



TR-5002: Kostensenkung für Oracle Active Data Guard mit Azure NetApp Files

NetApp database solutions

NetApp
August 18, 2025

Inhalt

TR-5002: Kostensenkung für Oracle Active Data Guard mit Azure NetApp Files	1
Zweck	1
Publikum	1
Test- und Validierungsumgebung für Lösungen	2
Architektur	2
Hardware- und Softwarekomponenten	2
Oracle Data Guard-Konfiguration mit hypothetischem DR-Setup von NY nach LA	3
Wichtige Faktoren für die Bereitstellungsüberlegungen	3
Lösungsbereitstellung	4
Voraussetzungen für die Bereitstellung	4
Vorbereiten der primären Datenbank für Data Guard	7
Standby-Datenbank vorbereiten und Data Guard aktivieren	16
Data Guard Broker einrichten	26
Klonen Sie die Standby-Datenbank für andere Anwendungsfälle	29
Wo Sie weitere Informationen finden	43

TR-5002: Kostensenkung für Oracle Active Data Guard mit Azure NetApp Files

Die Lösung bietet eine Übersicht und Details zur Konfiguration von Oracle Data Guard unter Verwendung von Microsoft Azure NetApp Files (ANF) als primären und Standby-Datenbankspeicher, um die Lizenz- und Betriebskosten der Oracle Data Guard HA/DR-Lösung in der Azure-Cloud zu senken.

Zweck

Oracle Data Guard gewährleistet hohe Verfügbarkeit, Datenschutz und Notfallwiederherstellung für Unternehmensdaten in einer primären Datenbank- und Standby-Datenbankreplikationskonfiguration. Oracle Active Data Guard ermöglicht Benutzern den Zugriff auf Standby-Datenbanken, während die Datenreplikation von der primären Datenbank zu den Standby-Datenbanken aktiv ist. Data Guard ist eine Funktion der Oracle Database Enterprise Edition. Es ist keine separate Lizenzierung erforderlich. Andererseits ist Active Data Guard eine Option der Oracle Database Enterprise Edition und erfordert daher eine separate Lizenzierung. Mehrere Standby-Datenbanken können im Active Data Guard-Setup Datenreplikationen von einer primären Datenbank empfangen. Allerdings erfordert jede zusätzliche Standby-Datenbank eine Active Data Guard-Lizenz und zusätzlichen Speicherplatz in der Größe der primären Datenbank. Die Betriebskosten summieren sich schnell.

Wenn Sie die Kosten für Ihren Oracle-Datenbankbetrieb senken möchten und planen, einen Active Data Guard in der Azure-Cloud einzurichten, sollten Sie eine Alternative in Betracht ziehen. Verwenden Sie anstelle von Active Data Guard Data Guard, um die Replikation von der primären Datenbank in eine einzelne physische Standbydatenbank im Azure NetApp Files -Speicher durchzuführen. Anschließend können mehrere Kopien dieser Standby-Datenbank geklont und für Lese-/Schreibzugriff geöffnet werden, um viele andere Anwendungsfälle wie Berichterstellung, Entwicklung, Test usw. zu erfüllen. Die Nettoergebnisse liefern effektiv die Funktionen von Active Data Guard, während die Active Data Guard-Lizenz entfällt. In dieser Dokumentation zeigen wir, wie Sie einen Oracle Data Guard mit Ihrer vorhandenen primären Datenbank und physischen Standby-Datenbank auf ANF-Speicher einrichten. Die Standby-Datenbank wird für den Lese-/Schreibzugriff für Anwendungsfälle nach Wunsch über das Datenbankverwaltungstool NetApp SnapCenter gesichert und geklont. Das NetApp Solutions Engineering-Team bietet außerdem ein Automatisierungs-Toolkit zum Aktualisieren von Klonen nach benutzerdefiniertem Zeitplan für ein vollständiges, automatisiertes Lebenszyklusmanagement von Datenbankklonen ohne Benutzereingriffe.

Diese Lösung ist für die folgenden Anwendungsfälle geeignet:

- Implementierung von Oracle Data Guard zwischen einer primären Datenbank und einer physischen Standbydatenbank im Microsoft Azure NetApp Files Speicher in allen Azure-Regionen.
- Sichern und klonen Sie die physische Standby-Datenbank, um Anwendungsfälle wie Berichterstellung, Entwicklung, Test usw. zu unterstützen.
- Lebenszyklusverwaltung für die Aktualisierung von Oracle-Datenbankklonen durch Automatisierung.

Publikum

Diese Lösung ist für folgende Personen gedacht:

- Ein DBA, der Oracle Active Data Guard in der Azure-Cloud für hohe Verfügbarkeit, Datenschutz und Notfallwiederherstellung einrichtet.

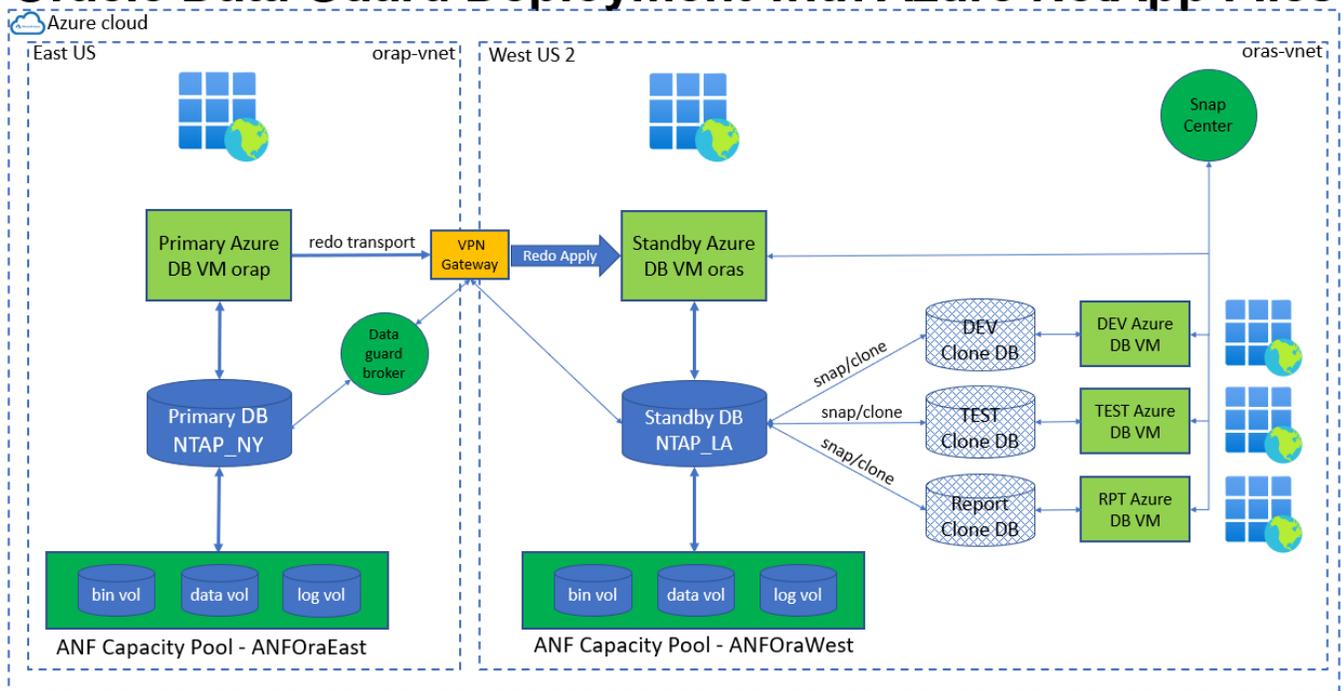
- Ein Datenbanklösungsarchitekt, der an der Konfiguration von Oracle Active Data Guard in der Azure-Cloud interessiert ist.
- Ein Speicheradministrator, der Azure NetApp Files Speicher verwaltet, der Oracle Data Guard unterstützt.
- Ein Anwendungsbesitzer, der Oracle Data Guard in einer Azure-Cloudumgebung einsetzen möchte.

Test- und Validierungsumgebung für Lösungen

Das Testen und Validieren dieser Lösung wurde in einer Azure-Cloud-Laborumgebung durchgeführt, die möglicherweise nicht der tatsächlichen Benutzerbereitstellungsumgebung entspricht. Weitere Informationen finden Sie im Abschnitt [Wichtige Faktoren für die Bereitstellungsüberlegungen](#).

Architektur

Oracle Data Guard Deployment with Azure NetApp Files



Hardware- und Softwarekomponenten

Hardware		
Azure NetApp Files	Aktuelle Version von Microsoft	Zwei 3-TiB-Kapazitätspools, Standard-Servicelevel, Auto-QoS
Azure-VMs für DB-Server	Standard B4ms (4 vcpus, 16 GiB Speicher)	Drei DB-VMs, eine als primärer DB-Server, eine als Standby-DB-Server und die dritte als Klon-DB-Server
Software		
RedHat Linux	Red Hat Enterprise Linux 8.6 (LVM) – x64 Gen2	RedHat-Abonnement zum Testen bereitgestellt

Oracle-Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet
Oracle OPatch	Version 12.2.0.1.36	Neuester Patch p6880880_190000_Linux-x86-64.zip
SnapCenter	Version 6.0.1	Bauen 6.0.1.4487
NFS	Version 3.0	dNFS für Oracle aktiviert

Oracle Data Guard-Konfiguration mit hypothetischem DR-Setup von NY nach LA

Datenbank	DB_EINDEUTIGER_NAME	Oracle Net-Dienstname
Primär	NTAP_NY	NTAP_NY.internal.cloudapp.net
Stehen zu	NTAP_LA	NTAP_LA.internal.cloudapp.net

Wichtige Faktoren für die Bereitstellungsüberlegungen

- **Standby-Datenbankklon.** Während Transaktionsprotokolle von der primären Datenbank empfangen und angewendet werden, kann die physische Standby-Datenbank geklont und auf einer DB-VM bereitgestellt werden, um andere Workloads wie DEV, TEST oder Report zu unterstützen. Der Klon kann ein dünner oder dicker Klon sein. Derzeit unterstützt ANF nur Thick Clone, also eine vollständige Kopie der Standby-Datenbank. Die ANF-Thin-Clone-Option wird in Kürze veröffentlicht. Für dünn geklonte Kopien von Datenbankvolumen werden dieselben DB-Volumen der Standby-Datenbank gemeinsam genutzt und die Copy-on-Write-Technologie zur Ausführung von Schreib-E/As verwendet. Daher sind die Klone sehr speichereffizient und können für viele andere Anwendungsfälle mit minimaler und inkrementeller neuer Speicherzuweisung für neue Schreib-E/As verwendet werden. Dies ermöglicht enorme Speichereinsparungen durch eine deutliche Reduzierung des Active Data Guard-Speicherbedarfs. NetApp empfiehlt, die FlexClone -Aktivitäten im Falle einer Datenbankumschaltung vom Primärspeicher auf den Standby-ANF-Speicher zu minimieren, um die Oracle-Leistung auf einem hohen Niveau zu halten.
- **Oracle-Softwareanforderungen.** Im Allgemeinen muss eine physische Standby-Datenbank dieselbe Datenbank-Home-Version wie die primäre Datenbank haben, einschließlich Patch Set Exceptions (PSEs), Critical Patch Updates (CPUs) und Patch Set Updates (PSUs), es sei denn, ein Oracle Data Guard Standby-First Patch Apply-Prozess ist im Gange (wie in My Oracle Support-Hinweis 1265700.1 unter "support.oracle.com").
- **Überlegungen zur Verzeichnisstruktur der Standby-Datenbank.** Wenn möglich, sollten die Datendateien, Protokolldateien und Steuerdateien auf dem Primär- und Standby-System dieselben Namen und Pfadnamen haben und die Namenskonventionen der Optimal Flexible Architecture (OFA) verwenden. Die Archivverzeichnisse in der Standby-Datenbank sollten zwischen den Sites ebenfalls identisch sein, einschließlich Größe und Struktur. Diese Strategie ermöglicht es, dass bei anderen Vorgängen wie Sicherungen, Umschaltungen und Failovers die gleichen Schritte ausgeführt werden, wodurch die Komplexität der Wartung reduziert wird.
- **Protokollierungsmodus erzwingen.** Um sich vor nicht protokollierten direkten Schreibvorgängen in der Primärdatenbank zu schützen, die nicht an die Standbydatenbank weitergegeben werden können, aktivieren Sie FORCE LOGGING in der Primärdatenbank, bevor Sie Datendateisicherungen für die Standby-Erstellung durchführen.
- **Größenbestimmung für Azure-VMs.** Bei diesen Tests und Validierungen haben wir eine Azure-VM – Standard_B4ms mit 4 vCPUs und 16 GiB Speicher verwendet. Sie müssen die Azure DB-VM

entsprechend der Anzahl der vCPUs und der RAM-Menge entsprechend den tatsächlichen Arbeitslastanforderungen dimensionieren.

- *** Azure NetApp Files -Konfiguration.*** Azure NetApp Files werden im Azure NetApp -Speicherkonto wie folgt zugewiesen: `Capacity Pools` . Bei diesen Tests und Validierungen haben wir einen 3-TiB-Kapazitätspool bereitgestellt, um Oracle primär in der Region Ost und eine Standby-Datenbank in der Region West 2 zu hosten. Der ANF-Kapazitätspool verfügt über drei Servicelevel: Standard, Premium und Ultra. Die E/A-Kapazität des ANF-Kapazitätspools basiert auf der Größe des Kapazitätspools und seinem Servicelevel. Für die Produktionsbereitstellung empfiehlt NetApp eine umfassende Bewertung Ihres Durchsatzbedarfs für Oracle-Datenbanken und die entsprechende Dimensionierung des Datenbankkapazitätspools. Bei der Erstellung eines Kapazitätspools können Sie QoS auf „Automatisch“ oder „Manuell“ und die Datenverschlüsselung im Ruhezustand auf „Einfach“ oder „Doppelt“ einstellen.
- **dNFS-Konfiguration.** Durch die Verwendung von dNFS kann eine Oracle-Datenbank, die auf einer Azure Virtual Machine mit ANF-Speicher ausgeführt wird, deutlich mehr E/A-Vorgänge ausführen als der native NFS-Client. Die automatisierte Oracle-Bereitstellung mit dem NetApp Automatisierungs-Toolkit konfiguriert dNFS automatisch auf NFSv3.

Lösungsbereitstellung

Es wird davon ausgegangen, dass Sie Ihre primäre Oracle-Datenbank bereits in einer Azure-Cloudumgebung innerhalb eines VNet als Ausgangspunkt für die Einrichtung von Oracle Data Guard bereitgestellt haben. Idealerweise wird die primäre Datenbank auf einem ANF-Speicher mit NFS-Mount bereitgestellt. Für den Oracle-Datenbankspeicher werden drei NFS-Mount-Punkte erstellt: Mount /u01 für die Oracle-Binärdateien, Mount /u02 für die Oracle-Datendateien und eine Steuerdatei, Mount /u03 für die aktuellen und archivierten Oracle-Protokolldateien und eine redundante Steuerdatei.

Ihre primäre Oracle-Datenbank kann auch auf einem NetApp ONTAP -Speicher oder einem anderen Speicher Ihrer Wahl entweder innerhalb des Azure-Ökosystems oder eines privaten Rechenzentrums ausgeführt werden. Der folgende Abschnitt enthält schrittweise Bereitstellungsverfahren zum Einrichten eines Oracle Data Guard zwischen einer primären Oracle-Datenbank in Azure mit ANF-Speicher und einer physischen Standby-Oracle-Datenbank in Azure mit ANF-Speicher.

Voraussetzungen für die Bereitstellung

Für die Bereitstellung sind die folgenden Voraussetzungen erforderlich.

1. Ein Azure-Cloud-Konto wurde eingerichtet und die erforderlichen VNet- und Netzwerksubnetze wurden innerhalb Ihres Azure-Kontos erstellt.
2. Über die Azure-Cloudportalkonsole müssen Sie mindestens drei Azure Linux-VMs bereitstellen: eine als primären Oracle-DB-Server, eine als Standby-Oracle-DB-Server und einen Klon-Ziel-DB-Server für Berichterstellung, Entwicklung, Tests usw. Weitere Einzelheiten zur Einrichtung der Umgebung finden Sie im Architekturdiagramm im vorherigen Abschnitt. Lesen Sie auch die Microsoft "[Virtuelle Azure-Computer](#)" für weitere Informationen.
3. Die primäre Oracle-Datenbank sollte auf dem primären Oracle-DB-Server installiert und konfiguriert worden sein. Auf dem Standby-Oracle-DB-Server oder dem geklonten Oracle-DB-Server hingegen wird nur Oracle-Software installiert und es werden keine Oracle-Datenbanken erstellt. Idealerweise sollte das Layout der Oracle-Datenbanken auf allen Oracle-DB-Servern genau übereinstimmen. Weitere Informationen zu den NetApp -Empfehlungen für die automatisierte Oracle-Bereitstellung in der Azure-Cloud und ANF finden Sie in den folgenden technischen Berichten.
 - "[TR-4987: Vereinfachte, automatisierte Oracle-Bereitstellung auf Azure NetApp Files mit NFS](#)"



Stellen Sie sicher, dass Sie im Stammvolumen der Azure-VMs mindestens 128 GB zugewiesen haben, um ausreichend Speicherplatz für die Bereitstellung der Oracle-Installationsdateien zu haben.

4. Stellen Sie über die Azure-Cloudportalkonsole zwei ANF-Speicherkapazitätspools bereit, um Oracle-Datenbankvolumen zu hosten. Die ANF-Speicherkapazitätspools sollten in verschiedenen Regionen liegen, um eine echte DataGuard-Konfiguration zu simulieren. Wenn Sie mit der Bereitstellung von ANF-Speicher nicht vertraut sind, lesen Sie die Dokumentation "[Schnellstart: Einrichten von Azure NetApp Files und Erstellen eines NFS-Volumes](#)" für schrittweise Anleitungen.

Name	Type	Resource group	Location	Subscription
ANFOraEast	NetApp account	ANFAVSRG	East US	Hybrid Cloud TME Onprem
ANFOraWest	NetApp account	ANFAVSRG	West US 2	Hybrid Cloud TME Onprem

5. Wenn sich die primäre Oracle-Datenbank und die Standby-Oracle-Datenbank in zwei verschiedenen Regionen befinden, sollte ein VPN-Gateway konfiguriert werden, um den Datenverkehr zwischen zwei separaten VNets zu ermöglichen. Eine detaillierte Netzwerkkonfiguration in Azure geht über den Rahmen dieses Dokuments hinaus. Die folgenden Screenshots bieten einige Hinweise dazu, wie die VPN-Gateways konfiguriert und verbunden werden und wie der Datenverkehrsfluss im Labor bestätigt wird.

VPN-Gateways im Labor:

Microsoft Azure

Virtual network gateways

Showing 1 to 3 of 3 records.

Name	Virtual network	Gateway type	Resource group	Location	Subscription
orap-vnet-gw	orap-vnet	Vpn	ANFAVSRG	East US	Hybrid Cloud TME Onprem
oras-vnet-gw	oras-vnet	Vpn	ANFAVSRG	West US 2	Hybrid Cloud TME Onprem
vNetgw	EHCvNet	Vpn	NSOL	Central US	Hybrid Cloud TME Onprem

Das primäre VNET-Gateway:

Microsoft Azure

Virtual network gateway: orap-vnet-gw

Essentials

- Resource group: ANFAVSRG
- Location: East US
- Subscription: Hybrid Cloud TME Onprem
- Subscription ID: Defa2dfb-917c-4497-b56a-b3f4eadb8111
- Tags: database: oracle, product_line: Field use - various

Health check: Perform a quick health check to detect possible gateway issues. [Go to Resource health](#)

Advisor Recommendations: Check Critical, Warning, and Informational Recommendations. [Go to Advisor](#)

Advanced troubleshooting: Run a troubleshooting tool to investigate failure causes and perform repair actions. [Go to VPN Troubleshooting](#)

Documentation: View guidance on helpful topics related to VPN gateway. [View documentation](#)

Total tunnel ingress and egress graphs showing data for the last 1 hour.

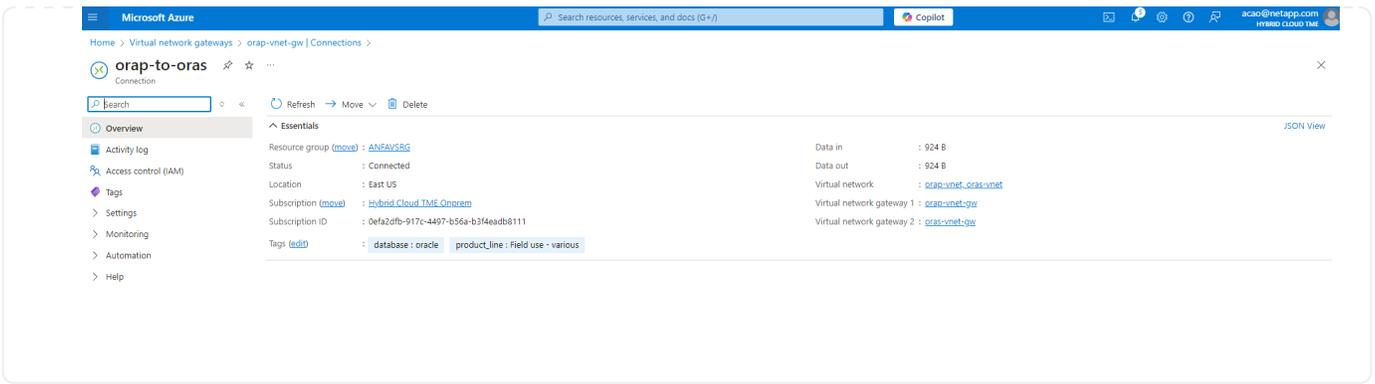
Verbindungsstatus des VNET-Gateways:

Microsoft Azure

Virtual network gateway: orap-vnet-gw | Connections

Name	Status	Connection type	Peer
orap-to-oras	Connected	VNet-to-VNet	oras-vnet-gw
oras-to-orap	Connected	VNet-to-VNet	oras-vnet-gw

Überprüfen Sie, ob die Verkehrsflüsse eingerichtet sind (klicken Sie auf die drei Punkte, um die Seite zu öffnen):



Vorbereiten der primären Datenbank für Data Guard

In dieser Demonstration haben wir eine primäre Oracle-Datenbank namens NTAP auf dem primären Azure DB-Server mit drei NFS-Mount-Punkten eingerichtet: /u01 für die Oracle-Binärdatei, /u02 für die Oracle-Datendateien und eine Oracle-Steuerdatei, /u03 für die aktiven Oracle-Protokolle, archivierten Protokolldateien und eine redundante Oracle-Steuerdatei. Im Folgenden werden die detaillierten Verfahren zum Einrichten der primären Datenbank für den Oracle Data Guard-Schutz veranschaulicht. Alle Schritte sollten als Oracle-Datenbankbesitzer oder als Standard ausgeführt werden `oracle` Benutzer.

1. Die primäre Datenbank NTAP auf dem primären Azure DB-Server `orap.internal.cloudapp.net` wird zunächst als eigenständige Datenbank mit dem ANF als Datenbankspeicher bereitgestellt.

```
orap.internal.cloudapp.net:
resource group: ANFAVSRG
Location: East US
size: Standard B4ms (4 vcpus, 16 GiB memory)
OS: Linux (redhat 8.6)
pub_ip: 172.190.207.231
pri_ip: 10.0.0.4

[oracle@orap ~]$ df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  7.7G      4.0K   7.7G   1% /dev
tmpfs                     7.8G         0   7.8G   0% /dev/shm
tmpfs                     7.8G    209M   7.5G   3% /run
tmpfs                     7.8G         0   7.8G   0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv 22G      413M   22G    2% /
/dev/mapper/rootvg-usrlv  10G      2.1G   8.0G   21% /usr
/dev/sda1                 496M    181M   315M   37% /boot
/dev/mapper/rootvg-homelv 2.0G      47M   2.0G    3% /home
/dev/sda15                495M     5.8M   489M    2% /boot/efi
/dev/mapper/rootvg-varlv  8.0G     1.1G   7.0G   13% /var
/dev/mapper/rootvg-tmplv  12G     120M   12G    1% /tmp
/dev/sdb1                 32G      49M   30G    1% /mnt
10.0.2.36:/orap-u02       500G     7.7G  493G    2% /u02
10.0.2.36:/orap-u03       450G     6.1G  444G    2% /u03
10.0.2.36:/orap-u01       100G     9.9G   91G   10% /u01

[oracle@orap ~]$ 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.
#
#
NTAP:/u01/app/oracle/product/19.0.0/NTAP:N

```

2. Melden Sie sich als Oracle-Benutzer beim primären DB-Server an. Melden Sie sich über SQLPlus bei der Datenbank an und aktivieren Sie die erzwungene Protokollierung auf dem primären Server.

```
alter database force logging;
```

```

[oracle@orap admin]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Tue Nov 26 20:12:02
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> alter database force logging;

Database altered.

```

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

```
alter database flashback on;
```

```
SQL> alter database flashback on;
```

```
Database altered.
```

4. Konfigurieren Sie die Redo-Transportauthentifizierung mithilfe der Oracle-Kennwortdatei. Erstellen Sie mithilfe des Dienstprogramms orapwd eine Kennwortdatei auf dem Primärserver, falls diese nicht festgelegt ist, und kopieren Sie sie in das Verzeichnis \$ORACLE_HOME/dbs der Standby-Datenbank.
5. Erstellen Sie Standby-Redo-Protokolle auf der primären Datenbank mit derselben Größe wie die aktuelle Online-Protokolldatei. Protokollgruppen sind eine mehr als Online-Protokolldateigruppen. Die primäre Datenbank kann dann bei einem Failover schnell in die Standby-Rolle wechseln und beginnt, Redo-Daten zu empfangen. Wiederholen Sie den folgenden Befehl viermal, um vier Standby-Protokolldateien zu erstellen.

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

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

```
Database altered.
```

```
SQL> /
```

```
Database altered.
```

```
SQL> /
```

```
Database altered.
```

```
SQL> /
```

```
Database altered.
```

```
SQL> set lin 200
```

```
SQL> col member for a80
```

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

GROUP#	TYPE	MEMBER
3	ONLINE	/u03/orareco/NTAP/onlinelog/redo03.log
2	ONLINE	/u03/orareco/NTAP/onlinelog/redo02.log
1	ONLINE	/u03/orareco/NTAP/onlinelog/redo01.log
4	STANDBY	/u03/orareco/NTAP/onlinelog/o1_mf_4__2m115vkv_.log
5	STANDBY	/u03/orareco/NTAP/onlinelog/o1_mf_5__2m3c5cyd_.log
6	STANDBY	/u03/orareco/NTAP/onlinelog/o1_mf_6__2m4d7dhh_.log
7	STANDBY	/u03/orareco/NTAP/onlinelog/o1_mf_7__2m5ct7g1_.log

6. Erstellen Sie aus SQLPlus eine P-Datei aus der SP-Datei zur Bearbeitung.

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

7. Überarbeiten Sie die P-Datei und fügen Sie die folgenden Parameter hinzu.

```
vi /home/oracle/initNTAP.ora
```

Update the following parameters if not set:

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

8. Erstellen Sie von sqlplus aus die SP-Datei aus der überarbeiteten P-Datei neu, um die vorhandene SP-Datei im Verzeichnis \$ORACLE_HOME/dbs zu überschreiben.

```
create spfile='$ORACLE_HOME/dbs/spfileNTAP.ora' from
pfile='/home/oracle/initNTAP.ora';
```

9. Ändern Sie Oracle tnsnames.ora im Verzeichnis \$ORACLE_HOME/network/admin, um db_unique_name für die Namensauflösung hinzuzufügen.

```
vi $ORACLE_HOME/network/admin/tnsnames.ora
```

```

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

NTAP_NY =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST =
orap.internal.cloudapp.net) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = NTAP)
    )
  )

NTAP_LA =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST =
oras.internal.cloudapp.net) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = NTAP)
    )
  )

LISTENER_NTAP =
  (ADDRESS = (PROTOCOL = TCP) (HOST =
orap.internal.cloudapp.net) (PORT = 1521))

```



Wenn Sie Ihrem Azure DB-Server einen anderen Namen als den Standardnamen geben möchten, fügen Sie die Namen zur Hostnamenauflösung der lokalen Hostdatei hinzu.

10. Fügen Sie der Datei listener.ora den Data Guard-Dienstnamen NTAP_NY_DGMGRL.internal.cloudapp.net für die primäre Datenbank hinzu.

```
vi $ORACLE_HOME/network/admin/listener.ora
```

```

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

LISTENER.NTAP =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST =
orap.internal.cloudapp.net) (PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
    )
  )

SID_LIST_LISTENER.NTAP =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = NTAP_NY_DGMGRL.internal.cloudapp.net)
      (ORACLE_HOME = /u01/app/oracle/product/19.0.0/NTAP)
      (SID_NAME = NTAP)
    )
  )
)

```

11. Fahren Sie die Datenbank über SQLPlus herunter und starten Sie sie neu. Überprüfen Sie, ob die Data Guard-Parameter jetzt aktiv sind.

```
shutdown immediate;
```

```
startup;
```

```
SQL> show parameter name
```

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

cdb_cluster_name	string	
cell_offloadgroup_name	string	
db_file_name_convert	string	
db_name	string	NTAP
db_unique_name	string	NTAP_NY
global_names	boolean	FALSE
instance_name	string	NTAP
lock_name_space	string	

```

log_file_name_convert      string
pdb_file_name_convert      string
processor_group_name       string

```

```

NAME                        TYPE                        VALUE
-----

```

```

service_names              string
NTAP_NY.internal.cloudapp.net

```

```
SQL> sho parameter log_archive_dest
```

```

NAME                        TYPE                        VALUE
-----

```

```

log_archive_dest           string
log_archive_dest_1         string

```

```
LOCATION=USE_DB_RECOVERY_FILE_
```

```
DEST
```

```
VALID_FOR=(ALL_LOGFILES,A
```

```
LL_ROLES)
```

```
DB_UNIQUE_NAME=NTAP_
```

```
NY
```

```

log_archive_dest_10        string
log_archive_dest_11        string
log_archive_dest_12        string
log_archive_dest_13        string
log_archive_dest_14        string
log_archive_dest_15        string

```

```

NAME                        TYPE                        VALUE
-----

```

```

log_archive_dest_16        string
log_archive_dest_17        string
log_archive_dest_18        string
log_archive_dest_19        string

```

```

log_archive_dest_2         string
ASYNC VALID_FO

```

```
SERVICE=NTAP_LA
```

```
R=(ONLINE_LOGFILES,PRIMARY_ROL
```

```
E)
```

```
DB_UNIQUE_NAME=NTAP_LA
```

```

log_archive_dest_20        string
log_archive_dest_21        string

```

```
.
```

```
.
```

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

Standby-Datenbank vorbereiten und Data Guard aktivieren

Oracle Data Guard erfordert eine Betriebssystemkernelkonfiguration und Oracle-Software-Stacks einschließlich Patch-Sets auf dem Standby-DB-Server, um eine Übereinstimmung mit dem primären DB-Server zu gewährleisten. Zur Vereinfachung der Verwaltung und Vereinfachung sollte die Datenbankspeicherkonfiguration des Standby-DB-Servers idealerweise auch mit der des primären DB-Servers übereinstimmen, beispielsweise das Datenbankverzeichnislayout und die Größen der NFS-Mount-Punkte. Im Folgenden finden Sie detaillierte Verfahren zum Einrichten des Standby-Oracle-DB-Servers und zum Aktivieren von Oracle DataGuard für HA/DR-Schutz. Alle Befehle sollten mit der Standard-Benutzer-ID des Oracle-Besitzer ausgeführt werden. `oracle`.

1. Überprüfen Sie zunächst die Konfiguration der primären Datenbank auf dem primären Oracle DB-Server. In dieser Demonstration haben wir eine primäre Oracle-Datenbank namens NTAP auf dem primären DB-Server mit drei NFS-Mounts auf ANF-Speicher eingerichtet.
2. Wenn Sie der NetApp -Dokumentation TR-4987 folgen, um den Oracle-Standby-DB-Server einzurichten "[TR-4987: Vereinfachte, automatisierte Oracle-Bereitstellung auf Azure NetApp Files mit NFS](#)", verwenden Sie ein Tag `-t software_only_install` in Schritt 2 von `Playbook execution` um eine automatisierte Oracle-Installation auszuführen. Die überarbeitete Befehlssyntax ist unten aufgeführt. Das Tag ermöglicht die Installation und Konfiguration des Oracle-Software-Stacks, reicht jedoch nicht aus, um eine Datenbank zu erstellen.

```
ansible-playbook -i hosts 4-oracle_config.yml -u azureuser -e
@vars/vars.yml -t software_only_install
```

3. Die Standby-Oracle-DB-Serverkonfiguration am Standby-Standort im Demolabor.

```
oras.internal.cloudapp.net:
resource group: ANFAVSRG
Location: West US 2
size: Standard B4ms (4 vcpus, 16 GiB memory)
OS: Linux (redhat 8.6)
pub_ip: 172.179.119.75
pri_ip: 10.0.1.4
```

```
[oracle@oras ~]$ 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    265M  7.5G   4% /run
tmpfs                      7.8G         0  7.8G   0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv  22G    413M   22G   2% /
/dev/mapper/rootvg-usrlv   10G    2.1G   8.0G  21% /usr
/dev/sda1                  496M    181M  315M  37% /boot
/dev/mapper/rootvg-varlv   8.0G    985M   7.1G  13% /var
/dev/mapper/rootvg-homelv  2.0G     52M   2.0G   3% /home
/dev/mapper/rootvg-tmplv   12G    120M   12G   1% /tmp
/dev/sda15                 495M    5.8M  489M   2% /boot/efi
/dev/sdb1                  32G     49M   30G   1% /mnt
10.0.3.36:/oras-u01        100G    9.5G   91G  10% /u01
10.0.3.36:/oras-u02        500G    8.1G  492G   2% /u02
10.0.3.36:/oras-u03        450G    4.8G  446G   2% /u03
```

4. Sobald die Oracle-Software installiert und konfiguriert ist, legen Sie Oracle Home und Pfad fest. Kopieren Sie außerdem aus dem Standby-DB-Verzeichnis \$ORACLE_HOME das Oracle-Passwort aus der primären Datenbank, falls Sie dies noch nicht getan haben.

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

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

```
scp oracle@10.0.0.4:$ORACLE_HOME/dbs/orapwNTAP .
```

5. Aktualisieren Sie die Datei tnsnames.ora mit den folgenden Einträgen.

```
vi $ORACLE_HOME/network/admin/tnsnames.ora
```

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

NTAP_NY =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST =
orap.internal.cloudapp.net) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = NTAP)
    )
  )

NTAP_LA =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP) (HOST =
oras.internal.cloudapp.net) (PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SID = NTAP)
    )
  )
```

6. Fügen Sie der Datei listener.ora den Namen des DB-Data-Guard-Dienstes hinzu.

```
vi $ORACLE_HOME/network/admin/listener.ora
```

```

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

LISTENER.NTAP =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP) (HOST =
oras.internal.cloudapp.net) (PORT = 1521))
      (ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
    )
  )

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (SID_NAME = NTAP)
    )
  )

SID_LIST_LISTENER.NTAP =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = NTAP_LA_DGMGRL.internal.cloudapp.net)
      (ORACLE_HOME = /u01/app/oracle/product/19.0.0/NTAP)
      (SID_NAME = NTAP)
    )
  )

LISTENER =
  (ADDRESS_LIST =
    (ADDRESS = (PROTOCOL = TCP) (HOST =
oras.internal.cloudapp.net) (PORT = 1521))
  )

```

7. Starten Sie dbca, um die Standby-Datenbank aus der primären Datenbank NTAP zu instanzieren.

```

dbca -silent -createDuplicateDB -gdbName NTAP
-primaryDBConnectionString
oras.internal.cloudapp.net:1521/NTAP_NY.internal.cloudapp.net -sid
NTAP -initParams fal_server=NTAP_NY -createAsStandby -dbUniqueName
NTAP_LA

```

```

[oracle@oras admin]$ dbca -silent -createDuplicateDB -gdbName NTAP
-primaryDBConnectionString
orap.internal.cloudapp.net:1521/NTAP_NY.internal.cloudapp.net -sid
NTAP -initParams fal_server=NTAP_NY -createAsStandby -dbUniqueName
NTAP_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/NTAP_LA/NTAP_LA.log" for further
details.

```

8. Validieren Sie die duplizierte Standby-Datenbank. Neu duplizierte Standby-Datenbank wird zunächst im NUR-LESEN-Modus geöffnet.

```

[oracle@oras 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 $ORACLE_SID are not allowed.
#
#
NTAP:/u01/app/oracle/product/19.0.0/NTAP:N
[oracle@oras admin]$ export ORACLE_SID=NTAP
[oracle@oras admin]$ sqlplus / as sysdba

```

```

SQL*Plus: Release 19.0.0.0.0 - Production on Tue Nov 26 23:04:07
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 from v$database;

```

NAME	OPEN_MODE
NTAP	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	NTAP
db_unique_name	string	NTAP_LA
global_names	boolean	FALSE
instance_name	string	NTAP
lock_name_space	string	
log_file_name_convert	string	
pdb_file_name_convert	string	
processor_group_name	string	

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

```
-----  
-----  
service_names                                string  
NTAP_LA.internal.cloudapp.net  
SQL> show parameter log_archive_config
```

```
NAME                                          TYPE      VALUE  
-----  
-----  
log_archive_config                          string  
DG_CONFIG=(NTAP_NY,NTAP_LA)  
SQL> show parameter fal_server
```

```
NAME                                          TYPE      VALUE  
-----  
-----  
fal_server                                  string    NTAP_NY  
SQL> select name from v$datafile;
```

```
NAME  
-----
```

```
-----  
/u02/oradata/NTAP/system01.dbf  
/u02/oradata/NTAP/sysaux01.dbf  
/u02/oradata/NTAP/undotbs01.dbf  
/u02/oradata/NTAP/pdbseed/system01.dbf  
/u02/oradata/NTAP/pdbseed/sysaux01.dbf  
/u02/oradata/NTAP/users01.dbf  
/u02/oradata/NTAP/pdbseed/undotbs01.dbf  
/u02/oradata/NTAP/NTAP_pdb1/system01.dbf  
/u02/oradata/NTAP/NTAP_pdb1/sysaux01.dbf  
/u02/oradata/NTAP/NTAP_pdb1/undotbs01.dbf  
/u02/oradata/NTAP/NTAP_pdb1/users01.dbf
```

```
NAME  
-----
```

```
-----  
/u02/oradata/NTAP/NTAP_pdb2/system01.dbf  
/u02/oradata/NTAP/NTAP_pdb2/sysaux01.dbf  
/u02/oradata/NTAP/NTAP_pdb2/undotbs01.dbf  
/u02/oradata/NTAP/NTAP_pdb2/users01.dbf  
/u02/oradata/NTAP/NTAP_pdb3/system01.dbf  
/u02/oradata/NTAP/NTAP_pdb3/sysaux01.dbf  
/u02/oradata/NTAP/NTAP_pdb3/undotbs01.dbf  
/u02/oradata/NTAP/NTAP_pdb3/users01.dbf
```

```
19 rows selected.
```

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

```
NAME
```

```
-----  
-----  
/u02/oradata/NTAP/control01.ctl  
/u03/orareco/NTAP_LA/control02.ctl
```

```
SQL> col member form a80
```

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

```
GROUP# TYPE MEMBER  
-----  
-----  
1 ONLINE  
/u03/orareco/NTAP_LA/onlinelog/o1_mf_1_mndl6mxh_.log  
2 ONLINE  
/u03/orareco/NTAP_LA/onlinelog/o1_mf_2_mndl7jdb_.log  
3 ONLINE  
/u03/orareco/NTAP_LA/onlinelog/o1_mf_3_mndl8f03_.log  
4 STANDBY  
/u03/orareco/NTAP_LA/onlinelog/o1_mf_4_mndl99m7_.log  
5 STANDBY  
/u03/orareco/NTAP_LA/onlinelog/o1_mf_5_mndlb67d_.log  
6 STANDBY  
/u03/orareco/NTAP_LA/onlinelog/o1_mf_6_mndlc2tw_.log  
7 STANDBY  
/u03/orareco/NTAP_LA/onlinelog/o1_mf_7_mndlczhh_.log
```

```
7 rows selected.
```

9. Starten Sie die Standby-Datenbank neu in mount Führen Sie die Phase aus und führen Sie den folgenden Befehl aus, um die verwaltete Wiederherstellung der Standby-Datenbank 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 6442449688 bytes
Fixed Size                  9177880 bytes
Variable Size              1090519040 bytes
Database Buffers          5335154688 bytes
Redo Buffers               7598080 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.

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

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

ROLE	THREAD#	SEQUENCE#	ACTION
post role transition	0	0	IDLE
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	18	APPLYING_LOG
managed recovery	0	0	IDLE
RFS async	1	18	IDLE
RFS ping	1	18	IDLE
archive redo	0	0	IDLE
redo transport timer	0	0	IDLE

ROLE	THREAD#	SEQUENCE#	ACTION
gap manager	0	0	IDLE
archive redo	0	0	IDLE
archive redo	0	0	IDLE
redo transport monitor	0	0	IDLE
log writer	0	0	IDLE
archive local	0	0	IDLE

```
17 rows selected.
```

```
SQL>
```

Damit ist die Einrichtung des Data Guard-Schutzes für NTAP vom Primär- zum Standby-System mit aktivierter verwalteter Standby-Wiederherstellung abgeschlossen.

Data Guard Broker einrichten

Oracle Data Guard Broker ist ein verteiltes Verwaltungsframework, das die Erstellung, Wartung und Überwachung von Oracle Data Guard-Konfigurationen automatisiert und zentralisiert. Der folgende Abschnitt zeigt, wie Sie Data Guard Broker einrichten, um die Data Guard-Umgebung zu verwalten.

1. Starten Sie den Data Guard Broker sowohl auf der primären als auch auf der Standby-Datenbank mit dem folgenden Befehl über SQLPlus.

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

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

```
[oracle@orap ~]$ dgmgrl sys@NTAP_NY
DGMGRL for Linux: Release 19.0.0.0.0 - Production on Wed Dec 11
20:53:20 2024
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 "NTAP_NY"
Connected as SYSDBA.
DGMGRL>
```

3. Erstellen und aktivieren Sie die Data Guard Broker-Konfiguration.

```
DGMGRL> create configuration dg_config as primary database is
NTAP_NY connect identifier is NTAP_NY;
Configuration "dg_config" created with primary database "ntap_ny"
DGMGRL> add database NTAP_LA as connect identifier is NTAP_LA;
Database "ntap_la" added
DGMGRL> enable configuration;
Enabled.
DGMGRL> show configuration;

Configuration - dg_config

Protection Mode: MaxPerformance
Members:
  ntap_ny - Primary database
  ntap_la - Physical standby database

Fast-Start Failover: Disabled

Configuration Status:
SUCCESS (status updated 3 seconds ago)
```

4. Validieren Sie den Datenbankstatus im Data Guard Broker-Verwaltungsframework.

```
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 Fehlers kann Data Guard Broker verwendet werden, um ein sofortiges Failover der primären Datenbank auf die Standby-Datenbank durchzuführen. Wenn `Fast-Start Failover` aktiviert ist, kann Data Guard Broker bei Erkennung eines Fehlers ohne Benutzereingriff ein Failover der primären Datenbank auf die Standby-Datenbank durchführen.

Klonen Sie die Standby-Datenbank für andere Anwendungsfälle

Der Hauptvorteil des Hostens der Oracle-Standbydatenbank auf dem ANF im Oracle Data Guard-Setup besteht darin, dass sie schnell geklont werden kann, um viele andere Anwendungsfälle mit minimaler zusätzlicher Speicherinvestition zu bedienen, wenn ein Thin Clone aktiviert ist. NetApp empfiehlt die Verwendung des SnapCenter -UI-Tools zur Verwaltung Ihrer Oracle DataGuard-Datenbank. Im folgenden Abschnitt zeigen wir, wie Sie mit dem NetApp SnapCenter -Tool einen Snapshot der gemounteten und wiederherzustellenden Standby-Datenbankvolumen auf dem ANF für andere Zwecke wie DEV, TEST, REPORT usw. erstellen und klonen.

Nachfolgend finden Sie allgemeine Verfahren zum Klonen einer READ/WRITE-Datenbank aus der verwalteten physischen Standby-Datenbank im Oracle Data Guard mithilfe von SnapCenter. Ausführliche Anweisungen zum Einrichten und Konfigurieren von SnapCenter für Oracle auf ANF finden Sie in TR-4988 "[Sicherung, Wiederherstellung und Klonen von Oracle-Datenbanken auf ANF mit SnapCenter](#)" für Details.

1. Wir beginnen die Anwendungsfallvalidierung, indem wir eine Testtabelle erstellen und eine Zeile in die Testtabelle in der primären Datenbank einfügen. Wir werden dann überprüfen, ob die Transaktion zum Standby und schließlich zum Klon durchläuft.

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

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Dec 11 16:33:17
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 session set container=ntap_pdb1;

Session altered.

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

Table created.

SQL> insert into test values(1, sysdate, 'a test transaction at
primary database NTAP on DB server orap.internal.cloudapp.net');

1 row created.

SQL> commit;
```

```
Commit complete.
```

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

```
          ID
```

```
-----
```

```
DT
```

```
-----
```

```
-----
```

```
EVENT
```

```
-----
```

```
-----
```

```
1
```

```
11-DEC-24 04.38.44.000000 PM
```

```
a test transaction at primary database NTAP on DB server
```

```
orap.internal.cloudapp.
```

```
net
```

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

```
INSTANCE_NAME
```

```
-----
```

```
HOST_NAME
```

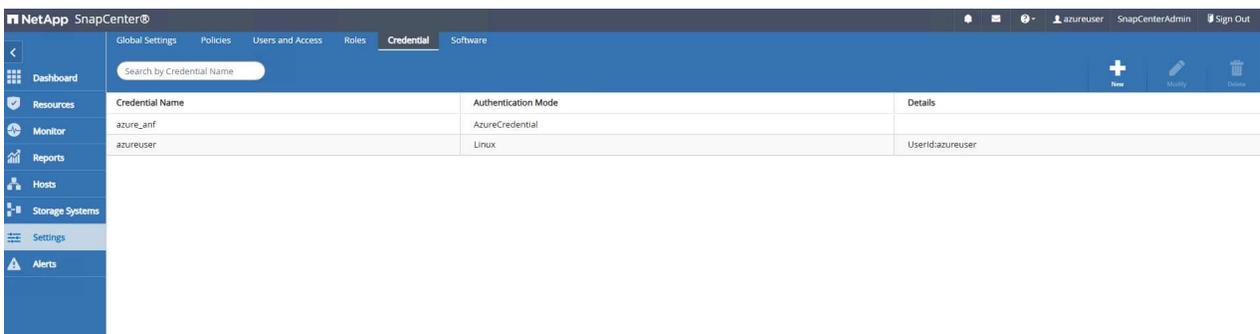
```
-----
```

```
NTAP
```

```
orap
```

```
SQL>
```

2. In der SnapCenter -Konfiguration wurden ein Unix-Benutzer (azureuser für Demo) und eine Azure-Anmeldeinformation (azure_anf für Demo) hinzugefügt zu Credential In Settings .



3. Verwenden Sie die Anmeldeinformationen „azure_anf“, um den ANF-Speicher hinzuzufügen zu Storage Systems . Wenn Ihr Azure-Abonnement mehrere ANF-Speicherkonten enthält, klicken Sie auf die Dropdownliste, um das richtige Speicherkonto auszuwählen. Wir haben für diese Demonstration zwei dedizierte Oracle-Speicherkonten erstellt.

NetApp Account	Resource Group	Credential
ANFOraEast	ANFAVSRG	azure_anf
ANFOraWest	ANFAVSRG	azure_anf

4. Alle Oracle DB-Server wurden zu SnapCenter hinzugefügt Hosts .

Name	Type	System	Plug-in	Version	Overall Status
orac.internal.cloudapp.net	Linux	Stand-alone	Oracle Database, UNIX	6.0.1	Running
orac.internal.cloudapp.net	Linux	Stand-alone	Oracle Database, UNIX	6.0.1	Running
orac.internal.cloudapp.net	Linux	Stand-alone	Oracle Database, UNIX	6.0.1	Running

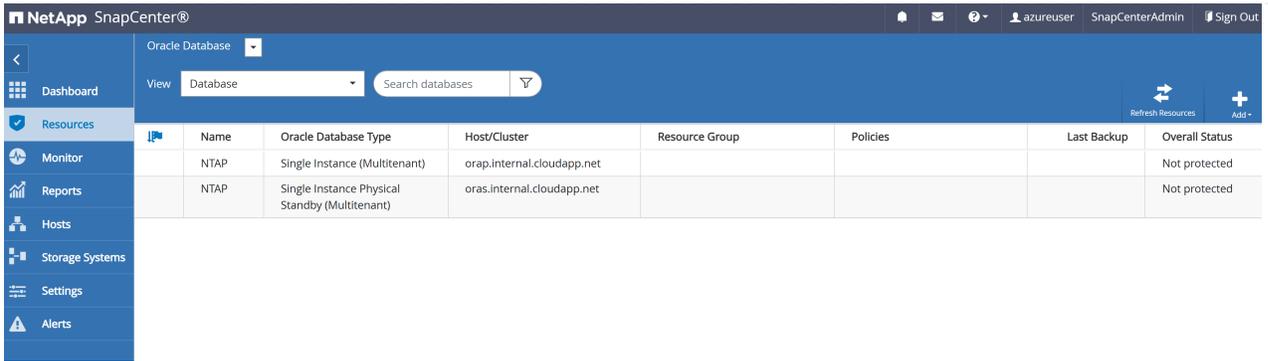


Auf dem Klon-DB-Server sollten identische Oracle-Software-Stacks installiert und konfiguriert sein. In unserem Testfall ist die Oracle 19C-Software installiert und konfiguriert, aber es wurde keine Datenbank erstellt.

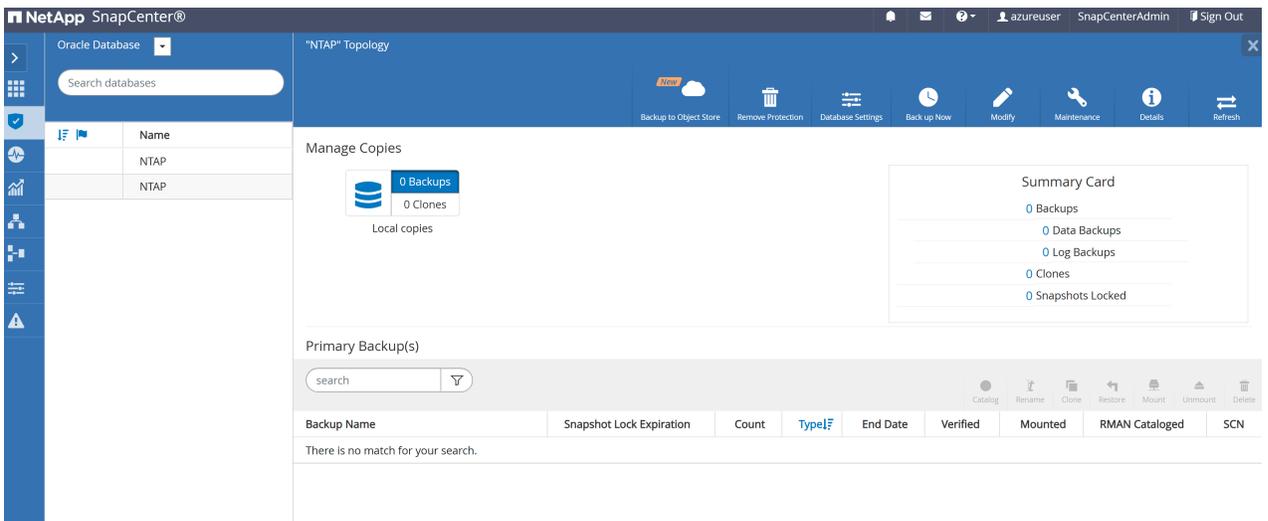
5. Erstellen Sie eine Sicherungsrichtlinie, die auf die Offline-/Mount-Volldatenbanksicherung zugeschnitten ist.

Name	Scope	Schedule Type	Snapshot	Backup	Replication
Oracle full offline backup	DATA, OFFLINEMOUNT	On demand	Retain data copies for : 7 days		
Oracle full offline backup hourly	DATA, OFFLINEMOUNT	Hourly	Data copies to keep : 7 copies		
Oracle full online backup	FULL, ONLINE	On demand	Retain data copies for : 7 days Retain log copies for : 7 days		

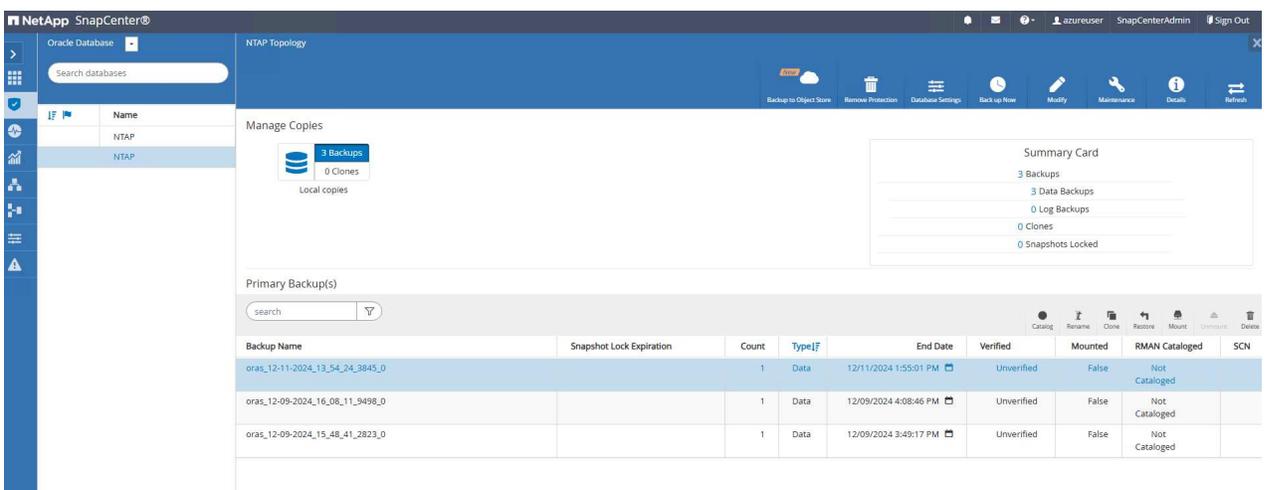
6. Wenden Sie die Sicherungsrichtlinie an, um die Standby-Datenbank zu schützen in Resources Tab. Bei der ersten Erkennung wird der Datenbankstatus wie folgt angezeigt: Not protected .



7. Sie haben die Möglichkeit, eine Sicherung entweder manuell auszulösen oder sie nach Anwendung einer Sicherungsrichtlinie zu einem festgelegten Zeitpunkt zu planen.



8. Klicken Sie nach einer Sicherung auf den Datenbanknamen, um die Seite mit den Datenbanksicherungen zu öffnen. Wählen Sie eine Sicherung aus, die zum Klonen der Datenbank verwendet werden soll, und klicken Sie auf **CLONE** Schaltfläche, um den Klon-Workflow zu starten.



9. Wählen Sie die **Complete Database Clone** und benennen Sie die SID der Kloninstanz.

Clone from NTAP



- 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

10. Wählen Sie den Klon-DB-Server aus, der die geklonte Datenbank aus der Standby-DB hostet. Akzeptieren Sie die Standardeinstellung für Datendateien und Redo-Protokolle. Legen Sie eine Steuerdatei auf dem Einhängpunkt /u03 ab.

Clone from NTAP

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 ?

Redo logs ?

Group	Size	Unit	Number of files	
▶ RedoGroup 1	<input type="button" value="X"/>	200	MB	<input type="text" value="1"/> <input type="button" value="+"/>
▶ RedoGroup 2	<input type="button" value="X"/>	200	MB	<input type="text" value="1"/> <input type="button" value="+"/>
▶ RedoGroup 3	<input type="button" value="X"/>	200	MB	<input type="text" value="1"/> <input type="button" value="+"/>

Previous

Next

11. Für die betriebssystembasierte Authentifizierung sind keine Datenbankmeldeinformationen erforderlich. Passen Sie die Oracle-Home-Einstellung an die Konfiguration auf dem Klon-DB-Server an.

1 Name

Database Credentials for the clone

2 Locations

Credential name for sys user

None



3 Credentials

Database port

1521

4 PreOps

5 PostOps

Oracle Home Settings i

6 Notification

Oracle Home

/u01/app/oracle/product/19.0.0/NTAP

7 Summary

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

12. Ändern Sie bei Bedarf die Parameter der Klondatenbank, z. B. indem Sie die PGA- oder SGA-Größe für eine Klondatenbank verringern. Geben Sie ggf. Skripte an, die vor dem Klonen ausgeführt werden sollen.

Clone from NTAP

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

pga_aggregate_target	500M	<input type="button" value="x"/>	<input type="button" value="+"/>
processes	320	<input type="button" value="x"/>	<input type="button" value="Reset"/>
remote_login_passwordfile	EXCLUSIVE	<input type="button" value="x"/>	
sga_target	2G	<input type="button" value="x"/>	<input type="button" value="-"/>

Previous

Next

13. Geben Sie SQL ein, das nach dem Klonen ausgeführt werden soll. In der Demo haben wir Befehle ausgeführt, um den Datenbankarchivmodus für eine Dev/Test/Report-Datenbank zu deaktivieren.

Clone from NTAP



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

Until Cancel recovery will be performed for Physical Standby Dataguard/Active Dataguard database.

- Create new DBID
- Create tempfile for temporary tablespace
- Enter SQL queries to apply when clone is created

shutdown immediate; startup mount; alter database noarchivelog; alter database open;



Enter scripts to run after clone operation

Previous

Next

14. Konfigurieren Sie bei Bedarf die E-Mail-Benachrichtigung.

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

Previous

Next

15. Überprüfen Sie die Zusammenfassung, klicken Sie auf `Finish` um den Klon zu starten.

Clone from NTAP

1 Name	Summary	
2 Locations	Clone from backup	oras_12-11-2024_13_54_24_3845_0
3 Credentials	Clone SID	NTAPDEV
4 PreOps	Capacity Pool Max. Throughput (MiB/s)	none
5 PostOps	Clone server	orac.internal.cloudapp.net
6 Notification	Exclude PDBs	none
7 Summary	Oracle home	/u01/app/oracle/product/19.0.0/NTAP
	Oracle OS user	oracle
	Oracle OS group	oinstall
	Datafile mountpaths	/u02_NTAPDEV /u03_NTAPDEV
	Control files	/u02_NTAPDEV/NTAPDEV/control/control01.ctl /u03_NTAPDEV/NTAPDEV/control/control02.ctl
	Redo groups	RedoGroup =1 TotalSize =200 Path =/u03_NTAPDEV/NTAPDEV/redolog/redo01_01.log RedoGroup =2 TotalSize =200 Path =/u03_NTAPDEV/NTAPDEV/redolog/redo02_01.log RedoGroup =3 TotalSize =200 Path =/u03_NTAPDEV/NTAPDEV/redolog/redo03_01.log RedoGroup =4 TotalSize =200 Path =/u03_NTAPDEV/NTAPDEV/redolog/redo04_01.log RedoGroup =5 TotalSize =200 Path =/u03_NTAPDEV/NTAPDEV/redolog/redo05_01.log RedoGroup =6 TotalSize =200 Path =/u03_NTAPDEV/NTAPDEV/redolog/redo06_01.log RedoGroup =7 TotalSize =200 Path =/u03_NTAPDEV/NTAPDEV/redolog/redo07_01.log
	Recovery scope	Until Cancel
	Prescript full path	none
	Prescript arguments	
	Postscript full path	none

16. Überwachen Sie den Klonjob in **Monitor** Tab. Wir haben festgestellt, dass das Klonen einer Datenbank mit einer Datenbankvolumengröße von etwa 950 GB etwa 14 Minuten dauerte.

Job Details



Clone from backup 'oras_12-11-2024_13_54_24_3845_0'

- ✓ ▾ Clone from backup 'oras_12-11-2024_13_54_24_3845_0'
- ✓ ▾ orac.internal.cloudapp.net
 - ✓ ▶ Prescripts
 - ✓ ▶ Query Host Information
 - ✓ ▶ Prepare for Cloning
 - ✓ ▶ Cloning Resources
 - ✓ ▶ FileSystem Clone
 - ✓ ▶ Application Clone
 - ✓ ▶ Postscripts
 - ✓ ▶ Register Clone
 - ✓ ▶ Data Collection

Task Name: orac.internal.cloudapp.net Start Time: 12/11/2024 2:53:11 PM End Time: 12/11/2024 3:07:33 PM

View Logs

Cancel Job

Close

17. Validieren Sie die Klondatenbank von SnapCenter, die sofort in registriert ist Resources Registerkarte direkt nach dem Klonvorgang.

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
NTAP	Single Instance (Multitenant)	orac.internal.cloudapp.net		Oracle full online backup	12/06/2024 11:45:35 AM	Backup succeeded
NTAP	Single Instance Physical Standby (Multitenant)	oras.internal.cloudapp.net		Oracle full offline backup	12/11/2024 1:55:01 PM	Backup succeeded
NTAPDB1	Single Instance Physical Standby (Multitenant)	orac.internal.cloudapp.net				Not protected

18. Fragen Sie die Klondatenbank vom Klon-DB-Server ab. Wir haben bestätigt, dass die in der primären Datenbank aufgetretene Testtransaktion bis zur Klondatenbank durchgedrungen ist.

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

SQL*Plus: Release 19.0.0.0.0 - Production on Wed Dec 11 20:16:09
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
-----
NTAPDEV       READ WRITE         NOARCHIVELOG

SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME
-----
HOST_NAME
-----
NTAPDEV
orac

SQL> alter pluggable database all open;

Pluggable database altered.

SQL> alter pluggable database all save state;

Pluggable database altered.

SQL> alter session set container=ntap_pdb1;

Session altered.
```

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

```
          ID
```

```
-----
```

```
DT
```

```
-----
```

```
-----
```

```
EVENT
```

```
-----
```

```
-----
```

```
          1
```

```
11-DEC-24 04.38.44.000000 PM
```

```
a test transaction at primary database NTAP on DB server
```

```
orap.internal.cloudapp.
```

```
net
```

Damit ist die Demonstration des Oracle-Standbydatenbankklons im Oracle Data Guard auf dem Azure ANF-Speicher für DEV, TEST, REPORT oder andere Anwendungsfälle abgeschlossen. Mehrere Oracle-Datenbanken können aus derselben Standby-Datenbank im Oracle Data Guard auf ANF geklont werden.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Informationen finden Sie in den folgenden Dokumenten und/oder auf den folgenden Websites:

- Azure NetApp Files

["https://azure.microsoft.com/en-us/products/netapp"](https://azure.microsoft.com/en-us/products/netapp)

- TR-4988: Sicherung, Wiederherstellung und Klonen von Oracle-Datenbanken auf ANF mit SnapCenter

["TR-4988: Sicherung, Wiederherstellung und Klonen von Oracle-Datenbanken auf ANF mit SnapCenter"](#)

- TR-4987: Vereinfachte, automatisierte Oracle-Bereitstellung auf Azure NetApp Files mit NFS

["TR-4987: Vereinfachte, automatisierte Oracle-Bereitstellung auf Azure NetApp Files mit NFS"](#)

- Konzepte und Verwaltung von Oracle Data Guard

["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)

Copyright-Informationen

Copyright © 2025 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.