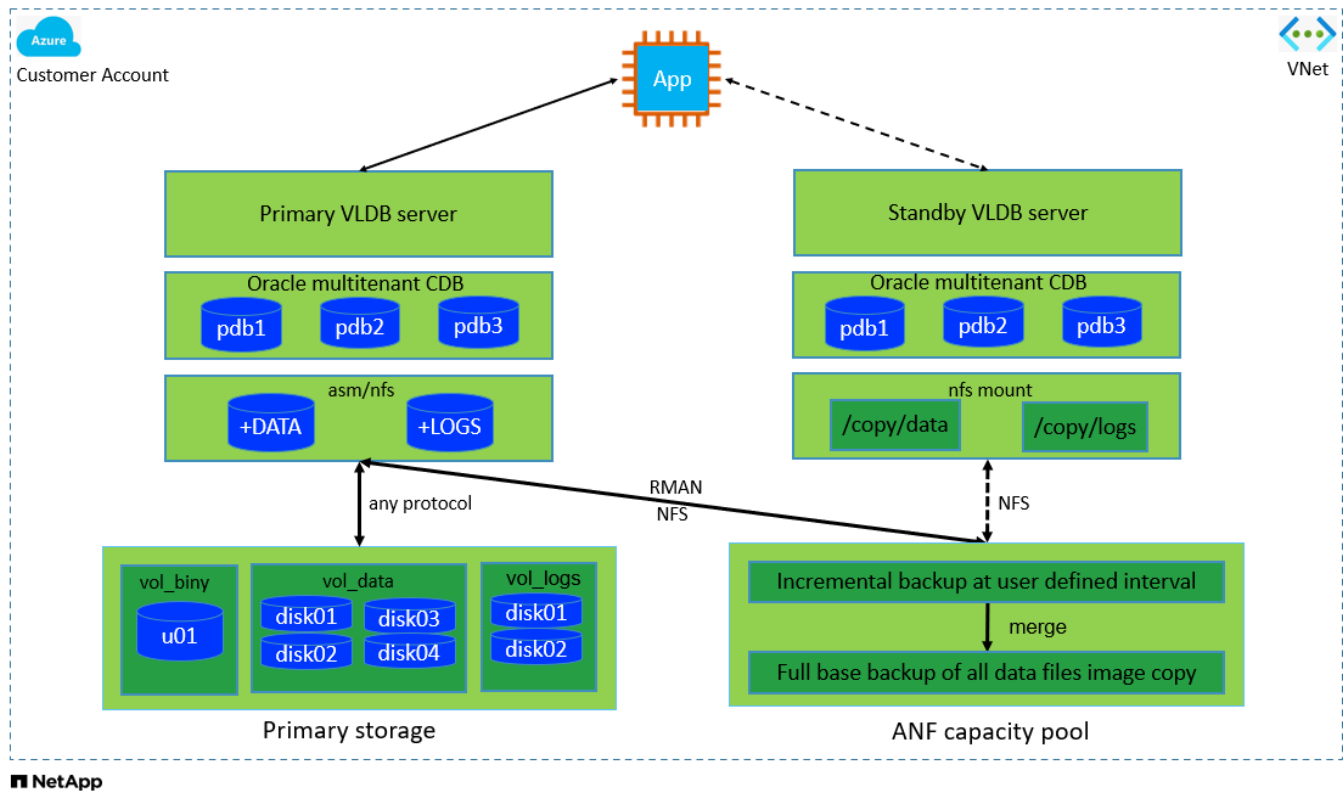
- Ein DBA, der die inkrementelle Zusammenführung von Oracle VLDB-Bildkopien über RMAN in Azure für eine schnellere Datenbankwiederherstellung eingerichtet hat.
- Ein Database Solution Architect, der Oracle-Workloads in der Azure Public Cloud testet.
- Ein Storage-Administrator, der Oracle-Datenbanken managt, die auf ANF-Kapazitäts-Pool-Storage bereitgestellt werden.
- Applikationseigentümer, die Oracle-Datenbanken in der Azure-Cloud-Umgebung einrichten möchten.

Test- und Validierungsumgebung der Lösung

Tests und Validierung dieser Lösung wurden in einem Microsoft ANF Kapazitäts-Pool-Storage und Azure VM Computing-Umgebungen durchgeführt, die möglicherweise nicht der endgültigen Implementierungsumgebung entsprechen. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind

Oracle VLDB Incremental Merge via RMAN on ANF



Hardware- und Softwarekomponenten

Hardware		
ANF-Lagerung	Aktuelle Version von Microsoft angeboten	2 tib ANF Kapazitäts-Pool-Storage mit Premium-Service-Level
Azure VM für DB-Server	Standard_B4ms – 4 vCPUs, 16 gib	2 VMs, eine als primärer DB-Server und die andere als Standby
Software		
Redhat Linux	RHEL Linux 8.6 (LVM) – x64 Gen2	Bereitstellung der RedHat Subscription für Tests
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip

NFS	Version 3.0	Oracle dNFS aktiviert
-----	-------------	-----------------------

Wichtige Faktoren für die Implementierung

- **Oracle VLDB Speicherlayout für RMAN Incremental Merge.** in unseren Tests und Validierungen wird das NFS-Volume für Oracle Incremental Backup and Merge aus einem einzigen ANF Kapazitätspool zugewiesen, der 100 tib pro Volume und 1000 tib Gesamtkapazitätslimit hat. Bei der Implementierung über die Schwellenwerte können mehrere Volumes und ANF-Kapazitäts-Pools parallel mit mehreren NFS-Mount-Punkten verkettet werden, um mehr Kapazität bereitzustellen.
- **Oracle Wiederherstellbarkeit mit RMAN Incremental Merge.** das inkrementelle RMAN Backup und Merge wird in der Regel in einer benutzerdefinierten Frequenz basierend auf Ihren RTO- und RPO-Zielen ausgeführt. Bei einem vollständigen Verlust des primären Storage und/oder archivierter Protokolle kann es zu Datenverlusten kommen. Die Oracle-Datenbank kann bis zum letzten inkrementellen Backup wiederhergestellt werden, das über die ANF-Datenbank-Backup-Image-Kopie verfügbar ist. Um Datenverluste zu minimieren, kann der Oracle Flash Recovery-Bereich auf dem ANF NFS-Bereitstellungspunkt eingerichtet werden. Archivierte Protokolle werden zusammen mit Datenbank-Image-Kopien auf dem ANF NFS-Mount gesichert.
- **Ausführung von Oracle VLDB auf ANF NFS-Dateisystem.** im Gegensatz zu anderen Massenspeichern für Datenbank-Backups ist Microsoft ANF ein Cloud-fähiger, produktionsfähiger Storage, der ein hohes Maß an Performance und Speichereffizienz bietet. Sobald Oracle VLDB vom Primär-Storage auf die Image-Kopie im ANF NFS-Dateisystem umschaltet, kann die Datenbank-Performance auf hohem Niveau aufrechterhalten werden, während der Ausfall des primären Speichers behoben wird. Sie können sicher sein, dass die Benutzererfahrung bei primären Storage-Ausfällen nicht beeinträchtigt wird.
- **Azure Compute-Instanzen.** in diesen Tests und Validierungen verwendeten wir Azure-VMs Standard_B4ms als Oracle-Datenbankserver. Es gibt noch andere Azure VMs, die möglicherweise optimiert werden und für Datenbank-Workloads besser geeignet sind. Außerdem müssen Sie die Größe der Azure VM entsprechend der Anzahl der vCPUs und der Menge des RAM anpassen, basierend auf den tatsächlichen Workload-Anforderungen.
- **ANF Kapazitäts-Pool-Service-Level.** ANF Kapazitäts-Pool bietet drei Service-Level: Standard, Premium, Ultra. Standardmäßig wird eine automatische QoS auf ein Volume angewendet, das innerhalb eines Kapazitäts-Pools erstellt wird und dadurch den Durchsatz auf das Volume einschränkt. Der Durchsatz auf einem Volume kann manuell basierend auf der Größe des Kapazitäts-Pools und Service Levels angepasst werden.
- **DNFS-Konfiguration.** dNFS ist in den Oracle-Kernel integriert und ist dafür bekannt, die Performance von Oracle-Datenbanken drastisch zu steigern, wenn Oracle auf NFS-Speicher bereitgestellt wird. DNFS ist in Oracle-Binärdatei verpackt, ist aber nicht standardmäßig aktiviert. Sie sollte für jede Oracle Database-Bereitstellung auf NFS aktiviert werden. Für die Bereitstellung mehrerer ANF-Kapazitätspools für eine VLDB sollten dNFS-Mehrpfade zu verschiedenen ANF-Kapazitätspools richtig konfiguriert werden.

Lösungsimplementierung

Es wird davon ausgegangen, dass Sie Ihre Oracle VLDB bereits in einer Azure Cloud-Umgebung innerhalb eines vnet implementiert haben. Wenn Sie Hilfe zur Oracle-Bereitstellung in Azure benötigen, lesen Sie bitte die folgenden technischen Berichte, um Hilfe zu erhalten.

- ["Vereinfachte, automatisierte Oracle-Implementierung auf Azure NetApp Files mit NFS"](#)
- ["Implementierung und Schutz von Oracle Datenbanken auf Azure NetApp Files"](#)

Ihre Oracle VLDB kann entweder auf einem ANF-Speicher oder einem beliebigen Speicher innerhalb des Azure-Cloud-Ecosystems ausgeführt werden. Im folgenden Abschnitt werden schrittweise Bereitstellungsverfahren zum Einrichten der inkrementellen Zusammenführung von RMAN mit einer Image-

Kopie einer Oracle VLDB beschrieben, die in einem NFS-Mount-Off-ANF-Speicher bereitgestellt wird.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wurde ein Azure-Konto eingerichtet und die erforderlichen Azure vnet- und Netzwerksegmente in Ihrem Azure-Konto erstellt.
2. Über die Azure-Portalkonsole müssen Sie zwei Azure VM-Instanzen implementieren, eine als primärer Oracle DB Server und einen optionalen Standby-DB-Server. Im Architekturdiagramm im vorherigen Abschnitt finden Sie weitere Details zum Umgebungs-Setup. Sehen Sie sich auch die an ["Azure Virtual Machine Serie"](#) Finden Sie weitere Informationen.
3. Implementieren Sie über die Azure-Portalkonsole ANF Storage, um die NFS-Volumes zu hosten, auf denen die Standby-Image-Kopie der Oracle Datenbank gespeichert ist. Wenn Sie mit der Bereitstellung von ANF nicht vertraut sind, lesen Sie die Dokumentation ["QuickStart: Azure NetApp Files einrichten und ein NFS-Volume erstellen"](#) Schritt-für-Schritt-Anleitungen.

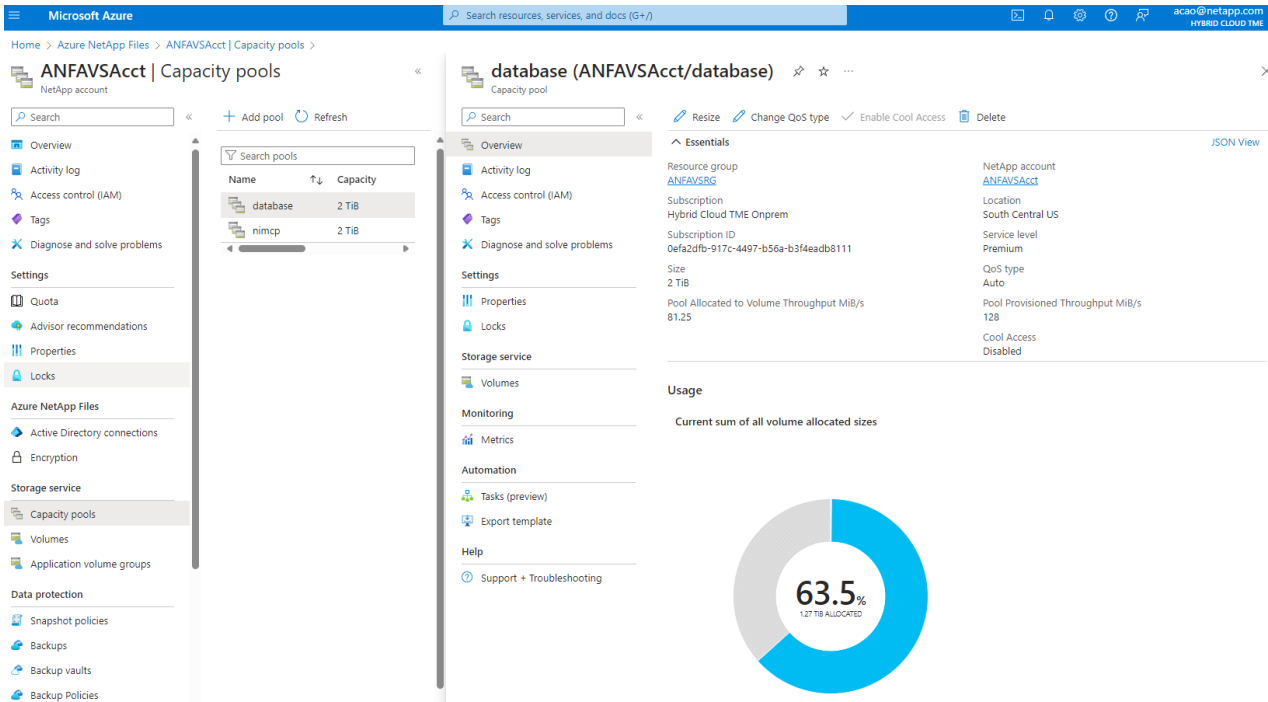


Stellen Sie sicher, dass Sie mindestens 128 G im Stammvolume der Azure VM zugewiesen haben, damit ausreichend Speicherplatz für das Stage von Oracle-Installationsdateien zur Verfügung steht.

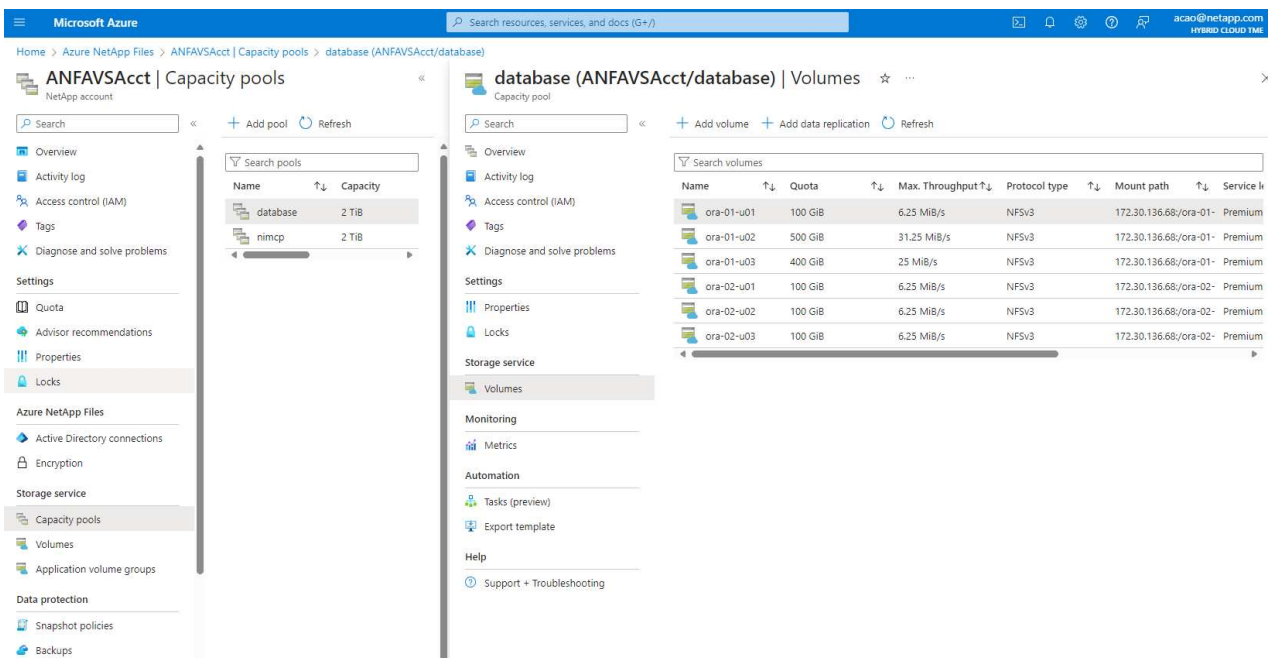
Bereitstellen und Exportieren des NFS-Volumes, das auf dem primären Oracle VLDB-Server gemountet werden soll

In diesem Abschnitt zeigen wir die Bereitstellung eines NFS-Volumens aus einem ANF-Kapazitätspool über die Azure-Portalkonsole. Wiederholen Sie die Verfahren für andere ANF-Kapazitätspools, wenn mehr als ein ANF-Kapazitätspool für die Größe der Datenbank eingerichtet ist.

1. Zunächst navigieren Sie über die Azure-Portalkonsole zum ANF-Kapazitätspool, der zum Stage von Oracle VLDB-Image-Kopien verwendet wird.



2. Aus ausgewähltem Kapazitäts-Pool - database`Klicken Sie auf `Volumes Und dann Add volume Zum Starten des Add-Volume-Workflows.



3. Ausfüllen Volume name, Quota, Virtual network, und Delegated subnet Zu bewegen Protocol Seite.

Create a volume ...

Basics Protocol Tags Review + create

This page will help you create an Azure NetApp Files volume in your subscription and enable you to access the volume from within your virtual network. [Learn more about Azure NetApp Files](#)

Volume details

Volume name *	<input type="text" value="ora-01-u02-copy"/> ✓
Available quota (GiB) ⓘ	<input type="text" value="748"/> 748 GiB
Quota (GiB) * ⓘ	<input type="text" value="500"/> ✓ 500 GiB
Available throughput (MiB/s) ⓘ	<input type="text" value="46.75"/>
Max. Throughput (MiB/s) ⓘ	<input type="text" value="31.25"/>
Enable Cool Access ⓘ	<input type="checkbox"/>
Coolness Period ⓘ	<input type="text" value="31"/>
Cool Access Retrieval Policy ⓘ	<input type="text" value="Default"/> ▼
Virtual network * ⓘ	<input type="text" value="ANFAVSVa1 (172.30.136.64/26,172.30.137.128/25,172.30.152.0/27)"/> ▼ Create new virtual network
Delegated subnet * ⓘ	<input type="text" value="ANF_Sub (172.30.136.64/26)"/> ▼ Create new subnet
Network features ⓘ	<input type="radio"/> Basic <input checked="" type="radio"/> Standard
Availability Zone ⓘ	<input type="text" value="None"/> ▼
Encryption key source ⓘ	<input type="text"/> ▼
Show advanced section	<input type="checkbox"/>

Review + create

< Previous

Next : Protocol >

- Notieren Sie sich den Dateipfad, geben Sie den zulässigen CIDR-Bereich für Clients ein, und aktivieren Sie `Root Access` Für das Volume.

Create a volume ...

Basics **Protocol** Tags Review + create

Configure access to your volume.

Access

Protocol type NFS SMB Dual-protocol

Configuration

File path *

Versions *

Kerberos Enabled Disabled

LDAP Enabled Disabled

Unix Permissions

Azure VMware Solution DataStore

Export policy


Configure the volume's export policy. This can be edited later. [Learn more](#)

<input type="checkbox"/>	Index	Allowed clients	Access	Root Access	Chown Mode
<input type="checkbox"/>	1	<input type="text" value="172.30.137.128/25,1"/>	<input type="text" value="Read & Write"/>	<input type="text" value="On"/>	<input type="text" value="Restricted"/>
		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>




5. Fügen Sie bei Bedarf ein Volume-Tag hinzu.

Create a volume ...

Basics Protocol **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#) 

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name 	Value 	
<input type="text" value="database"/>	:	<input type="text" value="oracle"/> 
<input type="text"/>	:	<input type="text"/>

Review + create

< Previous

Next : Review + create >

6. Volume prüfen und erstellen.

Create a volume ...

✓ Validation passed

Basics Protocol Tags Review + create

Basics

Subscription	Hybrid Cloud TME Onprem
Resource group	ANFAVSRG
Region	South Central US
Volume name	ora-01-u02-copy
Capacity pool	database
Service level	Premium
Quota	500 GiB
Encryption key source	None
Availability Zone	None

Networking

Virtual network	ANFAVSVAl (172.30.136.64/26,172.30.137.128/25,172.30.152.0/27)
Delegated subnet	ANF_Sub (172.30.136.64/26)
Network features	Standard

Protocol

Protocol	NFSv3
File path	ora-01-u02-copy
Unix Permissions	0770

Tags

database	oracle
----------	--------

Create

< Previous

Next >

[Download a template for automation](#)

7. Melden Sie sich beim primären Oracle VLDB-Server als Benutzer mit Sudo-Berechtigung an und mounten Sie das aus ANF-Speicher exportierte NFS-Volume. Ändern Sie bei Bedarf die IP-Adresse und den Dateipfad des ANF NFS-Servers. Die IP-Adresse des ANF NFS-Servers kann von der ANF Volume-Konsoleseite abgerufen werden.

```
sudo mkdir /nfsanf
```

```
sudo mount 172.30.136.68:/ora-01-u02-copy /nfsanf -o  
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsiz=262144,wsiz=262144,noi  
tr
```

8. Ändern Sie Mount Point Ownership in oracle:oisntall, ändern Sie ggf. Ihren oracle-Benutzernamen und die primäre Gruppe.

```
sudo chown oracle:oinstall /nfsanf
```

Einrichtung der inkrementellen Zusammenführung von Oracle RMAN zu Image-Kopien auf ANF

RMAN Incremental Merge Aktualisieren Sie die Staging-Datenbank-Datendateien-Image-Kopie kontinuierlich bei jedem inkrementellen Backup/Merge-Intervall. Die Image-Kopie der Datenbanksicherung ist so aktuell wie die Häufigkeit, in der Sie die inkrementelle Sicherung/Zusammenführung durchführen. Berücksichtigen Sie also die Datenbankleistung, Ihre RTO- und RPO-Ziele bei der Entscheidung über die Häufigkeit der inkrementellen Backups und Merge von RMAN.

1. Melden Sie sich beim primären oracle VLDB-Server als oracle-Benutzer an.
2. Erstellen Sie ein oracopy-Verzeichnis unter Mount Point /nfsanf, um oracle Datendateien Image-Kopien und archlog-Verzeichnis für Oracle Flash Recovery-Bereich zu speichern.

```
mkdir /nfsanf/oracopy
```

```
mkdir /nfsanf/archlog
```

3. Melden Sie sich über sqlplus bei der Oracle Datenbank an, aktivieren Sie die Nachverfolgung von Blockänderungen für schnellere inkrementelle Backups und ändern Sie den Oracle Flash Recovery-Bereich in ANF NFS-Mount, wenn er sich derzeit im Primärspeicher befindet. Auf diese Weise können die RMAN-Standard-Steuerdatei/SPFile-Autobackups und archivierte Protokolle zum Recovery auf dem ANF-NFS-Mount gesichert werden.

```
sqlplus / as sysdba
```

Führen Sie an der Eingabeaufforderung sqlplus folgenden Befehl aus.

```
alter database enable block change tracking using file  
'/nfsanf/oracopy/bct_ntap1.ctf'
```

```
alter system set db_recovery_file_dest='/nfsanf/archlog/'  
scope=both;
```

Erwartete Ausgabe:


```
[oracle@ora-01 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Mar 20 16:44:21
2024
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> alter database enable block change tracking using file
'/nfsanf/oracopy/bct_ntap1.ctf';

Database altered.

SQL> alter system set db_recovery_file_dest='/nfsanf/archlog/'
scope=both;

System altered.

SQL>
```

4. Erstellen Sie ein RMAN-Backup und ein inkrementelles Merge-Skript. Das Skript weist mehrere Kanäle für die parallele Sicherung und Zusammenführung von RMAN zu. Bei der ersten Ausführung würde die erste vollständige Basisplan-Image-Kopie erzeugt. In einem vollständigen Durchlauf löscht es zunächst veraltete Backups, die sich außerhalb des Aufbewahrungsfensters befinden, um den Staging-Bereich sauber zu halten. Es schaltet dann die aktuelle Protokolldatei vor dem Zusammenführen und Sichern um. Das inkrementelle Backup folgt der Zusammenführung, sodass die Kopie des Datenbank-Images den aktuellen Datenbankstatus um einen Sicherungs-/Mergezyklus zurückverfolgt. Die Merge- und Backup-Reihenfolge kann rückgängig gemacht werden, um die Wiederherstellung nach Belieben des Benutzers zu beschleunigen. Das RMAN-Skript kann in ein einfaches Shell-Skript integriert werden, das von crontab auf dem primären DB-Server ausgeführt wird. Stellen Sie sicher, dass die automatische Sicherung der Steuerdatei in der RMAN-Einstellung aktiviert ist.

```
vi /home/oracle/rman_bkup_merge.cmd
```

Add following lines:

```
RUN
```

```
{  
  allocate channel c1 device type disk format '/nfsanf/oracopy/%U';  
  allocate channel c2 device type disk format '/nfsanf/oracopy/%U';  
  allocate channel c3 device type disk format '/nfsanf/oracopy/%U';  
  allocate channel c4 device type disk format '/nfsanf/oracopy/%U';  
  delete obsolete;  
  sql 'alter system archive log current';  
  recover copy of database with tag 'OraCopyBKUPonANF_level_0';  
  backup incremental level 1 copies=1 for recover of copy with tag  
'OraCopyBKUPonANF_level_0' database;  
}
```

5. Melden Sie sich auf dem primären Oracle VLDB-Server lokal als oracle-Benutzer mit oder ohne RMAN-Katalog bei RMAN an. In dieser Demo stellen wir keine Verbindung zu einem RMAN-Katalog her.

```
rman target / nocatalog;
```

output:

```
[oracle@ora-01 ~]$ rman target / nocatalog
```

```
Recovery Manager: Release 19.0.0.0.0 - Production on Wed Mar 20  
16:54:24 2024  
Version 19.18.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights  
reserved.
```

```
connected to target database: NTAP1 (DBID=2441823937)  
using target database control file instead of recovery catalog
```

6. Führen Sie an der Eingabeaufforderung von RMAN das Skript aus. Bei der ersten Ausführung wird eine Kopie des Basisgrads der Datenbank erstellt, und die nachfolgenden Ausführungen werden zusammengeführt und die Basisgrafkopie schrittweise aktualisiert. Im Folgenden wird beschrieben, wie das Skript und die typische Ausgabe ausgeführt werden. Legen Sie die Anzahl der Kanäle fest, die den CPU-Kernen auf dem Host entsprechen.

```
RMAN> @/home/oracle/rman_bkup_merge.cmd
```

```

RMAN> RUN
2> {
3>  allocate channel c1 device type disk format
'/nfsanf/oracopy/%U';
4>  allocate channel c2 device type disk format
'/nfsanf/oracopy/%U';
5>  allocate channel c3 device type disk format
'/nfsanf/oracopy/%U';
6>  allocate channel c4 device type disk format
'/nfsanf/oracopy/%U';
7>  delete obsolete;
8>  sql 'alter system archive log current';
9>  recover copy of database with tag 'OraCopyBKUPonANF_level_0';
10> backup incremental level 1 copies=1 for recover of copy with
tag 'OraCopyBKUPonANF_level_0' database;
11> }
allocated channel: c1
channel c1: SID=142 device type=DISK

allocated channel: c2
channel c2: SID=277 device type=DISK

allocated channel: c3
channel c3: SID=414 device type=DISK

allocated channel: c4
channel c4: SID=28 device type=DISK

RMAN retention policy will be applied to the command
RMAN retention policy is set to redundancy 1
Deleting the following obsolete backups and copies:
Type                Key      Completion Time      Filename/Handle
-----
Backup Set          1        18-MAR-24
  Backup Piece      1        18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163958359__04h19dg
r_.bkp
Backup Set          2        18-MAR-24
  Backup Piece      2        18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163961675__0711m21
g_.bkp
Backup Set          3        18-MAR-24
  Backup Piece      3        18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163962888__08p6y71
x_.bkp
Backup Set          4        18-MAR-24

```

```

Backup Piece      4      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163963796__09k8g1m
4_.bkp
Backup Set        5      18-MAR-24
Backup Piece      5      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163964697__0bd3tqg
3_.bkp
Backup Set        6      18-MAR-24
Backup Piece      6      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163965895__0chx6mz
t_.bkp
Backup Set        7      18-MAR-24
Backup Piece      7      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163966806__0dbyx34
4_.bkp
Backup Set        8      18-MAR-24
Backup Piece      8      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163968012__0fgvg80
5_.bkp
Backup Set        9      18-MAR-24
Backup Piece      9      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163968919__0g9x5t1
v_.bkp
Backup Set       10      18-MAR-24
Backup Piece     10      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163969821__0h4rfdz
j_.bkp
Backup Set       11      18-MAR-24
Backup Piece     11      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163971026__0j8o4wk
8_.bkp
Backup Set       12      18-MAR-24
Backup Piece     12      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163971931__0k3pnn2
o_.bkp
Backup Set       13      18-MAR-24
Backup Piece     13      18-MAR-24
/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163972835__0kyg92t
1_.bkp
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163963796__
09k8g1m4_.bkp RECID=4 STAMP=1163963804
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163962888__

```

08p6y7lx_.bkp RECID=3 STAMP=1163962897
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163961675___
0711m2lg_.bkp RECID=2 STAMP=1163961683
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163958359___
04h19dgr_.bkp RECID=1 STAMP=1163958361
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163964697___
0bd3tqg3_.bkp RECID=5 STAMP=1163964705
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163965895___
0chx6mzt_.bkp RECID=6 STAMP=1163965906
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163966806___
0dbyx344_.bkp RECID=7 STAMP=1163966814
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163968012___
0fgvg805_.bkp RECID=8 STAMP=1163968018
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163968919___
0g9x5t1v_.bkp RECID=9 STAMP=1163968926
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163969821___
0h4rfdzj_.bkp RECID=10 STAMP=1163969827
Deleted 3 objects

deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163971026___
0j8o4wk8_.bkp RECID=11 STAMP=1163971032
Deleted 3 objects

deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163971931___
0k3pnn2o_.bkp RECID=12 STAMP=1163971938
Deleted 3 objects

```
deleted backup piece
backup piece
handle=/u03/orareco/NTAP1/autobackup/2024_03_18/o1_mf_s_1163972835__
0kyg92t1_.bkp RECID=13 STAMP=1163972837
Deleted 4 objects
```

```
sql statement: alter system archive log current
```

```
Starting recover at 20-MAR-24
no copy of datafile 1 found to recover
no copy of datafile 3 found to recover
no copy of datafile 4 found to recover
.
.
no copy of datafile 31 found to recover
no copy of datafile 32 found to recover
Finished recover at 20-MAR-24
```

```
Starting backup at 20-MAR-24
no parent backup or copy of datafile 1 found
no parent backup or copy of datafile 3 found
no parent backup or copy of datafile 4 found
.
.
no parent backup or copy of datafile 19 found
no parent backup or copy of datafile 20 found
channel c1: starting datafile copy
input datafile file number=00021
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_01.dbf
channel c2: starting datafile copy
input datafile file number=00022
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_02.dbf
channel c3: starting datafile copy
input datafile file number=00023
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_03.dbf
channel c4: starting datafile copy
input datafile file number=00024
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_04.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-22_0g2m6br1 tag=ORACOPYBKUPONANF_LEVEL_0 RECID=4
STAMP=1164132108
channel c2: datafile copy complete, elapsed time: 01:06:39
channel c2: starting datafile copy
input datafile file number=00025
```

```
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_05.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-24_0i2m6brl tag=ORACOPYBKUPONANF_LEVEL_0 RECID=5
STAMP=1164132121
channel c4: datafile copy complete, elapsed time: 01:06:45
channel c4: starting datafile copy
input datafile file number=00026
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_06.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-23_0h2m6brl tag=ORACOPYBKUPONANF_LEVEL_0 RECID=6
STAMP=1164132198
channel c3: datafile copy complete, elapsed time: 01:08:05
channel c3: starting datafile copy
input datafile file number=00027
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_07.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-21_0f2m6brl tag=ORACOPYBKUPONANF_LEVEL_0 RECID=7
STAMP=1164132248
channel c1: datafile copy complete, elapsed time: 01:08:57
channel c1: starting datafile copy
input datafile file number=00028
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_08.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-25_0j2m6fol tag=ORACOPYBKUPONANF_LEVEL_0 RECID=9
STAMP=1164136123
channel c2: datafile copy complete, elapsed time: 01:06:46
channel c2: starting datafile copy
input datafile file number=00029
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_09.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-26_0k2m6fot tag=ORACOPYBKUPONANF_LEVEL_0 RECID=8
STAMP=1164136113
channel c4: datafile copy complete, elapsed time: 01:06:36
channel c4: starting datafile copy
input datafile file number=00030
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_10.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-27_0l2m6frc tag=ORACOPYBKUPONANF_LEVEL_0 RECID=10
STAMP=1164136293
channel c3: datafile copy complete, elapsed time: 01:08:10
channel c3: starting datafile copy
input datafile file number=00031
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_11.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-28_0m2m6fsu tag=ORACOPYBKUPONANF_LEVEL_0 RECID=11
STAMP=1164136333
```

```
channel c1: datafile copy complete, elapsed time: 01:07:52
channel c1: starting datafile copy
input datafile file number=00032
name=/u02/oradata/NTAP1/NTAP1_pdb1/soe_12.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-29_0n2m6jlr tag=ORACOPYBKUPONANF_LEVEL_0 RECID=12
STAMP=1164140082
channel c2: datafile copy complete, elapsed time: 01:06:01
channel c2: starting datafile copy
input datafile file number=00001
name=/u02/oradata/NTAP1/system01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-30_0o2m6jlr tag=ORACOPYBKUPONANF_LEVEL_0 RECID=13
STAMP=1164140190
channel c4: datafile copy complete, elapsed time: 01:07:49
channel c4: starting datafile copy
input datafile file number=00003
name=/u02/oradata/NTAP1/sysaux01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-1_0r2m6nhk tag=ORACOPYBKUPONANF_LEVEL_0 RECID=14
STAMP=1164140240
channel c2: datafile copy complete, elapsed time: 00:02:38
channel c2: starting datafile copy
input datafile file number=00004
name=/u02/oradata/NTAP1/undotbs01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-4_0t2m6nml tag=ORACOPYBKUPONANF_LEVEL_0 RECID=15
STAMP=1164140372
channel c2: datafile copy complete, elapsed time: 00:02:15
channel c2: starting datafile copy
input datafile file number=00011
name=/u02/oradata/NTAP1/NTAP1_pdb1/undotbs01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAux_FNO-3_0s2m6n1l tag=ORACOPYBKUPONANF_LEVEL_0 RECID=16
STAMP=1164140377
channel c4: datafile copy complete, elapsed time: 00:03:01
channel c4: starting datafile copy
input datafile file number=00010
name=/u02/oradata/NTAP1/NTAP1_pdb1/sysaux01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-32_0q2m6jsi tag=ORACOPYBKUPONANF_LEVEL_0 RECID=17
STAMP=1164140385
channel c1: datafile copy complete, elapsed time: 01:07:29
channel c1: starting datafile copy
input datafile file number=00014
name=/u02/oradata/NTAP1/NTAP1_pdb2/sysaux01.dbf
```



```
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SOE_FNO-31_0p2m6jrb tag=ORACOPYBKUPONANF_LEVEL_0 RECID=18
STAMP=1164140406
channel c3: datafile copy complete, elapsed time: 01:08:31
channel c3: starting datafile copy
input datafile file number=00018
name=/u02/oradata/NTAP1/NTAP1_pdb3/sysaux01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAux_FNO-10_0v2m6nqs tag=ORACOPYBKUPONANF_LEVEL_0 RECID=19
STAMP=1164140459
channel c4: datafile copy complete, elapsed time: 00:01:26
channel c4: starting datafile copy
input datafile file number=00006
name=/u02/oradata/NTAP1/pdbseed/sysaux01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAux_FNO-14_102m6nr3 tag=ORACOPYBKUPONANF_LEVEL_0 RECID=20
STAMP=1164140468
channel c1: datafile copy complete, elapsed time: 00:01:22
channel c1: starting datafile copy
input datafile file number=00009
name=/u02/oradata/NTAP1/NTAP1_pdb1/system01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-11_0u2m6nqs tag=ORACOPYBKUPONANF_LEVEL_0 RECID=21
STAMP=1164140471
channel c2: datafile copy complete, elapsed time: 00:01:33
channel c2: starting datafile copy
input datafile file number=00013
name=/u02/oradata/NTAP1/NTAP1_pdb2/system01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAux_FNO-18_112m6nrt tag=ORACOPYBKUPONANF_LEVEL_0 RECID=22
STAMP=1164140476
channel c3: datafile copy complete, elapsed time: 00:00:57
channel c3: starting datafile copy
input datafile file number=00017
name=/u02/oradata/NTAP1/NTAP1_pdb3/system01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAux_FNO-6_122m6nti tag=ORACOPYBKUPONANF_LEVEL_0 RECID=23
STAMP=1164140488
channel c4: datafile copy complete, elapsed time: 00:00:25
channel c4: starting datafile copy
input datafile file number=00005
name=/u02/oradata/NTAP1/pdbseed/system01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-13_142m6ntp tag=ORACOPYBKUPONANF_LEVEL_0 RECID=24
STAMP=1164140532
channel c2: datafile copy complete, elapsed time: 00:01:06
```

```
channel c2: starting datafile copy
input datafile file number=00008
name=/u02/oradata/NTAP1/pdbseed/undotbs01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-17_152m6nts tag=ORACOPYBKUPONANF_LEVEL_0 RECID=25
STAMP=1164140539
channel c3: datafile copy complete, elapsed time: 00:01:03
channel c3: starting datafile copy
input datafile file number=00015
name=/u02/oradata/NTAP1/NTAP1_pdb2/undotbs01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-9_132m6ntm tag=ORACOPYBKUPONANF_LEVEL_0 RECID=26
STAMP=1164140541
channel c1: datafile copy complete, elapsed time: 00:01:13
channel c1: starting datafile copy
input datafile file number=00019
name=/u02/oradata/NTAP1/NTAP1_pdb3/undotbs01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-5_162m6nuc tag=ORACOPYBKUPONANF_LEVEL_0 RECID=27
STAMP=1164140541
channel c4: datafile copy complete, elapsed time: 00:00:41
channel c4: starting datafile copy
input datafile file number=00007 name=/u02/oradata/NTAP1/users01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-8_172m6nvr tag=ORACOPYBKUPONANF_LEVEL_0 RECID=28
STAMP=1164140552
channel c2: datafile copy complete, elapsed time: 00:00:16
channel c2: starting datafile copy
input datafile file number=00012
name=/u02/oradata/NTAP1/NTAP1_pdb1/users01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-15_182m6nvs tag=ORACOPYBKUPONANF_LEVEL_0 RECID=30
STAMP=1164140561
channel c3: datafile copy complete, elapsed time: 00:00:24
channel c3: starting datafile copy
input datafile file number=00016
name=/u02/oradata/NTAP1/NTAP1_pdb2/users01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-7_1a2m6o01 tag=ORACOPYBKUPONANF_LEVEL_0 RECID=29
STAMP=1164140560
channel c4: datafile copy complete, elapsed time: 00:00:16
channel c4: starting datafile copy
input datafile file number=00020
name=/u02/oradata/NTAP1/NTAP1_pdb3/users01.dbf
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-19_192m6nvv tag=ORACOPYBKUPONANF_LEVEL_0 RECID=31
```

```

STAMP=1164140564
channel c1: datafile copy complete, elapsed time: 00:00:21
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-12_1b2m6o0e tag=ORACOPYBKUPONANF_LEVEL_0 RECID=32
STAMP=1164140564
channel c2: datafile copy complete, elapsed time: 00:00:02
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-16_1c2m6o0k tag=ORACOPYBKUPONANF_LEVEL_0 RECID=34
STAMP=1164140565
channel c3: datafile copy complete, elapsed time: 00:00:01
output file name=/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-20_1d2m6o0k tag=ORACOPYBKUPONANF_LEVEL_0 RECID=33
STAMP=1164140565
channel c4: datafile copy complete, elapsed time: 00:00:01
Finished backup at 20-MAR-24

Starting Control File and SPFILE Autobackup at 20-MAR-24
piece
handle=/nfsanf/archlog/NTAP1/autobackup/2024_03_20/o1_mf_s_116414056
5__5g56ypks_.bkp comment=NONE
Finished Control File and SPFILE Autobackup at 20-MAR-24
released channel: c1
released channel: c2
released channel: c3
released channel: c4

RMAN> **end-of-file**

RMAN>

```

- Führen Sie nach dem Backup eine Datenbank-Image-Kopie auf, um zu beobachten, dass im ANF NFS-Bereitstellungspunkt eine Datenbank-Image-Kopie erstellt wurde.

```

RMAN> list copy of database tag 'OraCopyBKUPonANF_level_0';

List of Datafile Copies
=====

Key          File S Completion Time Ckp SCN      Ckp Time      Sparse
-----
14           1    A 20-MAR-24      4161498      20-MAR-24      NO
           Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-1_0r2m6nhk
           Tag: ORACOPYBKUPONANF_LEVEL_0

16           3    A 20-MAR-24      4161568      20-MAR-24      NO

```

```

      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAUX_FNO-3_0s2m6nl1
      Tag: ORACOPYBKUPONANF_LEVEL_0

15      4      A 20-MAR-24      4161589      20-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-4_0t2m6nml
      Tag: ORACOPYBKUPONANF_LEVEL_0

27      5      A 20-MAR-24      2379694      18-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-5_162m6nuc
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 2, PDB Name: PDB$SEED

23      6      A 20-MAR-24      2379694      18-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAUX_FNO-6_122m6nti
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 2, PDB Name: PDB$SEED

29      7      A 20-MAR-24      4161872      20-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-7_1a2m6o01
      Tag: ORACOPYBKUPONANF_LEVEL_0

28      8      A 20-MAR-24      2379694      18-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-8_172m6nvr
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 2, PDB Name: PDB$SEED

26      9      A 20-MAR-24      4161835      20-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-9_132m6ntm
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 3, PDB Name: NTAP1_PDB1

19      10     A 20-MAR-24      4161784      20-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAUX_FNO-10_0v2m6nqs
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 3, PDB Name: NTAP1_PDB1

21      11     A 20-MAR-24      4161780      20-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-

```

```

UNDOTBS1_FNO-11_0u2m6nqs
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 3, PDB Name: NTAP1_PDB1

32      12      A 20-MAR-24      4161880      20-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-12_1b2m6o0e
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 3, PDB Name: NTAP1_PDB1

24      13      A 20-MAR-24      4161838      20-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-13_142m6ntp
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 4, PDB Name: NTAP1_PDB2

20      14      A 20-MAR-24      4161785      20-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAUX_FNO-14_102m6nr3
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 4, PDB Name: NTAP1_PDB2

30      15      A 20-MAR-24      4161863      20-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-15_182m6nvs
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 4, PDB Name: NTAP1_PDB2

34      16      A 20-MAR-24      4161884      20-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-16_1c2m6o0k
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 4, PDB Name: NTAP1_PDB2

25      17      A 20-MAR-24      4161841      20-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-17_152m6nts
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 5, PDB Name: NTAP1_PDB3

22      18      A 20-MAR-24      4161810      20-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAUX_FNO-18_112m6nrt
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 5, PDB Name: NTAP1_PDB3

```

31	19	A	20-MAR-24	4161869	20-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-19_192m6nvv					
	Tag: ORACOPYBKUPONANF_LEVEL_0					
	Container ID: 5, PDB Name: NTAP1_PDB3					
33	20	A	20-MAR-24	4161887	20-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-20_1d2m6o0k					
	Tag: ORACOPYBKUPONANF_LEVEL_0					
	Container ID: 5, PDB Name: NTAP1_PDB3					
7	21	A	20-MAR-24	4152514	20-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-21_0f2m6brl					
	Tag: ORACOPYBKUPONANF_LEVEL_0					
	Container ID: 3, PDB Name: NTAP1_PDB1					
4	22	A	20-MAR-24	4152518	20-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-22_0g2m6brl					
	Tag: ORACOPYBKUPONANF_LEVEL_0					
	Container ID: 3, PDB Name: NTAP1_PDB1					
6	23	A	20-MAR-24	4152522	20-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-23_0h2m6brl					
	Tag: ORACOPYBKUPONANF_LEVEL_0					
	Container ID: 3, PDB Name: NTAP1_PDB1					
5	24	A	20-MAR-24	4152529	20-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-24_0i2m6brl					
	Tag: ORACOPYBKUPONANF_LEVEL_0					
	Container ID: 3, PDB Name: NTAP1_PDB1					
9	25	A	20-MAR-24	4156120	20-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-25_0j2m6fol					
	Tag: ORACOPYBKUPONANF_LEVEL_0					
	Container ID: 3, PDB Name: NTAP1_PDB1					
8	26	A	20-MAR-24	4156130	20-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-26_0k2m6fot					
	Tag: ORACOPYBKUPONANF_LEVEL_0					

```

Container ID: 3, PDB Name: NTAP1_PDB1

10      27      A 20-MAR-24      4156159      20-MAR-24      NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
27_0l2m6frc
Tag: ORACOPYBKUPONANF_LEVEL_0
Container ID: 3, PDB Name: NTAP1_PDB1

11      28      A 20-MAR-24      4156183      20-MAR-24      NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
28_0m2m6fsu
Tag: ORACOPYBKUPONANF_LEVEL_0
Container ID: 3, PDB Name: NTAP1_PDB1

12      29      A 20-MAR-24      4158795      20-MAR-24      NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
29_0n2m6jlr
Tag: ORACOPYBKUPONANF_LEVEL_0
Container ID: 3, PDB Name: NTAP1_PDB1

13      30      A 20-MAR-24      4158803      20-MAR-24      NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
30_0o2m6jlr
Tag: ORACOPYBKUPONANF_LEVEL_0
Container ID: 3, PDB Name: NTAP1_PDB1

18      31      A 20-MAR-24      4158871      20-MAR-24      NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
31_0p2m6jrb
Tag: ORACOPYBKUPONANF_LEVEL_0
Container ID: 3, PDB Name: NTAP1_PDB1

17      32      A 20-MAR-24      4158886      20-MAR-24      NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
32_0q2m6jsi
Tag: ORACOPYBKUPONANF_LEVEL_0
Container ID: 3, PDB Name: NTAP1_PDB1

```

8. Melden Sie das Schema über die Eingabeaufforderung von Oracle RMAN, um zu beobachten, dass sich die aktuellen VLDB-Datendateien auf dem primären Speicher befinden.

```

RMAN> report schema;

Report of database schema for database with db_unique_name NTAP1

List of Permanent Datafiles

```

```

=====
File Size(MB) Tablespace          RB segs Datafile Name
-----
1      1060      SYSTEM                YES
/u02/oradata/NTAP1/system01.dbf
3      1000      SYSAUX                 NO
/u02/oradata/NTAP1/sysaux01.dbf
4      695       UNDOTBS1              YES
/u02/oradata/NTAP1/undotbs01.dbf
5      400       PDB$SEED:SYSTEM      NO
/u02/oradata/NTAP1/pdbseed/system01.dbf
6      440       PDB$SEED:SYSAUX     NO
/u02/oradata/NTAP1/pdbseed/sysaux01.dbf
7      5         USERS                 NO
/u02/oradata/NTAP1/users01.dbf
8      235      PDB$SEED:UNDOTBS1   NO
/u02/oradata/NTAP1/pdbseed/undotbs01.dbf
9      410      NTAP1_PDB1:SYSTEM   YES
/u02/oradata/NTAP1/NTAP1_pdb1/system01.dbf
10     520     NTAP1_PDB1:SYSAUX   NO
/u02/oradata/NTAP1/NTAP1_pdb1/sysaux01.dbf
11     580     NTAP1_PDB1:UNDOTBS1 YES
/u02/oradata/NTAP1/NTAP1_pdb1/undotbs01.dbf
12     5       NTAP1_PDB1:USERS    NO
/u02/oradata/NTAP1/NTAP1_pdb1/users01.dbf
13     410     NTAP1_PDB2:SYSTEM   YES
/u02/oradata/NTAP1/NTAP1_pdb2/system01.dbf
14     500     NTAP1_PDB2:SYSAUX   NO
/u02/oradata/NTAP1/NTAP1_pdb2/sysaux01.dbf
15     235     NTAP1_PDB2:UNDOTBS1 YES
/u02/oradata/NTAP1/NTAP1_pdb2/undotbs01.dbf
16     5       NTAP1_PDB2:USERS    NO
/u02/oradata/NTAP1/NTAP1_pdb2/users01.dbf
17     410     NTAP1_PDB3:SYSTEM   YES
/u02/oradata/NTAP1/NTAP1_pdb3/system01.dbf
18     500     NTAP1_PDB3:SYSAUX   NO
/u02/oradata/NTAP1/NTAP1_pdb3/sysaux01.dbf
19     235     NTAP1_PDB3:UNDOTBS1 YES
/u02/oradata/NTAP1/NTAP1_pdb3/undotbs01.dbf
20     5       NTAP1_PDB3:USERS    NO
/u02/oradata/NTAP1/NTAP1_pdb3/users01.dbf
21     31744   NTAP1_PDB1:SOE      NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_01.dbf
22     31744   NTAP1_PDB1:SOE      NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_02.dbf
23     31744   NTAP1_PDB1:SOE      NO

```



```

/u02/oradata/NTAP1/NTAP1_pdb1/soe_03.dbf
24 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_04.dbf
25 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_05.dbf
26 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_06.dbf
27 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_07.dbf
28 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_08.dbf
29 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_09.dbf
30 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_10.dbf
31 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_11.dbf
32 31744 NTAP1_PDB1:SOE NO
/u02/oradata/NTAP1/NTAP1_pdb1/soe_12.dbf

```

List of Temporary Files

=====

File	Size (MB)	Tablespace	Maxsize (MB)	Tempfile Name
1	123	TEMP	32767	/u02/oradata/NTAP1/temp01.dbf
2	123	PDB\$SEED:TEMP	32767	/u02/oradata/NTAP1/pdbseed/temp012024-03-18_16-07-32-463-PM.dbf
3	31744	NTAP1_PDB1:TEMP	32767	/u02/oradata/NTAP1/NTAP1_pdb1/temp01.dbf
4	123	NTAP1_PDB2:TEMP	32767	/u02/oradata/NTAP1/NTAP1_pdb2/temp01.dbf
5	123	NTAP1_PDB3:TEMP	32767	/u02/oradata/NTAP1/NTAP1_pdb3/temp01.dbf
6	31744	NTAP1_PDB1:TEMP	31744	/u02/oradata/NTAP1/NTAP1_pdb1/temp02.dbf

RMAN>

9. Validieren der Datenbank-Image-Kopie vom NFS-Bereitstellungspunkt des Betriebssystems

```

[oracle@ora-01 ~]$ ls -l /nfsanf/oracopy
total 399482176
-rw-r----- 1 oracle oinstall 11600384 Mar 20 21:44 bct_ntap1.ctf
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 18:03 data_D-

```

```

NTAP1_I-2441823937_TS-SOE_FNO-21_0f2m6brl
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 18:01 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-22_0g2m6brl
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 18:03 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-23_0h2m6brl
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 18:02 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-24_0i2m6brl
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 19:08 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-25_0j2m6fol
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 19:08 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-26_0k2m6fot
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 19:11 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-27_0l2m6frc
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 19:12 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-28_0m2m6fsu
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 20:14 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-29_0n2m6jlr
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 20:16 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-30_0o2m6jlr
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 20:20 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-31_0p2m6jrb
-rw-r----- 1 oracle oinstall 33286004736 Mar 20 20:19 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-32_0q2m6jsi
-rw-r----- 1 oracle oinstall 545267712 Mar 20 20:20 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-10_0v2m6nqs
-rw-r----- 1 oracle oinstall 524296192 Mar 20 20:21 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-14_102m6nr3
-rw-r----- 1 oracle oinstall 524296192 Mar 20 20:21 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-18_112m6nrt
-rw-r----- 1 oracle oinstall 1048584192 Mar 20 20:19 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-3_0s2m6nl1
-rw-r----- 1 oracle oinstall 461381632 Mar 20 20:21 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-6_122m6nti
-rw-r----- 1 oracle oinstall 1111498752 Mar 20 20:17 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-1_0r2m6nhk
-rw-r----- 1 oracle oinstall 429924352 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-13_142m6ntp
-rw-r----- 1 oracle oinstall 429924352 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-17_152m6nts
-rw-r----- 1 oracle oinstall 419438592 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-5_162m6nuc
-rw-r----- 1 oracle oinstall 429924352 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-9_132m6ntm
-rw-r----- 1 oracle oinstall 608182272 Mar 20 20:21 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-11_0u2m6nqs
-rw-r----- 1 oracle oinstall 246423552 Mar 20 20:22 data_D-

```

```
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-15_182m6nvs
-rw-r----- 1 oracle oinstall 246423552 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-19_192m6nvv
-rw-r----- 1 oracle oinstall 728768512 Mar 20 20:19 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-4_0t2m6nml
-rw-r----- 1 oracle oinstall 246423552 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-8_172m6nvr
-rw-r----- 1 oracle oinstall 5251072 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-USERS_FNO-12_1b2m6o0e
-rw-r----- 1 oracle oinstall 5251072 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-USERS_FNO-16_1c2m6o0k
-rw-r----- 1 oracle oinstall 5251072 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-USERS_FNO-20_1d2m6o0k
-rw-r----- 1 oracle oinstall 5251072 Mar 20 20:22 data_D-
NTAP1_I-2441823937_TS-USERS_FNO-7_1a2m6o01
[oracle@ora-01 ~]$
```

Damit ist die Einrichtung eines Backup- und Merge-Backups von Oracle VLDB-Standby-Images abgeschlossen.

Wechseln Sie zum schnellen Wiederherstellen von Oracle VLDB zu Image Copy

Im Falle eines Fehlers aufgrund eines Problems im Primärspeicher, wie z. B. Datenverlust oder -Beschädigung, kann die Datenbank schnell auf eine Image-Kopie im ANF NFS-Mount umgeschaltet und ohne Datenbank-Wiederherstellung in den aktuellen Zustand versetzt werden. Durch die Eliminierung der Medienwiederherstellung wird die Datenbank-Recovery für ein VLDB erheblich beschleunigt. Dieser Anwendungsfall setzt voraus, dass der Oracle VLDB DB-Server intakt ist und dass die Datenbanksteuerungsdatei, die archivierten und die aktuellen Protokolle für die Recovery verfügbar sind.

1. Melden Sie sich beim primären VLDB-Server von Azure als oracle-Benutzer an und erstellen Sie vor dem Umschalten eine Testtabelle.

```
[oracle@ora-01 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Mar 21 15:13:52
2024
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> show pdbs

          CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
          2 PDB$SEED                                READ ONLY  NO
          3 NTAP1_PDB1                                READ WRITE NO
          4 NTAP1_PDB2                                READ WRITE NO
          5 NTAP1_PDB3                                READ WRITE NO
SQL> alter session set container=ntap1_pdb1;

Session altered.

SQL> create table test (id integer, dt timestamp, event
varchar(100));

Table created.

SQL> insert into test values(1, sysdate, 'test oracle incremental
merge switch to copy');

1 row created.

SQL> commit;
```

```
Commit complete.
```

```
SQL> select * from test;
```

```
          ID
-----
DT
-----
EVENT
-----
          1
21-MAR-24 03.15.03.000000 PM
test oracle incremental merge switch to copy
```

2. Simulieren Sie einen Fehler, indem Sie die Datenbank herunterfahren und dann oracle in der Bereitstellungsphase starten.

```
SQL> shutdown abort;
ORACLE instance shut down.
SQL> startup mount;
ORACLE instance started.
```

```
Total System Global Area 6442449688 bytes
Fixed Size                  9177880 bytes
Variable Size               1325400064 bytes
Database Buffers           5100273664 bytes
Redo Buffers                 7598080 bytes
Database mounted.
SQL> exit
```

3. Stellen Sie als oracle-Benutzer eine Verbindung zur Oracle-Datenbank über RMAN her, um die Datenbank zum Kopieren zu wechseln.

```
[oracle@ora-01 ~]$ rman target / nocatalog

Recovery Manager: Release 19.0.0.0.0 - Production on Thu Mar 21
15:20:58 2024
Version 19.18.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights
reserved.
```

```
connected to target database: NTAP1 (DBID=2441823937, not open)
using target database control file instead of recovery catalog
```

```
RMAN> switch database to copy;
```

```
datafile 1 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-1_0r2m6nhk"
datafile 3 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-3_0s2m6nl1"
datafile 4 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-4_0t2m6nml"
datafile 5 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-5_162m6nuc"
datafile 6 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-6_122m6nti"
datafile 7 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-7_1a2m6o01"
datafile 8 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-8_172m6nvr"
datafile 9 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-9_132m6ntm"
datafile 10 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-10_0v2m6nqs"
datafile 11 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-11_0u2m6nqs"
datafile 12 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-12_1b2m6o0e"
datafile 13 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-13_142m6ntp"
datafile 14 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-14_102m6nr3"
datafile 15 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-15_182m6nvs"
datafile 16 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-16_1c2m6o0k"
datafile 17 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-17_152m6nts"
datafile 18 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-18_112m6nrt"
datafile 19 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-19_192m6nvv"
datafile 20 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-20_1d2m6o0k"
datafile 21 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-21_0f2m6brl"
datafile 22 switched to datafile copy "/nfsanf/oracopy/data_D-
```

```

NTAP1_I-2441823937_TS-SOE_FNO-22_0g2m6brl"
datafile 23 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-23_0h2m6brl"
datafile 24 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-24_0i2m6brl"
datafile 25 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-25_0j2m6fol"
datafile 26 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-26_0k2m6fot"
datafile 27 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-27_0l2m6frc"
datafile 28 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-28_0m2m6fsu"
datafile 29 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-29_0n2m6jlr"
datafile 30 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-30_0o2m6jlr"
datafile 31 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-31_0p2m6jrb"
datafile 32 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-32_0q2m6jsi"

```

4. Stellen Sie die Datenbank wieder her und öffnen Sie sie, um sie vom letzten inkrementellen Backup auf den aktuellen Stand zu bringen.

```

RMAN> recover database;

Starting recover at 21-MAR-24
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=392 device type=DISK
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup
set
destination for restore of datafile 00009: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-9_0q1sd7cm
destination for restore of datafile 00023: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-23_041sd6s5
destination for restore of datafile 00027: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-27_081sd70i
destination for restore of datafile 00031: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-31_0c1sd74u
destination for restore of datafile 00034: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-34_0f1sd788
channel ORA_DISK_1: reading from backup piece
/nfsanf/oracopy/321sfous_98_1_1
channel ORA_DISK_1: piece handle=/nfsanf/oracopy/321sfous_98_1_1

```

```

tag=ORACOPYBKUPONANF_LEVEL_0
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup
set
destination for restore of datafile 00010: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-10_0k1sd7bb
destination for restore of datafile 00021: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-21_021sd6pv
destination for restore of datafile 00025: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-25_061sd6uc
.
.
.
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup
set
destination for restore of datafile 00016: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-16_121sd7dn
channel ORA_DISK_1: reading from backup piece
/nfsanf/oracopy/3i1sfov0_114_1_1
channel ORA_DISK_1: piece handle=/nfsanf/oracopy/3i1sfov0_114_1_1
tag=ORACOPYBKUPONANF_LEVEL_0
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01
channel ORA_DISK_1: starting incremental datafile backup set restore
channel ORA_DISK_1: specifying datafile(s) to restore from backup
set
destination for restore of datafile 00020: /nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-20_131sd7do
channel ORA_DISK_1: reading from backup piece
/nfsanf/oracopy/3j1sfov0_115_1_1
channel ORA_DISK_1: piece handle=/nfsanf/oracopy/3j1sfov0_115_1_1
tag=ORACOPYBKUPONANF_LEVEL_0
channel ORA_DISK_1: restored backup piece 1
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01

starting media recovery
media recovery complete, elapsed time: 00:00:01

Finished recover at 21-MAR-24

RMAN> alter database open;

Statement processed

```



```
RMAN>
```

5. Überprüfen Sie die Datenbankstruktur von sqlplus nach der Wiederherstellung, um zu beobachten, dass alle VLDB-Datendateien mit Ausnahme von Steuerungs-, Temp- und aktuellen Protokolldateien nun auf das ANF NFS-Dateisystem kopiert werden.

```
SQL> select name from v$datafile
2 union
3 select name from v$tempfile
4 union
5 select name from v$controlfile
6 union
7* select member from v$logfile
SQL> /
```

```
NAME
```

```
-----
-----
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-21_0f2m6brl
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-22_0g2m6brl
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-23_0h2m6brl
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-24_0i2m6brl
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-25_0j2m6fol
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-26_0k2m6fot
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-27_0l2m6frc
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-28_0m2m6fsu
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-29_0n2m6jlr
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-30_0o2m6jlr
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-31_0p2m6jrb
```

```
NAME
```

```
-----
-----
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-32_0q2m6jsi
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-10_0v2m6nqs
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-14_102m6nr3
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-18_112m6nrt
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-3_0s2m6n11
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-6_122m6nti
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-13_142m6ntp
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-17_152m6nts
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-1_0r2m6nhk
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-5_162m6nuc
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-9_132m6ntm
```

NAME

```
-----  
-----  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-  
11_0u2m6nqs  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-  
15_182m6nvs  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-  
19_192m6nvv  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-4_0t2m6nml  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-8_172m6nvr  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-12_1b2m6o0e  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-16_1c2m6o0k  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-20_1d2m6o0k  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-7_1a2m6o01  
/u02/oradata/NTAP1/NTAP1_pdb1/temp01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb1/temp02.dbf
```

NAME

```
-----  
-----  
/u02/oradata/NTAP1/NTAP1_pdb2/temp01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb3/temp01.dbf  
/u02/oradata/NTAP1/control01ctl  
/u02/oradata/NTAP1/pdbseed/temp012024-03-18_16-07-32-463-PM.dbf  
/u02/oradata/NTAP1/temp01.dbf  
/u03/orareco/NTAP1/control02.ctl  
/u03/orareco/NTAP1/onlinelog/redo01.log  
/u03/orareco/NTAP1/onlinelog/redo02.log  
/u03/orareco/NTAP1/onlinelog/redo03.log
```

42 rows selected.

6. Überprüfen Sie in SQL plus den Inhalt der Testtabelle, die wir vor dem Wechsel zum Kopieren eingefügt haben.

```
SQL> alter session set container=ntapl_pdb1;
```

```
Session altered.
```

```
SQL> select * from test;
```

```
          ID
-----
DT
-----
EVENT
-----
          1
21-MAR-24 03.15.03.000000 PM
test oracle incremental merge switch to copy

SQL>
```

7. Sie können die Oracle VLDB in ANF NFS-Mount für einen längeren Zeitraum ausführen und dabei das erwartete Leistungsniveau beibehalten. Wenn das Problem mit dem primären Storage behoben ist, können Sie darauf zurückwechseln, indem Sie die inkrementellen Backup-Merge-Prozesse mit minimalen Ausfallzeiten umkehren.

Oracle VLDB-Wiederherstellung von der Image-Kopie auf einen Standby-DB-Server

Bei einem Ausfall, bei dem sowohl der primäre Speicher als auch der Host des primären DB-Servers verloren gehen, kann keine Wiederherstellung vom ursprünglichen Server aus durchgeführt werden. Allerdings ist Ihre Backup-Image-Kopie für Oracle-Datenbanken, die auf dem ANF NFS-Dateisystem verfügbar ist, äußerst praktisch. Sie können die primäre Datenbank mithilfe der Backup-Image-Kopie schnell auf einem Standby-DB-Server wiederherstellen, sofern einer verfügbar ist. In diesem Abschnitt werden wir die schrittweisen Verfahren für eine solche Wiederherstellung erläutern.

1. Fügen Sie eine Zeile in die Testtabelle ein, die wir zuvor für die Wiederherstellung auf alternative Hostvalidierung von Oracle VLDB erstellt haben.

```
SQL> insert into test values(2, sysdate, 'test recovery on a new
Azure VM host with image copy on ANF');
```

```
1 row created.
```

```
SQL> commit;
```

```
Commit complete.
```

```
SQL> select * from test;
```

```
          ID
-----
DT
-----
EVENT
-----
          1
21-MAR-24 03.15.03.000000 PM
test oracle incremental merge switch to copy

          2
22-MAR-24 02.22.06.000000 PM
test recovery on a new Azure VM host with image copy on ANF
```

```
          ID
-----
DT
-----
EVENT
-----
```

```
SQL>
```

2. Führen Sie als oracle-Benutzer ein inkrementelles RMAN-Backup aus und führen Sie die Transaktion zusammen, um das Backup-Set auf dem ANF-NFS-Mount zu löschen.

```
[oracle@ip-172-30-15-99 ~]$ rman target / nocatalog

Recovery Manager: Release 19.0.0.0.0 - Production on Tue May 30
17:26:03 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights
reserved.

connected to target database: NTAP1 (DBID=2441823937)
using target database control file instead of recovery catalog

RMAN> @rman_bkup_merge.cmd
```

3. Fahren Sie den primären VLDB-Server-Host herunter, um einen Totalausfall von Speicher und DB-Server-Host zu simulieren.
4. Auf dem Standby-DB-Server ora-02 mit demselben Betriebssystem und derselben Version sollte OS Kernel als primärer VLDB-Server-Host gepatcht werden. Außerdem wurden die gleiche Version und Patches von Oracle auf Standby-DB-Server mit rein softwarebasierter Option installiert und konfiguriert.
5. Konfigurieren Sie die oracle-Umgebung ähnlich wie den primären VLDB-Server ora_01, z. B. oratab und oracle-Benutzer .bash_profile usw. In der Praxis wird empfohlen, diese Dateien auf dem ANF NFS-Bereitstellungspunkt zu sichern.
6. Die Backup-Image-Kopie der Oracle-Datenbank auf dem ANF NFS-Dateisystem wird dann zur Wiederherstellung auf dem Standby-DB-Server gemountet. Die folgenden Verfahren zeigen die Prozessdetails.

Erstellen Sie als Azueruser den Bereitstellungspunkt.

```
sudo mkdir /nfsanf
```

Mounten Sie als Azureuser das NFS-Volume, das die Oracle VLDB Backup-Image-Kopie gespeichert hat.

```
sudo mount 172.30.136.68:/ora-01-u02-copy /nfsanf -o
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=262144,wsizer=262144,noi
ntr
```

7. Backup-Image-Kopie der Oracle-Datenbank auf ANF NFS-Bereitstellungspunkt validieren

```
[oracle@ora-02 ~]$ ls -ltr /nfsanf/oracopy/
total 400452728
-rw-r-----. 1 oracle oinstall 461381632 Mar 21 23:47 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-6_242m9oan
```

```

-rw-r-----. 1 oracle oinstall 419438592 Mar 21 23:49 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-5_282m9oem
-rw-r-----. 1 oracle oinstall 246423552 Mar 21 23:49 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-8_292m9oem
-rw-r-----. 1 oracle oinstall 21438464 Mar 22 14:35
2h2mbccv_81_1_1
-rw-r-----. 1 oracle oinstall 17956864 Mar 22 14:35
2i2mbcd0_82_1_1
-rw-r-----. 1 oracle oinstall 17956864 Mar 22 14:35
2j2mbcd1_83_1_1
-rw-r-----. 1 oracle oinstall 15245312 Mar 22 14:35
2k2mbcd3_84_1_1
-rw-r-----. 1 oracle oinstall 1638400 Mar 22 14:35
2m2mbcdn_86_1_1
-rw-r-----. 1 oracle oinstall 40042496 Mar 22 14:35
2l2mbcdn_85_1_1
-rw-r-----. 1 oracle oinstall 21856256 Mar 22 14:35
2n2mbcd0_87_1_1
-rw-r-----. 1 oracle oinstall 3710976 Mar 22 14:35
2o2mbcdv_88_1_1
-rw-r-----. 1 oracle oinstall 3416064 Mar 22 14:35
2p2mbcdv_89_1_1
-rw-r-----. 1 oracle oinstall 2596864 Mar 22 14:35
2r2mbce0_91_1_1
-rw-r-----. 1 oracle oinstall 2531328 Mar 22 14:35
2s2mbce1_92_1_1
-rw-r-----. 1 oracle oinstall 4718592 Mar 22 14:35
2v2mbce2_95_1_1
-rw-r-----. 1 oracle oinstall 4243456 Mar 22 14:35
302mbce2_96_1_1
-rw-r-----. 1 oracle oinstall 57344 Mar 22 14:35
312mbce3_97_1_1
-rw-r-----. 1 oracle oinstall 57344 Mar 22 14:35
322mbce3_98_1_1
-rw-r-----. 1 oracle oinstall 57344 Mar 22 14:35
332mbce3_99_1_1
-rw-r-----. 1 oracle oinstall 608182272 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-11_202m9o22
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-30_1q2m9k7a
-rw-r-----. 1 oracle oinstall 555753472 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-10_212m9o52
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-26_1m2m9g9j
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-27_1n2m9g9j

```

```
-rw-r-----. 1 oracle oinstall 429924352 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-9_252m9oc5
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-22_1i2m9cap
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-23_1j2m9cap
-rw-r-----. 1 oracle oinstall 5251072 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-USERS_FNO-12_2d2m9ofs
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-28_1o2m9gd4
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-31_1r2m9kfk
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-29_1p2m9ju6
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-32_1s2m9kkg
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-25_1l2m9g3u
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-24_1k2m9cap
-rw-r-----. 1 oracle oinstall 33286004736 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SOE_FNO-21_1h2m9cap
-rw-r-----. 1 oracle oinstall 1121984512 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-1_1t2m9nij
-rw-r-----. 1 oracle oinstall 1142956032 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-3_1u2m9nog
-rw-r-----. 1 oracle oinstall 728768512 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-4_1v2m9nu6
-rw-r-----. 1 oracle oinstall 534781952 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-14_222m9o53
-rw-r-----. 1 oracle oinstall 534781952 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-18_232m9oa8
-rw-r-----. 1 oracle oinstall 429924352 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-13_262m9oca
-rw-r-----. 1 oracle oinstall 246423552 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-15_2a2m9of6
-rw-r-----. 1 oracle oinstall 429924352 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-17_272m9oel
-rw-r-----. 1 oracle oinstall 5251072 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-USERS_FNO-7_2c2m9ofn
-rw-r-----. 1 oracle oinstall 5251072 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-USERS_FNO-16_2e2m9og8
-rw-r-----. 1 oracle oinstall 246423552 Mar 22 15:31 data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-19_2b2m9ofn
-rw-r-----. 1 oracle oinstall 5251072 Mar 22 15:32 data_D-
NTAP1_I-2441823937_TS-USERS_FNO-20_2f2m9og8
```



```

-rw-r-----. 1 oracle oinstall      76546048 Mar 22 15:37
362mbft5_102_1_1
-rw-r-----. 1 oracle oinstall      14671872 Mar 22 15:37
392mbgli_105_1_1
-rw-r-----. 1 oracle oinstall      79462400 Mar 22 15:37
372mbftb_103_1_1
-rw-r-----. 1 oracle oinstall         917504 Mar 22 15:37
3a2mbg23_106_1_1
-rw-r-----. 1 oracle oinstall     428498944 Mar 22 15:37
352mbfst_101_1_1
-rw-r-----. 1 oracle oinstall      88702976 Mar 22 15:37
382mbftm_104_1_1
-rw-r-----. 1 oracle oinstall      5021696 Mar 22 15:37
3b2mbg2b_107_1_1
-rw-r-----. 1 oracle oinstall       278528 Mar 22 15:38
3c2mbg2f_108_1_1
-rw-r-----. 1 oracle oinstall       278528 Mar 22 15:38
3d2mbg2i_109_1_1
-rw-r-----. 1 oracle oinstall       425984 Mar 22 15:38
3f2mbg2m_111_1_1
-rw-r-----. 1 oracle oinstall      442368 Mar 22 15:38
3g2mbg2q_112_1_1
-rw-r-----. 1 oracle oinstall       278528 Mar 22 15:38
3j2mbg37_115_1_1
-rw-r-----. 1 oracle oinstall      270336 Mar 22 15:38
3k2mbg3a_116_1_1
-rw-r-----. 1 oracle oinstall       57344 Mar 22 15:38
3l2mbg3f_117_1_1
-rw-r-----. 1 oracle oinstall       57344 Mar 22 15:38
3n2mbg3k_119_1_1
-rw-r-----. 1 oracle oinstall       57344 Mar 22 15:38
3m2mbg3g_118_1_1
-rw-r-----. 1 oracle oinstall     11600384 Mar 22 15:52 bct_ntap1.ctf
[oracle@ora-02 ~]$

```

8. Überprüfen Sie die verfügbaren archivierten Oracle-Protokolle auf dem ANF-NFS-Mount für die Wiederherstellung, und notieren Sie sich die letzte Protokollsequenznummer. In diesem Fall ist es 10. Unser Wiederherstellungspunkt liegt bei der Protokollierung der Sequenznummer 11.

```

[oracle@ora-02 ~]$ ls -ltr
/nfsanf/archlog/NTAP1/archivelog/2024_03_22
total 1429548
-r--r-----. 1 oracle oinstall 176650752 Mar 22 12:00
o1_mf_1_2__9m198x6t_.arc
-r--r-----. 1 oracle oinstall 17674752 Mar 22 14:34
o1_mf_1_3__9vn701r5_.arc
-r--r-----. 1 oracle oinstall 188782080 Mar 22 15:20
o1_mf_1_4__9y6gn5co_.arc
-r--r-----. 1 oracle oinstall 183638016 Mar 22 15:21
o1_mf_1_5__9y7p68s6_.arc
-r--r-----. 1 oracle oinstall 193106944 Mar 22 15:21
o1_mf_1_6__9y8ygtss_.arc
-r--r-----. 1 oracle oinstall 179439104 Mar 22 15:22
o1_mf_1_7__9ybjdp55_.arc
-r--r-----. 1 oracle oinstall 198815232 Mar 22 15:23
o1_mf_1_8__9yctxjgy_.arc
-r--r-----. 1 oracle oinstall 185494528 Mar 22 15:24
o1_mf_1_9__9yfrj0b1_.arc
-r--r-----. 1 oracle oinstall 134470144 Mar 22 15:29
o1_mf_1_10__9yomybbc_.arc
[oracle@ora-02 ~]$

```

9. Setzen Sie als oracle-Benutzer die Variable ORACLE_HOME auf die aktuelle Oracle-Installation auf dem Standby-DB-Server ora-02, ORACLE_SID auf die primäre Oracle-Instanz SID. In diesem Fall ist es NTAP1.

```

[oracle@ora-02 ~]$ export
ORACLE_HOME=/u01/app/oracle/product/19.0.0/NTAP2
[oracle@ora-02 ~]$ export ORACLE_SID=NTAP1
[oracle@ora-02 ~]$ export PATH=$PATH:$ORACLE_HOME/bin

```

10. Erstellen Sie als oracle-Benutzer eine allgemeine Oracle-Init-Datei im Oracle_HOME/dbs-Verzeichnis mit einer Konfiguration der richtigen Administratorverzeichnisse. Vor allem aber Oracle flash recovery area Zeigen Sie auf den ANF NFS-Mount-Pfad, wie im primären Oracle VLDB-Server definiert. flash recovery area Die Konfiguration wird in Abschnitt demonstriert Setup Oracle RMAN incremental merge to image copy on ANF. Legen Sie die Oracle-Steuerdatei auf das ANF-NFS-Dateisystem fest.

```
vi $ORACLE_HOME/dbs/initNTAP1.ora
```

Mit folgenden Beispieleinträgen:

```
*.audit_file_dest='/u01/app/oracle/admin/NTAP1/adump'  
*.audit_trail='db'  
*.compatible='19.0.0'  
*.control_files=('/nfsanf/oracopy/NTAP1.ctl')  
*.db_block_size=8192  
*.db_create_file_dest='/nfsanf/oracopy/'  
*.db_domain='solutions.netapp.com'  
*.db_name='NTAP1'  
*.db_recovery_file_dest_size=85899345920  
*.db_recovery_file_dest='/nfsanf/archlog/'  
*.diagnostic_dest='/u01/app/oracle'  
*.dispatchers='(PROTOCOL=TCP) (SERVICE=NTAP1XDB) '  
*.enable_pluggable_database=true  
*.local_listener='LISTENER'  
*.nls_language='AMERICAN'  
*.nls_territory='AMERICA'  
*.open_cursors=300  
*.pga_aggregate_target=1024m  
*.processes=320  
*.remote_login_passwordfile='EXCLUSIVE'  
*.sga_target=10240m  
*.undo_tablespace='UNDOTBS1'
```

Die oben genannte init-Datei sollte im Falle einer Abweichung durch eine wiederhergestellte Backup-init-Datei vom primären Oracle VLDB-Server ersetzt werden.

11. Starten Sie als oracle-Benutzer RMAN, um Oracle Recovery auf dem Standby-DB-Server-Host auszuführen. Starten Sie zunächst die Oracle-Instanz in `nomount` Bundesland.

```
[oracle@ora-02 ~]$ rman target / nocatalog

Recovery Manager: Release 19.0.0.0.0 - Production on Fri Mar 22
16:02:55 2024
Version 19.18.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates. All rights
reserved.

connected to target database (not started)

RMAN> startup nomount;

Oracle instance started

Total System Global Area      10737418000 bytes

Fixed Size                     9174800 bytes
Variable Size                  1577058304 bytes
Database Buffers               9126805504 bytes
Redo Buffers                    24379392 bytes
```

12. Datenbank-ID festlegen. Die Datenbank-ID kann aus dem Oracle-Dateinamen der Image-Kopie am ANF NFS-Bereitstellungspunkt abgerufen werden.

```
RMAN> set dbid = 2441823937;

executing command: SET DBID
```

13. Stellen Sie die controlfile aus dem automatischen Backup wieder her. Wenn Oracle controlfile und spfile autobackup aktiviert sind, werden sie in jedem inkrementellen Backup- und Merge-Zyklus gesichert. Die letzte Sicherung wird wiederhergestellt, wenn mehrere Kopien verfügbar sind.

```

RMAN> restore controlfile from autobackup;

Starting restore at 22-MAR-24
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=2 device type=DISK

recovery area destination: /nfsanf/archlog/
database name (or database unique name) used for search: NTAP1
channel ORA_DISK_1: AUTOBACKUP
/nfsanf/archlog/NTAP1/autobackup/2024_03_22/o1_mf_s_1164296325__9z77
zyxb_.bkp found in the recovery area
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20240322
channel ORA_DISK_1: restoring control file from AUTOBACKUP
/nfsanf/archlog/NTAP1/autobackup/2024_03_22/o1_mf_s_1164296325__9z77
zyxb_.bkp
channel ORA_DISK_1: control file restore from AUTOBACKUP complete
output file name=/nfsanf/oracopy/NTAP1.ctl
Finished restore at 22-MAR-24

```

14. Wiederherstellen der init-Datei aus spfile in einen /tmp-Ordner, um die Parameterdatei später zu aktualisieren und mit der primären VLDB zu vergleichen.

```

RMAN> restore spfile to pfile '/tmp/archive/initNTAP1.ora' from
autobackup;

Starting restore at 22-MAR-24
using channel ORA_DISK_1

recovery area destination: /nfsanf/archlog/
database name (or database unique name) used for search: NTAP1
channel ORA_DISK_1: AUTOBACKUP
/nfsanf/archlog/NTAP1/autobackup/2024_03_22/o1_mf_s_1164296325__9z77
zyxb_.bkp found in the recovery area
channel ORA_DISK_1: looking for AUTOBACKUP on day: 20240322
channel ORA_DISK_1: restoring spfile from AUTOBACKUP
/nfsanf/archlog/NTAP1/autobackup/2024_03_22/o1_mf_s_1164296325__9z77
zyxb_.bkp
channel ORA_DISK_1: SPFILE restore from AUTOBACKUP complete
Finished restore at 22-MAR-24

```

15. Mounten Sie die Steuerdatei und validieren Sie die Image-Kopie des Datenbank-Backup.

```

RMAN> alter database mount;

```

released channel: ORA_DISK_1

Statement processed

RMAN> list copy of database tag 'ORACOPYBKUPONANF_LEVEL_0';

List of Datafile Copies

=====

Key	File S	Completion Time	Ckp SCN	Ckp Time	Sparse
82	1 A	22-MAR-24	4598427	22-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-1_1t2m9nij				
	Tag: ORACOPYBKUPONANF_LEVEL_0				
83	3 A	22-MAR-24	4598423	22-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-3_1u2m9nog				
	Tag: ORACOPYBKUPONANF_LEVEL_0				
84	4 A	22-MAR-24	4598431	22-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-4_1v2m9nu6				
	Tag: ORACOPYBKUPONANF_LEVEL_0				
58	5 A	21-MAR-24	2379694	18-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-5_282m9oem				
	Tag: ORACOPYBKUPONANF_LEVEL_0				
	Container ID: 2, PDB Name: PDB\$SEED				
52	6 A	21-MAR-24	2379694	18-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-6_242m9oan				
	Tag: ORACOPYBKUPONANF_LEVEL_0				
	Container ID: 2, PDB Name: PDB\$SEED				
90	7 A	22-MAR-24	4598462	22-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-7_2c2m9ofn				
	Tag: ORACOPYBKUPONANF_LEVEL_0				
59	8 A	21-MAR-24	2379694	18-MAR-24	NO
	Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-8_292m9oem				
	Tag: ORACOPYBKUPONANF_LEVEL_0				

Container ID: 2, PDB Name: PDB\$SEED

```
71      9      A 22-MAR-24      4598313      22-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-9_252m9oc5
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 3, PDB Name: NTAP1_PDB1

68      10     A 22-MAR-24      4598308      22-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAUX_FNO-10_212m9o52
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 3, PDB Name: NTAP1_PDB1

66      11     A 22-MAR-24      4598304      22-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-11_202m9o22
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 3, PDB Name: NTAP1_PDB1

74      12     A 22-MAR-24      4598318      22-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-12_2d2m9ofs
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 3, PDB Name: NTAP1_PDB1

86      13     A 22-MAR-24      4598445      22-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-13_262m9oca
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 4, PDB Name: NTAP1_PDB2

85      14     A 22-MAR-24      4598437      22-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAUX_FNO-14_222m9o53
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 4, PDB Name: NTAP1_PDB2

87      15     A 22-MAR-24      4598454      22-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-15_2a2m9of6
      Tag: ORACOPYBKUPONANF_LEVEL_0
      Container ID: 4, PDB Name: NTAP1_PDB2

89      16     A 22-MAR-24      4598466      22-MAR-24      NO
      Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
```

```

USERS_FNO-16_2e2m9og8
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 4, PDB Name: NTAP1_PDB2

91      17      A 22-MAR-24      4598450      22-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSTEM_FNO-17_272m9oel
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 5, PDB Name: NTAP1_PDB3

88      18      A 22-MAR-24      4598441      22-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
SYSAUX_FNO-18_232m9oa8
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 5, PDB Name: NTAP1_PDB3

92      19      A 22-MAR-24      4598458      22-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
UNDOTBS1_FNO-19_2b2m9ofn
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 5, PDB Name: NTAP1_PDB3

93      20      A 22-MAR-24      4598470      22-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-
USERS_FNO-20_2f2m9og8
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 5, PDB Name: NTAP1_PDB3

81      21      A 22-MAR-24      4598318      22-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
21_1h2m9cap
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 3, PDB Name: NTAP1_PDB1

72      22      A 22-MAR-24      4598304      22-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
22_1i2m9cap
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 3, PDB Name: NTAP1_PDB1

73      23      A 22-MAR-24      4598308      22-MAR-24      NO
  Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
23_1j2m9cap
  Tag: ORACOPYBKUPONANF_LEVEL_0
  Container ID: 3, PDB Name: NTAP1_PDB1

```


80	24	A	22-MAR-24	4598313	22-MAR-24	NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-						
24_1k2m9cap						
Tag: ORACOPYBKUPONANF_LEVEL_0						
Container ID: 3, PDB Name: NTAP1_PDB1						
79	25	A	22-MAR-24	4598318	22-MAR-24	NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-						
25_112m9g3u						
Tag: ORACOPYBKUPONANF_LEVEL_0						
Container ID: 3, PDB Name: NTAP1_PDB1						
69	26	A	22-MAR-24	4598304	22-MAR-24	NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-						
26_1m2m9g9j						
Tag: ORACOPYBKUPONANF_LEVEL_0						
Container ID: 3, PDB Name: NTAP1_PDB1						
70	27	A	22-MAR-24	4598308	22-MAR-24	NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-						
27_1n2m9gcg						
Tag: ORACOPYBKUPONANF_LEVEL_0						
Container ID: 3, PDB Name: NTAP1_PDB1						
75	28	A	22-MAR-24	4598313	22-MAR-24	NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-						
28_1o2m9gd4						
Tag: ORACOPYBKUPONANF_LEVEL_0						
Container ID: 3, PDB Name: NTAP1_PDB1						
77	29	A	22-MAR-24	4598318	22-MAR-24	NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-						
29_1p2m9ju6						
Tag: ORACOPYBKUPONANF_LEVEL_0						
Container ID: 3, PDB Name: NTAP1_PDB1						
67	30	A	22-MAR-24	4598304	22-MAR-24	NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-						
30_1q2m9k7a						
Tag: ORACOPYBKUPONANF_LEVEL_0						
Container ID: 3, PDB Name: NTAP1_PDB1						
76	31	A	22-MAR-24	4598308	22-MAR-24	NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-						
31_1r2m9kfk						
Tag: ORACOPYBKUPONANF_LEVEL_0						

```
Container ID: 3, PDB Name: NTAP1_PDB1
```

```
78      32      A 22-MAR-24      4598313      22-MAR-24      NO
Name: /nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-
32_1s2m9kkg
Tag: ORACOPYBKUPONANF_LEVEL_0
Container ID: 3, PDB Name: NTAP1_PDB1
```

16. Wechseln Sie zwischen Datenbank und Kopie, um die Recovery ohne Datenbank-Wiederherstellung auszuführen.

```
RMAN> switch database to copy;
```

```
Starting implicit crosscheck backup at 22-MAR-24
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=12 device type=DISK
Crosschecked 33 objects
Finished implicit crosscheck backup at 22-MAR-24
```

```
Starting implicit crosscheck copy at 22-MAR-24
using channel ORA_DISK_1
Crosschecked 31 objects
Finished implicit crosscheck copy at 22-MAR-24
```

```
searching for all files in the recovery area
cataloging files...
cataloging done
```

```
List of Cataloged Files
```

```
=====
```

```
File Name:
```

```
/nfsanf/archlog/NTAP1/autobackup/2024_03_20/o1_mf_s_1164140565__5g56
ypks_.bkp
```

```
File Name:
```

```
/nfsanf/archlog/NTAP1/autobackup/2024_03_22/o1_mf_s_1164296325__9z77
zyxb_.bkp
```

```
datafile 1 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-1_1t2m9nij"
datafile 3 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-3_1u2m9nog"
datafile 4 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-4_1v2m9nu6"
datafile 5 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-5_282m9oem"
datafile 6 switched to datafile copy "/nfsanf/oracopy/data_D-
```

NTAP1_I-2441823937_TS-SYSAUX_FNO-6_242m9oan"
datafile 7 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-7_2c2m9ofn"
datafile 8 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-8_292m9oem"
datafile 9 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-9_252m9oc5"
datafile 10 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-10_212m9o52"
datafile 11 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-11_202m9o22"
datafile 12 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-12_2d2m9ofs"
datafile 13 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-13_262m9oca"
datafile 14 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-14_222m9o53"
datafile 15 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-15_2a2m9of6"
datafile 16 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-16_2e2m9og8"
datafile 17 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSTEM_FNO-17_272m9oel"
datafile 18 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SYSAUX_FNO-18_232m9oa8"
datafile 19 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-UNDOTBS1_FNO-19_2b2m9ofn"
datafile 20 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-USERS_FNO-20_2f2m9og8"
datafile 21 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-21_1h2m9cap"
datafile 22 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-22_1i2m9cap"
datafile 23 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-23_1j2m9cap"
datafile 24 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-24_1k2m9cap"
datafile 25 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-25_1l2m9g3u"
datafile 26 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-26_1m2m9g9j"
datafile 27 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-27_1n2m9gcg"
datafile 28 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-28_1o2m9gd4"
datafile 29 switched to datafile copy "/nfsanf/oracopy/data_D-

```
NTAP1_I-2441823937_TS-SOE_FNO-29_1p2m9ju6"
datafile 30 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-30_1q2m9k7a"
datafile 31 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-31_1r2m9kfk"
datafile 32 switched to datafile copy "/nfsanf/oracopy/data_D-
NTAP1_I-2441823937_TS-SOE_FNO-32_1s2m9kkg"
```

17. Führen Sie die Oracle Recovery bis zum letzten verfügbaren Archivprotokoll im Flash-Recovery-Bereich aus.

```
RMAN> run {
2> set until sequence=11;
3> recover database;
4> }

executing command: SET until clause

Starting recover at 22-MAR-24
using channel ORA_DISK_1

starting media recovery

archived log for thread 1 with sequence 4 is already on disk as file
/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_4__9y6gn5co_.arc
archived log for thread 1 with sequence 5 is already on disk as file
/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_5__9y7p68s6_.arc
archived log for thread 1 with sequence 6 is already on disk as file
/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_6__9y8ygtss_.arc
archived log for thread 1 with sequence 7 is already on disk as file
/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_7__9ybjdp55_.arc
archived log for thread 1 with sequence 8 is already on disk as file
/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_8__9yctxjgy_.arc
archived log for thread 1 with sequence 9 is already on disk as file
/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_9__9yfrj0b1_.arc
archived log for thread 1 with sequence 10 is already on disk as
file
/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_10__9yomybbc_.ar
c
archived log file
name=/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_4__9y6gn5co
_.arc thread=1 sequence=4
archived log file
name=/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_5__9y7p68s6
_.arc thread=1 sequence=5
archived log file
```

```

name=/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_6__9y8ygtss
_.arc thread=1 sequence=6
archived log file
name=/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_7__9ybjdp55
_.arc thread=1 sequence=7
archived log file
name=/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_8__9yctxjgy
_.arc thread=1 sequence=8
archived log file
name=/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_9__9yfrj0b1
_.arc thread=1 sequence=9
archived log file
name=/nfsanf/archlog/NTAP1/archivelog/2024_03_22/o1_mf_1_10__9yomybb
c_.arc thread=1 sequence=10
media recovery complete, elapsed time: 00:01:17
Finished recover at 22-MAR-24

RMAN> exit

```

Recovery Manager complete.



Für eine schnellere Recovery sollten Sie parallele Sitzungen mit dem Parameter `Recovery_parallelism` aktivieren oder den Grad der Parallelität im Wiederherstellungsbefehl für die Datenbankwiederherstellung angeben: `RECOVER DATABASE PARALLEL (DEGREE d INSTANCES DEFAULT)`; . Im Allgemeinen sollte der Grad der Parallelität der Anzahl der CPU-Kerne auf dem Host entsprechen.

18. Beenden Sie RMAN, melden Sie sich mit sqlplus als oracle-Benutzer an, um die Datenbank zu öffnen und das Protokoll nach einer unvollständigen Recovery zurückzusetzen.

```

SQL> select name, open_mode from v$database;

NAME          OPEN_MODE
-----
NTAP1         MOUNTED

SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME
-----
HOST_NAME
-----

NTAP1
ora-02

```

```
SQL>
```

```
SQL> select member from v$logfile;
```

```
MEMBER
```

```
-----  
-----
```

```
/u03/orareco/NTAP1/onlinelog/redo03.log
```

```
/u03/orareco/NTAP1/onlinelog/redo02.log
```

```
/u03/orareco/NTAP1/onlinelog/redo01.log
```

```
SQL> alter database rename file
```

```
'/u03/orareco/NTAP1/onlinelog/redo01.log' to
```

```
'/nfsanf/oracopy/redo01.log';
```

```
Database altered.
```

```
SQL> alter database rename file
```

```
'/u03/orareco/NTAP1/onlinelog/redo02.log' to
```

```
'/nfsanf/oracopy/redo02.log';
```

```
Database altered.
```

```
SQL> alter database rename file
```

```
'/u03/orareco/NTAP1/onlinelog/redo03.log' to
```

```
'/nfsanf/oracopy/redo03.log';
```

```
Database altered.
```

```
SQL> alter database open resetlogs;
```

```
Database altered.
```

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	NTAP1_PDB1	READ WRITE	NO
4	NTAP1_PDB2	READ WRITE	NO
5	NTAP1_PDB3	READ WRITE	NO

19. Validieren Sie die auf dem neuen Host wiederhergestellte Datenbankstruktur sowie die Testreihe, die wir vor dem primären VLDB-Fehler eingefügt haben.

```
SQL> select name from v$datafile;
```

```
NAME
```

```
-----  
-----  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-1_1t2m9nij  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-3_1u2m9nog  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-4_1v2m9nu6  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-5_282m9oem  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-6_242m9oan  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-7_2c2m9ofn  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-8_292m9oem  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-9_252m9oc5  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-10_212m9o52  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-  
11_202m9o22  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-12_2d2m9ofs
```

```
NAME
```

```
-----  
-----  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-13_262m9oca  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-14_222m9o53  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-  
15_2a2m9of6  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-16_2e2m9og8  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSTEM_FNO-17_272m9oe1  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SYSAUX_FNO-18_232m9oa8  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-UNDOTBS1_FNO-  
19_2b2m9ofn  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-USERS_FNO-20_2f2m9og8  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-21_1h2m9cap  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-22_1i2m9cap  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-23_1j2m9cap
```

```
NAME
```

```
-----  
-----  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-24_1k2m9cap  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-25_1l2m9g3u  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-26_1m2m9g9j  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-27_1n2m9gcg  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-28_1o2m9gd4  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-29_1p2m9ju6  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-30_1q2m9k7a  
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-31_1r2m9kfk
```

```
/nfsanf/oracopy/data_D-NTAP1_I-2441823937_TS-SOE_FNO-32_1s2m9kgg
```

```
31 rows selected.
```

```
SQL> select member from v$logfile;
```

```
MEMBER
```

```
-----  
-----
```

```
/nfsanf/oracopy/redo03.log
```

```
/nfsanf/oracopy/redo02.log
```

```
/nfsanf/oracopy/redo01.log
```

```
SQL> select name from v$controlfile;
```

```
NAME
```

```
-----  
-----
```

```
/nfsanf/oracopy/NTAP1.ctl
```

```
SQL> alter session set container=ntap1_pdb1;
```

```
Session altered.
```

```
SQL> select * from test;
```

```
          ID
```

```
-----  
-----
```

```
DT
```

```
-----  
-----
```

```
EVENT
```

```
-----  
-----
```

```
          1
```

```
21-MAR-24 03.15.03.000000 PM
```

```
test oracle incremental merge switch to copy
```

```
          2
```

```
22-MAR-24 02.22.06.000000 PM
```

```
test recovery on a new Azure VM host with image copy on ANF
```

20. Löschen Sie ungültige Tempfiles und fügen Sie neue Tempfiles zu temporären Tablespaces hinzu.

```
SQL> select name from v$tempfile;
```



```
NAME
```

```
-----  
-----
```

```
/u02/oradata/NTAP1/NTAP1_pdb1/temp01.dbf
```

```
/u02/oradata/NTAP1/NTAP1_pdb1/temp02.dbf
```

```
SQL> alter tablespace temp add tempfile  
'/nfsanf/oracopy/ntap1_pdb1_temp01.dbf' size 100M;
```

```
Tablespace altered.
```

```
SQL> select name from v$tempfile;
```

```
NAME
```

```
-----  
-----
```

```
/u02/oradata/NTAP1/NTAP1_pdb1/temp01.dbf
```

```
/u02/oradata/NTAP1/NTAP1_pdb1/temp02.dbf
```

```
/nfsanf/oracopy/ntap1_pdb1_temp01.dbf
```

```
SQL> alter database tempfile  
'/u02/oradata/NTAP1/NTAP1_pdb1/temp01.dbf' offline;
```

```
Database altered.
```

```
SQL> alter database tempfile  
'/u02/oradata/NTAP1/NTAP1_pdb1/temp01.dbf' drop;
```

```
Database altered.
```

```
SQL> alter database tempfile  
'/u02/oradata/NTAP1/NTAP1_pdb1/temp02.dbf' offline;
```

```
Database altered.
```

```
SQL> alter database tempfile  
'/u02/oradata/NTAP1/NTAP1_pdb1/temp02.dbf' drop;
```

```
Database altered.
```

```
SQL> select name from v$tempfile;
```

```
NAME
```

```
-----  
-----
```

```
/nfsanf/oracopy/ntap1_pdb1_temp01.dbf
```

SQL>

21. Andere Aufgaben nach der Wiederherstellung

- Add ANF NFS mount to fstab so that the NFS file system will be mounted when DB server host rebooted.

As azureuser, sudo vi /etc/fstab and add following entry:

```
172.30.136.68:/ora-01-u02-copy      /nfsanf      nfs
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsiz=262144,wsiz=262144,noi
tr 0      0
```

- Update the Oracle init file from primary database init file backup that is restored to /tmp/archive and create spfile as needed.

Damit ist die Wiederherstellung der Oracle VLDB-Datenbank von der Backup-Image-Kopie auf dem ANF NFS-Dateisystem auf einen Standby-DB-Server-Host abgeschlossen.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- RMAN: Zusammengeführte inkrementelle Backup-Strategien (Doc-ID 745798.1)

["https://support.oracle.com/knowledge/Oracle%20Database%20Products/745798_1.html"](https://support.oracle.com/knowledge/Oracle%20Database%20Products/745798_1.html)

- RMAN Backup und Recovery Benutzerhandbuch

["https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/getting-started-rman.html"](https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/getting-started-rman.html)

- Azure NetApp Dateien

["https://azure.microsoft.com/en-us/products/netapp"](https://azure.microsoft.com/en-us/products/netapp)

TR-4987: Vereinfachte, automatisierte Oracle-Implementierung auf Azure NetApp Files mit NFS

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Das Ausführen von latenzkritischen Oracle-Workloads mit hohen Performance-Anforderungen in der Cloud kann eine Herausforderung darstellen. Mit Azure NetApp Files (ANF) können Geschäftsbereichsmitarbeiter und Storage-Experten anspruchsvolle Oracle Workloads ganz einfach ohne Code-Änderungen migrieren und ausführen. Azure NetApp Files wird weithin als zugrunde liegender Shared-File-Storage-Service in verschiedenen Szenarien verwendet, beispielsweise für neue Implementierungen oder Migrationen (Lift and Shift) von Oracle-Datenbanken aus lokalen Umgebungen zu Azure.

In dieser Dokumentation wird die vereinfachte Implementierung von Oracle-Datenbanken in Azure NetApp Files über NFS-Mounts mithilfe von Ansible-Automatisierung demonstriert. Die Oracle Datenbank wird in einer Konfiguration mit Container-Datenbank (CDB) und steckbaren Datenbanken (PDB) implementiert, wobei das Oracle dNFS-Protokoll aktiviert ist, um die Performance zu steigern. Darüber hinaus kann die lokale Oracle Single Instance-Datenbank oder PDB mithilfe automatisierter PDB-Versetzungsmethodik mit minimaler Serviceunterbrechung in eine neu implementierte Container-Datenbank in Azure migriert werden. Er bietet auch Informationen zu schnellen Backups, Wiederherstellungen und Klonvorgängen für Oracle-Datenbanken mit dem UI-Tool von NetApp SnapCenter in der Azure Cloud.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Automatisierte Implementierung von Oracle Container-Datenbanken auf Azure NetApp Files
- Automatisierte Migration der Oracle-Datenbank zwischen On-Premises und der Azure Cloud

Zielgruppe

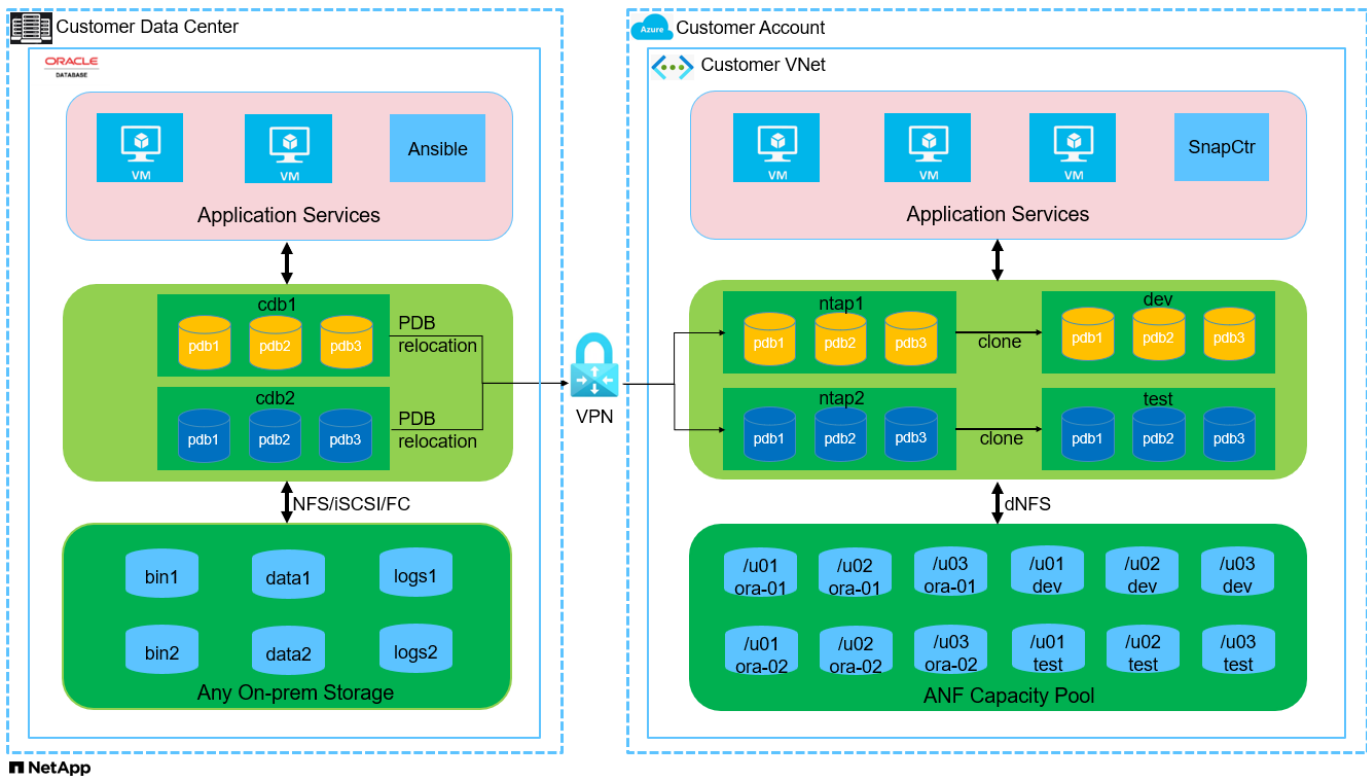
Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle auf Azure NetApp Files implementieren möchte.
- Ein Solution Architect für Datenbanken, der Oracle-Workloads auf Azure NetApp Files testen möchte.
- Ein Storage-Administrator, der eine Oracle Datenbank auf Azure NetApp Files implementieren und managen möchte.
- Ein Applikationseigentümer, der eine Oracle Database auf Azure NetApp Files einrichten möchte.

Test- und Validierungsumgebung der Lösung

Die Lösung wurde in einer Testumgebung getestet und validiert. Siehe Abschnitt [\[Key Factors for Deployment Consideration\]](#) Finden Sie weitere Informationen.

Der Netapp Architektur Sind



Hardware- und Softwarekomponenten

Hardware		
Azure NetApp Dateien	Aktuelles Angebot in Azure von Microsoft	Ein Kapazitäts-Pool mit Premium-Service-Level
Azure VM für DB-Server	Standard_B4ms – 4 vCPUs, 16 gib	Zwei virtuelle Linux-Maschineninstanzen für die gleichzeitige Bereitstellung
Azure VM für SnapCenter	Standard_B4ms – 4 vCPUs, 16 gib	Eine virtuelle Windows-Maschineninstanz
Software		
Redhat Linux	RHEL Linux 8.6 (LVM) – x64 Gen2	Bereitstellung der RedHat Subscription für Tests
Windows Server	2022 DataCenter; Azure Edition Hotpatch - x64 Gen2	Hosting von SnapCenter-Servern
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
SnapCenter Server	Version 5.0	Workgroup-Bereitstellung
Öffnen Sie JDK	Version java-11-openjdk	Anforderungen für SnapCenter Plugin auf DB VMs

NFS	Version 3.0	Oracle dNFS aktiviert
Ansible	Kern 2.16.2	Python 3.6.8

Konfiguration der Oracle-Datenbank in der Laborumgebung

Server	* Datenbank*	DB-Speicher
ora-01	NTAP1(NTAP1_PDB1,NTAP1_PDB2,NTAP1_PDB3)	/U01, /u02, /u03 NFS-Mounts auf ANF-Kapazitäts-Pool
ora-02	NTAP2(NTAP2_PDB1,NTAP2_PDB2,NTAP2_PDB3)	/U01, /u02, /u03 NFS-Mounts auf ANF-Kapazitäts-Pool

Wichtige Faktoren für die Implementierung

- **Speicherlayout der Oracle-Datenbank.** in dieser automatisierten Oracle-Implementierung stellen wir drei Datenbankvolumes für jede Datenbank bereit, um standardmäßig Oracle-Binärdaten, -Daten und -Protokolle zu hosten. Die Volumes werden auf Oracle DB Server als /u01 - binär, /u02 - Data, /u03 - logs via NFS eingebunden. Dual-Control-Dateien werden auf den Mount-Punkten /u02 und /u03 für Redundanz konfiguriert.
- **Implementierung mehrerer DB-Server.** die Automatisierungslösung kann eine Oracle-Container-Datenbank auf mehreren DB-Servern in einem einzelnen Ansible-Playbook bereitstellen. Unabhängig von der Anzahl der DB-Server bleibt die Playbook-Ausführung gleich. Sie können mehrere Container-Datenbanken auf einer einzelnen VM-Instanz implementieren, indem Sie die Implementierung mit unterschiedlichen Datenbankinstanzkennungen (Oracle SID) wiederholen. Stellen Sie jedoch sicher, dass auf dem Host ausreichend Speicher zur Unterstützung der bereitgestellten Datenbanken vorhanden ist.
- **DNFS-Konfiguration.** mit dNFS (verfügbar seit Oracle 11g) kann eine Oracle-Datenbank, die auf einer Azure Virtual Machine ausgeführt wird, deutlich mehr I/O als der native NFS-Client steuern. Die automatisierte Oracle-Implementierung konfiguriert dNFS standardmäßig auf NFSv3.
- **Zuweisen großer Volumes zur Beschleunigung der Bereitstellung.** der ANF Filesystem-I/O-Durchsatz wird basierend auf der Größe des Volumes geregelt. Bei der ersten Bereitstellung können große Volumes zugewiesen werden, um die Implementierung zu beschleunigen. Die Volumes können anschließend dynamisch ohne Beeinträchtigung der Applikationen skaliert werden.
- **Datenbanksicherung.** NetApp bietet eine SnapCenter Software Suite für Datenbank-Backup, -Wiederherstellung und -Klonen mit einer benutzerfreundlichen Benutzeroberfläche. NetApp empfiehlt die Implementierung eines solchen Managementtools, um Snapshots schnell (unter einer Minute), schnelle Datenbank-Restores (in Minuten) und Datenbankklone zu ermöglichen.

Lösungsimplementierung

In den folgenden Abschnitten werden Schritt-für-Schritt-Verfahren für die automatisierte Implementierung von Oracle 19c und die Datenbankmigration auf Azure NetApp Files mit direkt gemounteten Datenbank-Volumes über NFS zu Azure VMs beschrieben.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Ein Azure-Konto wurde eingerichtet und die erforderlichen vnet- und Netzwerksegmente wurden in Ihrem Azure-Konto erstellt.
2. Implementieren Sie im Azure-Cloud-Portal Azure Linux-VMs als Oracle DB-Server. Erstellen Sie einen Azure NetApp Files-Kapazitätspool und Datenbank-Volumes für die Oracle-Datenbank. VM-SSH-Authentifizierung für privaten/öffentlichen Schlüssel für Azure-Benutzer für DB-Server aktivieren. Details zur Umgebungs-Einrichtung finden Sie im Architekturdiagramm im vorherigen Abschnitt. Auch genannt "[Schritt-für-Schritt-Anweisungen zur Oracle-Implementierung auf Azure VM und Azure NetApp Files](#)" Ausführliche Informationen finden Sie unter.



Stellen Sie bei Azure-VMs, die mit lokaler Festplattenredundanz implementiert werden, sicher, dass Sie mindestens 128 G auf der VM-Root-Festplatte zugewiesen haben, damit ausreichend Speicherplatz für die Bereitstellung von Oracle-Installationsdateien und die Hinzufügen der OS-Swap-Datei zur Verfügung steht. Erweitern Sie die Partition /tmpv und /rootlv OS entsprechend. Stellen Sie sicher, dass die Benennung des Datenbank-Volumes der Konvention VMname-u01, VMname-u02 und VMname-u03 entspricht.

```
sudo lvresize -r -L +20G /dev/mapper/rootvg-rootlv
```

```
sudo lvresize -r -L +10G /dev/mapper/rootvg-tmplv
```

3. Stellen Sie im Azure-Cloud-Portal einen Windows-Server bereit, damit das UI-Tool NetApp SnapCenter mit der neuesten Version ausgeführt wird. Details finden Sie unter folgendem Link: "[Installieren Sie den SnapCenter-Server](#)"
4. Stellen Sie eine Linux VM als Ansible-Controller-Node mit der neuesten Version von Ansible und Git bereit. Details finden Sie unter folgendem Link: "[Erste Schritte mit der Automatisierung von NetApp Lösungen](#)" In Abschnitt -
Setup the Ansible Control Node for CLI deployments on RHEL / CentOS Oder
Setup the Ansible Control Node for CLI deployments on Ubuntu / Debian.



Der Ansible-Controller-Node kann entweder On-PreMises oder in der Azure-Cloud finden, sofern er Azure DB VMs über ssh-Port erreichen kann.

5. Klonen Sie eine Kopie des NetApp Toolkit zur Implementierungsautomatisierung für NFS.

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-  
bb/na_oracle_deploy_nfs.git
```

6. Stellen Sie die folgenden Oracle 19c-Installationsdateien auf das Azure DB VM /tmp/Archive-Verzeichnis mit 777 Berechtigungen bereit.

```
installer_archives:
  - "LINUX.X64_193000_db_home.zip"
  - "p34765931_190000_Linux-x86-64.zip"
  - "p6880880_190000_Linux-x86-64.zip"
```

7. Sehen Sie sich das folgende Video an:

[Vereinfachte und automatisierte Oracle-Implementierung auf Azure NetApp Files mit NFS](#)

Automatisierungsparameter-Dateien

In dem Playbook „Ansible“ werden die Installations- und Konfigurationsaufgaben von Datenbanken mit vordefinierten Parametern ausgeführt. Für diese Oracle-Automatisierungslösung gibt es drei benutzerdefinierte Parameterdateien, die vor der Ausführung des Playbooks Benutzereingaben erfordern.

- Hosts: Legen Sie Ziele fest, für die das Automatisierungs-Playbook ausgeführt wird.
- vars/vars.yml - die globale Variablendatei, die Variablen definiert, die für alle Ziele gelten.
- Host_VARS/Host_Name.yml - die lokale Variablendatei, die Variablen definiert, die nur auf ein benanntes Ziel angewendet werden. In unserem Anwendungsbeispiel handelt es sich um die Oracle DB-Server.

Zusätzlich zu diesen benutzerdefinierten Variablendateien gibt es mehrere standardmäßige Variablendateien, die Standardparameter enthalten, die nicht geändert werden müssen, sofern dies nicht erforderlich ist. In den folgenden Abschnitten wird die Konfiguration der benutzerdefinierten Variablendateien erläutert.

Konfiguration von Parameterdateien

1. Ansible Ziel hosts Dateikonfiguration:

```
# Enter Oracle servers names to be deployed one by one, follow by
each Oracle server public IP address, and ssh private key of
azureuser for the server.
[oracle]
ora-01 ansible_host=10.61.180.21 ansible_ssh_private_key_file=ora-
01.pem
ora-02 ansible_host=10.61.180.23 ansible_ssh_private_key_file=ora-
02.pem
```

2. Weltweit vars/vars.yml Dateikonfiguration


```

#####
##
##### Oracle 19c deployment user configuration variables
#####
##### Consolidate all variables from ANF, linux and oracle
#####
#####
#####

#####
### ANF env specific config variables   ###
#####

# Prerequisite to create three volumes in NetApp storage pool from
cloud dashboard with following naming convention:
# db_hostname-u01 - Oracle binary
# db_hostname-u02 - Oracle data
# db_hostname-u03 - Oracle redo
# It is important to strictly follow the name convention or the
automation will fail.

# NFS lif ip address to access database volumes in ANF storage pool
(retrievable from cloud dashboard)
nfs_lif: 172.30.136.68

#####
### Linux env specific config variables ###
#####

redhat_sub_username: XXXXXXXXX
redhat_sub_password: XXXXXXXXX

#####
### DB env specific install and config variables ###
#####

# Database domain name
db_domain: solutions.netapp.com

# Set initial password for all required Oracle passwords. Change
them after installation.
initial_pwd_all: XXXXXXXXX

```

3. Lokaler DB-Server host_vars/host_name.yml Konfiguration wie ora_01.yml, ora_02.yml ...

```
# User configurable Oracle host specific parameters

# Enter container database SID. By default, a container DB is
created with 3 PDBs within the CDB
oracle_sid: NTAP1

# Enter database shared memory size or SGA. CDB is created with SGA
at 75% of memory_limit, MB. The grand total of SGA should not exceed
75% available RAM on node.
memory_limit: 8192
```

Ausführung des Playbook

Das Automatisierungs-Toolkit enthält insgesamt fünf Playbooks. Jede führt unterschiedliche Aufgabenblöcke aus und erfüllt unterschiedliche Zwecke.

```
0-all_playbook.yml - execute playbooks from 1-4 in one playbook run.
1-ansible_requirements.yml - set up Ansible controller with required
libs and collections.
2-linux_config.yml - execute Linux kernel configuration on Oracle DB
servers.
4-oracle_config.yml - install and configure Oracle on DB servers and
create a container database.
5-destroy.yml - optional to undo the environment to dismantle all.
```

Es gibt drei Optionen, um Playbooks mit den folgenden Befehlen auszuführen.

1. Führen Sie alle Playbooks für die Implementierung in einem kombinierten Durchlauf aus.

```
ansible-playbook -i hosts 0-all_playbook.yml -u azureuser -e
@vars/vars.yml
```

2. Führen Sie Playbooks einzeln mit der Zahlenfolge von 1 bis 4 aus.

```
ansible-playbook -i hosts 1-ansible_requirements.yml -u azureuser -e
@vars/vars.yml
```

```
ansible-playbook -i hosts 2-linux_config.yml -u azureuser -e
@vars/vars.yml
```

```
ansible-playbook -i hosts 4-oracle_config.yml -u azureuser -e
@vars/vars.yml
```

3. Führen Sie 0-all_Playbook.yml mit einem Tag aus.

```
ansible-playbook -i hosts 0-all_playbook.yml -u azureuser -e
@vars/vars.yml -t ansible_requirements
```

```
ansible-playbook -i hosts 0-all_playbook.yml -u azureuser -e
@vars/vars.yml -t linux_config
```

```
ansible-playbook -i hosts 0-all_playbook.yml -u azureuser -e  
@vars/vars.yml -t oracle_config
```

4. Die Umgebung rückgängig machen

```
ansible-playbook -i hosts 5-destroy.yml -u azureuser -e  
@vars/vars.yml
```

Validierung nach der Ausführung

Melden Sie sich nach der Ausführung des Playbook bei der VM des Oracle DB Servers an, um zu überprüfen, ob Oracle installiert und konfiguriert ist und eine Container-Datenbank erfolgreich erstellt wurde. Im Folgenden finden Sie ein Beispiel für die Validierung von Oracle-Datenbanken auf Host ora-01.

1. Validieren von NFS-Mounts

```
[azureuser@ora-01 ~]$ cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Thu Sep 14 11:04:01 2023
#
# Accessible filesystems, by reference, are maintained under
# '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for
# more info.
#
# After editing this file, run 'systemctl daemon-reload' to update
# systemd
# units generated from this file.
#
/dev/mapper/rootvg-rootlv /                xfs      defaults
0 0
UUID=268633bd-f9bb-446d-9a1d-8fca4609a1e1 /boot
xfs      defaults          0 0
UUID=89D8-B037 /boot/efi          vfat
defaults,uid=0,gid=0,umask=077,shortname=winnt 0 2
/dev/mapper/rootvg-homelv /home          xfs      defaults
0 0
/dev/mapper/rootvg-tmplv /tmp           xfs      defaults
0 0
/dev/mapper/rootvg-usrlv /usr           xfs      defaults
0 0
/dev/mapper/rootvg-varlv /var           xfs      defaults
0 0
/mnt/swapfile swap swap defaults 0 0
172.30.136.68:/ora-01-u01 /u01 nfs
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536 0 0
172.30.136.68:/ora-01-u02 /u02 nfs
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536 0 0
172.30.136.68:/ora-01-u03 /u03 nfs
rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536 0 0

[azureuser@ora-01 ~]$ df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  7.7G         0   7.7G  0% /dev
```

```

tmpfs                7.8G    0    7.8G    0% /dev/shm
tmpfs                7.8G   8.6M   7.7G    1% /run
tmpfs                7.8G    0    7.8G    0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv  22G   17G   5.8G   74% /
/dev/mapper/rootvg-usrlv   10G   2.0G   8.1G   20% /usr
/dev/mapper/rootvg-varlv   8.0G   890M   7.2G   11% /var
/dev/sda1             496M  106M   390M   22% /boot
/dev/mapper/rootvg-homelv 1014M   40M   975M    4% /home
/dev/sda15            495M   5.9M   489M    2% /boot/efi
/dev/mapper/rootvg-tmplv   12G   8.4G   3.7G   70% /tmp
tmpfs                1.6G    0    1.6G    0% /run/user/54321
172.30.136.68:/ora-01-u01 500G   11G   490G    3% /u01
172.30.136.68:/ora-01-u03 250G   1.2G   249G    1% /u03
172.30.136.68:/ora-01-u02 250G   7.1G   243G    3% /u02
tmpfs                1.6G    0    1.6G    0% /run/user/1000

```

2. Oracle Listener validieren

```

[azureuser@ora-01 ~]$ sudo su
[root@ora-01 azureuser]# su - oracle
Last login: Thu Feb  1 16:13:44 UTC 2024
[oracle@ora-01 ~]$ lsnrctl status listener.ntap1

LSNRCTL for Linux: Version 19.0.0.0.0 - Production on 01-FEB-2024
16:25:37

Copyright (c) 1991, 2022, Oracle. All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=ora-
01.internal.cloudapp.net)(PORT=1521)))
STATUS of the LISTENER
-----
Alias                LISTENER.NTAP1
Version              TNSLSNR for Linux: Version 19.0.0.0.0 -
Production
Start Date           01-FEB-2024 16:13:49
Uptime                0 days 0 hr. 11 min. 49 sec
Trace Level          off
Security              ON: Local OS Authentication
SNMP                 OFF
Listener Parameter File
/u01/app/oracle/product/19.0.0/NTAP1/network/admin/listener.ora
Listener Log File    /u01/app/oracle/diag/tnslsnr/ora-
01/listener.ntap1/alert/log.xml
Listening Endpoints Summary...

```

```

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp) (HOST=ora-
01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net) (PORT=1521)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc) (KEY=EXTPROC1521)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcps) (HOST=ora-
01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net) (PORT=5500)) (
Security=(my_wallet_directory=/u01/app/oracle/product/19.0.0/NTAP1/a
dmin/NTAP1/xdb_wallet)) (Presentation=HTTP) (Session=RAW))
Services Summary...
Service "104409ac02da6352e063bb891eacf34a.solutions.netapp.com" has
1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "104412c14c2c63cae063bb891eacf64d.solutions.netapp.com" has
1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "1044174670ad63ffe063bb891eac6b34.solutions.netapp.com" has
1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "NTAP1.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "NTAP1XDB.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "ntap1_pdb1.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "ntap1_pdb2.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
Service "ntap1_pdb3.solutions.netapp.com" has 1 instance(s).
  Instance "NTAP1", status READY, has 1 handler(s) for this
service...
The command completed successfully

```

3. Oracle-Datenbank und dNFS validieren

```

[oracle@ora-01 ~]$ cat /etc/oratab
#
# This file is used by ORACLE utilities.  It is created by root.sh
# and updated by either Database Configuration Assistant while
# creating
# a database or ASM Configuration Assistant while creating ASM

```

```

instance.

# A colon, ':', is used as the field terminator.  A new line
terminates
# the entry.  Lines beginning with a pound sign, '#', are comments.
#
# Entries are of the form:
#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:
#
# The first and second fields are the system identifier and home
# directory of the database respectively.  The third field indicates
# to the dbstart utility that the database should , "Y", or should
not,
# "N", be brought up at system boot time.
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
NTAP1:/u01/app/oracle/product/19.0.0/NTAP1:Y

```

```
[oracle@ora-01 ~]$ sqlplus / as sysdba
```

```

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Feb 1 16:37:51 2024
Version 19.18.0.0.0

```

```
Copyright (c) 1982, 2022, Oracle. All rights reserved.
```

```
Connected to:
```

```

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

```

```
SQL> select name, open_mode, log_mode from v$database;
```

NAME	OPEN_MODE	LOG_MODE
NTAP1	READ WRITE	ARCHIVELOG

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	NTAP1_PDB1	READ WRITE	NO
4	NTAP1_PDB2	READ WRITE	NO


```
SQL> select name from v$datafile;
```

```
NAME
```

```
-----  
-----  
/u02/oradata/NTAP1/system01.dbf  
/u02/oradata/NTAP1/sysaux01.dbf  
/u02/oradata/NTAP1/undotbs01.dbf  
/u02/oradata/NTAP1/pdbseed/system01.dbf  
/u02/oradata/NTAP1/pdbseed/sysaux01.dbf  
/u02/oradata/NTAP1/users01.dbf  
/u02/oradata/NTAP1/pdbseed/undotbs01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb1/system01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb1/sysaux01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb1/undotbs01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb1/users01.dbf
```

```
NAME
```

```
-----  
-----  
/u02/oradata/NTAP1/NTAP1_pdb2/system01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb2/sysaux01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb2/undotbs01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb2/users01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb3/system01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb3/sysaux01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb3/undotbs01.dbf  
/u02/oradata/NTAP1/NTAP1_pdb3/users01.dbf
```

```
19 rows selected.
```

```
SQL> select name from v$controlfile;
```

```
NAME
```

```
-----  
-----  
/u02/oradata/NTAP1/control01.ctl  
/u03/orareco/NTAP1/control02.ctl
```

```
SQL> select member from v$logfile;
```

```
MEMBER
```

```
-----  
-----  
/u03/orareco/NTAP1/onlineelog/redo03.log
```

```
/u03/orareco/NTAP1/onlineelog/redo02.log
```

```
/u03/orareco/NTAP1/onlineelog/redo01.log
```

```
SQL> select svrname, dirname, nfsversion from v$dnfs_servers;
```

```
SVRNAME
```

```
-----  
-----
```

```
DIRNAME
```

```
-----  
-----
```

```
NFSVERSION
```

```
-----
```

```
172.30.136.68
```

```
/ora-01-u02
```

```
NFSv3.0
```

```
172.30.136.68
```

```
/ora-01-u03
```

```
NFSv3.0
```

```
SVRNAME
```

```
-----  
-----
```

```
DIRNAME
```

```
-----  
-----
```

```
NFSVERSION
```

```
-----
```

```
172.30.136.68
```

```
/ora-01-u01
```

```
NFSv3.0
```

4. Melden Sie sich bei Oracle Enterprise Manager Express an, um die Datenbank zu validieren.

ORACLE ENTERPRISE MANAGER DATABASE EXPRESS

Username:

Password:

Container Name:

Log In

ORACLE

Copyright 2013, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle Enterprise Manager Database Express

Instance: NTAP1 (19.18.0.0.0) | Performance | Storage

Database Home

Time Zone: Browser (GMT-00:00) | 1 min Auto-Refresh | Refresh

Status

- Up Time: 34 minutes, 43 seconds
- Type: Single Instance (NTAP1)
- CDB (3 PDB(s))
- Version: 19.18.0.0.0 Enterprise Edition
- Platform Name: Linux x86 64-bit
- Thread: 1
- Archiver: Started
- Last Backup Time: N/A
- Incident(s): 1

Performance

Activity Services Containers

Graph showing activity over time (Feb 1, 2024 GMT-05:00).

Resources

- Host CPU: 0%
- Active Sessions: 0
- Memory: 14 GB total, 11.2 GB used
- Data Storage: 3.7 GB total, 2.8 GB used

SQL Monitor - Last Hour (20 max)

Top 20 by Last Active Time

Status	Duration	SQL ID	SQL Plan Hash	User Name	Parallel	Database Time	I/O Requests	SQL Text

Migrieren Sie die Oracle-Datenbank zu Azure

Die Oracle-Datenbankmigration aus lokalen Umgebungen in die Cloud nimmt die Arbeit stark in sich auf. Die richtige Strategie und Automatisierung sorgt für einen reibungslosen Prozess und eine Minimierung von Serviceunterbrechungen und Ausfallzeiten. Befolgen Sie diese detaillierten Anweisungen ["Datenbankmigration von On-Premises-Systemen in die Azure Cloud"](#) Als Leitfaden für Ihre Datenbankmigration.

Backup, Wiederherstellung und Klonen von Oracle mit SnapCenter

NetApp empfiehlt das SnapCenter UI-Tool für das Management der in der Azure-Cloud implementierten Oracle-Datenbank. Informationen finden Sie im Bericht TR-4988: ["Oracle Database Backup, Recovery und Klonen auf ANF mit SnapCenter"](#) Entsprechende Details.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- Oracle Database Backup, Recovery und Klonen auf ANF mit SnapCenter

["Oracle Database Backup, Recovery und Klonen auf ANF mit SnapCenter"](#)

- Azure NetApp Dateien

["https://azure.microsoft.com/en-us/products/netapp"](https://azure.microsoft.com/en-us/products/netapp)

- Bereitstellung von Oracle Direct NFS

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/deploying-dnfs.html#GUID-D06079DB-8C71-4F68-A1E3-A75D7D96DCE2"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/deploying-dnfs.html#GUID-D06079DB-8C71-4F68-A1E3-A75D7D96DCE2)

- Installieren und Konfigurieren von Oracle Database mithilfe von Antwortdateien

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7)

Implementierung und Schutz von Oracle Datenbanken auf Azure NetApp Files

TR-4954: Implementierung und Schutz von Oracle Datenbanken unter Azure NetApp Files

Autor(en): Allen Cao, Niyaz Mohamed, NetApp

Überblick

Viele geschäftskritische Oracle Enterprise-Datenbanken werden nach wie vor lokal gehostet, und viele Unternehmen möchten diese Oracle Datenbanken in eine Public Cloud migrieren. Häufig sind diese Oracle-Datenbanken Applikationsorientierung vorhanden und benötigen daher benutzerspezifische Konfigurationen. Diese Funktionen fehlen bei vielen Public-Cloud-Angeboten für Datenbanken als Service. Aus diesem Grund erfordert die aktuelle Datenbanklandschaft eine Public-Cloud-basierte Oracle Datenbanklösung, die auf einem hochperformanten, skalierbaren Computing- und Storage-Service aufbaut und individuelle Anforderungen erfüllt. Azure Computing-Instanzen für Virtual Machines und der Azure NetApp Files Storage-Service sind möglicherweise die fehlenden Bestandteile dieses Puzzles, das Sie zum Erstellen und Migrieren Ihrer geschäftskritischen Oracle-Datenbank-Workloads in eine Public Cloud nutzen können.

Azure Virtual Machine

Azure Virtual Machines sind eine von mehreren Arten von bedarfsgerechten und skalierbaren Computing-Ressourcen, die Azure bietet. In der Regel wählen Sie eine Virtual Machine, wenn Sie mehr Kontrolle über die Computing-Umgebung benötigen als die anderen Optionen bieten. Mit Azure Virtual Machines lassen sich Computer schnell und einfach mit spezifischen Konfigurationen erstellen, die für die Ausführung der Oracle Datenbank erforderlich sind – sowohl für Rechen- als auch für speicherintensive Workloads. Virtuelle

Maschinen in einem virtuellen Azure-Netzwerk können einfach mit dem Netzwerk Ihres Unternehmens verbunden werden, zum Beispiel über einen gesicherten VPN-Tunnel.

Azure NetApp Dateien (ANF)

Azure NetApp Files ist ein vollständig gemanagter Microsoft Service, mit dem Sie Ihren Datenbank-Workload schneller und sicherer als je zuvor in die Cloud verschieben können. Sie wurde entwickelt, um die Hauptanforderungen der Ausführung hochperformanter Workloads, wie z. B. Oracle Databases in der Cloud, zu erfüllen. Sie bietet Performance-Tiers, die reale IOPS-Anforderungen erfüllen, niedrige Latenz, hohe Verfügbarkeit, hohe Langlebigkeit, einfaches Management nach Maß Backup, Recovery und Klonen können schnell und effizient durchgeführt werden. Diese Funktionen sind möglich, da Azure NetApp Files auf physischen All-Flash ONTAP Systemen basiert, die innerhalb der Azure Datacenter-Umgebung ausgeführt werden. Azure NetApp Files ist vollständig in die Azure Datacenters und das Azure Portal integriert und Kunden können zur Erstellung und Verwaltung von gemeinsam genutzten Dateien wie jedes andere Azure Objekt die gleiche komfortable grafische Oberfläche und APIs verwenden. Mit Azure NetApp File können Sie alle Funktionen von Azure nutzen – ohne zusätzliches Risiko, zusätzliche Kosten oder mehr Zeit. Sie können sich darauf verlassen, dass der einzige Enterprise-Fileservice von Azure nativ ist.

Schlussfolgerung

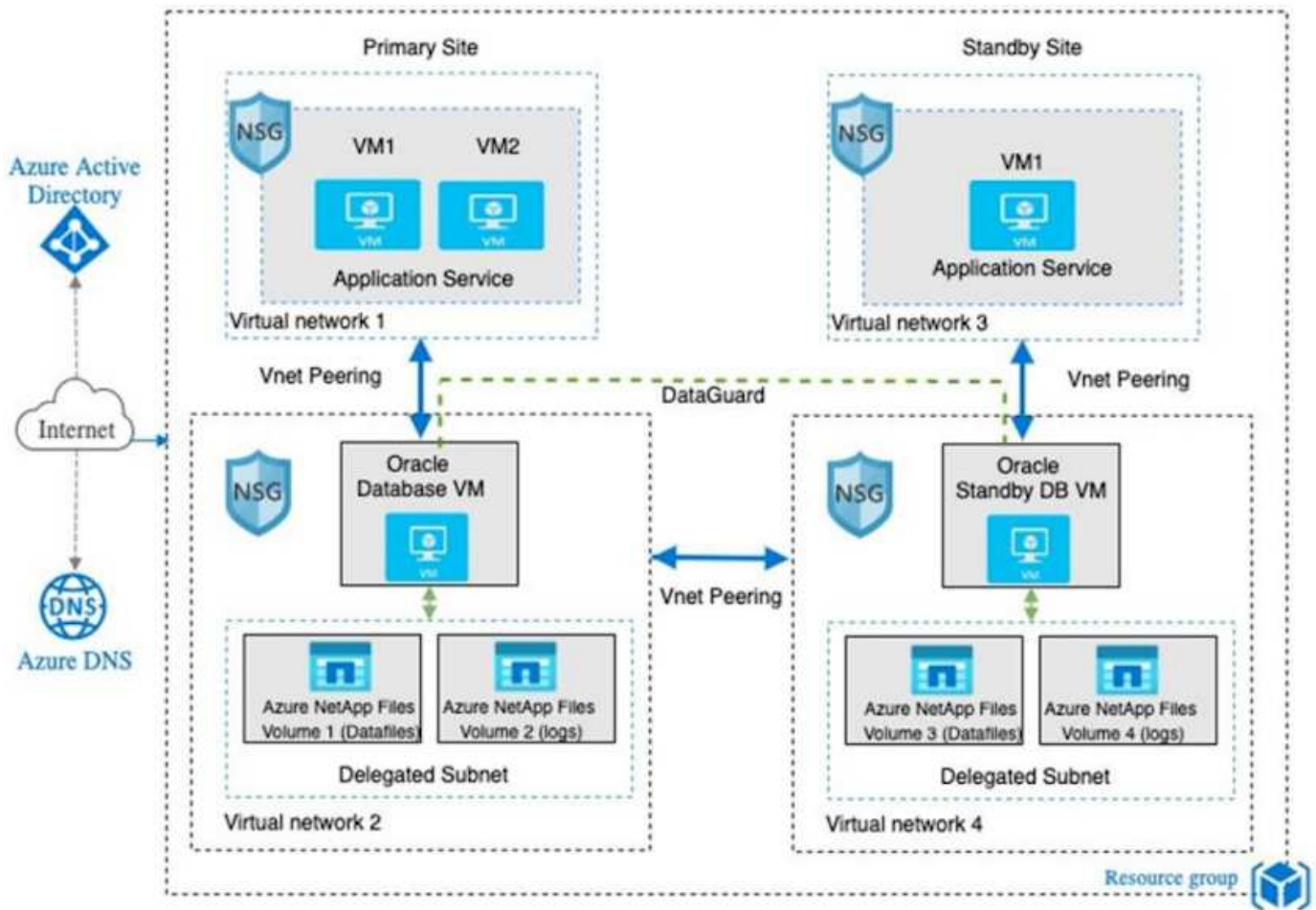
In dieser Dokumentation wird detailliert beschrieben, wie eine Oracle Database mit einer Azure Virtual Machine und einem Azure NetApp Files Storage-Service implementiert, konfiguriert und gesichert wird, der eine Performance und Beständigkeit ähnlich wie bei lokalen Systemen bietet. Best Practices-Anleitung finden Sie im technischen Bericht TR-4780 "[Oracle-Datenbanken auf Microsoft Azure](#)". Zudem stellt NetApp Automatisierungs-Toolkits zur Verfügung, mit denen die meisten Aufgaben automatisiert werden, die für Implementierung, Konfiguration, Datensicherung, Migration und Management Ihrer Oracle Datenbank-Workloads in der Azure Public Cloud erforderlich sind. Die Automatisierungs-Toolkits stehen auf der öffentlichen NetApp GitHub Website zum Download bereit: "[NetApp-Automatisierung](#)".

Lösungsarchitektur

Das folgende Architekturdiagramm zeigt eine hochverfügbare Oracle Datenbankbereitstellung auf Azure VM Instanzen und den Azure NetApp Files Storage.

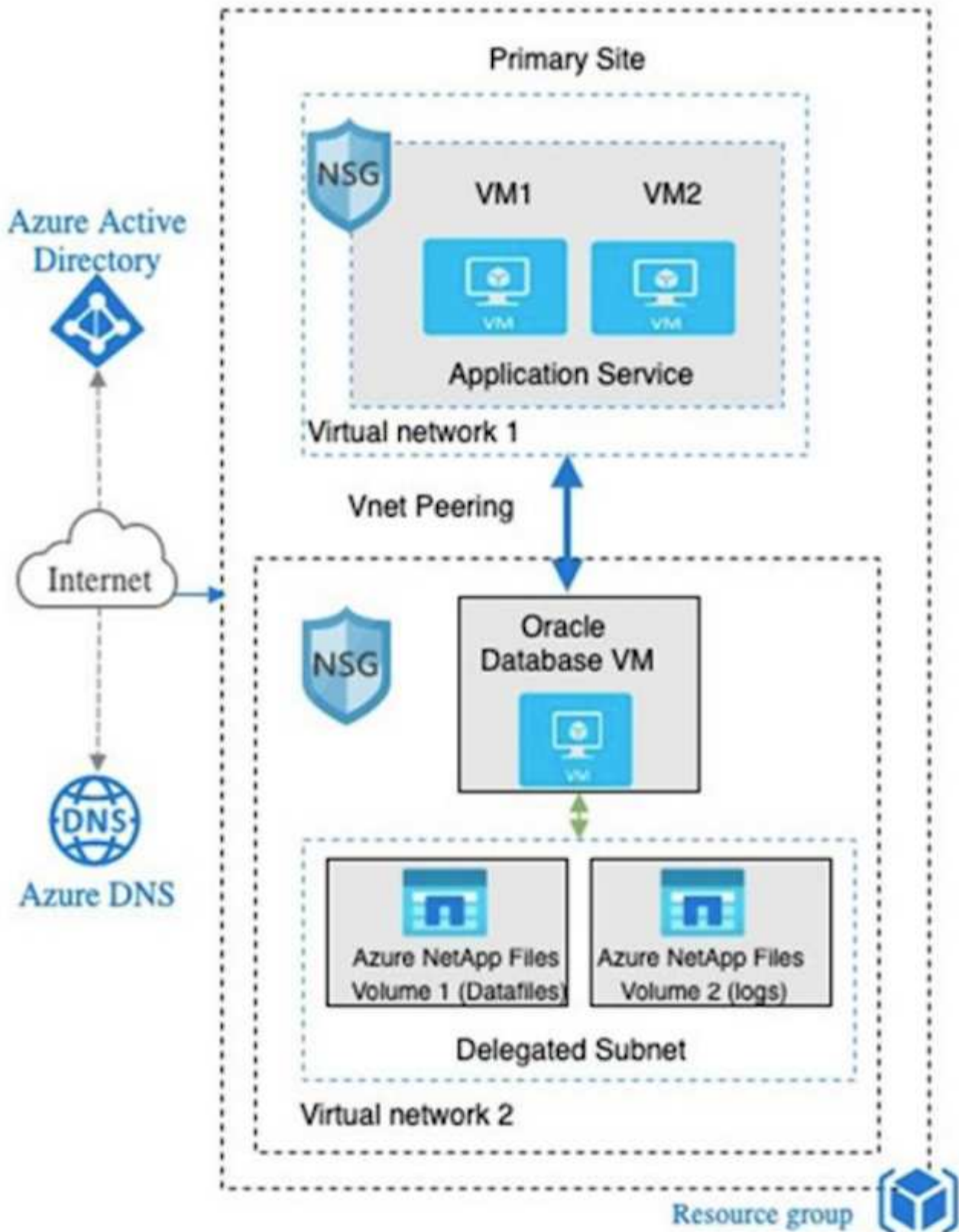
In der Umgebung wird die Oracle Computing-Instanz über eine Azure Services VM Konsole bereitgestellt. In der Konsole sind mehrere Azure Instanztypen verfügbar. NetApp empfiehlt die Implementierung einer datenbankorientierten Azure VM-Instanz, die den erwarteten Workload erfüllt.

Oracle Datenbank-Storage hingegen wird mit dem Azure NetApp Files Service bereitgestellt, der über die Azure-Konsole verfügbar ist. Die Oracle Binär-, Daten- oder Log-Volumes werden anschließend präsentiert und auf einem Azure VM Instance Linux-Host gemountet.



In vielerlei Hinsicht ist die Implementierung von Azure NetApp Files in Azure Cloud einer ONTAP Storage-Architektur vor Ort mit vielen integrierten Redundanzen wie RAID und Dual-Controller sehr ähnlich. Für Disaster Recovery kann ein Standby-Standort in verschiedenen Regionen eingerichtet werden, und die Datenbank kann mithilfe der Replizierung auf Applikationsebene (z. B. Oracle Data Guard) mit dem primären Standort synchronisiert werden.

In unserer Testvalidierung für die Implementierung und Datensicherung von Oracle Datenbanken wird die Oracle Datenbank auf einer einzelnen Azure VM bereitgestellt, wie im folgenden Diagramm dargestellt:



Die Azure Oracle Umgebung kann mit einem Ansible-Controller-Node zur Automatisierung mithilfe von NetApp Tool Kits für Datenbankbereitstellung, Backup, Recovery und Datenbankmigration gemanagt werden. Alle Updates zum Betriebssystemkern oder Oracle Patching der Oracle Azure VM Instance können parallel ausgeführt werden, um das primäre und das Standby-System synchron zu halten. Die anfänglichen Toolkits können sogar problemlos erweitert werden, um bei Bedarf tägliche Oracle-Aufgaben durchzuführen.

Informationen zum Einrichten eines CLI-Ansible-Controllers finden Sie unter ["Automatisierung der NetApp Lösung"](#) Und legen Sie los.

Für die Implementierung von Oracle Database sind Faktoren zu berücksichtigen

Eine Public Cloud bietet eine große Auswahl an Computing- und Storage-Ressourcen. Der Einsatz der richtigen Computing-Instanz und der richtigen Storage Engine ist ein guter Ausgangspunkt für die Datenbankimplementierung. Wählen Sie außerdem Computing- und Storage-Konfigurationen aus, die für Oracle Datenbanken optimiert sind.

In den folgenden Abschnitten werden die wichtigsten Überlegungen bei der Implementierung einer Oracle Database in der Azure Public Cloud auf einer Azure Virtual Machine Instanz mit Azure NetApp Files Storage beschrieben.

VM-Typ und Größenbestimmung

Die Auswahl des richtigen VM-Typs und der richtigen Größe ist für die optimale Performance einer relationalen Datenbank in einer Public Cloud wichtig. Eine Azure Virtual Machine bietet eine Vielzahl von Computing-Instanzen, die zum Hosten von Oracle Datenbank-Workloads verwendet werden können. Siehe Microsoft-Dokumentation ["Größen für die Virtual Machines in Azure"](#) Für unterschiedliche Arten von Azure Virtual Machines und ihre Größenbestimmung. Im Allgemeinen empfiehlt NetApp die Nutzung einer allgemeinen Azure Virtual Machine für die Implementierung kleiner und mittlerer Oracle Datenbanken. Für den Einsatz größerer Oracle-Datenbanken eignet sich eine speicheroptimierte Azure VM. Mit mehr verfügbarem RAM kann ein größerer Oracle SGA- oder Smart Flash-Cache konfiguriert werden, um den physischen I/O zu verringern, wodurch wiederum die Datenbank-Performance verbessert wird.

Azure NetApp Files arbeitet als NFS-Mount mit Anbindung an eine Azure Virtual Machine. Dies bietet einen höheren Durchsatz und überwindet das Storage-optimierte VM-Durchsatzlimit mit dem lokalen Storage. Daher könnte die Nutzung von Oracle auf Azure NetApp Files die Anzahl der lizenzierbaren CPU-Kerne und die Lizenzkosten von Oracle reduzieren. Siehe ["TR-4780: Oracle Databases on Microsoft Azure"](#), Abschnitt 7 - Wie funktioniert Oracle-Lizenzierung?

Weitere Faktoren, die Sie berücksichtigen sollten:

- Wählen Sie basierend auf Workload-Merkmalen die richtige vCPU- und RAM-Kombination aus. Wenn sich die RAM-Größe auf der VM erhöht, steigt auch die Anzahl der vCPU-Kerne. Es sollte zu einem bestimmten Zeitpunkt ein Gleichgewicht geben, da die Oracle Lizenzgebühren auf der Anzahl der vCPU-Kerne berechnet werden.
- Fügen Sie Swap-Speicherplatz zu einer VM hinzu. Die standardmäßige Implementierung von Azure VMs erstellt keinen Swap-Speicherplatz, der nicht für eine Datenbank optimal ist.

Performance von Azure NetApp Files

Azure NetApp Files Volumes werden aus einem Kapazitäts-Pool zugewiesen, den der Kunde in seinem Azure NetApp Files Storage-Konto bereitstellen muss. Jeder Kapazitäts-Pool wird wie folgt zugewiesen:

- Auf ein Service Level, das die allgemeine Performance definiert.
- Die anfänglich bereitgestellte Speicherkapazität oder das Tiering für diesen Kapazitäts-Pool. Ein Quality-of-Service-Level (QoS), das den maximalen Gesamtdurchsatz pro bereitgestelltem Speicherplatz definiert.

Das Service-Level und die anfänglich bereitgestellte Storage-Kapazität bestimmen das Performance-Level für ein bestimmtes Oracle Datenbank-Volume.

1. Service Levels für Azure NetApp Files

Azure NetApp Files unterstützt drei Service-Level: Ultra, Premium und Standard.

- **Ultra Storage.** Diese Ebene bietet einen Durchsatz von bis zu 128 MiB pro 1 tib Volume Kontingent.
- **Premium-Speicher.** dieser Tier bietet einen Durchsatz von bis zu 64 MiB pro 1 tib Volume Kontingent.
- **Standard-Speicher.** Diese Ebene bietet einen Durchsatz von bis zu 16 MiB pro 1 tib Volume Kontingent.

2. Kapazitäts-Pool und Quality of Service

Jedes der gewünschten Service-Level verursacht damit verbundene Kosten für die bereitgestellte Kapazität und umfasst ein Quality of Service-Level (QoS), das den maximalen Gesamtdurchsatz für den bereitgestellten Speicherplatz definiert.

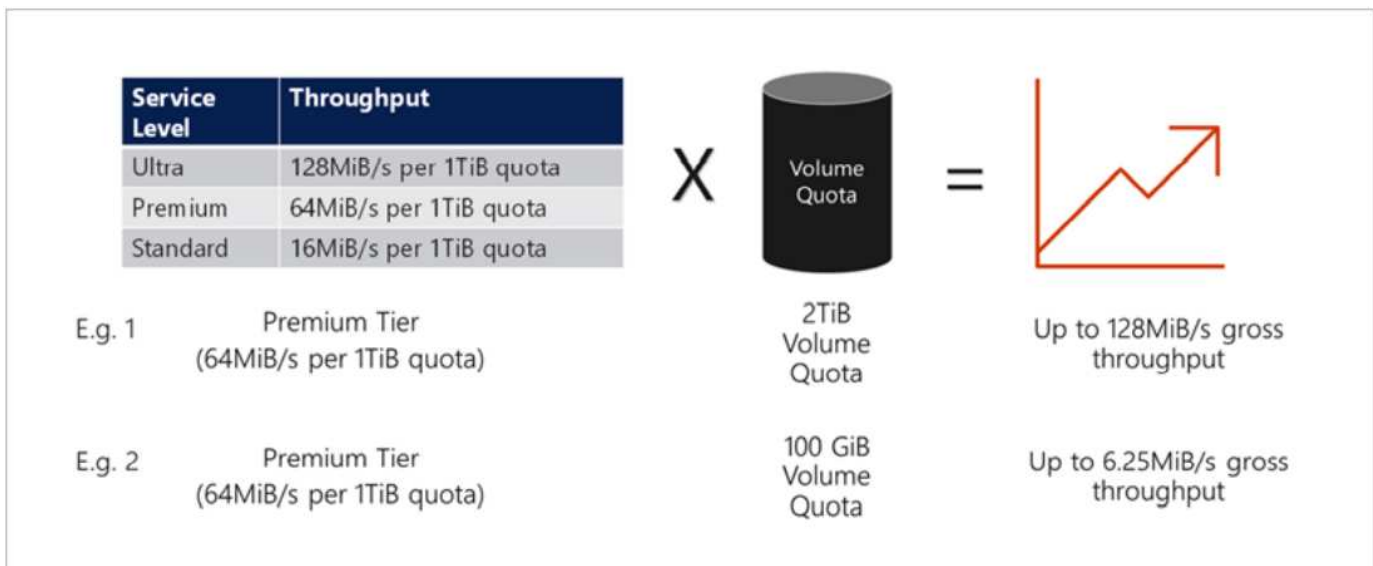
Ein über 10 tib bereitgestellter Single-Capacity-Pool mit dem Premium-Service-Level bietet beispielsweise einen insgesamt verfügbaren Durchsatz für alle Volumes in diesem Kapazitäts-Pool mit $10 \times 64 \text{ MB/s}$, also 640 MB mit 40,000 (16.000) IOPS oder 80,000 (8.000) IOPS.

Die minimale Kapazitäts-Pool-Größe ist 4 tib. Sie können die Größe eines Kapazitäts-Pools in 1-tib-Schritten ändern, um Änderungen an den Workload-Anforderungen zum Managen von Storage-Anforderungen und -Kosten zu reagieren.

3. Berechnen Sie den Service-Level auf einem Datenbank-Volume

Das Durchsatzlimit für ein Oracle Datenbank-Volume wird durch eine Kombination aus folgenden Faktoren bestimmt: Dem Service Level des Kapazitäts-Pools, zu dem das Volume gehört, und dem dem Volume zugewiesenen Kontingent.

Das folgende Diagramm zeigt, wie das Durchsatzlimit eines Oracle Datenbank-Volumes berechnet wird.



Beispiel 1 wird einem Volume aus einem Kapazitäts-Pool mit der Premium-Storage-Tier, dem 2 tib Kontingent zugewiesen ist, ein Durchsatzlimit von 128 MiPS ($2 \text{ tib} \times 64 \text{ MiB}$) zugewiesen. Dieses Szenario gilt unabhängig von der Größe des Kapazitäts-Pools oder dem tatsächlichen Volume-Verbrauch.

In Beispiel 2 wird einem Volume aus einem Kapazitäts-Pool mit der Premium-Storage-Tier, dem 100 gib an Kontingent zugewiesen ist, ein Durchsatzlimit von 6,25 MiB zugewiesen ($0,09765625 \text{ tib} \times 64 \text{ MiB}$). Dieses

Szenario gilt unabhängig von der Größe des Kapazitäts-Pools oder dem tatsächlichen Volume-Verbrauch.

Beachten Sie, dass die minimale Volume-Größe 100 gib beträgt.

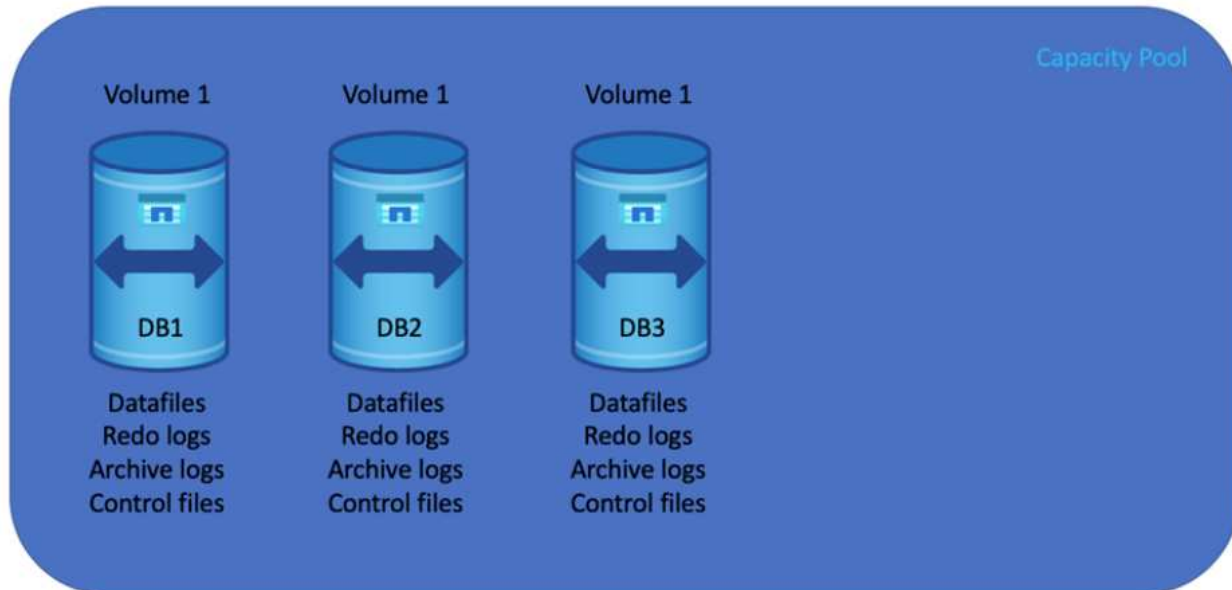
Storage-Layout und -Einstellungen

NetApp empfiehlt das folgende Storage Layout:

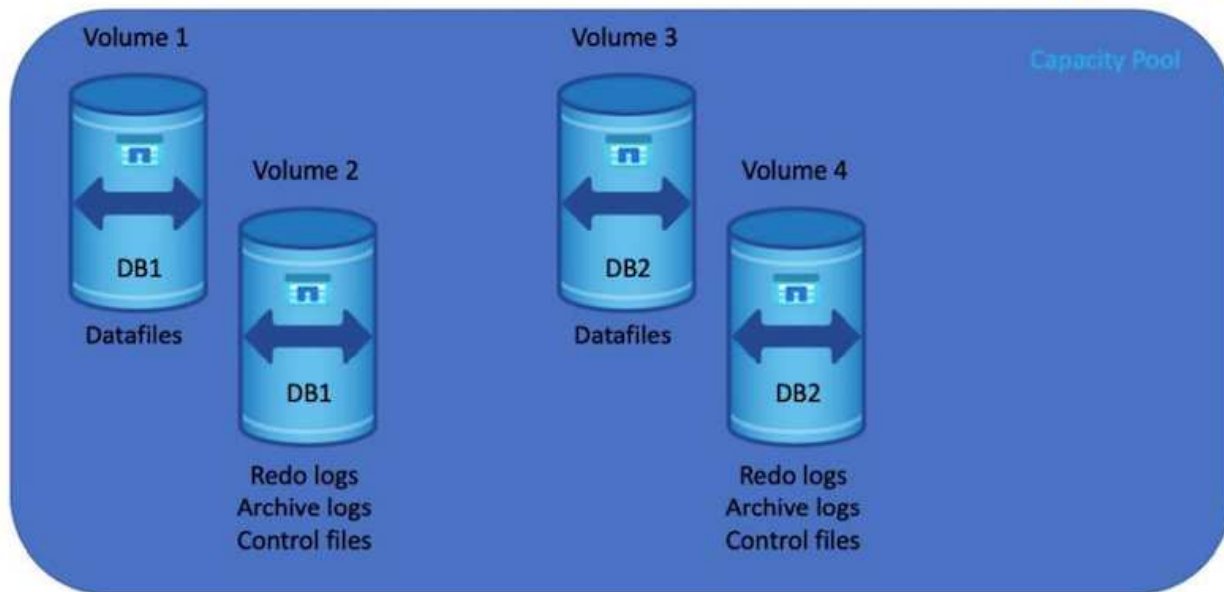
- Für kleine Datenbanken. Verwenden Sie ein einzelnes Volume-Layout für alle Oracle-Dateien.

Microsoft Azure

Azure Capacity Pool



- Bei großen Datenbanken empfiehlt sich das Volume-Layout aus mehreren Volumes: Eines für Oracle Daten und eine doppelte Kontrolldatei und eines für das aktive Protokoll von Oracle, ein archiviertes Protokoll und eine Kontrolldatei. NetApp empfiehlt dringend, ein Volume für die Oracle-Binärdatei anstelle des lokalen Laufwerks zuzuweisen, damit die Datenbank auf einen neuen Host verlagert und schnell wiederhergestellt werden kann.



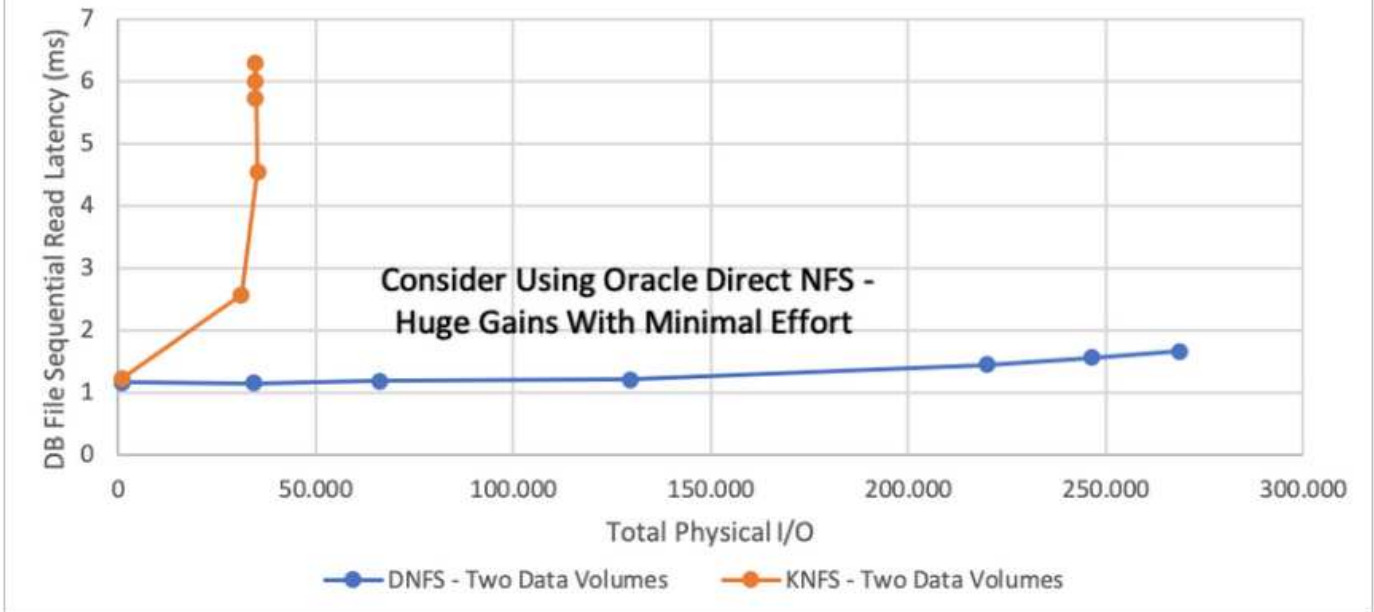
NFS-Konfiguration

Linux, das gängigste Betriebssystem, umfasst native NFS-Funktionen. Oracle bietet einen direkten NFS-Client (dNFS), der nativ in Oracle integriert ist. Oracle dNFS umgeht den BS-Cache und ermöglicht die parallele Verarbeitung zur Verbesserung der Datenbank-Performance. Oracle unterstützt NFSv3 seit über 20 Jahren, und NFSv4 wird mit Oracle 12.1.0.2 und höher unterstützt.

Durch die Verwendung von dNFS (verfügbar seit Oracle 11g) kann eine Oracle Datenbank, die auf einer Azure Virtual Machine ausgeführt wird, deutlich mehr I/O als der native NFS-Client ermöglichen. Die automatisierte Oracle-Implementierung mit dem NetApp Automatisierungs-Toolkit konfiguriert dNFS auf NFSv3 automatisch.

Das folgende Diagramm zeigt den SLOB-Benchmark auf Azure NetApp Files mit Oracle dNFS.

Oracle and Azure NetApp Files Comparing dNFS and Native NFS (Kernel NFS) 75% Read, 25% Update SLOB2 Workload



Weitere Faktoren, die berücksichtigt werden sollten:

- TCP-Slot-Tabellen entsprechen dem NFS-Äquivalent zur Warteschlangentiefe des Host-Bus-Adapters (HBA). Diese Tabellen steuern die Anzahl der NFS-Vorgänge, die zu einem beliebigen Zeitpunkt ausstehen können. Der Standardwert ist normalerweise 16, was für eine optimale Performance viel zu niedrig ist. Das entgegengesetzte Problem tritt auf neueren Linux-Kerneln auf, die automatisch die Begrenzung der TCP-Slot-Tabelle auf ein Niveau erhöhen können, das den NFS-Server mit Anforderungen sättigt.

Um eine optimale Performance zu erzielen und Performance-Probleme zu vermeiden, passen Sie die Kernel-Parameter an, die TCP-Slot-Tabellen steuern, auf 128 an.

```
sysctl -a | grep tcp.*.slot_table
```

- Die folgende Tabelle enthält die empfohlenen NFS-Mount-Optionen für eine einzelne Instanz von Linux NFSv3.

File Type	Mount Options
<ul style="list-style-type: none"> • Control files • Data files • Redo logs 	rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536
<ul style="list-style-type: none"> • ORACLE_HOME • ORACLE_BASE 	rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536



Überprüfen Sie vor der Verwendung von dNFS, ob die in Oracle Doc 1495104.1 beschriebenen Patches installiert sind. Die NetApp Support-Matrix für NFSv3 und NFSv4 enthält keine spezifischen Betriebssysteme. Alle Betriebssysteme, die der RFC entsprechen, werden unterstützt. Wenn Sie die Online-IMT nach Unterstützung für NFSv3 oder NFSv4 suchen, wählen Sie kein bestimmtes Betriebssystem aus, da keine Treffer angezeigt werden. Alle Betriebssysteme werden implizit von der allgemeinen Richtlinie unterstützt.

Schritt-für-Schritt-Anweisungen zur Oracle-Implementierung auf Azure VM und Azure NetApp Files

Implementieren Sie eine Azure VM mit ANF für Oracle über die Azure-Portalkonsole

Falls Sie noch nicht mit Azure arbeiten, müssen Sie zunächst eine Azure-Account-Umgebung einrichten. Dazu gehört auch, dass Sie Ihr Unternehmen zur Nutzung von Azure Active Directory registrieren. Der folgende Abschnitt enthält eine Zusammenfassung dieser Schritte. Weitere Informationen finden Sie in der verlinkten Dokumentation zu Azure.

Azure Ressourcen erstellen und nutzen

Nachdem die Azure Umgebung eingerichtet und ein Konto erstellt und mit einem Abonnement verknüpft wurde, können Sie sich beim Azure-Portal mit dem Konto anmelden, um die zum Ausführen von Oracle erforderlichen Ressourcen zu erstellen.

1. Erstellen Sie ein virtuelles Netzwerk oder vnet

Azure Virtual Network (vnet) ist der grundlegende Baustein für Ihr privates Netzwerk in Azure. Vnet ermöglicht vielen Arten von Azure Ressourcen, wie z. B. Azure Virtual Machines (VMs), die sichere Kommunikation untereinander, im Internet und in lokalen Netzwerken. Vor der Bereitstellung einer Azure VM muss zunächst eine vnet (wo eine VM implementiert ist) konfiguriert werden.

Siehe "[Erstellen Sie ein virtuelles Netzwerk mit dem Azure Portal](#)" Um ein vnet zu erstellen.

2. Erstellen Sie ein NetApp Storage-Konto und einen Kapazitäts-Pool für ANF

In diesem Implementierungsszenario wird ein Azure VM OS mit regelmäßigem Azure Storage bereitgestellt, aber ANF Volumes werden bereitgestellt, um die Oracle Datenbank über NFS auszuführen. Zunächst müssen Sie ein NetApp Storage-Konto und einen Kapazitäts-Pool erstellen, um die Storage Volumes zu hosten.

Siehe "[Einrichtung von Azure NetApp Files und Erstellung eines NFS Volumes](#)" So richten Sie einen ANF-Kapazitätspool ein.

3. Azure VM für Oracle bereitstellen

Bestimmen Sie basierend auf Ihren Workloads, welchen Typ von Azure VM Sie benötigen, und die Größe der VM-vCPU und des RAM, die für Oracle implementiert werden sollen. Klicken Sie dann in der Azure Konsole auf das VM-Symbol, um den VM-Implementierungs-Workflow zu starten.

1. Klicken Sie auf der Azure VM Seite auf **Erstellen** und wählen Sie dann **Azure Virtual Machine**.

Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual machines Hybrid Cloud TME

[Create](#)
[Switch to classic](#)
[Reservations](#)
[Manage view](#)
[Refresh](#)
[Export to CSV](#)
[Open query](#)
[Assign tags](#)
[Start](#)
[Restart](#)
[Stop](#)
[Delete](#)
[Services](#)
[Maintenance](#)

Filter for any field...
 [Subscription equals all](#)
[Type equals all](#)
[Resource group equals all](#)
[Location equals all](#)
[Add filter](#)

No grouping List view

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
acao-ora01	Virtual machine	Hybrid Cloud TME Onprem	TMEtstres	South Central US	Stopped (deallocated)	Linux	Standard_B4ms	13.65.63.157	1
ANFAV5val2JH	Virtual machine	Hybrid Cloud TME Onprem	ANFAV5VAL2	West Europe	Running	Windows	Standard_DS2_v2	20.229.80.88	1
ANFAV5f001	Virtual machine	Hybrid Cloud TME Onprem	anfavsrg	South Central US	Stopped (deallocated)	Linux	Standard_DS2ds_v4	-	1
ANFAV5f0AZ1	Virtual machine	Hybrid Cloud TME Onprem	anfavsrg	South Central US	Running	Linux	Standard_E32as_v4	40.124.74.246	1
ANFAV5f0AZ2	Virtual machine	Hybrid Cloud TME Onprem	anfavsrg	South Central US	Stopped (deallocated)	Linux	Standard_E32as_v4	40.124.178.111	1
ANFAV5f0AZ3	Virtual machine	Hybrid Cloud TME Onprem	anfavsrg	South Central US	Stopped (deallocated)	Linux	Standard_E32as_v4	40.124.194.32	1
ANFAV5valDC	Virtual machine	Hybrid Cloud TME Onprem	anfavsrg	South Central US	Stopped (deallocated)	Windows	Standard_B4ms	-	1
ANFAV5valIH	Virtual machine	Hybrid Cloud TME Onprem	anfavsrg	South Central US	Running	Windows	Standard_B2ms	70.37.66.218	1
ANFAV5valIH2	Virtual machine	Hybrid Cloud TME Onprem	anfavsrg	South Central US	Running	Windows	Standard_B2s	20.225.210.195	1
ANFCVOCM	Virtual machine	Hybrid Cloud TME Onprem	anfavsval2	West Europe	Running	Linux	Standard_DS3_v2	-	1
ANFCVODRDC2	Virtual machine	Hybrid Cloud TME Onprem	anfavsval2	West Europe	Running	Windows	Standard_B2s	-	1
ANFCVODRDemo	Virtual machine	Hybrid Cloud TME Onprem	anfvcodrdemo-rg	West Europe	Running	Linux	Standard_E4s_v3	-	5
AVSCVOPerfinguest	Virtual machine	Hybrid Cloud TME Onprem	avscvoperfinguest-rg	West Europe	Stopped (deallocated)	Linux	Standard_DS15_v2	-	5

2. Wählen Sie die Abonnement-ID für die Implementierung aus und wählen Sie dann die Ressourcengruppe, die Region, den Hostnamen, das VM-Image, die Größe Und Authentifizierungsmethode. Wechseln Sie zur Seite Festplatte.

Home > Virtual machines >

Create a virtual machine ...

Basics | Disks | Networking | Management | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Instance details

Virtual machine name * ⓘ

Region * ⓘ

Availability options ⓘ

Security type ⓘ

Image * ⓘ [See all images](#) | [Configure VM generation](#)

Run with Azure Spot discount ⓘ

Size * ⓘ [See all sizes](#)

Administrator account

Authentication type ⓘ

SSH public key

Password

Review + create

< Previous

Next : Disks >

[Home](#) > [Virtual machines](#) >

Create a virtual machine ...

Size * ⓘ [See all sizes](#)

Administrator account

Authentication type ⓘ

 SSH public key
 Password

Username * ⓘ

Password * ⓘ

Confirm password * ⓘ

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ

 None
 Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

If you have eligible Red Hat Enterprise Linux subscriptions that are enabled for Red Hat Cloud Access, you can use Azure Hybrid Benefit to attach your Red Hat subscriptions to this VM and save money on compute costs [Learn more](#)

Your Azure subscription is currently not a part of Red Hat Cloud Access. In order to enable AHB for this VM, you must add this Azure subscription to Cloud Access. [Learn more](#)

[Review + create](#)[< Previous](#)[Next : Disks >](#)

3. Wählen Sie **Premium SSD** für lokale Betriebssystemredundanz und lassen Sie die Datenfestplatte leer, da die Datenfestplatten vom ANF-Speicher bereitgestellt werden. Wechseln Sie zur Netzwerkseite.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) [Advanced](#) [Tags](#) [Review + create](#)

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type * Delete with VM Enable encryption at host

i Encryption at host is not registered for the selected subscription. [Learn more about enabling this feature](#)

Encryption type * Enable Ultra Disk compatibility

Data disks for acao-ora01

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
Create and attach a new disk	Attach an existing disk				

[Advanced](#)[Review + create](#)[< Previous](#)[Next : Networking >](#)

4. Wählen Sie vnet und Subnetz. Weisen Sie eine öffentliche IP für externen VM-Zugriff zu. Wechseln Sie dann zur Seite Verwaltung.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	<input type="text" value="ANFAVSval"/>
	Create new
Subnet *	<input type="text" value="VM_Sub (172.30.137.128/25)"/>
	Manage subnet configuration
Public IP	<input type="text" value="(new) acao-ora01-ip"/>
	Create new
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
Select inbound ports *	<input type="text" value="SSH (22)"/>

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Delete public IP and NIC when VM is deleted	<input checked="" type="checkbox"/>
Enable accelerated networking	<input checked="" type="checkbox"/>

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution?	<input type="checkbox"/>
--	--------------------------

[Review + create](#)[< Previous](#)[Next : Management >](#)

5. Behalten Sie alle Standardeinstellungen für die Verwaltung bei, und wechseln Sie zur Seite Erweitert.



Create a virtual machine ...

- Basics
- Disks
- Networking
- Management**
- Advanced
- Tags
- Review + create

Configure monitoring and management options for your VM.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

Your subscription is protected by Microsoft Defender for Cloud basic plan.

Monitoring

- Boot diagnostics Enable with managed storage account (recommended)
 Enable with custom storage account
 Disable

Enable OS guest diagnostics

Identity

Enable system assigned managed identity

Azure AD

Login with Azure AD

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine User Login is required when using Azure AD login. [Learn more](#)

Azure AD login now uses SSH certificate-based authentication. You will need to use an SSH client that supports OpenSSH certificates. You can use Azure CLI or Cloud Shell from the Azure Portal. [Learn more](#)

Auto-shutdown

Enable auto-shutdown

Backup

- Review + create**
- < Previous
- Next : Advanced >

6. Behalten Sie alle Standardeinstellungen für die Seite „Erweitert“ bei, es sei denn, Sie müssen eine VM nach der Implementierung mit benutzerdefinierten Skripten anpassen. Gehen Sie dann zur Seite Tags.

[Home](#) > [Virtual machines](#) >

Create a virtual machine

[Basics](#) [Disks](#) [Networking](#) [Management](#) **[Advanced](#)** [Tags](#) [Review + create](#)

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ [Select an extension to install](#)

VM applications

VM applications contain application files that are securely and reliably downloaded on your VM after deployment. In addition to the application files, an install and uninstall script are included in the application. You can easily add or remove applications on your VM after create. [Learn more](#) ↗

[Select a VM application to install](#)

Custom data

Pass a script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#) ↗

Custom data

ⓘ Your image must have a code to support consumption of custom data. If your image supports cloud-init, custom-data will be processed by cloud-init. [Learn more about custom data for VMs](#) ↗

User data

Pass a script, configuration file, or other data that will be accessible to your applications **throughout the lifetime of the virtual machine**. Don't use user data for storing your secrets or passwords. [Learn more about user data for VMs](#) ↗

Enable user data

[Review + create](#)[< Previous](#)[Next : Tags >](#)

7. Fügen Sie bei Bedarf ein Tag für die VM hinzu. Gehen Sie dann zur Seite „Prüfen + Erstellen“.

[Home](#) > [Virtual machines](#) >

Create a virtual machine ...

Basics Disks Networking Management Advanced **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ	Value ⓘ	Resource
<input type="text" value="database"/>	<input type="text" value="oracle"/>	12 selected  
<input type="text"/>	<input type="text"/>	12 selected 

[Review + create](#)[< Previous](#)[Next: Review + create >](#)

- Der Bereitstellungsworkflow führt eine Validierung der Konfiguration aus, und wenn die Validierung erfolgreich ist, klicken Sie auf **Erstellen**, um die VM zu erstellen.

Create a virtual machine

✓ Validation passed

Basics Disks Networking Management Advanced Tags Review + create

i Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

PRODUCT DETAILS

1 X Standard D8s v3
by Microsoft
[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ
0.3740 USD/hr
[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name	<input type="text" value="Allen Cao"/>
Preferred e-mail address	<input type="text" value="allen.cao@netapp.com"/>
Preferred phone number	<input type="text"/>

⚠ You have set SSH port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Create

< Previous

Next >

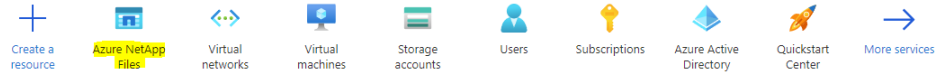
[Download a template for automation](#)

4. ANF Datenbank-Volumes für Oracle bereitstellen

Sie müssen drei NFS-Volumes für einen ANF-Kapazitätspool für die Oracle-Binärdaten, Daten und Log-Volumes erstellen.

1. Klicken Sie in der Azure Konsole unter der Liste der Azure Services auf Azure NetApp Files, um den Erstellungsworkflow für Volumes zu öffnen. Wenn Sie über mehr als ein ANF-Storage-Konto verfügen, klicken Sie auf das Konto, über das Sie Volumes bereitstellen möchten.

Azure services



Resources

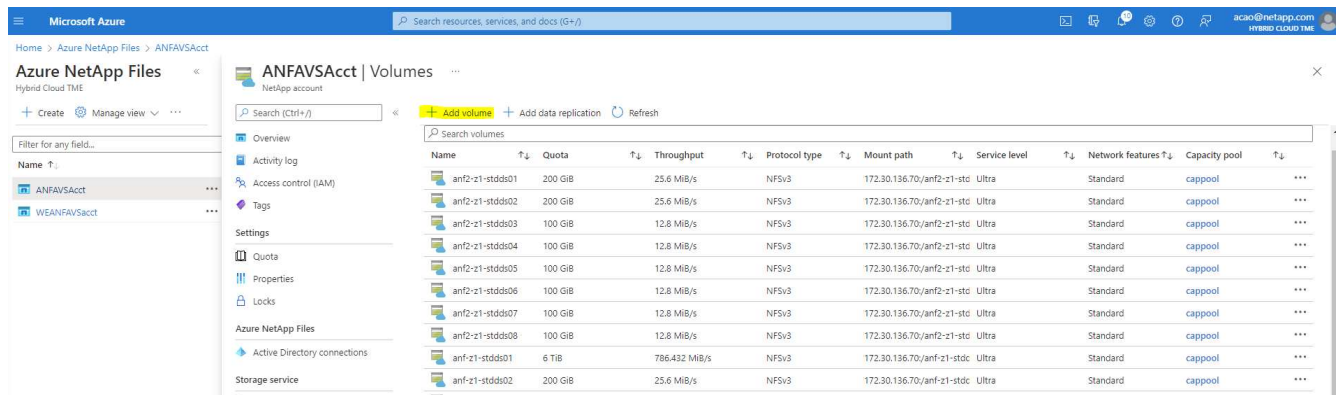
Recent Favorite

Name	Type	Last Viewed
ANFAVSAcct	NetApp account	a few seconds ago
ANFAVSval	Virtual network	3 hours ago
acao-ora01	Virtual machine	5 days ago
Hybrid Cloud TME Onprem	Subscription	2 weeks ago
WEANFAVSAcct	NetApp account	2 weeks ago
ANFAVSAcct/CapPool/acao-ora01-u03	Volume	2 weeks ago
ANFAVSAcct/CapPool/acao-ora01-u02	Volume	2 weeks ago
ANFAVSAcct/CapPool/acao-ora01-u01	Volume	2 weeks ago
acao-ora01_OsDisk_1_673bad70ccce4709afc81278e2bc97cb	Disk	2 weeks ago
acao-ora0166	Network Interface	3 weeks ago
TMEtstres	Resource group	3 weeks ago

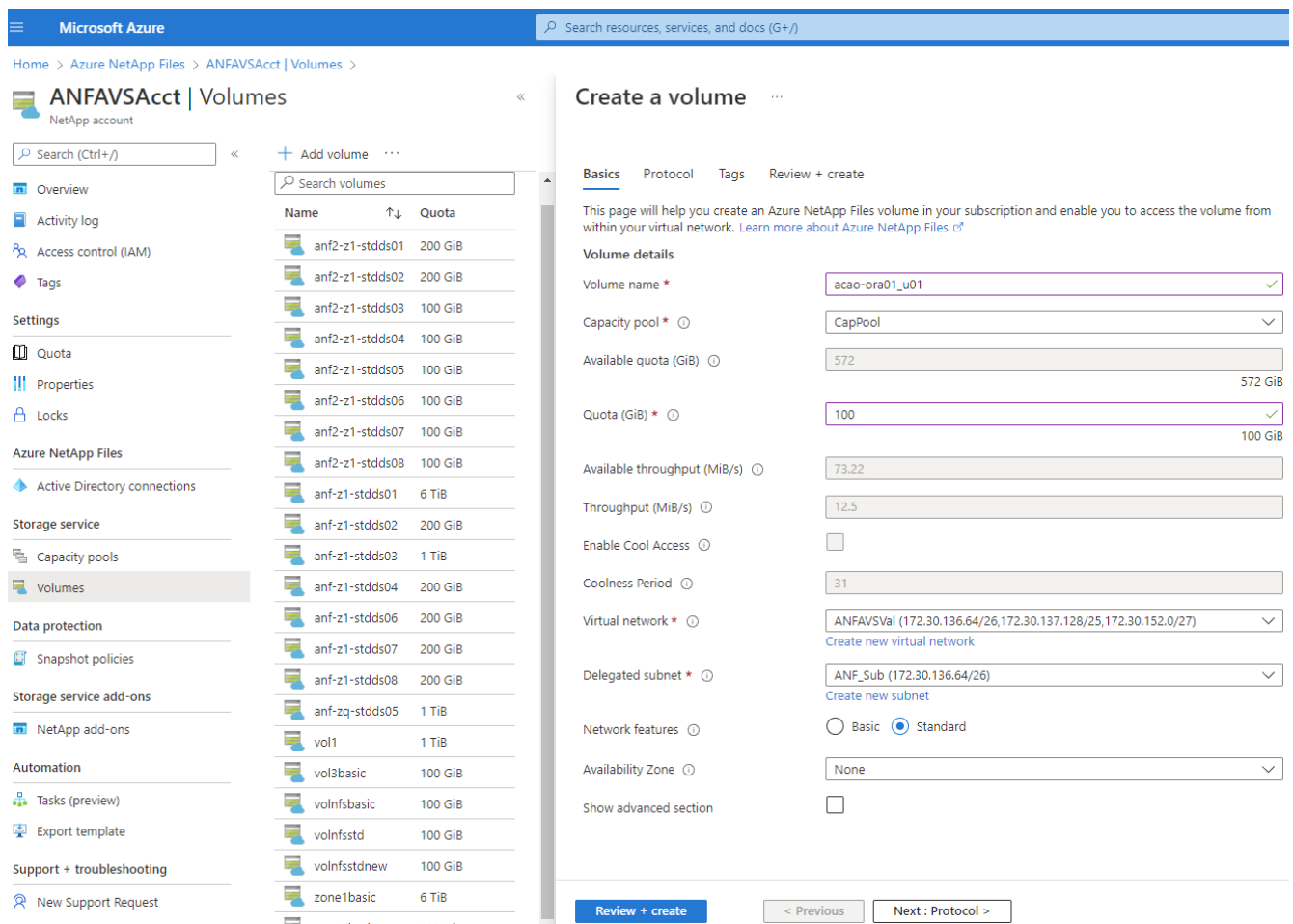
See all

2. Klicken Sie auf Ihrem NetApp Storage Account auf **Volumes** und dann auf **Add Volume**, um neue Oracle Volumes zu erstellen.

The screenshot shows the Azure NetApp Files console for the resource 'ANFAVSAcct'. The left-hand navigation pane is open, and the 'Volumes' option under 'Storage service' is highlighted in yellow. The main content area displays the 'Essentials' section for the NetApp account, including details like Resource group (ANFAVSRG), Location (South Central US), and Subscription (Hybrid Cloud TME Onprem). Below this, there is a section titled 'Enterprise files storage, powered by NetApp' with three main actions: 'Connect to Active Directory', 'Capacity pools', and 'Volumes'. Each action has a brief description and a 'View' button.



- Eine gute Vorgehensweise: Ermitteln Sie Oracle Volumes mit dem VM-Hostnamen als Präfix und anschließend den Mount-Punkt auf dem Host, z. B. u01 für Oracle binär, u02 für Oracle Daten und u03 für Oracle log. Wählen Sie dieselbe vnet-Anzahl für das Volume wie für die VM. Klicken Sie Auf **Weiter: Protokoll**>.



- Wählen Sie das NFS-Protokoll, fügen Sie die Oracle-Host-IP-Adresse dem zulässigen Client hinzu und entfernen Sie die Standardrichtlinie, die alle IP-Adressen 0.0.0.0/0 zulässt. Klicken Sie dann auf **Weiter: Tags**>.

Microsoft Azure Search resources, services, and docs (G+)

Home > Azure NetApp Files > ANFAVSAcct | Volumes >

ANFAVSAcct | Volumes

NetApp account

Search (Ctrl+/) Add volume

Search volumes

Name	Quota
anf2-z1-stdds01	200 GiB
anf2-z1-stdds02	200 GiB
anf2-z1-stdds03	100 GiB
anf2-z1-stdds04	100 GiB
anf2-z1-stdds05	100 GiB
anf2-z1-stdds06	100 GiB
anf2-z1-stdds07	100 GiB
anf2-z1-stdds08	100 GiB
anf-z1-stdds01	6 TiB
anf-z1-stdds02	200 GiB
anf-z1-stdds03	1 TiB
anf-z1-stdds04	200 GiB
anf-z1-stdds06	200 GiB
anf-z1-stdds07	200 GiB
anf-z1-stdds08	200 GiB
anf-zq-stdds05	1 TiB
vol1	1 TiB
vol3basic	100 GiB
volnfsbasic	100 GiB
volnfsstd	100 GiB
volnfsstdnew	100 GiB
zone1basic	6 TiB
zone2basic	100 GiB

Create a volume

Basics Protocol Tags Review + create

Configure access to your volume.

Access

Protocol type NFS SMB Dual-protocol

Configuration

File path *

Versions *

Kerberos Enabled Disabled

LDAP Enabled Disabled

Azure VMware Solution DataStore

Export policy

Configure the volume's export policy. This can be edited later. [Learn more](#)

↑ Move up ↓ Move down ↕ Move to top ↓ Move to bottom 🗑 Delete

<input type="checkbox"/>	Index	Allowed clients	Access	Root Access	...
<input type="checkbox"/>	1	0.0.0.0	Read & Write	On	...
<input type="checkbox"/>	2	172.30.137.142 ✓	Read & Write	On	...

Review + create < Previous Next: Tags >

5. Fügen Sie bei Bedarf ein Volume-Tag hinzu. Klicken Sie dann auf **Review + Create**.

Microsoft Azure Search resources, services, and docs (G+)

Home > Azure NetApp Files > ANFAVSAcct | Volumes >

ANFAVSAcct | Volumes

NetApp account

Search (Ctrl+/) Add volume

Search volumes

Name	Quota
anf2-z1-stdds01	200 GiB
anf2-z1-stdds02	200 GiB
anf2-z1-stdds03	100 GiB
anf2-z1-stdds04	100 GiB
anf2-z1-stdds05	100 GiB
anf2-z1-stdds06	100 GiB
anf2-z1-stdds07	100 GiB
anf2-z1-stdds08	100 GiB
anf-z1-stdds01	6 TiB
anf-z1-stdds02	200 GiB
anf-z1-stdds03	1 TiB
anf-z1-stdds04	200 GiB
anf-z1-stdds06	200 GiB
anf-z1-stdds07	200 GiB
anf-z1-stdds08	200 GiB
anf-zq-stdds05	1 TiB
vol1	1 TiB
vol3basic	100 GiB
volnfsbasic	100 GiB
volnfsstd	100 GiB
volnfsstdnew	100 GiB
zone1basic	6 TiB
zone2basic	100 GiB

Create a volume

Basics Protocol **Tags** Review + create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name Value

database : oracle

Review + create < Previous Next : Review + create >

6. Wenn die Validierung erfolgreich ist, klicken Sie auf **Erstellen**, um das Volume zu erstellen.

Microsoft Azure Search resources, services, and docs (G+)

Home > Azure NetApp Files > ANFAVSAcct | Volumes >

ANFAVSAcct | Volumes NetApp account

Search (Ctrl+/) Add volume

Search volumes

Name	Quota
anf2-z1-stdds01	200 GiB
anf2-z1-stdds02	200 GiB
anf2-z1-stdds03	100 GiB
anf2-z1-stdds04	100 GiB
anf2-z1-stdds05	100 GiB
anf2-z1-stdds06	100 GiB
anf2-z1-stdds07	100 GiB
anf2-z1-stdds08	100 GiB
anf-z1-stdds01	6 TiB
anf-z1-stdds02	200 GiB
anf-z1-stdds03	1 TiB
anf-z1-stdds04	200 GiB
anf-z1-stdds06	200 GiB
anf-z1-stdds07	200 GiB
anf-z1-stdds08	200 GiB
anf-zq-stdds05	1 TiB
vol1	1 TiB
vol3basic	100 GiB
volnfsbasic	100 GiB
volnfsstd	100 GiB
volnfsstdnew	100 GiB
zone1basic	6 TiB
zone2basic	100 GiB

Create a volume

Validation passed

Basics Protocol Tags **Review + create**

Basics

Subscription Hybrid Cloud TME Onprem
 Resource group ANFAVSRG
 Region South Central US
 Volume name acao-ora01-u01
 Capacity pool CapPool
 Service level Ultra
 Quota 100 GiB
 Encryption key source Microsoft.NetApp
 Availability Zone None

Networking

Virtual network ANFAVVal (172.30.136.64/26,172.30.137.128/25,172.30.152.0/27)
 Delegated subnet ANF_Sub (172.30.136.64/26)
 Network features Standard

Protocol

Protocol NFSv3
 File path acao-ora01-u01

Tags

database oracle

Create < Previous Next > Download a template for automation

Installation und Konfiguration von Oracle auf Azure VM mit ANF

Das NetApp Lösungs-Team hat zahlreiche Ansible-basierte Automatisierungs-Toolkits für die reibungslose Implementierung von Oracle in Azure erstellt. Gehen Sie zur Implementierung von Oracle auf einer Azure VM folgendermaßen vor.

Richten Sie einen Ansible-Controller ein

Wenn Sie keinen Ansible-Controller eingerichtet haben, lesen Sie "[Automatisierung der NetApp Lösung](#)", Mit ausführlichen Anweisungen zum Einrichten eines Ansible Controllers.

Erhalten Sie das Oracle Deployment Automation Toolkit

Klonen Sie unter der Benutzer-ID, die Sie zur Anmeldung beim Ansible-Controller verwenden, eine Kopie des Oracle Deployment Toolkit in Ihrem Home-Verzeichnis.

```
git clone https://github.com/NetApp-Automation/na_oracle19c_deploy.git
```

Führen Sie das Toolkit mit Ihrer Konfiguration aus

Siehe "[CLI-Implementierung einer Oracle 19c Datenbank](#)" Zum Ausführen des Playbooks über die CLI. Sie

können den ONTAP-Teil der Variablenkonfiguration in der globalen VARS-Datei ignorieren, wenn Sie Datenbank-Volumes von der Azure-Konsole statt von der CLI erstellen.



Der Toolkit-Standard implementiert Oracle 19c mit RU 19.8. Es lässt sich leicht an jede andere Patch-Ebene mit kleineren Standard-Konfigurationsänderungen anpassen. Das Daten-Volume wird außerdem automatisch mit aktiven Standardprotokolldateien der Seed-Datenbank bereitgestellt. Wenn Sie aktive Log-Dateien auf dem Protokoll-Volume benötigen, sollten diese nach der anfänglichen Implementierung verschoben werden. Wenden Sie sich bei Bedarf an das NetApp Solution Team, um Unterstützung zu erhalten.

Einrichten des AzAcSnap Backup-Tools für applikationskonsistente Snapshots für Oracle

Das Azure Application-konsistente Snapshot Tool (AzAcSnap) ist ein Befehlszeilen-Tool, das die Datensicherung für Datenbanken anderer Anbieter ermöglicht. Sie übernimmt dabei die gesamte Orchestrierung, die erforderlich ist, um sie in einen applikationskonsistenten Zustand zu versetzen, bevor ein Storage-Snapshot erstellt wird. Anschließend werden diese Datenbanken in einen Betriebszustand zurückversetzt. NetApp empfiehlt, das Tool auf dem Datenbankserver-Host zu installieren. Siehe folgende Installations- und Konfigurationsverfahren.

Installieren Sie das AzAcSnap-Tool

1. Holen Sie sich die neueste Version des ["Der AzArcSnap Installer"](#).
2. Kopieren Sie das heruntergeladene Selbstinstallationsprogramm auf das Zielsystem.
3. Führen Sie das Self-Installer als Root-Benutzer mit der Standardinstallationsoption aus. Machen Sie die Datei bei Bedarf mit dem ausführbar `chmod +x *.run` Befehl.

```
./azacsnap_installer_v5.0.run -I
```

Konfigurieren Sie die Oracle-Konnektivität

Die Snapshot-Tools kommunizieren mit der Oracle-Datenbank und benötigen einen Datenbankbenutzer mit entsprechenden Berechtigungen, um den Backup-Modus zu aktivieren oder zu deaktivieren.

1. Richten Sie den Benutzer der AzAcSnap-Datenbank ein

Die folgenden Beispiele zeigen die Einrichtung des Oracle-Datenbankbenutzers und die Verwendung von sqlplus für die Kommunikation mit der Oracle-Datenbank. Die Beispielbefehle richten einen Benutzer (AZACNAP) in der Oracle-Datenbank ein und ändern gegebenenfalls die IP-Adresse, Benutzernamen und Passwörter.

1. Starten Sie sqlplus von der Oracle-Datenbankinstallation, um sich bei der Datenbank anzumelden.

```
su - oracle  
sqlplus / AS SYSDBA
```

2. Erstellen Sie den Benutzer.

```
CREATE USER azacsnap IDENTIFIED BY password;
```

3. Gewähren Sie den Benutzern Berechtigungen. In diesem Beispiel wird die Berechtigung für den AZACNAP-Benutzer festgelegt, damit die Datenbank in den Backup-Modus versetzt werden kann.

```
GRANT CREATE SESSION TO azacsnap;  
GRANT SYSBACKUP TO azacsnap;
```

4. Ändern Sie den Ablauf des Standardpassworts für den Benutzer auf unbegrenzt.

```
ALTER PROFILE default LIMIT PASSWORD_LIFE_TIME unlimited;
```

5. Validieren Sie azacsnap-Konnektivität für die Datenbank.

```
connect azacsnap/password  
quit;
```

2. Konfigurieren Sie Linux-Benutzer azacSnap für DB-Zugriff mit Oracle Wallet

Die AzAcSnap Standardinstallation erstellt einen azacSnap OS-Benutzer. Die Bash-Shell-Umgebung muss für den Zugriff auf die Oracle-Datenbank mit dem in einer Oracle-Brieftasche gespeicherten Passwort konfiguriert werden.

1. Führen Sie als Root-Benutzer den aus `cat /etc/oratab` Befehl zur Identifizierung DER VARIABLEN `ORACLE_HOME` und `ORACLE_SID` auf dem Host.

```
cat /etc/oratab
```

2. Fügen Sie `ORACLE_HOME`, `ORACLE_SID`, `TNS_ADMIN` und `PFADVARIABLEN` zum azacSnap-Benutzer-Bash-Profil hinzu. Ändern Sie die Variablen nach Bedarf.

```
echo "export ORACLE_SID=ORATEST" >> /home/azacsnap/.bash_profile  
echo "export ORACLE_HOME=/u01/app/oracle/product/19800/ORATST" >>  
/home/azacsnap/.bash_profile  
echo "export TNS_ADMIN=/home/azacsnap" >> /home/azacsnap/.bash_profile  
echo "export PATH=\$PATH:\$ORACLE_HOME/bin" >>  
/home/azacsnap/.bash_profile
```

3. Erstellen Sie als Linux-Benutzer azacsnap das Portemonnaie. Sie werden aufgefordert, das Passwort für das Guthaben einzugeben.

```
sudo su - azacsnap

mkstore -wrl $TNS_ADMIN/.oracle_wallet/ -create
```

4. Fügen Sie die Anmeldeinformationen für die Verbindungszeichenfolge zum Oracle Wallet hinzu. Im folgenden Beispiel-Befehl ist AZACSNAP der ConnectString, der von AzAcSnap verwendet werden soll, azacsnap der Oracle Database User und AzPasswd1 das Datenbankpasswort des Oracle-Benutzers. Sie werden erneut aufgefordert, das Passwort für das Guthaben einzugeben.

```
mkstore -wrl $TNS_ADMIN/.oracle_wallet/ -createCredential AZACSNAP
azacsnap AzPasswd1
```

5. Erstellen Sie die `tnsnames.ora` Datei: Im folgenden Beispielbefehl sollte DER HOST auf die IP-Adresse der Oracle Datenbank gesetzt werden und der Server SID auf die Oracle Database SID gesetzt werden.

```
echo "# Connection string
AZACSNAP=\"(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP) (HOST=172.30.137.142) (PORT=1521)) (CONNECT_DATA=(SID=ORATST)))\"
" > $TNS_ADMIN/tnsnames.ora
```

6. Erstellen Sie die `sqlnet.ora` Datei:

```
echo "SQLNET.WALLET_OVERRIDE = TRUE
WALLET_LOCATION= (
    SOURCE=(METHOD=FILE)
    (METHOD_DATA=(DIRECTORY=\$TNS_ADMIN/.oracle_wallet))
) " > $TNS_ADMIN/sqlnet.ora
```

7. Testen Sie den Oracle-Zugriff über das Portemonnaie.

```
sqlplus /@AZACSNAP as SYSBACKUP
```

Die erwartete Ausgabe des Befehls:

```
[azacsnap@acao-ora01 ~]$ sqlplus /@AZACSNAP as SYSBACKUP

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Sep 8 18:02:07 2022
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL>
```

ANF-Konnektivität konfigurieren

Dieser Abschnitt erläutert die Aktivierung der Kommunikation mit Azure NetApp Files (mit einer VM).

1. Stellen Sie sicher, dass Sie innerhalb einer Azure Cloud-Shell-Sitzung bei dem Abonnement angemeldet sind, dem Sie standardmäßig dem Service-Principal zugeordnet werden möchten.

```
az account show
```

2. Wenn das Abonnement nicht korrekt ist, verwenden Sie den folgenden Befehl:

```
az account set -s <subscription name or id>
```

3. Erstellen Sie einen Service-Principal unter Verwendung der Azure CLI wie im folgenden Beispiel:

```
az ad sp create-for-rbac --name "AzAcSnap" --role Contributor --scopes
/subscriptions/{subscription-id} --sdk-auth
```

Die erwartete Ausgabe:

```
{
  "clientId": "00aa000a-aaaa-0000-00a0-00aa000aaa0a",
  "clientSecret": "00aa000a-aaaa-0000-00a0-00aa000aaa0a",
  "subscriptionId": "00aa000a-aaaa-0000-00a0-00aa000aaa0a",
  "tenantId": "00aa000a-aaaa-0000-00a0-00aa000aaa0a",
  "activeDirectoryEndpointUrl": "https://login.microsoftonline.com",
  "resourceManagerEndpointUrl": "https://management.azure.com/",
  "activeDirectoryGraphResourceId": "https://graph.windows.net/",
  "sqlManagementEndpointUrl":
"https://management.core.windows.net:8443/",
  "galleryEndpointUrl": "https://gallery.azure.com/",
  "managementEndpointUrl": "https://management.core.windows.net/"
}
```

4. Ausschneiden und Einfügen des Ausgabeinhalts in eine Datei namens `oracle.json` Gespeichert im Verzeichnis der Benutzer-azacsnap-Benutzerfächer des Linux-Benutzers und sichern Sie die Datei mit den entsprechenden Systemberechtigungen.



Stellen Sie sicher, dass das Format der JSON-Datei genau wie oben beschrieben ist, insbesondere mit den URLs, die in doppelten Anführungszeichen (") eingeschlossen sind.

Führen Sie die Einrichtung des AzAcSnap-Tools durch

Führen Sie die folgenden Schritte aus, um die Snapshot-Tools zu konfigurieren und zu testen. Nach den erfolgreichen Tests können Sie den ersten datenbankkonsistenten Storage-Snapshot durchführen.

1. Ändern Sie das Snapshot-Benutzerkonto.

```
su - azacsnap
```

2. Ändern Sie den Speicherort von Befehlen.

```
cd /home/azacsnap/bin/
```

3. Konfigurieren einer Speicherdetaildatei. Dadurch wird ein erzeugt `azacsnap.json` Konfigurationsdatei

```
azacsnap -c configure --configuration new
```

Die erwartete Ausgabe mit drei Oracle Volumen:

```
[azacsnap@acao-ora01 bin]$ azacsnap -c configure --configuration new
Building new config file
Add comment to config file (blank entry to exit adding comments): Oracle
```



```

snapshot bkup
Add comment to config file (blank entry to exit adding comments):
Enter the database type to add, 'hana', 'oracle', or 'exit' (for no
database): oracle

=== Add Oracle Database details ===
Oracle Database SID (e.g. CDB1): ORATST
Database Server's Address (hostname or IP address): 172.30.137.142
Oracle connect string (e.g. /@AZACSNAP): /@AZACSNAP

=== Azure NetApp Files Storage details ===
Are you using Azure NetApp Files for the database? (y/n) [n]: y
--- DATA Volumes have the Application put into a consistent state before
they are snapshot ---
Add Azure NetApp Files resource to DATA Volume section of Database
configuration? (y/n) [n]: y
Full Azure NetApp Files Storage Volume Resource ID (e.g.
/subscriptions/.../resourceGroups/.../providers/Microsoft.NetApp/netAppA
ccounts/.../capacityPools/Premium/volumes/...): /subscriptions/0efa2dfb-
917c-4497-b56a-
b3f4eadb8111/resourceGroups/ANFAVSRG/providers/Microsoft.NetApp/netAppAc
counts/ANFAVSAcct/capacityPools/CapPool/volumes/acao-ora01-u01
Service Principal Authentication filename or Azure Key Vault Resource ID
(e.g. auth-file.json or https://...): oracle.json
Add Azure NetApp Files resource to DATA Volume section of Database
configuration? (y/n) [n]: y
Full Azure NetApp Files Storage Volume Resource ID (e.g.
/subscriptions/.../resourceGroups/.../providers/Microsoft.NetApp/netAppA
ccounts/.../capacityPools/Premium/volumes/...): /subscriptions/0efa2dfb-
917c-4497-b56a-
b3f4eadb8111/resourceGroups/ANFAVSRG/providers/Microsoft.NetApp/netAppAc
counts/ANFAVSAcct/capacityPools/CapPool/volumes/acao-ora01-u02
Service Principal Authentication filename or Azure Key Vault Resource ID
(e.g. auth-file.json or https://...): oracle.json
Add Azure NetApp Files resource to DATA Volume section of Database
configuration? (y/n) [n]: n
--- OTHER Volumes are snapshot immediately without preparing any
application for snapshot ---
Add Azure NetApp Files resource to OTHER Volume section of Database
configuration? (y/n) [n]: y
Full Azure NetApp Files Storage Volume Resource ID (e.g.
/subscriptions/.../resourceGroups/.../providers/Microsoft.NetApp/netAppA
ccounts/.../capacityPools/Premium/volumes/...): /subscriptions/0efa2dfb-
917c-4497-b56a-
b3f4eadb8111/resourceGroups/ANFAVSRG/providers/Microsoft.NetApp/netAppAc
counts/ANFAVSAcct/capacityPools/CapPool/volumes/acao-ora01-u03

```

```

Service Principal Authentication filename or Azure Key Vault Resource ID
(e.g. auth-file.json or https://...): oracle.json
Add Azure NetApp Files resource to OTHER Volume section of Database
configuration? (y/n) [n]: n

=== Azure Managed Disk details ===
Are you using Azure Managed Disks for the database? (y/n) [n]: n

=== Azure Large Instance (Bare Metal) Storage details ===
Are you using Azure Large Instance (Bare Metal) for the database? (y/n)
[n]: n

Enter the database type to add, 'hana', 'oracle', or 'exit' (for no
database): exit

Editing configuration complete, writing output to 'azacsnap.json'.

```

4. Führen Sie als Benutzer von azacsnap Linux den Befehl azacsnap Test für ein Oracle Backup aus.

```

cd ~/bin
azacsnap -c test --test oracle --configfile azacsnap.json

```

Die erwartete Ausgabe:

```

[azacsnap@acao-ora01 bin]$ azacsnap -c test --test oracle --configfile
azacsnap.json
BEGIN : Test process started for 'oracle'
BEGIN : Oracle DB tests
PASSED: Successful connectivity to Oracle DB version 1908000000
END   : Test process complete for 'oracle'
[azacsnap@acao-ora01 bin]$

```

5. Führen Sie Ihre erste Snapshot-Sicherung aus.

```

azacsnap -c backup --volume data --prefix ora_test --retention=1

```

Schutz Ihrer Oracle Datenbank in Azure Cloud

Allen Cao, NetApp Solutions Engineering

In diesem Abschnitt wird beschrieben, wie Sie Ihre Oracle-Datenbank mit azacsnap-Tool schützen und Snapshot-Backup, Restore und Snapshots Tiering zu Azure Blob.

Sichern Sie die Oracle Datenbank mit Snapshot mit dem AzAcSnap Tool

Das Azure Application-konsistenter Snapshot-Tool (AzAcSnap) ist ein Befehlszeilen-Tool, das die Datensicherung für Datenbanken anderer Anbieter ermöglicht. Sie übernimmt die gesamte Orchestrierung, die erforderlich ist, um sie in einen applikationskonsistenten Zustand zu versetzen, bevor sie einen Storage-Snapshot erstellt. Anschließend werden die Datenbanken in einen Betriebszustand zurückversetzt.

Im Fall von Oracle versetzen Sie die Datenbank in den Backup-Modus, um einen Snapshot zu erstellen und dann den Backup-Modus aus dem Datenbank zu nehmen.

Backup-Daten und Protokoll-Volumes

Die Sicherung kann auf dem Datenbank-Server-Host mit einfachen Shell-Skript eingerichtet werden, das den Snapshot-Befehl ausführt. Anschließend kann das Skript so geplant werden, dass es von crontab ausgeführt wird.

Im Allgemeinen hängt die Häufigkeit der Backups von dem gewünschten RTO und RPO ab. Die regelmäßige Erstellung von Snapshots belegt mehr Speicherplatz. Es besteht ein Kompromiss zwischen der Häufigkeit von Backup und dem Platzbedarf.

Daten-Volumes verbrauchen in der Regel mehr Storage als Protokoll-Volumes. Daher können Sie alle 15 bis 30 Minuten Snapshots auf Daten-Volumes erstellen und häufigere Snapshots auf Log-Volumes erstellen.

Sehen Sie sich die folgenden Beispiele für Backup-Skripte und Zeitplanung an.

Für Daten-Volume Snapshots:

```
# /bin/sh
cd /home/azacsnap/bin
. ~/.bash_profile
azacsnap -c backup --volume data --prefix acao-ora01-data --retention 36
azacsnap -c backup --volume other --prefix acao-ora01-log --retention 250
```

Für Momentaufnahmen des Protokollvolumens:

```
# /bin/sh
cd /home/azacsnap/bin
. ~/.bash_profile
azacsnap -c backup --volume other --prefix acao-ora01-log --retention 250
```

Crontab-Zeitplan:

```
15,30,45 * * * * /home/azacsnap/snap_log.sh
0 */2 * * * /home/azacsnap/snap_data.sh
```



Beim Einrichten des Backups `azacsnap.json` Konfigurationsdatei: Fügen Sie alle Daten-Volumes, einschließlich des binären Volumes, zu hinzu `dataVolume` Und alle Log-Volumes auf `otherVolume`. Die maximale Aufbewahrung von Snapshots beträgt 250 Kopien.

Überprüfen Sie die Snapshots

Besuchen Sie das Azure-Portal > Azure NetApp Files/Volumes, um zu überprüfen, ob die Snapshots erfolgreich erstellt wurden.

The first screenshot shows the 'Snapshots' view for volume 'acao-ora01-u01'. The table lists two snapshots:

Name	Location	Created
acao-ora01-data_2022-09-09T16:52:55-023088322	South Central US	09/09/2022, 12:53:22 PM
acao-ora01-data_2022-09-12T16:05:56-98009392	South Central US	09/12/2022, 12:05:55 PM

The second screenshot shows the 'Snapshots' view for volume 'acao-ora01-u03'. The table lists ten snapshots:

Name	Location	Created
acao-ora01-data_2022-09-12T16:06:28-87547982	South Central US	09/12/2022, 12:06:31 PM
acao-ora01-log_2022-09-12T16:45:01-79659232	South Central US	09/12/2022, 12:45:04 PM
acao-ora01-log_2022-09-12T17:15:01-80326612	South Central US	09/12/2022, 01:15:04 PM
acao-ora01-log_2022-09-12T17:30:01-47879192	South Central US	09/12/2022, 01:30:04 PM
acao-ora01-log_2022-09-12T17:45:01-50106142	South Central US	09/12/2022, 01:45:04 PM
acao-ora01-log_2022-09-12T18:00:53-50298742	South Central US	09/12/2022, 02:00:55 PM
acao-ora01-log_2022-09-12T18:15:02-38570272	South Central US	09/12/2022, 02:15:05 PM
acao-ora01-log_2022-09-12T18:30:02-44073992	South Central US	09/12/2022, 02:30:07 PM

Oracle Restore und Recovery aus lokalem Backup

Einer der wichtigsten Vorteile von Snapshot Backups besteht darin, dass es mit den Quell-Datenbank-Volumes verbunden ist und die primären Datenbank-Volumes nahezu sofort zurückgesetzt werden können.

Wiederherstellung von Oracle auf dem primären Server

Das folgende Beispiel zeigt, wie eine Oracle Datenbank über das Azure Dashboard und über die CLI auf demselben Oracle Host wiederhergestellt und wiederhergestellt wird.

1. Erstellen Sie eine Testtabelle in der Datenbank, die wiederhergestellt werden soll.

```

[oracle@acao-ora01 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Mon Sep 12 19:02:35 2022
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL> create table testsnapshot(
    id integer,
    event varchar(100),
    dt timestamp);

Table created.

SQL> insert into testsnapshot values(1,'insert a data marker to validate
snapshot restore',sysdate);

1 row created.

SQL> commit;

Commit complete.

SQL> select * from testsnapshot;

   ID
-----
EVENT
-----
DT
-----
---
          1
insert a data marker to validate snapshot restore
12-SEP-22 07.07.35.000000 PM

```

2. Werfen Sie die Tabelle nach den Snapshot-Backups.

```
[oracle@acao-ora01 ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Tue Sep 13 14:20:22 2022  
Version 19.8.0.0.0
```

```
Copyright (c) 1982, 2019, Oracle. All rights reserved.
```

```
Connected to:
```

```
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production  
Version 19.8.0.0.0
```

```
SQL> drop table testsnapshot;
```

```
Table dropped.
```

```
SQL> select * from testsnapshot;  
select * from testsnapshot  
*
```

```
ERROR at line 1:
```

```
ORA-00942: table or view does not exist
```

```
SQL> shutdown immediate;
```

```
Database closed.
```

```
Database dismounted.
```

```
ORACLE instance shut down.
```

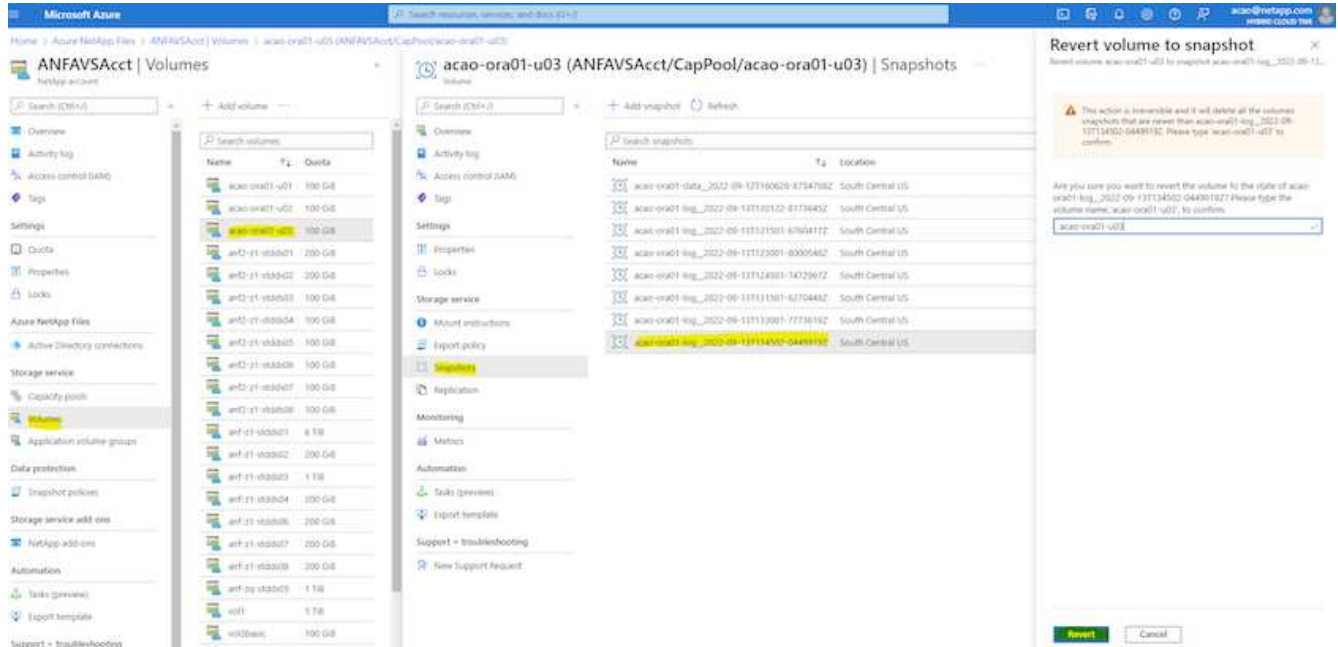
```
SQL> exit
```

```
Disconnected from Oracle Database 19c Enterprise Edition Release  
19.0.0.0.0 - Production  
Version 19.8.0.0.0
```

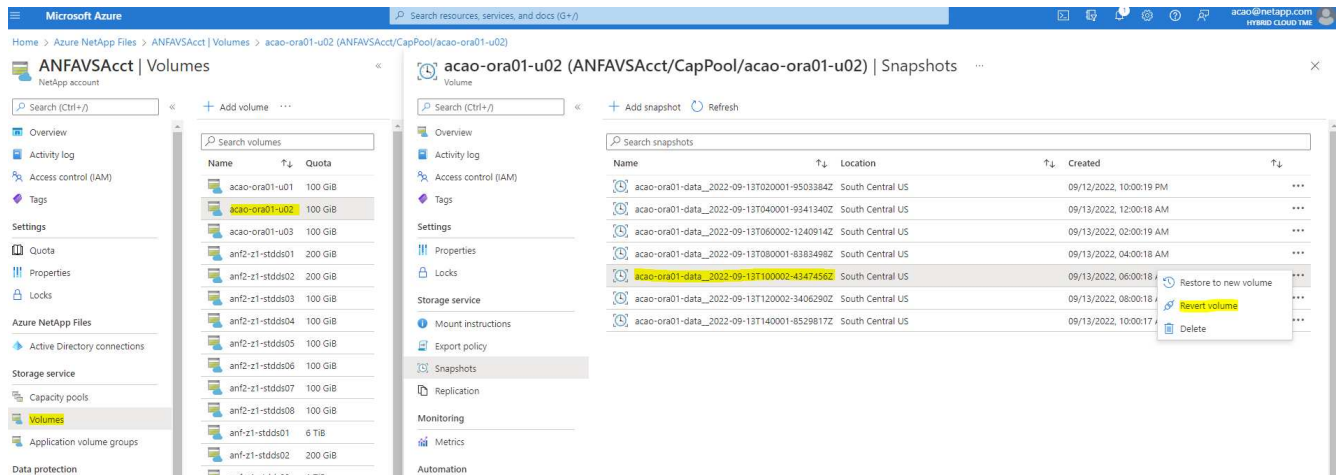
3. Stellen Sie im Azure NetApp Files Dashboard das Protokoll-Volumen in den letzten verfügbaren Snapshot wieder her. Wählen Sie **Lautstärke zurücksetzen**.

The screenshot shows the Azure NetApp Files dashboard. On the left, the 'Volumes' section is expanded, showing a list of volumes including 'acao-ora01-u03'. The main pane displays the 'Snapshots' view for the selected volume. A table lists snapshots with columns for Name, Location, and Created. The most recent snapshot, 'acao-ora01-log_2022-09-13T134502-04499192', is highlighted. A context menu is open over this snapshot, showing options: 'Restore to new volume', 'Revert volume', and 'Delete'.

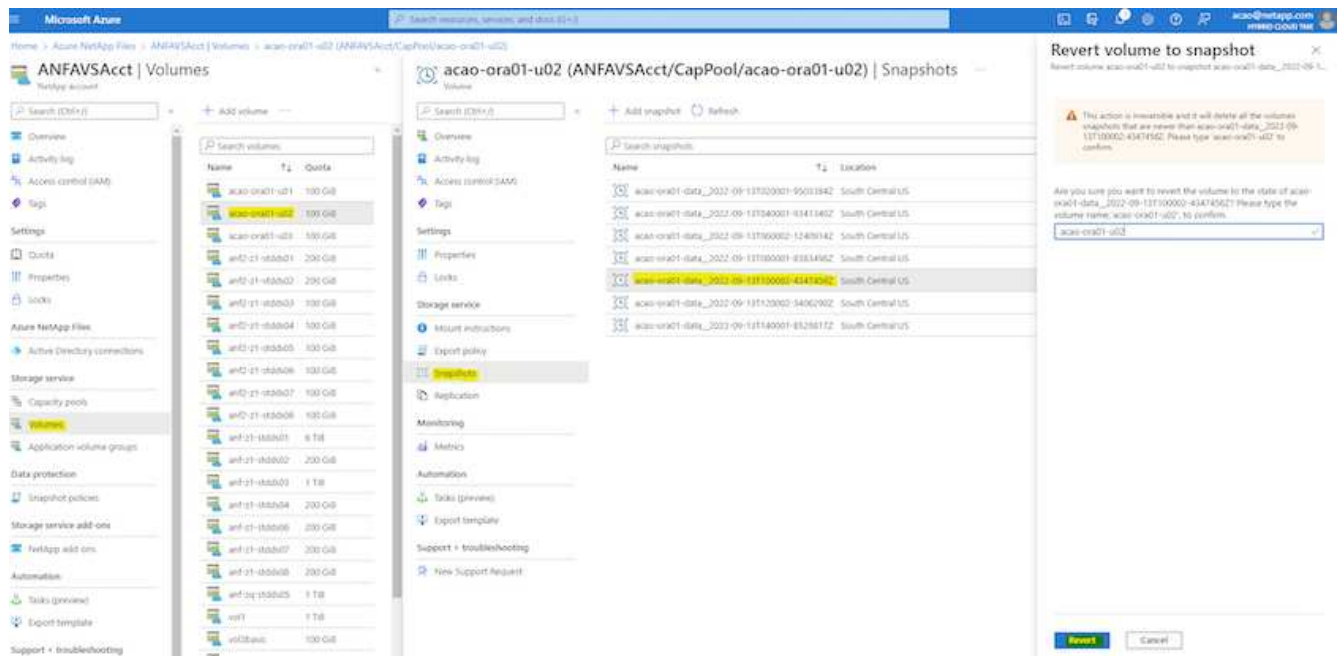
- Bestätigen Sie das Zurücksetzen des Volumes und klicken Sie auf **revert**, um die Umversion des Volumes auf die neueste verfügbare Sicherung abzuschließen.



- Wiederholen Sie die gleichen Schritte für das Datenvolumen, und stellen Sie sicher, dass das Backup die Tabelle enthält, die wiederhergestellt werden soll.



- Bestätigen Sie erneut die Umversion des Volumes und klicken Sie auf „Zurücksetzen“.



7. Synchronisieren Sie die Kontrolldateien neu, wenn Sie mehrere Kopien von ihnen haben, und ersetzen Sie die alte Kontrolldatei mit der neuesten verfügbaren Kopie.

```
[oracle@acao-ora01 ~]$ mv /u02/oradata/ORATST/control01.ct1
/u02/oradata/ORATST/control01.ct1.bk
[oracle@acao-ora01 ~]$ cp /u03/orareco/ORATST/control02.ct1
/u02/oradata/ORATST/control01.ct1
```

8. Melden Sie sich bei der Oracle-Server-VM an, und führen Sie Datenbank-Recovery mit sqlplus aus.

```
[oracle@acao-ora01 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Tue Sep 13 15:10:17 2022
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to an idle instance.

SQL> startup mount;
ORACLE instance started.

Total System Global Area 6442448984 bytes
Fixed Size 8910936 bytes
Variable Size 1090519040 bytes
Database Buffers 5335154688 bytes
Redo Buffers 7864320 bytes
Database mounted.
```



```
SQL> recover database using backup controlfile until cancel;
ORA-00279: change 3188523 generated at 09/13/2022 10:00:09 needed for
thread 1
ORA-00289: suggestion :
/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_43__22rnjq9q_.arc
ORA-00280: change 3188523 for thread 1 is in sequence #43

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

ORA-00279: change 3188862 generated at 09/13/2022 10:01:20 needed for
thread 1
ORA-00289: suggestion :
/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_44__29f2lgb5_.arc
ORA-00280: change 3188862 for thread 1 is in sequence #44
ORA-00278: log file
'/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_43__22rnjq9q_.arc' no
longer
needed for this recovery

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

ORA-00279: change 3193117 generated at 09/13/2022 12:00:08 needed for
thread 1
ORA-00289: suggestion :
/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_45__29h6qqyw_.arc
ORA-00280: change 3193117 for thread 1 is in sequence #45
ORA-00278: log file
'/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_44__29f2lgb5_.arc' no
longer
needed for this recovery

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}

ORA-00279: change 3193440 generated at 09/13/2022 12:01:20 needed for
thread 1
ORA-00289: suggestion :
/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_46_%u_.arc
ORA-00280: change 3193440 for thread 1 is in sequence #46
ORA-00278: log file
'/u03/orareco/ORATST/archivelog/2022_09_13/o1_mf_1_45__29h6qqyw_.arc' no
longer
needed for this recovery

Specify log: {<RET>=suggested | filename | AUTO | CANCEL}
cancel
Media recovery cancelled.
```

```

SQL> alter database open resetlogs;

Database altered.

SQL> select * from testsnapshot;

   ID
-----
EVENT
-----
-----
DT
-----
---
          1
insert a data marker to validate snapshot restore
12-SEP-22 07.07.35.000000 PM

SQL> select systimestamp from dual;

SYSTIMESTAMP
-----
---
13-SEP-22 03.28.52.646977 PM +00:00

```

Dieser Bildschirm zeigt, dass die abfallende Tabelle mit lokalen Snapshot-Backups wiederhergestellt wurde.

Datenbankmigration von On-Premises-Systemen in die Azure Cloud

Als Ergebnis der Entscheidung von Oracle, Datenbanken mit einer einzigen Instanz auszuplanen, haben viele Unternehmen Oracle Datenbanken mit einer Instanz in mandantenfähige Container-Datenbanken umgewandelt. Dies ermöglicht die einfache Verschiebung eines Teiles der Container-Datenbanken, genannt PDB in die Cloud, mit der Option für maximale Verfügbarkeit, die die Ausfallzeit während der Migration auf ein Minimum reduziert.

Wenn Sie jedoch weiterhin über eine einzelne Instanz einer Oracle-Datenbank verfügen, kann sie zunächst in eine mandantenfähige Container-Datenbank konvertiert werden, bevor Sie eine PDB-Verschiebung durchführen.

In den folgenden Abschnitten werden Einzelheiten zur Migration von lokalen Oracle Datenbanken in die Azure Cloud in beiden Szenarien beschrieben.

Konvertieren einer einzelnen nicht-CDB-Instanz in eine PDB in einer mandantenfähigen CDB

Falls Sie auch weiterhin über eine Oracle-Single-Instance-Datenbank verfügen, muss diese in eine mandantenfähige Container-Datenbank konvertiert werden, unabhängig davon, ob Sie die Datenbank in die Cloud migrieren möchten oder nicht, da Oracle einige Zeit lang keine Single-Instance-Datenbanken mehr

unterstützt.

Im folgenden Verfahren wird eine einzelne Instanzdatenbank als steckbare Datenbank oder eine PDB in eine Container-Datenbank gesteckt.

1. Erstellen Sie eine Shell-Container-Datenbank auf demselben Host wie die Single-Instance-Datenbank in einem separaten Server `ORACLE_HOME`.
2. Fahren Sie die Single Instance-Datenbank herunter, und starten Sie sie im schreibgeschützten Modus neu.
3. Führen Sie die aus `DBMS_PDB.DESCRIBE` Verfahren zum Generieren der Datenbank-Metadaten.

```
BEGIN
  DBMS_PDB.DESCRIBE (
    pdb_descr_file => '/home/oracle/ncdb.xml');
END;
/
```

4. Fahren Sie die Single-Instance-Datenbank herunter.
5. Starten Sie die Container-Datenbank.
6. Führen Sie die aus `DBMS_PDB.CHECK_PLUG_COMPATIBILITY` Funktion, um zu bestimmen, ob die nicht-CDB mit der CDB kompatibel ist.

```
SET SERVEROUTPUT ON
DECLARE
  compatible CONSTANT VARCHAR2(3) :=
    CASE DBMS_PDB.CHECK_PLUG_COMPATIBILITY(
      pdb_descr_file => '/disk1/oracle/ncdb.xml',
      pdb_name       => 'NCDB')
    WHEN TRUE THEN 'YES'
    ELSE 'NO'
END;
BEGIN
  DBMS_OUTPUT.PUT_LINE(compatible);
END;
/
```

Wenn die Ausgabe JA ist, ist die nicht-CDB kompatibel, und Sie können mit dem nächsten Schritt fortfahren.

Wenn DIE Ausgabe NEIN ist, ist die nicht-CDB nicht kompatibel, und Sie können die überprüfen `PDB_PLUG_IN_VIOLATIONS` Zeigen Sie an, warum es nicht kompatibel ist. Alle Verstöße müssen korrigiert werden, bevor Sie fortfahren. Beispielsweise sollten Versions- oder Patch-Fehlmatches durch Ausführen eines Upgrades oder des Opatch-Dienstprogramms behoben werden. Führen Sie nach der Korrektur der Verstöße den Lauf aus `DBMS_PDB.CHECK_PLUG_COMPATIBILITY` Um sicherzustellen, dass die nicht-CDB mit der CDB kompatibel ist.

7. Schließen Sie die einzelne nicht-CDB-Instanz an.

```
CREATE PLUGGABLE DATABASE ncdb USING '/home/oracle/ncdb.xml'
COPY
FILE_NAME_CONVERT = ('/disk1/oracle/dbs/', '/disk2/oracle/ncdb/')
;
```



Wenn auf dem Host nicht genügend Speicherplatz vorhanden ist, wird das angezeigt `NOCOPY`. Die Option kann verwendet werden, um die PDB zu erstellen. In diesem Fall ist eine Single-Instance nicht-CDB nach dem Plug-in als PDB nicht verwendbar, da die Originaldateien für die PDB verwendet wurden. Stellen Sie sicher, dass Sie vor der Konvertierung ein Backup erstellen, so dass es etwas gibt, auf das Sie zurückgreifen können, wenn etwas schief geht.

- Beginnen Sie mit PDB Upgrade nach der Konvertierung, wenn die Version zwischen der Quell-Einzelinstanz nicht-CDB und dem Ziel-CDB unterschiedlich sind. Bei der Konvertierung derselben Version kann dieser Schritt übersprungen werden.

```
sqlplus / as sysdba;
alter session set container=ncdb
alter pluggable database open upgrade;
exit;
dbupgrade -c ncdb -l /home/oracle
```

Überprüfen Sie die Aktualisierungsprotokolldatei im `/home/oracle` Verzeichnis.

- Öffnen Sie die steckbare Datenbank, überprüfen Sie auf Verstöße gegen das pdb-Plug-in und kompilieren Sie die ungültigen Objekte neu.

```
alter pluggable database ncdb open;
alter session set container=ncdb;
select message from pdb_plug_in_violations where type like '%ERR%' and
status <> 'RESOLVED';
$ORACLE_HOME/perl/bin/perl $ORACLE_HOME/rdbms/admin/catcon.pl -n 1 -c
'ncdb' -e -b utlrp -d $ORACLE_HOME/rdbms/admin utlrp.sql
```

- Ausführen `noncdb_to_pdb.sql` Um das Datenwörterbuch zu aktualisieren.

```
sqlplus / as sysdba
alter session set container=ncdb;
@$ORACLE_HOME/rdbms/admin/noncdb_to_pdb.sql;
```

Fahren Sie herunter, und starten Sie die Container-DB neu. Die `ncdb` wird aus dem eingeschränkten Modus entfernt.

Migrieren Sie lokale Oracle Datenbanken mit PDB-Verschiebung zu Azure

Die Oracle PDB-Verlagerung mit der Option für maximale Verfügbarkeit nutzt die Hot-Clone-Technologie von PDB, die die Verfügbarkeit von Quell-PDB ermöglicht, während die PDB auf das Ziel kopiert wird. Bei der Umschaltung werden die Benutzerverbindungen automatisch zur Ziel-PDB umgeleitet. So werden Ausfallzeiten unabhängig von der Größe der PDB minimiert. NetApp bietet ein auf Ansible basierendes Toolkit, das den Migrationsvorgang automatisiert.

1. Erstellen einer CDB in der öffentlichen Azure Cloud auf einer Azure VM mit derselben Version und Patch-Ebene
2. Klonen Sie im Ansible Controller eine Kopie des Automatisierungs-Toolkits.

```
git clone https://github.com/NetApp-Automation/na_ora_aws_migration.git
```

3. Lesen Sie die Anweisung in der README-Datei.
4. Konfigurieren Sie die Ansible-Host-Variablen-Dateien für die Oracle Quell- und Ziel-Server sowie die Konfigurationsdatei des DB-Server-Hosts für die Namensauflösung.
5. Installieren Sie die Voraussetzungen für den Ansible-Controller auf dem Ansible-Controller.

```
ansible-playbook -i hosts requirements.yml
ansible-galaxy collection install -r collections/requirements.yml
--force
```

6. Ausführen aller Aufgaben vor der Migration auf dem lokalen Server

```
ansible-playbook -i hosts ora_pdb_relocate.yml -u admin -k -K -t
ora_pdb_relo_onprem
```



Der Admin-Benutzer ist der Managementbenutzer auf dem lokalen Oracle Server-Host mit sudo-Berechtigungen. Der Admin-Benutzer wurde mit einem Passwort authentifiziert.

7. Oracle PDB-Verlagerung von lokalem Storage zum Azure Oracle Ziel-Host durchführen.

```
ansible-playbook -i hosts ora_pdb_relocate.yml -u azureuser --private
-key db1.pem -t ora_pdb_relo_primary
```



Der Ansible-Controller kann sich entweder vor Ort oder in der Azure Cloud befinden. Der Controller benötigt Konnektivität mit dem lokalen Oracle Server-Host und dem Azure Oracle VM-Host. Der Oracle-Datenbank-Port (z. B. 1521) ist offen zwischen dem lokalen Oracle-Server-Host und dem Azure Oracle-VM-Host.

Zusätzliche Optionen für die Migration von Oracle Datenbanken

In der Microsoft Dokumentation finden Sie weitere Migrationsoptionen: ["Entscheidungsprozess für die Oracle"](#)

On-Premises/Hybrid-Cloud

TR-4983: Vereinfachte, automatisierte Oracle-Implementierung auf NetApp ASA mit iSCSI

Allen Cao, Niyaz Mohamed, NetApp

Zweck

NetApp ASA Systeme bieten moderne Lösungen für Ihre SAN-Infrastruktur. Sie vereinfachen die Skalierung und ermöglichen es Ihnen, geschäftskritische Applikationen wie Datenbanken zu beschleunigen, stets verfügbar zu sein (99.9999 % Uptime) sowie TCO und Kohlendioxid ausstoß zu reduzieren. Die NetApp ASA Systeme umfassen Modelle der A-Serie, die für Applikationen mit höchsten Performance-Anforderungen konzipiert wurden, sowie Modelle der C-Serie, die für kostengünstige Implementierungen mit großer Kapazität optimiert sind. Gemeinsam bieten die Systeme der ASA A-Serie und C-Serie eine außergewöhnliche Performance, die eine bessere Kundenerfahrung ermöglicht, Ergebnisse schneller liefert, geschäftskritische Daten verfügbar, geschützt und sicher hält, und sie bieten mehr effektive Kapazität für alle Workloads, unterstützt mit der effektivsten Garantie der Branche.

In dieser Dokumentation wird die vereinfachte Implementierung von Oracle-Datenbanken in einer SAN-Umgebung mit ASA Systemen mithilfe von Ansible-Automatisierung demonstriert. Die Oracle-Datenbank wird in einer eigenständigen Neustartkonfiguration mit iSCSI-Protokoll für den Datenzugriff und Oracle ASM für das Management von Datenbankfestplatten auf dem ASA Storage-Array bereitgestellt. Darüber hinaus bietet es mit dem UI-Tool NetApp SnapCenter Informationen zum Backup, zur Wiederherstellung und zum Klonen von Oracle Datenbanken für einen speichereffizienten Betrieb von Datenbanken in NetApp ASA Systemen.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Automatisierte Implementierung von Oracle Datenbanken in NetApp ASA Systemen als primären Datenbank-Storage
- Backup und Restore von Oracle Datenbanken in NetApp ASA Systemen mit dem Tool NetApp SnapCenter
- Klonen von Oracle Datenbanken für Entwicklung/Test oder andere Anwendungsfälle in NetApp ASA Systemen mit dem Tool NetApp SnapCenter

Zielgruppe

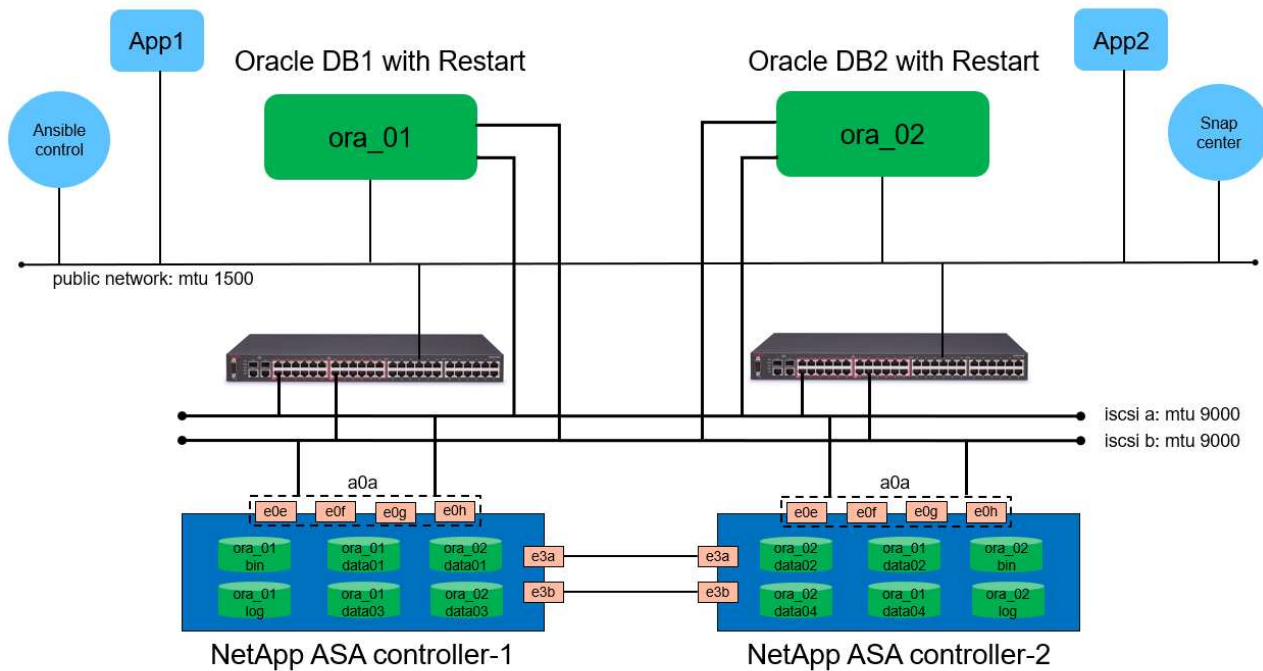
Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle in NetApp ASA Systemen einsetzen möchte.
- Ein Solution Architect für Datenbanken, der Oracle-Workloads in NetApp ASA-Systemen testen möchte.
- Ein Storage-Administrator, der eine Oracle Datenbank auf NetApp ASA Systemen implementieren und managen möchte.
- Ein Applikationseigentümer, der eine Oracle Datenbank in NetApp ASA Systemen einrichten möchte.

Test- und Validierungsumgebung der Lösung

Die Lösung wurde in einer Testumgebung getestet und validiert. Siehe Abschnitt [\[Key Factors for Deployment Consideration\]](#) Finden Sie weitere Informationen.

Simplified, Automated Oracle Database Deployment on NetApp ASA with iSCSI



NetApp

Hardware- und Softwarekomponenten

Hardware		
NetApp ASA A400	Version 9.13.1P1	2 NS224-Shelfs, 48 NVMe-AFF-Laufwerke mit einer Gesamtkapazität von 69.3 tib
UCSB-B200-M4	Intel® Xeon® CPU E5-2690 v4 @ 2,60 GHz	VMware ESXi Cluster mit 4 Nodes
Software		
Redhat Linux	RHEL-8.6, 4.18.0-372.9.1.el8.x86_64-Kernel	Bereitstellung der RedHat Subscription für Tests
Windows Server	2022 Standard, 10.0.20348 Build 20348	Hosting von SnapCenter-Servern
Oracle Grid Infrastructure	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
SnapCenter Server	Version 4.9P1	Workgroup-Bereitstellung

VMware vSphere Hypervisor	Version 6.5.0.20000	VMware Tools, Version: 11365 - Linux, 12352 - Windows
Öffnen Sie JDK	Version java-1.8.0-openjdk.x86_64	Anforderungen für SnapCenter Plugin auf DB VMs

Konfiguration der Oracle-Datenbank in der Laborumgebung

Server	* Datenbank*	DB-Speicher
ora_01	NTAP1(NTAP1_PDB1,NTAP1_PDB2,NTAP1_PDB3)	ISCSI-luns auf ASA A400
ora_02	NTAP2(NTAP2_PDB1,NTAP2_PDB2,NTAP2_PDB3)	ISCSI-luns auf ASA A400

Wichtige Faktoren für die Implementierung

- **Speicherlayout der Oracle-Datenbank.** in dieser automatisierten Oracle-Bereitstellung stellen wir vier Datenbankvolumes bereit, um Oracle-Binärdaten, -Daten und -Protokolle standardmäßig zu hosten. Dann erstellen wir zwei ASM-Festplattengruppen aus Daten und Protokoll-luns. Innerhalb der +DATA asm-Festplattengruppe stellen wir zwei Daten-luns in einem Volume auf jedem ASA A400-Cluster-Node bereit. Innerhalb der +LOGS asm-Festplattengruppe erstellen wir zwei luns in einem Protokoll-Volume auf einem einzelnen ASA A400 Knoten. Mehrere luns in einem ONTAP Volume bieten im Allgemeinen eine bessere Performance.
- **Implementierung mehrerer DB-Server.** die Automatisierungslösung kann eine Oracle-Container-Datenbank auf mehreren DB-Servern in einem einzelnen Ansible-Playbook bereitstellen. Unabhängig von der Anzahl der DB-Server bleibt die Playbook-Ausführung gleich. Bei Server-Implementierungen mit mehreren DB baut das Playbook mit einem Algorithmus auf, um Datenbank-luns optimal auf Dual-Controllern der ASA A400 zu platzieren. Die binären und logs luns der ungeraden Zahl DB Server in Server Hosts Index Platz auf Controller 1. Die binären und Protokolle luns der geraden Zahl DB-Server in den Server-Hosts Index Platz auf Controller 2. Die DB-Daten-luns sind gleichmäßig auf zwei Controller verteilt. Oracle ASM kombiniert die Daten-luns auf zwei Controllern in einer einzigen ASM-Festplattengruppe, um die Verarbeitungsleistung beider Controller voll auszuschöpfen.
- **ISCSI-Konfiguration.** die Datenbank-VMs werden über das iSCSI-Protokoll zum Speicherzugriff mit dem ASA-Speicher verbunden. Sie sollten duale Pfade auf jedem Controller-Knoten konfigurieren, um Redundanz zu gewährleisten, und iSCSI Multi-Path auf dem DB-Server für Multi-Path-Storage-Zugriff einrichten. Aktivieren Sie Jumbo Frame im Speichernetzwerk, um Performance und Durchsatz zu maximieren.
- **Oracle ASM-Redundanzebene, die für jede von Ihnen erstellte Oracle ASM-Laufwerksgruppe verwendet werden soll.** Da die ASA A400 den Speicher in RAID DP für den Datenschutz auf Clusterplattenebene konfiguriert, sollten Sie dies verwenden `External Redundancy`, Das bedeutet, dass die Option Oracle ASM nicht erlaubt, den Inhalt der Datenträgergruppe zu spiegeln.
- **Datenbanksicherung.** NetApp bietet eine SnapCenter Software Suite für Datenbank-Backup, -Wiederherstellung und -Klonen mit einer benutzerfreundlichen Benutzeroberfläche. NetApp empfiehlt die Implementierung eines solchen Management Tools, damit Snapshot Backups (unter einer Minute), schnelle Datenbank-Restores (in Minuten) und Datenbankklone möglich sind.

Lösungsimplementierung

In den folgenden Abschnitten werden schrittweise Verfahren für die automatisierte Bereitstellung und den Schutz von Oracle 19c in NetApp ASA A400 mit direkt gemounteten Datenbank-luns über iSCSI an DB-VM in

einem einzelnen Knoten beschrieben. Starten Sie die Konfiguration mit Oracle ASM als Datenbank-Volumen-Manager neu.

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wird davon ausgegangen, dass das NetApp ASA-Speicher-Array installiert und konfiguriert wurde. Dies umfasst iSCSI-Broadcast-Domäne, LACP-Schnittstellengruppen a0a auf beiden Controller-Nodes, iSCSI-VLAN-Ports (a0a-<iscsi-a-vlan-id>, a0a-<iscsi-b-vlan-id>) auf beiden Controller-Nodes. Unter dem folgenden Link finden Sie detaillierte Schritt-für-Schritt-Anleitungen, wenn Sie Hilfe benötigen. "[Detaillierter Leitfaden - ASA A400](#)"
2. Stellen Sie eine Linux-VM als Ansible-Controller-Node bereit, wobei die neueste Version von Ansible und Git installiert ist. Details finden Sie unter folgendem Link: "[Erste Schritte mit der Automatisierung von NetApp Lösungen](#)" In Abschnitt - Setup the Ansible Control Node for CLI deployments on RHEL / CentOS Oder Setup the Ansible Control Node for CLI deployments on Ubuntu / Debian.
3. Klonen Sie eine Kopie des NetApp Toolkit zur Implementierungsautomatisierung für iSCSI.

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-  
bb/na_oracle_deploy_iscsi.git
```

4. Stellen Sie einen Windows-Server bereit, um das UI-Tool NetApp SnapCenter mit der neuesten Version auszuführen. Details finden Sie unter folgendem Link: "[Installieren Sie den SnapCenter-Server](#)"
5. Erstellen Sie zwei RHEL Oracle DB Server entweder Bare Metal oder virtualisierte VM. Erstellen Sie einen Admin-Benutzer auf DB-Servern mit sudo ohne Passwortberechtigung und aktivieren Sie die SSH-Authentifizierung für private/öffentliche Schlüssel zwischen Ansible-Host und Oracle DB-Server-Hosts. Stellen Sie die folgenden Oracle 19c-Installationsdateien auf DB-Servern /tmp/Archive-Verzeichnis bereit.

```
installer_archives:  
- "LINUX.X64_193000_grid_home.zip"  
- "p34762026_190000_Linux-x86-64.zip"  
- "LINUX.X64_193000_db_home.zip"  
- "p34765931_190000_Linux-x86-64.zip"  
- "p6880880_190000_Linux-x86-64.zip"
```



Stellen Sie sicher, dass Sie mindestens 50G im Oracle VM Root-Volume zugewiesen haben, um ausreichend Speicherplatz für die Erstellung von Oracle Installationsdateien zu haben.

6. Sehen Sie sich das folgende Video an:

[Vereinfachte und automatisierte Oracle-Implementierung auf NetApp ASA mit iSCSI](#)

Automatisierungsparameter-Dateien

In dem Playbook „Ansible“ werden die Installations- und Konfigurationsaufgaben von Datenbanken mit vordefinierten Parametern ausgeführt. Für diese Oracle-Automatisierungslösung gibt es drei benutzerdefinierte Parameterdateien, die vor der Ausführung des Playbooks Benutzereingaben erfordern.

- Hosts: Legen Sie Ziele fest, für die das Automatisierungs-Playbook ausgeführt wird.
- vars/vars.yml - die globale Variablendatei, die Variablen definiert, die für alle Ziele gelten.
- Host_VARS/Host_Name.yml - die lokale Variablendatei, die Variablen definiert, die nur auf ein lokales Ziel angewendet werden. In unserem Anwendungsbeispiel handelt es sich um die Oracle DB-Server.

Zusätzlich zu diesen benutzerdefinierten Variablendateien gibt es mehrere standardmäßige Variablendateien, die Standardparameter enthalten, die nicht geändert werden müssen, sofern dies nicht erforderlich ist. Die folgenden Abschnitte zeigen, wie die benutzerdefinierten Variablendateien konfiguriert werden.

Konfiguration von Parameterdateien

1. Ansible Ziel hosts Dateikonfiguration:

```
# Enter NetApp ASA controller management IP address
[ontap]
172.16.9.32

# Enter Oracle servers names to be deployed one by one, follow by
each Oracle server public IP address, and ssh private key of admin
user for the server.
[oracle]
ora_01 ansible_host=10.61.180.21 ansible_ssh_private_key_file
=ora_01.pem
ora_02 ansible_host=10.61.180.23 ansible_ssh_private_key_file
=ora_02.pem
```

2. Weltweit vars/vars.yml Dateikonfiguration

```
#####
#####
#####          Oracle 19c deployment global user
configurable variables          #####
#####          Consolidate all variables from ONTAP, linux
and oracle          #####
#####
#####
#####          ONTAP env specific config variables
#####
#####
#####
#####
#####
#####          on-prem platform specific user defined variables #####
#####
#####          # Enter the supported ONTAP platform: on-prem, aws-fsx.
ontap_platform: on-prem

# Enter ONTAP cluster management user credentials
username: "xxxxxxxx"
password: "xxxxxxxx"

#####
#####          # Enter Oracle SVM iSCSI lif addresses. Each controller configures
```

```

with dual paths iscsi_a, iscsi_b for redundancy
ora_iscsi_lif_mgmt:
  - {name: '{{ svm_name }}_mgmt', address: 172.21.253.220, netmask:
255.255.255.0, vlan_name: ora_mgmt, vlan_id: 3509}

ora_iscsi_lifs_node1:
  - {name: '{{ svm_name }}_lif_1a', address: 172.21.234.221,
netmask: 255.255.255.0, vlan_name: ora_iscsi_a, vlan_id: 3490}
  - {name: '{{ svm_name }}_lif_1b', address: 172.21.235.221,
netmask: 255.255.255.0, vlan_name: ora_iscsi_b, vlan_id: 3491}
ora_iscsi_lifs_node2:
  - {name: '{{ svm_name }}_lif_2a', address: 172.21.234.223,
netmask: 255.255.255.0, vlan_name: ora_iscsi_a, vlan_id: 3490}
  - {name: '{{ svm_name }}_lif_2b', address: 172.21.235.223,
netmask: 255.255.255.0, vlan_name: ora_iscsi_b, vlan_id: 3491}

#####
#####
###           Linux env specific config variables
###
#####
#####

# Enter RHEL subscription to enable repo
redhat_sub_username: xxxxxxxx
redhat_sub_password: "xxxxxxx"

#####
#####
###           Oracle DB env specific config variables
###
#####
#####

# Enter Database domain name
db_domain: solutions.netapp.com

# Enter initial password for all required Oracle passwords. Change
them after installation.
initial_pwd_all: xxxxxxxx

```

3. Lokaler DB-Server host_vars/host_name.yml Konfiguration

```
# User configurable Oracle host specific parameters

# Enter container database SID. By default, a container DB is
created with 3 PDBs within the CDB
oracle_sid: NTAP1

# Enter database shared memory size or SGA. CDB is created with SGA
at 75% of memory_limit, MB. The grand total of SGA should not exceed
75% available RAM on node.
memory_limit: 8192
```

Ausführung des Playbook

Das Automatisierungs-Toolkit enthält insgesamt sechs Playbooks. Jede führt unterschiedliche Aufgabenblöcke aus und erfüllt unterschiedliche Zwecke.

```
0-all_playbook.yml - execute playbooks from 1-4 in one playbook run.
1-ansible_requirements.yml - set up Ansible controller with required
libs and collections.
2-linux_config.yml - execute Linux kernel configuration on Oracle DB
servers.
3-ontap_config.yml - configure ONTAP svm/volumes/luns for Oracle
database and grant DB server access to luns.
4-oracle_config.yml - install and configure Oracle on DB servers for
grid infrastructure and create a container database.
5-destroy.yml - optional to undo the environment to dismantle all.
```

Es gibt drei Optionen, um Playbooks mit den folgenden Befehlen auszuführen.

1. Führen Sie alle Playbooks für die Implementierung in einem kombinierten Durchlauf aus.

```
ansible-playbook -i hosts 0-all_playbook.yml -u admin -e
@vars/vars.yml
```

2. Führen Sie Playbooks einzeln mit der Zahlenfolge von 1 bis 4 aus.

```
ansible-playbook -i hosts 1-ansible_requirements.yml -u admin -e
@vars/vars.yml
```

```
ansible-playbook -i hosts 2-linux_config.yml -u admin -e
@vars/vars.yml
```

```
ansible-playbook -i hosts 3-ontap_config.yml -u admin -e
@vars/vars.yml
```

```
ansible-playbook -i hosts 4-oracle_config.yml -u admin -e
@vars/vars.yml
```

3. Führen Sie 0-all_Playbook.yml mit einem Tag aus.

```
ansible-playbook -i hosts 0-all_playbook.yml -u admin -e  
@vars/vars.yml -t ansible_requirements
```

```
ansible-playbook -i hosts 0-all_playbook.yml -u admin -e  
@vars/vars.yml -t linux_config
```

```
ansible-playbook -i hosts 0-all_playbook.yml -u admin -e  
@vars/vars.yml -t ontap_config
```

```
ansible-playbook -i hosts 0-all_playbook.yml -u admin -e  
@vars/vars.yml -t oracle_config
```

4. Die Umgebung rückgängig machen

```
ansible-playbook -i hosts 5-destroy.yml -u admin -e @vars/vars.yml
```

Validierung nach der Ausführung

Melden Sie sich nach der Ausführung des Playbooks als oracle-Benutzer beim oracle DB-Server an, um zu überprüfen, ob die Grid-Infrastruktur und die Datenbank von Oracle erfolgreich erstellt wurden. Im Folgenden sehen Sie ein Beispiel für die Validierung von Oracle-Datenbanken auf Host ora_01.

1. Die Grid-Infrastruktur und die erstellten Ressourcen validieren

```
[oracle@ora_01 ~]$ df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  7.7G       40K   7.7G   1% /dev
tmpfs                     7.8G      1.1G   6.7G  15% /dev/shm
tmpfs                     7.8G       312M   7.5G   4% /run
tmpfs                     7.8G        0   7.8G   0% /sys/fs/cgroup
/dev/mapper/rhel-root      44G       38G   6.8G  85% /
/dev/sda1                 1014M     258M   757M  26% /boot
tmpfs                     1.6G       12K   1.6G   1% /run/user/42
tmpfs                     1.6G       4.0K   1.6G   1% /run/user/1000
/dev/mapper/ora_01_biny_01p1 40G      21G    20G  52% /u01
[oracle@ora_01 ~]$ asm
[oracle@ora_01 ~]$ crsctl stat res -t
-----
-----
Name                Target  State          Server          State
details
-----
-----
Local Resources
-----
-----
ora.DATA.dg
                ONLINE  ONLINE        ora_01          STABLE
ora.LISTENER.lsnr
                ONLINE  INTERMEDIATE  ora_01          Not All
Endpoints Re
gistered, STABLE
ora.LOGS.dg
                ONLINE  ONLINE        ora_01          STABLE
ora.asm
                ONLINE  ONLINE        ora_01
Started, STABLE
ora.ons
                OFFLINE OFFLINE        ora_01          STABLE
-----
-----
Cluster Resources
-----
```



```

-----
ora.cssd
  1          ONLINE  ONLINE      ora_01      STABLE
ora.diskmon
  1          OFFLINE OFFLINE
ora.driver.afd
  1          ONLINE  ONLINE      ora_01      STABLE
ora.evmd
  1          ONLINE  ONLINE      ora_01      STABLE
ora.ntap1.db
  1          ONLINE  ONLINE      ora_01
Open,HOME=/u01/app/o

racle/product/19.0.0

/NTAP1, STABLE
-----
-----
[oracle@ora_01 ~]$

```



Ignorieren Sie die Not All Endpoints Registered Unter Statusdetails. Dies resultiert aus einem Konflikt der manuellen und dynamischen Datenbankregistrierung mit dem Listener und kann sicher ignoriert werden.

2. Überprüfen Sie, ob der ASM-Filtertreiber wie erwartet funktioniert.

```

[oracle@ora_01 ~]$ asmcmd
ASMCMDB> lsdg
State      Type      Rebal  Sector  Logical_Sector  Block      AU
Total_MB  Free_MB  Req_mir_free_MB  Usable_file_MB  Offline_disks
Voting_files  Name
MOUNTED   EXTERN  N      512     512    4096    4194304
327680    318644          0      318644          0
N  DATA/
MOUNTED   EXTERN  N      512     512    4096    4194304
81920     78880          0      78880          0
N  LOGS/
ASMCMDB> lsdsk
Path
AFD:ORA_01_DAT1_01
AFD:ORA_01_DAT1_03
AFD:ORA_01_DAT1_05
AFD:ORA_01_DAT1_07
AFD:ORA_01_DAT2_02
AFD:ORA_01_DAT2_04
AFD:ORA_01_DAT2_06
AFD:ORA_01_DAT2_08
AFD:ORA_01_LOGS_01
AFD:ORA_01_LOGS_02
ASMCMDB> afd_state
ASMCMDB-9526: The AFD state is 'LOADED' and filtering is 'ENABLED' on
host 'ora_01'
ASMCMDB>

```

3. Melden Sie sich bei Oracle Enterprise Manager Express an, um die Datenbank zu validieren.



ORACLE ENTERPRISE MANAGER DATABASE EXPRESS

Username

Password

Container Name

Log in



Copyright 2013, 2020, Oracle and/or its affiliates. All rights reserved.

ORACLE Enterprise Manager Database Express

NTAP1 (19.18.0.0.0) Performance Storage system

Database Home

Time Zone

Browser (GMT-05:00)

1 min Auto-Refresh

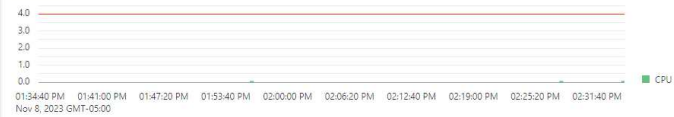
Refresh

Status

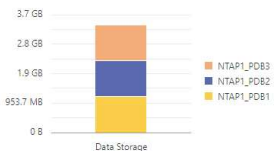
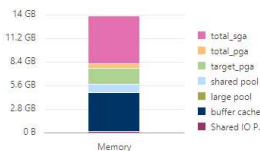
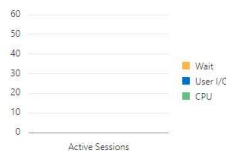
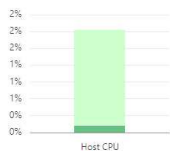
Up Time 1 hours, 7 minutes, 23 seconds
Type Single Instance (NTAP1)
CDB (3 PDB(s))
Version 19.18.0.0.0 Enterprise Edition
Platform Name Linux x86_64-bit
Thread 1
Archiver Stopped
Last Backup Time N/A
Incident(s) 4

Performance

Activity Services Containers



Resources



SQL Monitor - Last Hour (20 max)

Top 20 by Last Active Time

Filter by Status, SQL ID or User Name

Enable additional port from sqlplus for login to individual container database or PDBs.

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	NTAP1_PDB1	READ WRITE	NO
4	NTAP1_PDB2	READ WRITE	NO
5	NTAP1_PDB3	READ WRITE	NO

```
SQL> alter session set container=NTAP1_PDB1;
```

Session altered.

```
SQL> select dbms_xdb_config.gethttpsport() from dual;
```

```
DBMS_XDB_CONFIG.GETHTTPS()
-----
0
```

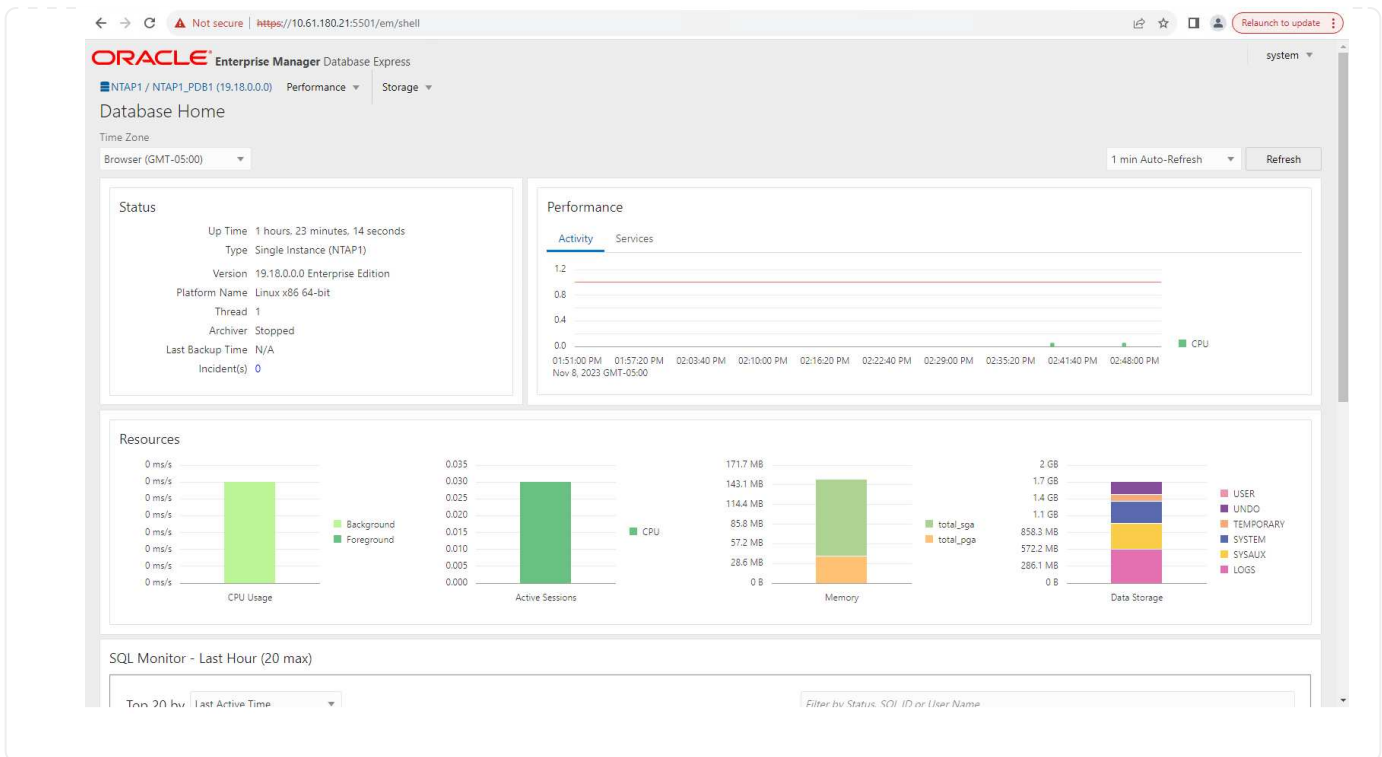
```
SQL> exec DBMS_XDB_CONFIG.SETHTTPS(5501);
```

PL/SQL procedure successfully completed.

```
SQL> select dbms_xdb_config.gethttpsport() from dual;
```

```
DBMS_XDB_CONFIG.GETHTTPS()
-----
5501
```

login to NTAP1_PDB1 from port 5501.



Backup, Wiederherstellung und Klonen von Oracle mit SnapCenter

Siehe TR-4979 "[Vereinfachtes, automatisiertes Oracle in VMware Cloud on AWS mit Gast-Mounted FSX ONTAP](#)" Abschnitt Oracle backup, restore, and clone with SnapCenter Bietet Details zur Einrichtung von SnapCenter und zur Ausführung von Datenbank-Backup-, Wiederherstellungs- und Klon-Workflows.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- NetApp ASA: REIN FLASH-BASIERTES SAN-ARRAY

["https://www.netapp.com/data-storage/all-flash-san-storage-array/"](https://www.netapp.com/data-storage/all-flash-san-storage-array/)

- Installieren der Oracle Grid-Infrastruktur für einen eigenständigen Server mit einer neuen Datenbankinstallation

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-oracle-grid-infrastructure-for-a-standalone-server-with-a-new-database-installation.html#GUID-0B1CEE8C-C893-46AA-8A6A-7B5FAAEC72B3)

- Installieren und Konfigurieren von Oracle Database mithilfe von Antwortdateien

["https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-r-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7"](https://docs.oracle.com/en/database/oracle/oracle-database/19/ladbi/installing-and-configuring-oracle-database-using-r-response-files.html#GUID-D53355E9-E901-4224-9A2A-B882070EDDF7)

- Verwenden Sie Red hat Enterprise Linux 8.2 mit ONTAP

["https://docs.netapp.com/us-en/ontap-sanhost/hu_rhel_82.html#all-san-array-configurations"](https://docs.netapp.com/us-en/ontap-sanhost/hu_rhel_82.html#all-san-array-configurations)

NVA-1155: Oracle 19c RAC-Datenbanken on FlexPod Datacenter with Cisco UCS and NetApp AFF A800 over FC - Design and Deployment Guide

Allen Cao, NetApp

Dieser Design- und Implementierungsleitfaden für Oracle 19c RAC-Datenbanken unter FlexPod Datacenter mit Cisco UCS und NetApp AFF A800 über FC bietet Details zum Lösungsdesign und schrittweise Implementierungsprozesse für das Hosting von Oracle RAC-Datenbanken auf der neuesten FlexPod Datacenter-Infrastruktur mit Oracle Linux 8.2 Betriebssystem und einen Red hat kompatiblen Kernel.

["NVA-1155: Oracle 19c RAC-Datenbanken on FlexPod Datacenter with Cisco UCS and NetApp AFF A800 over FC"](#)

TR-4250: SAP with Oracle on UNIX and NFS with NetApp Clustered Data ONTAP and SnapManager for SAP 3.4

Nils Bauer, NetApp

TR-4250 erläutert die Herausforderungen bei der Entwicklung von Storage-Lösungen zur Unterstützung von SAP Business Suite Produkten unter Verwendung einer Oracle Database. Das Hauptaugenmerk dieses Dokuments liegt auf dem allgemeinen Bedarf an Storage-Infrastruktur-Design, -Implementierung, -Betrieb und -Management-Herausforderungen. Geschäftliche und IT-Führungskräfte stehen dabei vor der Herausforderung, die auf der neuesten Generation von SAP-Lösungen basieren. Die Empfehlungen in diesem Dokument sind allgemein, nicht spezifisch für eine SAP-Anwendung oder Größe und Umfang der SAP-Implementierung. TR-4250 geht davon aus, dass der Leser über die grundlegenden Kenntnisse der Technologie und des Betriebs der NetApp- und SAP-Produkte verfügt. TR-4250 wurde entwickelt nach dem Zusammenspiel des technischen Personals von NetApp, SAP, Oracle und unseren Kunden.

["TR-4250: SAP with Oracle on UNIX and NFS with NetApp Clustered Data ONTAP and SnapManager for SAP 3.4"](#)

Implementieren Von Oracle Database

Lösungsüberblick

Automated Deployment of Oracle19c for ONTAP on NFS

Unternehmen automatisieren ihre Umgebungen, um die Effizienz zu steigern, Implementierungen zu beschleunigen und manuelle Aufgaben zu reduzieren. Konfigurationsmanagement-Tools wie Ansible werden zur Optimierung der Abläufe in Unternehmensdatenbanken eingesetzt. Diese Lösung zeigt, wie sich mit Ansible die Bereitstellung und Konfiguration von Oracle 19c mit NetApp ONTAP automatisieren lässt. Da Storage-Administratoren, Systemadministratoren und DBAs in der Lage sind, neuen Storage konsistent und schnell bereitzustellen, Datenbankserver zu konfigurieren und Oracle 19c Software zu installieren, profitieren Sie von folgenden Vorteilen:

- Vermeiden Sie Designkomplexität und menschliche Fehler und implementieren Sie eine wiederholbare, konsistente Implementierung und Best Practices
- Verkürzung der Zeit für Provisionierung von Speicher, Konfiguration von DB-Hosts sowie für Oracle-Installation
- Erhöhen Sie die Produktivität von Datenbank-Administratoren, -Systemen und -Storage-Administratoren
- Vereinfachen Sie die Skalierung von Storage und Datenbanken

NetApp bietet Kunden validierte Ansible-Module und -Rollen, um die Implementierung, Konfiguration und das Lifecycle-Management Ihrer Oracle-Datenbankumgebung zu beschleunigen. Diese Lösung bietet Anweisungen und Ansible-Playbook-Code, um Sie bei folgenden Aufgaben zu unterstützen:

- Erstellen und Konfigurieren von ONTAP-NFS-Storage für Oracle-Datenbank
- Installation von Oracle 19c auf RedHat Enterprise Linux 7/8 oder Oracle Linux 7/8
- Konfiguration von Oracle 19c auf ONTAP NFS Storage

Weitere Informationen erhalten Sie in den Übersichtsvideos unten.

AWX/Tower-Implementierungen

Teil 1: Erste Schritte, Anforderungen, Automatisierungsdetails und erste AWX/Tower-Konfiguration

[AWX-Bereitstellung](#)

Teil 2: Variablen und Ausführen des Playbooks

[AWX Playbook ausführen](#)

CLI-Implementierung

Teil 1: Erste Schritte, Anforderungen, Automatisierungsdetails und Ansible Control Host Setup

[CLI-Implementierung](#)

Teil 2: Variablen und Ausführen des Playbooks

[CLI Playbook ausgeführt](#)

Erste Schritte

Diese Lösung wurde für die Ausführung in einer AWX/Tower-Umgebung oder über CLI auf einem Ansible-Kontroll-Host entwickelt.

AWX/Tower

Für AWX-/Tower-Umgebungen werden Sie geleitet durch das Erstellen einer Bestandsaufnahme für das ONTAP Cluster-Management und den Oracle Server (IPs und Hostnamen), das Erstellen von Anmeldeinformationen, das Konfigurieren eines Projekts, das den Ansible-Code aus NetApp Automation Github zieht, und durch die Jobvorlage, die die Automatisierung startet.

1. Füllen Sie die Variablen aus, die für Ihre Umgebung spezifisch sind, und kopieren Sie sie in die Felder Extra Vars in Ihrer Job-Vorlage.
2. Nachdem die zusätzlichen Vars zu Ihrer Job-Vorlage hinzugefügt wurden, können Sie die Automatisierung starten.
3. Die Job-Vorlage wird in drei Phasen ausgeführt, indem Tags für `ontap_config`, `linux_config` und `oracle_config` angegeben werden.

CLI über den Ansible-Steuerhost

1. Konfigurieren des Linux-Hosts, sodass er als Ansible-Steuerhost verwendet werden kann "[Klicken Sie hier für detaillierte Anweisungen](#)"

2. Nach der Konfiguration des Ansible-Steuerhosts können Sie das Ansible Automation-Repository git klonen.
3. Bearbeiten Sie die Hostdatei mit den IPs und/oder Hostnamen Ihrer ONTAP-Clusterverwaltung und der Management-IPs des Oracle-Servers.
4. Geben Sie die Variablen ein, die für Ihre Umgebung spezifisch sind, und kopieren Sie sie in die `vars.yml` Datei:
5. Jeder Oracle Host verfügt über eine `variable` Datei, die über einen Hostnamen mit Host-spezifischen Variablen identifiziert wird.
6. Nachdem alle `variables` Dateien abgeschlossen wurden, können Sie das Playbook in drei Phasen ausführen, indem Sie Tags für `ontap_config`, `linux_config`, und `oracle_config`.

Anforderungen

Umgebung	Anforderungen
Ansible-Umgebung	AWX/Tower- oder Linux-Host, um der Ansible-Steuerungshost zu sein
	Ansible v.2.10 und höher
	Python 3
	Python Libraries - netapp-lib - xmltodict - jmespath
ONTAP	ONTAP Version 9.3 - 9.7
	Zwei Datenaggregate
	NFS vlan und iffrp wurden erstellt
Oracle Server	RHEL 7/8
	Oracle Linux 7/8
	Netzwerkschnittstellen für das NFS-, öffentlichen und optionalen Management
	Oracle Installationsdateien auf Oracle Servern

Automatisierungsdetails

Diese automatisierte Implementierung basiert auf einem einzigen Ansible-Playbook, das aus drei separaten Rollen besteht. Rollen sind Konfigurationen von ONTAP, Linux und Oracle. In der folgenden Tabelle werden die automatisierten Aufgaben beschrieben.

Rolle	Aufgaben
ontap_config	Vorabprüfung der ONTAP-Umgebung
	Erstellung NFS-basierter SVM für Oracle
	Erstellung einer Exportrichtlinie
	Erstellung von Volumes für Oracle
	Erstellung von NFS LIFs

Rolle	Aufgaben
linux_config	Erstellen von Bereitstellungspunkten und Mounten von NFS Volumes
	Überprüfen Sie die NFS-Mounts
	OS-spezifische Konfiguration
	Erstellen von Oracle Verzeichnissen
	konfigurieren Sie hugepages
	Deaktivieren Sie SELinux und den Firewall-Daemon
	Aktivieren und starten Sie den Chronyd-Dienst
	Erhöhen Sie die harte Grenze für den Dateideskriptor
	Erstellen Sie eine pam.d-Sitzungsdatei
oracle_config	Oracle Software-Installation
	Oracle Listener erstellen
	Erstellen Sie Oracle Datenbanken
	Konfiguration der Oracle Umgebung
	PDB-Status speichern
	Aktivieren Sie den Instanzarchivierungsmodus
	Aktivieren Sie den DNFS-Client
	Aktivieren Sie das automatische Starten und Herunterfahren der Datenbank zwischen einem Neustart des Betriebssystems

Standardparameter

Um die Automatisierung zu vereinfachen, haben wir viele erforderliche Oracle Implementierungsparameter mit Standardwerten voreingestellt. In der Regel ist es nicht erforderlich, die Standardparameter für die meisten Implementierungen zu ändern. Ein fortgeschrittener Benutzer kann mit Vorsicht Änderungen an den Standardparametern vornehmen. Die Standardparameter befinden sich in jedem Rollenordner unter dem Standardverzeichnis.

Implementierungsanleitungen

Laden Sie vor dem Start die folgenden Oracle-Installations- und Patch-Dateien herunter, und legen Sie sie in den ein `/tmp/archive` Verzeichnis mit Lese-, Schreib- und Lesezugriff für alle Benutzer auf jedem zu implementierenden DB-Server. Die Automatisierungsaufgaben suchen nach den benannten Installationsdateien in diesem speziellen Verzeichnis für die Installation und Konfiguration von Oracle.

```
LINUX.X64_193000_db_home.zip -- 19.3 base installer
p31281355_190000_Linux-x86-64.zip -- 19.8 RU patch
p6880880_190000_Linux-x86-64.zip -- opatch version 12.2.0.1.23
```

Lizenz

Sie sollten die Lizenzinformationen wie im Github-Repository angegeben lesen. Durch Zugriff, Herunterladen, Installation oder Nutzung des Inhalts in diesem Repository stimmen Sie den Bedingungen der Lizenz zu "[Hier](#)".

Beachten Sie, dass es bestimmte Beschränkungen bezüglich der Erstellung und/oder Freigabe abgeleiteter Werke mit dem Inhalt in diesem Repository gibt. Bitte lesen Sie die Bedingungen des "[Lizenz](#)" Vor der Verwendung des Inhalts. Wenn Sie nicht mit allen Bedingungen einverstanden sind, dürfen Sie den Inhalt in diesem Repository nicht aufrufen, herunterladen oder verwenden.

Klicken Sie anschließend auf "[Hier finden Sie ausführliche AWX/Tower-Implementierungsverfahren](#)" Oder "[Hier geht es zur CLI-Implementierung](#)".

Schritt-für-Schritt-Anweisungen zur Implementierung

AWX/Tower-Implementierung der Oracle 19c-Datenbank

1. Erstellen Sie das Inventar, die Gruppe, die Hosts und die Anmeldeinformationen für Ihre Umgebung

In diesem Abschnitt wird die Einrichtung von Inventar, Gruppen, Hosts und Zugangsdaten im AWX/Ansible Tower beschrieben, die die Umgebung für den Einsatz automatisierter NetApp Lösungen vorbereiten.

1. Konfigurieren Sie den Bestand.
 - a. Navigieren Sie zu Ressourcen → Inventar → Hinzufügen, und klicken Sie auf Inventar hinzufügen.
 - b. Geben Sie den Namen und die Organisationsdetails ein, und klicken Sie auf Speichern.
 - c. Klicken Sie auf der Seite Inventar auf den erstellten Bestand.
 - d. Wenn es Bestandsvariablen gibt, fügen Sie diese in das Feld Variablen ein.
 - e. Navigieren Sie zum Untermenü Gruppen, und klicken Sie auf Hinzufügen.
 - f. Geben Sie den Namen der Gruppe für ONTAP ein, fügen Sie die Gruppenvariablen ein (falls vorhanden) und klicken Sie auf Speichern.
 - g. Wiederholen Sie den Vorgang für eine andere Gruppe für Oracle.
 - h. Wählen Sie die erstellte ONTAP-Gruppe aus, gehen Sie zum Untermenü Hosts und klicken Sie auf Neuen Host hinzufügen.
 - i. Geben Sie die IP-Adresse der ONTAP-Cluster-Management-IP an, fügen Sie die Host-Variablen ein (falls vorhanden), und klicken Sie auf Speichern.
 - j. Dieser Prozess muss für die Oracle-Gruppe und für Oracle-Host(s)-Management-IP/Hostname wiederholt werden.
2. Erstellen von Anmeldungstypen. Bei Lösungen, die ONTAP verwenden, müssen Sie den Anmeldeinformationstyp so konfigurieren, dass er mit den Einträgen für Benutzernamen und Kennwort übereinstimmt.
 - a. Navigieren Sie zu Administration → Credential Types, und klicken Sie auf Add.
 - b. Geben Sie den Namen und eine Beschreibung an.
 - c. Fügen Sie den folgenden Inhalt in die Eingabekonfiguration ein:

```
fields:
  - id: username
    type: string
    label: Username
  - id: password
    type: string
    label: Password
    secret: true
  - id: vsadmin_password
    type: string
    label: vsadmin_password
    secret: true
```

1. Fügen Sie folgenden Inhalt in die Konfiguration des Injektors ein:

```
extra_vars:
  password: '{{ password }}'
  username: '{{ username }}'
  vsadmin_password: '{{ vsadmin_password }}'
```

1. Konfigurieren Sie die Anmeldedaten.

- a. Navigieren Sie zu Resources → Credentials, und klicken Sie auf Add.
- b. Geben Sie den Namen und die Organisationsdetails für ONTAP ein.
- c. Wählen Sie den benutzerdefinierten Anmeldungstyp aus, den Sie für ONTAP erstellt haben.
- d. Geben Sie unter „Type Details“ den Benutzernamen, das Passwort und das vsadmin_password ein.
- e. Klicken Sie auf Zurück zur Anmeldeinformation, und klicken Sie auf Hinzufügen.
- f. Geben Sie den Namen und die Organisationsdetails für Oracle ein.
- g. Wählen Sie den Typ der Geräteanmeldeinformationen aus.
- h. Geben Sie unter „Typdetails“ den Benutzernamen und das Kennwort für die Oracle-Hosts ein.
- i. Wählen Sie die richtige Privilege-Eskalationsmethode aus, und geben Sie Benutzernamen und Kennwort ein.

2. Erstellen Sie ein Projekt

1. Gehen Sie zu Ressourcen → Projekte, und klicken Sie auf Hinzufügen.
 - a. Geben Sie den Namen und die Organisationsdetails ein.
 - b. Wählen Sie im Feld Quellenkontrolle Credential Type die Option Git aus.
 - c. Eingabe <https://github.com/NetApp-Automation/na_oracle19c_deploy.git> Als URL für die Quellensteuerung.
 - d. Klicken Sie auf Speichern .
 - e. Das Projekt muss gelegentlich synchronisiert werden, wenn sich der Quellcode ändert.

3. Oracle Host_vars konfigurieren

Die in diesem Abschnitt definierten Variablen werden auf jeden einzelnen Oracle Server und jede Datenbank angewendet.

1. Geben Sie Ihre umgebungsspezifischen Parameter in das folgende eingebettete Oracle-Hosts-Variablen oder Host_vars-Formular ein.



Die blauen Elemente müssen an Ihre Umgebung angepasst werden.

Host VARS-Konfiguration

```
#####
##### Host Variables Configuration #####
#####

# Add your Oracle Host
ansible_host: "10.61.180.15"

# Oracle db log archive mode: true - ARCHIVELOG or false - NOARCHIVELOG
log_archive_mode: "true"

# Number of pluggable databases per container instance identified by sid.
Pdb_name specifies the prefix for container database naming in this case
cdb2_pdb1, cdb2_pdb2, cdb2_pdb3
oracle_sid: "cdb2"
pdb_num: "3"
pdb_name: "{{ oracle_sid }}_pdb"

# CDB listener port, use different listener port for additional CDB on
same host
listener_port: "1523"

# CDB is created with SGA at 75% of memory_limit, MB. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB. The grand total SGA should not exceed 75% available RAM on node.
memory_limit: "5464"

# Set "em_configuration: DBEXPRESS" to install enterprise manager express
and choose a unique port from 5500 to 5599 for each sid on the host.
# Leave them black if em express is not installed.
em_configuration: "DBEXPRESS"
em_express_port: "5501"

# {{groups.oracle[0]}} represents first Oracle DB server as defined in
Oracle hosts group [oracle]. For concurrent multiple Oracle DB servers
deployment, [0] will be incremented for each additional DB server. For
```

example, `{{groups.oracle[1]}}`" represents DB server 2, `{{groups.oracle[2]}}`" represents DB server 3 ... As a good practice and the default, minimum three volumes is allocated to a DB server with corresponding `/u01`, `/u02`, `/u03` mount points, which store oracle binary, oracle data, and oracle recovery files respectively. Additional volumes can be added by click on "More NFS volumes" but the number of volumes allocated to a DB server must match with what is defined in global vars file by `volumes_nfs` parameter, which dictates how many volumes are to be created for each DB server.

```
host_datastores_nfs:
  - {vol_name: "{{groups.oracle[0]}}_u01", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
  - {vol_name: "{{groups.oracle[0]}}_u02", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
  - {vol_name: "{{groups.oracle[0]}}_u03", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
```

1. Füllen Sie alle Variablen in die blauen Felder ein.
2. Klicken Sie nach Abschluss der Variablen auf die Schaltfläche Kopieren im Formular, um alle Variablen zu kopieren, die an AWX oder Tower übertragen werden sollen.
3. Navigieren Sie zurück zu AWX oder Tower, und gehen Sie zu Ressourcen → Hosts, und wählen Sie und öffnen Sie die Konfigurationsseite für den Oracle-Server.
4. Klicken Sie auf der Registerkarte Details auf Bearbeiten und fügen Sie die kopierten Variablen aus Schritt 1 in das Feld Variablen unter der Registerkarte YAML ein.
5. Klicken Sie auf Speichern .
6. Wiederholen Sie diesen Vorgang für alle weiteren Oracle Server im System.

4. Globale Variablen konfigurieren

Die in diesem Abschnitt definierten Variablen gelten für alle Oracle Hosts, Datenbanken und den ONTAP Cluster.

1. Geben Sie Ihre umgebungsspezifischen Parameter in das folgende eingebettete globale Variablen oder Vars-Formular ein.



Die blauen Elemente müssen an Ihre Umgebung angepasst werden.

```
#####
##### Oracle 19c deployment global user configuration variables #####
##### Consolidate all variables from ontap, linux and oracle #####
#####

#####
### Ontap env specific config variables ###
#####
```

```

#Inventory group name
#Default inventory group name - 'ontap'
#Change only if you are changing the group name either in inventory/hosts
file or in inventory groups in case of AWX/Tower
hosts_group: "ontap"

#CA_signed_certificates (ONLY CHANGE to 'true' IF YOU ARE USING CA SIGNED
CERTIFICATES)
ca_signed_certs: "false"

#Names of the Nodes in the ONTAP Cluster
nodes:
  - "AFF-01"
  - "AFF-02"

#Storage VLANs
#Add additional rows for vlans as necessary
storage_vlans:
  - {vlan_id: "203", name: "infra_NFS", protocol: "NFS"}
More Storage VLANsEnter Storage VLANs details

#Details of the Data Aggregates that need to be created
#If Aggregate creation takes longer, subsequent tasks of creating volumes
may fail.
#There should be enough disks already zeroed in the cluster, otherwise
aggregate create will zero the disks and will take long time
data_aggregates:
  - {aggr_name: "aggr01_node01"}
  - {aggr_name: "aggr01_node02"}

#SVM name
svm_name: "ora_svm"

# SVM Management LIF Details
svm_mgmt_details:
  - {address: "172.21.91.100", netmask: "255.255.255.0", home_port: "e0M"}

# NFS storage parameters when data_protocol set to NFS. Volume named after
Oracle hosts name identified by mount point as follow for oracle DB server
1. Each mount point dedicates to a particular Oracle files: u01 - Oracle
binary, u02 - Oracle data, u03 - Oracle redo. Add additional volumes by
click on "More NFS volumes" and also add the volumes list to corresponding
host_vars as host_datastores_nfs variable. For multiple DB server
deployment, additional volumes sets needs to be added for additional DB
server. Input variable "{{groups.oracle[1]}}_u01",
 "{{groups.oracle[1]}}_u02", and "{{groups.oracle[1]}}_u03" as vol_name for

```

second DB server. Place volumes for multiple DB servers alternately between controllers for balanced IO performance, e.g. DB server 1 on controller node1, DB server 2 on controller node2 etc. Make sure match lif address with controller node.

```
volumes_nfs:
  - {vol_name: "{{groups.oracle[0]}}_u01", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
  - {vol_name: "{{groups.oracle[0]}}_u02", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
  - {vol_name: "{{groups.oracle[0]}}_u03", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
```

```
#NFS LIFs IP address and netmask
```

```
nfs_lifs_details:
  - address: "172.21.94.200" #for node-1
    netmask: "255.255.255.0"
  - address: "172.21.94.201" #for node-2
    netmask: "255.255.255.0"
```

```
#NFS client match
```

```
client_match: "172.21.94.0/24"
```

```
#####
### Linux env specific config variables ###
#####
```

```
#NFS Mount points for Oracle DB volumes
```

```
mount_points:
  - "/u01"
  - "/u02"
  - "/u03"
```

```
# Up to 75% of node memory size divided by 2mb. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB.
```

```
# Leave it blank if hugepage is not configured on the host.
```

```
hugepages_nr: "1234"
```

```
# RedHat subscription username and password
```

```
redhat_sub_username: "xxx"
redhat_sub_password: "xxx"
```

```
#####
### DB env specific install and config variables ###
#####

db_domain: "your.domain.com"

# Set initial password for all required Oracle passwords. Change them
after installation.

initial_pwd_all: "netapp123"
```

1. Alle Variablen in blaue Felder eintragen.
2. Klicken Sie nach Abschluss der Variablen auf die Schaltfläche Kopieren im Formular, um alle Variablen zu kopieren, die an AWX oder Tower übertragen werden sollen, in die folgende Jobvorlage.

5. Konfigurieren und starten Sie die Jobvorlage.

1. Erstellen Sie die Job-Vorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen → Hinzufügen, und klicken Sie auf Job Template hinzufügen.
 - b. Geben Sie den Namen und die Beschreibung ein
 - c. Wählen Sie den Jobtyp aus. Führen Sie die Konfiguration des Systems anhand eines Playbooks aus, und prüfen Sie, ob ein Playbook trocken ausgeführt wird, ohne das System tatsächlich zu konfigurieren.
 - d. Wählen Sie den entsprechenden Bestand, das Projekt, das Playbook und die Zugangsdaten für das Playbook aus.
 - e. Wählen Sie all_Playbook.yml als Standard-Playbook aus, das ausgeführt werden soll.
 - f. Fügen Sie globale Variablen, die aus Schritt 4 kopiert wurden, in das Feld Vorlagenvariablen unter der Registerkarte YAML ein.
 - g. Aktivieren Sie das Kontrollkästchen Aufforderung zum Starten im Feld Job-Tags.
 - h. Klicken Sie auf Speichern .
2. Starten Sie die Jobvorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen.
 - b. Klicken Sie auf die gewünschte Vorlage und dann auf Starten.
 - c. Wenn Sie beim Start nach Job-Tags gefragt werden, geben Sie Anforderungen_config ein. Möglicherweise müssen Sie unter Requirements_config auf die Zeile Job-Tag erstellen klicken, um die Job-Tag-Nummer einzugeben.



Requirements_config stellt sicher, dass Sie über die richtigen Bibliotheken verfügen, um die anderen Rollen auszuführen.

1. Klicken Sie auf Weiter und dann auf Start, um den Job zu starten.
2. Klicken Sie auf Ansicht → Jobs, um die Jobausgabe und den Fortschritt zu überwachen.

3. Wenn Sie zur Einführung von Job-Tags aufgefordert werden, geben sie `ontap_config` ein. Sie müssen möglicherweise direkt unter `ontap_config` auf die Zeile „Job Tag erstellen“ klicken, um das Job-Tag einzugeben.
4. Klicken Sie auf Weiter und dann auf Start, um den Job zu starten.
5. Klicken Sie auf Ansicht → Jobs, um die Jobausgabe und den Fortschritt zu überwachen
6. Führen Sie nach Abschluss der rolle `ontap_config` den Prozess für `linux_config` erneut aus.
7. Navigieren Sie zu Ressourcen → Vorlagen.
8. Wählen Sie die gewünschte Vorlage aus, und klicken Sie dann auf Starten.
9. Wenn Sie beim Start aufgefordert werden, geben Sie die Job-Tags in `linux_config` ein, müssen Sie möglicherweise die Zeile „Job-Tag erstellen“ direkt unter `linux_config` auswählen, um das Job-Tag einzugeben.
10. Klicken Sie auf Weiter und dann auf Start, um den Job zu starten.
11. Wählen Sie Ansicht → Jobs, um die Jobausgabe und den Fortschritt zu überwachen.
12. Führen Sie nach Abschluss der rolle `linux_config` den Prozess für `oracle_config` erneut aus.
13. Gehen Sie zu Ressourcen → Vorlagen.
14. Wählen Sie die gewünschte Vorlage aus, und klicken Sie dann auf Starten.
15. Wenn Sie beim Start nach Job-Tags gefragt werden, geben sie `oracle_config` ein. Sie müssen möglicherweise die Zeile „Job Tag erstellen“ direkt unter `oracle_config` auswählen, um das Job-Tag einzugeben.
16. Klicken Sie auf Weiter und dann auf Start, um den Job zu starten.
17. Wählen Sie Ansicht → Jobs, um die Jobausgabe und den Fortschritt zu überwachen.

6. Implementieren Sie zusätzliche Datenbank auf demselben Oracle Host

Der Oracle Teil des Playbook erstellt pro Ausführung eine einzelne Oracle-Container-Datenbank auf einem Oracle-Server. Führen Sie die folgenden Schritte aus, um zusätzliche Container-Datenbanken auf demselben Server zu erstellen.

1. `Host_Vars`-Variablen überarbeiten.
 - a. Zurück zu Schritt 2 - Oracle `Host_Vars` konfigurieren.
 - b. Ändern Sie Oracle SID zu einer anderen Namenskonvention.
 - c. Ändern Sie den Listener-Port in eine andere Zahl.
 - d. Ändern Sie den EM Express-Port in eine andere Nummer, wenn Sie EM Express installieren.
 - e. Kopieren Sie die überarbeiteten Hostvariablen in das Feld Oracle Host Variables auf der Registerkarte Host Configuration Detail.
2. Starten Sie die Jobvorlage für die Bereitstellung nur mit dem tag `oracle_config`.
3. Melden Sie sich beim Oracle-Server als Oracle-Benutzer an und führen Sie die folgenden Befehle aus:

```
ps -ef | grep ora
```



Auf diese Weise werden die oracle-Prozesse aufgeführt, wenn die Installation wie erwartet abgeschlossen wurde und die oracle DB gestartet wurde

4. Melden Sie sich bei der Datenbank an, um die db-Konfigurationseinstellungen und die PDBs zu überprüfen, die mit den folgenden Befehlsätzen erstellt wurden.

```
[oracle@localhost ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 12:52:51 2021
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL>

SQL> select name, log_mode from v$database;
NAME          LOG_MODE
-----
CDB2          ARCHIVELOG

SQL> show pdbs

          CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
          2 PDB$SEED                                READ ONLY  NO
          3 CDB2_PDB1                              READ WRITE NO
          4 CDB2_PDB2                              READ WRITE NO
          5 CDB2_PDB3                              READ WRITE NO

col svrname form a30
col dirname form a30
select svrname, dirname, nfsversion from v$dnfs_servers;

SQL> col svrname form a30
SQL> col dirname form a30
SQL> select svrname, dirname, nfsversion from v$dnfs_servers;

SVRNAME                                DIRNAME                                NFSVERSION
-----
172.21.126.200                        /rhelora03_u02                        NFSv3.0
172.21.126.200                        /rhelora03_u03                        NFSv3.0
172.21.126.200                        /rhelora03_u01                        NFSv3.0
```

Dies bestätigt, dass dNFS richtig funktioniert.

5. Stellen Sie über Listener eine Verbindung zur Datenbank her, um die Konfiguration des Oracle Listener mit dem folgenden Befehl zu überprüfen. Wechseln Sie zum entsprechenden Listener-Port und Datenbankdienstnamen.

```
[oracle@localhost ~]$ sqlplus
system@//localhost:1523/cdb2_pdb1.cie.netapp.com

SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 13:19:57 2021
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Enter password:
Last Successful login time: Wed May 05 2021 17:11:11 -04:00

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL> show user
USER is "SYSTEM"
SQL> show con_name
CON_NAME
CDB2_PDB1
```

Dies bestätigt, dass Oracle Listener ordnungsgemäß funktioniert.

Wo Hilfe benötigt wird?

Wenn Sie Hilfe mit dem Toolkit benötigen, nehmen Sie bitte an der Teil ["NetApp Solution Automation Community Support Slack Channel"](#) Und suchen Sie den Kanal zur Lösungsautomatisierung, um Ihre Fragen zu stellen oder zu fragen.

Schritt-für-Schritt-Anweisungen zur Implementierung

In diesem Dokument wird die Implementierung von Oracle 19c über die Befehlszeilenschnittstelle (cli) der Automatisierung beschrieben.

CLI-Implementierung einer Oracle 19c Datenbank

In diesem Abschnitt werden die Schritte beschrieben, die für die Vorbereitung und Implementierung der Oracle19c-Datenbank mit der CLI erforderlich sind. Stellen Sie sicher, dass Sie den geprüft haben ["Erste Schritte und Abschnitt zu den Anforderungen"](#) Und Ihre Umgebung entsprechend vorbereitet.

Oracle19c repo herunterladen

1. Führen Sie auf Ihrem ansible-Controller den folgenden Befehl aus:

```
git clone https://github.com/NetApp-Automation/na_oracle19c_deploy.git
```

2. Ändern Sie nach dem Herunterladen des Projektarchivs die Verzeichnisse in na_oracle19c_Deploy <cd na_oracle19c_deploy>.

Bearbeiten Sie die Host-Datei

Vor der Bereitstellung Folgendes abschließen:

1. Bearbeiten Sie die Host-Datei na_oracle19c_Deploy.
2. Ändern Sie unter [ONTAP] die IP-Adresse in Ihre Cluster-Management-IP.
3. Fügen Sie unter der Gruppe [oracle] die namen der oracle-Hosts hinzu. Der Host-Name muss für seine IP-Adresse entweder über DNS oder über die Hosts-Datei aufgelöst werden, oder er muss im Host angegeben werden.
4. Speichern Sie nach Abschluss dieser Schritte alle Änderungen.

Im folgenden Beispiel wird eine Host-Datei dargestellt:

```
#ONTAP Host

[ontap]

"10.61.184.183"

#Oracle hosts

[oracle]

"rtpora01"

"rtpora02"
```

Dieses Beispiel führt das Playbook aus und implementiert oracle 19c gleichzeitig auf zwei oracle DB Servern. Sie können auch mit nur einem DB-Server testen. In diesem Fall müssen Sie nur eine Host-Variablendatei konfigurieren.



Das Playbook wird unabhängig davon, wie viele Oracle Hosts und Datenbanken Sie implementieren, auf dieselbe Weise ausgeführt.

Bearbeiten Sie die Datei Host_Name.yml unter Host_vars

Jeder Oracle Host verfügt über seine Host-Variablendatei, die durch den Hostnamen identifiziert wird, der Host-spezifische Variablen enthält. Sie können einen beliebigen Namen für Ihren Host angeben. Bearbeiten und kopieren Sie die host_vars Fügen Sie sie im Abschnitt Host VARS Config in Ihre gewünschte ein host_name.yml Datei:



Die blauen Elemente müssen an Ihre Umgebung angepasst werden.

Host VARS-Konfiguration

```
#####
##### Host Variables Configuration #####
#####

# Add your Oracle Host
ansible_host: "10.61.180.15"

# Oracle db log archive mode: true - ARCHIVELOG or false - NOARCHIVELOG
log_archive_mode: "true"

# Number of pluggable databases per container instance identified by sid.
Pdb_name specifies the prefix for container database naming in this case
cdb2_pdb1, cdb2_pdb2, cdb2_pdb3
oracle_sid: "cdb2"
pdb_num: "3"
pdb_name: "{{ oracle_sid }}_pdb"

# CDB listener port, use different listener port for additional CDB on
same host
listener_port: "1523"

# CDB is created with SGA at 75% of memory_limit, MB. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB. The grand total SGA should not exceed 75% available RAM on node.
memory_limit: "5464"

# Set "em_configuration: DBEXPRESS" to install enterprise manager express
and choose a unique port from 5500 to 5599 for each sid on the host.
# Leave them black if em express is not installed.
em_configuration: "DBEXPRESS"
em_express_port: "5501"

# {{groups.oracle[0]}} represents first Oracle DB server as defined in
Oracle hosts group [oracle]. For concurrent multiple Oracle DB servers
deployment, [0] will be incremented for each additional DB server. For
example, {{groups.oracle[1]}}" represents DB server 2,
"{{groups.oracle[2]}}" represents DB server 3 ... As a good practice and
the default, minimum three volumes is allocated to a DB server with
corresponding /u01, /u02, /u03 mount points, which store oracle binary,
oracle data, and oracle recovery files respectively. Additional volumes
can be added by click on "More NFS volumes" but the number of volumes
allocated to a DB server must match with what is defined in global vars
```

file by volumes_nfs parameter, which dictates how many volumes are to be created for each DB server.

```
host_datastores_nfs:
  - {vol_name: "{{groups.oracle[0]}}_u01", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
  - {vol_name: "{{groups.oracle[0]}}_u02", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
  - {vol_name: "{{groups.oracle[0]}}_u03", aggr_name: "aggr01_node01",
    lif: "172.21.94.200", size: "25"}
```

Bearbeiten Sie die Datei Vars.yml

Der vars.yml Die Datei konsolidiert alle umgebungsspezifischen Variablen (ONTAP, Linux oder Oracle) für die Implementierung von Oracle.

1. Bearbeiten und kopieren Sie die Variablen aus dem Abschnitt VARS und fügen Sie diese Variablen in Ihr ein vars.yml Datei:

```
#####
##### Oracle 19c deployment global user configuration variables #####
##### Consolidate all variables from ontap, linux and oracle #####
#####

#####
### Ontap env specific config variables ###
#####

#Inventory group name
#Default inventory group name - 'ontap'
#Change only if you are changing the group name either in inventory/hosts
file or in inventory groups in case of AWX/Tower
hosts_group: "ontap"

#CA_signed_certificates (ONLY CHANGE to 'true' IF YOU ARE USING CA SIGNED
CERTIFICATES)
ca_signed_certs: "false"

#Names of the Nodes in the ONTAP Cluster
nodes:
  - "AFF-01"
  - "AFF-02"

#Storage VLANs
#Add additional rows for vlans as necessary
storage_vlans:
  - {vlan_id: "203", name: "infra_NFS", protocol: "NFS"}
```

More Storage VLANsEnter Storage VLANs details

```
#Details of the Data Aggregates that need to be created
#If Aggregate creation takes longer, subsequent tasks of creating volumes
may fail.
#There should be enough disks already zeroed in the cluster, otherwise
aggregate create will zero the disks and will take long time
data_aggregates:
  - {aggr_name: "aggr01_node01"}
  - {aggr_name: "aggr01_node02"}

#SVM name
svm_name: "ora_svm"

# SVM Management LIF Details
svm_mgmt_details:
  - {address: "172.21.91.100", netmask: "255.255.255.0", home_port: "e0M"}

# NFS storage parameters when data_protocol set to NFS. Volume named after
Oracle hosts name identified by mount point as follow for oracle DB server
1. Each mount point dedicates to a particular Oracle files: u01 - Oracle
binary, u02 - Oracle data, u03 - Oracle redo. Add additional volumes by
click on "More NFS volumes" and also add the volumes list to corresponding
host_vars as host_datastores_nfs variable. For multiple DB server
deployment, additional volumes sets needs to be added for additional DB
server. Input variable "{{groups.oracle[1]}}_u01",
 "{{groups.oracle[1]}}_u02", and "{{groups.oracle[1]}}_u03" as vol_name for
second DB server. Place volumes for multiple DB servers alternately
between controllers for balanced IO performance, e.g. DB server 1 on
controller node1, DB server 2 on controller node2 etc. Make sure match lif
address with controller node.

volumes_nfs:
  - {vol_name: "{{groups.oracle[0]}}_u01", aggr_name: "aggr01_node01",
lif: "172.21.94.200", size: "25"}
  - {vol_name: "{{groups.oracle[0]}}_u02", aggr_name: "aggr01_node01",
lif: "172.21.94.200", size: "25"}
  - {vol_name: "{{groups.oracle[0]}}_u03", aggr_name: "aggr01_node01",
lif: "172.21.94.200", size: "25"}

#NFS LIFs IP address and netmask

nfs_lifs_details:
  - address: "172.21.94.200" #for node-1
    netmask: "255.255.255.0"
  - address: "172.21.94.201" #for node-2
```

```

netmask: "255.255.255.0"

#NFS client match

client_match: "172.21.94.0/24"

#####
### Linux env specific config variables ###
#####

#NFS Mount points for Oracle DB volumes

mount_points:
  - "/u01"
  - "/u02"
  - "/u03"

# Up to 75% of node memory size divided by 2mb. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB.
# Leave it blank if hugepage is not configured on the host.

hugepages_nr: "1234"

# RedHat subscription username and password

redhat_sub_username: "xxx"
redhat_sub_password: "xxx"

#####
### DB env specific install and config variables ###
#####

db_domain: "your.domain.com"

# Set initial password for all required Oracle passwords. Change them
after installation.

initial_pwd_all: "netapp123"

```

Führen Sie das Playbook aus

Nach Abschluss der erforderlichen Umgebungsvoraussetzungen und Kopieren der Variablen in `vars.yml` und `your_host.yml`, Sie sind jetzt bereit, die Playbooks zu implementieren.



<username> muss an Ihre Umgebung angepasst werden.

1. Führen Sie das ONTAP Playbook durch, indem Sie die richtigen Tags und den richtigen ONTAP Cluster-Benutzernamen eingeben. Geben Sie das Passwort für den ONTAP Cluster ein, und vsadmin, wenn Sie dazu aufgefordert werden.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t
ontap_config -e @vars/vars.yml
```

2. Führen Sie das Linux-Playbook aus, um den Linux-Teil der Bereitstellung auszuführen. Eingabe für admin ssh Passwort sowie sudo Passwort.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t
linux_config -e @vars/vars.yml
```

3. Führen Sie das Oracle Playbook aus, um den Oracle Teil der Implementierung auszuführen. Eingabe für admin ssh Passwort sowie sudo Passwort.

```
ansible-playbook -i hosts all_playbook.yml -u username -k -K -t
oracle_config -e @vars/vars.yml
```

Implementieren Sie zusätzliche Datenbanken auf demselben Oracle Host

Der Oracle Teil des Playbook erstellt pro Ausführung eine einzelne Oracle-Container-Datenbank auf einem Oracle-Server. Gehen Sie wie folgt vor, um eine zusätzliche Container-Datenbank auf demselben Server zu erstellen:

1. Ändern der Variablen `Host_Vars`.
 - a. Gehen Sie zurück zu Schritt 3 - Bearbeiten Sie den `host_name.yml` Datei unter `host_vars`.
 - b. Ändern Sie Oracle SID zu einer anderen Namenskonvention.
 - c. Ändern Sie den Listener-Port in eine andere Zahl.
 - d. Ändern Sie den EM Express-Port in eine andere Nummer, wenn Sie EM Express installiert haben.
 - e. Kopieren Sie die überarbeiteten Hostvariablen in die Oracle-Host-Variablendatei unter `host_vars`.
2. Führen Sie das Playbook mit dem aus `oracle_config` Tag wie oben in dargestellt [Führen Sie das Playbook aus](#).

Oracle-Installation validieren

1. Melden Sie sich beim Oracle-Server als Oracle-Benutzer an und führen Sie die folgenden Befehle aus:

```
ps -ef | grep ora
```



Auf diese Weise werden die oracle-Prozesse aufgeführt, wenn die Installation wie erwartet abgeschlossen wurde und die oracle DB gestartet wurde

2. Melden Sie sich bei der Datenbank an, um die db-Konfigurationseinstellungen und die PDBs zu überprüfen, die mit den folgenden Befehlsätzen erstellt wurden.

```
[oracle@localhost ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 12:52:51 2021
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL>

SQL> select name, log_mode from v$database;
NAME          LOG_MODE
-----
CDB2          ARCHIVELOG

SQL> show pdbs

          CON_ID CON_NAME                                OPEN MODE  RESTRICTED
-----
          2 PDB$SEED                                READ ONLY  NO
          3 CDB2_PDB1                              READ WRITE NO
          4 CDB2_PDB2                              READ WRITE NO
          5 CDB2_PDB3                              READ WRITE NO

col svrname form a30
col dirname form a30
select svrname, dirname, nfsversion from v$dnfs_servers;

SQL> col svrname form a30
SQL> col dirname form a30
SQL> select svrname, dirname, nfsversion from v$dnfs_servers;

SVRNAME                                DIRNAME                                NFSVERSION
-----
172.21.126.200                          /rhelora03_u02                          NFSv3.0
172.21.126.200                          /rhelora03_u03                          NFSv3.0
172.21.126.200                          /rhelora03_u01                          NFSv3.0
```

Dies bestätigt, dass dNFS richtig funktioniert.

3. Stellen Sie über Listener eine Verbindung zur Datenbank her, um die Konfiguration des Oracle Listener mit dem folgenden Befehl zu überprüfen. Wechseln Sie zum entsprechenden Listener-Port und Datenbankdienstnamen.

```
[oracle@localhost ~]$ sqlplus
system@//localhost:1523/cdb2_pdb1.cie.netapp.com

SQL*Plus: Release 19.0.0.0.0 - Production on Thu May 6 13:19:57 2021
Version 19.8.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Enter password:
Last Successful login time: Wed May 05 2021 17:11:11 -04:00

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL> show user
USER is "SYSTEM"
SQL> show con_name
CON_NAME
CDB2_PDB1
```

Dies bestätigt, dass Oracle Listener ordnungsgemäß funktioniert.

Wo Hilfe benötigt wird?

Wenn Sie Hilfe mit dem Toolkit benötigen, nehmen Sie bitte an der Teil ["NetApp Solution Automation Community Support Slack Channel"](#) Und suchen Sie den Kanal zur Lösungsautomatisierung, um Ihre Fragen zu stellen oder zu fragen.

Lösungsüberblick

Automatisierte Datensicherung für Oracle Datenbanken

Unternehmen automatisieren ihre Umgebungen, um die Effizienz zu steigern, Implementierungen zu beschleunigen und manuelle Aufgaben zu reduzieren. Konfigurationsmanagement-Tools wie Ansible werden zur Optimierung der Abläufe in Unternehmensdatenbanken eingesetzt. Diese Lösung zeigt, wie Sie mit Ansible die Datensicherung von Oracle mit NetApp ONTAP automatisieren können. Storage-Administratoren, Systemadministratoren und DBAs können die Datenreplizierung konsistent und schnell auf ein externes Datacenter oder in die Public Cloud einrichten. Sie profitieren von folgenden Vorteilen:

- Vermeiden Sie Designkomplexität und menschliche Fehler und implementieren Sie eine wiederholbare, konsistente Implementierung und Best Practices
- Verkürzung der Zeit für die Konfiguration von Intercluster-Replizierung, CVO Instanziation und Recovery von Oracle-Datenbanken

- Erhöhen Sie die Produktivität von Datenbank-Administratoren, -Systemen und -Storage-Administratoren
- Bietet Datenbank-Recovery-Workflow zum einfachen Testen eines DR-Szenarios.

NetApp bietet Kunden validierte Ansible-Module und -Rollen, um die Implementierung, Konfiguration und das Lifecycle-Management Ihrer Oracle-Datenbankumgebung zu beschleunigen. Diese Lösung bietet Anweisungen und Ansible-Playbook-Code, um Sie bei folgenden Aufgaben zu unterstützen:

Replizierung vor Ort und in On-Premises-Umgebungen

- Erstellen von Intercluster-Libs an Quelle und Ziel
- Cluster- und vServer-Peering einrichten
- SnapMirror von Oracle Volumes erstellen und initialisieren
- Erstellen Sie einen Replikationszeitplan über AWX/Tower für Oracle-Binärdateien, -Datenbanken und -Protokolle
- Stellen Sie Oracle DB auf dem Ziel wieder her und bringen Sie die Datenbank in den Online-Modus

Von On-Premises zu CVO in AWS

- AWS Connector erstellen
- CVO-Instanz in AWS erstellen
- Hinzufügen eines On-Premises-Clusters zu Cloud Manager
- Erstellen von Intercluster-Libs auf der Quelle
- Cluster- und vServer-Peering einrichten
- SnapMirror von Oracle Volumes erstellen und initialisieren
- Erstellen Sie einen Replikationszeitplan über AWX/Tower für Oracle-Binärdateien, -Datenbanken und -Protokolle
- Stellen Sie Oracle DB auf dem Ziel wieder her und bringen Sie die Datenbank in den Online-Modus

Klicken Sie anschließend auf "[Hier sind erste Schritte mit der Lösung](#)".

Erste Schritte

Diese Lösung wurde für den Betrieb in einer AWX/Tower-Umgebung entwickelt.

AWX/Tower

Für AWX-/Tower-Umgebungen werden Sie geleitet durch das Erstellen einer Bestandsaufnahme für das ONTAP Cluster-Management und den Oracle Server (IPs und Hostnamen), das Erstellen von Anmeldeinformationen, das Konfigurieren eines Projekts, das den Ansible-Code aus NetApp Automation Github zieht, und durch die Jobvorlage, die die Automatisierung startet.

1. Die Lösung wurde für die Ausführung in einem Private-Cloud-Szenario (vor Ort und lokal) und in einer Hybrid Cloud (On-Premises zu Public-Cloud-Cloud Volumes ONTAP [CVO]) entwickelt.
2. Füllen Sie die Variablen aus, die für Ihre Umgebung spezifisch sind, und kopieren Sie sie in die Felder Extra Vars in Ihrer Job-Vorlage.
3. Nachdem die zusätzlichen Vars zu Ihrer Job-Vorlage hinzugefügt wurden, können Sie die Automatisierung starten.

4. Die Automatisierung umfasst drei Phasen (Setup, Replizierungsplan für Oracle Binaries, Database, Logs und Replication Schedule nur für Logs) und einen vierten Schritt zur Wiederherstellung der Datenbank an einem DR-Standort.
5. Detaillierte Anweisungen zum Abrufen der für den CVO-Datenschutz erforderlichen Schlüssel und Token finden Sie unter "[Sammeln von Voraussetzungen für CVO- und Connector-Implementierungen](#)"

Anforderungen

<starke Klasse=„groß“>On-Prem <stark>

Umgebung	Anforderungen
Ansible-Umgebung	AWX/Tower
	Ansible v.2.10 und höher
	Python 3
	Python Libraries - netapp-lib - xmltodict - jmespath
ONTAP	ONTAP Version 9.8 +
	Zwei Datenaggregate
	NFS vlan und iffrp wurden erstellt
Oracle Server	RHEL 7/8
	Oracle Linux 7/8
	Netzwerkschnittstellen für das NFS-, öffentlichen und optionalen Management
	Vorhandene Oracle Umgebung auf Quelle und das entsprechende Linux Betriebssystem am Zielort (DR-Standort oder Public Cloud)

<Strong class=„big“>CVO

Umgebung	Anforderungen
Ansible-Umgebung	AWX/Tower
	Ansible v.2.10 und höher
	Python 3
	Python Libraries - netapp-lib - xmltodict - jmespath
ONTAP	ONTAP Version 9.8 +
	Zwei Datenaggregate
	NFS vlan und iffrp wurden erstellt
Oracle Server	RHEL 7/8
	Oracle Linux 7/8
	Netzwerkschnittstellen für das NFS-, öffentlichen und optionalen Management
	Vorhandene Oracle Umgebung auf Quelle und das entsprechende Linux Betriebssystem am Zielort (DR-Standort oder Public Cloud)
	Legen Sie auf der Oracle EC2-Instanz angemessenen Swap-Speicherplatz fest. Standardmäßig sind einige EC2-Instanzen mit 0-Swap bereitgestellt
Cloud Manager/AWS	AWS Zugriff/geheimer Schlüssel
	NetApp Cloud Manager Konto
	NetApp Cloud Manager – Token für die Aktualisierung

<starke Klasse=„groß“>On-Prem <stark>

Diese automatisierte Implementierung basiert auf einem einzigen Ansible-Playbook, das aus drei separaten Rollen besteht. Rollen sind Konfigurationen von ONTAP, Linux und Oracle. In der folgenden Tabelle werden die automatisierten Aufgaben beschrieben.

Playbook	Aufgaben
ontap_Setup	Vorabprüfung der ONTAP-Umgebung
	Erstellung von Intercluster LIFs am Quell-Cluster (OPTIONAL)
	Erstellung von Intercluster LIFs am Ziel-Cluster (OPTIONAL)
	Erstellung von Cluster- und SVM-Peering
	Erstellung des Ziel-SnapMirror und Initialisierung designierter Oracle Volumes
Ora_Replication_cg	Aktivieren Sie den Backup-Modus für jede Datenbank in /etc/oratab
	Snapshot von Oracle Binary und Datenbank-Volumes erstellt
	Snapmirror Aktualisiert
	Deaktivieren Sie den Backup-Modus für jede Datenbank in /etc/oratab
Ora_Replication_log	Schalten Sie das aktuelle Protokoll für jede Datenbank in /etc/oratab um
	Snapshot vom Oracle Log Volume erstellt
	Snapmirror Aktualisiert
Ora_Erholung	SnapMirror unterbrechen
	Aktivieren Sie NFS und erstellen Sie Verbindungspfad für Oracle Volumes auf dem Ziel
	Konfigurieren Sie den Oracle-Host für DR
	Mounten und überprüfen Sie Oracle Volumes
	Stellen Sie die Oracle Datenbank wieder her und starten Sie sie

<Strong class=„big“>CVO

Diese automatisierte Implementierung basiert auf einem einzigen Ansible-Playbook, das aus drei separaten Rollen besteht. Rollen sind Konfigurationen von ONTAP, Linux und Oracle. In der folgenden Tabelle werden die automatisierten Aufgaben beschrieben.

Playbook	Aufgaben
cvo_Setup	Vorabprüfung der Umgebung
	AWS konfigurieren/AWS Zugriffsschlüssel-ID/geheimer Schlüssel/Standardregion
	Erstellung der AWS Rolle
	Erstellung der NetApp Cloud Manager Connector-Instanz in AWS
	Erstellung der Cloud Volumes ONTAP-Instanz (CVO) in AWS
	Fügen Sie ein On-Premises-Quell-ONTAP-Cluster zu NetApp Cloud Manager hinzu
	Erstellung des Ziel-SnapMirror und Initialisierung designierter Oracle Volumes
Ora_Replication_cg	Aktivieren Sie den Backup-Modus für jede Datenbank in /etc/oratab
	Snapshot von Oracle Binary und Datenbank-Volumes erstellt
	Snapmirror Aktualisiert
	Deaktivieren Sie den Backup-Modus für jede Datenbank in /etc/oratab
Ora_Replication_log	Schalten Sie das aktuelle Protokoll für jede Datenbank in /etc/oratab um
	Snapshot vom Oracle Log Volume erstellt
	Snapmirror Aktualisiert
Ora_Erholung	SnapMirror unterbrechen
	Aktivieren Sie NFS und erstellen Sie den Verbindungspfad für Oracle Volumes auf dem Ziel-CVO
	Konfigurieren Sie den Oracle-Host für DR
	Mounten und überprüfen Sie Oracle Volumes
	Stellen Sie die Oracle Datenbank wieder her und starten Sie sie

Standardparameter

Um die Automatisierung zu vereinfachen, haben wir viele erforderliche Oracle Parameter mit Standardwerten voreingestellt. In der Regel ist es nicht erforderlich, die Standardparameter für die meisten Implementierungen zu ändern. Ein fortgeschrittener Benutzer kann mit Vorsicht Änderungen an den Standardparametern vornehmen. Die Standardparameter befinden sich in jedem Rollenordner unter dem Standardverzeichnis.

Lizenz

Sie sollten die Lizenzinformationen wie im Github-Repository angegeben lesen. Durch Zugriff, Herunterladen, Installation oder Nutzung des Inhalts in diesem Repository stimmen Sie den Bedingungen der Lizenz zu "[Hier](#)".

Beachten Sie, dass es bestimmte Beschränkungen bezüglich der Erstellung und/oder Freigabe abgeleiteter Werke mit dem Inhalt in diesem Repository gibt. Bitte lesen Sie die Bedingungen des "[Lizenz](#)" Vor der Verwendung des Inhalts. Wenn Sie nicht mit allen Bedingungen einverstanden sind, dürfen Sie den Inhalt in diesem Repository nicht aufrufen, herunterladen oder verwenden.

Klicken Sie anschließend auf "[Hier finden Sie ausführliche AWX/Tower-Verfahren](#)".

Schritt-für-Schritt-Anweisungen zur Implementierung

AWX/Tower Oracle Data Protection

Erstellen Sie Inventar, Gruppe, Hosts und Anmeldedaten für Ihre Umgebung

In diesem Abschnitt wird die Einrichtung von Inventar, Gruppen, Hosts und Zugangsdaten im AWX/Ansible Tower beschrieben, die die Umgebung für den Einsatz automatisierter NetApp Lösungen vorbereiten.

1. Konfigurieren Sie den Bestand.
 - a. Navigieren Sie zu Ressourcen → Inventar → Hinzufügen, und klicken Sie auf Inventar hinzufügen.
 - b. Geben Sie den Namen und die Organisationsdetails ein, und klicken Sie auf Speichern.
 - c. Klicken Sie auf der Seite Inventar auf den erstellten Bestand.
 - d. Navigieren Sie zum Untermenü Gruppen, und klicken Sie auf Hinzufügen.
 - e. Geben Sie den Namen oracle für Ihre erste Gruppe ein, und klicken Sie auf Speichern.
 - f. Wiederholen Sie den Vorgang für eine zweite Gruppe namens dr_oracle.
 - g. Wählen Sie die erstellte oracle-Gruppe aus, gehen Sie zum Untermenü Hosts und klicken Sie auf Neuen Host hinzufügen.
 - h. Geben Sie die IP-Adresse der Management-IP des Oracle Quell-Hosts an, und klicken Sie auf Speichern.
 - i. Dieser Prozess muss für die dr_oracle-Gruppe wiederholt werden und die Management-IP/den Host für DR/Ziel Oracle-Host hinzufügen.



Im Folgenden werden die Typen und Anmeldedaten für Zugangsdaten, entweder für On-Premises mit ONTAP oder CVO in AWS, erstellt.

Lokal

1. Konfigurieren Sie die Anmeldedaten.
2. Credential-Typen Erstellen. Bei Lösungen, die ONTAP verwenden, müssen Sie den Anmeldeinformationstyp so konfigurieren, dass er mit den Einträgen für Benutzernamen und Kennwort übereinstimmt.
 - a. Navigieren Sie zu Administration → Credential Types, und klicken Sie auf Add.
 - b. Geben Sie den Namen und eine Beschreibung an.
 - c. Fügen Sie den folgenden Inhalt in die Eingabekonfiguration ein:

```
fields:
  - id: dst_cluster_username
    type: string
    label: Destination Cluster Username
  - id: dst_cluster_password
    type: string
    label: Destination Cluster Password
    secret: true
  - id: src_cluster_username
    type: string
    label: Source Cluster Username
  - id: src_cluster_password
    type: string
    label: Source Cluster Password
    secret: true
```

- d. Fügen Sie den folgenden Inhalt in die Konfiguration des Injektors ein, und klicken Sie dann auf Speichern:

```
extra_vars:
  dst_cluster_username: '{{ dst_cluster_username }}'
  dst_cluster_password: '{{ dst_cluster_password }}'
  src_cluster_username: '{{ src_cluster_username }}'
  src_cluster_password: '{{ src_cluster_password }}'
```

3. Credential für ONTAP erstellen
 - a. Navigieren Sie zu Resources → Credentials, und klicken Sie auf Add.
 - b. Geben Sie den Namen und die Organisationsdetails für die ONTAP Credentials ein
 - c. Wählen Sie den im vorherigen Schritt erstellten Anmeldeinformationstyp aus.
 - d. Geben Sie unter „Typdetails“ den Benutzernamen und das Kennwort für Ihre Quell- und Zielcluster ein.
 - e. Klicken Sie Auf Speichern
4. Credential für Oracle erstellen

- a. Navigieren Sie zu Resources → Credentials, und klicken Sie auf Add.
- b. Geben Sie den Namen und die Organisationsdetails für Oracle ein
- c. Wählen Sie den Typ der Geräteanmeldeinformationen aus.
- d. Geben Sie unter „Typdetails“ den Benutzernamen und das Kennwort für die Oracle-Hosts ein.
- e. Wählen Sie die richtige Privilege-Eskalationsmethode aus, und geben Sie Benutzernamen und Kennwort ein.
- f. Klicken Sie Auf Speichern
- g. Wiederholen Sie den Vorgang, falls dies für eine andere Anmeldedaten für den dr_oracle-Host erforderlich ist.

CVO

1. Konfigurieren Sie die Anmeldedaten.
2. Erstellen von Anmeldungstypen. Bei Lösungen, die ONTAP nutzen, müssen Sie den Anmeldeinformationstyp so konfigurieren, dass er mit den Einträgen für Benutzername und Passwort übereinstimmt, werden auch Einträge für Cloud Central und AWS hinzugefügt.
 - a. Navigieren Sie zu Administration → Credential Types, und klicken Sie auf Add.
 - b. Geben Sie den Namen und eine Beschreibung an.
 - c. Fügen Sie den folgenden Inhalt in die Eingabekonfiguration ein:

```
fields:
  - id: dst_cluster_username
    type: string
    label: CVO Username
  - id: dst_cluster_password
    type: string
    label: CVO Password
    secret: true
  - id: cvo_svm_password
    type: string
    label: CVO SVM Password
    secret: true
  - id: src_cluster_username
    type: string
    label: Source Cluster Username
  - id: src_cluster_password
    type: string
    label: Source Cluster Password
    secret: true
  - id: regular_id
    type: string
    label: Cloud Central ID
    secret: true
  - id: email_id
    type: string
    label: Cloud Manager Email
    secret: true
  - id: cm_password
    type: string
    label: Cloud Manager Password
    secret: true
  - id: access_key
    type: string
    label: AWS Access Key
    secret: true
  - id: secret_key
    type: string
    label: AWS Secret Key
    secret: true
  - id: token
    type: string
    label: Cloud Central Refresh Token
    secret: true
```

d. Fügen Sie den folgenden Inhalt in die Konfiguration des Injektors ein, und klicken Sie auf

Speichern:

```
extra_vars:
  dst_cluster_username: '{{ dst_cluster_username }}'
  dst_cluster_password: '{{ dst_cluster_password }}'
  cvo_svm_password: '{{ cvo_svm_password }}'
  src_cluster_username: '{{ src_cluster_username }}'
  src_cluster_password: '{{ src_cluster_password }}'
  regular_id: '{{ regular_id }}'
  email_id: '{{ email_id }}'
  cm_password: '{{ cm_password }}'
  access_key: '{{ access_key }}'
  secret_key: '{{ secret_key }}'
  token: '{{ token }}'
```

3. Credential für ONTAP/CVO/AWS erstellen

- a. Navigieren Sie zu Resources → Credentials, und klicken Sie auf Add.
- b. Geben Sie den Namen und die Organisationsdetails für die ONTAP Credentials ein
- c. Wählen Sie den im vorherigen Schritt erstellten Anmeldeinformationstyp aus.
- d. Geben Sie unter „Type Details“ den Benutzernamen und das Kennwort für Ihre Quell- und CVO-Cluster, Cloud Central/Manager, AWS Access/Secret Key und Cloud Central Refresh Token ein.
- e. Klicken Sie Auf Speichern

4. Credential für Oracle (Quelle) erstellen

- a. Navigieren Sie zu Resources → Credentials, und klicken Sie auf Add.
- b. Geben Sie den Namen und die Organisationsdetails für Oracle Host ein
- c. Wählen Sie den Typ der Geräteanmeldeinformationen aus.
- d. Geben Sie unter „Typdetails“ den Benutzernamen und das Kennwort für die Oracle-Hosts ein.
- e. Wählen Sie die richtige Privilege-Eskalationsmethode aus, und geben Sie Benutzernamen und Kennwort ein.
- f. Klicken Sie Auf Speichern

5. Credential für Oracle Destination erstellen

- a. Navigieren Sie zu Resources → Credentials, und klicken Sie auf Add.
- b. Geben Sie den Namen und die Organisationsdetails für den DR Oracle-Host ein
- c. Wählen Sie den Typ der Geräteanmeldeinformationen aus.
- d. Geben Sie unter „Typdetails“ den Benutzernamen (ec2-user oder wenn Sie ihn von der Standardeinstellung geändert haben, geben Sie diesen ein) und den SSH Private Key ein
- e. Wählen Sie die richtige Methode zur Eskalation von Berechtigungen (sudo) aus, und geben Sie bei Bedarf den Benutzernamen und das Kennwort ein.
- f. Klicken Sie Auf Speichern

Erstellen Sie ein Projekt

1. Gehen Sie zu Ressourcen → Projekte, und klicken Sie auf Hinzufügen.
 - a. Geben Sie den Namen und die Organisationsdetails ein.
 - b. Wählen Sie im Feld Quellenkontrolle Credential Type die Option Git aus.
 - c. Eingabe <https://github.com/NetApp-Automation/na_oracle19c_data_protection.git> Als URL für die Quellensteuerung.
 - d. Klicken Sie auf Speichern .
 - e. Das Projekt muss gelegentlich synchronisiert werden, wenn sich der Quellcode ändert.

Globale Variablen konfigurieren

Die in diesem Abschnitt definierten Variablen gelten für alle Oracle Hosts, Datenbanken und den ONTAP Cluster.

1. Geben Sie Ihre umgebungsspezifischen Parameter in das folgende eingebettete globale Variablen oder Vars-Formular ein.



Die blauen Elemente müssen an Ihre Umgebung angepasst werden.

Lokal

```
# Oracle Data Protection global user configuration variables
# Ontap env specific config variables
hosts_group: "ontap"
ca_signed_certs: "false"

# Inter-cluster LIF details
src_nodes:
  - "AFF-01"
  - "AFF-02"

dst_nodes:
  - "DR-AFF-01"
  - "DR-AFF-02"

create_source_intercluster_lifs: "yes"

source_intercluster_network_port_details:
  using_dedicated_ports: "yes"
  using_ifgrp: "yes"
  using_vlans: "yes"
  failover_for_shared_individual_ports: "yes"
  ifgrp_name: "a0a"
  vlan_id: "10"
  ports:
    - "e0b"
    - "e0g"
  broadcast_domain: "NFS"
  ipspace: "Default"
  failover_group_name: "iclifs"

source_intercluster_lif_details:
  - name: "icl_1"
    address: "10.0.0.1"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "AFF-01"
  - name: "icl_2"
    address: "10.0.0.2"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "AFF-02"

create_destination_intercluster_lifs: "yes"
```



```

destination_intercluster_network_port_details:
  using_dedicated_ports: "yes"
  using_ifgrp: "yes"
  using_vlans: "yes"
  failover_for_shared_individual_ports: "yes"
  ifgrp_name: "a0a"
  vlan_id: "10"
  ports:
    - "e0b"
    - "e0g"
  broadcast_domain: "NFS"
  ipspace: "Default"
  failover_group_name: "iclifs"

destination_intercluster_lif_details:
  - name: "icl_1"
    address: "10.0.0.3"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "DR-AFF-01"
  - name: "icl_2"
    address: "10.0.0.4"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "DR-AFF-02"

# Variables for SnapMirror Peering
passphrase: "your-passphrase"

# Source & Destination List
dst_cluster_name: "dst-cluster-name"
dst_cluster_ip: "dst-cluster-ip"
dst_vserver: "dst-vserver"
dst_nfs_lif: "dst-nfs-lif"
src_cluster_name: "src-cluster-name"
src_cluster_ip: "src-cluster-ip"
src_vserver: "src-vserver"

# Variable for Oracle Volumes and SnapMirror Details
cg_snapshot_name_prefix: "oracle"
src_orabinary_vols:
  - "binary_vol"
src_db_vols:
  - "db_vol"
src_archivelog_vols:
  - "log_vol"

```

```

snapmirror_policy: "async_policy_oracle"

# Export Policy Details
export_policy_details:
  name: "nfs_export_policy"
  client_match: "0.0.0.0/0"
  ro_rule: "sys"
  rw_rule: "sys"

# Linux env specific config variables
mount_points:
  - "/u01"
  - "/u02"
  - "/u03"
hugepages_nr: "1234"
redhat_sub_username: "xxx"
redhat_sub_password: "xxx"

# DB env specific install and config variables
recovery_type: "scn"
control_files:
  - "/u02/oradata/CDB2/control01.ctl"
  - "/u03/orareco/CDB2/control02.ctl"

```

CVO

```

#####
### Ontap env specific config variables ###
#####

#Inventory group name
#Default inventory group name - "ontap"
#Change only if you are changing the group name either in
inventory/hosts file or in inventory groups in case of AWX/Tower
hosts_group: "ontap"

#CA_signed_certificates (ONLY CHANGE to "true" IF YOU ARE USING CA
SIGNED CERTIFICATES)
ca_signed_certs: "false"

#Names of the Nodes in the Source ONTAP Cluster
src_nodes:
  - "AFF-01"
  - "AFF-02"

#Names of the Nodes in the Destination CVO Cluster

```

```

dst_nodes:
  - "DR-AFF-01"
  - "DR-AFF-02"

#Define whether or not to create intercluster lifs on source cluster
(ONLY CHANGE to "No" IF YOU HAVE ALREADY CREATED THE INTERCLUSTER LIFS)
create_source_intercluster_lifs: "yes"

source_intercluster_network_port_details:
  using_dedicated_ports: "yes"
  using_ifgrp: "yes"
  using_vlans: "yes"
  failover_for_shared_individual_ports: "yes"
  ifgrp_name: "a0a"
  vlan_id: "10"
  ports:
    - "e0b"
    - "e0g"
  broadcast_domain: "NFS"
  ipspace: "Default"
  failover_group_name: "iclifs"

source_intercluster_lif_details:
  - name: "icl_1"
    address: "10.0.0.1"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "AFF-01"
  - name: "icl_2"
    address: "10.0.0.2"
    netmask: "255.255.255.0"
    home_port: "a0a-10"
    node: "AFF-02"

#####
### CVO Deployment Variables ###
#####

##### Access Keys Variables #####

# Region where your CVO will be deployed.
region_deploy: "us-east-1"

##### CVO and Connector Vars #####

# AWS Managed Policy required to give permission for IAM role creation.

```

```

aws_policy: "arn:aws:iam::1234567:policy/OCCM"

# Specify your aws role name, a new role is created if one already does
not exist.
aws_role_name: "arn:aws:iam::1234567:policy/OCCM"

# Name your connector.
connector_name: "awx_connector"

# Name of the key pair generated in AWS.
key_pair: "key_pair"

# Name of the Subnet that has the range of IP addresses in your VPC.
subnet: "subnet-12345"

# ID of your AWS security group that allows access to on-prem
resources.
security_group: "sg-123123123"

# Your Cloud Manager Account ID.
account: "account-A23123A"

# Name of the your CVO instance
cvo_name: "test_cvo"

# ID of the VPC in AWS.
vpc: "vpc-123123123"

#####
#####
# Variables for - Add on-prem ONTAP to Connector in Cloud Manager
#####
#####

# For Federated users, Client ID from API Authentication Section of
Cloud Central to generate access token.
sso_id: "123123123123123123123"

# For regular access with username and password, please specify "pass"
as the connector_access. For SSO users, use "refresh_token" as the
variable.
connector_access: "pass"

#####
#####
# Variables for SnapMirror Peering
#####

```

```

#####
passphrase: "your-passphrase"

#####
#####
# Source & Destination List
#####
#####
#Please Enter Destination Cluster Name
dst_cluster_name: "dst-cluster-name"

#Please Enter Destination Cluster (Once CVO is Created Add this
Variable to all templates)
dst_cluster_ip: "dst-cluster-ip"

#Please Enter Destination SVM to create mirror relationship
dst_vserver: "dst-vserver"

#Please Enter NFS Lif for dst vserver (Once CVO is Created Add this
Variable to all templates)
dst_nfs_lif: "dst-nfs-lif"

#Please Enter Source Cluster Name
src_cluster_name: "src-cluster-name"

#Please Enter Source Cluster
src_cluster_ip: "src-cluster-ip"

#Please Enter Source SVM
src_vserver: "src-vserver"

#####
#####
# Variable for Oracle Volumes and SnapMirror Details
#####
#####
#Please Enter Source Snapshot Prefix Name
cg_snapshot_name_prefix: "oracle"

#Please Enter Source Oracle Binary Volume(s)
src_orabinary_vols:
- "binary_vol"
#Please Enter Source Database Volume(s)
src_db_vols:
- "db_vol"
#Please Enter Source Archive Volume(s)

```

```

src_archivelog_vols:
  - "log_vol"
#Please Enter Destination Snapmirror Policy
snapmirror_policy: "async_policy_oracle"

#####
#####
# Export Policy Details
#####
#####
#Enter the destination export policy details (Once CVO is Created Add
this Variable to all templates)
export_policy_details:
  name: "nfs_export_policy"
  client_match: "0.0.0.0/0"
  ro_rule: "sys"
  rw_rule: "sys"

#####
#####
### Linux env specific config variables ###
#####
#####

#NFS Mount points for Oracle DB volumes
mount_points:
  - "/u01"
  - "/u02"
  - "/u03"

# Up to 75% of node memory size divided by 2mb. Consider how many
databases to be hosted on the node and how much ram to be allocated to
each DB.
# Leave it blank if hugepage is not configured on the host.
hugepages_nr: "1234"

# RedHat subscription username and password
redhat_sub_username: "xxx"
redhat_sub_password: "xxx"

#####
### DB env specific install and config variables ###
#####
#Recovery Type (leave as scn)
recovery_type: "scn"

```

```
#Oracle Control Files
control_files:
  - "/u02/oradata/CDB2/control01.ctl"
  - "/u03/orareco/CDB2/control02.ctl"
```

Automation Playbooks

Es gibt vier separate Playbooks, die ausgeführt werden müssen.

1. Playbook zur Einrichtung Ihrer Umgebung, vor Ort oder CVO
2. Playbook für die Replizierung von Oracle Binaries und Datenbanken nach einem Zeitplan
3. Playbook für die Replizierung von Oracle Logs nach einem Zeitplan
4. Playbook für die Wiederherstellung Ihrer Datenbank auf einem Ziel-Host

ONTAP/CVO Einrichtung

ONTAP- und CVO-Einrichtung

Konfigurieren und starten Sie die Jobvorlage.

1. Erstellen Sie die Job-Vorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen → Hinzufügen, und klicken Sie auf Job Template hinzufügen.
 - b. Geben Sie den Namen „ONTAP/CVO Setup“ ein
 - c. Wählen Sie den Jobtyp aus; Ausführen konfiguriert das System anhand eines Playbooks.
 - d. Wählen Sie den entsprechenden Bestand, das Projekt, das Playbook und die Zugangsdaten für das Playbook aus.
 - e. Wählen Sie das Playbook „ontap_Setup.yml“ für eine On-Premises-Umgebung aus oder wählen Sie das playbook cvo_Setup.yml zur Replizierung in eine CVO Instanz aus.
 - f. Fügen Sie globale Variablen, die aus Schritt 4 kopiert wurden, in das Feld Vorlagenvariablen unter der Registerkarte YAML ein.
 - g. Klicken Sie auf Speichern .
2. Starten Sie die Jobvorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen.
 - b. Klicken Sie auf die gewünschte Vorlage und dann auf Starten.



Wir verwenden diese Vorlage und kopieren sie in andere Playbooks.

Replizierung für Binär- und Datenbank-Volumes

Zeitplanung für das Playbook „Binary and Database Replication“

Konfigurieren und starten Sie die Jobvorlage.

1. Kopieren Sie die zuvor erstellte Jobvorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen.
 - b. Suchen Sie die ONTAP/CVO Setup-Vorlage und klicken Sie rechts ganz auf Copy Template
 - c. Klicken Sie auf Vorlage bearbeiten in der kopierten Vorlage, und ändern Sie den Namen in Binary and Database Replication Playbook.
 - d. Behalten Sie für die Vorlage denselben Bestand, dasselbe Projekt und dieselben Anmeldeinformationen bei.
 - e. Wählen Sie das Playbook ora_Replication_cg.yml als ausführtes Playbook aus.
 - f. Die Variablen bleiben die gleichen, aber die CVO Cluster-IP muss in der Variablen dst_Cluster_ip festgelegt werden.
 - g. Klicken Sie auf Speichern .
2. Planen Sie die Jobvorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen.
 - b. Klicken Sie auf die Playbook-Vorlage „Binary and Database Replication“, und klicken Sie anschließend oben auf „Schedules“.

- c. Klicken Sie auf Hinzufügen, fügen Sie den Namenszeitplan für die Binärdatei und die Datenbankreplikation hinzu, wählen Sie das Startdatum/die Startzeit am Anfang der Stunde, wählen Sie die Zeitzone Lokale Zeitzone und die Häufigkeit aus. Ausführungshäufigkeit wird häufig aktualisiert, dass die SnapMirror Replizierung aktualisiert wird.



Für die Log-Volume-Replizierung wird ein separater Zeitplan erstellt, sodass der Zeitplan in einer häufigeren Kadenz repliziert werden kann.

Replizierung für Protokoll-Volumes

Planen des Log Replication Playbook

Konfigurieren und starten Sie die Jobvorlage.

1. Kopieren Sie die zuvor erstellte Jobvorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen.
 - b. Suchen Sie die ONTAP/CVO Setup-Vorlage und klicken Sie rechts ganz auf Copy Template
 - c. Klicken Sie auf Vorlage bearbeiten in der kopierten Vorlage, und ändern Sie den Namen in Log Replication Playbook.
 - d. Behalten Sie für die Vorlage denselben Bestand, dasselbe Projekt und dieselben Anmeldeinformationen bei.
 - e. Wählen Sie als auszuführenden Playbook die ora_Replication_logs.yml aus.
 - f. Die Variablen bleiben die gleichen, aber die CVO Cluster-IP muss in der Variablen dst_Cluster_ip festgelegt werden.
 - g. Klicken Sie auf Speichern .
2. Planen Sie die Jobvorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen.
 - b. Klicken Sie auf die Playbook-Vorlage für Protokollreplikation, und klicken Sie anschließend oben auf „Schedules“.
 - c. Klicken Sie auf Hinzufügen, fügen Sie den Namensplan für die Protokollreplizierung hinzu, wählen Sie das Startdatum/die Startzeit am Beginn der Stunde, wählen Sie die Zeitzone Lokal und die Häufigkeit der Ausführung aus. Ausführungshäufigkeit wird häufig aktualisiert, dass die SnapMirror Replizierung aktualisiert wird.



Es wird empfohlen, den Protokollplan so einzustellen, dass er jede Stunde aktualisiert wird, um sicherzustellen, dass die Wiederherstellung auf die letzte stündliche Aktualisierung erfolgt.

Wiederherstellen und Wiederherstellen von Datenbanken

Planen des Log Replication Playbook

Konfigurieren und starten Sie die Jobvorlage.

1. Kopieren Sie die zuvor erstellte Jobvorlage.
 - a. Navigieren Sie zu Ressourcen → Vorlagen.
 - b. Suchen Sie die ONTAP/CVO Setup-Vorlage und klicken Sie rechts ganz auf Copy Template

- c. Klicken Sie auf Vorlage bearbeiten auf der kopierten Vorlage, und ändern Sie den Namen in „Playbook wiederherstellen und wiederherstellen“.
- d. Behalten Sie für die Vorlage denselben Bestand, dasselbe Projekt und dieselben Anmeldeinformationen bei.
- e. Wählen Sie die ora_Recovery.yml als auszuführenden Playbook aus.
- f. Die Variablen bleiben die gleichen, aber die CVO Cluster-IP muss in der Variablen dst_Cluster_ip festgelegt werden.
- g. Klicken Sie auf Speichern .



Dieses Playbook wird erst ausgeführt, nachdem Sie bereit sind, Ihre Datenbank am Remote-Standort wiederherzustellen.

Oracle Database Wird Wiederhergestellt

1. Daten-Volumes für Oracle-Produktionsdatenbanken vor Ort werden über NetApp SnapMirror Replizierung auf einen redundanten ONTAP Cluster im sekundären Datacenter oder Cloud Volume ONTAP in der Public Cloud gesichert. In einer vollständig konfigurierten Disaster-Recovery-Umgebung sind die Recovery von Computing-Instanzen im sekundären Datacenter oder in der Public Cloud Standby und im Notfall bereit, die Produktionsdatenbank wiederherzustellen. Die Standby-Computing-Instanzen werden mit On-Prem-Instanzen synchronisiert, indem parallel-Updates auf OS-Kernel-Patch ausgeführt oder ein Upgrade in einem Lockstep durchgeführt wird.
2. In dieser demonstrierten Lösung wird das Oracle Binary Volume zum Ziel repliziert und an einer Zielinstanz gemountet, um den Oracle Software Stack zu erstellen. Dieser Ansatz zur Wiederherstellung von Oracle hat den Vorteil, dass Oracle in letzter Minute bei einem Ausfall neu installiert wird. Es garantiert, dass die Oracle Installation vollständig mit der aktuellen Installation der On-Prem-Produktionssoftware und den Patch-Leveln synchronisiert ist. Dies kann jedoch je nach Struktur der Softwarelizenzierung mit Oracle für das replizierte Oracle Binary Volume am Recovery-Standort zusätzliche Konsequenzen haben oder diese nicht haben. Der Benutzer wird empfohlen, sich mit seinem Softwarelizenzierungspersonal zu erkundigen, um die potenziellen Lizenzierungsanforderungen für Oracle zu bewerten, bevor er sich für denselben Ansatz entscheidet.
3. Der Standby-Oracle-Host am Ziel ist mit den Oracle-Vorbedingung-Konfigurationen konfiguriert.
4. Die SnapMirror-Spiegelungen werden beschädigt und die Volumes werden beschreibbar gemacht und auf den Standby-Oracle Host eingebunden.
5. Das Oracle Recovery-Modul führt die folgenden Aufgaben zur Wiederherstellung und dem Start von Oracle am Recovery-Standort aus, nachdem alle DB-Volumes auf der Standby-Compute-Instanz gemountet wurden.
 - a. Sync the Control file: Wir haben duplizierte Oracle Steuerdateien auf verschiedenen Datenbank-Volumes implementiert, um die kritische Datenbankkontrolldatei zu schützen. Eine ist auf dem Daten-Volume und eine ist auf dem Log-Volume. Da Daten und Protokoll-Volumes unterschiedlich häufig repliziert werden, sind sie zum Zeitpunkt der Wiederherstellung nicht synchron.
 - b. Relink Oracle Binary: Da die Oracle-Binärdatei auf einen neuen Host verlagert wird, braucht es eine Relink.
 - c. Recovery von Oracle Datenbank: Der Recovery-Mechanismus ruft die letzte Systemänderungsnummer in der letzten verfügbaren archivierten Protokolldatei von Oracle ab und stellt die Oracle Datenbank wieder her, um alle Geschäftstransaktionen wiedergewonnen zu haben, die zum Zeitpunkt eines Ausfalls auf den DR-Standort repliziert werden konnten. Die Datenbank wird dann in einer neuen Inkarnation gestartet, um Benutzerverbindungen und Geschäftstransaktionen am Recovery-Standort durchzuführen.



Bevor Sie das Recovery-Playbook ausführen, stellen Sie sicher, dass Sie Folgendes haben:
Vergewissern Sie sich, dass es über /etc/oratab und /etc/orainst.loc vom Oracle-Quellhost zum Zielhost kopiert wird

TR-4794: Oracle Databases on NetApp EF-Series

Mitch Blackburn, Ebin Kadavy, NetApp

TR-4794 soll Storage-Administratoren und Datenbankadministratoren helfen, Oracle erfolgreich auf NetApp EF-Series Storage zu implementieren.

["TR-4794: Oracle Databases on NetApp EF-Series"](#)

Microsoft SQL Server

TR-4951: Backup und Recovery for Microsoft SQL Server on AWS FSX for ONTAP

Autor(en): Niyaz Mohammed, Carine Ngwekwe - NetApp Solutions Engineering

Dieses Dokument enthält die erforderlichen Schritte für das Backup und Recovery für Microsoft SQL Server auf AWS FSX für ONTAP mit SnapCenter. Dazu gehören folgende Informationen:

- Konfiguration von NetApp SnapCenter
- SnapCenter-Backup-Vorgänge
- Backup-Vorgang für eine FCI-Datenbank
- Backup-Vorgang für mehrere Datenbanken
- Restore und Recovery

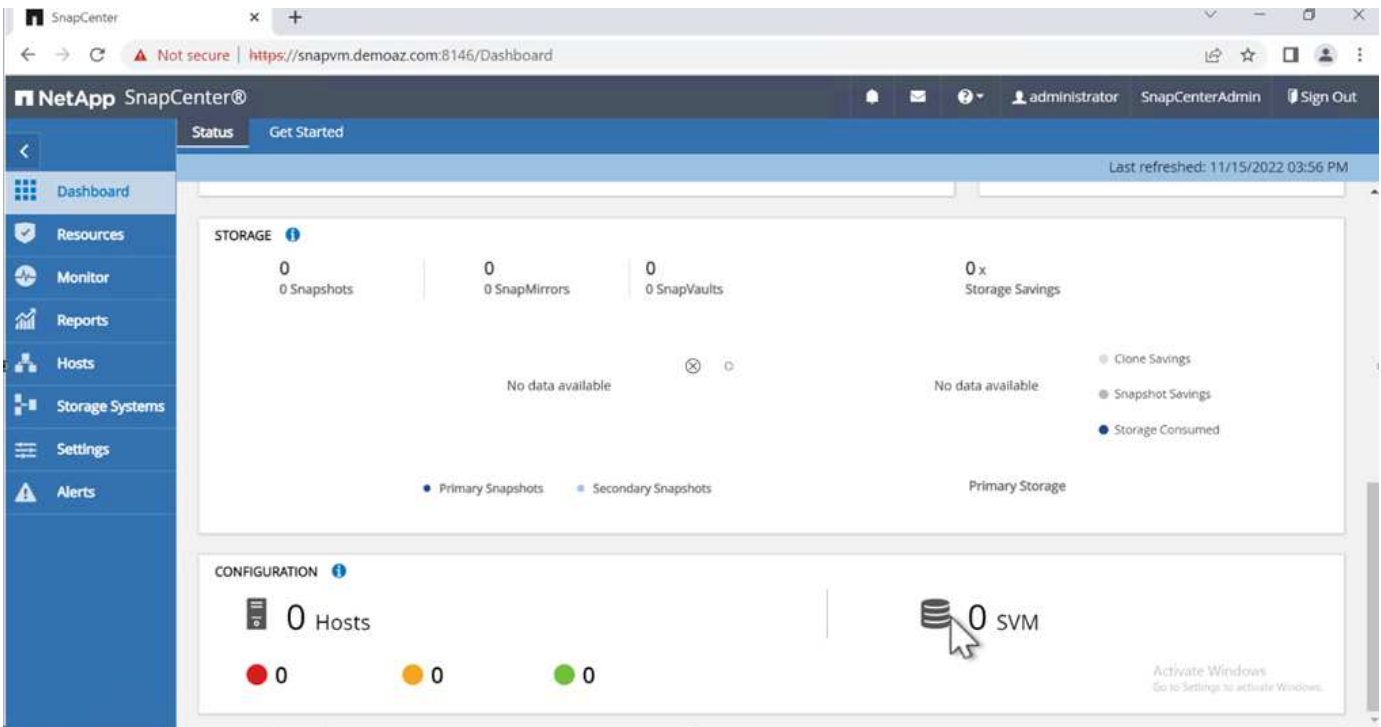
SnapCenter-Konfiguration

Die folgenden Schritte müssen für die SnapCenter-Konfiguration und den Schutz von Microsoft SQL Server-Ressourcen durchgeführt werden. Jeder der folgenden Schritte wird in den folgenden Abschnitten beschrieben.

1. Konfigurieren Sie die Sysadmin-Anmeldeinformationen für den Benutzer „SQL Server Backup and Restore“.
2. Speichereinstellungen konfigurieren. Geben Sie die AWS (Amazon Web Services) Management-Zugangsdaten für den Zugriff auf die Storage Virtual Machines (SVMs) von SnapCenter in Amazon FSX for NetApp ONTAP an.
3. Fügen Sie einen SQL Server-Host zu SnapCenter hinzu. Implementieren und installieren Sie die erforderlichen SnapCenter-Plug-ins.
4. Richtlinien konfigurieren. Definieren Sie den Backup-Vorgang, die Aufbewahrung und die optionale Snapshot-Backup-Replizierung.
5. Konfigurieren und schützen Sie die Microsoft SQL Server-Datenbank.

SnapCenter neu installierte Benutzeroberfläche

Konfigurieren Sie die Anmeldeinformationen für die SQL Server-Sicherung, und stellen Sie den Benutzer mit den sysadmin-Rechten wieder her.

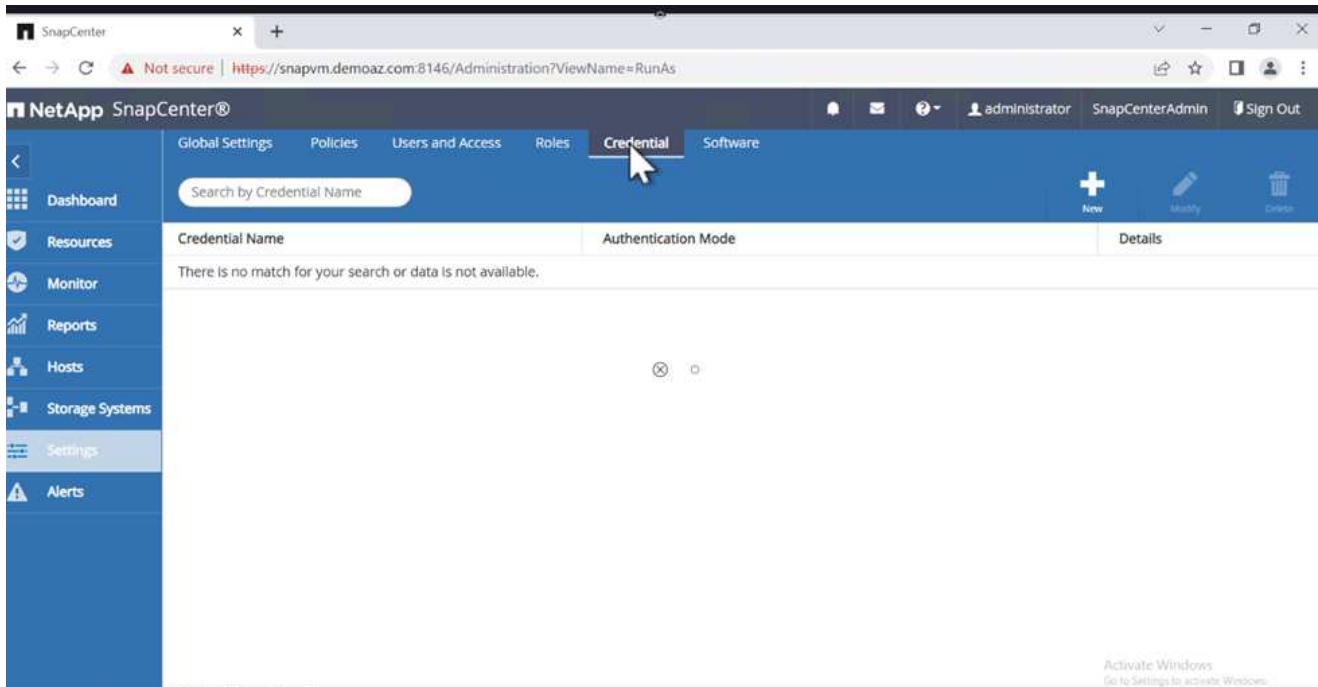


NetApp empfiehlt den Einsatz rollensbasierter Zugriffssteuerung (Role Based Access Control, RBAC), um Datenschutz- und Managementfunktionen an einzelne Benutzer über das SnapCenter und Fenster-Hosts zu delegieren. Der Benutzer muss Zugriff auf den SQL Server haben, der die Datenbank hostet. Bei mehreren Hosts müssen Benutzername und Passwort auf den verschiedenen Hosts gleich sein. Damit SnapCenter das erforderliche Plug-in auf SQL Server Hosts bereitstellen kann, müssen Sie darüber hinaus die Domäneninformationen für SnapCenter registrieren, um Ihre Anmeldedaten und Hosts zu validieren.

Erweitern Sie die folgenden Abschnitte, um detaillierte Anweisungen zum Abschließen der einzelnen Schritte zu erhalten.

Fügen Sie die Anmeldeinformationen hinzu

Gehen Sie zu **Einstellungen**, wählen Sie **Anmeldeinformationen** und klicken Sie auf (+).



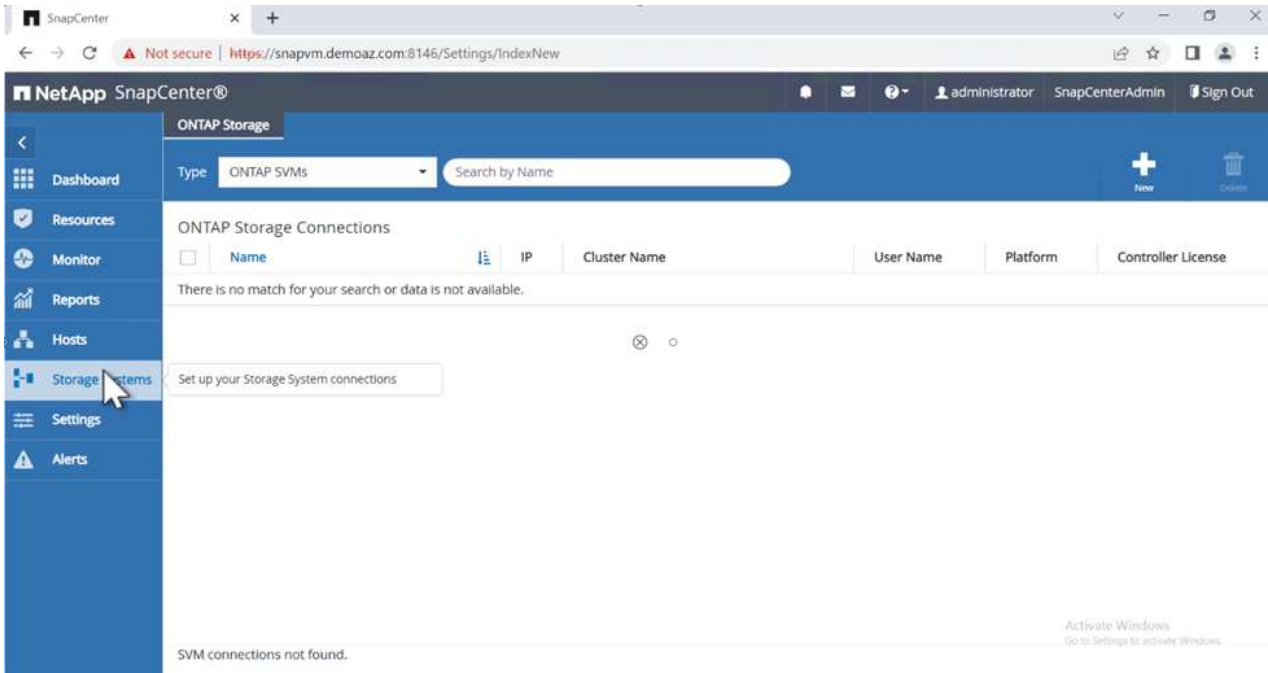
Der neue Benutzer muss über Administratorrechte auf dem SQL Server-Host verfügen.

The screenshot shows the 'Credential' dialog box in NetApp SnapCenter. The dialog has a title bar 'Credential' with a close button (X). It contains four input fields: 'Credential Name' with the value 'Demoaz', 'Authentication Mode' with a dropdown menu set to 'Windows', 'Username' with the value 'demoaz\clusteradmin', and 'Password' with a masked password '*****'. There is an information icon (i) next to the Username field. At the bottom of the dialog, there is a progress indicator 'Setting credential...' and two buttons: 'Cancel' and 'OK'.

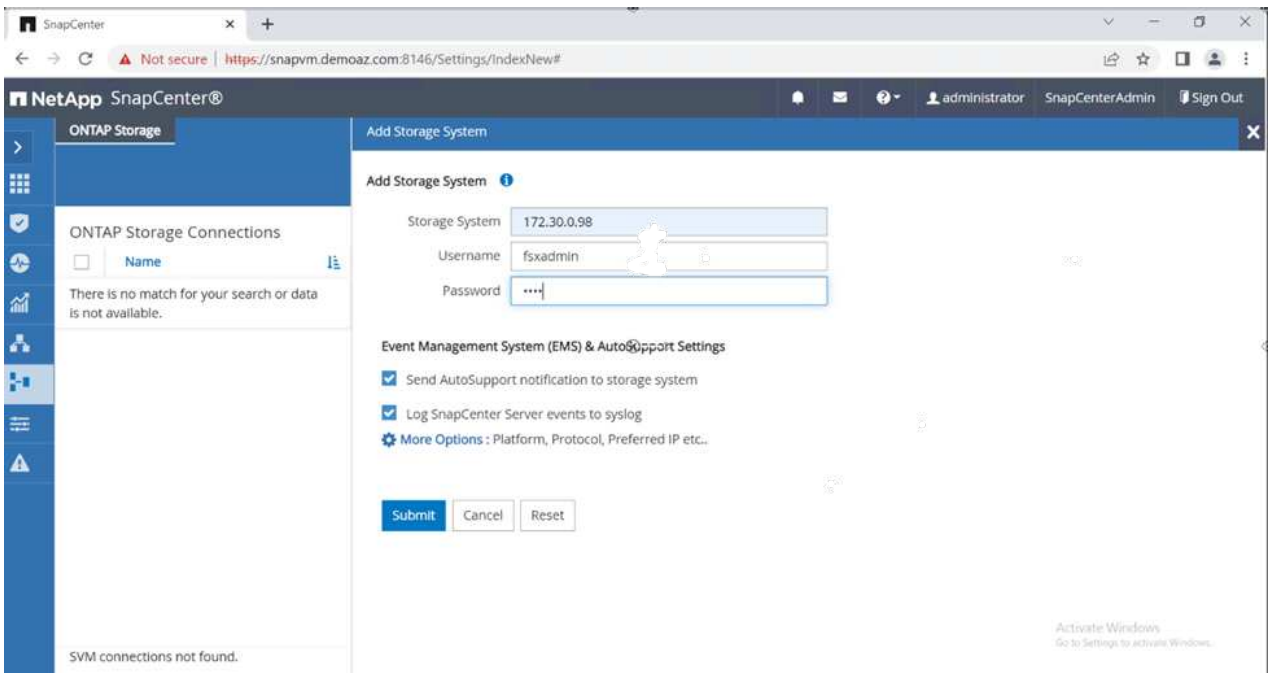
Speicher konfigurieren

Gehen Sie wie folgt vor, um Speicher in SnapCenter zu konfigurieren:

1. Wählen Sie in der SnapCenter-Benutzeroberfläche **Speichersysteme** aus. Es gibt zwei Speichertypen, **ONTAP SVM** und **ONTAP Cluster**. Standardmäßig ist der Speichertyp **ONTAP SVM**.
2. Klicken Sie auf (+), um die Informationen zum Speichersystem hinzuzufügen.



3. Stellen Sie den * FSX für ONTAP-Management*-Endpunkt bereit.



4. Die SVM ist jetzt in SnapCenter konfiguriert.

NetApp SnapCenter®

ONTAP Storage

Type: Search by Name

ONTAP Storage Connections

<input type="checkbox"/>	Name	IP	Cluster Name	User Name	Platform	Controller License
<input type="checkbox"/>	ESNSVMTESTRDS		rdsfsxTest01		FSx	Not applicable

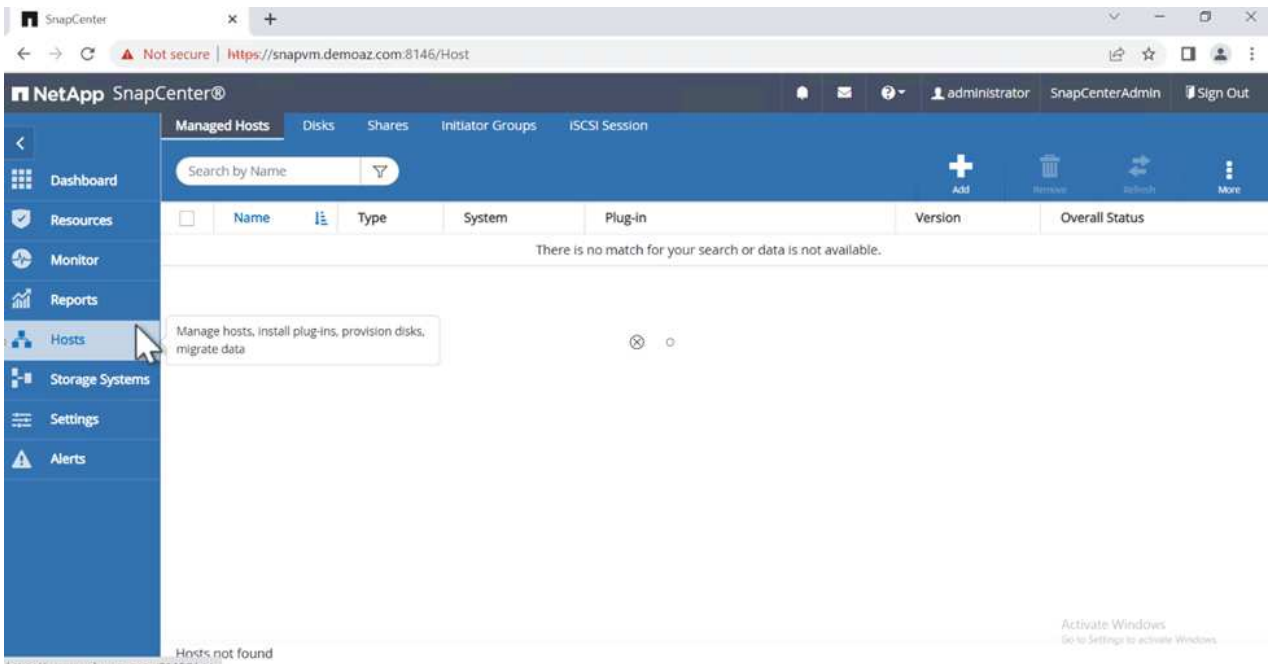
Total 1

Activate Windows
Go to Settings to activate Windows.

Fügen Sie einen SQL Server-Host zu SnapCenter hinzu

Führen Sie die folgenden Schritte aus, um einen SQL Server-Host hinzuzufügen:

1. Klicken Sie auf der Registerkarte Host auf (+), um den Microsoft SQL Server-Host hinzuzufügen.

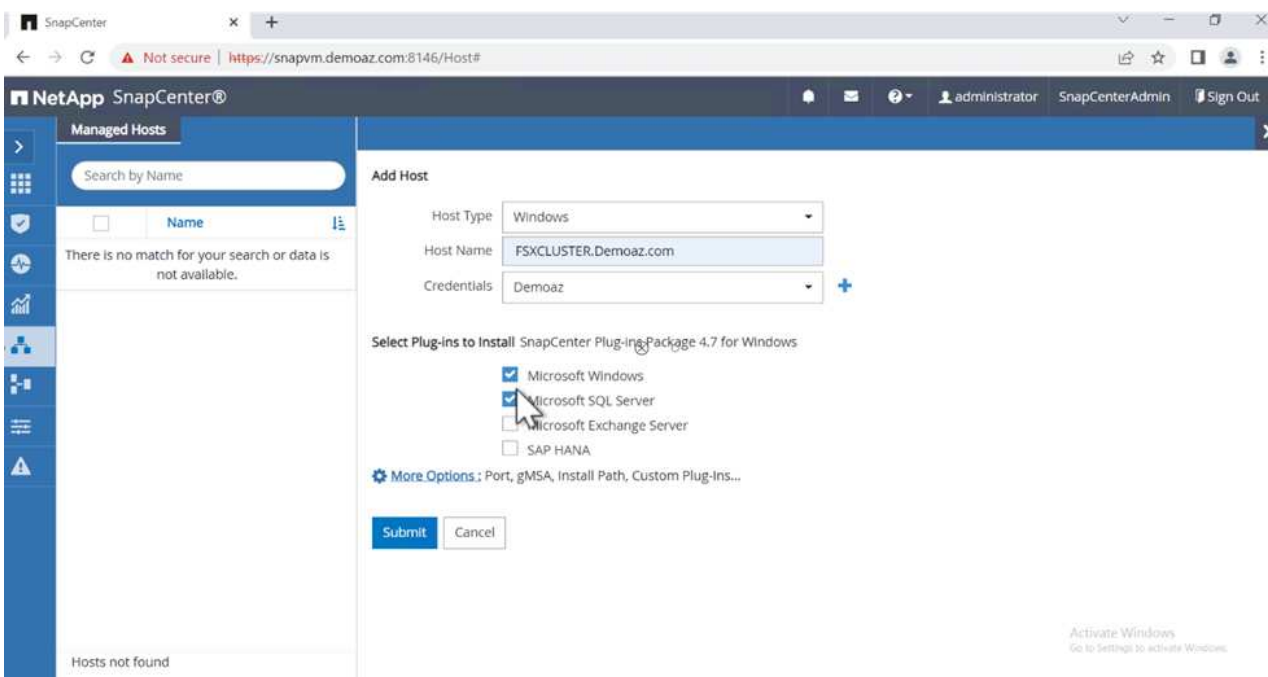


2. Geben Sie den vollständig qualifizierten Domännennamen (FQDN) oder die IP-Adresse des Remote-Hosts an.

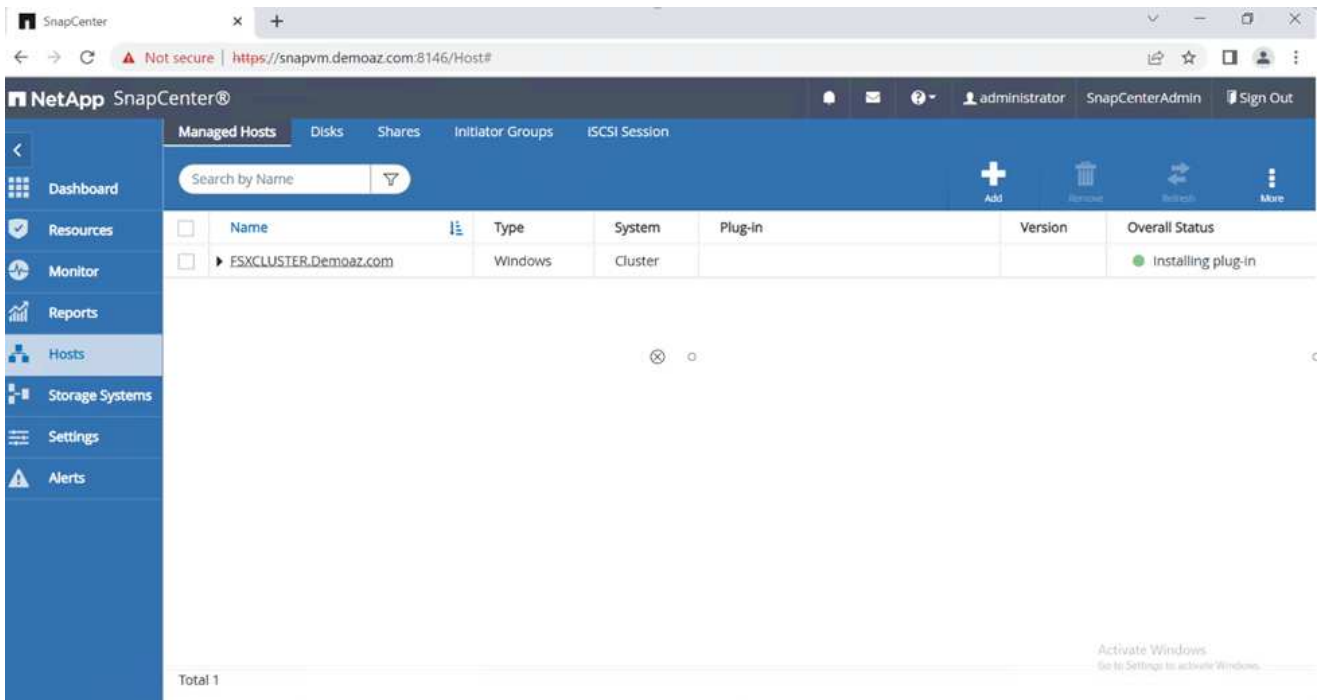


Die Anmeldeinformationen werden standardmäßig ausgefüllt.

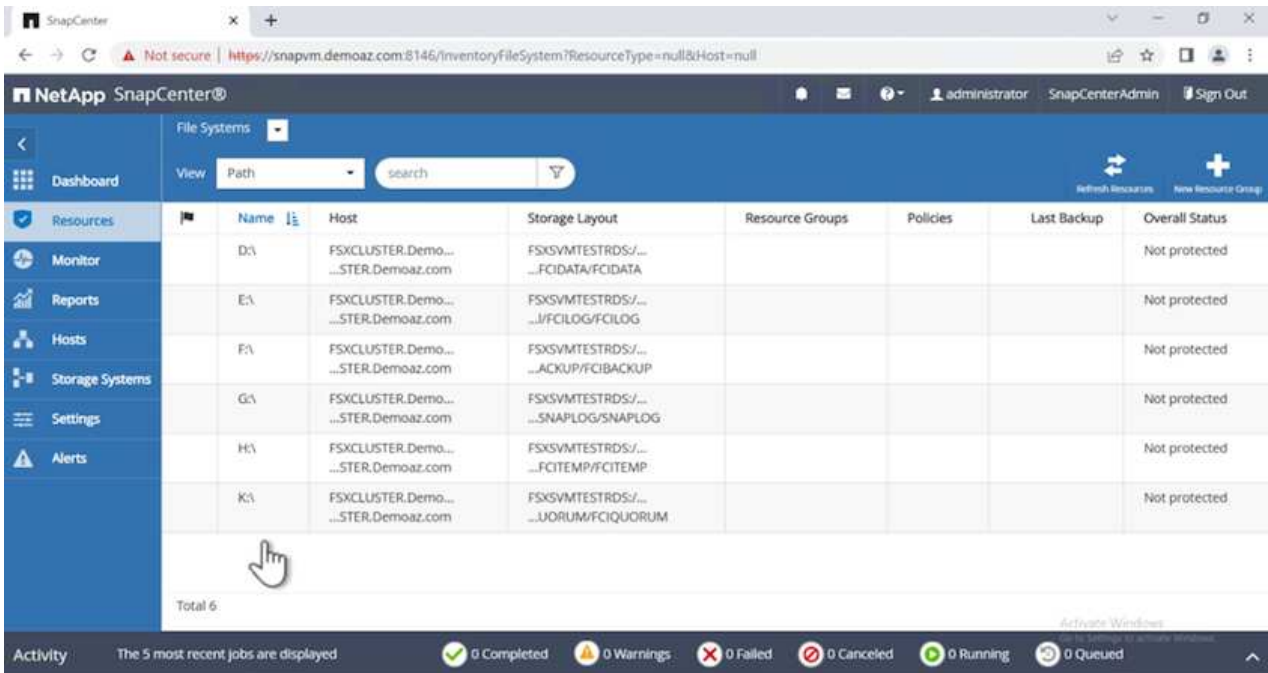
3. Wählen Sie die Option für Microsoft Windows und Microsoft SQL Server aus, und senden Sie sie anschließend ab.



Die SQL Server-Pakete werden installiert.



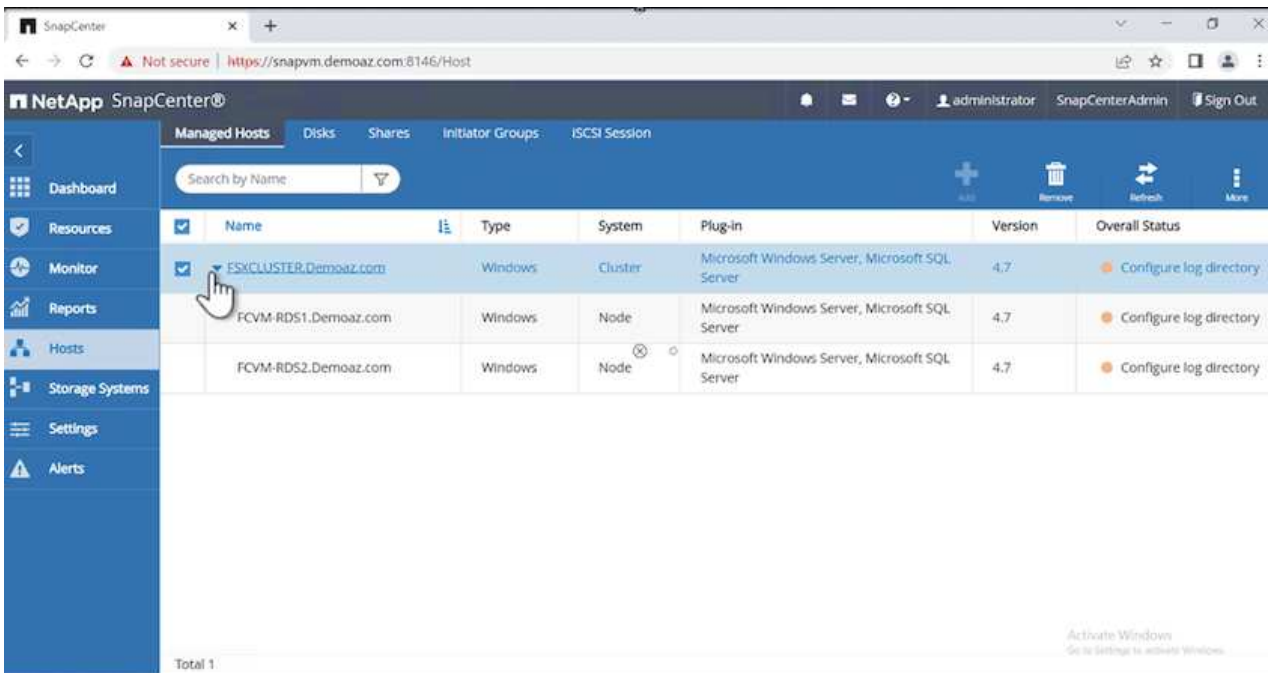
1. Nachdem die Installation abgeschlossen ist, gehen Sie auf die Registerkarte **Ressource**, um zu überprüfen, ob alle FSX für ONTAP iSCSI-Volumes vorhanden sind.



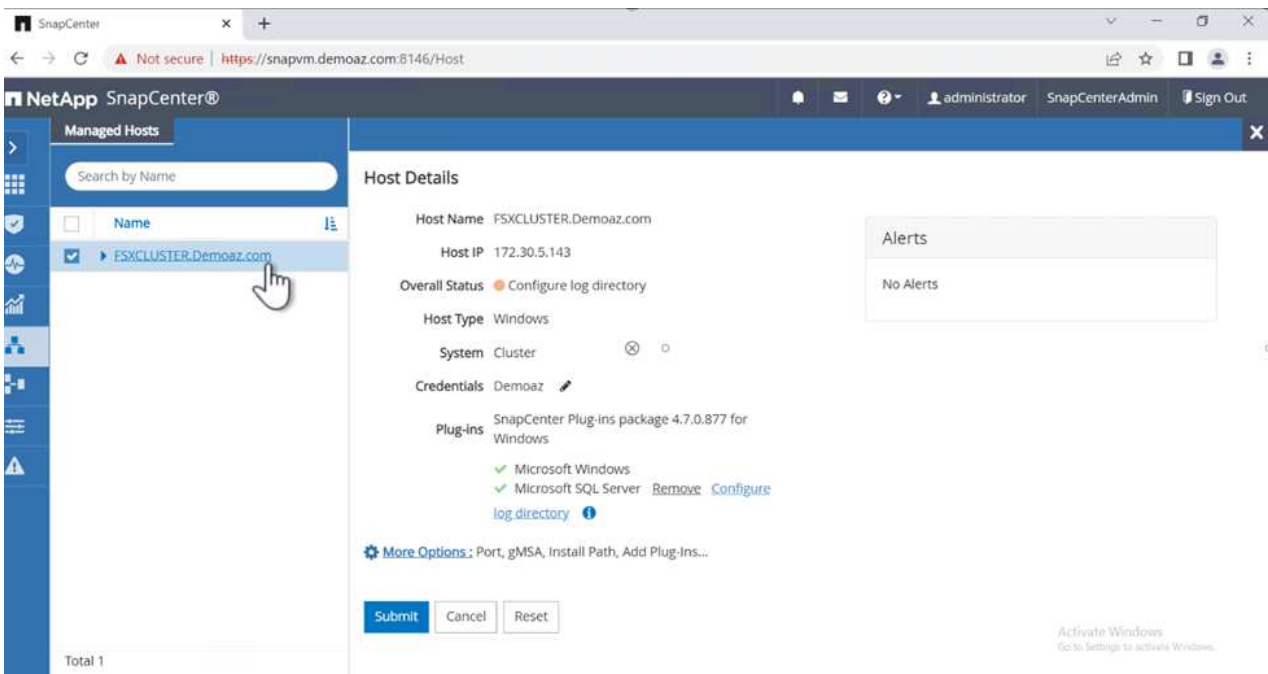
Protokollverzeichnis konfigurieren

Führen Sie zum Konfigurieren eines Host-Protokollverzeichnisses die folgenden Schritte aus:

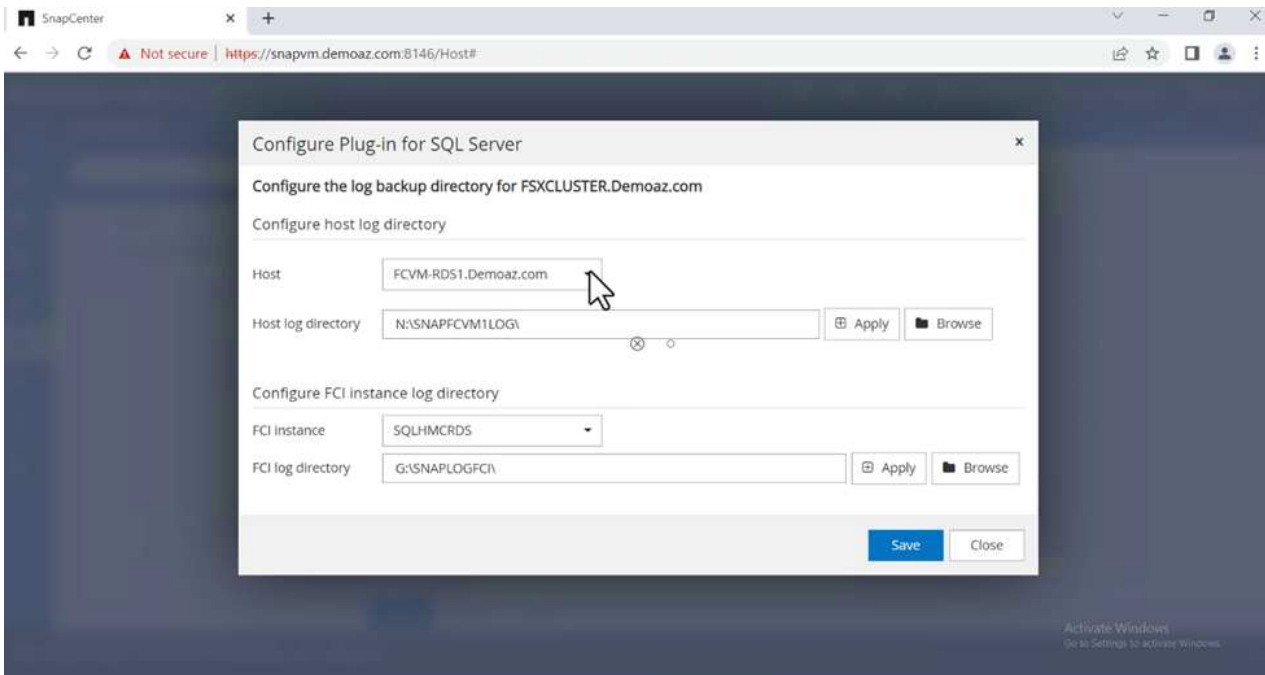
1. Aktivieren Sie das Kontrollkästchen. Eine neue Registerkarte wird geöffnet.



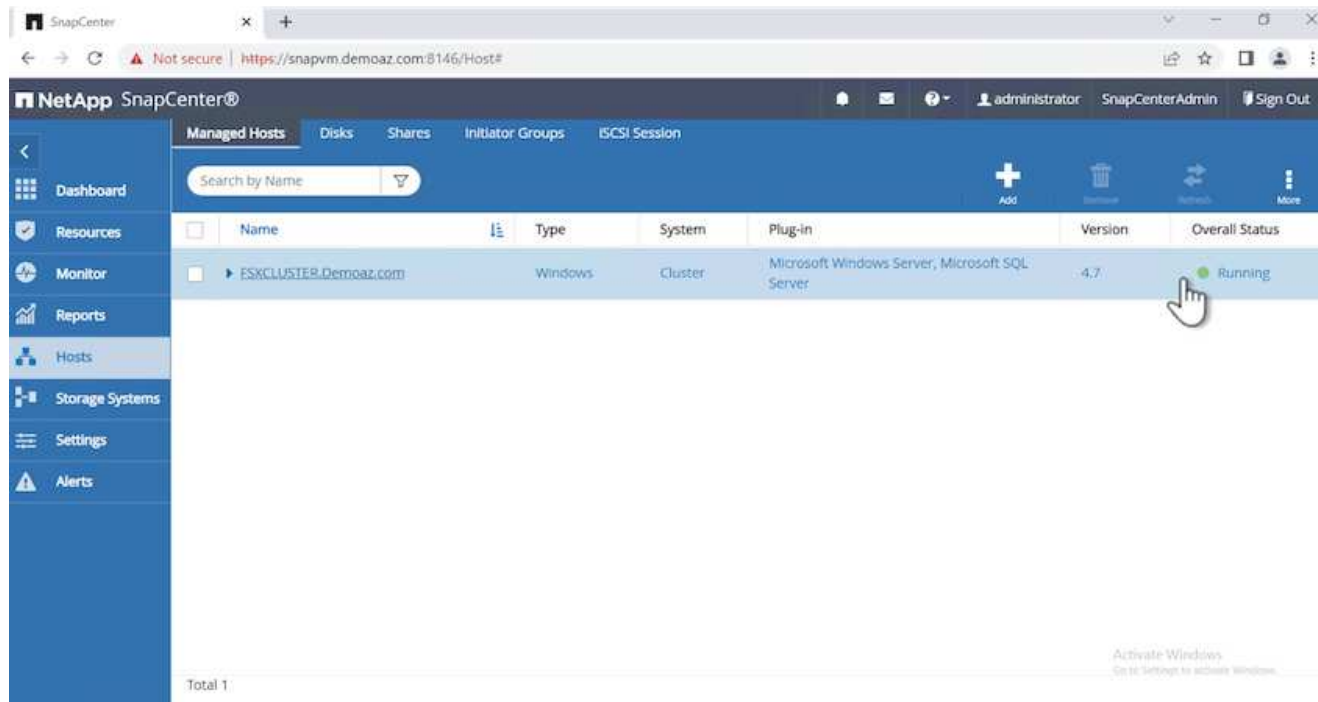
2. Klicken Sie auf den Link **configure log Directory**.



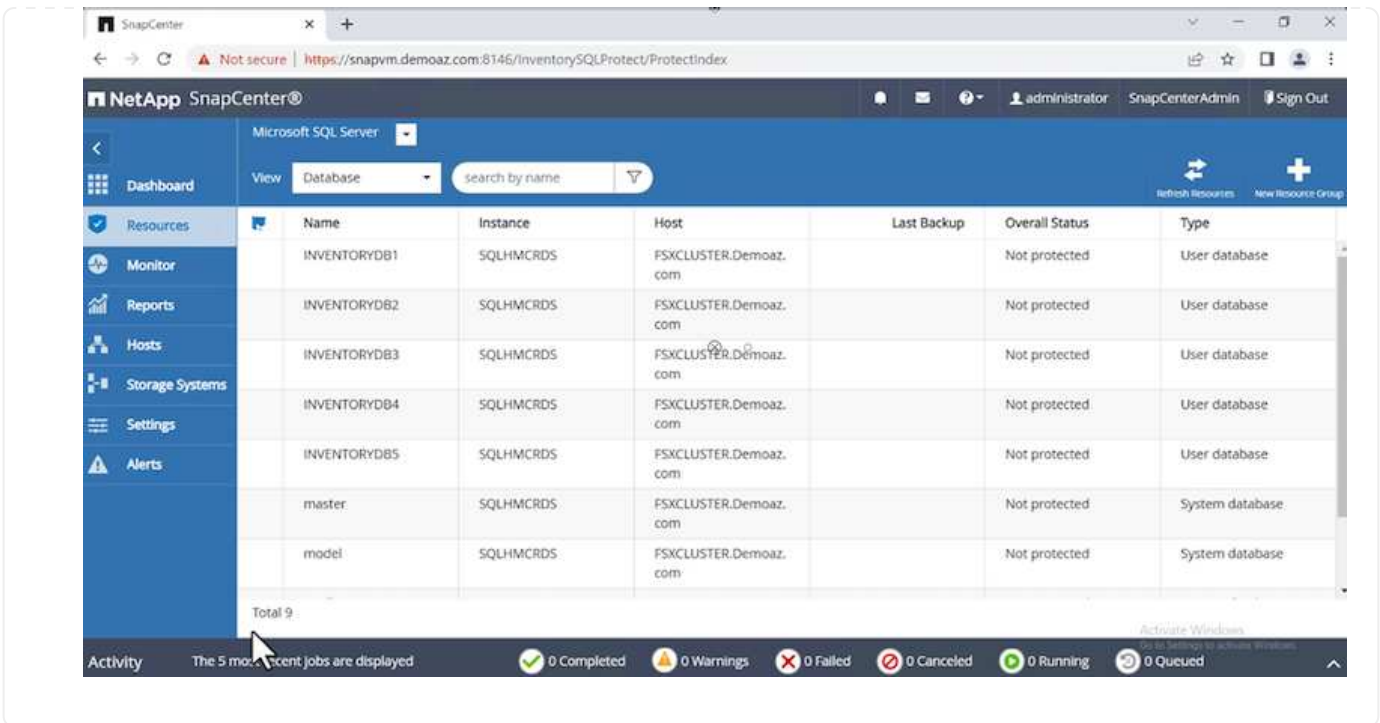
3. Wählen Sie das Laufwerk für das Host-Protokollverzeichnis und das Protokollverzeichnis der FCI-Instanz aus. Klicken Sie Auf **Speichern**. Wiederholen Sie denselben Prozess für den zweiten Node im Cluster. Schließen Sie das Fenster.



Der Host befindet sich jetzt im Status „aktiv“.



1. Auf der Registerkarte **Ressourcen** haben wir alle Server und Datenbanken.



Konfigurieren Sie eine Backup Policy

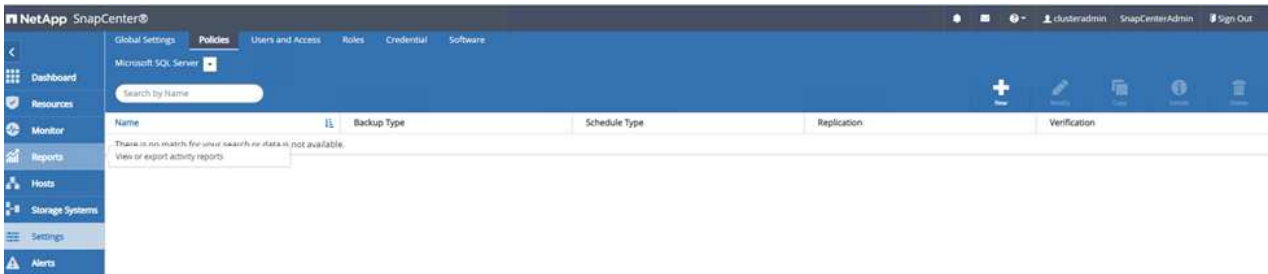
Eine Sicherungsrichtlinie ist eine Reihe von Regeln, die festlegen, wie Backups gemanagt, geplant und aufbewahrt werden. Es ist hilfreich, die Art und Häufigkeit von Backups zu nutzen, die auf dem SLA Ihres Unternehmens basieren.

Erweitern Sie die folgenden Abschnitte, um detaillierte Anweisungen zum Abschließen der einzelnen Schritte zu erhalten.

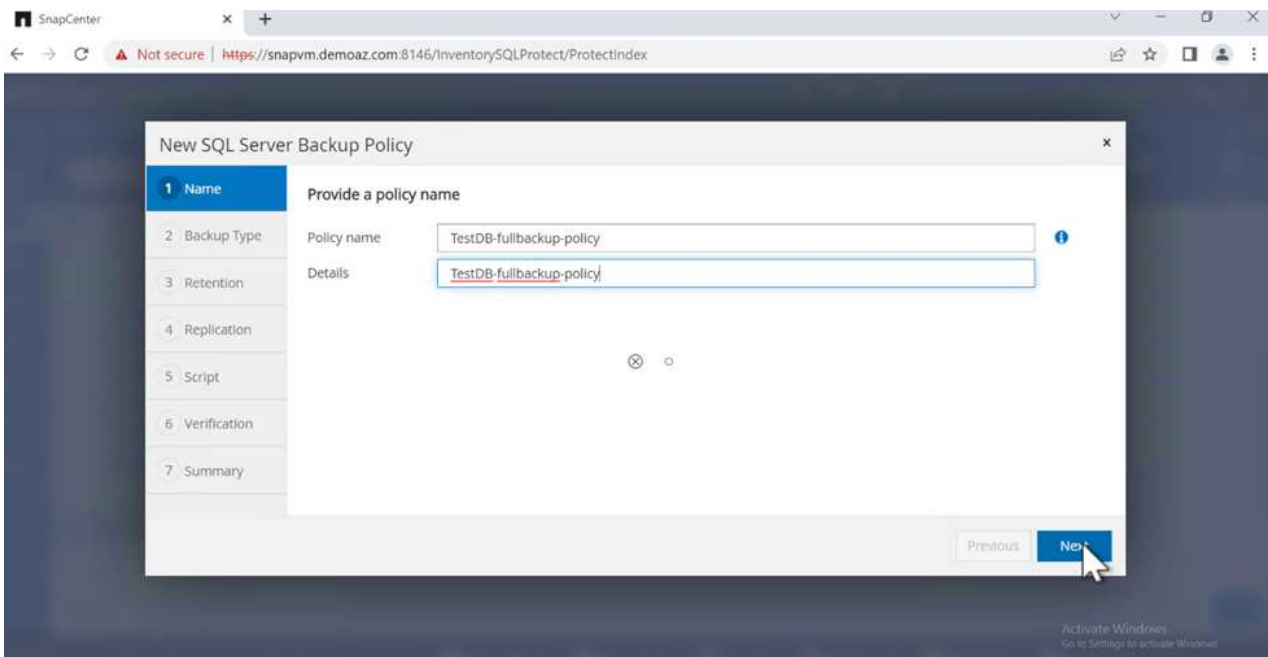
Konfigurieren Sie den Sicherungsvorgang für eine FCI-Datenbank

Führen Sie die folgenden Schritte aus, um eine Sicherungsrichtlinie für eine FCI-Datenbank zu konfigurieren:

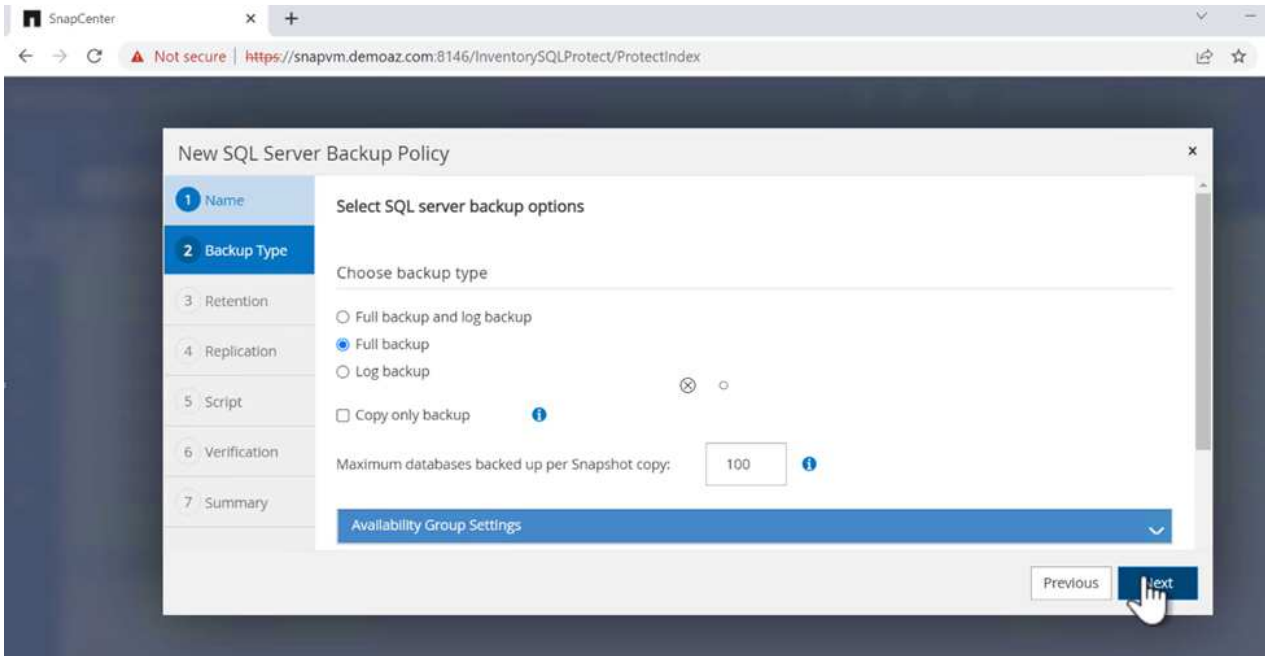
1. Gehen Sie zu **Einstellungen** und wählen Sie **Richtlinien** oben links. Klicken Sie dann auf **Neu**.



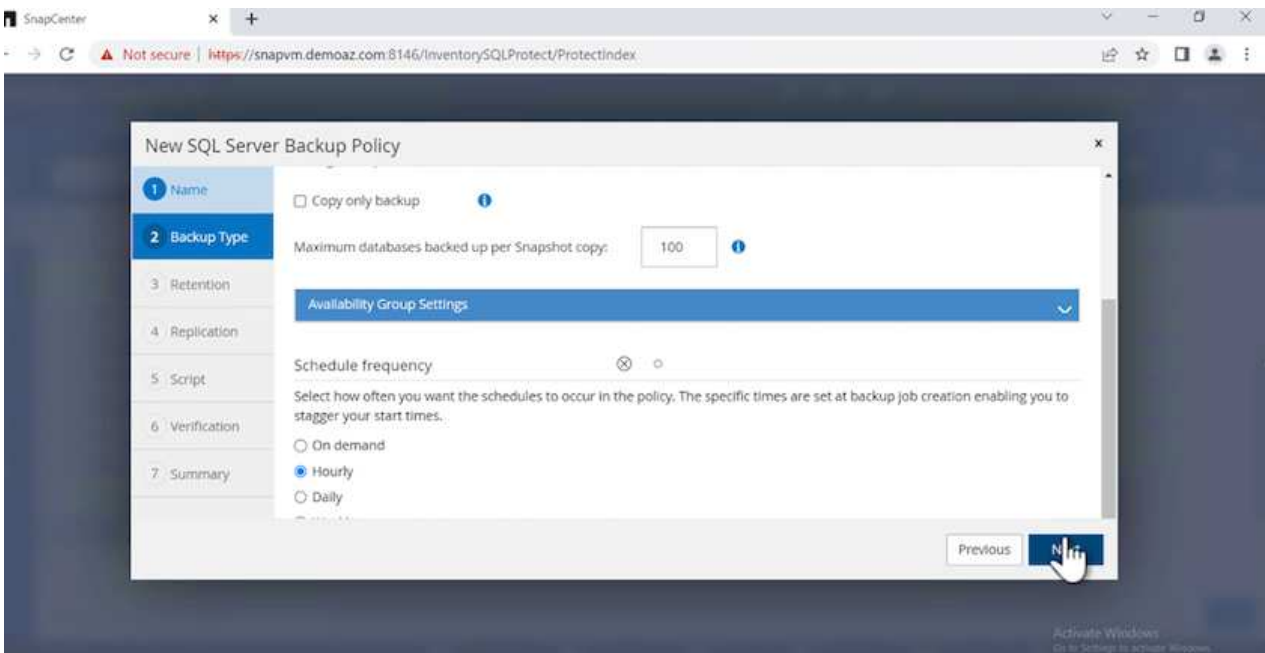
2. Geben Sie den Richtliniennamen und eine Beschreibung ein. Klicken Sie Auf **Weiter**.



3. Wählen Sie **Full Backup** als Sicherungstyp.



4. Wählen Sie die Zeitplanhäufigkeit aus (dies basiert auf dem Unternehmens-SLA). Klicken Sie Auf **Weiter**.



5. Konfigurieren Sie die Aufbewahrungseinstellungen für das Backup.

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention**
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

Keep log backups applicable to last full backups

Keep log backups applicable to last days

Full backup retention settings ⓘ

Weekly

Total Snapshot copies to keep

Keep Snapshot copies for days

6. Konfigurieren der Replikationsoptionen.

New SQL Server Backup Policy ×

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label ⓘ

Error retry count ⓘ

7. Geben Sie ein Skript zum Ausführen vor und nach der Ausführung eines Backupjobs an (falls vorhanden).

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout secs

Previous Next

8. Überprüfung auf Basis des Backup-Zeitplans durchführen.

New SQL Server Backup Policy

- Name
- Backup Type
- Retention
- Replication
- Script
- Verification**
- Summary

Select the options to run backup verification

Run verifications for the following backup schedules

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

Weekly

Database consistency checks options

Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)

Suppress all information message (NO_INFOMSGS)

Display all reported error messages per object (ALL_ERRORMSG)

Do not check non-clustered indexes (NOINDEX)

Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Verification script settings

Script timeout: secs

Prescript full path:

Prescript arguments:

Postscript full path:

Postscript arguments:

Previous **Next**

9. Die Seite **Summary** enthält Details zur Backup Policy. Etwaige Fehler können hier korrigiert werden.

Browser: SnapCenter

URL: <https://snapvm.demoaz.com:8146/InventorySQLProtect/ProtectIndex>

New SQL Server Backup Policy

- Name
- Backup Type
- Retention
- Replication
- Script
- Verification
- Summary**

Summary

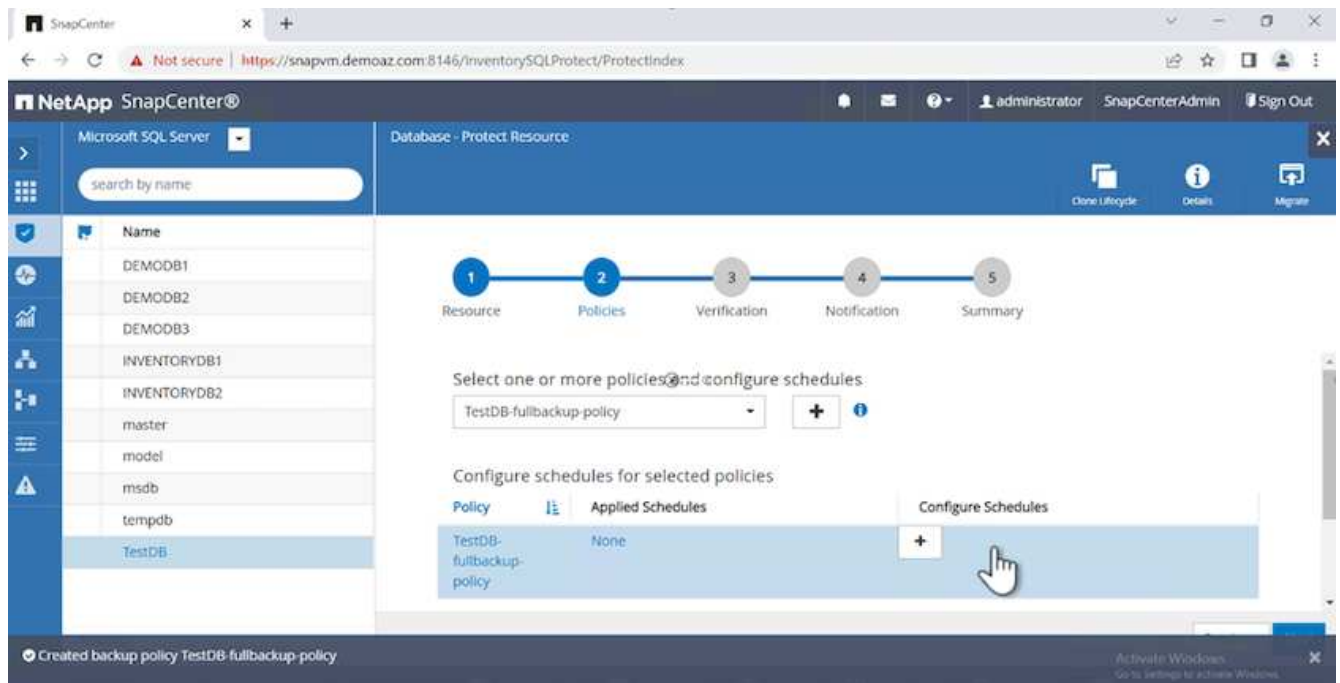
Policy name	TestDB-fullbackup-policy
Details	TestDB-fullbackup-policy
Backup type	Full backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Hourly <input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>
UTM retention	Total backup copies to retain : 7
Hourly Full backup retention	Total backup copies to retain : 7
Replication	none
Backup prescript settings	undefined
Prescript arguments:	

Previous **Finish**

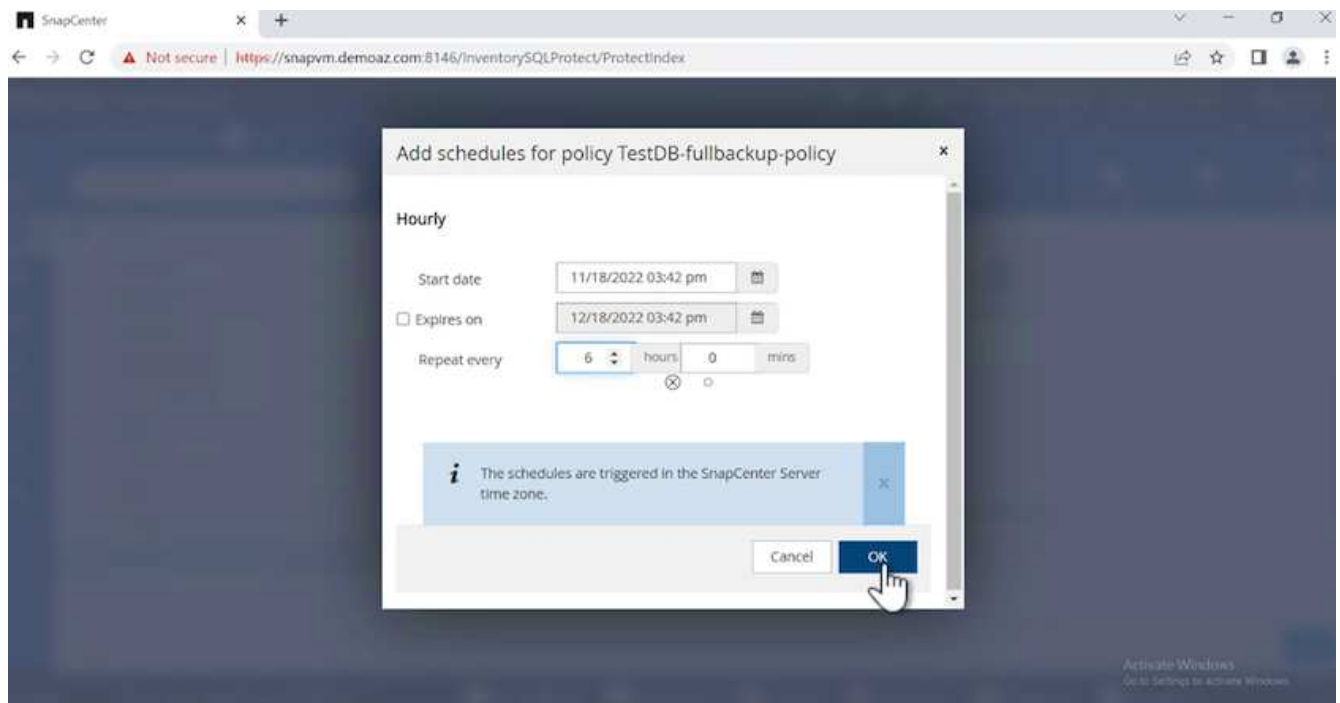
Activate Windows
Go to Settings to activate Windows

Konfiguration und Schutz der MSSQL Server-Datenbank

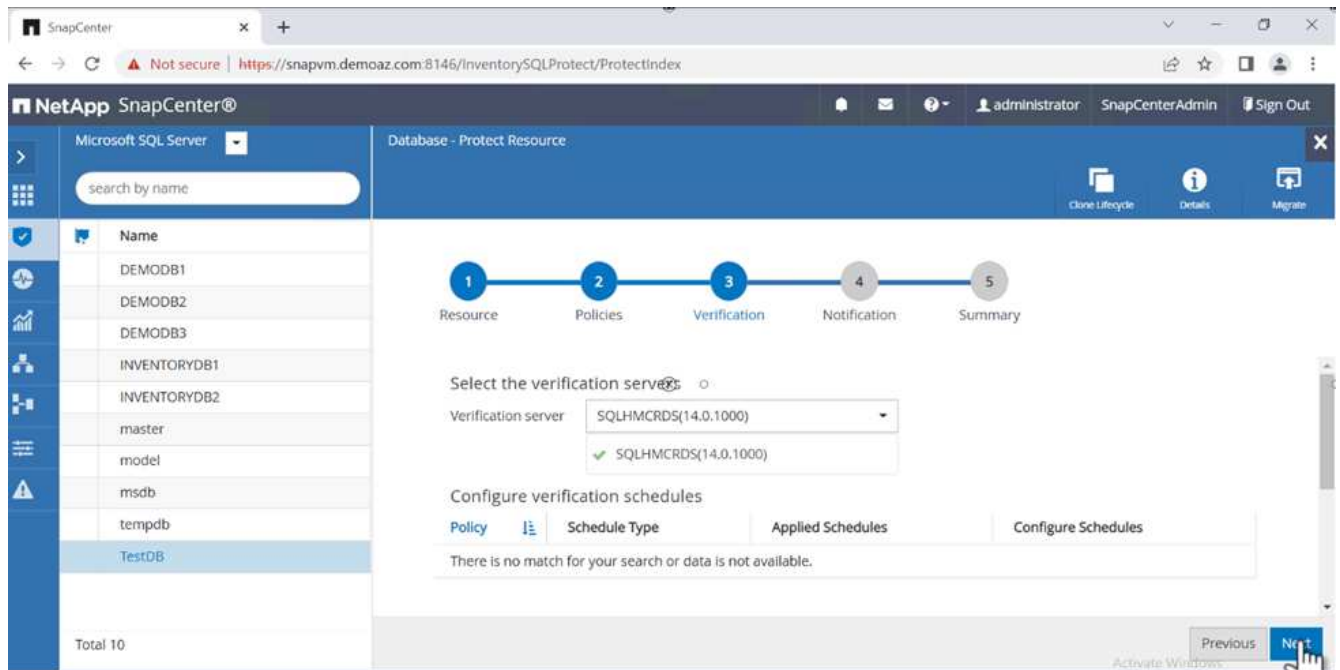
1. Legen Sie das Startdatum und das Ablaufdatum der Backup-Richtlinie fest.



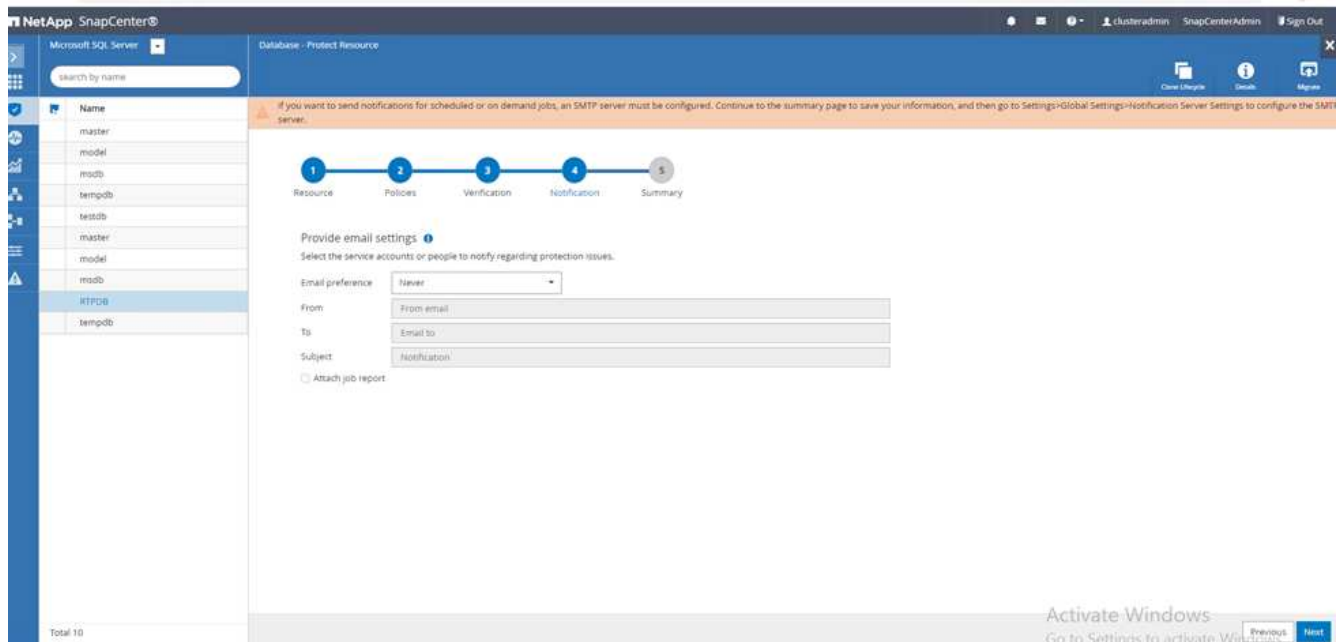
2. Legen Sie den Zeitplan für das Backup fest. Klicken Sie dazu auf (+), um einen Zeitplan zu konfigurieren. Geben Sie das Datum **Start** und **läuft am** ein. Stellen Sie die Uhrzeit auf Basis des SLA des Unternehmens ein.



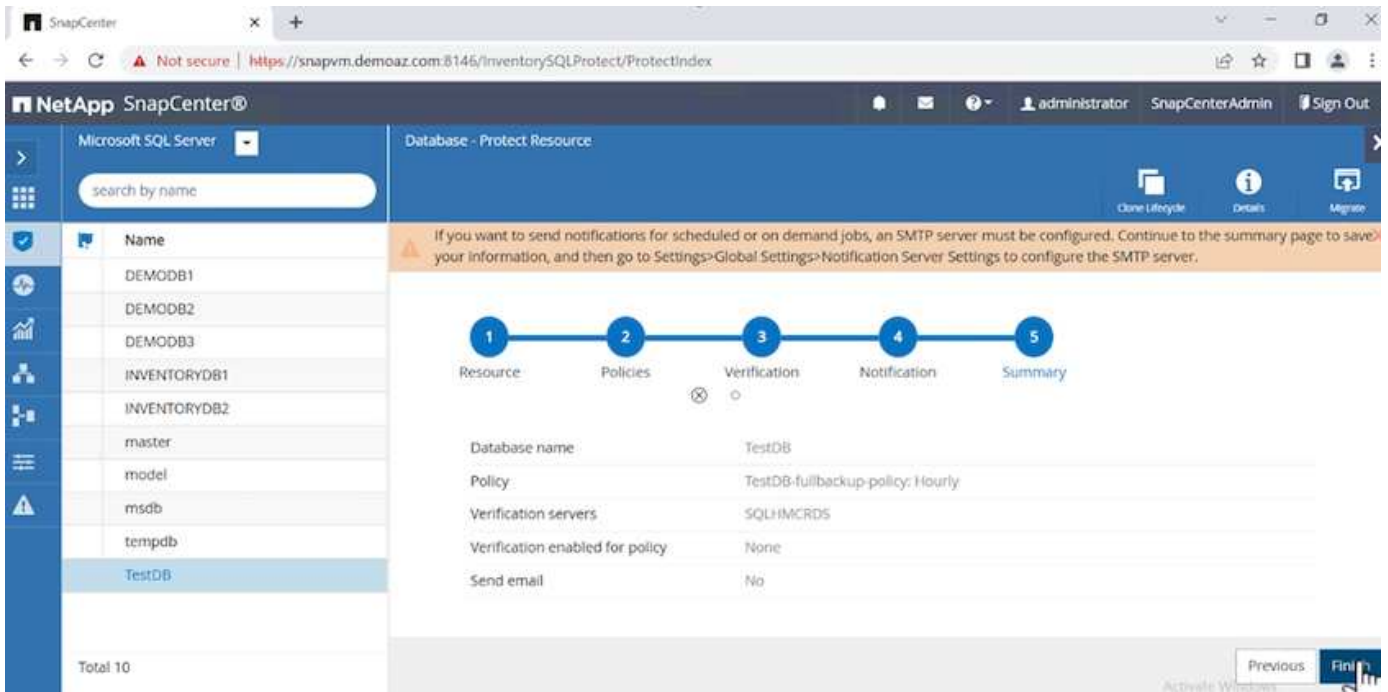
3. Konfigurieren Sie den Überprüfungsserver. Wählen Sie im Dropdown-Menü den Server aus.



4. Bestätigen Sie den konfigurierten Zeitplan, indem Sie auf das Pluszeichen klicken und bestätigen.
5. Geben Sie Informationen für E-Mail-Benachrichtigungen an. Klicken Sie Auf **Weiter**.



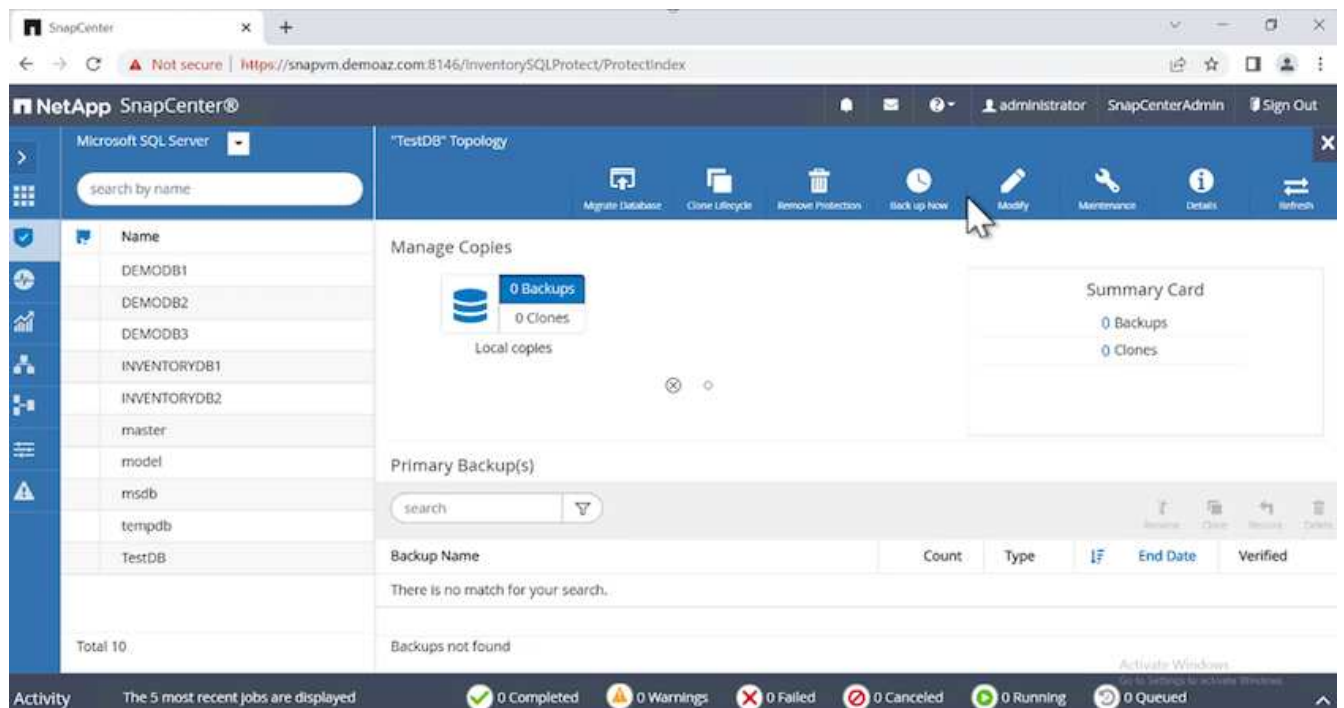
Die Zusammenfassung der Sicherheitsrichtlinie für die SQL Server-Datenbank ist jetzt konfiguriert.



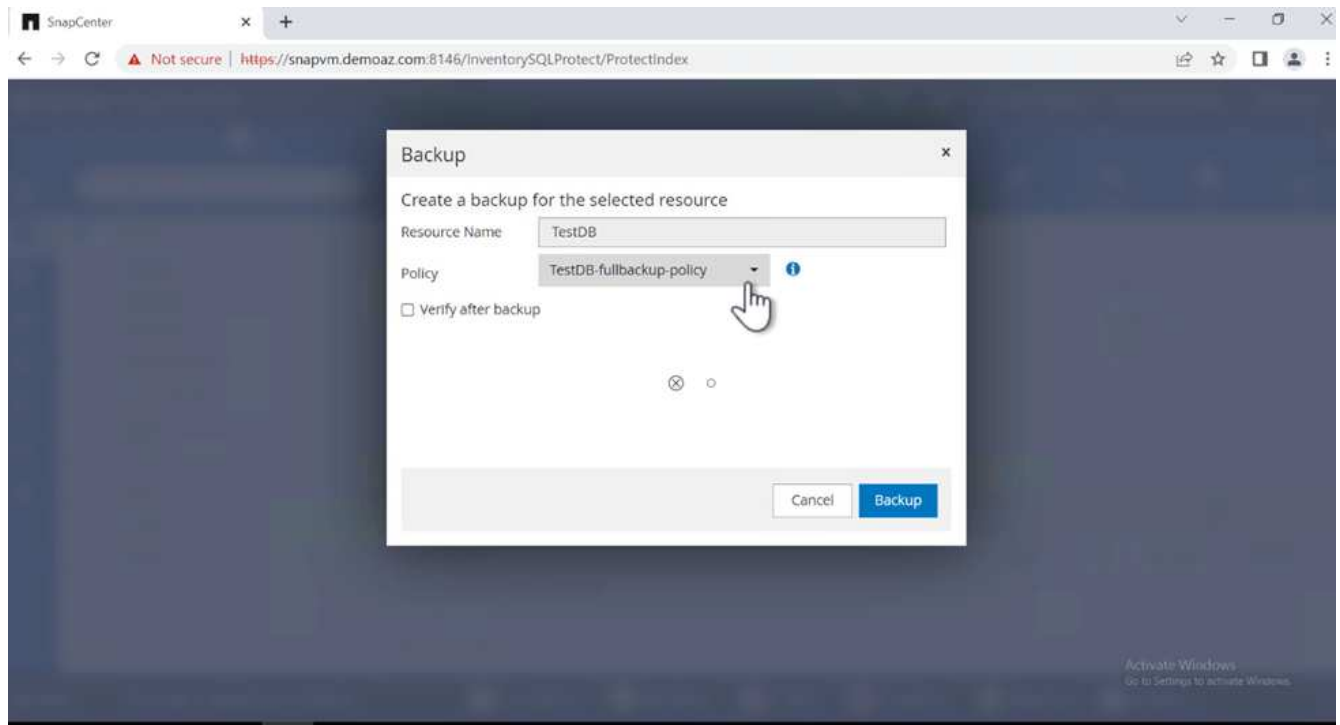
SnapCenter-Backup-Vorgänge

Führen Sie die folgenden Schritte aus, um On-Demand SQL Server-Backups zu erstellen:

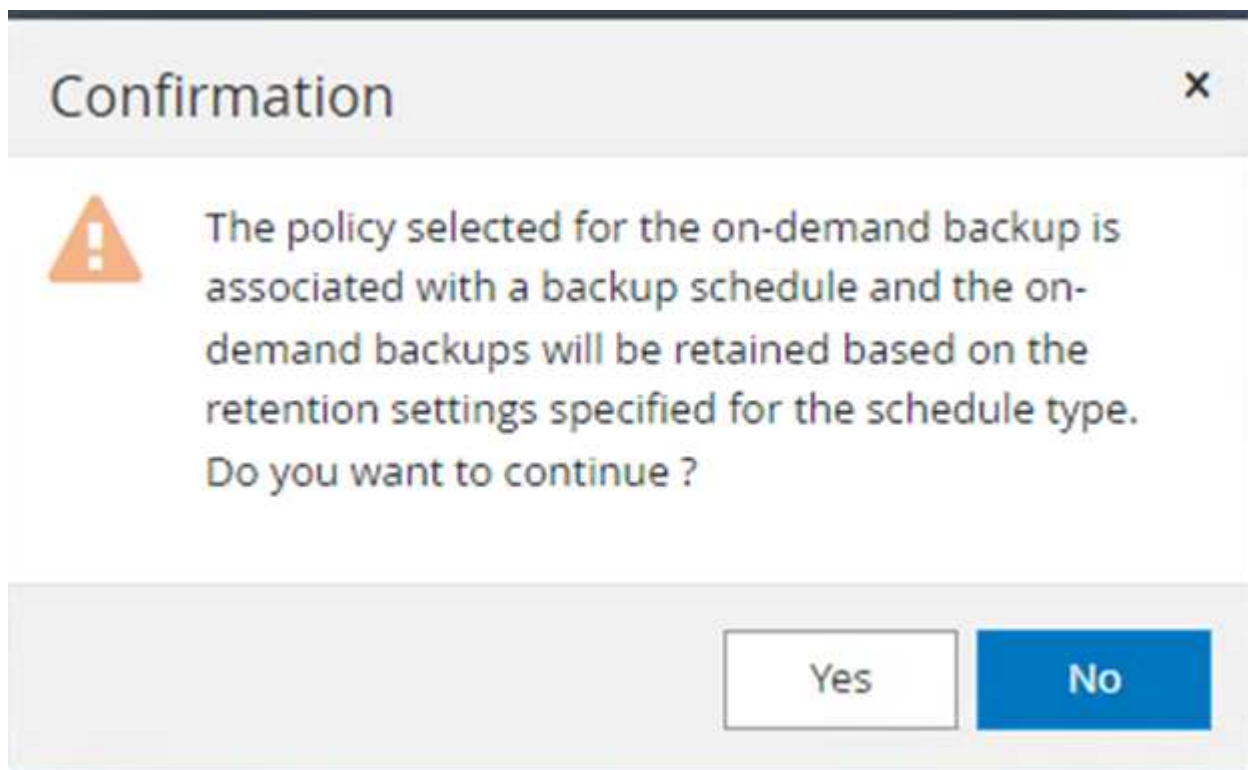
1. Wählen Sie in der Ansicht **Resource** die Ressource aus und wählen Sie **Backup now**.



2. Klicken Sie im Dialogfeld **Backup** auf **Backup**.

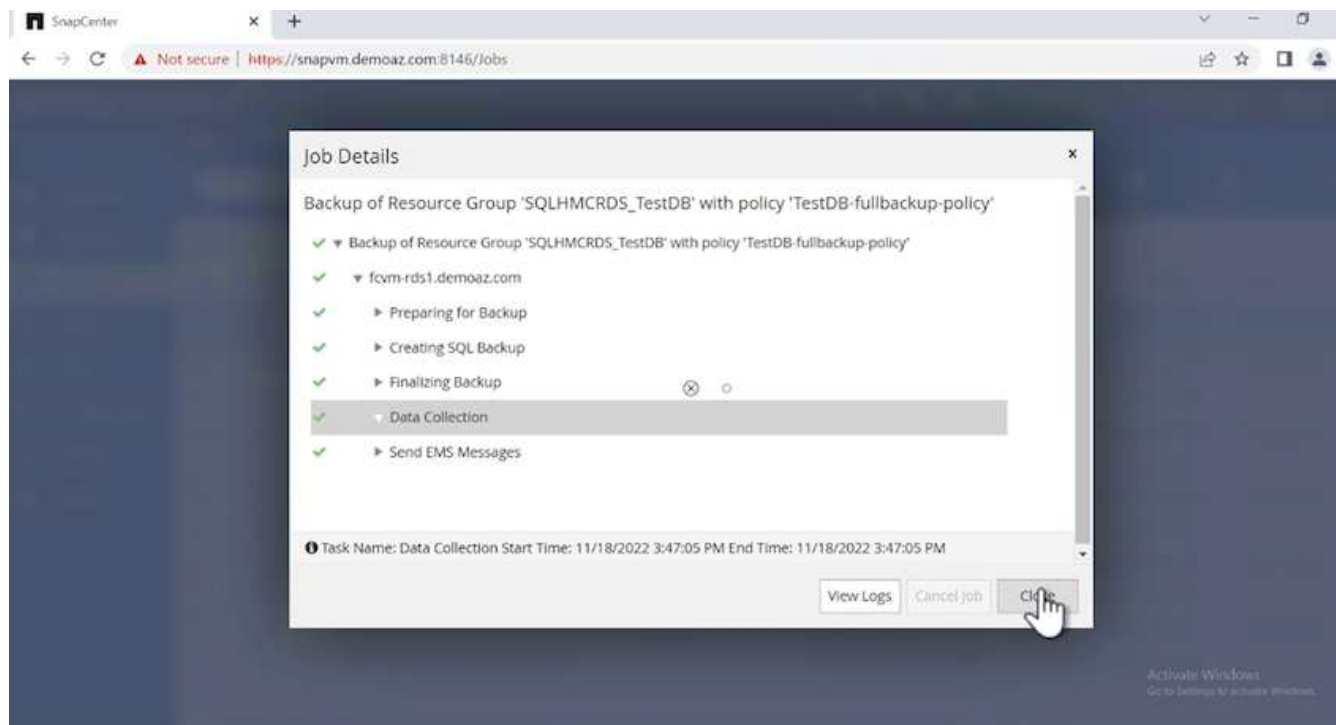
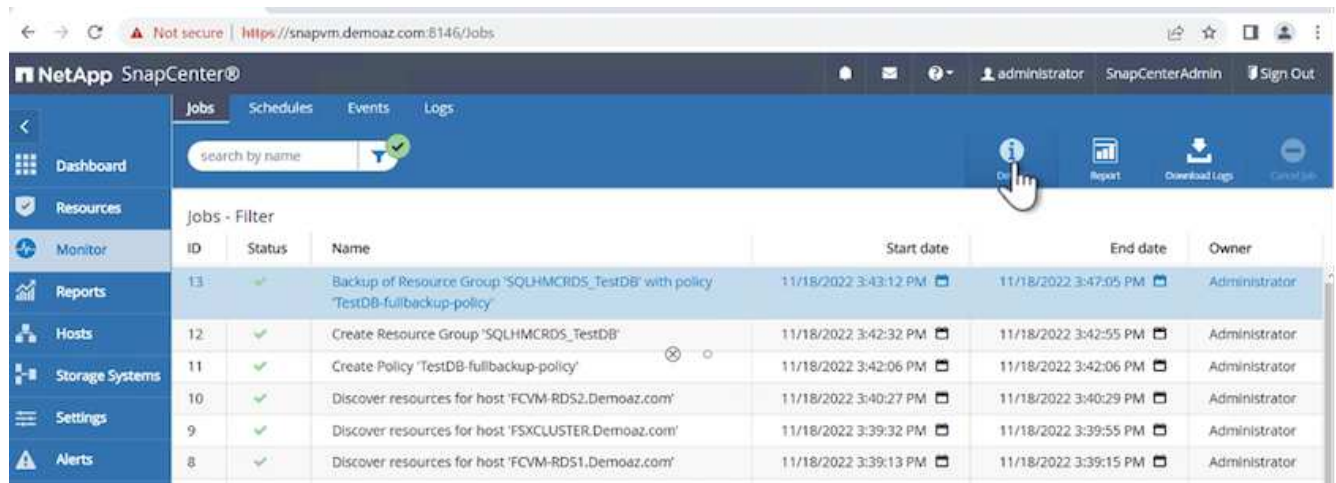


3. Ein Bestätigungsbildschirm wird angezeigt. Klicken Sie zur Bestätigung auf **Ja**.



Überwachen Sie den Backupjob

1. Klicken Sie auf der Registerkarte **Monitor** auf den Job und wählen Sie rechts **Details**, um die Jobs anzuzeigen.

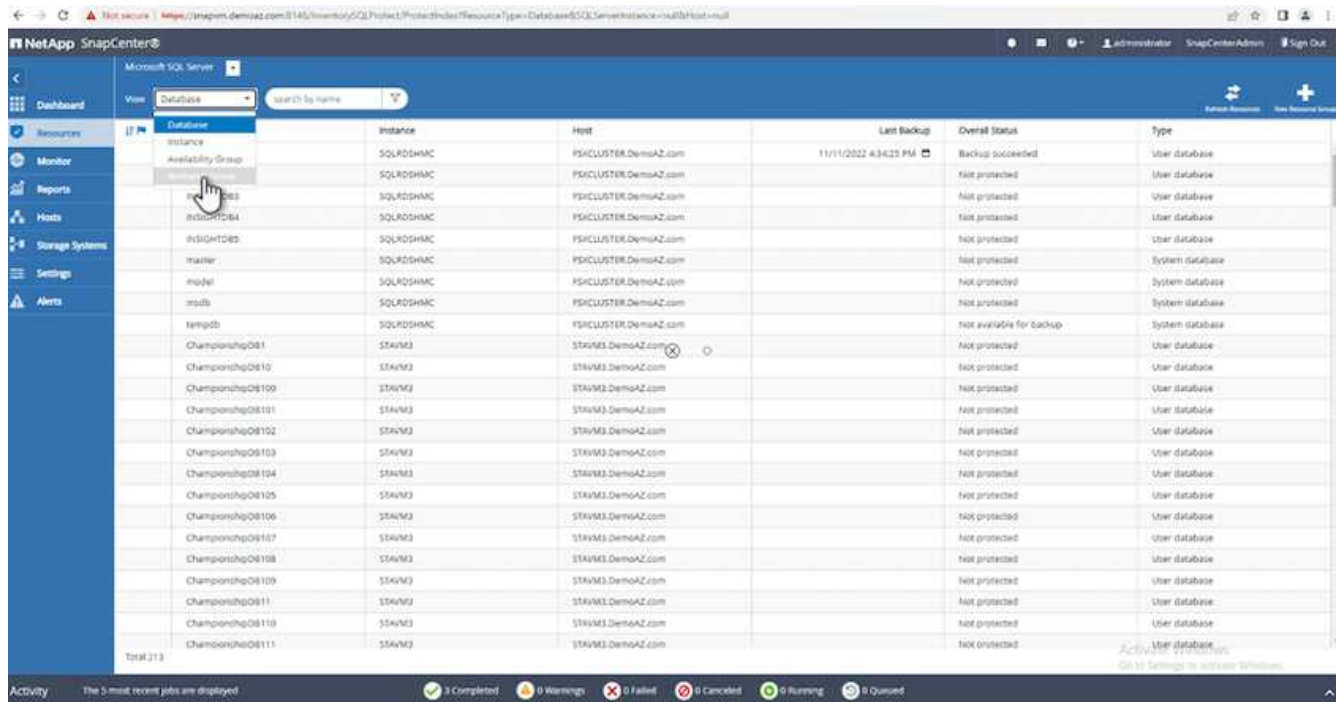


Wenn die Sicherung abgeschlossen ist, wird in der Topologieansicht ein neuer Eintrag angezeigt.

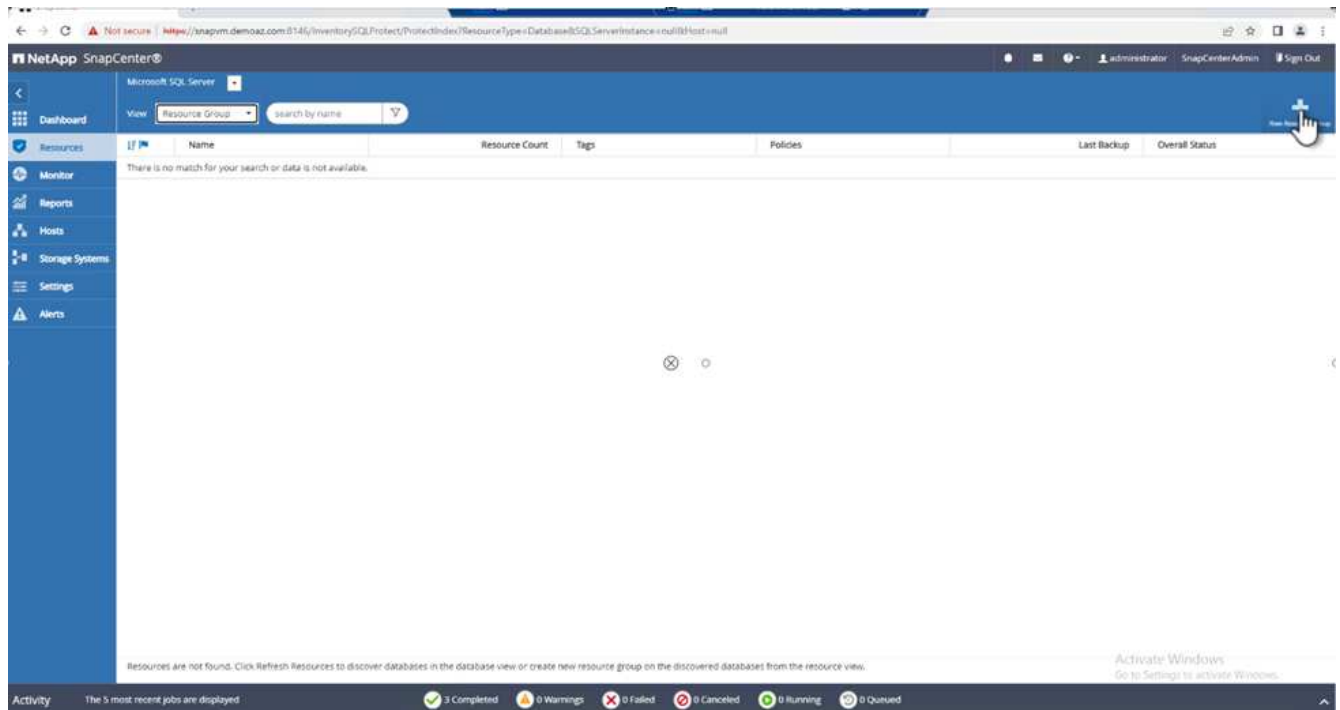
Backup-Vorgang für mehrere Datenbanken

Um eine Sicherungsrichtlinie für mehrere SQL Server-Datenbanken zu konfigurieren, erstellen Sie Richtlinien für Ressourcengruppen, indem Sie die folgenden Schritte ausführen:

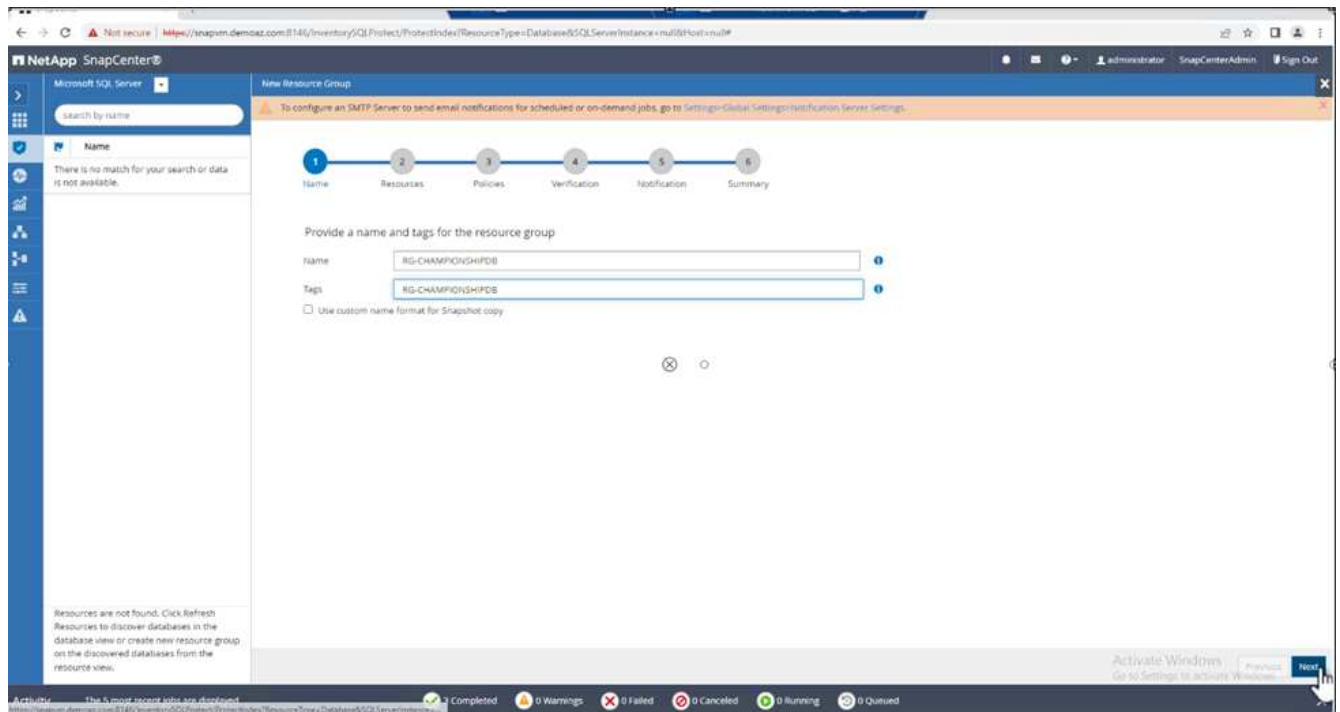
1. Wechseln Sie im Register **Ressourcen** aus dem Menü **Ansicht** über das Dropdown-Menü zu einer Ressourcengruppe.



2. Klicken Sie für eine neue Ressourcengruppe auf (+).

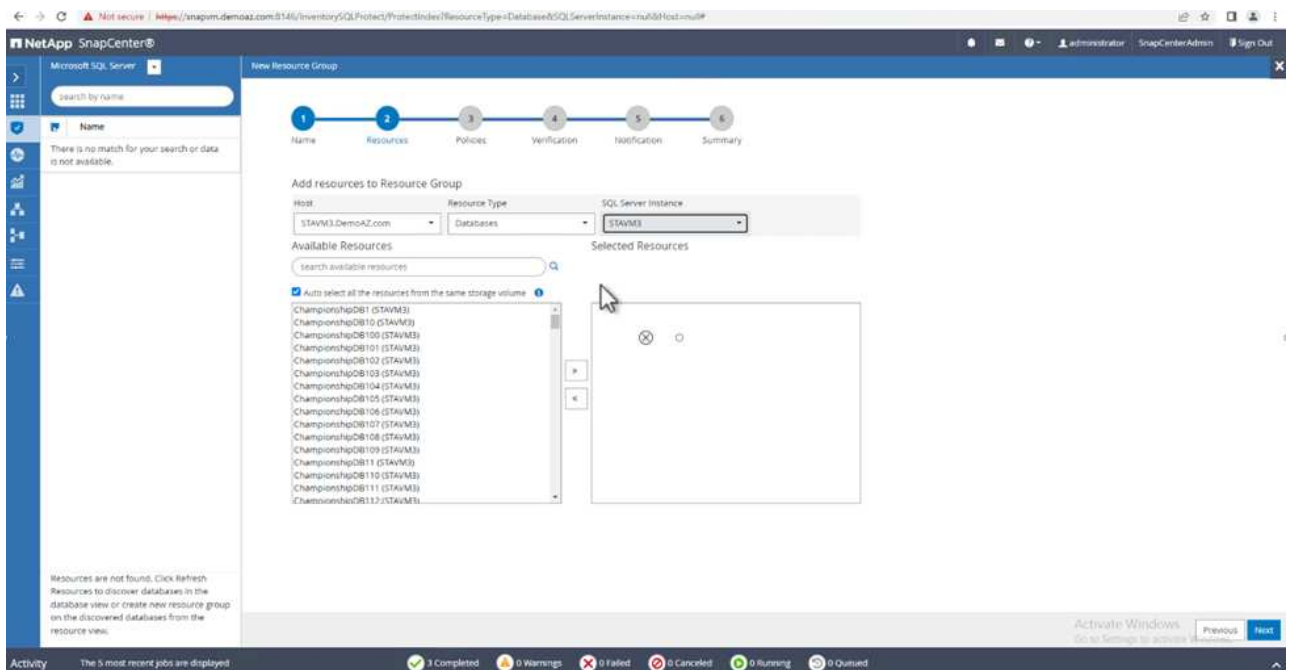


3. Geben Sie einen Namen und ein Tag an. Klicken Sie Auf **Weiter**.

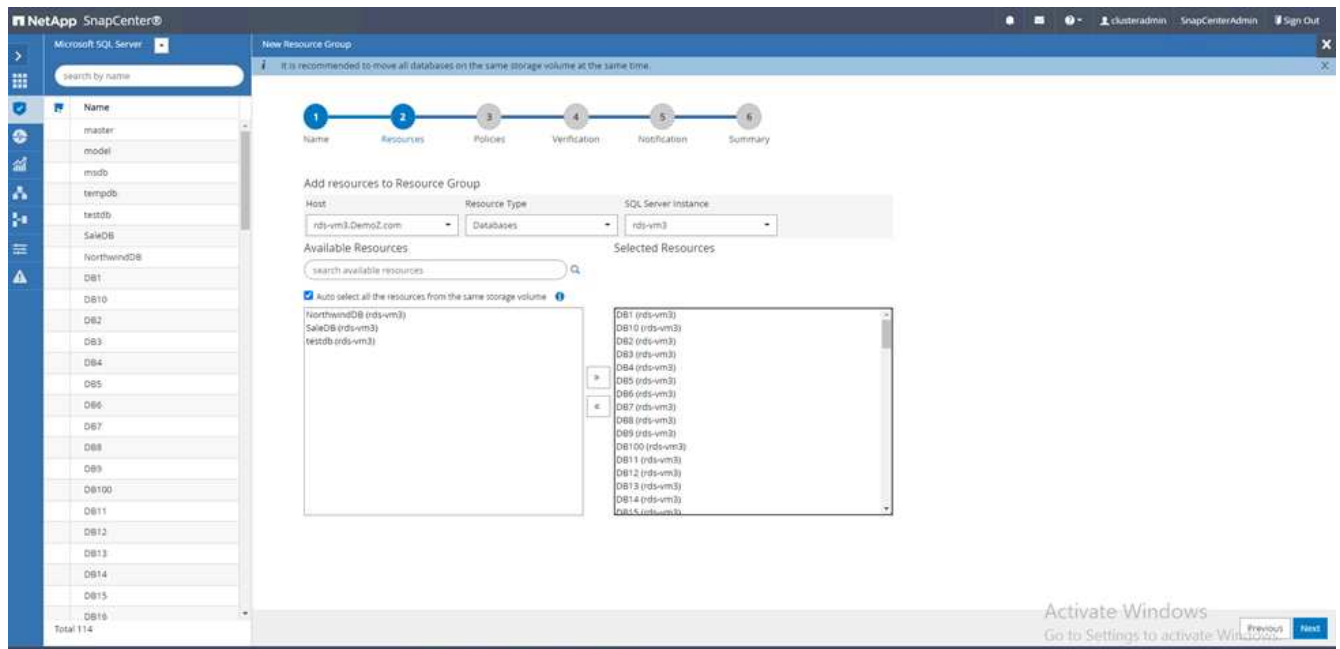


4. Ressourcen zur Ressourcengruppe hinzufügen:

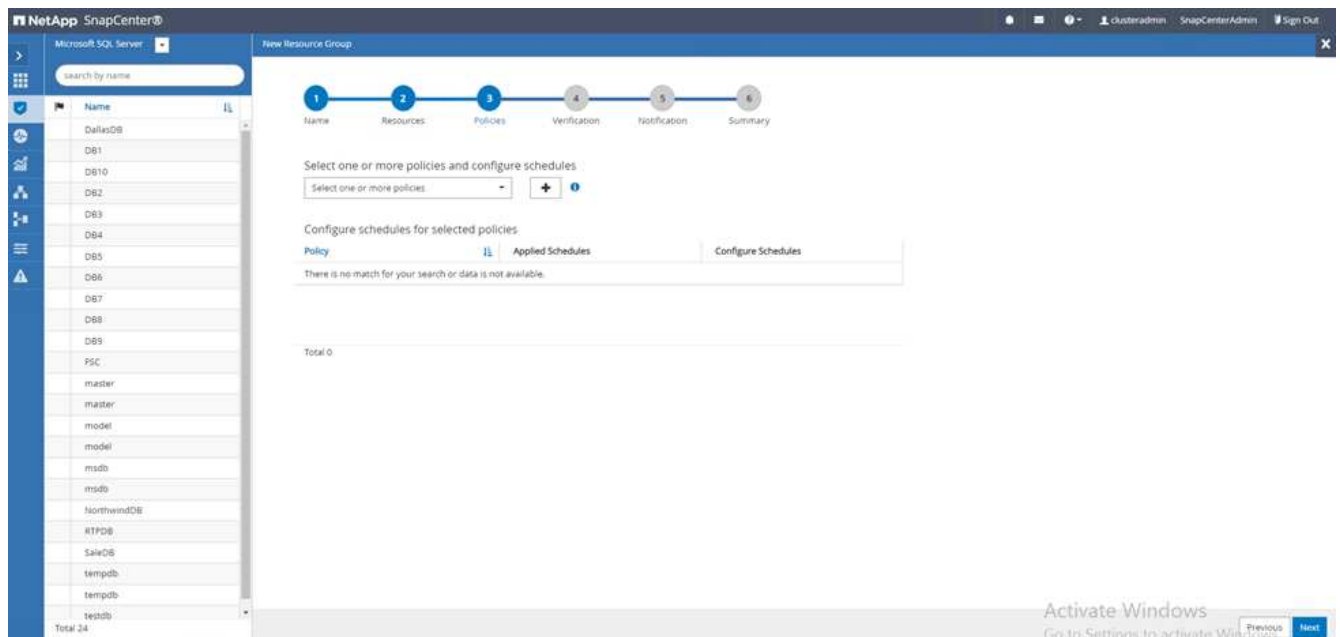
- **Host.** Wählen Sie den Server aus dem Dropdown-Menü, das die Datenbank hostet.
- **Ressourcentyp.** Wählen Sie aus dem Dropdown-Menü **Datenbank**.
- **SQL Server-Instanz.** Wählen Sie den Server aus.



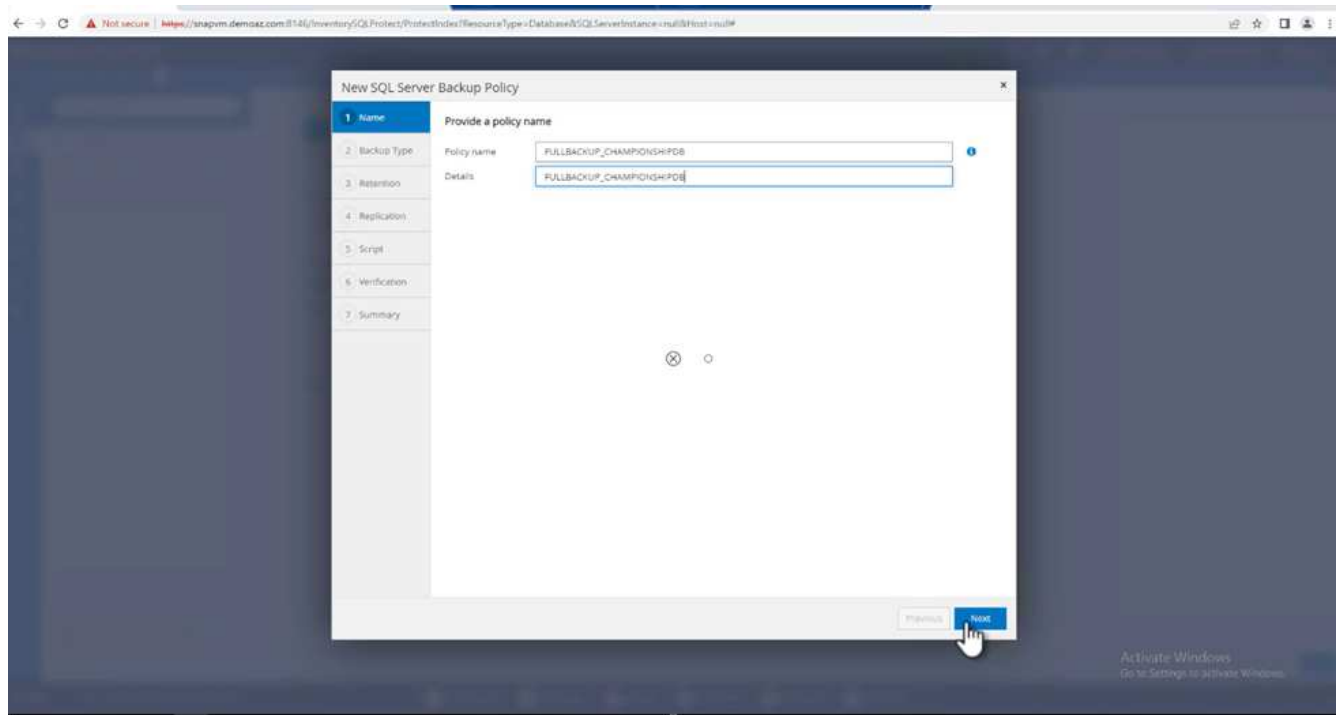
Die Option **Option Auto** wählt alle Ressourcen aus demselben Speichervolume aus* ist standardmäßig ausgewählt. Deaktivieren Sie die Option und wählen Sie nur die Datenbanken aus, die Sie der Ressourcengruppe hinzufügen möchten. Klicken Sie auf den Pfeil, den Sie hinzufügen möchten, und klicken Sie auf **Weiter**.



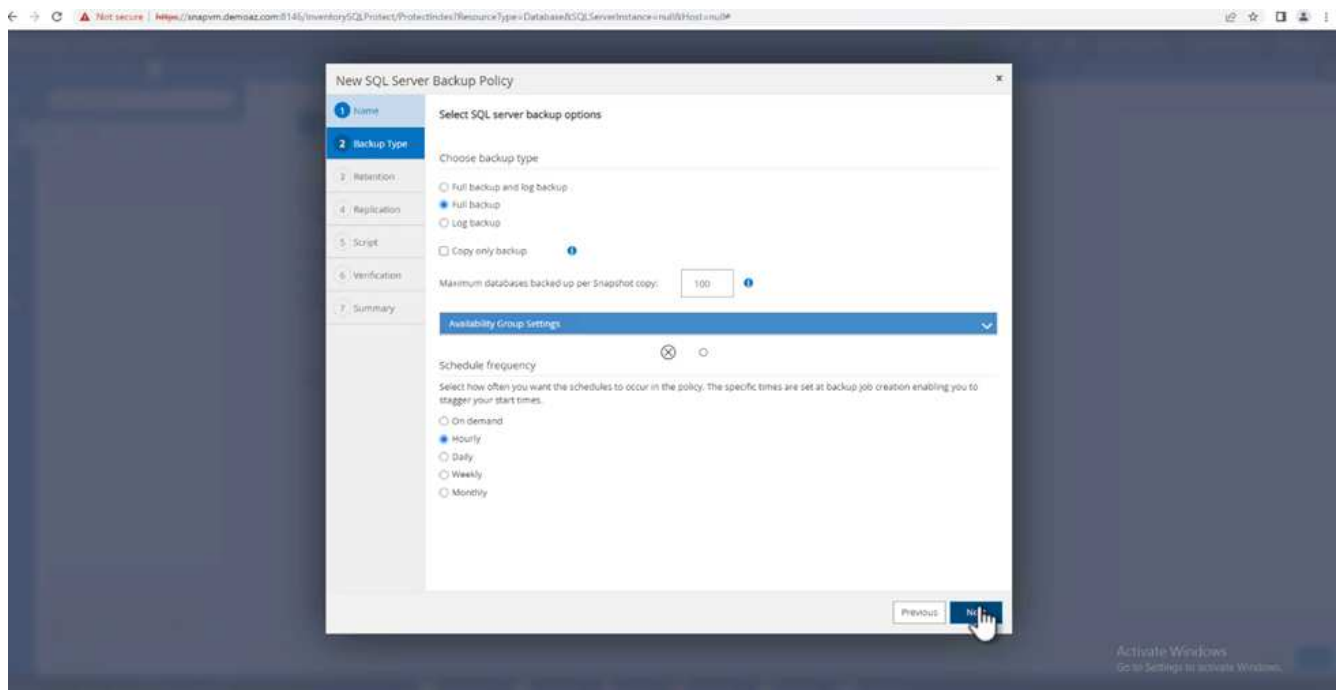
5. Klicken Sie in den Richtlinien auf (+).



6. Geben Sie den Richtliniennamen der Ressourcengruppe ein.



7. Wählen Sie **Full Backup** und die Zeitplanhäufigkeit je nach SLA Ihres Unternehmens.



8. Konfigurieren Sie die Aufbewahrungseinstellungen.

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention**
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

Keep log backups applicable to last full backups

Keep log backups applicable to last days

Full backup retention settings ⓘ

Weekly

Total Snapshot copies to keep

Keep Snapshot copies for days

9. Konfigurieren der Replikationsoptionen.

New SQL Server Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label ⓘ

Error retry count ⓘ

10. Konfigurieren Sie die Skripte, die vor der Durchführung eines Backups ausgeführt werden sollen. Klicken Sie Auf **Weiter**.

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script**
- 6 Verification
- 7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout secs

11. Bestätigen Sie die Verifizierung für die folgenden Backup-Pläne.

New SQL Server Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

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

Hourly

Database consistency checks options

Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)

Suppress all information message (NO_INFOMSGS)

Display all reported error messages per object (ALL_ERRORMSG5)

Do not check non-clustered indexes (NOINDEX)

Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Verification script settings ?

Script timeout SECS

Prescript full path

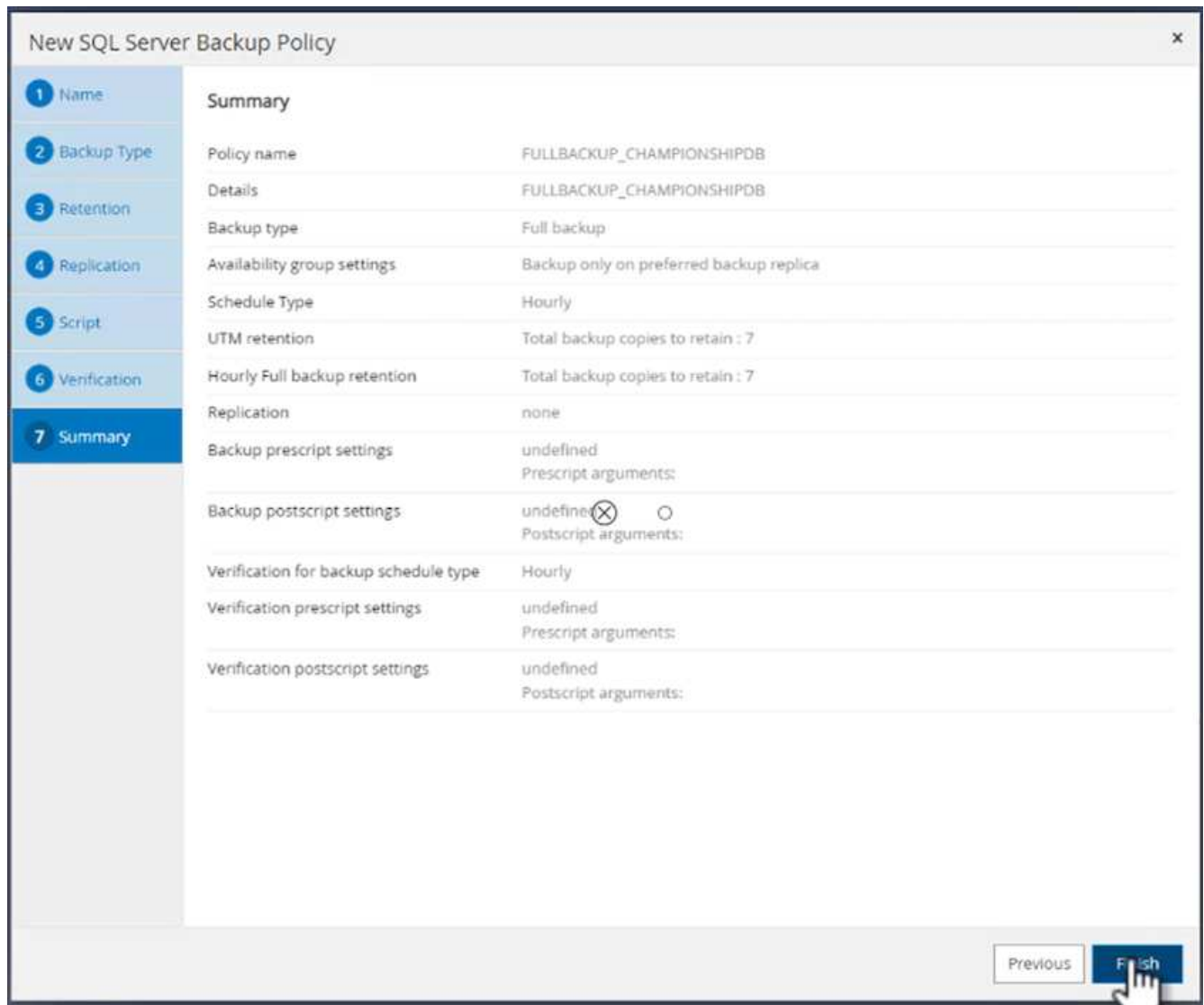
Prescript arguments

Postscript full path

Postscript arguments

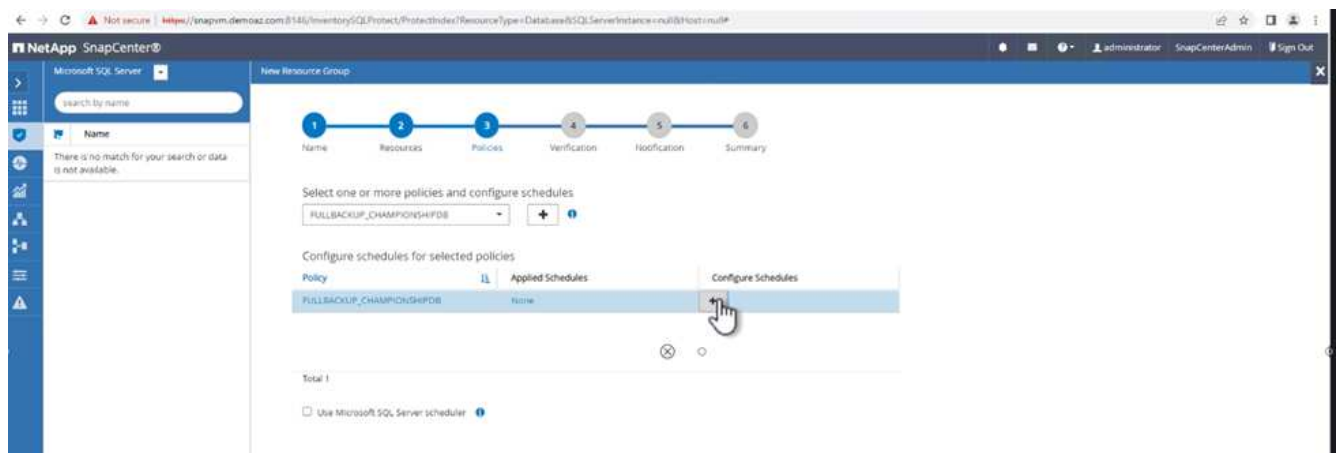
Previous Next

12. Überprüfen Sie auf der Seite **Summary** die Informationen, und klicken Sie auf **Finish**.



Konfigurieren und sichern Sie mehrere SQL Server-Datenbanken

1. Klicken Sie auf das (+)-Zeichen, um das Startdatum und das Ablaufdatum zu konfigurieren.



2. Stellen Sie die Uhrzeit ein.

Add schedules for policy FULLBACKUP_CHAMPIONSHIPDB



Hourly

Start date

11/11/2022 05:30 pm



Expires on

12/11/2022 05:27 pm



Repeat every

1



hours

0

mins



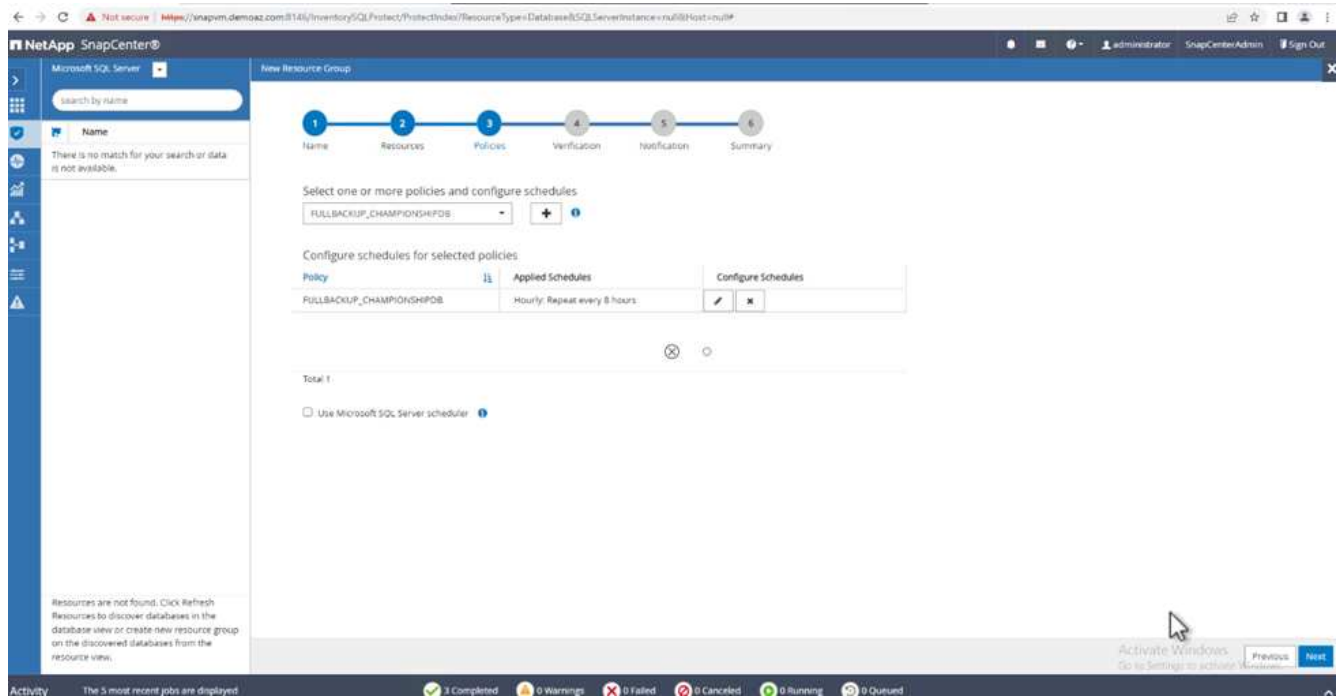
The schedules are triggered in the SnapCenter Server time zone.



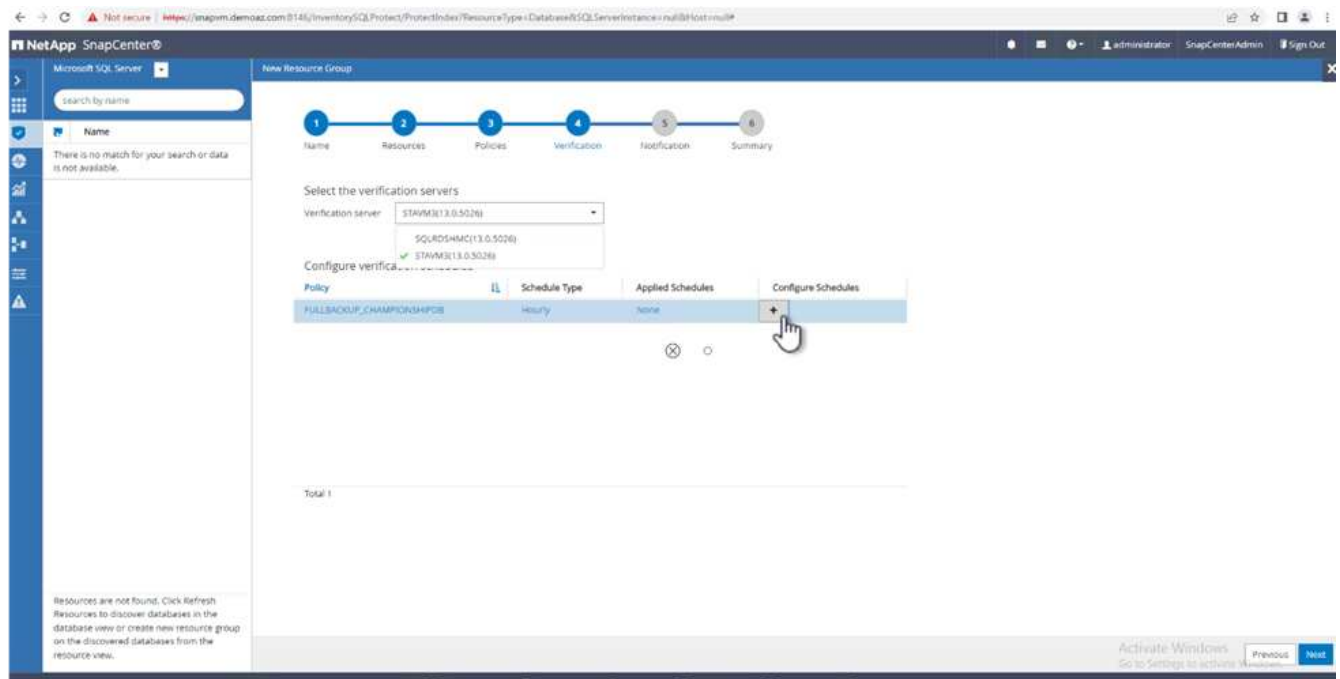
Cancel

OK

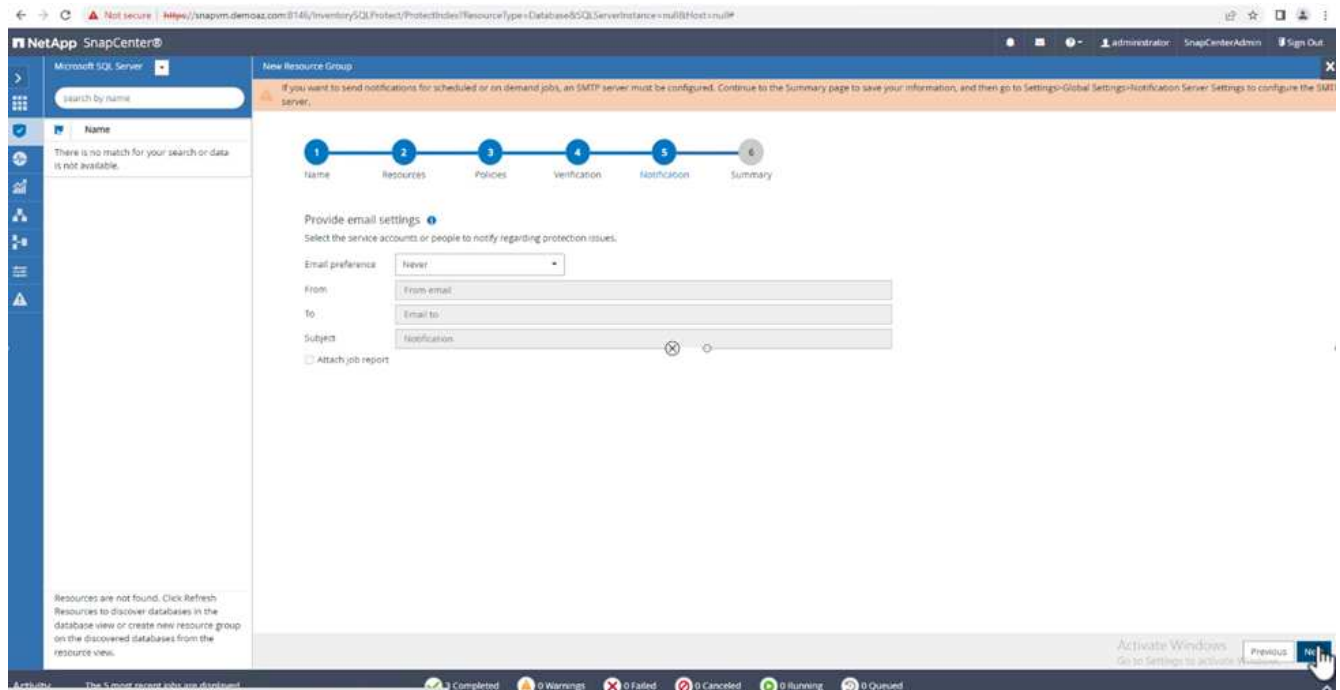




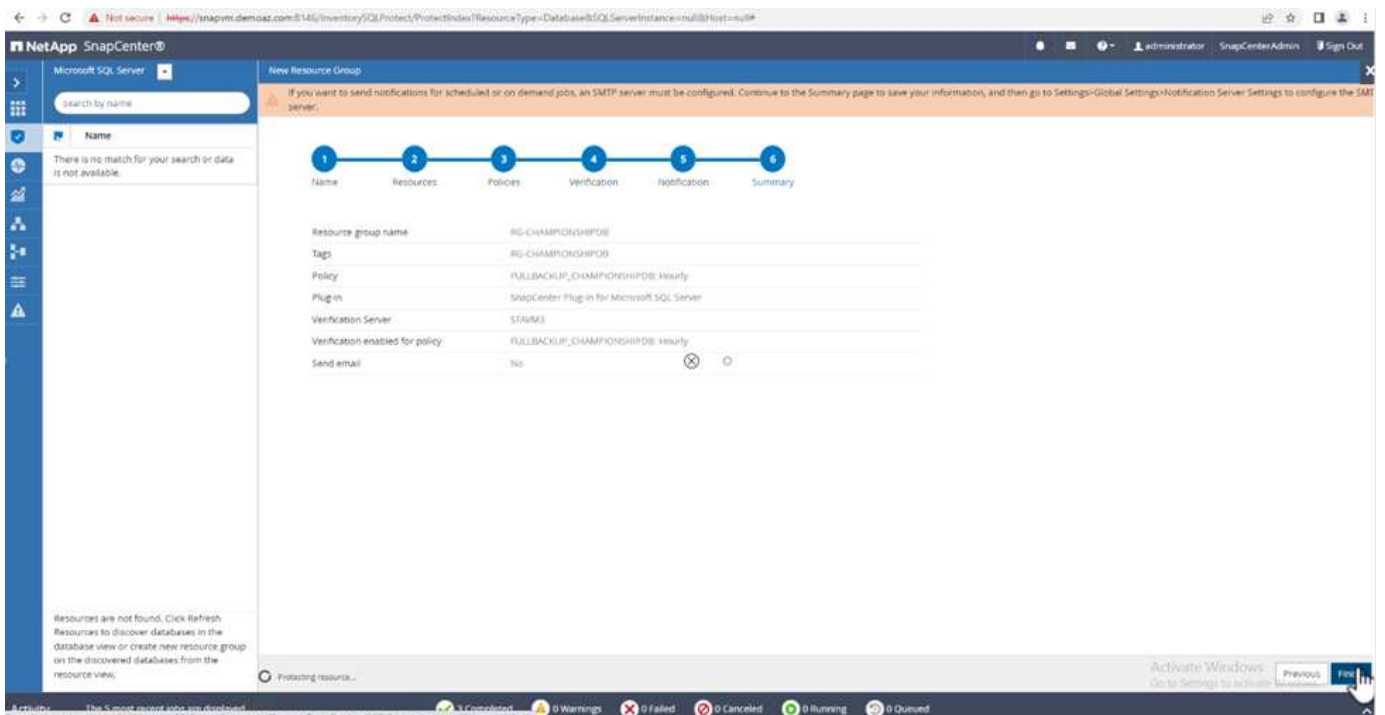
3. Wählen Sie auf der Registerkarte **Verifizierung** den Server aus, konfigurieren Sie den Zeitplan und klicken Sie auf **Weiter**.



4. Konfigurieren Sie Benachrichtigungen zum Senden einer E-Mail.

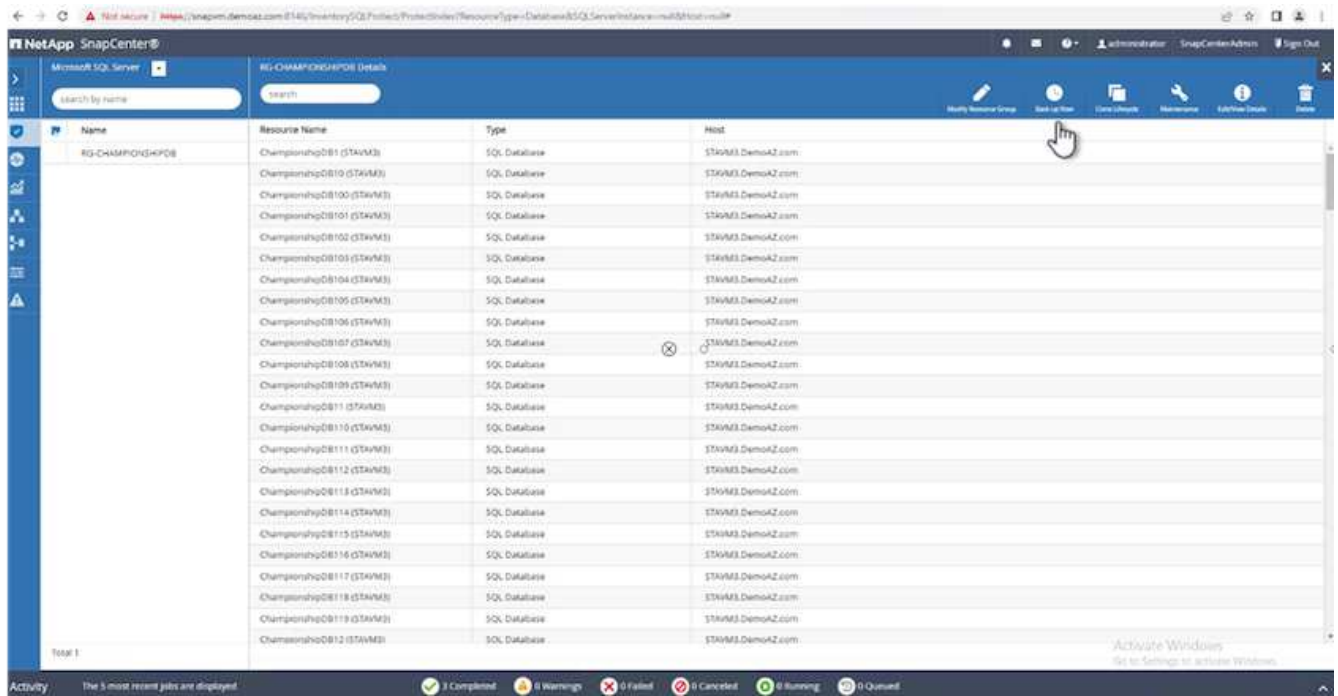


Die Richtlinie ist jetzt für das Backup mehrerer SQL Server-Datenbanken konfiguriert.



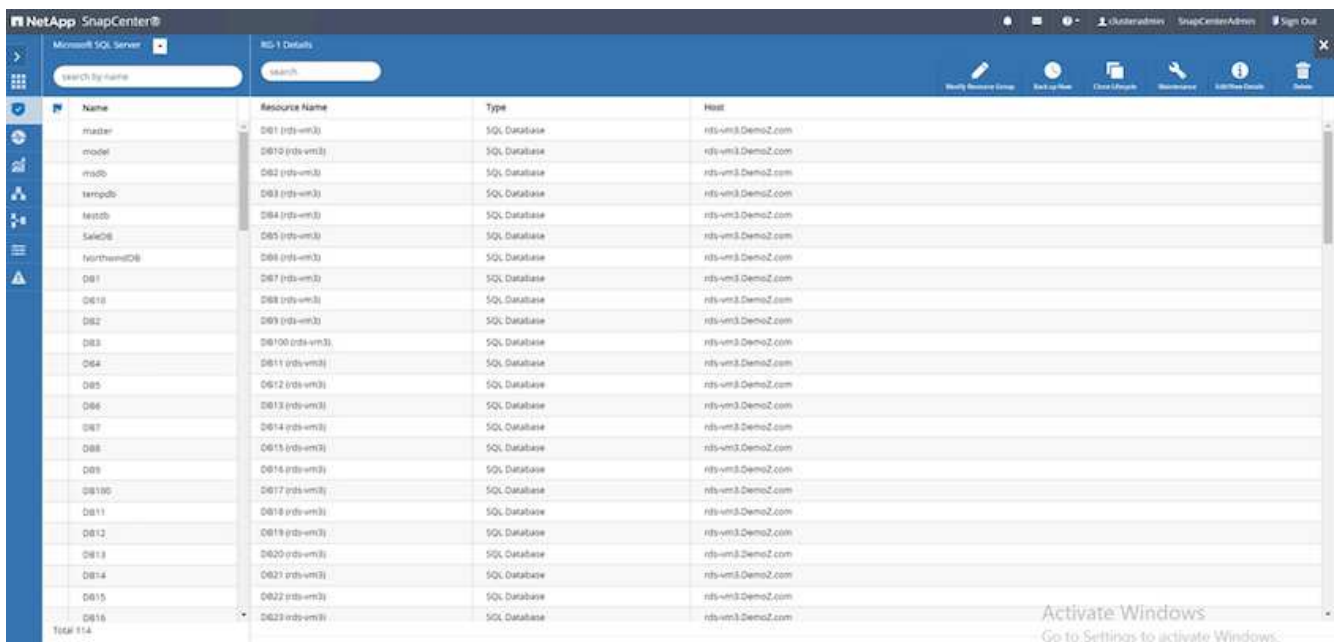
On-Demand-Backups für mehrere SQL Server-Datenbanken werden ausgelöst

1. Wählen Sie auf der Registerkarte **Ressource** die Option Ansicht. Wählen Sie im Dropdown-Menü **Ressourcengruppe** aus.

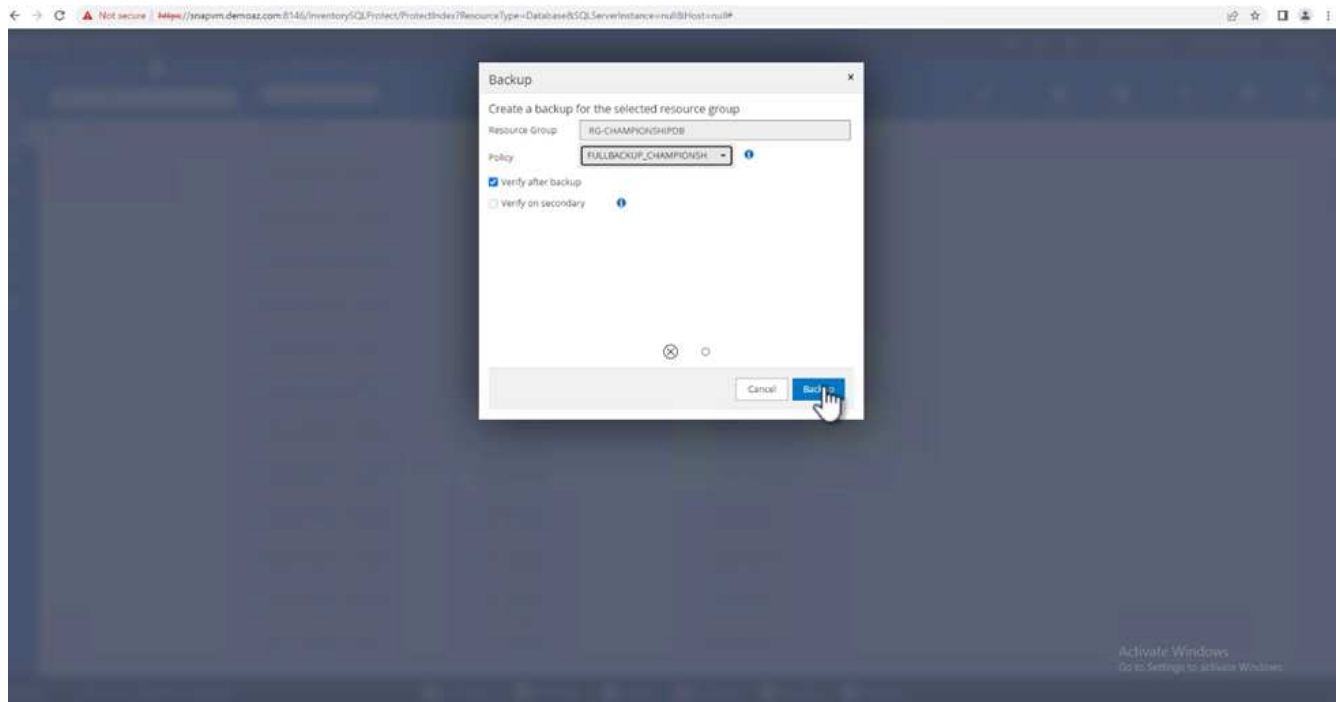


2. Wählen Sie den Namen der Ressourcengruppe aus.

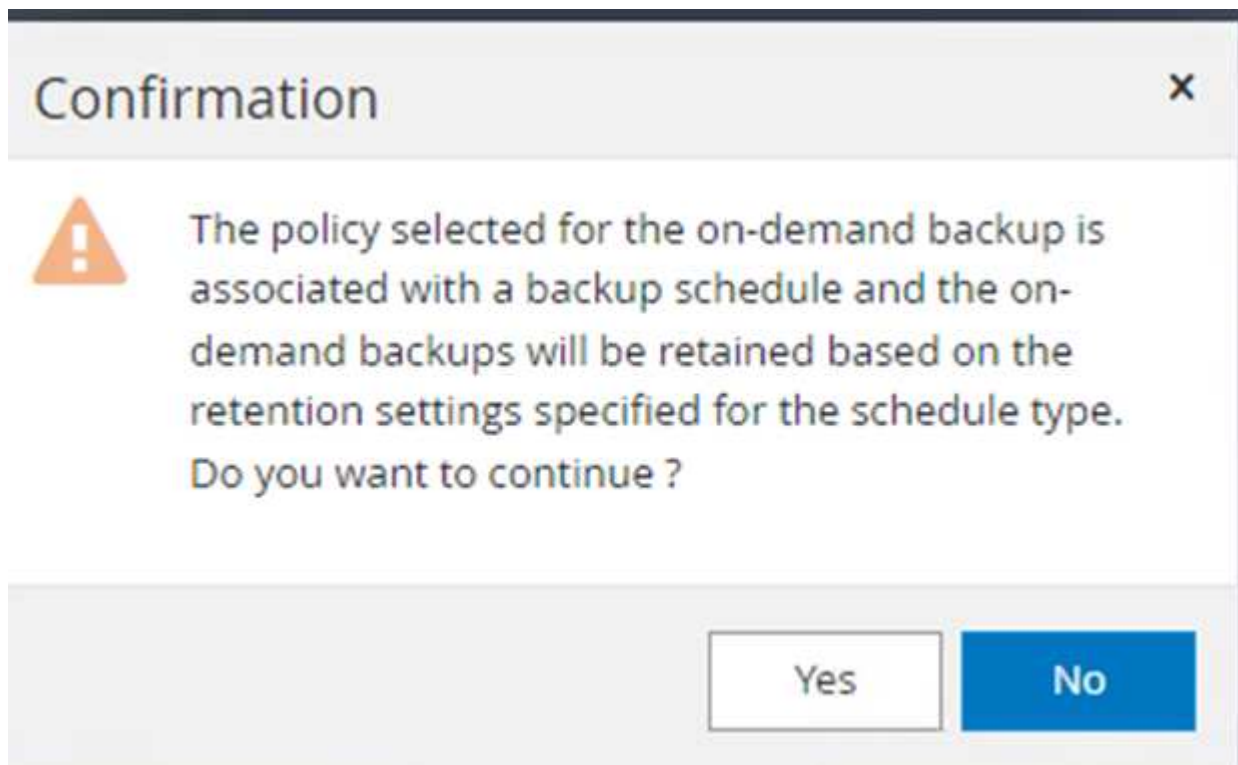
3. Klicken Sie oben rechts auf **Backup now**.



4. Ein neues Fenster wird geöffnet. Klicken Sie auf das Kontrollkästchen **nach Sicherung prüfen** und dann auf Sicherung.



5. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie Auf **Ja**.

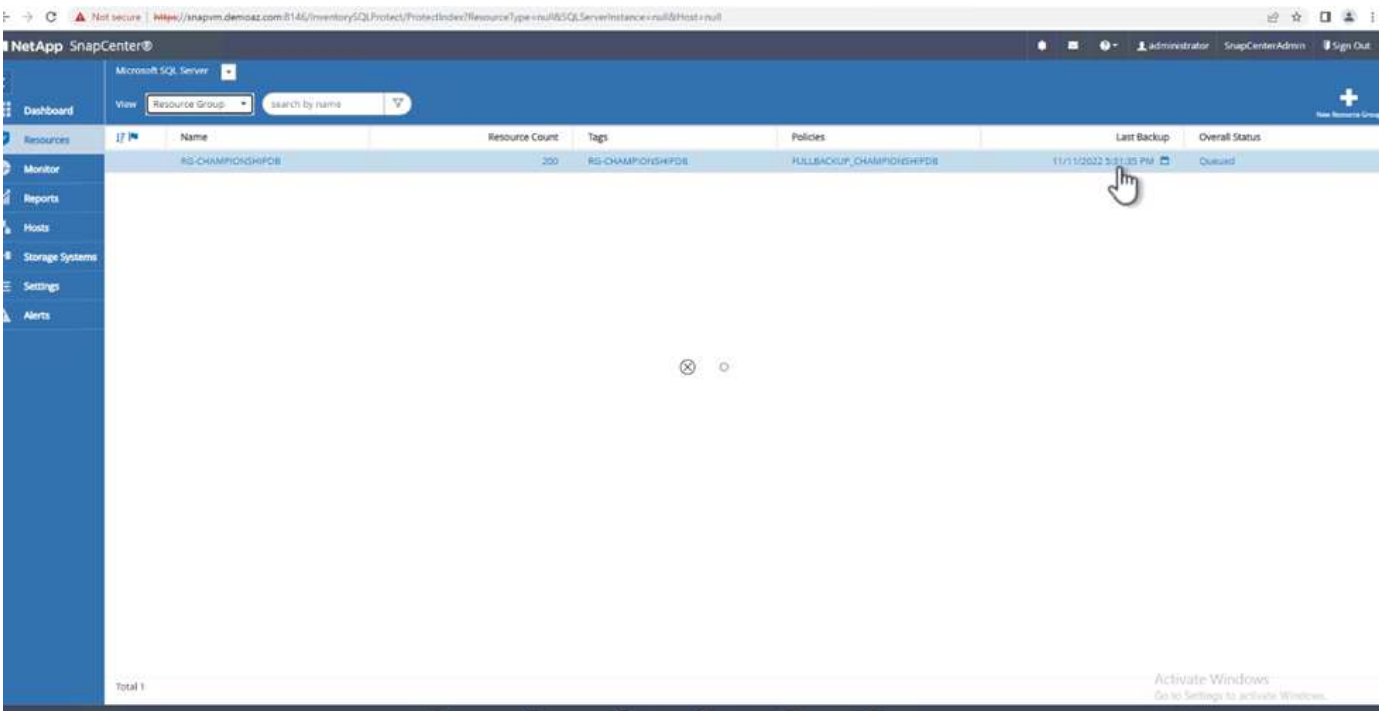


Überwachen von Backup-Jobs für mehrere Datenbanken

Klicken Sie in der linken Navigationsleiste auf **Monitor**, wählen Sie den Sicherungsauftrag aus und klicken Sie auf **Details**, um den Auftragsfortschritt anzuzeigen.



Klicken Sie auf die Registerkarte **Ressource**, um die Zeit anzuzeigen, die für den Abschluss der Sicherung benötigt wird.

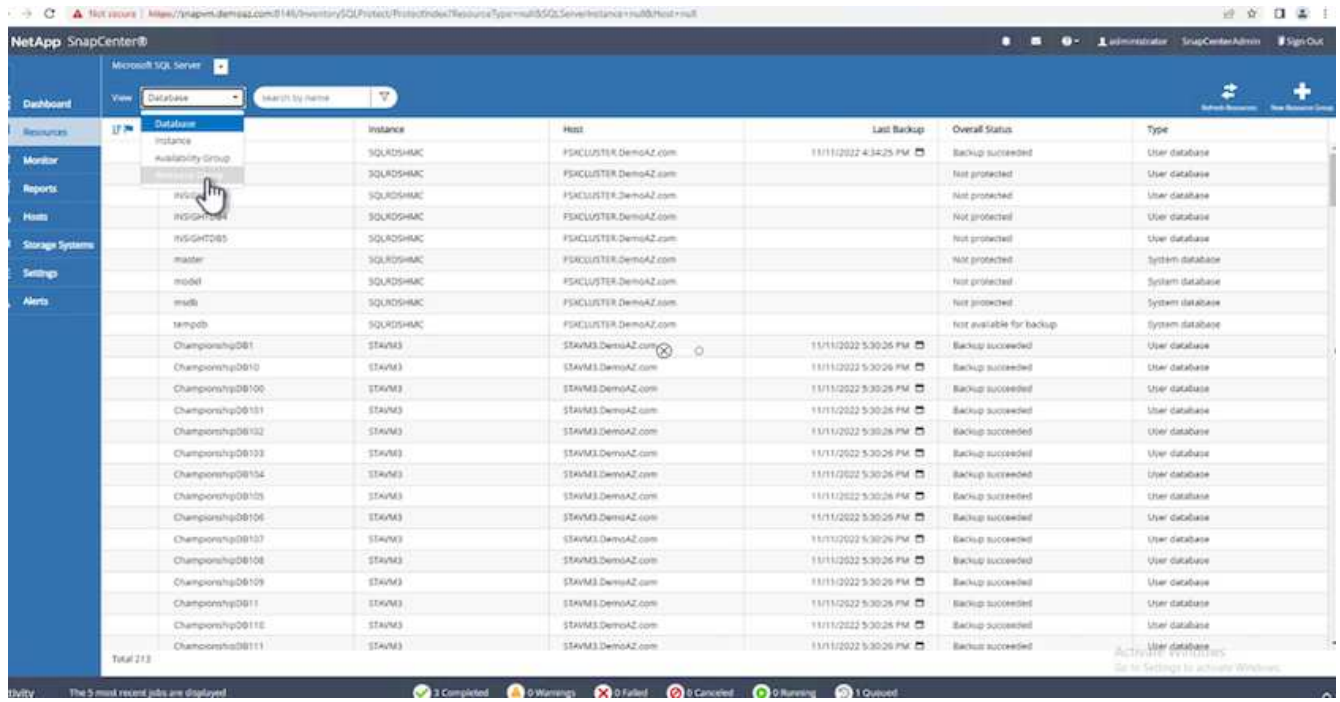


Transaktions-Log-Backup für mehrere Datenbank-Backups

SnapCenter unterstützt die vollständigen, überzeichneten und einfachen Wiederherstellungsmodelle. Der einfache Wiederherstellungsmodus unterstützt keine Sicherung von Transaktionsprotokollen.

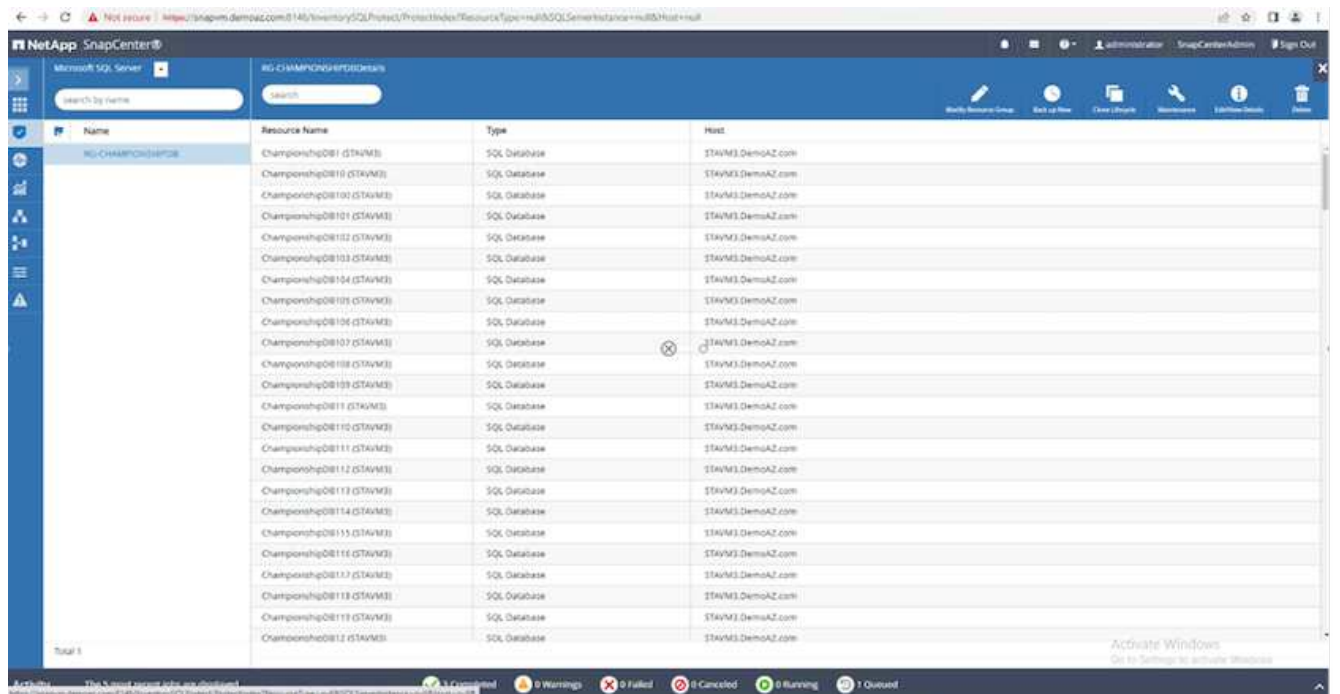
Führen Sie die folgenden Schritte aus, um ein Backup des Transaktionsprotokolls durchzuführen:

1. Ändern Sie auf der Registerkarte **Ressourcen** das Ansichtsmenü von **Datenbank** in **Ressourcengruppe**.



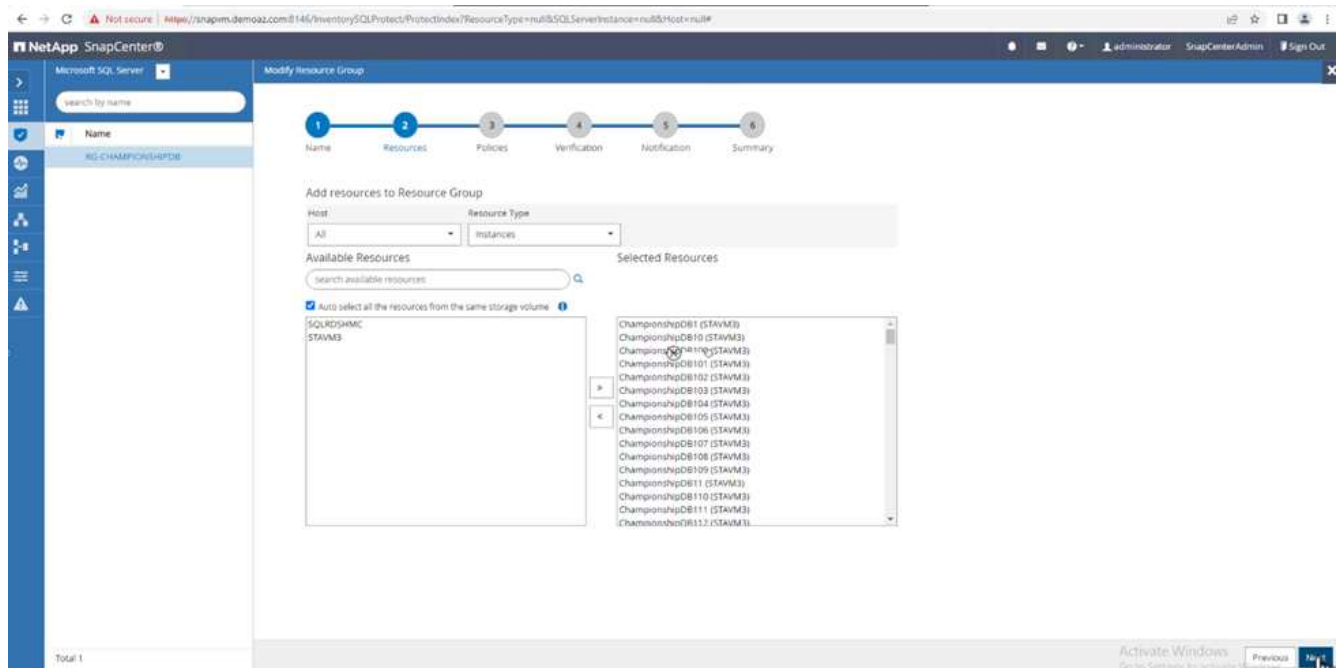
2. Wählen Sie die erstellte Richtlinie für die Ressourcengruppe aus.

3. Wählen Sie oben rechts **Ressourcengruppe ändern**.

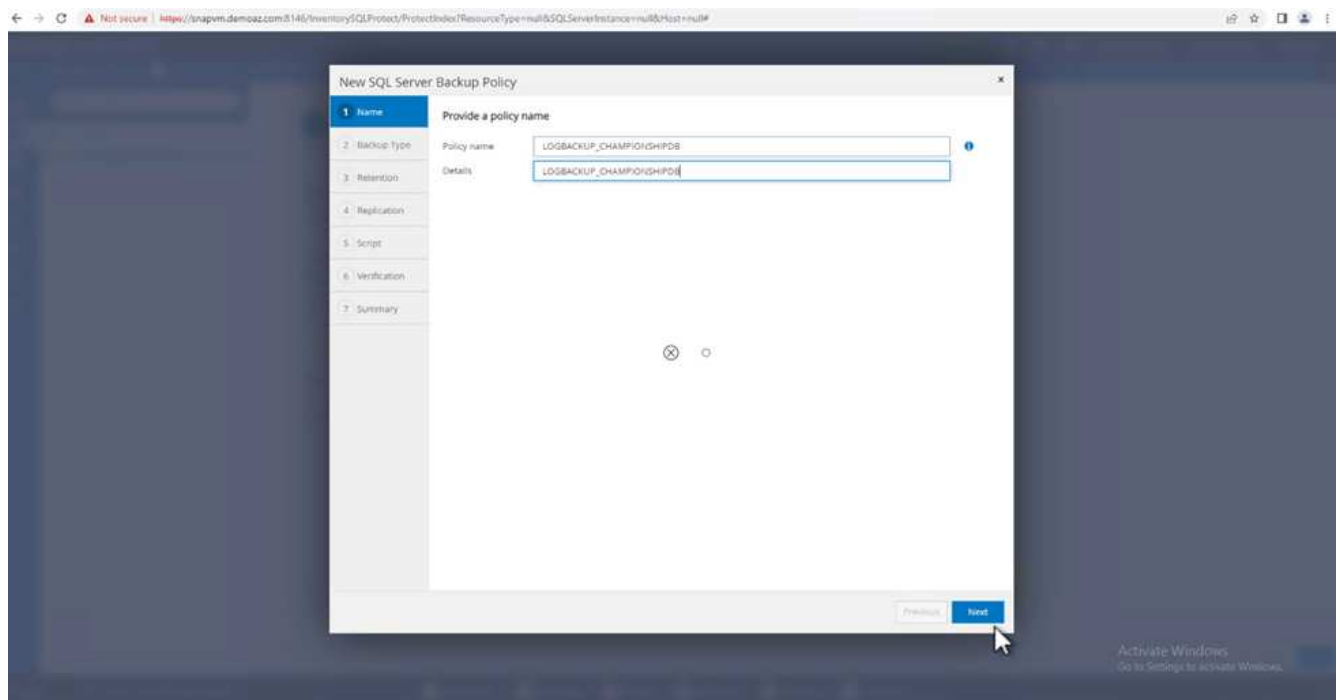


4. Im Abschnitt **Name** werden standardmäßig der Name und das Tag der Sicherungsrichtlinie angegeben. Klicken Sie Auf **Weiter**.

Auf der Registerkarte **Resources** werden die Basen hervorgehoben, für die die Backup-Policy für Transaktionen konfiguriert werden soll.



5. Geben Sie den Richtliniennamen ein.



6. Wählen Sie die SQL Server-Backup-Optionen aus.

7. Wählen Sie Protokollsicherung.

8. Legen Sie das Zeitplanintervall auf der Grundlage der RTO Ihres Unternehmens fest. Klicken Sie Auf **Weiter**.

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type**
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Select SQL server backup options

Choose backup type

Full backup and log backup

Full backup

Log backup

Copy only backup i

Maximum databases backed up per Snapshot copy: i

Availability Group Settings v

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

9. Konfigurieren Sie die Aufbewahrungseinstellungen für das Protokoll-Backup. Klicken Sie Auf **Weiter**.

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

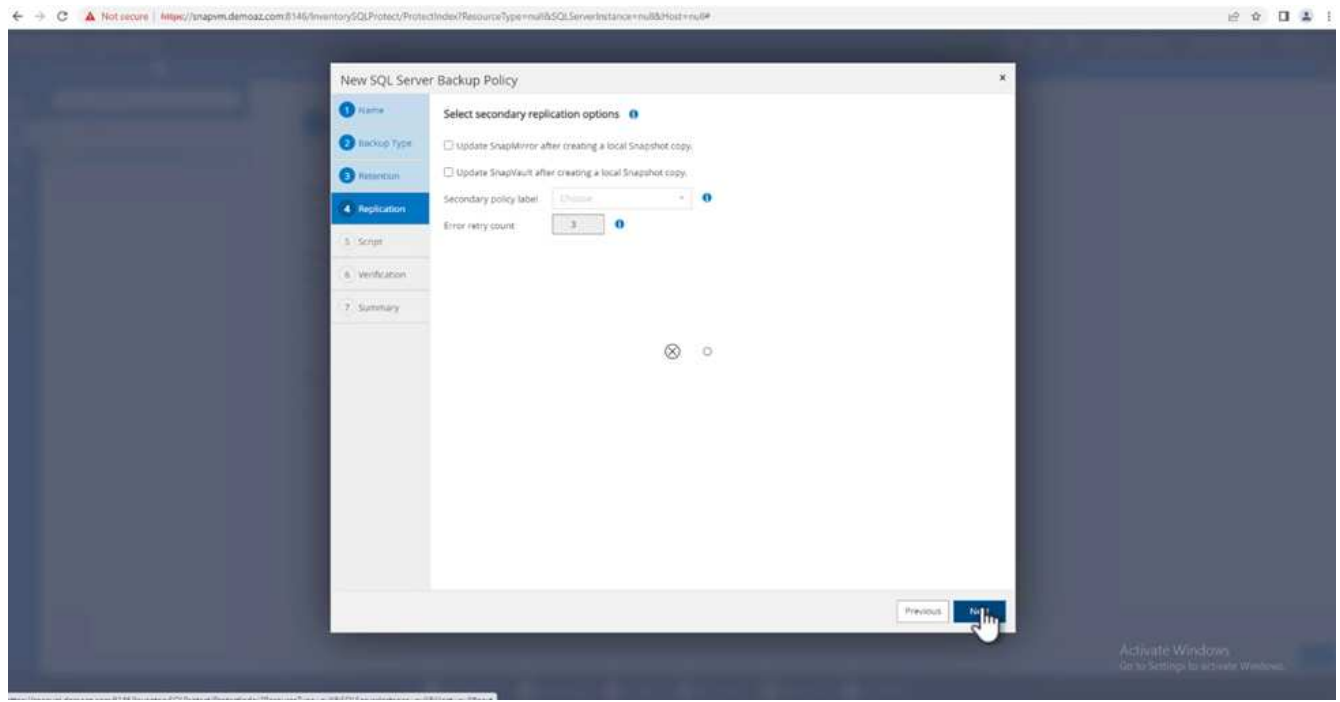
Log backup retention settings

Up-to-the-minute (UTM) retention settings retains log backups created as part of full backup and full and log backup operations. UTM retention settings also decides for how many full backups the log backups are to be retained. For example, if UTM retention settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained and the rest are deleted.

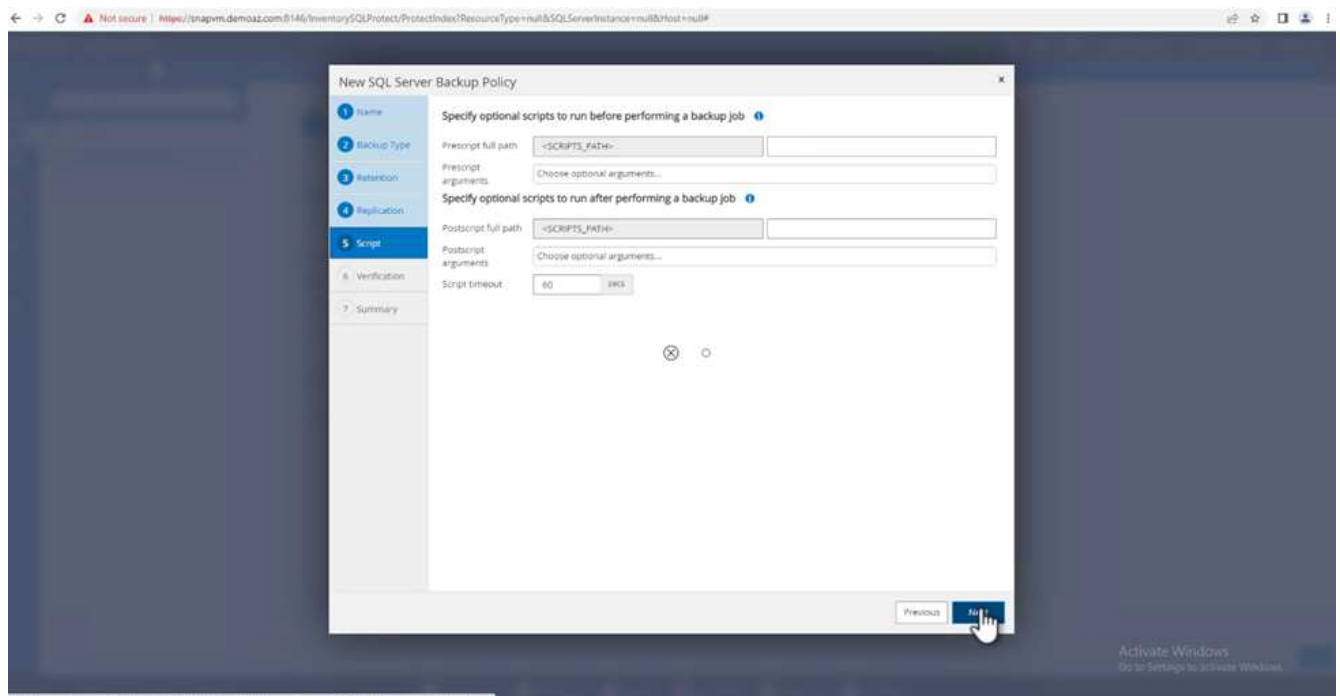
Previous

Next

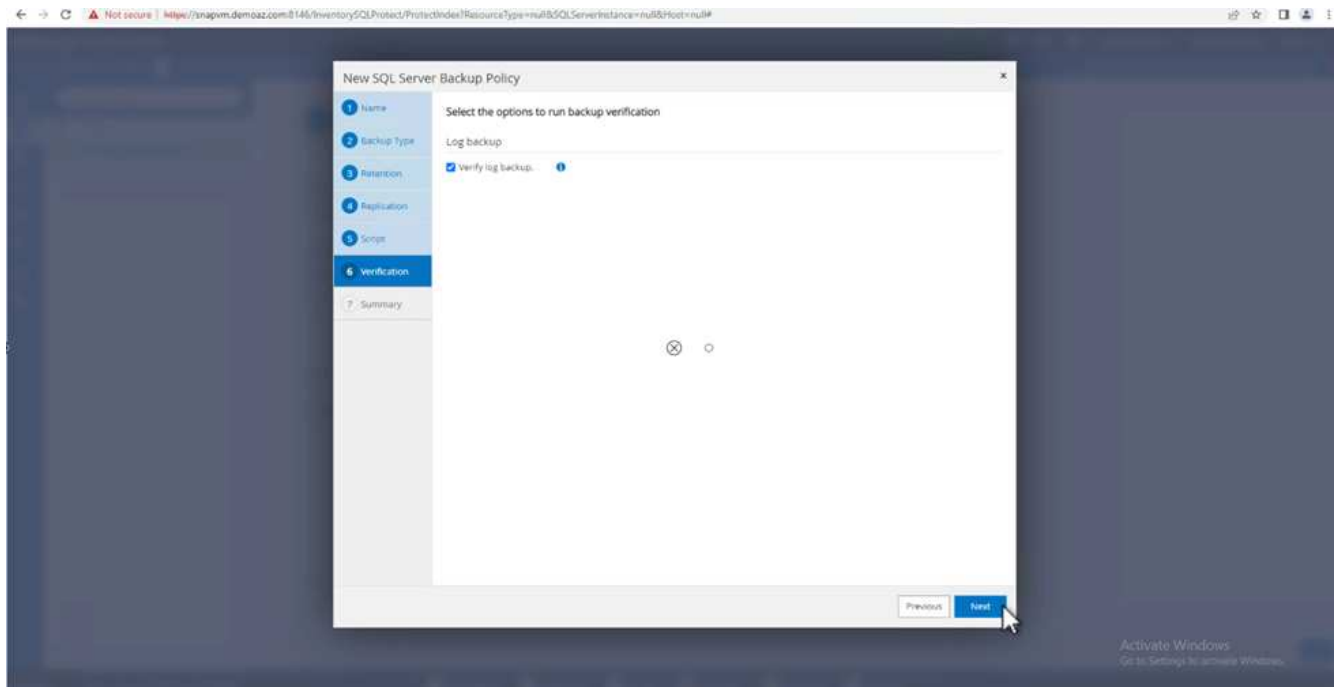
10. (Optional) Konfigurieren Sie die Replikationsoptionen.



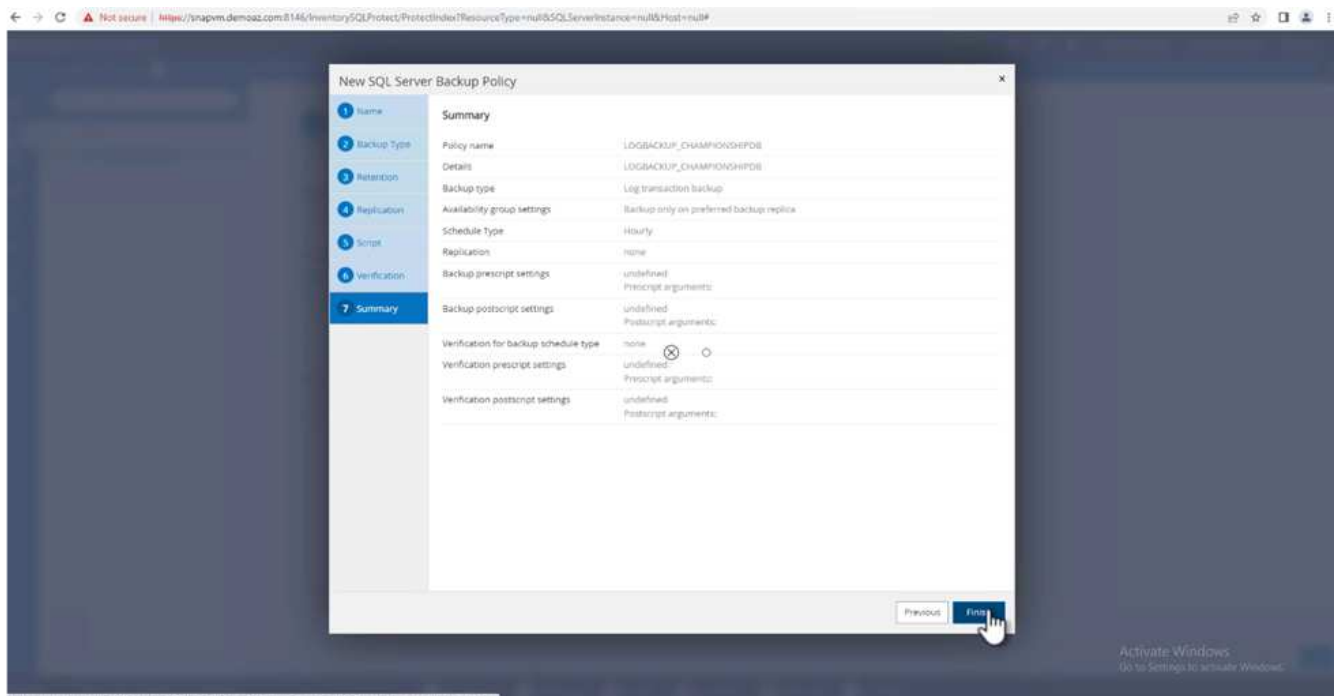
11. (Optional) Konfigurieren Sie alle Skripte, die ausgeführt werden sollen, bevor Sie einen Backupjob ausführen.



12. (Optional) Konfigurieren Sie die Backup-Verifikation.

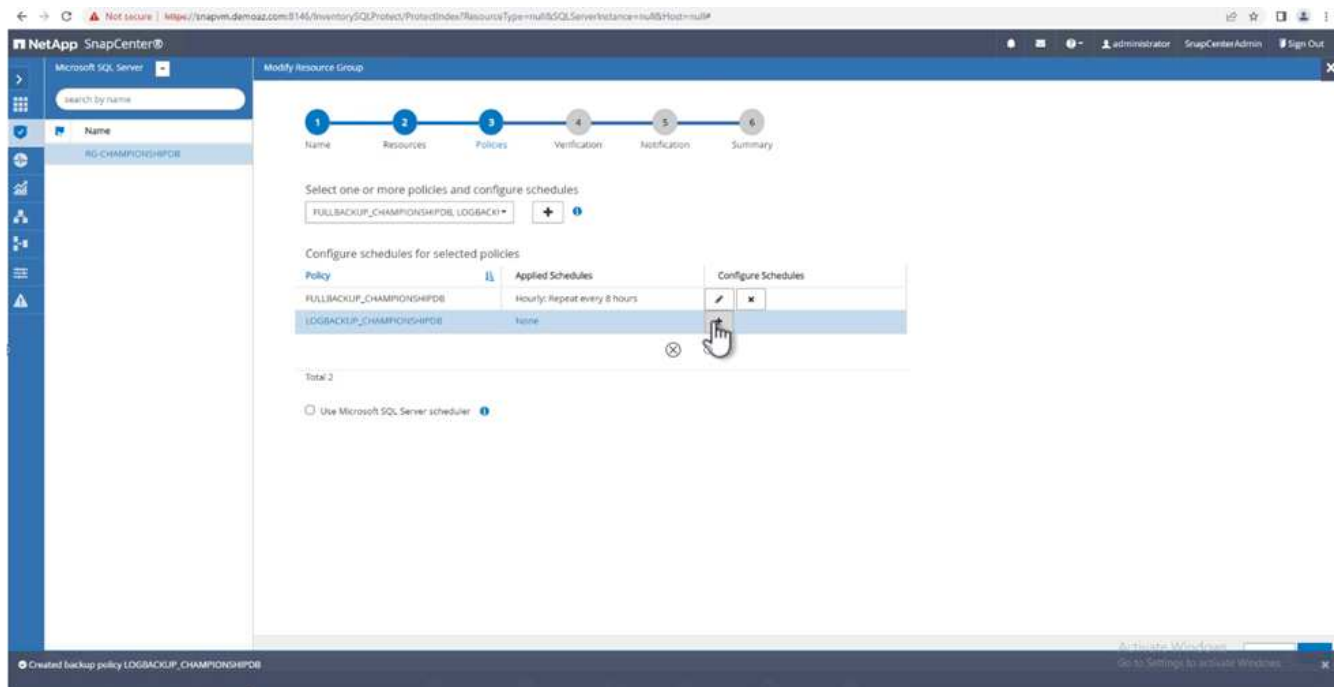


13. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertig stellen**.

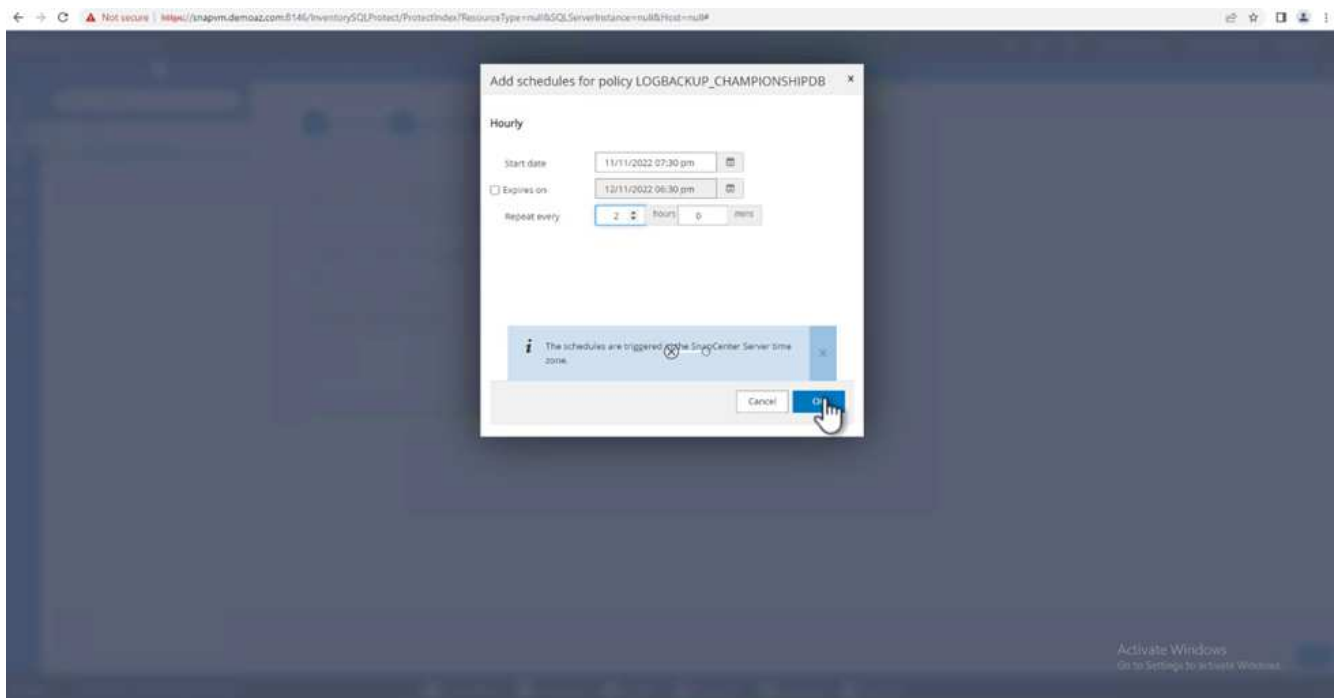


Konfiguration und Schutz mehrerer MSSQL Server-Datenbanken

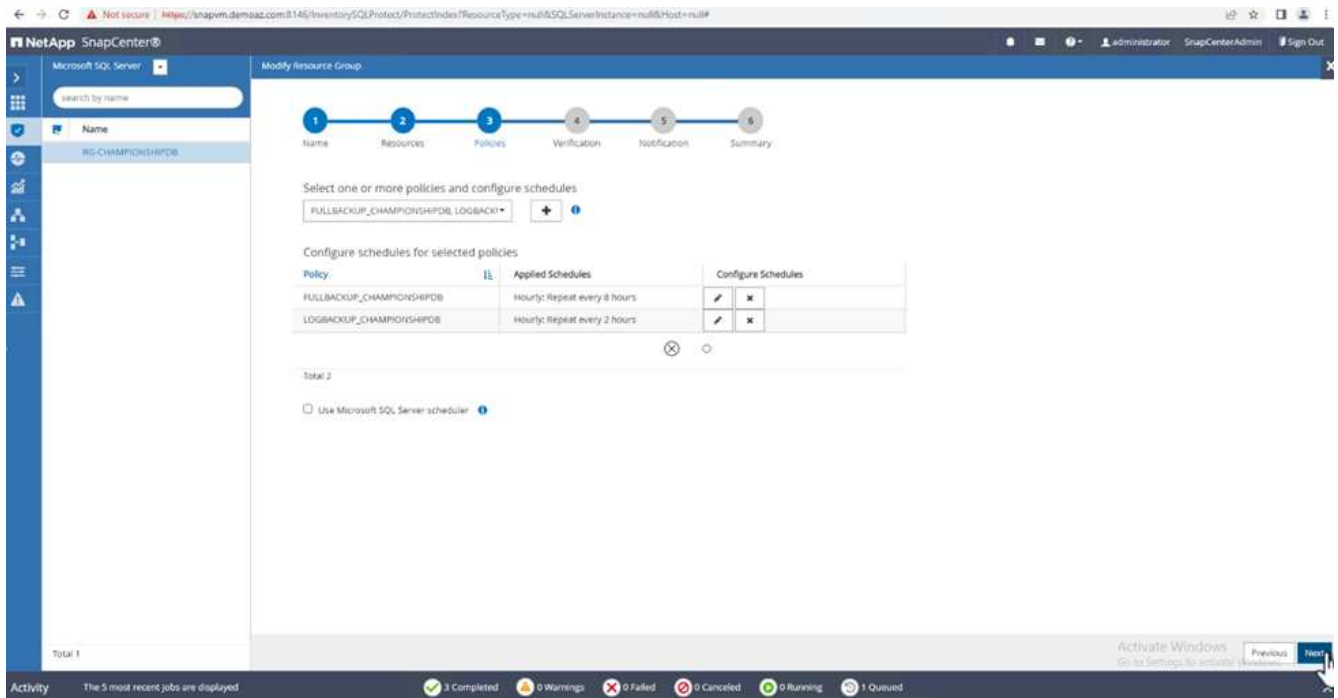
1. Klicken Sie auf die neu erstellte Backup-Richtlinie für das Transaktionsprotokoll.



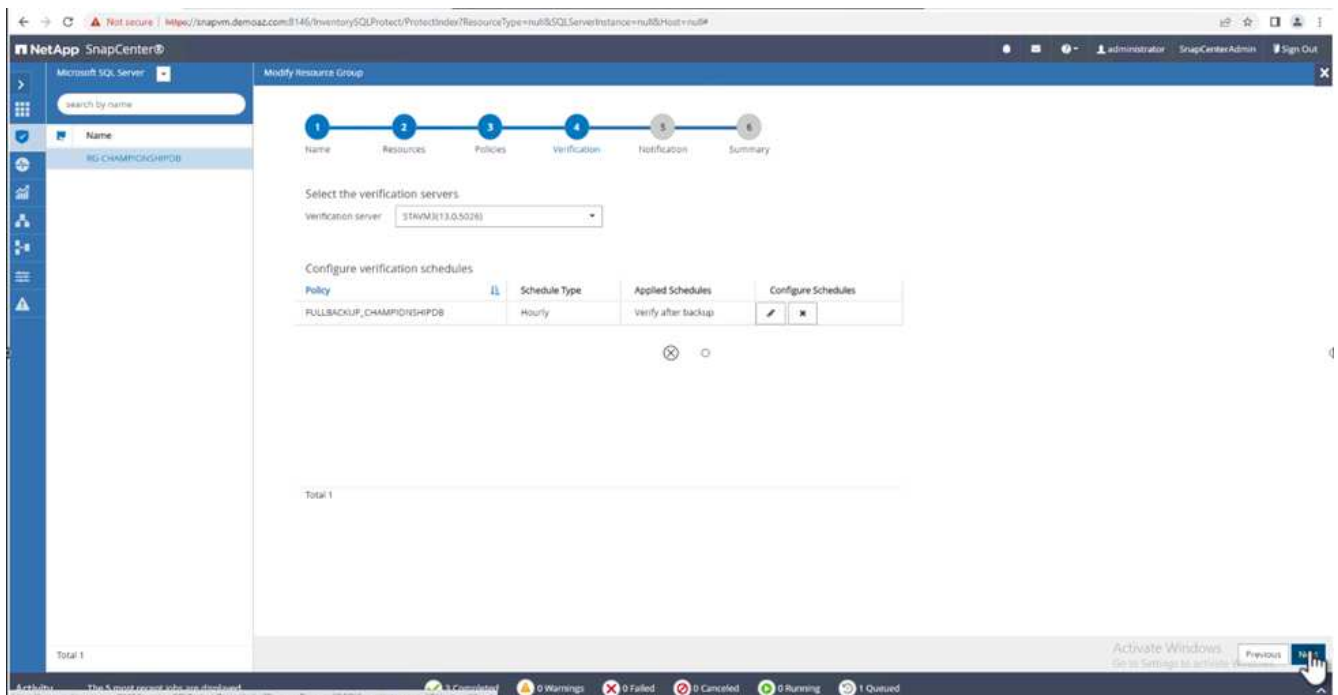
2. Stellen Sie das Datum **Start** und **läuft am** ein.
3. Geben Sie die Häufigkeit der Backup-Richtlinie für Protokolle in Abhängigkeit von SLA, RTP und RPO ein. Klicken Sie auf **OK**.



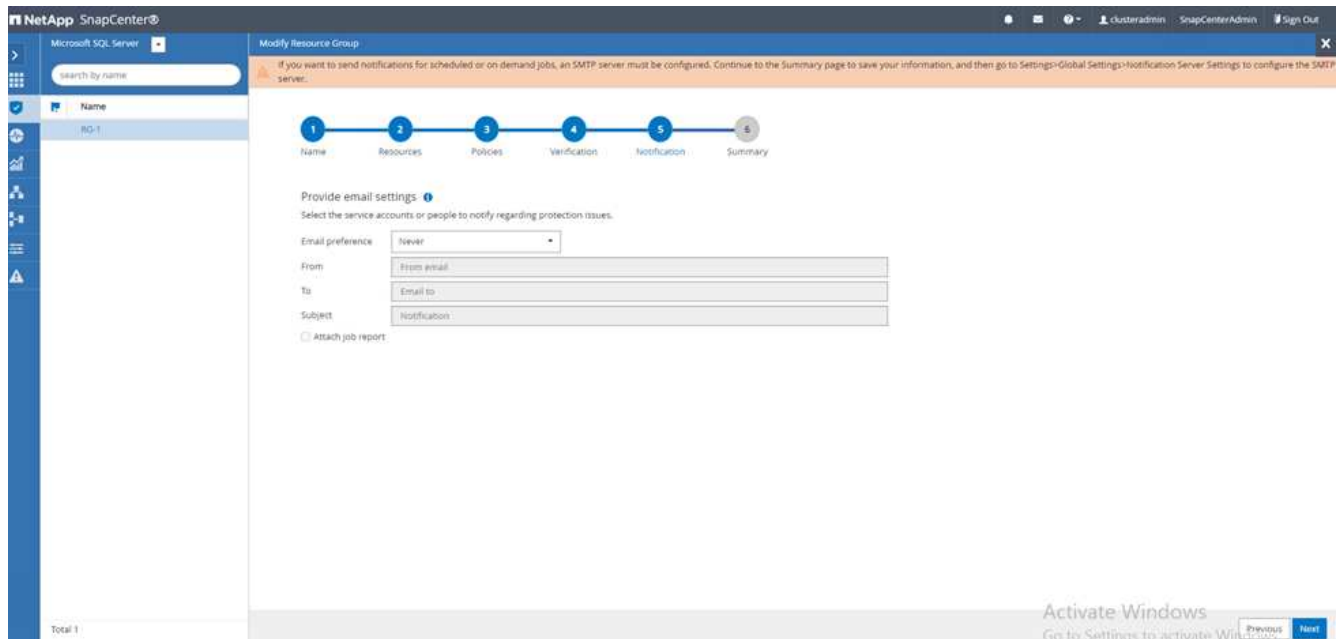
4. Sie können beide Richtlinien sehen. Klicken Sie Auf **Weiter**.



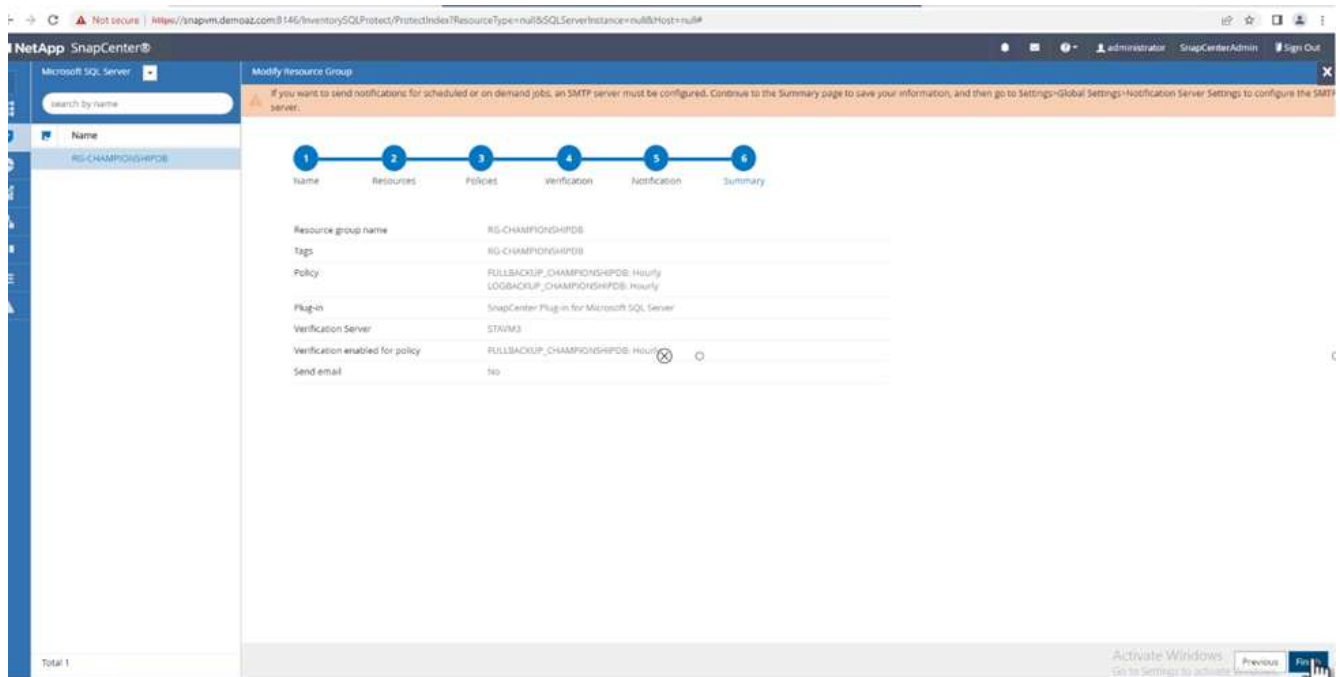
5. Konfigurieren Sie den Überprüfungsserver.



6. Konfigurieren Sie die E-Mail-Benachrichtigung.



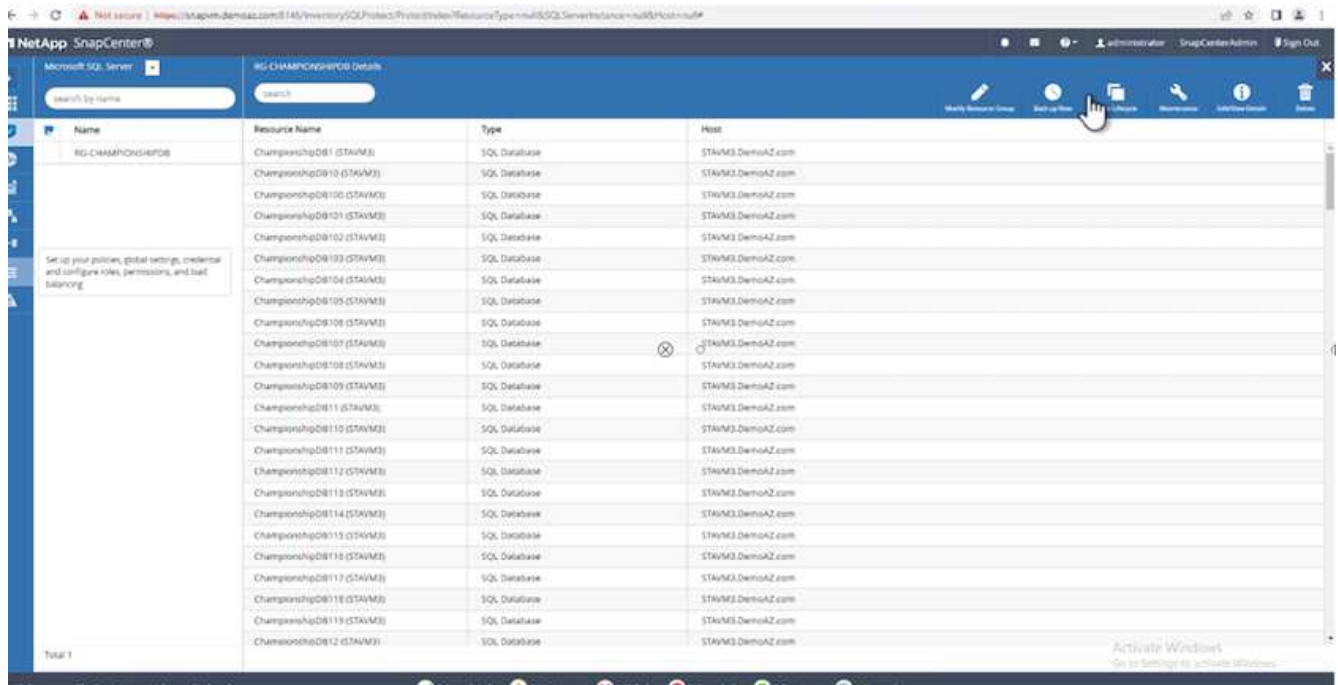
7. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertig stellen**.



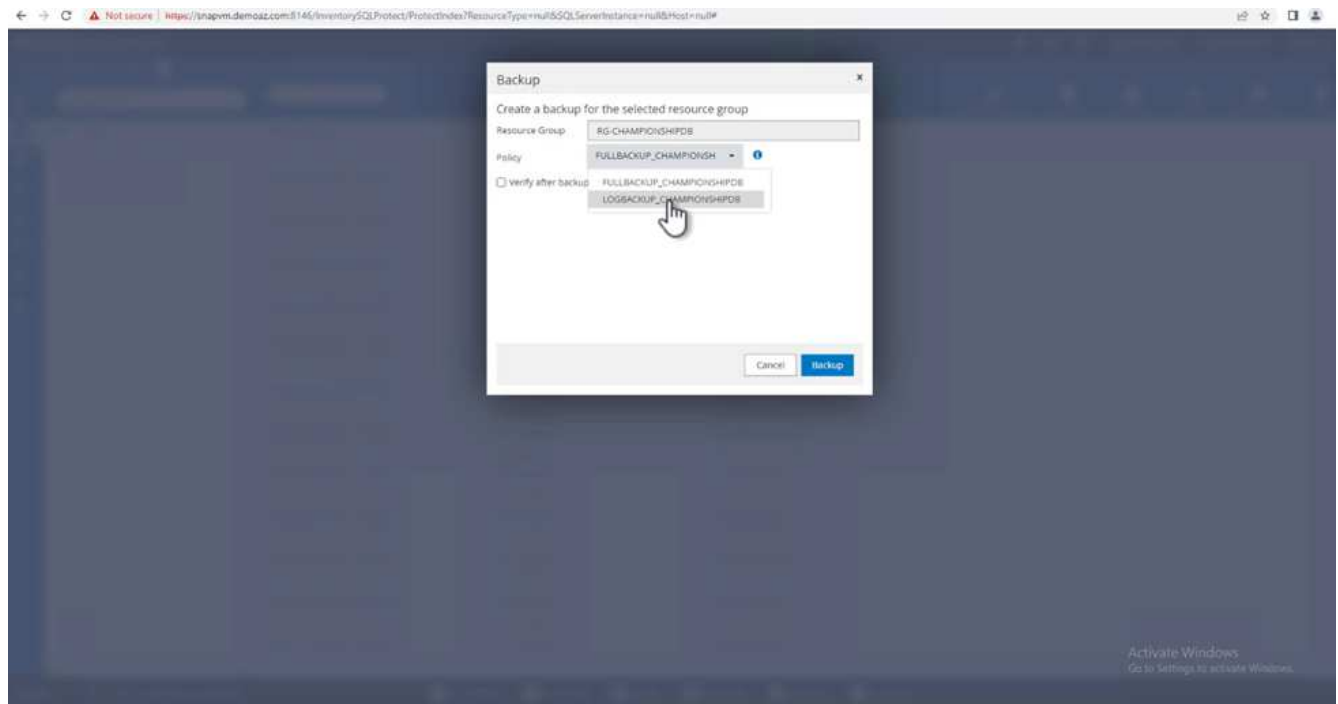
Auslösung einer On-Demand-Transaktions-Log-Sicherung für mehrere SQL Server-Datenbanken

Führen Sie die folgenden Schritte aus, um ein On-Demand-Backup des Transaktionsprotokolls für mehrere SQL-Server-Datenbanken auszulösen:

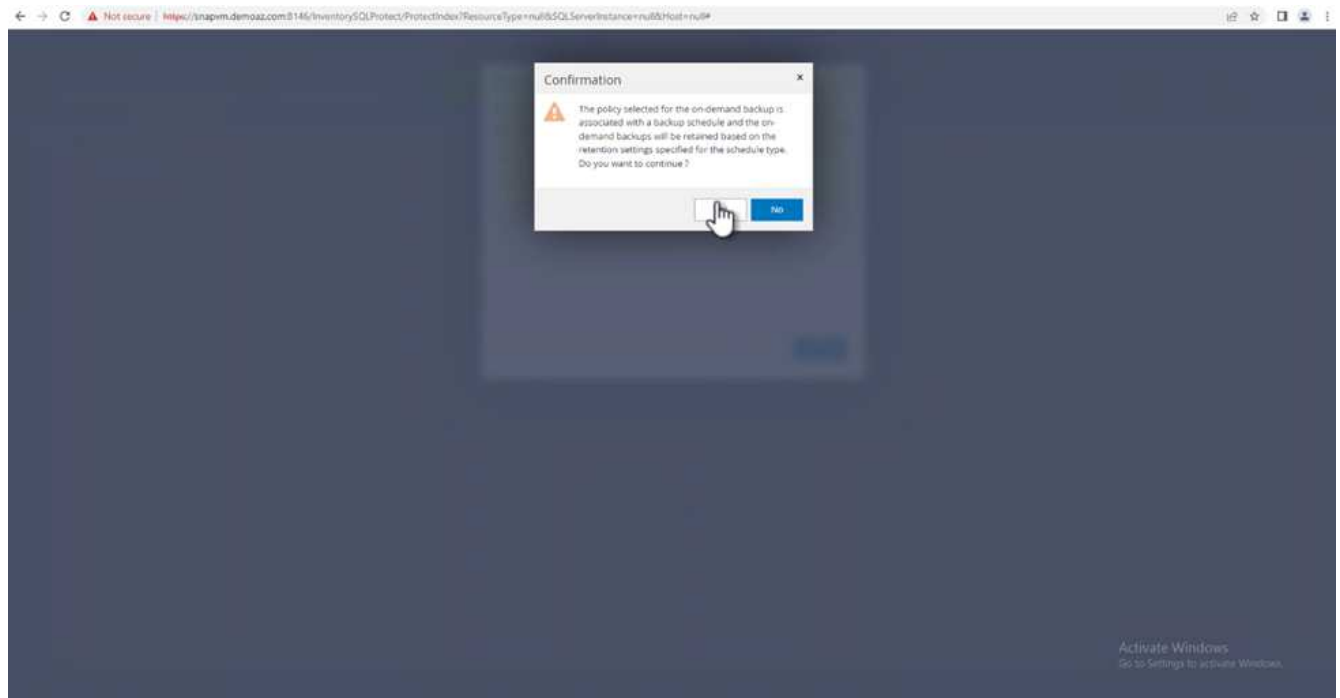
1. Wählen Sie auf der neu erstellten Richtlinienseite oben rechts auf der Seite die Option **Jetzt sichern** aus.



- Wählen Sie im Popup-Fenster auf der Registerkarte **Policy** das Dropdown-Menü aus, wählen Sie die Sicherungsrichtlinie aus und konfigurieren Sie die Sicherung des Transaktionsprotokolls.

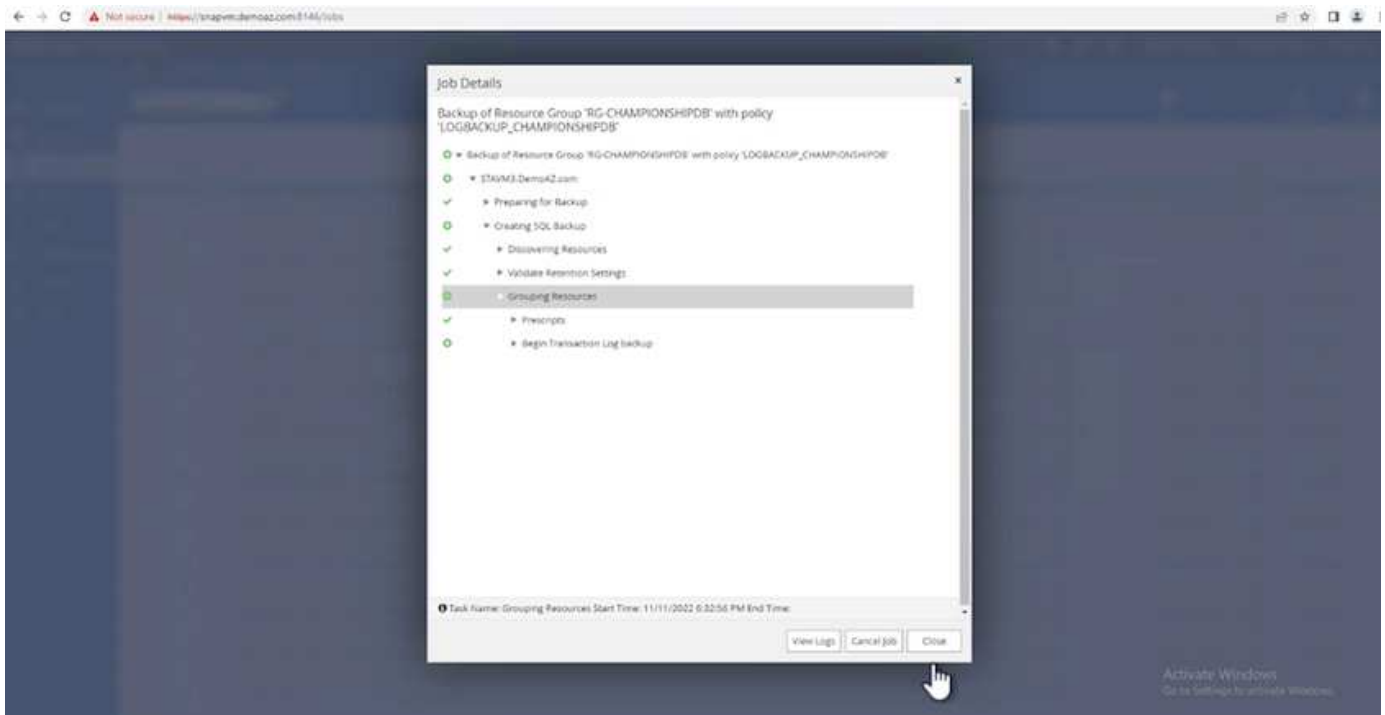


- Klicken Sie Auf **Backup**. Ein neues Fenster wird angezeigt.
- Klicken Sie auf **Ja**, um die Sicherungsrichtlinie zu bestätigen.



Monitoring

Wechseln Sie zur Registerkarte **Monitoring** und überwachen Sie den Fortschritt des Backupjobs.



Restore und Recovery

Lesen Sie die folgenden Voraussetzungen, die für die Wiederherstellung einer SQL Server-Datenbank in SnapCenter erforderlich sind.

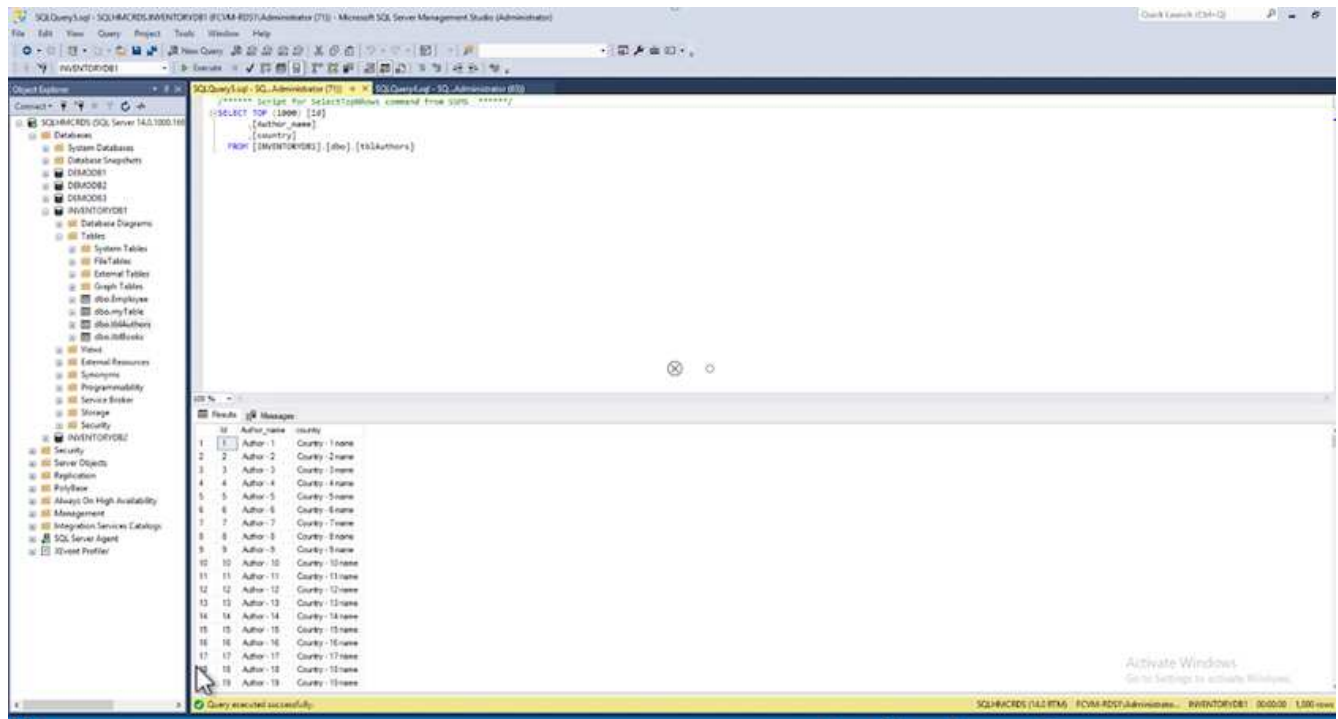
- Die Zielinstanz muss online sein und ausgeführt werden, bevor ein Wiederherstellungsauftrag abgeschlossen ist.

- SnapCenter-Vorgänge, die für die Ausführung für die SQL Server-Datenbank geplant sind, müssen deaktiviert werden, einschließlich aller Aufgaben, die auf Remote Management- oder Remote Verification-Servern geplant sind.
- Wenn Sie benutzerdefinierte Protokollverzeichnis-Backups auf einem alternativen Host wiederherstellen, müssen auf dem SnapCenter-Server und dem Plugin-Host dieselbe SnapCenter-Version installiert sein.
- Sie können die Systemdatenbank auf einem alternativen Host wiederherstellen.
- SnapCenter kann eine Datenbank in einem Windows Cluster wiederherstellen, ohne die SQL Server Cluster Gruppe offline zu schalten.

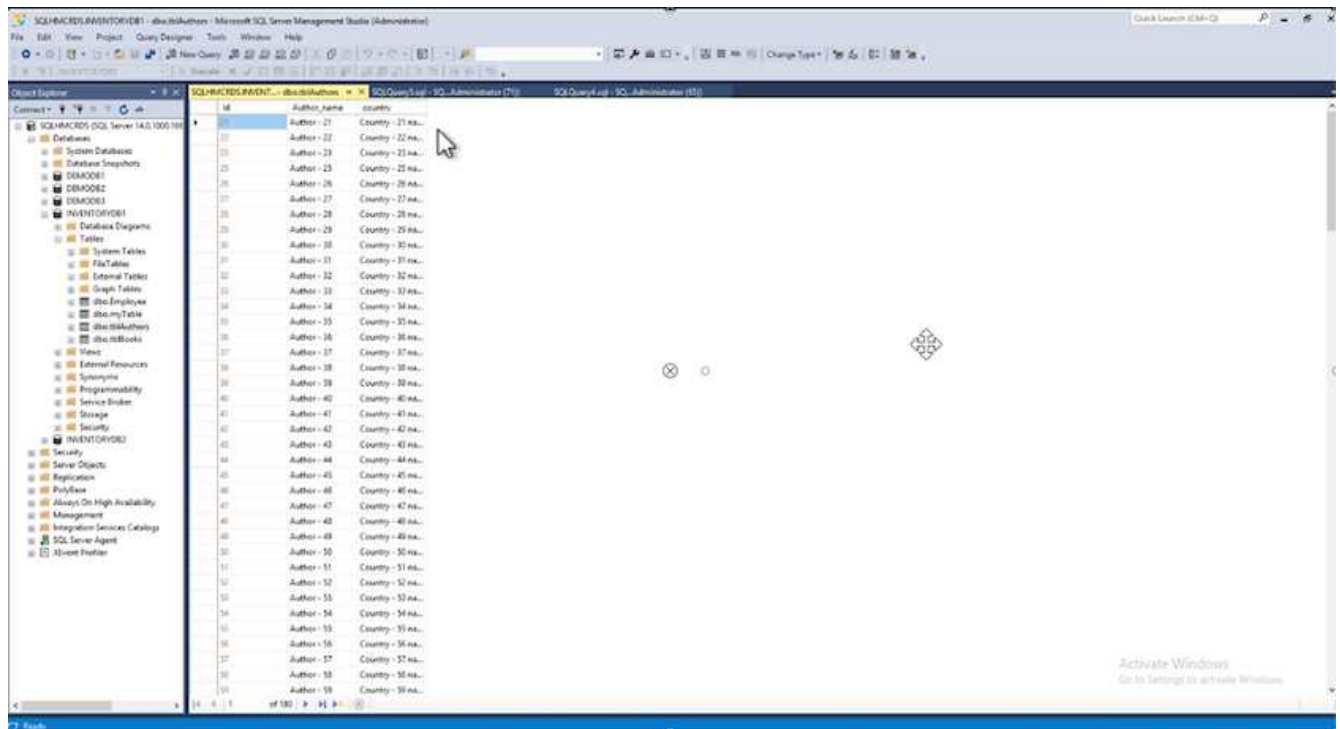
Wiederherstellen gelöschter Tabellen in einer SQL Server-Datenbank zu einem bestimmten Zeitpunkt

Führen Sie die folgenden Schritte aus, um eine SQL Server-Datenbank auf einen bestimmten Zeitpunkt wiederherzustellen:

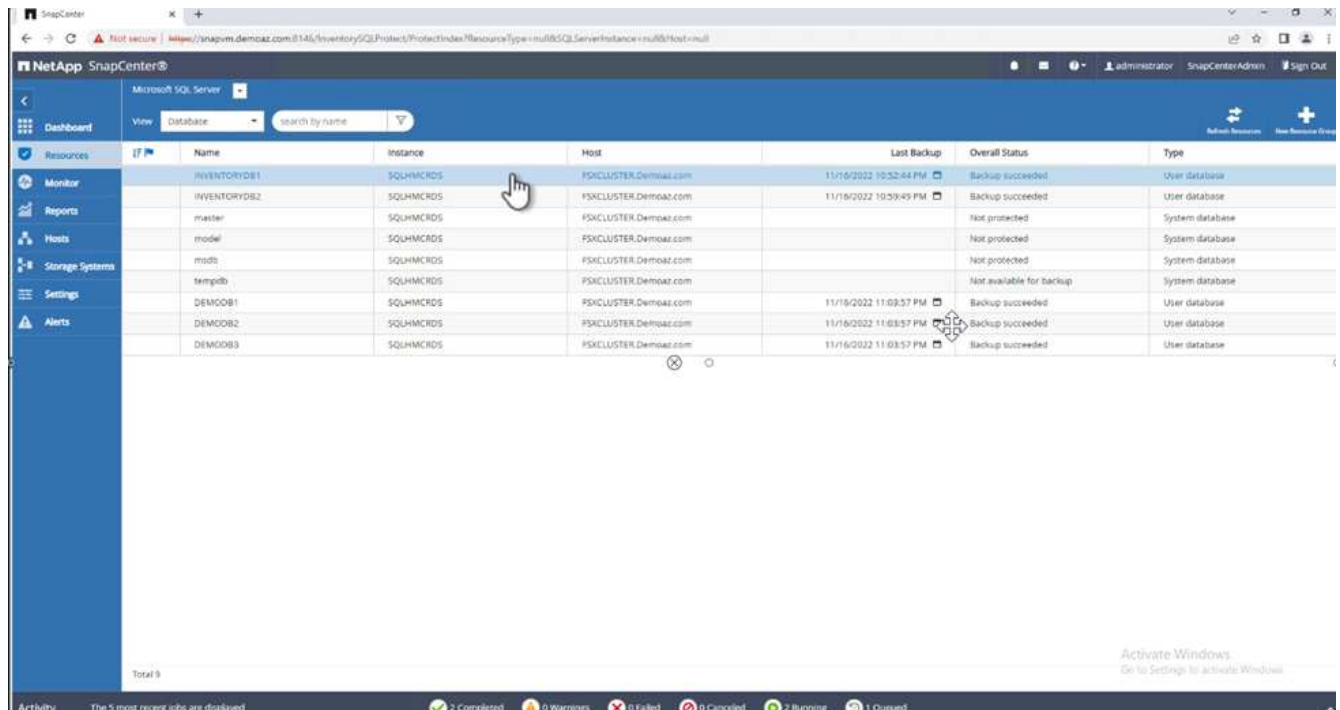
1. Der folgende Screenshot zeigt den Anfangsstatus der SQL Server-Datenbank vor den gelöschten Tabellen.



Der Screenshot zeigt, dass 20 Zeilen aus der Tabelle gelöscht wurden.

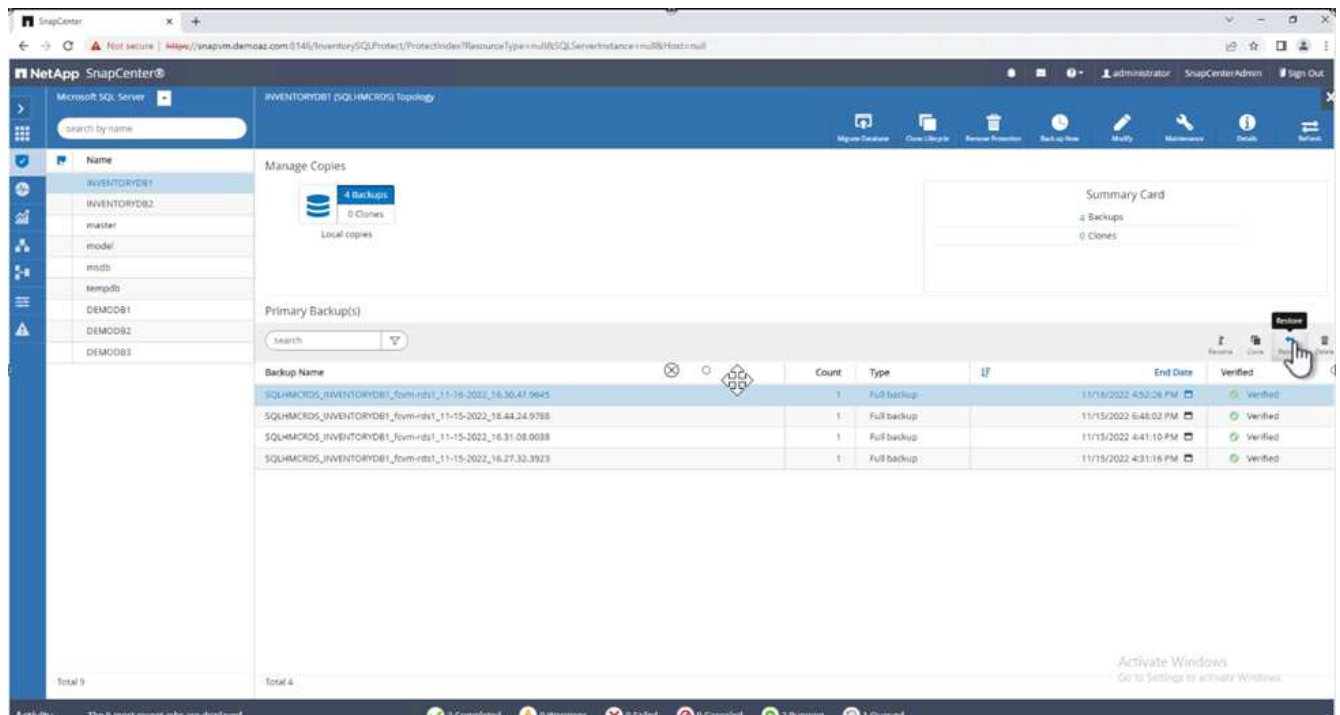


2. Melden Sie sich beim SnapCenter-Server an. Wählen Sie auf der Registerkarte **Ressourcen** die Datenbank aus.

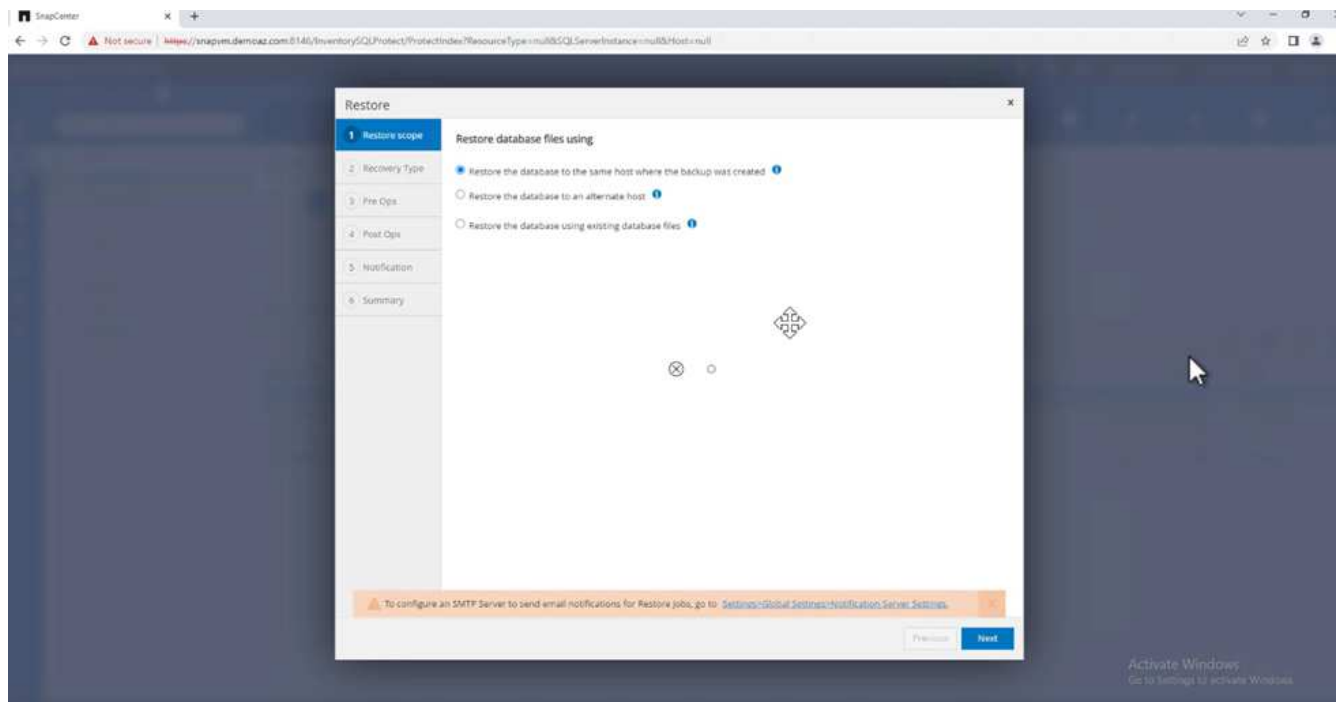


3. Wählen Sie die letzte Sicherung aus.

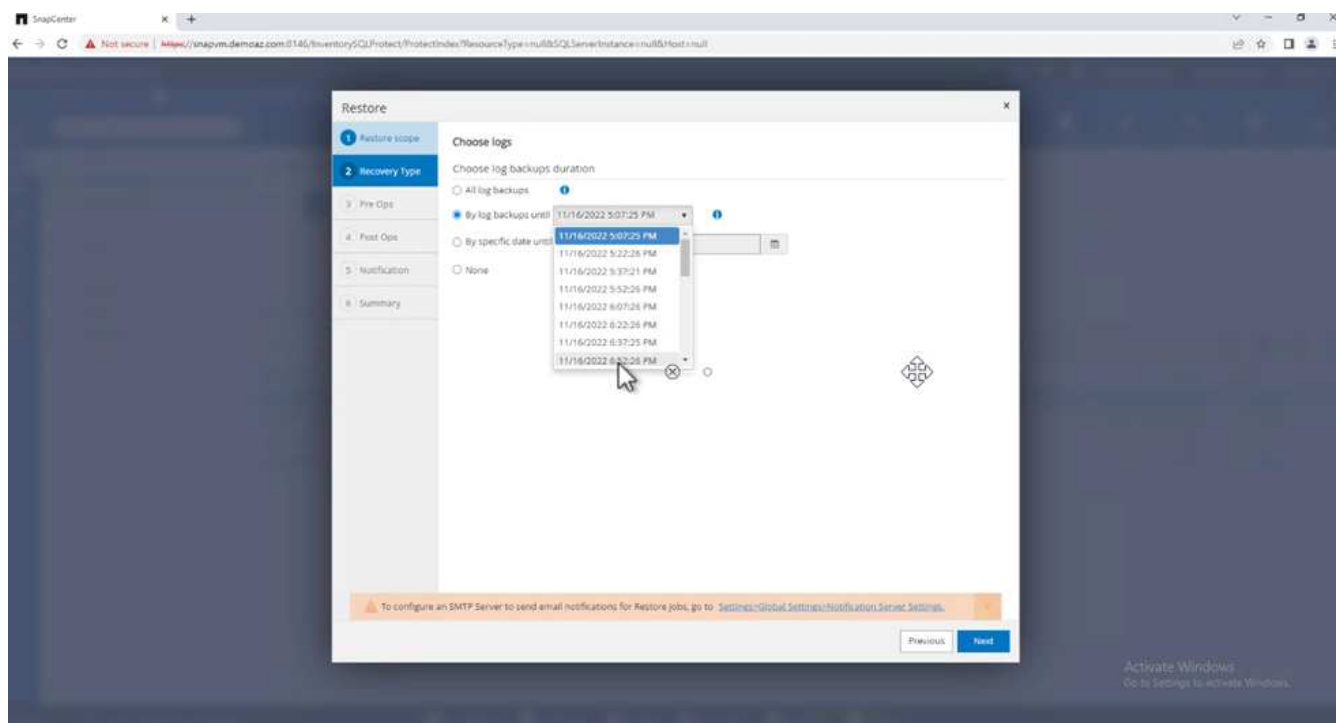
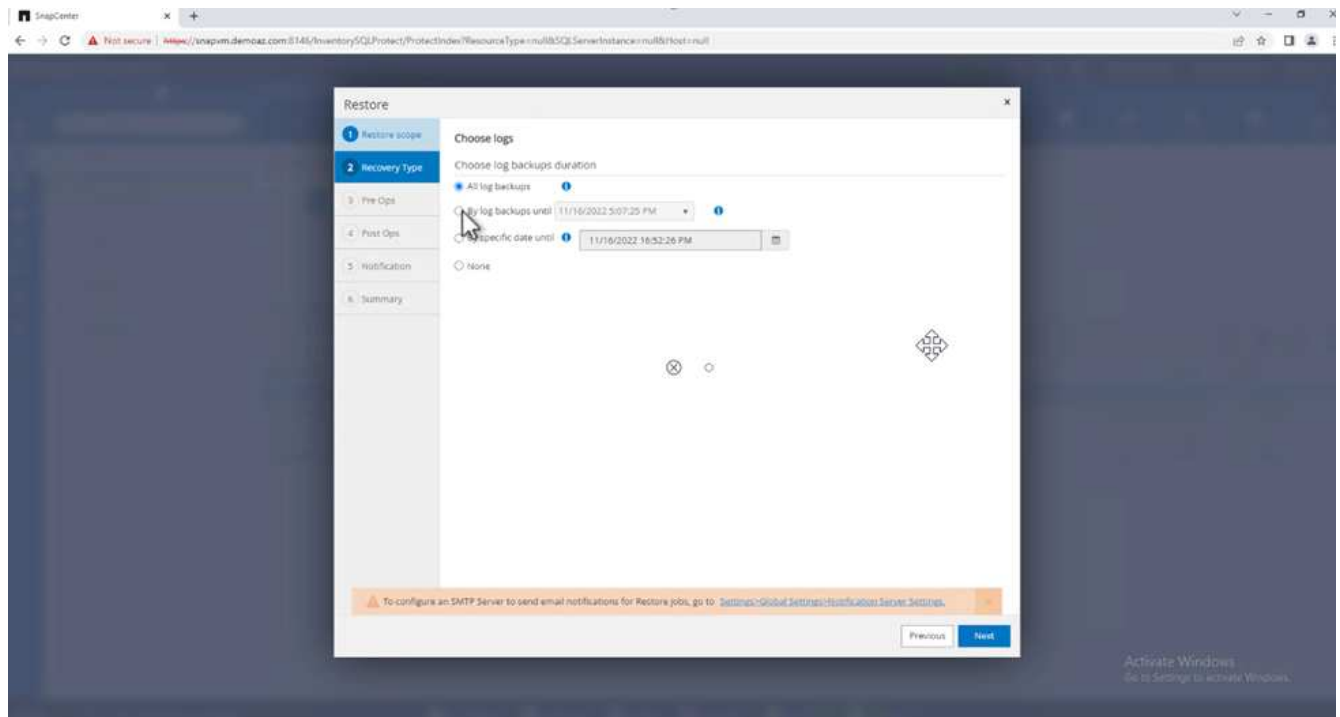
4. Wählen Sie auf der rechten Seite **Wiederherstellen**.



- Ein neues Fenster wird angezeigt. Wählen Sie die Option * Wiederherstellen*.
- Stellen Sie die Datenbank auf demselben Host wieder her, auf dem das Backup erstellt wurde. Klicken Sie Auf **Weiter**.

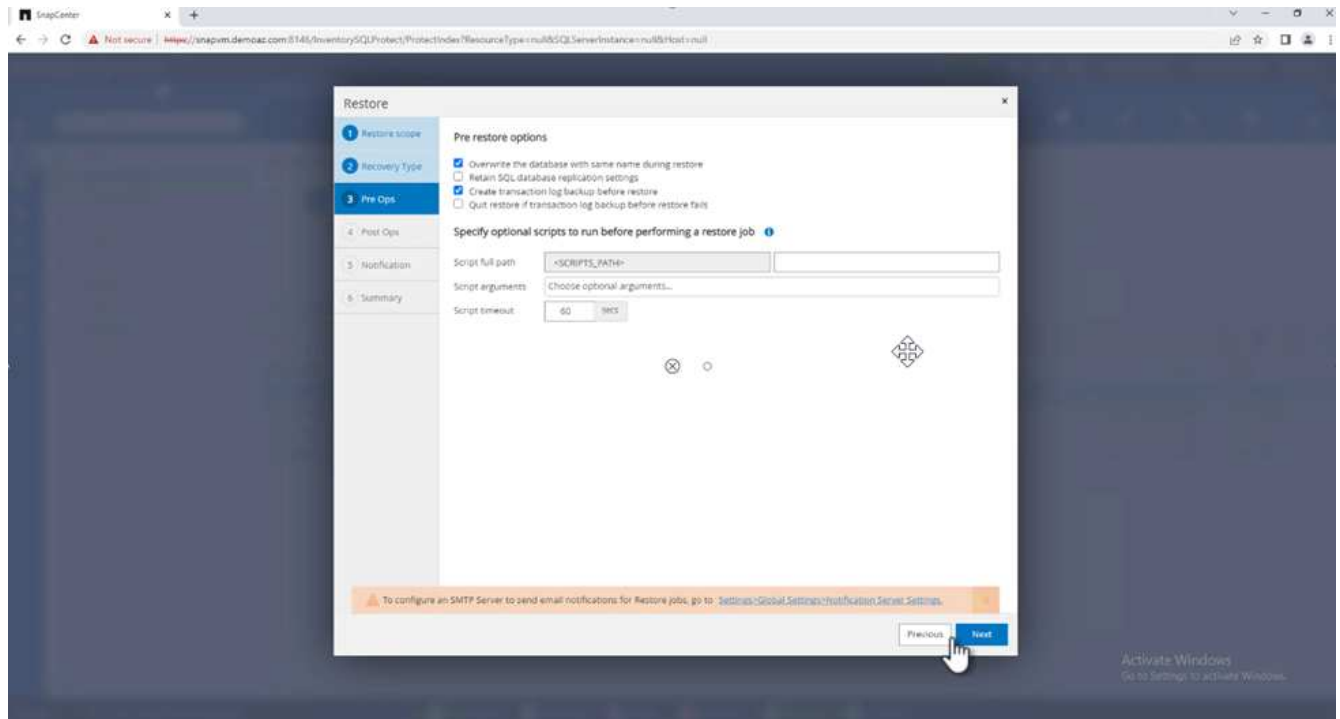


- Wählen Sie für den Typ **Recovery Alle Protokollsicherungen** aus. Klicken Sie Auf **Weiter**.



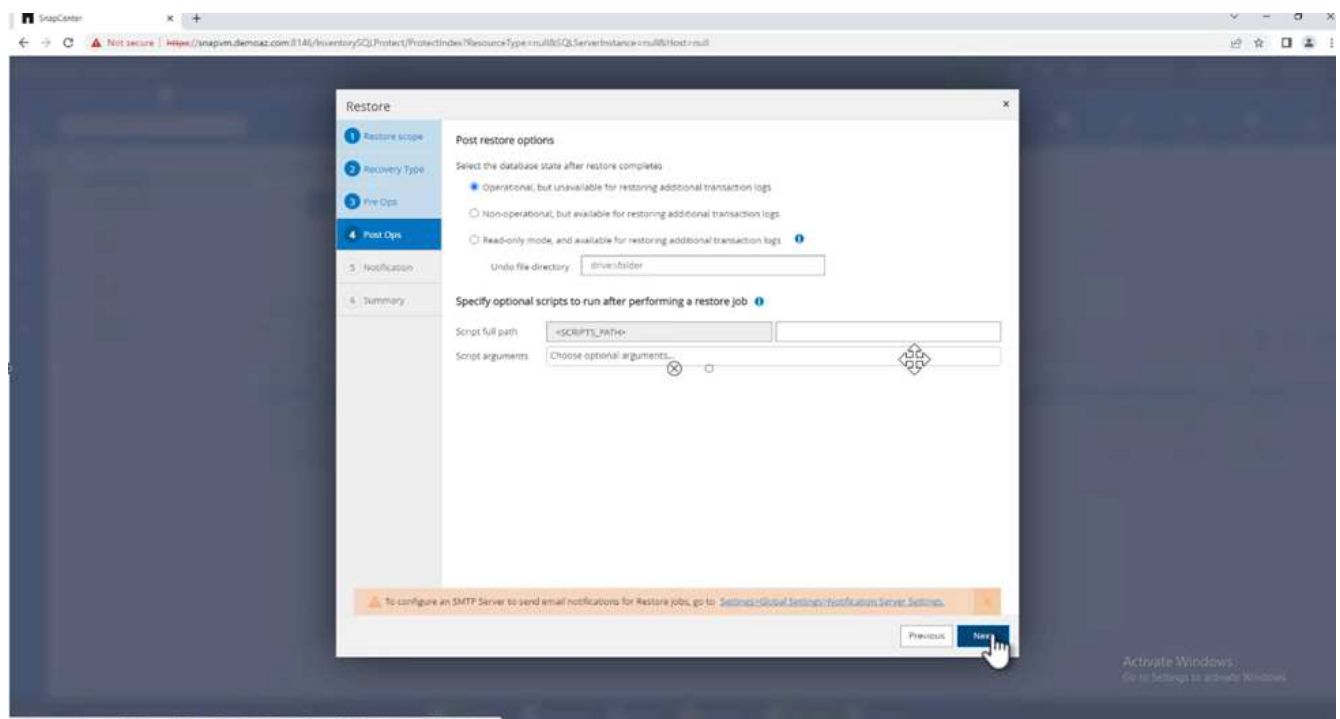
Optionen vor der Wiederherstellung:

1. Wählen Sie die Option **beim Wiederherstellen die Datenbank mit dem gleichen Namen überschreiben**. Klicken Sie Auf **Weiter**.

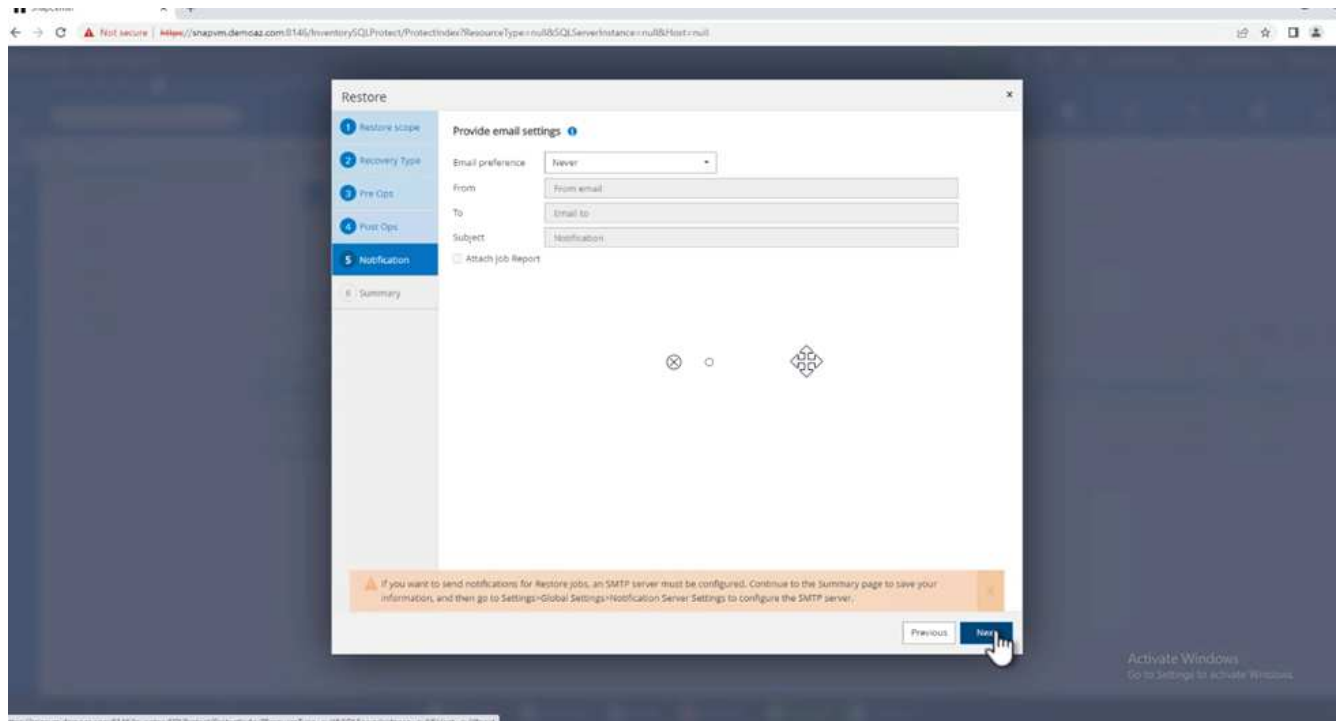


Optionen nach der Wiederherstellung:

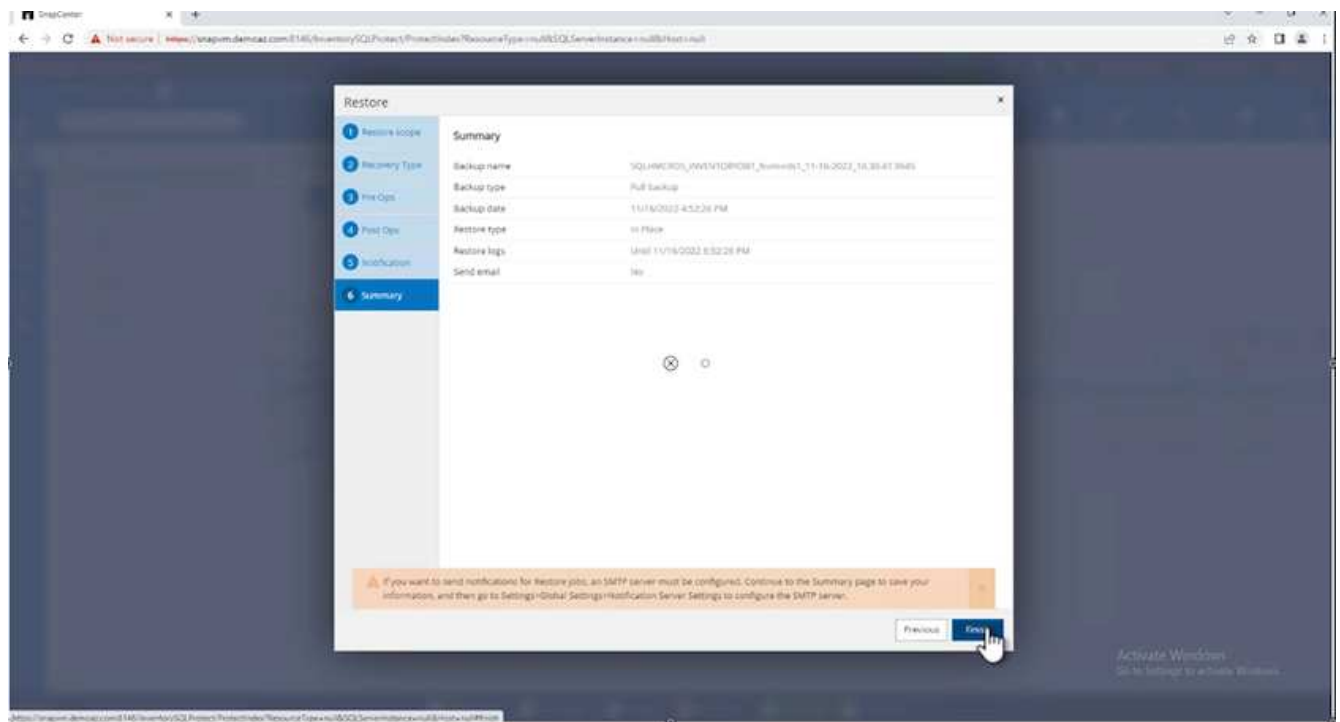
1. Wählen Sie die Option **operativ, aber nicht verfügbar für die Wiederherstellung zusätzlicher Transaktions-Logs**. Klicken Sie Auf **Weiter**.



2. Geben Sie die E-Mail-Einstellungen an. Klicken Sie Auf **Weiter**.



3. Klicken Sie auf der Seite **Zusammenfassung** auf **Fertig stellen**.



Überwachen des Wiederherstellungsfortschritts

1. Klicken Sie auf der Registerkarte **Überwachung** auf die Details des Wiederherstellungsjobs, um den Fortschritt des Wiederherstellungsjobs anzuzeigen.

ID	Status	Name	Start date	End date	Owner
124	✓	Restore 'SQLMCRDS\INVENTORYDB1'	11/16/2022 11:11:03 PM		Administrator
130	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 11:00:01 PM		Administrator
134	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:59:02 PM	11/16/2022 11:10:54 PM	Administrator
133	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB2' with policy 'InventoryDB2_fullbackup'	11/16/2022 10:55:01 PM	11/16/2022 10:58:50 PM	Administrator
132	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:45:01 PM	11/16/2022 11:10:54 PM	Administrator
131	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:44:02 PM	11/16/2022 10:55:53 PM	Administrator
150	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:30:01 PM	11/16/2022 10:55:54 PM	Administrator
148	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:29:02 PM	11/16/2022 10:40:53 PM	Administrator
146	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:15:01 PM	11/16/2022 10:40:53 PM	Administrator
147	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 10:14:02 PM	11/16/2022 10:25:53 PM	Administrator
146	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 10:00:01 PM	11/16/2022 10:25:53 PM	Administrator
145	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:59:02 PM	11/16/2022 10:10:53 PM	Administrator
143	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:45:01 PM	11/16/2022 10:10:53 PM	Administrator
142	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:44:02 PM	11/16/2022 9:55:54 PM	Administrator
142	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:30:01 PM	11/16/2022 9:55:54 PM	Administrator
141	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:29:02 PM	11/16/2022 9:40:53 PM	Administrator
140	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:15:01 PM	11/16/2022 9:40:53 PM	Administrator
139	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 9:14:02 PM	11/16/2022 9:25:54 PM	Administrator
138	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 9:00:01 PM	11/16/2022 9:25:54 PM	Administrator
137	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:59:02 PM	11/16/2022 9:10:53 PM	Administrator
136	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 8:45:01 PM	11/16/2022 9:10:53 PM	Administrator
135	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:44:02 PM	11/16/2022 8:55:54 PM	Administrator
134	✓	Backup of Resource Group 'SQLMCRDS\INVENTORYDB1' with policy 'InventoryDB_logbackup_policy'	11/16/2022 8:30:01 PM	11/16/2022 8:55:54 PM	Administrator
133	✓	Backup of Resource Group 'RG1-DEMO08' with policy 'demoDB_logbackup_policy'	11/16/2022 8:29:02 PM	11/16/2022 8:40:53 PM	Administrator

2. Stellen Sie die Jobdetails wieder her.

Job Details

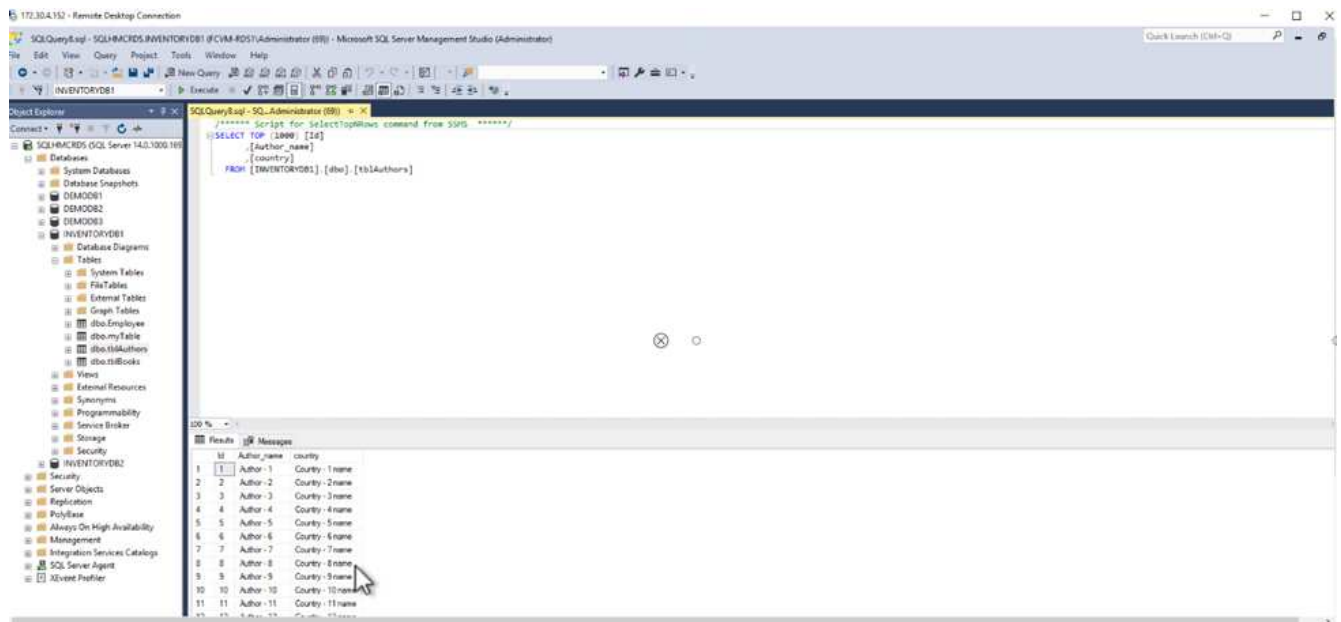
Restore 'SQLMCRDS\INVENTORYDB1'

- ✓ Restore 'SQLMCRDS\INVENTORYDB1'
- ✓ [Job '157'] Full log backup of SQLMCRDS\INVENTORYDB1'
 - ✓ JCVM-RGS1-Demo08.com
 - ✓ Preparing for Backup
 - ✓ Creating SQL Backup
 - ✓ Finalizing Backup
 - ✓ Send SMS Messages
- ✓ JCVM-RGS1-Demo08.com

Task Name: Send SMS Messages Start Time: 11/16/2022 11:18:54 PM End Time: 11/16/2022 11:18:54 PM

View Logs Cancel Close

3. Zurück zum SQL Server-Host > Datenbank > Tabelle vorhanden.



Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- ["TR-4714: Best Practices Guide für Microsoft SQL Server mit NetApp SnapCenter"](#)

<https://www.netapp.com/pdf.html?item=/media/12400-tr4714pdf.pdf>

- ["Anforderungen für das Wiederherstellen einer Datenbank"](#)

https://docs.netapp.com/us-en/snapcenter-45/protect-scsql/concept_requirements_for_restoring_a_database.html

- Allgemeines zu geklonten Datenbank-Lebenszyklen

<https://library.netapp.com/ecmdocs/ECMP1217281/html/GUID-4631AFF4-64FE-4190-931E-690FCADA5963.html>

TR-4923: SQL Server auf AWS EC2 unter Verwendung von Amazon FSX für NetApp ONTAP

Autoren: Pat Sithusan und Niyaz Mohamed, NetApp

Einführung

Viele Unternehmen, die Applikationen von lokalen Storage-Systemen und Cloud-Storage-Services migrieren möchten, stellen fest, dass sie diesem Aufwand durch die Unterschiede in den Funktionen von On-Premises-Storage-Systemen und Cloud-Storage-Services gedient haben. Diese Lücke hat die Migration von Enterprise-Applikationen wie Microsoft SQL Server erheblich problematisch gemacht. Insbesondere Mängel bei den Services, die zur Ausführung einer Enterprise-Applikation erforderlich sind, wie beispielsweise zuverlässige Snapshots, Storage-Effizienz-Funktionen, hohe Verfügbarkeit, Zuverlässigkeit und konsistente Performance, haben Kunden gezwungen, Kompromisse beim Design einzugehen oder Applikationsmigration zu gehen. Mit FSX für NetApp ONTAP müssen Kunden keine Kompromisse mehr eingehen. FSX für NetApp ONTAP ist ein

nativer AWS-Service (vom ersten Anbieter), der von AWS vertrieben, unterstützt, abgerechnet und vollständig gemanagt wird. Mit der leistungsstarken ONTAP bietet diese Architektur dieselben Storage- und Datenmanagement-Funktionen der Enterprise-Klasse, die NetApp seit drei Jahrzehnten in AWS als Managed Service vor Ort bietet.

Mit SQL Server auf EC2 Instanzen können Datenbankadministratoren ihre Datenbankumgebung und das zugrunde liegende Betriebssystem aufrufen und anpassen. Eine SQL Server auf EC2-Instanz in Kombination mit **"AWS FSX ONTAP"** Zum Speichern der Datenbankdateien bietet das Unternehmen hohe Performance, Datenmanagement und einen einfachen und einfachen Migrationspfad über Replizierung auf Blockebene. Daher können Sie Ihre komplexe Datenbank auf AWS VPC mit einem einfachen „Lift-and-Shift“-Ansatz, weniger Klicks und keine Schemakonvertierung ausführen.

Vorteile bei der Verwendung von Amazon FSX für NetApp ONTAP mit SQL Server

Amazon FSX für NetApp ONTAP ist die ideale File-Storage-Lösung für SQL Server-Implementierungen in AWS. Dies bietet unter anderem folgende Vorteile:

- Konsistent hohe Performance und hoher Durchsatz mit niedriger Latenz
- Intelligentes Caching mit NVMe-Cache für bessere Performance
- Flexible Dimensionierung, um Kapazität, Durchsatz und IOPS im Handumdrehen zu erhöhen oder zu reduzieren
- Effiziente Block-Replizierung zwischen On-Premises-Systemen und AWS
- Verwendung von iSCSI, einem bekannten Protokoll für die Datenbankumgebung
- Storage-Effizienzfunktionen wie Thin Provisioning und Klone ohne zusätzlichen Platzbedarf
- Verkürzung der Backup-Zeit von Stunden auf Minuten und dadurch Reduzierung der RTO
- Granulares Backup und Recovery von SQL-Datenbanken mit der intuitiven SnapCenter UI von NetApp
- Die Möglichkeit, vor der eigentlichen Migration mehrere Testmigrationen durchzuführen
- Kürzere Ausfallzeiten während der Migration und Bewältigung von Migrationsherausforderungen mit Kopien auf Datei- oder I/O-Ebene
- Verringerung der MTTR durch Ermittlung der Ursache nach einem Major Release oder Patch-Update

Die Implementierung von SQL Server Datenbanken auf FSX ONTAP mit dem iSCSI-Protokoll, wie in der Regel vor Ort, bietet eine ideale Storage-Umgebung für Datenbanken mit überlegener Performance, Storage-Effizienz und Datenmanagement-Funktionen. Es wurden mehrere iSCSI-Sitzungen verwendet, bei einer Arbeitsmenge von 5 %, vorausgesetzt, der Einsatz eines Flash Cache liefert über 100.000 IOPS mit dem FSX ONTAP Service. Diese Konfiguration bietet eine vollständige Kontrolle über die Performance für anspruchsvollste Applikationen. SQL Server, der auf kleineren EC2 Instanzen ausgeführt wird, die mit FSX für ONTAP verbunden sind, kann dieselben Vorgänge ausführen wie SQL Server, der auf einer viel größeren EC2 Instanz ausgeführt wird, da nur Bandbreitenbeschränkungen für Netzwerke auf FSX für ONTAP angewendet werden. Durch die Verringerung der Größe von Instanzen werden auch die Computing-Kosten gesenkt, wodurch eine TCO-optimierte Implementierung ermöglicht wird. Die Kombination von SQL mit iSCSI und SMB3.0 mit Multichannel-Freigaben für die kontinuierliche Verfügbarkeit auf FSX für ONTAP bietet große Vorteile für SQL-Workloads.

Bevor Sie beginnen

Die Kombination von Amazon FSX für NetApp ONTAP und SQL Server auf EC2 Instanzen ermöglicht die Erstellung von Datenbank-Storage-Designs der Enterprise-Klasse, die die anspruchsvollsten Applikationsanforderungen bis heute erfüllen können. Zur Optimierung beider Technologien ist es wichtig, die I/O-Muster und Eigenschaften von SQL Server zu verstehen. Ein gut geplantes Storage-Layout für eine SQL

Server Datenbank unterstützt die Performance von SQL Server und das Management der SQL Server Infrastruktur. Ein gutes Storage-Layout sorgt auch dafür, dass die ursprüngliche Implementierung erfolgreich ist und die Umgebung mit dem Laufe der Zeit reibungslos wachsen kann, wenn Ihr Unternehmen wächst.

Voraussetzungen

Bevor Sie die Schritte in diesem Dokument ausführen, sollten Sie die folgenden Voraussetzungen erfüllen:

- Ein AWS Konto
- Entsprechende IAM-Rollen zur Bereitstellung von EC2 und FSX für ONTAP
- Eine Windows Active Directory-Domäne auf EC2
- Alle SQL Server-Knoten müssen miteinander kommunizieren können
- Stellen Sie sicher, dass die DNS-Auflösung funktioniert und die Hostnamen aufgelöst werden können. Falls nicht, verwenden Sie den Eintrag für die Host-Datei.
- Allgemeine Kenntnisse zur SQL Server-Installation

Weitere Informationen finden Sie auch in den NetApp Best Practices für Umgebungen mit SQL Server, um die beste Storage-Konfiguration zu gewährleisten.

Best Practice-Konfigurationen für SQL Server-Umgebungen auf EC2

Mit FSX ONTAP ist die Beschaffung von Speicher die einfachste Aufgabe und kann durch Aktualisierung des Dateisystems durchgeführt werden. Dieser einfache Prozess ermöglicht bei Bedarf dynamische Kosten- und Performance-Optimierung, sorgt für den Ausgleich des SQL Workloads und liefert außerdem Thin Provisioning. FSX ONTAP Thin Provisioning wurde entwickelt, um EC2-Instanzen, die SQL Server ausführen, mehr logischen Storage anzubieten, als im Filesystem bereitgestellt wird. Storage muss nicht im Voraus verteilt werden, sondern wird den einzelnen Volumes oder LUNs dynamisch beim Schreiben der Daten zugewiesen. In den meisten Konfigurationen wird freier Speicherplatz wieder freigegeben, wenn Daten auf dem Volume oder der LUN gelöscht werden (und nicht durch Snapshot Kopien gespeichert werden). Die folgende Tabelle enthält Konfigurationseinstellungen für die dynamische Zuweisung von Speicher.

Einstellung	Konfiguration
Volume-Garantie	Keine (standardmäßig festgelegt)
LUN-Reservierung	Aktiviert
Fraktionale_Reserve	0% (standardmäßig festgelegt)
Snap_Reserve	0 %
Automatisches Löschen	Volume / älteste_First
Autosize	Ein
Versuchen Sie es zuerst	Autogrow
Volume Tiering-Richtlinie	Nur Snapshot
Snapshot-Richtlinie	Keine

Mit dieser Konfiguration kann die Gesamtgröße der Volumes größer sein als der tatsächlich im Dateisystem verfügbare Speicher. Wenn die LUNs oder Snapshot Kopien mehr Speicherplatz benötigen, als im Volume verfügbar ist, wachsen die Volumes automatisch und nehmen mehr Speicherplatz aus dem zugehörigen File-System in Anspruch. Autogrow ermöglicht FSX ONTAP, die Volume-Größe automatisch auf eine maximale Größe zu erhöhen, die Sie vorab bestimmen. Um das automatische Wachstum des Volumes zu unterstützen, muss im Filesystem Platz vorhanden sein. Bei aktiviertem Autogrow sollten Sie daher den freien Speicherplatz im Dateisystem überwachen und bei Bedarf das Dateisystem aktualisieren.

Stellen Sie außerdem das ein "[Speicherplatzzuweisung](#)" Option bei LUN aktivieren, damit FSX ONTAP den EC2-Host benachrichtigt, wenn der Speicherplatz des Volume knapp wird, und die LUN im Volume keine Schreibvorgänge akzeptieren kann. Mit dieser Option kann FSX für ONTAP außerdem automatisch Speicherplatz zurückgewinnen, wenn SQL Server auf EC2 Host Daten löscht. Die Option für die Speicherplatzzuweisung ist standardmäßig auf deaktiviert eingestellt.



Wenn eine space-reservierte LUN in einem ohne garantierte Performance-Volume erstellt wird, verhält sich die LUN wie eine nicht-space-reservierte LUN. Das liegt daran, dass ein nicht garantiertes Volume keinen Platz hat, der LUN zuzuweisen. Das Volume selbst kann aufgrund seiner keinen Garantie nur Speicherplatz zuweisen, da es geschrieben wird.

Mit dieser Konfiguration können FSX ONTAP-Administratoren die Größe des Volumes in der Regel so festlegen, dass sie den belegten Speicherplatz auf der LUN-Seite auf der Host-Seite und im Filesystem managen und überwachen müssen.



NetApp empfiehlt die Verwendung eines separaten Filesystems für SQL Server Workloads. Wenn das Dateisystem für mehrere Anwendungen verwendet wird, überwachen Sie die Speicherplatznutzung sowohl des Dateisystems als auch der Volumes innerhalb des Dateisystems, um sicherzustellen, dass die Volumes nicht auf verfügbaren Speicherplatz konkurrieren.



Snapshot Kopien, die zur Erstellung von FlexClone Volumes genutzt werden, werden durch die Option Autodelete nicht gelöscht.



Eine Überbelegung von Storage muss für eine geschäftskritische Applikation wie SQL Server sorgfältig geprüft und gemanagt werden. Selbst ein minimaler Ausfall ist nicht tolerierbar. In solch einem Fall ist es am besten, Trends in der Storage-Nutzung zu überwachen, um festzustellen, wie viel oder wann überhaupt eine Überbelegung akzeptabel ist.

Best Practices

1. Für eine optimale Storage-Performance sollten Sie die Filesystem-Kapazität bis zum 1,35-fachen der gesamten Datenbankauslastung bereitstellen.
2. Zur Vermeidung von Applikations-Downtime ist eine angemessene Überwachung sowie ein effektiver Aktionsplan mit Thin Provisioning erforderlich.
3. Achten Sie darauf, die Warnmeldungen zu CloudWatch und anderen Monitoring-Tools so einzurichten, dass jederzeit Kontakt mit Mitarbeitern aufgenommen wird, wenn der Storage gefüllt ist.

Konfiguration von Storage für SQL Server und Bereitstellung von SnapCenter für Backup-, Restore- und Klonvorgänge

Um SQL-Servervorgänge mit SnapCenter durchzuführen, müssen Sie zuerst Volumes und LUNs für SQL Server erstellen.

Erstellung von Volumes und LUNs für SQL Server

Führen Sie die folgenden Schritte aus, um Volumes und LUNs für SQL Server zu erstellen:

1. Öffnen Sie die Amazon FSX-Konsole bei <https://console.aws.amazon.com/fsx/>
2. Erstellen Sie mit der Option „Standard erstellen“ unter „Erstellungsmethode“ ein Amazon FSX für das Filesystem von NetApp ONTAP. So können Sie FSxadmin- und vsadmin-Anmeldeinformationen definieren.

Creation method

Quick create
Use recommended best-practice configurations. Most configuration options can be changed after the file system is created.

Standard create
You set all of the configuration options, including specifying performance, networking, security, backups, and maintenance.

3. Geben Sie das Passwort für fsxadmin an.

File system administrative password

Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password
 Specify a password

Password

Confirm password

4. Geben Sie das Passwort für SVMs an.

SVM administrative password

Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

- Don't specify a password
 Specify a password

Password

Confirm password

5. Erstellen Sie Volumes, indem Sie den Schritt befolgen, der in aufgeführt ist "[Erstellung eines Volumes auf FSX für NetApp ONTAP](#)".

Best Practices

- Deaktivieren Sie Zeitpläne für Storage Snapshot Kopien und Aufbewahrungsrichtlinien. Verwenden Sie stattdessen NetApp SnapCenter, um Snapshot Kopien der SQL Server Daten und Protokoll-Volumes zu koordinieren.
- Konfigurieren Sie Datenbanken auf einzelnen LUNs auf separaten Volumes, um von einer schnellen und granularen Restore-Funktion zu profitieren.
- Platzieren Sie Benutzerdatendateien (.mdf) auf separaten Volumes, da es sich um Workloads mit zufälligen Lese-/Schreibzugriffen handelt. Es ist üblich, Transaktions-Log-Backups häufiger zu erstellen als Datenbank-Backups. Aus diesem Grund legen Sie Transaktions-Log-Dateien (.ldf) auf ein separates Volume von den Datendateien ab, so dass für jedes einzelne unabhängige Backup-Zeitpläne erstellt werden können. Durch diese Trennung werden auch die I/O-Vorgänge bei sequenziellen Schreibvorgängen aus den I/O-Vorgängen für zufällige Lese-/Schreibzugriffe von Datendateien isoliert und die SQL Server Performance deutlich verbessert.
- Tempdb ist eine Systemdatenbank, die von Microsoft SQL Server als temporärer Arbeitsbereich verwendet wird, insbesondere für I/O-intensive DBCC CHECKDB-Vorgänge. Platzieren Sie daher diese Datenbank auf einem dedizierten Volume. In großen Umgebungen, in denen die Volume-Anzahl eine Herausforderung ist, können Sie tempdb in weniger Volumes konsolidieren und im gleichen Volume wie andere Systemdatenbanken nach einer sorgfältigen Planung speichern. Datensicherung für tempdb ist keine hohe Priorität, da diese Datenbank bei jedem Neustart von Microsoft SQL Server neu erstellt wird.

6. Verwenden Sie den folgenden SSH-Befehl zum Erstellen von Volumes:

```
vol create -vserver svm001 -volume vol_awssqlprod01_data -aggregate
aggr1 -size 800GB -state online -tiering-policy snapshot-only
-percent-snapshot-space 0 -autosize-mode grow -snapshot-policy none
-security-style ntfs
volume modify -vserver svm001 -volume vol_awssqlprod01_data
-fractional-reserve 0
volume modify -vserver svm001 -volume vol_awssqlprod01_data -space
-mgmt-try-first vol_grow
volume snapshot autodelete modify -vserver svm001 -volume
vol_awssqlprod01_data -delete-order oldest_first
```

7. Starten Sie den iSCSI-Dienst mit PowerShell unter Verwendung erhöhter Berechtigungen in Windows-Servern.

```
Start-Service -Name msiscsi
Set-Service -Name msiscsi -StartupType Automatic
```

8. Installieren Sie Multipath IO mit PowerShell unter Verwendung erhöhter Berechtigungen in Windows Servern.

```
Install-WindowsFeature -name Multipath-IO -Restart
```

9. Suchen Sie den Windows-Initiatorenamen mit PowerShell unter Verwendung von erhöhten Berechtigungen in Windows-Servern.

```
Get-InitiatorPort | select NodeAddress
```

```
PS C:\Users\administrator.CONTOSO> Get-InitiatorPort | select NodeAddress

NodeAddress
-----
iqn.1991-05.com.microsoft:ws2019-sql1.contoso.net
```

10. Stellen Sie eine Verbindung zu Storage Virtual Machines (SVM) mithilfe von putty her und erstellen Sie eine iGroup.

```
igroup create -igroup igrp_ws2019sql1 -protocol iscsi -ostype windows -initiator iqn.1991-05.com.microsoft:ws2019-sql1.contoso.net
```

11. Verwenden Sie den folgenden SSH-Befehl, um LUNs zu erstellen:

```
lun create -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -size 700GB -ostype windows_2008 -space-allocation enabled
lun create -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -size 100GB -ostype windows_2008 -space-allocation enabled
```

```
svmsql:> lun create -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -size 700GB -ostype windows_2008
Created a LUN of size 700g (751619276800)

svmsql:> lun create -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -size 100GB -ostype windows_2008
Created a LUN of size 100g (107374182400)

svmsql:> lun show
Vserver Path State Mapped Type Size
-----
svmsql /vol/vol_awssqlprod01_data/lun_awssqlprod01_data online unmapped windows_2008 700GB
svmsql /vol/vol_awssqlprod01_log/lun_awssqlprod01_log online unmapped windows_2008 100GB
2 entries were displayed.
```

12. Verwenden Sie Windows_2008 als empfohlenen LUN-Typ, um die I/O-Ausrichtung mit dem OS-Partitionierungsschema zu erreichen. Siehe ["Hier"](#) Finden Sie weitere Informationen.
13. Verwenden Sie den folgenden SSH-Befehl für die Zuordnung der Initiatorgruppe zu den LUNs, die Sie gerade erstellt haben.

```
lun show
lun map -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -igroup igrp_awssqlprod01
lun map -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -igroup igrp_awssqlprod01
```



```

svmsql::> lun show
Vserver      Path                                                                 State  Mapped  Type      Size
-----
svmsql      /vol/vol_awssqlprod01_data/lun_awssqlprod01_data                 online unmapped windows_2008
                                                    700GB
svmsql      /vol/vol_awssqlprod01_log/lun_awssqlprod01_log                   online unmapped windows_2008
                                                    100GB
2 entries were displayed.

svmsql::> lun map -path /vol/vol_awssqlprod01_data/lun_awssqlprod01_data -igroup igrp_awssqlprod01
svmsql::> lun map -path /vol/vol_awssqlprod01_log/lun_awssqlprod01_log -igroup igrp_awssqlprod01

svmsql::>
svmsql::> lun show
Vserver      Path                                                                 State  Mapped  Type      Size
-----
svmsql      /vol/vol_awssqlprod01_data/lun_awssqlprod01_data                 online mapped  windows_2008
                                                    700GB
svmsql      /vol/vol_awssqlprod01_log/lun_awssqlprod01_log                   online mapped  windows_2008
                                                    100GB
2 entries were displayed.

```

14. Führen Sie für eine freigegebene Festplatte, die Windows Failover Cluster verwendet, einen SSH-Befehl aus, um die gleiche LUN der Initiatorgruppe zuzuordnen, die zu allen Servern gehört, die am Windows Failover Cluster teilnehmen.
15. Windows Server mit einer SVM mit einem iSCSI-Ziel verbinden. Suchen Sie die Ziel-IP-Adresse aus dem AWS Portal.

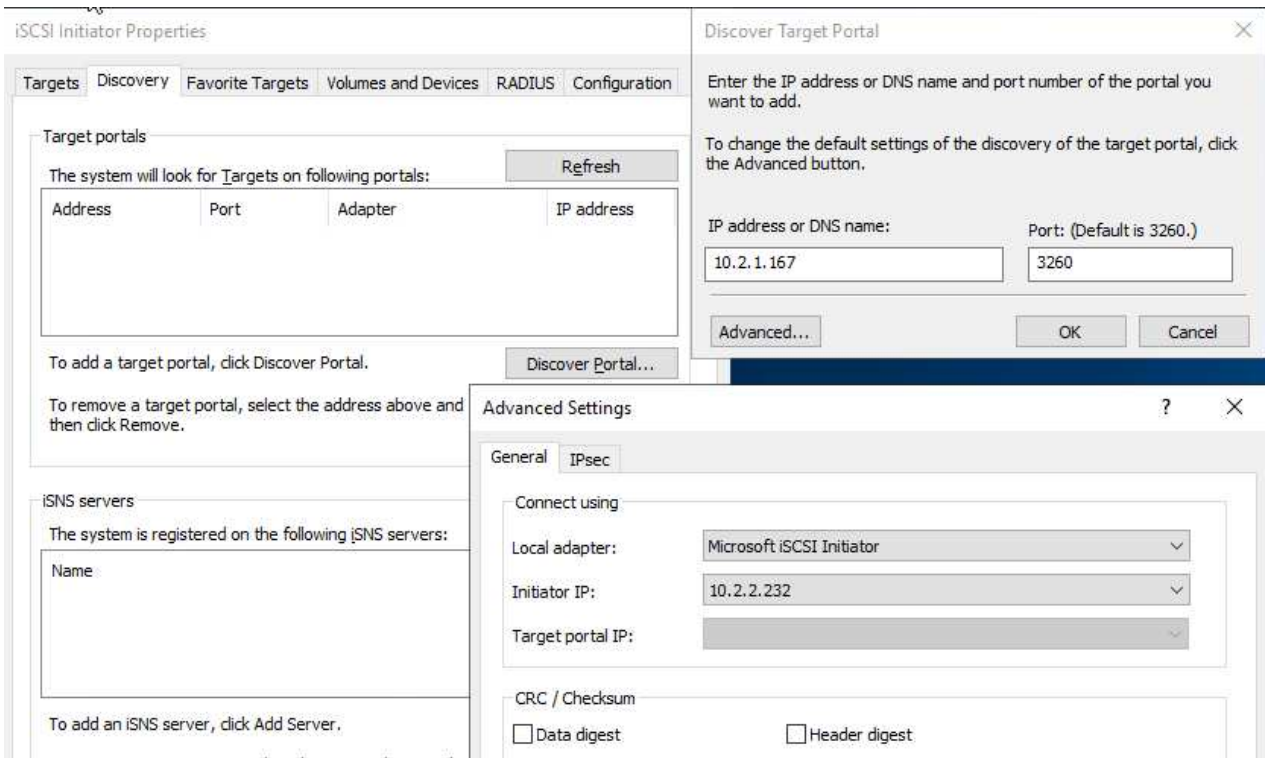
svmsql (svm-09e98ab33a31b724a)

Summary	
SVM ID svm-09e98ab33a31b724a	Creation time 2021-09-21T13:19:34-07:00
SVM name svmsql	Lifecycle state Created
UUID ea00ea2d-1b1d-11ec-9de1-6f9cef731025	Subtype DEFAULT
File system ID fs-0ab4b447ebd6082aa	
Resource ARN arn:aws:fsx:us-west-2:139763910815:storage-virtual-machine/fs-0ab4b447ebd6082aa/svm-09e98ab33a31b724a	

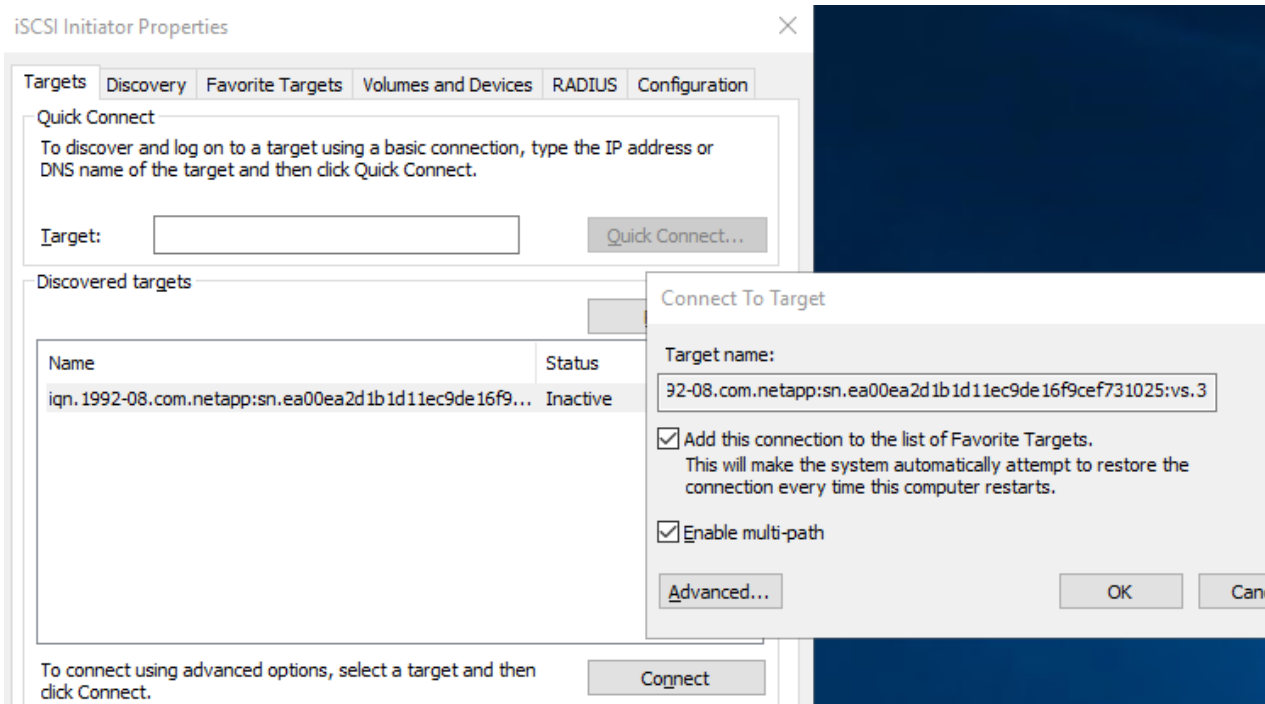
Endpoints	
Management DNS name svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	Management IP address 198.19.255.153
NFS DNS name svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	NFS IP address 198.19.255.153
iSCSI DNS name iscsi.svm-09e98ab33a31b724a.fs-0ab4b447ebd6082aa.fsx.us-west-2.amazonaws.com	iSCSI IP addresses 10.2.1.167, 10.2.2.12

16. Wählen Sie im Server Manager und im Menü Extras den iSCSI-Initiator aus. Wählen Sie die Registerkarte Ermittlung aus, und wählen Sie dann Portal ermitteln aus. Geben Sie im vorherigen Schritt die iSCSI-IP-Adresse ein, und wählen Sie Erweitert. Wählen Sie im lokalen Adapter Microsoft iSCSI Initiator aus. Wählen Sie in Initiator-IP die IP des Servers aus. Wählen Sie anschließend OK,

um alle Fenster zu schließen.



- 17. Wiederholen Sie Schritt 12 für die zweite iSCSI-IP-Adresse der SVM.
- 18. Wählen Sie die Registerkarte **Ziele** aus, wählen Sie **Verbinden** und wählen Sie **multi-Pfad aktivieren**.



- 19. Fügen Sie für eine optimale Performance weitere Sitzungen hinzu. NetApp empfiehlt die Erstellung von fünf iSCSI-Sitzungen. Wählen Sie **Eigenschaften** *> **Sitzung hinzufügen** *> **Erweitert** aus, und wiederholen Sie Schritt 12.

```
$TargetPortals = ('10.2.1.167', '10.2.2.12')
foreach ($TargetPortal in $TargetPortals) {New-IscsiTargetPortal
-TargetPortalAddress $TargetPortal}
```

```
$TargetPortals = ('10.2.1.167', '10.2.2.12')
foreach ($TargetPortal in $TargetPortals) {New-IscsiTargetPortal -TargetPortalAddress $TargetPortal}

InitiatorInstanceName :
InitiatorPortalAddress :
IsDataDigest           : False
IsHeaderDigest         : False
TargetPortalAddress    : 10.2.1.167
TargetPortalPortNumber : 3260
PSComputerName         :

InitiatorInstanceName :
InitiatorPortalAddress :
IsDataDigest           : False
IsHeaderDigest         : False
TargetPortalAddress    : 10.2.2.12
TargetPortalPortNumber : 3260
PSComputerName         :
```

Best Practices

- Konfigurieren Sie fünf iSCSI-Sitzungen pro Zielschnittstelle, um eine optimale Performance zu erzielen.
- Konfiguration einer Round Robin-Richtlinie zur besten iSCSI-Performance insgesamt
- Stellen Sie beim Formatieren der LUNs sicher, dass die Zuordnungseinheit für Partitionen auf 64K eingestellt ist
 - a. Führen Sie den folgenden PowerShell-Befehl aus, um sicherzustellen, dass die iSCSI-Sitzung beibehalten wird.

```
$targets = Get-IscsiTarget
foreach ($target in $targets)
{
Connect-IscsiTarget -IsMultipathEnabled $true -NodeAddress
$target.NodeAddress -IsPersistent $true
}
```

```
PS C:\windows\system32> Connect-IscsiTarget -NodeAddress (Get-IscsiTarget | select -ExpandProperty NodeAddress)

AuthenticationType      : NONE
InitiatorInstanceName   : ROOT\ISCSIPT\0000_0
InitiatorNodeAddress    : iqn.1991-05.com.microsoft:awssqlprod01.cloudheroes.dom
InitiatorPortalAddress  : 0.0.0.0
InitiatorsSideIdentifier : 400001370000
IsConnected             : True
IsDataDigest            : False
IsDiscovered            : True
IsHeaderDigest          : False
IsPersistent            : True
NumberOfConnections     : 1
SessionIdentifier       : ffff9988350ff010-4000013700000012
TargetNodeAddress       : iqn.1992-08.com.netapp:sn.ea00ea2d1b1d11ec9de16f9cef731025:vs.3
TargetSideIdentifier    : 0200
PSComputerName          :
```

- b. Initialisieren Sie die Festplatten mit dem folgenden PowerShell-Befehl.

```
$disks = Get-Disk | where PartitionStyle -eq raw
foreach ($disk in $disks) {Initialize-Disk $disk.Number}
```

```
PS C:\Windows\system32> $disks = Get-Disk | where PartitionStyle -eq raw
foreach ($disk in $disks) {Initialize-Disk $disk.Number}
PS C:\Windows\system32> Get-Disk
```

Number	Friendly Name	Serial Number	HealthStatus	OperationalStatus	Total Size	Partition Style
0	AWS PVDISK	vo105d1c31fcb4c790ab	Healthy	Online	30 GB	MBR
1	NETAPP LUN C-Mode	1wB0p7RmR2s2	Healthy	Online	700 GB	GPT
2	NETAPP LUN C-Mode	1wB0p7RmR2s3	Healthy	Online	100 GB	GPT

c. Führen Sie die Befehle Partition erstellen und Disk formatieren mit PowerShell aus.

```
New-Partition -DiskNumber 1 -DriveLetter F -UseMaximumSize
Format-Volume -DriveLetter F -FileSystem NTFS -AllocationUnitSize
65536
New-Partition -DiskNumber 2 -DriveLetter G -UseMaximumSize
Format-Volume -DriveLetter G -FileSystem NTFS -AllocationUnitSize
65536
```

Sie können die Erstellung von Volumes und LUNs mit dem PowerShell Skript aus Anhang B. automatisieren LUNs können auch mit SnapCenter erstellt werden.

Sobald die Volumes und LUNs definiert sind, müssen Sie SnapCenter einrichten, um die Datenbankvorgänge ausführen zu können.

Übersicht über SnapCenter

NetApp SnapCenter ist eine Datensicherungssoftware der nächsten Generation für Tier-1-Enterprise-Applikationen. Mit der zentralen Management-Oberfläche automatisiert und vereinfacht SnapCenter manuelle, komplexe und zeitintensive Prozesse, die im Zusammenhang mit Backup, Recovery und dem Klonen zahlreicher Datenbanken und anderer Applikations-Workloads anfallen. SnapCenter nutzt NetApp Technologien, darunter NetApp Snapshot, NetApp SnapMirror, SnapRestore und NetApp FlexClone. Dank dieser Integration können IT-Abteilungen ihre Storage-Infrastruktur skalieren, zunehmend anspruchsvolle SLA-Verpflichtungen erfüllen und die Produktivität der Administratoren im gesamten Unternehmen verbessern.

Anforderungen für SnapCenter Server

In der folgenden Tabelle sind die Mindestanforderungen für die Installation des SnapCenter-Servers und des Plug-ins unter Microsoft Windows Server aufgeführt.

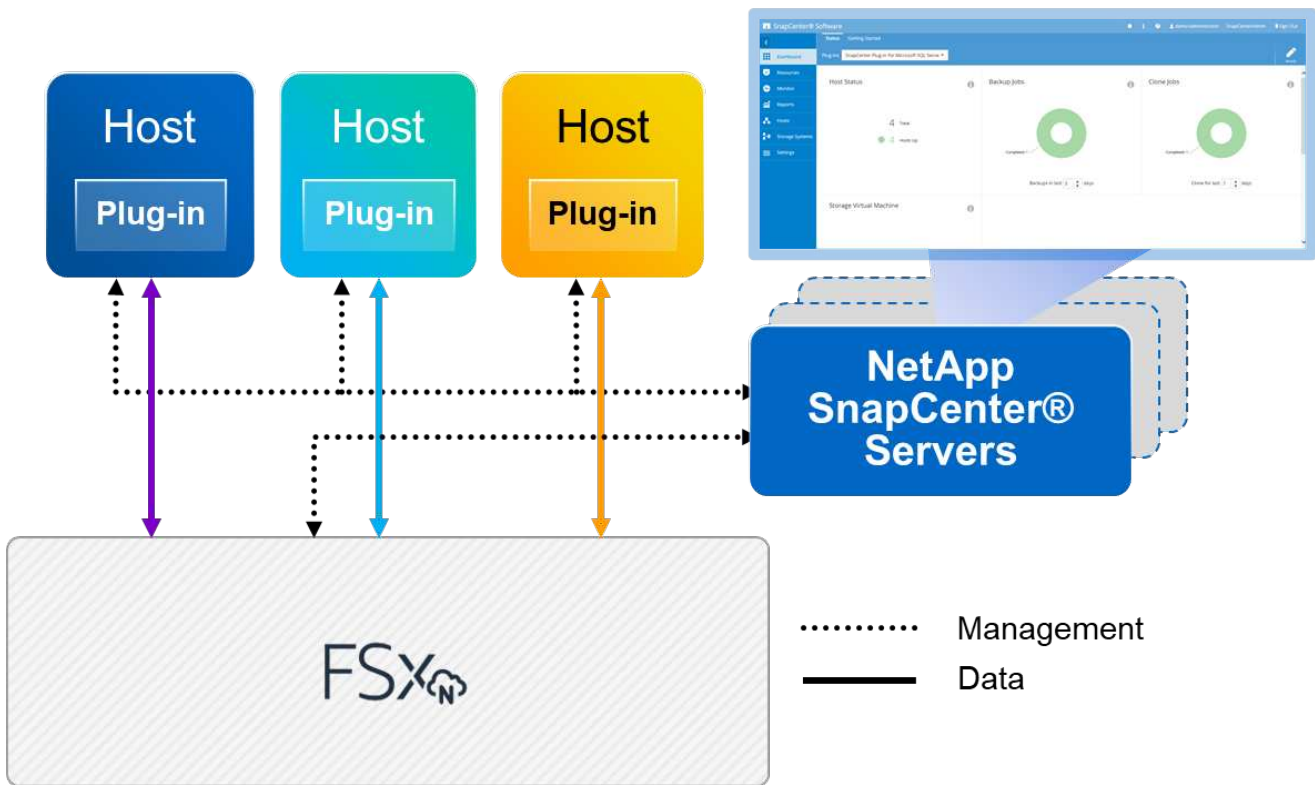
Komponenten	Anforderungen
Minimale CPU-Anzahl	Vier Kerne/vCPUs
Speicher	Minimum: 8 GB empfohlen: 32 GB
Speicherplatz	Minimaler Installationsspeicherplatz: 10 GB für das Repository: 10 GB
Unterstütztes Betriebssystem	<ul style="list-style-type: none">• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019
Softwarepakete	<ul style="list-style-type: none">• .NET 4.5.2 oder höher• Windows Management Framework (WMF) 4.0 oder höher• PowerShell 4.0 oder höher

Weitere Informationen finden Sie unter ["Platz- und Dimensionierungsanforderungen"](#).

Informationen zur Versionskompatibilität finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

Datenbank-Storage-Layout

Die folgende Abbildung zeigt einige Überlegungen beim Erstellen des Microsoft SQL Server Datenbank-Storage-Layouts beim Backup mit SnapCenter.



Best Practices

1. Platzieren Sie Datenbanken mit I/O-intensiven Abfragen oder einer großen Datenbankgröße (beispielsweise 500 GB oder mehr) auf einem separaten Volume, um eine schnellere Recovery zu ermöglichen. Dieses Volumen sollte auch durch separate Jobs gesichert werden.
2. Konsolidierung von Datenbanken kleiner bis mittlerer Größe, die weniger kritisch sind oder weniger I/O-Anforderungen auf ein einzelnes Volume haben. Wenn eine große Anzahl von Datenbanken auf demselben Volume gesichert wird, benötigen Sie weniger Snapshot Kopien. Als Best Practice wird außerdem empfohlen, Microsoft SQL Server Instanzen zu konsolidieren, um dieselben Volumes zu verwenden, um die Anzahl der erstellten Backup-Snapshot-Kopien zu steuern.
3. Erstellen Sie separate LUNs, um Dateien zu vollständigen Text und Datei-Streaming zu speichern.
4. Weisen Sie separate LUNs pro Host zu, um Microsoft SQL Server-Protokoll-Backups zu speichern.
5. Systemdatenbanken, in denen Metadaten des Datenbankservers konfiguriert und Einzelheiten zu Jobs gespeichert sind, werden nicht häufig aktualisiert. Legen Sie Systemdatenbanken/tempdb in separate Laufwerke oder LUNs. Platzieren Sie keine Systemdatenbanken auf demselben Volume wie die Benutzerdatenbanken. Benutzerdatenbanken haben eine andere Backup-Richtlinie, und die Häufigkeit der Backups in der Benutzerdatenbank ist bei Systemdatenbanken nicht identisch.
6. Legen Sie für die Einrichtung der Microsoft SQL Server Availability Group Daten und Protokolldateien für Replikate in einer identischen Ordnerstruktur auf allen Knoten ab.

Neben dem Performance-Vorteil, den das Benutzerdatenbanklayout in verschiedene Volumes aufzuteilen, wirkt sich die Datenbank auch deutlich auf die für Backups und Restores erforderliche Zeit aus. Die Verwendung separater Volumes für Daten- und Log-Dateien verkürzt die Wiederherstellungszeit

erheblich, im Vergleich zu einem Volume, das mehrere Benutzerdatendateien hostet. Außerdem sind Benutzerdatenbanken mit einer hohen I/O-intensiven Applikation anfällig für eine höhere Backup-Zeit. Eine ausführlichere Erläuterung der Backup- und Restore-Verfahren finden Sie weiter unten in diesem Dokument.



Beginnend mit SQL Server 2012 (11.x), Systemdatenbanken (Master, Model, MSDB und tempdb), Zudem können Datenbanken mit Database Engine Benutzern als Storage-Option mit einem SMB-Dateiserver installiert werden. Dies gilt sowohl für Standalone SQL Server als auch für SQL Server Failover Cluster-Installationen. Damit können Sie FSX für ONTAP mit sämtlichen Performance- und Datenmanagementfunktionen einsetzen, einschließlich Volume-Kapazität, Performance-Skalierbarkeit und Datensicherungsfunktionen, die SQL Server nutzen kann. Freigaben, die von den Applikationsservern verwendet werden, müssen mit der kontinuierlich verfügbaren Eigenschaft konfiguriert werden. Das Volume sollte dann mit dem NTFS-Sicherheitsstil erstellt werden. NetApp SnapCenter kann nicht zusammen mit Datenbanken verwendet werden, die auf SMB-Freigaben von FSX für ONTAP platziert sind.



Für SQL Server-Datenbanken, die keine Backups mit SnapCenter durchführen, empfiehlt Microsoft, die Daten und Log-Dateien auf separaten Laufwerken zu platzieren. Bei Anwendungen, die gleichzeitig Daten aktualisieren und anfordern, ist die Protokolldatei schreibintensiv und die Datendatei (je nach Anwendung) ist Lese-/schreibintensiv. Für den Datenabruf wird die Protokolldatei nicht benötigt. Daher können Datenanfragen aus der Datendatei auf dem eigenen Laufwerk bearbeitet werden.



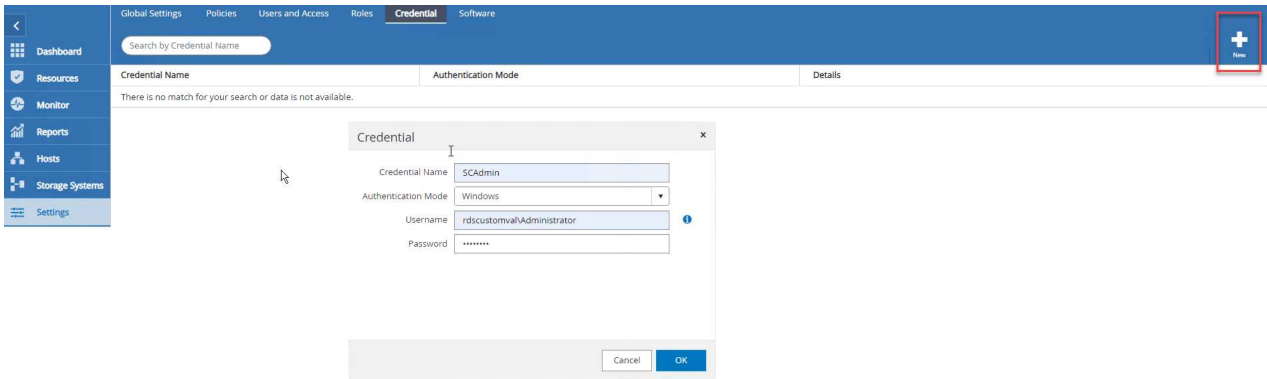
Wenn Sie eine neue Datenbank erstellen, empfiehlt Microsoft, getrennte Laufwerke für die Daten und Protokolle anzugeben. Um Dateien nach der Datenbankerstellung zu verschieben, muss die Datenbank offline geschaltet werden. Weitere Empfehlungen von Microsoft finden Sie unter Daten und Protokolldateien auf separaten Laufwerken platzieren.

Installation und Einrichtung für SnapCenter

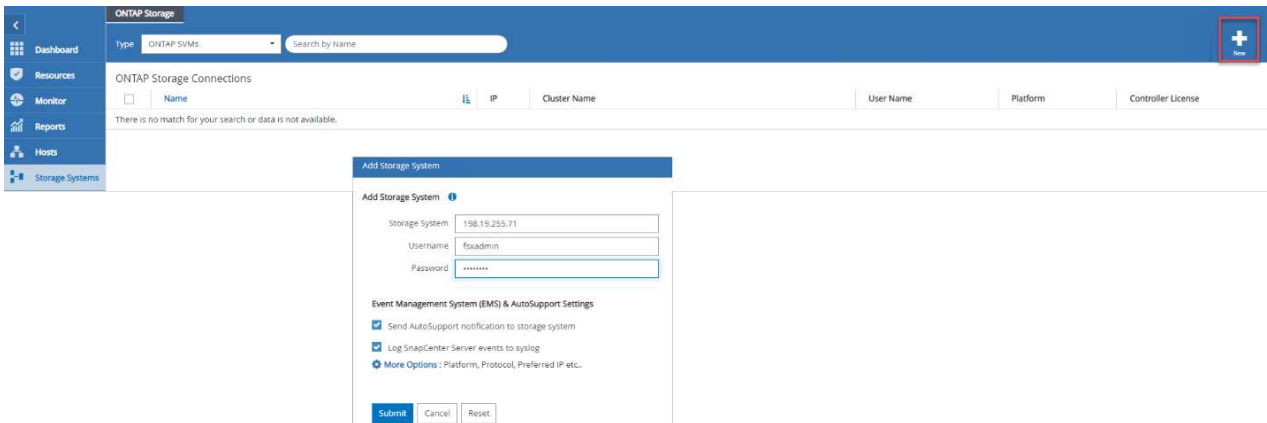
Folgen Sie den "[Installieren Sie den SnapCenter-Server](#)" Und "[Installieren des SnapCenter Plug-ins für Microsoft SQL Server](#)" Um SnapCenter zu installieren und einzurichten.

Führen Sie nach der Installation von SnapCenter die folgenden Schritte aus, um sie einzurichten.

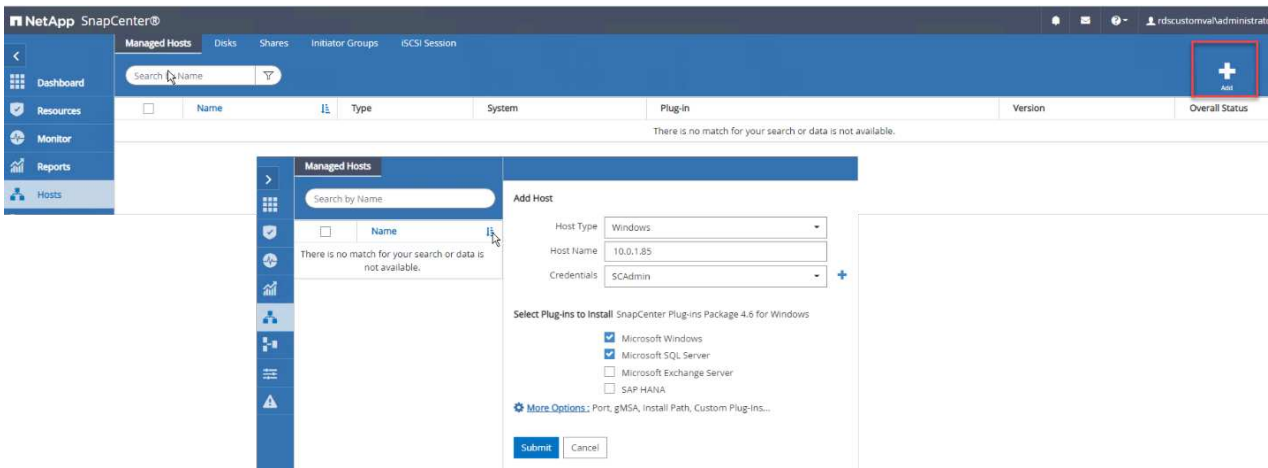
1. Um Anmeldeinformationen einzurichten, wählen Sie **Einstellungen > Neu** und geben Sie die Anmeldeinformationen ein.



2. Fügen Sie das Storage-System hinzu, indem Sie Storage-Systeme > Neu auswählen und die entsprechende FSX für ONTAP-Storage-Informationen bereitstellen.



3. Fügen Sie Hosts hinzu, indem Sie **Hosts > Add** auswählen und dann die Hostinformationen angeben. SnapCenter installiert das Windows und SQL Server Plug-in automatisch. Dieser Vorgang kann einige Zeit in Anspruch nehmen.



Nachdem alle Plug-ins installiert sind, müssen Sie das Protokollverzeichnis konfigurieren. Dies ist der Speicherort, an dem sich das Transaktions-Log-Backup befindet. Sie können das Protokollverzeichnis konfigurieren, indem Sie den Host auswählen und dann das Protokollverzeichnis konfigurieren auswählen.



SnapCenter verwendet ein Host-Protokollverzeichnis zum Speichern von Backup-Daten für Transaktionsprotokolle. Dieser Punkt befindet sich auf Host- und Instanzebene. Jeder von SnapCenter verwendete SQL Server-Host muss über ein Host-Protokollverzeichnis für die Durchführung von Protokoll-Backups verfügen. Bei SnapCenter gibt es ein Datenbank-Repository, sodass Metadaten, die mit Backup-, Restore- oder Klonvorgängen verbunden sind, in einem zentralen Datenbank-Repository gespeichert werden.

Die Größe des Host-Protokollverzeichnisses wird wie folgt berechnet:

Größe des Host-Log-Verzeichnisses = Größe der Systemdatenbank + (maximale DB LDF-Größe × tägliche Log-Änderungsrate % × (Snapshot-Kopie-Aufbewahrung) ÷ (1 – LUN-Overhead-Platz %))

Die Größenformel für das Host-Protokoll-Verzeichnis setzt folgende voraus:

- Eine Systemdatenbank-Sicherung, die die tempdb-Datenbank nicht enthält
- Eine 10% LUN Overheadfläche somit ist das Host-Log-Verzeichnis auf einem dedizierten Volume oder einer LUN vorhanden. Die Datenmenge im Host-Log-Verzeichnis hängt von der Größe der Backups und der Anzahl der Tage ab, die Backups aufbewahrt werden.

Managed Hosts

Search by Name

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	RDSAMAZ-FFIDFMR.rdscustomval.com

Host Details

Host Name RDSAMAZ-FFIDFMR.rdscustomval.com

Host IP 10.0.1.56

Overall Status ● Configure log directory

Host Type Windows

System Stand-alone

Credentials SCAdmin

Plug-ins SnapCenter Plug-ins package 4.6.0.6965 for Windows

- ✓ Microsoft Windows
- ✓ Microsoft SQL Server [Remove](#) [Configure log directory](#)

More Options : Port, gMSA, Install Path, Add Plug-Ins...

Wenn die LUNs bereits bereitgestellt wurden, können Sie den Bereitstellungspunkt auswählen, der das Host-Protokollverzeichnis darstellt.

Configure Plug-in for SQL Server x

Configure the log backup directory for RDSAMAZ-FFIDFMR.rdscustomval.com

Configure host log directory

Host log directory

Choose directory on NetApp Storage

RDSAMAZ-FFIDFMR.rdscustomval.com

- D:\FSxN\Data\
- D:\FSxN\HLD\
- D:\FSxN\Log\

Sie können nun Backup-, Restore- und Klonvorgänge für SQL Server ausführen.

Backup der Datenbank mit SnapCenter

Nachdem Sie die Datenbank und die Protokolldateien auf den FSX ONTAP LUNs platziert haben, kann SnapCenter zum Sichern der Datenbanken verwendet werden. Mit den folgenden Prozessen wird ein vollständiges Backup erstellt.

Best Practices

- In SnapCenter wird RPO als Backup-Häufigkeit identifiziert, beispielsweise wie oft das Backup geplant werden soll, damit sich der Datenverlust auf bis zu wenige Minuten reduzieren lässt. Mit SnapCenter lassen sich Backups alle fünf Minuten planen. Allerdings kann es einige Instanzen geben, in denen ein Backup während der Transaktionszeiten nicht innerhalb von fünf Minuten abgeschlossen wird, oder wenn die Änderungsrate der Daten in der gegebenen Zeit eher liegt. Als Best Practice empfiehlt es sich, häufige Transaktions-Log-Backups anstelle vollständiger Backups zu planen.
- Es gibt zahlreiche Ansätze für RPO und RTO. Eine Alternative zu diesem Backup-Ansatz besteht darin, separate Backup-Richtlinien für Daten und Protokolle mit unterschiedlichen Intervallen zu verwenden. Von SnapCenter aus sollten Sie beispielsweise Backup-Protokolle in 15-Minuten-Intervallen planen und Daten-Backups in 6-Stunden-Intervallen durchführen.
- Verwenden Sie eine Ressourcengruppe für eine Backup-Konfiguration zur Snapshot-Optimierung und zur Anzahl der zu verwaltenden Jobs.
 - a. Wählen Sie **Ressourcen**, und wählen Sie dann **Microsoft SQL Server** *im Dropdown-Menü oben links. Wählen Sie ***Ressourcen Aktualisieren**.

IT	Name	Instance	Host	Last Backup	Overall Status	Type
	DWConfiguration	RD5AMAZ-FFDFMR	RD5AMAZ-FFDFMR.us-east-1.amazonaws.com		Not available for backup	User database
	DWQueue	RD5AMAZ-FFDFMR	RD5AMAZ-FFDFMR.us-east-1.amazonaws.com		Not available for backup	User database
	master	RD5AMAZ-FFDFMR	RD5AMAZ-FFDFMR.us-east-1.amazonaws.com		Not available for backup	System database
	model	RD5AMAZ-FFDFMR	RD5AMAZ-FFDFMR.us-east-1.amazonaws.com		Not available for backup	System database
	msdb	RD5AMAZ-FFDFMR	RD5AMAZ-FFDFMR.us-east-1.amazonaws.com		Not available for backup	System database
	SeattleRetail	RD5AMAZ-FFDFMR	RD5AMAZ-FFDFMR.us-east-1.amazonaws.com		Not processed	User database
	tempdb	RD5AMAZ-FFDFMR	RD5AMAZ-FFDFMR.us-east-1.amazonaws.com		Not available for backup	System database

- b. Wählen Sie die zu sichernde Datenbank aus, und wählen Sie dann **Weiter** und **(*)**, um die **Policy hinzuzufügen, falls noch keine Policy erstellt wurde. Befolgen Sie die * Neue SQL Server Backup Policy**, um eine neue Richtlinie zu erstellen.

Name
DWConfiguration
DWDiagnostics
DWQueue
master
model
msdb
SeattleRetail
tempdb



Select one or more policies and configure schedules

Full Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
Full Backup	None	To schedule operations select a policy that has the appropriate schedule associated, or modify the selected policy to allow schedules.

- c. Wählen Sie ggf. den Überprüfungsserver aus. Dieser Server ist der Server, auf dem SnapCenter DBCC CHECKDB ausgeführt wird, nachdem eine vollständige Sicherung erstellt wurde. Klicken Sie auf **Weiter**, um eine Benachrichtigung zu erhalten, und wählen Sie zur Überprüfung **Zusammenfassung**. Klicken Sie nach der Überprüfung auf **Fertig stellen**.

Name
DWConfiguration
DWDiagnostics
DWQueue
master
model
msdb
SeattleRetail
tempdb

1 Resource 2 Policies 3 Verification 4 Notification 5 Summary

Select the verification servers

Verification server:

Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

d. Klicken Sie auf **Jetzt sichern**, um das Backup zu testen. Wählen Sie in den Popup-Fenstern die Option **Backup** aus.

Backup

Create a backup for the selected resource

Resource Name:

Policy: ⓘ

Verify after backup

e. Wählen Sie **Monitor**, um zu überprüfen, ob die Sicherung abgeschlossen wurde.

ID	Status	Name	Start date	End date	Owner
14	✓	Backup of Resource Group 'RDSAMAZ-FIDFMR-SeattleRetail' with policy 'Full Backup'	03/29/2022 1:47:30 AM	03/29/2022 1:47:41 AM	RDS\CUSTOMER\Administrator
18	✓	Create Resource Group 'RDSAMAZ-FIDFMR-SeattleRetail'	03/29/2022 1:45:24 AM	03/29/2022 1:45:26 AM	RDS\CUSTOMER\Administrator
12	✓	Create Policy 'Full Backup'	03/29/2022 1:41:37 AM	03/29/2022 1:41:40 AM	RDS\CUSTOMER\Administrator
11	✓	Discover resources for all hosts	03/29/2022 1:38:12 AM	03/29/2022 1:38:17 AM	RDS\CUSTOMER\Administrator

Best Practices

- Sichern Sie das Transaktions-Log-Backup von SnapCenter, damit SnapCenter während des Wiederherstellungsprozesses alle Backup-Dateien lesen und automatisch nacheinander wiederherstellen kann.
- Wenn Produkte von Drittanbietern für Backups verwendet werden, wählen Sie Backup in SnapCenter kopieren aus, um Probleme mit der Protokollsequenz zu vermeiden, und testen Sie die Wiederherstellungsfunktion, bevor Sie in die Produktion gehen.

Datenbank mit SnapCenter wiederherstellen

Einer der größten Vorteile von FSX ONTAP mit SQL Server auf EC2 ist die Möglichkeit, auf jeder Datenbankebene schnelle und granulare Wiederherstellungen durchzuführen.

Führen Sie die folgenden Schritte aus, um eine individuelle Datenbank auf einen bestimmten Zeitpunkt oder bis zu einer Minute mit SnapCenter wiederherzustellen.

1. Wählen Sie Ressourcen und dann die Datenbank aus, die Sie wiederherstellen möchten.



Backup Name	Count	Type	End Date	Verified
RDSAMAZ-FFIDFMR_SeattleRetail_RDSAMAZ-FFIDFMR_03-29-2022_01.47.31.3117	1	Full backup	03/29/2022 1:47:31 AM	Unverified

2. Wählen Sie den Backupnamen aus, von dem die Datenbank wiederhergestellt werden soll, und wählen Sie anschließend Wiederherstellen.
3. Folgen Sie den *Restore* Pop-up-Fenstern, um die Datenbank wiederherzustellen.
4. Wählen Sie **Monitor**, um zu überprüfen, ob der Wiederherstellungsprozess erfolgreich ist.



ID	Status	Name	Start date	End date	Owner
106	✓	Restore 'RDSAMAZ-FFIDFMR/SeattleRetail'	03/29/2022 1:54:21 AM	03/29/2022 1:56:29 AM	RDSCLTOMPAK\Administrator
104	✓	Backup of Resource Group 'RDSAMAZ-FFIDFMR/SeattleRetail' with policy 'Full Backup'	03/29/2022 1:47:30 AM	03/29/2022 1:47:41 AM	RDSCLTOMPAK\Administrator
93	✓	Create Resource Group 'RDSAMAZ-FFIDFMR/SeattleRetail'	03/29/2022 1:45:24 AM	03/29/2022 1:45:24 AM	RDSCLTOMPAK\Administrator
92	✓	Create Policy 'Full Backup'	03/29/2022 1:41:37 AM	03/29/2022 1:41:40 AM	RDSCLTOMPAK\Administrator
81	✓	Discover resources for all hosts	03/29/2022 1:38:12 AM	03/29/2022 1:38:17 AM	RDSCLTOMPAK\Administrator
88	✓	Discover resources for host 'RDSAMAZ-FFIDFMR.rds.amazonaws.com'	03/29/2022 10:55:17 PM	03/29/2022 10:55:18 PM	RDSCLTOMPAK\Administrator
87	✓	Discover resources for host 'RDSAMAZ-FFIDFMR.rds.amazonaws.com'	03/28/2022 10:41:18 PM	03/28/2022 10:41:19 PM	RDSCLTOMPAK\Administrator

Überlegungen für eine Instanz mit einer großen Anzahl von Datenbanken kleiner bis großer Größe

SnapCenter kann eine große Anzahl an umfangreichen Datenbanken in einer Instanz oder Gruppe von Instanzen innerhalb einer Ressourcengruppe sichern. Die Größe einer Datenbank ist kein entscheidender Faktor für die Backup-Zeit. Die Dauer eines Backups kann je nach Anzahl der LUNs pro Volume, der Belastung von Microsoft SQL Server, der Gesamtzahl der Datenbanken pro Instanz und insbesondere der I/O-Bandbreite und -Nutzung variieren. Während Sie die Richtlinie für das Backup von Datenbanken aus einer Instanz oder Ressourcengruppe konfigurieren, empfiehlt NetApp, die maximal pro Snapshot-Kopie gesicherte Datenbank auf 100 pro Host einzuschränken. Stellen Sie sicher, dass die Gesamtzahl an Snapshot Kopien die Begrenzung von 1,023 Kopien nicht überschreitet.

NetApp empfiehlt zudem, die laufenden Backup-Jobs parallel zu begrenzen, indem Sie die Anzahl der Datenbanken gruppieren, anstatt für jede Datenbank oder jede Instanz mehrere Jobs zu erstellen. Für eine optimale Performance der Backup-Dauer ist die Anzahl der Backup-Jobs auf eine Anzahl reduziert, die rund 100 oder weniger Datenbanken gleichzeitig sichern kann.

Wie bereits erwähnt, ist die I/O-Nutzung ein wichtiger Faktor für den Backup-Prozess. Der Backup-Prozess muss warten, bis alle I/O-Vorgänge einer Datenbank abgeschlossen sind. Datenbanken mit sehr intensiven I/O-Vorgängen sollten auf eine andere Backup-Zeit zurückgestellt werden oder von anderen Backup-Jobs isoliert werden, um zu vermeiden, dass andere Ressourcen innerhalb derselben Ressourcengruppe, die gesichert werden soll, beeinträchtigt werden.

Setzen Sie für eine Umgebung mit sechs Microsoft SQL Server Hosts, die 200 Datenbanken pro Instanz hosten. Angenommen, vier LUNs pro Host und eine LUN pro erstelltem Volume sollten Sie die vollständige Backup-Richtlinie mit der maximalen Anzahl an Datenbanken, die pro Snapshot Kopie gesichert werden, auf 100 ein. Zweihundert Datenbanken auf jeder Instanz werden als 200 Datendateien verteilt auf zwei LUNs verteilt, und 200 Log-Dateien werden gleichmäßig auf zwei LUNs verteilt: 100 Dateien pro LUN pro Volume.

Planen Sie drei Backup-Jobs, indem Sie drei Ressourcengruppen erstellen, wobei jeweils zwei Instanzen mit insgesamt 400 Datenbanken gruppiert werden.

Alle drei Backup-Jobs werden parallel ausgeführt und sichern gleichzeitig 1,200 Datenbanken. Abhängig von der Last für den Server und der I/O-Nutzung können die Start- und Endzeit jeder Instanz variieren. In dieser Instanz werden insgesamt 24 Snapshot Kopien erstellt.

Zusätzlich zum vollständigen Backup empfiehlt NetApp, ein Transaktions-Log-Backup für kritische Datenbanken zu konfigurieren. Stellen Sie sicher, dass die Datenbankeneigenschaft auf ein vollständiges Recovery-Modell eingestellt ist.

Best Practices

1. Nehmen Sie die tempdb-Datenbank nicht in ein Backup auf, da die darin enthaltenen Daten temporär sind. Platzieren Sie tempdb auf eine LUN oder eine SMB-Freigabe, die sich in einem Storage-System-Volume befindet, in dem keine Snapshot Kopien erstellt werden.
2. Eine Microsoft SQL Server Instanz mit einer hohen I/O-intensiven Applikation sollte in einem anderen Backup-Job isoliert werden, um die gesamte Backup-Zeit für andere Ressourcen zu reduzieren.
3. Begrenzen Sie die Anzahl der Datenbanken, die gleichzeitig auf etwa 100 gesichert werden sollen, und Staffeln Sie die übrigen Datenbank-Backups, um einen gleichzeitigen Prozess zu vermeiden.
4. Verwenden Sie den Instanznamen für Microsoft SQL Server in der Ressourcengruppe anstelle mehrerer Datenbanken, da SnapCenter beim Erstellen neuer Datenbanken in der Microsoft SQL Server-Instanz automatisch eine neue Datenbank für das Backup berücksichtigt.
5. Wenn Sie die Datenbankkonfiguration ändern, wie beispielsweise das Datenbank-Recovery-Modell in

das vollständige Recovery-Modell ändern, führen Sie sofort ein Backup durch, um up-to-the-minute-Wiederherstellungsvorgänge zu ermöglichen.

6. SnapCenter kann Transaktions-Log-Backups, die außerhalb von SnapCenter erstellt wurden, nicht wiederherstellen.
7. Stellen Sie beim Klonen von FlexVol Volumes sicher, dass ausreichend Speicherplatz für die Klon-Metadaten vorhanden ist.
8. Stellen Sie beim Wiederherstellen von Datenbanken sicher, dass auf dem Volume ausreichend Speicherplatz verfügbar ist.
9. Erstellen einer separaten Richtlinie für das Management und die Sicherung von Systemdatenbanken mindestens einmal pro Woche

Klonen von Datenbanken mit SnapCenter

Um eine Datenbank an einem anderen Standort in einer Entwicklungs- oder Testumgebung oder zur Erstellung einer Kopie für geschäftliche Analysen zu wiederherstellen, empfiehlt NetApp die Nutzung der Cloning-Methodik, um eine Kopie der Datenbank auf derselben Instanz oder einer alternativen Instanz zu erstellen.

Das Klonen von Datenbanken, die 500 GB auf einer iSCSI-Festplatte sind, die auf einer FSX für ONTAP-Umgebung gehostet wird, dauert normalerweise weniger als fünf Minuten. Nach Abschluss des Klonens kann der Benutzer anschließend alle erforderlichen Lese-/Schreibvorgänge für die geklonte Datenbank ausführen. Die meiste Zeit wird für das Scannen von Festplatten benötigt (diskpart). Das Klonverfahren von NetApp dauert unabhängig von der Größe der Datenbanken normalerweise weniger als 2 Minuten.

Das Klonen einer Datenbank kann mit der dualen Methode durchgeführt werden: Sie können einen Klon aus dem letzten Backup erstellen oder das Lebenszyklusmanagement von Klonen verwenden, mit dem die neueste Kopie auf der sekundären Instanz zur Verfügung gestellt werden kann.

SnapCenter ermöglicht Ihnen, die Klonkopie auf der erforderlichen Festplatte zu mounten, um das Format der Ordnerstruktur auf der sekundären Instanz beizubehalten und Backup-Jobs weiterhin zu planen.

Klonen von Datenbanken auf den neuen Datenbanknamen in derselben Instanz

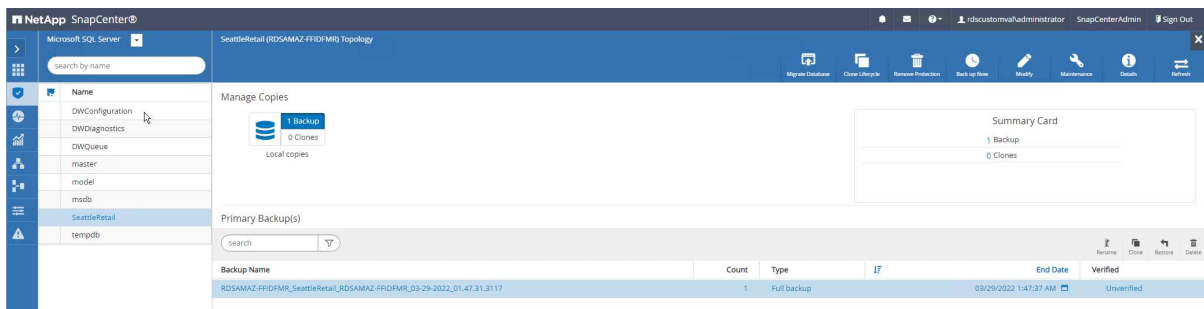
Mit den folgenden Schritten können Datenbanken in derselben SQL Server Instanz geklont werden, die auf EC2 ausgeführt wird:

1. Wählen Sie Ressourcen und dann die Datenbank aus, die geklont werden soll.
2. Wählen Sie den Backup-Namen aus, den Sie klonen möchten, und wählen Sie Clone aus.
3. Befolgen Sie die Anweisungen zum Klonen im Backup-Fenster, um den Klonprozess abzuschließen.
4. Wählen Sie Überwachen, um sicherzustellen, dass das Klonen abgeschlossen ist.

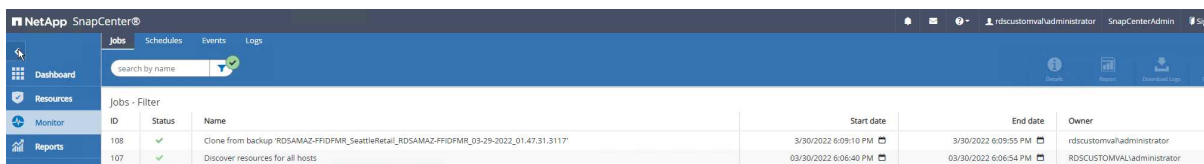
Klonen von Datenbanken in der neuen SQL Server-Instanz, die auf EC2 ausgeführt wird

Mit dem folgenden Schritt werden Datenbanken zu der neuen SQL Server-Instanz geklont, die auf EC2 läuft:

1. Einen neuen SQL Server auf EC2 in derselben VPC erstellen.
2. Aktivieren Sie das iSCSI-Protokoll und MPIO, und richten Sie dann die iSCSI-Verbindung zu FSX für ONTAP ein, indem Sie Schritt 3 und 4 im Abschnitt „Volumes und LUNs für SQL Server erstellen“ befolgen.
3. Fügen Sie einen neuen SQL Server auf EC2 in SnapCenter durch folgen Sie Schritt 3 im Abschnitt „Installieren und Einrichten für SnapCenter.“
4. Wählen Sie Ressource > Instanz anzeigen, und wählen Sie Ressource aktualisieren.
5. Wählen Sie Ressourcen und dann die Datenbank aus, die Sie klonen möchten.
6. Wählen Sie den Backup-Namen aus, den Sie klonen möchten, und wählen Sie dann Klonen aus.



7. Befolgen Sie die Anweisungen zum Klonen aus Backup, indem Sie die neue SQL Server Instanz auf EC2 und den Instanznamen angeben, um den Klonprozess abzuschließen.
8. Wählen Sie Überwachen, um sicherzustellen, dass das Klonen abgeschlossen ist.



Sehen Sie sich das folgende Video an, um mehr über diesen Prozess zu erfahren:

[Klonen von Datenbanken in der neuen SQL Server-Instanz, die auf EC2 ausgeführt wird](#)

Anhänge

Anhang A: YAML-Datei zur Verwendung in Cloud-Formationsvorlage

Die folgende .yaml-Datei kann mit der Cloud-Formationsvorlage in der AWS-Konsole verwendet werden.

- ["https://github.com/NetApp/fsxn-iscsisetup-cft"](https://github.com/NetApp/fsxn-iscsisetup-cft)

Um DIE ISCSI-LUN-Erstellung und die NetApp SnapCenter-Installation mit PowerShell zu automatisieren, klonen Sie die repo von ["Dieser GitHub-Link"](#).

Anhang B: PowerShell Skripte für die Bereitstellung von Volumes und LUNs

Das folgende Skript wird verwendet, um Volumes und LUNs bereitzustellen und iSCSI auf der Grundlage der oben angegebenen Anleitung einzurichten. Es gibt zwei PowerShell Skripte:

- `_EnableMPIO.ps1`

```
Function Install_MPIO_ssh {
    $hostname = $env:COMPUTERNAME
    $hostname = $hostname.Replace('-', '_')

    #Add schedule action for the next step
    $path = Get-Location
    $path = $path.Path + '\2_CreateDisks.ps1'
    $arg = '-NoProfile -WindowStyle Hidden -File ' + $path
    $schAction = New-ScheduledTaskAction -Execute "Powershell.exe"
-Argument $arg
    $schTrigger = New-ScheduledTaskTrigger -AtStartup
    $schPrincipal = New-ScheduledTaskPrincipal -UserId "NT AUTHORITY
\SYSTEM" -LogonType ServiceAccount -RunLevel Highest
    $return = Register-ScheduledTask -Action $schAction -Trigger
$schTrigger -TaskName "Create Vols and LUNs" -Description "Scheduled
Task to run configuration Script At Startup" -Principal $schPrincipal
    #Install -Module PosH-SSH
    Write-host 'Enable MPIO and SSH for PowerShell' -ForegroundColor
Yellow
    $return = Find-PackageProvider -Name 'Nuget' -ForceBootstrap
-IncludeDependencies
    $return = Find-Module PoSH-SSH | Install-Module -Force
    #Install Multipath-IO with PowerShell using elevated privileges in
Windows Servers
    Write-host 'Enable MPIO' -ForegroundColor Yellow
    $return = Install-WindowsFeature -name Multipath-IO -Restart
}
Install_MPIO_ssh
Remove-Item -Path $MyInvocation.MyCommand.Source
```

- `_CreateDisks.ps1`

```
....
#Enable MPIO and Start iSCSI Service
Function PrepISCSI {
    $return = Enable-MSDSMAutomaticClaim -BusType iSCSI
    #Start iSCSI service with PowerShell using elevated privileges in
Windows Servers
```

```

$return = Start-service -Name msiscsi
$return = Set-Service -Name msiscsi -StartupType Automatic
}
Function Create_igroup_vols_luns ($fsxN){
    $hostname = $env:COMPUTERNAME
    $hostname = $hostname.Replace('-', '_')
    $volsluns = @()
    for ($i = 1;$i -lt 10;$i++){
        if ($i -eq 9){
            $volsluns
+=(@{volname=('v_'+$hostname+'_log');volsize=$fsxN.logvolsize;lunname=(
'l_'+$hostname+'_log');lunsize=$fsxN.loglunsize})
        } else {
            $volsluns
+=(@{volname=('v_'+$hostname+'_data'+[string]$i);volsize=$fsxN.datavols
ize;lunname=('l_'+$hostname+'_data'+[string]$i);lunsize=$fsxN.datalunsi
ze})
        }
    }
    $secStringPassword = ConvertTo-SecureString $fsxN.password
-AsPlainText -Force
    $credObject = New-Object System.Management.Automation.PSCredential
($fsxN.login, $secStringPassword)
    $igroup = 'igrp_'+$hostname
    #Connect to FSx N filesystem
    $session = New-SSHSession -ComputerName $fsxN.svmip -Credential
$credObject -AcceptKey:$true
    #Create igroup
    Write-host 'Creating igroup' -ForegroundColor Yellow
    #Find Windows initiator Name with PowerShell using elevated
privileges in Windows Servers
    $initport = Get-InitiatorPort | select -ExpandProperty NodeAddress
    $sshcmd = 'igroup create -igroup ' + $igroup + ' -protocol iscsi
-ostype windows -initiator ' + $initport
    $ret = Invoke-SSHCommand -Command $sshcmd -SSHSession $session
    #Create vols
    Write-host 'Creating Volumes' -ForegroundColor Yellow
    foreach ($vollun in $volsluns){
        $sshcmd = 'vol create ' + $vollun.volname + ' -aggregate agr1
-size ' + $vollun.volsize #+ ' -vserver ' + $vserver
        $return = Invoke-SSHCommand -Command $sshcmd -SSHSession
$session
    }
    #Create LUNs and mapped LUN to igroup
    Write-host 'Creating LUNs and map to igroup' -ForegroundColor
Yellow

```

```

    foreach ($vollun in $volsluns){
        $sshcmd = "lun create -path /vol/" + $vollun.volname + "/" +
$vollun.lunname + " -size " + $vollun.lunsize + " -ostype Windows_2008
" #-vserver " +$vserver
        $return = Invoke-SSHCommand -Command $sshcmd -SSHSession
$session
        #map all luns to igroup
        $sshcmd = "lun map -path /vol/" + $vollun.volname + "/" +
$vollun.lunname + " -igroup " + $igroup
        $return = Invoke-SSHCommand -Command $sshcmd -SSHSession
$session
    }
}
Function Connect_iSCSI_to_SVM ($TargetPortals){
    Write-host 'Online, Initialize and format disks' -ForegroundColor
Yellow
    #Connect Windows Server to svm with iSCSI target.
    foreach ($TargetPortal in $TargetPortals) {
        New-IscsiTargetPortal -TargetPortalAddress $TargetPortal
        for ($i = 1; $i -lt 5; $i++){
            $return = Connect-IscsiTarget -IsMultipathEnabled $true
-IsPersistent $true -NodeAddress (Get-iscsiTarget | select
-ExpandProperty NodeAddress)
        }
    }
}
Function Create_Partition_Format_Disks{

    #Create Partion and format disk
    $disks = Get-Disk | where PartitionStyle -eq raw
    foreach ($disk in $disks) {
        $return = Initialize-Disk $disk.Number
        $partition = New-Partition -DiskNumber $disk.Number
-AssignDriveLetter -UseMaximumSize | Format-Volume -FileSystem NTFS
-AllocationUnitSize 65536 -Confirm:$false -Force
        # $return = Format-Volume -DriveLetter $partition.DriveLetter
-FileSystem NTFS -AllocationUnitSize 65536
    }
}
Function UnregisterTask {
    Unregister-ScheduledTask -TaskName "Create Vols and LUNs"
-Confirm:$false
}
Start-Sleep -s 30
$fsxN = @{svmip ='198.19.255.153';login =
'vsadmin';password='net@pp11';datavolsize='10GB';datalunsize='8GB';logv

```

```
olsize='8GB';loglunsize='6GB'}
$TargetPortals = ('10.2.1.167', '10.2.2.12')
PrepISCSI
Create_igroup_vols_luns $fsxN
Connect_iSCSI_to_SVM $TargetPortals
Create_Partition_Format_Disks
UnregisterTask
Remove-Item -Path $MyInvocation.MyCommand.Source
.....
```

Führen Sie die Datei aus `EnableMPIO.ps1` Zuerst und das zweite Skript wird automatisch ausgeführt, nachdem der Server neu gestartet wurde. Diese PowerShell Skripte können aufgrund von Berechtigungen für den SVM entfernt werden, nachdem sie ausgeführt wurden.

Wo Sie weitere Informationen finden

- Amazon FSX für NetApp ONTAP

["https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html"](https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html)

- Erste Schritte mit FSX für NetApp ONTAP

["https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/getting-started.html"](https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/getting-started.html)

- Überblick über die SnapCenter Schnittstelle

<https://www.youtube.com/watch?v=IVEBF4kV6Ag&t=0s>

- Tour durch Optionen im SnapCenter-Navigationsbereich

https://www.youtube.com/watch?v=_IDKt-koySQ

- SnapCenter 4.0 für SQL Server Plug-in einrichten

<https://www.youtube.com/watch?v=MopbUFSdHKE>

- So sichern und wiederherstellen Sie Datenbanken mit SnapCenter mit SQL Server Plug-in

https://www.youtube.com/watch?v=K343qPD5_Ys

- Wie man eine Datenbank mit SnapCenter mit SQL Server Plug-in klonen kann

<https://www.youtube.com/watch?v=ogEc4DkGv1E>

TR-4897: SQL Server auf Azure NetApp Files - Real Deployment View

Niyaz Mohamed, NetApp

IT-Abteilungen stehen vor der ständigen Veränderung. Gartner meldet, dass bis 2022 fast 75 % aller Datenbanken Cloud-basierten Storage benötigen werden. Microsoft SQL Server ist eine führende Lösung für relationale Datenbanken-Managementsysteme (RDBMS) und eignet sich für Windows-Plattformen sowie Unternehmen, die sich von SQL Server für alles verlassen – von der Enterprise Resource Planning (ERP) über

Big-Data-Analysen bis hin zum Content-Management. SQL Server hat dazu beigetragen, die Art und Weise zu revolutionieren, wie Unternehmen umfangreiche Datensätze managen und ihre Applikationen an die Anforderungen der Schemaschemen und Performance anpassen.

Die meisten IT-Abteilungen verfolgen einen Ansatz, bei dem der „Cloud First“-Ansatz verfolgt. Kunden in einer Transformationsphase: Bewerten Sie ihre aktuelle IT-Umgebung und migrieren sie ihre Datenbank-Workloads anschließend anhand einer Analyse- und Bestandsaufnahme in die Cloud. Einige Faktoren, die Kunden für die Cloud-Migration antreibt, sind Flexibilität/Burst, Datacenter-Ausstieg, Datacenter-Konsolidierung, End-of-Life-Szenarien, Fusionen, Firmenübernahmen usw. Der Grund für die Migration kann je nach Unternehmen und ihren jeweiligen Geschäftsprioritäten variieren. Bei der Umstellung auf die Cloud ist die Wahl des richtigen Cloud-Storage sehr wichtig, um das Potenzial der Cloud-Implementierung von SQL Server Datenbanken auszuschöpfen.

Anwendungsfall

Die Verlagerung der SQL Server-Daten in Azure und die Integration von SQL Server in die zahlreichen Plattform-als-Service-Funktionen (PaaS) von Azure wie Azure Data Factory, Azure IoT Hub und Azure Machine Learning schaffen einen enormen geschäftlichen Nutzen, um die digitale Transformation zu unterstützen. Durch die Einführung der Cloud kann sich auch der jeweilige Geschäftsbereich stärker auf die Produktivität konzentrieren und neue Funktionen und Verbesserungen schneller bereitstellen (DevTest Anwendungsfall), als auf das CAPEX- Modell oder herkömmliche Private Cloud-Modelle zurückgreifen zu müssen. In diesem Dokument wird eine Echtzeit-Implementierung von SQL Server „Always On Availability Group“ (AOAG) auf Azure NetApp Files behandelt, die virtuelle Azure Maschinen nutzen.

Azure NetApp Files bietet Storage der Enterprise-Klasse mit kontinuierlich verfügbaren Dateifreigaben. Kontinuierlich verfügbare Freigaben werden von SQL Server Produktionsdatenbanken auf SMB-Dateifreigaben benötigt, um sicherzustellen, dass der Node immer auf den Datenbank-Storage zugreifen kann, auch in störenden Szenarien wie Controller-Upgrades oder -Ausfälle. Dank kontinuierlich verfügbarer Dateifreigaben ist die Replizierung von Daten zwischen Storage-Nodes nicht mehr erforderlich. Azure NetApp Files nutzt horizontale Skalierbarkeit mit SMB 3.0, persistente Griffe und transparentes Failover zur Unterstützung von unterbrechungsfreiem Betrieb bei geplanten und ungeplanten Ausfallzeiten, einschließlich vieler administrativer Aufgaben.

Wenn Sie Cloud-Migrationen planen, sollten Sie sich immer den besten Ansatz für deren Nutzung entscheiden. Der häufigste und einfachste Ansatz für die Applikationsmigration ist das Rehosting (auch bekannt als „Lift and Shift“). Das Beispielszenario in diesem Dokument verwendet die Methode zum Rehosting. SQL Server auf virtuellen Azure Machines mit Azure NetApp Files ermöglicht Ihnen die Verwendung vollständiger Versionen von SQL Server in der Cloud, ohne dass Sie Hardware vor Ort verwalten müssen. SQL Server Virtual Machines (VMs) vereinfachen außerdem die Lizenzkosten, wenn Sie für Kunden zahlen. Darüber hinaus bieten sie Elastizität und Bursting-Funktionen für Entwicklungs-, Test- und Immobilienaktualisierungen.

Zu berücksichtigende Faktoren

VM-Performance

Für die optimale Performance einer relationalen Datenbank in einer Public Cloud ist die Auswahl der richtigen VM-Größe wichtig. Microsoft empfiehlt, weiterhin dieselben Optionen zur Verbesserung der Datenbank-Performance zu verwenden, die für SQL Server in lokalen Serverumgebungen relevant sind. Nutzung ["Speicheroptimierung"](#) VM-Größen für die beste Performance von SQL Server Workloads Sammeln der Performance-Daten einer vorhandenen Bereitstellung, um die RAM- und CPU-Auslastung zu identifizieren und gleichzeitig die richtigen Instanzen auszuwählen Die meisten Implementierungen wählen zwischen der D-, E- oder M-Serie.

Hinweise:

- Verwenden Sie für die beste Performance von SQL Server Workloads eine speicheroptimierte VM-Größe.
- NetApp und Microsoft empfehlen, die Anforderungen an die Storage-Performance zu identifizieren, bevor Sie den Instanztyp mit dem entsprechenden Speicher-zu-Vcore-Verhältnis auswählen. Dadurch ist auch die Auswahl eines Instanztyps mit der richtigen Netzwerkbandbreite möglich, um die Storage-Durchsatzbegrenzungen der VM zu überwinden.

VM-Redundanz

Um Redundanz und Hochverfügbarkeit zu erhöhen, sollten SQL Server VMs sich entweder in derselben befinden "[Verfügbarkeitsgruppe](#)" Oder anders "[Verfügbarkeitszonen](#)". Bei der Erstellung von Azure VMs müssen Sie zwischen der Konfiguration von Verfügbarkeitsgruppen und den Verfügbarkeitszonen wählen. Eine Azure VM kann nicht an beiden teilnehmen.

Hochverfügbarkeit

Für hohe Verfügbarkeit ist die Konfiguration von SQL Server AOAG oder Always On Failover Cluster Instance (FCI) die beste Option. Bei AOAG werden mehrere Instanzen von SQL Server auf Azure Virtual Machines in einem virtuellen Netzwerk durchgeführt. Wenn auf Datenbankebene eine hohe Verfügbarkeit erforderlich ist, sollten Sie die Konfiguration von SQL Server-Verfügbarkeitsgruppen in Betracht ziehen.

Storage-Konfiguration

Microsoft SQL Server kann mit SMB-Dateifreigaben als Storage-Option implementiert werden. Beginnend mit SQL Server 2012, Systemdatenbanken (Master, Model, msdb oder tempdb), Zudem können Benutzerdatenbanken mit dem Server Message Block (SMB)-Dateiserver als Storage-Option installiert werden. Dies gilt sowohl für Standalone-SQL Server als auch für SQL Server FCI.



File Share Storage für SQL Server-Datenbanken sollte kontinuierlich verfügbare Eigenschaft unterstützen. Dadurch ist unterbrechungsfreier Zugriff auf die Dateifreigabedaten möglich.

Azure NetApp Files bietet hochperformanten File-Storage für jeden anspruchsvollen Workload und reduziert die TCO von SQL Server im Vergleich zu Block-Storage-Lösungen. Bei Block-Storage haben VMs Beschränkungen für I/O und Bandbreite für Festplattenoperationen festgelegt. Beschränkungen der Netzwerkbandbreite allein werden auf Azure NetApp Files angewendet. Das heißt, auf Azure NetApp Files werden keine I/O-Limits auf VM-Ebene angewendet. Ohne diese I/O-Limits kann SQL Server auf kleineren, mit Azure NetApp Files verbundenen VMs ihre Performance ebenso wie SQL Server auf wesentlich größeren VMs liefern. Azure NetApp Files senken die Implementierungskosten für SQL Server durch niedrigere Computing- und Softwarelizenzkosten. Detaillierte Kostenanalysen und Performance-Vorteile der Verwendung von Azure NetApp Files für SQL Server-Implementierungen finden Sie im "[Vorteile der Nutzung von Azure NetApp Files für die SQL Server-Implementierung](#)".

Vorteile

Die Verwendung von Azure NetApp Files für SQL Server bietet u. a. folgende Vorteile:

- Durch den Einsatz von Azure NetApp Files können kleinere Instanzen verwendet und somit die Computing-Kosten gesenkt werden.
- Azure NetApp Files reduziert auch die Kosten für Softwarelizenzen und dadurch die TCO insgesamt.
- Die Volume-Umgestaltung und die dynamische Service Level-Funktion optimieren die Kosten, indem sie für stabile Workloads angepasst werden und eine Überprovisionierung vermieden wird.

Hinweise:

- Um Redundanz und Hochverfügbarkeit zu erhöhen, sollten SQL Server VMs sich entweder in derselben befinden "[Verfügbarkeitsgruppe](#)" Oder in einem anderen "[Verfügbarkeitszonen](#)". Beachten Sie die Dateipfadanforderungen, wenn benutzerdefinierte Datendateien erforderlich sind; wählen Sie in diesem Fall SQL FCI über SQL AOAG aus.
- Der folgende UNC-Pfad wird unterstützt: "[\\ANFSMB-b4ca.anf.Test\SQLDB](#) und [\\ANFSMB-b4ca.anf.Test\SQLDB\](#)".
- Der Loopback UNC-Pfad wird nicht unterstützt.
- Verwenden Sie für die Dimensionierung historische Daten aus Ihrer lokalen Umgebung. Bei OLTP-Workloads passen Sie die Ziel-IOPS den Performance-Anforderungen an, wobei Workloads mit durchschnittlichen und Spitzenzeiten sowie den Leistungszählern für Festplattenzugriffe/s und Festplattenschreibvorgänge/s verwendet werden. Bei Data Warehouse- und Reporting-Workloads wird der Zieldurchsatz anhand von Workloads mit durchschnittlichen und Spitzenzeiten sowie den Byte/s der Festplattenschreibdaten und den Byte/Sek. des Festplattenschreibvorgangs angepasst Die Durchschnittswerte können zusammen mit den Funktionen zur Volumenumformung verwendet werden.

Kontinuierlich verfügbare Shares erstellen

Kontinuierlich verfügbare Shares erstellen mit dem Azure Portal oder der Azure CLI Wählen Sie im Portal die Option Eigenschaft kontinuierliche Verfügbarkeit aktivieren aus. Geben Sie bei der Azure-CLI die Freigabe als kontinuierlich verfügbare Freigabe über das an `az netappfiles volume create with the smb-continuously-avl` Die Option ist auf eingestellt `$True`. Weitere Informationen zum Erstellen eines neuen, für kontinuierliche Verfügbarkeit bestimmten Volumes finden Sie unter "[Erstellen einer kontinuierlich verfügbaren Freigabe](#)".

Hinweise:

- Sorgen Sie für eine kontinuierliche Verfügbarkeit des SMB Volume, wie in der folgenden Abbildung dargestellt.
- Wenn ein Domain-Konto ohne Administrator verwendet wird, stellen Sie sicher, dass dem Konto die erforderliche Sicherheitsberechtigung zugewiesen ist.
- Legen Sie die entsprechenden Berechtigungen auf Share-Ebene und die entsprechenden Berechtigungen auf Dateiebene fest.
- Eine kontinuierlich verfügbare Eigenschaft kann auf vorhandenen SMB Volumes nicht aktiviert werden. Um ein vorhandenes Volume zu konvertieren, wird ein kontinuierlich verfügbarer Share verwendet. Nutzen Sie die NetApp Snapshot Technologie. Weitere Informationen finden Sie unter "[Vorhandene SMB Volumes werden konvertiert, um kontinuierliche Verfügbarkeit zu nutzen](#)".

Create a volume ...



Basics **Protocol** Tags Review + create

Configure access to your volume.

Access

Protocol type NFS SMB Dual-protocol (NFSv3 and SMB)

Configuration

Active Directory * ⓘ

Share name * ⓘ

Enable Continuous Availability ⓘ

Review + create

< Previous

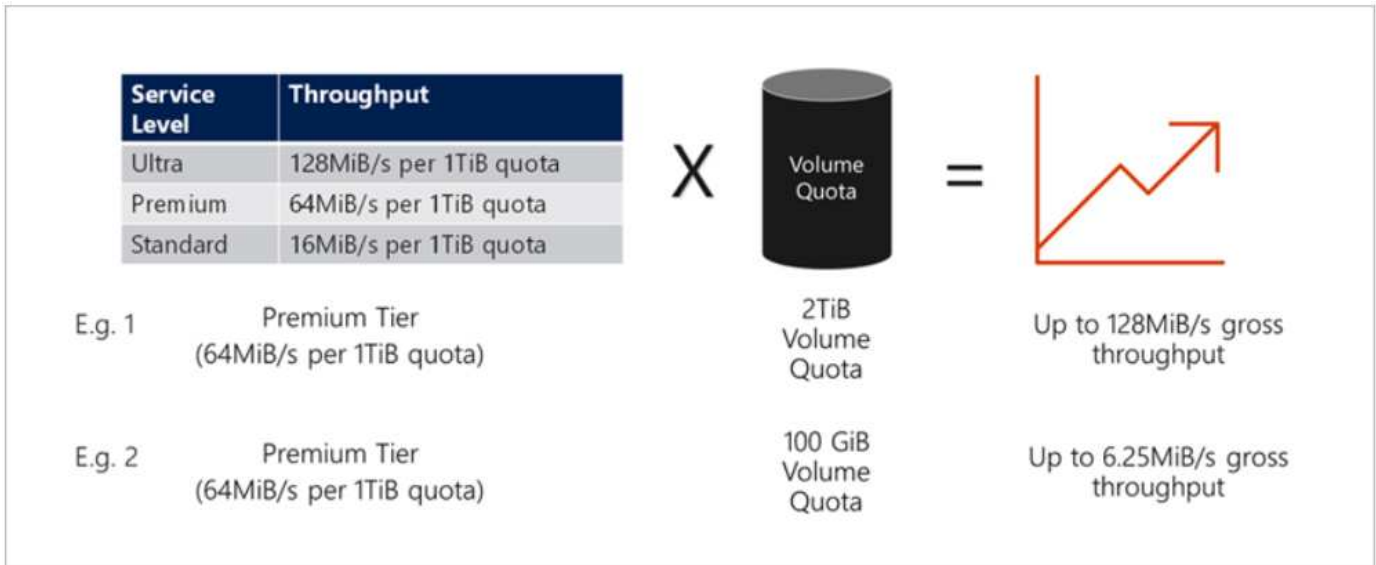
Next : Tags >

Leistung

Azure NetApp Files unterstützt drei Service-Level: Standard (16 Mbit/s pro Terabyte), Premium (64 Mbit/s pro Terabyte) und Ultra (128 Mbit/s pro Terabyte). Die Bereitstellung der passenden Volume-Größe ist für eine optimale Performance des Datenbank-Workloads wichtig. Bei Azure NetApp Files basieren die Volume-Performance und die Durchsatzbegrenzung auf einer Kombination der folgenden Faktoren:

- Der Service Level des Kapazitäts-Pools, zu dem das Volume gehört
- Der dem Volume zugewiesene Kontingent
- Die QoS-Art (Quality of Service) (automatisch oder manuell) des Kapazitäts-Pools

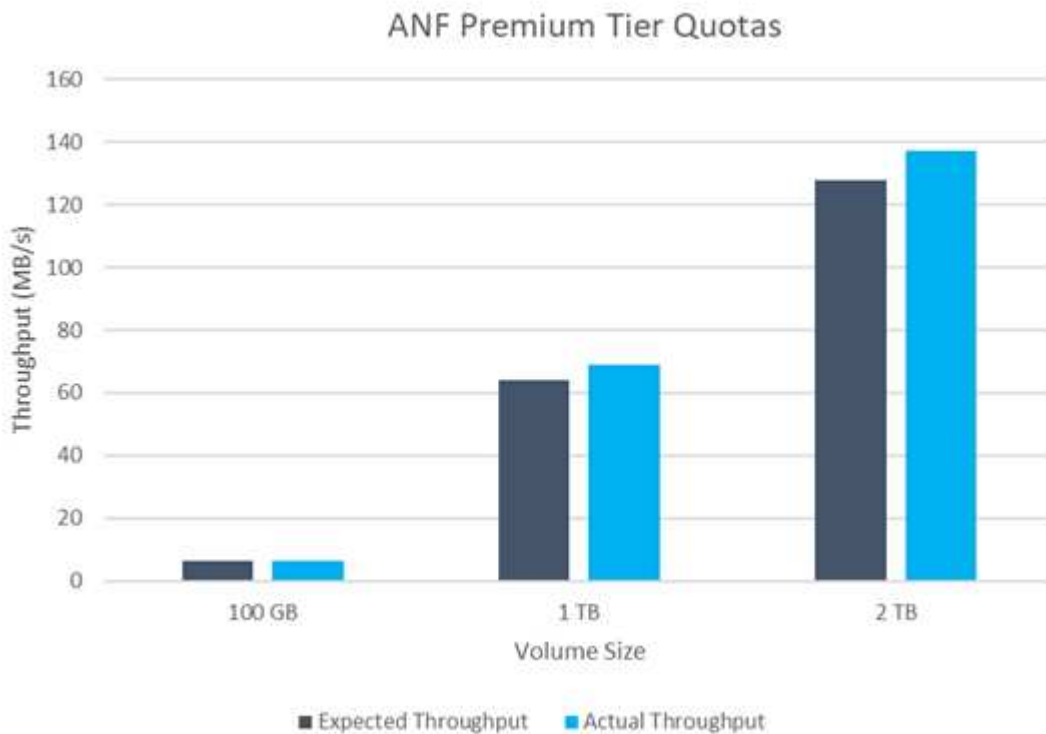
Weitere Informationen finden Sie unter "[Service-Level für Azure NetApp Files](#)".



Performance-Validierung

Wie bei jeder Implementierung sind auch VM- und Storage-Tests entscheidend. Für die Storage-Validierung Tools wie HammerDB, Apploader, die "SQL Server Storage Benchmark-Tool (SB)", Oder jedes benutzerdefinierte Skript oder FIO mit der entsprechenden Lese-Schreib-Mischung verwendet werden sollte. Man sollte jedoch daran denken, dass die meisten SQL Server Workloads, selbst überlastete OLTP-Workloads, näher bei 80–90 % Lese- und 10–20 % Schreibvorgängen liegen.

Um die Performance zu demonstrieren, wurde für ein Volume ein kurzer Test mithilfe von Premium-Service-Leveln durchgeführt. In diesem Test wurde die Volume-Größe spontan von 100 GB auf 2 TB erhöht, ohne dass der Applikationszugriff unterbrochen wird und keine Datenmigration erforderlich ist.



Hier sehen Sie ein weiteres Beispiel für Echtzeit-Performance-Tests mit HammerDB für die in diesem Dokument behandelte Implementierung. Für diese Tests haben wir eine kleine Instanz mit acht vCPUs, einer

500 GB Premium SSD und einem 500 GB SMB Azure NetApp Files Volume verwendet. HammerDB wurde mit 80 Lagerhäusern und acht Anwendern konfiguriert.

Das folgende Diagramm zeigt, dass Azure NetApp Files bei einem Volume einer vergleichbaren Größe (500 GB) eine 2,6-mal so viele Transaktionen pro Minute liefern konnte.

Ein zusätzlicher Test wurde durchgeführt, indem die Größe auf eine größere Instanz mit 32x vCPUs und einem 16-TB-Azure NetApp Files Volume angepasst wurde. Die Anzahl der Transaktionen pro Minute wurde mit einer konsistenten Latenz von 1 ms deutlich erhöht. HammerDB wurde für diesen Test mit 80 Lagerhäusern und 64 Anwendern konfiguriert.



Kostenoptimierung

Azure NetApp Files ermöglicht eine unterbrechungsfreie, transparente Volume-Anpassung und das Ändern der Service Level ohne Ausfallzeiten und Beeinträchtigung von Applikationen. Dies ist eine einzigartige Funktion für ein dynamisches Kostenmanagement, das die Datenbankdimensionierung mit Metriken nicht mehr erfordert. Sie können stattdessen stabile Workloads verwenden, wodurch Vorlaufkosten vermieden werden. Durch die Volume-Umgestaltung und die dynamische Service Level-Änderung können Sie die Bandbreite und das Service Level von Azure NetApp Files Volumes nahezu sofort und ohne Unterbrechung des I/O-Zugriffs anpassen und den Datenzugriff erhalten.

Mit Azure PaaS-Angeboten wie LogicApp oder Funktionen kann die Volume-Größe anhand eines bestimmten Web-Hook- oder Alarm-Regelauslösens problemlos angepasst werden, um die Workload-Anforderungen zu erfüllen und gleichzeitig die Kosten dynamisch zu bewältigen.

Nehmen wir beispielsweise an, eine Datenbank, die 250 MB/s für den stabilen Betrieb benötigt, benötigt jedoch auch einen Spitzendurchsatz von 400 MB/s. In diesem Fall sollte die Implementierung mit einem 4-TB-Volume innerhalb des Premium Service-Levels durchgeführt werden, um die Performance-Anforderungen in stabilem Zustand zu erfüllen. Um Spitzenlasten zu kompensieren, erhöhen Sie die Volume-Größe mithilfe von Azure Funktionen für diesen speziellen Zeitraum auf 7 TB und verkleinern Sie das Volume, um die Bereitstellung kostengünstig zu gestalten. Bei dieser Konfiguration wird eine Überprovisionierung des Storage vermieden.

High-Level-Referenzdesign in Echtzeit

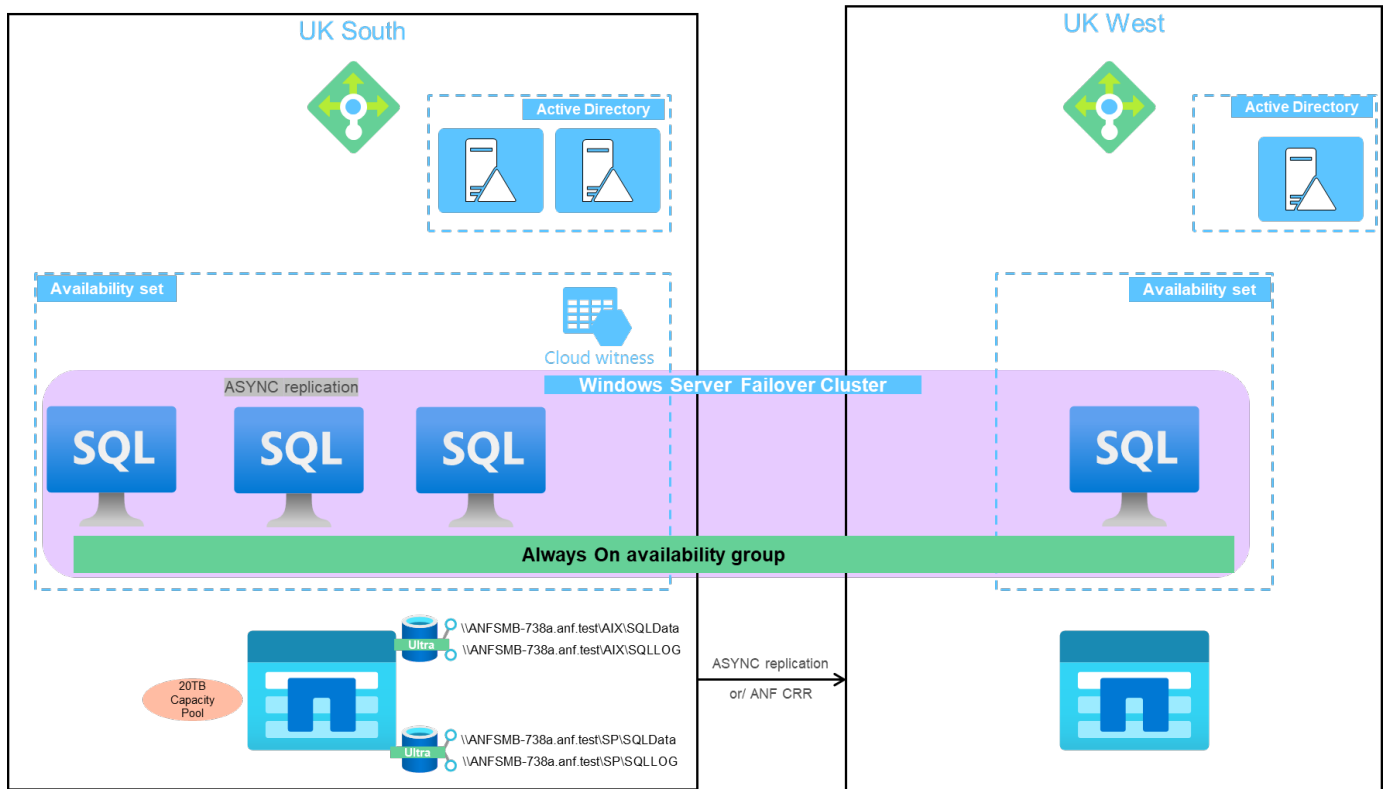
In diesem Abschnitt wird die Echtzeit-Implementierung einer SQL-Datenbank in einer AOAG-Konfiguration

unter Verwendung eines Azure NetApp Files SMB Volume behandelt.

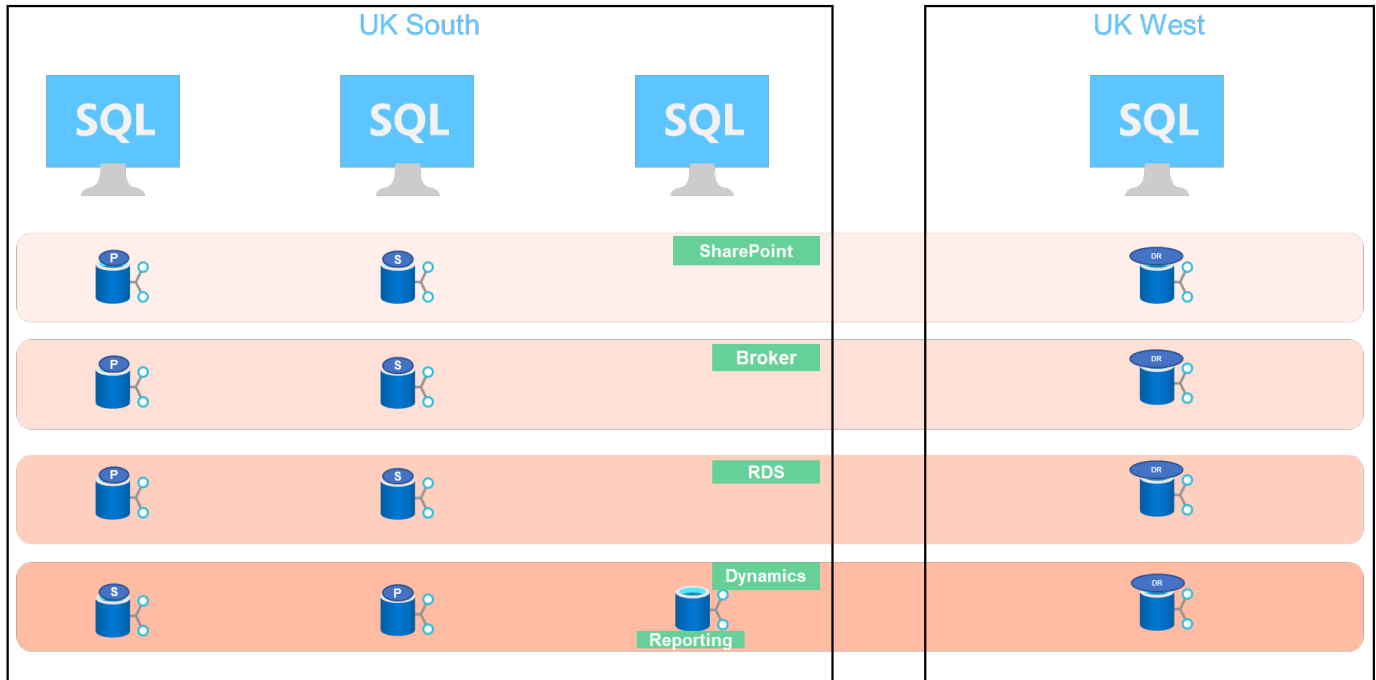
- Anzahl der Knoten: 4
- Anzahl der Datenbanken: 21
- Anzahl der Verfügbarkeitsgruppen: 4
- Backup-Aufbewahrung: 7 Tage
- Backup-Archiv: 365 Tage



Durch die Implementierung von FCI mit SQL Server auf Azure Virtual Machines mit einer Azure NetApp Files-Freigabe wird ein kostengünstiges Modell mit einer einzigen Kopie der Daten bereitgestellt. Mit dieser Lösung können Probleme beim Betrieb von Add-Dateien vermieden werden, wenn sich der Dateipfad vom sekundären Replikat unterscheidet.



Das folgende Bild zeigt die Datenbanken in AOAG, die über die Knoten verteilt sind.



Datenlayout

Die Benutzerdatenbank-Dateien (.mdf) und Transaktions-Log-Dateien der Benutzerdatenbank (.ldf) zusammen mit tempdb werden auf demselben Volume gespeichert. Der Service-Level ist Ultra.

Die Konfiguration besteht aus vier Knoten und vier AGs. Alle 21 Datenbanken (Teil von Dynamic AX, SharePoint, RDS Connection Broker und Indizierungsdienste) werden auf den Azure NetApp Files Volumes gespeichert. Die Datenbanken sind zwischen den AOAG-Knoten ausgeglichen, um die Ressourcen auf den Knoten effektiv zu nutzen. Vier D32 v3-Instanzen werden im WSFC hinzugefügt, der an der AOAG-Konfiguration beteiligt ist. Diese vier Nodes werden im virtuellen Azure-Netzwerk bereitgestellt und nicht von On-Premises-Systemen migriert.

Hinweise:

- Wenn die Protokolle abhängig von der Art der Anwendung und den ausgeführten Abfragen mehr Performance und Durchsatz benötigen, können die Datenbankdateien auf dem Premium-Service-Level platziert werden und die Protokolle können auf dem Ultra-Service-Level gespeichert werden.
- Wenn die tempdb-Dateien auf Azure NetApp Files abgelegt wurden, sollte das Azure NetApp Files-Volume von den Benutzerdatenbankdateien getrennt werden. Hier ist eine Beispielerverteilung der Datenbankdateien in AOAG.

Hinweise:

- Um die Vorteile der auf Snapshot Kopien basierenden Datensicherung weiterhin nutzen zu können, empfiehlt NetApp, Daten und Log-Daten nicht in ein einziges Volume zu kombinieren.
- Ein auf dem primären Replikat durchgeführter Add-File-Vorgang kann auf den sekundären Datenbanken fehlschlagen, wenn sich der Dateipfad einer sekundären Datenbank vom Pfad der entsprechenden primären Datenbank unterscheidet. Dies kann passieren, wenn der Freigabepfad auf primären und sekundären Knoten unterschiedlich ist (aufgrund verschiedener Computerkonten). Der Ausfall kann dazu führen, dass die sekundären Datenbanken ausgesetzt werden. Wenn das Wachstum oder das

Performance-Muster nicht vorhergesagt werden kann und der Plan darin besteht, später Dateien hinzuzufügen, ist ein SQL Server Failover-Cluster mit Azure NetApp Files eine akzeptable Lösung. Bei den meisten Implementierungen erfüllt Azure NetApp Files die Performance-Anforderungen.

Migration

Es gibt verschiedene Möglichkeiten, eine lokale SQL Server Benutzerdatenbank zu SQL Server in einer Azure Virtual Machine zu migrieren. Die Migration kann online oder offline sein. Die ausgewählten Optionen hängen von der SQL Server-Version, den geschäftlichen Anforderungen und den im Unternehmen definierten SLAs ab. Um Ausfallzeiten während des Datenbankmigrationsprozesses zu minimieren, empfiehlt NetApp, entweder die AlwaysOn Option oder die Option zur transaktionsorientierten Replizierung zu verwenden. Wenn es nicht möglich ist, diese Methoden zu verwenden, können Sie die Datenbank manuell migrieren.

Der einfachste und am genauesten getestete Ansatz zum Verschieben von Datenbanken zwischen Maschinen ist Backup und Restore. In der Regel können Sie mit einem Datenbank-Backup und einer Kopie des Datenbank-Backups in Azure beginnen. Anschließend können Sie die Datenbank wiederherstellen. Um die optimale Datentransferleistung zu erzielen, migrieren Sie die Datenbankdateien mithilfe einer komprimierten Backup-Datei in die Azure VM. Das in diesem Dokument erwähnte High-Level-Design verwendet den Backup-Ansatz beim Azure-File-Storage mit Azure File Sync und stellt dann die Wiederherstellung auf Azure NetApp Files her.



Mit Azure Migrate können SQL Server-Workloads ermittelt, bewertet und migriert werden.

Führen Sie die folgenden grundlegenden Schritte aus, um eine Migration durchzuführen:

1. Richten Sie je nach Ihren Anforderungen Konnektivität ein.
2. Ein vollständiges Datenbank-Backup an einem lokalen File-Share-Speicherort
3. Backup-Dateien werden mit Azure-Dateisynchronisation in eine Azure-Dateifreigabe kopiert.
4. Stellen Sie die VM mit der gewünschten Version von SQL Server bereit.
5. Kopieren Sie die Backup-Dateien mit der in die VM `copy` Befehl an einer Eingabeaufforderung.
6. Stellen Sie die vollständigen Datenbanken auf SQL Server auf Azure Virtual Machines wieder her.



Zur Wiederherstellung von 21 Datenbanken dauerte der Einsatz ungefähr neun Stunden. Dieser Ansatz ist spezifisch für dieses Szenario. Die unten aufgeführten Migrationstechniken können jedoch basierend auf Ihrer Situation und Ihren Anforderungen verwendet werden.

Zu den anderen Migrationsoptionen, die Daten von einem lokalen SQL Server auf Azure NetApp Files verschieben, zählen:

- Trennen Sie die Daten- und Protokolldateien, kopieren Sie sie in den Azure Blob Storage und verbinden Sie sie anschließend über die URL mit SQL Server in der Azure VM. Dabei wird eine ANF-Dateifreigabe angehängt.
- Wenn Sie eine lokale Implementierung von Always-On-Verfügbarkeitsgruppen verwenden, verwenden Sie das ["Assistent Zum Hinzufügen Von Azure Replikaten"](#) Um ein Replikat in Azure zu erstellen und dann Failover auszuführen.
- Verwenden Sie SQL Server ["Transaktionsorientierte Replizierung"](#) Um die Azure SQL Server-Instanz als Abonnement zu konfigurieren, deaktivieren Sie die Replikation und weisen Sie Benutzer auf die Azure-Datenbankinstanz zu.
- Senden Sie die Festplatte mithilfe des Windows Import/Export-Dienstes.

Backup und Recovery

Backup und Recovery sind ein wichtiger Aspekt jeder SQL Server-Implementierung. Es ist zwingend erforderlich, dass das entsprechende Sicherheitsnetz in Verbindung mit Hochverfügbarkeitslösungen wie AOAG schnell von verschiedenen Datenversagen- und -Verlustszenarien wiederhergestellt wird. Zum Ausführen eines applikationskonsistenten Backups der Datenbanken können SQL Server Database Quiesce Tool, Azure Backup (Streaming) oder ein Backup-Tool eines Drittanbieters wie beispielsweise CommVault verwendet werden.

Mit der Azure NetApp Files Snapshot Technologie können Sie ganz einfach eine zeitpunktgenaue Kopie der Benutzerdatenbanken erstellen, ohne die Performance oder Netzwerkauslastung zu beeinträchtigen. Mit dieser Technologie können Sie außerdem eine Snapshot Kopie auf einem neuen Volume wiederherstellen oder das betroffene Volume schnell auf den Zustand zurücksetzen, in dem es sich zum Zeitpunkt der Erstellung der Snapshot Kopie mithilfe der Funktion zum Zurücksetzen des Volumes befand. Der Azure NetApp Files-Snapshot-Prozess ist sehr schnell und effizient, wodurch mehrere tägliche Backups möglich sind, im Gegensatz zum Streaming Backup des Azure-Backup. Da mehrere Snapshot Kopien an einem bestimmten Tag möglich sind, lassen sich die RPO- und RTO-Zeiten erheblich reduzieren. Um die Applikationskonsistenz der intakten Daten und vor dem Erstellen der Snapshot-Kopie ordnungsgemäß auf der Festplatte zu speichern, nutzen Sie das Quiesce-Tool für die SQL Server-Datenbank ("[SCSQLAPI-Tool](#)"; Für den Zugriff auf diesen Link sind NetApp SSO Login-Anmeldedaten erforderlich). Dieses Tool kann in PowerShell ausgeführt werden, das die SQL Server Datenbank enthält und wiederum die applikationskonsistente Storage Snapshot Kopie für Backups erstellen kann.

*Hinweise: *

- Das SCSQLAPI-Tool unterstützt nur die SQL Server 2016- und 2017-Versionen.
- Das SCSQLAPI-Tool funktioniert jeweils nur mit einer Datenbank.
- Isolieren Sie die Dateien von der jeweiligen Datenbank, indem Sie sie auf einem separaten Azure NetApp Files Volume ablegen.

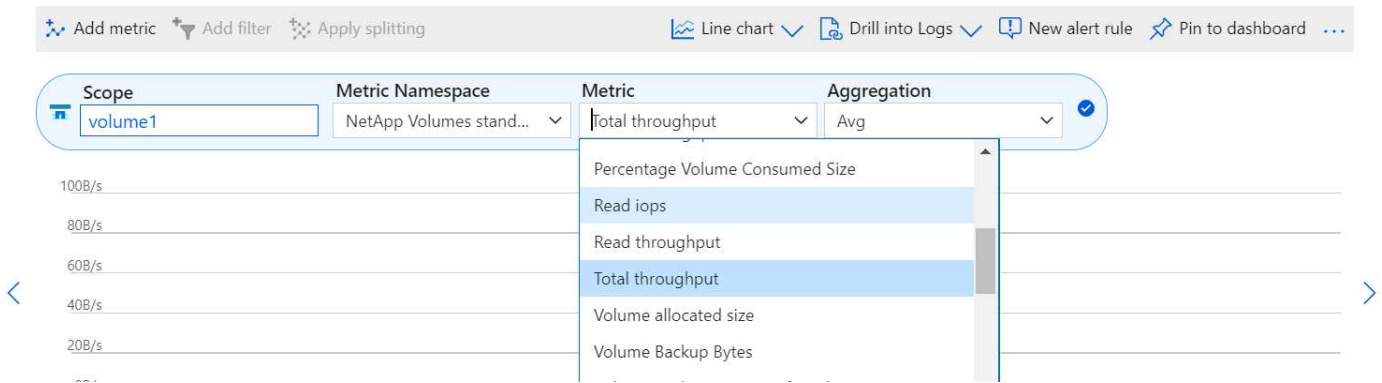
Wegen der großen Einschränkungen der SCSQL API, "[Azure Backup](#)" wurde für die Datensicherung zur Erfüllung der SLA-Anforderungen eingesetzt. Sie bietet ein Stream-basiertes Backup von SQL Server, das in Azure Virtual Machines und Azure NetApp Files ausgeführt wird. Azure Backup ermöglicht einen RPO von 15 Minuten mit häufigen Protokoll-Backups und zeitpunktgenauer Recovery von bis zu einer Sekunde.

Monitoring

Azure NetApp Files ist für die Zeitreihendaten in Azure Monitor integriert und bietet Metriken zu zugewiesenem Storage, tatsächlicher Storage-Auslastung, Volume-IOPS, Durchsatz, Lesebytes/s für Festplatten, Schreibbytes/s der Festplatte, Lesen/s der Festplatte und Schreiben/s der Festplatte sowie zugehörige Latenz. Diese Daten können zur Identifizierung von Engpässen mit Alarmfunktionen und zur Durchführung von Systemprüfungen eingesetzt werden, um zu überprüfen, ob Ihre SQL Server Implementierung in einer optimalen Konfiguration ausgeführt wird.

In dieser HLD wird ScienceLogic zur Überwachung von Azure NetApp Files verwendet, indem die Kennzahlen unter Verwendung des entsprechenden Service-Principal offengelegt werden. Das folgende Bild ist ein Beispiel für die Option Azure NetApp Files Metric.

Avg Total throughput for volume1



DevTest mit Thick Clones

Mit Azure NetApp Files können Sie sofortige Kopien von Datenbanken erstellen, um die Funktionalität zu testen, die mithilfe der aktuellen Datenbankstruktur und des Inhalts während der Applikationsentwicklungszyklen implementiert werden sollte. So können Sie beim Befüllen von Data Warehouses die Tools zur Datenextraktion und -Bearbeitung verwenden. Oder sogar um Daten wiederherzustellen, die versehentlich gelöscht oder geändert wurden. Bei diesem Prozess müssen Daten nicht aus Azure Blob Containern kopiert werden, was sie sehr effizient macht. Nach der Wiederherstellung des Volumes können Lese-/Schreibvorgänge genutzt werden, was die Validierung und die Produkteinführungszeit erheblich verkürzt. Dies muss in Verbindung mit SCSQLAPI verwendet werden, um die Anwendungskonsistenz zu gewährleisten. Dieser Ansatz stellt zusammen mit Azure NetApp Files eine weitere kontinuierliche Kostenoptimierung dar, die die Option „auf neues Volume wiederherstellen“ nutzt.

Hinweise:

- Das mit der Option Neues Volume wiederherstellen erstellte Volume nutzt Kapazität aus dem Kapazitäts-Pool.
- Die geklonten Volumes können über DIE REST- oder Azure CLI gelöscht werden, um zusätzliche Kosten zu vermeiden (falls der Kapazitäts-Pool erhöht werden muss).

Hybrid Storage-Optionen

Obwohl NetApp empfiehlt, in SQL Server Verfügbarkeitsgruppen denselben Storage für alle Nodes zu verwenden, gibt es Szenarien, in denen mehrere Storage-Optionen verwendet werden können. Das Szenario ist für Azure NetApp Files möglich, bei dem ein Node in AOAG mit einer Azure NetApp Files SMB-Dateifreigabe verbunden ist und der zweite Node mit einer Azure Premium-Festplatte verbunden wird. Vergewissern Sie sich in diesen Fällen, dass die Azure NetApp Files SMB-Freigabe die primäre Kopie der Benutzerdatenbanken enthält und die Premium-Festplatte als sekundäre Kopie verwendet wird.

Hinweise:

- In diesen Implementierungen zur Vermeidung von Failover-Problemen muss sichergestellt werden, dass die kontinuierliche Verfügbarkeit auf dem SMB Volume aktiviert ist. Ohne kontinuierlich verfügbares Attribut kann die Datenbank ausfallen, wenn Hintergrundwartung auf der Speicherebene durchgeführt wird.
- Bewahren Sie die primäre Kopie der Datenbank auf der Azure NetApp Files SMB-Dateifreigabe auf.

Business Continuity Remote replizieren

Disaster Recovery ist bei jeder Implementierung im Allgemeinen ein Nebensache. Disaster Recovery muss jedoch während der ersten Design- und Implementierungsphase berücksichtigt werden, um Auswirkungen auf

Ihr Geschäft zu vermeiden. Mit Azure NetApp Files kann die CRR-Funktion (Cross-Region Replication) verwendet werden, um die Volume-Daten auf Blockebene in die gepaarte Region zu replizieren, um unerwartete regionale Ausfälle zu bewältigen. Das CRR-fähige Ziel-Volumen kann für Lesevorgänge verwendet werden, was es zu einem idealen Kandidaten für Disaster-Recovery-Simulationen macht. Darüber hinaus kann das CRR-Ziel mit dem niedrigsten Service-Level (z. B. Standard) zugewiesen werden, um die Gesamtbetriebskosten zu senken. Im Falle eines Failover kann die Replizierung beschädigt werden, sodass das entsprechende Volumen Lese-/Schreibzugriff möglich ist. Durch dynamische Service Level-Funktionalität kann darüber hinaus der Service-Level des Volumens angepasst werden, was die Disaster Recovery-Kosten erheblich senkt. Dies ist eine weitere einzigartige Funktion von Azure NetApp Files mit Blockreplizierung in Azure.

Langfristiges Archiv der Snapshot-Kopien

Viele Unternehmen müssen ihre Snapshot-Daten langfristig aus Datenbankdateien aufbewahren, um Compliance-Anforderungen zu erfüllen. Obwohl dieser Prozess in dieser HLD nicht verwendet wird, kann er einfach mit einem einfachen Batch-Skript durchgeführt werden **"AzCopy"** Um das Snapshot-Verzeichnis in den Azure Blob-Container zu kopieren. Das Batch-Skript kann unter Verwendung geplanter Aufgaben nach einem bestimmten Zeitplan ausgelöst werden. Der Prozess ist unkompliziert und beinhaltet folgende Schritte:

1. Laden Sie die ausführbare Datei AzCopy V10 herunter. Es gibt nichts zu installieren, weil es eine `exe`-Datei ist:
2. Autorisieren Sie AzCopy, indem Sie ein SAS-Token auf der Containerebene mit den entsprechenden Berechtigungen verwenden.
3. Nach der Autorisierung von AzCopy beginnt die Datenübertragung.

Hinweise:

- Stellen Sie in Batch-Dateien sicher, dass die in SAS-Token angezeigten %-Zeichen nicht mehr verwendet werden. Dies kann durch Hinzufügen eines zusätzlichen %-Zeichens neben vorhandenen %-Zeichen in der SAS-Token-Zeichenfolge erreicht werden.
- Der **"Sichere Übertragung Erforderlich"** Die Einrichtung eines Speicherkontos bestimmt, ob die Verbindung zu einem Speicherkonto mit Transport Layer Security (TLS) gesichert ist. Diese Einstellung ist standardmäßig aktiviert. Das folgende Batch-Skript-Beispiel kopiert rekursiv Daten aus dem Verzeichnis der Snapshot-Kopie in einen festgelegten Blob-Container:

```
SET source="Z:\~snapshot"
echo %source%
SET
dest="https://testanfacct.blob.core.windows.net/azcoptst?sp=racwdl&st=2020-10-21T18:41:35Z&se=2021-10-22T18:41:00Z&sv=2019-12-12&sr=c&sig=ZxRUJwFlLXgHS8As7HzXJOaDXXVJ7PxxIX3ACpx56XY%%3D"
echo %dest%
```

Das folgende Beispiel `cmd` wird in PowerShell ausgeführt:

```
-recursive
```

```
INFO: Scanning...
INFO: Any empty folders will not be processed, because source and/or
destination doesn't have full folder support
Job b3731dd8-da61-9441-7281-17a4db09ce30 has started
Log file is located at: C:\Users\niyaz\.azcopy\b3731dd8-da61-9441-7281-
17a4db09ce30.log
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
INFO: azcopy.exe: A newer version 10.10.0 is available to download
0.0 %, 0 Done, 0 Failed, 2 Pending, 0 Skipped, 2 Total,
Job b3731dd8-da61-9441-7281-17a4db09ce30 summary
Elapsed Time (Minutes): 0.0333
Number of File Transfers: 2
Number of Folder Property Transfers: 0
Total Number of Transfers: 2
Number of Transfers Completed: 2
Number of Transfers Failed: 0
Number of Transfers Skipped: 0
TotalBytesTransferred: 5
Final Job Status: Completed
```

Hinweise:

- Eine ähnliche Backup-Funktion zur langfristigen Aufbewahrung wird in Kürze in Azure NetApp Files verfügbar sein.
- Das Batch-Skript kann in jedem Szenario verwendet werden, in dem Daten in den Blob-Container einer beliebigen Region kopiert werden müssen.

Kostenoptimierung

Mit Volume-Umgestaltung und der dynamischen Service Level-Änderung, die für die Datenbank vollständig transparent ist, ermöglicht Azure NetApp Files eine kontinuierliche Kostenoptimierung in Azure. Diese Funktion wird in dieser HLD umfassend eingesetzt, um eine Überprovisionierung von zusätzlichem Storage zu vermeiden, um Workload-Spitzen auszugleichen.

Die Größe des Volumes kann einfach angepasst werden, indem eine Azure Funktion in Verbindung mit den Azure Alarmprotokollen erstellt wird.

Schlussfolgerung

Ganz gleich, ob Sie mit Stretch-Datenbanken auf eine All-Cloud oder Hybrid Cloud setzen – Azure NetApp Files bietet Ihnen hervorragende Optionen für die Implementierung und das Management von Datenbank-Workloads und reduziert gleichzeitig die TCO, da die Datenanforderungen nahtlos auf die Applikationsebene reduziert werden.

Dieses Dokument behandelt Empfehlungen für die Planung, Entwicklung, Optimierung und Skalierung von Microsoft SQL Server Implementierungen mit Azure NetApp Files, die zwischen Implementierungen stark variieren können. Die richtige Lösung hängt sowohl von den technischen Details der Implementierung als auch von den geschäftlichen Anforderungen ab, die für das Projekt ausschlaggebend sind.

Erkenntnisse Aus

Zu den wichtigsten Punkten dieses Dokuments gehören:

- Sie können nun Azure NetApp Files verwenden, um die Datenbank und den Dateifreigabezeuge für das SQL Server Cluster zu hosten.
- Sie können die Reaktionszeiten von Applikationen verkürzen und eine Verfügbarkeit von 99.9999 % erzielen, um Zugriff auf SQL Server-Daten zu jeder Zeit und an jedem Ort zu ermöglichen.
- Sie können die Gesamtkomplexität der SQL Server-Bereitstellung und des fortlaufenden Managements, wie RAID-Striping, durch einfache und sofortige Anpassung vereinfachen.
- Mit intelligenten Funktionen lassen sich SQL Server Datenbanken in Minutenschnelle implementieren und Entwicklungszyklen verkürzen.
- Wenn Azure Cloud Ziel ist, ist Azure NetApp Files die richtige Storage-Lösung für eine optimierte Implementierung.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie unter den folgenden Links:

- Lösungsarchitekturen mit Azure NetApp Files nutzen
["https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-solution-architectures"](https://docs.microsoft.com/en-us/azure/azure-netapp-files/azure-netapp-files-solution-architectures)
- Vorteile der Nutzung von Azure NetApp Files für die SQL Server-Implementierung
["https://docs.microsoft.com/en-us/azure/azure-netapp-files/solutions-benefits-azure-netapp-files-sql-server"](https://docs.microsoft.com/en-us/azure/azure-netapp-files/solutions-benefits-azure-netapp-files-sql-server)
- SQL Server auf Azure Deployment Guide Using Azure NetApp Files
<https://www.netapp.com/pdf.html?item=/media/27154-tr-4888.pdf>
- Fehlertoleranz, Hochverfügbarkeit und Ausfallsicherheit mit Azure NetApp Files
["https://cloud.netapp.com/blog/azure-anf-blg-fault-tolerance-high-availability-and-resilience-with-azure-netapp-files"](https://cloud.netapp.com/blog/azure-anf-blg-fault-tolerance-high-availability-and-resilience-with-azure-netapp-files)

TR-4467: SAP with Microsoft SQL Server on Windows – Best Practices Using NetApp Clustered Data ONTAP and SnapCenter

Marco Schoen, NetApp

TR-4467 bietet Kunden und Partnern Best Practices für die Implementierung von Clustered NetApp Data ONTAP zur Unterstützung von SAP Business Suite Lösungen, die in einem Microsoft SQL Server auf Windows-Umgebungen ausgeführt werden.

["TR-4467: SAP with Microsoft SQL Server on Windows – Best Practices Using NetApp Clustered Data ONTAP and SnapCenter"](#)

Modernisieren Ihrer Microsoft SQL Server Umgebung

Optimierter Betrieb und optimale Nutzung der Daten – vor Ort und in der Cloud

["Modernisieren Ihrer Microsoft SQL Server Umgebung"](#)

TR-4590: Best Practice Guide für Microsoft SQL Server mit ONTAP

Manohar Kulkarni und Pat Sinthusan, NetApp

Dieses Dokument beschreibt Best Practices und bietet Einblicke in Designüberlegungen für die Bereitstellung von SQL Server auf NetApp-Speichersystemen mit NetApp ONTAP®-Software mit dem Ziel, eine effektive und effiziente Speicherbereitstellung sowie eine lückenlose Planung der Datensicherheit und -Aufbewahrung zu erreichen.

["TR-4590: Best Practices Guide für Microsoft SQL Server mit ONTAP"](#)

TR-4764: Best Practices for Microsoft SQL Server with NetApp EF-Series

Mitch Blackburn, Pat Sinthusan, NetApp

Dieser Best Practices-Leitfaden soll Storage-Administratoren und Datenbankadministratoren bei der erfolgreichen Implementierung von Microsoft SQL Server auf NetApp EF-Series Storage unterstützen.

["TR-4764: Best Practices for Microsoft SQL Server with NetApp EF-Series"](#)

Open Source-Datenbanken

TR-4956: Automatisierte PostgreSQL High Availability Implementierung und Disaster Recovery in AWS FSX/EC2

Allen Cao, Niyaz Mohamed, NetApp

Zweck

PostgreSQL ist eine häufig verwendete Open-Source-Datenbank, die auf Platz vier unter den zehn beliebtesten Datenbank-Engines von rangiert ["DB-Engines"](#). Auf der einen Seite, PostgreSQL leitet seine Popularität aus seinem lizenzfreien, Open-Source-Modell, während noch mit ausgereiften Features. Da es sich um Open-Source-Lösungen handelt, fehlen insbesondere in der Public Cloud detaillierte Leitfäden zur Implementierung produktionsfertiger Datenbanken. Dies gilt für Hochverfügbarkeit und Disaster Recovery (HA/DR). Im Allgemeinen kann es schwierig sein, ein typisches PostgreSQL HA/DR-System mit warmem Standby, Streaming-Replizierung usw. einzurichten. Das Testen der HA/DR-Umgebung durch Beförderung des Standby-Standorts und dann das Zurückschalten zum primären Standort kann mit der Produktion zu Störungen führen. Es gibt auf dem primären Volume gut dokumentierte Performance-Probleme, wenn Lese-Workloads auf dem Streaming des Hot-Standby-Modus ausgeführt werden.

In dieser Dokumentation zeigen wir, wie Sie eine PostgreSQL Streaming HA/DR-Lösung auf Applikationsebene hinter sich lassen und eine PostgreSQL HA/DR-Lösung auf Basis von AWS FSX ONTAP Storage und EC2 Computing-Instanzen mittels Storage-Level-Replizierung aufbauen können. Die Lösung erstellt ein einfacheres, vergleichbares System und liefert ähnliche Ergebnisse im Vergleich zur herkömmlichen Streaming-Replizierung auf PostgreSQL-Applikationsebene für HA/DR.

Diese Lösung basiert auf der bewährten und ausgereiften NetApp SnapMirror Replizierungstechnologie auf Storage-Ebene, die auch in FSX ONTAP Cloud-Storage für PostgreSQL HA/DR in AWS verfügbar ist. Die Implementierung ist mit einem vom NetApp Solutions Team bereitgestellten Automatisierungs-Toolkit einfach. Es bietet ähnliche Funktionen und beseitigt gleichzeitig die Komplexität- und Performance-Einbußen am primären Standort mit der auf Applikationsebene basierenden Streaming-basierten HA/DR-Lösung auf Applikationsebene. Die Lösung kann einfach implementiert und getestet werden, ohne dass der aktive primäre Standort davon betroffen ist.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- HA/DR-Implementierung auf Produktionsniveau für PostgreSQL in der Public AWS Cloud
- Testen und Validieren eines PostgreSQL-Workloads in der Public AWS Cloud
- Testen und Validieren einer PostgreSQL HA/DR-Strategie auf der Basis der NetApp SnapMirror Replizierungstechnologie

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Der DBA, der an der Implementierung von PostgreSQL mit HA/DR in der Public AWS Cloud interessiert ist.
- Der Datenbanklösungsarchitekt, der PostgreSQL-Workloads in der Public AWS Cloud testen möchte.
- Storage-Administrator, der an der Implementierung und dem Management von PostgreSQL-Instanzen interessiert ist, die auf AWS FSX Storage bereitgestellt werden.
- Der Applikationseigentümer, der an der Einrichtung einer PostgreSQL-Umgebung in AWS FSX/EC2 interessiert ist.

Test- und Validierungsumgebung der Lösung

Tests und Validierungen dieser Lösung wurden in einer AWS FSX- und EC2-Umgebung durchgeführt, die möglicherweise nicht mit der endgültigen Implementierungsumgebung übereinstimmt. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind

Hardware- und Softwarekomponenten

Hardware		
FSX ONTAP-Storage	Aktuelle Version	Zwei FSX HA-Paare in derselben VPC und Verfügbarkeitszone wie primäre und Standby HA-Cluster
EC2 Instanz für Computing	t2.xlarge/4vCPU/16G	Zwei EC2 T2 xlarge als primäre und Standby-Computing-Instanzen
Ansible-Controller	CentOS VM On-Prem./4vCPU/8 G	VM zum Hosten des Ansible-Automatisierungs-Controllers entweder vor Ort oder in der Cloud
Software		
Redhat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Bereitstellung der RedHat Subscription für Tests
Centos Linux	CentOS Linux Version 8.2.2004 (Core)	Hosting des Ansible-Controllers im On-Premises-Lab
PostgreSQL	Version 14.5	Automation zieht die neueste verfügbare Version von PostgreSQL aus der postgresql.org yum repo

Ansible	Version 2.10.3	Voraussetzungen für erforderliche Sammlungen und Bibliotheken, die mit dem Requirements Playbook installiert sind
---------	----------------	---

Wichtige Faktoren für die Implementierung

- **Sicherung, Wiederherstellung und Wiederherstellung von PostgreSQL-Datenbanken.** Eine PostgreSQL-Datenbank unterstützt eine Reihe von Backup-Methoden wie ein logisches Backup mit `pg_dump`, ein physisches Online-Backup mit `pg_basebackup` oder einen niedrigeren Level-Befehl zum Sichern von Betriebssystemen sowie konsistente Snapshots auf Storage-Ebene. Diese Lösung verwendet NetApp Consistency-Group Snapshots für PostgreSQL-Datenbankdaten und WAL Volumes für Backup, Restore und Recovery am Standby-Standort. Die NetApp Consistency Group Volume Snapshots sequenzieren die I/O-Vorgänge, während sie in den Storage geschrieben werden, und schützen die Integrität von Datenbankdatendateien.
- **EC2 Compute-Instanzen.** bei diesen Tests und Validierungen haben wir den AWS EC2 Instanztyp für die PostgreSQL-Datenbank-Computing-Instanz verwendet. NetApp empfiehlt die Verwendung einer M5-Typ-EC2-Instanz als Computing-Instanz für PostgreSQL bei der Implementierung, da sie für Datenbank-Workloads optimiert ist. Die Standby-Computing-Instanz sollte immer in derselben Zone wie das passive (Standby) Filesystem, das für das FSX HA-Cluster bereitgestellt wird, bereitgestellt werden.
- **FSX Storage HA Cluster Single- oder Multi-Zone-Implementierung.** bei diesen Tests und Validierungen haben wir einen FSX HA-Cluster in einer einzelnen AWS Verfügbarkeitszone implementiert. Für die Implementierung in der Produktion empfiehlt NetApp die Implementierung eines FSX HA-Paars in zwei verschiedenen Verfügbarkeitszonen. Ein Disaster Recovery-Standby-HA-Paar für Business Continuity kann in einer anderen Region eingerichtet werden, wenn zwischen dem primären und dem Standby eine bestimmte Entfernung erforderlich ist. Ein FSX HA-Cluster wird in einem HA-Paar bereitgestellt, das in einem Paar aktiv/Passiv-Filesysteme gespiegelt wird, um Redundanz auf Storage-Ebene bereitzustellen.
- **PostgreSQL Daten- und Log-Platzierung.** Typische PostgreSQL-Bereitstellungen teilen sich das gleiche Stammverzeichnis oder dieselben Volumes für Daten- und Log-Dateien. Bei unseren Tests und Validierungen haben wir PostgreSQL Daten und Logs zu zwei separaten Volumes für die Leistung getrennt. Ein Soft-Link wird im Datenverzeichnis verwendet, um auf das Logverzeichnis oder Volume zu verweisen, das PostgreSQL WAL-Logs und archivierte WAL-Logs hostet.
- **PostgreSQL Service Startup Delay Timer.** Diese Lösung verwendet NFS gemountete Volumes, um die PostgreSQL Datenbank-Datei und WAL Log-Dateien zu speichern. Während eines Neustart eines Datenbank-Hosts versucht der PostgreSQL-Dienst möglicherweise, zu starten, während das Volume nicht angehängt ist. Dies führt zu einem Fehler beim Starten des Datenbankdienstes. Für den korrekten Start der PostgreSQL-Datenbank ist eine Zeitverzögerung von 10 bis 15 Sekunden erforderlich.
- **RPO/RTO für Business Continuity.** FSX Datenreplikation vom primären zum Standby für DR basiert auf ASYNC, das bedeutet, dass der RPO von der Häufigkeit von Snapshot Backups und SnapMirror Replikation abhängt. Je häufiger Snapshot Kopien und SnapMirror Replizierung erstellt werden, desto geringer die RPO. Daher gibt es ein Gleichgewicht zwischen potentiell Datenverlust im Falle eines Notfalls und inkrementellen Storage-Kosten. Wir haben festgestellt, dass Snapshot Kopie und SnapMirror Replizierung in nur 5-Minuten-Intervallen für RPO implementiert werden können und dass PostgreSQL in der Regel innerhalb einer Minute am DR-Standby-Standort wiederhergestellt werden kann.
- **Datenbank-Backup.** Nachdem eine PostgreSQL-Datenbank von einem On-premises Data Center aus implementiert oder in den AWS FSX-Speicher migriert wurde, werden die Daten zur Absicherung im FSX HA-Paar automatisch gespiegelt. Daten werden im Notfall über einen replizierten Standby-Standort weiter gesichert. Für eine längerfristige Backup-Aufbewahrung oder Datensicherung empfiehlt NetApp die Nutzung des integrierten PostgreSQL `pg_baseBackup` Utility, um ein vollständiges Datenbank-Backup auszuführen, das auf S3 Blob-Storage portiert werden kann.

Lösungsimplementierung

Die Implementierung dieser Lösung kann mit dem auf NetApp Ansible basierenden Automatisierungs-Toolkit automatisch abgeschlossen werden. Befolgen Sie die detaillierten Anweisungen unten.

1. Lesen Sie die Anweisungen im Automations-Toolkit Readme.md "["na_postgresql_aws_Deploy_hadr"](#)".
2. Sehen Sie sich das folgende Video an.

Automatisierte PostgreSQL-Implementierung und -Sicherung

1. Konfigurieren Sie die erforderlichen Parameterdateien (`hosts`, `host_vars/host_name.yml`, `fsx_vars.yml`) Durch Eingabe benutzerspezifischer Parameter in die Vorlage in den entsprechenden Abschnitten. Dann kopieren Sie mit der Schaltfläche Kopieren Dateien auf den Ansible-Controller-Host.

Voraussetzungen für die automatisierte Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Es wurde ein AWS Konto eingerichtet, und die erforderlichen VPC und Netzwerksegmente wurden in Ihrem AWS Konto erstellt.
2. Über die AWS EC2-Konsole müssen Sie zwei EC2 Linux-Instanzen bereitstellen, eine als primärer PostgreSQL DB-Server auf dem primären und eine am Standby-DR-Standort. Um Rechenredundanz auf dem primären und Standby-DR-Standort zu erreichen, sollten zwei zusätzliche EC2 Linux Instanzen als Standby PostgreSQL DB Server implementiert werden. Im Architekturdiagramm im vorherigen Abschnitt finden Sie weitere Details zum Umgebungs-Setup. Sehen Sie sich auch die an "[Benutzerhandbuch für Linux-Instanzen](#)" Finden Sie weitere Informationen.
3. Implementieren Sie über die AWS EC2 Konsole zwei FSX ONTAP Storage HA-Cluster, um die PostgreSQL Datenbank-Volumes zu hosten. Wenn Sie mit der Bereitstellung von FSX-Speicher nicht vertraut sind, lesen Sie die Dokumentation "[Erstellen von FSX für ONTAP-Dateisysteme](#)" Schritt-für-Schritt-Anleitungen.
4. Eine CentOS Linux VM aufbauen, um den Ansible-Controller zu hosten. Der Ansible-Controller kann sich entweder vor Ort oder in der AWS Cloud befinden. Falls die Daten lokal gespeichert sind, müssen SSH-Konnektivität mit der VPC, EC2 Linux Instanzen und FSX Storage-Cluster vorhanden sein.
5. Richten Sie den Ansible-Controller wie in dem Abschnitt „Ansible-Steuerungsknoten für CLI-Bereitstellungen auf RHEL/CentOS einrichten“ von der Ressource aus ein "[Erste Schritte mit der Automatisierung von NetApp Lösungen](#)".
6. Klonen einer Kopie des Automatisierungs-Toolkit auf der öffentlichen NetApp GitHub Website.

```
git clone https://github.com/NetApp-  
Automation/na_postgresql_aws_deploy_hadr.git
```

1. Führen Sie im Root-Verzeichnis des Toolkit die erforderlichen Playbooks aus, um die für den Ansible Controller erforderlichen Sammlungen und Bibliotheken zu installieren.

```
ansible-playbook -i hosts requirements.yml
```



```
ansible-galaxy collection install -r collections/requirements.yml --force
--force-with-deps
```

1. Rufen Sie die erforderlichen EC2 FSX-Instanzparameter für die DB-Hostvariablen-Datei ab `host_vars/*` Und die globale Variablendatei `fsx_vars.yml` Konfiguration.

Konfigurieren Sie die Host-Datei

Geben Sie die primäre FSX ONTAP-Cluster-Management-IP und EC2-Instanzen Hostnamen in die Hosts-Datei ein.

```
# Primary FSx cluster management IP address
[fsx_ontap]
172.30.15.33
```

```
# Primary PostgreSQL DB server at primary site where database is
initialized at deployment time
[postgresql]
psql_01p ansible_ssh_private_key_file=psql_01p.pem
```

```
# Primary PostgreSQL DB server at standby site where postgresql service is
installed but disabled at deployment
# Standby DB server at primary site, to setup this server comment out
other servers in [dr_postgresql]
# Standby DB server at standby site, to setup this server comment out
other servers in [dr_postgresql]
[dr_postgresql] --
psql_01s ansible_ssh_private_key_file=psql_01s.pem
#psql_01ps ansible_ssh_private_key_file=psql_01ps.pem
#psql_01ss ansible_ssh_private_key_file=psql_01ss.pem
```

Konfigurieren Sie die Datei `Host_Name.yml` im Ordner `Host_vars`

```

# Add your AWS EC2 instance IP address for the respective PostgreSQL
server host
ansible_host: "10.61.180.15"

# "{{groups.postgresql[0]}}" represents first PostgreSQL DB server as
defined in PostgreSQL hosts group [postgresql]. For concurrent multiple
PostgreSQL DB servers deployment, [0] will be incremented for each
additional DB server. For example, "{{groups.postgresql[1]}}" represents
DB server 2, "{{groups.postgresql[2]}}" represents DB server 3 ... As a
good practice and the default, two volumes are allocated to a PostgreSQL
DB server with corresponding /pgdata, /pglogs mount points, which store
PostgreSQL data, and PostgreSQL log files respectively. The number and
naming of DB volumes allocated to a DB server must match with what is
defined in global fsx_vars.yml file by src_db_vols, src_archivelog_vols
parameters, which dictates how many volumes are to be created for each DB
server. aggr_name is aggr1 by default. Do not change. lif address is the
NFS IP address for the SVM where PostgreSQL server is expected to mount
its database volumes. Primary site servers from primary SVM and standby
servers from standby SVM.
host_datastores_nfs:
  - {vol_name: "{{groups.postgresql[0]}}_pgdata", aggr_name: "aggr1", lif:
"172.21.94.200", size: "100"}
  - {vol_name: "{{groups.postgresql[0]}}_pglogs", aggr_name: "aggr1", lif:
"172.21.94.200", size: "100"}

# Add swap space to EC2 instance, that is equal to size of RAM up to 16G
max. Determine the number of blocks by dividing swap size in MB by 128.
swap_blocks: "128"

# Postgresql user configurable parameters
psql_port: "5432"
buffer_cache: "8192MB"
archive_mode: "on"
max_wal_size: "5GB"
client_address: "172.30.15.0/24"

```

Konfigurieren Sie die globale fsx_Vars.yml-Datei im Ordner Vars

```

#####
##### PostgreSQL HADR global user configuration variables #####
##### Consolidate all variables from FSx, Linux, and postgresql #####
#####

#####
### Ontap env specific config variables ###

```

```
#####  
  
#####  
#####  
# Variables for SnapMirror Peering  
#####  
#####  
  
#Passphrase for cluster peering authentication  
passphrase: "xxxxxxx"  
  
#Please enter destination or standby FSx cluster name  
dst_cluster_name: "FsxId0cf8e0bccb14805e8"  
  
#Please enter destination or standby FSx cluster management IP  
dst_cluster_ip: "172.30.15.90"  
  
#Please enter destination or standby FSx cluster inter-cluster IP  
dst_inter_ip: "172.30.15.13"  
  
#Please enter destination or standby SVM name to create mirror  
relationship  
dst_vserver: "dr"  
  
#Please enter destination or standby SVM management IP  
dst_vserver_mgmt_lif: "172.30.15.88"  
  
#Please enter destination or standby SVM NFS lif  
dst_nfs_lif: "172.30.15.88"  
  
#Please enter source or primary FSx cluster name  
src_cluster_name: "FsxId0cf8e0bccb14805e8"  
  
#Please enter source or primary FSx cluster management IP  
src_cluster_ip: "172.30.15.20"  
  
#Please enter source or primary FSx cluster inter-cluster IP  
src_inter_ip: "172.30.15.5"  
  
#Please enter source or primary SVM name to create mirror relationship  
src_vserver: "prod"  
  
#Please enter source or primary SVM management IP  
src_vserver_mgmt_lif: "172.30.15.115"  
  
#####  
#####
```

```

# Variable for PostgreSQL Volumes, lif - source or primary FSx NFS lif
address
#####
#####

src_db_vols:
  - {vol_name: "{{groups.postgresql[0]}}_pgdata", aggr_name: "aggr1", lif:
"172.21.94.200", size: "100"}

src_archivelog_vols:
  - {vol_name: "{{groups.postgresql[0]}}_pglogs", aggr_name: "aggr1", lif:
"172.21.94.200", size: "100"}

#Names of the Nodes in the ONTAP Cluster
nfs_export_policy: "default"

#####
#####
### Linux env specific config variables ###
#####
#####

#NFS Mount points for PostgreSQL DB volumes
mount_points:
  - "/pgdata"
  - "/pglogs"

#RedHat subscription username and password
redhat_sub_username: "xxxxx"
redhat_sub_password: "xxxxx"

#####
### DB env specific install and config variables ###
#####
#The latest version of PostgreSQL RPM is pulled/installed and config file
is deployed from a preconfigured template
#Recovery type and point: default as all logs and promote and leave all
PITR parameters blank

```

PostgreSQL Implementierung und HA/DR-Einrichtung

Die folgenden Aufgaben implementieren den PostgreSQL DB Serverdienst und initialisieren die Datenbank am primären Standort auf dem primären EC2 DB-Serverhost. Ein Standby-primären EC2 DB-Server-Host wird dann am Standby-Standort eingerichtet. Schließlich wird die DB-Volume-Replizierung aus dem FSX-Cluster des primären Standorts auf dem FSX-Cluster des Standby-Standorts eingerichtet, um Disaster Recovery zu ermöglichen.

1. Erstellen Sie DB-Volumes auf dem primären FSX-Cluster und richten sie postgresql auf dem primären EC2-Instance-Host ein.

```
ansible-playbook -i hosts postgresql_deploy.yml -u ec2-user --private-key psql_01p.pem -e @vars/fsx_vars.yml
```

2. Richten Sie den Standby-DR EC2-Instance-Host ein.

```
ansible-playbook -i hosts postgresql_standby_setup.yml -u ec2-user --private-key psql_01s.pem -e @vars/fsx_vars.yml
```

3. FSX ONTAP-Cluster-Peering und Datenbank-Volume-Replizierung einrichten

```
ansible-playbook -i hosts fsx_replication_setup.yml -e @vars/fsx_vars.yml
```

4. Konsolidieren Sie die vorherigen Schritte in einer PostgreSQL Implementierung mit einem Schritt und HA/DR-Einrichtung.

```
ansible-playbook -i hosts postgresql_hadr_setup.yml -u ec2-user -e @vars/fsx_vars.yml
```

5. Um einen Standby PostgreSQL DB-Host entweder auf dem primären oder Standby-Standort einzurichten, kommentieren Sie alle anderen Server im Abschnitt Hosts-Datei [dr_postgresql] und führen Sie dann das Playbook postgresql_Standby_Setup.yml mit dem jeweiligen Zielhost aus (z. B. psql_01ps oder Standby EC2 Compute-Instanz am primären Standort). Stellen Sie sicher, dass eine Host-Parameterdatei wie z. B. psql_01ps.yml Wird unter konfiguriert host_vars Verzeichnis.

```
[dr_postgresql] --  
#psql_01s ansible_ssh_private_key_file=psql_01s.pem  
psql_01ps ansible_ssh_private_key_file=psql_01ps.pem  
#psql_01ss ansible_ssh_private_key_file=psql_01ss.pem
```

```
ansible-playbook -i hosts postgresql_standby_setup.yml -u ec2-user --private-key psql_01ps.pem -e @vars/fsx_vars.yml
```

Snapshot-Backup und Replikation der PostgreSQL-Datenbank auf Standby-Standort

Die Sicherung und Replikation von PostgreSQL-Datenbank-Snapshots auf den Standby-Standort können auf dem Ansible-Controller mit einem benutzerdefinierten Intervall gesteuert und ausgeführt werden. Wir haben validiert, dass das Intervall nur 5 Minuten betragen kann. Daher kann bei einem Ausfall am primären Standort direkt vor dem nächsten geplanten Snapshot Backup ein Datenverlust von 5 Minuten auftreten.

```
*/15 * * * * /home/admin/na_postgresql_aws_deploy_hadr/data_log_snap.sh
```

Failover zum Standby-Standort für DR

Führen Sie zum Testen des PostgreSQL HA/DR-Systems als DR-Übung Failover und Wiederherstellung der PostgreSQL Datenbank auf der primären Standby EC2 DB Instanz am Standby-Standort durch, indem Sie das folgende Playbook ausführen. Führen Sie in einem DR-Szenario die gleiche Ausführung für ein tatsächlicher Failover zum DR-Standort aus.

```
ansible-playbook -i hosts postgresql_failover.yml -u ec2-user --private-key psql_01s.pem -e @vars/fsx_vars.yml
```

Synchronisieren Sie replizierte DB-Volumes nach Failover-Test

Führen Sie die Resynchronisierung nach dem Failover-Test durch, um die SnapMirror Replikation des Datenbankvolumens wiederherzustellen.

```
ansible-playbook -i hosts postgresql_standby_resync.yml -u ec2-user --private-key psql_01s.pem -e @vars/fsx_vars.yml
```

Failover vom primären EC2 DB-Server zum Standby-EC2-DB-Server aufgrund des Ausfalls der EC2-Computing-Instanz

NetApp empfiehlt, manuelle Failover-Vorgänge auszuführen oder bewährte Betriebssystem-Cluster-Software zu verwenden, die möglicherweise eine Lizenz erfordern.

Wo Sie weitere Informationen finden

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- Amazon FSX für NetApp ONTAP

["https://aws.amazon.com/fsx/netapp-ontap/"](https://aws.amazon.com/fsx/netapp-ontap/)

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bcd9843&sc_channel=ps&s_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2

- Automatisierung der NetApp Lösung

["Einführung"](#)

TR-4722: Best Practices für MySQL Datenbanken auf NetApp ONTAP

Anup Bharti, Manohar Kulkarni, Jeffrey Steiner NetApp

MySQL und seine Varianten, darunter MariaDB und Percona, sind weit verbreitet für viele Unternehmensanwendungen. Diese Anwendungen reichen von globalen Websites sozialer Netzwerke und massiven E-Commerce-Systemen bis hin zu SMB-Hosting-Systemen mit Tausenden von Datenbankinstanzen. Dieses Dokument beschreibt die Konfigurationsanforderungen und bietet Anleitung zum Tuning und zur Speicherkonfiguration für die Bereitstellung von MySQL auf NetApp® ONTAP® Datenmanagement-Software. Um zu ermitteln, ob die in diesem Bericht angegebene Umgebung, die Konfigurationen und Versionen Ihre Umgebung unterstützen, finden Sie im Interoperabilitäts-Matrix-Tool (IMT).

["TR-4722: Best Practices für MySQL Datenbanken auf NetApp ONTAP"](#)

SnapCenter für Datenbanken

SnapCenter Lifecycle Automation für Oracle-Klone

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Kunden sind begeistert von der FlexClone Funktion von NetApp ONTAP Storage für Datenbanken, mit deutlichen Einsparungen bei den Storage-Kosten. Dieses Ansible-basierte Toolkit automatisiert die Einrichtung, das Klonen und die Aktualisierung von geklonten Oracle Datenbanken anhand der NetApp SnapCenter Befehlszeilen-Dienstprogramme für ein optimiertes Lifecycle Management. Das Toolkit ist auf Oracle-Datenbanken anwendbar, die auf ONTAP Storage entweder bei Vorliegen oder in der Public Cloud bereitgestellt und über das UI Tool NetApp SnapCenter gemanagt werden.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Richten Sie die Konfigurationsdatei für die Klonspezifikation der Oracle-Datenbank ein.
- Erstellen und aktualisieren Sie die Oracle-Datenbank nach benutzerdefiniertem Zeitplan.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle Datenbanken mit SnapCenter managt.
- Ein Storage-Administrator, der ONTAP Storage mit SnapCenter managt
- Ein Anwendungseigentümer, der Zugriff auf die SnapCenter-Benutzeroberfläche hat.

Lizenz

Durch den Zugriff auf, das Herunterladen, die Installation oder die Verwendung der Inhalte in diesem GitHub-Repository stimmen Sie den Bedingungen der in dargelegten Lizenz zu ["Lizenzdatei"](#).



Es gibt bestimmte Beschränkungen bezüglich der Erstellung und/oder Freigabe von abgeleiteten Arbeiten mit dem Inhalt in diesem GitHub-Repository. Bitte lesen Sie die Lizenzbedingungen, bevor Sie den Inhalt verwenden. Wenn Sie nicht allen Bedingungen zustimmen, dürfen Sie nicht auf den Inhalt dieses Repositories zugreifen, ihn herunterladen oder verwenden.

Lösungsimplementierung

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

```
Ansible controller:  
  Ansible v.2.10 and higher  
  ONTAP collection 21.19.1  
  Python 3  
  Python libraries:  
    netapp-lib  
    xmltodict  
    jmespath
```

```
SnapCenter server:  
  version 5.0  
  backup policy configured  
  Source database protected with a backup policy
```

```
Oracle servers:  
  Source server managed by SnapCenter  
  Target server managed by SnapCenter  
  Target server with identical Oracle software stack as source server  
  installed and configured
```

Toolkit herunterladen

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-  
bb/na_oracle_clone_lifecycle.git
```

Dateikonfiguration der Ansible Ziel-Hosts

Das Toolkit enthält eine Host-Datei, die die Ziele definiert, für die ein Ansible-Playbook ausgeführt wird. In der Regel sind dies die Ziel-Clones-Hosts von Oracle. Im Folgenden finden Sie eine Beispieldatei. Ein Hosteintrag enthält die IP-Adresse des Zielhosts sowie den SSH-Schlüssel für den Zugriff eines Admin-Benutzers auf den Host, um den Klon- oder Aktualisierungsbefehl auszuführen.

#Oracle-Clone-Hosts

```
[clone_1]
ora_04.cie.netapp.com ansible_host=10.61.180.29
ansible_ssh_private_key_file=ora_04.pem
```

```
[clone_2]
[clone_3]
```

Konfiguration globaler Variablen

Die Ansible-Playbooks verwenden variable Eingaben aus mehreren variablen Dateien. Unten finden Sie ein Beispiel für die globale Variablendatei VARs.yml.

```
# ONTAP specific config variables
# SnapCtr specific config variables
```

```
snapctr_usr: xxxxxxxx
snapctr_pwd: 'xxxxxxxx'
```

```
backup_policy: 'Oracle Full offline Backup'
# Linux specific config variables
# Oracle specific config variables
```

Konfiguration der Host-Variablen

Hostvariablen werden im Verzeichnis Host_VARS mit dem Namen {{ Host_Name }}.yml definiert. Unten ist ein Beispiel für die Oracle-Zieldatei ora_04.cie.netapp.com.yml, die eine typische Konfiguration zeigt.

```
# User configurable Oracle clone db host specific parameters
```

```
# Source database to clone from
source_db_sid: NTAP1
source_db_host: ora_03.cie.netapp.com
```

```
# Clone database
clone_db_sid: NTAP1DEV
```

```
snapctr_obj_id: '{{ source_db_host }}\{{ source_db_sid }}'
```

Zusätzliche Clone-Ziel-Oracle-Serverkonfiguration

Der Oracle-Zielserver für Clones sollte denselben Oracle-Softwarestack aufweisen wie der Oracle-Quellserver, der installiert und gepatcht ist. Oracle-Benutzer .bash_profile hat ORACLE_BASE in Höhe von USD und ORACLE_HOME in Höhe von USD konfiguriert. Außerdem sollte die Variable „ORACLE_HOME“ mit der Oracle-Quellservereinstellung übereinstimmen. Hier ein Beispiel.

```
# .bash_profile
```

```
# Get the aliases and functions
if [ -f ~/.bashrc ]; then
    . ~/.bashrc
fi
```

```
# User specific environment and startup programs
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/NTAP1
```

Ausführung des Playbook

Es gibt insgesamt drei Playbooks zur Ausführung des Lebenszyklus von Oracle Datenbankklonen mit SnapCenter CLI-Dienstprogrammen.

1. Einmalige Installation von Ansible-Controller-Voraussetzungen

```
ansible-playbook -i hosts ansible_requirements.yml
```

2. Spezifikationsdatei für Clone einrichten – nur einmalig.

```
ansible-playbook -i hosts clone_1_setup.yml -u admin -e  
@vars/vars.yml
```

3. Erstellen und aktualisieren Sie die Klondatenbank regelmäßig von crontab mit einem Shell-Skript, um ein Aktualisierungs-Playbook aufzurufen.

```
0 */4 * * * /home/admin/na_oracle_clone_lifecycle/clone_1_refresh.sh
```

Erstellen Sie für eine zusätzliche Clone-Datenbank separate Clones_n_Setup.yml und Clone_n_refresh.yml sowie Clone_n_refresh.sh. Konfigurieren Sie die Ansible-Zielhosts und die Datei hostname.yml im Verzeichnis Host_vars entsprechend.

Wo Sie weitere Informationen finden

Weitere Informationen zur Automatisierung von NetApp Lösungen finden Sie auf der folgenden Website ["Automatisierung der NetApp Lösung"](#)

TR-4988: Backup, Recovery und Klonen von Oracle Datenbanken auf ANF mit SnapCenter

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Die NetApp SnapCenter Software ist eine unkomplizierte Enterprise-Plattform, die die Koordination und das Management der Datensicherung für alle Applikationen, Datenbanken und Filesysteme sicher gestaltet. Die Software vereinfacht das Backup-, Wiederherstellungs- und Klon-Lifecycle-Management, indem sie diese Aufgaben an die Anwendungseigentümer überträgt, ohne darauf zu verzichten, Aktivitäten auf den Speichersystemen zu überwachen und zu regulieren. Storage-basiertes Datenmanagement steigert die Performance und Verfügbarkeit sowie verkürzt Test- und Entwicklungszeiten.

Im technischen Bericht TR-4987 ["Vereinfachte, automatisierte Oracle-Implementierung auf Azure NetApp Files mit NFS"](#), Wir demonstrieren die automatisierte Oracle-Implementierung auf Azure NetApp Files (ANF) in der Azure-Cloud. In dieser Dokumentation stellen wir die Sicherung und das Management von Oracle-Datenbanken auf ANF in der Azure-Cloud mit einem sehr benutzerfreundlichen SnapCenter-UI-Tool vor.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Backup und Recovery von Oracle Database auf ANF in der Azure Cloud mit SnapCenter implementiert.
- Managen Sie Datenbank-Snapshots und Klonkopien, um die Applikationsentwicklung zu beschleunigen und das Management des Daten-Lebenszyklus zu optimieren.

Zielgruppe

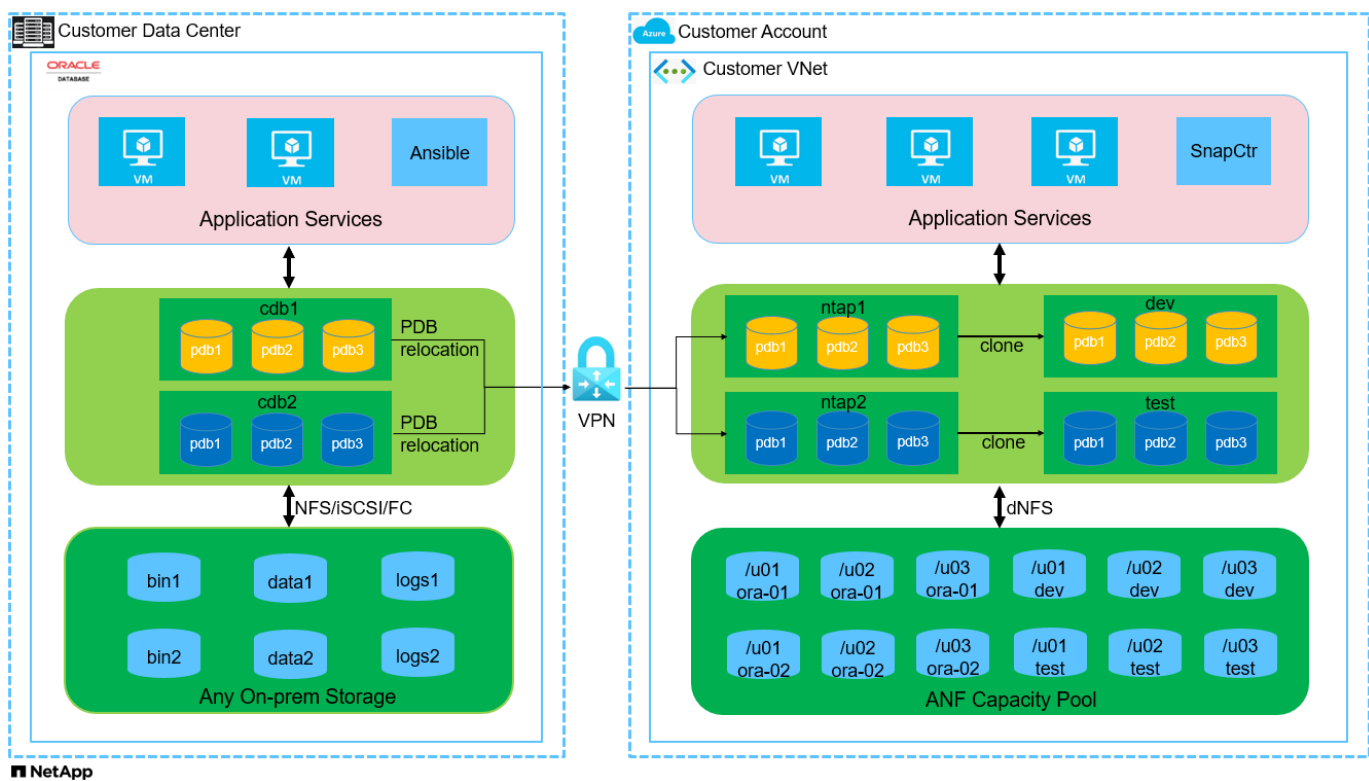
Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle-Datenbanken auf Azure NetApp Files implementieren möchte.
- Ein Solution Architect für Datenbanken, der Oracle-Workloads auf Azure NetApp Files testen möchte.
- Ein Storage-Administrator, der Oracle Datenbanken auf Azure NetApp Files implementieren und managen möchte.
- Ein Applikationseigentümer, der eine Oracle Database auf Azure NetApp Files einrichten möchte.

Test- und Validierungsumgebung der Lösung

Die Lösung wurde in einer Testumgebung getestet und validiert. Siehe Abschnitt [\[Key Factors for Deployment Consideration\]](#) Finden Sie weitere Informationen.

Der Netapp Architektur Sind



Hardware- und Softwarekomponenten

Hardware		
Azure NetApp Dateien	Aktuelles Angebot in Azure von Microsoft	Kapazitäts-Pool mit Premium-Service Level

Azure VM für DB-Server	Standard_B4ms – 4 vCPUs, 16 gib	Zwei Instanzen von Linux Virtual Machines
Azure VM für SnapCenter	Standard_B4ms – 4 vCPUs, 16 gib	Eine virtuelle Windows-Maschineninstanz
Software		
Redhat Linux	RHEL Linux 8.6 (LVM) – x64 Gen2	Bereitstellung der RedHat Subscription für Tests
Windows Server	2022 DataCenter; AE-Hotpatch - x64 Gen2	Hosting von SnapCenter-Servern
Oracle Datenbank	Version 19.18	Patch p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Version 12.2.0.1.36	Patch p6880880_190000_Linux-x86-64.zip
SnapCenter Server	Version 5.0	Workgroup-Bereitstellung
Öffnen Sie JDK	Version java-11-openjdk	Anforderungen für SnapCenter Plugin auf DB VMs
NFS	Version 3.0	Oracle dNFS aktiviert
Ansible	Kern 2.16.2	Python 3.6.8

Konfiguration der Oracle-Datenbank in der Laborumgebung

Server	* Datenbank*	DB-Speicher
ora-01	NTAP1(NTAP1_PDB1,NTAP1_PDB2,NTAP1_PDB3)	/U01, /u02, /u03 NFS-Mounts auf ANF-Kapazitäts-Pool
ora-02	NTAP2(NTAP2_PDB1,NTAP2_PDB2,NTAP2_PDB3)	/U01, /u02, /u03 NFS-Mounts auf ANF-Kapazitäts-Pool

Wichtige Faktoren für die Implementierung

- **SnapCenter-Bereitstellung.** SnapCenter kann in einer Windows-Domäne oder Workgroup-Umgebung bereitgestellt werden. Bei einer domänenbasierten Bereitstellung sollte das Domänenbenutzerkonto ein Domänenadministratorkonto sein, oder der Domänenbenutzer gehört zur Gruppe des lokalen Administrators auf dem SnapCenter-Hostserver.
- **Namensauflösung.** der SnapCenter-Server muss den Namen auf die IP-Adresse für jeden verwalteten Server der Zieldatenbank auflösen. Jeder Host des Zieldatenbankservers muss den Namen des SnapCenter-Servers in die IP-Adresse auflösen. Wenn ein DNS-Server nicht verfügbar ist, fügen Sie den lokalen Hostdateien Namen zur Auflösung hinzu.
- **Konfiguration der Ressourcengruppe.** die Ressourcengruppe in SnapCenter ist eine logische Gruppierung ähnlicher Ressourcen, die gemeinsam gesichert werden kann. Dadurch wird die Anzahl der Backup-Jobs in einer großen Datenbankumgebung vereinfacht und verringert.
- **Separate vollständige Datenbank- und Archiv-Log-Sicherung.** vollständige Datenbank-Backup beinhaltet Datenvolumen und Log-Volumen konsistente Gruppen-Snapshots. Ein häufiger vollständiger Datenbank-Snapshot verursacht zwar mehr Storage-Verbrauch, verbessert aber die RTO. Eine Alternative sind seltener vollständige Datenbank-Snapshots und häufigere Backups von Archivprotokollen. Dies

verbraucht weniger Speicherplatz und verbessert die RPO, kann aber die RTO erweitern. Berücksichtigen Sie bei der Einrichtung des Backup-Schemas Ihre RTO- und RPO-Ziele. Es gibt auch eine Begrenzung (1023) der Anzahl der Snapshot Backups auf einem Volume.

- **Privilegien-Delegierung.** Nutzen Sie die in der SnapCenter-Benutzeroberfläche integrierte rollenbasierte Zugriffssteuerung, um Berechtigungen an Anwendungs- und Datenbankteams zu delegieren, falls gewünscht.

Lösungsimplementierung

In den folgenden Abschnitten werden Schritt-für-Schritt SnapCenter-Verfahren für die Implementierung, Konfiguration und das Backup, Recovery und Klonen von Oracle-Datenbanken auf Azure NetApp Files in der Azure Cloud beschrieben.

Voraussetzungen für die Bereitstellung

Für die Implementierung sind vorhandene Oracle-Datenbanken erforderlich, die auf ANF in Azure ausgeführt werden. Falls nicht, führen Sie die folgenden Schritte aus, um zwei Oracle-Datenbanken für die Lösungsvalidierung zu erstellen. Weitere Informationen zur Implementierung von Oracle Database auf ANF in Azure Cloud mit Automatisierung finden Sie in TR-4987: "[Vereinfachte, automatisierte Oracle-Implementierung auf Azure NetApp Files mit NFS](#)"

1. Ein Azure-Konto wurde eingerichtet und die erforderlichen vnet- und Netzwerksegmente wurden in Ihrem Azure-Konto erstellt.
2. Implementieren Sie im Azure-Cloud-Portal Azure Linux-VMs als Oracle DB-Server. Erstellen Sie einen Azure NetApp Files-Kapazitätspool und Datenbank-Volumes für die Oracle-Datenbank. VM-SSH-Authentifizierung für privaten/öffentlichen Schlüssel für Azure-Benutzer für DB-Server aktivieren. Details zur Umgebungs-Einrichtung finden Sie im Architekturdiagramm im vorherigen Abschnitt. Auch genannt "[Schritt-für-Schritt-Anweisungen zur Oracle-Implementierung auf Azure VM und Azure NetApp Files](#)" Ausführliche Informationen finden Sie unter.



Stellen Sie bei Azure-VMs, die mit lokaler Festplattenredundanz implementiert werden, sicher, dass Sie mindestens 128 G auf der VM-Root-Festplatte zugewiesen haben, damit ausreichend Speicherplatz für die Bereitstellung von Oracle-Installationsdateien und die Hinzufügen der OS-Swap-Datei zur Verfügung steht. Erweitern Sie die Partition /tmp und /rootlv OS entsprechend. Stellen Sie sicher, dass die Benennung des Datenbank-Volumes der Konvention VMname-u01, VMname-u02 und VMname-u03 entspricht.

```
sudo lvresize -r -L +20G /dev/mapper/rootvg-rootlv
```

```
sudo lvresize -r -L +10G /dev/mapper/rootvg-tmplv
```

3. Stellen Sie im Azure-Cloud-Portal einen Windows-Server bereit, damit das UI-Tool NetApp SnapCenter mit der neuesten Version ausgeführt wird. Details finden Sie unter folgendem Link: "[Installieren Sie den SnapCenter-Server](#)".
4. Stellen Sie eine Linux VM als Ansible-Controller-Node mit der neuesten Version von Ansible und Git bereit. Details finden Sie unter folgendem Link: "[Erste Schritte mit der Automatisierung von NetApp Lösungen](#)" In Abschnitt -
Setup the Ansible Control Node for CLI deployments on RHEL / CentOS Oder
Setup the Ansible Control Node for CLI deployments on Ubuntu / Debian.



Der Ansible-Controller-Node kann entweder On-PreMises oder in der Azure-Cloud finden, sofern er Azure DB VMs über ssh-Port erreichen kann.

5. Klonen Sie eine Kopie des NetApp Toolkit zur Implementierungsautomatisierung für NFS. Folgen Sie den Anweisungen unter "[TR-4887](#)" Um Playbooks auszuführen.

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-bb/na_oracle_deploy_nfs.git
```

6. Stellen Sie die folgenden Oracle 19c-Installationsdateien auf das Azure DB VM /tmp/Archive-

Verzeichnis mit 777 Berechtigungen bereit.

```
installer_archives:  
- "LINUX.X64_193000_db_home.zip"  
- "p34765931_190000_Linux-x86-64.zip"  
- "p6880880_190000_Linux-x86-64.zip"
```

7. Sehen Sie sich das folgende Video an:

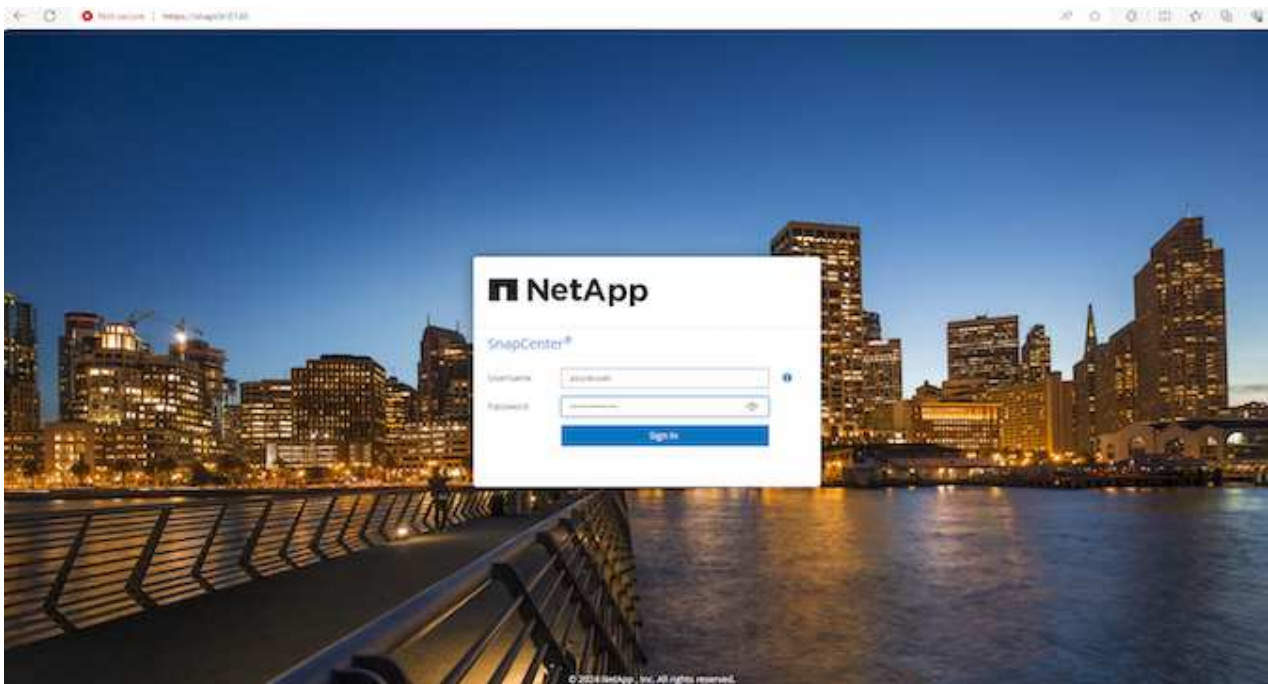
[Oracle Database Backup, Recovery und Klonen auf ANF mit SnapCenter](#)

8. Überprüfen Sie die `Get Started` Online-Menü.

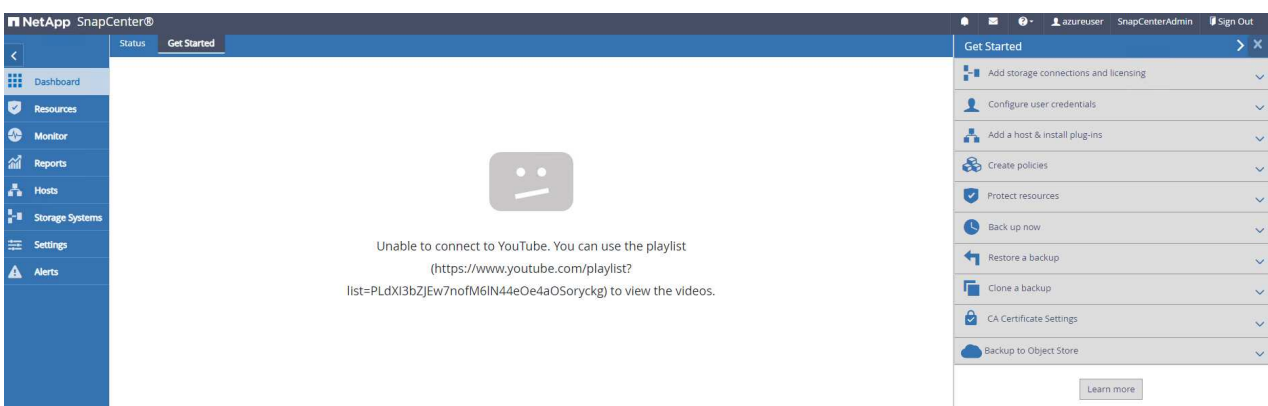
Installation und Einrichtung von SnapCenter

Wir empfehlen, durch online zu gehen "[SnapCenter-Softwaredokumentation](#)" Bevor Sie mit der SnapCenter-Installation und -Konfiguration fortfahren: . Im Folgenden finden Sie eine allgemeine Zusammenfassung der Schritte für die Installation und Einrichtung der SnapCenter Software für Oracle auf Azure ANF.

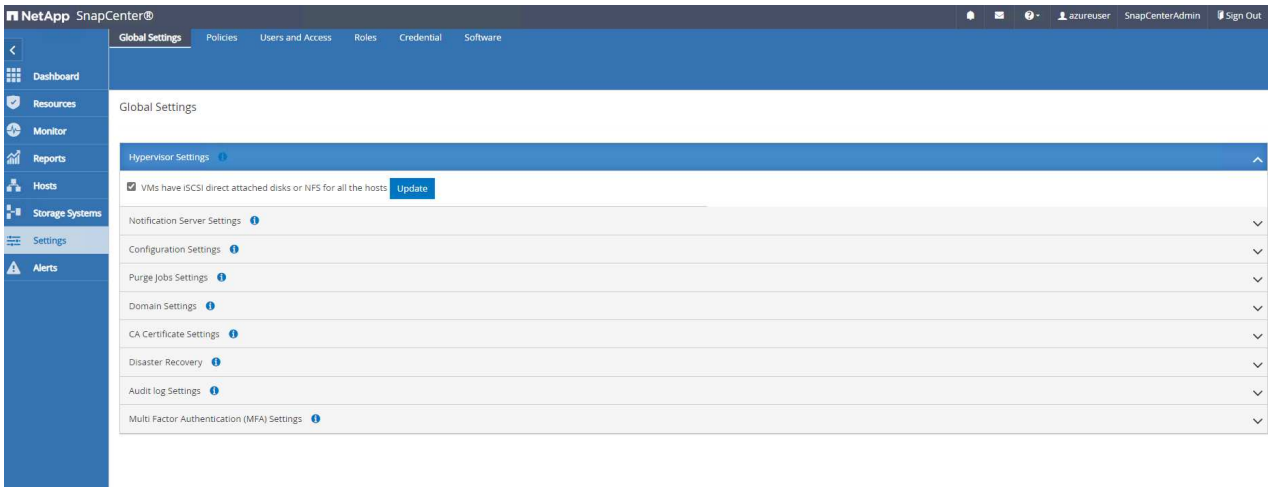
1. Laden Sie vom SnapCenter-Windows-Server die neueste java-JDK herunter, und installieren Sie sie unter "[Holen Sie sich Java für Desktop-Anwendungen](#)".
2. Laden Sie vom SnapCenter Windows-Server die neueste Version (derzeit 5.0) der ausführbaren SnapCenter-Installationsdatei von der NetApp Support-Website herunter, und installieren Sie sie: "[NetApp Support](#)".
3. Starten Sie nach der Installation des SnapCenter-Servers den Browser, um sich bei SnapCenter mit den Anmeldeinformationen des lokalen Windows-Administrators oder des Domänenbenutzers über Port 8146 anzumelden.



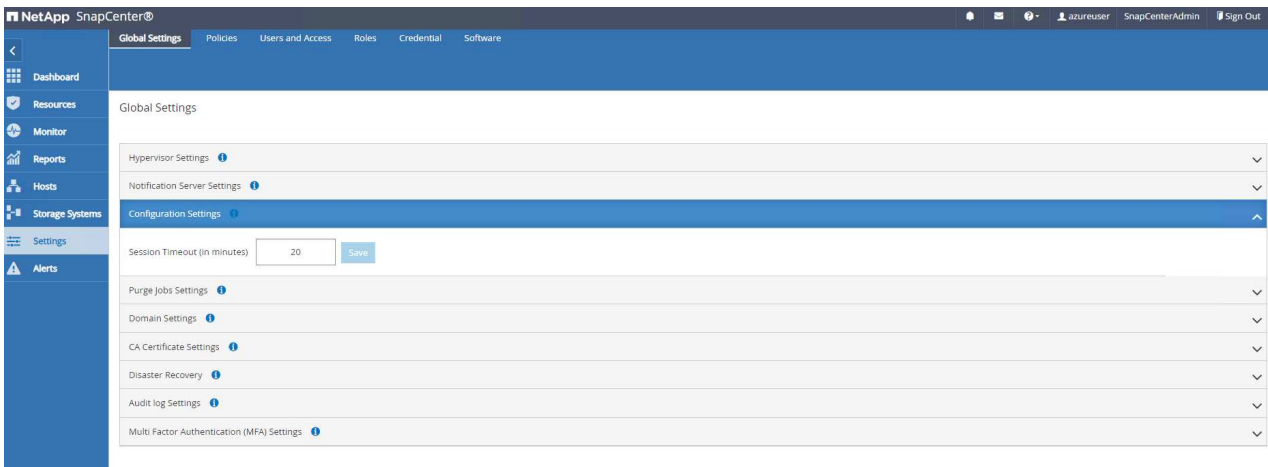
4. Prüfen Get Started Online-Menü.



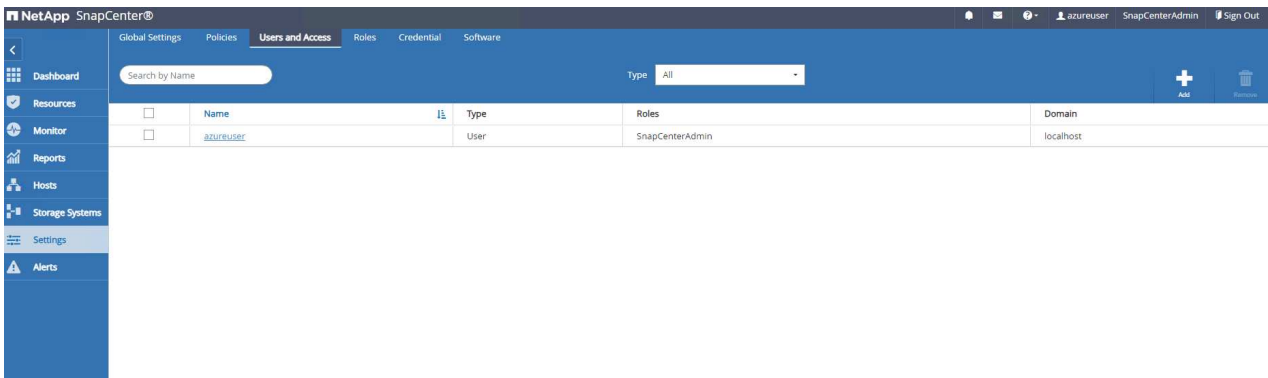
5. In Settings-Global Settings, Überprüfen Hypervisor Settings Und klicken Sie auf Aktualisieren.



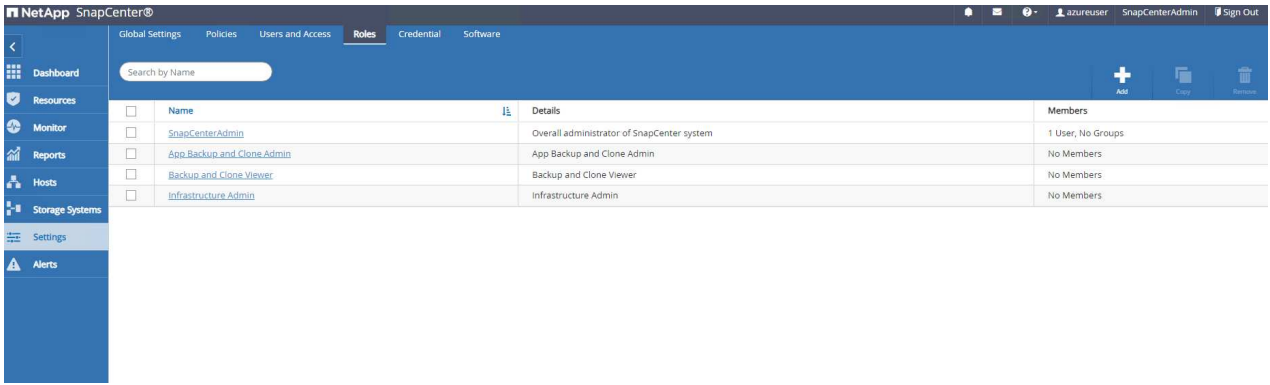
6. Bei Bedarf einstellen `Session Timeout` Für die SnapCenter-Benutzeroberfläche das gewünschte Intervall.



7. Fügen Sie bei Bedarf weitere Benutzer zu SnapCenter hinzu.



8. Der `Roles` Auf der Registerkarte werden die integrierten Rollen aufgeführt, die verschiedenen SnapCenter-Benutzern zugewiesen werden können. Benutzerdefinierte Rollen können auch vom Admin-Benutzer mit den gewünschten Berechtigungen erstellt werden.



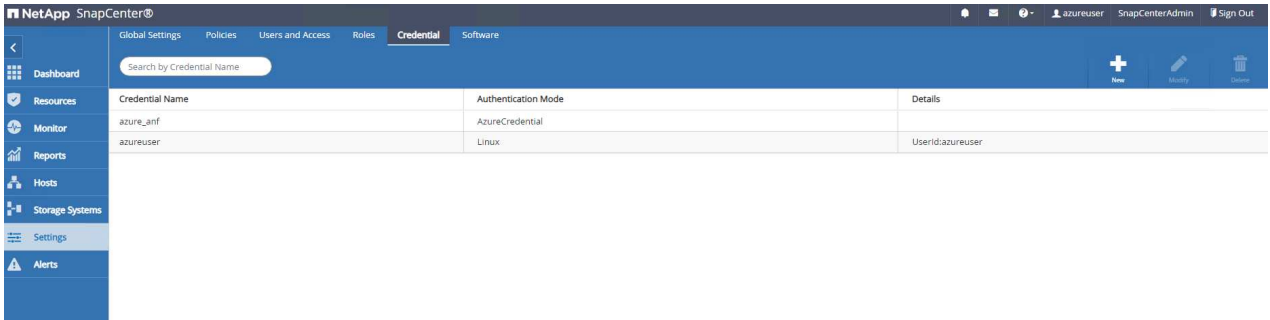
NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

Search by Name

Name	Details	Members
SnapCenterAdmin	Overall administrator of SnapCenter system	1 User, No Groups
App Backup and Clone Admin	App Backup and Clone Admin	No Members
Backup and Clone Viewer	Backup and Clone Viewer	No Members
Infrastructure Admin	Infrastructure Admin	No Members

9. Von `Settings-Credential` Erstellen Sie Anmeldeinformationen für SnapCenter-Management-Ziele. In diesem Demo-Anwendungsfall sind sie linux-Benutzer für die Anmeldung bei Azure VM und ANF-Berechtigungen für den Zugriff auf den Kapazitäts-Pool.



NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

Search by Credential Name

Credential Name	Authentication Mode	Details
azure_anf	AzureCredential	
azureuser	Linux	UserId:azureuser

Credential



Credential Name

Authentication Mode

Authentication Type Password Based SSH Key Based

Username

SSH Private Key

```
XRlRk1QCaE0Hg==  
-----END RSA PRIVATE KEY-----
```

Use sudo privileges

Cancel

OK

Credential ✕

Credential Name

Authentication Mode ▼

Azure Details ⓘ

Tenant ID

Client ID

Client Secret Key

10. Von Storage Systems Registerkarte, hinzufügen Azure NetApp Files Mit oben erstellten Zugangsdaten.

NetApp SnapCenter®

ONTAP Storage **Azure NetApp Files**

Search by NetApp Account

<input type="checkbox"/>	NetApp Account	Resource Group	Credential
<input type="checkbox"/>	ANFAVSAcct	ANFAVSRG	azure_anf

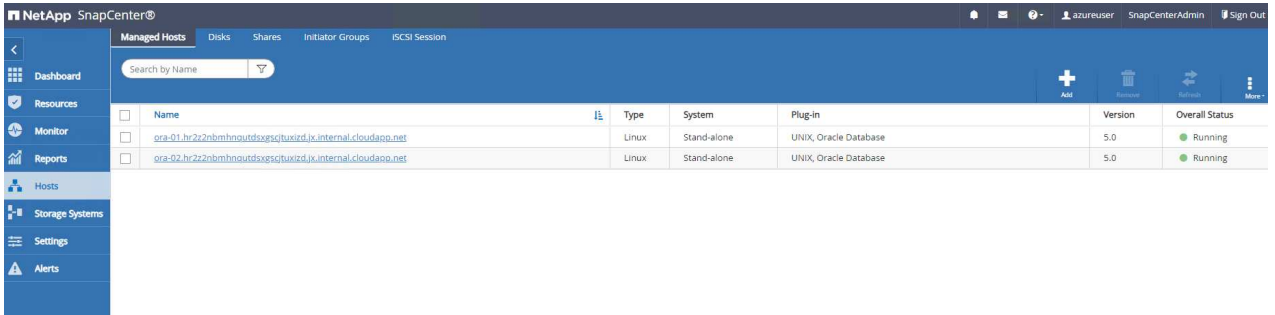
Add Azure NetApp Account ✕

Credential ⓘ

Subscription ⓘ

NetApp Account ⓘ

11. Von Hosts Fügen Sie die Azure DB VMs hinzu, die das SnapCenter Plug-in für Oracle auf Linux installieren.



The screenshot shows the NetApp SnapCenter interface. The 'Managed Hosts' tab is active, displaying a table with the following data:

Name	Type	System	Plug-in	Version	Overall Status
ora-01.hr2z2nbmhnoudsqsqfuxoz4x.internal.cloudapp.net	Linux	Stand-alone	UNIX, Oracle Database	5.0	Running
ora-02.hr2z2nbmhnoudsqsqfuxoz4x.internal.cloudapp.net	Linux	Stand-alone	UNIX, Oracle Database	5.0	Running

Add Host

Host Type: Linux

Host Name: ora-01

Credentials: azureuser

Select Plug-ins to Install SnapCenter Plug-ins Package 5.0 for Linux

- Oracle Database
- SAP HANA
- Unix File Systems

[More Options](#): Port, Install Path, Custom Plug-Ins...

Submit Cancel

More Options ✕

Port i

Installation Path i

Skip optional preinstall checks i

Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

No plug-ins found.

12. Sobald das Host-Plug-in auf der VM des DB-Servers installiert ist, werden die Datenbanken auf dem Host automatisch erkannt und in sichtbar **Resources** Registerkarte. Zurück zu **Settings-Policies**, Erstellen Sie Backup-Richtlinien für vollständige Oracle-Datenbank Online-Backup und Archiv Protokolle nur Backup. Weitere Informationen finden Sie in diesem Dokument "[Erstellung von Backup-Richtlinien für Oracle Datenbanken](#)" Für detaillierte Schritte.

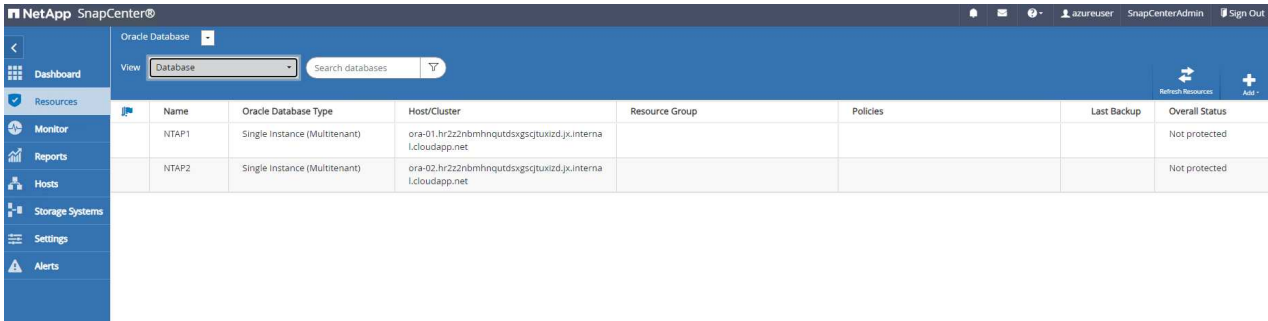
The screenshot shows the NetApp SnapCenter interface. The left sidebar contains navigation options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled 'Oracle Database' and shows a table of backup policies. The table has columns for Name, Backup Type, Schedule Type, Replication, and Verification. Two policies are listed: 'Oracle archive/logs backup' with 'LOG, ONLINE' backup type and 'Hourly' schedule, and 'Oracle full online backup' with 'FULL, ONLINE' backup type and 'Hourly' schedule.

Name	Backup Type	Schedule Type	Replication	Verification
Oracle archive/logs backup	LOG, ONLINE	Hourly		
Oracle full online backup	FULL, ONLINE	Hourly		

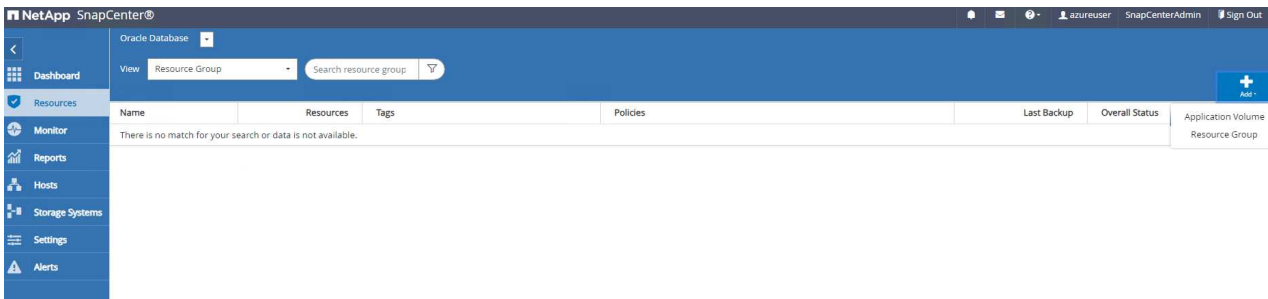
Datenbank-Backup

Ein NetApp-Snapshot-Backup erstellt ein zeitpunktgenaues Image der Datenbank-Volumes, mit denen Sie im Falle eines Systemausfalls oder Datenverlusts eine Wiederherstellung durchführen können. Snapshot Backups dauern sehr wenig Zeit, in der Regel weniger als eine Minute. Das Backup Image verbraucht nur minimalen Storage und verursacht vernachlässigbaren Performance-Overhead, da seit Erstellung der letzten Snapshot Kopie nur Änderungen an Dateien aufgezeichnet werden. Im folgenden Abschnitt wird die Implementierung von Snapshots für Oracle-Datenbank-Backups in SnapCenter demonstriert.

1. Navigieren zu Resources Registerkarte, die die Datenbanken auflistet, die nach der Installation des SnapCenter-Plug-ins auf der Datenbank-VM ermittelt wurden. Zu Beginn der Overall Status Der Datenbank wird als angezeigt Not protected.



2. Klicken Sie auf View Zum Ändern in Resource Group. Klicken Sie auf Add melden sie sich rechts an, um eine Ressourcengruppe hinzuzufügen.



3. Benennen Sie Ihre Ressourcengruppe, Ihre Tags und jede benutzerdefinierte Benennung.

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name

Tags

Use custom name format for Snapshot copy

Backup settings

Exclude archive log destinations from backup

Previous Next

4. Fügen Sie Ihrem Ressourcen hinzu `Resource Group`. Durch die Gruppierung ähnlicher Ressourcen lässt sich das Datenbankmanagement in einer großen Umgebung vereinfachen.

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host

Available Resources

Selected Resources

NTAP1 (ora-01.hr2z2nbmhnqutdsxsgjtuxizd.jk.internal.cloudapp.i
NTAP2 (ora-02.hr2z2nbmhnqutdsxsgjtuxizd.jk.internal.cloudapp.i

><

Previous Next

5. Wählen Sie die Sicherungsrichtlinie aus, und legen Sie einen Zeitplan fest, indem Sie auf „+“ unter klicken `Configure Schedules`.



Select one or more policies and configure schedules

Oracle full online backup + ⓘ

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
Oracle full online backup	None	+

Total 1

Previous Next

Add schedules for policy Oracle full online backup

Hourly

Start date 02/06/2024 05:55 pm

Expires on 03/06/2024 05:51 pm

Repeat every 2 hours 0 mins

i The schedules are triggered in the SnapCenter Server time zone.

Cancel OK

6. Wenn die Backup-Verifizierung nicht in der Richtlinie konfiguriert ist, lassen Sie die Überprüfungsseite wie angezeigt.

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

Total 0

Previous Next

7. Um einen Backup-Bericht und eine Benachrichtigung per E-Mail zu versenden, wird in der Umgebung ein SMTP-Mailserver benötigt. Oder lassen Sie sie schwarz, wenn kein Mailserver eingerichtet ist.

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings ⓘ

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

Attach job report

Previous Next

8. Zusammenfassung der neuen Ressourcengruppe.

New Resource Group

1 — 2 — 3 — 4 — 5 — 6
 Name — Resources — Policies — Verification — Notification — Summary

Resource group name: full_online_bkup
 Tags: oradata
 Policy: Oracle full online backup: Hourly
 Plug-in: SnapCenter Plug-in for Oracle Database
 Verification enabled for policy: None
 Send email: No

Previous Finish

9. Wiederholen Sie die oben genannten Verfahren, um ein Datenbank-Archiv-Protokoll nur Backup mit entsprechenden Backup-Policy zu erstellen.

NetApp SnapCenter®

Oracle Database

View: Resource Group Search resource group

Name	Resources	Tags	Policies	Last Backup	Overall Status
full_online_bkup	2	oradata	Oracle full online backup	02/06/2024 6:00:44 PM	Completed
archivelog_bkup	2	oralog	Oracle archivelogs backup	02/06/2024 5:59:25 PM	Completed

10. Klicken Sie auf eine Ressourcengruppe, um die darin vorhandenen Ressourcen anzuzeigen. Neben dem geplanten Backup-Job kann durch Klicken auf eine einmalige Sicherung ausgelöst werden Backup Now.

NetApp SnapCenter®

Oracle Database full_online_bkup Details

Search resource groups search

Name	Resource Name	Type	Host
full_online_bkup	NTAP1	Oracle Database	ora-01.hr222nbmhnqudsxgscjtuxizd.jx.internal.cloudapp.net
archivelog_bkup	NTAP2	Oracle Database	ora-02.hr222nbmhnqudsxgscjtuxizd.jx.internal.cloudapp.net

Modify Resource Group Backup Now Maintenance Delete

Backup



Create a backup for the selected resource group

Resource Group

full_online_bkup

Policy

Oracle full online backup



Verify after backup

Cancel

Backup

11. Klicken Sie auf den laufenden Job, um ein Überwachungsfenster zu öffnen, in dem der Bediener den Auftragsfortschritt in Echtzeit verfolgen kann.

Job Details



Backup of Resource Group 'full_online_bkup' with policy 'Oracle full online backup'

- ✓ Backup of Resource Group 'full_online_bkup' with policy 'Oracle full online backup'
- ✓ ▶ ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net
- ✓ ▶ ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net

i Task Name: Backup of Resource Group 'full_online_bkup' with policy 'Oracle full online backup' Start Time: 02/06/2024 6:00:05 PM End Time: 02/06/2024 6:00:44 PM

View Logs

Cancel Job

Close

- Ein Snapshot-Backup-Satz wird unter der Datenbanktopologie angezeigt, sobald ein erfolgreicher Backup-Job abgeschlossen ist. Ein vollständiges Datenbank-Backup-Set umfasst einen Snapshot der Datenbankdatenvolumes und einen Snapshot der Datenbankprotokollvolumes. Ein nur-Protokoll-Backup enthält nur einen Snapshot der Datenbankprotokollvolumes.

The screenshot displays the NetApp SnapCenter interface for an Oracle Database. The main content area is titled "NTAP1 Topology" and shows "Manage Copies" with 3 Backups and 0 Clones. A "Summary Card" provides a quick overview: 3 Backups (1 Data Backup, 2 Log Backups), 0 Clones, and 0 Snapshots Locked. Below this is a table of "Primary Backup(s)" with columns for Backup Name, Snapshot Lock Expiration, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The table lists three backups: two Log backups and one Data backup.

Backup Name	Snapshot Lock Expiration	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora-01_02-06-2024_18_00_06_0582_1		1	Log	02/06/2024 6:00:41 PM	Not Applicable	False	Not Cataloged	3374950
ora-01_02-06-2024_18_00_06_0582_0		1	Data	02/06/2024 6:00:26 PM	Unverified	False	Not Cataloged	3374903
ora-01_02-06-2024_17_59_01_1158_1		1	Log	02/06/2024 5:59:18 PM	Not Applicable	False	Not Cataloged	3374762

Datenbank-Recovery

Die Datenbank-Recovery über SnapCenter stellt eine Snapshot-Kopie des zeitpunktgenauen Images des Datenbank-Volumes wieder her. Die Datenbank wird dann per SCN/Timestamp oder einem Punkt, wie von den verfügbaren Archivprotokollen im Backup-Set erlaubt, an einen gewünschten Punkt weitergeleitet. Im folgenden Abschnitt wird der Workflow der Datenbank-Recovery mithilfe der UI von SnapCenter dargestellt.

1. Von **Resources** Öffnen Sie die Datenbank **Primary Backup(s)** Seite. Wählen Sie den Snapshot des Datenbank-Daten-Volumes aus, und klicken Sie auf **Restore** Um den Datenbank-Recovery-Workflow zu starten. Notieren Sie sich die SCN-Nummer oder den Zeitstempel in den Backup-Sätzen, wenn Sie die Recovery durch Oracle SCN oder Zeitstempel ausführen möchten.

NTAP1 Topology

Backup to Object Store Protect Refresh

Manage Copies

3 Backups
0 Clones
Local copies

Summary Card

3 Backups
1 Data Backup
2 Log Backups
0 Clones
0 Snapshots Locked

Primary Backup(s)

search

Catalog Rename Clone **Restore** Mount Unmount Delete

Backup Name	Snapshot Lock Expiration	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora-01_02-06-2024_18_00_06_0582_1		1	Log	02/06/2024 6:00:41 PM	Not Applicable	False	Not Cataloged	3374950
ora-01_02-06-2024_18_00_06_0582_0		1	Data	02/06/2024 6:00:26 PM	Unverified	False	Not Cataloged	3374903
ora-01_02-06-2024_17_59_01_1158_1		1	Log	02/06/2024 5:59:18 PM	Not Applicable	False	Not Cataloged	3374762

2. Wählen Sie **Restore Scope**. Bei einer Container-Datenbank kann SnapCenter flexibel eine vollständige Container-Datenbank (alle Datendateien), steckbare Datenbanken oder Restores auf Tablespace-Ebene durchführen.

Restore NTAP1 ×

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Restore Scope ⓘ

All Datafiles

Pluggable databases (PDBs)

Pluggable database (PDB) tablespaces

Control files

Database State

Change database state if needed for restore and recovery

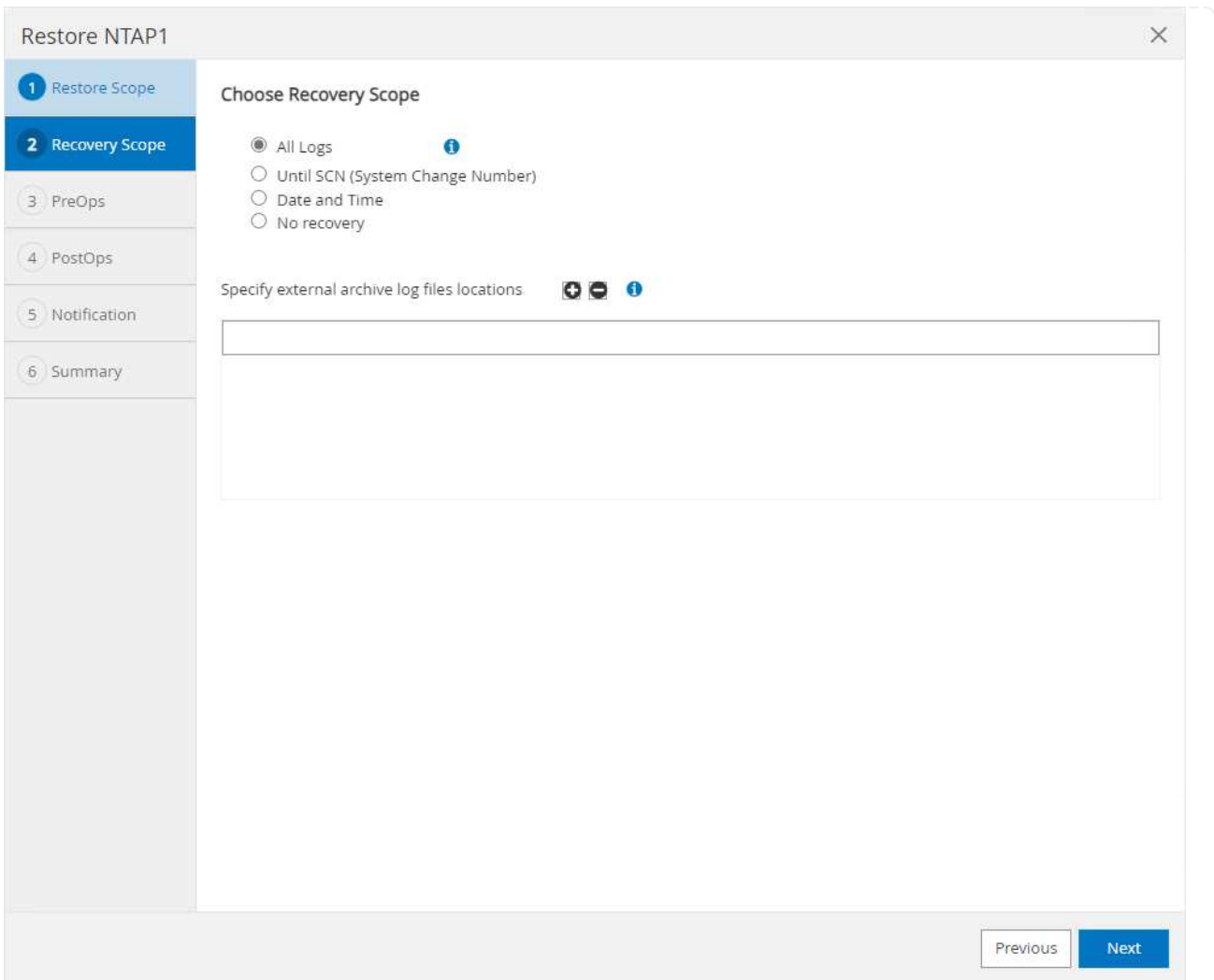
Restore Mode ⓘ

Force in place restore

If this check box is not selected and if any of the in place restore criteria is not met, restore will be performed using the connect and copy method. The connect and copy restore method might take time based on the files being restored.

Previous Next

3. Wählen Sie **Recovery Scope**. **All logs** bedeutet, alle verfügbaren Archivprotokolle im Backup-Satz anzuwenden. Point-in-Time-Wiederherstellung durch SCN oder Zeitstempel sind ebenfalls verfügbar.



4. Der `PreOps` Ermöglicht die Ausführung von Skripts für die Datenbank vor der Wiederherstellung/Wiederherstellung.

Restore NTAP1



1 Restore Scope

Specify optional scripts to run before performing a restore job ⓘ

2 Recovery Scope

Prescript full path Enter Prescript path

3 PreOps

Arguments

4 PostOps

Script timeout secs

5 Notification

6 Summary

Previous

Next

5. Der `PostOps` Ermöglicht die Ausführung von Skripts für die Datenbank nach der Wiederherstellung/Wiederherstellung.

Restore NTAP1 ×

1 Restore Scope **Specify optional scripts to run after performing a restore job** ⓘ

2 Recovery Scope Postscript full path /var/opt/snapcenter/spl/scripts/ Enter Postscript path

3 PreOps Arguments

4 PostOps Open the database or container database in READ-WRITE mode after recovery

5 Notification

6 Summary

6. Benachrichtigung per E-Mail, falls gewünscht.

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification**
- 6 Summary

Provide email settings ⓘ

Email preference:

From:

To:

Subject:

Attach job report

⚠ If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous **Next**

7. Jobzusammenfassung wiederherstellen

Restore NTAP1
✕

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary

Summary

Backup name	ora-01_02-06-2024_18_00_06_0582_0
Backup date	02/06/2024 6:00:26 PM
Restore scope	All DataFiles
Recovery scope	All Logs
Options	Change database state if necessary , Open the database or container database in READ-WRITE mode after recovery
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

Previous
Finish

8. Klicken Sie auf Job ausführen, um sie zu öffnen Job Details Fenster. Der Jobstatus kann auch über das geöffnet und angezeigt werden Monitor Registerkarte.

Job Details



Restore 'ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net\NTAP1'

✓ ▾ Restore 'ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net\NTAP1'

✓ ▾ ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net

- ✓ ▶ Prescripts
- ✓ ▶ Mount log backups
- ✓ ▶ Pre Restore
- ✓ ▶ Restore
- ✓ ▶ Post Restore
- ✓ ▶ Unmount log backups
- ✓ ▶ Postscripts
- ✓ ▶ Post Restore Cleanup
- ✓ ▶ Data Collection

 Task Name: ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net Start Time: 02/06/2024 4:04:55 PM End Time: 02/06/2024 4:08:42 PM

View Logs

Cancel Job

Close

Datenbankklone

Ein Datenbankklon über SnapCenter wird durch die Erstellung eines neuen Volumes aus einem Snapshot eines Volumes durchgeführt. Das System verwendet die Snapshot-Informationen, um ein neues Volume mithilfe der Daten auf dem Volume zu klonen, als der Snapshot erstellt wurde. Zudem ist es schnell (einige Minuten) und effizient im Vergleich zu anderen Methoden, eine geklonte Kopie der Produktionsdatenbank zu Entwicklungs- oder Testzwecken zu erstellen. Auf diese Weise wird das Lifecycle Management Ihrer Datenbankapplikation deutlich verbessert. Im folgenden Abschnitt wird der Workflow des Datenbankklons mithilfe der UI von SnapCenter dargestellt.

1. Von Resources Öffnen Sie die Datenbank Primary Backup(s) Seite. Wählen Sie den Snapshot des Datenbank-Daten-Volumes aus, und klicken Sie auf clone Um den Workflow für Datenbankklone zu starten.

NTAP1 Topology

Manage Copies

3 Backups
0 Clones
Local copies

Summary Card

- 3 Backups
- 1 Data Backup
- 2 Log Backups
- 0 Clones
- 0 Snapshots Locked

Primary Backup(s)

search

Clone

Backup Name	Snapshot Lock Expiration	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora-01_02-06-2024_18_00_06_0582_1		1	Log	02/06/2024 6:00:41 PM	Not Applicable	False	Not Cataloged	3374950
ora-01_02-06-2024_18_00_06_0582_0		1	Data	02/06/2024 6:00:26 PM	Unverified	False	Not Cataloged	3374903
ora-01_02-06-2024_17_59_01_1158_1		1	Log	02/06/2024 5:59:18 PM	Not Applicable	False	Not Cataloged	3374762

2. Benennen Sie die SID der Klondatenbank. Optional kann für eine Container-Datenbank auch der Klon auf PDB-Ebene durchgeführt werden.

Clone from NTAP1



- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Capacity Pool Max. Throughput (MiB/s) 

Complete Database Clone

Clone SID

Exclude PDBs:

PDB Clone

Previous

Next

3. Wählen Sie den DB-Server aus, auf dem die geklonte Datenbankkopie gespeichert werden soll. Behalten Sie die standardmäßigen Dateispeicherorte bei, es sei denn, Sie möchten sie anders benennen.

Clone from NTAP1
✕

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Select the host to create a clone

Clone host:

Datafile locations ⓘ

Reset

Control files ⓘ

<input type="text" value="/u02_ntap1dev/ntap1dev/control/control01.ctl"/>	✕	↑	+
<input type="text" value="/u02_ntap1dev/ntap1dev/control/control02.ctl"/>	✕	↓	Reset

Redo logs ⓘ

Group	Size	Unit	Number of files			
▶ RedoGroup 1	✕	200	MB	1	+	+ Reset
▶ RedoGroup 2	✕	200	MB	1	+	
▶ RedoGroup 3	✕	200	MB	1	+	

Previous
Next

4. Ein identischer Oracle-Software-Stack wie in der Quelldatenbank hätte auf geklontem DB-Host installiert und konfiguriert werden sollen. Behalten Sie die Standardanmeldedaten bei, ändern Sie sie jedoch Oracle Home Settings Zur Abstimmung mit den Einstellungen auf dem Clone-DB-Host.

1 Name

Database Credentials for the clone

2 Locations

Credential name for sys user

None



3 Credentials

Database port

1521

4 PreOps

Oracle Home Settings i

5 PostOps

Oracle Home

/u01/app/oracle/product/19.0.0/NTAP2

6 Notification

Oracle OS User

oracle

7 Summary

Oracle OS Group

oinstall

Previous

Next

5. Der `PreOps` Ermöglicht die Ausführung von Skripten vor dem Klonvorgang. Datenbankparameter können an die Anforderungen einer Klon-Datenbank im Gegensatz zu einer Produktionsdatenbank angepasst werden, beispielsweise ein verringertes SGA-Ziel.

1 Name

Specify scripts to run before clone operation ⓘ

2 Locations

Prescript full path

3 Credentials

Arguments

4 PreOps

Script timeout

5 PostOps

Database Parameter settings

processes	320	✕	▲
remote_login_passwordfile	EXCLUSIVE	✕	+
sga_target	<input type="text" value="3G"/>	✕	
undo_tablespace	UNDOTBS1	✕	▼

Reset

6 Notification

7 Summary

Previous

Next

6. Der `PostOps` Ermöglicht die Ausführung von Skripten für die Datenbank nach dem Klonvorgang. Die Wiederherstellung der Klondatenbank kann SCN, Zeitstempel-basiert oder bis zum Abbrechen (ein Rolling Forward der Datenbank zum letzten archivierten Protokoll im Backup-Satz) sein.

Clone from NTAP1



- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps**
- 6 Notification
- 7 Summary

Recover Database

Until Cancel

Date and Time



Date-time format: MM/DD/YYYY hh:mm:ss

Until SCN (System Change Number)



Specify external archive log locations

Create new DBID

Create tempfile for temporary tablespace

Enter SQL queries to apply when clone is created

Enter scripts to run after clone operation

Previous

Next

7. Benachrichtigung per E-Mail, falls gewünscht.

1 Name

Provide email settings ⓘ

2 Locations

Email preference

Never ▾

3 Credentials

From

From email

4 PreOps

To

Email to

5 PostOps

Subject

Notification

6 Notification

 Attach job report

7 Summary

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Next

8. Jobzusammenfassung klonen.

Clone from NTAP1



1 Name	Summary	
2 Locations	Clone from backup	ora-01_02-06-2024_18_00_06_0582_0
3 Credentials	Clone SID	ntap1dev
4 PreOps	Capacity Pool Max. Throughput (MiB/s)	none
5 PostOps	Clone server	ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net
6 Notification	Exclude PDBs	none
7 Summary	Oracle home	/u01/app/oracle/product/19.0.0/NTAP2
	Oracle OS user	oracle
	Oracle OS group	oinstall
	Datafile mountpaths	/u02_ntap1dev
	Control files	/u02_ntap1dev/ntap1dev/control/control01.ctl /u02_ntap1dev/ntap1dev/control/control02.ctl
	Redo groups	RedoGroup =1 TotalSize =200 Path =/u02_ntap1dev/ntap1dev/redolog/redo01_01.log RedoGroup =2 TotalSize =200 Path =/u02_ntap1dev/ntap1dev/redolog/redo02_01.log RedoGroup =3 TotalSize =200 Path =/u02_ntap1dev/ntap1dev/redolog/redo03_01.log
	Recovery scope	Until Cancel
	Prescript full path	none
	Prescript arguments	
	Postscript full path	none
	Postscript arguments	
	Send email	No

[Previous](#)[Finish](#)

9. Klicken Sie auf Job ausführen, um sie zu öffnen Job Details Fenster. Der Jobstatus kann auch über das geöffnet und angezeigt werden Monitor Registerkarte.

Job Details

Clone from backup 'ora-01_02-06-2024_18_00_06_0582_0'

- ✓ ▾ Clone from backup 'ora-01_02-06-2024_18_00_06_0582_0'
 - ✓ ▾ ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net
 - ✓ ▶ Prescripts
 - ✓ ▶ Query Host Information
 - ✓ ▶ Prepare for Cloning
 - ✓ ▶ Cloning Resources
 - ✓ ▶ FileSystem Clone
 - ✓ ▶ Application Clone
 - ✓ ▶ Postscripts
 - ✓ ▶ Register Clone
 - ✓ ▶ Unmount Clone
 - ✓ ▶ Data Collection

Task Name: ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net Start Time: 02/06/2024 6:21:59 PM End Time: 02/06/2024 6:28:10 PM

View Logs

Cancel Job

Close

10. Unmittelbar geklonte Datenbank wird bei SnapCenter registriert.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
NTAP1	Single Instance (Multitenant)	ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net	archivelog_bkup full_online_bkup	Oracle archivelogs backup Oracle full online backup	02/06/2024 7:29:18 PM	Backup succeeded
ntap1dev	Single Instance (Multitenant)	ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net				Not protected
NTAP2	Single Instance (Multitenant)	ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net	archivelog_bkup full_online_bkup	Oracle archivelogs backup Oracle full online backup	02/06/2024 7:29:19 PM	Backup succeeded

11. Validierung der Klondatenbank auf dem DB-Server-Host Für eine geklonte Entwicklungsdatenbank sollte der Datenbankarchivierungsmodus deaktiviert werden.


```

[azureuser@ora-02 ~]$ sudo su
[root@ora-02 azureuser]# su - oracle
Last login: Tue Feb  6 16:26:28 UTC 2024 on pts/0

[oracle@ora-02 ~]$ uname -a
Linux ora-02 4.18.0-372.9.1.el8.x86_64 #1 SMP Fri Apr 15 22:12:19
EDT 2022 x86_64 x86_64 x86_64 GNU/Linux
[oracle@ora-02 ~]$ df -h

```

Filesystem	Size	Used	Avail
Use% Mounted on			
devtmpfs	7.7G	0	7.7G
0% /dev			
tmpfs	7.8G	0	7.8G
0% /dev/shm			
tmpfs	7.8G	49M	7.7G
1% /run			
tmpfs	7.8G	0	7.8G
0% /sys/fs/cgroup			
/dev/mapper/rootvg-rootlv	22G	17G	5.6G
75% /			
/dev/mapper/rootvg-usrlv	10G	2.0G	8.1G
20% /usr			
/dev/mapper/rootvg-homelv	1014M	40M	975M
4% /home			
/dev/sda1	496M	106M	390M
22% /boot			
/dev/mapper/rootvg-varlv	8.0G	958M	7.1G
12% /var			
/dev/sda15	495M	5.9M	489M
2% /boot/efi			
/dev/mapper/rootvg-tmplv	12G	8.4G	3.7G
70% /tmp			
tmpfs	1.6G	0	1.6G
0% /run/user/54321			
172.30.136.68:/ora-02-u03	250G	2.1G	248G
1% /u03			
172.30.136.68:/ora-02-u01	100G	10G	91G
10% /u01			
172.30.136.68:/ora-02-u02	250G	7.5G	243G
3% /u02			
tmpfs	1.6G	0	1.6G
0% /run/user/1000			
tmpfs	1.6G	0	1.6G
0% /run/user/0			
172.30.136.68:/ora-01-u02-Clone-020624161543077	250G	8.2G	242G

```
4% /u02_ntapldev
```

```
[oracle@ora-02 ~]$ cat /etc/oratab
```

```
#
```

```
# This file is used by ORACLE utilities.  It is created by root.sh  
# and updated by either Database Configuration Assistant while  
creating  
# a database or ASM Configuration Assistant while creating ASM  
instance.
```

```
# A colon, ':', is used as the field terminator.  A new line  
terminates
```

```
# the entry.  Lines beginning with a pound sign, '#', are comments.
```

```
#
```

```
# Entries are of the form:
```

```
#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:
```

```
#
```

```
# The first and second fields are the system identifier and home  
# directory of the database respectively.  The third field indicates  
# to the dbstart utility that the database should , "Y", or should  
not,
```

```
# "N", be brought up at system boot time.
```

```
#
```

```
# Multiple entries with the same $ORACLE_SID are not allowed.
```

```
#
```

```
#
```

```
NTAP2:/u01/app/oracle/product/19.0.0/NTAP2:Y
```

```
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT  
REMOVE THIS LINE)
```

```
ntapldev:/u01/app/oracle/product/19.0.0/NTAP2:N
```

```
[oracle@ora-02 ~]$ export ORACLE_SID=ntapldev
```

```
[oracle@ora-02 ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Tue Feb 6 16:29:02 2024  
Version 19.18.0.0.0
```

```
Copyright (c) 1982, 2022, Oracle.  All rights reserved.
```

```
Connected to:
```

```
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
```

```
Production
```

```
Version 19.18.0.0.0
```

```
SQL> select name, open_mode, log_mode from v$database;
```

NAME	OPEN_MODE	LOG_MODE
NTAP1DEV	READ WRITE	ARCHIVELOG

```
SQL> shutdown immediate;
```

```
Database closed.
```

```
Database dismounted.
```

```
ORACLE instance shut down.
```

```
SQL> startup mount;
```

```
ORACLE instance started.
```

```
Total System Global Area 3221223168 bytes
```

```
Fixed Size 9168640 bytes
```

```
Variable Size 654311424 bytes
```

```
Database Buffers 2550136832 bytes
```

```
Redo Buffers 7606272 bytes
```

```
Database mounted.
```

```
SQL> alter database noarchivelog;
```

```
Database altered.
```

```
SQL> alter database open;
```

```
Database altered.
```

```
SQL> select name, open_mode, log_mode from v$database;
```

NAME	OPEN_MODE	LOG_MODE
NTAP1DEV	READ WRITE	NOARCHIVELOG

```
SQL> show pdba
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	NTAP1_PDB1	MOUNTED	
4	NTAP1_PDB2	MOUNTED	
5	NTAP1_PDB3	MOUNTED	

```
SQL> alter pluggable database all open;
```

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- Azure NetApp Dateien

["https://azure.microsoft.com/en-us/products/netapp"](https://azure.microsoft.com/en-us/products/netapp)

- SnapCenter-Softwaredokumentation

["https://docs.netapp.com/us-en/snapcenter/index.html"](https://docs.netapp.com/us-en/snapcenter/index.html)

- TR-4987: Vereinfachte, automatisierte Oracle-Implementierung auf Azure NetApp Files mit NFS

["Bereitstellungsverfahren"](#)

TR-4977: Sicherung, Wiederherstellung und Klonen von Oracle Datenbanken mit SnapCenter Services - Azure

Allen Cao, Niyaz Mohamed, NetApp

Zweck

SnapCenter Services ist die SaaS-Version des klassischen UI-Tools für das SnapCenter-Datenbankmanagement, die über die NetApp BlueXP Cloud-Managementkonsole verfügbar ist. Es ist integraler Bestandteil des NetApp Cloud-Backup- und Datensicherungsangebots für Datenbanken wie Oracle und HANA, die auf Azure NetApp Files ausgeführt werden. Dieser SaaS-basierte Service vereinfacht die Bereitstellung herkömmlicher SnapCenter Standalone-Server, für die in der Regel ein Windows-Server in einer Windows-Domänenumgebung erforderlich ist.

In dieser Dokumentation zeigen wir, wie Sie SnapCenter-Services für Backups, Restores und Klonvorgänge von Oracle-Datenbanken einrichten, die auf Azure NetApp Files Volumes und Azure Computing-Instanzen implementiert sind. Es ist sehr einfach, Datensicherung für die auf Azure NetApp Files implementierte Oracle Database mit einer webbasierten BlueXP Benutzeroberfläche einzurichten.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Datenbank-Backup mit Snapshots für Oracle Datenbanken, die in Azure NetApp Files und Azure VMs gehostet werden
- Wiederherstellung der Oracle-Datenbank im Falle eines Ausfalls
- Schnelles Klonen primärer Datenbanken für Entwicklungs-, Test- und andere Anwendungsfälle

Zielgruppe

Diese Lösung ist für folgende Zielgruppen konzipiert:

- Der DBA, der Oracle Datenbanken managt, die auf Azure NetApp Files Storage laufen
- Lösungsarchitekt, der an Tests der Sicherung, Wiederherstellung und Klonvorgänge für Oracle-Datenbanken in Azure interessiert ist
- Der Storage-Administrator, der den Azure NetApp Files Storage unterstützt und managt
- Applikationseigentümer, die Eigentümer von Applikationen sind, die auf Azure NetApp Files Storage und

Azure VMs bereitgestellt werden

Test- und Validierungsumgebung der Lösung

Das Testen und Validieren dieser Lösung erfolgte in einer Lab-Umgebung, die der endgültigen Implementierungsumgebung möglicherweise nicht mehr entspricht. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind

Dieses Image bietet ein detailliertes Bild von BlueXP Backup und Recovery für Applikationen innerhalb der BlueXP Konsole, einschließlich der Benutzeroberfläche, der Connector und der gemanagten Ressourcen.

Hardware- und Softwarekomponenten

Hardware

Azure NetApp Files Storage durchführt	Premium Service Level	Typ „Auto QoS“ und 4 TB Storage-Kapazität für Tests
Azure Instanz für Computing	Standard-B4 ms (4 vcpus, 16 gib Speicher)	Zwei Instanzen wurden bereitgestellt, eine als primärer DB-Server und die andere als Clone-DB-Server

Software

Redhat Linux	Red hat Enterprise Linux 8.7 (LVM) – x64 Gen2	Bereitstellung der RedHat Subscription für Tests
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
SnapCenter-Service	Version v2.5.0-2822	Agent Version v2.5.0-2822

Wichtige Faktoren für die Implementierung

- **Connector soll im selben virtuellen Netzwerk / Subnetz wie Datenbanken und Azure NetApp Files bereitgestellt werden.** Wenn möglich, sollte der Connector in denselben virtuellen Azure Netzwerken und Ressourcengruppen bereitgestellt werden, was die Anbindung an den Azure NetApp Files-Speicher und die Azure-Recheninstanzen ermöglicht.
- **Ein im Azure Portal für SnapCenter Connector erstelltes Azure-Benutzerkonto oder Active Directory-Serviceprinzip.** für die Implementierung eines BlueXP Connectors sind bestimmte Berechtigungen erforderlich, um eine Virtual Machine und andere Compute-Ressourcen zu erstellen und zu konfigurieren, Netzwerke zu konfigurieren und Zugriff auf das Azure Abonnement zu erhalten. Außerdem sind Berechtigungen erforderlich, um später Rollen und Berechtigungen für den Connector zu erstellen. Benutzerdefinierte Rolle in Azure mit Berechtigungen erstellen und dem Benutzerkonto oder dem Dienstprinzip zuweisen. Details finden Sie unter folgendem Link: ["Azure-Berechtigungen einrichten"](#).
- **Ein in der Azure-Ressourcengruppe erstelltes SSH-Schlüsselpaar.** das SSH-Schlüsselpaar wird dem Azure-VM-Benutzer zur Anmeldung beim Connector-Host und auch dem Datenbank-VM-Host zur Bereitstellung und Ausführung eines Plug-ins zugewiesen. Die BlueXP Konsole-UI verwendet den ssh-Schlüssel zur Implementierung des SnapCenter Service-Plug-ins im Datenbank-Host für die einstufige

Plug-in-Installation und die Erkennung der Applikations-Host-Datenbank.

- **Zugangsdaten wurden zur BlueXP Konsoleneinstellung hinzugefügt.** um Azure NetApp Files Storage zur BlueXP Arbeitsumgebung hinzuzufügen, müssen in der BlueXP Konsoleneinstellung Zugangsdaten eingerichtet werden, die Berechtigungen für den Zugriff auf Azure NetApp Files über die BlueXP Konsole gewähren.
- **java-11-openjdk auf dem Host der Azure VM-Datenbankinstanz installiert.** die Installation des SnapCenter-Dienstes erfordert die java-Version 11. Sie muss auf dem Anwendungshost installiert werden, bevor die Plug-in-Bereitstellung versucht wird.

Lösungsimplementierung

Die umfassende NetApp Dokumentation bietet ein breiteres Spektrum, um Sie beim Schutz Ihrer Cloud-nativen Applikationsdaten zu unterstützen. Ziel dieser Dokumentation ist es, Schritt-für-Schritt-Verfahren zur Implementierung von SnapCenter Services über die BlueXP Konsole bereitzustellen, um die auf einem Azure NetApp Files Storage und einer Azure Computing-Instanz implementierte Oracle Datenbank zu sichern.

Um zu beginnen, gehen Sie wie folgt vor:

- Lesen Sie die allgemeinen Anweisungen "[Sichern Sie Ihre Daten aus Cloud-nativen Applikationen](#)" Und die Abschnitte zu Oracle und Azure NetApp Files.
- Sehen Sie sich das folgende Video an

[Video der Bereitstellung von Oracle und ANF](#)

Voraussetzungen für die Bereitstellung des SnapCenter Services

Die Bereitstellung erfordert die folgenden Voraussetzungen.

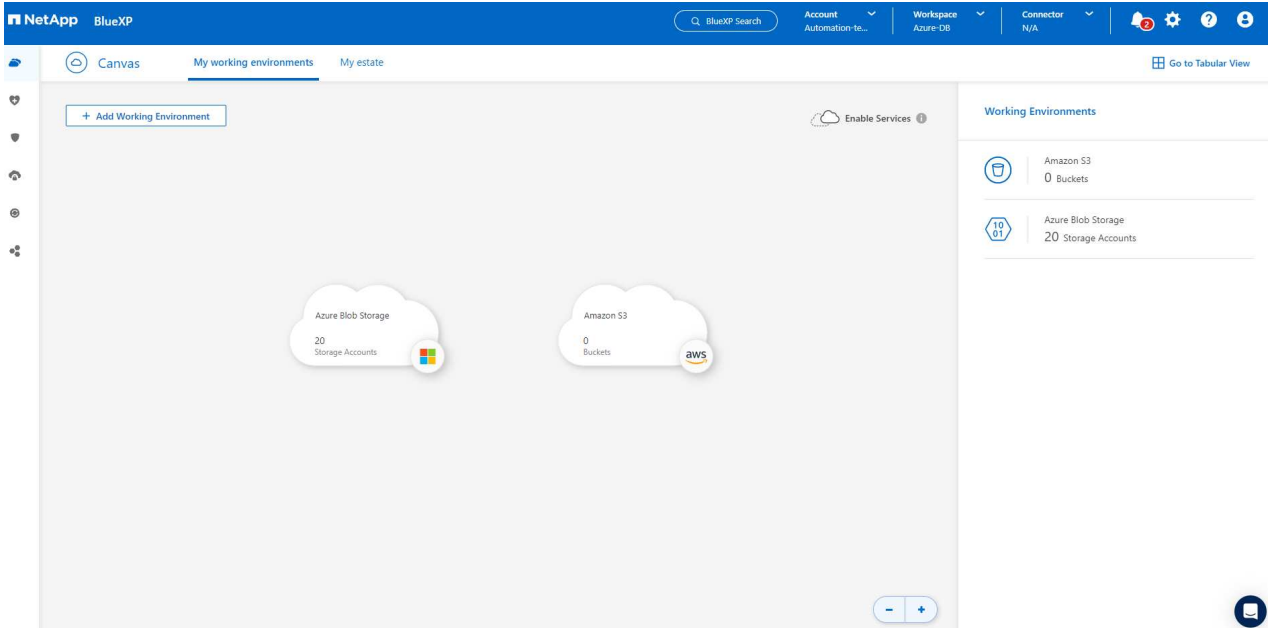
1. Ein primärer Oracle-Datenbankserver auf einer Azure VM-Instanz mit einer Oracle-Datenbank, die vollständig bereitgestellt ist und ausgeführt wird.
2. Ein in Azure bereitgestellter Azure NetApp Files-Storage-Service-Kapazitäts-Pool mit Kapazitäten zur Erfüllung der im Abschnitt „Hardwarekomponenten“ aufgeführten Anforderungen an Datenbank-Storage.
3. Ein sekundärer Datenbankserver auf einer Azure VM-Instanz, der zum Testen des Klonens einer Oracle-Datenbank auf einen alternativen Host verwendet werden kann, um einen Entwicklungs-/Test-Workload zu unterstützen, oder andere Anwendungsfälle, für die ein vollständiger Datensatz der Oracle-Produktionsdatenbank erforderlich ist.
4. Weitere Informationen zur Implementierung von Oracle-Datenbanken auf Azure NetApp Files- und Azure-Computing-Instanzen finden Sie unter "[Implementierung und Schutz von Oracle Datenbanken auf Azure NetApp Files](#)".

Onboarding bei der BlueXP Vorbereitung

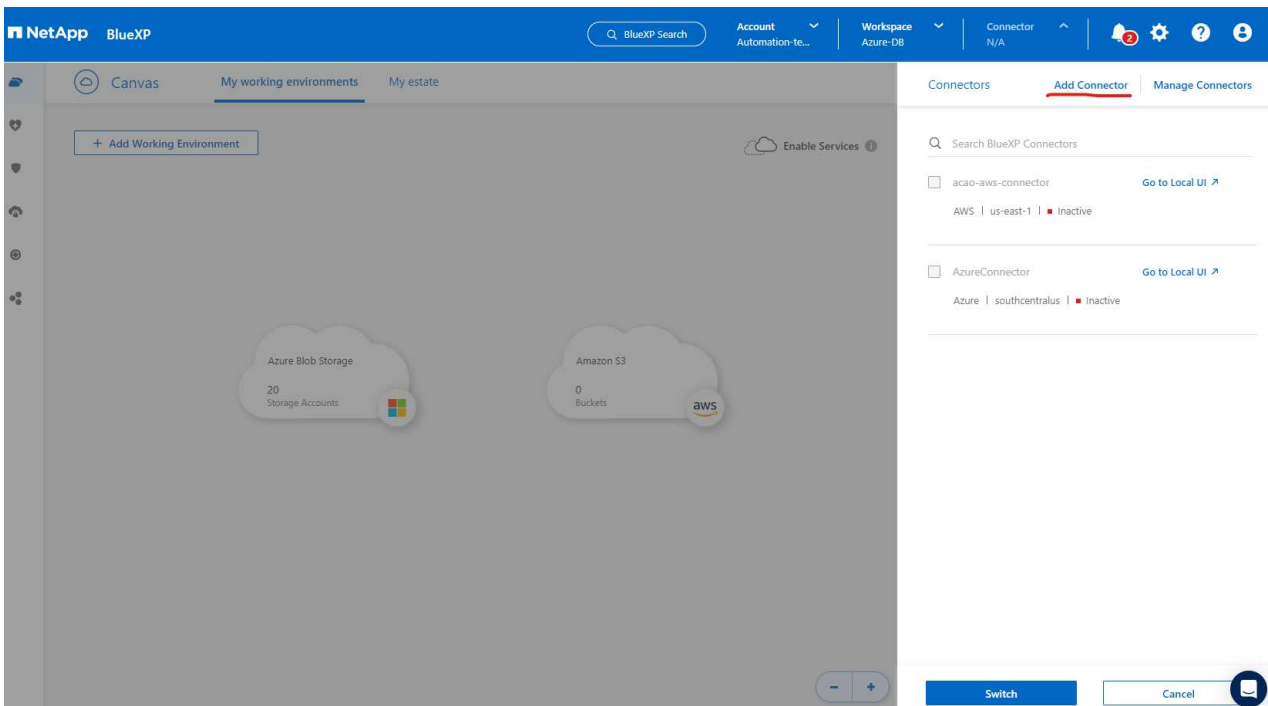
1. Verwenden Sie den Link "[NetApp BlueXP](#)" Um sich für den Konsolenzugriff von BlueXP zu registrieren.
2. Ein Azure-Benutzerkonto oder ein Active Directory-Dienstprinzip erstellen und mit Rolle im Azure-Portal Berechtigungen für die Azure-Connector-Implementierung erteilen.
3. Um BlueXP für das Management von Azure Ressourcen einzurichten, fügen Sie eine BlueXP Zugangsdaten mit Details zu einem Active Directory-Dienstprinzipal hinzu, die BlueXP zur Authentifizierung mit Azure Active Directory (App-Client-ID) verwenden kann, einem Client Secret für die Serviceprinzipalapplikation (Client Secret), und die Active Directory-ID für Ihre Organisation (Mandanten-ID).
4. Sie benötigen auch das virtuelle Azure Netzwerk, die Ressourcengruppe, die Sicherheitsgruppe, einen SSH-Schlüssel für den VM-Zugriff usw., die für die Connector-Bereitstellung und die Installation von Datenbank-Plug-ins bereit sind.

Stellen Sie einen Connector für SnapCenter-Services bereit

1. Melden Sie sich bei der BlueXP Konsole an.



2. Klicken Sie auf **Connector** Drop-down-Pfeil und **Add Connector**, um den Connector-Provisioning-Workflow zu starten.



3. Wählen Sie Ihren Cloud-Provider (in diesem Fall **Microsoft Azure**).

Provider

Choose the cloud provider where you want to run the BlueXP Connector:



[Deploy the Connector on your premises](#)

Continue



- Überspringen Sie die Schritte **permission**, **Authentication** und **Networking**, wenn Sie sie bereits in Ihrem Azure-Konto eingerichtet haben. Wenn nicht, müssen Sie diese konfigurieren, bevor Sie fortfahren. Von hier aus können Sie auch die Berechtigungen für die Azure-Richtlinie abrufen, auf die im vorherigen Abschnitt „[Onboarding bei der BlueXP Vorbereitung](#).“

Deploying a BlueXP Connector

The BlueXP Connector is a crucial component for the day-to-day use of BlueXP.

It's used to connect BlueXP's services to your hybrid-cloud environments.

The BlueXP Connector can then manage the resources and processes within your public cloud environment.

Before you begin the deployment process, ensure that you have completed the required preparations. This guide will enable you to focus on the minimum requirements for BlueXP Connector installation.

Permissions

Ensure that the Azure user or service principal you've provided has sufficient permissions

Authentication

Choose between two methods: an [Azure user account](#) or an [Active Directory service principal](#)

Networking

Ensure that you have details on the VNet and subnet in which the BlueXP Connector will reside

[Skip to Deployment](#)

[Previous](#)

[Continue](#)



5. Klicken Sie auf **Skip to Deployment**, um Ihren Connector zu konfigurieren **Virtual Machine Authentication**. Fügen Sie das SSH-Schlüsselpaar, das Sie während des Onboarding in der Azure-Ressourcengruppe erstellt haben, zu BlueXP hinzu, um die Connector-OS-Authentifizierung vorzubereiten.

1 VM Authentication 2 Details 3 Network 4 Security Group 5 Review

Virtual Machine Authentication

You are logged in with Azure user: [acao@netapp.com](#) | Tenant: Hybrid Cloud TME

Subscription

Hybrid Cloud TME Onprem

Location

South Central US

Resource Group

Create New Use Existing

Resource Group

ANFAVSRG

Authentication Method

Password Public Key

User Name

azureuser

Enter SSH Public Key

-----BEGIN RSA PRIVATE KEY----- MIIGSAIBAAKCA...

Previous

Next



6. Geben Sie einen Namen für die Connector-Instanz ein, wählen Sie unter **Details Create** und akzeptieren Sie den Standard **role Name**, und wählen Sie das Abonnement für das Azure-Konto aus.

✓ VM Authentication 2 Details 3 Network 4 Security Group 5 Review

Details

Connector Instance Name ?

AzureConnector

Connector Role

Create Attach existing Manual

Role Name

BlueXP Operator-5519248

Subscriptions to apply with the role

Hybrid Cloud TME Onprem ▼

+ Add Tags to Connector Instance

Previous

Next

7. Konfigurieren Sie das Netzwerk mit dem richtigen **vnet**, **Subnetz**, und deaktivieren Sie **Public IP**, stellen Sie jedoch sicher, dass der Connector den Internetzugang in Ihrer Azure-Umgebung hat.

✓ VM Authentication ✓ Details 3 Network 4 Security Group 5 Review

Network

Connectivity

VNet

ANFAVSVal ▼

Subnet

VM_Sub ▼

Public IP

Disable ▼

Proxy Configuration (Optional)

HTTP Proxy

Example: http://172.16.254.1:8080

Define Credentials for this Proxy ▼

Upload a root certificate ▼

Notice: Ensure that the subnet has internet connectivity through a NAT device or proxy server so that the Connector can communicate with Azure services.

Previous

Next

8. Konfigurieren Sie die **Sicherheitsgruppe** für den Konnektor, der HTTP-, HTTPS- und SSH-Zugriff zulässt.

The screenshot shows the 'Add BlueXP Connector - Azure' wizard in the 'Security Group' step. The breadcrumb trail at the top indicates the progress: VM Authentication, Details, Network, Security Group (current step), and Review. A 'More Information' link is visible in the top right corner. Below the breadcrumb, a message states: 'The security group must allow inbound HTTP, HTTPS and SSH access.' The main configuration area is titled 'Assign a security group:' and has two radio buttons: 'Create a new security group' (selected) and 'Select an existing security group'. Below this, there are three columns for configuring inbound rules for HTTP (Port 80), HTTPS (Port 443), and SSH (Port 22). Each column contains a 'Source Type' dropdown menu set to 'Anywhere' and a 'Source (CIDR)' text input field containing '0.0.0.0/0'. At the bottom of the wizard, there are 'Previous' and 'Next' buttons, and a help icon in the bottom right corner.

9. Überprüfen Sie die Übersichtsseite, und klicken Sie auf **Hinzufügen**, um die Verbindungserstellung zu starten. Die Implementierung dauert in der Regel etwa 10 Minuten. Sobald dieser Vorgang abgeschlossen ist, wird die VM der Connector-Instanz im Azure-Portal angezeigt.

✓ VM Authentication ✓ Details ✓ Network ✓ Security Group **5** Review

Review

[Code for Terraform Automation](#)

BlueXP Connector Name	AzureConnector
Subscription	Hybrid Cloud TME Onprem
Location	South Central US
Resource Group	Existing - ANFAVSRG
Role	New - BlueXP Operator-5519248
Authentication Method	Password (user: azureuser)
VNet	ANFAVSV1
Subnet	VM_Sub
Public IP	Enable
Proxy	None
Security Group	HTTP: 0.0.0.0/0, HTTPS: 0.0.0.0/0, SSH: 0.0.0.0/0

Previous

Add

10. Nachdem der Connector bereitgestellt wurde, erscheint der neu erstellte Connector unter **Connector** Drop-down.

NetApp BlueXP

Account Automation-te... Workspace Azure-DB Connector AzureConnector

Canvas My working environments My estate Go to Tabular View

+ Add Working Environment Enable Services ⓘ

Azure Blob Storage
20 Storage Accounts

Amazon S3
0 Buckets

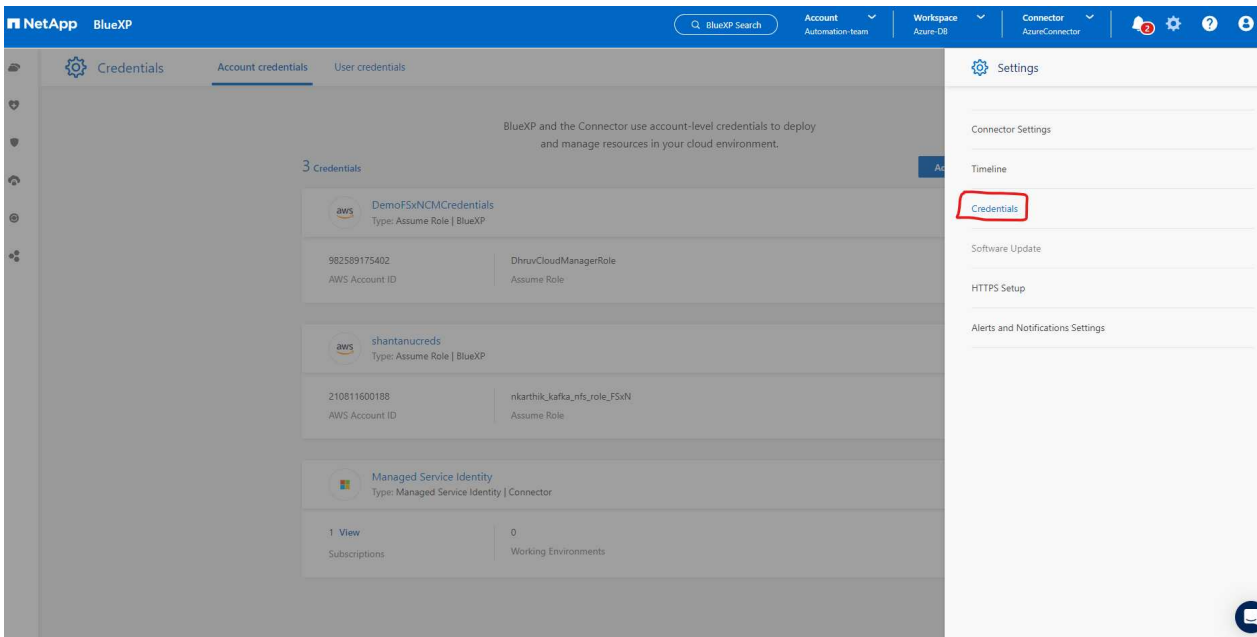
Working Environments

Amazon S3
0 Buckets

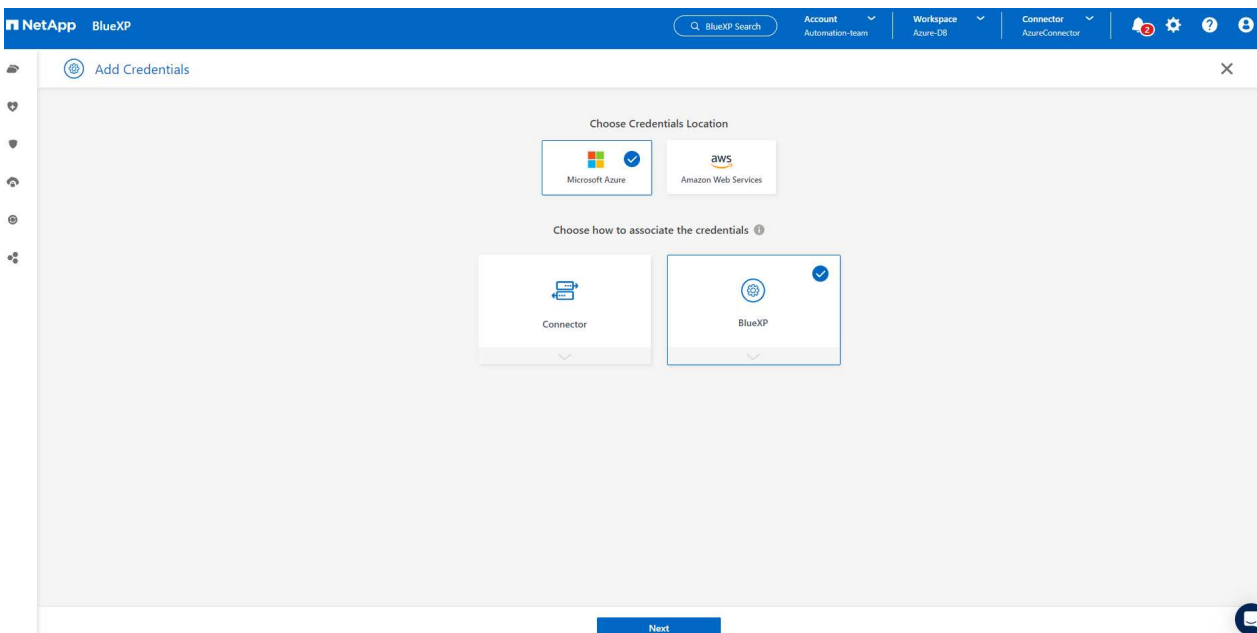
Azure Blob Storage
20 Storage Accounts

Zugangsdaten für Azure Ressourcenzugriff in BlueXP definieren

1. Klicken Sie auf das Einstellungssymbol in der oberen rechten Ecke der BlueXP-Konsole, um die Seite **Account Credentials** zu öffnen, klicken Sie auf **Add Credentials**, um den Workflow für die Anmeldedatenkonfiguration zu starten.



2. Wählen Sie den Anmeldeinformationsspeicherort als **- Microsoft Azure - BlueXP**.



3. Definieren Sie Azure-Anmeldeinformationen mit den richtigen **Client Secret**, **Client-ID** und **Tenant-ID**, die während des vorherigen BlueXP Onboarding-Prozesses gesammelt werden sollten.

NetApp BlueXP

Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector

Add Credentials Credentials Type Define Credentials Marketplace Subscription Review

Define Microsoft Azure Credentials

Learn more about Azure application credentials

Credentials Name: Azure_Hybrid_TME Client Secret:

Application (client) ID: 2fbc9be5-a259-4539-bb57-036b176f5c... Directory (tenant) ID: 9bb0aab6-5c98-419b-9cfd-7a38bd496...

I have verified that the Azure role assigned to the Active Directory service principal matches BlueXP policy requirements.

Previous Next

4. Bewertung und Hinzufügen.

NetApp BlueXP

Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector

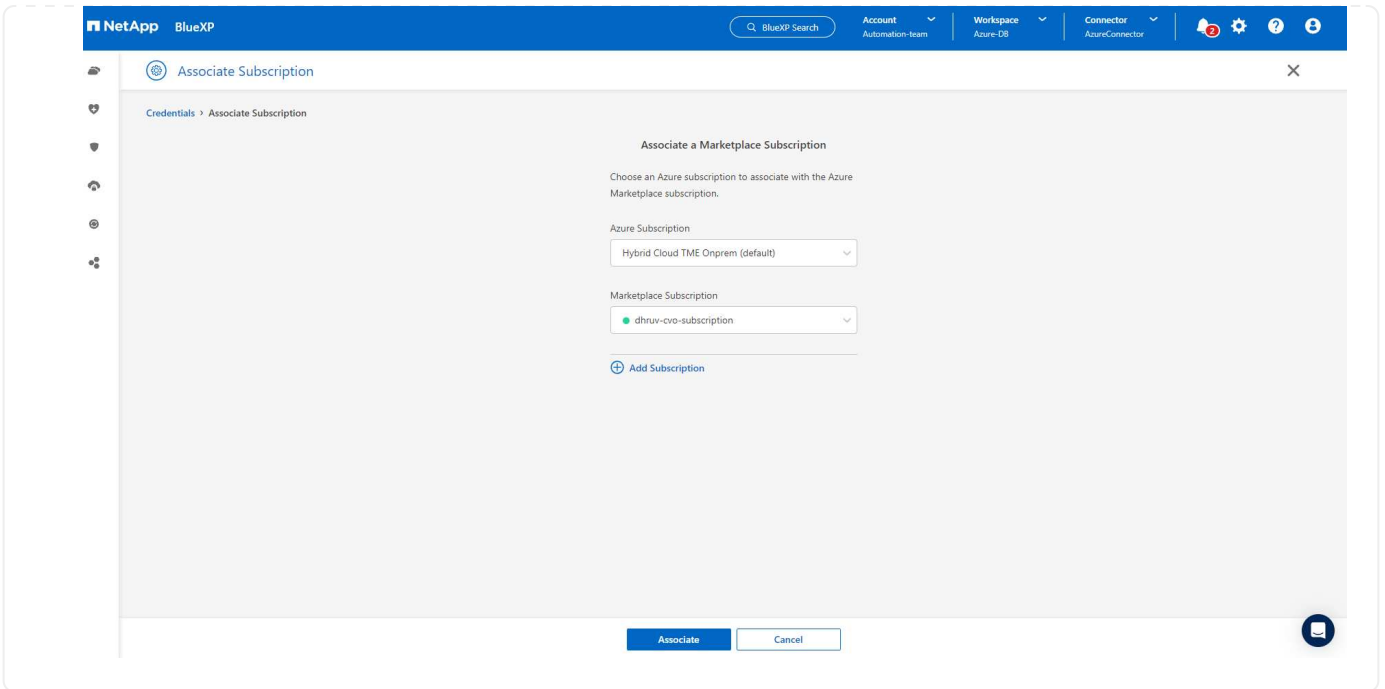
Add Credentials Credentials Type Define Credentials Review

Review

Credentials Type	Azure
Credentials Name	Azure_Hybrid_TME
Credential Storage	Cloud Manager
Application (client) ID	2fbc9be5-a259-4539-bb57-036b176f5cc7
Directory (tenant) ID	9bb0aab6-5c98-419b-9cfd-7a38bd496e1f

Previous Add

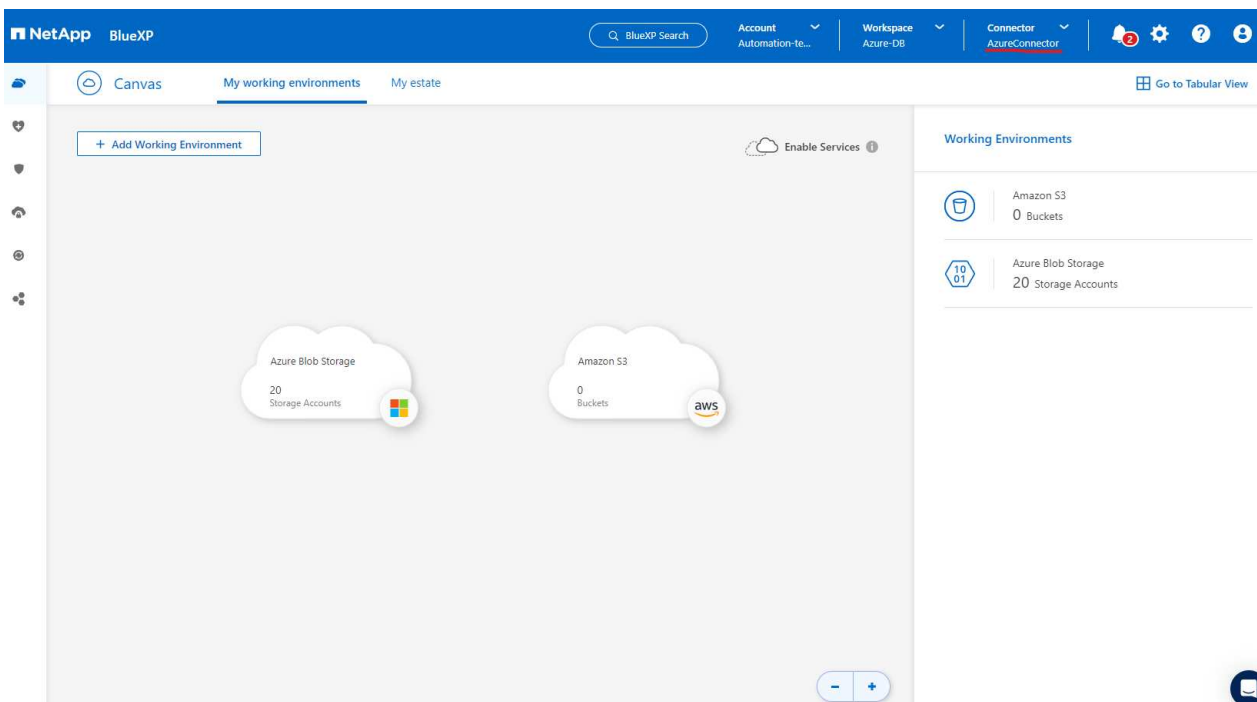
5. Möglicherweise müssen Sie auch ein **Marketplace-Abonnement** mit den Zugangsdaten verknüpfen.



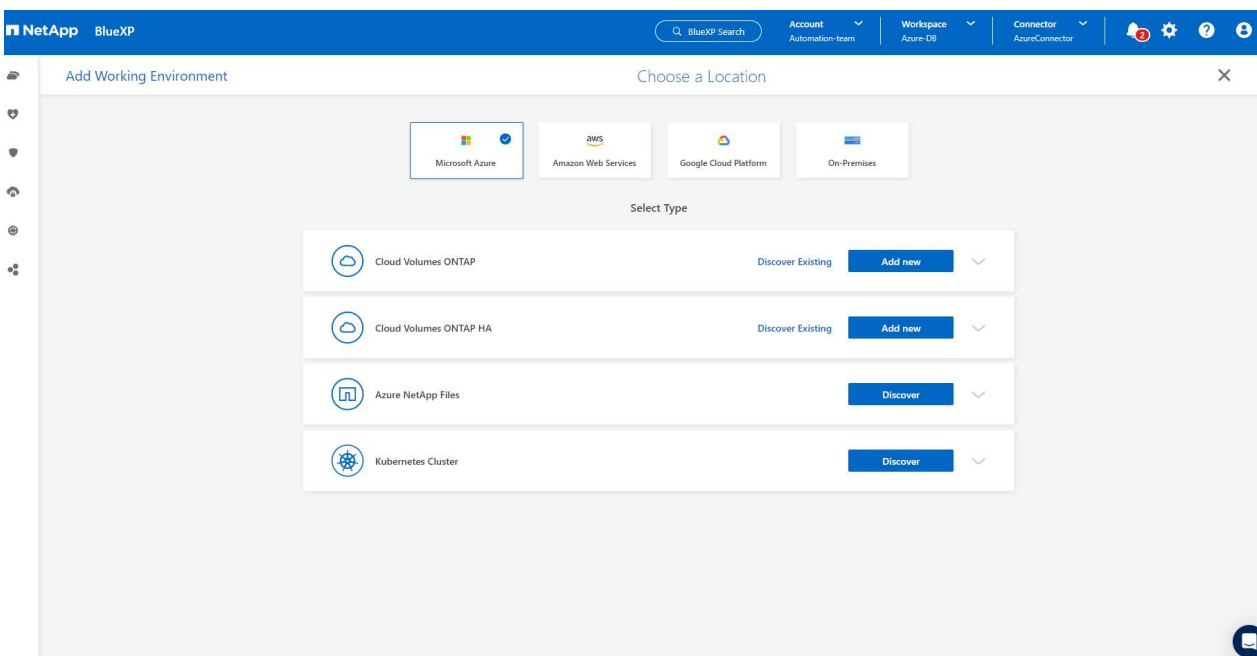
Einrichtung der SnapCenter Services

Wenn die Azure-Zugangsdaten konfiguriert sind, können SnapCenter-Services jetzt wie folgt eingerichtet werden:

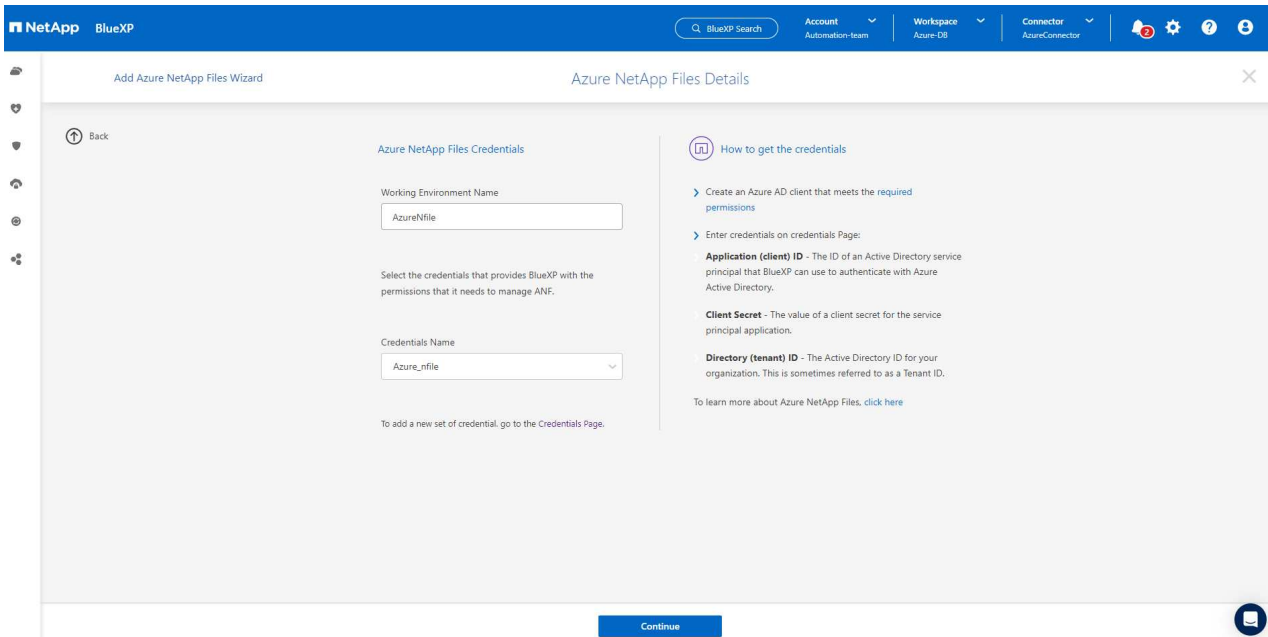
1. Zurück zur Bildschirmseite, von **Meine Arbeitsumgebung** Klicken Sie auf **Arbeitsumgebung hinzufügen**, um Azure NetApp Files in Azure zu entdecken.



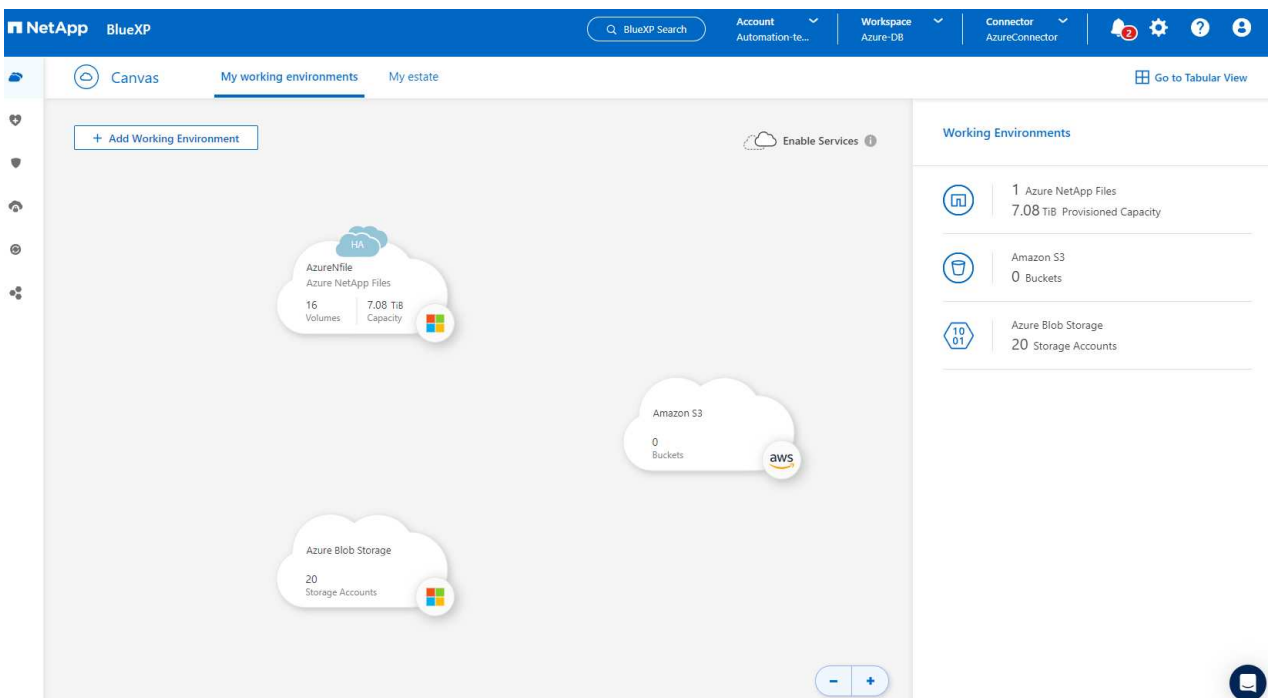
2. Wählen Sie **Microsoft Azure** als Speicherort und klicken Sie auf **Discover**.



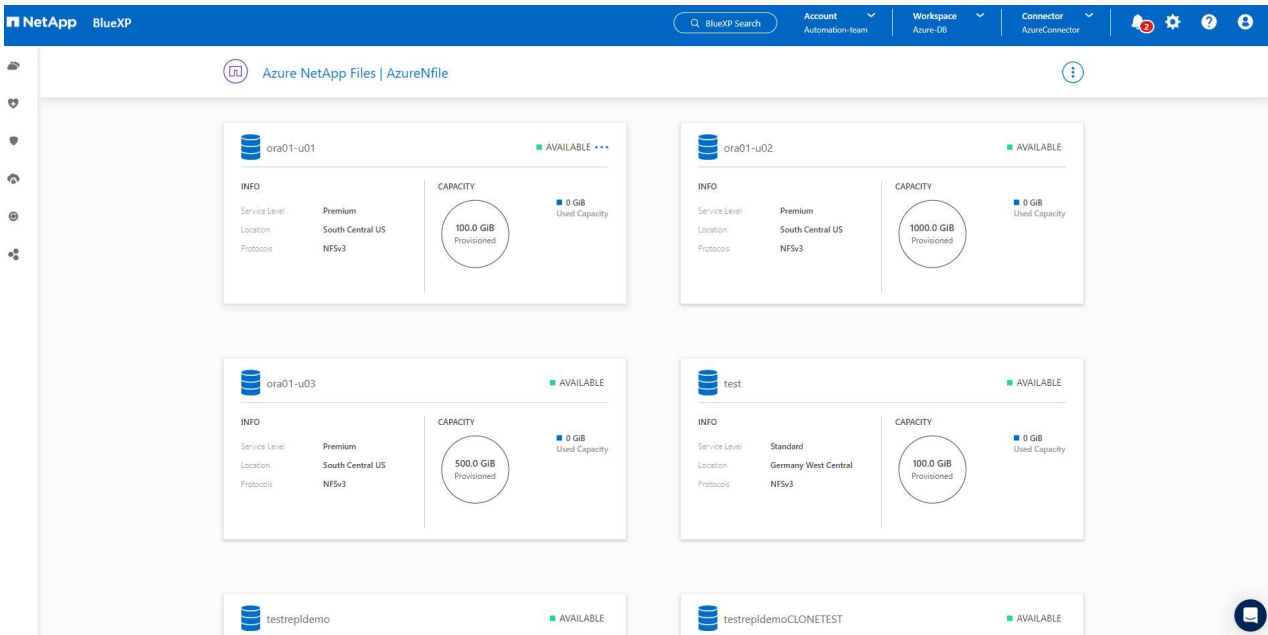
3. Name **Arbeitsumgebung** und wählen Sie **Credential Name** erstellt im vorherigen Abschnitt, und klicken Sie auf **Weiter**.



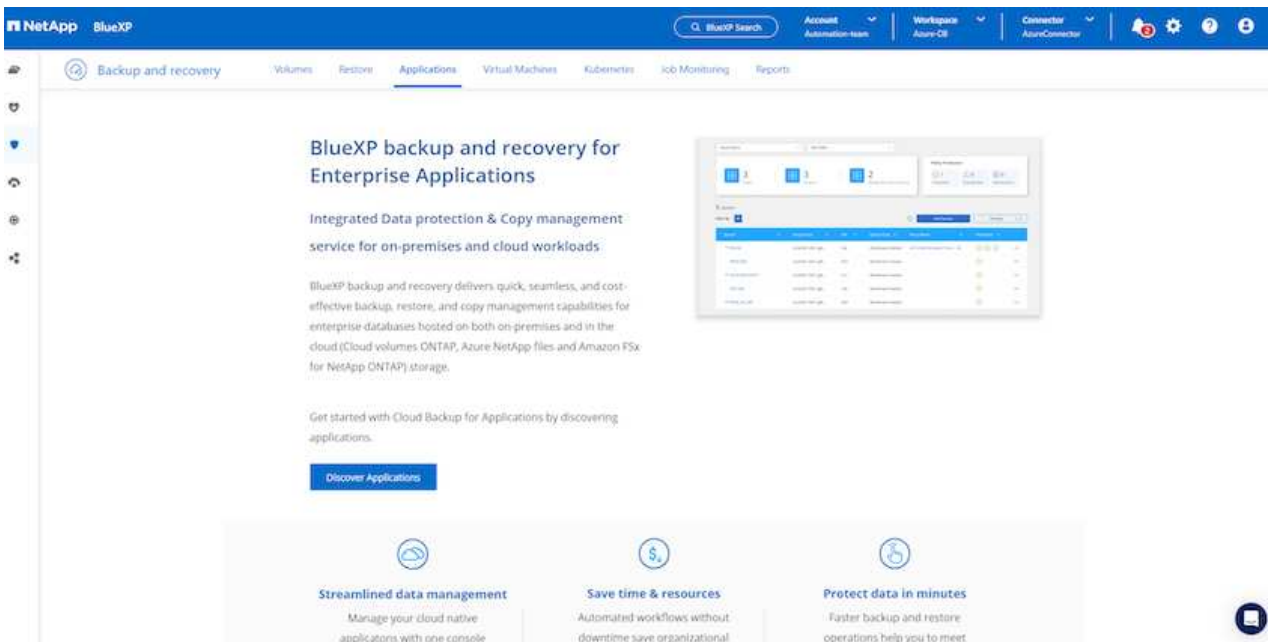
4. BlueXP-Konsole kehrt zu **Meine Arbeitsumgebungen** zurück und entdeckte Azure NetApp Files aus Azure erscheint jetzt auf **Leinwand**.



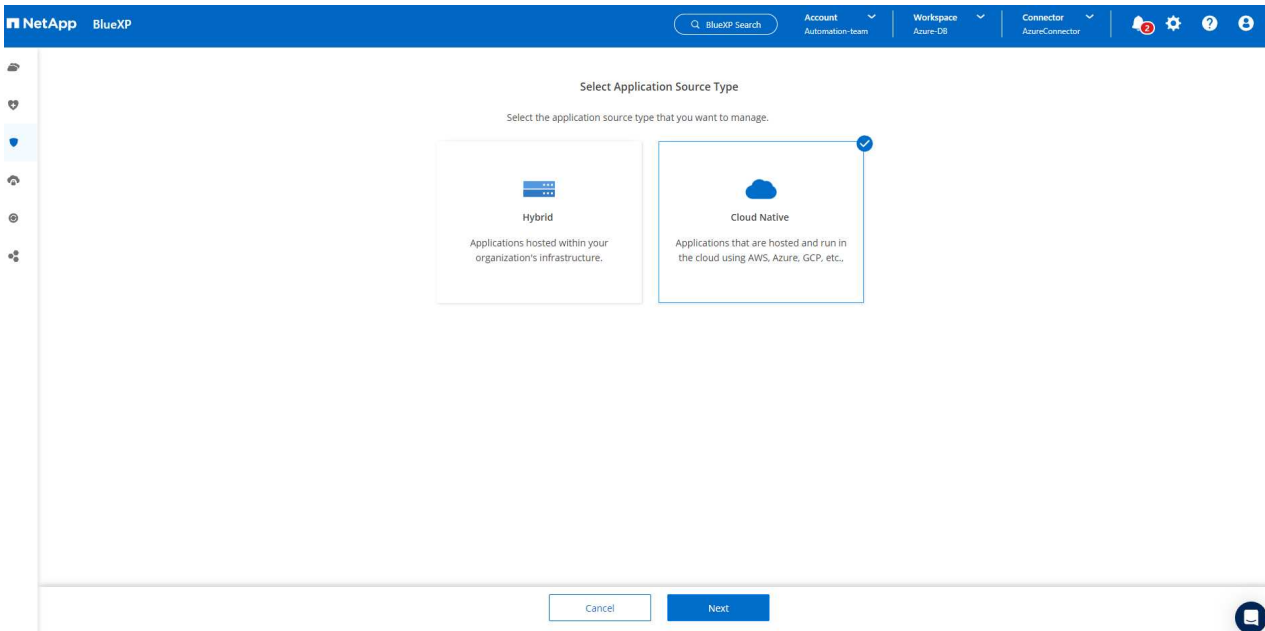
5. Klicken Sie auf das Symbol **Azure NetApp Files** und dann auf **Arbeitsumgebung eingeben**, um die im Azure NetApp Files-Speicher bereitgestellten Oracle-Datenbank-Volumes anzuzeigen.



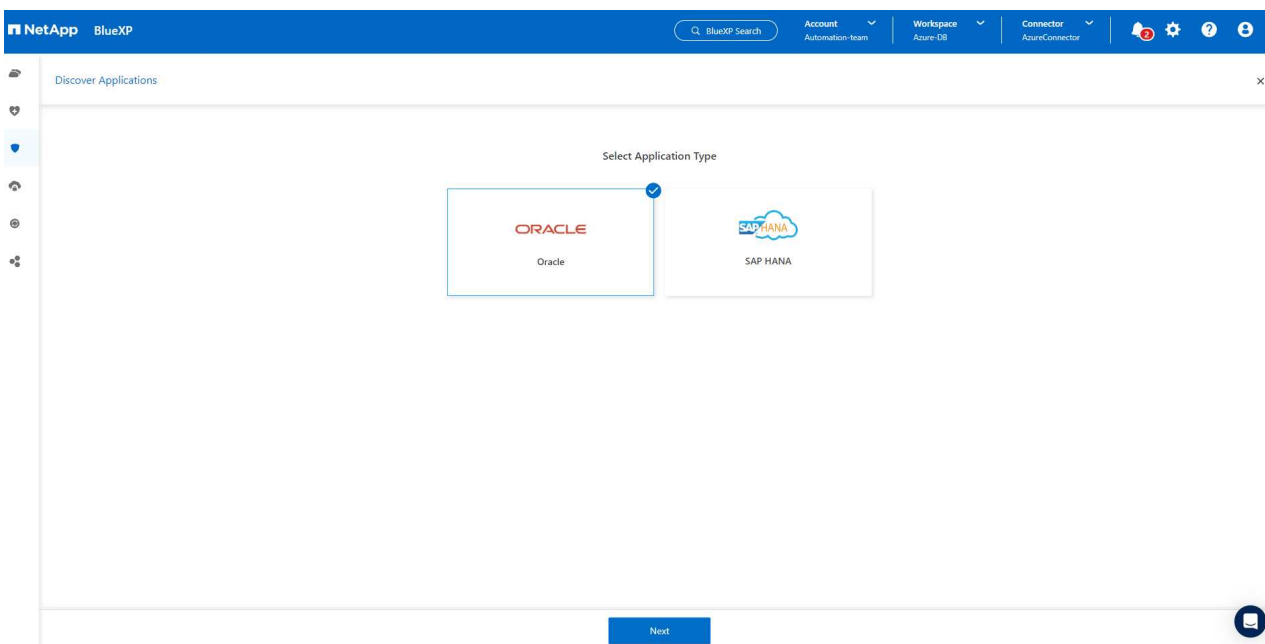
6. Bewegen Sie in der linken Seitenleiste der Konsole Ihre Maus über das Schutzsymbol und klicken Sie dann auf **Schutz > Anwendungen**, um die Startseite der Anwendungen zu öffnen. Klicken Sie Auf **Anwendungen Entdecken**.



7. Wählen Sie **Cloud Native** als Quelltyp der Anwendung aus.



8. Wählen Sie **Oracle** für den Anwendungstyp klicken Sie auf **Weiter**, um die Seite mit den Hostdetails zu öffnen.



9. Wählen Sie **using SSH** aus und geben Sie die Oracle Azure VM-Details wie **IP-Adresse**, **Connector**, Azure VM Management **Username** wie azureuser an. Klicken Sie auf **Add SSH Private Key**, um das SSH-Schlüsselpaar, das Sie zur Bereitstellung der Oracle Azure VM verwendet haben, einzufügen. Sie werden außerdem aufgefordert, den Fingerabdruck zu bestätigen.

NetApp BlueXP

Discover Applications

Host Details Configuration Review

Select host type

Provide the following details to add host and discover applications

Host Installation Type Manual Using SSH

Host FQDN or IP: 172.30.137.142

Connector: AzureConnector

Username: azureuser

SSH Port: 22

Plug-in Port: 8145

Previous Next

Discover Applications

Host Details Configuration Review

Select host type

Provide the following details to add host and discover applications

Host Installation Type Manual Using SSH

Validate fingerprint

Algorithm: ssh-rsa

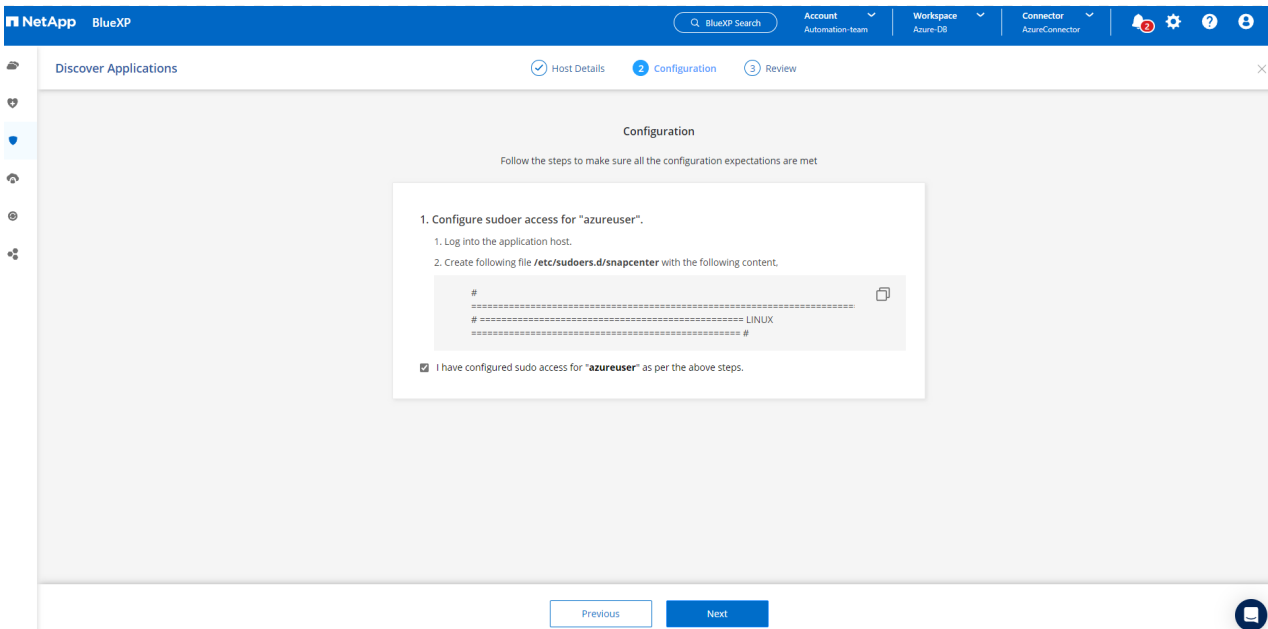
Fingerprint: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAAB...

By proceeding further, I confirm that the above fingerprint for host is valid.

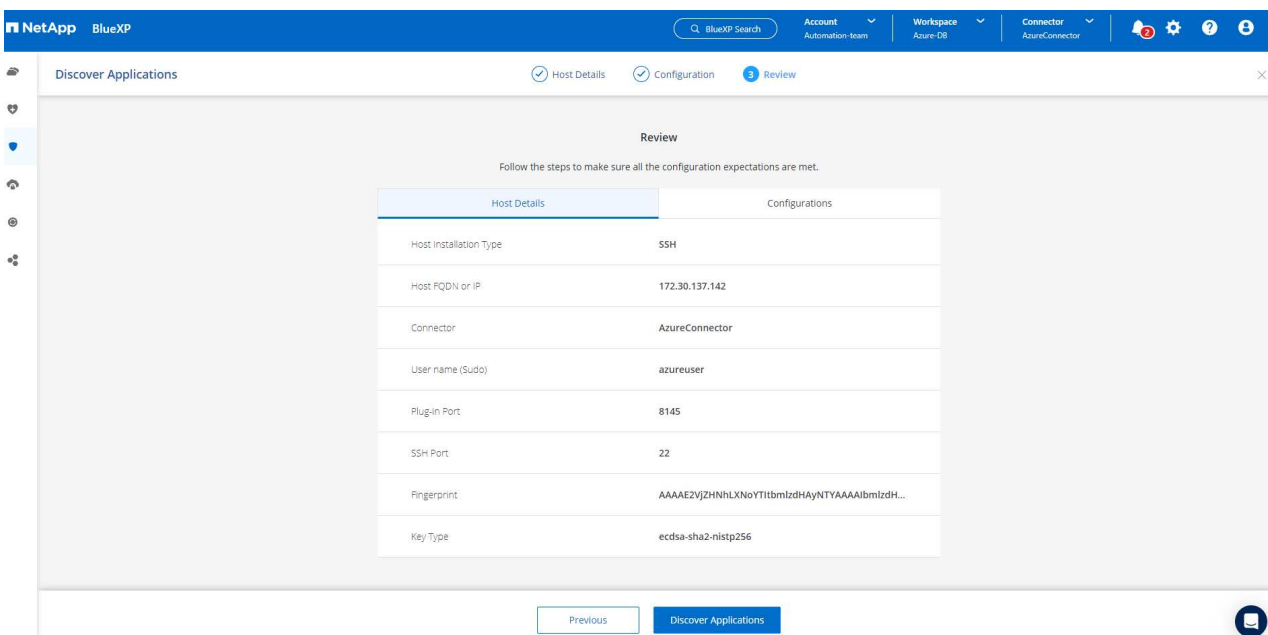
Proceed Cancel

Previous Next

10. Fahren Sie mit der nächsten Seite **Konfiguration** fort, um den sudoer-Zugriff auf Oracle Azure VM einzurichten.



11. Überprüfen und klicken Sie auf **Anwendungen entdecken**, um ein Plugin auf der Oracle Azure VM zu installieren und Oracle-Datenbank auf der VM in einem Schritt zu entdecken.



12. Entdeckte Oracle-Datenbanken auf Azure VM werden zu **Applications** hinzugefügt, und auf der Seite **Applications** wird die Anzahl der Hosts und Oracle-Datenbanken innerhalb der Umgebung aufgelistet. Die Datenbank **Schutzstatus** wird zunächst als **ungeschützt** angezeigt.

The screenshot shows the NetApp BlueXP interface for Oracle database protection. At the top, there are navigation tabs for 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. The 'Applications' tab is active. Below the navigation, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows 3 Hosts, 3 ORACLE, and 0 Clones. An 'Application Protection' summary shows 0 Protected and 3 Unprotected. Below this is a table of databases with 3 entries, all marked as 'Unprotected'.

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1st	172.30.15.124		Unprotected

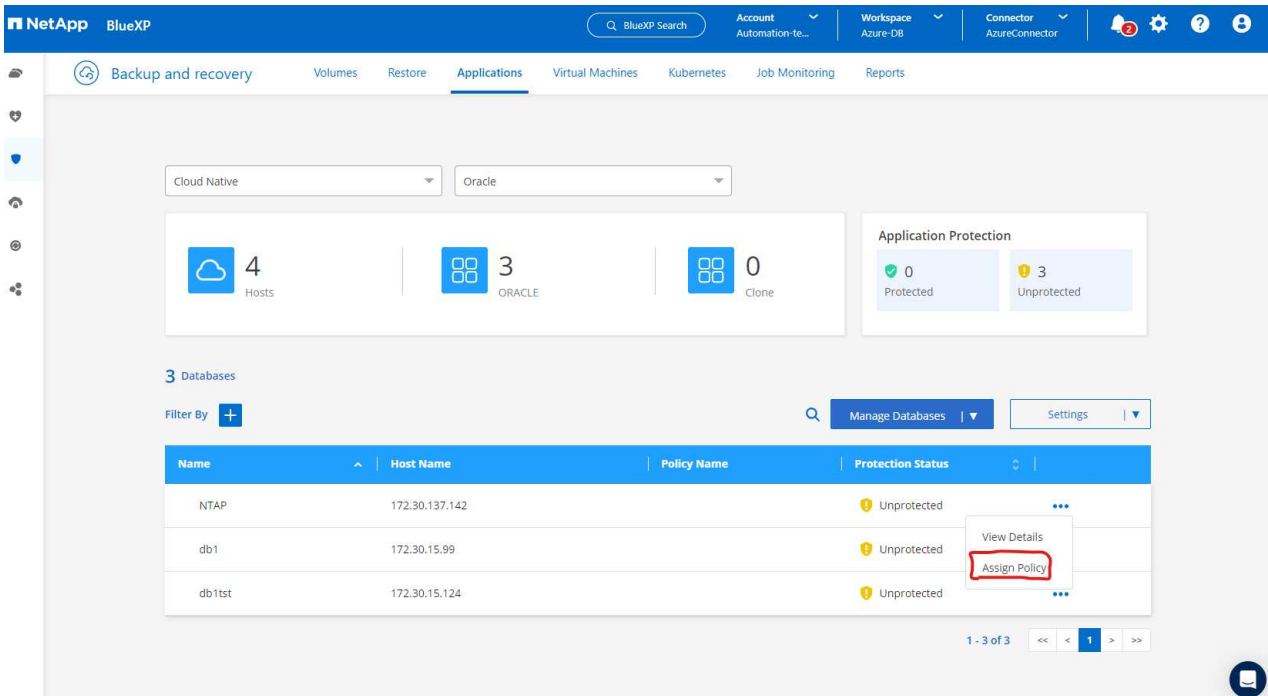
Damit ist die Ersteinrichtung der SnapCenter Services für Oracle abgeschlossen. In den nächsten drei Abschnitten dieses Dokuments werden die Backup-, Restore- und Klonvorgänge für Oracle-Datenbanken beschrieben.

Backup von Oracle Datenbanken

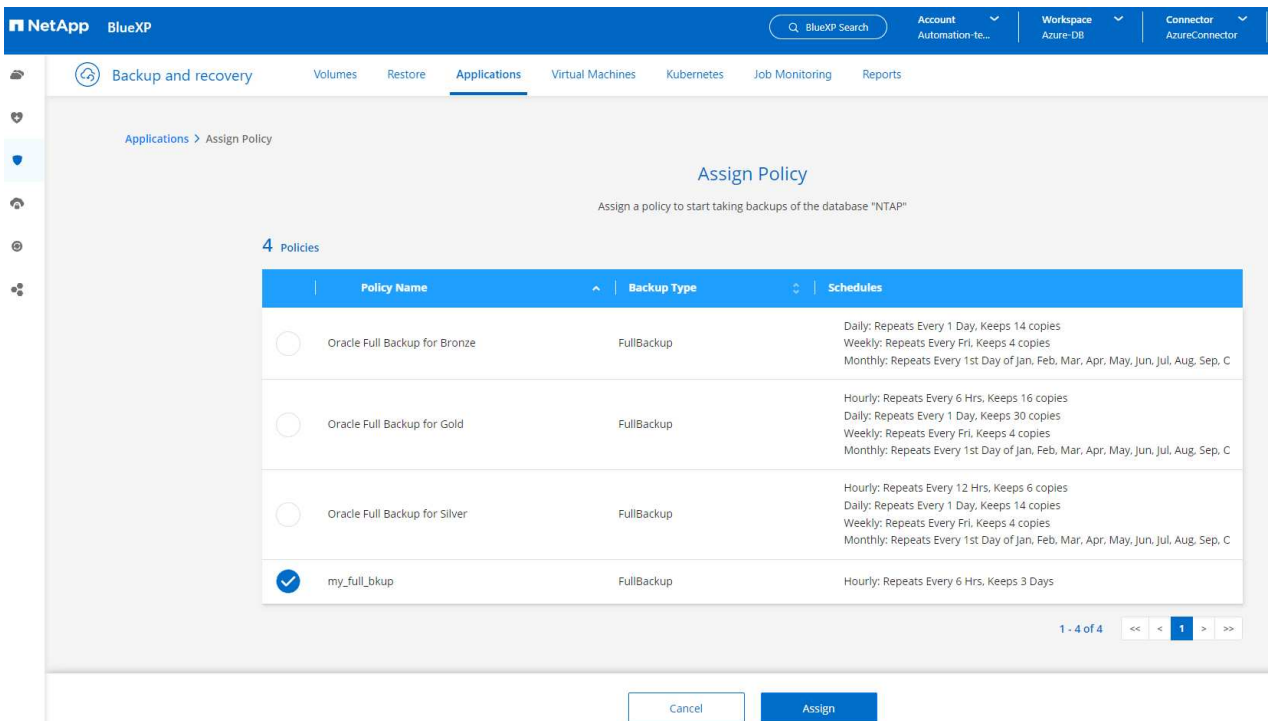
1. Unsere Test-Oracle-Datenbank in Azure VM ist mit drei Volumen mit einem aggregierten Gesamtspeicher über 1.6 tib konfiguriert. Dies gibt den Kontext über das Timing für die Snapshot-Sicherung, Wiederherstellung und den Klon einer Datenbank dieser Größe.

```
[oracle@acao-ora01 ~]$ df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  7.9G         0  7.9G   0% /dev
tmpfs                      7.9G         0  7.9G   0% /dev/shm
tmpfs                      7.9G      17M   7.9G   1% /run
tmpfs                      7.9G         0  7.9G   0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv  40G       23G   15G   62% /
/dev/mapper/rootvg-usrlv   9.8G      1.6G   7.7G  18% /usr
/dev/sda2                  496M      115M   381M  24% /boot
/dev/mapper/rootvg-varlv   7.9G      787M   6.7G  11% /var
/dev/mapper/rootvg-homelv  976M      323M   586M  36% /home
/dev/mapper/rootvg-optlv   2.0G       9.6M   1.8G   1% /opt
/dev/mapper/rootvg-tmplv   2.0G       22M   1.8G   2% /tmp
/dev/sda1                   500M       6.8M   493M   2% /boot/efi
172.30.136.68:/ora01-u01   100G       23G    78G   23% /u01
172.30.136.68:/ora01-u03   500G      117G   384G  24% /u03
172.30.136.68:/ora01-u02  1000G     804G   197G  81% /u02
tmpfs                      1.6G         0  1.6G   0% /run/user/1000
[oracle@acao-ora01 ~]$
```

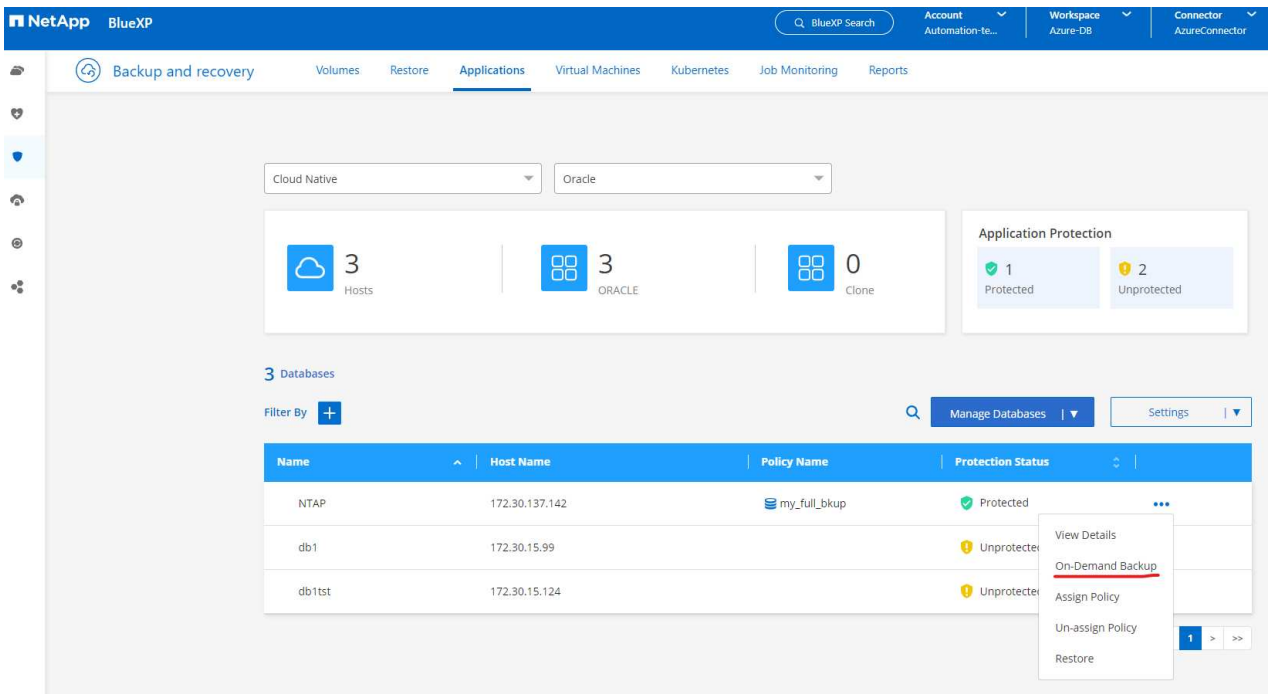
1. Um die Datenbank zu schützen, klicken Sie auf die drei Punkte neben der Datenbank **Schutzstatus** und dann auf **Richtlinie zuweisen**, um die vorinstallierten oder benutzerdefinierten Datenbank-Schutzrichtlinien anzuzeigen, die auf Ihre Oracle-Datenbanken angewendet werden können. Unter **Settings - Policies** haben Sie die Möglichkeit, Ihre eigene Policy mit einer angepassten Sicherungshäufigkeit und einem Backup-Datenaufbewahrungsfenster zu erstellen.



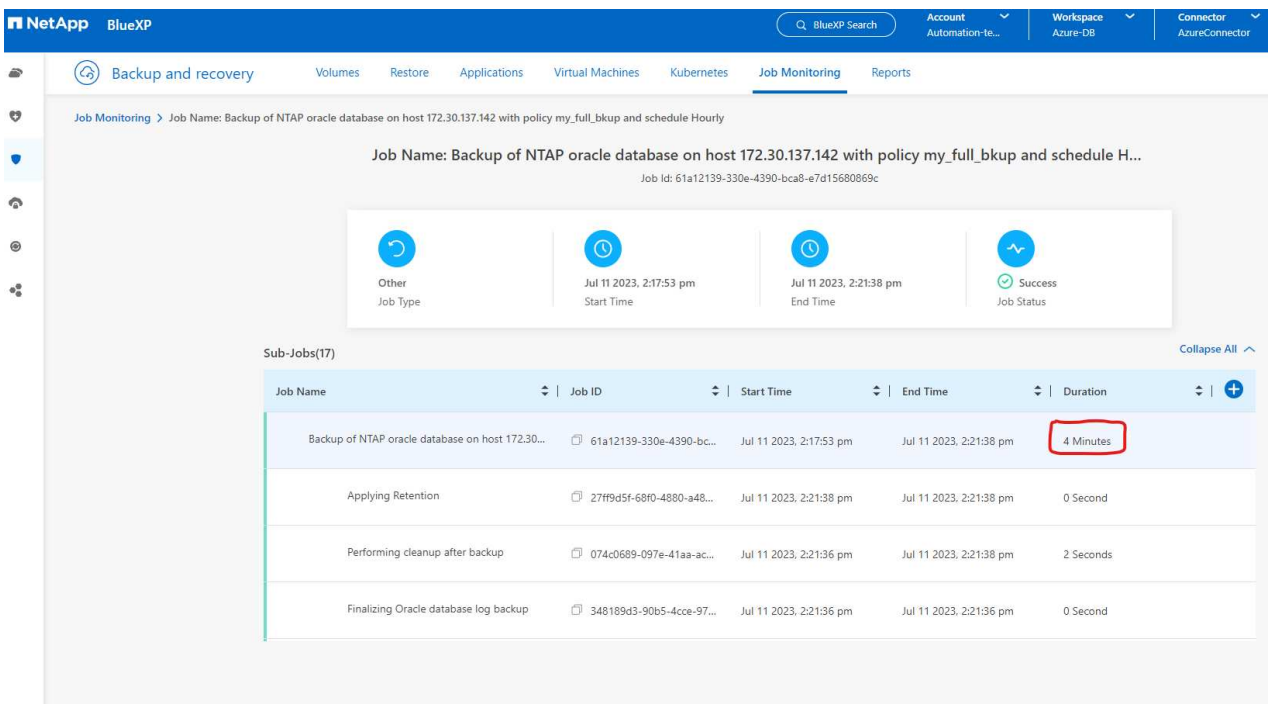
2. Wenn Sie mit der Richtlinienkonfiguration zufrieden sind, können Sie dann **Assign** Ihre Richtlinie Ihrer Wahl zuweisen, um die Datenbank zu schützen.



3. Nachdem die Richtlinie angewendet wurde, wurde der Datenbankschutzstatus mit einem grünen Häkchen in **protected** geändert. BlueXP führt das Snapshot Backup gemäß dem definierten Zeitplan aus. Darüber hinaus ist **ON-Demand Backup** über das drei-Punkt-Dropdown-Menü verfügbar, wie unten gezeigt.



4. Auf der Registerkarte **Job Monitoring** können die Details des Backup-Jobs angezeigt werden. Unsere Testergebnisse zeigten, dass das Backup einer Oracle Datenbank bei etwa 1.6 tib etwa 4 Minuten dauerte.



5. Im drei-Punkt-Dropdown-Menü **Details anzeigen** können Sie die aus Snapshot-Backups erstellten Backup-Sets anzeigen.

The screenshot shows the NetApp BlueXP interface for Applications. At the top, there are navigation tabs: Backup and recovery, Volumes, Restore, Applications (selected), Virtual Machines, Kubernetes, Job Monitoring, and Reports. Below the navigation, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows 4 Hosts, 3 ORACLE, and 0 Clones. An 'Application Protection' section indicates 2 Protected and 1 Unprotected databases. Below this is a table of databases with a context menu open over the 'db1tst' row.

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

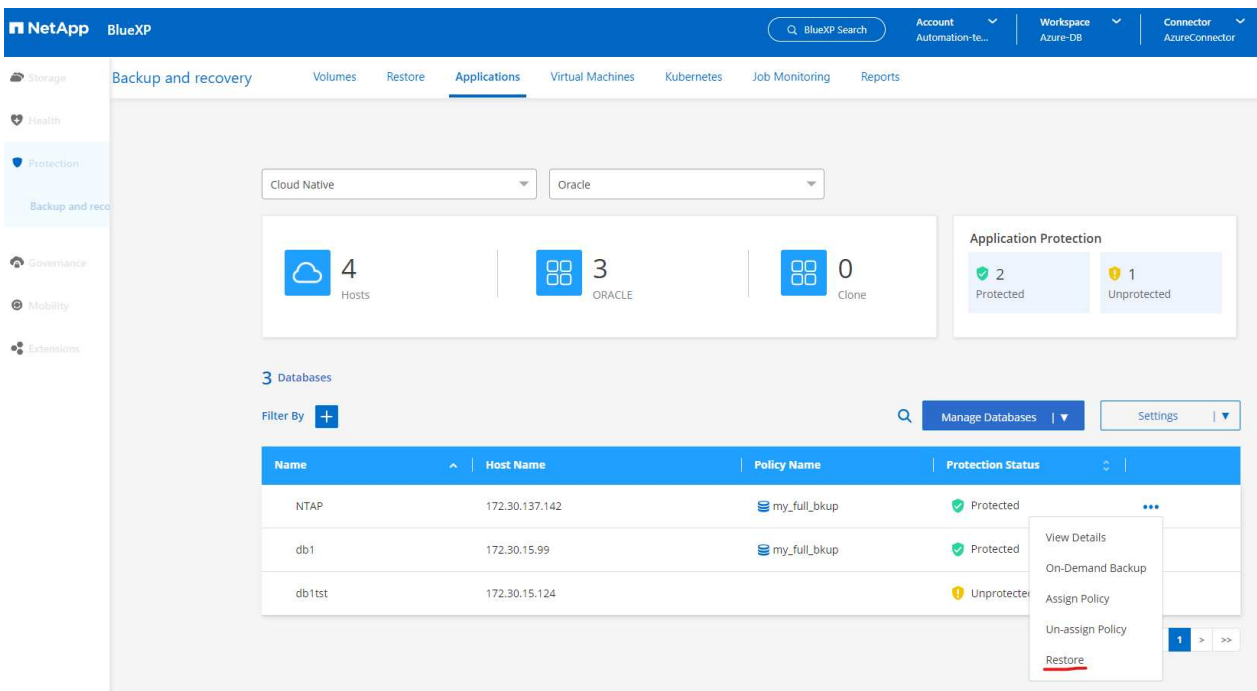
6. Zu den Details der Datenbanksicherung zählen **Backup-Name**, **Backup-Typ**, **SCN**, **RMAN-Katalog** und **Backup-Zeit**. Ein Backup-Satz enthält applikationskonsistente Snapshots für Daten-Volumen bzw. Protokoll-Volumen. Ein Snapshot eines Protokollvolumens erfolgt direkt nach einem Snapshot eines Datenbank-Datenvolumens. Sie können einen Filter anwenden, wenn Sie nach einem bestimmten Backup in der Sicherungsliste suchen.

The screenshot shows the 'Database Details' page for the 'NTAP' database. It displays various attributes such as Database Name, Host Name, Clones, Protection Status, Host Storage, Parent Database, Policy Names, Database Version, RMAN Catalog, Database Type, Connector Id, and RMAN catalog repository. Below this is a table of backups with columns for Backup Name, Backup Type, SCN, RMAN Catalog, Backup Time, and a Delete button.

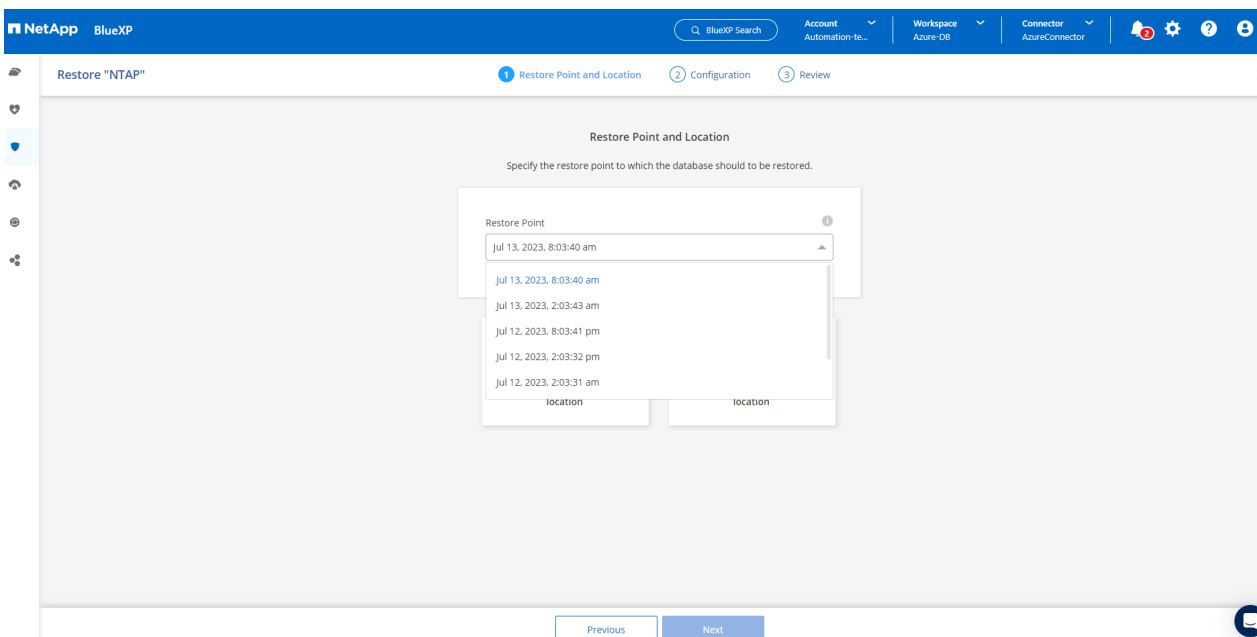
Backup Name	Backup Type	SCN	RMAN Catalog	Backup Time	
my_full_bkup_Hourly_NTAP_2023_07_13_12_04_28_8376...	Log	29192187	Not Cataloged	Jul 13, 2023, 8:06:22 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_4363...	Data	29192136	Not Cataloged	Jul 13, 2023, 8:03:40 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_04_28_5618...	Log	29178022	Not Cataloged	Jul 13, 2023, 2:05:50 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_03_03_6371...	Data	29177972	Not Cataloged	Jul 13, 2023, 2:03:43 am	Delete

Wiederherstellung und Recovery von Oracle-Datenbanken

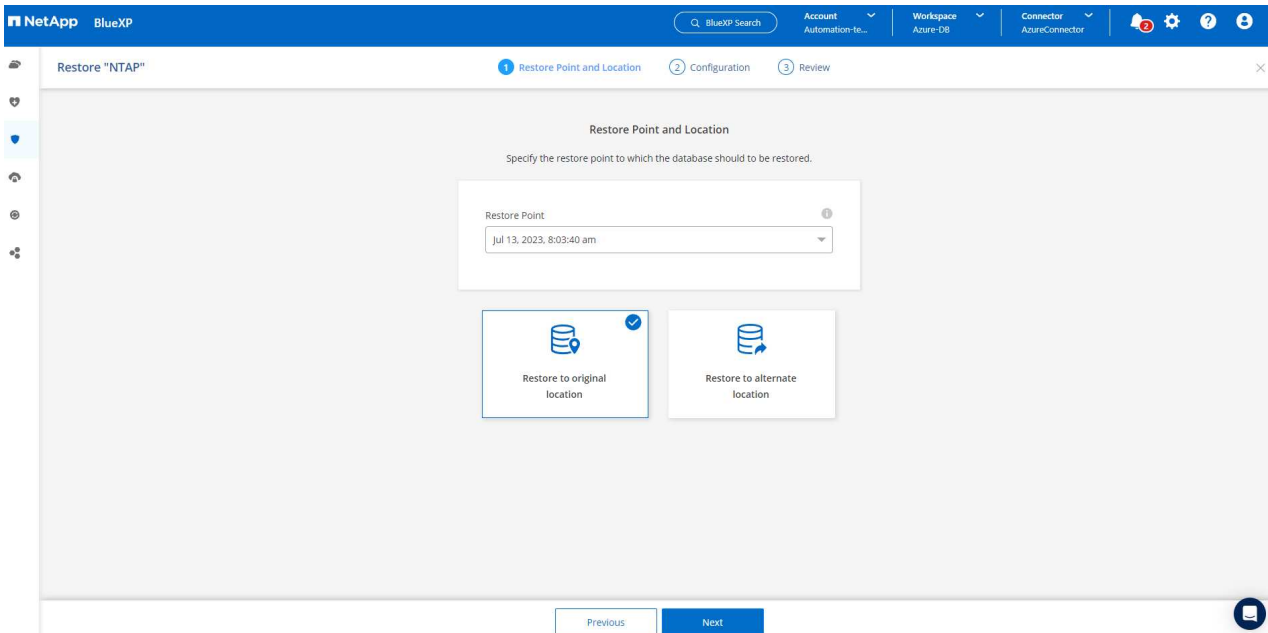
1. Für eine Datenbankwiederherstellung klicken Sie auf das drei-Punkt-Dropdown-Menü für die jeweilige Datenbank, die in **Anwendungen** wiederhergestellt werden soll, und klicken Sie dann auf **Wiederherstellen**, um den Datenbank-Wiederherstellungs- und Wiederherstellungsworkflow zu starten.



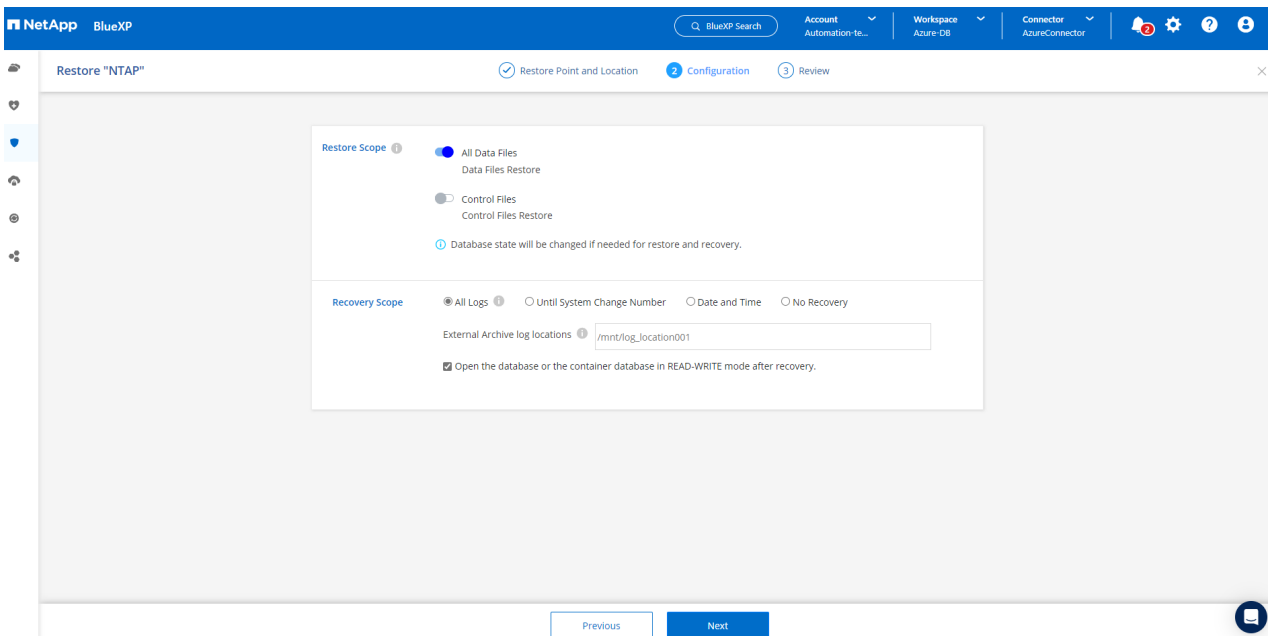
2. Wählen Sie Ihren **Wiederherstellungspunkt** nach Zeitstempel. Jeder Zeitstempel in der Liste stellt einen verfügbaren Datenbank-Backup-Satz dar.



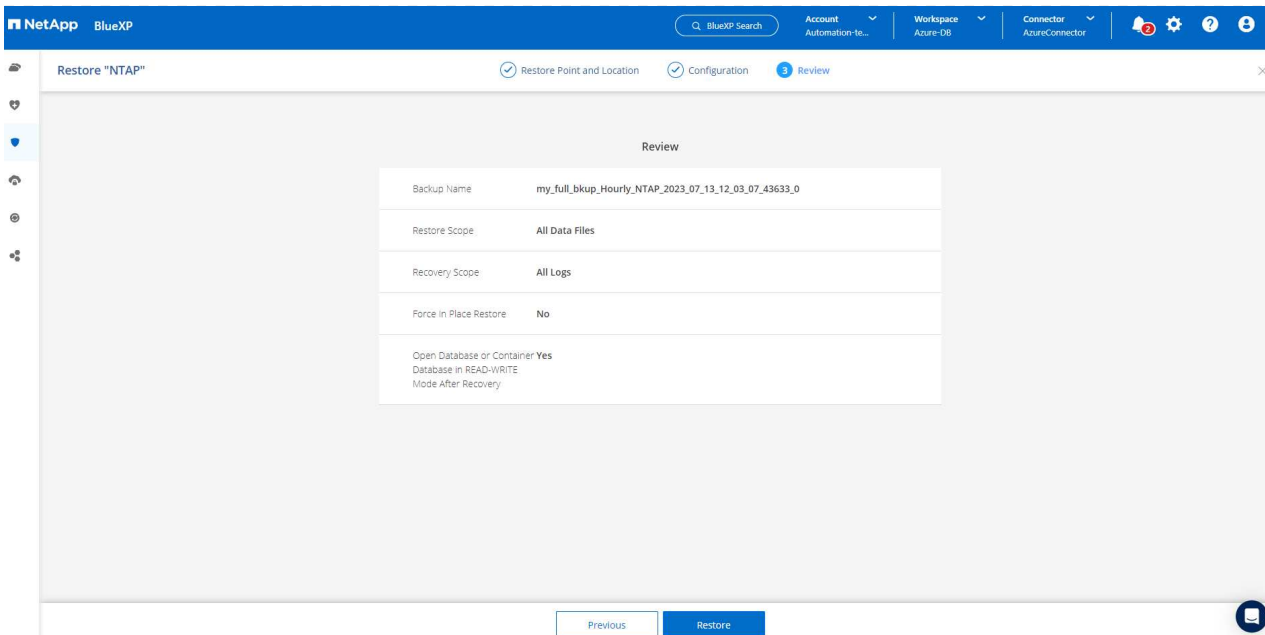
3. Wählen Sie Ihren **Speicherort** für die **Wiederherstellung** und **Wiederherstellung einer Oracle-Datenbank an *ursprünglichem Speicherort** aus.



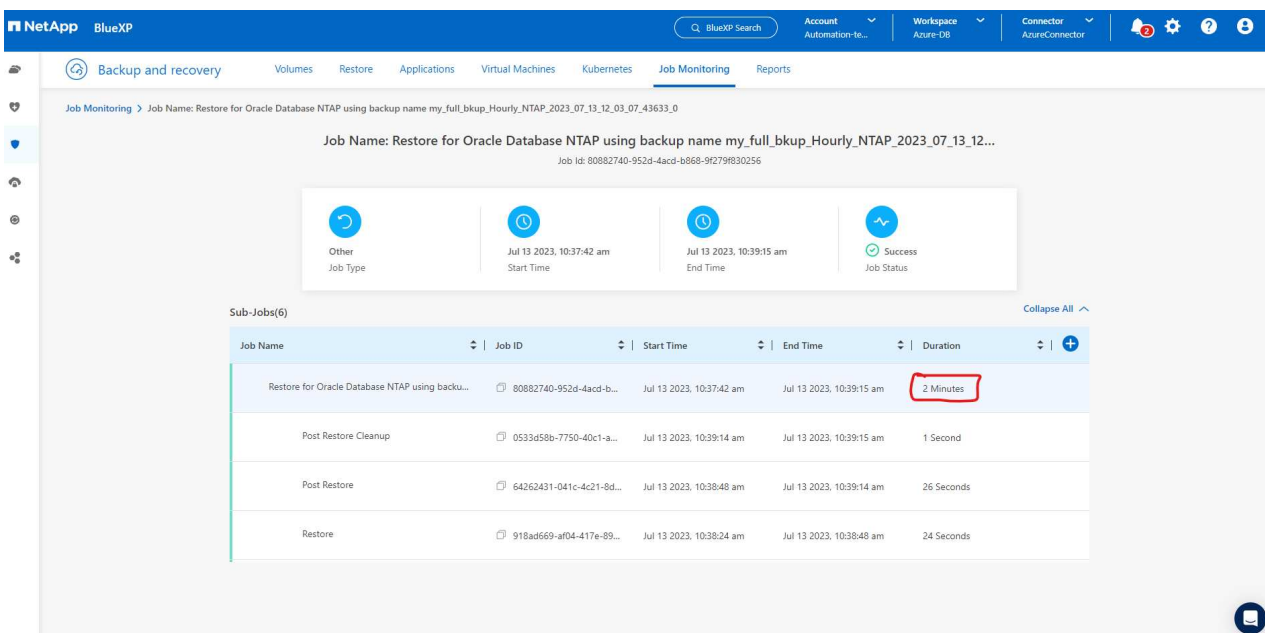
4. Definieren Sie Ihren Bereich *** Wiederherstellung*** und *** Wiederherstellungsumfang***. Alle Protokolle bedeuten eine vollständige Wiederherstellung auf dem neuesten Stand, einschließlich der aktuellen Protokolle.



5. Überprüfen und *** Wiederherstellen***, um die Wiederherstellung und Wiederherstellung der Datenbank zu starten.



6. Auf der Registerkarte **Job Monitoring** haben wir festgestellt, dass es 2 Minuten gedauert hat, bis eine vollständige Wiederherstellung der Datenbank und ein aktuelles Recovery durchgeführt wurden.



Klon einer Oracle Datenbank

Verfahren zum Klonen von Datenbanken ähneln denen der Wiederherstellung, sind aber mit einer alternativen Azure VM mit identischem Oracle-Software-Stack vorinstalliert und konfiguriert.



Stellen Sie sicher, dass der Azure NetApp File-Storage über genügend Kapazität für eine geklonte Datenbank in derselben Größe wie die zu klonende primäre Datenbank verfügt. Die alternative Azure VM wurde zu **Applications** hinzugefügt.

1. Klicken Sie auf das Drop-Down-Menü mit drei Punkten für die zu klonende Datenbank in **Applications**, und klicken Sie dann auf **Restore**, um den Clone-Workflow zu initiieren.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and dropdown menus for 'Account', 'Workspace', and 'Connector'. The main navigation tabs are 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. The 'Applications' tab is active, showing a summary of 'Cloud Native' (4 Hosts) and 'Oracle' (3 ORACLE, 0 Clone) environments. An 'Application Protection' summary shows 2 Protected and 1 Unprotected applications. Below this is a table of databases:

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

A context menu is open for the 'db1tst' database, showing options: 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore' (which is highlighted).

2. Wählen Sie den **Wiederherstellungspunkt** und aktivieren Sie die Option **an alternativen Speicherort wiederherstellen**.

The screenshot shows the 'Restore "NTAP"' configuration screen in NetApp BlueXP. The page has three steps: '1 Restore Point and Location', '2 Configuration', and '3 Review'. The current step is 'Restore Point and Location', which asks to 'Specify the restore point to which the database should be restored.' A dropdown menu for 'Restore Point' is set to 'Jul 13, 2023, 8:03:40 am'. Below this are two options: 'Restore to original location' and 'Restore to alternate location', with the latter being selected (checked).

3. Legen Sie auf der nächsten Seite **Configuration** alternative **Host**, neue Datenbank **SID** und **Oracle Home** wie bei einer alternativen Azure VM konfiguriert fest.

NetApp BlueXP

Restore "NTAP"

Restore Point and Location Configuration Review

Configuration

Specify the alternate host details on which the database will be restored and throughput.

Host: 172.30.137.147 SID: NTAP1

Oracle Home: /u01/app/oracle/product/19.0.0/clone Database Credentials: Optional

Maximum storage throughput (MIB/s): Optional

Enter throughput (1-4500)

Previous Next

4. Die Seite Review **General** zeigt die Details der geklonten Datenbank wie SID, alternativer Host, Speicherort der Datendateien, Wiederherstellungsumfang usw.

NetApp BlueXP

Restore "NTAP"

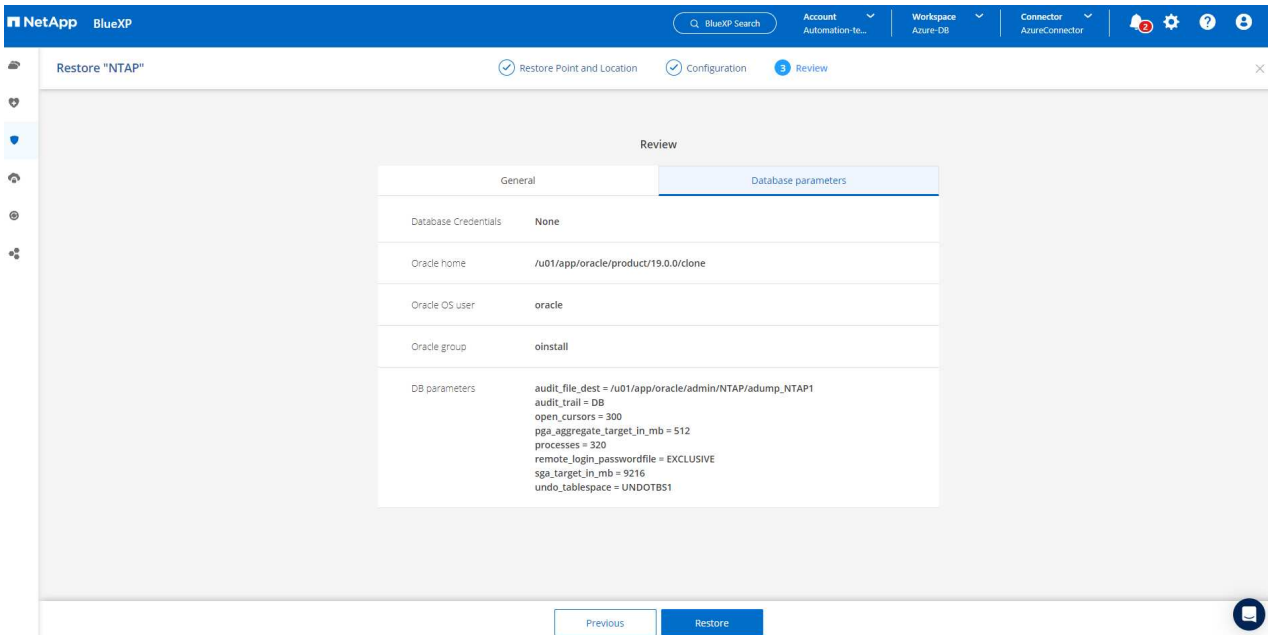
Restore Point and Location Configuration Review

Review

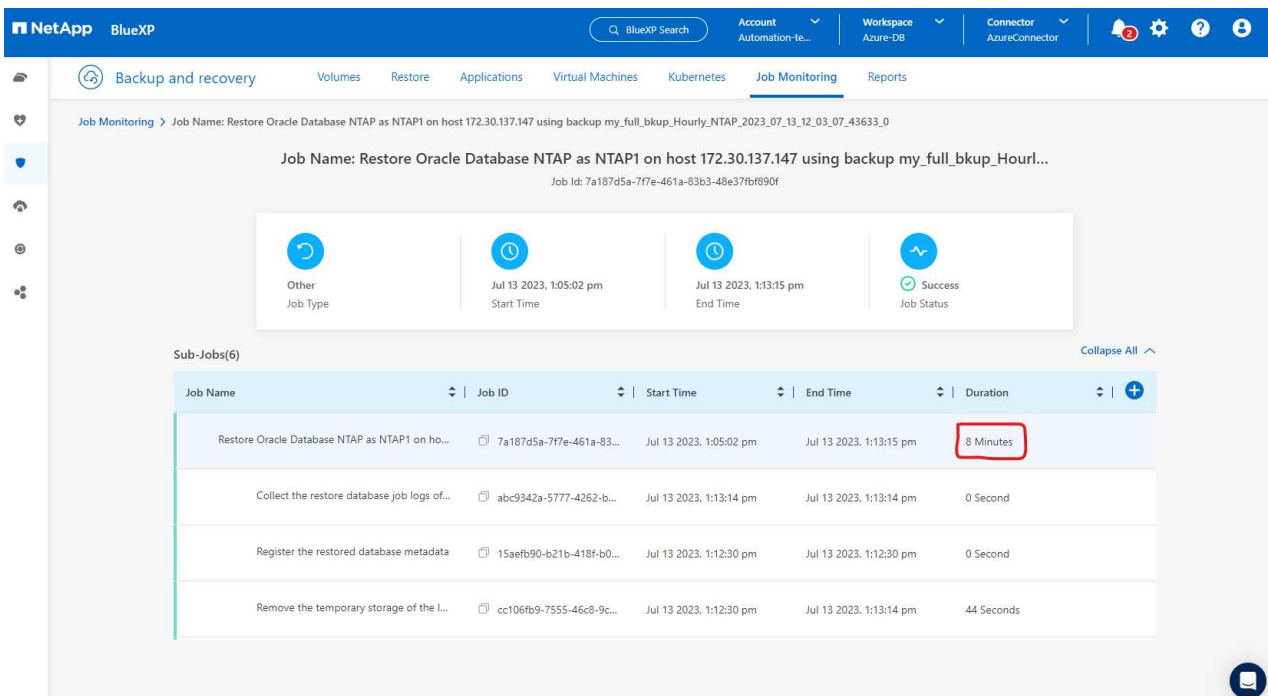
General	Database parameters
Backup Name	my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_43633_0
SID	NTAP1
Host	172.30.137.147
Datafile locations	/u02_NTAP1
Control files	/u02_NTAP1/NTAP1/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redo01.log RedoGroup = 2 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redo02.log RedoGroup = 3 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redo03.log
Recovery scope	Until cancel using selected backup's archive logs
Recovery Point	Jul 13, 2023, 8:03:40 am
Location	Alternate Location

Previous Restore

5. Die Seite Review **Datenbankparameter** zeigt die Details der geklonten Datenbankkonfiguration sowie einige Datenbankparameter an.



6. Überwachen Sie den Status des Klonjobs auf der Registerkarte **Job Monitoring** haben wir festgestellt, dass das Klonen einer 1.6 tib Oracle-Datenbank 8 Minuten dauerte.



7. Validieren Sie die geklonte Datenbank auf der BlueXP * Applications * -Seite, aus der geht, dass die geklonte Datenbank sofort bei BlueXP registriert wurde.

NetApp BlueXP

Backup and recovery | Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring | Reports

Cloud Native | Oracle

4 Hosts | 4 ORACLE | 0 Clone

Application Protection: 2 Protected, 2 Unprotected

4 Databases

Filter By +

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
NTAP1	172.30.137.147		Unprotected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

1 - 4 of 4

8. Validierung der geklonten Datenbank auf der Oracle Azure VM, aus der heraus ging, dass die geklonte Datenbank wie erwartet ausgeführt wurde

```

[oracle@acao-ora02 admin]$ cat /etc/oratab
#
# This file is used by ORACLE utilities.  It is created by root.sh
# and updated by either Database Configuration Assistant while creating
# a database or ASM Configuration Assistant while creating ASM instance.
#
# A colon, ':', is used as the field terminator.  A new line terminates
# the entry.  Lines beginning with a pound sign, '#', are comments.
#
# Entries are of the form:
#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:
#
# The first and second fields are the system identifier and home
# directory of the database respectively.  The third field indicates
# to the dbstart utility that the database should, "Y", or should not,
# "N", be brought up at system boot time.
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
NTAPI:/u01/app/oracle/product/19.0.0/clone:N
[oracle@acao-ora02 admin]$ export ORACLE_SID=NTAPI
[oracle@acao-ora02 admin]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/clone
[oracle@acao-ora02 admin]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@acao-ora02 admin]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Jul 13 17:16:31 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.18.0.0.0

SQL> select name, open_mode, log_mode from v$databases;

NAME          OPEN_MODE          LOG_MODE
-----
NTAPI         READ WRITE         NOARCHIVELOG

```

Hiermit ist die Demonstration von Backup, Wiederherstellung und Klonen einer Oracle-Datenbank in Azure mit der NetApp BlueXP Konsole über den SnapCenter Service abgeschlossen.

Weitere Informationen

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- Richten Sie BlueXP ein und verwalten Sie sie

["https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html"](https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html)

- BlueXP Backup- und Recovery-Dokumentation

["https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html"](https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html)

- Azure NetApp Dateien

["https://azure.microsoft.com/en-us/products/netapp"](https://azure.microsoft.com/en-us/products/netapp)

- Erste Schritte mit Azure

["https://azure.microsoft.com/en-us/get-started/"](https://azure.microsoft.com/en-us/get-started/)

TR-4964: Sicherung, Wiederherstellung und Klonen von Oracle-Datenbanken mit SnapCenter Services - AWS

Allen Cao, Niyaz Mohamed, NetApp

Zweck

SnapCenter Services ist die SaaS-Version des klassischen UI-Tools für das SnapCenter-Datenbankmanagement, die über die NetApp BlueXP Cloud-Managementkonsole verfügbar ist. Es ist integraler Bestandteil des NetApp Cloud-Backup- und Datensicherungsangebots für Datenbanken wie Oracle und HANA, die auf NetApp Cloud-Storage ausgeführt werden. Dieser SaaS-basierte Service vereinfacht die Bereitstellung herkömmlicher SnapCenter Standalone-Server, für die in der Regel ein Windows-Server in einer Windows-Domänenumgebung erforderlich ist.

In dieser Dokumentation zeigen wir, wie Sie SnapCenter Services für das Backup, Restore und Klonen von Oracle Datenbanken einrichten können, die auf Amazon FSX für ONTAP Storage und EC2 Computing-Instanzen implementiert sind. Die Einrichtung und Nutzung sind zwar wesentlich einfacher, jedoch bieten SnapCenter Services wichtige Funktionen, die im alten UI-Tool SnapCenter zur Verfügung stehen.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Datenbank-Backup mit Snapshots für Oracle-Datenbanken, die in Amazon FSX for ONTAP gehostet werden
- Wiederherstellung der Oracle-Datenbank im Falle eines Ausfalls
- Schnelles und Storage-effizientes Klonen primärer Datenbanken für Entwicklungs- und Testumgebungen oder andere Anwendungsfälle

Zielgruppe

Diese Lösung ist für folgende Zielgruppen konzipiert:

- Der DBA, der Oracle Datenbanken managt, die auf Amazon FSX for ONTAP Storage ausgeführt werden
- Lösungsarchitekt, der daran interessiert ist, das Backup, die Wiederherstellung und das Klonen von Oracle-Datenbanken in der Public AWS-Cloud zu testen
- Der Storage-Administrator, der den Amazon FSX für ONTAP Storage unterstützt und managt
- Der Applikationseigentümer ist Eigentümer der Applikationen, die für Amazon FSX for ONTAP Storage implementiert werden

Test- und Validierungsumgebung der Lösung

Tests und Validierungen dieser Lösung wurden in einer AWS FSX- und EC2-Umgebung durchgeführt, die möglicherweise nicht mit der endgültigen Implementierungsumgebung übereinstimmt. Weitere Informationen finden Sie im Abschnitt [\[Key Factors for Deployment Consideration\]](#).

Der Netapp Architektur Sind

Dieses Image bietet ein detailliertes Bild von BlueXP Backup und Recovery für Applikationen innerhalb der BlueXP Konsole, einschließlich der Benutzeroberfläche, der Connector und der gemanagten Ressourcen.

Hardware- und Softwarekomponenten

Hardware

FSX ONTAP-Storage	Aktuelle Version von AWS angeboten	Ein FSX HA-Cluster in der gleichen VPC und Verfügbarkeitszone
EC2 Instanz für Computing	t2.xlarge/4vCPU/16G	Zwei EC2 T2 xlarge EC2-Instanzen, eine als primärer DB-Server und die andere als Clone-DB-Server

Software

Redhat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Bereitstellung der RedHat Subscription für Tests
Oracle Grid Infrastructure	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet
Oracle Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuestes Patch p6880880_190000_Linux-x86-64.zip
SnapCenter-Service	Version	v2.3.1.2324

Wichtige Faktoren für die Implementierung

- **Connector in der gleichen VPC wie Datenbank und FSX bereitgestellt werden.** Wenn möglich, sollte der Connector in der gleichen AWS VPC bereitgestellt werden, was die Anbindung an den FSX Storage und die EC2-Compute-Instanz ermöglicht.
- **Eine für den SnapCenter-Konnektor erstellte AWS IAM-Richtlinie.** die Richtlinie im JSON-Format ist in der detaillierten SnapCenter-Service-Dokumentation verfügbar. Wenn Sie die Connector-Implementierung über die BlueXP Konsole starten, werden Sie auch aufgefordert, die Voraussetzungen mit Details der erforderlichen Berechtigung im JSON-Format einzurichten. Die Richtlinie sollte dem AWS-Benutzerkonto zugewiesen werden, dem der Connector gehört.
- **Der Zugriffsschlüssel für das AWS-Konto und das im AWS-Konto erstellte SSH-Schlüsselpaar.** das SSH-Schlüsselpaar wird dem ec2-Benutzer zur Anmeldung am Connector-Host und zur Bereitstellung eines Datenbank-Plug-ins an den EC2-DB-Server-Host zugewiesen. Der Zugriffsschlüssel gewährt die Berechtigung zum Bereitstellen des erforderlichen Connectors mit der oben genannten IAM-Richtlinie.
- **Zugangsdaten wurden zur BlueXP Konsoleinstellung hinzugefügt.** um Amazon FSX for ONTAP zur BlueXP Arbeitsumgebung hinzuzufügen, sind in der BlueXP Konsoleinstellung Zugangsdaten eingerichtet, die BlueXP Berechtigungen für den Zugriff auf Amazon FSX for ONTAP gewähren.

- **java-11-openjdk auf dem Host der EC2-Datenbankinstanz installiert.** die Installation des SnapCenter-Dienstes erfordert die java-Version 11. Sie muss auf dem Anwendungshost installiert werden, bevor die Plug-in-Bereitstellung versucht wird.

Lösungsimplementierung

Die umfassende NetApp Dokumentation bietet ein breiteres Spektrum, um Sie beim Schutz Ihrer Cloud-nativen Applikationsdaten zu unterstützen. Ziel dieser Dokumentation ist es, Schritt-für-Schritt-Verfahren zur Implementierung der SnapCenter Services über die BlueXP Konsole bereitzustellen, um die in Amazon FSX for ONTAP und einer EC2 Computing-Instanz implementierte Oracle Datenbank zu sichern. Dieses Dokument füllt bestimmte Details aus, die möglicherweise in allgemeineren Anweisungen fehlen.

Um zu beginnen, gehen Sie wie folgt vor:

- Lesen Sie die allgemeinen Anweisungen "[Sichern Sie Ihre Daten aus Cloud-nativen Applikationen](#)" sowie die Abschnitte zu Oracle und Amazon FSX for ONTAP.
- Sehen Sie sich das folgende Video an.

Lösungsimplementierung

Voraussetzungen für die Bereitstellung des SnapCenter Services

Die Bereitstellung erfordert die folgenden Voraussetzungen.

1. Ein primärer Oracle Datenbankserver auf einer EC2-Instanz mit einer Oracle-Datenbank, die vollständig bereitgestellt ist und ausgeführt wird.
2. Ein in AWS implementierter Amazon FSX for ONTAP-Cluster, der die obigen Datenbank-Volumes hostet.
3. Ein optionaler Datenbankserver auf einer EC2-Instanz, der zum Testen des Klonens einer Oracle-Datenbank auf einem alternativen Host verwendet werden kann, um einen Entwicklungs-/Test-Workload zu unterstützen, oder andere Anwendungsfälle, die einen vollständigen Datensatz einer Oracle-Produktionsdatenbank erfordern.
4. Wenn Sie Hilfe bei der Erfüllung der oben genannten Voraussetzungen für die Implementierung der Oracle-Datenbank auf Amazon FSX for ONTAP und EC2-Compute-Instanz benötigen, finden Sie weitere Informationen unter "[Implementierung und Schutz von Oracle Database in AWS FSX/EC2 mit iSCSI/ASM](#)" Oder Whitepaper "[Oracle Database Deployment on EC2 und FSX Best Practices](#)"

Onboarding bei der BlueXP Vorbereitung

1. Verwenden Sie den Link "NetApp BlueXP" Um sich für den Konsolenzugriff von BlueXP zu registrieren.
2. Melden Sie sich bei Ihrem AWS-Konto an, um eine IAM-Richtlinie mit entsprechenden Berechtigungen zu erstellen und die Richtlinie dem AWS-Konto zuzuweisen, das für die Implementierung des BlueXP Connectors verwendet wird.

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with categories like 'Dashboard', 'Access management', 'Policies', 'Access reports', and 'Service control policies (SCPs)'. The main content area is titled 'Policies > snapcenter Summary'. It shows the 'Policy ARN' as 'arn:aws:iam::541696183547:policy/snapcenter' and the 'Description' as 'Policy to grant snapcenter service permission to create connector in AWS.'. Below this are tabs for 'Permissions', 'Policy usage', 'Tags', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is active, showing a 'Policy summary' and an 'Edit policy' button. A JSON string is displayed in a code editor, defining the policy's permissions. The JSON string is as follows:

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:CreateRole",
8         "iam:DeleteRole",
9         "iam:PutRolePolicy",
10        "iam:CreateInstanceProfile",
11        "iam:DeleteRolePolicy",
12        "iam:AddRoleToInstanceProfile",
13        "iam:RemoveRoleFromInstanceProfile",
14        "iam:DeleteInstanceProfile",
15        "iam:PassRole",
16        "iam:ListRoles",
17        "ec2:DescribeInstanceStatus",
18        "ec2:RunInstances",
19        "ec2:ModifyInstanceAttribute",
20        "ec2:CreateSecurityGroup",
21        "ec2:DeleteSecurityGroup",
22        "ec2:DescribeSecurityGroups",
23        "ec2:RevokeSecurityGroupEgress",
24        "ec2:AuthorizeSecurityGroupEgress",
25        "ec2:AuthorizeSecurityGroupIngress",
26        "ec2:RevokeSecurityGroupIngress",
27        "ec2:CreateNetworkInterface",
28        "ec2:DescribeNetworkInterfaces"

```

Die Richtlinie sollte mit einem JSON-String konfiguriert werden, der in der NetApp-Dokumentation verfügbar ist. Die JSON-Zeichenfolge kann auch von der Seite abgerufen werden, wenn die Connector-Bereitstellung gestartet wird und Sie zur Berechtigungszuweisung für die Voraussetzungen aufgefordert werden.

3. Sie benötigen außerdem die AWS VPC, das Subnetz, die Sicherheitsgruppe, den Zugriffsschlüssel und Schlüssel für das AWS Benutzerkonto, einen SSH-Schlüssel für ec2-User usw. für die Connector-Bereitstellung.

Stellen Sie einen Connector für SnapCenter-Services bereit

1. Melden Sie sich bei der BlueXP Konsole an. Für ein freigegebenes Konto empfiehlt es sich, einen individuellen Arbeitsbereich zu erstellen, indem Sie auf **Konto > Konto verwalten > Arbeitsbereich** klicken, um einen neuen Arbeitsbereich hinzuzufügen.

The screenshot shows the 'Workspaces' page in the BlueXP console for the account 'Automation-team'. The page has a navigation bar with tabs for 'Overview', 'Members', 'Workspaces' (which is active), and 'BlueXP Connector'. Below the navigation bar, the main heading is 'Manage the BlueXP connector Workspaces'. There is a '+ Add New Workspace' link. A table lists four existing workspaces: 'Database', 'Database-2', 'sufians-k8', and 'Workspace-1'. Each workspace name is followed by a trash icon and an edit icon. In the bottom right corner of the main content area, there is a dark blue circular button with a white speech bubble icon.

Manage the BlueXP connector Workspaces	
+ Add New Workspace	
Database	
Database-2	
sufians-k8	
Workspace-1	

2. Klicken Sie auf **Add a Connector**, um den Connector-Provisioning-Workflow zu starten.

NetApp Cloud Manager Account Automation-team Workspace new-workspace Connector N/A

Backup & Restore Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

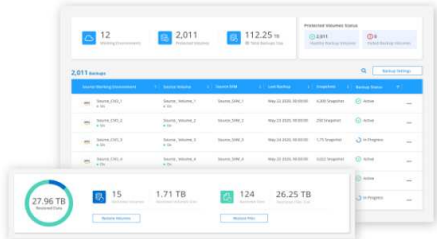
Backup & Restore

Fully integrated data protection for ONTAP anywhere

Cloud Backup dramatically reduces the complexity of backing up critical structured and unstructured data across your ONTAP hybrid cloud environments to cost-effective object storage. All you need to do is select the source, the target and the protection policy and you're protected


To start your Backup & Restore experience, please deploy our connector

[Add a Connector](#)




Connector Name	Source	Target	Status	Created	Updated	Actions
Connector 1	Source Volume 1	Target Volume 1	Ready	May 20, 2020, 10:00:00	10:00:00	View
Connector 2	Source Volume 2	Target Volume 2	Ready	May 20, 2020, 10:00:00	10:00:00	View
Connector 3	Source Volume 3	Target Volume 3	Ready	May 20, 2020, 10:00:00	10:00:00	View
Connector 4	Source Volume 4	Target Volume 4	Ready	May 20, 2020, 10:00:00	10:00:00	View

27.96 TB 15 1.71 TB 124 26.25 TB




Simple & intuitive

No backup or cloud expertise required. Simply click the button above and follow the instructions



Hybrid Multicloud

Backup from On-premises or Cloud Volumes ONTAP to AWS, Azure, GCP or StorageGRID



Unmatched Efficiency


Combines incremental, block-level operation and storage efficiencies to reduce time and cost

1. Wählen Sie Ihren Cloud-Provider (in diesem Fall **Amazon Web Services**).


Add Connector ×

Provider


Choose the cloud provider where you want to run the Connector:



Microsoft Azure



Amazon Web Services



Google Cloud Platform

[Continue](#)

1. Überspringen Sie die Schritte **permission**, **Authentication** und **Networking**, wenn Sie sie bereits in Ihrem AWS-Konto eingerichtet haben. Wenn nicht, müssen Sie diese konfigurieren, bevor Sie fortfahren. Von hier aus könnten Sie auch die Berechtigungen für die AWS-Richtlinie abrufen, auf die

im vorherigen Abschnitt „Onboarding bei der BlueXP Vorbereitung.“

Add Connector - AWS ✕


Deploying a Connector

The Connector is a crucial component for the day-to-day use of Cloud Manager.
It's used to connect Cloud Manager's services to your hybrid-cloud environments.
The Connector can then manage the resources and processes within your public cloud environment.

Before you begin the deployment process, ensure that you have completed the required preparations. This guide will enable you to focus on the minimum requirements for Connector installation.

Permissions Set up an IAM role with the required permissions	Authentication Choose between two AWS authentication methods: AWS keys or assuming an IAM role	Networking Obtain details about the VPC and subnet in which the Connector will reside
--	--	---

[Skip to Deployment](#)

[Previous](#) [Continue](#) 

1. Geben Sie die Authentifizierung Ihres AWS-Kontos mit **Zugriffsschlüssel** und **geheimer Schlüssel** ein.

- 1 AWS Credentials 2 Details 3 Network 4 Security Group 5 Review

AWS Authentication

Region

us-east-1 | US East (N. Virginia)

Select the Authentication Method: Assume Role AWS Keys

AWS Access Key

AKIA6JRXA6ZVGVFUSHMO3

AWS Secret Key

.....

Want to launch an instance without AWS Credentials? ▾

Previous

Next

2. Benennen Sie die Connector-Instanz und wählen Sie unter **Details** *Rolle erstellen.

- 1 AWS Credentials 2 Details 3 Network 4 Security Group 5 Review

Details

Connector Instance Name ⓘ

SnapCenterSvs

[+](#) Add Tags to Connector Instance

Connector Role ⓘ

 Create Role Select an existing Role

Role Name

Cloud-Manager-Operator-VZzSSP9-SnapCenter

 AWS Managed Encryption ⓘ

Master Key: aws/ebs (default)

[Change Key](#)

Previous

Next

1. Konfigurieren Sie das Netzwerk mit dem richtigen **VPC**, **Subnetz** und **SSH Key Pair** für den Connector-Zugriff.

Add BlueXP Connector - AWS More Information ×

✓ AWS Credentials ✓ Details **3 Network** 4 Security Group 5 Review

Network

Connectivity

VPC

Subnet

Key Pair ?

Public IP


Notice: Ensure that the subnet has internet connectivity through a NAT device or proxy server so that the Connector can communicate with AWS services.

Proxy Configuration (Optional)

HTTP Proxy

Define Credentials for this Proxy ∨

Upload a root certificate ∨



2. Stellen Sie die **Sicherheitsgruppe** für den Konnektor ein.

 AWS Credentials  Details  Network ** Security Group**  Review

Security Group

The security group must allow inbound HTTP, HTTPS and SSH access.

Assign a security group: Create a new security group Select an existing security group

1 Security Group 

Security Group Name	Description
<input checked="" type="radio"/> default	default VPC security group

Previous

Next 

- Überprüfen Sie die Übersichtsseite, und klicken Sie auf **Hinzufügen**, um die Verbindungserstellung zu starten. Die Implementierung dauert in der Regel etwa 10 Minuten. Sobald der Vorgang abgeschlossen ist, wird die Connector-Instanz im AWS EC2-Dashboard angezeigt.

- ✓ AWS Credentials
- ✓ Details
- ✓ Network
- ✓ Security Group
- 5** Review

Review

[Code for Terraform Automation](#)

BlueXP Connector Name	aws-snapctr-us-east
AWS Access Key	AKIAX4H43ZT5GIWWR3TI
Region	us-east-1
VPC	vpc-0b522d5e982a50ceb - 172.30.15.0/25
Subnet	172.30.15.0/25 priv-subnet-01
Key Pair	sufi_new
Public IP	Use subnet settings (Disable)
Proxy	None
Security Group	default

Previous

Add



Definieren Sie Zugangsdaten für den Zugriff auf AWS Ressourcen in BlueXP

1. Erstellen Sie zunächst in der AWS EC2-Konsole eine Rolle im Menü **Identity and Access Management (IAM) Roles, Create role**, um den Workflow für die Rollenerstellung zu starten.

2. Wählen Sie auf der Seite **Select Trusted entity** die Option **AWS-Konto, ein anderes AWS-Konto** aus und fügen Sie die BlueXP Konto-ID ein, die von der BlueXP Konsole abgerufen werden kann.

3. Filtern Sie Berechtigungsrichtlinien nach fsx und fügen Sie der Rolle **Berechtigungsrichtlinien** hinzu.

Add permissions InfoPermissions policies (Selected 1/889) Info

Choose one or more policies to attach to your new role.

 4 matches

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AmazonFSxReadOnlyAccess	AWS ma...	Provides read only access to Amazon FSx.
<input checked="" type="checkbox"/>	AmazonFSxFullAccess	AWS ma...	Provides full access to Amazon FSx and access to related AWS services.
<input type="checkbox"/>	AmazonFSxConsoleReadOnlyAccess	AWS ma...	Provides read only access to Amazon FSx and access to related AWS services via the AWS Management Console.
<input type="checkbox"/>	AmazonFSxConsoleFullAccess	AWS ma...	Provides full access to Amazon FSx and access to related AWS services via the AWS Management Console.

▶ Set permissions boundary - optional Info

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

4. Geben Sie auf der Seite **Rollendetails** einen Namen für die Rolle ein, fügen Sie eine Beschreibung hinzu, und klicken Sie dann auf **Rolle erstellen**.

Name, review, and create Info

Role details

Role name

Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+, @, _' characters.

Description

Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and '+, @, _' characters.

Step 1: Select trusted entities

```

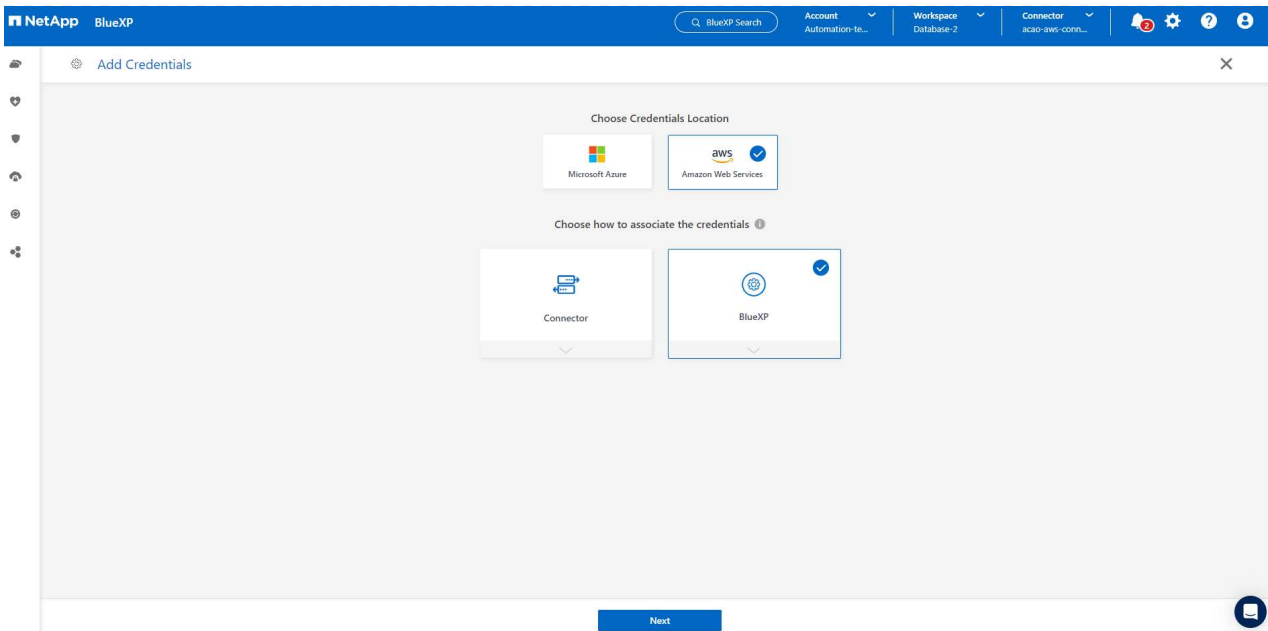
1- {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "952013314444"
9       },
10      "Condition": {}
11    }
12  ]
13 }

```

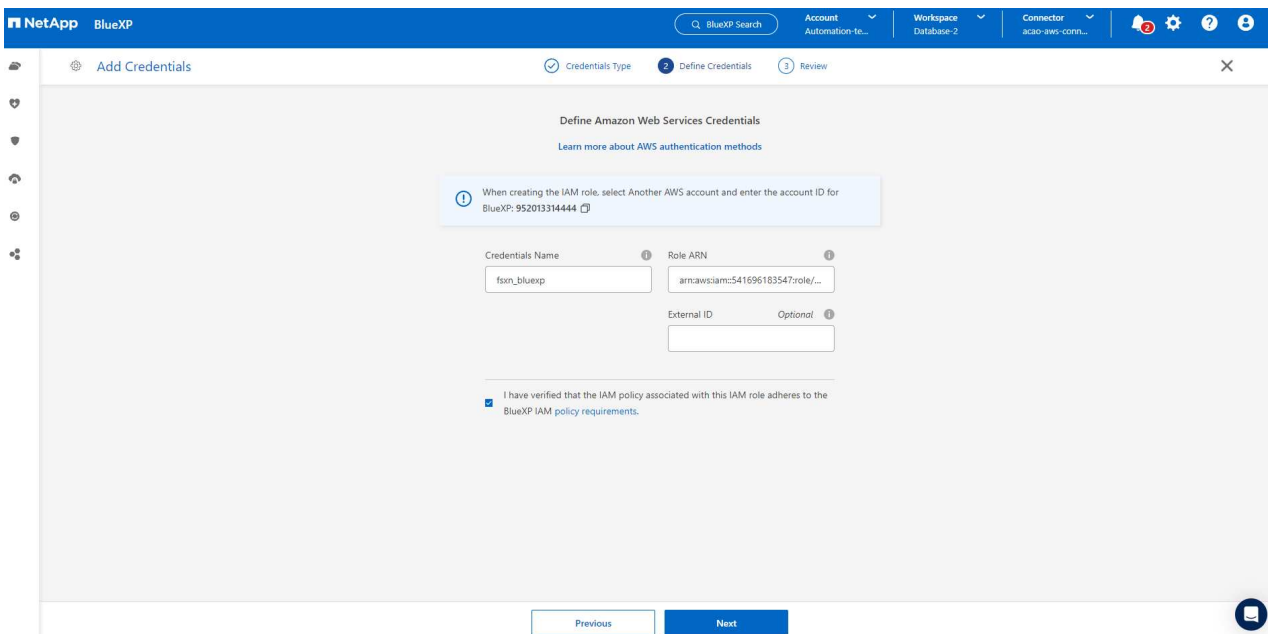
5. Zurück zur BlueXP-Konsole, klicken Sie auf das Einstellungssymbol oben rechts in der Konsole, um die Seite **Account Credentials** zu öffnen, klicken Sie auf **Add credentials**, um den Workflow der Anmeldedatenkonfiguration zu starten.

The screenshot shows the NetApp BlueXP console interface. At the top, there's a navigation bar with 'NetApp BlueXP', a search bar, and several dropdown menus. Below that, the 'Credentials' section is active, showing 'Account credentials' and 'User credentials' tabs. A central message states: 'BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.' Below this, a list of 5 credentials is shown. One credential, 'shantanucreds', is highlighted, showing its type as 'Assume Role | BlueXP' and its AWS Account ID as '210811600188'. An 'Add credentials' button is visible in the top right of the list.

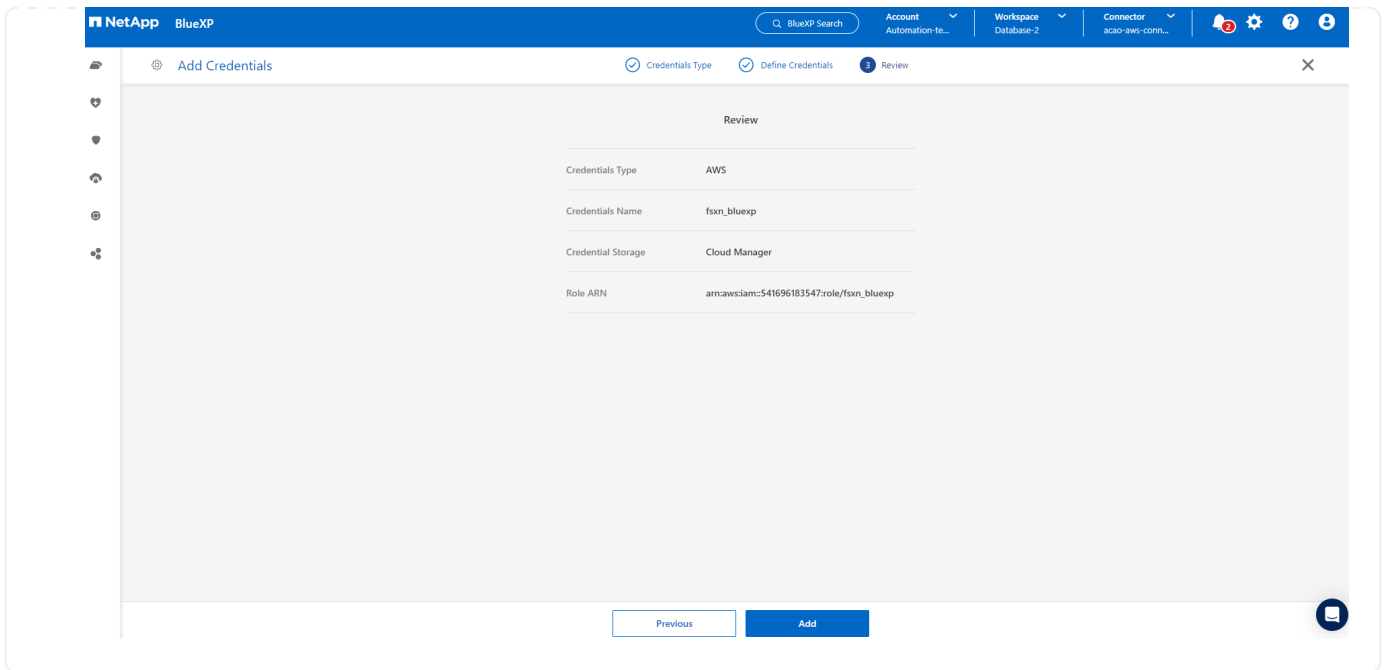
6. Wählen Sie den Anmeldeinformationsspeicherort als - **Amazon Web Services - BlueXP**.



7. Definieren Sie AWS-Anmeldeinformationen mit richtiger **role ARN**, die aus der in Schritt 1 oben erstellten AWS IAM-Rolle abgerufen werden kann. BlueXP **Account-ID**, die zur Erstellung der AWS IAM-Rolle in Schritt 1 verwendet wird.



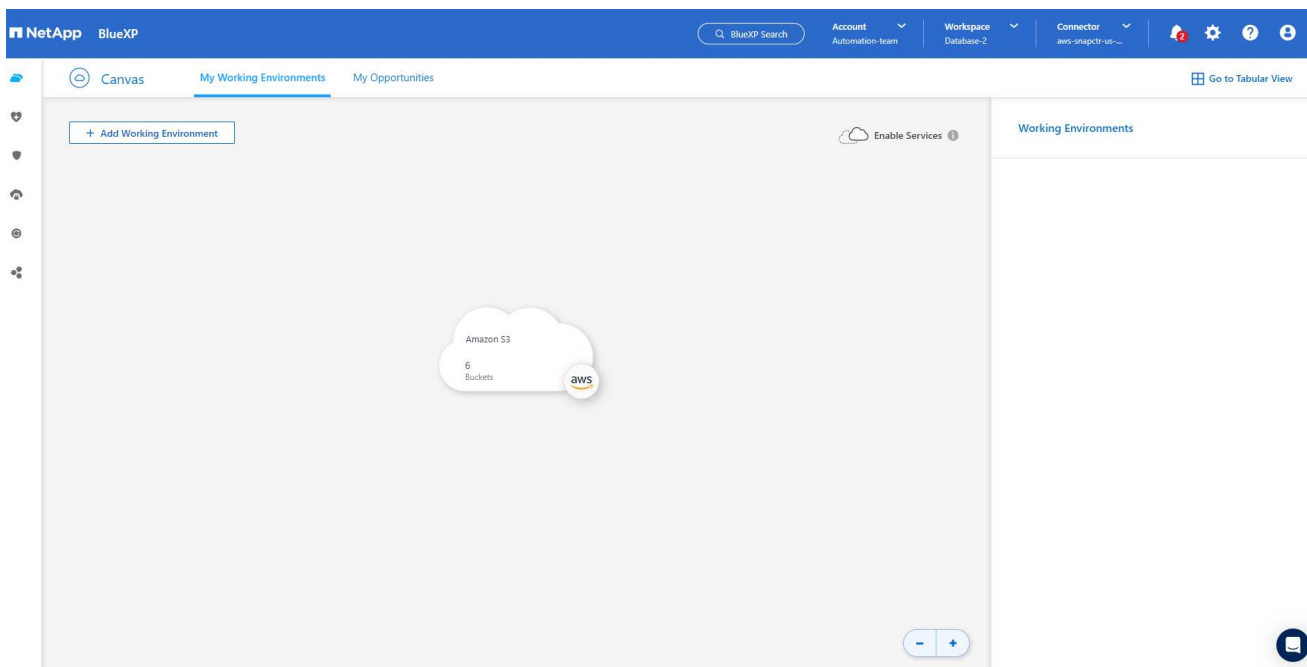
8. Bewertung und **Hinzufügen**.



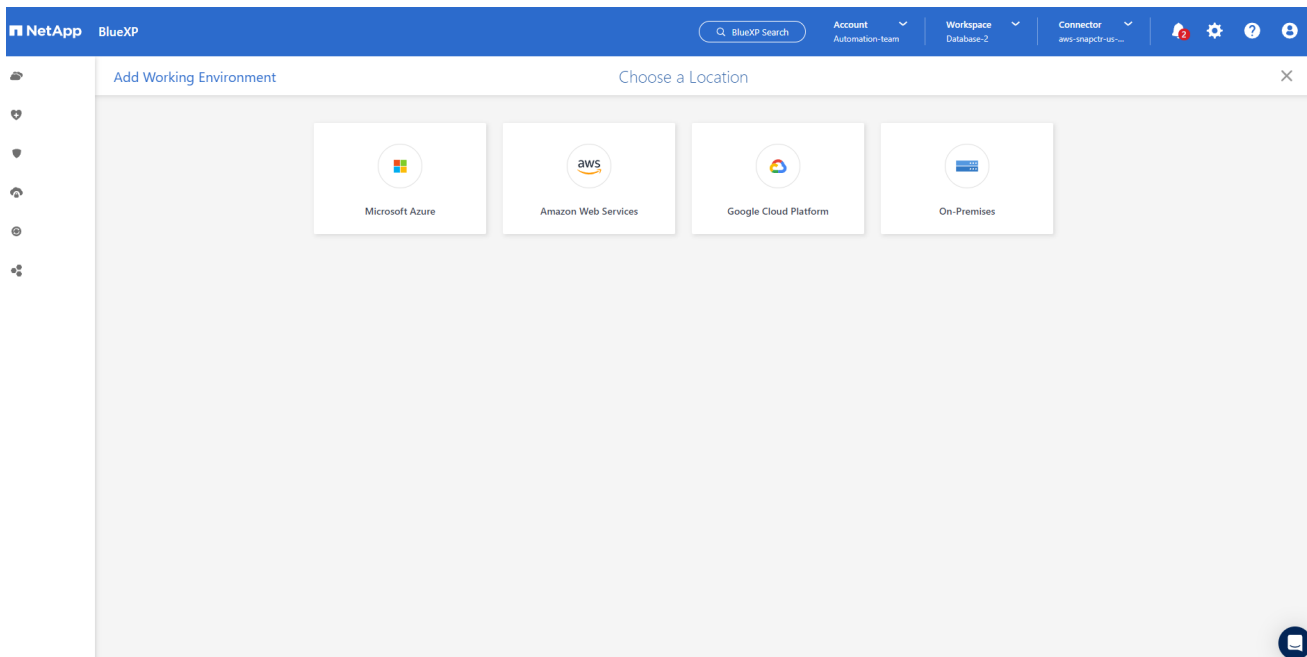
Einrichtung der SnapCenter Services

Wenn der Connector bereitgestellt und die Zugangsdaten hinzugefügt wurden, können SnapCenter-Services jetzt wie folgt eingerichtet werden:

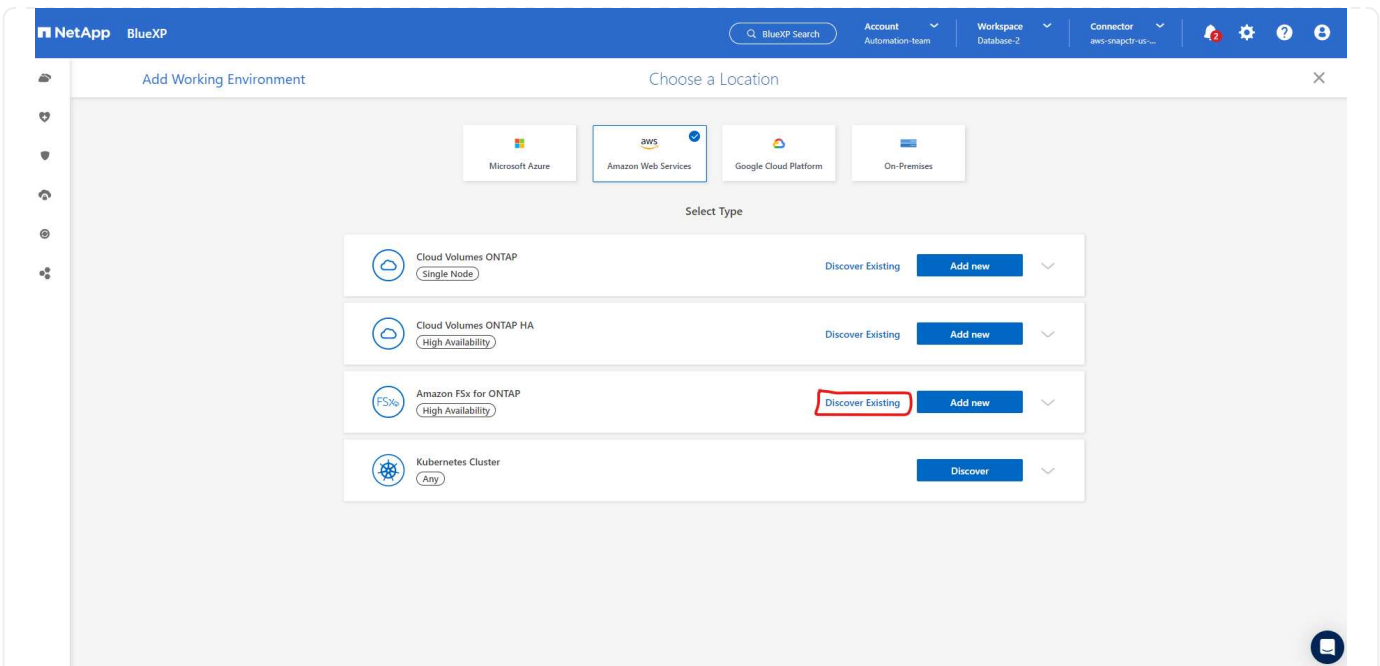
1. Klicken Sie unter **Meine Arbeitsumgebung** auf **Arbeitsumgebung hinzufügen**, um FSX in AWS bereitzustellen.



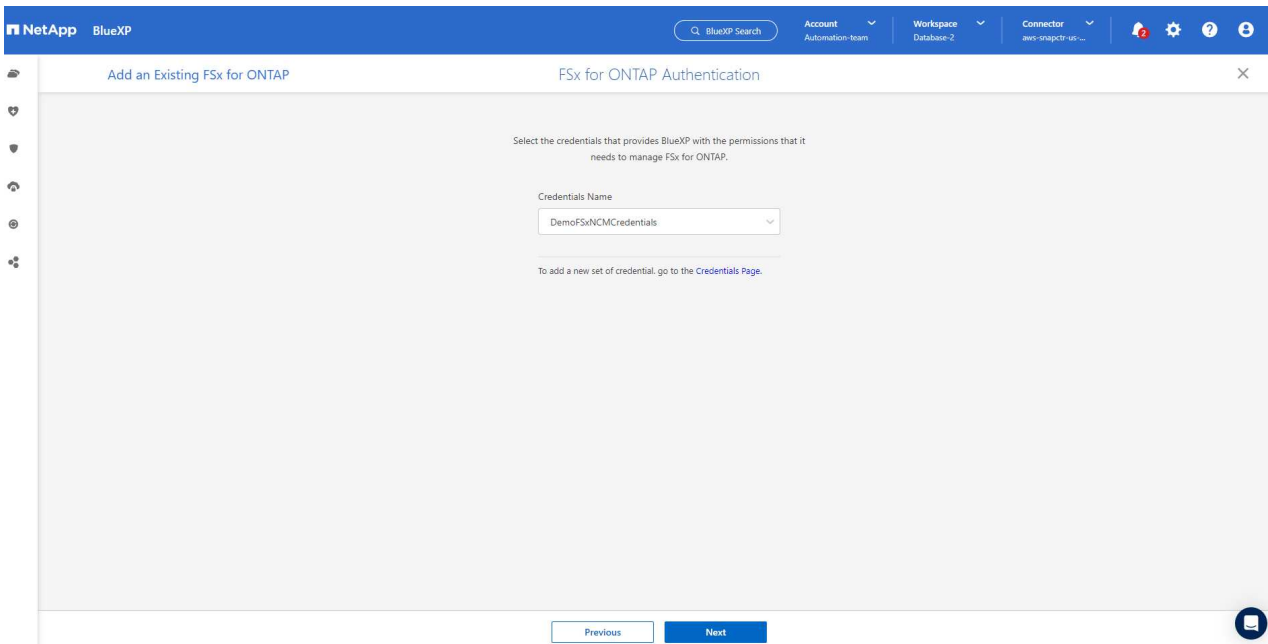
1. Wählen Sie **Amazon Web Services** als Speicherort.



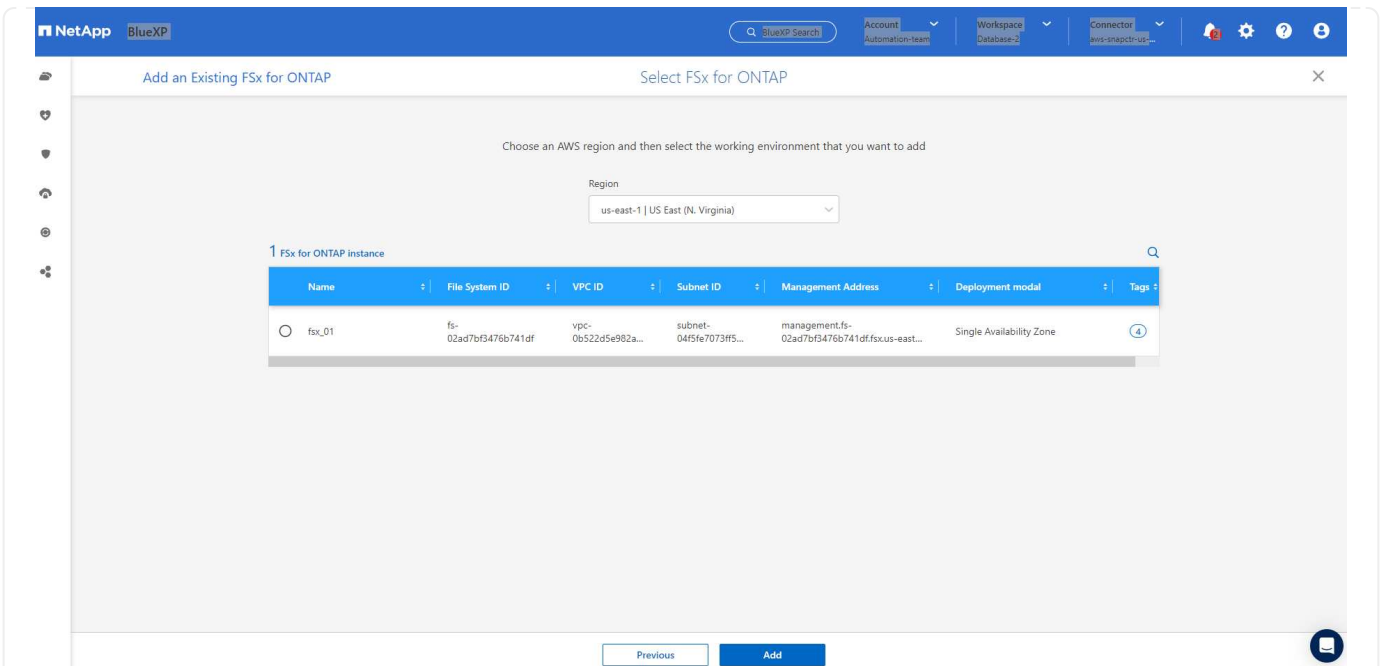
1. Klicken Sie neben **Amazon FSX for ONTAP** auf **existing** entdecken.



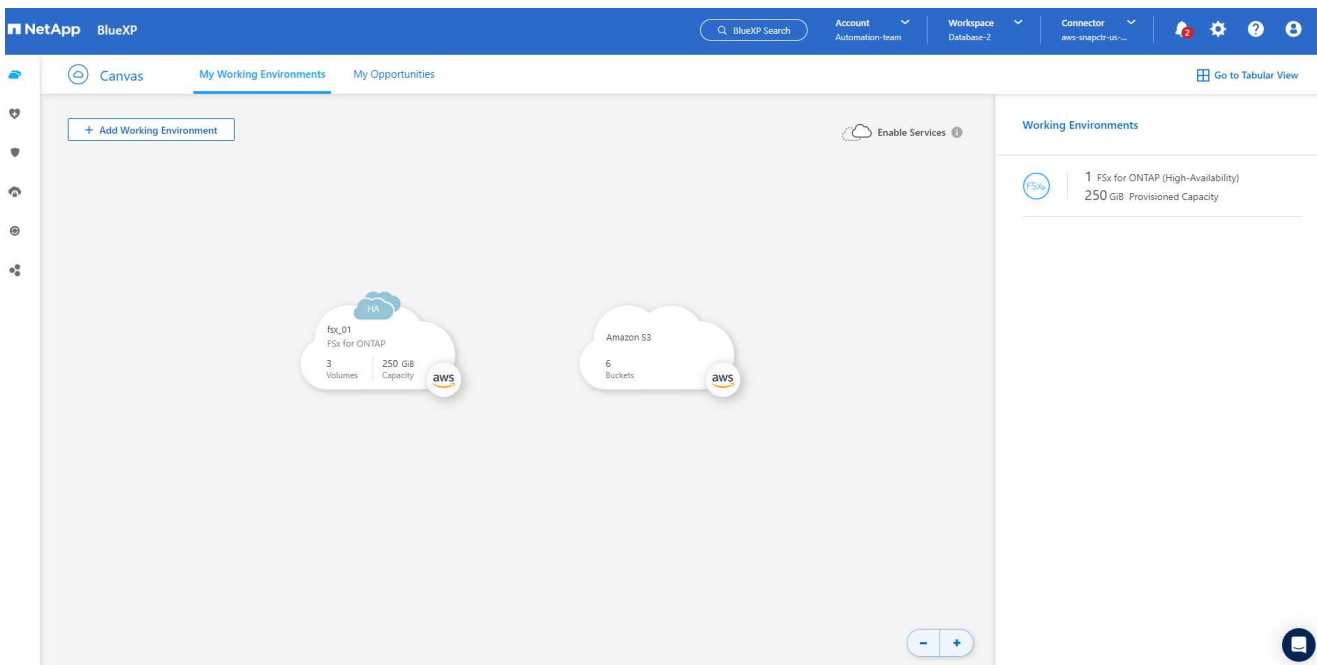
1. Wählen Sie den **Zugangsdaten-Namen** aus, den Sie im vorherigen Abschnitt erstellt haben, um BlueXP die Berechtigungen zu erteilen, die es benötigt, um FSX for ONTAP zu verwalten. Wenn Sie keine Zugangsdaten hinzugefügt haben, können Sie diese über das Menü **Einstellungen** oben rechts in der BlueXP Konsole hinzufügen.



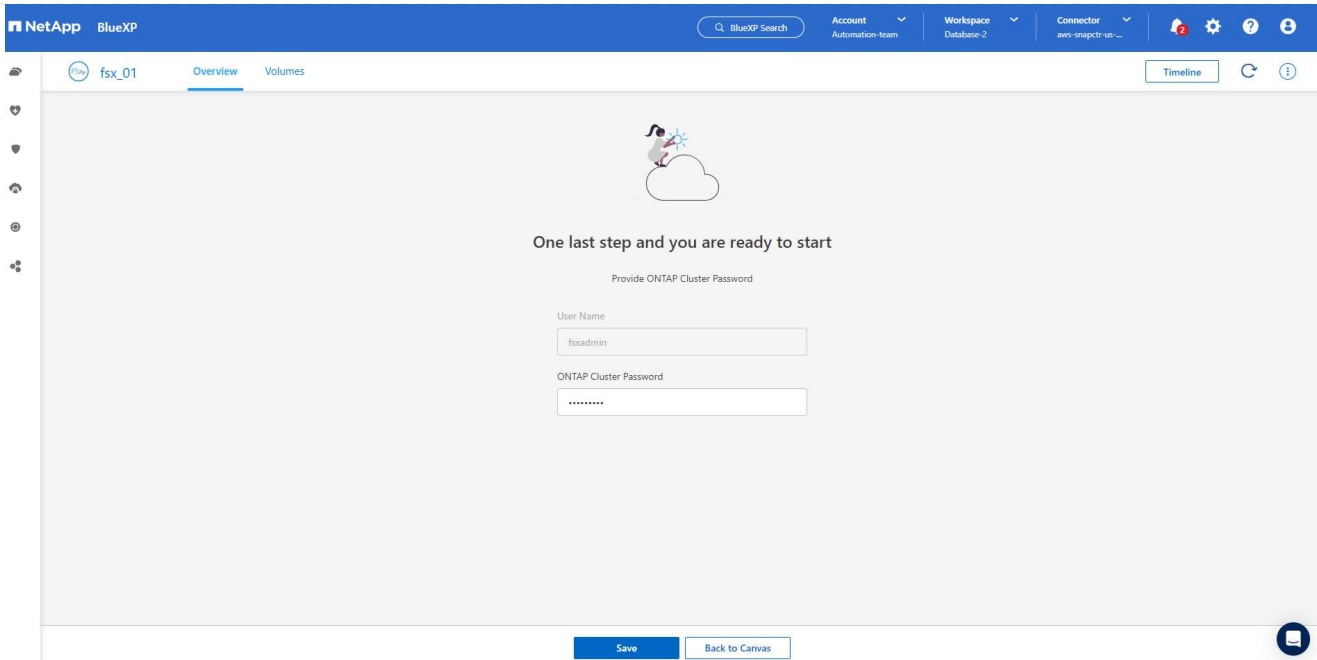
2. Wählen Sie die AWS-Region aus, in der Amazon FSX for ONTAP bereitgestellt wird, wählen Sie den FSX-Cluster aus, der die Oracle-Datenbank hostet, und klicken Sie auf Hinzufügen.



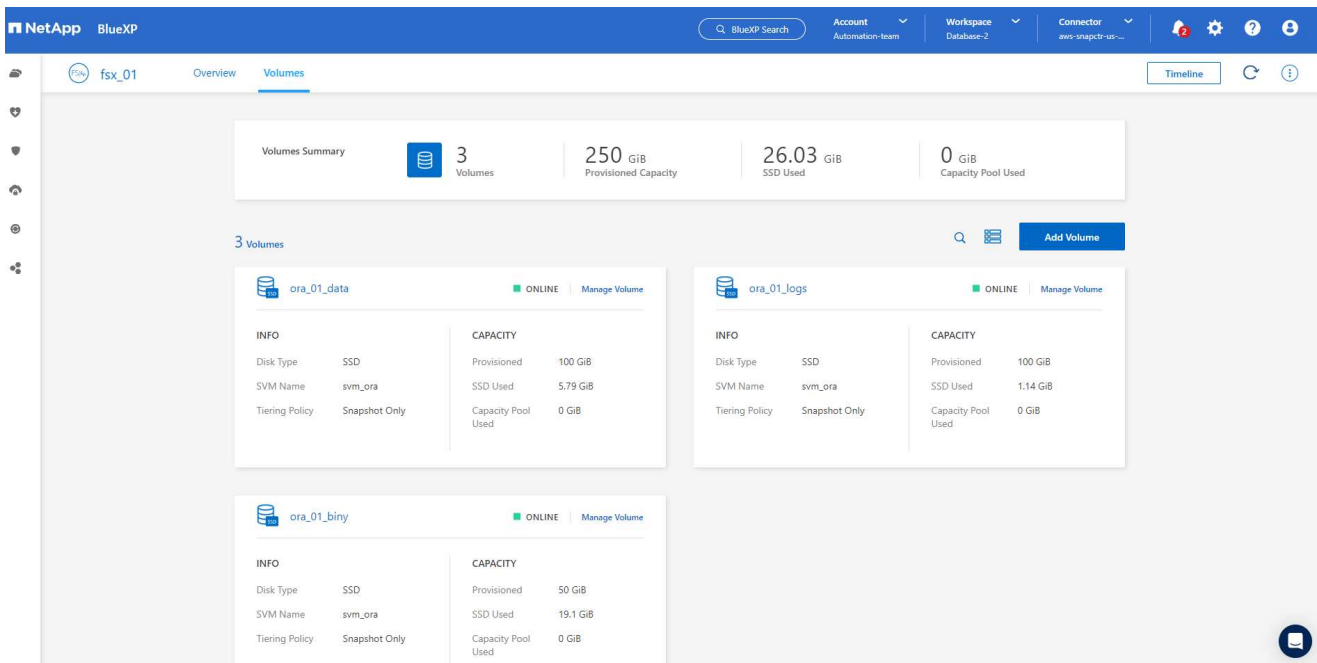
1. Die entdeckte Amazon FSX for ONTAP-Instanz erscheint jetzt in der Arbeitsumgebung.



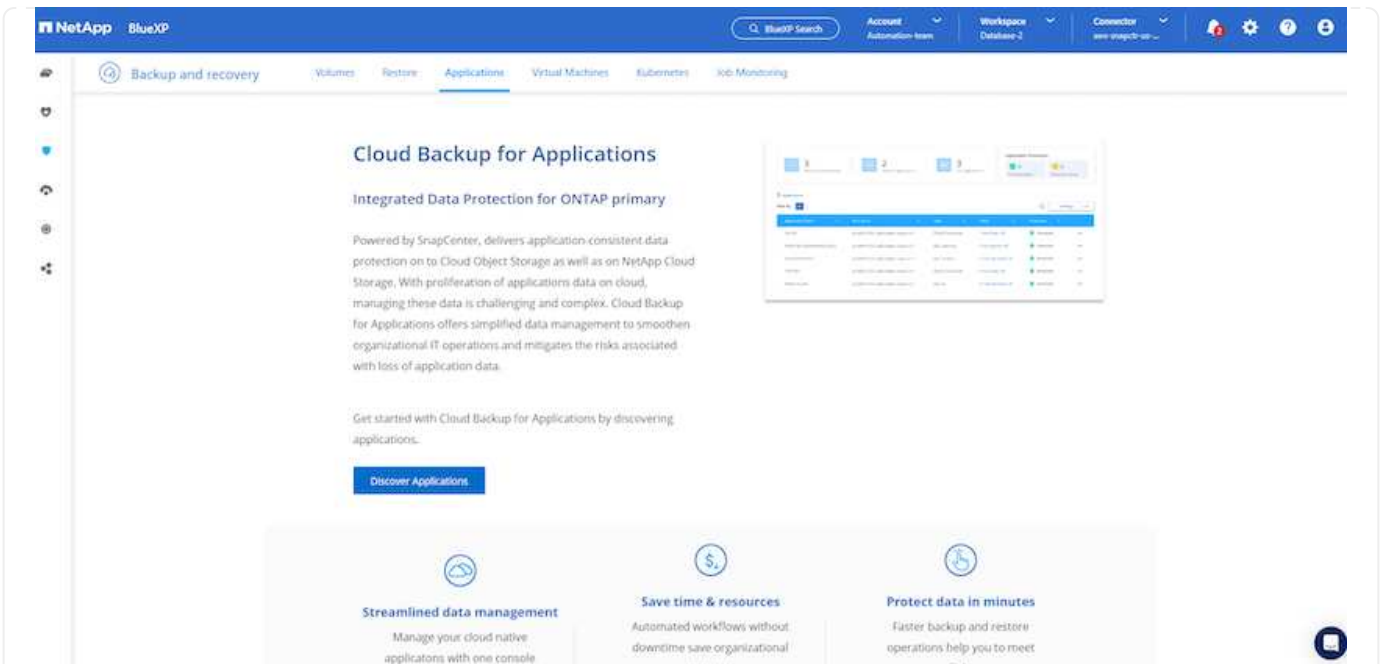
1. Sie können sich mit Ihren fsxadmin-Anmeldeinformationen im FSX-Cluster anmelden.



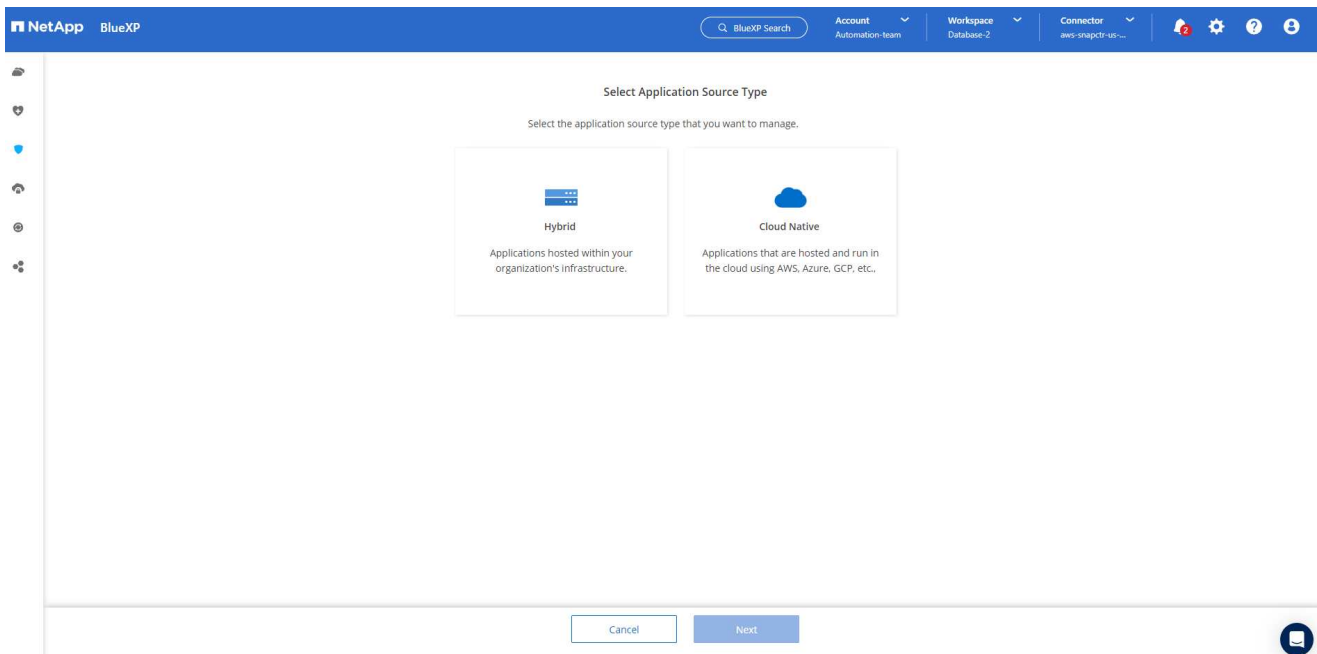
1. Nachdem Sie sich bei Amazon FSX for ONTAP angemeldet haben, prüfen Sie Ihre Informationen zum Datenbank-Storage (z. B. Datenbank-Volumes).



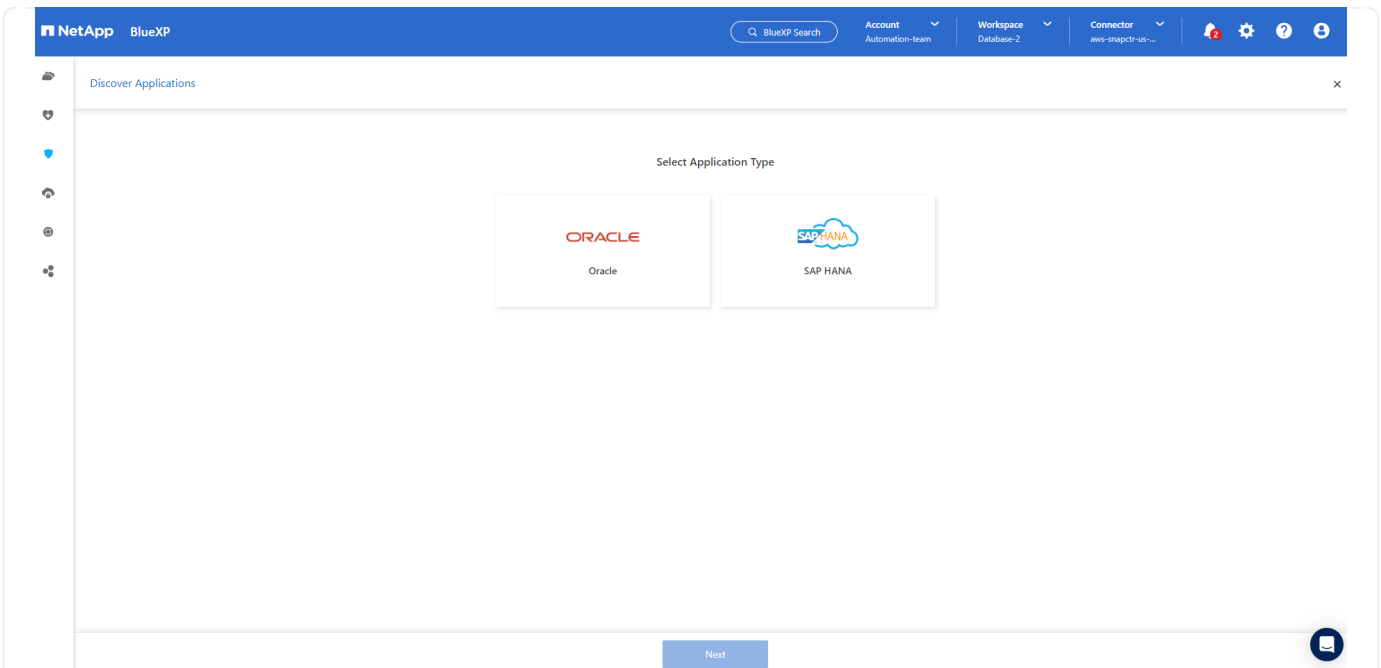
1. Bewegen Sie in der linken Seitenleiste der Konsole Ihre Maus über das Schutzsymbol und klicken Sie dann auf **Schutz > Anwendungen**, um die Startseite der Anwendungen zu öffnen. Klicken Sie Auf **Anwendungen Entdecken**.



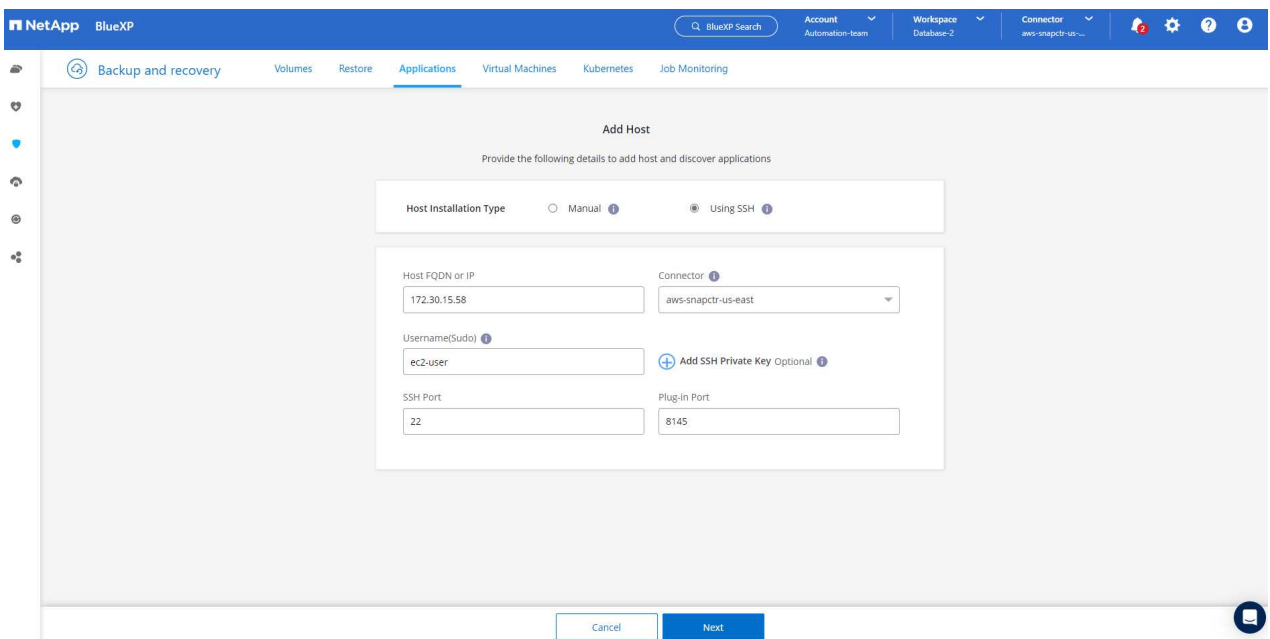
1. Wählen Sie **Cloud Native** als Quelltyp der Anwendung aus.



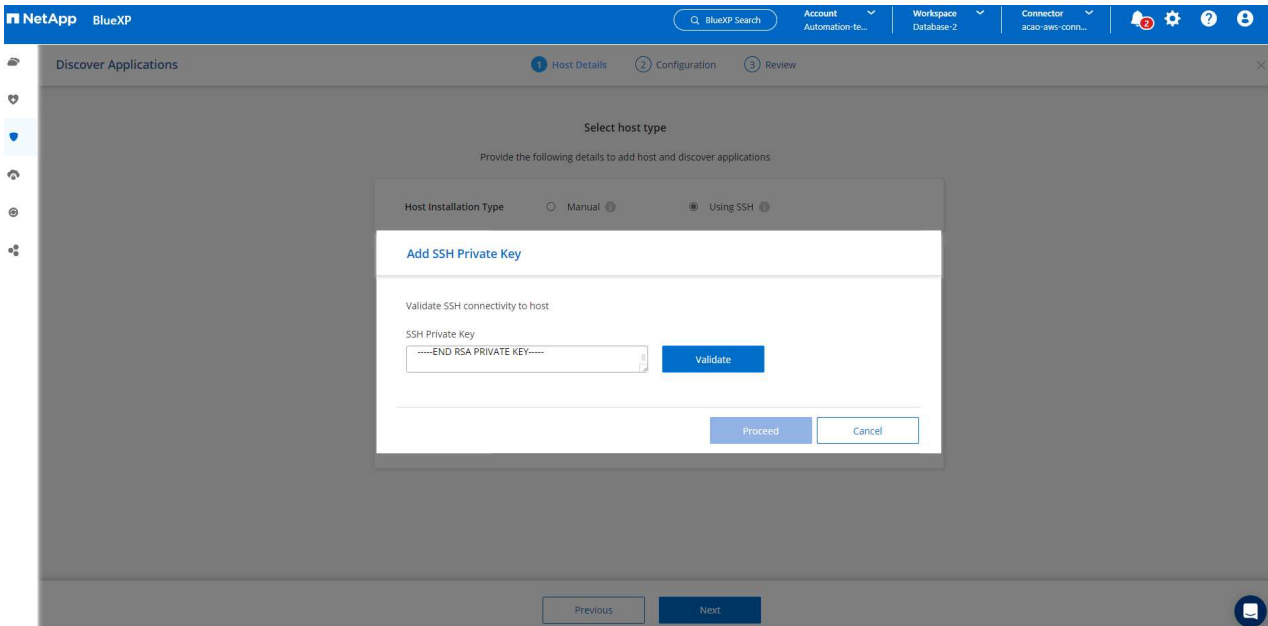
1. Wählen Sie **Oracle** für den Anwendungstyp.



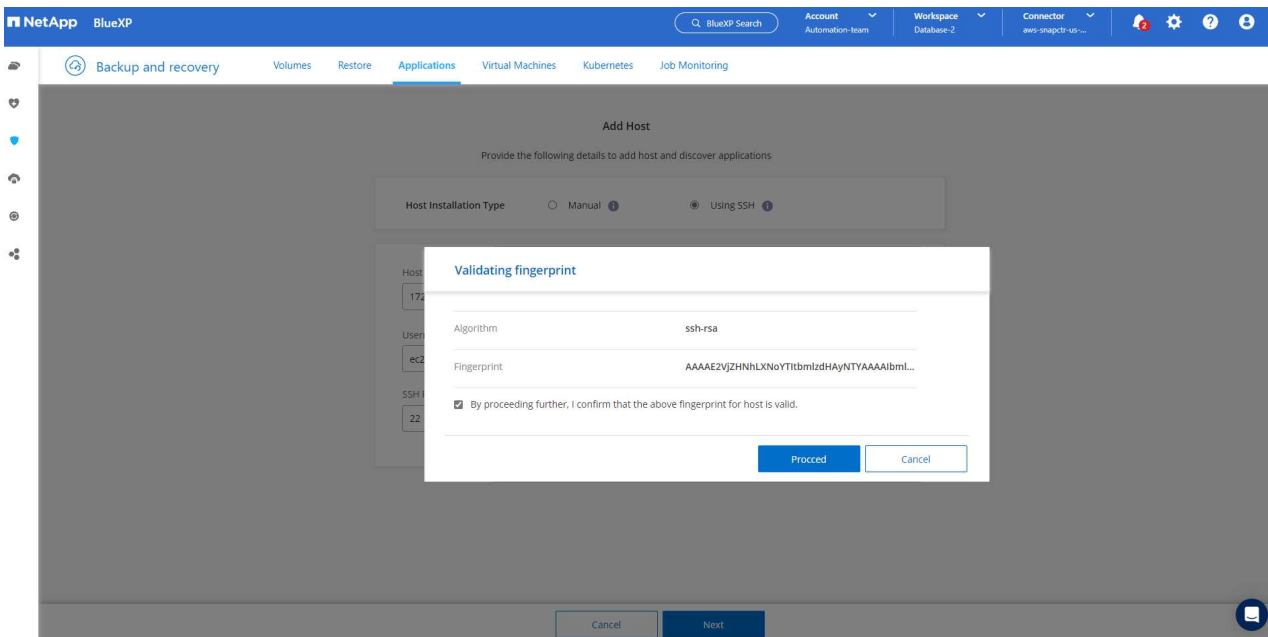
1. Geben Sie Details zum Host der AWS EC2 Oracle Applikation ein. Wählen Sie **mit SSH** als **Host-Installationstyp** für eine schrittweise Plugin-Installation und Datenbankerkennung. Klicken Sie dann auf **SSH Private Key hinzufügen**.



2. Fügen Sie Ihren ec2-User SSH-Schlüssel für die Datenbank EC2-Host ein und klicken Sie auf **Validate**, um fortzufahren.



3. Sie werden aufgefordert, **Validating Fingerprint** einzugeben, um fortzufahren.



4. Klicken Sie auf **Weiter**, um ein Oracle Datenbank Plugin zu installieren und die Oracle Datenbanken auf dem EC2 Host zu ermitteln. Entdeckte Datenbanken werden zu **Anwendungen** hinzugefügt. Die Datenbank **Schutzstatus** wird als **ungeschützt** angezeigt, wenn sie zuerst entdeckt wird.

The screenshot shows the NetApp BlueXP console interface. At the top, there's a navigation bar with 'NetApp BlueXP' and a search bar. Below that, a secondary navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The main content area is titled 'Applications' and shows a summary of resources: 1 Hosts, 1 ORACLE, and 0 Clones. To the right, an 'Application Protection' summary shows 0 Protected and 1 Unprotected items. Below this, a table lists 1 Database with the name 'db1', host name '172.30.15.58', and protection status 'Unprotected'.

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

Damit ist die Ersteinrichtung der SnapCenter Services für Oracle abgeschlossen. In den nächsten drei Abschnitten dieses Dokuments werden die Backup-, Restore- und Klonvorgänge für Oracle-Datenbanken beschrieben.

Backup von Oracle Datenbanken

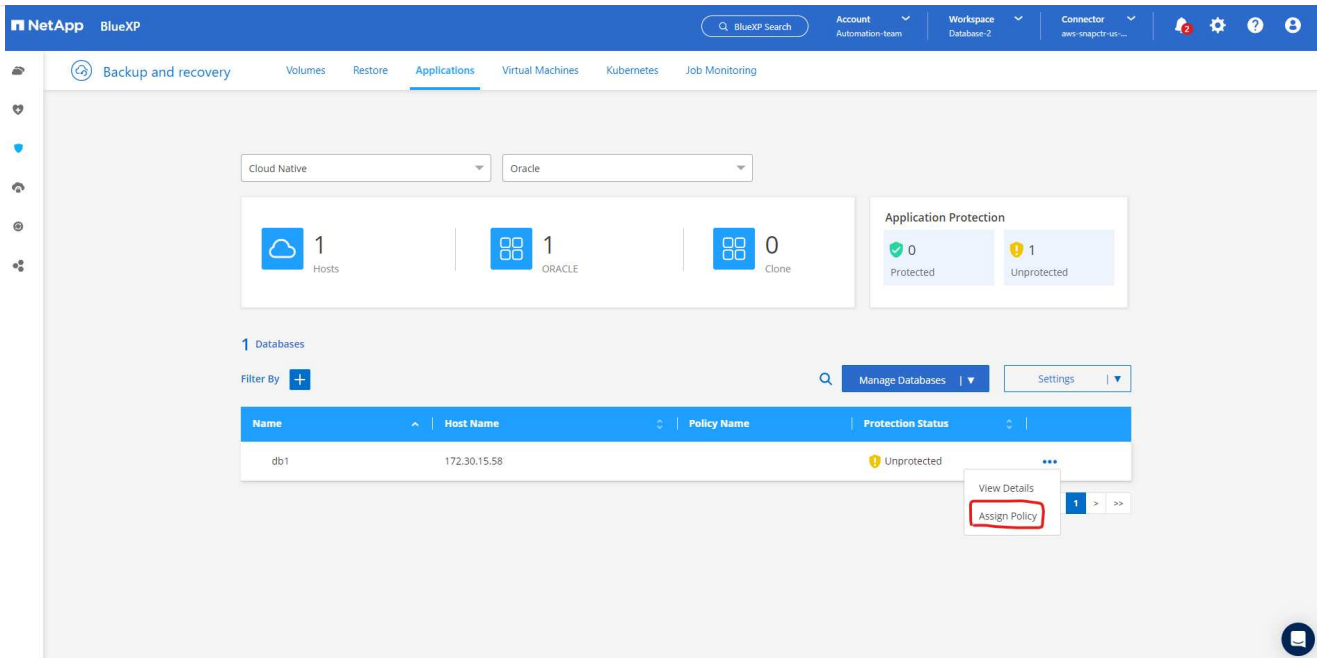
1. Klicken Sie auf die drei Punkte neben der Datenbank **Schutzstatus** und dann auf **Richtlinien**, um die vorinstallierten Standardrichtlinien für den Datenbankschutz anzuzeigen, die zum Schutz Ihrer Oracle-Datenbanken angewendet werden können.

The screenshot shows the NetApp BlueXP interface. At the top, there's a navigation bar with 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. Below this, there are filters for 'Cloud Native' and 'Oracle'. A summary card shows '1 Hosts', '1 ORACLE', and '0 Clone'. An 'Application Protection' card shows '0 Protected' and '1 Unprotected'. A table lists databases with columns for Name, Host Name, Policy Name, and Protection Status. The table shows one database 'db1' with host '172.30.15.58' and status 'Unprotected'. A 'Settings' dropdown menu is open, showing options for Policies, About, and Hosts.

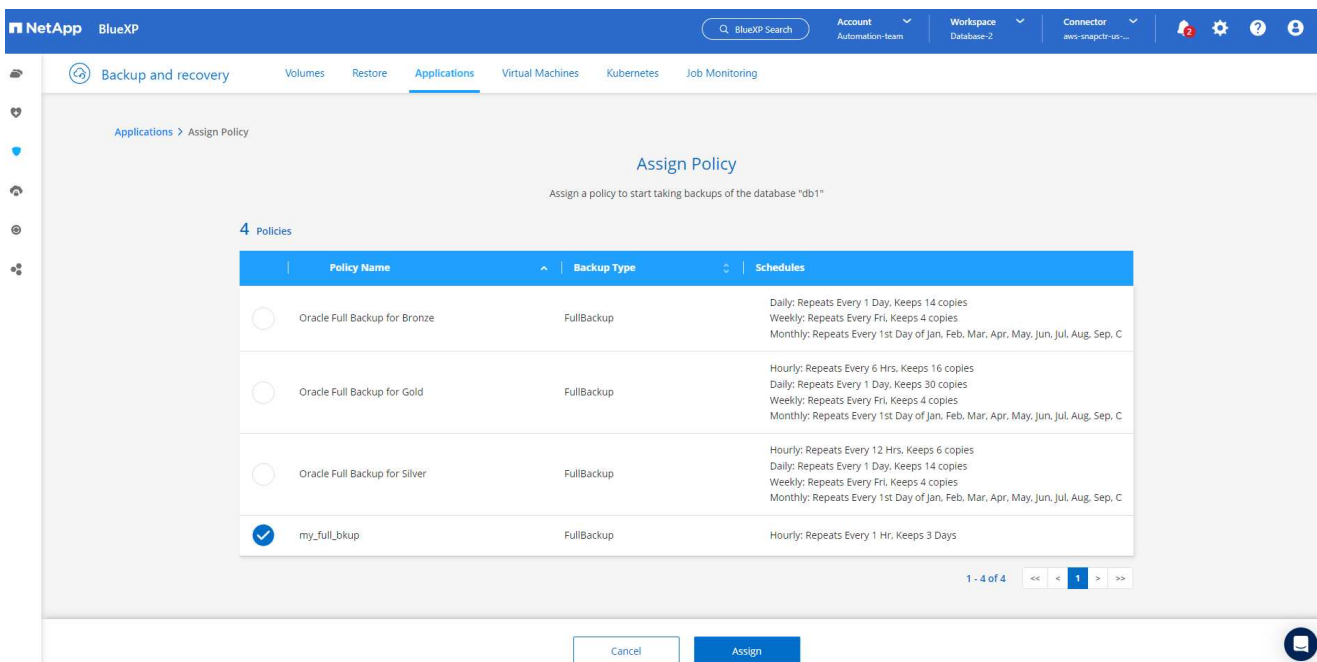
1. Darüber hinaus können Sie mit einer angepassten Backup-Häufigkeit und dem Zeitfenster für die Backup-Datenaufbewahrung Ihre eigenen Richtlinien erstellen.

The screenshot shows the NetApp BlueXP interface for 'Applications > Policies'. It features filters for 'Cloud Native' and 'Oracle'. A 'Create Policy' button is visible. A table lists four policies with columns for Policy Name, Backup Type, and Schedules and Retention. The policies are: 'Oracle Full Backup for Bronze', 'Oracle Full Backup for Gold', 'Oracle Full Backup for Silver', and 'my_full_bkup'. Each policy row includes details about its backup frequency and retention period, along with a three-dot menu icon for further actions.

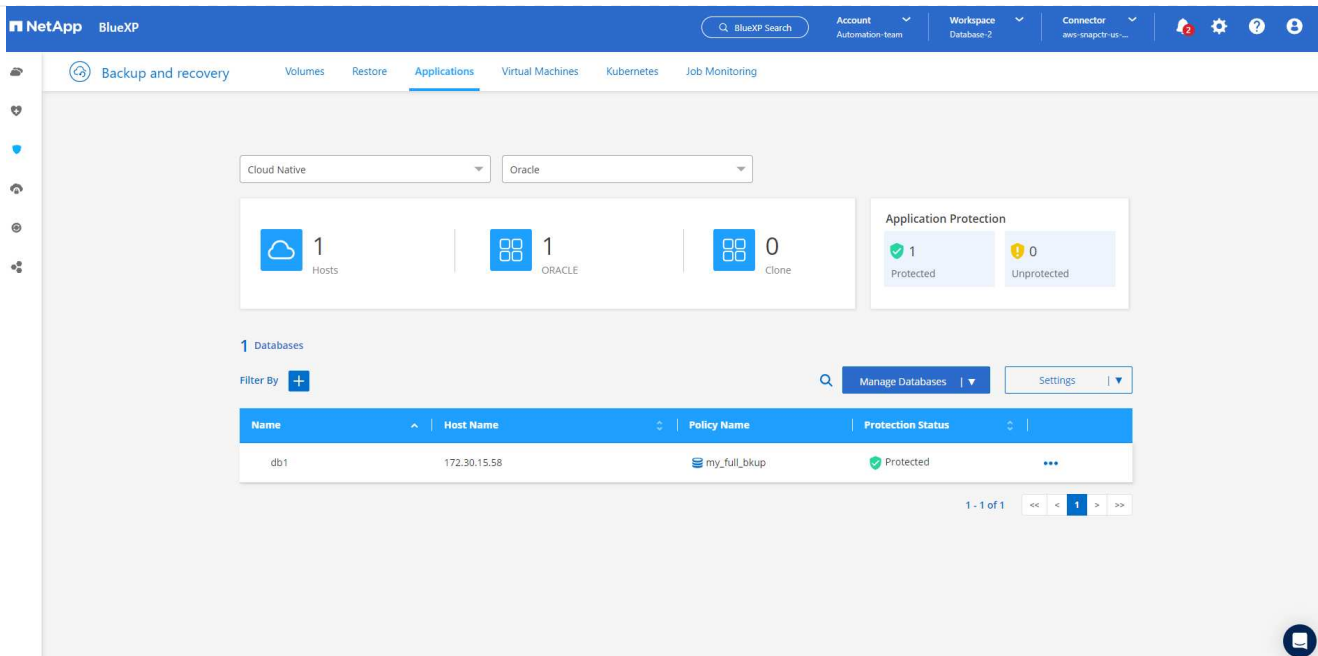
1. Wenn Sie mit der Richtlinienkonfiguration zufrieden sind, können Sie die gewünschte Richtlinie zum Schutz der Datenbank zuweisen.



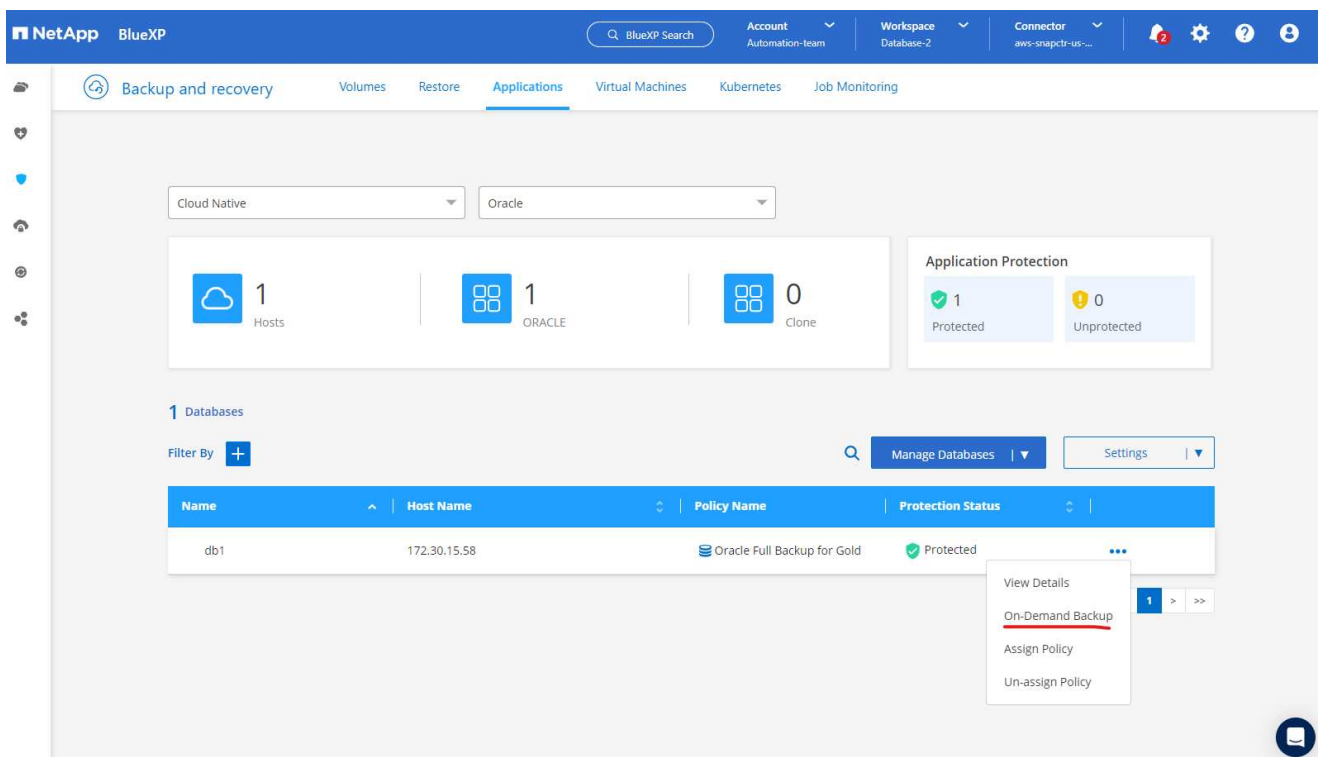
1. Wählen Sie die Richtlinie aus, die der Datenbank zugewiesen werden soll.



1. Nachdem die Richtlinie angewendet wurde, wurde der Datenbankschutzstatus mit einem grünen Häkchen in **protected** geändert.



1. Das Datenbank-Backup wird nach einem vordefinierten Zeitplan ausgeführt. Sie können auch ein einzelnes On-Demand-Backup ausführen, wie unten gezeigt.



1. Die Details der Datenbank-Backups können durch Klicken auf **Details anzeigen** aus der Menüliste angezeigt werden. Dazu gehören der Backup-Name, der Backup-Typ, der SCN und das Backup-Datum. Ein Backup-Satz deckt einen Snapshot sowohl für Daten-Volumen als auch für Protokoll-Volumen ab. Ein Snapshot eines Protokollvolumens erfolgt direkt nach einem Snapshot eines Datenbank-Volumens. Sie können einen Filter anwenden, wenn Sie nach einem bestimmten Backup in einer langen Liste suchen.

NetApp BlueXP

Account Automation-team | Workspace Database-2 | Connector aws-snapctr-us...

Backup and recovery | Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring

Applications > Database Details

Database Details

db1 Database Name	Protected Protection	Oracle Full Backup for Gold Policy Names	Database Type
172.30.15.58 Host Name	FSx Host Storage	Unreachable Database Version	bKed8yv2T19Bj0V5Qyqva... Agent Id
- Clones	- Parent Database		

8 Backups

Filter By +

Select Timeframe

Backup Name	Backup Type	SCN	Backup Date	
Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_12_18_60900_1	Log	2589354	Mar 24, 2023, 3:12:34 pm	Delete
Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_11_51_51476_0	Data	2589306	Mar 24, 2023, 3:12:18 pm	...
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1	Log	2586621	Mar 24, 2023, 2:10:45 pm	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_03_70535_0	Data	2586557	Mar 24, 2023, 2:10:31 pm	...

Wiederherstellung und Recovery von Oracle-Datenbanken

1. Wählen Sie für eine Datenbank-Wiederherstellung das richtige Backup aus, entweder durch die SCN oder die Backup-Zeit. Klicken Sie auf die drei Punkte der Datenbankdatensicherung und dann auf **Wiederherstellen**, um die Wiederherstellung der Datenbank zu starten.

The screenshot shows the 'Database Details' page for a database named 'db1'. Below the details, there is a 'Backups' section with a table listing several backup entries. The 'Restore' button for the backup 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_37_04_98851_1' is highlighted with a red box.

Backup Name	Backup Type	SCN	Backup Date	
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1	Log	2586621	Mar 24, 2023, 2:10:45 pm	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_03_70535_0	Data	2586557	Mar 24, 2023, 2:10:31 pm	...
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_37_04_98851_1	Log	2580577	Mar 24, 2023, 11:37:1	Restore
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_36_33_27205_0	Data	2580524	Mar 24, 2023, 11:37:0	Delete Clone

1. Wählen Sie Ihre Wiederherstellungseinstellung aus. Wenn Sie sicher sind, dass sich nach dem Backup nichts in der physischen Datenbankstruktur geändert hat (wie z.B. das Hinzufügen einer Datendatei oder einer Datenträgergruppe), können Sie die Option **Force in Place Restore** verwenden, die im Allgemeinen schneller ist. Markieren Sie andernfalls dieses Kontrollkästchen nicht.

The screenshot shows the 'Restore Settings' page for the database 'db1'. The 'Restore Scope' section has 'All Data Files' selected. The 'Force in place restore' checkbox is checked. The 'Recovery Scope' section has 'All Logs' selected.

Restore Scope

- All Data Files
Data Files Restore
- Control Files
Control Files Restore
- Force in place restore
In place restore will skip the foreign files/files which are not part of the database) validation check. The Oracle database and the ASM disk group will be restored to the point when the backup was created.
- Database state will be changed if needed for restore and recovery.

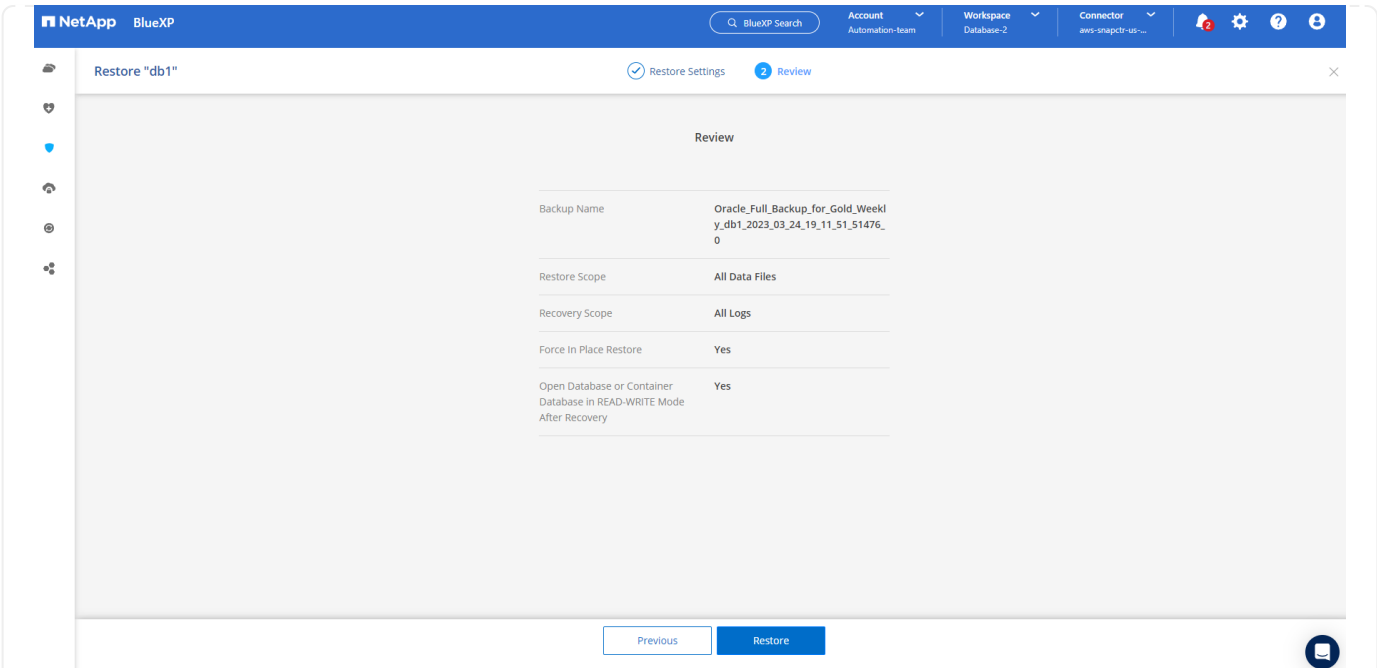
Recovery Scope

- All Logs
- Until System Change Number
- Date and Time
- No Recovery

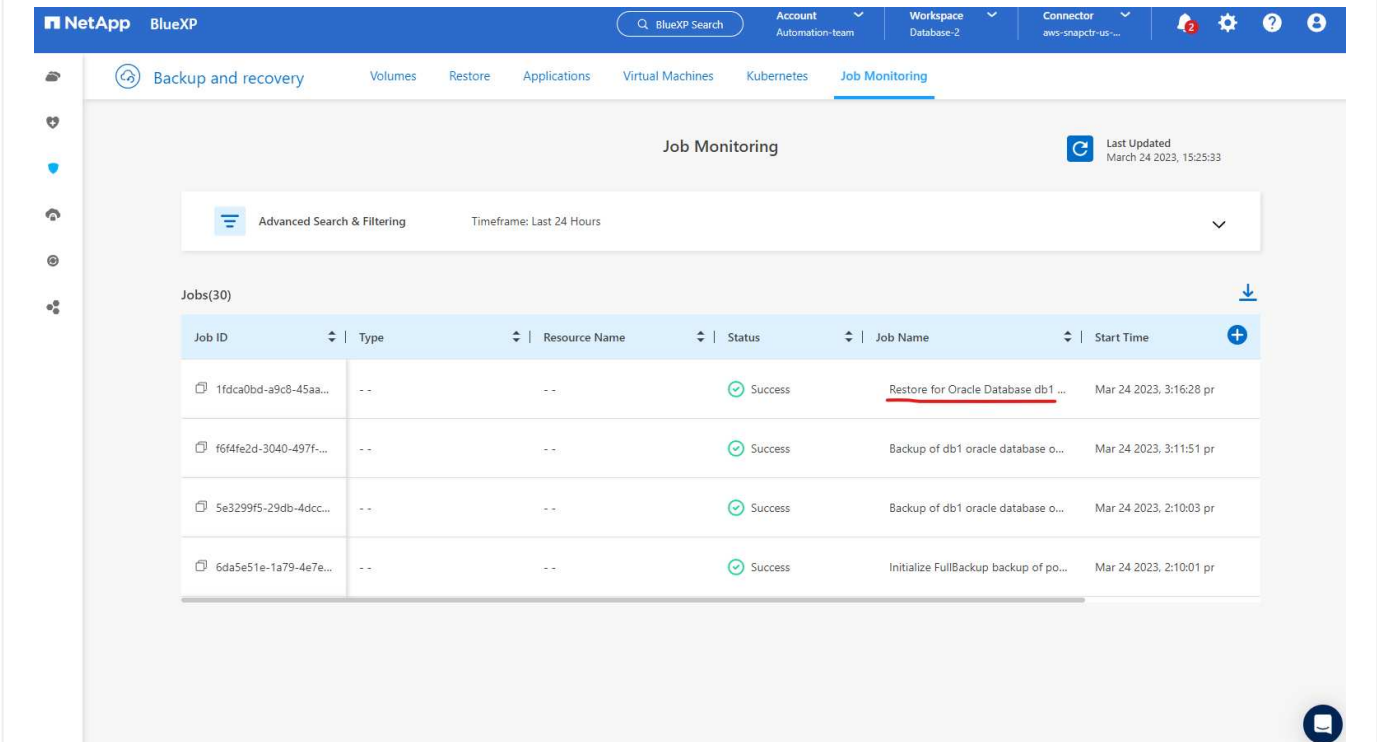
Archive Log Files Locations: /mnt/log_location001

Open the database or the container database in READ-WRITE mode after recovery.

1. Überprüfen und starten Sie die Datenbank-Wiederherstellung und -Wiederherstellung.



1. Auf der Registerkarte **Job-Überwachung** können Sie den Status des Wiederherstellungsjobs sowie alle Details anzeigen, während er ausgeführt wird.



NetApp BlueXP

Account Automation-team | Workspace Database-2 | Connector aws-snapctr-us-...

Backup and recovery | Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring

Job Monitoring > Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4

Job Details

Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4 Expand All

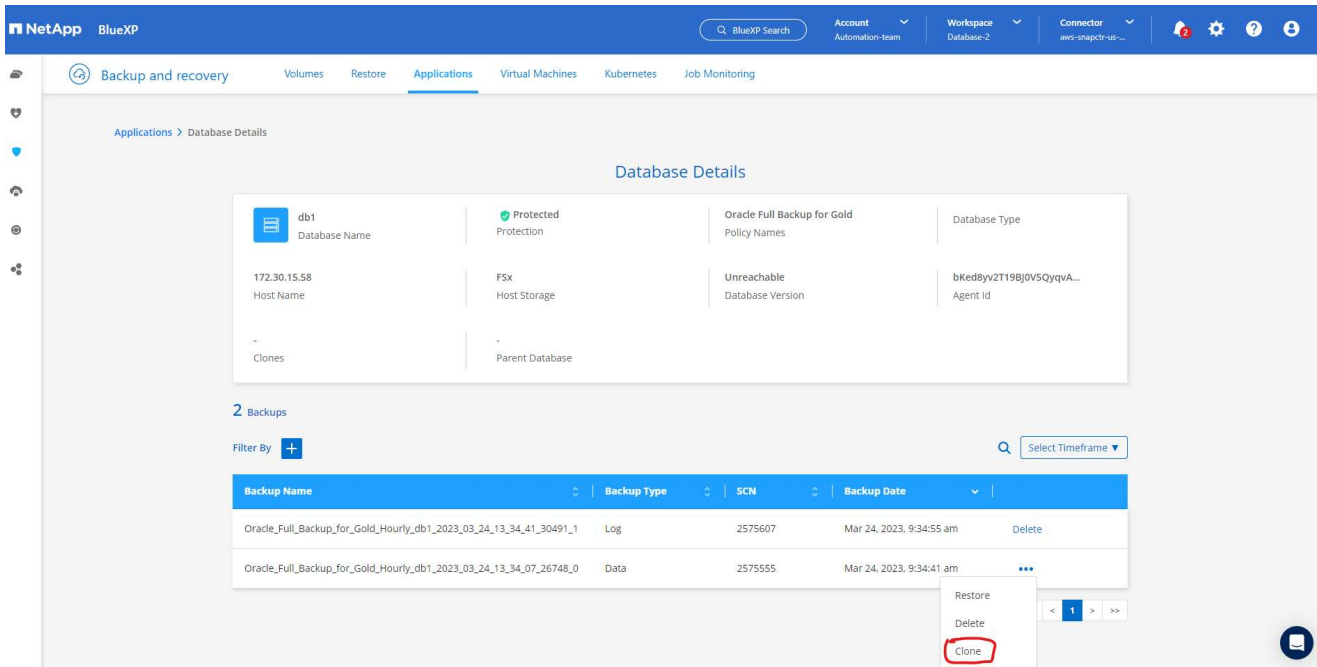
Sub-Jobs(6)

Job Name	Job ID	Start Time	End Time	Duration
Restore for Oracle Database db1 using backup ...	1fdca0bd-a9c8-45aa-9d...	Mar 24 2023, 3:16:28 pm	Mar 24 2023, 3:23:33 pm	7 Minutes
Post Restore Cleanup	2096a8e4-889d-4b2a-9...	Mar 24 2023, 3:23:18 pm	Mar 24 2023, 3:23:32 pm	14 Seconds
Post Restore	fb7b1171-966f-4228-9e...	Mar 24 2023, 3:20:06 pm	Mar 24 2023, 3:23:19 pm	3 Minutes
Restore	0f4580d0-6598-458b-a7...	Mar 24 2023, 3:17:49 pm	Mar 24 2023, 3:20:07 pm	2 Minutes

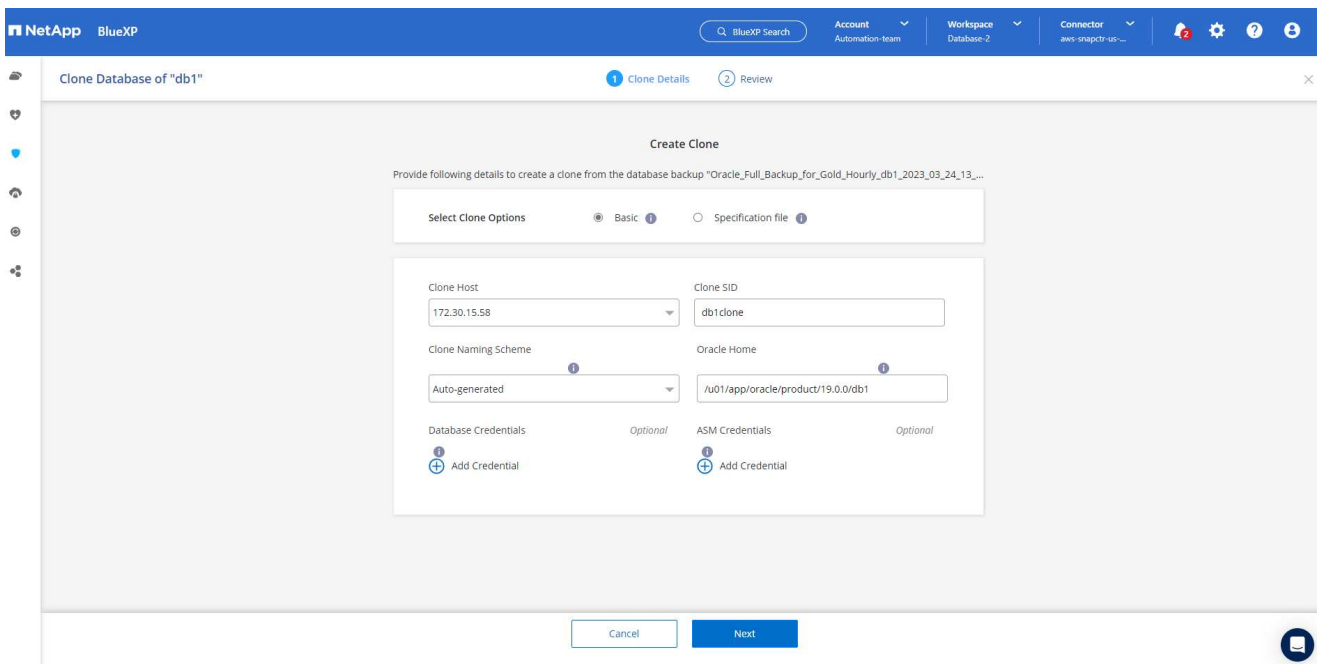
Klon einer Oracle Datenbank

Um eine Datenbank zu klonen, starten Sie den Klon-Workflow über dieselbe Seite mit den Details zum Datenbank-Backup.

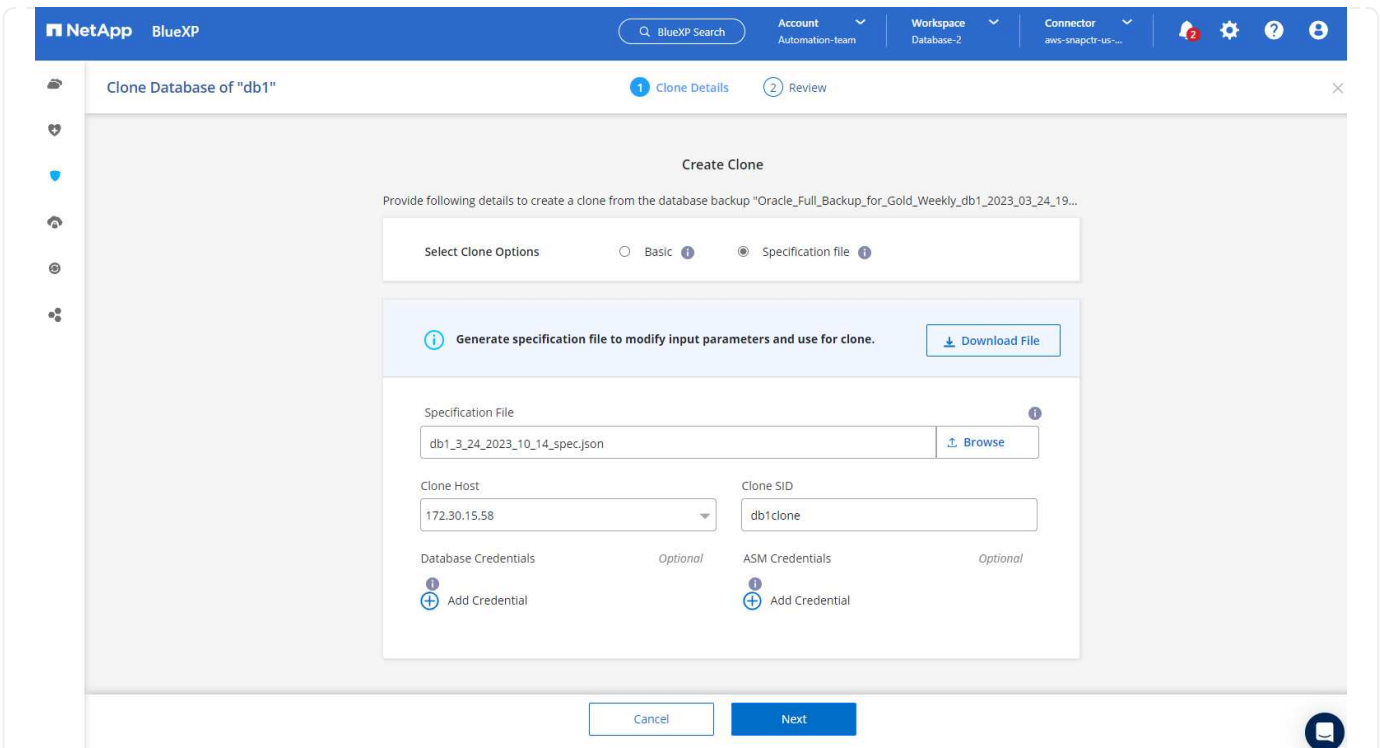
1. Wählen Sie die richtige Datenbank-Backup-Kopie, klicken Sie auf die drei Punkte, um das Menü anzuzeigen, und wählen Sie die Option **Clone**.



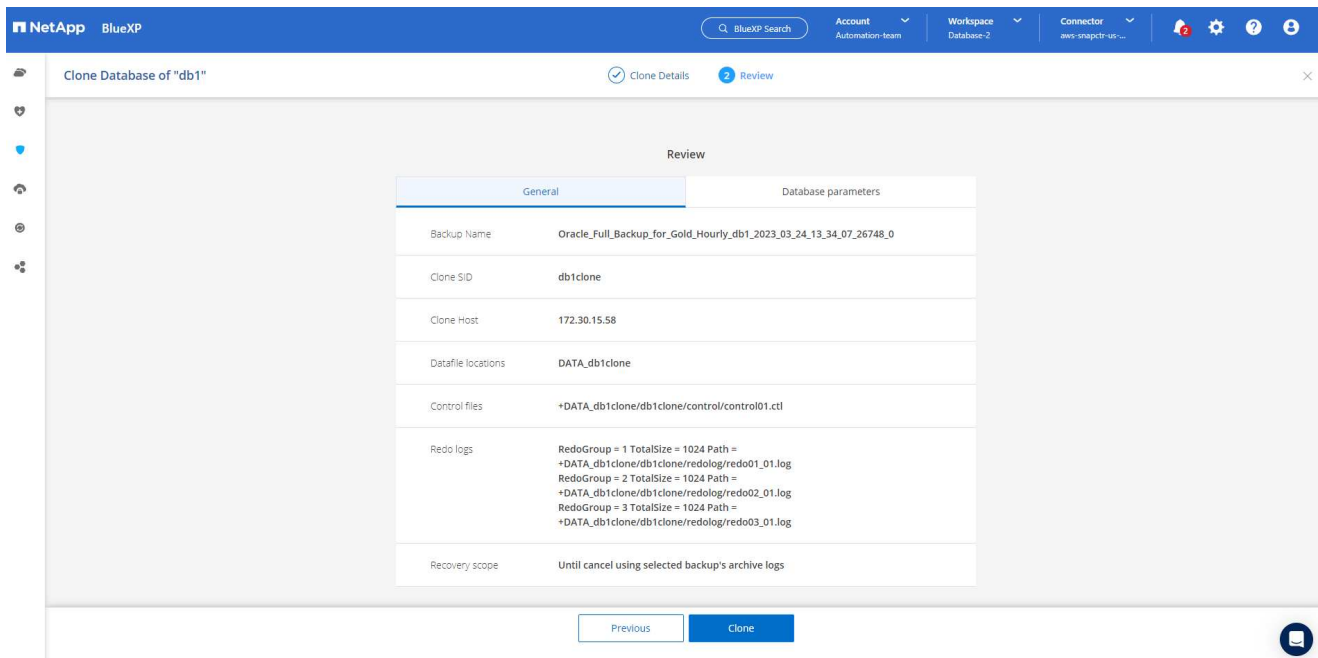
1. Wählen Sie die Option **Basic**, wenn Sie keine geklonten Datenbankparameter ändern müssen.



1. Alternativ können Sie **Specification file** auswählen, um die aktuelle init-Datei herunterzuladen, Änderungen vorzunehmen und sie dann wieder in den Job hochzuladen.



1. Überprüfen und starten Sie den Job.



1. Überwachen Sie den Status des Klonjobs über die Registerkarte **Job Monitoring**.

The screenshot displays the NetApp BlueXP interface for job monitoring. The top navigation bar includes the NetApp logo, a search bar, and dropdown menus for Account (Automation-team), Workspace (Database-2), and Connector (aws-snapc1r-1b...). The main content area is titled "Job Monitoring" and shows details for a specific job with ID "cd30abaf-fbe2-4052-a6db-4bf965a8d29b". The job details section, titled "Job Details", shows the job ID and an "Expand All" button. Below this, a table lists "Sub-Jobs(2)".

Job Name	Job ID	Start Time	End Time	Duration
Cloning Oracle Database db1 as db1clone on h...	cd30abaf-fbe2-4052-a6...	Mar 24 2023, 1:30:36 pm		--
Running pre scripts	511f52c1-853a-4ec6-a4f...	Mar 24 2023, 1:30:41 pm	Mar 24 2023, 1:30:41 pm	0 Second
Validating clone request	f93a6c44-2eb2-4c5e-9f...	Mar 24 2023, 1:30:35 pm	Mar 24 2023, 1:30:42 pm	7 Seconds

1. Validierung der geklonten Datenbank auf dem EC2 Instanzhost

```

#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
+ASM:/u01/app/oracle/product/19.0.0/grid:N
db1:/u01/app/oracle/product/19.0.0/db1:N
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
db1clone:/u01/app/oracle/product/19.0.0/db1:N
[oracle@ip-172-30-15-58 ~]$ crsctl stat res -t
-----
Name                Target  State        Server                    State details
-----
Local Resources
-----
ora.DATA.dg
      ONLINE  ONLINE      ip-172-30-15-58          STABLE
ora.DATA_DB1CLONE.dg
      ONLINE  ONLINE      ip-172-30-15-58          STABLE
ora.LISTENER.lsnr
      ONLINE  ONLINE      ip-172-30-15-58          STABLE
ora.LOGS.dg
      ONLINE  ONLINE      ip-172-30-15-58          STABLE
ora.LOGS_SCO_2748138658.dg
      ONLINE  ONLINE      ip-172-30-15-58          STABLE
ora.asm
      ONLINE  ONLINE      ip-172-30-15-58          Started,STABLE
ora.ons
      OFFLINE OFFLINE      ip-172-30-15-58          STABLE
-----
Cluster Resources
-----
ora.cssd
      1        ONLINE  ONLINE      ip-172-30-15-58          STABLE
ora.db1.db
      1        ONLINE  ONLINE      ip-172-30-15-58          Open,HOME=/u01/app/oracle/product/19.0.0/db1,STABLE
ora.db1clone.db
      1        ONLINE  ONLINE      ip-172-30-15-58          Open,HOME=/u01/app/oracle/product/19.0.0/db1,STABLE
ora.diskmon
      1        OFFLINE OFFLINE
      STABLE
ora.driver.afd
      1        ONLINE  ONLINE      ip-172-30-15-58          STABLE
ora.evmd
      1        ONLINE  ONLINE      ip-172-30-15-58          STABLE
-----
[oracle@ip-172-30-15-58 ~]$ █

```

```

[oracle@ip-172-30-15-58 ~]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
[oracle@ip-172-30-15-58 ~]$ export ORACLE_SID=db1clone
[oracle@ip-172-30-15-58 ~]$ export PATH=$ORACLE_HOME/bin:$PATH
[oracle@ip-172-30-15-58 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Mar 24 18:32:21 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.18.0.0.0

SQL> select name, open_mode from v$databases;

NAME                OPEN_MODE
-----
DB1CLONE            READ WRITE

SQL> █

```

Weitere Informationen

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- Richten Sie BlueXP ein und verwalten Sie sie

["https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html"](https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html)

- BlueXP Backup- und Recovery-Dokumentation

["https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html"](https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html)

- Amazon FSX für NetApp ONTAP

["https://aws.amazon.com/fsx/netapp-ontap/"](https://aws.amazon.com/fsx/netapp-ontap/)

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

Hybrid-Cloud-Datenbanklösungen mit SnapCenter

TR-4908: Übersicht zu Hybrid-Cloud-Datenbanklösungen mit SnapCenter

Alan Cao, Felix Melligan, NetApp

Diese Lösung bietet Außendienstmitarbeiter und Kunden Anweisungen und Anleitungen für die Konfiguration, den Betrieb und die Migration von Datenbanken in eine Hybrid-Cloud-Umgebung mithilfe des GUI-basierten NetApp SnapCenter Tools und des NetApp Storage-Service CVO in Public Clouds, um in folgenden Fällen verfügbar zu machen:

- Entwicklungs-/Testprozesse für Datenbanken in der Hybrid Cloud
- Datenbank-Disaster-Recovery in der Hybrid Cloud

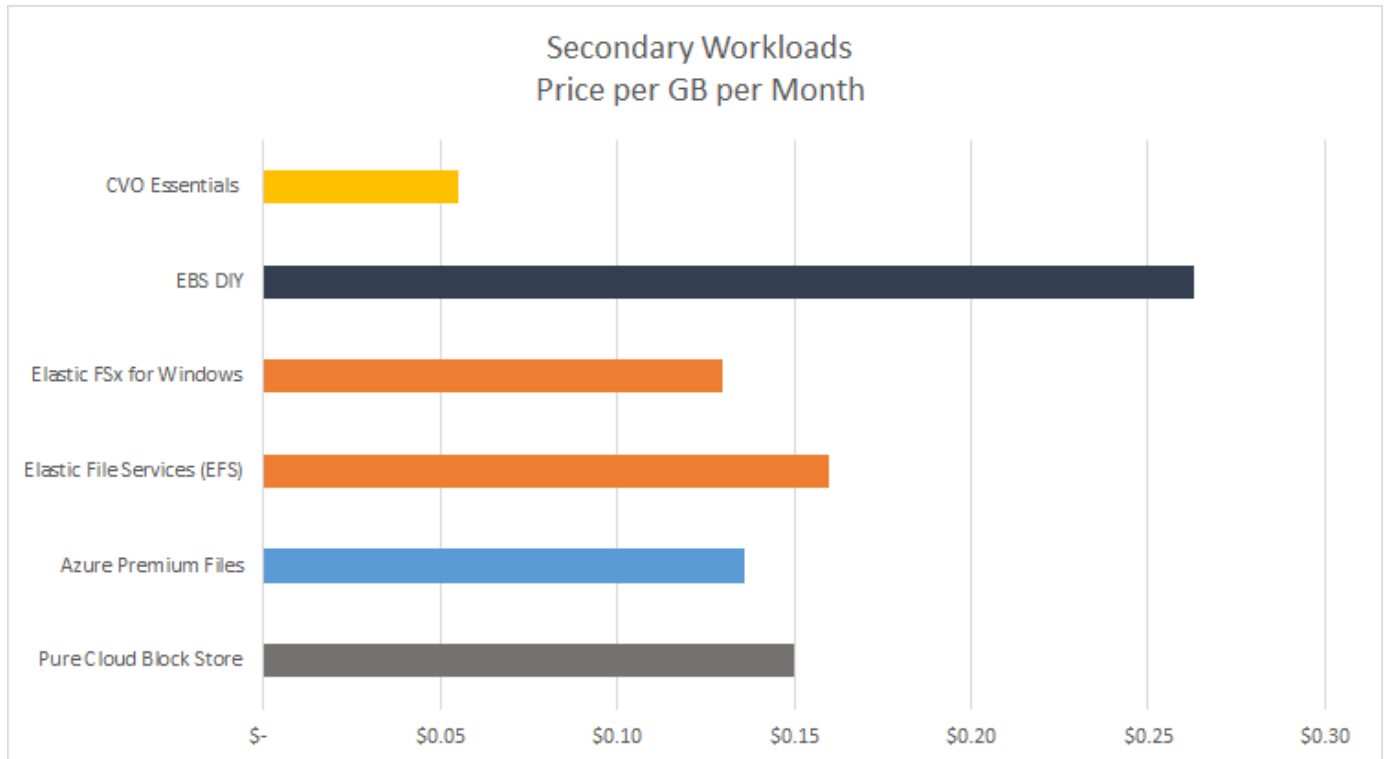
Heute befinden sich viele Enterprise-Datenbanken aus Performance-, Sicherheits- und anderen Gründen immer noch in privaten Datacentern eines Unternehmens. Diese Hybrid-Cloud-Datenbanklösung ermöglicht Unternehmen, ihre primären Datenbanken vor Ort zu betreiben und gleichzeitig eine Public Cloud für Test- und Entwicklungsdatenbanken zu nutzen sowie Disaster Recovery zu nutzen, um die Lizenz- und Betriebskosten zu senken.

Viele Enterprise-Datenbanken wie Oracle, SQL Server, SAP HANA usw. Hohe Lizenz- und Betriebskosten Viele Kunden zahlen eine einmalige Lizenzgebühr sowie jährliche Support-Kosten, die auf der Anzahl der Computing-Kerne in ihrer Datenbankumgebung basieren und unabhängig davon, ob die Kerne für Entwicklung, Tests, Produktion oder Disaster Recovery verwendet werden. Viele dieser Umgebungen sind möglicherweise nicht während des gesamten Applikationslebenszyklus vollständig ausgelastet.

Die Lösungen bieten Kunden die Möglichkeit, die Anzahl ihrer lizenzierbaren Kerne zu reduzieren, indem sie ihre Datenbankumgebungen für Entwicklung, Tests oder Disaster Recovery in die Cloud verschieben. Durch den Einsatz von Skalierbarkeit, Redundanz, Hochverfügbarkeit und einer nutzungsbasierten Abrechnung auf Basis von Public Clouds können Lizenzgebühren und Betriebsabläufe erheblich gesenkt werden, ohne dabei

die Benutzerfreundlichkeit oder Verfügbarkeit der Applikationen zu beeinträchtigen.

Neben den potenziellen Einsparungen bei Datenbanklizenzkosten ermöglicht das kapazitätsbasierte CVO Lizenzmodell von NetApp Kunden, Storage-Kosten pro GB zu sparen. Gleichzeitig profitieren sie von einem hohen Maß an Datenbankverwaltung, das in den Storage-Services anderer Anbieter nicht möglich ist. Das folgende Diagramm zeigt einen Storage-Kostenvergleich für gängige Storage-Services, die in der Public Cloud verfügbar sind.



Die Lösung zeigt, dass mithilfe des GUI-basierten Software-Tools SnapCenter und der NetApp SnapMirror Technologie Hybrid-Cloud-Datenbankvorgänge einfach eingerichtet, implementiert und betrieben werden können.

SnapCenter wird in der Praxis in den folgenden Videos gezeigt:

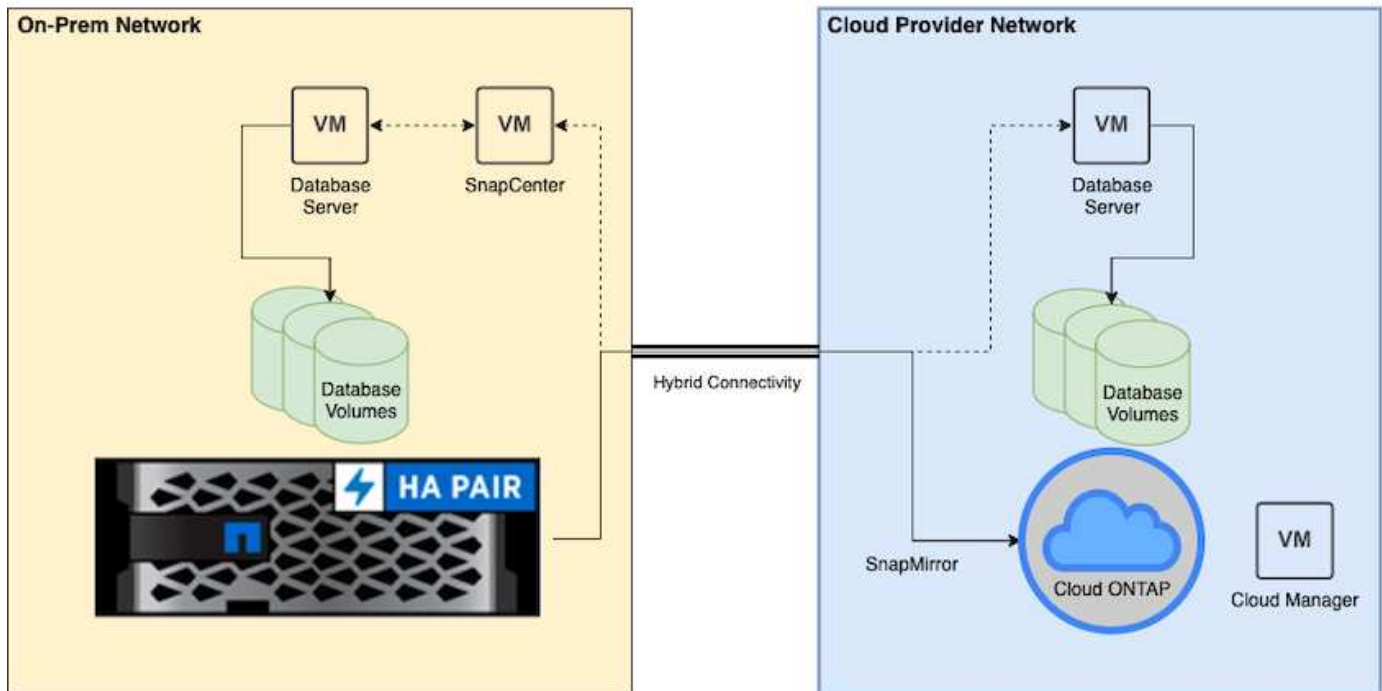
- ["Backup einer Oracle-Datenbank in einer Hybrid Cloud mit SnapCenter"](#)
- ["SnapCenter – KLONEN SIE ENTWICKLUNG/TEST für eine Oracle Datenbank in AWS Cloud"](#)

Zwar zeigen die Abbildungen in diesem Dokument zeigen CVO als Ziel-Storage-Instanz in der Public Cloud, doch ist die Lösung auch für die neue Version der FSX ONTAP Storage-Engine für AWS vollständig validiert.

Ein NetApp Lab-on-Demand SL10680 kann über folgenden Link angefordert werden: [TL_AWS_004 HCoD: AWS - NW, SnapCenter \(OnPrem\)](#).

Lösungsarchitektur

Das folgende Architekturdiagramm zeigt eine typische Implementierung von Unternehmensdatenbankvorgängen in einer Hybrid Cloud für Entwicklungs-/Test- und Disaster-Recovery-Vorgänge.



Im normalen Geschäftsbetrieb können synchronisierte Datenbank-Volumes in der Cloud geklont und in Entwicklungs-/Testdatenbankinstanzen für Applikationen zum entwickeln oder Testen gemountet werden. Bei einem Ausfall können die synchronisierten Datenbank-Volumes in der Cloud dann für die Disaster Recovery aktiviert werden.

SnapCenter-Anforderungen erfüllt

Die Lösung wurde für eine Hybrid-Cloud-Einstellung entwickelt, um On-Premises-Produktionsdatenbanken zu unterstützen, die für Entwicklungs-/Test- und Disaster-Recovery-Vorgänge einen Burst in die gängigen Public Clouds ausführen können.

Diese Lösung unterstützt alle Datenbanken, die derzeit von SnapCenter unterstützt werden, obwohl hier nur Oracle- und SQL Server-Datenbanken gezeigt werden. Diese Lösung wurde mit virtualisierten Datenbank-Workloads validiert, obwohl auch Bare-Metal-Workloads unterstützt werden.

Wir gehen davon aus, dass die produktiven Datenbankserver On-Premises mit DB-Volumes gehostet werden, die von einem ONTAP-Storage-Cluster an DB-Hosts präsentiert werden. SnapCenter Software wird lokal für Datenbank-Backups und Datenreplizierung in die Cloud installiert. Ein Ansible-Controller wird empfohlen, ist aber nicht für eine Automatisierung der Datenbankbereitstellung erforderlich, oder für eine Synchronisierung des OS-Kernels und der DB-Konfiguration mit einer Standby-DR-Instanz oder Entwicklungs-/Testinstanzen in der Public Cloud.

Anforderungen

Umgebung	Anforderungen
Auf dem Gelände	Alle Datenbanken und Versionen, die von SnapCenter unterstützt werden
	SnapCenter Version 4.4 oder höher
	Ansible Version 2.09 oder höher
	ONTAP Cluster 9.x
	Intercluster LIFs konfiguriert
	Konnektivität von On-Premises zu einer Cloud-VPC (VPN, Interconnect usw.)
	Netzwerkports offen - ssh 22 - tcp 8145, 8146, 10000, 11104, 11105
Cloud - AWS	"Cloud Manager Connector"
	"Cloud Volumes ONTAP"
	Zuordnen von DB-OS-EC2-Instanzen zu On-Premises
Cloud - Azure	"Cloud Manager Connector"
	"Cloud Volumes ONTAP"
	Abgleich von DB OS Azure Virtual Machines mit On-Premises
Cloud - GCP	"Cloud Manager Connector"
	"Cloud Volumes ONTAP"
	Abgleich von DB OS Google Compute Engine Instanzen mit On-Premises

Konfiguration der Voraussetzungen

Bestimmte Voraussetzungen müssen sowohl On-Premises als auch in der Cloud konfiguriert werden, bevor die Ausführung von Hybrid-Cloud-Datenbank-Workloads ausgeführt wird. Der folgende Abschnitt bietet einen allgemeinen Überblick über diesen Prozess und die folgenden Links führen zu weiteren Informationen über die erforderliche Systemkonfiguration.

On-Premises

- Installation und Konfiguration von SnapCenter
- Storage-Konfiguration des lokalen Datenbankservers
- Lizenzierungsanforderungen
- Networking und Sicherheit
- Automatisierung

Public Cloud

- NetApp Cloud Central Anmeldung
- Netzwerkzugriff über einen Webbrowser zu mehreren Endpunkten
- Ein Netzwerkspeicherort für einen Anschluss
- Berechtigungen für Cloud-Provider

- Vernetzung für einzelne Services

Wichtige Überlegungen:

1. Wo wird der Cloud Manager Connector bereitgestellt?
2. Sizing und Architektur für Cloud Volume ONTAP
3. Single Node oder Hochverfügbarkeit?

Die folgenden Links bieten weitere Einzelheiten:

["On-Premises"](#)

["Public Cloud"](#)

Voraussetzungen vor Ort

Die folgenden Aufgaben müssen vor Ort ausgeführt werden, um die SnapCenter Hybrid-Cloud-Datenbank-Workload-Umgebung vorzubereiten.

Installation und Konfiguration von SnapCenter

Das NetApp SnapCenter Tool ist eine auf Windows basierende Applikation, die normalerweise in einer Windows Domain-Umgebung ausgeführt wird, obwohl auch eine Implementierung von Arbeitsgruppen möglich ist. Sie basiert auf einer Multi-Tier-Architektur, die einen zentralen Management-Server (den SnapCenter Server) sowie ein SnapCenter-Plug-in auf den Datenbank-Server-Hosts für Datenbank-Workloads umfasst. Folgende wichtige Aspekte sollten bei der Implementierung der Hybrid Cloud beachtet werden:

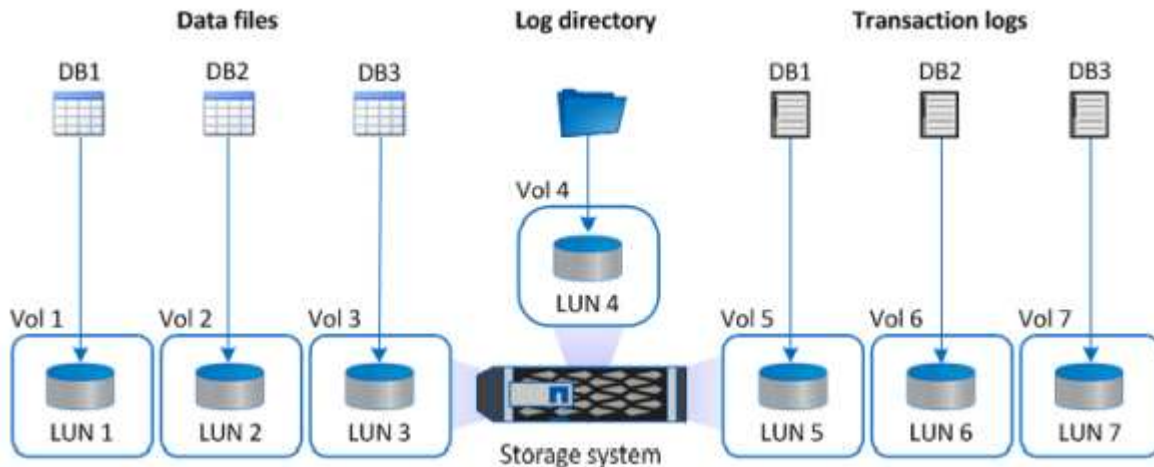
- **Single Instance oder HA-Bereitstellung.** HA-Bereitstellung bietet Redundanz bei Ausfall eines SnapCenter-Instanz-Servers.
- **Namensauflösung.** DNS muss auf dem SnapCenter-Server konfiguriert sein, um alle Datenbank-Hosts sowie auf der Speicher-SVM aufzulösen, damit die Suche vorwärts und rückwärts ausgeführt werden kann. DNS muss auch auf Datenbankservern konfiguriert werden, um den SnapCenter-Server und die Storage-SVM für die vorwärts und rückwärts Suche zu lösen.
- **Rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC)-Konfiguration.** für gemischte Datenbank-Workloads sollten Sie die RBAC verwenden, um die Management-Verantwortung für verschiedene DB-Plattformen zu verteilen, z. B. einen Administrator für Oracle Database oder einen Administrator für SQL Server. Für den DB-Admin-Benutzer müssen die erforderlichen Berechtigungen erteilt werden.
- **Ermöglicht eine richtlinienbasierte Backup-Strategie.** zur Durchsetzung der Backup-Konsistenz und -Zuverlässigkeit.
- **Öffnen Sie erforderliche Netzwerkanschlüsse an der Firewall.** damit der On-Premise SnapCenter Server mit Agenten kommunizieren kann, die im Cloud DB-Host installiert sind.
- **Die Ports müssen offen sein, um SnapMirror Traffic zwischen On-Premises und Public Cloud zu ermöglichen.** der SnapCenter Server nutzt ONTAP SnapMirror zur Replizierung von Snapshot Backups vor Ort in Cloud-CVO Storage-SVMs.

Klicken Sie nach sorgfältiger Planung und Prüfung vor der Installation auf diese Schaltfläche ["SnapCenter Installations-Workflow"](#) Einzelheiten zur Installation und Konfiguration von SnapCenter finden Sie im Dokument.

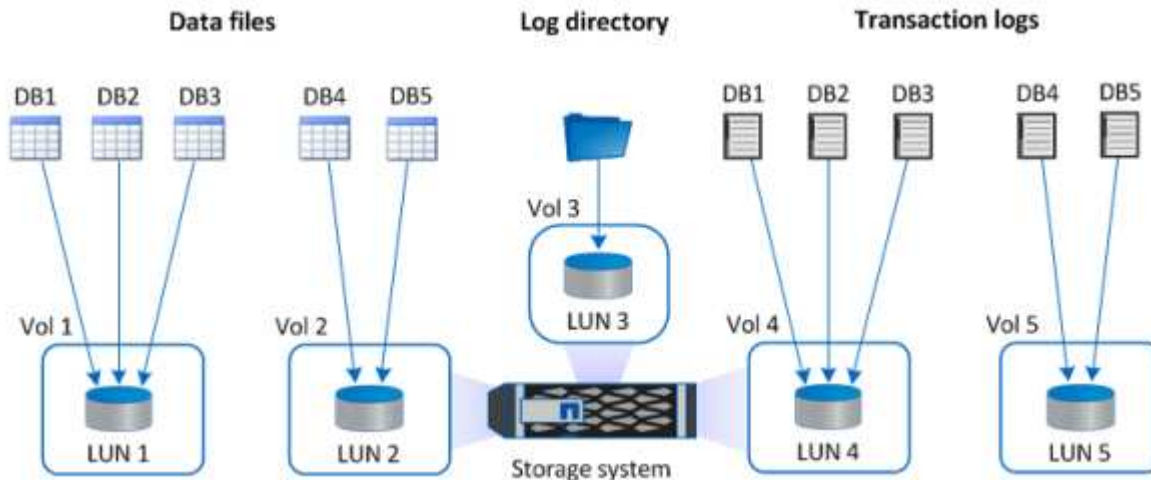
Storage-Konfiguration des lokalen Datenbankservers

Die Storage-Performance spielt für die Gesamt-Performance von Datenbanken und Applikationen eine wichtige Rolle. Mit einem gut durchdachten Storage-Layout kann nicht nur die Datenbank-Performance verbessert werden, sondern auch das Management von Datenbank-Backup und -Recovery vereinfacht wird. Bei der Definition des Storage-Layouts sind mehrere Faktoren zu berücksichtigen. Dazu gehören die Größe der Datenbank, die erwartete Datenänderung der Datenbank und die Häufigkeit der Backups.

Das direkte Anbinden von Storage-LUNs an die Gast-VM entweder über NFS oder iSCSI für virtualisierte Datenbank-Workloads liefert im Allgemeinen eine bessere Performance als über VMDK zugewiesener Storage. NetApp empfiehlt das Storage-Layout für eine große SQL Server Datenbank auf LUNs, die in der folgenden Abbildung dargestellt sind.



Die folgende Abbildung zeigt das von NetApp empfohlene Storage-Layout für kleine oder mittlere SQL Server-Datenbank auf LUNs.



Das Log-Verzeichnis ist SnapCenter dediziert, um Transaktions-Log-Rollup für Datenbank-Recovery durchzuführen. Für eine besonders große Datenbank können einem Volume mehrere LUNs zugewiesen werden, um eine bessere Performance zu erzielen.

Bei Oracle-Datenbank-Workloads unterstützt SnapCenter Datenbankumgebungen, die über ONTAP Storage gesichert sind, die als physische oder virtuelle Geräte auf dem Host gemountet werden. Je nach Wichtigkeit der Umgebung können Sie die gesamte Datenbank auf einem einzigen oder mehreren Storage-Geräten

hosten. In der Regel isolieren Kunden Datendateien im dedizierten Storage von allen anderen Dateien, z. B. Kontrolldateien, Wiederherstellungsdateien und Archivprotokolldateien. So sind Administratoren in ONTAP der Lage, in wenigen Sekunden oder Minuten eine große kritische Datenbank (Petabyte-Größe) mit Snapshot Technologie wiederherzustellen (Single-File SnapRestore) oder zu klonen.



Für geschäftskritische Workloads, die von der Latenz abhängig sind, sollte ein dediziertes Storage Volume auf verschiedene Arten von Oracle Dateien implementiert werden, um die bestmögliche Latenz zu erzielen. Bei einer großen Datenbank sollten mehrere LUNs (NetApp empfiehlt bis zu acht) pro Volume Datendateien zugewiesen werden.



Bei kleineren Oracle Datenbanken unterstützt SnapCenter Shared-Storage-Layouts, in denen mehrere Datenbanken oder Teile einer Datenbank auf demselben Storage-Volume oder derselben LUN gehostet werden können. Als Beispiel für dieses Layout können Sie Datendateien für alle Datenbanken auf einer +DATA ASM Laufwerksgruppe oder einer Volume-Gruppe hosten. Der Rest der Dateien (Redo-, Archivprotokoll- und Kontrolldateien) kann auf einer anderen dedizierten Laufwerksgruppe oder Volume-Gruppe (LVM) gehostet werden. Ein solches Implementierungsszenario wird im Folgenden dargestellt.



Um die Verschiebung von Oracle Datenbanken zu erleichtern, sollte Oracle-Binärdatei auf einer separaten LUN installiert werden, die in der regelmäßigen Backup-Richtlinie enthalten ist. So wird sichergestellt, dass bei der Datenbankverschiebung zu einem neuen Serverhost der Oracle Stack für eine Recovery ohne potenzielle Probleme aufgrund einer aus der Synchronisierung bestehenden Oracle-Binärdatei gestartet werden kann.

Lizenzierungsanforderungen

SnapCenter ist eine lizenzierte Software von NetApp. Sie ist im Allgemeinen in einer ONTAP Lizenz vor Ort enthalten. Bei der Hybrid-Cloud-Implementierung ist jedoch auch eine Cloud-Lizenz für SnapCenter erforderlich, um CVO zu SnapCenter als Ziel-Datenreplizierungsziel zu hinzufügen. Weitere Informationen erhalten Sie unter folgenden Links zu der kapazitätsbasierten SnapCenter Standardlizenz:

Networking und Sicherheit

Wenn ein hybrider Datenbankbetrieb eine lokale Produktionsdatenbank benötigt, die nicht stabil in der Cloud für Entwicklung/Test und Disaster Recovery ist, müssen Netzwerke und Sicherheit beim Einrichten der Umgebung sowie die Verbindung zur Public Cloud aus einem lokalen Datacenter berücksichtigt werden.

Public Clouds verwenden in der Regel eine Virtual Private Cloud (VPC), um verschiedene Benutzer innerhalb einer Public-Cloud-Plattform zu isolieren. Innerhalb eines individuellen VPC wird die Sicherheit mithilfe von Maßnahmen wie Sicherheitsgruppen gesteuert, die je nach Benutzeranforderungen für die Sperrung eines VPC konfiguriert werden können.

Die Konnektivität vom lokalen Datacenter zur VPC kann über einen VPN-Tunnel gesichert werden. Auf dem VPN-Gateway kann die Sicherheit durch NAT- und Firewall-Regeln, die Versuche blockieren, Netzwerkverbindungen von Hosts im Internet zu Hosts im unternehmenseigenen Rechenzentrum herzustellen, abgehärtet werden.

Networking- und Sicherheitsaspekte finden Sie in den relevanten ein- und ausgehenden CVO-Regeln für die beliebige Public Cloud:

- ["Regeln für Sicherheitsgruppen für CVO – AWS"](#)
- ["Regeln für Sicherheitsgruppen für CVO – Azure"](#)
- ["Firewall-Regeln für CVO - GCP"](#)

Nutzung von Ansible-Automatisierung zur Synchronisierung von DB-Instanzen zwischen On-Premises und der Cloud – optional

Um das Management einer Hybrid-Cloud-Datenbankumgebung zu vereinfachen, empfiehlt NetApp unbedingt den Einsatz eines Ansible-Controllers, um einige Managementaufgaben zu automatisieren, z. B. um Computing-Instanzen lokal und in der Cloud synchron zu halten. Dies ist besonders wichtig, da eine Out-of-Sync-Computing-Instanz in der Cloud die wiederhergestellte Datenbank im Cloud-Fehler aufgrund fehlender Kernel-Pakete und anderer Probleme anfällig machen könnte.

Mit den Automatisierungsfunktionen eines Ansible-Controllers lässt sich SnapCenter für bestimmte Aufgaben erweitern, beispielsweise durch Aufbrechen der SnapMirror Instanz zur Aktivierung der DR-Datenkopie für die Produktion.

Folgen Sie diesen Anweisungen, um Ihren Ansible-Steuerungsknoten für RedHat- oder CentOS-Maschinen einzurichten: ["Redhat/CentOS Ansible Controller-Setup"](#).

Befolgen Sie diese Anweisungen, um Ihren Ansible-Steuerungsknoten für Ubuntu oder Debian-Maschinen einzurichten: ["Ubuntu/Debian Ansible-Controller-Setup"](#).

Voraussetzungen für die Public Cloud

Bevor wir den Cloud Manager Connector installieren und Cloud Volumes ONTAP konfigurieren und SnapMirror konfigurieren, müssen wir einige Vorbereitungen für unsere Cloud-Umgebung durchführen. Auf dieser Seite werden die erforderlichen Arbeiten sowie die Überlegungen bei der Implementierung von Cloud Volumes ONTAP beschrieben.

Checkliste zu den Implementierungsvoraussetzungen für Cloud Manager und Cloud Volumes ONTAP

- NetApp Cloud Central Anmeldung

- Netzwerkzugriff über einen Webbrowser zu mehreren Endpunkten
- Ein Netzwerkstandort für einen Konnektor
- Berechtigungen für Cloud-Provider
- Vernetzung für einzelne Services

Weitere Informationen zu den ersten Schritten erhalten Sie auf unserer ["Cloud-Dokumentation"](#).

Überlegungen

1. Was ist ein Cloud-Manager-Konnektor?

In den meisten Fällen muss ein Cloud Central Account-Administrator einen Connector in Ihrer Cloud oder Ihrem On-Premises-Netzwerk bereitstellen. Über den Connector kann Cloud Manager Ressourcen und Prozesse in Ihrer Public-Cloud-Umgebung managen.

Weitere Informationen zu Connectors finden Sie auf unserer ["Cloud-Dokumentation"](#).

2. Dimensionierung und Architektur von Cloud Volumes ONTAP

Bei der Bereitstellung von Cloud Volumes ONTAP haben Sie die Wahl zwischen einem vordefinierten Paket oder der Erstellung Ihrer eigenen Konfiguration. Obwohl sich viele dieser Werte später unterbrechungsfrei ändern lassen, müssen vor der Implementierung auf der Grundlage der zu implementierenden Workloads in der Cloud einige wichtige Entscheidungen getroffen werden.

Jeder Cloud-Provider verfügt über unterschiedliche Implementierungsmöglichkeiten, und fast jeder Workload verfügt über eigene einzigartige Eigenschaften. NetApp hat eine ["CVO-Sizing-Tool"](#) Damit können Implementierungen auf der Basis von Kapazität und Performance korrekt ausgerichtet werden. Allerdings basieren sie auf einigen grundlegenden Konzepten, die sich lohnen:

- Erforderliche Kapazität
- Netzwerkfähigkeit der Cloud Virtual Machine
- Performance-Merkmale von Cloud-Storage

Entscheidend ist dabei die Planung einer Konfiguration, die nicht nur die aktuellen Kapazitäts- und Performance-Anforderungen erfüllt, sondern auch das künftige Wachstum berücksichtigt. Dies wird im Allgemeinen als Kapazitätsreserve und Performance Reserve bezeichnet.

Wenn Sie weitere Informationen wünschen, lesen Sie die Dokumentation zur Planung richtig für ["AWS"](#), ["Azure"](#), und ["GCP"](#).

3. Single Node oder Hochverfügbarkeit?

In allen Clouds besteht die Möglichkeit, CVO entweder in einem einzelnen Node oder in einem hochverfügbaren Cluster-Paar mit zwei Nodes zu implementieren. Je nach Anwendungsfall können Sie einen einzelnen Node implementieren, um Kosten zu sparen, oder ein HA-Paar, um weitere Verfügbarkeit und Redundanz zu ermöglichen.

Einzelne Nodes sind für einen DR-Anwendungsfall oder das Aufsetzen von temporemem Storage für Entwicklung und Tests häufig vorgängig, da die Auswirkungen eines plötzlichen zonalen beziehungsweise Infrastrukturausfalls geringer sind. Wenn sich die Daten jedoch in einem Produktionsfall nur an einem einzelnen Standort befinden oder wenn der Datensatz mehr Redundanz und Verfügbarkeit haben muss, wird Hochverfügbarkeit empfohlen.

Weitere Informationen zur Architektur der Hochverfügbarkeit der einzelnen Cloud-Versionen finden Sie in der Dokumentation für ["AWS"](#), ["Azure"](#) Und ["GCP"](#).

Erste Schritte – Übersicht

Dieser Abschnitt enthält eine Zusammenfassung der Aufgaben, die erfüllt werden müssen, um die Anforderungen zu erfüllen, wie im vorherigen Abschnitt beschrieben. Der folgende Abschnitt enthält eine allgemeine Aufgabenliste für den Betrieb am Standort sowie in der Public Cloud. Auf die detaillierten Prozesse und Verfahren kann durch Anklicken der entsprechenden Links zugegriffen werden.

On-Premises

- Einrichten des Datenbank-Admin-Benutzers in SnapCenter
- Installationsvoraussetzungen für das SnapCenter Plug-in
- SnapCenter Host Plug-in-Installation
- DB-Ressourcenerkennung
- Storage-Cluster-Peering und DB-Volume-Replizierung einrichten
- Fügen Sie die CVO Datenbank-Storage-SVM zu SnapCenter hinzu
- Backup-Richtlinie für Datenbanken in SnapCenter einrichten
- Backup-Richtlinie zum Schutz der Datenbank implementieren
- Backup validieren

AWS Public Cloud

- Scheck vor dem Flug
- Schritte zur Implementierung von Cloud Manager und Cloud Volumes ONTAP in AWS
- Implementieren Sie EC2 Computing-Instanz für Datenbank-Workloads

Details finden Sie unter folgenden Links:

["On-Premises"](#), ["Public Cloud – AWS"](#)

Erste Schritte vor Ort

Das NetApp SnapCenter Tool verwendet die rollenbasierte Zugriffssteuerung (RBAC) zum Management der Benutzerressourcen für den Zugriff und die Berechtigungszuschüsse. SnapCenter Installationen erstellen vorbestückte Rollen. Sie können auch benutzerdefinierte Rollen erstellen, die Ihren Anforderungen oder Applikationen entsprechen.

On-Premises

1. Einrichten Datenbank Admin Benutzer in SnapCenter

Es ist sinnvoll, eine dedizierte Admin-Benutzer-ID für jede von SnapCenter unterstützte Datenbankplattform zur Sicherung, Wiederherstellung und/oder Disaster Recovery von Datenbanken zu haben. Sie können auch eine einzige ID zum Managen aller Datenbanken verwenden. In unseren Test-Cases und Demos haben wir für

Oracle und SQL Server einen dedizierten Admin-Benutzer erstellt.

Bestimmte SnapCenter Ressourcen können nur mit der Funktion „SnapCenterAdmin“ bereitgestellt werden. Ressourcen können dann anderen Benutzer-IDs für den Zugriff zugewiesen werden.

In einer vorkonfigurierten und konfigurierten lokalen SnapCenter-Umgebung wurden möglicherweise die folgenden Aufgaben bereits ausgeführt. Wenn nicht, erstellen Sie mit den folgenden Schritten einen Datenbank-Admin-Benutzer:

1. Fügen Sie den Admin-Benutzer zu Windows Active Directory hinzu.
2. Melden SnapCenter Sie sich mit einer ID an, die mit der SnapCenterAdmin-Rolle erteilt wurde.
3. Navigieren Sie zur Registerkarte Zugriff unter Einstellungen und Benutzer, und klicken Sie auf Hinzufügen, um einen neuen Benutzer hinzuzufügen. Die neue Benutzer-ID ist mit dem in Windows Active Directory in Schritt 1 erstellten Admin-Benutzer verknüpft. . Weisen Sie dem Benutzer nach Bedarf die richtige Rolle zu. Weisen Sie dem Admin-Benutzer nach Bedarf Ressourcen zu.

<input type="checkbox"/>	Name	Type	Roles	Domain
<input type="checkbox"/>	administrator	User	SnapCenterAdmin	demo
<input type="checkbox"/>	oradba	User	App Backup and Clone Admin	demo
<input type="checkbox"/>	sqldba	User	App Backup and Clone Admin	demo

2. Installationsvoraussetzungen für das SnapCenter Plugin

SnapCenter führt Backup, Wiederherstellung, Klonen und weitere Funktionen mithilfe eines Plug-in-Agenten aus, der auf den DB-Hosts ausgeführt wird. Er verbindet sich mit dem Datenbank-Host und der Datenbank über Anmeldeinformationen, die unter der Registerkarte Einstellungen und Anmeldeinformationen für die Plugin-Installation und andere Verwaltungsfunktionen konfiguriert sind. Es gibt spezielle Berechtigungsanforderungen auf der Grundlage des Ziel-Host-Typs, wie Linux oder Windows, sowie der Datenbanktyp.

DB Hosts die Zugangsdaten müssen vor der SnapCenter Plugin-Installation konfiguriert werden. In der Regel möchten Sie ein Administrator-Benutzerkonto auf dem DB-Host als Ihre Host-Verbindungsdaten für die Plugin-Installation verwenden. Sie können auch dieselbe Benutzer-ID für den Datenbankzugriff über die BS-basierte Authentifizierung gewähren. Auf der anderen Seite können Sie auch Datenbank-Authentifizierung mit verschiedenen Datenbank-Benutzer-IDs für DB-Management-Zugriff. Wenn Sie sich für die Verwendung der OS-basierten Authentifizierung entscheiden, muss der BS-Admin-Benutzer-ID DB-Zugriff gewährt werden. Für die Windows-domänenbasierte SQL Server-Installation kann ein Domain-Administratorkonto verwendet werden, um alle SQL-Server innerhalb der Domäne zu verwalten.

Windows Host für SQL Server:

1. Wenn Sie Windows-Anmeldeinformationen zur Authentifizierung verwenden, müssen Sie die Anmeldedaten vor dem Installieren von Plug-ins einrichten.
2. Wenn Sie eine SQL Server-Instanz zur Authentifizierung verwenden, müssen Sie die Anmeldeinformationen nach der Installation von Plugins hinzufügen.
3. Wenn Sie die SQL-Authentifizierung beim Einrichten der Anmeldeinformationen aktiviert haben, wird die

erkannte Instanz oder Datenbank mit einem roten Sperrsymbol angezeigt. Wenn das Sperrsymbol angezeigt wird, müssen Sie die Instanz oder die Datenbankanmeldeinformationen angeben, um die Instanz oder Datenbank einer Ressourcengruppe erfolgreich hinzuzufügen.

4. Sie müssen die Anmeldedaten einem RBAC-Benutzer ohne sysadmin-Zugriff zuweisen, wenn die folgenden Bedingungen erfüllt sind:
 - Die Anmeldeinformationen werden einer SQL-Instanz zugewiesen.
 - Die SQL Instanz oder der Host wird einem RBAC-Benutzer zugewiesen.
 - Der RBAC-DB-Admin-Benutzer muss sowohl die Gruppen- als auch die Backup-Rechte besitzen.

UNIX Host für Oracle:

1. Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder nicht-Root-Benutzer aktiviert haben, indem Sie sshd.conf bearbeiten und den sshd-Dienst neu starten. Die passwortbasierte SSH-Authentifizierung für die AWS-Instanz ist standardmäßig deaktiviert.
2. Konfigurieren Sie die Sudo-Berechtigungen für den nicht-Root-Benutzer, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plugins werden die Prozesse als effektiver Root-Benutzer ausgeführt.
3. Erstellen Sie Anmeldedaten im Linux-Authentifizierungsmodus für den Installationsbenutzer.
4. Sie müssen Java 1.8.x (64-bit) auf Ihrem Linux-Host installieren.
5. Die Installation des Oracle Database Plugins installiert auch das SnapCenter Plugin für Unix.

3. SnapCenter Host Plugin Installation

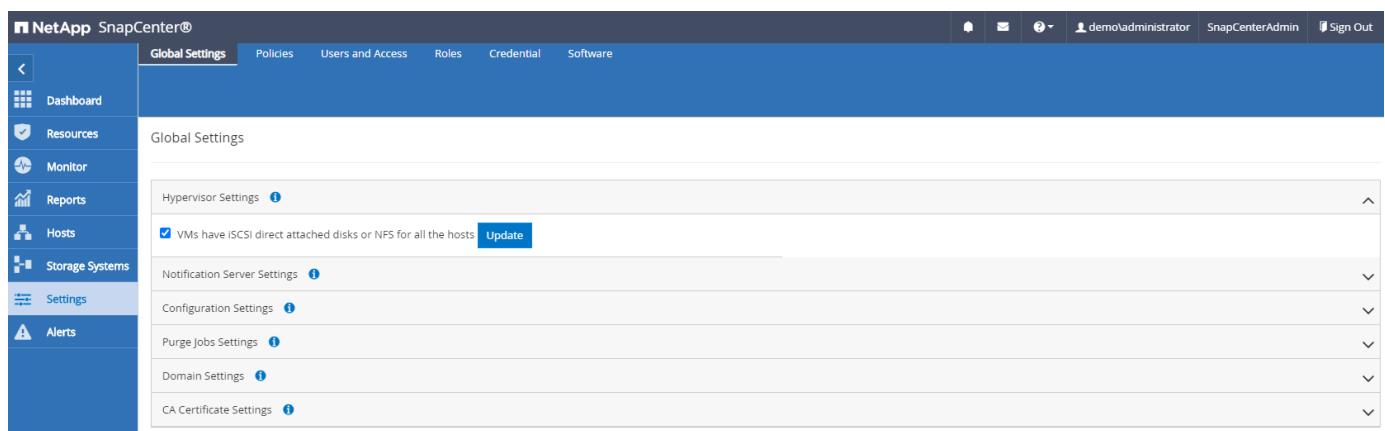


Bevor Sie versuchen, SnapCenter-Plugins auf Cloud-DB-Serverinstanzen zu installieren, stellen Sie sicher, dass alle Konfigurationsschritte wie im entsprechenden Cloud-Abschnitt für die Bereitstellung von Computing-Instanzen aufgeführt abgeschlossen wurden.

Die folgenden Schritte veranschaulichen, wie ein Datenbank-Host zu SnapCenter hinzugefügt wird, während ein SnapCenter-Plugin auf dem Host installiert ist. Das Verfahren gilt für das Hinzufügen von On-Premises-Hosts und Cloud-Hosts. Die folgende Demonstration führt zu einem Windows- oder Linux-Host in AWS.

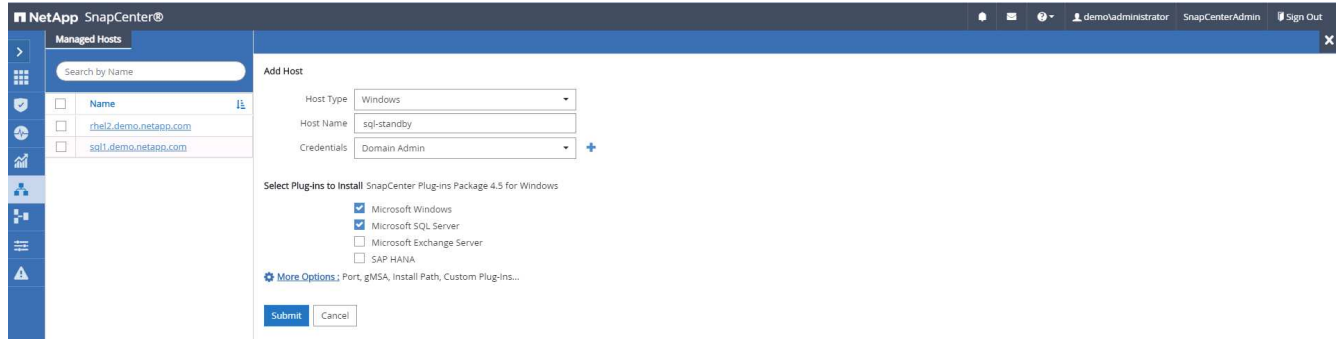
Konfigurieren Sie die globalen Einstellungen von SnapCenter VMware

Navigieren Sie zu Einstellungen > Globale Einstellungen. Wählen Sie unter Hypervisor-Einstellungen „VMs verfügen über direkt verbundene iSCSI-Festplatten oder NFS für alle Hosts“ aus und klicken Sie auf „Update“.

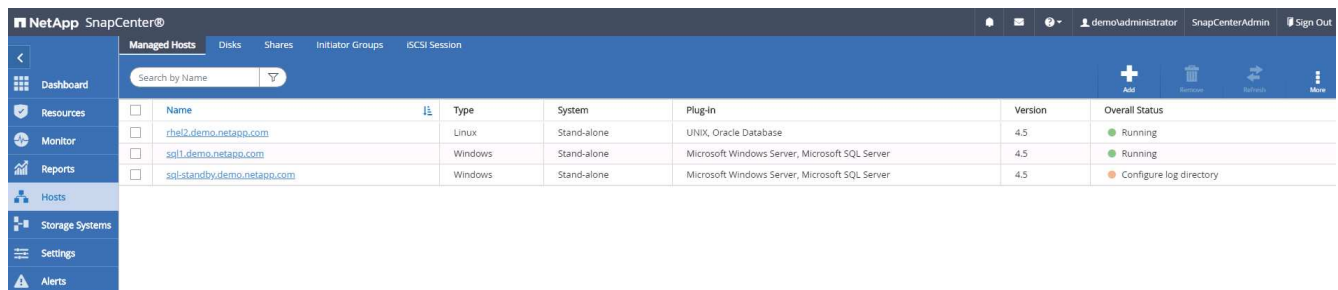


Fügen Sie den Windows-Host und die Installation des Plugins auf dem Host hinzu

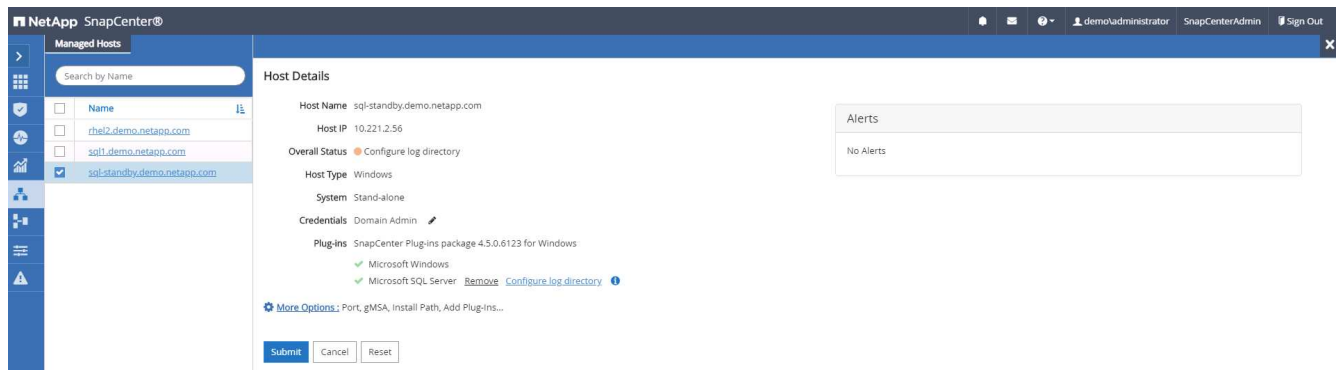
1. Melden Sie sich mit einer Benutzer-ID mit SnapCenterAdmin-Berechtigungen beim SnapCenter an.
2. Klicken Sie im linken Menü auf die Registerkarte Hosts und dann auf Hinzufügen, um den Host-Workflow hinzuzufügen zu öffnen.
3. Wählen Sie Windows für den Hosttyp. Der Hostname kann entweder ein Hostname oder eine IP-Adresse sein. Der Hostname muss vom SnapCenter-Host auf die richtige Host-IP-Adresse aufgelöst werden. Wählen Sie die in Schritt 2 erstellten Hostanmeldeinformationen aus. Wählen Sie Microsoft Windows und Microsoft SQL Server als die zu installierenden Plugin-Pakete.



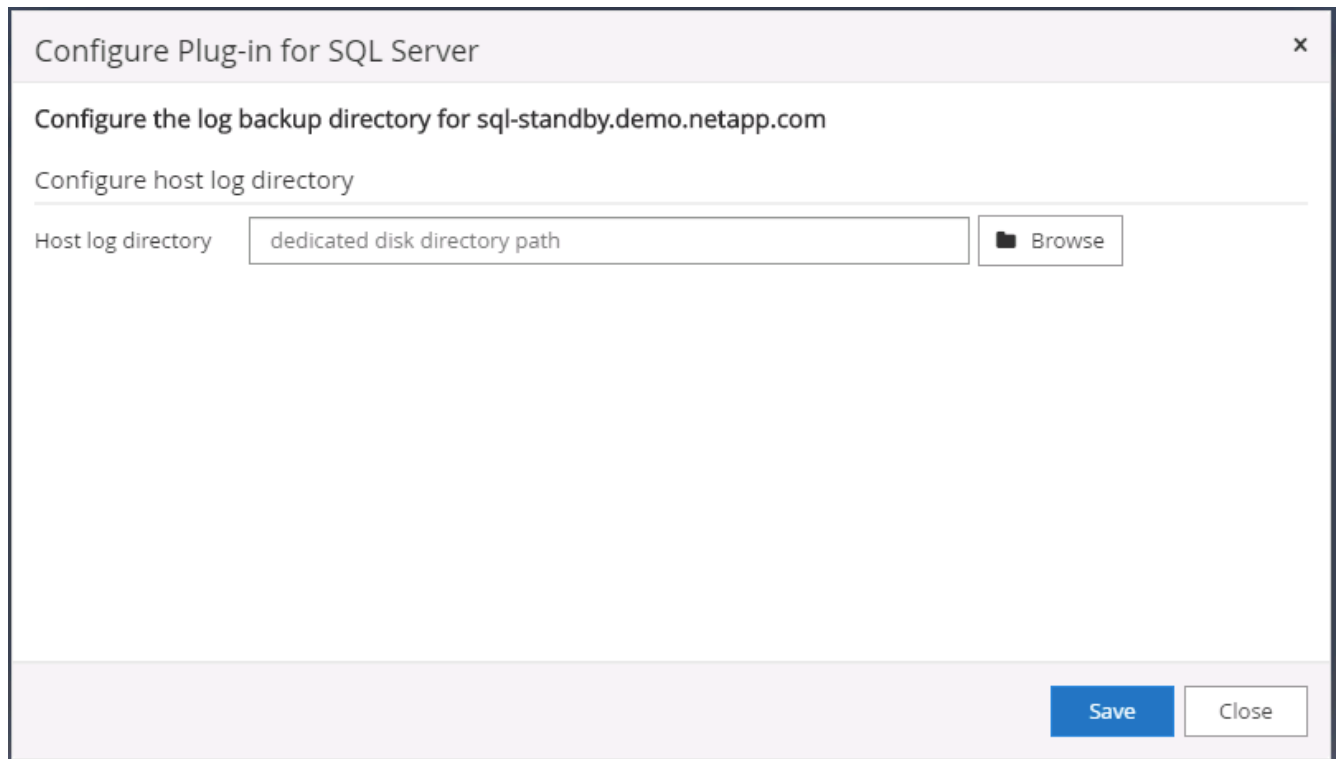
4. Nach der Installation des Plug-ins auf einem Windows-Host wird sein Gesamtstatus als „Protokollverzeichnis konfigurieren“ angezeigt.



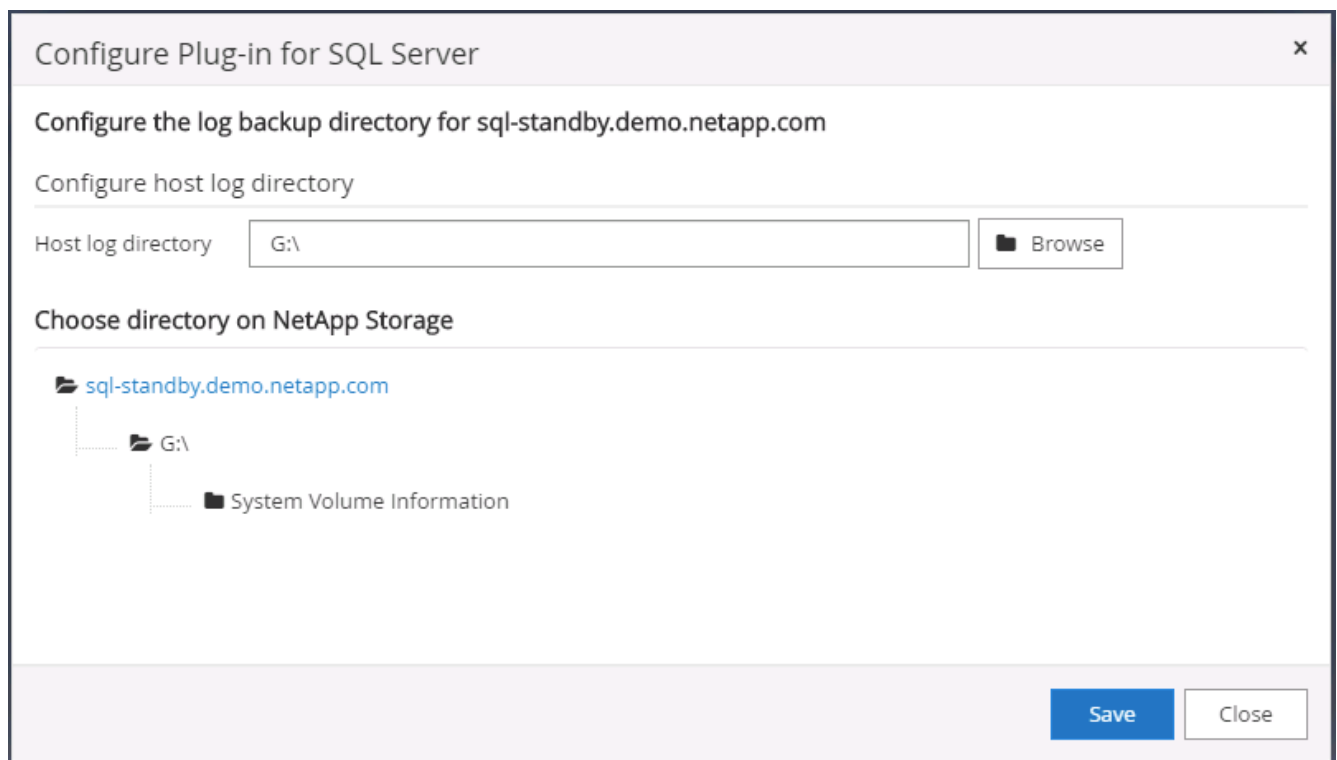
5. Klicken Sie auf den Hostnamen, um die Konfiguration des SQL Server-Protokollverzeichnisses zu öffnen.



6. Klicken Sie auf „Protokollverzeichnis konfigurieren“, um „Plug-in für SQL Server konfigurieren“ zu öffnen.



7. Klicken Sie auf Browse, um NetApp Storage zu entdecken, so dass ein Log-Verzeichnis eingestellt werden kann; SnapCenter verwendet dieses Log-Verzeichnis, um die Transaktions-Log-Dateien für SQL Server zu öffnen. Klicken Sie dann auf Speichern.



Wenn NetApp Storage, der einem DB-Host zur Ermittlung bereitgestellt wird, hinzugefügt werden soll, muss der Storage (On-Prem oder CVO) zum SnapCenter hinzugefügt werden, wie in Schritt 6 für CVO als Beispiel dargestellt.

8. Nach der Konfiguration des Protokollverzeichnisses wird der Gesamtstatus des Windows-Host-Plug-ins in „Ausführen“ geändert.

Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

9. Um den Host der Benutzer-ID der Datenbankverwaltung zuzuweisen, navigieren Sie zur Registerkarte Zugriff unter Einstellungen und Benutzer, klicken Sie auf die Datenbank-Management-Benutzer-ID (in unserem Fall der sqldba, dem der Host zugewiesen werden muss), und klicken Sie auf Speichern, um die Host-Ressourcenzuweisung abzuschließen.

Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oraoba	User	App Backup and Clone Admin	demo
sqldba	User	App Backup and Clone Admin	demo

Assign Assets

Asset Type: Host

search

Asset Name
rhel2.demo.netapp.com
sql1.demo.netapp.com
<input checked="" type="checkbox"/> sql-standby.demo.netapp.com

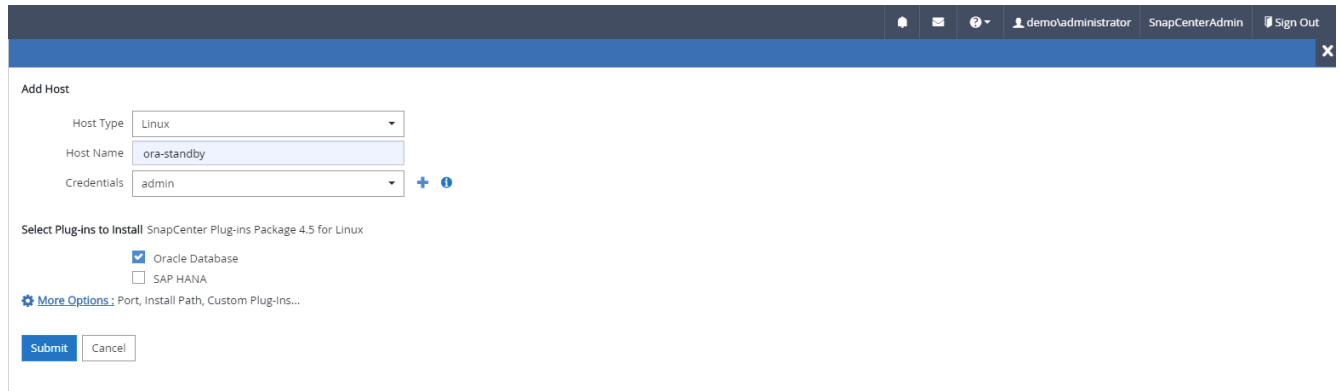
Save Close

Fügen Sie den Unix-Host hinzu und installieren Sie das Plugin auf dem Host

1. Melden Sie sich mit einer Benutzer-ID mit SnapCenterAdmin-Berechtigungen beim SnapCenter an.
2. Klicken Sie im linken Menü auf die Registerkarte Hosts, und klicken Sie auf Hinzufügen, um den Host-

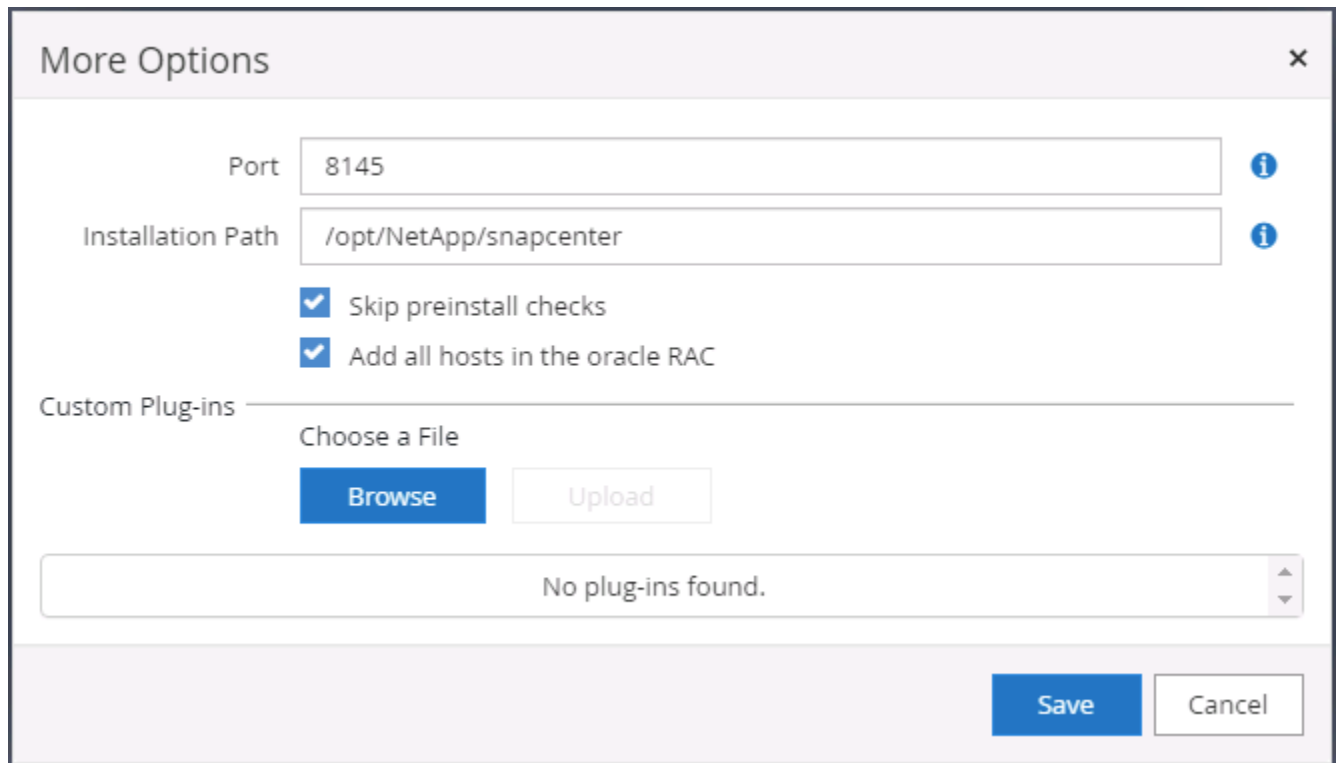
Workflow hinzufügen zu öffnen.

3. Wählen Sie Linux als Host-Typ. Der Hostname kann entweder der Hostname oder eine IP-Adresse sein. Der Host-Name muss jedoch aufgelöst werden, um die Host-IP-Adresse vom SnapCenter-Host zu korrigieren. Wählen Sie die in Schritt 2 erstellten Hostanmeldeinformationen aus. Die Hostanmeldeinformationen erfordern Sudo-Berechtigungen. Überprüfen Sie Oracle Database als das zu installierende Plug-in, das sowohl Oracle- als auch Linux-Host-Plug-ins installiert.



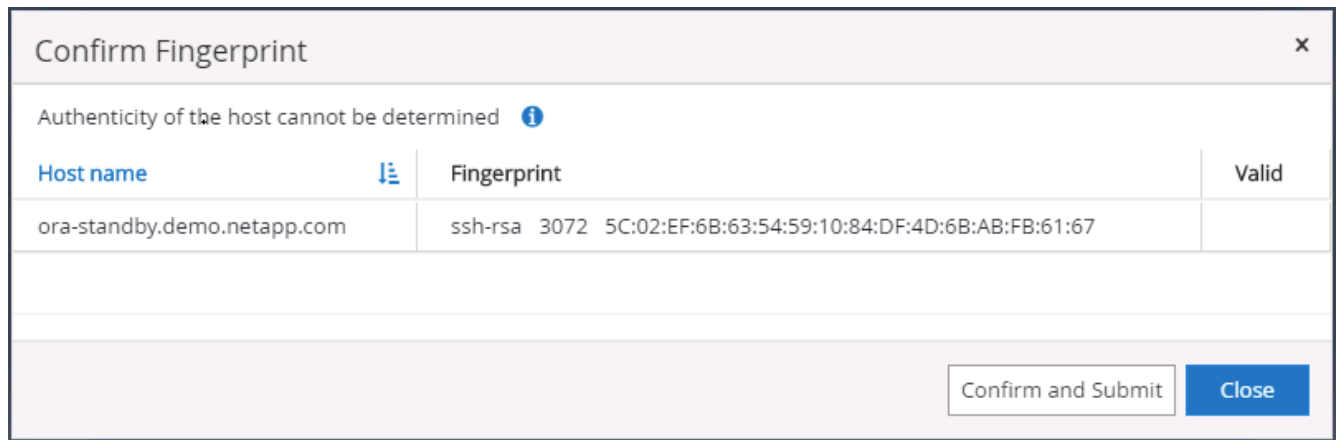
The screenshot shows the 'Add Host' configuration page. The 'Host Type' is set to 'Linux', 'Host Name' is 'ora-standby', and 'Credentials' is 'admin'. Under 'Select Plug-ins to Install', 'Oracle Database' is selected. A 'More Options' link is present, and 'Submit' and 'Cancel' buttons are at the bottom.

4. Klicken Sie auf Weitere Optionen und wählen Sie „Prüfung vor der Installation überspringen“. Sie werden aufgefordert, das Überspringen der Vorinstallationsüberprüfung zu bestätigen. Klicken Sie auf Ja und dann auf Speichern.



The 'More Options' dialog box is shown. The 'Port' is 8145 and the 'Installation Path' is /opt/NetApp/snapcenter. The 'Skip preinstall checks' and 'Add all hosts in the oracle RAC' options are checked. The 'Custom Plug-ins' section shows a 'Choose a File' button with 'Browse' and 'Upload' options. A message 'No plug-ins found.' is displayed in a list box. 'Save' and 'Cancel' buttons are at the bottom right.

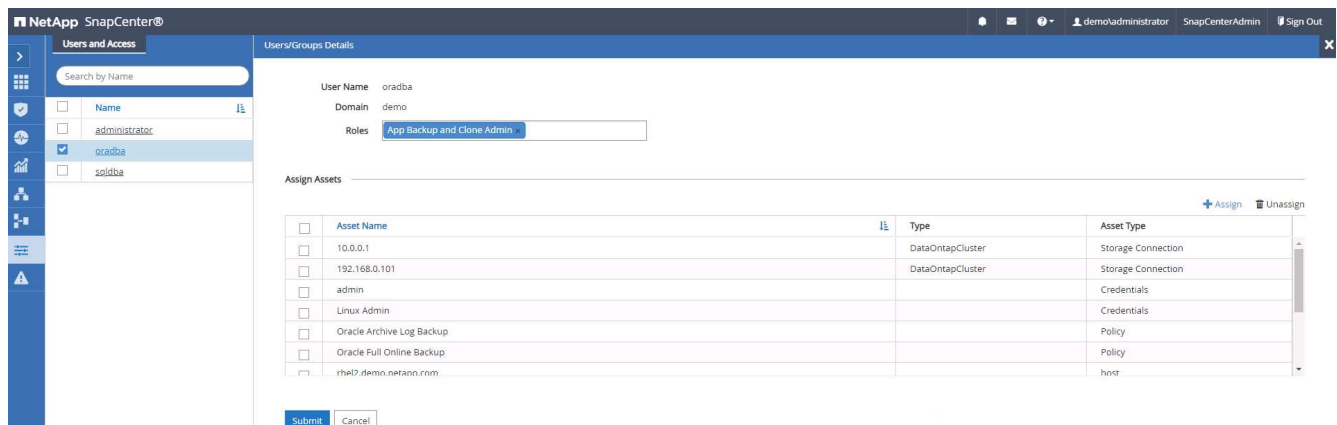
5. Klicken Sie auf Senden, um die Plugin-Installation zu starten. Sie werden wie unten gezeigt aufgefordert, den Fingerabdruck zu bestätigen.

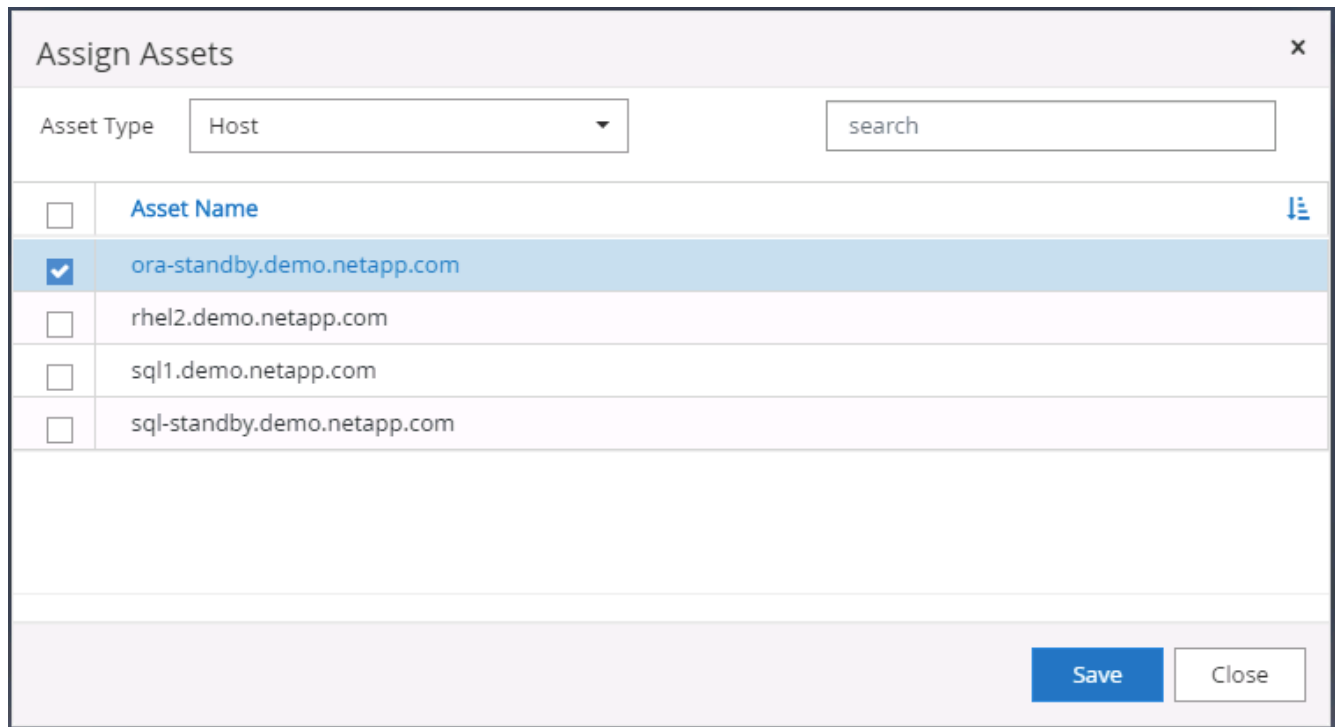


6. SnapCenter führt die Host-Validierung und -Registrierung durch, anschließend wird das Plug-in auf dem Linux Host installiert. Der Status wird von Plugin installieren auf Ausführen geändert.



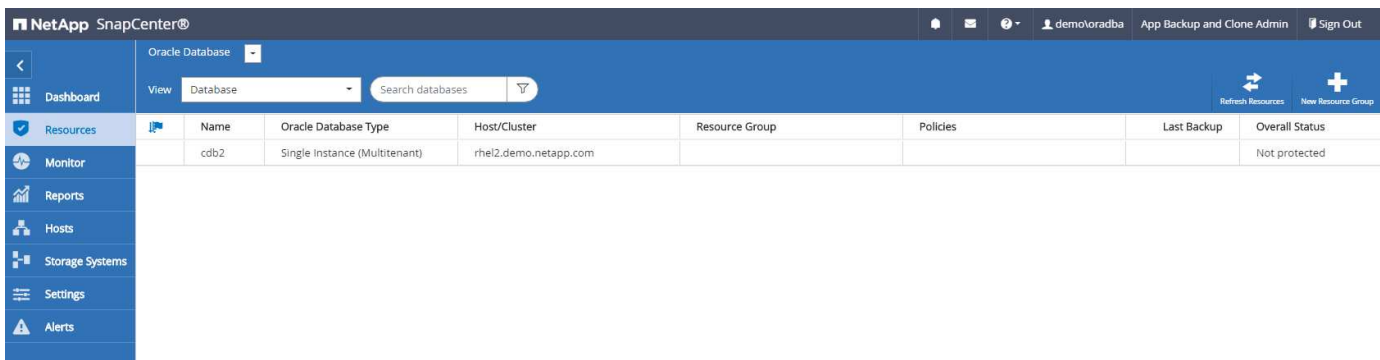
7. Weisen Sie den neu hinzugefügten Host der korrekten Datenbank-Management-Benutzer-ID zu (in unserem Fall oradba).





4. Ermittlung von Datenbankressourcen

Bei erfolgreicher Plugin-Installation können die Datenbankressourcen auf dem Host sofort erkannt werden. Klicken Sie im linken Menü auf die Registerkarte Ressourcen. Je nach Typ der Datenbankplattform stehen verschiedene Ansichten zur Verfügung, z. B. die Datenbank, die Ressourcengruppe usw. Möglicherweise müssen Sie auf die Registerkarte Ressourcen aktualisieren klicken, wenn die Ressourcen auf dem Host nicht erkannt und angezeigt werden.



Wenn die Datenbank zunächst erkannt wird, wird der Gesamtstatus als „nicht geschützt“ angezeigt. Der vorherige Screenshot zeigt eine Oracle Datenbank, die noch nicht durch eine Sicherungsrichtlinie geschützt ist.

Wenn eine Backup-Konfiguration oder -Richtlinie eingerichtet und ein Backup ausgeführt wurde, zeigt der Gesamtstatus der Datenbank den Backup-Status als „Backup erfolgreich“ und den Zeitstempel des letzten Backups an. Der folgende Screenshot zeigt den Sicherungsstatus einer SQL Server Benutzerdatenbank.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/14/2021 2:35:07 PM	Backup succeeded	User database

Wenn die Anmeldeinformationen für den Datenbankzugriff nicht ordnungsgemäß eingerichtet sind, zeigt eine rote Sperrtaste an, dass auf die Datenbank nicht zugegriffen werden kann. Wenn beispielsweise Windows-Anmeldeinformationen keinen sysadmin-Zugriff auf eine Datenbankinstanz haben, müssen die Datenbank-Anmeldeinformationen neu konfiguriert werden, um die rote Sperre zu entsperren.

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com			Running	Standalone ()
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)

The Microsoft SQL server or Windows credentials are necessary to unlock the selected instance. Click Refresh Resources to run a discovery with the associated Auth.

Name: sql-standby
 Resource Group: None
 Policy: None
 Selectable: Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.

Nachdem die entsprechenden Anmeldeinformationen entweder auf Windows-Ebene oder auf Datenbankebene konfiguriert wurden, wird das rote Schloss ausgeblendet und Informationen zum SQL Server-Typ gesammelt und überprüft.

Name	Host	Resource Groups	Policies	State	Type
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

5. Storage Cluster-Peering und DB Volumes Replication einrichten

Um Ihre On-Premises-Datenbankdaten mithilfe einer Public Cloud als Ziel zu schützen, werden On-Premises ONTAP Cluster-Datenbank-Volumes mithilfe von NetApp SnapMirror Technologie in die Cloud-CVO repliziert. Die replizierten Ziel-Volumes können dann für ENTWICKLUNG/Betrieb oder Disaster Recovery geklont werden. Mit den folgenden grundlegenden Schritten können Sie Cluster-Peering und DB-Volumes-Replikation

einrichten.

1. Konfigurieren Sie Intercluster LIFs für Cluster-Peering sowohl auf dem On-Premises-Cluster als auch auf der CVO-Cluster-Instanz. Dieser Schritt kann mit ONTAP System Manager ausgeführt werden. In einer CVO-Standardimplementierung werden automatisch Inter-Cluster-LIFs konfiguriert.

On-Premises-Cluster:

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type
onPrem-01_LIC	✓		Default	192.168.0.113	onPrem-01	e0b		Intercluster
onPrem-01_mgmt1	✓		Default	192.168.0.111	onPrem-01	e0c		Cluster/Node Mgmt
cluster_mgmt	✓		Default	192.168.0.101	onPrem-01	e0a		Cluster/Node Mgmt

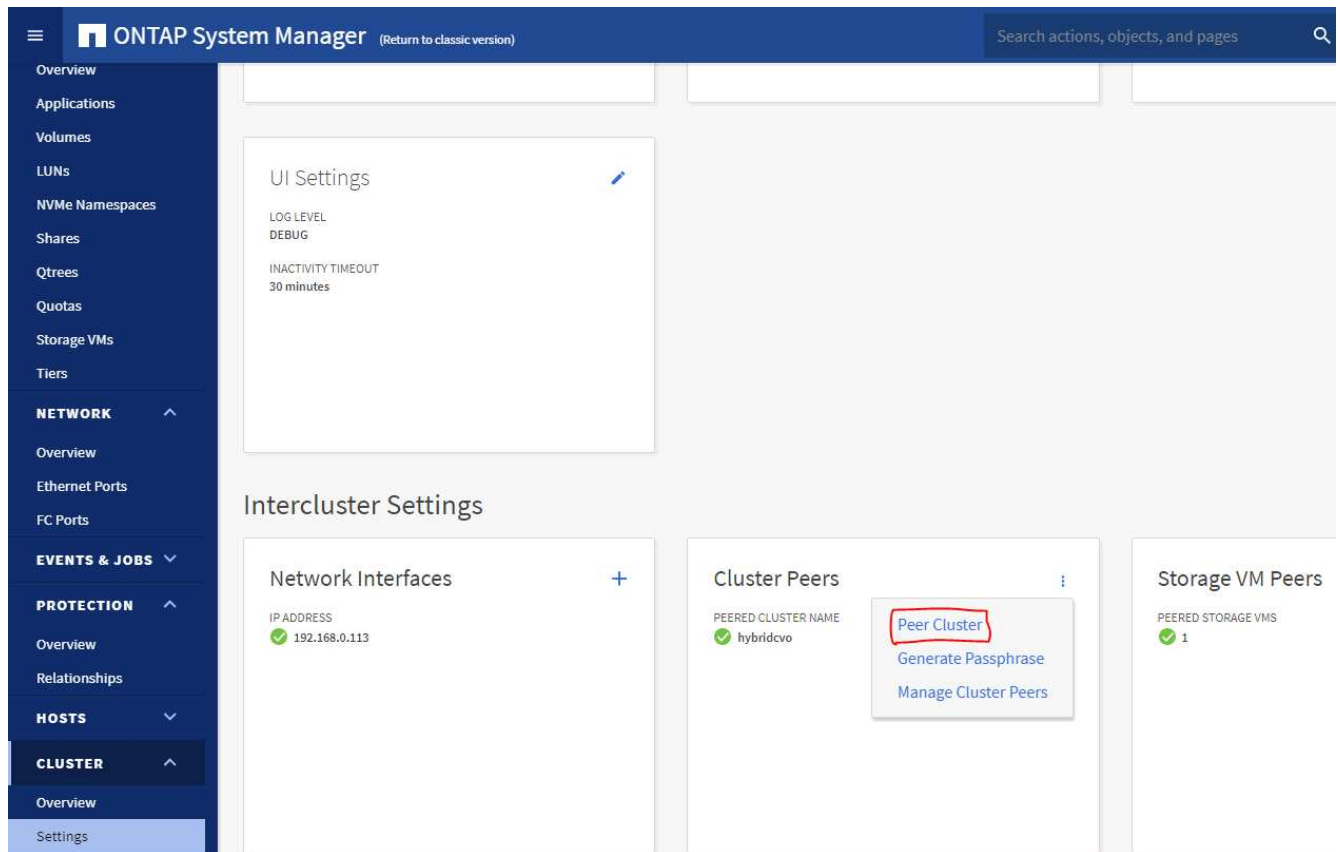
Ziel-CVO-Cluster:

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type	Throughput (I)
hybridcvo-02_mgmt1	✓		Default	10.221.2.104	hybridcvo-02	e0a		Cluster/Node Mgmt	0
inter_1	✓		Default	10.221.1.180	hybridcvo-01	e0a		Intercluster,Cluster/Node Mgmt	0.02
inter_2	✓		Default	10.221.2.250	hybridcvo-02	e0a		Intercluster,Cluster/Node Mgmt	0.03
iscsi_1	✓	svm_hybridcvo	Default	10.221.1.15	hybridcvo-01	e0a	ISCSI	Data	0
iscsi_2	✓	svm_hybridcvo	Default	10.221.2.168	hybridcvo-02	e0a	ISCSI	Data	0

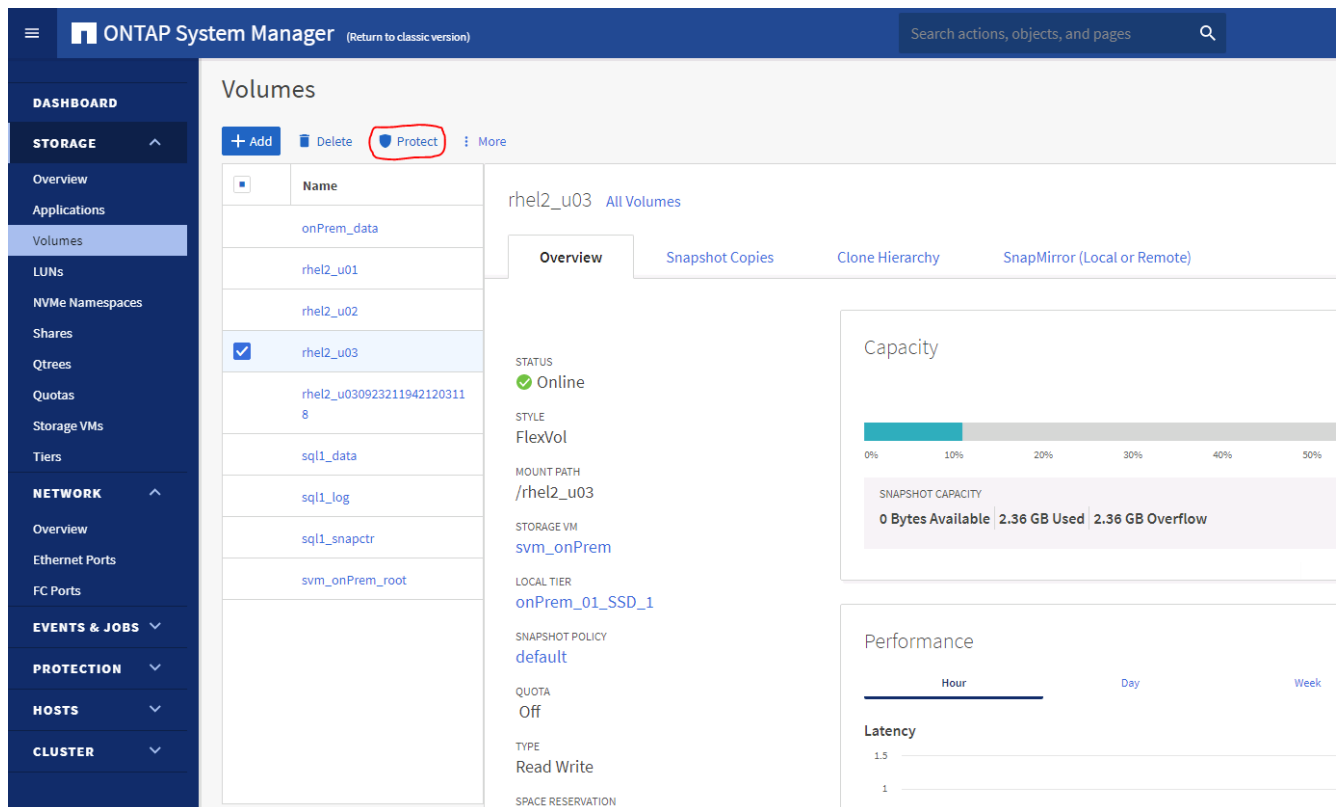
2. Bei konfigurierten Intercluster LIFs können Cluster-Peering und Volume-Replizierung mithilfe von Drag-and-Drop in NetApp Cloud Manager eingerichtet werden. Siehe ["Erste Schritte – AWS Public Cloud"](#) Entsprechende Details.

Alternativ können Cluster-Peering und die Replizierung von DB-Volumes mithilfe von ONTAP System Manager wie folgt durchgeführt werden:

3. Melden Sie sich bei ONTAP System Manager an. Navigieren Sie zu Cluster > Einstellungen, und klicken Sie auf Peer Cluster, um Cluster-Peering mit der CVO-Instanz in der Cloud einzurichten.

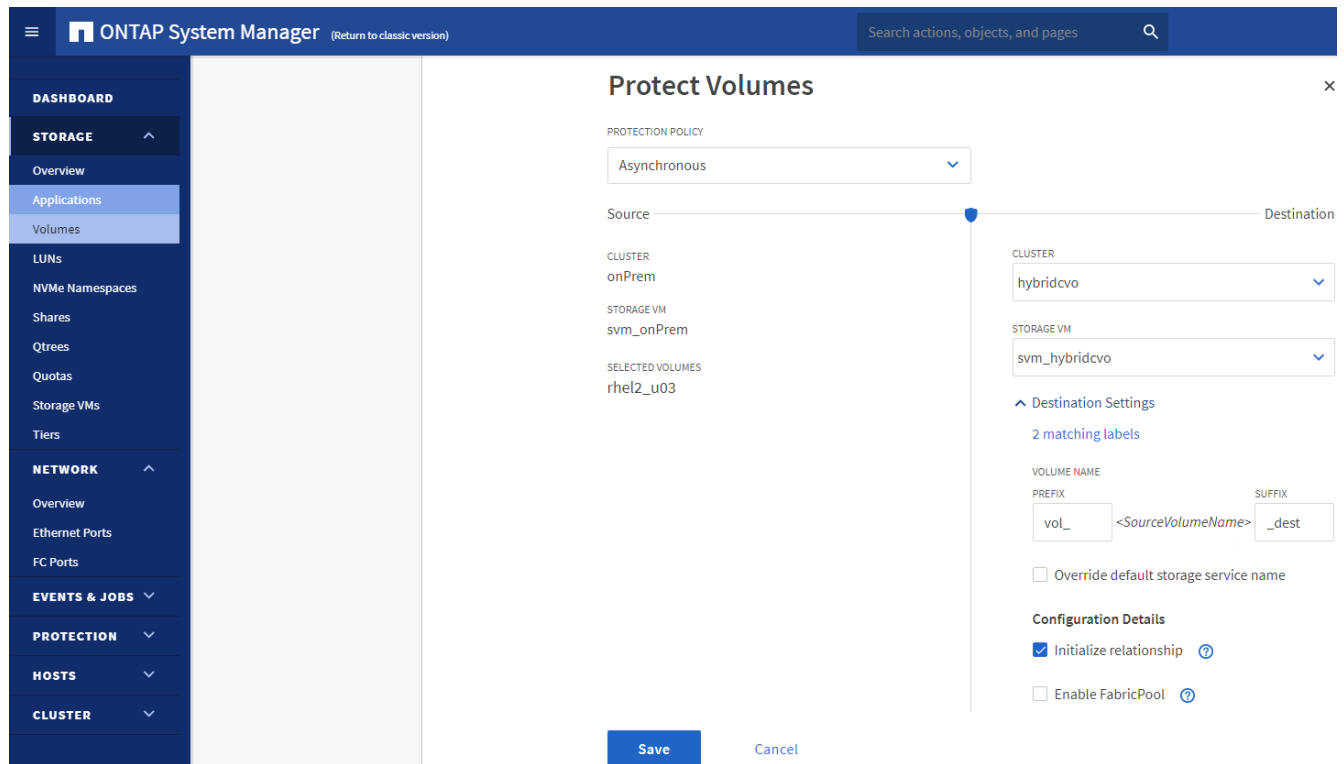


4. Wechseln Sie zur Registerkarte Volumes. Wählen Sie das zu replizierende Datenbank-Volumen aus, und klicken Sie auf „Schützen“.

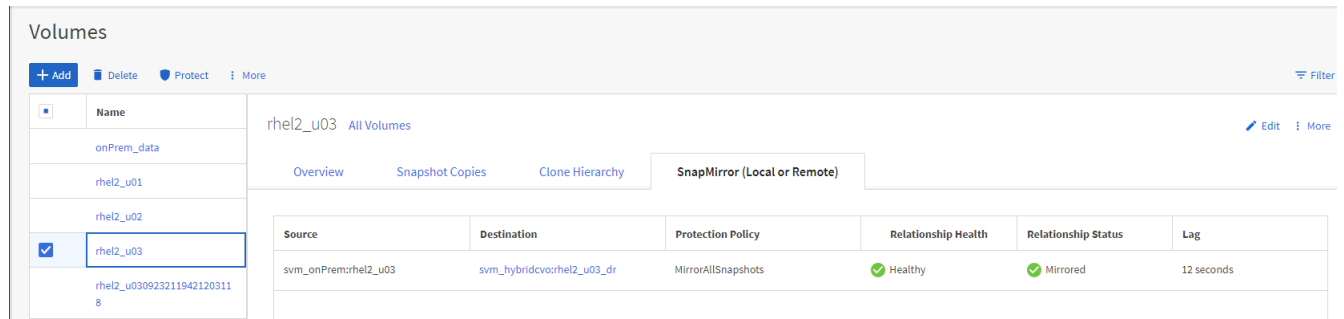


5. Legen Sie die Schutzrichtlinie auf Asynchron fest. Wählen Sie das Ziel-Cluster und die Storage-SVM

aus.

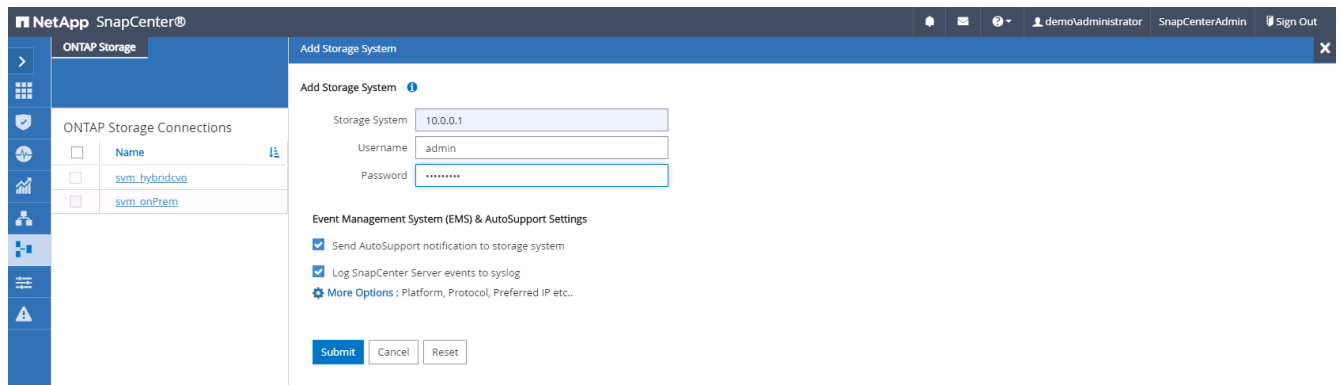


6. Überprüfen Sie, ob das Volume zwischen Quelle und Ziel synchronisiert wird und ob die Replikationsbeziehung ordnungsgemäß ist.

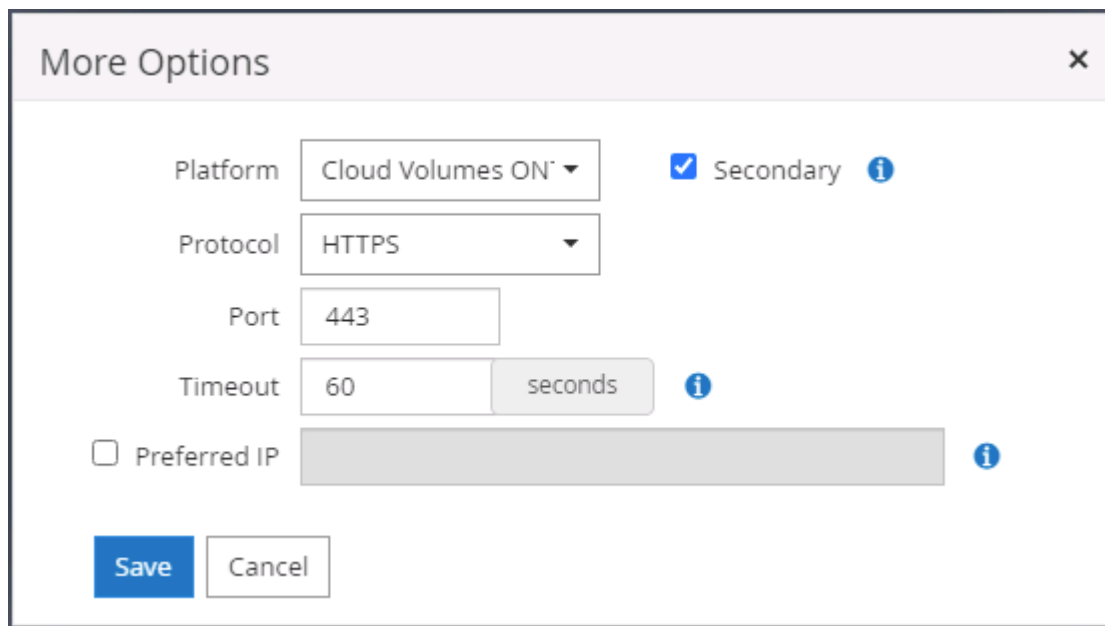


6. CVO Datenbank-Storage-SVM zu SnapCenter hinzufügen

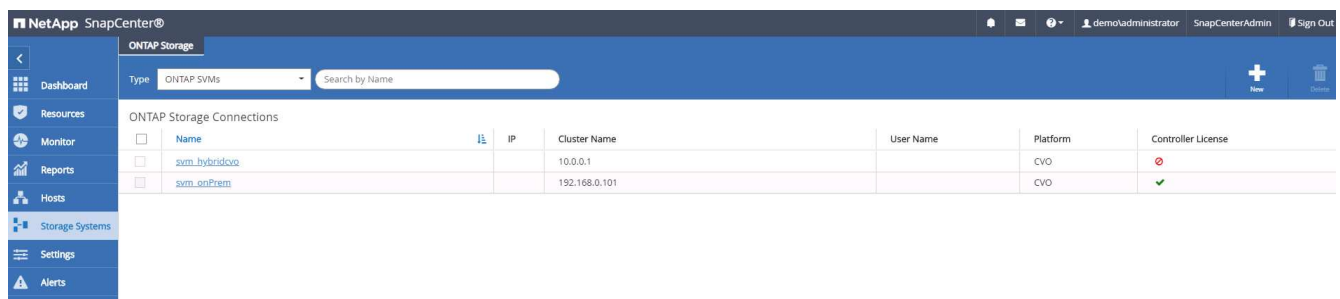
1. Melden Sie sich mit einer Benutzer-ID mit SnapCenterAdmin-Berechtigungen beim SnapCenter an.
2. Klicken Sie im Menü auf die Registerkarte Storage-System und dann auf Neu, um eine CVO-Storage-SVM hinzuzufügen, die replizierte Ziel-Datenbank-Volumes als Host für SnapCenter hostet. Geben Sie im Feld Storage-System die Cluster-Management-IP ein, und geben Sie den entsprechenden Benutzernamen und das entsprechende Passwort ein.



3. Klicken Sie auf Mehr Optionen, um weitere Storage-Konfigurationsoptionen zu öffnen. Wählen Sie im Feld Plattform die Option Cloud Volumes ONTAP aus, aktivieren Sie Sekundär und klicken Sie dann auf Speichern.



4. Weisen Sie die Storage-Systeme den Benutzer-IDs der SnapCenter-Datenbankverwaltung zu, wie in dargestellt 3. [SnapCenter Host Plugin Installation](#).

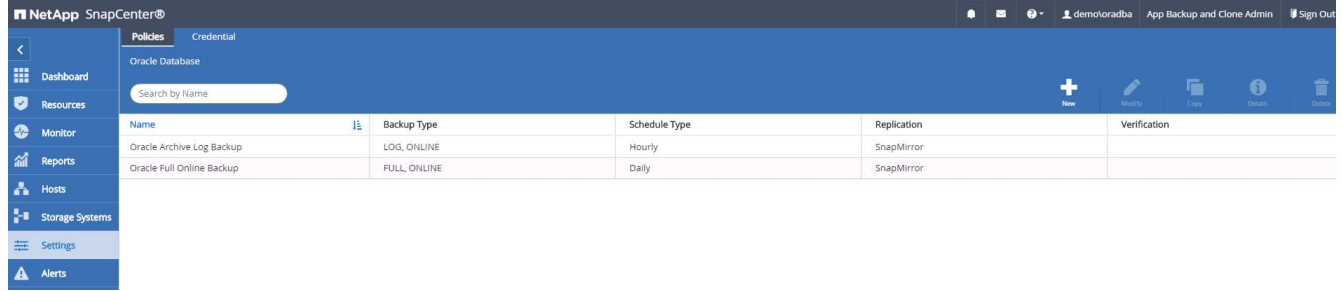


7. Einrichten der Datenbank Backup Policy in SnapCenter

Die folgenden Verfahren zeigen, wie eine vollständige Datenbank oder Backup-Richtlinie für Protokolldateien erstellt wird. Die Richtlinie kann dann zum Schutz von Datenbankressourcen implementiert werden. Der Recovery Point Objective (RPO) oder das Recovery Time Objective (RTO) bestimmt die Häufigkeit der Datenbank- und/oder Protokoll-Backups.

Erstellen einer vollständigen Datenbank-Backup-Richtlinie für Oracle

1. Melden Sie sich bei SnapCenter als Benutzer-ID für die Datenbankverwaltung an, klicken Sie auf Einstellungen und klicken Sie dann auf Richtlinien.



2. Klicken Sie auf Neu, um einen Workflow für die Erstellung einer neuen Backup-Richtlinie zu starten oder eine vorhandene Richtlinie zur Änderung auszuwählen.

The screenshot shows a dialog box titled 'Modify Oracle Database Backup Policy'. On the left is a vertical navigation pane with steps 1 through 7: Name, Backup Type, Retention, Replication, Script, Verification, and Summary. Step 1, 'Name', is currently selected. The main area of the dialog is titled 'Provide a policy name' and contains two input fields:

- 'Policy name' with the text 'Oracle Full Online Backup' and an information icon.
- 'Details' with the text 'Backup all data and log files'.

At the bottom right of the dialog are two buttons: 'Previous' (disabled) and 'Next' (active).

3. Wählen Sie den Sicherungstyp und die Zeitplanfrequenz aus.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

Online backup

- Datafiles, control files, and archive logs
- Datafiles and control files
- Archive logs

Offline backup i

- Mount
- Shutdown
- Save state of PDBs i

Choose 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

Previous Next

4. Legen Sie die Einstellung für die Backup-Aufbewahrung fest. Dies definiert, wie viele vollständige Datenbank-Backup-Kopien aufzubewahren sind.

Modify Oracle Database Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention**
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Retention settings ⓘ

Daily retention settings

Data backup retention settings ⓘ

Total Snapshot copies to keep

Keep Snapshot copies for days

Archive Log backup retention settings

Total Snapshot copies to keep

Keep Snapshot copies for days

Previous Next

5. Wählen Sie die sekundären Replizierungsoptionen aus, um lokale primäre Snapshots zu verschieben, die an einen sekundären Standort in der Cloud repliziert werden sollen.

Modify Oracle Database Backup Policy

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication**
- 5 Script
- 6 Verification
- 7 Summary

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label: ⓘ

Error retry count: ⓘ

6. Geben Sie ein optionales Skript an, das vor und nach einer Sicherungsfahrt ausgeführt werden soll.

Modify Oracle Database Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script**
- 6 Verification
- 7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

Prescript arguments

Postscript full path

Postscript arguments

Script timeout

7. Führen Sie bei Bedarf eine Backup-Überprüfung durch.

x
Modify Oracle Database Backup Policy

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

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

Daily

Verification script commands

Script timeout secs

Prescript full path

Prescript arguments

Postscript full path

Postscript arguments

8. Zusammenfassung.

✕
Modify Oracle Database Backup Policy

<div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6; border-radius: 3px; margin-bottom: 5px;">1 Name</div> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6; border-radius: 3px; margin-bottom: 5px;">2 Backup Type</div> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6; border-radius: 3px; margin-bottom: 5px;">3 Retention</div> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6; border-radius: 3px; margin-bottom: 5px;">4 Replication</div> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6; border-radius: 3px; margin-bottom: 5px;">5 Script</div> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6; border-radius: 3px; margin-bottom: 5px;">6 Verification</div> <div style="background-color: #0070c0; color: white; padding: 5px; border: 1px solid #0070c0; border-radius: 3px; margin-bottom: 5px;">7 Summary</div>	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> <p>Summary</p> </div> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Policy name</td> <td>Oracle Full Online Backup</td> </tr> <tr> <td colspan="2" style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"> <p>Details</p> </td> </tr> <tr> <td colspan="2">Backup all data and log files</td> </tr> <tr> <td>Backup type</td> <td>Online backup</td> </tr> <tr> <td>Schedule type</td> <td>Daily</td> </tr> <tr> <td>RMAN catalog backup</td> <td>Disabled</td> </tr> <tr> <td>Archive log pruning</td> <td>None</td> </tr> <tr> <td>On demand data backup retention</td> <td>None</td> </tr> <tr> <td>On demand archive log backup retention</td> <td>None</td> </tr> <tr> <td>Hourly data backup retention</td> <td>None</td> </tr> <tr> <td>Hourly archive log backup retention</td> <td>None</td> </tr> <tr> <td>Daily data backup retention</td> <td>Delete Snapshot copies older than : 14 days</td> </tr> <tr> <td>Daily archive log backup retention</td> <td>Delete Snapshot copies older than : 14 days</td> </tr> <tr> <td>Weekly data backup retention</td> <td>None</td> </tr> <tr> <td>Weekly archive log backup retention</td> <td>None</td> </tr> <tr> <td>Monthly data backup retention</td> <td>None</td> </tr> <tr> <td>Monthly archive log backup retention</td> <td>None</td> </tr> <tr> <td>Replication</td> <td>SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3</td> </tr> </table>	Policy name	Oracle Full Online Backup	<p>Details</p>		Backup all data and log files		Backup type	Online backup	Schedule type	Daily	RMAN catalog backup	Disabled	Archive log pruning	None	On demand data backup retention	None	On demand archive log backup retention	None	Hourly data backup retention	None	Hourly archive log backup retention	None	Daily data backup retention	Delete Snapshot copies older than : 14 days	Daily archive log backup retention	Delete Snapshot copies older than : 14 days	Weekly data backup retention	None	Weekly archive log backup retention	None	Monthly data backup retention	None	Monthly archive log backup retention	None	Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3
Policy name	Oracle Full Online Backup																																				
<p>Details</p>																																					
Backup all data and log files																																					
Backup type	Online backup																																				
Schedule type	Daily																																				
RMAN catalog backup	Disabled																																				
Archive log pruning	None																																				
On demand data backup retention	None																																				
On demand archive log backup retention	None																																				
Hourly data backup retention	None																																				
Hourly archive log backup retention	None																																				
Daily data backup retention	Delete Snapshot copies older than : 14 days																																				
Daily archive log backup retention	Delete Snapshot copies older than : 14 days																																				
Weekly data backup retention	None																																				
Weekly archive log backup retention	None																																				
Monthly data backup retention	None																																				
Monthly archive log backup retention	None																																				
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3																																				

Previous
Finish

Erstellen Sie eine Backup-Richtlinie für Datenbankprotokolle für Oracle

1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an, klicken Sie auf Einstellungen und klicken Sie dann auf Richtlinien.
2. Klicken Sie auf Neu, um einen Workflow für die Erstellung einer neuen Backup-Richtlinie zu starten, oder wählen Sie eine vorhandene Richtlinie zur Änderung aus.

New Oracle Database Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Provide a policy name

Policy name i

Details

PreviousNext

3. Wählen Sie den Sicherungstyp und die Zeitplanfrequenz aus.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

Online backup

- Datafiles, control files, and archive logs
- Datafiles and control files
- Archive logs

Offline backup ?

- Mount
- Shutdown
- Save state of PDBs ?

Choose 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

Previous Next

4. Legen Sie den Aufbewahrungszeitraum für das Protokoll fest.

New Oracle Database Backup Policy ×

- 1 Name
- 2 Backup Type
- 3 Retention**
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Retention settings ?

Hourly retention settings

Data backup retention settings ?

Total Snapshot copies to keep

Keep Snapshot copies for days

Archive Log backup retention settings

Total Snapshot copies to keep

Keep Snapshot copies for 7 days

Previous Next

5. Aktivieren Sie die Replizierung an einen sekundären Standort in der Public Cloud.

New Oracle Database Backup Policy ×

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label ⓘ

Error retry count ⓘ

Previous **Next**

6. Geben Sie alle optionalen Skripts an, die vor und nach der Protokollsicherung ausgeführt werden sollen.

New Oracle Database Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

Prescript arguments

Postscript full path

Postscript arguments

Script timeout

7. Geben Sie alle Skripts für die Backup-Überprüfung an.

New Oracle Database Backup Policy ✕

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

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

Verification script commands

Script timeout secs

Prescript full path Enter Prescript path

Prescript arguments

Postscript full path Enter Postscript path

Postscript arguments

Previous
Next

8. Zusammenfassung.

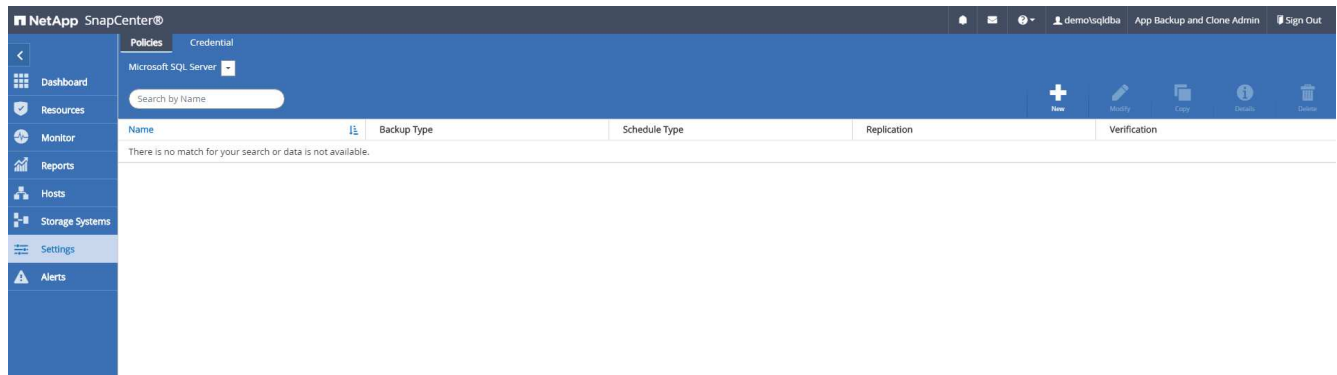
New Oracle Database Backup Policy

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary**

Summary	
Policy name	Oracle Archive Log Backup
Details	
Backup Oracle archive logs	
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	Delete Snapshot copies older than : 7 days
Daily data backup retention	None
Daily archive log backup retention	None
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3

Erstellen einer vollständigen Datenbank-Backup-Richtlinie für SQL

1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an, klicken Sie auf Einstellungen und klicken Sie dann auf Richtlinien.



2. Klicken Sie auf Neu, um einen Workflow für die Erstellung einer neuen Backup-Richtlinie zu starten, oder wählen Sie eine vorhandene Richtlinie zur Änderung aus.

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Provide a policy name

Policy name i

Details

Backup all data and log files

PreviousNext

3. Legen Sie die Backup-Option fest und planen Sie die Häufigkeit. Für SQL Server, der mit einer Verfügbarkeitsgruppe konfiguriert ist, kann ein bevorzugtes Backup-Replikat festgelegt werden.

New SQL Server Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

Full backup and log backup

Full backup

Log backup

Copy only backup i

Maximum databases backed up per Snapshot copy: i

Availability Group Settings v

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

4. Legen Sie den Aufbewahrungszeitraum für Backups fest.

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention**
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

Keep log backups applicable to last full backups

Keep log backups applicable to last days

Full backup retention settings ⓘ

Daily

Total Snapshot copies to keep

Keep Snapshot copies for days

5. Replizierung von Backup-Kopien an einen sekundären Standort in der Cloud aktivieren

New SQL Server Backup Policy x

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options i

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label i

Error retry count i

6. Geben Sie alle optionalen Skripts an, die vor oder nach einem Backupjob ausgeführt werden sollen.

New SQL Server Backup Policy x

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script**
- 6 Verification
- 7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

7. Geben Sie die Optionen für die Ausführung der Backup-Überprüfung an.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

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

Daily

Database consistency checks options

Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)

Suppress all information message (NO_INFOMSGS)

Display all reported error messages per object (ALL_ERRORMSGs)

Do not check non-clustered indexes (NOINDEX)

Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Log backup

Verify log backup. **i**

Verification script settings

Script timeout secs

Previous Next

8. Zusammenfassung.

New SQL Server Backup Policy
×

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Summary

Policy name	SQL Server Full Backup
Details	
Backup type	Backup all data and log files
Availability group settings	Full backup and log backup
Schedule Type	Backup only on preferred backup replica
UTM retention	Daily
Daily Full backup retention	Total backup copies to retain : 7
Replication	Total backup copies to retain : 7
Backup prescript settings	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3
Backup postscript settings	undefined Prescript arguments:
Verification for backup schedule type	undefined Postscript arguments:
Verification prescript settings	none
Verification postscript settings	undefined Prescript arguments:
	undefined Postscript arguments:

Previous
Finish

Erstellen Sie eine Backup-Richtlinie für Datenbankprotokolle für SQL.

1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an, klicken Sie auf Einstellungen > Richtlinien und dann auf Neu, um einen Workflow zur Erstellung neuer Richtlinien zu starten.

New SQL Server Backup Policy x

1 Name Provide a policy name

2 Backup Type Policy name i

3 Retention Details

4 Replication

5 Script

6 Verification

7 Summary

2. Legen Sie die Option zur Protokollsicherung fest und planen Sie die Häufigkeit. Für SQL Server, der mit einer Verfügbarkeitsgruppe konfiguriert ist, kann ein bevorzugtes Backup-Replikat festgelegt werden.

New SQL Server Backup Policy

- 1 Name
- 2 Backup Type**
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Select SQL server backup options

Choose backup type

Full backup and log backup

Full backup

Log backup

Copy only backup ?

Maximum databases backed up per Snapshot copy: ?

Availability Group Settings ▼

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

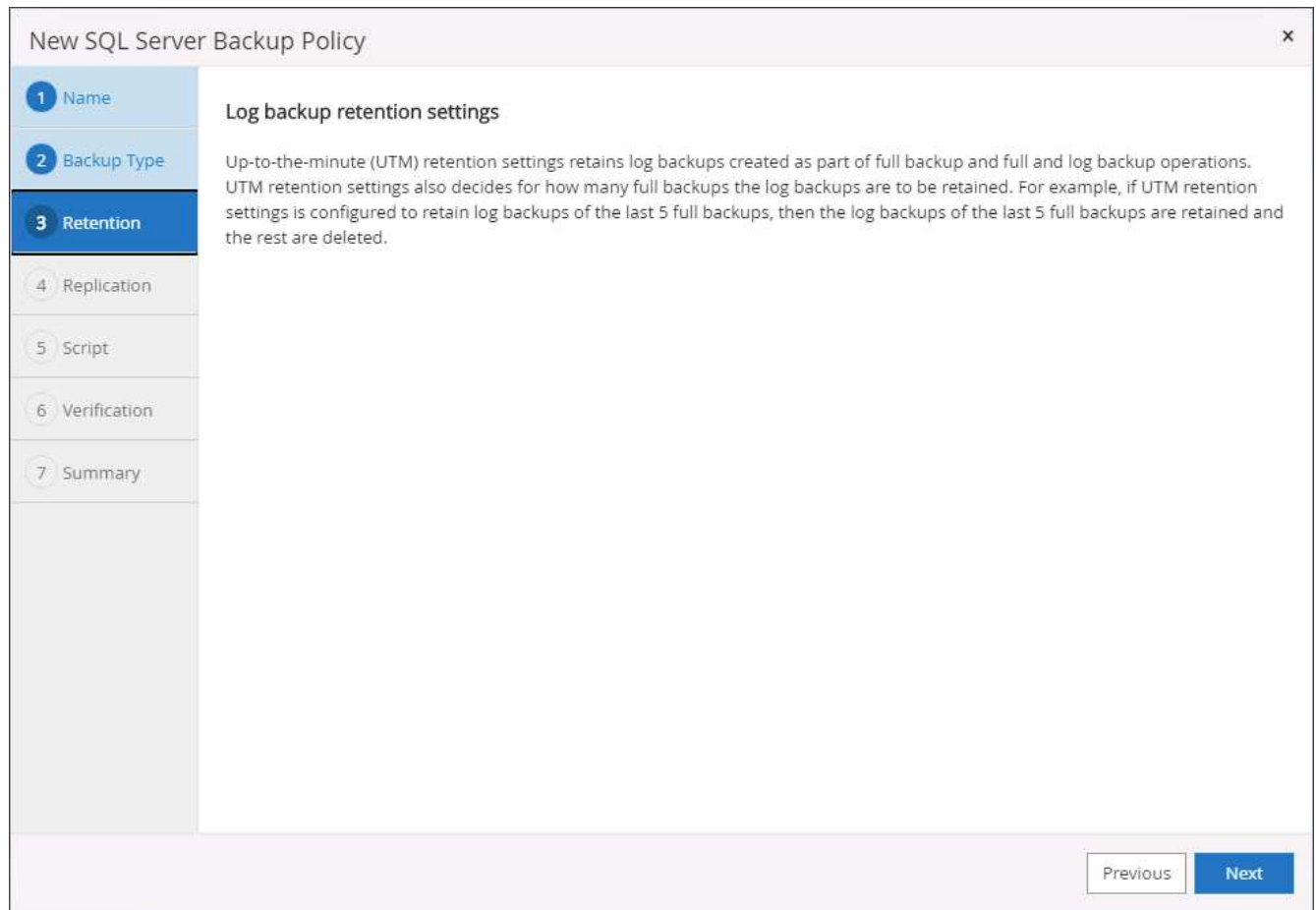
Daily

Weekly

Monthly

Previous Next

3. Die SQL Server Daten-Backup-Richtlinie definiert die Backup-Aufbewahrung für Protokolle. Akzeptieren Sie hier die Standardeinstellungen.



4. Aktivierung der Backup-Replizierung für Protokolle in der sekundären Umgebung in der Cloud

New SQL Server Backup Policy ✕

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options ⓘ

Update SnapMirror after creating a local Snapshot copy.

Update SnapVault after creating a local Snapshot copy.

Secondary policy label: Hourly ⓘ

Error retry count: 3 ⓘ

Previous Next

5. Geben Sie alle optionalen Skripts an, die vor oder nach einem Backupjob ausgeführt werden sollen.

New SQL Server Backup Policy ×

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script**
- 6 Verification
- 7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

6. Zusammenfassung.

New SQL Server Backup Policy
✕

- 1 Name
- 2 Backup Type
- 3 Retention
- 4 Replication
- 5 Script
- 6 Verification
- 7 Summary

Summary

Policy name	SQL Server Log Backup
Details	
Backup SQL server log	
Backup type	Log transaction backup
Availability group settings	
Backup only on preferred backup replica	
Schedule Type	Hourly
Replication	
SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3	
Backup prescript settings	
undefined	
Prescript arguments:	
Backup postscript settings	
undefined	
Postscript arguments:	
Verification for backup schedule type	
none	
Verification prescript settings	
undefined	
Prescript arguments:	
Verification postscript settings	
undefined	
Postscript arguments:	

Previous
Finish

8. Backup Policy implementieren, um Datenbank zu schützen

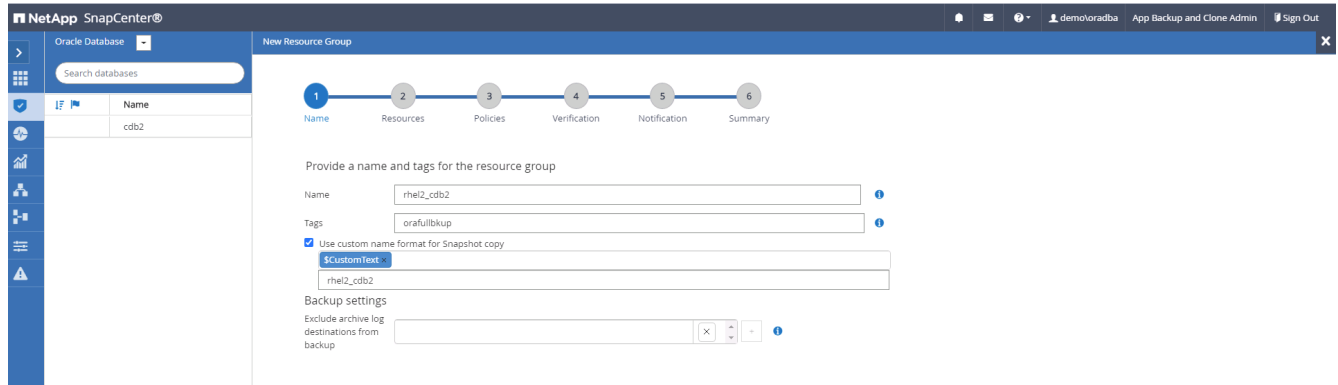
SnapCenter verwendet eine Ressourcengruppe, um eine Datenbank in einer logischen Gruppierung von Datenbankressourcen zu sichern, z. B. mehrere Datenbanken, die auf einem Server gehostet werden, eine Datenbank, die dieselben Storage Volumes nutzt, mehrere Datenbanken zur Unterstützung einer Business-Applikation usw. Durch den Schutz einer einzigen Datenbank wird eine eigene Ressourcengruppe erzeugt. Die folgenden Verfahren veranschaulichen die Implementierung einer in Abschnitt 7 erstellten Backup-Richtlinie zum Schutz von Oracle- und SQL Server-Datenbanken.

Erstellen Sie eine Ressourcengruppe für vollständige Oracle-Backups

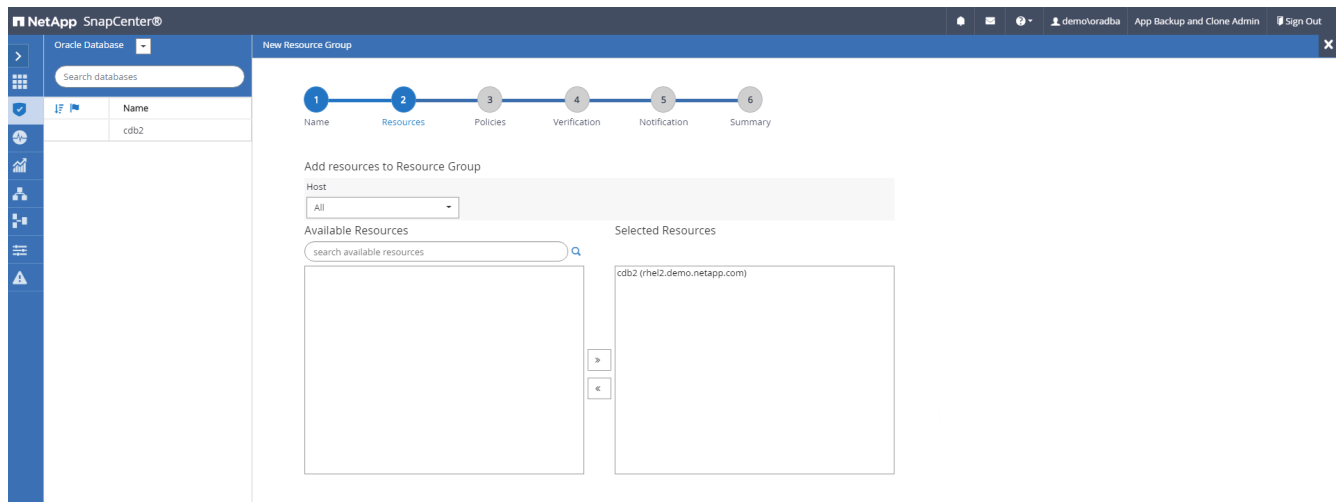
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdown-Liste Ansicht entweder Datenbank oder Ressourcengruppe aus, um den Arbeitsablauf für die Erstellung von Ressourcengruppen zu starten.

	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
	cdb2	Single instance (Multitenant)	rhe12.demo.netapp.com				Not protected

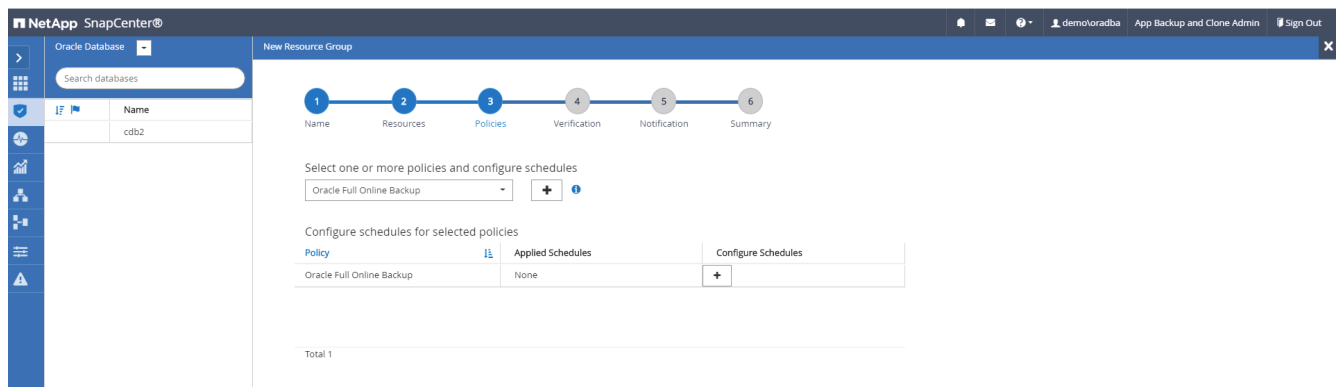
- Geben Sie einen Namen und Tags für die Ressourcengruppe an. Sie können ein Benennungsformat für die Snapshot Kopie definieren und, falls konfiguriert, das redundante Archivprotokollziel umgehen.



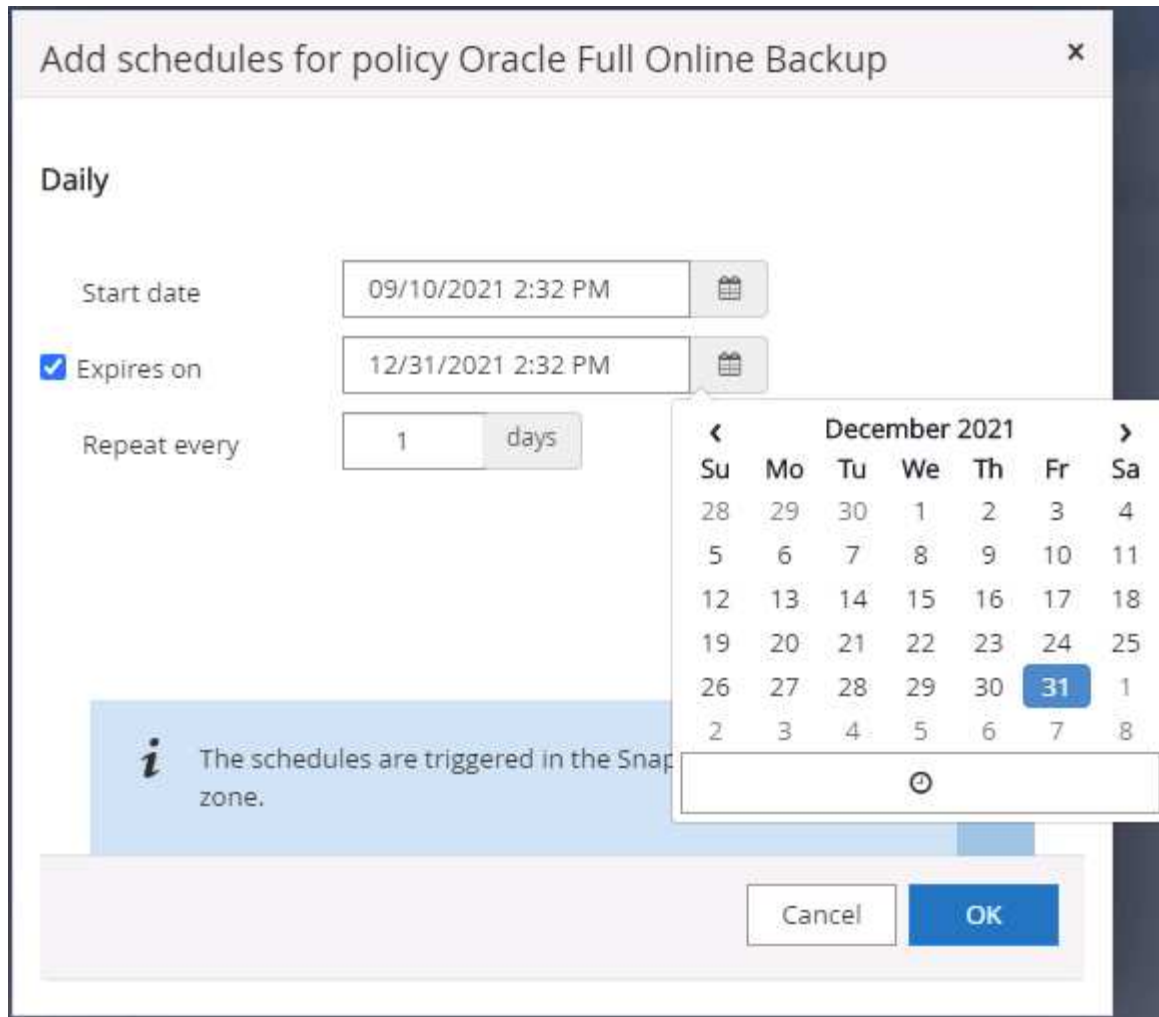
- Fügen Sie der Ressourcengruppe Datenbankressourcen hinzu.



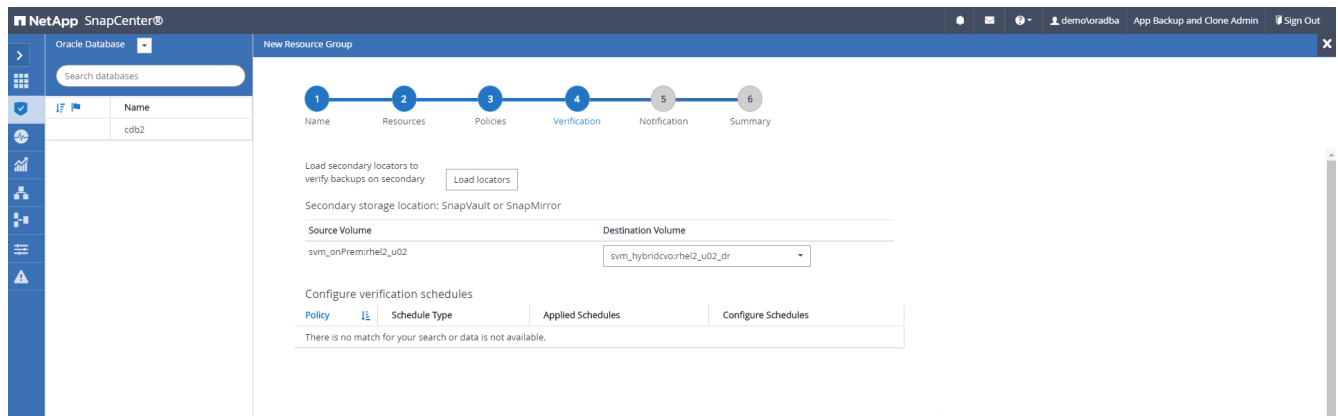
- Wählen Sie aus der Dropdown-Liste eine vollständige Backup Policy aus, die in Abschnitt 7 erstellt wurde.



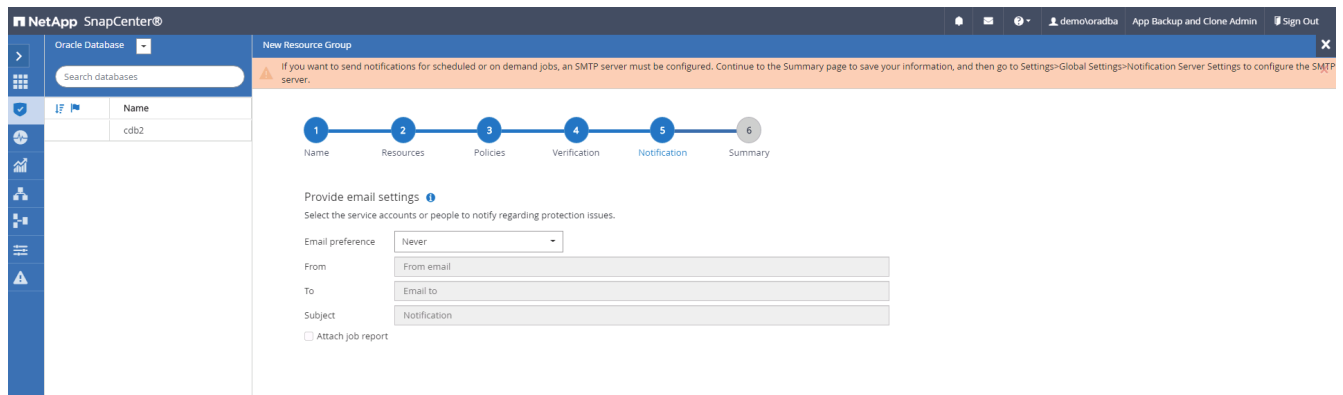
- Klicken Sie auf das Pluszeichen (+), um den gewünschten Backup-Zeitplan zu konfigurieren.



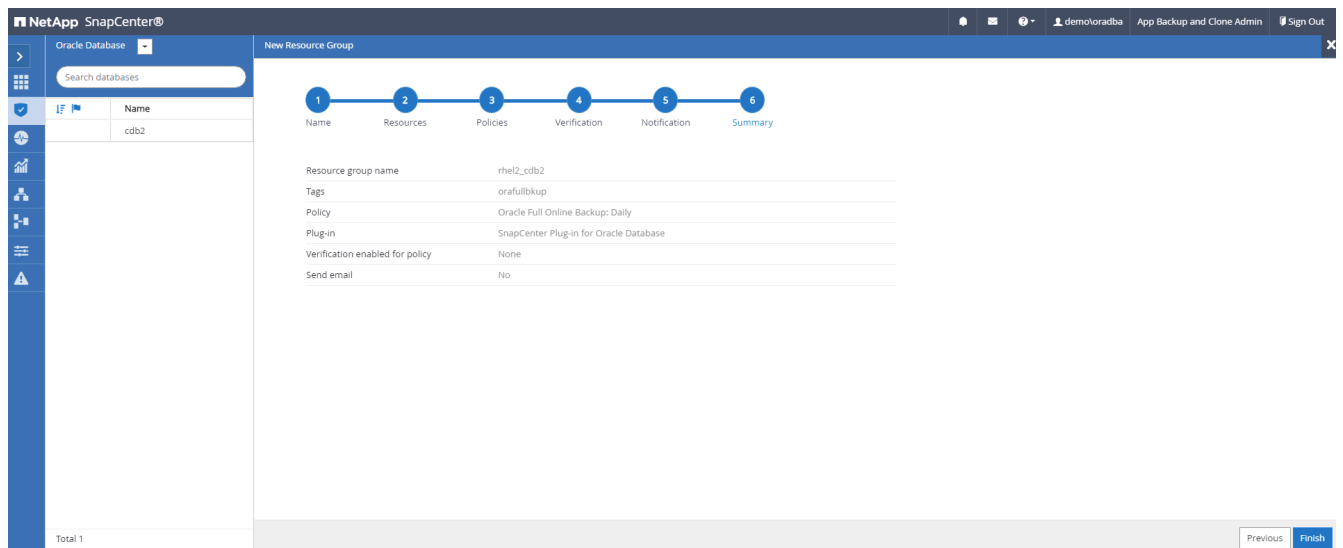
6. Klicken Sie auf Lokatoren laden, um das Quell- und Zielvolumen zu laden.



7. Konfigurieren Sie bei Bedarf den SMTP-Server für E-Mail-Benachrichtigungen.

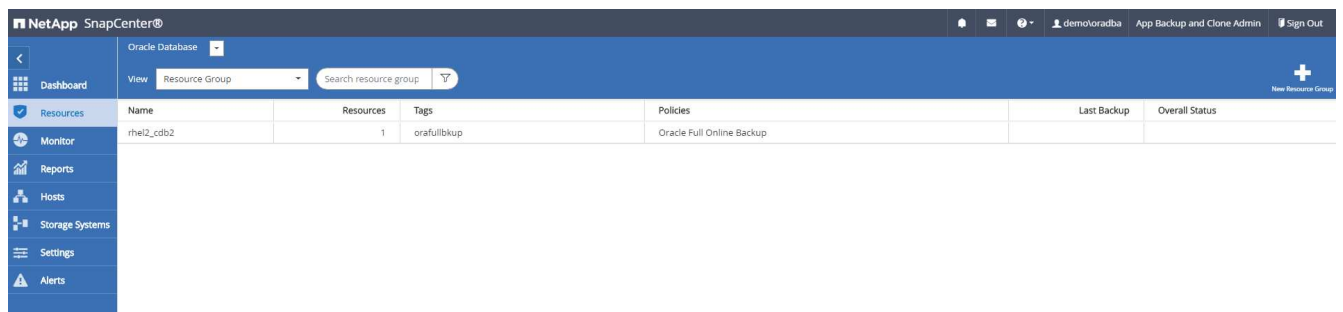


8. Zusammenfassung.

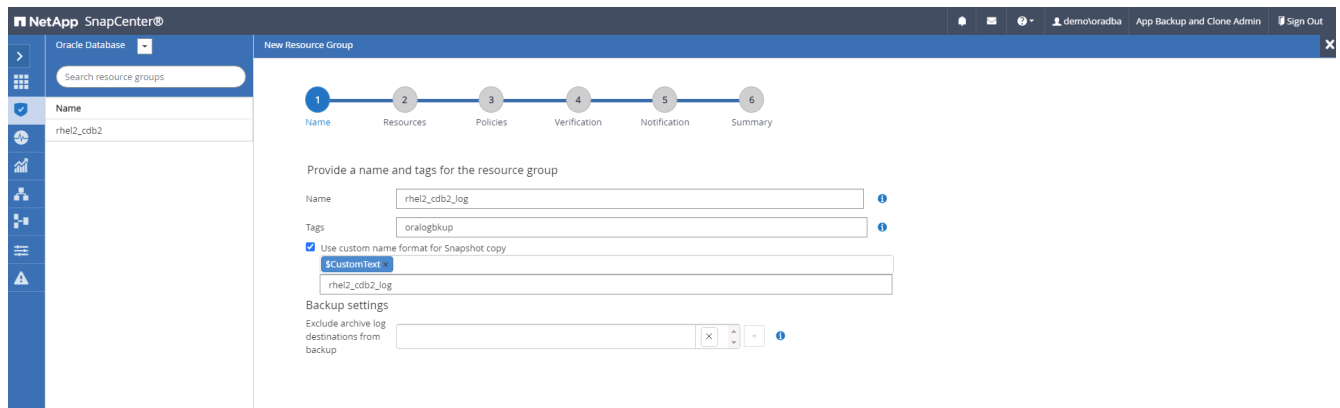


Erstellen Sie eine Ressourcengruppen für das Protokoll-Backup von Oracle

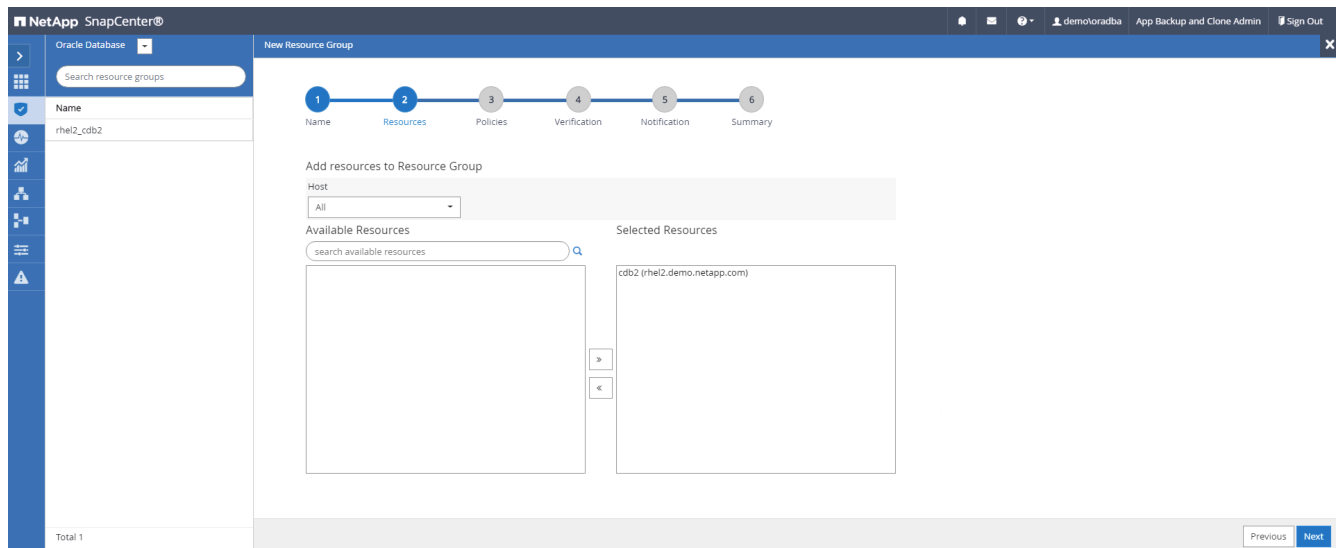
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdown-Liste Ansicht entweder Datenbank oder Ressourcengruppe aus, um den Arbeitsablauf für die Erstellung von Ressourcengruppen zu starten.



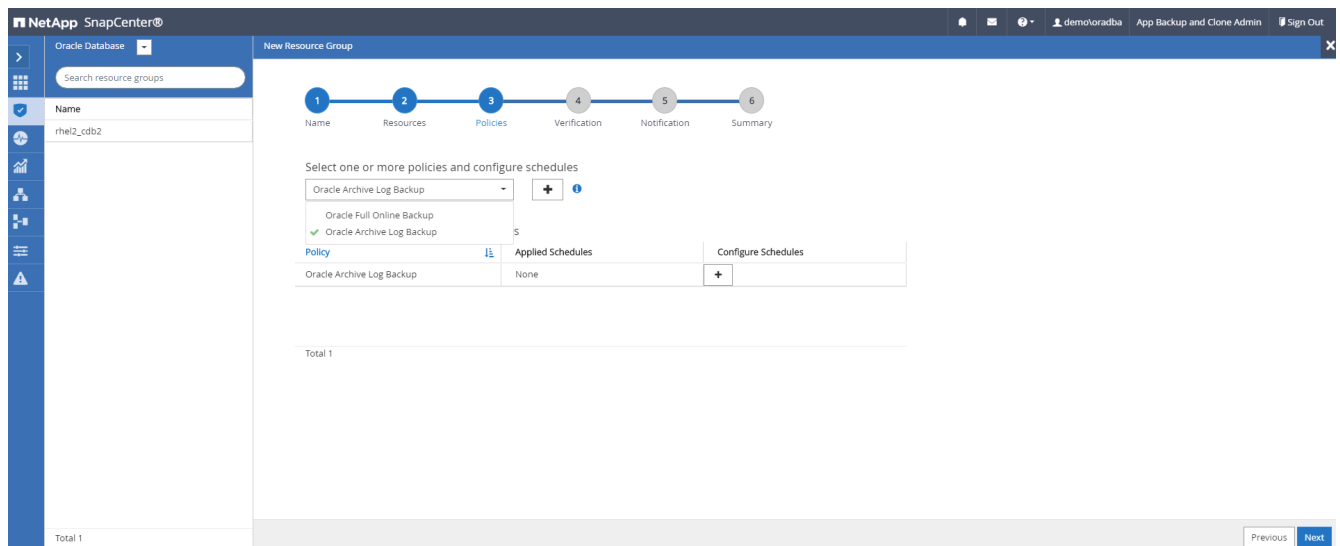
2. Geben Sie einen Namen und Tags für die Ressourcengruppe an. Sie können ein Benennungsformat für die Snapshot Kopie definieren und, falls konfiguriert, das redundante Archivprotokollziel umgehen.



3. Fügen Sie der Ressourcengruppe Datenbankressourcen hinzu.




4. Wählen Sie aus der Dropdown-Liste eine Protokoll-Backup-Richtlinie aus, die in Abschnitt 7 erstellt wurde.




5. Klicken Sie auf das Pluszeichen (+), um den gewünschten Backup-Zeitplan zu konfigurieren.

Add schedules for policy Oracle Archive Log Backup ✕

Hourly

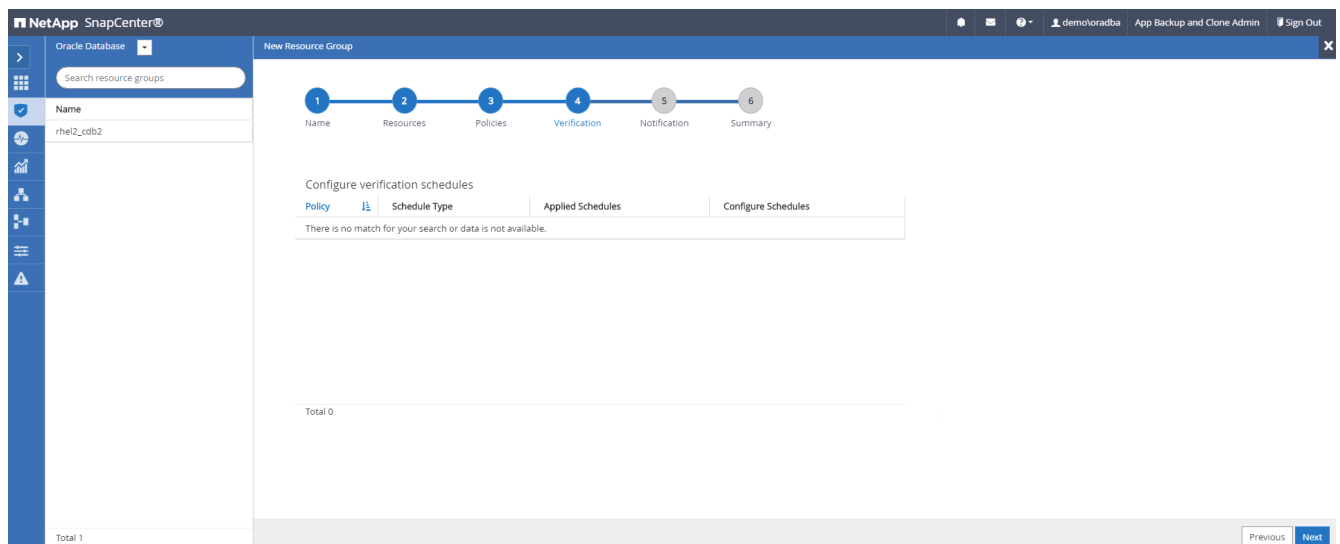
Start date 

Expires on 

Repeat every hours mins

i The schedules are triggered in the SnapCenter Server time zone. ✕

6. Wenn die Backup-Überprüfung konfiguriert ist, wird sie hier angezeigt.



NetApp SnapCenter®

Oracle Database

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

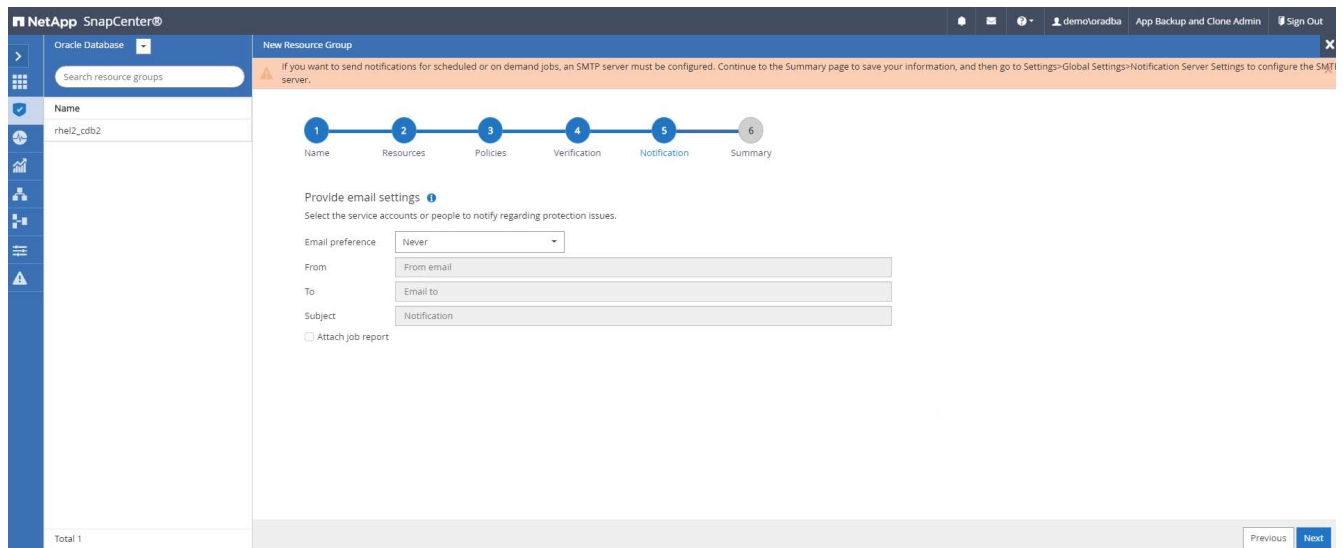
Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

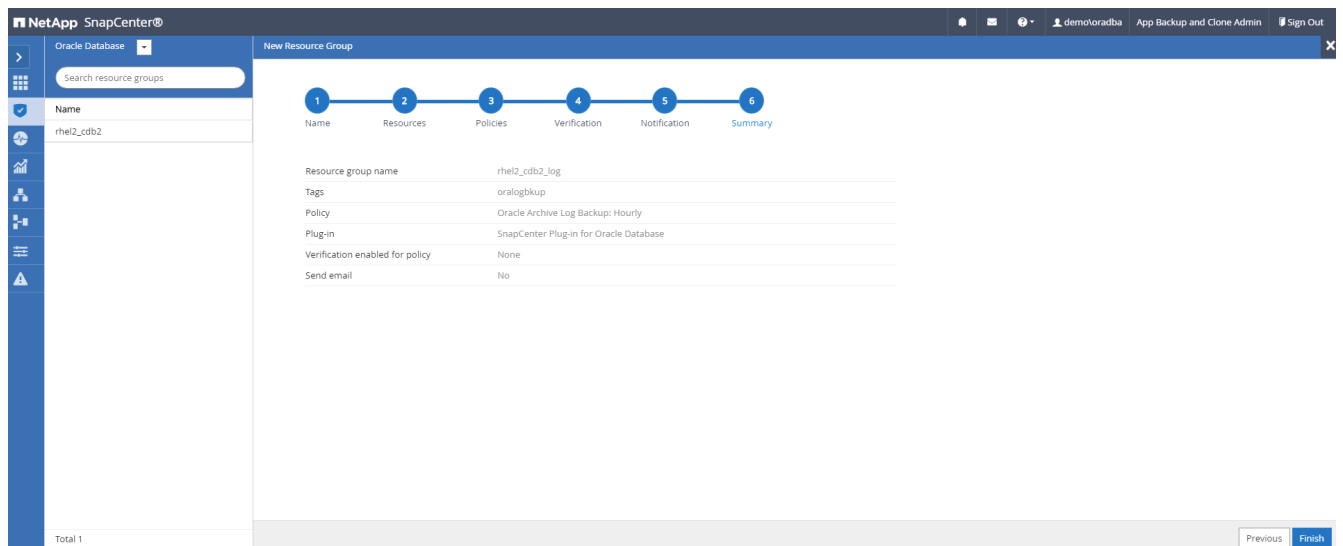
Total 0

Previous Next

7. Konfigurieren Sie bei Bedarf einen SMTP-Server für E-Mail-Benachrichtigungen.

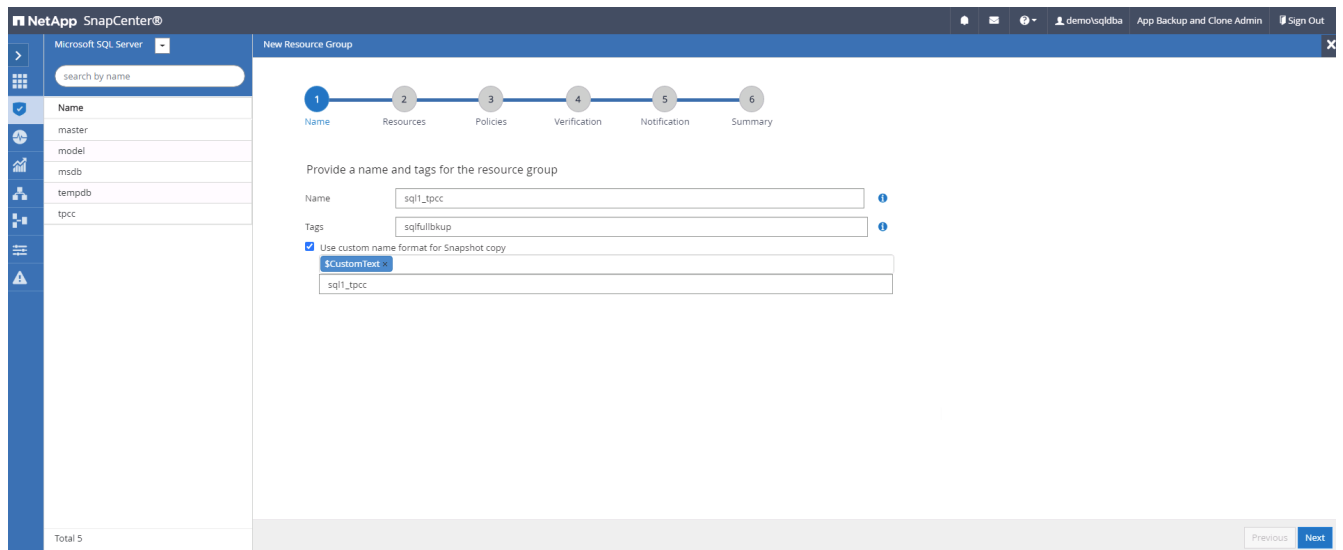


8. Zusammenfassung.

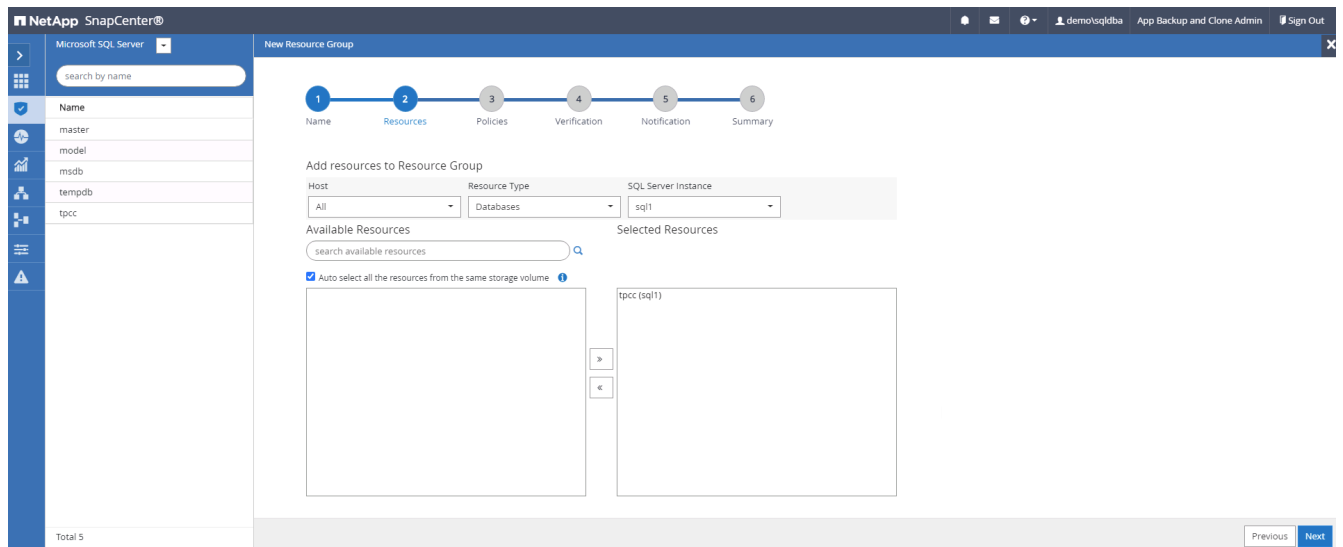


Erstellen Sie eine Ressourcengruppe für die vollständige Sicherung von SQL Server

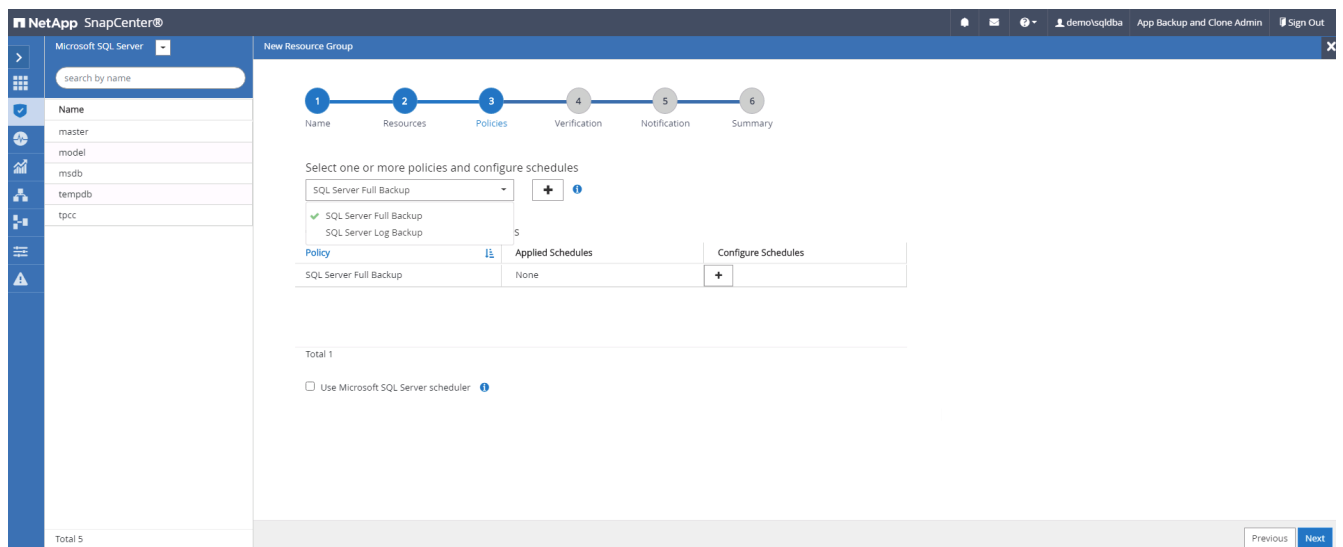
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdown-Liste Ansicht entweder eine Datenbank oder eine Ressourcengruppe aus, um den Arbeitsablauf für die Erstellung von Ressourcengruppen zu starten. Geben Sie einen Namen und Tags für die Ressourcengruppe an. Sie können ein Benennungsformat für die Snapshot Kopie definieren.



2. Wählen Sie die zu sichernden Datenbankressourcen aus.



3. Wählen Sie eine vollständige SQL-Backup-Richtlinie aus, die in Abschnitt 7 erstellt wurde.



4. Fügen Sie sowohl den genauen Zeitpunkt für Backups als auch die Häufigkeit hinzu.

Add schedules for policy SQL Server Full Backup

Daily

Start date 09/10/2021 6:20 PM

Expires on 12/31/2021 6:20 PM

Repeat every 1 days

i The schedules are triggered in the SnapCenter Server time zone.

Cancel OK

5. Wählen Sie den Verifizierungsserver für das Backup auf dem sekundären aus, wenn eine Backup-Überprüfung durchgeführt werden soll. Klicken Sie auf Load Locator, um den sekundären Speicherort zu füllen.

NetApp SnapCenter

Microsoft SQL Server

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select the verification servers

Verification server Select one or more servers

Load secondary locators to verify backups on secondary Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPremsql1_data	svm_hybridovosql1_data_dr
svm_onPremsql1_log	svm_hybridovosql1_log_dr

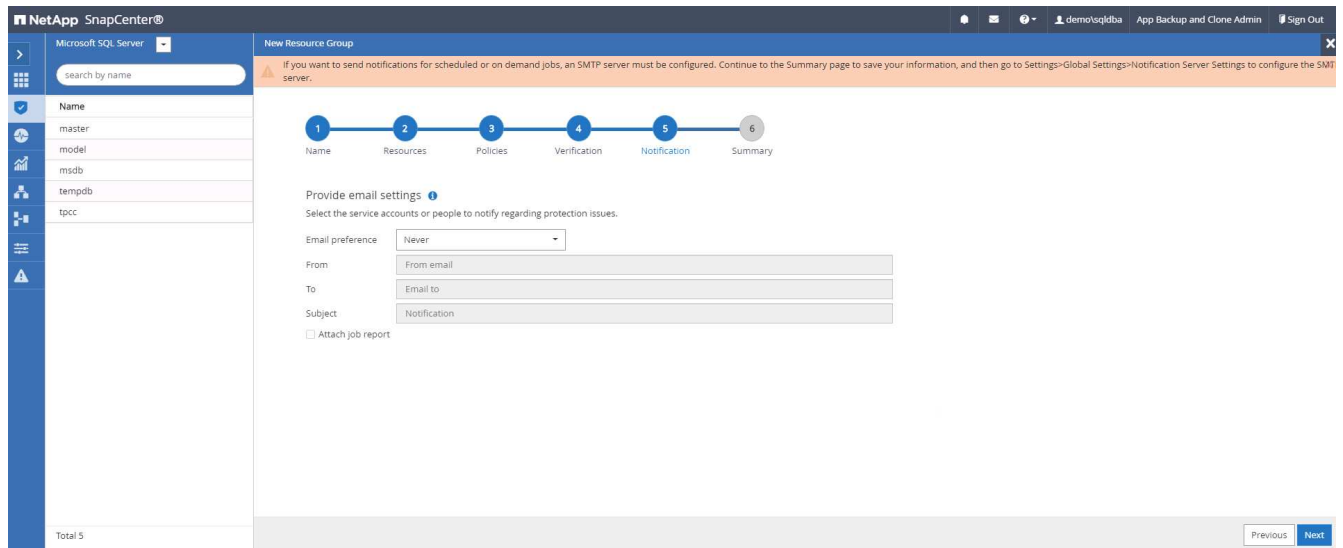
Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

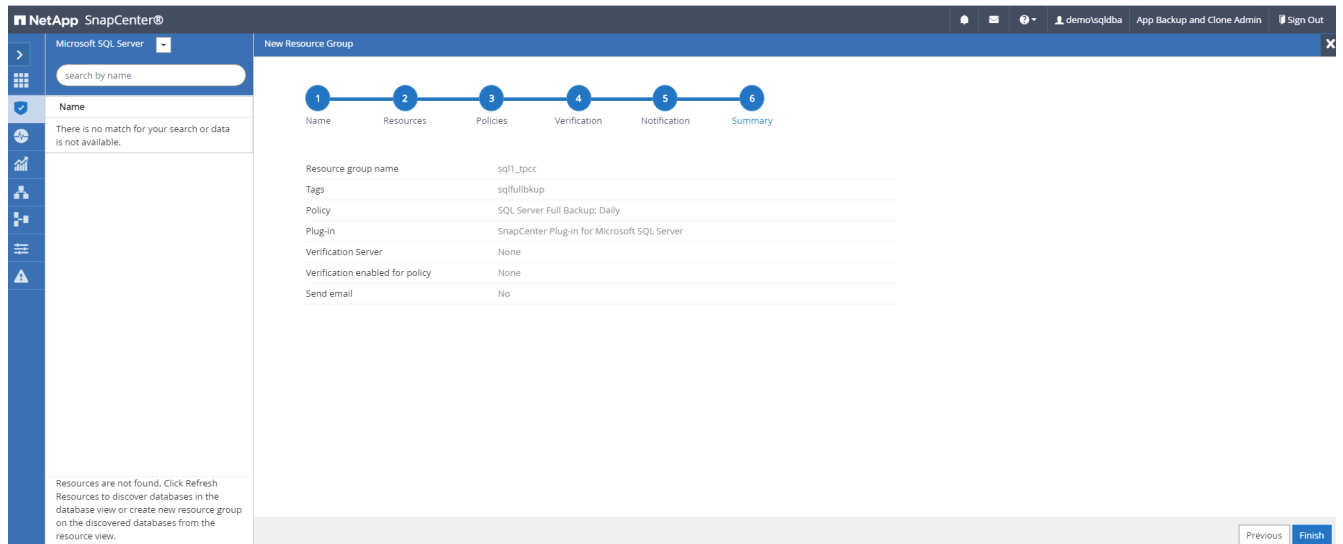
There is no match for your search or data is not available.

PREVIOUS Next

6. Konfigurieren Sie bei Bedarf den SMTP-Server für E-Mail-Benachrichtigungen.

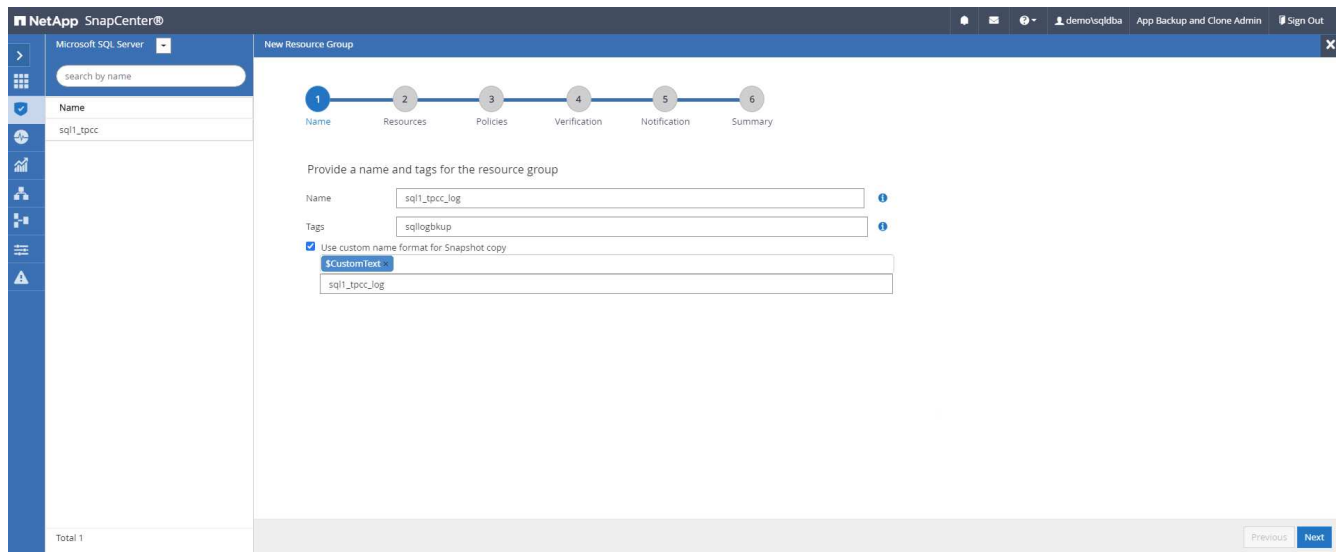


7. Zusammenfassung.

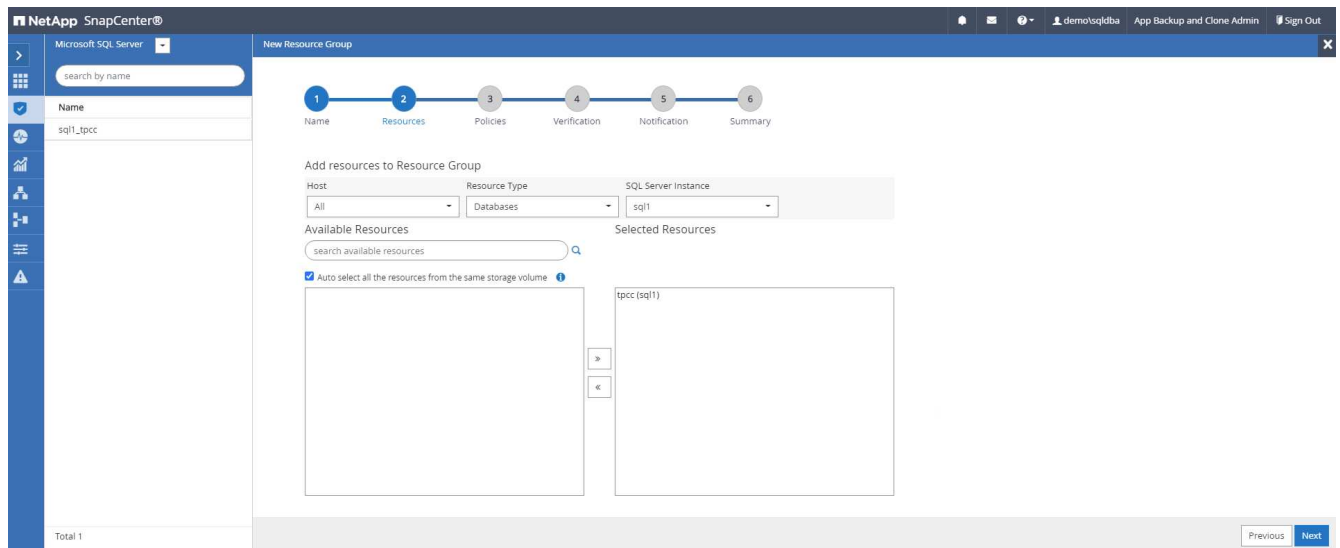


Erstellen Sie eine Ressourcengruppe für die Protokollsicherung von SQL Server

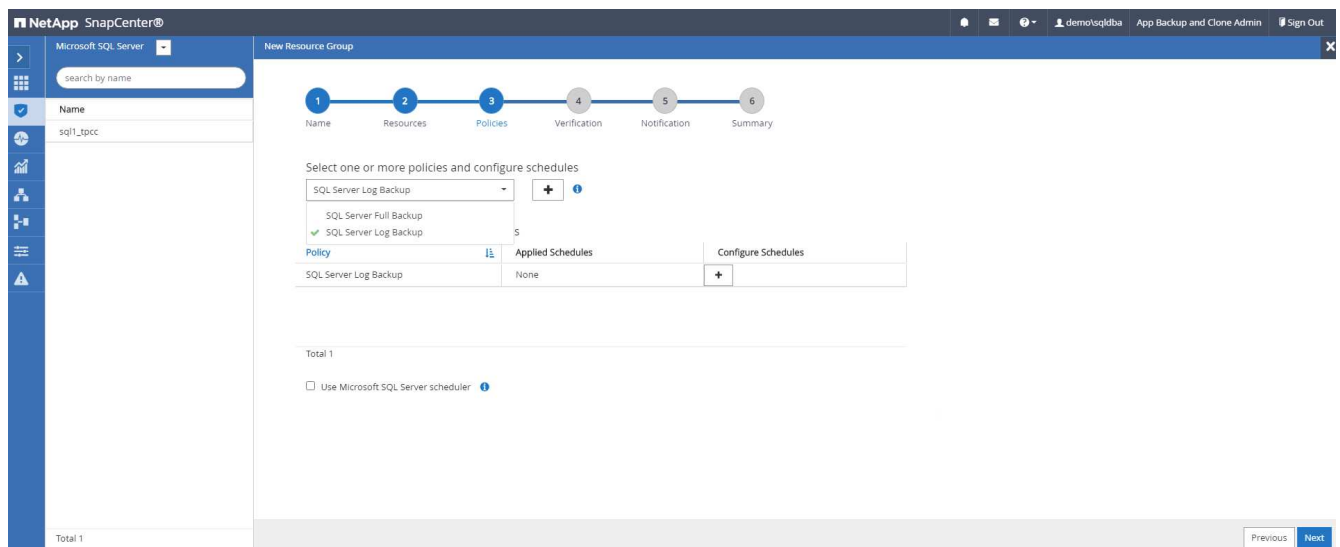
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdown-Liste Ansicht entweder eine Datenbank oder eine Ressourcengruppe aus, um den Arbeitsablauf für die Erstellung von Ressourcengruppen zu starten. Geben Sie den Namen und die Tags für die Ressourcengruppe an. Sie können ein Benennungsformat für die Snapshot Kopie definieren.



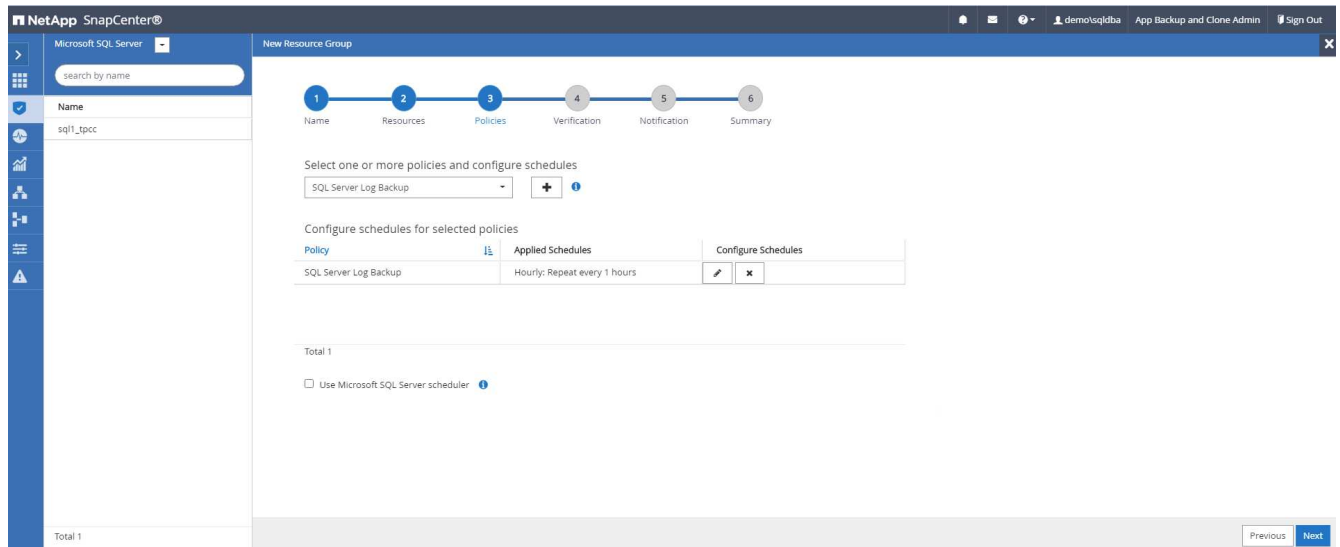
2. Wählen Sie die zu sichernden Datenbankressourcen aus.



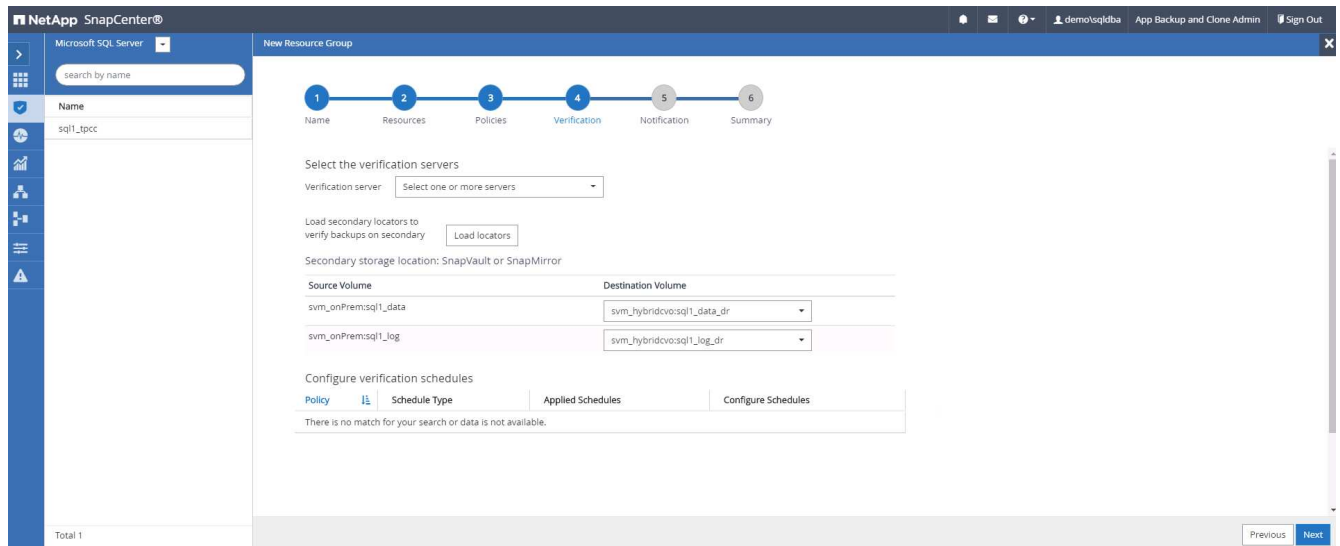
3. Wählen Sie eine in Abschnitt 7 erstellte SQL-Protokoll-Backup-Richtlinie aus.



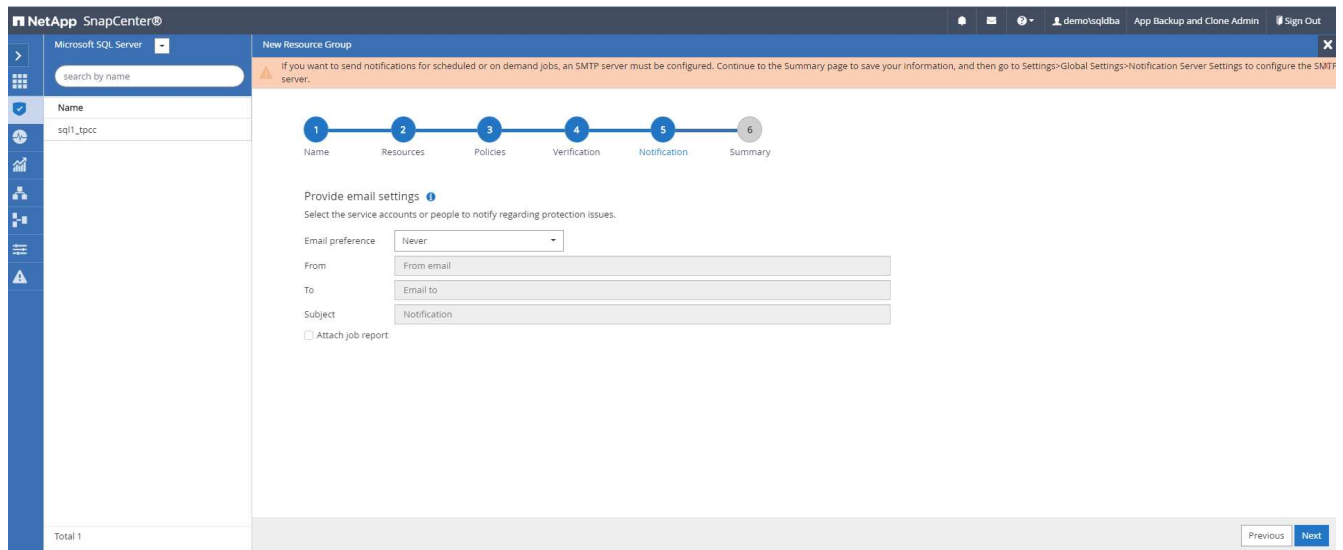
4. Fügen Sie den genauen Zeitpunkt für das Backup sowie die Häufigkeit hinzu.



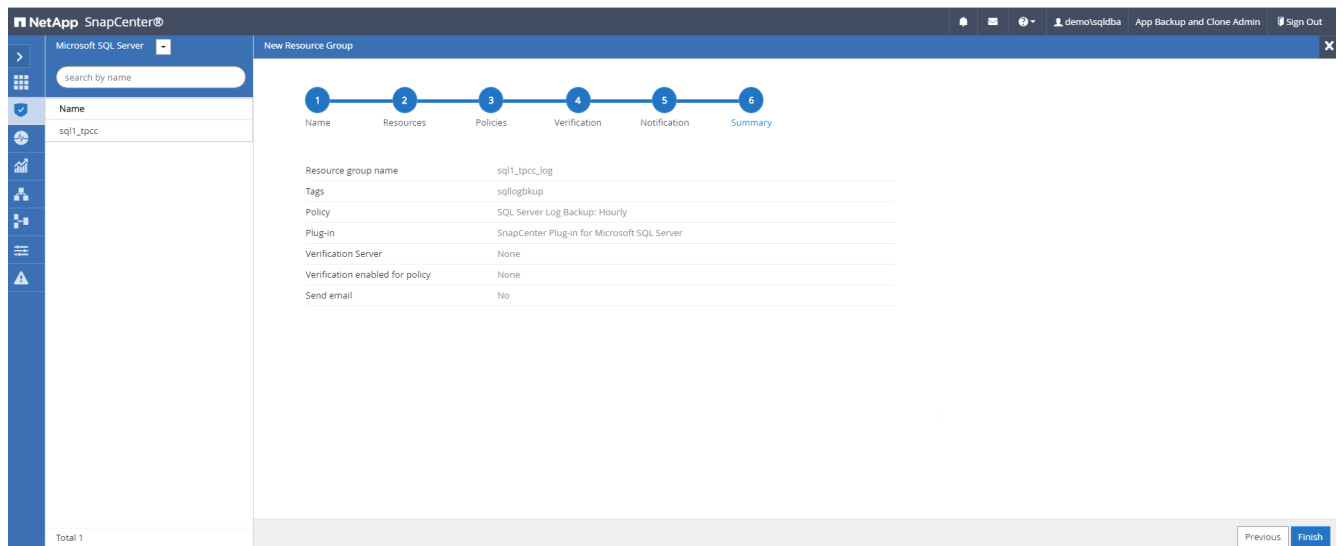
5. Wählen Sie den Verifizierungsserver für das Backup auf dem sekundären aus, wenn eine Backup-Überprüfung durchgeführt werden soll. Klicken Sie auf Load Locator, um den sekundären Speicherort zu füllen.



6. Konfigurieren Sie bei Bedarf den SMTP-Server für E-Mail-Benachrichtigungen.



7. Zusammenfassung.



9. Sicherung validieren

Nachdem Datenbanksicherungsressourcengruppen zum Schutz von Datenbankressourcen erstellt wurden, werden die Backupjobs gemäß dem vordefinierten Zeitplan ausgeführt. Überprüfen Sie den Status der Auftragsausführung auf der Registerkarte Überwachung.

ID	Status	Name	Start date	End date	Owner
532	Success	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM	09/14/2021 8:37:10 PM	demo\sqlqdba
528	Success	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM	09/14/2021 7:37:09 PM	demo\sqlqdba
524	Success	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 6:35:01 PM	09/14/2021 6:37:08 PM	demo\sqlqdba
521	Success	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM	demo\sqlqdba
517	Success	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 5:35:01 PM	09/14/2021 5:37:09 PM	demo\sqlqdba
513	Success	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 4:35:01 PM	09/14/2021 4:37:08 PM	demo\sqlqdba
509	Success	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM	09/14/2021 3:37:10 PM	demo\sqlqdba
503	Success	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM	09/14/2021 2:37:09 PM	demo\sqlqdba

Wechseln Sie zur Registerkarte Ressourcen, klicken Sie auf den Datenbanknamen, um Details zum

Datenbank-Backup anzuzeigen, und wechseln Sie zwischen lokalen Kopien und gespiegelten Kopien. So überprüfen Sie, ob Snapshot Backups an einem sekundären Standort in der Public Cloud repliziert werden.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhe12_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhe12_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhe12_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhe12_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhe12_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM	Not Applicable	False	Not Cataloged	6598735

Zu diesem Zeitpunkt sind Datenbank-Backup-Kopien in der Cloud bereit für das Klonen, um Entwicklungs-/Testprozesse auszuführen oder um bei einem primären Ausfall eine Disaster Recovery durchzuführen.

Erste Schritte mit der AWS Public Cloud

In diesem Abschnitt wird der Bereitstellungsprozess von Cloud Manager und Cloud Volumes ONTAP in AWS beschrieben.

AWS Public Cloud



Um die folgenden Elemente zu vereinfachen, haben wir dieses Dokument auf Basis einer Implementierung in AWS erstellt. Allerdings ist der Prozess für Azure und GCP sehr ähnlich.

1. Scheck vor dem Flug

Stellen Sie vor der Implementierung sicher, dass die Infrastruktur vorhanden ist, die eine Implementierung in der nächsten Phase ermöglicht. Dazu gehört Folgendes:

- AWS Konto
- VPC in Ihrer bevorzugten Region
- Subnetz mit Zugang zum öffentlichen Internet
- Berechtigungen zum Hinzufügen von IAM-Rollen in Ihrem AWS-Konto
- Ein geheimer Schlüssel und Zugriffsschlüssel für Ihren AWS-Benutzer

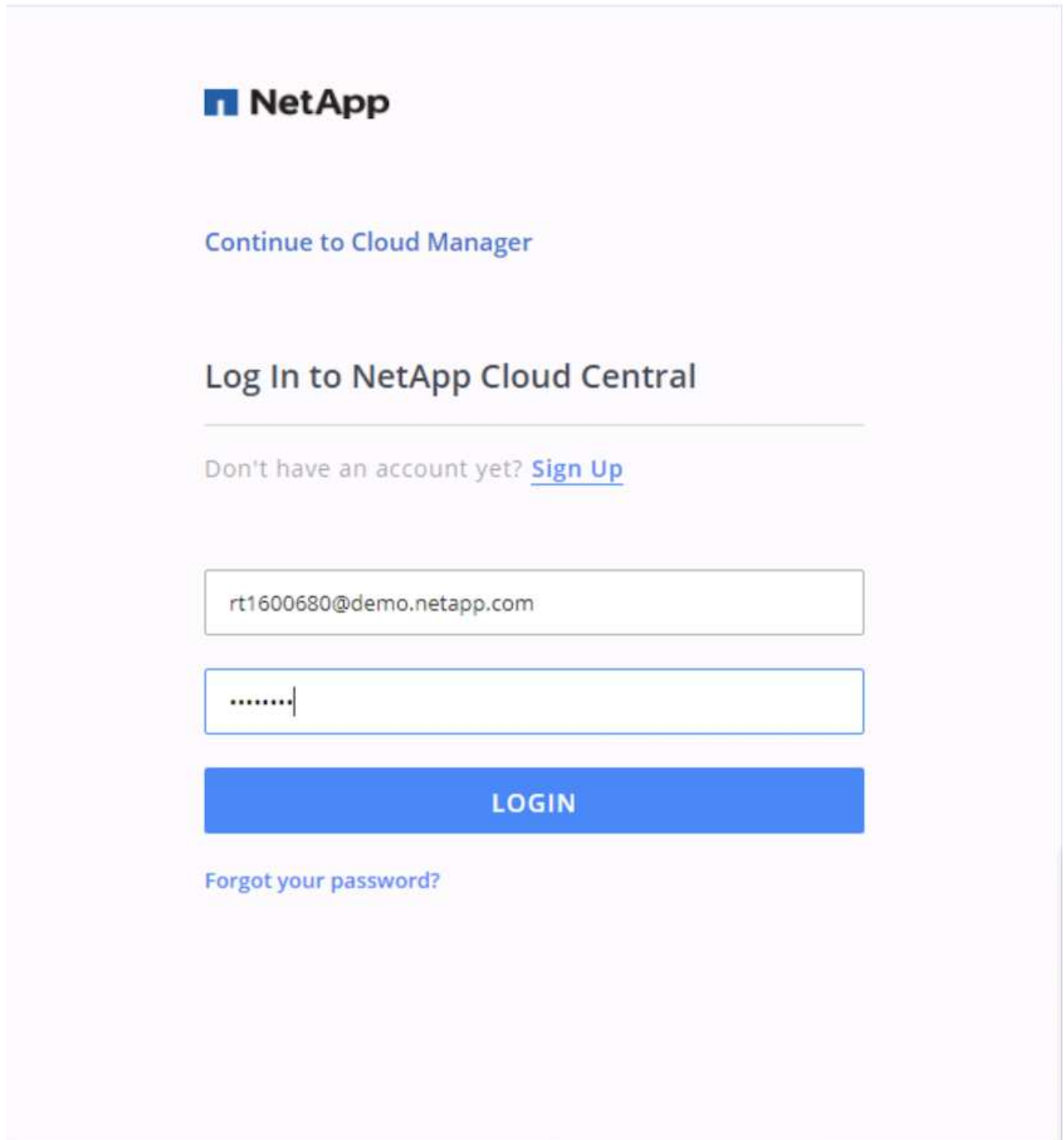
2. Schritte zur Implementierung von Cloud Manager und Cloud Volumes ONTAP in AWS



Für die Implementierung von Cloud Manager und Cloud Volumes ONTAP gibt es viele Methoden. Diese Methode ist die einfachste, erfordert jedoch die meisten Berechtigungen. Falls diese Methode für Ihre AWS-Umgebung nicht geeignet ist, schlagen Sie bitte in nach "[NetApp Cloud-Dokumentation](#)".

Implementieren Sie den Cloud Manager Connector

1. Navigieren Sie zu "NetApp Cloud Central" Und melden Sie sich an oder registrieren Sie sich.



NetApp

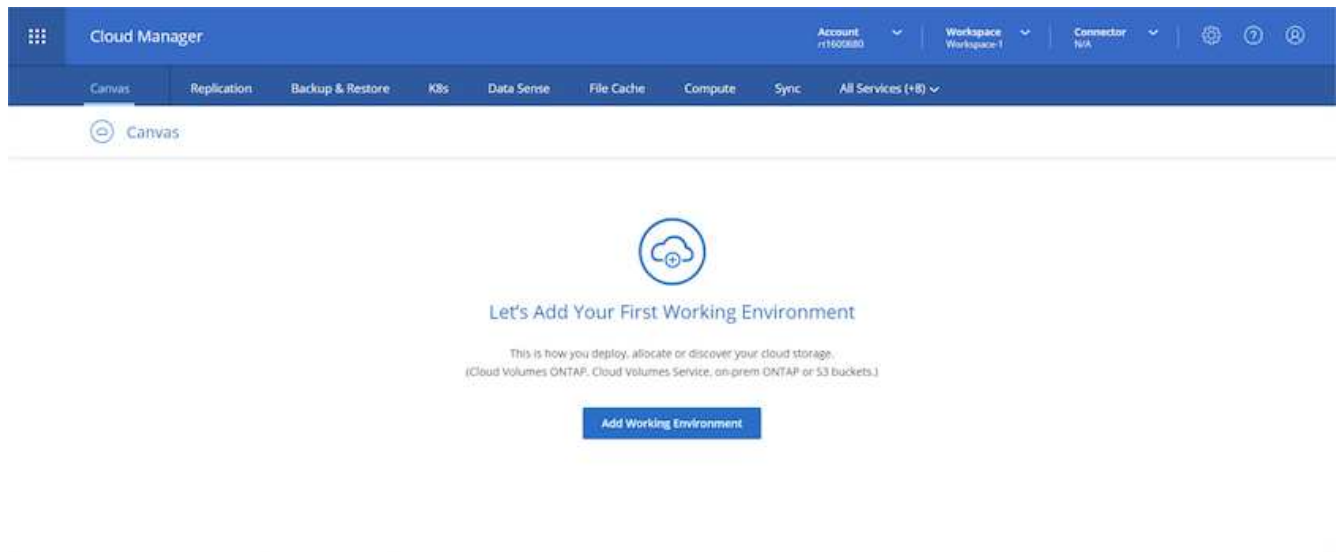
Continue to Cloud Manager

Log In to NetApp Cloud Central

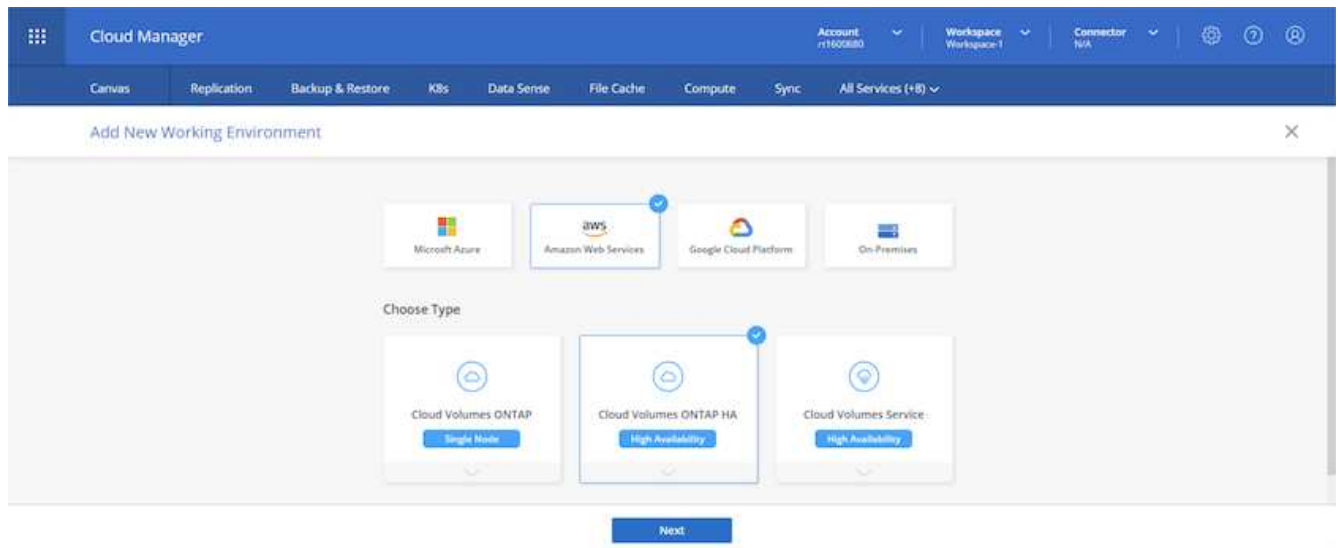
Don't have an account yet? [Sign Up](#)

LOGIN
[Forgot your password?](#)

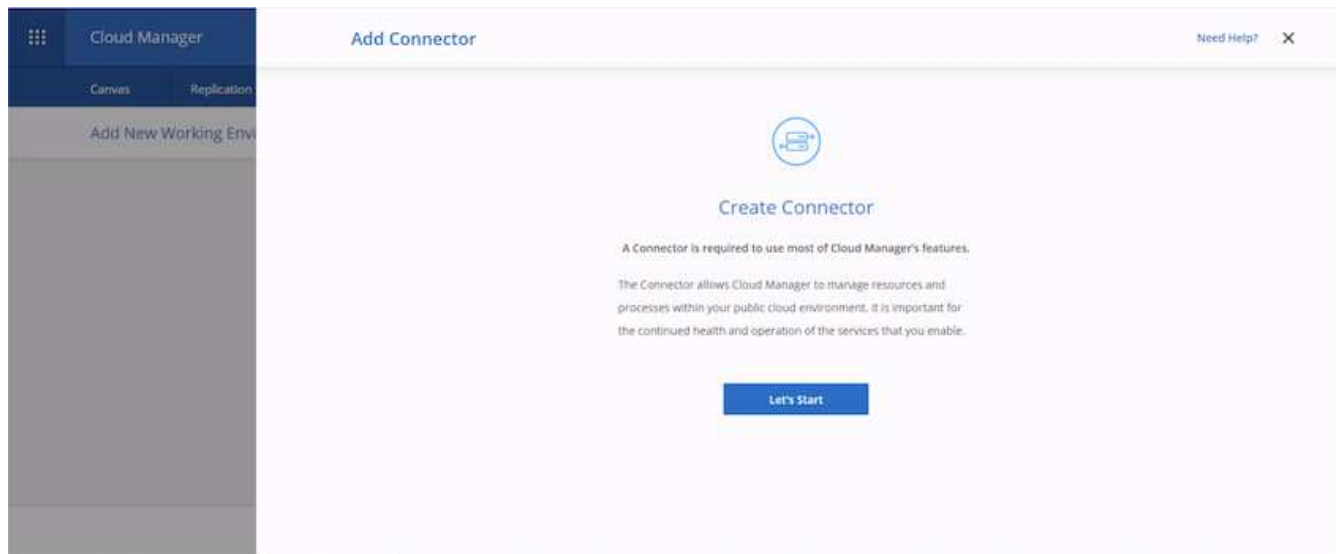
2. Nach der Anmeldung sollten Sie auf den Bildschirm gebracht werden.



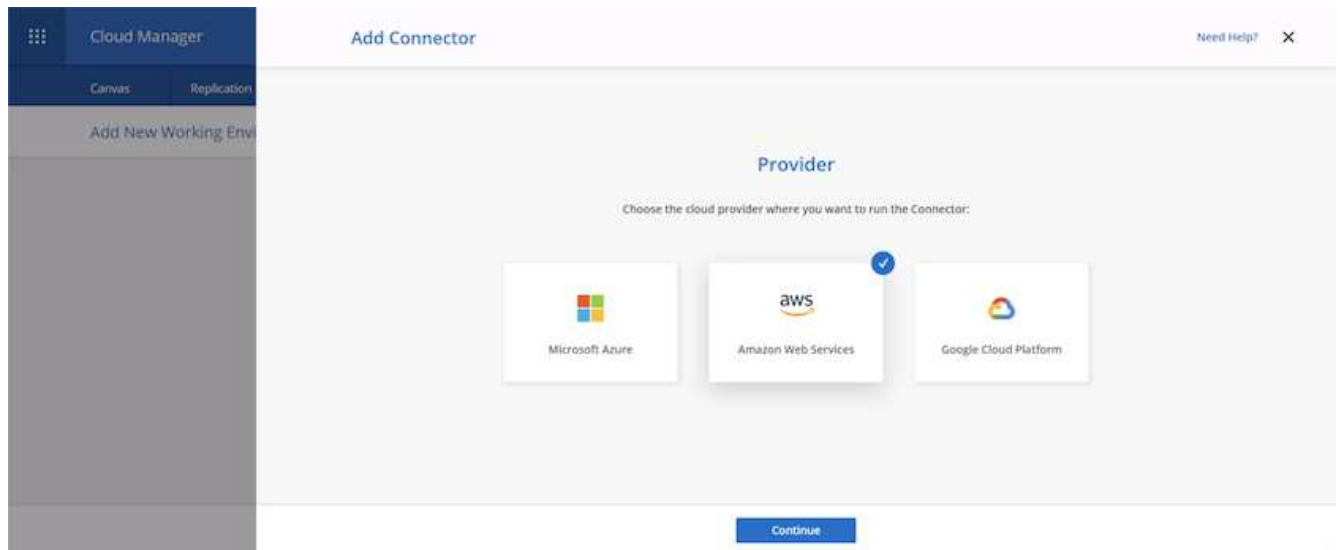
3. Klicken Sie auf „Arbeitsumgebung hinzufügen“ und wählen Sie Cloud Volumes ONTAP in AWS. Hier haben Sie außerdem die Wahl, ob Sie ein Single Node-System oder ein Hochverfügbarkeitspaar implementieren möchten. Ich habe mich entschieden, ein Hochverfügbarkeitspaar bereitzustellen.



4. Wenn kein Anschluss erstellt wurde, wird ein Popup-Fenster angezeigt, in dem Sie aufgefordert werden, einen Anschluss zu erstellen.



5. Klicken Sie auf „Start“ und anschließend auf „AWS“.



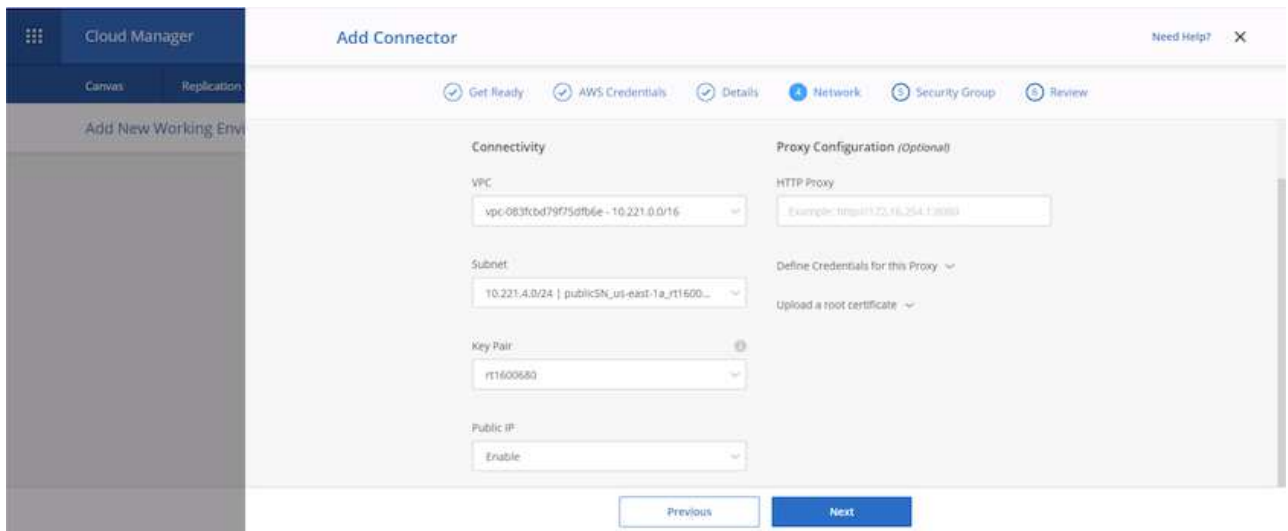
6. Geben Sie Ihren geheimen Schlüssel und den Zugriffsschlüssel ein. Stellen Sie sicher, dass Ihr Benutzer über die auf dem angegebenen korrekten Berechtigungen verfügt "[Die NetApp Richtlinien](#)".

The screenshot shows the 'Add Connector' wizard in AWS Cloud Manager. The current step is 'AWS Credentials'. The 'AWS Access Key' field is empty and has a red error message 'AWS Access Key is required' below it. The 'AWS Secret Key' field contains a masked password. The 'Region' dropdown is set to 'us-east-1 | US East (N. Virginia)'. There is a checkbox for 'Want to launch an instance without AWS Credentials?' which is currently unchecked. The 'Next' button is highlighted in blue.

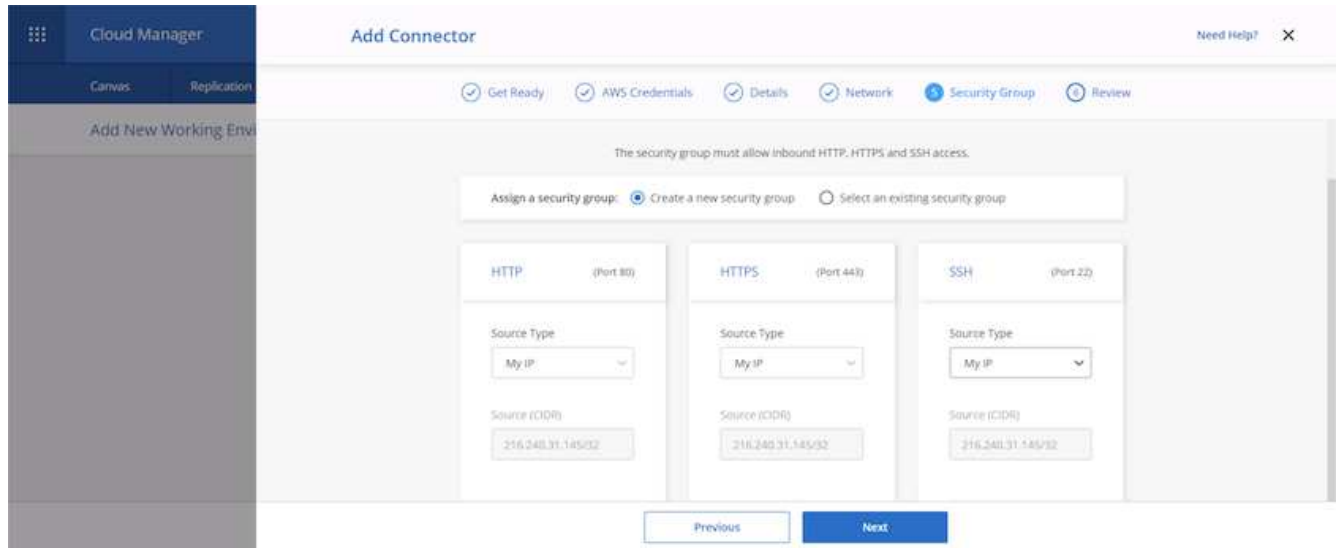
7. Geben Sie dem Konnektor einen Namen und verwenden Sie entweder eine vordefinierte Rolle, wie auf der beschriebenen "Die NetApp Richtlinien" Oder Fragen Sie Cloud Manager, welche Rolle Sie dabei spielen sollten.

The screenshot shows the 'Add Connector' wizard in AWS Cloud Manager. The current step is 'Details'. The 'Connector Instance Name' field contains 'awscloudmanager'. The 'Connector Role' section has 'Create Role' selected. The 'Role Name' field contains 'Cloud-Manager-Operator-IBnt24'. There is a '+ Add Tags to Connector Instance' button. The 'Next' button is highlighted in blue.

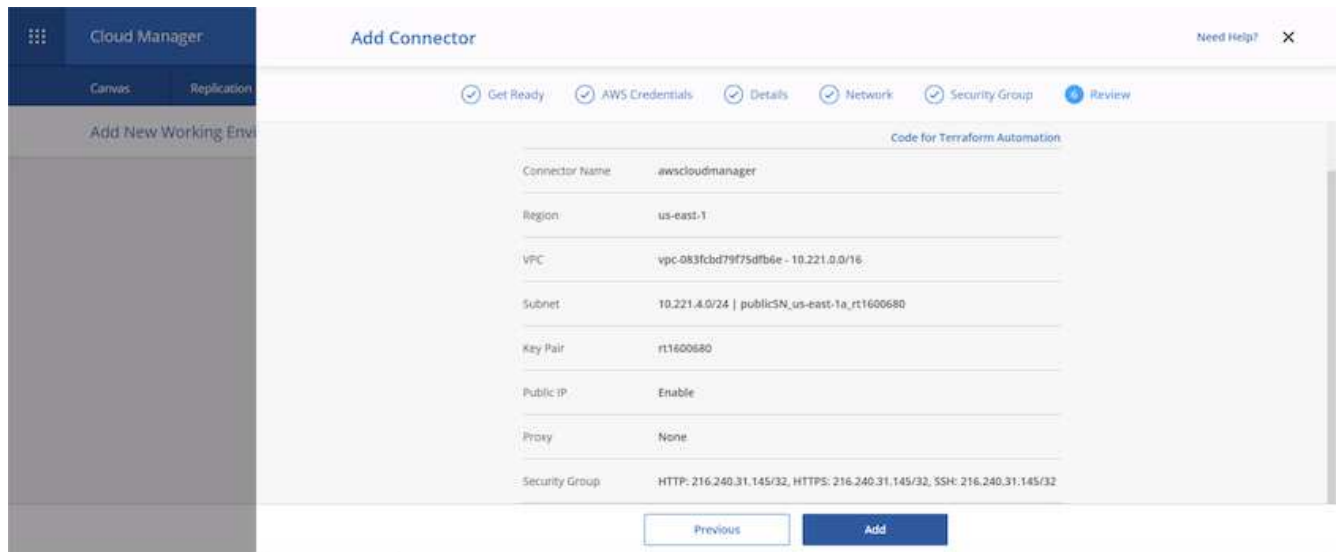
8. Geben Sie die für die Bereitstellung des Connectors erforderlichen Netzwerkinformationen an. Vergewissern Sie sich, dass der ausgehende Internetzugang aktiviert ist, indem Sie:
- Geben der Verbindung eine öffentliche IP-Adresse
 - Dem Anschluss einen Proxy zur Verfügung stellen, der funktioniert
 - Dem Anschluss eine Route zum öffentlichen Internet über ein Internet-Gateway geben



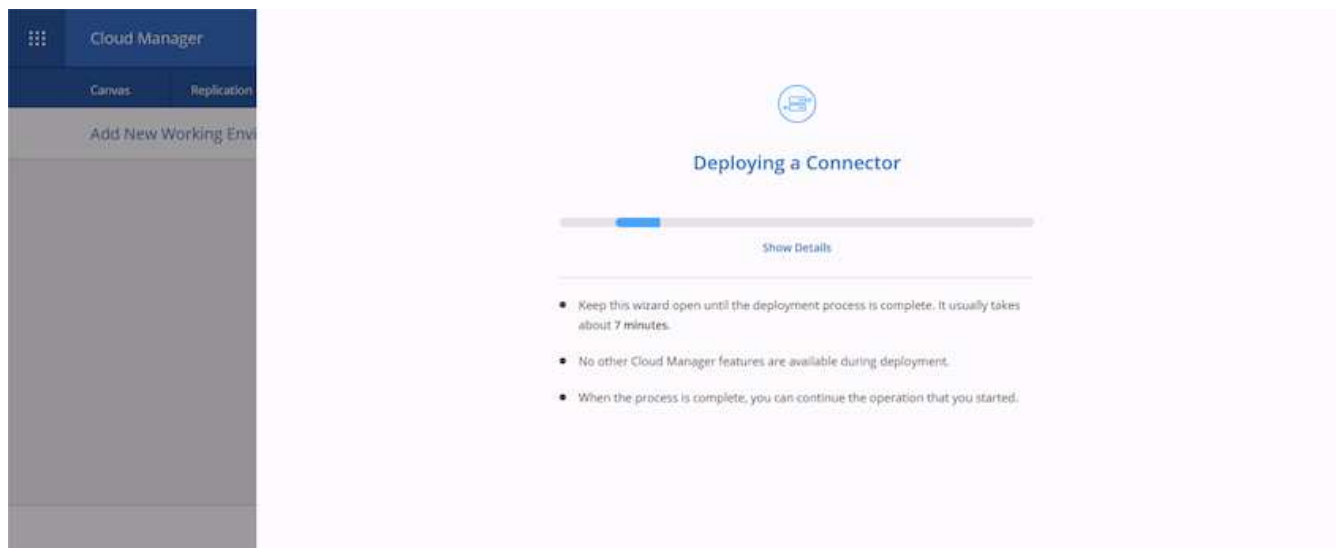
9. Ermöglichen Sie die Kommunikation mit dem Connector über SSH, HTTP und HTTPS, indem Sie entweder eine Sicherheitsgruppe bereitstellen oder eine neue Sicherheitsgruppe erstellen. Ich habe nur von meiner IP-Adresse aus den Zugriff auf den Konnektor aktiviert.



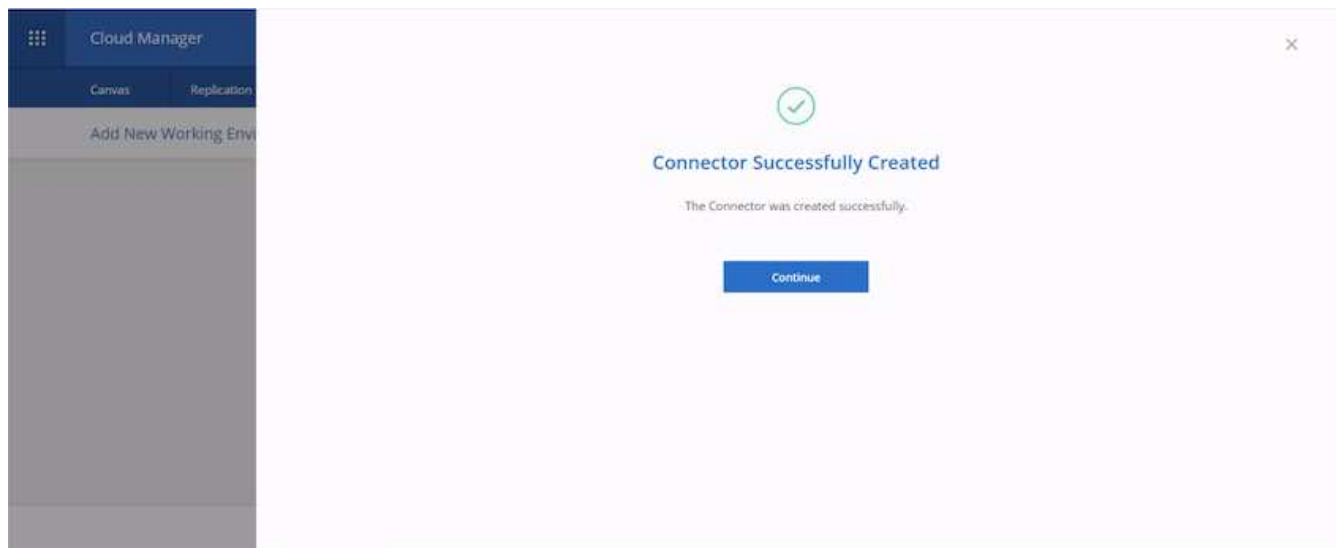
10. Überprüfen Sie die Informationen auf der Übersichtsseite, und klicken Sie auf Hinzufügen, um den Connector bereitzustellen.



11. Der Connector wird nun mit einem Cloud-Formierung-Stack implementiert. Sie können den Fortschritt von Cloud Manager oder über AWS überwachen.

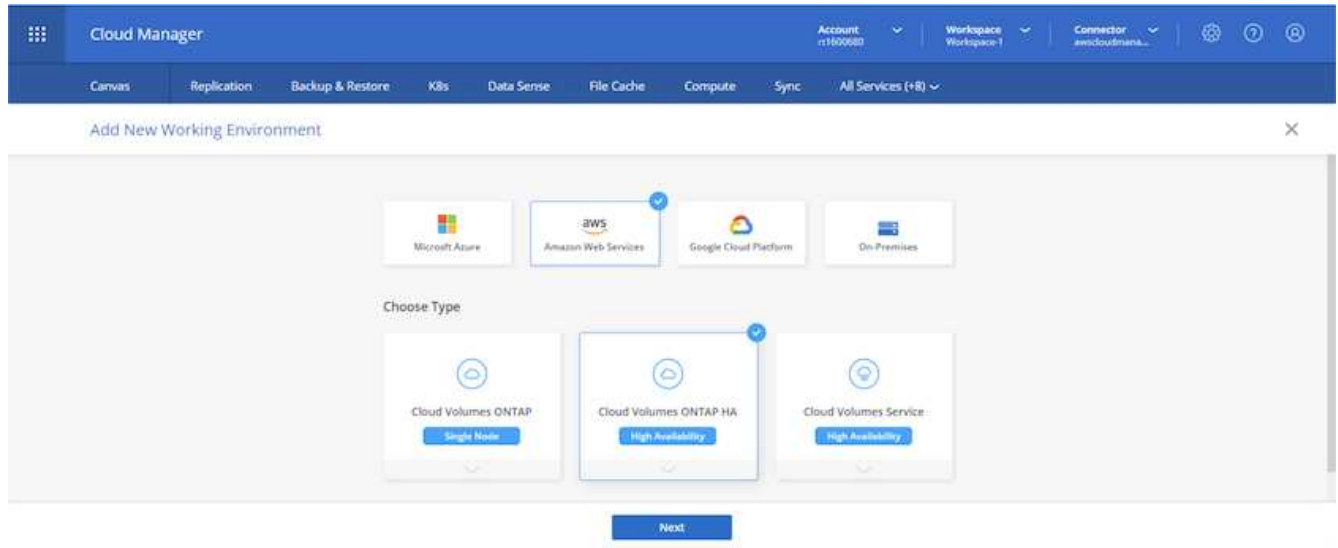


12. Wenn die Bereitstellung abgeschlossen ist, wird eine Seite mit dem Erfolg angezeigt.

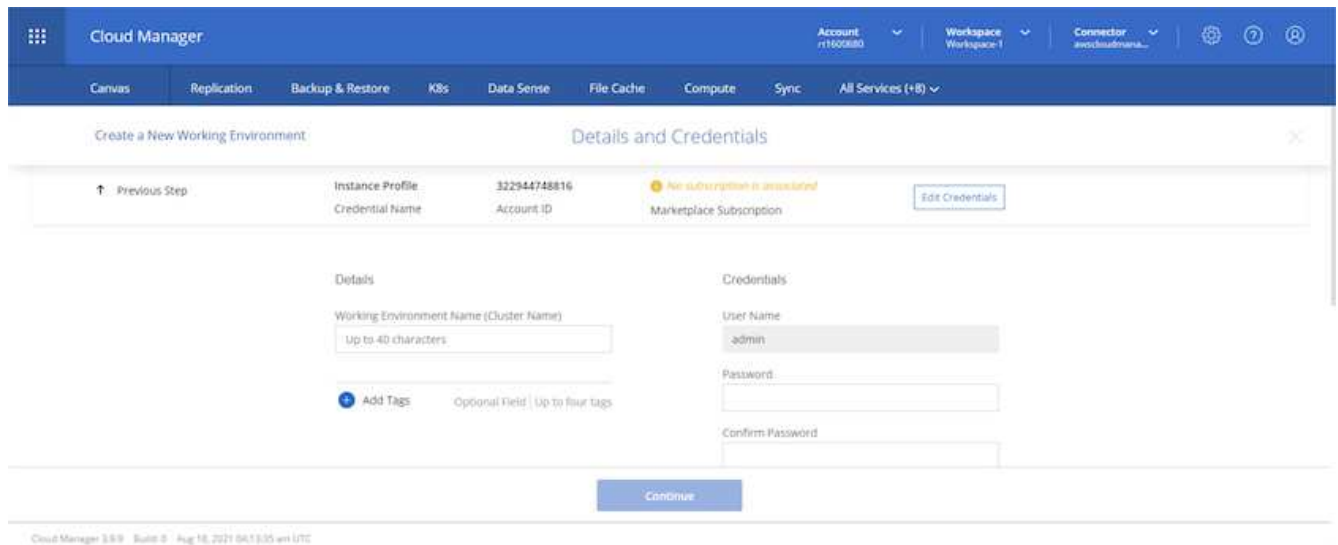


Implementieren Sie Cloud Volumes ONTAP

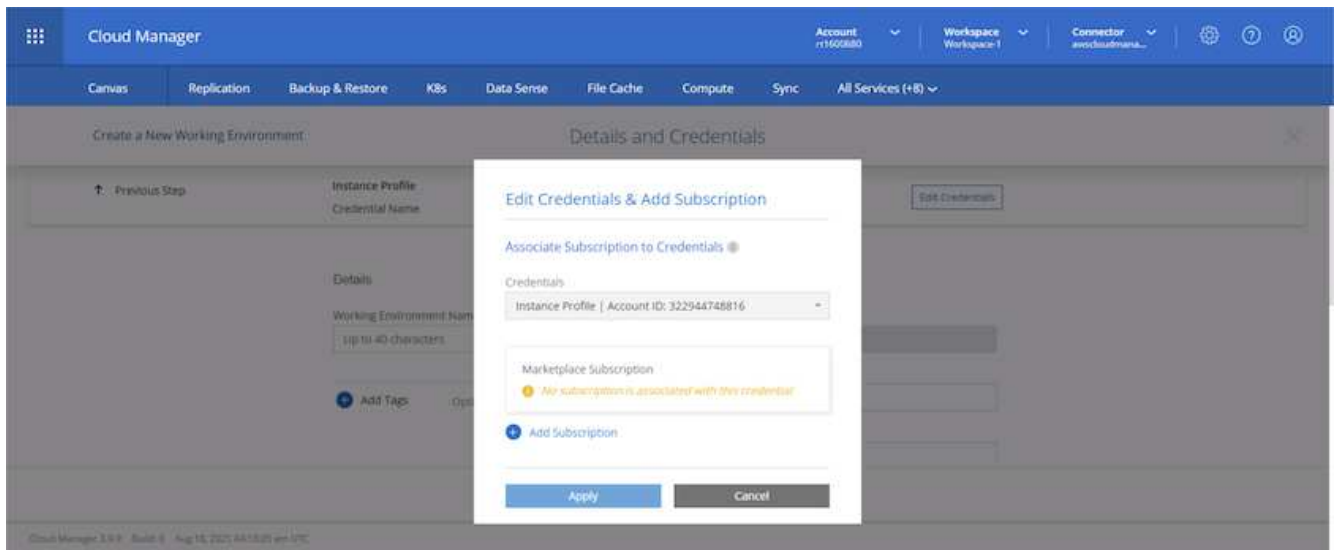
1. Wählen Sie AWS und die Art der Implementierung auf der Grundlage Ihrer Anforderungen aus.



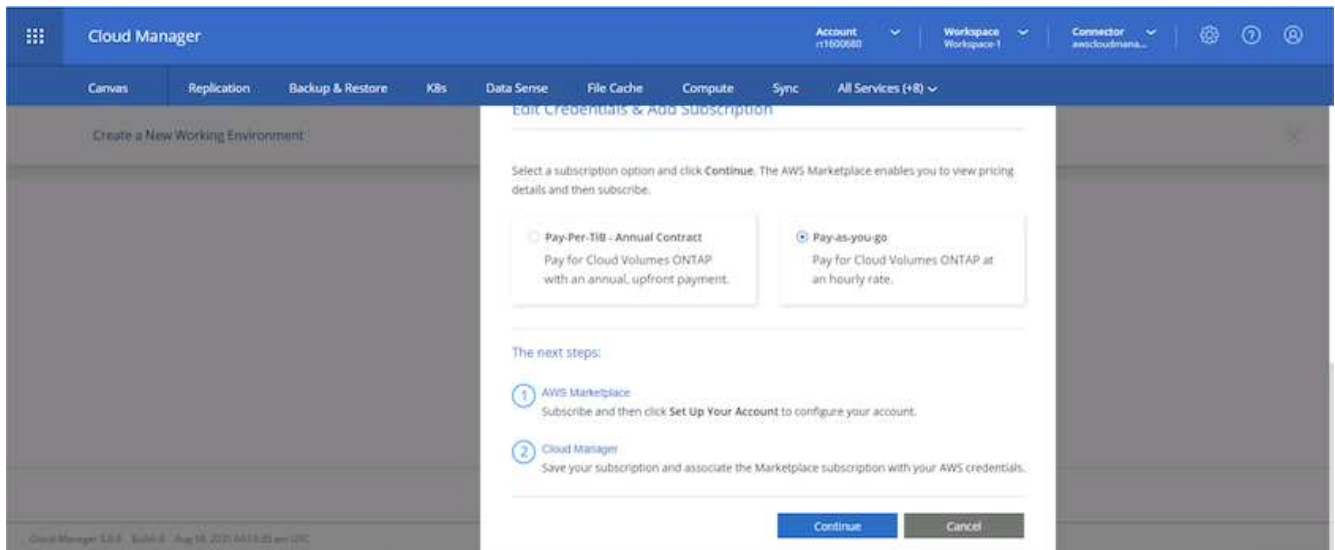
2. Wenn kein Abonnement zugewiesen wurde und Sie mit PAYGO kaufen möchten, wählen Sie Anmeldedaten bearbeiten.



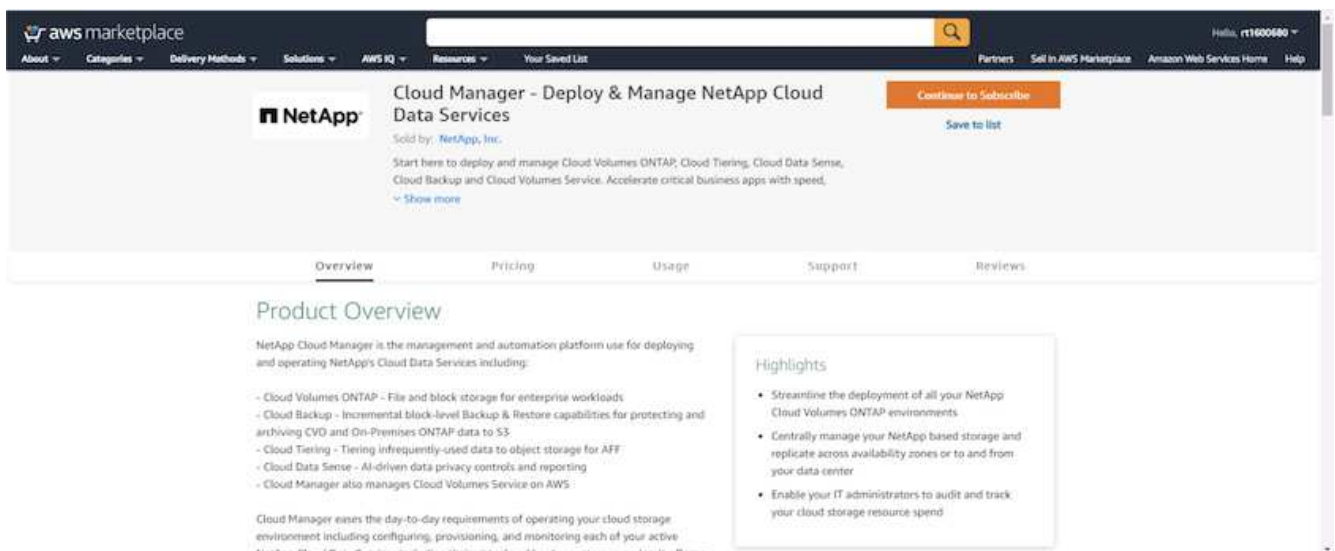
3. Wählen Sie Abonnement Hinzufügen.



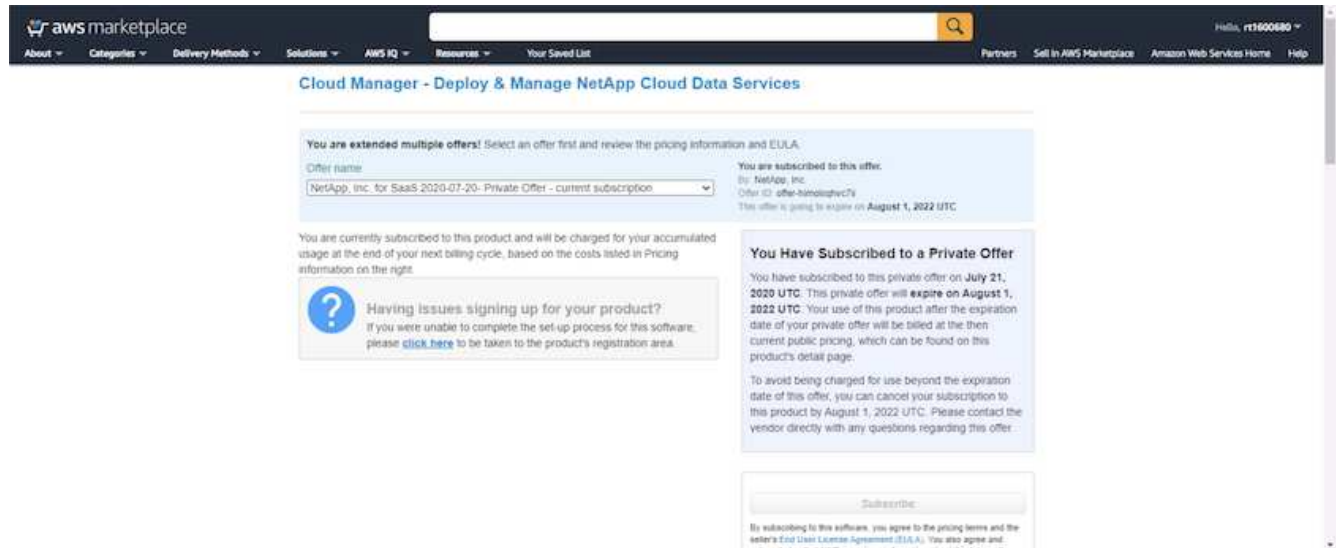
4. Wählen Sie den Vertrag aus, den Sie abonnieren möchten. Ich entschied mich für Pay-as-you-go.



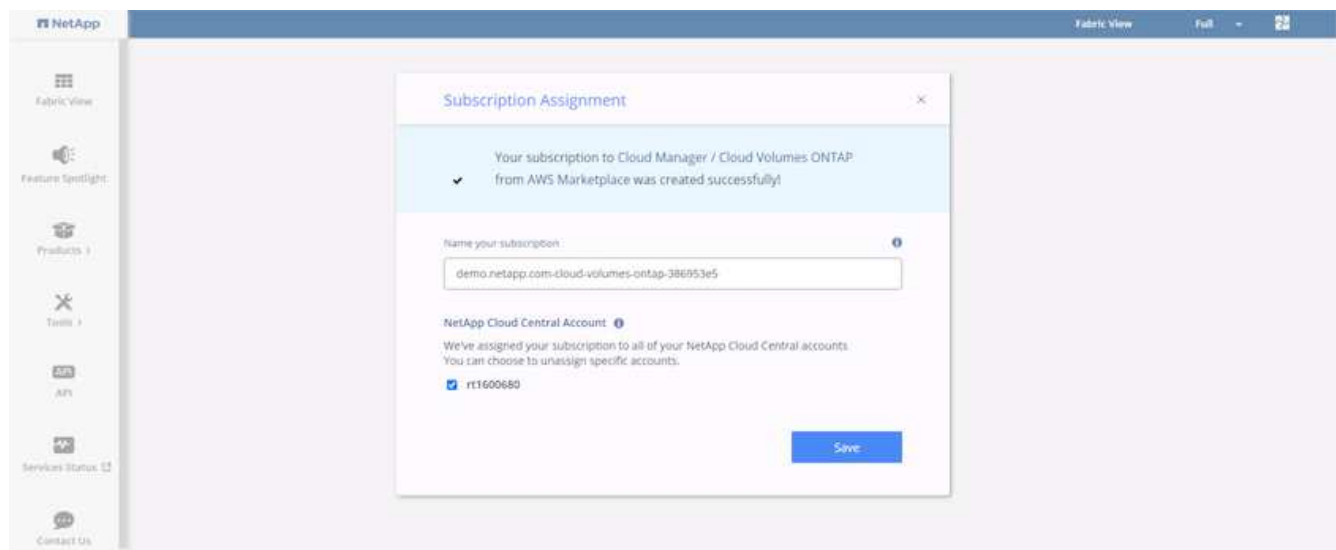
5. Sie werden zu AWS umgeleitet und wählen Sie „Weiter“, um sich Abonnieren zu öffnen.



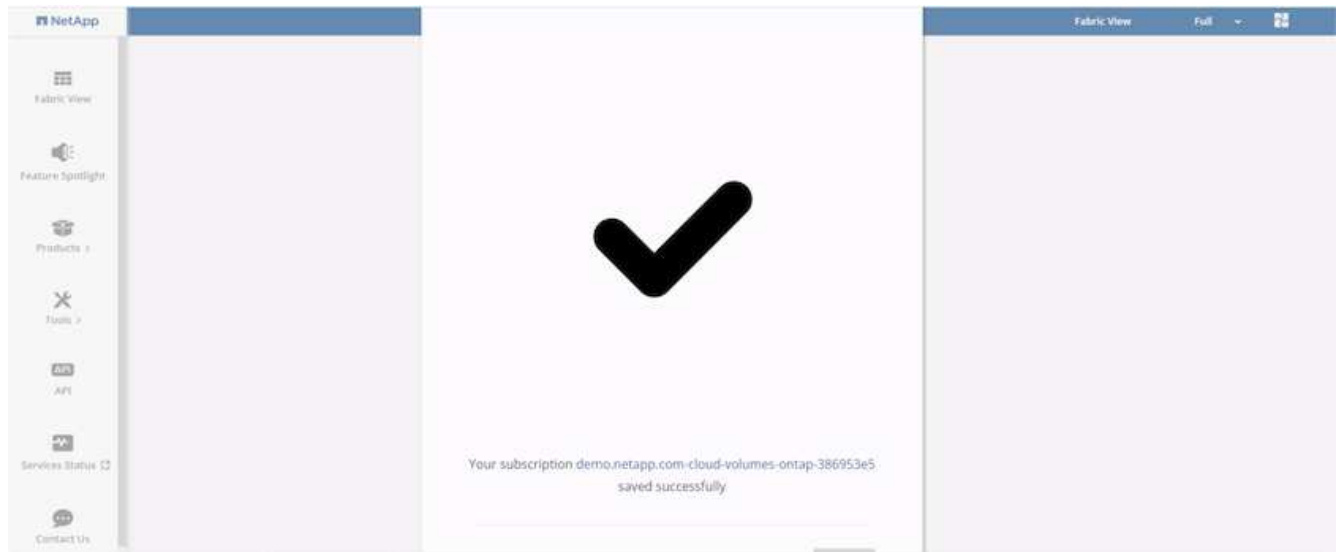
6. Melden Sie sich an und Sie werden zurück auf NetApp Cloud Central umgeleitet. Wenn Sie bereits abonniert haben und nicht umgeleitet werden, klicken Sie auf den Link "Hier klicken".



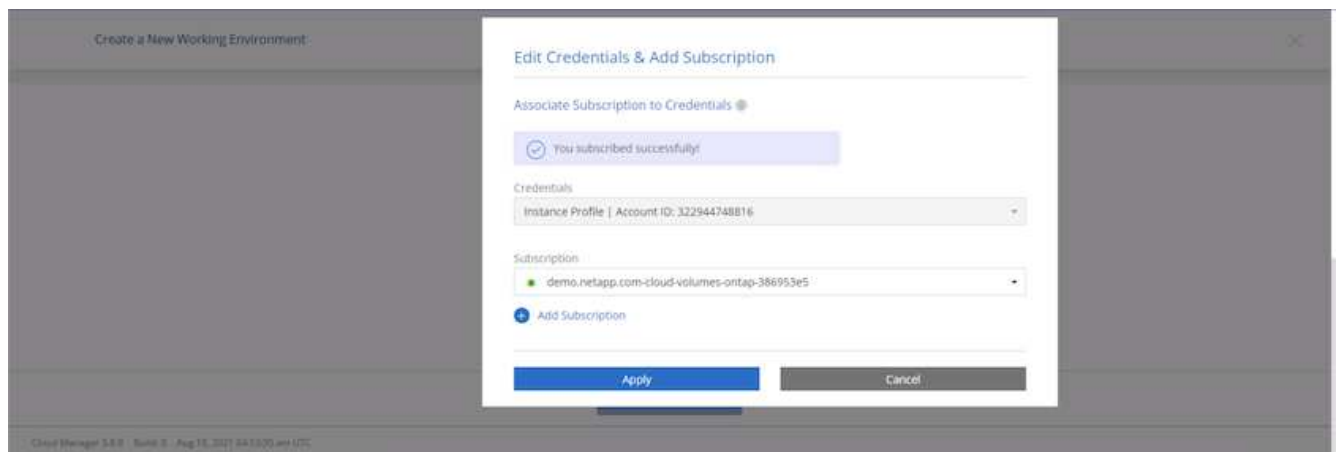
7. Sie werden zu Cloud Central umgeleitet. Dort müssen Sie die Namen Ihres Abonnements benennen und es Ihrem Cloud Central Konto zuweisen.



8. Wenn der Erfolg abgeschlossen ist, wird eine Seite mit den Häkchen angezeigt. Öffnen Sie die Registerkarte „Cloud Manager“.

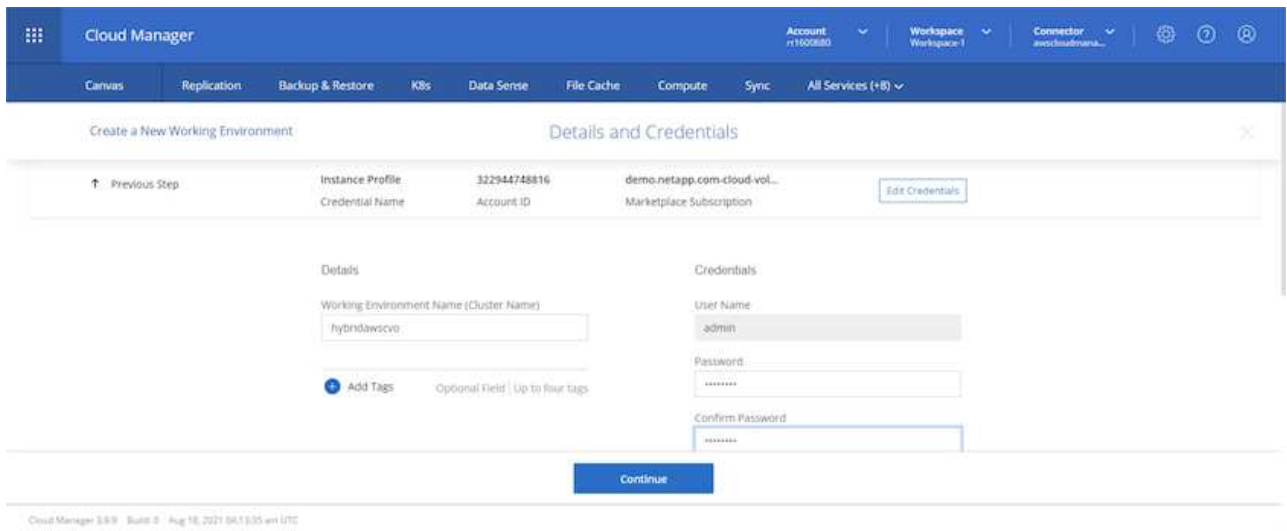


9. Das Abonnement wird jetzt in Cloud Central angezeigt. Klicken Sie auf Anwenden, um fortzufahren.

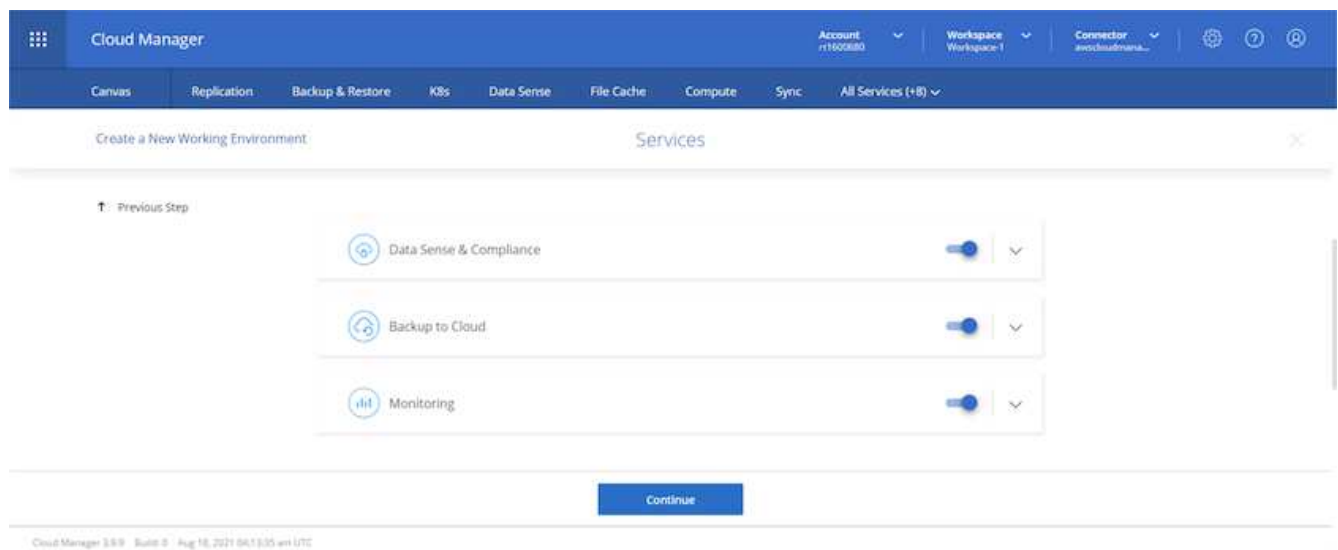


10. Geben Sie die Angaben zur Arbeitsumgebung ein, z. B.:

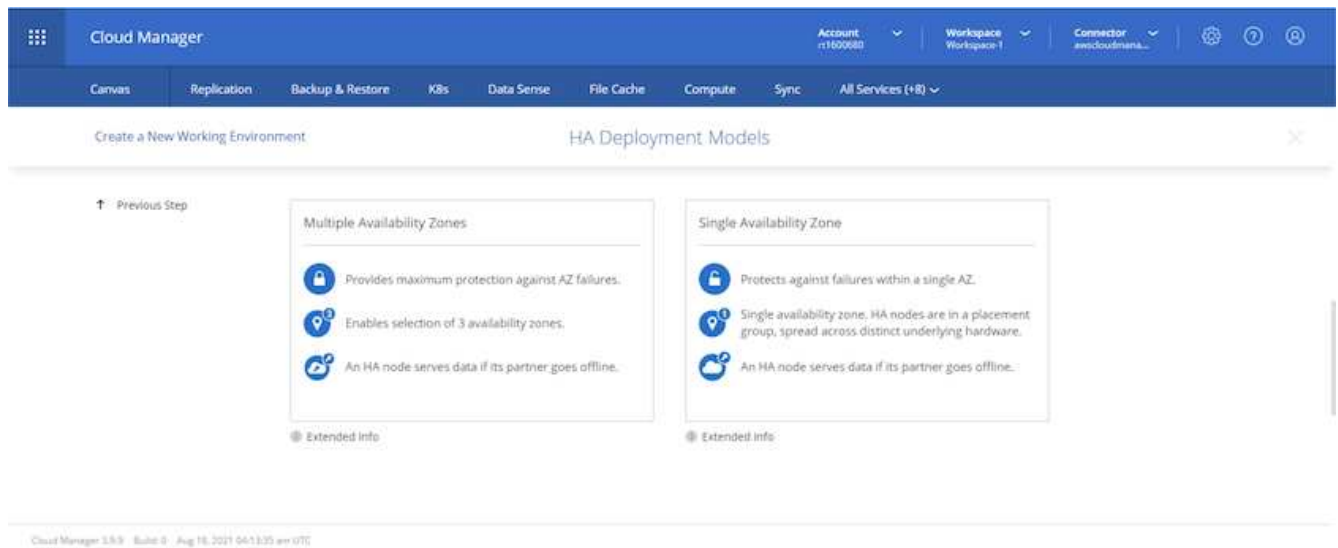
- a. Cluster-Name
- b. Cluster-Passwort
- c. AWS Tags (optional)



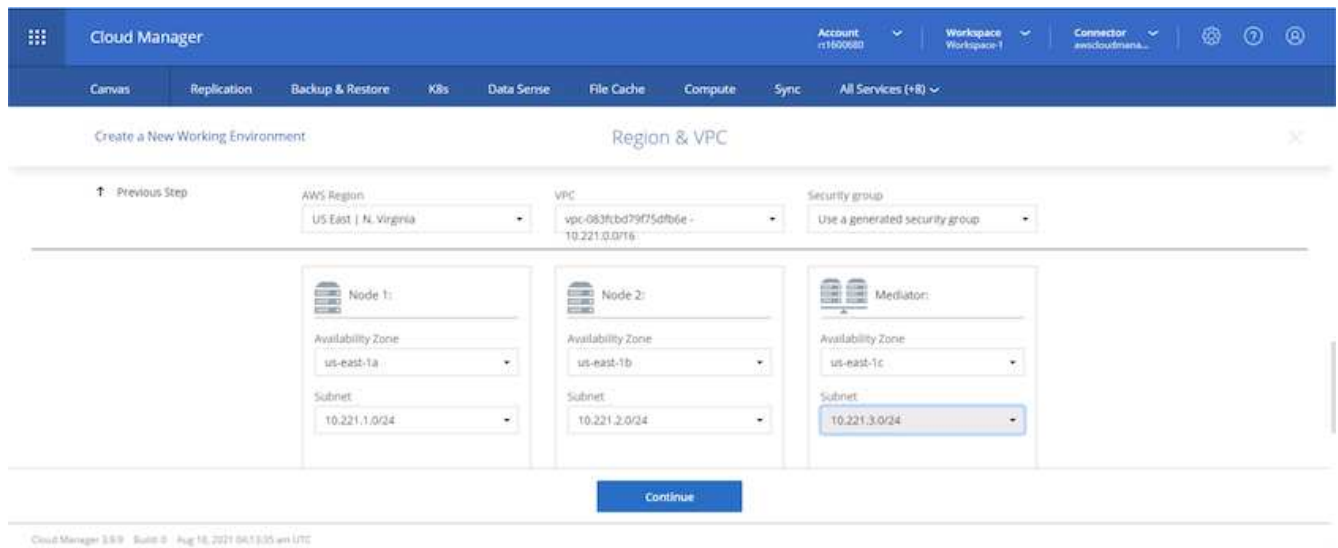
11. Wählen Sie aus, welche zusätzlichen Services Sie bereitstellen möchten. Weitere Informationen zu diesen Services finden Sie auf der "NetApp Cloud Homepage".



12. Wählen Sie, ob die Implementierung in mehreren Verfügbarkeitszonen erfolgen soll (erfordert drei Subnetze, jede in einer anderen Verfügbarkeitszone) oder eine einzelne Verfügbarkeitszone. Ich habe mehrere AZS ausgewählt.



13. Wählen Sie die Region, die VPC und die Sicherheitsgruppe für das zu implementierende Cluster aus. In diesem Abschnitt weisen Sie außerdem die Verfügbarkeitszonen pro Node (und Mediator) sowie die Subnetze zu, in denen sie tätig sind.



14. Wählen Sie die Verbindungsmethoden für die Nodes und den Mediator.



Der Mediator muss mit den AWS APIs kommunizieren. Es ist keine öffentliche IP-Adresse erforderlich, solange die APIs nach der Implementierung der Mediator EC2 Instanz erreichbar sind.

1. Mit fließenden IP-Adressen wird der Zugriff auf die verschiedenen von Cloud Volumes ONTAP verwendeten IP-Adressen ermöglicht, einschließlich Cluster-Management und DatenserverIPs. Diese Adressen müssen nicht bereits in Ihrem Netzwerk routingfähig sein und zu Routing-Tabellen in Ihrer AWS-Umgebung hinzugefügt werden. Sie sind erforderlich, um während des Failover konsistente IP-Adressen für ein HA-Paar zu aktivieren. Weitere Informationen zu schwimmenden IP-Adressen finden Sie im "[NetApp Cloud Documentation](#)".

2. Wählen Sie aus, zu welchen Routingtabellen die unverankerten IP-Adressen hinzugefügt werden sollen. Diese Routingtabellen werden von Clients für die Kommunikation mit Cloud Volumes ONTAP verwendet.

Cloud Manager

Account: rt1600680 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | KMs | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Route Tables

↑ Previous Step

Select the route tables that should include routes to the floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.

Additional information ⓘ

<input checked="" type="checkbox"/>	Name	Main	ID	Associate with Subnet	Tags
<input checked="" type="checkbox"/>	private_rt_rt1600680	No	rtb-08b4cb88f5c826a5	3 Subnets	1 Tags
<input checked="" type="checkbox"/>	public_rt_rt1600680	Yes	rtb-0e46720d9da10c593	1 Subnets	1 Tags

2 Route Tables | The main route table is the default for the VPC

Continue

Cloud Manager 3.8.9 | Build 2 | Aug 18, 2021 06:15:05 am UTC

3. Sie haben die Wahl, ob die von AWS gemanagte Verschlüsselung oder AWS KMS zur Verschlüsselung der ONTAP-Root-, Boot- und Datenfestplatten aktiviert werden sollen.

Cloud Manager

Account: rt1600680 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | KMs | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Data Encryption

↑ Previous Step

AWS Managed Encryption

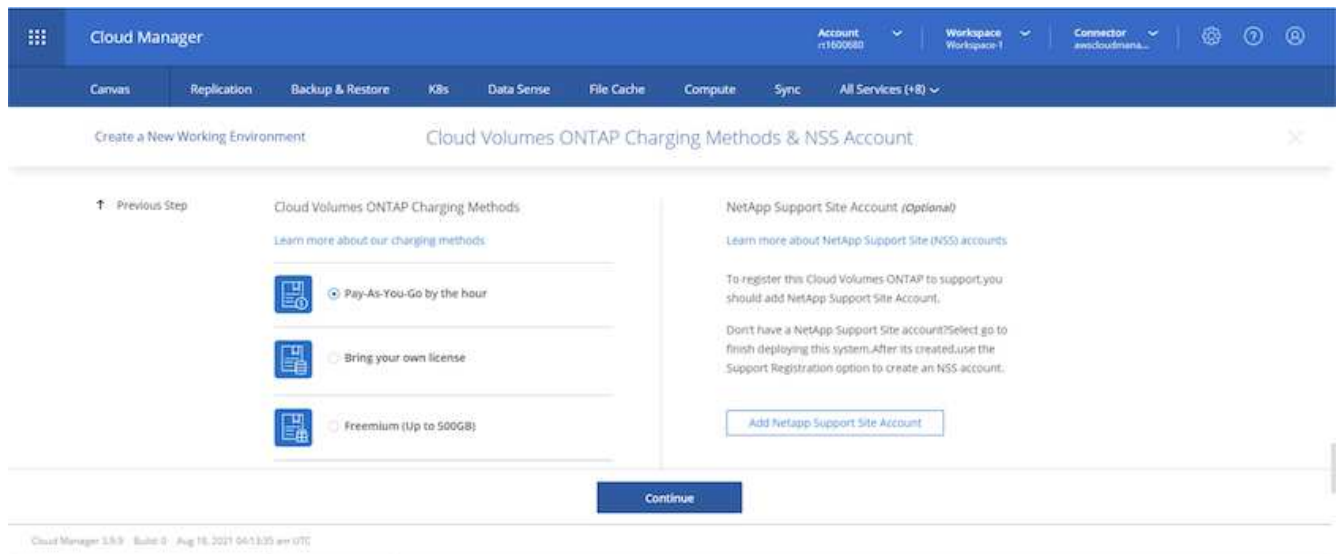
AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

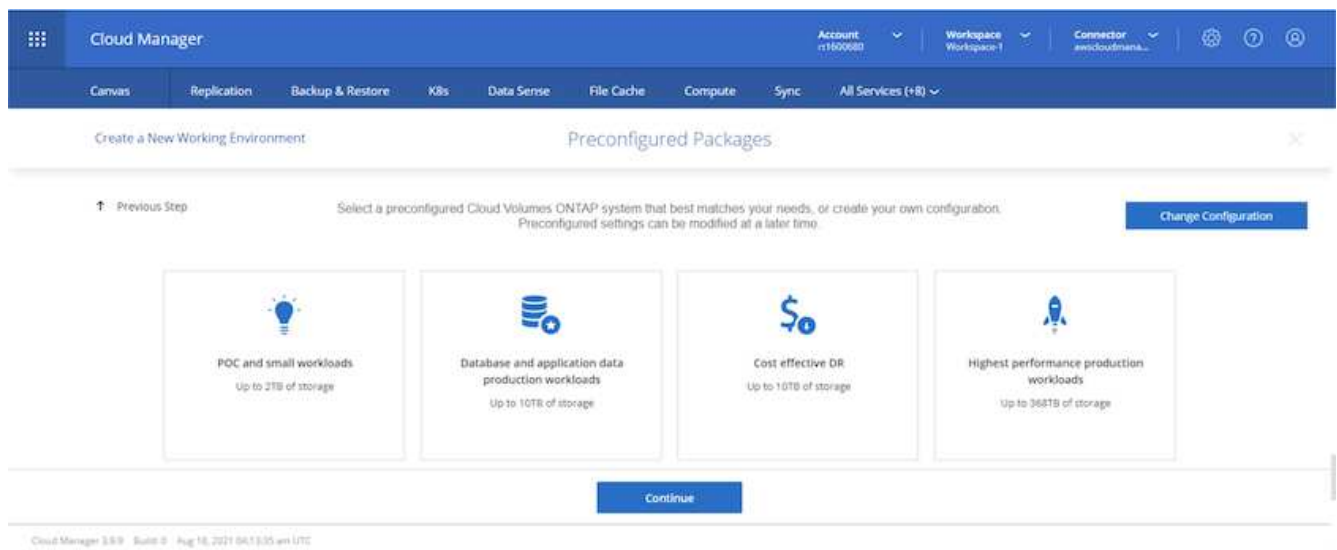
Continue

Cloud Manager 3.8.9 | Build 2 | Aug 18, 2021 06:15:05 am UTC

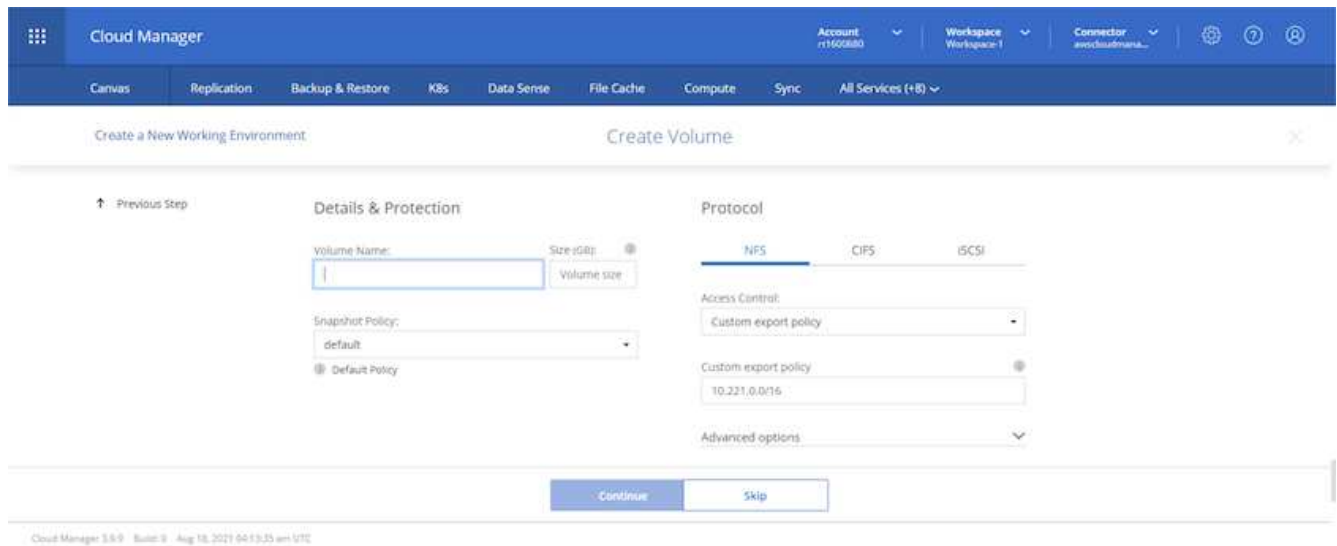
4. Wählen Sie Ihr Lizenzmodell. Wenn Sie nicht wissen, welche Option Sie wählen sollten, wenden Sie sich an Ihren NetApp Ansprechpartner.



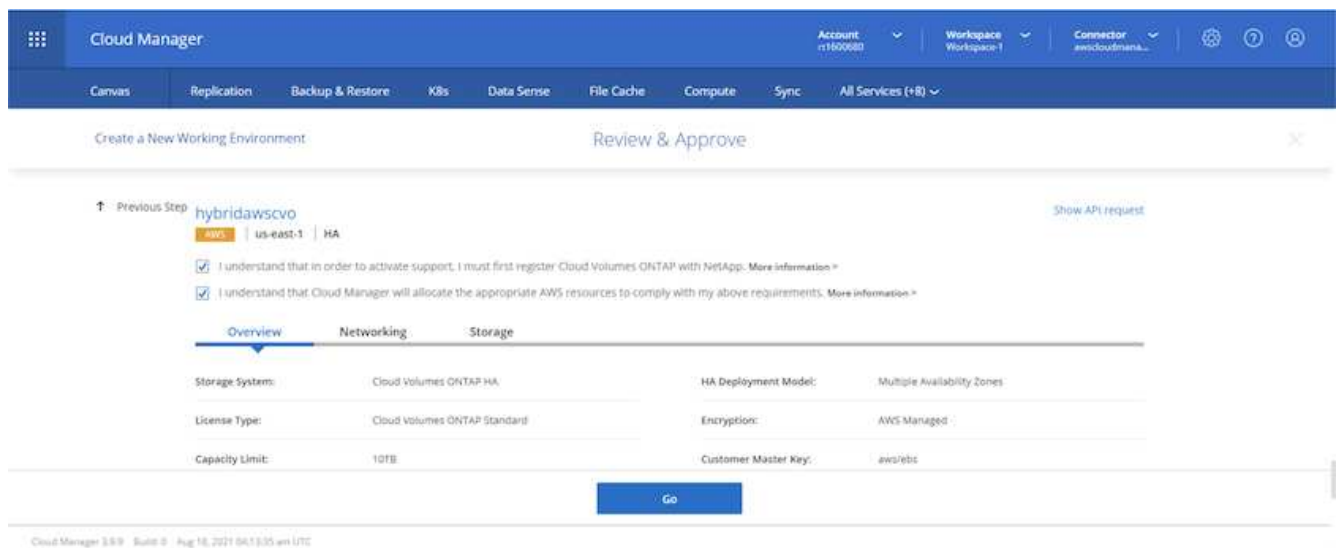
5. Wählen Sie die Konfiguration aus, die am besten zu Ihrem Anwendungsfall passt. Dies bezieht sich auf die Überlegungen zur Dimensionierung, die auf der Seite Voraussetzungen behandelt werden.



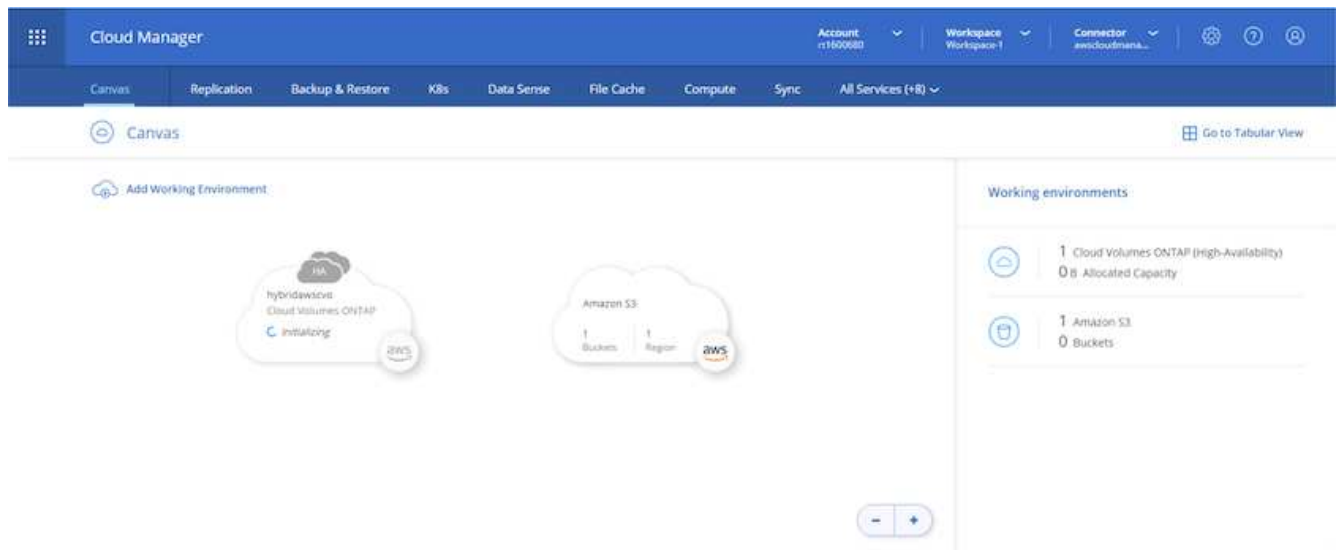
6. Erstellen Sie optional ein Volume. Dies ist nicht erforderlich, da in den nächsten Schritten SnapMirror verwendet wird, welches die Volumes für uns erstellt.



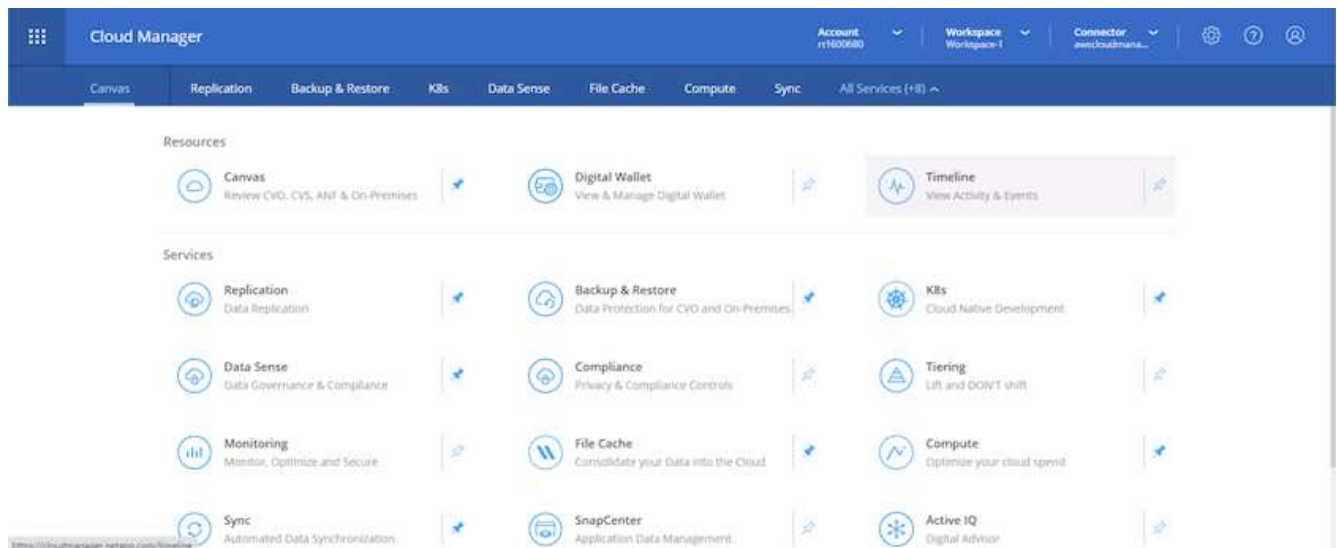
- Überprüfen Sie die getroffene Auswahl und aktivieren Sie die Kontrollkästchen, um zu überprüfen, ob Cloud Manager Ressourcen in Ihrer AWS-Umgebung implementiert. Klicken Sie abschließend auf „Go“.



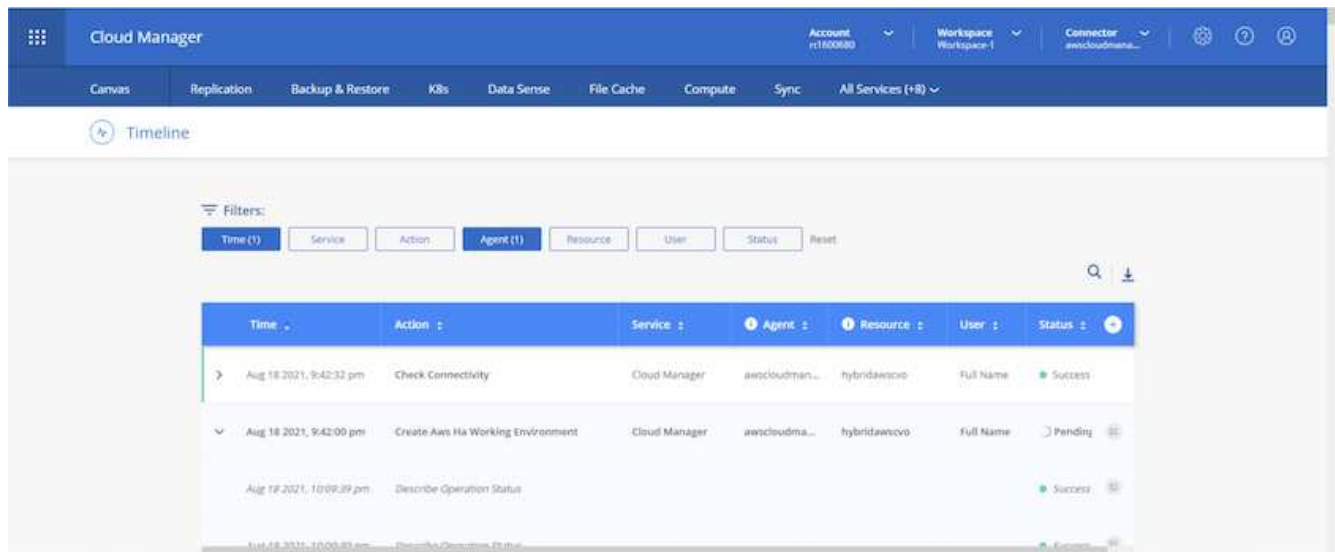
- Cloud Volumes ONTAP startet jetzt mit der Implementierung. Cloud Manager verwendet für die Implementierung von Cloud Volumes ONTAP APIs und Cloud-Formations-Stacks von AWS. Anschließend wird das System gemäß Ihren Spezifikationen konfiguriert, sodass ein sofort einsatzbereites System verfügbar ist. Der Zeitpunkt für diesen Prozess variiert je nach getroffene Auswahl.



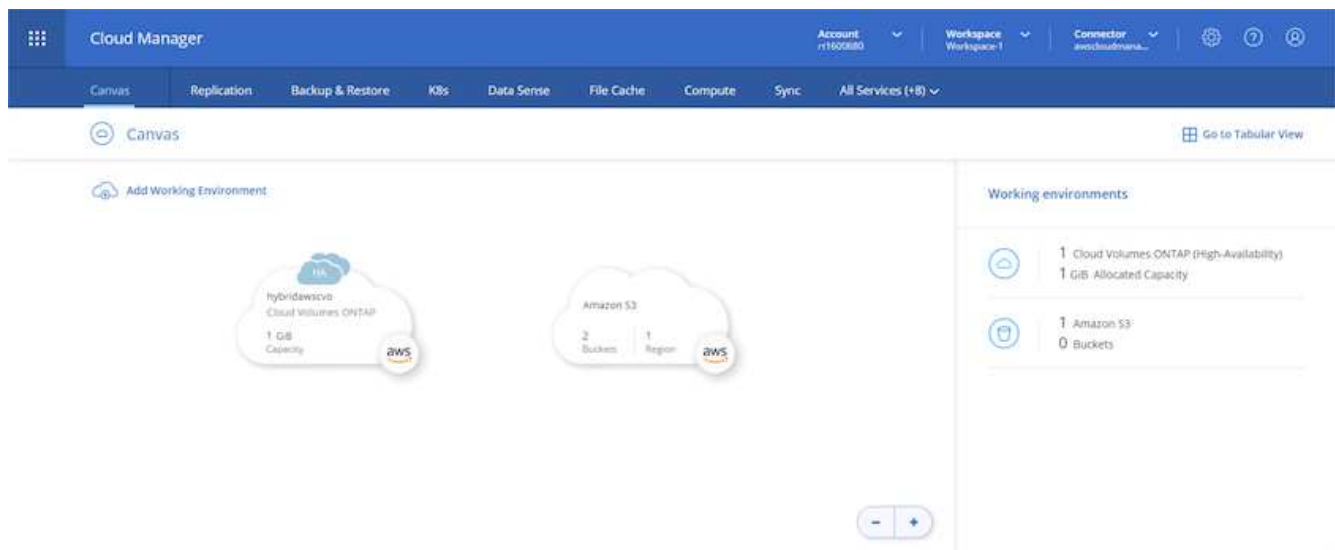
9. Sie können den Fortschritt überwachen, indem Sie zur Zeitleiste navigieren.



10. Die Zeitleiste dient als Audit aller in Cloud Manager ausgeführten Aktionen. Sie können alle API-Aufrufe anzeigen, die Cloud Manager bei der Einrichtung von AWS sowie dem ONTAP Cluster getätigt hat. Dies kann auch effektiv verwendet werden, um alle Probleme zu beheben, denen Sie gegenüberstehen.



11. Nach Abschluss der Bereitstellung erscheint der CVO-Cluster auf dem Canvas, der aktuellen Kapazität. Das ONTAP Cluster ist im aktuellen Status vollständig konfiguriert, um ein echtes, out-of-the-box-Erlebnis zu ermöglichen.

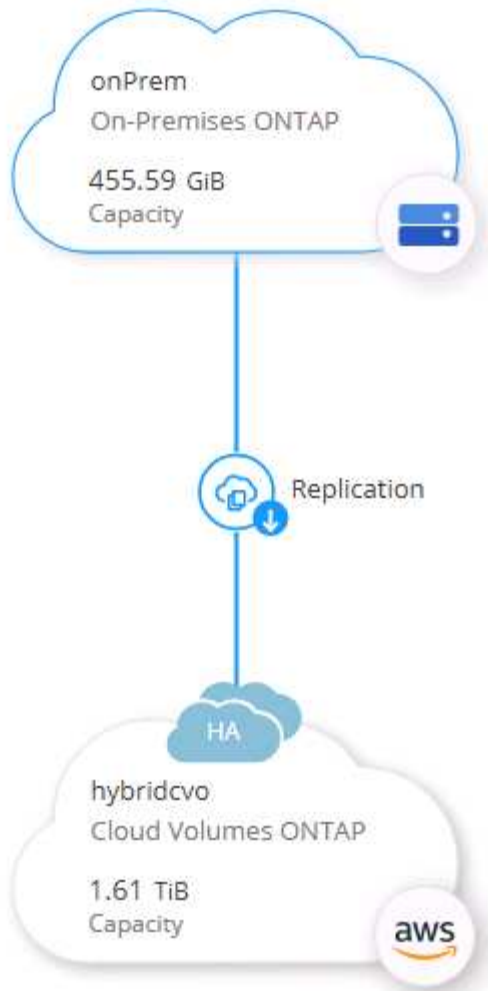


Konfigurieren Sie SnapMirror aus Ihrem lokalen Standort in die Cloud

Nachdem Sie nun ein ONTAP Quellsystem und ein implementierter Zielsystem von ONTAP haben, können Sie Volumes mit Datenbankdaten in die Cloud replizieren.

Einen Leitfaden zu kompatiblen ONTAP-Versionen für SnapMirror finden Sie im ["SnapMirror Kompatibilitätsmatrix"](#).

1. Klicken Sie auf das Quell-ONTAP-System (on-Premises), ziehen Sie es per Drag & Drop zum Ziel, wählen Sie Replikation > Aktivieren, oder wählen Sie Replikation > Menü > Replikation.

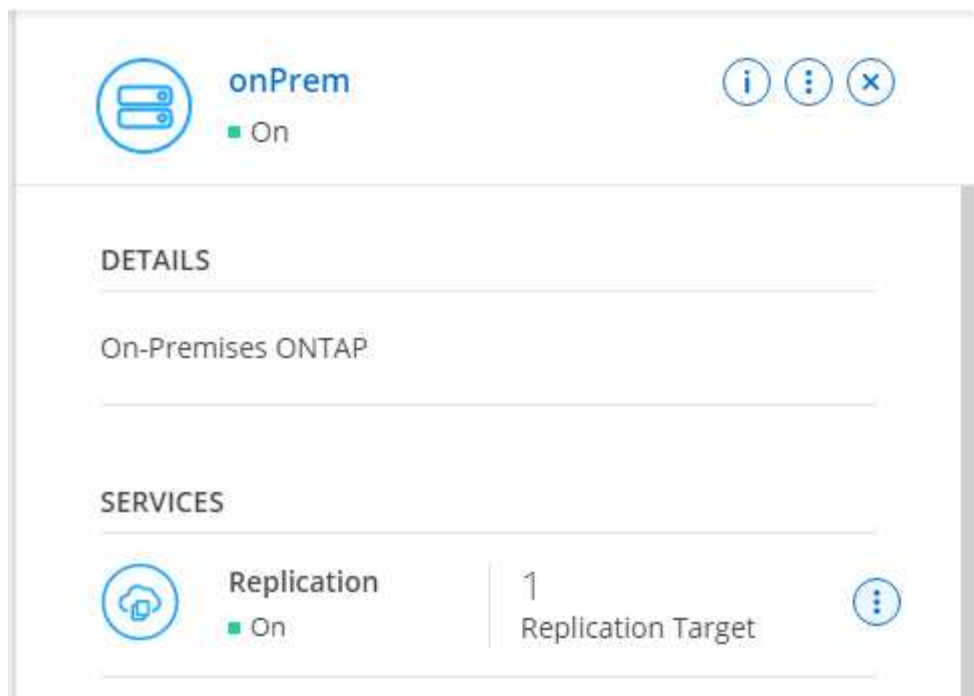


Wählen Sie Aktivieren.

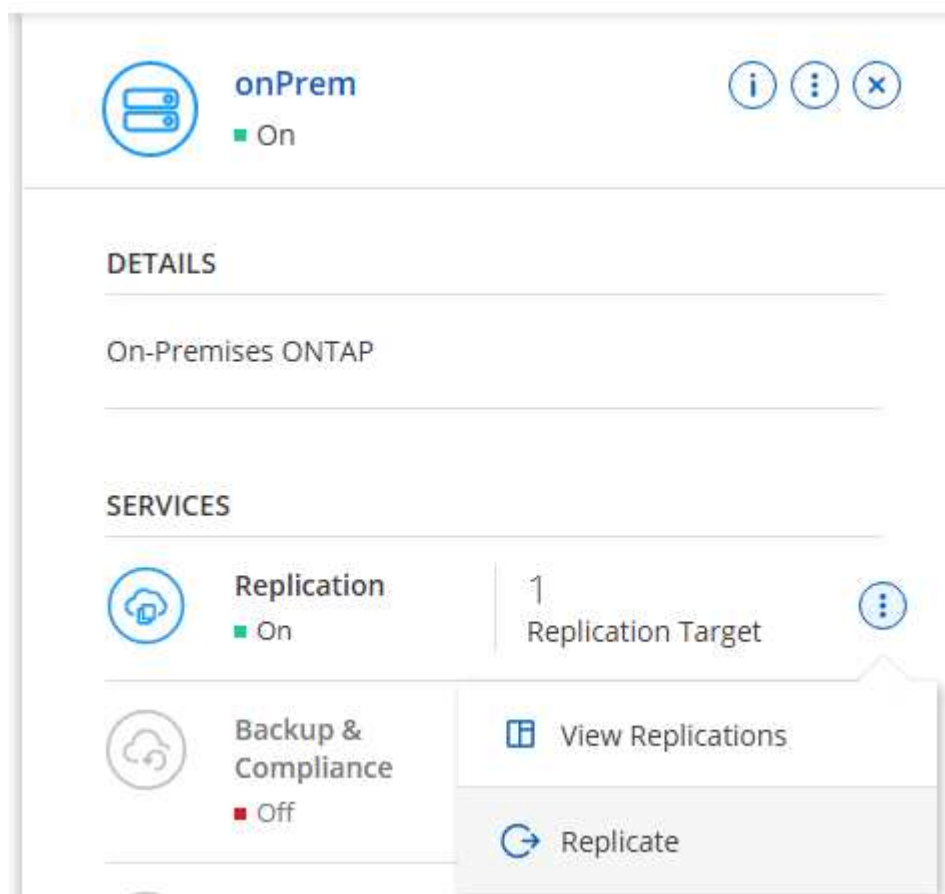
SERVICES

	Replication ■ Off	Enable	
---	-----------------------------	------------------------	---

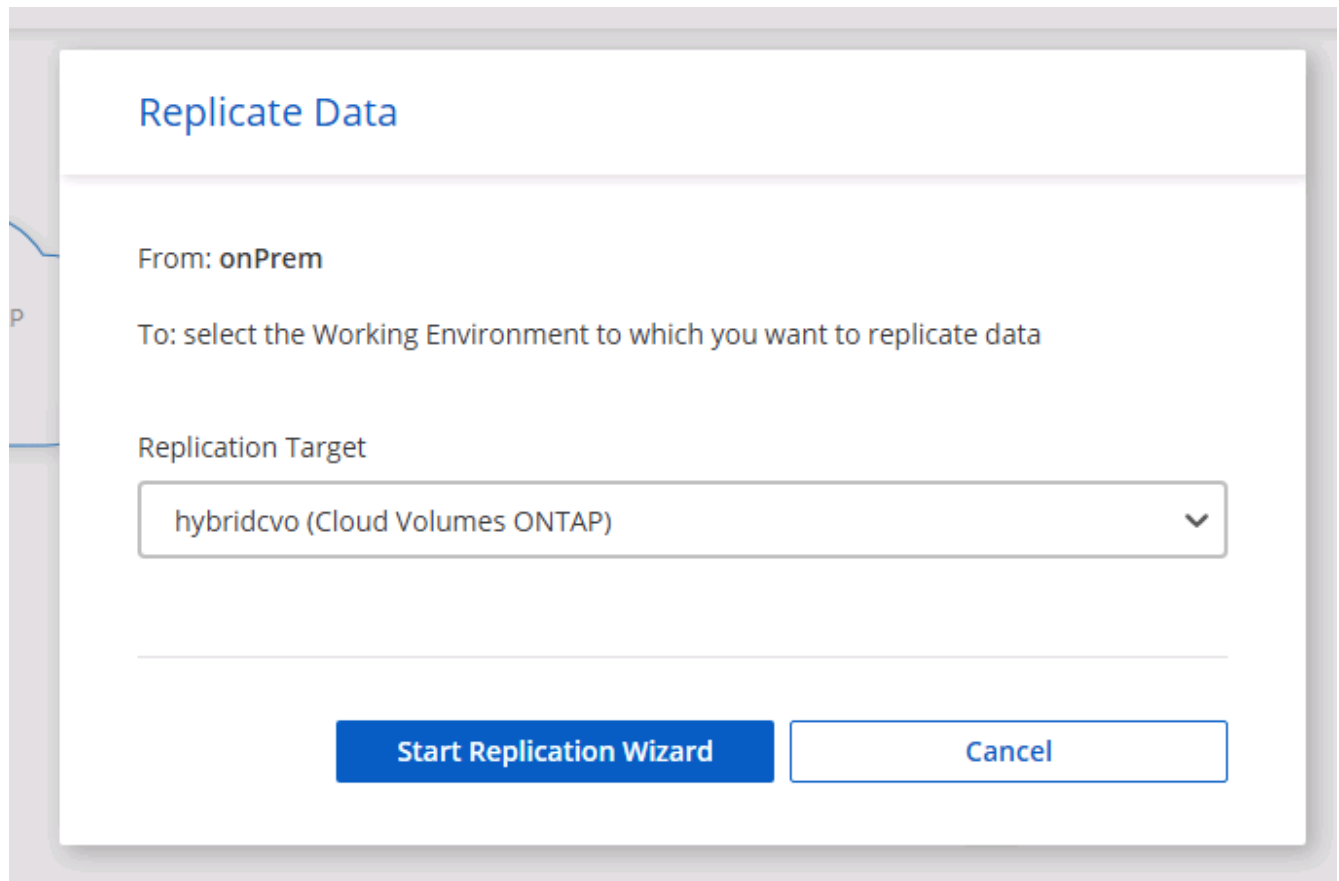
Oder Optionen.



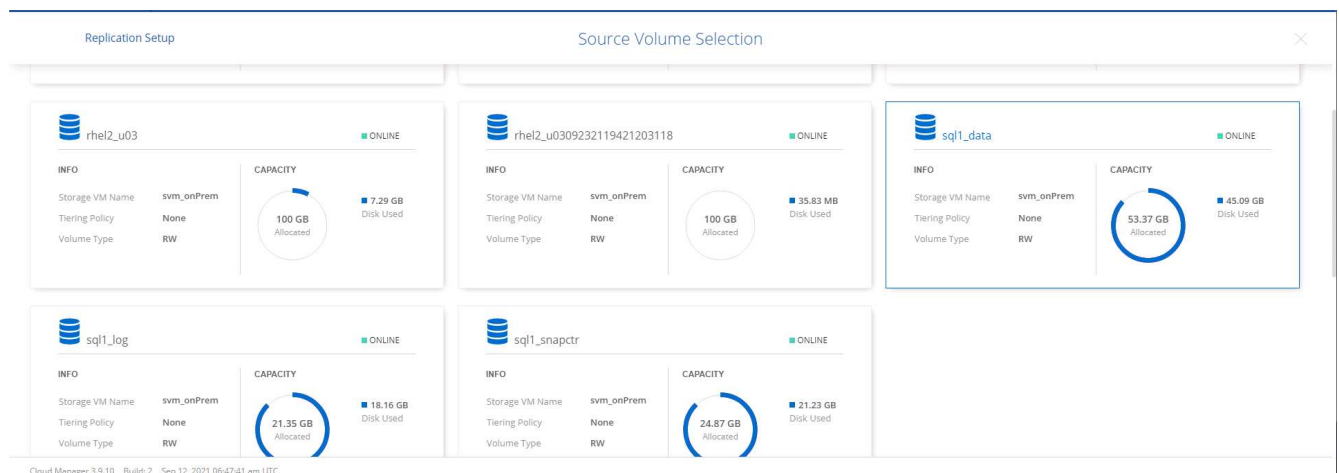
Replizierung:



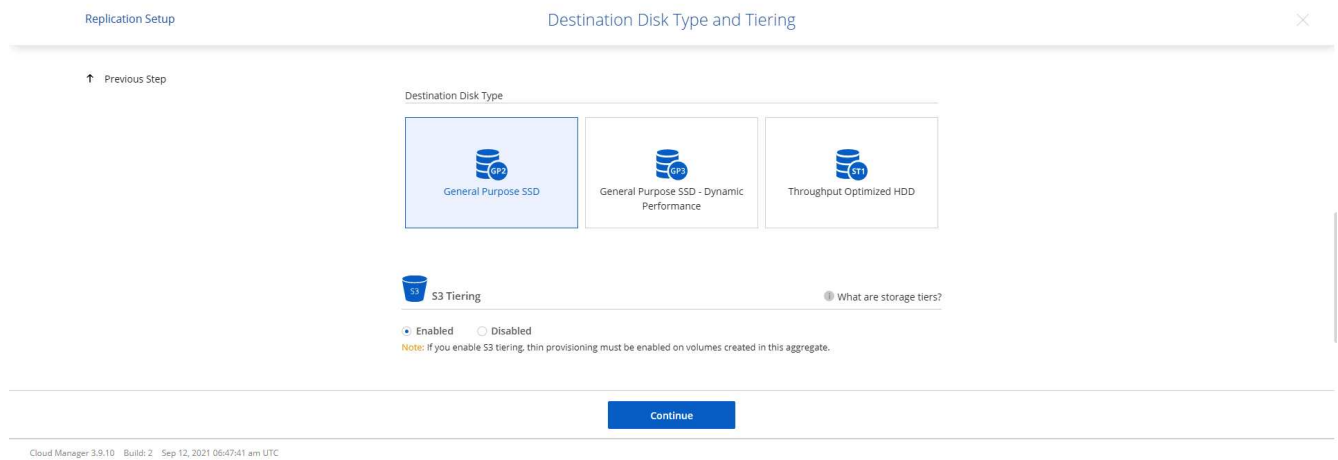
2. Wenn Sie keine Drag-and-Drop-Option haben, wählen Sie das Ziel-Cluster aus, zu dem Sie replizieren möchten.



3. Wählen Sie das Volume aus, das Sie replizieren möchten. Wir haben die Daten und alle Log-Volumes repliziert.



4. Wählen Sie den Zieldatentyp und die Tiering-Richtlinie. Für Disaster Recovery empfehlen wir eine SSD als Festplattentyp und zur Aufrechterhaltung des Daten-Tiering. Mit Daten-Tiering werden die gespiegelten Daten in kostengünstigem Objekt-Storage verschoben und Kosten auf lokalen Festplatten eingespart. Wenn Sie die Beziehung unterbrechen oder das Volume klonen, verwenden die Daten den schnellen lokalen Storage.



5. Wählen Sie den Zielvolumennamen: Wir haben ausgewählt `[source_volume_name]_dr`.



6. Wählen Sie die maximale Übertragungsrate für die Replikation aus. Dadurch sparen Sie Bandbreite, wenn Sie eine Verbindung mit einer niedrigen Bandbreite zur Cloud, wie zum Beispiel einem VPN, herstellen.

Max Transfer Rate


You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.

- Limited to: MB/s
- Unlimited (recommended for DR only machines)

7. Legen Sie die Replizierungsrichtlinie fest. Wir haben uns für einen Spiegel entschieden, der den letzten Datensatz aufnimmt und diesen in das Ziel-Volumen repliziert. Sie können auch eine andere Richtlinie auf Basis Ihrer Anforderungen wählen.


Replication Policy

Default Policies Additional Policies

 Mirror

Typically used for disaster recovery

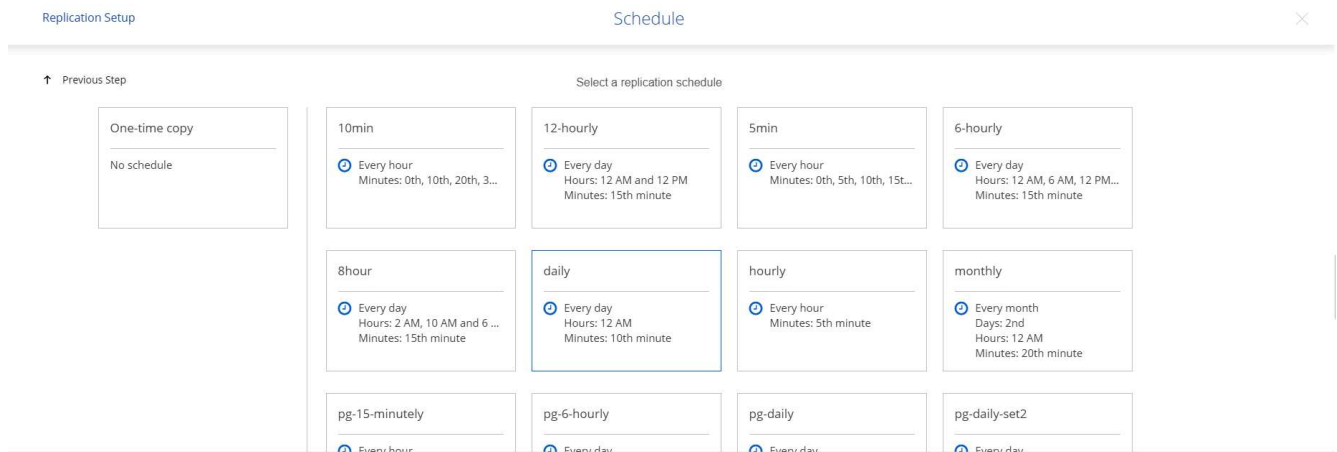
[More info](#)

 Mirror and Backup (1 month retention)

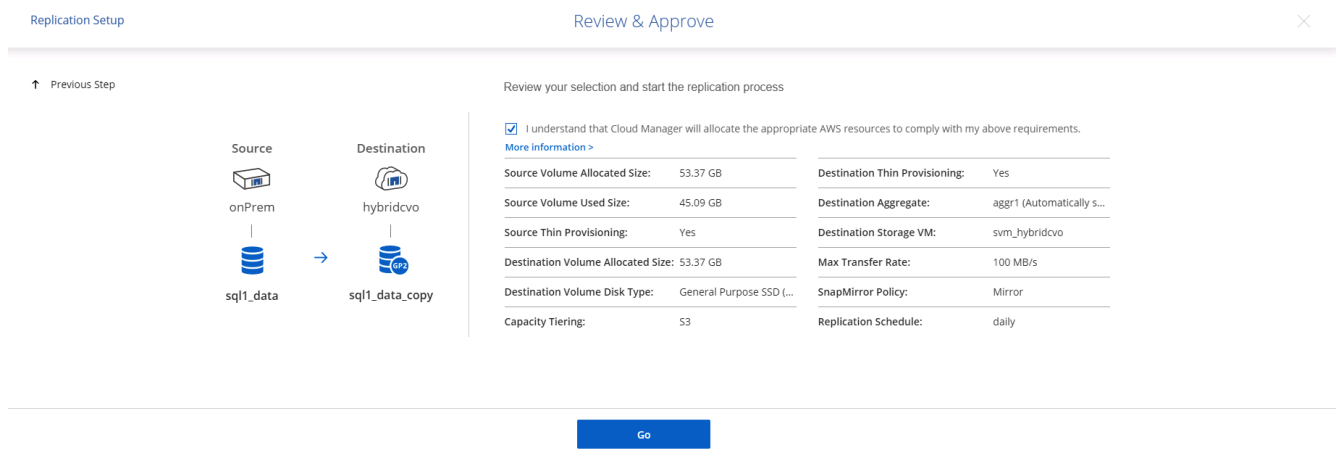
Configures disaster recovery and long-term retention of backups on the same destination volume

[More info](#)

8. Wählen Sie den Zeitplan für das Auslösen der Replikation aus. NetApp empfiehlt die Festlegung eines „täglichen“ Zeitplans für das Daten-Volumen und einen „stündlichen“ Zeitplan für die Log-Volumen, wobei diese jedoch je nach Anforderungen geändert werden können.

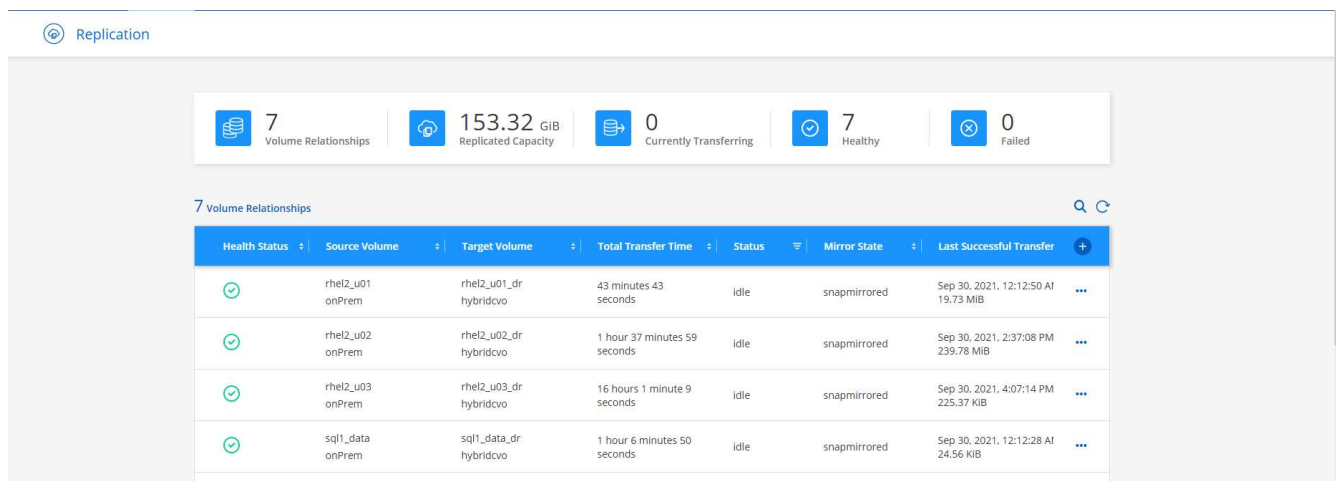


9. Überprüfen Sie die eingegebenen Informationen, klicken Sie auf Go, um den Cluster Peer und SVM Peer auszulösen (wenn dies Ihr erstes Mal ist, wenn Sie zwischen den beiden Clustern replizieren) und implementieren und initialisieren Sie dann die SnapMirror Beziehung.



10. Setzen Sie diesen Prozess für Datenvolumen und Protokoll-Volumen fort.

11. Wenn Sie alle Beziehungen überprüfen möchten, wechseln Sie zur Registerkarte „Replikation“ in Cloud Manager. Hier können Sie Ihre Beziehungen verwalten und ihren Status überprüfen.



12. Nachdem alle Volumes repliziert wurden, befinden Sie sich in einem stabilen Zustand und können zu den Workflows für Disaster Recovery und Entwicklung/Test wechseln.

3. EC2 Computing-Instanz für Datenbank-Workload implementieren

AWS verfügt über vorkonfigurierte EC2 Computing-Instanzen für verschiedene Workloads. Die Wahl des Instanztyps bestimmt die Anzahl der CPU-Kerne, die Speicherkapazität, den Speichertyp und die Kapazität sowie die Netzwerk-Performance. In den Anwendungsfällen wird mit Ausnahme der Betriebssystempartition der Haupt-Storage für die Ausführung des Datenbank-Workloads von CVO oder der FSX ONTAP-Storage-Engine zugewiesen. Daher müssen die wichtigsten Faktoren die Wahl der CPU-Cores, des Arbeitsspeichers und der Netzwerk-Performance sein. Typische AWS EC2 Instanztypen sind hier zu finden: ["EC2 Instanztyp"](#).

Dimensionierung der Computing-Instanz

1. Wählen Sie den richtigen Instanztyp basierend auf dem erforderlichen Workload aus. Zu berücksichtigende Faktoren sind die Anzahl der zu unterstützenden Geschäftstransaktionen, die Anzahl gleichzeitiger Benutzer, die Größenbemessung von Datensätze usw.
2. Die Implementierung der EC2-Instanz kann über das EC2 Dashboard gestartet werden. Die genauen Implementierungsverfahren gehen über den Umfang dieser Lösung hinaus. Siehe ["Amazon EC2"](#) Entsprechende Details.

Konfiguration einer Linux-Instanz für Oracle-Workload

Dieser Abschnitt enthält weitere Konfigurationsschritte, nachdem eine EC2 Linux Instanz implementiert wurde.

1. Fügen Sie eine Oracle-Standby-Instanz zum DNS-Server für die Namensauflösung in der SnapCenter-Managementdomäne hinzu.
2. Fügen Sie als SnapCenter OS-Anmeldeinformationen eine Linux-Management-Benutzer-ID mit sudo-Berechtigungen ohne Kennwort hinzu. Aktivieren Sie die ID mit SSH-Passwort-Authentifizierung auf der EC2-Instanz. (Bei EC2-Instanzen ist die SSH-Kennwortauthentifizierung und passwordless sudo standardmäßig deaktiviert.)
3. Konfiguration der Oracle Installation entsprechend der lokalen Oracle Installation, z. B. Betriebssystem-Patches, Oracle Versionen und Patches usw.
4. NetApp Ansible DB-Automatisierungsrollen können genutzt werden, um EC2 Instanzen für Anwendungsfälle in den Bereichen Entwicklung/Test und Disaster Recovery zu konfigurieren. Der Automatisierungscode kann auf der öffentlichen NetApp GitHub Website heruntergeladen werden: ["Automatisierte Oracle 19c Implementierung"](#). Ziel ist es, einen Datenbank-Software-Stack auf einer EC2 Instanz zu installieren und zu konfigurieren, der an lokale OS- und Datenbankkonfigurationen angepasst wird.

Windows-Instanzkonfiguration für den SQL Server-Workload

Dieser Abschnitt enthält zusätzliche Konfigurationsschritte, nachdem eine EC2 Windows-Instanz ursprünglich implementiert wurde.

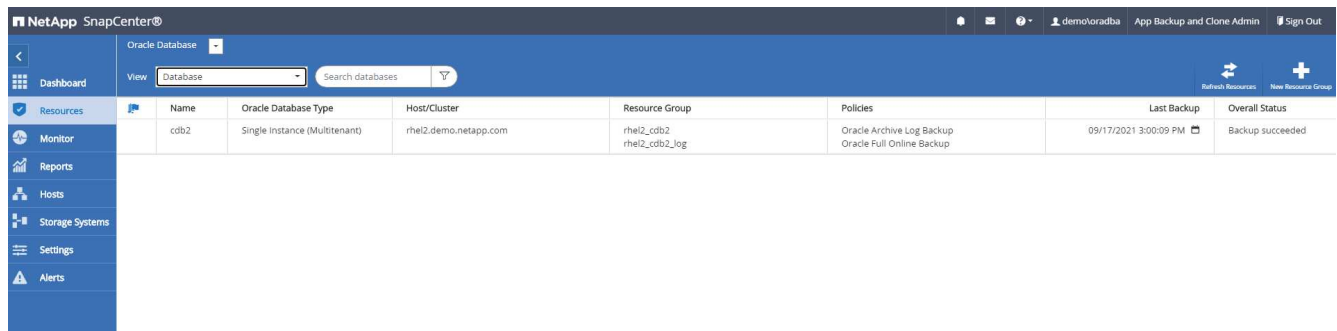
1. Rufen Sie das Windows-Administratorpasswort ab, um sich über RDP bei einer Instanz anzumelden.
2. Deaktivieren Sie die Windows-Firewall, treten Sie der Windows SnapCenter-Domäne des Hosts bei und fügen Sie die Instanz zum DNS-Server zur Namensauflösung hinzu.
3. Bereitstellen eines SnapCenter-Protokollvolumens zum Speichern von SQL Server-Protokolldateien
4. Konfigurieren Sie iSCSI auf dem Windows-Host, um das Volume zu mounten und das Festplattenlaufwerk zu formatieren.
5. Viele ihrer früheren Aufgaben können mit der NetApp Automatisierungslösung für SQL Server automatisiert werden. Informieren Sie sich auf der NetApp Public Automation GitHub Website über neu veröffentlichte Rollen und Lösungen: ["NetApp Automatisierung"](#).

Workflow für Entwicklungs- und Test-Bursting in die Cloud

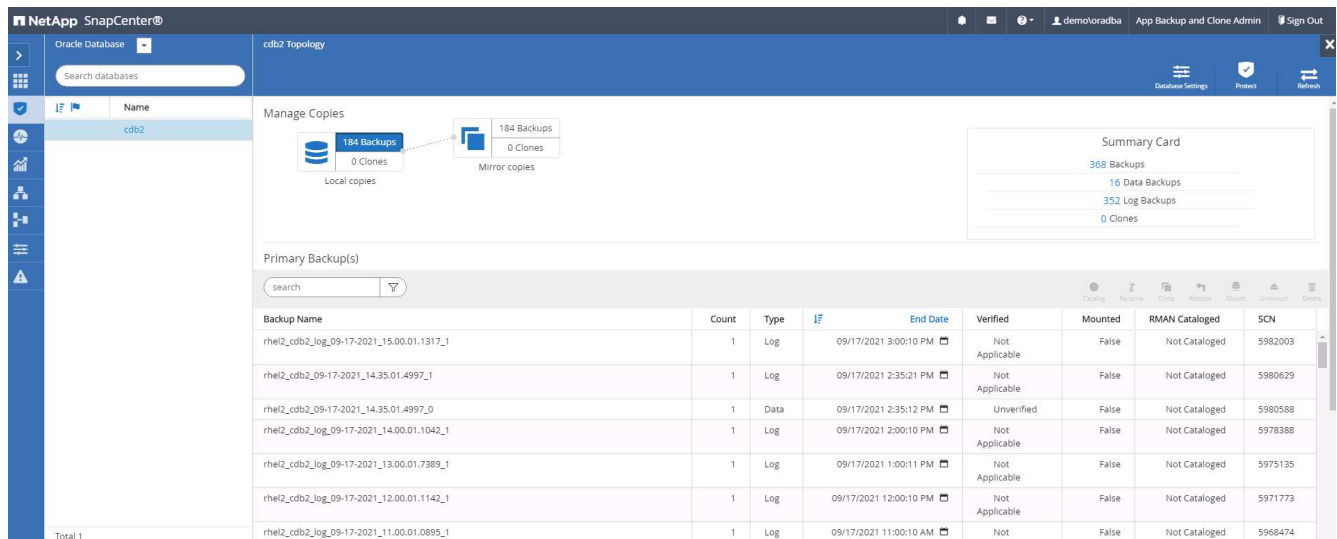
Die Agilität der Public Cloud, die Amortisierung und die Kosteneinsparungen sind sinnvolle Vorteile für Unternehmen, die sich für die Entwicklung und das Testen von Datenbankapplikationen durch die Public Cloud entscheiden. Es gibt kein besseres Werkzeug als SnapCenter, um dies Wirklichkeit werden zu lassen. Mit SnapCenter können Sie Ihre Produktionsdatenbank nicht nur vor Ort schützen, sondern auch schnell eine Kopie für Applikationsentwicklung oder Code-Tests in der Public Cloud klonen und belegen gleichzeitig nur sehr wenig zusätzlichen Storage. Im Folgenden finden Sie Details zu den Schritt-für-Schritt-Prozessen für dieses Tool.

Klonen einer Oracle Datenbank für Entwicklungs- und Testzwecke aus einem replizierten Snapshot Backup

1. Melden Sie sich mit einer Datenbank-Management-Benutzer-ID für Oracle bei SnapCenter an. Öffnen Sie die Registerkarte Ressourcen, auf der die von SnapCenter geschützten Oracle-Datenbanken angezeigt werden.



2. Klicken Sie auf den gewünschten Namen der lokalen Datenbank für die Backup-Topologie und die detaillierte Ansicht. Wenn ein sekundärer replizierter Standort aktiviert ist, werden verknüpfte Spiegelsicherungen angezeigt.



3. Klicken Sie auf „gespiegelte Backups“, um zur Ansicht „gespiegelte Backups“ zu gelangen. Anschließend werden die Backup(s) der sekundären Spiegelung angezeigt.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log	09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_09-17-2021_14.35.01.4997_1	1	Log	09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data	09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log	09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log	09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5975135
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log	09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log	09/17/2021 11:00:10 AM	Not Applicable	False	Not Cataloged	5968474

- Wählen Sie eine gespiegelte sekundäre Datenbank-Backup-Kopie, die geklont werden soll, und legen Sie einen Recovery-Zeitpunkt entweder nach Zeit- und Systemänderungsnummer oder nach SCN fest. Im Allgemeinen sollte der Recovery-Zeitpunkt hinter der vollständigen Datenbank-Backup-Zeit zurückliegen oder SCN zum Klonen stehen. Nach der Entscheidung für einen Wiederherstellungspunkt muss die erforderliche Protokolldatei-Sicherung für die Wiederherstellung eingebunden werden. Die Sicherung der Protokolldatei sollte auf dem Ziel-DB-Server gemountet werden, auf dem die Klondatenbank gehostet werden soll.

Oracle Database | cdb2 Topology

Search databases

Manage Copies

184 Backups
0 Clones
Local copies

184 Backups
1 Clone
Mirror copies

Summary Card

368 Backups
16 Data Backups
352 Log Backups
1 Clone

Secondary Mirror Backup(s)

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhe12_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhe12_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhe12_cdb2_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhe12_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhe12_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388



Wenn die Protokollbeschnidung aktiviert ist und der Wiederherstellungspunkt über den letzten Protokollschnitt hinaus erweitert wird, müssen möglicherweise mehrere Archiv-Log-Backups eingebunden werden.

5. Markieren Sie die vollständige Datenbank-Backup-Kopie, die geklont werden soll, und klicken Sie dann auf die Schaltfläche Klonen, um den DB-Klon-Workflow zu starten.

cdb2 Topology

search

Clone

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhe12_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhe12_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhe12_cdb2_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhe12_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhe12_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388

6. Wählen Sie eine geeignete Klon-DB-SID für eine vollständige Container-Datenbank oder einen CDB-Klon.

Clone from cdb2
✕

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Complete Database Clone

Clone SID

Exclude PDBs

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume	Destination Volume
svm_onPrem:rhel2_u02	<input style="width: 90%;" type="text" value="svm_hybridcvo:rhel2_u02_dr"/>

Logs

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	<input style="width: 90%;" type="text" value="svm_hybridcvo:rhel2_u03_dr"/>

7. Wählen Sie den Zielklonhost in der Cloud aus, und Datendatei, Kontrolldatei und Wiederherstellungsprotokolle werden vom Klon-Workflow erstellt.

Clone from cdb2
✕

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Select the host to create a clone

Clone host

Datafile locations ⓘ

Reset

Control files ⓘ

<input style="width: 95%;" type="text" value="/u02_cdb2test/cdb2test/control/control01.ctl"/>	✕	+
<input style="width: 95%;" type="text" value="/u02_cdb2test/cdb2test/control/control02.ctl"/>	✕	+

Reset

Redo logs ⓘ

Group	Size	Unit	Number of files		
RedoGroup 1	200	MB	1	✕	+
<input style="width: 95%;" type="text" value="/u02_cdb2test/cdb2test/redolog/redo03.log"/>					
RedoGroup 2	200	MB	1	✕	+

Reset

Previous
Next

8. Der Name für keine Anmeldeinformationen wird für die BS-basierte Authentifizierung verwendet, wodurch der Datenbankport irrelevant wird. Geben Sie die korrekte Oracle Home, Oracle OS User und Oracle OS Group ein, wie im Klon-DB-Server konfiguriert.

Clone from cdb2 x

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Database Credentials for the clone

Credential name for sys user: + ⓘ

Database port:

Oracle Home Settings ⓘ

Oracle Home:

Oracle OS User:

Oracle OS Group:

9. Geben Sie die vor dem Klonvorgang zu ausführenden Skripte an. Vor allem kann hier der Parameter der Datenbankinstanz angepasst oder definiert werden.

Clone from cdb2
✕

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Specify scripts to run before clone operation ?

Prescript full path

Arguments

Script timeout secs

⊖ Database Parameter settings

processes	320	✕	▲
remote_login_passwordfile	EXCLUSIVE	✕	+
sga_target	4311744512	✕	▼
undo_tablespace	UNDOTBS1	✕	

10. Geben Sie den Wiederherstellungspunkt entweder mit Datum und Uhrzeit oder mit SCN an. Bis Abbrechen die Datenbank bis zu den verfügbaren Archivprotokollen wiederherstellt. Geben Sie den externen Speicherort für das Archivprotokoll vom Zielhost an, auf dem das Archiv-Protokoll-Volume angehängt ist. Wenn sich der Oracle-Eigentümer des Zielservers von dem lokalen Produktionsserver unterscheidet, überprüfen Sie, ob das Archivprotokollverzeichnis vom Oracle Eigentümer des Zielservers lesbar ist.

Clone from cdb2

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps**
- 6 Notification
- 7 Summary

Recover Database

Until Cancel i
 Date and Time i
 Date-time format: MM/DD/YYYY hh:mm:ss
 Until SCN (System Change Number) i

Specify external archive log locations i

Create new DBID i
 Create tempfile for temporary tablespace i
 Enter SQL queries to apply when clone is created
 Enter scripts to run after clone operation i

```

oracle@ora-standby:tmp
[oracle@ora-standby tmp]$ ls /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/
2021_08_26 2021_08_28 2021_08_30 2021_09_01 2021_09_03 2021_09_05 2021_09_07 2021_09_09 2021_09_11 2021_09_13 2021_09_15 2021_09_17
2021_08_27 2021_08_29 2021_08_31 2021_09_02 2021_09_04 2021_09_06 2021_09_08 2021_09_10 2021_09_12 2021_09_14 2021_09_16
[oracle@ora-standby tmp]$
  
```

11. Konfigurieren Sie bei Bedarf den SMTP-Server für E-Mail-Benachrichtigungen.

Clone from cdb2

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification**
- 7 Summary

Provide email settings ?

Email preference:

From:

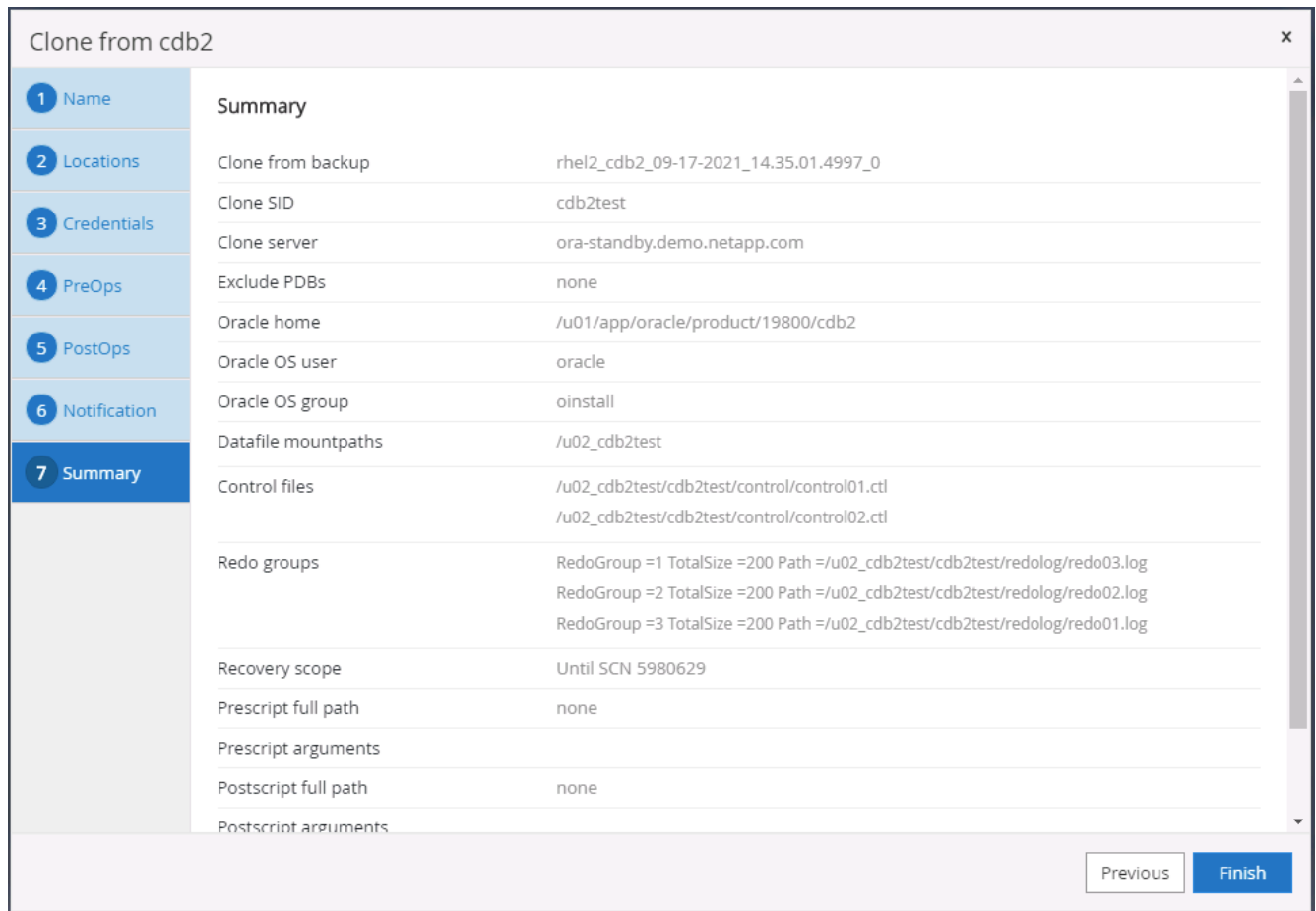
To:

Subject:

Attach job report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

12. Zusammenfassung des Klons:



13. Sie sollten nach dem Klonen validieren, um sicherzustellen, dass die geklonte Datenbank funktionsfähig ist. Einige zusätzliche Aufgaben, wie z. B. das Starten des Listeners oder das Deaktivieren des DB-Log-Archivmodus, können an der Entwicklungs-/Testdatenbank ausgeführt werden.

```

oracle@ora-standby/tmp
[oracle@ora-standby tmp]$ export ORACLE_SID=cdb2test
[oracle@ora-standby tmp]$ export ORACLE_HOME=/u01/app/oracle/product/19800/cdb2
[oracle@ora-standby tmp]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ora-standby tmp]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 17:49:29 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select name, log_mode from v$database;

NAME          LOG_MODE
-----
CDB2TEST      ARCHIVELOG

SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME
-----
HOST_NAME
-----
cdb2test
ora-standby.demo.netapp.com

SQL> show pdbs

  CON_ID CON_NAME          OPEN MODE  RESTRICTED
-----
2  PDB$SEED            READ ONLY  NO
3  CDB2_PDB1           READ WRITE NO
4  CDB2_PDB2           READ WRITE NO
5  CDB2_PDB3           READ WRITE NO

SQL>

```

Klonen einer SQL Datenbank für Entwicklungs- und Testzwecke aus einem replizierten Snapshot Backup

1. Melden Sie sich mit einer Datenbank-Management-Benutzer-ID für SQL Server bei SnapCenter an. Navigieren Sie zur Registerkarte Ressourcen, die die SQL Server-Benutzerdatenbanken anzeigt, die durch SnapCenter geschützt sind, und eine Ziel-Standby-SQL-Instanz in der Public Cloud.

The screenshot shows the NetApp SnapCenter interface with a list of Microsoft SQL Server resources. The table below represents the data shown in the interface.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/16/2021 7:35:05 PM	Backup succeeded	User database
master	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
model	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
msdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
tempdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database

2. Klicken Sie auf den gewünschten lokalen Namen der SQL Server-Benutzerdatenbank für die Backup-Topologie und die detaillierte Ansicht. Wenn ein sekundärer replizierter Standort aktiviert ist, werden verknüpfte Spiegelsicherungen angezeigt.

The screenshot shows the detailed backup topology for the 'tpcc' database. It displays a 'Manage Copies' section with 7 Backups and 0 Clones. Below this is a 'Primary Backup(s)' table listing individual backup records.

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-19-2021_18.25.01.4604	1	Full backup		09/19/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup		09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup		09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup		09/10/2021 6:36:29 PM	Unverified

3. Wechseln Sie zur Ansicht gespiegelte Backups, indem Sie auf gespiegelte Backups klicken. Sekundäre Spiegelsicherung(en) werden angezeigt. Da SnapCenter das Transaktions-Log von SQL Server auf einem dedizierten Laufwerk für die Wiederherstellung sichert, werden hier nur vollständige Datenbank-Backups angezeigt.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 0 Clones

Summary Card

14 Backups

0 Clones

Secondary Mirror Backup(s)

Backup Name	Count	Type	I/F	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup		09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup		09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup		09/10/2021 6:36:29 PM	Unverified

4. Wählen Sie eine Backup-Kopie aus, und klicken Sie dann auf die Schaltfläche Klonen, um den Klon aus dem Backup-Workflow zu starten.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 1 Clone

Summary Card

14 Backups

1 Clone

Secondary Mirror Backup(s)

Backup Name	Count	Type	I/F	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup		09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup		09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup		09/17/2021 6:25:05 PM	Unverified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified

Clone from backup
✕

- 1 Clone Options
- 2 Logs
- 3 Script
- 4 Notification
- 5 Summary

Clone settings

Clone server ⓘ

Clone instance ⓘ

Clone name

Choose mount option

Auto assign mount point ⓘ

Auto assign volume mount point under path ⓘ

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	<input style="width: 150px;" type="text" value="svm_hybridcvo:sql1_data_dr"/>
svm_onPrem:sql1_log	<input style="width: 150px;" type="text" value="svm_hybridcvo:sql1_log_dr"/>

5. Wählen Sie einen Cloud-Server als Ziel-Klonserver, als Kloninstanz und als Name der Klondatenbank aus. Wählen Sie entweder einen Mount-Punkt für die automatische Zuweisung oder einen benutzerdefinierten Mount-Point-Pfad.

×
Clone from backup

- 1 Clone Options
- 2 Logs
- 3 Script
- 4 Notification
- 5 Summary

Clone settings

Clone server ?

Clone instance ?

Clone name

Choose mount option

Auto assign mount point ?

Auto assign volume mount point under path ?

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	<input type="text" value="svm_hybridcvo:sql1_data_dr"/>
svm_onPrem:sql1_log	<input type="text" value="svm_hybridcvo:sql1_log_dr"/>

6. Legen Sie einen Recovery-Zeitpunkt entweder um eine Backup-Zeit für das Protokoll oder um ein bestimmtes Datum und eine bestimmte Uhrzeit fest.

Clone from backup x

- 1 Clone Options
- 2 Logs**
- 3 Script
- 4 Notification
- 5 Summary

Choose logs

All log backups

By log backups until

By specific date until

None

7. Legen Sie optionale Skripte fest, die vor und nach dem Klonvorgang ausgeführt werden sollen.

Clone from backup

- 1 Clone Options
- 2 Logs
- 3 Script**
- 4 Notification
- 5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments

Postscript full path

Postscript arguments

Script timeout

8. Konfigurieren Sie einen SMTP-Server, wenn eine E-Mail-Benachrichtigung gewünscht wird.

Clone from backup ✕

- 1 Clone Options
- 2 Logs
- 3 Script
- 4 Notification**
- 5 Summary

Provide email settings ?

Email preference

From

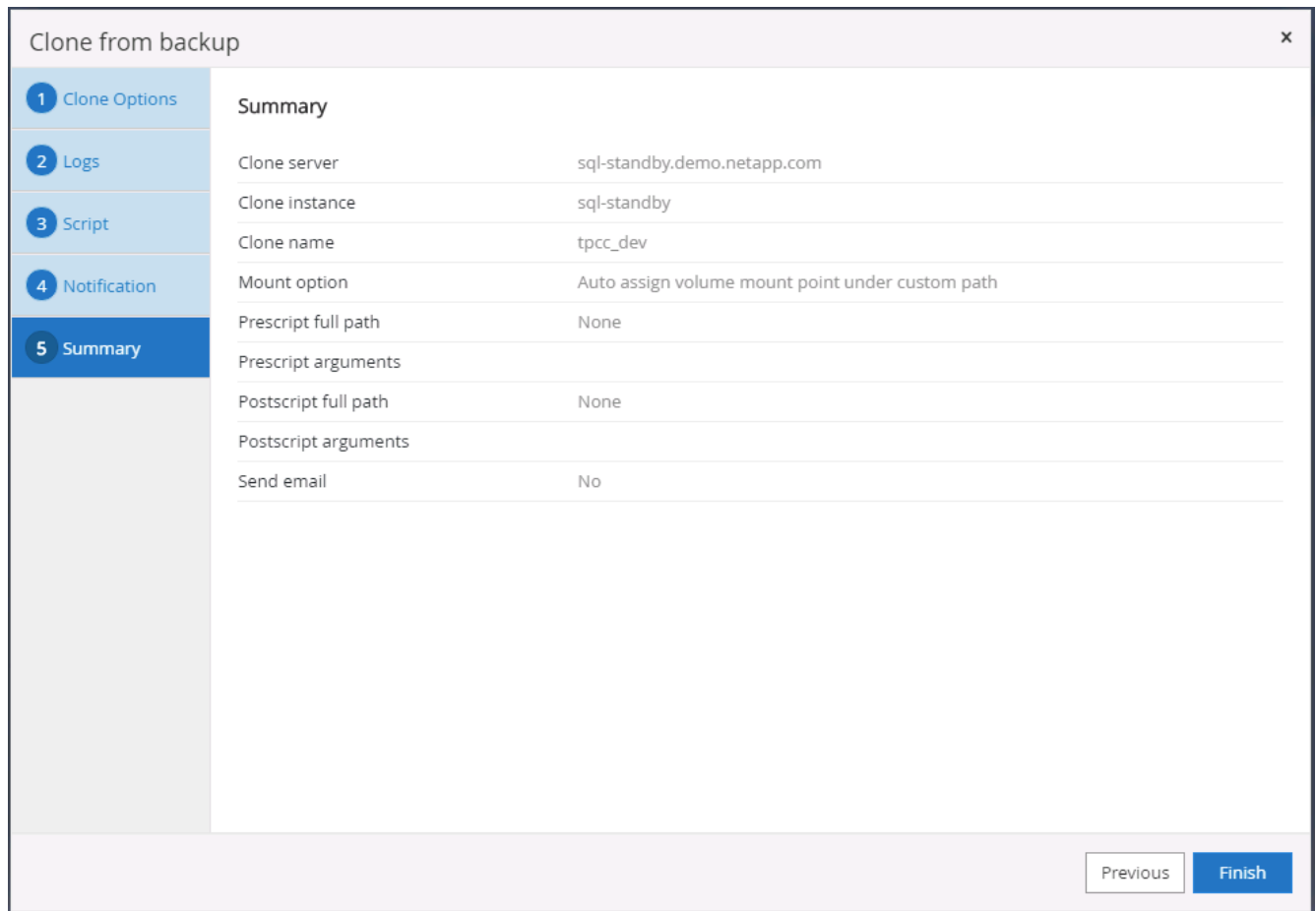
To

Subject

Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server. ✕

9. Zusammenfassung Klonen.



- Überwachen Sie den Job-Status und überprüfen Sie, ob die vorgesehene Benutzerdatenbank mit einer Ziel-SQL-Instanz im Cloud-Klon-Server verbunden wurde.

ID	Status	Name	Start date	End date	Owner
766	✓	Clone from backup 'sql1_tpcc_09-16-2021_18.25.01.4024'	09/16/2021 8:05:25 PM	09/16/2021 8:06:17 PM	demo:sqldba
763	✓	Discover resources for all hosts	09/16/2021 7:56:49 PM	09/16/2021 7:56:54 PM	demo:sqldba
761	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 7:35:00 PM	09/16/2021 7:37:08 PM	demo:sqldba
760	⚠	Discover resources for all hosts	09/16/2021 7:19:05 PM	09/16/2021 7:19:09 PM	demo:sqldba
759	⚠	Discover resources for all hosts	09/16/2021 7:18:43 PM	09/16/2021 7:18:48 PM	demo:sqldba
756	⚠	Discover resources for all hosts	09/16/2021 6:59:51 PM	09/16/2021 6:59:56 PM	demo:sqldba
753	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 6:35:00 PM	09/16/2021 6:37:07 PM	demo:sqldba
750	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/16/2021 6:25:01 PM	09/16/2021 6:27:14 PM	demo:sqldba
749	✓	Discover resources for host 'sql-standby.demo.netapp.com'	09/16/2021 6:19:00 PM	09/16/2021 6:19:05 PM	Demoadministrator
745	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 5:35:00 PM	09/16/2021 5:37:08 PM	demo:sqldba

Konfiguration nach dem Klonen

- Eine lokale Oracle Produktionsdatenbank wird normalerweise im Protokollarchivierungsmodus ausgeführt. Dieser Modus ist für eine Entwicklungs- oder Testdatenbank nicht erforderlich. Um den Protokollarchivmodus zu deaktivieren, melden Sie sich als sysdba in der Oracle DB an, führen Sie einen Änderungsbefehl für den Protokollmodus aus, und starten Sie die Datenbank für den Zugriff.
- Konfigurieren Sie einen Oracle-Listener oder registrieren Sie die neu geklonte DB für den Benutzerzugriff mit einem vorhandenen Listener.
- Ändern Sie für SQL Server den Protokollmodus von „voll“ in „einfach“, sodass die SQL Server Entwicklungs-/Test-Protokolldatei problemlos verkleinert werden kann, wenn sie das Protokoll-Volumen füllt.

Klondatenbank aktualisieren

1. Ablegen geklonter Datenbanken und Bereinigen der Serverumgebung der Cloud-Datenbanken. Anschließend sollten Sie eine neue DB mit frischen Daten klonen. Das Klonen einer neuen Datenbank dauert nur wenige Minuten.
2. Fahren Sie die Klondatenbank herunter, führen Sie mit der CLI einen Befehl zur Klonaktualisierung aus. Einzelheiten finden Sie in der folgenden SnapCenter-Dokumentation: ["Aktualisieren Sie einen Klon"](#).

Wo Hilfe benötigt wird?

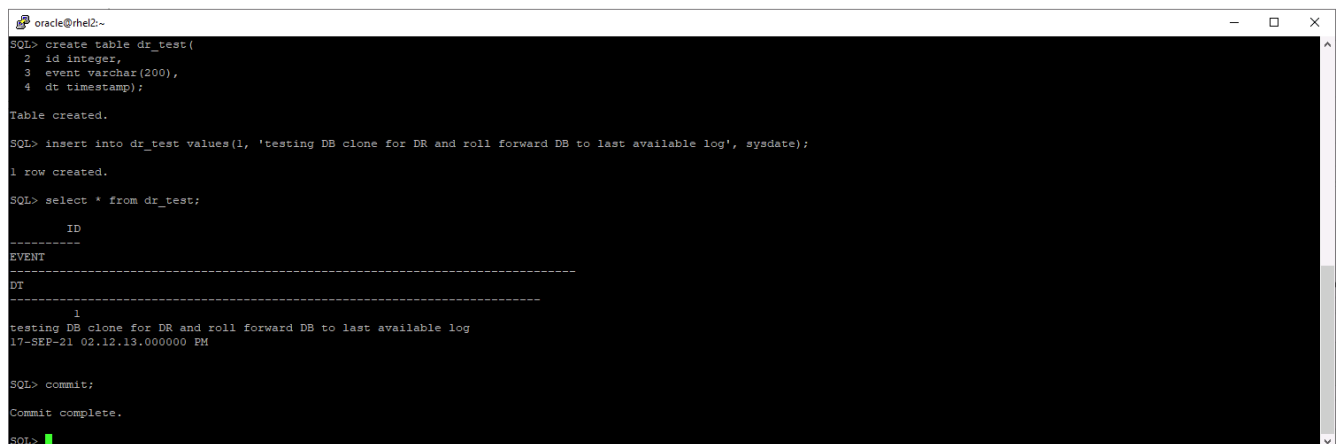
Wenn Sie Hilfe bei dieser Lösung und bei den Anwendungsfällen benötigen, treten Sie dem bei ["NetApp Solution Automation Community unterstützt Slack-Channel"](#) Und suchen Sie den Kanal zur Lösungsautomatisierung, um Ihre Fragen zu stellen oder zu fragen.

Disaster-Recovery-Workflow

Unternehmen nutzen die Public Cloud als praktikable Ressource und Ziel für die Disaster Recovery. SnapCenter macht diesen Prozess so nahtlos wie möglich. Dieser Disaster-Recovery-Workflow ähnelt dem Klon-Workflow sehr, doch die Datenbank-Recovery wird durch das letzte verfügbare Protokoll durchgeführt, das in die Cloud repliziert wurde, um alle möglichen Geschäftstransaktionen wiederherzustellen. Für Disaster Recovery gibt es jedoch noch weitere für die Konfiguration und die Nachbearbeitung ergänzende Schritte.

Klonen einer lokalen Oracle-Produktionsdatenbank in die Cloud für DR

1. Um zu überprüfen, ob die Klonwiederherstellung das letzte verfügbare Protokoll durchlaufen hat, haben wir eine kleine Testtabelle erstellt und eine Zeile eingefügt. Die Testdaten würden nach einer vollständigen Wiederherstellung des letzten verfügbaren Protokolls wiederhergestellt.



```
oracle@rhel2~$
SQL> create table dr_test(
  2 id integer,
  3 event varchar(200),
  4 dt timestamp);
Table created.
SQL> insert into dr_test values(1, 'testing DB clone for DR and roll forward DB to last available log', sysdate);
1 row created.
SQL> select * from dr_test;
-----
ID
-----
EVENT
-----
DT
-----
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM
SQL> commit;
Commit complete.
SQL>
```

2. Melden Sie sich bei SnapCenter als Benutzer-ID für das Datenbankmanagement für Oracle an. Öffnen Sie die Registerkarte Ressourcen, auf der die von SnapCenter geschützten Oracle-Datenbanken angezeigt werden.

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhel2_cdb2	1	orafullbkup	Oracle Full Online Backup	09/17/2021 2:38:16 PM	Completed
rhel2_cdb2_log	1	oralogbkup	Oracle Archive Log Backup	09/17/2021 6:02:13 PM	Completed

3. Wählen Sie die Oracle-Protokollressourcengruppe aus, und klicken Sie auf Jetzt sichern, um manuell ein Oracle-Protokoll-Backup auszuführen, um die letzte Transaktion zum Ziel in der Cloud zu bereinigen. In einem echten DR-Szenario hängt die letzte wiederherstellbare Transaktion von der Replizierungshäufigkeit des Datenbank-Protokoll-Volumes in die Cloud ab, was wiederum von der RTO- oder RPO-Richtlinie des Unternehmens abhängt.

Name	Resource Name	Type	Host
rhel2_cdb2	cdb2	Oracle Database	rhel2.demo.netapp.com
rhel2_cdb2_log			

Backup

Create a backup for the selected resource group

Resource Group:

Policy:



Asynchronous SnapMirror verliert im Rahmen eines Disaster-Recovery-Szenarios Daten, die sie nicht zum Cloud-Ziel gemacht haben. Zur Minimierung von Datenverlusten können häufigere Protokoll-Backups geplant werden. Allerdings gibt es eine Begrenzung auf die technisch machbar Backup Log-Frequenz.

4. Wählen Sie das letzte Protokoll-Backup auf den sekundären Spiegelsicherungs(s) aus, und mounten Sie das Protokoll-Backup.

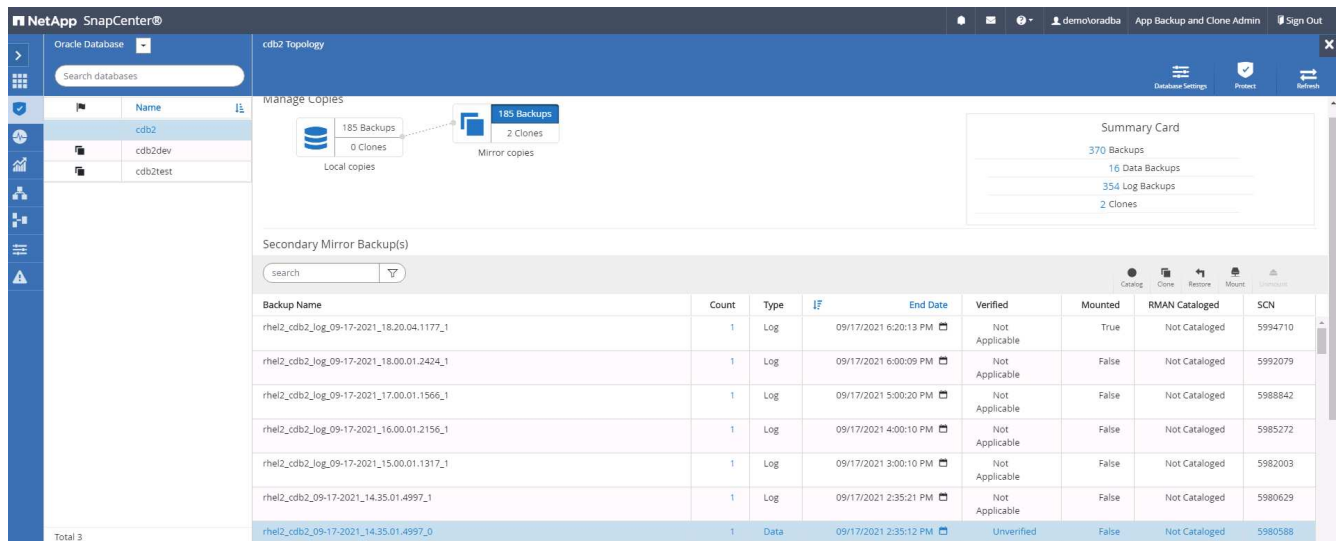
The screenshot shows the NetApp SnapCenter interface for Oracle Database. The main view is 'Manage Copies' for the 'cdb2' topology. It displays 'Local copies' with 185 Backups and 0 Clones, and 'Mirror copies' with 185 Backups and 2 Clones. A 'Summary Card' on the right shows: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this is a table of 'Secondary Mirror Backup(s)'. The table has columns: Backup Name, Count, Type, IF, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The data rows are:

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18:20:04.1177_1	1	Log		09/17/2021 6:20:13 PM	Not Applicable	False	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18:00:01.2424_1	1	Log		09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17:00:01.1566_1	1	Log		09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842

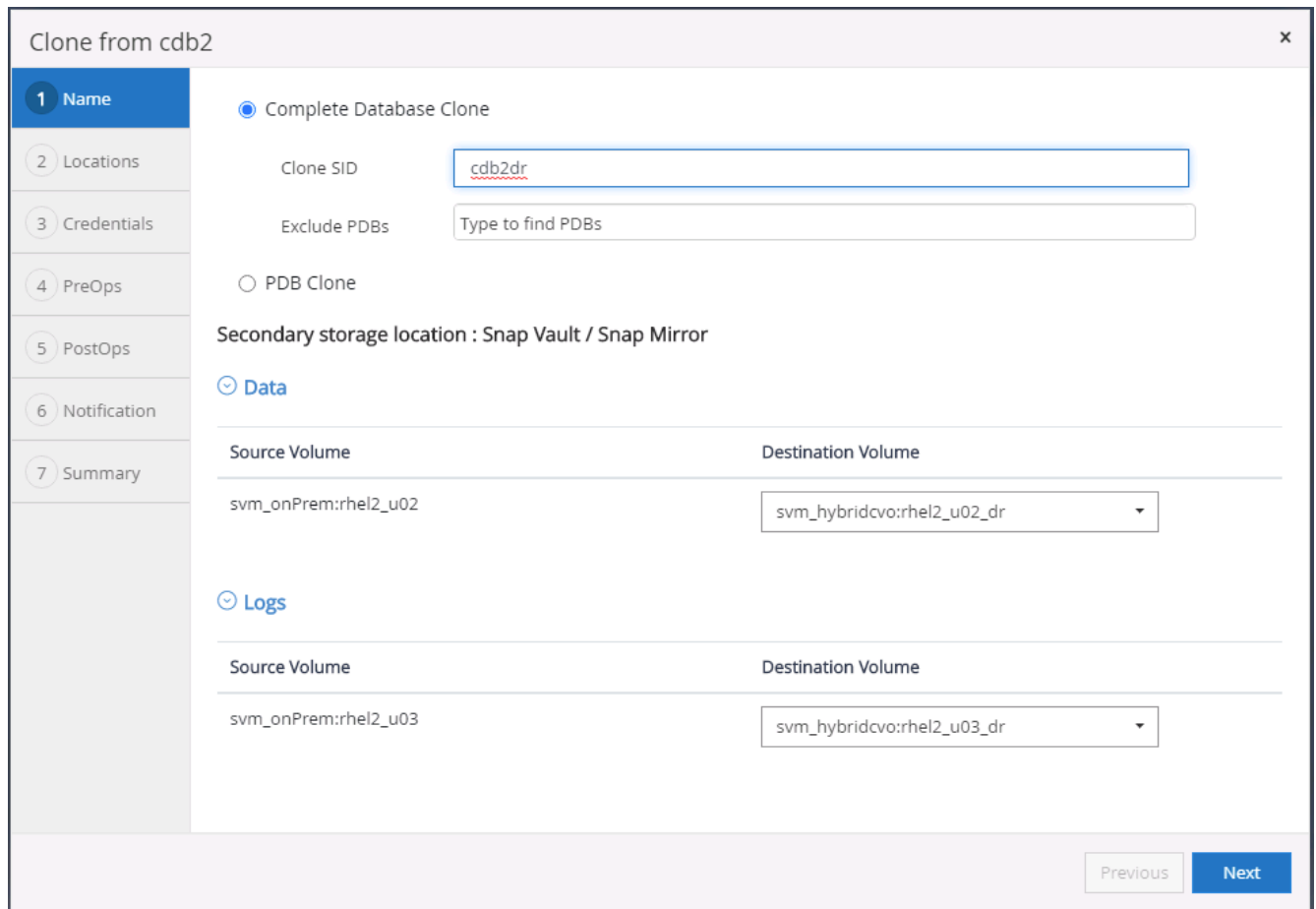
The screenshot shows the 'Mount backups' dialog box. It contains the following fields and options:

- Choose the host to mount the backup: ora-standby.demo.netapp.com
- Mount path: /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2
- Secondary storage location: Snap Vault / Snap Mirror
- Source Volume: svm_onPrem:rhel2_u03
- Destination Volume: svm_hybridcvo:rhel2_u03_dr
- Buttons: Mount, Cancel

5. Wählen Sie das letzte vollständige Datenbank-Backup aus und klicken Sie auf Klonen, um den Klon-Workflow zu initiieren.



6. Wählen Sie eine eindeutige Clone-DB-ID auf dem Host aus.



7. Stellen Sie ein Protokoll-Volumen bereit und mounten Sie es im Oracle Flash Recovery-Bereich und bei Online-Protokollen am Ziel-DR-Server.

ONTAP System Manager

Search actions, objects, and pages

Volumes

+ Add More

Name	Storage VM	Status	Capacity
ora_standby_u01	svm_hybridcvo	Online	12.3 GB used / 17.7 GB available / 31.6 GB
rhel2_u01_dr	svm_hybridcvo	Online	
rhel2_u02_dr	svm_hybridcvo	Online	
rhel2_u02_dr0917211608119360	svm_hybridcvo	Online	
rhel2_u02_dr0917211703534863	svm_hybridcvo	Online	
rhel2_u03_dr	svm_hybridcvo	Online	
rhel2_u03_dr0917211824574775	svm_hybridcvo	Online	

Add Volume

NAME: ora_standby_u03

CAPACITY: 20 GB

More Options Cancel Save

```

ec2-user@ora-standby/tmp
[ec2-user@ora-standby tmp]$ sudo mkdir /u03_cdb2dr
[ec2-user@ora-standby tmp]$ chown oracle:oinstall /u03_cdb2dr
chown: changing ownership of '/u03_cdb2dr': Operation not permitted
[ec2-user@ora-standby tmp]$ sudo chown oracle:oinstall /u03_cdb2dr
[ec2-user@ora-standby tmp]$ sudo mount -t nfs 10.221.1.6:/ora_standby_u03 /u03_cdb2dr
[ec2-user@ora-standby tmp]$ df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  7.6G         0  7.6G   0% /dev
tmpfs                     7.6G         0  7.6G   0% /dev/shm
tmpfs                     7.6G       17M  7.6G   1% /run
tmpfs                     7.6G         0  7.6G   0% /sys/fs/cgroup
/dev/nvme0n1p2            10G        9.0G  1.1G  90% /
10.221.1.6:/ora_standby_u01 31G        13G   18G  42% /u01
tmpfs                     1.6G         0  1.6G   0% /run/user/1000
10.221.1.6:/Sc28182452-3fa8-448c-9e4a-c5a9e465f353 100G       3.1G   97G   4% /u02_cdb2dev
tmpfs                     1.6G         0  1.6G   0% /run/user/54321
10.221.1.6:/Sc39c06df8-4b00-4b3a-853c-9d6d338e5df7 100G       3.7G   97G   4% /u02_cdb2test
10.221.1.6:/Sccf886a5c-3273-479e-ad97-472b2a8dccee 100G       3.8G   97G   4% /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1
10.221.1.6:/ora_standby_u03 21G       320K   20G   1% /u03_cdb2dr
[ec2-user@ora-standby tmp]$

```



Bei dem Klonverfahren von Oracle wird kein Protokoll-Volumen erstellt, das vor dem Klonen auf dem DR-Server bereitgestellt werden muss.

- Wählen Sie den Host und den Speicherort des Zielklons aus, um die Datendateien, Kontrolldateien und Wiederherstellungsprotokolle zu platzieren.

Clone from cdb2
✕

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Select the host to create a clone

Clone host

Datafile locations ⓘ

Reset

Control files ⓘ

✕

✕ Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
RedoGroup 1	200	MB	1
<input type="text" value="/u03_cdb2dr/cdb2dr/redolog/redo03.log"/>			
RedoGroup 2	200	MB	1

+ Reset

Previous
Next

9. Wählen Sie die Anmeldeinformationen für den Klon aus. Geben Sie die Details zur Oracle Home-Konfiguration auf dem Ziel-Server ein.

Clone from cdb2 x

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Database Credentials for the clone

Credential name for sys user + ⓘ

Database port

Oracle Home Settings ⓘ

Oracle Home

Oracle OS User

Oracle OS Group

10. Geben Sie die vor dem Klonen auszuführenden Skripte an. Datenbankparameter können bei Bedarf angepasst werden.

Clone from cdb2
✕

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Specify scripts to run before clone operation ?

Prescript full path

Arguments

Script timeout secs

⊙ Database Parameter settings

audit_file_dest	/u01/app/oracle/admin/cdb2dr/adump	✕	<input type="button" value="+"/> <input type="button" value="Reset"/>
audit_trail	DB	✕	
open_cursors	300	✕	
pga_aggregate_target	1432354816	✕	

11. Wählen Sie als Recovery-Option bis Abbrechen aus, sodass die Recovery alle verfügbaren Archivprotokolle ausgeführt wird, um die letzte Transaktion, die am sekundären Cloud-Standort repliziert wurde, wiederzugewinnen.

Clone from cdb2
x

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification
- 7 Summary

Recover Database

Until Cancel i
 Date and Time i
Date-time format: MM/DD/YYYY hh:mm:ss
 Until SCN (System Change Number) i

Specify external archive log locations i

Create new DBID i
 Create tempfile for temporary tablespace i
 Enter SQL queries to apply when clone is created
 Enter scripts to run after clone operation i

12. Konfigurieren Sie bei Bedarf den SMTP-Server für E-Mail-Benachrichtigungen.

Clone from cdb2

- 1 Name
- 2 Locations
- 3 Credentials
- 4 PreOps
- 5 PostOps
- 6 Notification**
- 7 Summary

Provide email settings ?

Email preference:

From:

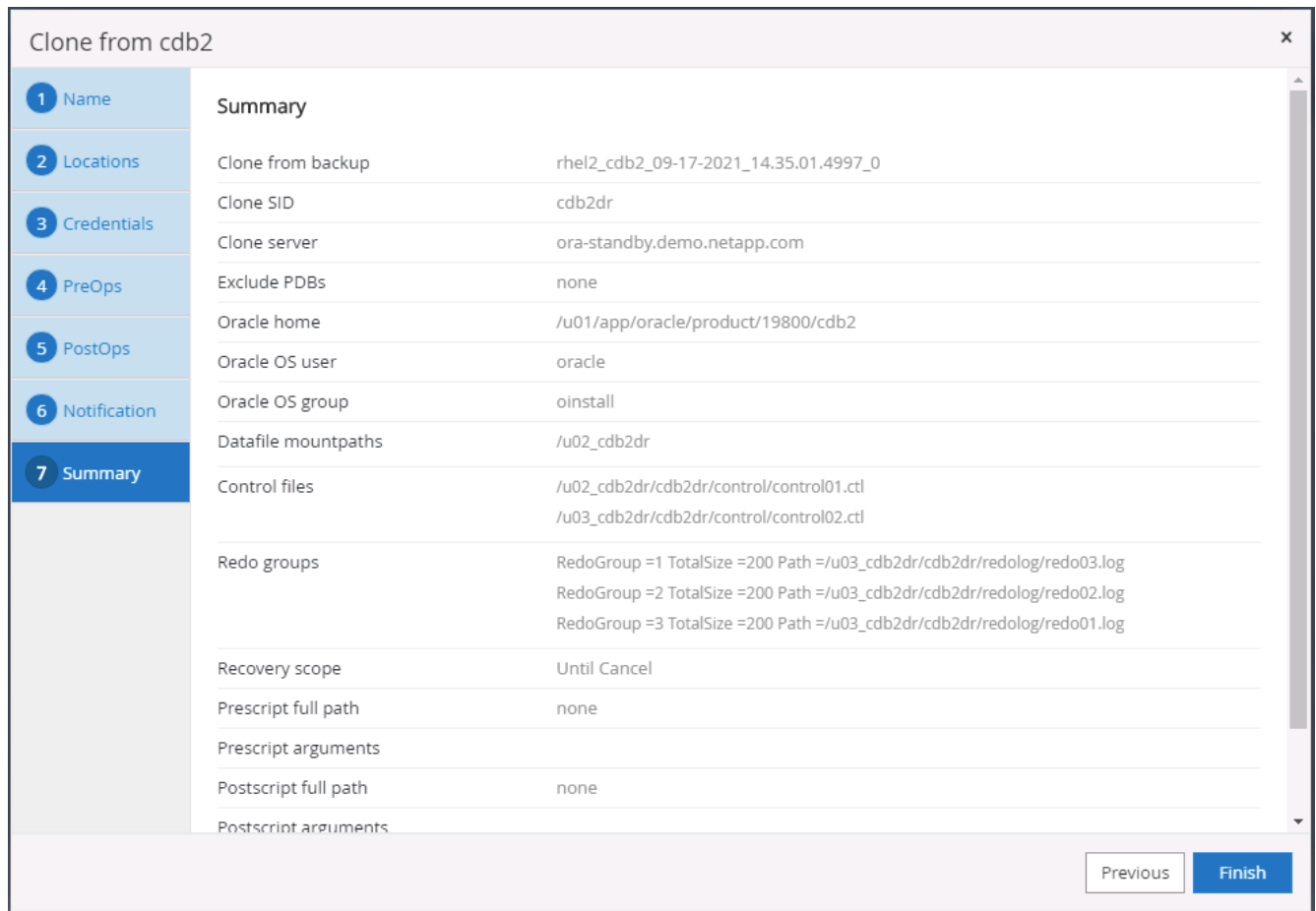
To:

Subject:

Attach job report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

13. Zusammenfassung DES DR-Klons:



14. Geklonte DBs sind sofort nach Abschluss des Klons mit SnapCenter registriert und sind dann für den Backup-Schutz verfügbar.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhe12.demo.netapp.com	rhe12_cdb2 rhe12_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 7:00:10 PM	Backup succeeded
cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected
cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected
cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected

Validierung und Konfiguration von Post-DR-Klonen für Oracle

1. Validierung der letzten Testtransaktion, die am DR-Standort in der Cloud gespeichert, repliziert und wiederhergestellt wurde

```

oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> set lin 200
SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME      HOST_NAME
-----
cdb2dr              ora-standby.demo.netapp.com

SQL> alter pluggable database cdb2_pdb1 open;

Pluggable database altered.

SQL> alter session set container=cdb2_pdb1;

Session altered.

SQL> select * from pdbadmin.dr_test;

-----
ID
-----
EVENT
-----
DT
-----
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL>

```

2. Konfigurieren Sie den Flash-Recovery-Bereich.

```

oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
[oracle@ora-standby:dbs]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 22:07:11 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> show parameter db_recovery_file_dest

NAME                                 TYPE        VALUE
-----
db_recovery_file_dest                 string      /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size            big integer 17208M
SQL> alter system set db_recovery_file_dest='/u03_cdb2dr/cdb2dr' scope=both;

System altered.

SQL> show parameter db_recovery_file_dest

NAME                                 TYPE        VALUE
-----
db_recovery_file_dest                 string      /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size            big integer 17208M

SQL>

```

3. Konfigurieren Sie den Oracle Listener für den Benutzerzugriff.
4. Verteilen Sie das geklonte Volume vom replizierten Quell-Volumen.
5. Die Replizierung wird von der Cloud in On-Premises-Systeme umkehren und der ausgefallene On-Premises-Datenbankserver neu erstellt.



Durch die Aufteilung des Klons wird möglicherweise eine temporäre Storage-Auslastung verursacht, die deutlich höher ist als der normale Betrieb. Nach der Rekonstruktion der lokalen DB-Server kann jedoch zusätzlicher Speicherplatz freigegeben werden.

Klonen einer lokalen SQL-Produktionsdatenbank in die Cloud für DR

1. Um sicherzustellen, dass die SQL-Klon-Recovery durch das letzte verfügbare Protokoll ausgeführt wurde, haben wir eine kleine Testtabelle erstellt und eine Reihe eingefügt. Die Testdaten würden nach einer vollständigen Wiederherstellung des letzten verfügbaren Protokolls wiederhergestellt.

```

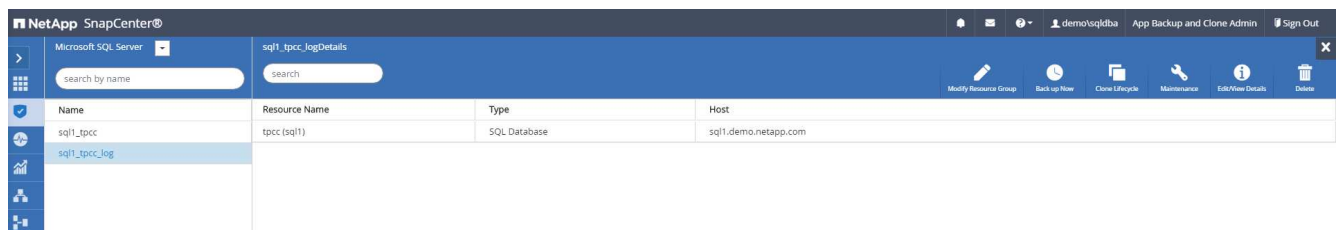
Administrator: Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

-----
SQL1
(1 rows affected)
1> use tpcc
2> go
Changed database context to 'tpcc'.
1> insert into snap_sync values ('test snap mirror DR for SQL', getdate())
2> go

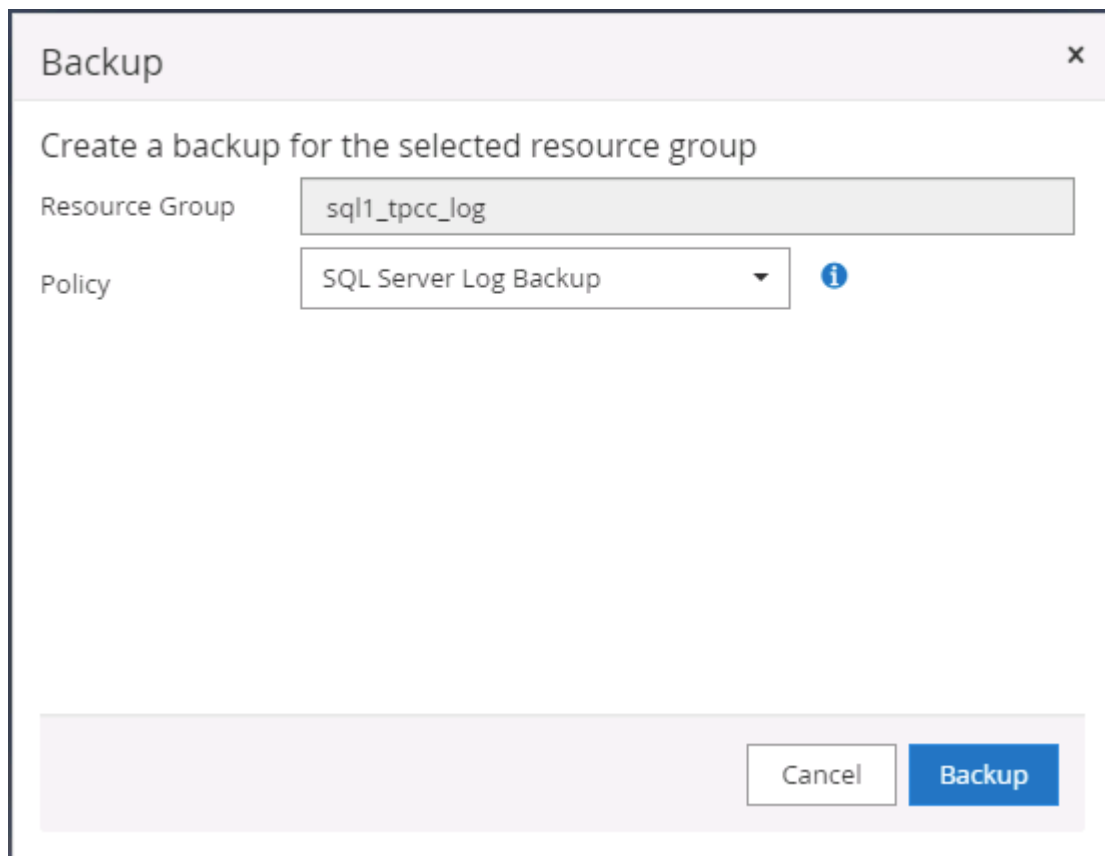
(1 rows affected)
1> select * from snap_sync
2> go
event                                     dt
-----
test snap mirror DR for SQL                2021-09-20 14:23:04.533
(1 rows affected)
1>

```

- Melden Sie sich mit einer Datenbank-Management-Benutzer-ID für SQL Server bei SnapCenter an. Navigieren Sie zur Registerkarte Ressourcen, auf der die SQL Server-Schutzressourcen-Gruppe angezeigt wird.



- Führen Sie ein Protokoll-Backup manuell aus, um die letzte Transaktion auszuführen, die in den sekundären Storage in der Public Cloud repliziert werden soll.



- Wählen Sie das letzte vollständige SQL Server-Backup für den Klon aus.

Backup Name	Count	Type	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup	09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup	09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup	09/17/2021 6:25:05 PM	Unverified

5. Legen Sie die Kloneinstellung fest, z. B. den Klon-Server, die Kloninstanz, den Klontnamen und die Mount-Option. Der sekundäre Storage-Standort, an dem das Klonen durchgeführt wird, ist automatisch gefüllt.

Clone from backup

1 Clone Options

Clone settings

Clone server: sql-standby.demo.netapp.com

Clone instance: sql-standby

Clone name: tpcc_dr

Choose mount option

Auto assign mount point

Auto assign volume mount point under path: full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous Next

6. Wählen Sie alle anzuwendenden Protokollsicherungen aus.

Clone from backup x

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

All log backups

By log backups until

By specific date until

None

7. Geben Sie alle optionalen Skripte an, die vor oder nach dem Klonen ausgeführt werden sollen.

Clone from backup

- 1 Clone Options
- 2 Logs
- 3 Script**
- 4 Notification
- 5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments

Postscript full path

Postscript arguments

Script timeout

8. Geben Sie einen SMTP-Server an, wenn eine E-Mail-Benachrichtigung gewünscht wird.

Clone from backup

- 1 Clone Options
- 2 Logs
- 3 Script
- 4 Notification**
- 5 Summary

Provide email settings ?

Email preference:

From:

To:

Subject:

Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

9. Zusammenfassung DES DR-Klons: Geklonte Datenbanken werden sofort in SnapCenter registriert und stehen für den Backup-Schutz zur Verfügung.

Clone from backup

- 1 Clone Options
- 2 Logs
- 3 Script
- 4 Notification
- 5 Summary

Summary

Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dr
Mount option	Auto Mount
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

Previous Finish

NetApp SnapCenter® Microsoft SQL Server

View Database search by name

Resources	Name	Instance	Host	Last Backup	Overall Status	Type
	master	sql1	sql1.demo.netapp.com		Not available for backup	System database
	model	sql1	sql1.demo.netapp.com		Not available for backup	System database
	msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
	tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
	tpcc	sql1	sql1.demo.netapp.com	09/22/2021 5:35:08 PM	Backup failed, Schedules on hold	User database
	master	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
	model	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
	msdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
	tempdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
	tpcc_clone	sql-standby	sql-standby.demo.netapp.com		Not protected	User database
	tpcc_dev	sql-standby	sql-standby.demo.netapp.com		Not protected	User database
	tpcc_dr	sql-standby	sql-standby.demo.netapp.com		Not protected	User database

Validierung und Konfiguration von SQL-Klonen nach dem DR-Verfahren

1. Überwachen des Auftragsstatus von Klonen.

NetApp SnapCenter® Jobs Schedules Events Logs

search by name

Jobs - Filter

ID	Status	Name	Start date	End date	Owner
1052	✓	Clone from backup 'sql1_tpcc_09-19-2021_18.25.01.4134'	09/20/2021 2:36:17 PM	09/20/2021 2:37:06 PM	demo:sqlqdba
1047	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:35:01 PM	09/20/2021 2:37:08 PM	demo:sqlqdba
1045	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:38:17 PM	09/20/2021 2:30:25 PM	demo:sqlqdba
1044	✓	Clone from backup 'sql1_tpcc_09-17-2021_18.25.01.4218'	09/20/2021 1:39:24 PM	09/20/2021 1:40:09 PM	demo:sqlqdba
1042	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:35:01 PM	09/20/2021 1:37:08 PM	demo:sqlqdba
1040	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 12:35:01 PM	09/20/2021 12:37:08 PM	demo:sqlqdba

2. Überprüfen Sie, ob die letzte Transaktion repliziert und mit allen Klonen von Protokolldateien und

Recovery wiederhergestellt wurde.

```
Administrator: Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go
-----
SQL-STANDBY
(1 rows affected)
1> use tpcc_dr
2> go
Changed database context to 'tpcc_dr'.
1> select * from snap_sync
2> go
event dt
-----
test snap mirror DR for SQL          2021-09-20 14:23:04.533
(1 rows affected)
1> select getdate()
2> go
-----
2021-09-20 14:39:19.937
(1 rows affected)
1>
```

3. Konfigurieren Sie ein neues SnapCenter-Protokollverzeichnis auf dem DR-Server für die Sicherung der SQL Server-Protokolle.
4. Verteilen Sie das geklonte Volume vom replizierten Quell-Volumen.
5. Die Replizierung wird von der Cloud in On-Premises-Systeme umkehren und der ausgefallene On-Premises-Datenbankserver neu erstellt.

Wo Hilfe benötigt wird?

Wenn Sie Hilfe bei dieser Lösung und diesen Anwendungsbeispielen benötigen, nehmen Sie an der Teil ["NetApp Solution Automation Community unterstützt Slack-Channel"](#) Und suchen Sie den Kanal zur Lösungsautomatisierung, um Ihre Fragen zu stellen oder zu fragen.

Toolkits für DB-Automatisierung

SnapCenter Lifecycle Automation für Oracle-Klone

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Kunden sind begeistert von der FlexClone Funktion von NetApp ONTAP Storage für Datenbanken, mit deutlichen Einsparungen bei den Storage-Kosten. Dieses Ansible-basierte Toolkit automatisiert die Einrichtung, das Klonen und die Aktualisierung von geklonten Oracle Datenbanken anhand der NetApp SnapCenter Befehlszeilen-Dienstprogramme für ein optimiertes Lifecycle Management. Das Toolkit ist auf Oracle-Datenbanken anwendbar, die auf ONTAP Storage entweder bei Vorliegen oder in der Public Cloud bereitgestellt und über das UI Tool NetApp SnapCenter gemanagt werden.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Richten Sie die Konfigurationsdatei für die Klonspezifikation der Oracle-Datenbank ein.
- Erstellen und aktualisieren Sie die Oracle-Datenbank nach benutzerdefiniertem Zeitplan.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle Datenbanken mit SnapCenter managt.

- Ein Storage-Administrator, der ONTAP Storage mit SnapCenter managt
- Ein Anwendungseigentümer, der Zugriff auf die SnapCenter-Benutzeroberfläche hat.

Lizenz

Durch den Zugriff auf, das Herunterladen, die Installation oder die Verwendung der Inhalte in diesem GitHub-Repository stimmen Sie den Bedingungen der in dargelegten Lizenz zu "[Lizenzdatei](#)".



Es gibt bestimmte Beschränkungen bezüglich der Erstellung und/oder Freigabe von abgeleiteten Arbeiten mit dem Inhalt in diesem GitHub-Repository. Bitte lesen Sie die Lizenzbedingungen, bevor Sie den Inhalt verwenden. Wenn Sie nicht allen Bedingungen zustimmen, dürfen Sie nicht auf den Inhalt dieses Repositories zugreifen, ihn herunterladen oder verwenden.

Lösungsimplementierung

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

```
Ansible controller:  
  Ansible v.2.10 and higher  
  ONTAP collection 21.19.1  
  Python 3  
Python libraries:  
  netapp-lib  
  xmldict  
  jmespath
```

```
SnapCenter server:  
  version 5.0  
  backup policy configured  
  Source database protected with a backup policy
```

```
Oracle servers:  
  Source server managed by SnapCenter  
  Target server managed by SnapCenter  
  Target server with identical Oracle software stack as source server  
  installed and configured
```

Toolkit herunterladen

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-  
bb/na_oracle_clone_lifecycle.git
```

Dateikonfiguration der Ansible Ziel-Hosts

Das Toolkit enthält eine Host-Datei, die die Ziele definiert, für die ein Ansible-Playbook ausgeführt wird. In der Regel sind dies die Ziel-Clones-Hosts von Oracle. Im Folgenden finden Sie eine Beispieldatei. Ein Hosteintrag enthält die IP-Adresse des Zielhosts sowie den SSH-Schlüssel für den Zugriff eines Admin-Benutzers auf den Host, um den Klon- oder Aktualisierungsbefehl auszuführen.

#Oracle-Clone-Hosts

```
[clone_1]  
ora_04.cie.netapp.com ansible_host=10.61.180.29  
ansible_ssh_private_key_file=ora_04.pem
```

```
[clone_2]  
[clone_3]
```

Konfiguration globaler Variablen

Die Ansible-Playbooks verwenden variable Eingaben aus mehreren variablen Dateien. Unten finden Sie ein Beispiel für die globale Variablendatei VARs.yml.

```
# ONTAP specific config variables  
# SnapCtr specific config variables
```

```
snapctr_usr: xxxxxxxx  
snapctr_pwd: 'xxxxxxx'
```

```
backup_policy: 'Oracle Full offline Backup'  
# Linux specific config variables  
# Oracle specific config variables
```

Konfiguration der Host-Variablen

Hostvariablen werden im Verzeichnis `Host_VARS` mit dem Namen `{{ Host_Name }}`.yml definiert. Unten ist ein Beispiel für die Oracle-Zieldatei `ora_04.cie.netapp.com.yml`, die eine typische Konfiguration zeigt.

```
# User configurable Oracle clone db host specific parameters
```

```
# Source database to clone from
source_db_sid: NTAP1
source_db_host: ora_03.cie.netapp.com
```

```
# Clone database
clone_db_sid: NTAP1DEV
```

```
snapctr_obj_id: '{{ source_db_host }}\{{ source_db_sid }}'
```

Zusätzliche Clone-Ziel-Oracle-Serverkonfiguration

Der Oracle-Zielserver für Clones sollte denselben Oracle-Softwarestack aufweisen wie der Oracle-Quellserver, der installiert und gepatcht ist. Oracle-Benutzer `.bash_profile` hat `ORACLE_BASE` in Höhe von `USD` und `ORACLE_HOME` in Höhe von `USD` konfiguriert. Außerdem sollte die Variable „`ORACLE_HOME`“ mit der Oracle-Quellservereinstellung übereinstimmen. Hier ein Beispiel.

```
# .bash_profile
```

```
# Get the aliases and functions
if [ -f ~/.bashrc ]; then
    . ~/.bashrc
fi
```

```
# User specific environment and startup programs
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/NTAP1
```

Ausführung des Playbook

Es gibt insgesamt drei Playbooks zur Ausführung des Lebenszyklus von Oracle Datenbankklonen mit SnapCenter CLI-Dienstprogrammen.

1. Einmalige Installation von Ansible-Controller-Voraussetzungen

```
ansible-playbook -i hosts ansible_requirements.yml
```

2. Spezifikationsdatei für Clone einrichten – nur einmalig.

```
ansible-playbook -i hosts clone_1_setup.yml -u admin -e  
@vars/vars.yml
```

3. Erstellen und aktualisieren Sie die Klondatenbank regelmäßig von crontab mit einem Shell-Skript, um ein Aktualisierungs-Playbook aufzurufen.

```
0 */4 * * * /home/admin/na_oracle_clone_lifecycle/clone_1_refresh.sh
```

Erstellen Sie für eine zusätzliche Clone-Datenbank separate Clones_n_Setup.yml und Clone_n_refresh.yml sowie Clone_n_refresh.sh. Konfigurieren Sie die Ansible-Zielhosts und die Datei hostname.yml im Verzeichnis Host_vars entsprechend.

Wo Sie weitere Informationen finden

Weitere Informationen zur Automatisierung von NetApp Lösungen finden Sie auf der folgenden Website "[Automatisierung der NetApp Lösung](#)"

Automatisierte Oracle-Migration

NetApp Solutions Engineering Team

Zweck

Dieses Toolkit automatisiert die Migration von Oracle Datenbanken von lokalen Systemen in die AWS Cloud mit FSX ONTAP Storage und EC2 Computing-Instanz als Zielinfrastruktur. Er geht davon aus, dass der Kunde bereits über eine Oracle-Datenbank vor Ort im CDB/PDB-Modell verfügt. Mit dem Toolkit kann der Kunde eine benannte PDB aus einer Container-Datenbank auf einem Oracle-Host verschieben. Dabei wird das Verfahren für die Oracle-PDB-Verschiebung mit einer Option für maximale Verfügbarkeit verwendet. Das bedeutet, dass die Quell-PDB auf jedem lokalen Storage-Array mit minimaler Serviceunterbrechung in eine neue Container-Datenbank verlagert wird. Bei der Oracle-Verlagerung werden die Oracle-Datendateien verschoben, während die Datenbank online ist. Er leitet Benutzer-Sessions zum Zeitpunkt des Umschaltens von lokalen Systemen in die umgelagerten Datenbank-Services um, wenn alle Datendateien in die AWS-Cloud verschoben werden. Die unterstrichene Technologie ist die bewährte Oracle PDB Hot Clone-Methodik.



Obwohl das Migrations-Toolkit für die AWS Cloud-Infrastruktur entwickelt und validiert wurde, basiert es auf Lösungen auf Applikationsebene von Oracle. Daher ist das Toolkit auch für andere Public-Cloud-Plattformen wie Azure, GCP usw. anwendbar

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Erstellen Sie einen Migrationsbenutzer und gewähren Sie die erforderlichen Berechtigungen auf dem lokalen Quell-DB-Server.
- Verlagerung einer PDB von einer lokalen CDB auf eine Ziel-CDB in der Cloud, während die Quell-PDB bis zum Umschalten online ist.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle-Datenbanken von On-Premises in die AWS Cloud migriert.
- Ein Database Solution Architect, der an der Migration der Oracle-Datenbank von On-Premises zur AWS Cloud interessiert ist.
- Ein Storage-Administrator, der für das Management von AWS FSX ONTAP Storage zur Unterstützung von Oracle-Datenbanken zuständig ist
- Ein Applikationsinhaber, der Oracle Database von On-Premises in die AWS Cloud migrieren möchte.

Lizenz

Durch den Zugriff auf, das Herunterladen, die Installation oder die Verwendung der Inhalte in diesem GitHub-Repository stimmen Sie den Bedingungen der in dargelegten Lizenz zu "[Lizenzdatei](#)".



Es gibt bestimmte Beschränkungen bezüglich der Erstellung und/oder Freigabe von abgeleiteten Arbeiten mit dem Inhalt in diesem GitHub-Repository. Bitte lesen Sie die Lizenzbedingungen, bevor Sie den Inhalt verwenden. Wenn Sie nicht allen Bedingungen zustimmen, dürfen Sie nicht auf den Inhalt dieses Repositories zugreifen, ihn herunterladen oder verwenden.

Lösungsimplementierung

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

```
Ansible v.2.10 and higher
ONTAP collection 21.19.1
Python 3
Python libraries:
  netapp-lib
  xmltodict
  jmespath
```

```
Source Oracle CDB with PDBs on-premises
Target Oracle CDB in AWS hosted on FSx and EC2 instance
Source and target CDB on same version and with same options installed
```

```
Network connectivity
  Ansible controller to source CDB
  Ansible controller to target CDB
  Source CDB to target CDB on Oracle listener port (typical 1521)
```

Toolkit herunterladen

```
git clone https://github.com/NetApp/na_ora_aws_migration.git
```

Konfiguration der Host-Variablen

Hostvariablen werden im Verzeichnis Host_VARS mit dem Namen {{ Host_Name }}.yml definiert. Eine Beispiel-Host-Variable Datei Host_Name.yml ist enthalten, um die typische Konfiguration zu demonstrieren. Wichtige Überlegungen:

```
Source Oracle CDB - define host specific variables for the on-prem CDB
ansible_host: IP address of source database server host
source_oracle_sid: source Oracle CDB instance ID
source_pdb_name: source PDB name to migrate to cloud
source_file_directory: file directory of source PDB data files
target_file_directory: file directory of migrated PDB data files
```

```
Target Oracle CDB - define host specific variables for the target CDB
including some variables for on-prem CDB
ansible_host: IP address of target database server host
target_oracle_sid: target Oracle CDB instance ID
target_pdb_name: target PDB name to be migrated to cloud (for max
availability option, the source and target PDB name must be the same)
source_oracle_sid: source Oracle CDB instance ID
source_pdb_name: source PDB name to be migrated to cloud
source_port: source Oracle CDB listener port
source_oracle_domain: source Oracle database domain name
source_file_directory: file directory of source PDB data files
target_file_directory: file directory of migrated PDB data files
```

Konfiguration der Hostdatei des DB-Servers

AWS EC2-Instanz verwenden standardmäßig die IP-Adresse für die Hostbenennung. Wenn Sie einen anderen Namen in der Hostdatei für Ansible verwenden, richten Sie die Auflösung der Hostbenennung in der Datei /etc/Hosts sowohl für den Quell- als auch für den Zielservers ein. Hier ein Beispiel.

```
127.0.0.1    localhost localhost.localdomain localhost4
localhost4.localhost4
::1         localhost localhost.localdomain localhost6
localhost6.localhost6
172.30.15.96 source_db_server
172.30.15.107 target_db_server
```

Ausführung des Playbooks – in der Reihenfolge ausgeführt

1. Voraussetzungen für die Installation des Ansible-Controllers

```
ansible-playbook -i hosts requirements.yml
```

```
ansible-galaxy collection install -r collections/requirements.yml  
--force
```

2. Führen Sie Aufgaben vor der Migration auf dem lokalen Server aus. Dabei wird davon ausgegangen, dass Admin ssh-Benutzer für die Verbindung zum lokalen Oracle-Host mit sudo-Berechtigung ist.

```
ansible-playbook -i hosts ora_pdb_relocate.yml -u admin -k -K -t  
ora_pdb_relo_onprem
```

3. Führen Sie die Oracle-PDB-Verlagerung von der lokalen CDB zur Ziel-CDB in der AWS ec2-Instanz aus, wobei ec2-User für die Verbindung mit der ec2-DB-Instanz und db1.pem mit SSH-Schlüsselpaaren für ec2-Benutzer vorausgesetzt werden.

```
ansible-playbook -i hosts ora_pdb_relocate.yml -u ec2-user --private  
-key db1.pem -t ora_pdb_relo_primary
```

Wo Sie weitere Informationen finden

Weitere Informationen zur Automatisierung von NetApp Lösungen finden Sie auf der folgenden Website ["Automatisierung der NetApp Lösung"](#)

Automatisierte Oracle HA/DR in AWS FSX ONTAP

NetApp Solutions Engineering Team

Zweck

Dieses Toolkit automatisiert die Aufgaben beim Einrichten und Managen einer Umgebung für Hochverfügbarkeit und Disaster Recovery (HR/DR) für Oracle Database, die in der AWS Cloud mit FSX für ONTAP Storage- und EC2 Computing-Instanzen implementiert wird.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Richten Sie HA/DR-Ziel-Host ein – Kernel-Konfiguration, Oracle-Konfiguration, die mit dem Quell-Server-Host übereinstimmt.
- Einrichtung von FSX ONTAP – Einrichtung von Cluster-Peering, vServer-Peering, Einrichtung der Oracle Volumes snapmirror Beziehung von der Quelle zum Ziel.
- Sichern Sie Oracle-Datenbankdaten per Snapshot - Ausführen von crontab
- Backup Oracle Datenbank Archiv Protokoll per Snapshot - Ausführen von crontab

- Failover und Recovery auf HA/DR-Host – testen und validieren der HA/DR-Umgebung
- Resynchronisierung nach Failover-Test durchführen - Datenbank-Volumes snapmirror-Beziehung wieder im HA-/DR-Modus einrichten

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle-Datenbanken in AWS für Hochverfügbarkeit, Datensicherung und Disaster Recovery eingerichtet hat.
- Ein Datenbanklösungsarchitekt, der an einer Oracle HA/DR-Lösung auf Storage-Ebene in der AWS-Cloud interessiert ist.
- Ein Storage-Administrator, der für das Management von AWS FSX ONTAP Storage zur Unterstützung von Oracle-Datenbanken zuständig ist
- Ein Applikationseigentümer, der Oracle Database für HA/DR in einer AWS FSX/EC2-Umgebung einrichten möchte.

Lizenz

Durch den Zugriff auf, das Herunterladen, die Installation oder die Verwendung der Inhalte in diesem GitHub-Repository stimmen Sie den Bedingungen der in dargelegten Lizenz zu "[Lizenzdatei](#)".



Es gibt bestimmte Beschränkungen bezüglich der Erstellung und/oder Freigabe von abgeleiteten Arbeiten mit dem Inhalt in diesem GitHub-Repository. Bitte lesen Sie die Lizenzbedingungen, bevor Sie den Inhalt verwenden. Wenn Sie nicht allen Bedingungen zustimmen, dürfen Sie nicht auf den Inhalt dieses Repositories zugreifen, ihn herunterladen oder verwenden.

Lösungsimplementierung

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

```
Ansible v.2.10 and higher
ONTAP collection 21.19.1
Python 3
Python libraries:
  netapp-lib
  xmltodict
  jmespath
```

```
AWS FSx storage as is available
```

```
AWS EC2 Instance
  RHEL 7/8, Oracle Linux 7/8
  Network interfaces for NFS, public (internet) and optional management
  Existing Oracle environment on source, and the equivalent Linux
  operating system at the target
```

Toolkit herunterladen

```
git clone https://github.com/NetApp/na_ora_hadr_failover_resync.git
```

Konfiguration globaler Variablen

Die Ansible-Playbooks sind variablengetrieben. Eine globale Beispieldatei `fsx_VARS_example.yml` ist enthalten, um eine typische Konfiguration zu demonstrieren. Wichtige Überlegungen:

ONTAP - retrieve FSx storage parameters using AWS FSx console for both source and target FSx clusters.

cluster name: source/destination

cluster management IP: source/destination

inter-cluster IP: source/destination

vserver name: source/destination

vserver management IP: source/destination

NFS lifs: source/destination

cluster credentials: fsxadmin and vsadmin pwd to be updated in `roles/ontap_setup/defaults/main.yml` file

Oracle database volumes - they should have been created from AWS FSx console, volume naming should follow strictly with following standard:

Oracle binary: `{{ host_name }}_bin`, generally one lun/volume

Oracle data: `{{ host_name }}_data`, can be multiple luns/volume, add additional line for each additional lun/volume in variable such as `{{ host_name }}_data_01`, `{{ host_name }}_data_02` ...

Oracle log: `{{ host_name }}_log`, can be multiple luns/volume, add additional line for each additional lun/volume in variable such as `{{ host_name }}_log_01`, `{{ host_name }}_log_02` ...

host_name: as defined in hosts file in root directory, the code is written to be specifically matched up with host name defined in host file.

Linux and DB specific global variables - keep it as is.

Enter redhat subscription if you have one, otherwise leave it black.

Konfiguration der Host-Variablen

Hostvariablen werden im Verzeichnis Host_VARS mit dem Namen {{ Host_Name }}.yml definiert. Eine Beispiel-Host-Variable Datei Host_Name.yml ist enthalten, um die typische Konfiguration zu demonstrieren. Wichtige Überlegungen:

```
Oracle - define host specific variables when deploying Oracle in
multiple hosts concurrently
  ansible_host: IP address of database server host
  log_archive_mode: enable archive log archiving (true) or not (false)
  oracle_sid: Oracle instance identifier
  pdb: Oracle in a container configuration, name pdb_name string and
number of pdbs (Oracle allows 3 pdbs free of multitenant license fee)
  listener_port: Oracle listener port, default 1521
  memory_limit: set Oracle SGA size, normally up to 75% RAM
  host_datastores_nfs: combining of all Oracle volumes (binary, data,
and log) as defined in global vars file. If multi luns/volumes, keep
exactly the same number of luns/volumes in host_var file
```

```
Linux - define host specific variables at Linux level
  hugepages_nr: set hugepage for large DB with large SGA for
performance
  swap_blocks: add swap space to EC2 instance. If swap exist, it will
be ignored.
```

Konfiguration der Hostdatei des DB-Servers

AWS EC2-Instanz verwenden standardmäßig die IP-Adresse für die Hostbenennung. Wenn Sie einen anderen Namen in der Hostdatei für Ansible verwenden, richten Sie die Auflösung der Hostbenennung in der Datei /etc/Hosts sowohl für Quell- als auch für Zielservers ein. Hier ein Beispiel.

```
127.0.0.1    localhost localhost.localdomain localhost4
localhost4.localhost4
::1         localhost localhost.localdomain localhost6
localhost6.localhost6
172.30.15.96 db1
172.30.15.107 db2
```

Ausführung des Playbooks – in der Reihenfolge ausgeführt

1. Controller-Prerequisites Ansible installieren

```
ansible-playbook -i hosts requirements.yml
```

```
ansible-galaxy collection install -r collections/requirements.yml  
--force
```

2. Einrichtung der Ziel-EC2 DB-Instanz.

```
ansible-playbook -i hosts ora_dr_setup.yml -u ec2-user --private-key  
db2.pem -e @vars/fsx_vars.yml
```

3. FSX ONTAP-snapmirror-Beziehung zwischen Quell- und Ziel-Datenbank-Volumes einrichten

```
ansible-playbook -i hosts ontap_setup.yml -u ec2-user --private-key  
db2.pem -e @vars/fsx_vars.yml
```

4. Sichern Sie die Datenvolumes der Oracle-Datenbank per Snapshot von crontab.

```
10 * * * * cd /home/admin/na_ora_hadr_failover_resync &&  
/usr/bin/ansible-playbook -i hosts ora_replication_cg.yml -u ec2-  
user --private-key db1.pem -e @vars/fsx_vars.yml >>  
logs/snap_data_`date +"%Y-%m%d-%H%M%S"`.log 2>&1
```

5. Backup von Protokollvolumes der Oracle-Datenbank per Snapshot von crontab.

```
0,20,30,40,50 * * * * cd /home/admin/na_ora_hadr_failover_resync &&  
/usr/bin/ansible-playbook -i hosts ora_replication_logs.yml -u ec2-  
user --private-key db1.pem -e @vars/fsx_vars.yml >>  
logs/snap_log_`date +"%Y-%m%d-%H%M%S"`.log 2>&1
```

6. Failover und Recovery von Oracle Datenbanken auf EC2 Ziel-DB-Instanz – HA/DR-Konfiguration testen und validieren

```
ansible-playbook -i hosts ora_recovery.yml -u ec2-user --private-key  
db2.pem -e @vars/fsx_vars.yml
```

7. Resynchronisierung nach Failover-Test durchführen - Datenbank-Volumes snapmirror-Beziehung im Replizierungsmodus wiederherstellen.

```
ansible-playbook -i hosts ontap_ora_resync.yml -u ec2-user --private  
-key db2.pem -e @vars/fsx_vars.yml
```

Wo Sie weitere Informationen finden

Weitere Informationen zur Automatisierung von NetApp Lösungen finden Sie auf der folgenden Website "[Automatisierung der NetApp Lösung](#)"

Bereitstellung von AWS FSX ONTAP-Clustern und EC2-Instanzen

NetApp Solutions Engineering Team

Zweck

Dieses Toolkit automatisiert die Aufgaben der Bereitstellung eines AWS FSX ONTAP Storage-Clusters und einer EC2 Computing-Instanz, die anschließend für die Datenbankimplementierung verwendet werden können.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Stellen Sie eine EC2 Computing-Instanz in der AWS Cloud in einem vordefinierten VPC-Subnetz bereit und legen Sie ssh-Schlüssel für den EC2-Instanzzugriff als ec2-User fest.
- Stellen Sie ein AWS FSX ONTAP Storage-Cluster in gewünschten Verfügbarkeitszonen bereit, konfigurieren Sie eine Storage-SVM und legen Sie das Cluster-Admin-Benutzerpasswort fsxadmin fest.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Datenbanken in der AWS EC2 Umgebung verwaltet.
- Ein Database Solution Architect, der an einer Datenbankimplementierung im AWS EC2 Ecosystem interessiert ist.
- Ein Storage-Administrator, der für das Management von AWS FSX ONTAP Storage, der Datenbanken unterstützt, zuständig ist
- Ein Applikationseigentümer, der eine Datenbank in AWS EC2 Ecosystem aufbauen möchte.

Lizenz

Durch den Zugriff auf, das Herunterladen, die Installation oder die Verwendung der Inhalte in diesem GitHub-Repository stimmen Sie den Bedingungen der in dargelegten Lizenz zu "[Lizenzdatei](#)".



Es gibt bestimmte Beschränkungen bezüglich der Erstellung und/oder Freigabe von abgeleiteten Arbeiten mit dem Inhalt in diesem GitHub-Repository. Bitte lesen Sie die Lizenzbedingungen, bevor Sie den Inhalt verwenden. Wenn Sie nicht allen Bedingungen zustimmen, dürfen Sie nicht auf den Inhalt dieses Repositories zugreifen, ihn herunterladen oder verwenden.

Lösungsimplementierung

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

```
An Organization and AWS account has been setup in AWS public cloud
An user to run the deployment has been created
IAM roles has been configured
IAM roles granted to user to permit provisioning the resources
```

```
VPC and security configuration
A VPC has been created to host the resources to be provisioned
A security group has been configured for the VPC
A ssh key pair has been created for EC2 instance access
```

```
Network configuration
Subnets has been created for VPC with network segments assigned
Route tables and network ACL configured
NAT gateways or internet gateways configured for internet access
```

Toolkit herunterladen

```
git clone https://github.com/NetApp/na_aws_fsx_ec2_deploy.git
```

Konnektivität und Authentifizierung

Das Toolkit soll von einer AWS Cloud-Shell ausgeführt werden. AWS Cloud Shell ist eine browserbasierte Shell, die es Ihnen leicht macht, Ihre AWS-Ressourcen sicher zu managen, zu erkunden und mit ihnen zu interagieren. CloudShell ist mit Ihren Konsolenanmeldeinformationen vorauthentifiziert. Allgemeine Entwicklungs- und Betriebstools sind vorinstalliert, sodass keine lokale Installation oder Konfiguration erforderlich ist.

Konfiguration der Dateien Terraform Provider.tf und main.tf

Der Provider.tf definiert den Provider, von dem Terraform Ressourcen über API-Aufrufe bereitstellt. Die main.tf definiert die Ressourcen und Attribute der Ressourcen, die bereitgestellt werden sollen. Im Folgenden finden Sie einige Details:

```
provider.tf:
terraform {
  required_providers {
    aws = {
      source = "hashicorp/aws"
      version = "~> 4.54.0"
    }
  }
}
```

```
main.tf:
resource "aws_instance" "ora_01" {
  ami = var.ami
  instance_type = var.instance_type
  subnet_id = var.subnet_id
  key_name = var.ssh_key_name
  root_block_device {
    volume_type = "gp3"
    volume_size = var.root_volume_size
  }
  tags = {
    Name = var.ec2_tag
  }
}
....
```

Terraform Variables.tf und terraform.tfvars Konfiguration

Die Variablen.tf deklariert die Variablen, die in main.tf verwendet werden sollen. Die terraform.tfvars enthält die tatsächlichen Werte für die Variablen. Im Folgenden einige Beispiele:

```
variables.tf:  
  ### EC2 instance variables ###
```

```
variable "ami" {  
  type      = string  
  description = "EC2 AMI image to be deployed"  
}
```

```
variable "instance_type" {  
  type      = string  
  description = "EC2 instance type"  
}
```

```
terraform.tfvars:  
# EC2 instance variables
```

```
ami = "ami-06640050dc3f556bb" //RedHat 8.6 AMI  
instance_type = "t2.micro"  
ec2_tag = "ora_01"  
subnet_id = "subnet-04f5fe7073ff514fb"  
ssh_key_name = "sufi_new"  
root_volume_size = 30
```

Schritt-für-Schritt-Verfahren - nacheinander ausgeführt

1. Terraform in der AWS-Cloud-Shell installieren.

```
git clone https://github.com/tfutils/tfenv.git ~/.tfenv
```

```
mkdir ~/bin
```

```
ln -s ~/.tfenv/bin/* ~/bin/
```

```
tfenv install
```

```
tfenv use 1.3.9
```

2. Laden Sie das Toolkit von der öffentlichen NetApp GitHub Website herunter

```
git clone https://github.com/NetApp-  
Automation/na_aws_fsx_ec2_deploy.git
```

3. Führen Sie init aus, um Terraform zu initialisieren

```
terraform init
```

4. Testsuite ausgeben

```
terraform plan -out=main.plan
```

5. Anwenden der Testsuite

```
terraform apply "main.plan"
```

6. Führen Sie „Destroy“ aus, um die Ressourcen nach Abschluss zu entfernen

```
terraform destroy
```

Wo Sie weitere Informationen finden

Weitere Informationen zur Automatisierung von NetApp Lösungen finden Sie auf der folgenden Website "[Automatisierung der NetApp Lösung](#)"

DB-Sizing-Toolkits

Oracle Sizing Guidance für Azure NetApp Files

Allen Cao, Niyaz Mohamed, NetApp

Zweck

Für das Verschieben vorhandener Oracle-Workloads von einer Plattform zur anderen, z. B. von On-Premises in die Public Cloud, muss die Größe von Computing und Storage in der Zielplattform festgelegt werden, um Performance- und Service-Level-Anforderungen zu erfüllen. In dieser Dokumentation wird ein einfaches Toolkit zur Erreichung dieses Ziels beschrieben.

Im Gegensatz zu einer neuen Datenbankapplikation, die mit der Zeit wachsen kann, hat ein vorhandener Oracle Workload Workload Workload Workload Workload-Muster in den Computing- und Storage-Anforderungen festgelegt, die in einem Oracle Workload Repository oder AWR aufgezeichnet werden. Dieses Toolkit verwendet einen HTML-Parser, um relevante Informationen aus Oracle AWR abzurufen. Die Ergebnisse werden durch zusätzliche Informationen zur Größenbemessung ergänzt, die über SQL-Skripte gegen die Datenbank abgerufen werden. So erhalten Sie beim Umzug der Oracle Datenbank aussagekräftige Informationen zu Computing- und Storage-Ressourcen.

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Leitfaden zur Größenbemessung für das Computing von Oracle Database Servern beim Verschieben der Datenbank von On-Premises-Storage in die Microsoft Azure Cloud.
- Anleitung zur Dimensionierung von Oracle Datenbank-Server-Storage beim verlagern von Datenbanken aus der On-Premises-Umgebung auf Microsoft Azure NetApp Files.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle-Datenbanken im lokalen Private-Data-Center oder in der Microsoft Azure Cloud-Umgebung managt.
- Ein Storage-Administrator, der den lokalen Storage oder Microsoft Azure NetApp Files Storage zur Unterstützung von Oracle-Datenbanken managt.
- Ein Applikationsinhaber, der Oracle Database aus On-Premises-Storage in die Microsoft Azure Cloud migriert.

Lizenz

Durch den Zugriff auf, das Herunterladen, die Installation oder die Verwendung des Inhalts in diesem Toolkit-Repository stimmen Sie den Bedingungen der in dargelegten Lizenz zu "[Lizenzdatei](#)".



Es gibt bestimmte Einschränkungen bei der Erstellung und/oder Freigabe abgeleiteter Werke mit dem Inhalt in diesem Toolkit-Repository. Bitte lesen Sie die Lizenzbedingungen, bevor Sie den Inhalt verwenden. Wenn Sie nicht allen Bedingungen zustimmen, dürfen Sie nicht auf den Inhalt dieses Repositories zugreifen, ihn herunterladen oder verwenden.

Lösungsimplementierung

Voraussetzungen für die Bereitstellung

Die Bereitstellung erfordert die folgenden Voraussetzungen.

- Oracle AWR-Berichte, die Snapshots von Datenbankaktivitäten während der Spitzenauslastung von Applikations-Workloads erfassen.
- Zugriff auf die Oracle-Datenbank zum Ausführen von SQL-Skripten mit DBA-Berechtigung.

Toolkit herunterladen

Rufen Sie das Toolkit aus dem Repository ab "[Oracle Sizing Guidance für ANF](#)"

Wie wird das Toolkit verwendet?

Das Toolkit besteht aus einem webbasierten HTML-Parser und zwei SQL-Skripten zur Erfassung von Oracle-Datenbankinformationen. Die Ausgabe wird anschließend in eine Excel-Vorlage eingegeben, um eine Anleitung zur Größenbemessung von Computing und Storage für den Oracle Datenbankserver zu erstellen.

- Verwenden Sie ein "[HTML-Parser](#)" AWR-Modul zum Abrufen von Dimensionierungsinformationen einer aktuellen Oracle-Datenbank aus einem AWR-Bericht.
- Führen Sie ora_db_Data_size.sql als DBA aus, um physische Oracle-Datendateigröße aus der Datenbank abzurufen.
- Führen Sie ora_db_logs_size.sql als DBA aus, um archivierte Oracle-Protokollgrößen mit dem Aufbewahrungsfenster für gewünschte Archivprotokolle (Tage) abzurufen.
- Geben Sie die oben erhaltenen Informationen zur Größenbemessung in die Excel-Vorlagendatei oracle_db_sizing_template_anf.xlsx ein, um eine Anleitung zur Größenbemessung für Compute und Storage für Oracle DB Server zu erstellen.

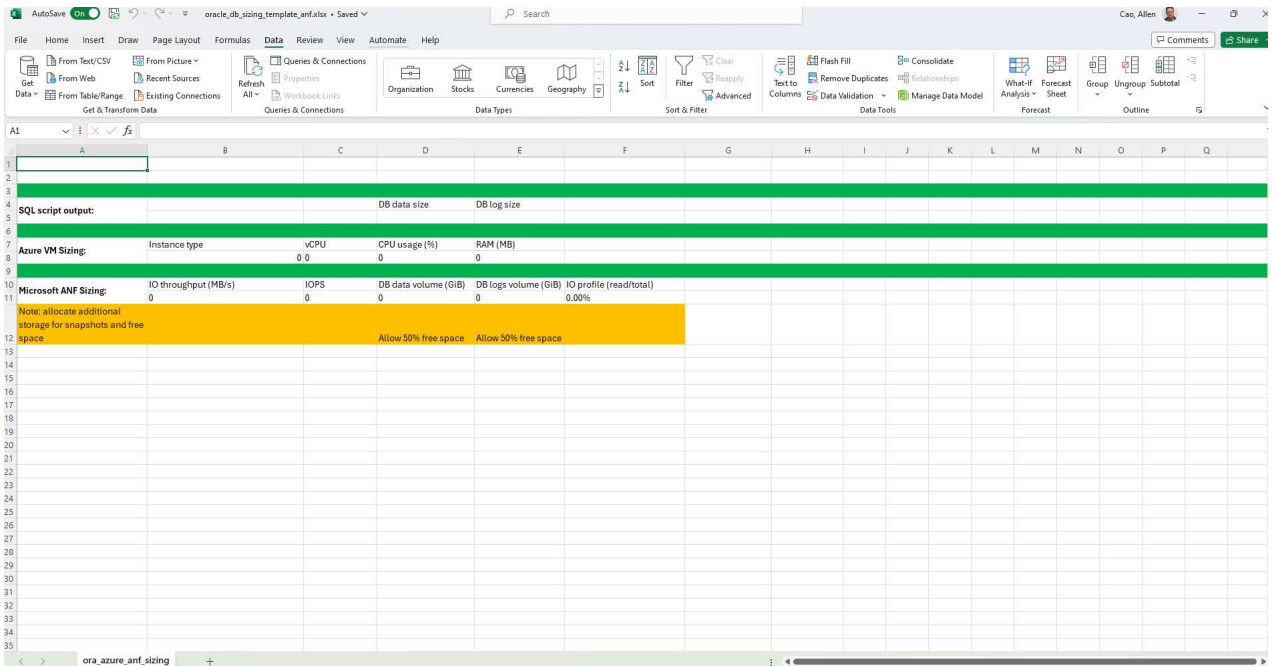
Toolkit-Nutzungsdemonstration

1. Öffnen Sie das HTML-Parser-AWR-Modul.

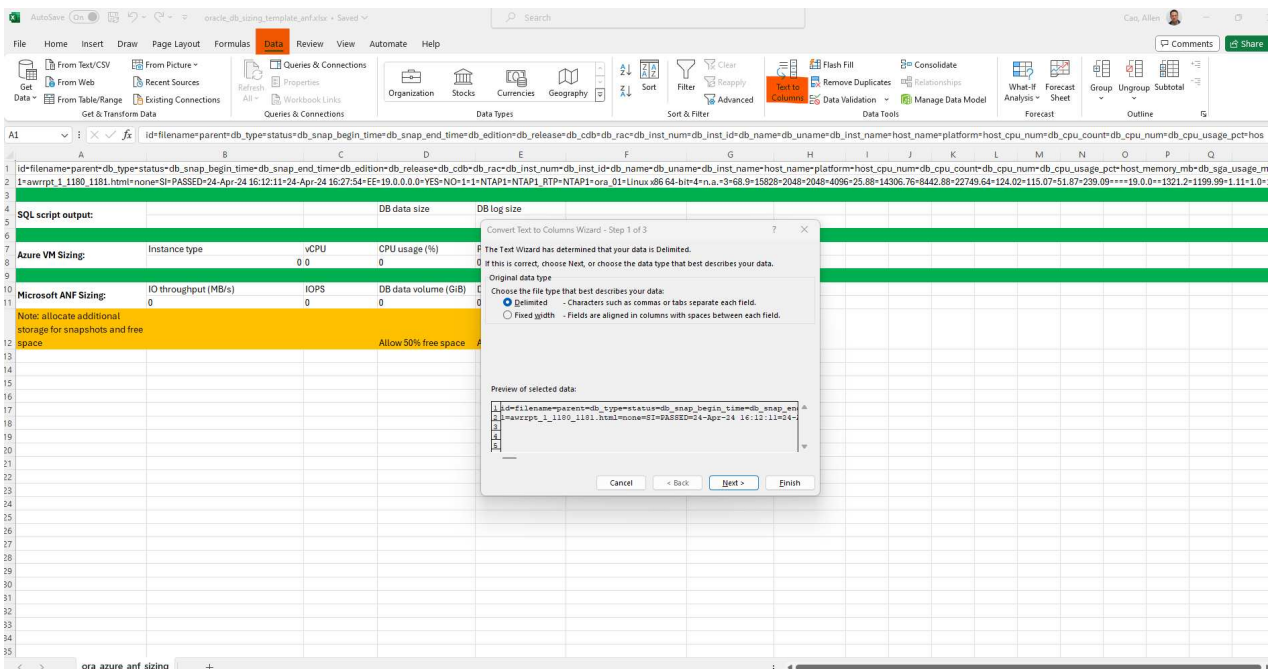
2. Prüfen Sie das Ausgabeformat als .csv, und klicken Sie auf Upload files Um den awr-Bericht hochzuladen. Der Parser gibt Ergebnisse in einer HTML-Seite mit einer Tabellenzusammenfassung sowie einer output.csv-Datei in zurück Download Ordner.

ID	Filename	Type	Status	DB name	InstID	Instance	Release	DB Size (gb)	CPUs	Used CPUs	Memor (mb)	Used Memor (mb)	Used IOPS	Used IO Throug (mbps)	Networ Bandwi (mbps)	Overfit DB IO Read (%)	AAS	Conso/Cluster	Conso/ClusterSKU
1	awrrpt_1_27_28.html	SI	PASSECDB1	1	cdb1	19.0.0.			8	7	31496	16384	54797	1643.48	13.19	5.35	97.12	77.07	Standard_D2_v5 (2 vCPU, 8 GiB)

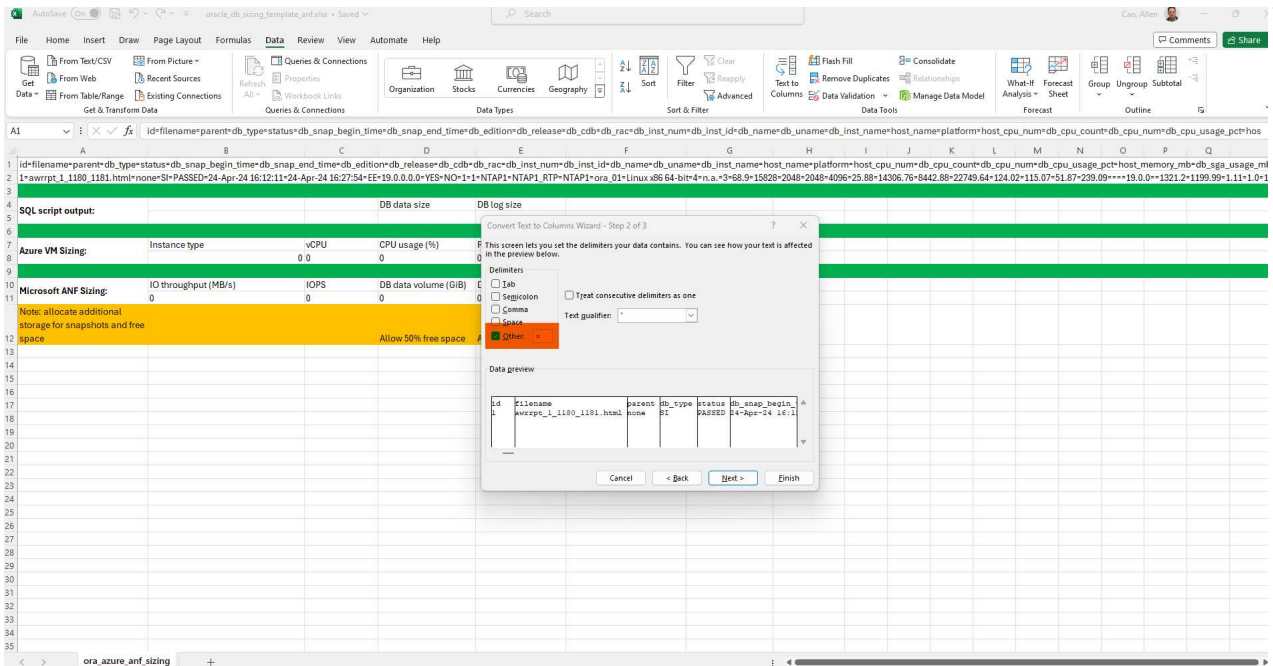
3. Öffnen Sie die Excel-Vorlagendatei, und kopieren Sie den csv-Inhalt in Spalte A und Zelle 1, um die Dimensionierungsinformationen des DB-Servers zu generieren.



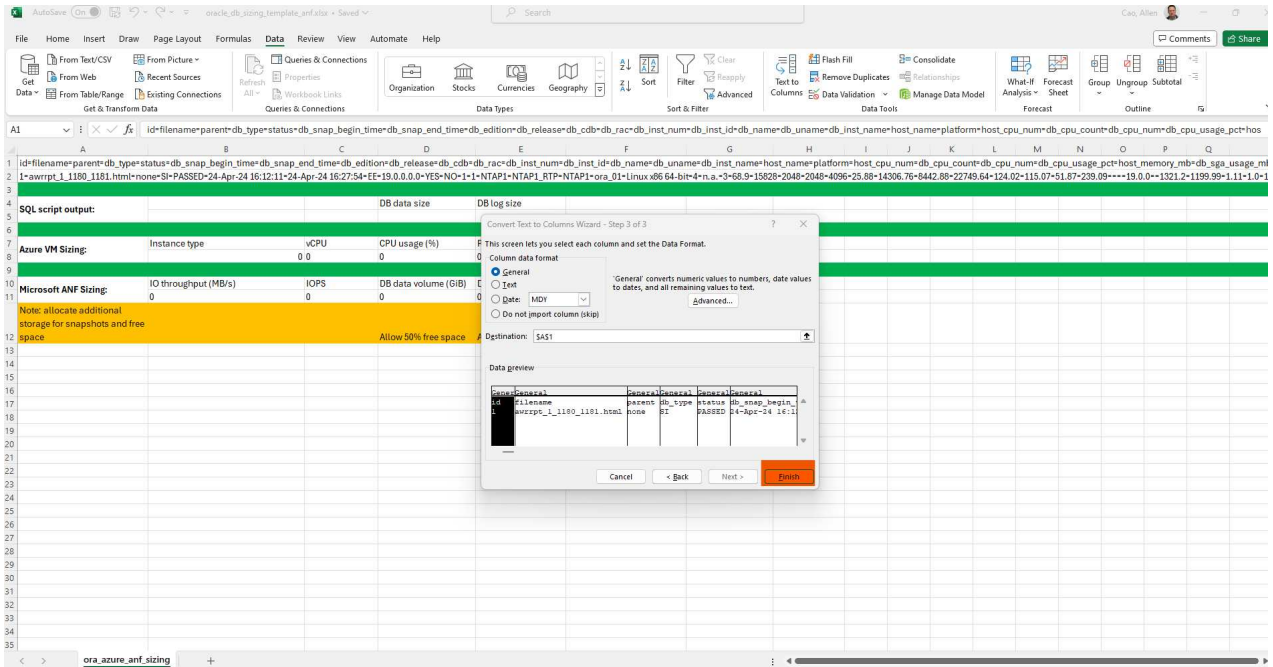
4. Markieren Sie Spalte A und Felder 1 und 2, und klicken Sie auf Data `Dann `Text to Columns Um den Text Wizzard zu öffnen. Wählen Delimited `Dann `Next Zum nächsten Bildschirm.



5. Prüfen Other `Geben Sie dann '=' als ein `Delimiters. Klicken Sie auf Next Zum nächsten Bildschirm.



6. Klicken Sie auf **Finish** Um die Konvertierung der Zeichenfolge in ein lesbares Spaltenformat abzuschließen. Hinweis: Die Felder für die VM- und ANF-Größenbestimmung wurden mit Daten gefüllt, die aus dem Oracle AWR-Bericht abgerufen wurden.



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q		
1	id	filename	parent	db_type	status	db_snap_begin_time	db_snap_end_time	db_edition	db_releas	db_cdb	db_rac	db_inst_ni	db_inst_ic	db_name	db_unam	db_inst_n	host_nam	platform
2		1 awrrpt_1_1180_1181.html	none	SI	PASSED	4/24/2024 16:12	4/24/2024 16:27	EE	19.0.0.0.0	YES	NO	1		NTAP1	NTAP1_RT	NTAP1	ora_01	Linux x86
4	SQL script output:			DB data size	DB log size													
7	Azure VM Sizing:																	
		Instance type	vCPU	CPU usage (%)	RAM (MB)													
		SI	4	68.9	15828													
10	Microsoft ANF Sizing:																	
		IO throughput (MB/s)	IOPS	DB data volume (GiB)	DB logs volume (GiB)	IO profile (read/total)												
		239.09	22749.64	0	0	62.89%												
12	Note: allocate additional storage for snapshots and free space			Allow 50% free space	Allow 50% free space													

7. Führen Sie das Skript ora_db_Data_size.sql, ora_db_logs_size.sql als DBA in sqlplus aus, um die Datengröße der Oracle-Datenbank und die Größe der archivierten Protokolle mit der Anzahl der Tage des Aufbewahrungsfensters abzurufen.

```

[oracle@ora_01 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Tue Mar 5 15:25:27 2024
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.18.0.0.0

SQL> @/home/oracle/ora_db_data_size.sql;

Aggregate DB File Size, GiB Aggregate DB File RW, GiB Aggregate DB
File RO, GiB
-----
-----
                                159.05                159.05
0

```

```

SQL> @/home/oracle/ora_db_logs_size.sql;
Enter value for archivelog_retention_days: 14
old 6:      where first_time >= sysdate -
&archivelog_retention_days
new 6:      where first_time >= sysdate - 14

Log Size, GiB
-----
          93.83

SQL>

```



Die mit den oben genannten Skripts abgerufenen Informationen zur Datenbankgröße ergibt sich aus der Summe der tatsächlichen Größe aller physischen Datenbankdatendateien oder Protokolldateien. Sie berücksichtigt nicht den freien Speicherplatz, der in jeder Datendatei verfügbar sein kann.

8. Geben Sie das Ergebnis in die Excel-Datei ein, um die Ausgabe der Anleitung zur Größenbestimmung abzuschließen.

id	filename	parent	db_type	status	db_snap_begin_time	db_snap_end_time	db_edition	db_release_cdb	db_rac	db_inst_ni	db_inst_lc	db_name	db_uname	db_inst_ni	host_name	platform	
1	awrrpt_1_1180_1181.html	none	SI	PASSED	4/24/2024 16:12	4/24/2024 16:27	EE	19.0.0.0.0	YES	NO	1	1	NTAP1	NTAP1_RT	NTAP1	ora_01	Linux x86
SQL script output:			DB data size	DB log size													
			159.05	93.83													
Azure VM Sizing:			Instance type	vCPU	CPU usage (%)	RAM (MB)											
			SI	4	66.9	15828											
Microsoft ANF Sizing:			IO throughput (MB/s)	IOPS	DB data volume (GiB)	DB logs volume (GiB)	IO profile (read/total)										
			239.09	22749.64	318.1	187.66	62.89%										
Note: allocate additional storage for snapshots and free space			Allow 50% free space		Allow 50% free space												

9. ANF verwendet ein drei-Tier-Service-Level (Standard, Premium, Ultra) für das Management der Durchsatzgrenze für Datenbank-Volumes. Siehe "[Service-Level für Azure NetApp Files](#)" Entsprechende Details. Wählen Sie basierend auf den Ergebnissen der Sizing-Anleitungen ein ANF-Service-Level aus, das den Durchsatz bietet, der die Anforderung für die Datenbank erfüllt.

Wo Sie weitere Informationen finden

Weitere Informationen zu NetApp Datenbanklösungen finden Sie auf der folgenden Website "[NetApp Lösungen für Enterprise Database](#)"

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, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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