



SnapCenter für Datenbanken

NetApp Solutions

NetApp
April 26, 2024

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions/databases/automation_ora_clone_lifecycle.html on April 26, 2024. Always check docs.netapp.com for the latest.

Inhalt

- SnapCenter für Datenbanken. 1
 - SnapCenter Lifecycle Automation für Oracle-Klone. 1
 - TR-4988: Backup, Recovery und Klonen von Oracle Datenbanken auf ANF mit SnapCenter 5
 - TR-4977: Sicherung, Wiederherstellung und Klonen von Oracle Datenbanken mit SnapCenter Services - Azure 46
 - TR-4964: Sicherung, Wiederherstellung und Klonen von Oracle-Datenbanken mit SnapCenter Services - AWS 80
 - Hybrid-Cloud-Datenbanklösungen mit SnapCenter 114

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 Klonpezifikation 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 Repositorys 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

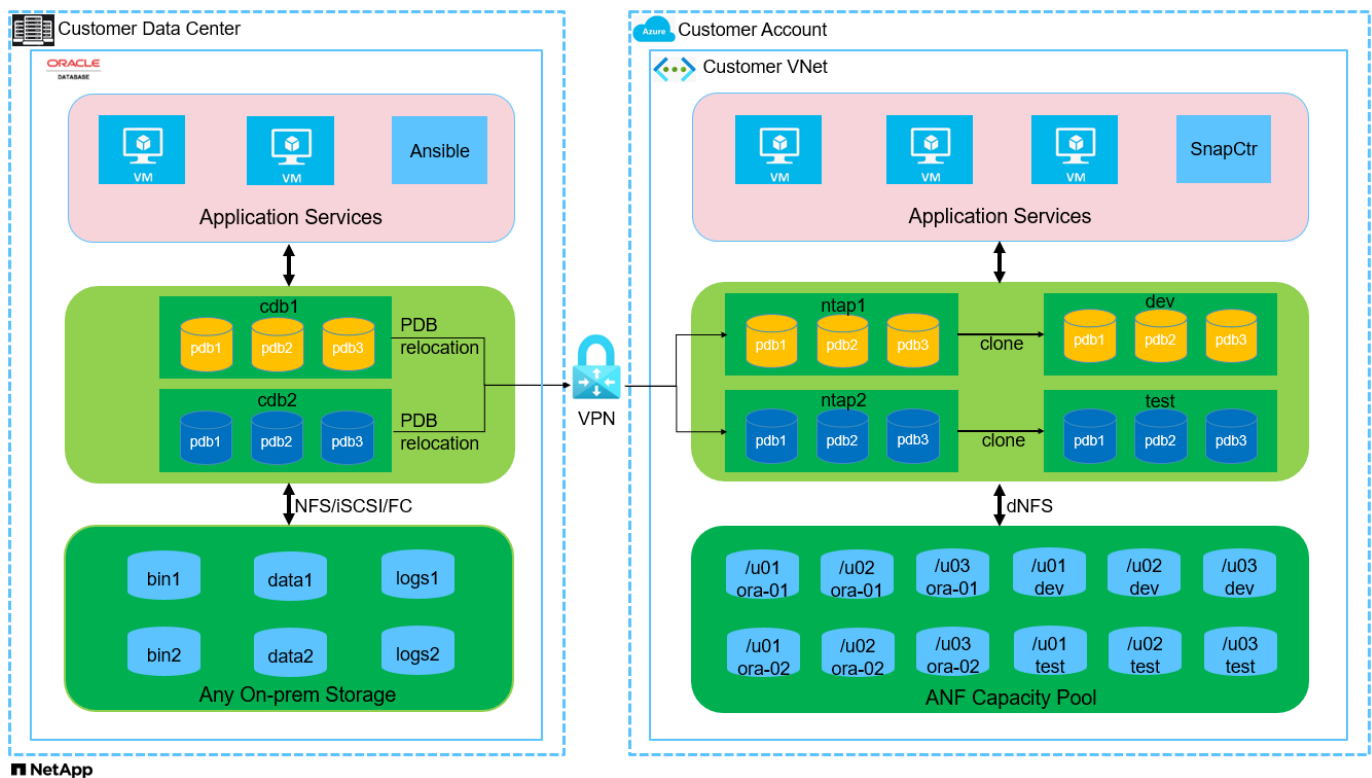
Diese Lösung ist für folgende Personen gedacht:

- 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 Datenvolumes und Log-Volumes 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:

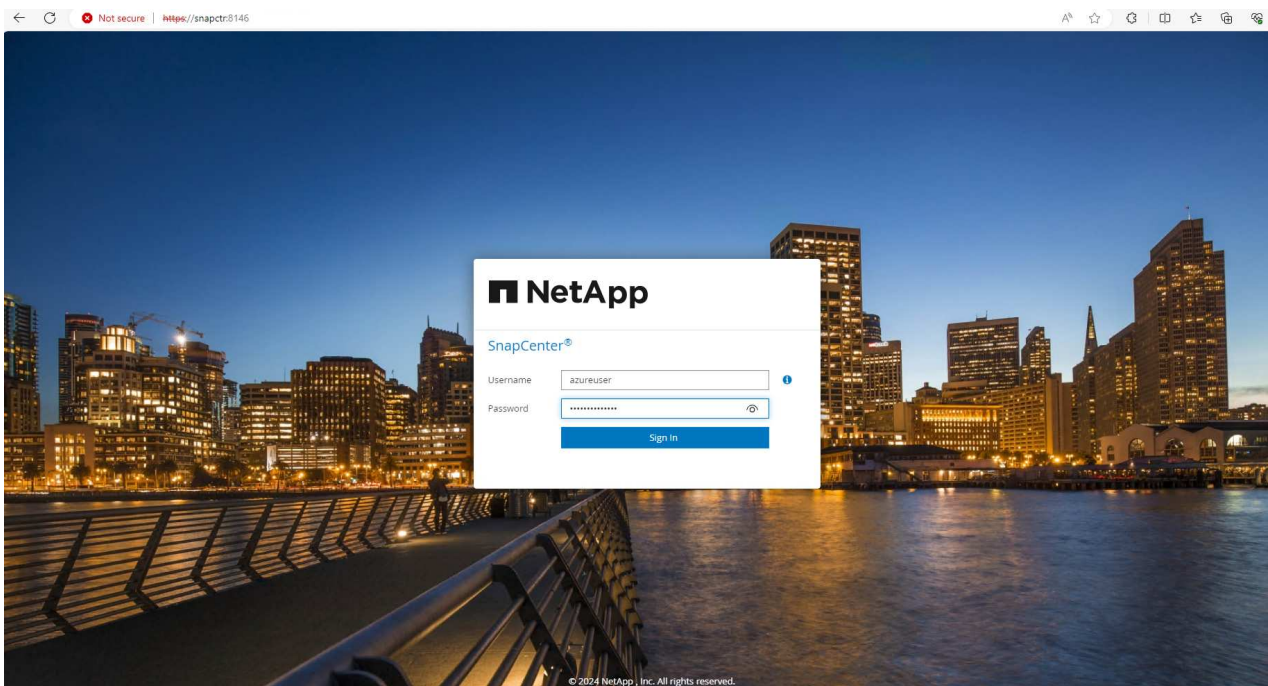
[Oracle Database Backup, Recovery und Klonen auf ANF mit SnapCenter](#)

8. Überprüfen Sie die Get Started Online-Menü.

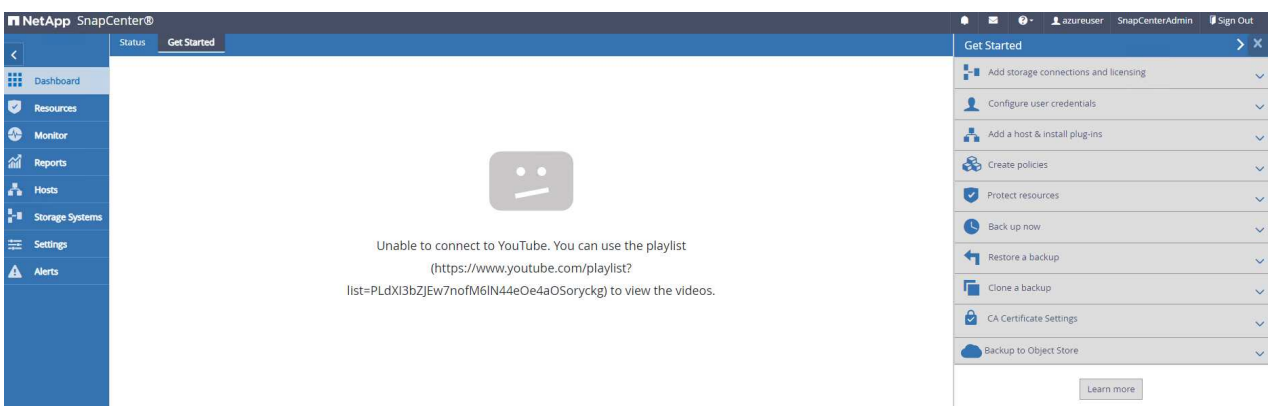
Installation und Einrichtung von SnapCenter

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.

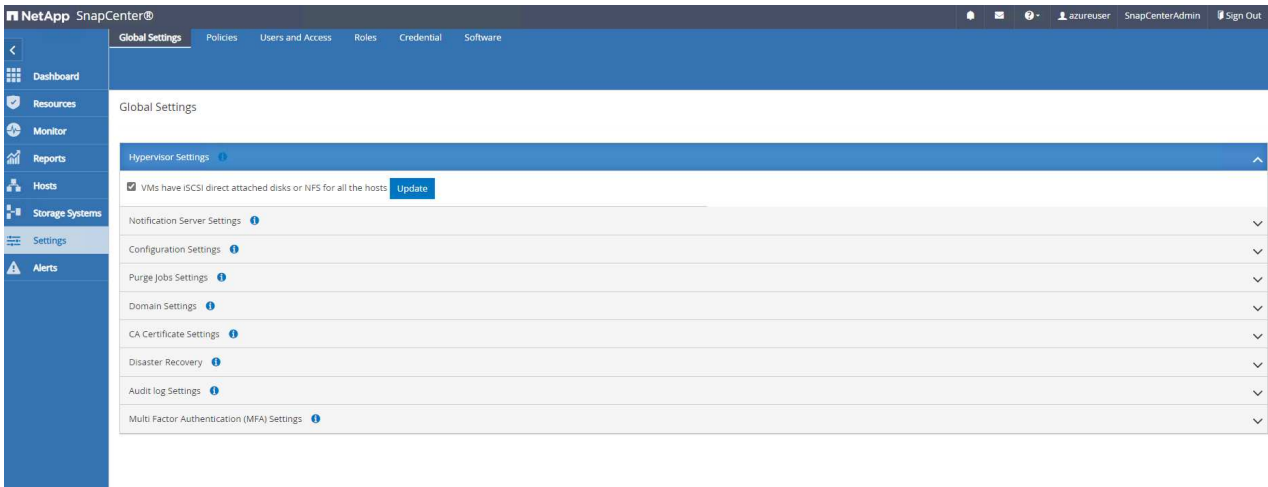
1. Laden Sie vom SnapCenter-Windows-Server die neueste java-JDK herunter, und installieren Sie sie unter "[Holen Sie sich Java für Desktop-Anwendungen](#)".
2. Laden Sie vom SnapCenter Windows-Server die neueste Version (derzeit 5.0) der ausführbaren SnapCenter-Installationsdatei von der NetApp Support-Website 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.



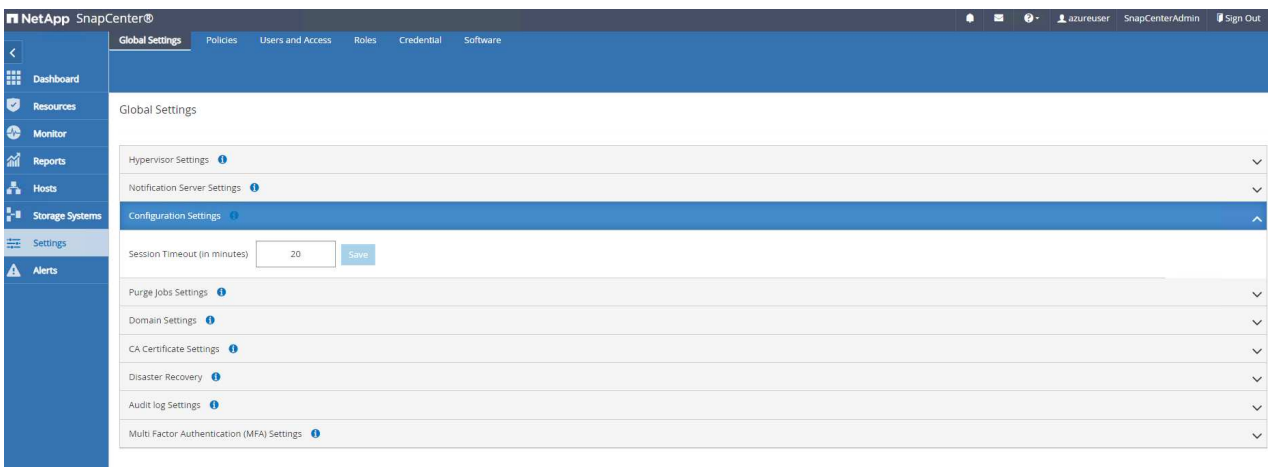
4. Prüfen Get Started Online-Menü.



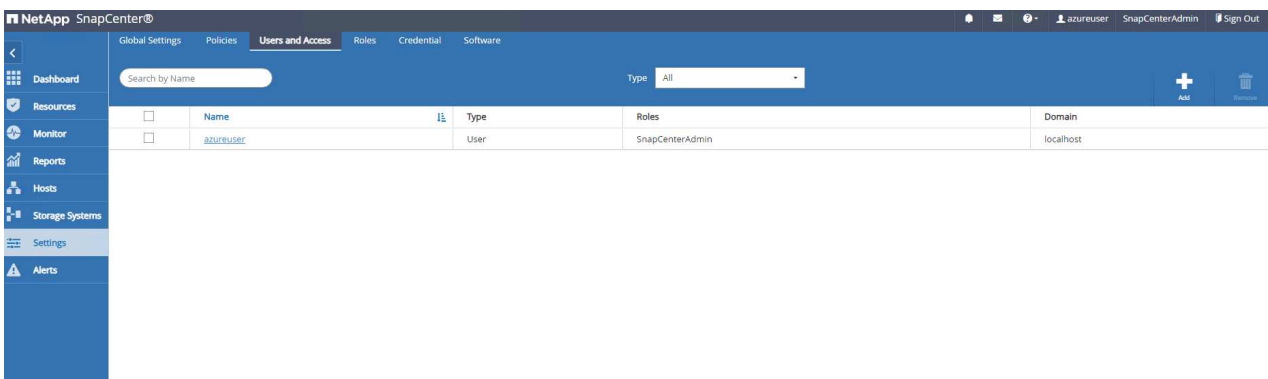
5. In Settings-Global Settings, Überprüfen Hypervisor Settings Und klicken Sie auf Aktualisieren.



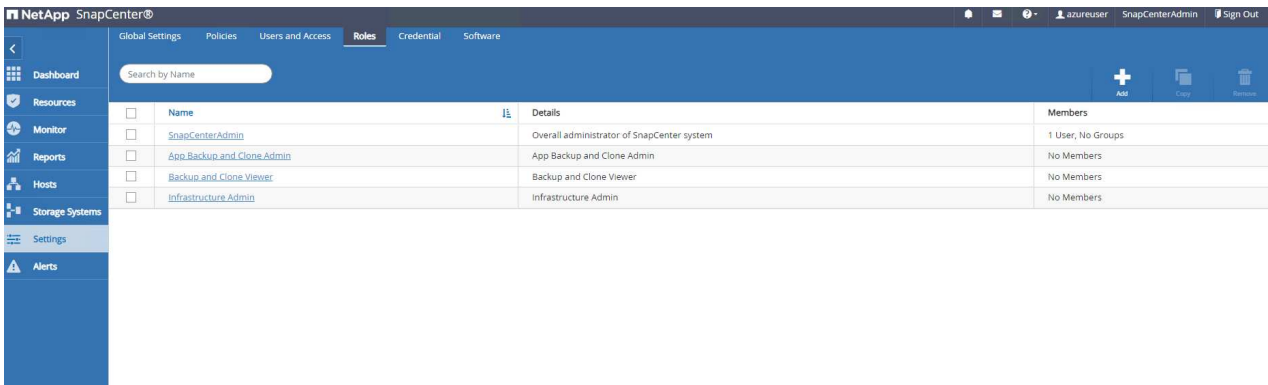
6. Bei Bedarf einstellen Session Timeout Für die SnapCenter-Benutzeroberfläche das gewünschte Intervall.



7. Fügen Sie bei Bedarf weitere Benutzer zu SnapCenter hinzu.



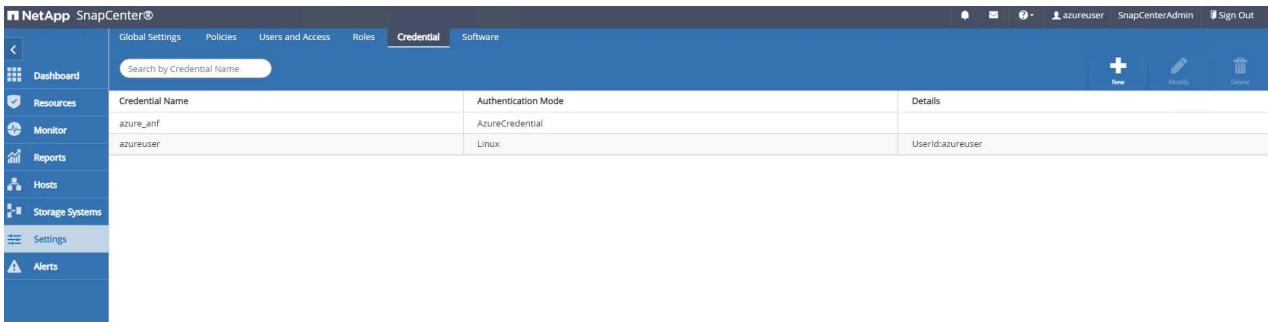
8. Der Roles Auf der Registerkarte werden die integrierten Rollen aufgeführt, die verschiedenen SnapCenter-Benutzern zugewiesen werden können. Benutzerdefinierte Rollen können auch vom Admin-Benutzer mit den gewünschten Berechtigungen erstellt werden.



The screenshot shows the NetApp SnapCenter web interface. The top navigation bar includes 'Global Settings', 'Policies', 'Users and Access', 'Roles' (selected), 'Credential', and 'Software'. The left sidebar contains 'Dashboard', 'Resources', 'Monitor', 'Reports', 'Hosts', 'Storage Systems', 'Settings', and 'Alerts'. The main content area displays a table of roles with columns for Name, Details, and Members. The roles listed are SnapCenterAdmin, App Backup and Clone Admin, Backup and Clone Viewer, and Infrastructure Admin. The SnapCenterAdmin role has one member: '1 User, No Groups'.

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.



The screenshot shows the NetApp SnapCenter web interface with the 'Credential' tab selected. The top navigation bar includes 'Global Settings', 'Policies', 'Users and Access', 'Roles', 'Credential' (selected), and 'Software'. The left sidebar is the same as the previous screenshot. The main content area displays a table of credentials with columns for Credential Name, Authentication Mode, and Details. The credentials listed are azure_anf (AzureCredential) and azureuser (Linux).

Credential Name	Authentication Mode	Details
azure_anf	AzureCredential	
azureuser	Linux	User: azureuser

Credential

✕

Credential Name

azureuser

Authentication Mode

Linux

▼

Authentication Type

☐ Password Based

☒ SSH Key Based

i

Username

azureuser

i

SSH Private Key

XRlRk1QCaE0Hg==
-----END RSA PRIVATE KEY-----

i

☒ Use sudo privileges

i

Cancel

OK

Credential ✕

Credential Name

Authentication Mode

Azure Credential ▼

Azure Details ⓘ

Tenant ID

Client ID

Client Secret Key

Cancel

OK

10. Von Storage Systems Registerkarte, hinzufügen Azure NetApp Files Mit oben erstellten Zugangsdaten.

NetApp SnapCenter®

ONTAP Storage

Azure NetApp Files

azureuser

SnapCenterAdmin

Sign Out

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

Search by NetApp Account

☐ NetApp Account

☐ ANFAVSAcct

Resource Group

ANFAVSRG

Credential

azure_anf

Add Azure NetApp Account

Credential

azure_anf

Subscription

Hybrid Cloud TME Onprem

NetApp Account

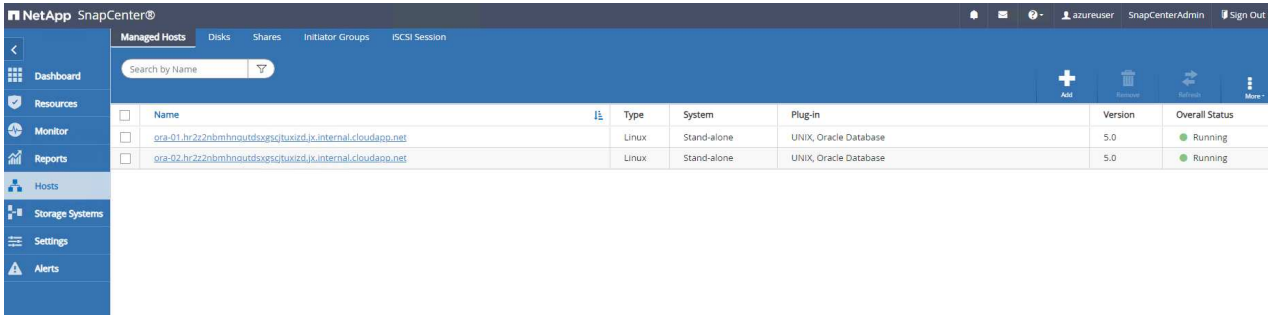
ANFAVSAcct (ResourceGroup: ANFAVSRG)

Submit

Cancel

15

11. Von Hosts Fügen Sie die Azure DB VMs hinzu, die das SnapCenter Plug-in für Oracle auf Linux installieren.



Name	Type	System	Plug-in	Version	Overall Status
ora-01.hr2z2nbmhnoutd5xsgtucvz4jx.internal.cloudapp.net	Linux	Stand-alone	UNIX, Oracle Database	5.0	Running
ora-02.hr2z2nbmhnoutd5xsgtucvz4jx.internal.cloudapp.net	Linux	Stand-alone	UNIX, Oracle Database	5.0	Running

Add Host

Host Type:

Host Name:

Credentials:  

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...

More Options

Port

8145

Installation Path

/opt/NetApp/snapcenter

☒

Skip optional preinstall checks

☒

Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse

Upload

No plug-ins found.

Save

Cancel

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.

NetApp SnapCenter®

Global Settings

Policies

Users and Access

Roles

Credential

Software

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

Oracle Database

Search by Name

+

Modify

Log

Details

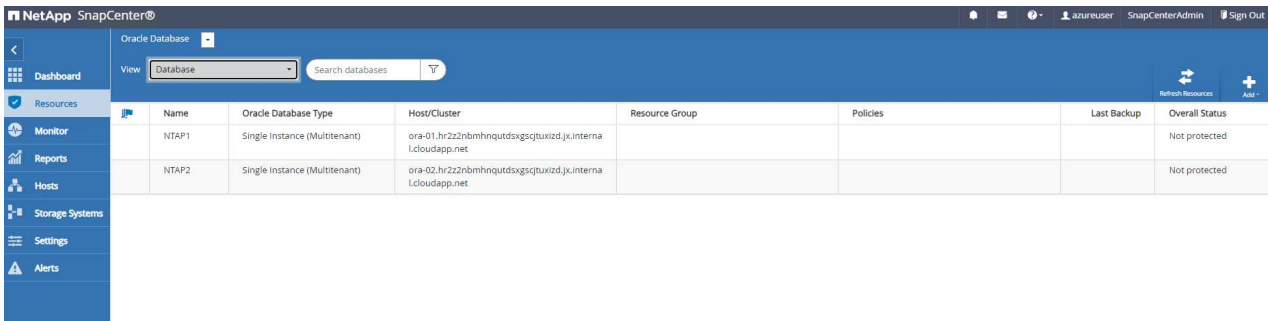
Delete

Name	Backup Type	Schedule Type	Replication	Verification
Oracle archivelogs 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.

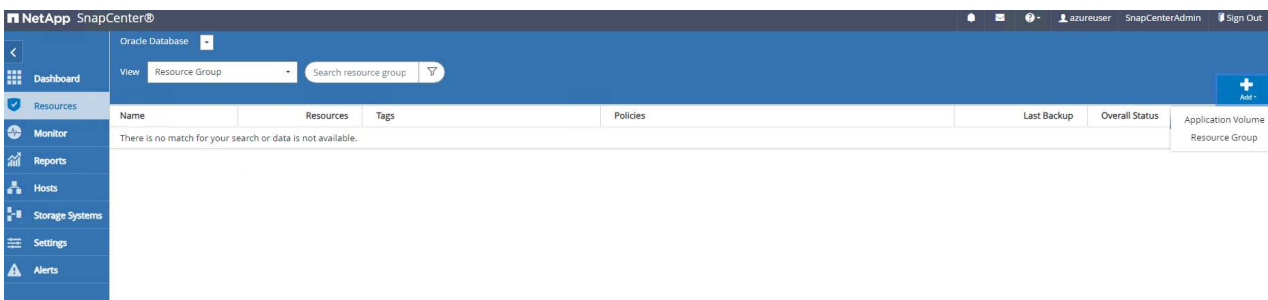
1. Navigieren zu **Resources** Registerkarte, die die Datenbanken auflistet, die nach der Installation des SnapCenter-Plug-ins auf der Datenbank-VM ermittelt wurden. Zu Beginn der **Overall Status** Der Datenbank wird als angezeigt **Not protected**.



The screenshot shows the NetApp SnapCenter web interface. The left sidebar contains navigation links: Dashboard, Resources (selected), Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main content area is titled 'Oracle Database' and has a 'View' dropdown set to 'Database'. Below this is a table with the following data:

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
NTAP1	Single Instance (Multitenant)	ora-01.hr2z2nbnhqnqdsxsgjwizd.jx.interna.lcloudapp.net				Not protected
NTAP2	Single Instance (Multitenant)	ora-02.hr2z2nbnhqnqdsxsgjwizd.jx.interna.lcloudapp.net				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.



The screenshot shows the NetApp SnapCenter web interface with the 'View' dropdown set to 'Resource Group'. The table below shows a message indicating no matches were found for the search.

Name	Resources	Tags	Policies	Last Backup	Overall Status	Application Volume	Resource Group
There is no match for your search or data is not available.							

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.hr2z2nbmhnqutdsxgsqtuxizd.jk.internal.cloudapp.net)
NTAP2 (ora-02.hr2z2nbmhnqutdsxgsqtuxizd.jk.internal.cloudapp.net)

»
«

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



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

2

3

4

5

6

Name

Resources

Policies

Verification

Notification

Summary

Configure verification schedules

Policy

1

2

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

2

3

4

5

6

Name

Resources

Policies

Verification

Notification

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

Modify Resource Group

Back up Now

Maintenance

Delete

Name	Resource Name	Type	Host
full_online_bkup	NTAP1	Oracle Database	ora-01.hr22nbnmqndtsxsgtjuxzdzjx.internal.cloudapp.net
archivelog_bkup	NTAP2	Oracle Database	ora-02.hr22nbnmqndtsxsgtjuxzdzjx.internal.cloudapp.net

Backup

×

Create a backup for the selected resource group

Resource Group

full_online_bkup

Policy

Oracle full online backup ▾

i

☐ 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

📌 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.

NetApp SnapCenter

azureuser SnapCenterAdmin Sign Out

Oracle Database

Search resource groups

full_online_bkup Details

search

NTAP1 Topology

NTAP1 Topology

Search resource groups

full_online_bkup

archivevelg_bkup

Resource Name

NTAP1

NTAP2

Manage Copies

3 Backups0 ClonesLocal copies

Summary Card

3 Backups1 Data Backup2 Log Backups0 Clones0 Snapshots Locked

Primary Backup(s)

search

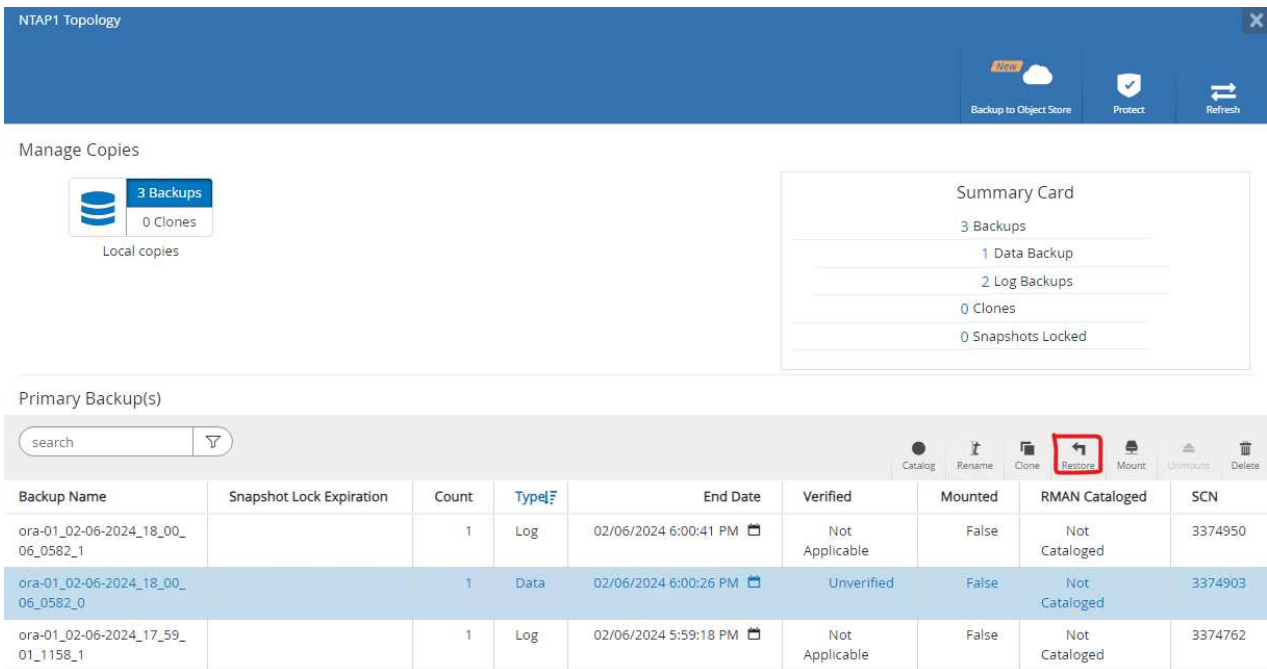
Backup Name	Snapshot Lock Expiration	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora-01_02-06-2024_18_00_06_0582_1		1	Log	02/06/2024 6:00:41 PM	Not Applicable	False	Not Cataloged	3374950
ora-01_02-06-2024_18_00_06_0582_0		1	Data	02/06/2024 6:00:26 PM	Unverified	False	Not Cataloged	3374903
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

Total 2Total 3

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

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

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

Buttons: Catalog, Rename, Clone, **Restore**, Mount, Unmount, Delete

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.

Restore NTAP1

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Choose Recovery Scope

☒ All Logs

☐ Until SCN (System Change Number)

☐ Date and Time

☐ No recovery

Specify external archive log files locations

Previous

Next

4. Der `PreOps` Ermöglicht die Ausführung von Skripts für die Datenbank vor der Wiederherstellung/Wiederherstellung.

Restore NTAP1

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

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Previous

Next

5. Der `PostOps` Ermöglicht die Ausführung von Skripts für die Datenbank nach der Wiederherstellung/Wiederherstellung.

Restore NTAP1

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

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Arguments

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

Previous

Next

6. Benachrichtigung per E-Mail, falls gewünscht.

Restore NTAP1

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ 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

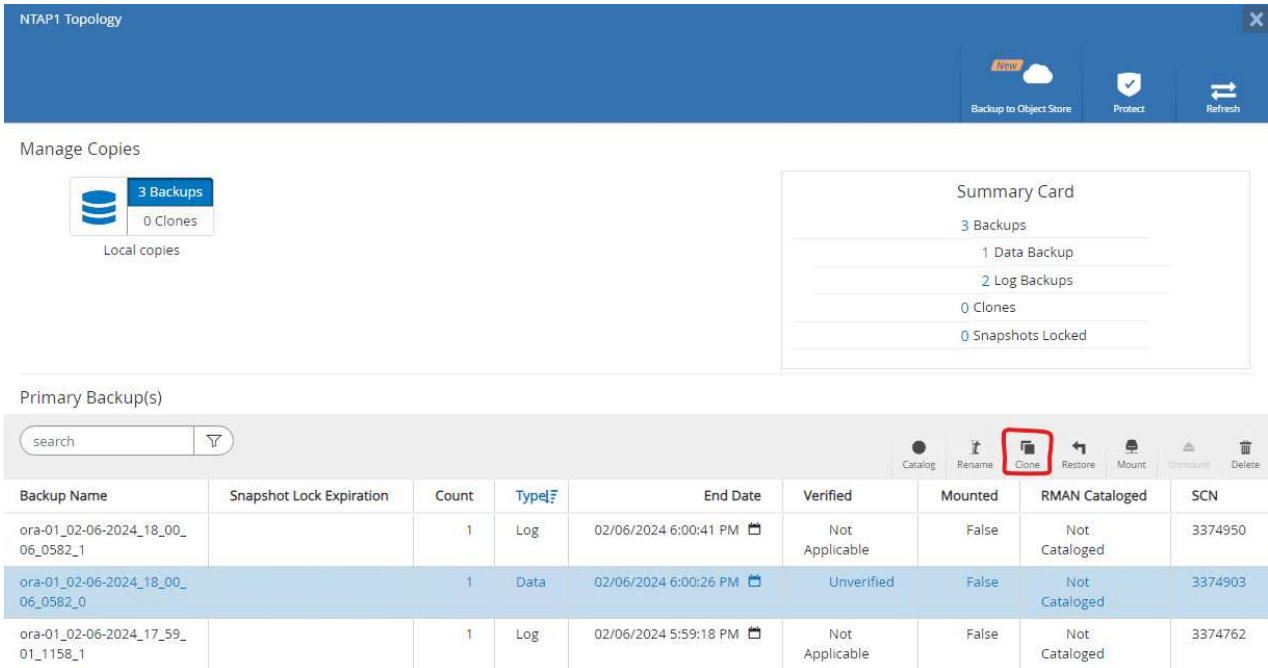
Cancel Job

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

ntap1dev

Exclude PDBs

Type to find 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

ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.inter ▾

⊙ Datafile locations ⓘ

/u02_ntap1dev

Reset

⊙ Control files ⓘ

/u02_ntap1dev/ntap1dev/control/control01.ctl

×

+

/u02_ntap1dev/ntap1dev/control/control02.ctl

×

Reset

⊙ Redo logs ⓘ

Group		Size	Unit	Number of files		
▶ RedoGroup 1	×	200	MB	1	+	<div>+</div> <div>Reset</div>
▶ RedoGroup 2	×	200	MB	1	+	
▶ RedoGroup 3	×	200	MB	1	+	

Previous

Next

- 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.

36

Clone from NTAP1

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

/u01/app/oracle/product/19.0.0/NTAP2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

5. Der `PreOps` Ermöglicht die Ausführung von Skripts vor dem Klonvorgang. Datenbankparameter können an die Anforderungen einer Klon-Datenbank im Gegensatz zu einer Produktionsdatenbank angepasst werden, beispielsweise ein verringertes SGA-Ziel.

Clone from NTAP1

×

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

processes	320	×	<div>+</div> <div>Reset</div>
remote_login_passwordfile	EXCLUSIVE	×	
sga_target	3G	×	
undo_tablespace	UNDOTBS1	×	

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.

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

Summary

Clone from backup	ora-01_02-06-2024_18_00_06_0582_0
Clone SID	ntap1dev
Capacity Pool Max. Throughput (MiB/s)	none
Clone server	ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net
Exclude PDBs	none
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.

NetApp SnapCenter®								
Oracle Database								
View Database Search databases								
	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.

42


```

[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 pdbs
```

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

["https://docs.netapp.com/us-en/netapp-solutions/databases/automation_ora_anf_nfs.html"](https://docs.netapp.com/us-en/netapp-solutions/databases/automation_ora_anf_nfs.html)

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 Konsoleinstellung hinzugefügt.** um Azure NetApp Files Storage zur BlueXP Arbeitsumgebung hinzuzufügen, müssen in der BlueXP Konsoleinstellung 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.

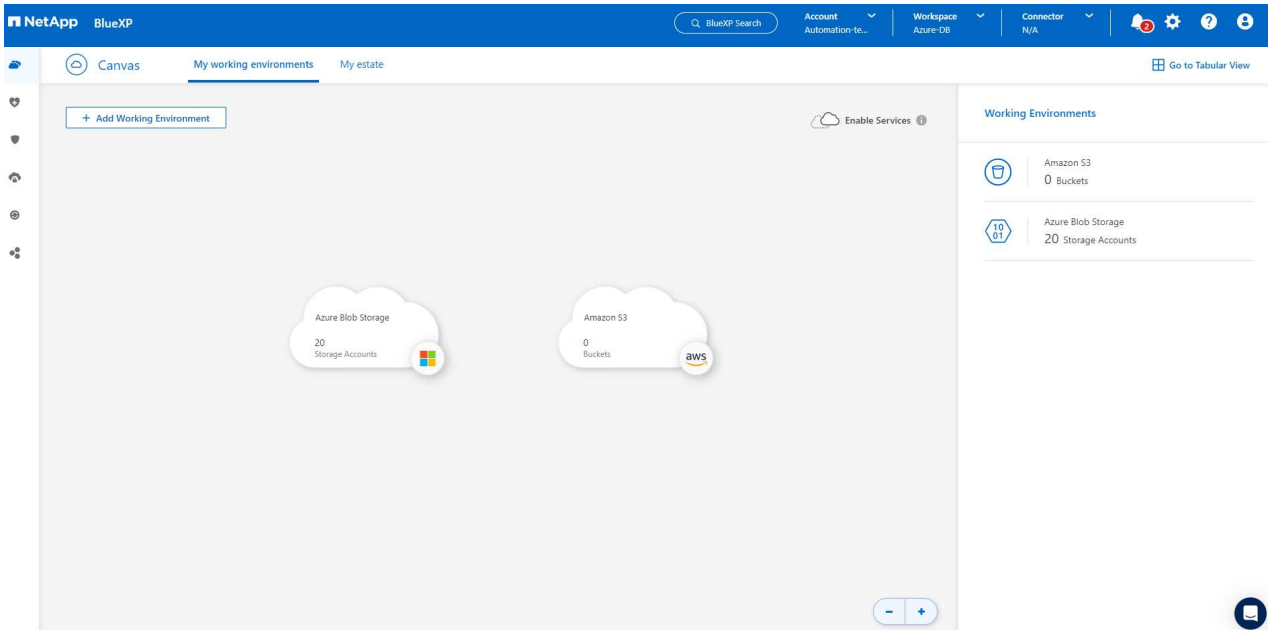
1. Ein primärer Oracle-Datenbankserver auf einer Azure VM-Instanz mit einer Oracle-Datenbank, die vollständig bereitgestellt ist und ausgeführt wird.
2. Ein in Azure bereitgestellter Azure NetApp Files-Storage-Service-Kapazitäts-Pool mit Kapazitäten zur Erfüllung der im Abschnitt „Hardwarekomponenten“ 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

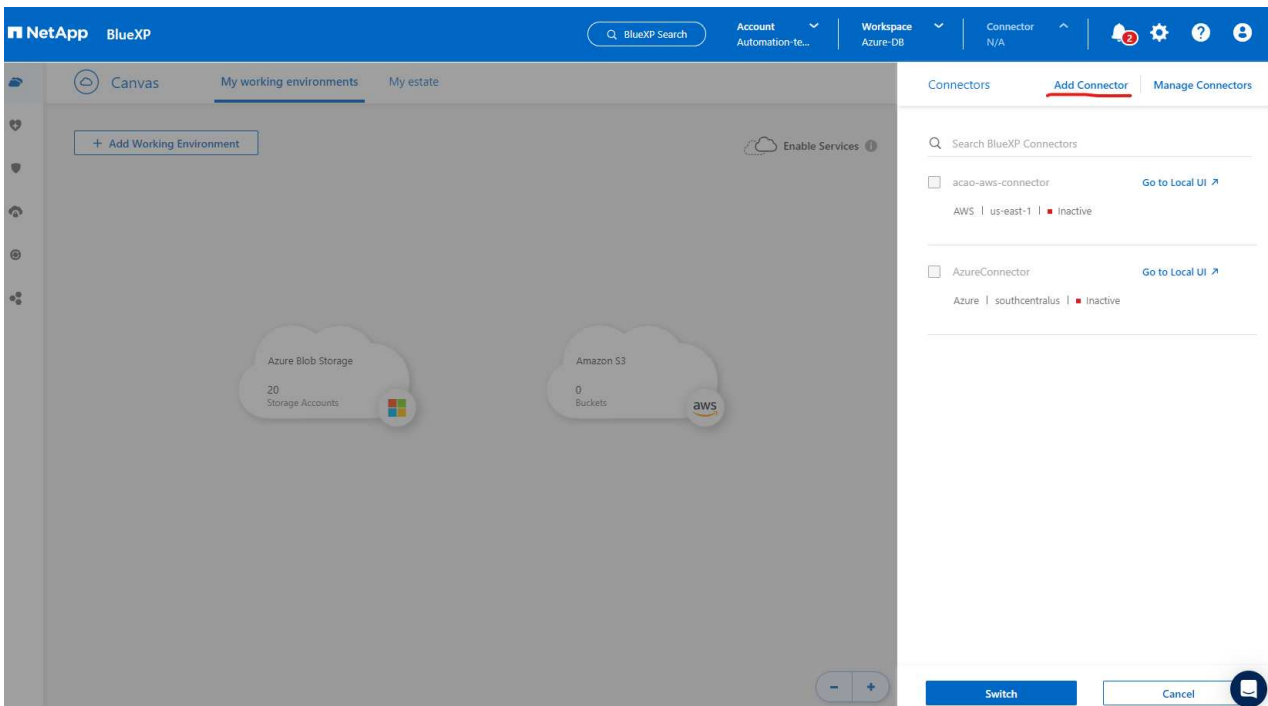
1. Verwenden Sie den Link ["NetApp BlueXP"](#) Um sich für den Konsolenzugriff von BlueXP zu registrieren.
2. Ein Azure-Benutzerkonto oder ein Active Directory-Dienstprinzip erstellen und mit Rolle im Azure-Portal Berechtigungen für die Azure-Connector-Implementierung erteilen.
3. Um BlueXP für das Management 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.

Add BlueXP Connector - Azure
More Information

1 VM Authentication
2 Details
3 Network
4 Security Group
5 Review

Details

Connector Instance Name
AzureConnector

+ Add Tags to Connector Instance

Connector Role

☒ Create
☐ Attach existing
☐ Manual

Role Name
BlueXP Operator-5519248

Subscriptions to apply with the role
Hybrid Cloud TME Onprem

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.

Add BlueXP Connector - Azure
More Information

1 VM Authentication
2 Details
3 Network
4 Security Group
5 Review

Network

Connectivity

VNet
ANFAVSVaI

Subnet
VM_Sub

Public IP
Disable

Notice: Ensure that the subnet has internet connectivity through a NAT device or proxy server so that the Connector can communicate with Azure services.

Proxy Configuration (Optional)

HTTP Proxy
Example: http://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

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 following steps: VM Authentication, Details, Network, Security Group (current), and Review. A 'More Information' link is available in the top right corner.

The main heading is 'Security Group'. Below it, a note states: 'The security group must allow inbound HTTP, HTTPS and SSH access.'

The 'Assign a security group' section has two radio buttons: 'Create a new security group' (selected) and 'Select an existing security group'.

Below this, there are three configuration panels for HTTP, HTTPS, and SSH access:

- HTTP (Port 80):** Source Type is set to 'Anywhere' (dropdown). Source (CIDR) is set to '0.0.0.0/0' (text input).
- HTTPS (Port 443):** Source Type is set to 'Anywhere' (dropdown). Source (CIDR) is set to '0.0.0.0/0' (text input).
- SSH (Port 22):** Source Type is set to 'Anywhere' (dropdown). Source (CIDR) is set to '0.0.0.0/0' (text input).

At the bottom, there are 'Previous' and 'Next' buttons. A help icon (speech bubble) is located 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.

Add BlueXP Connector - Azure

More Information

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	ANFAVSub
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

BlueXP Search

Account Automation-to...

Workspace Azure-DB

Connector AzureConnector

2

?

Canvas

My working environments

My estate

+ Add Working Environment

Enable Services

Azure Blob Storage 20 Storage Accounts

Amazon S3 0 Buckets

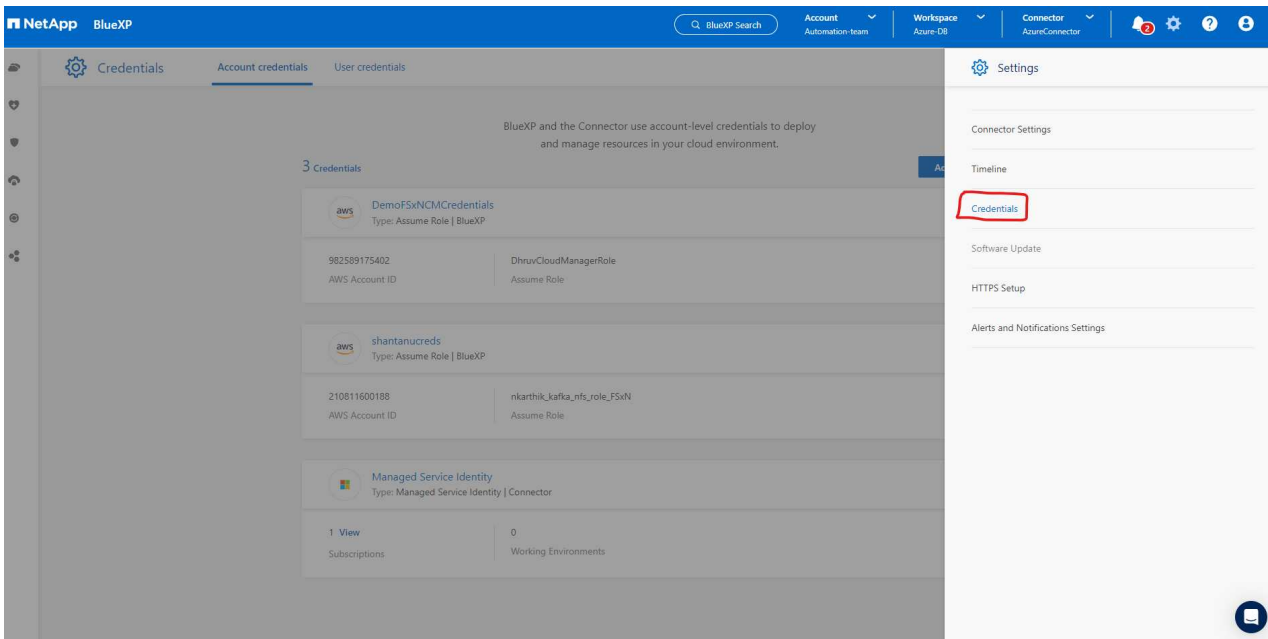
Working Environments

Amazon S3 0 Buckets

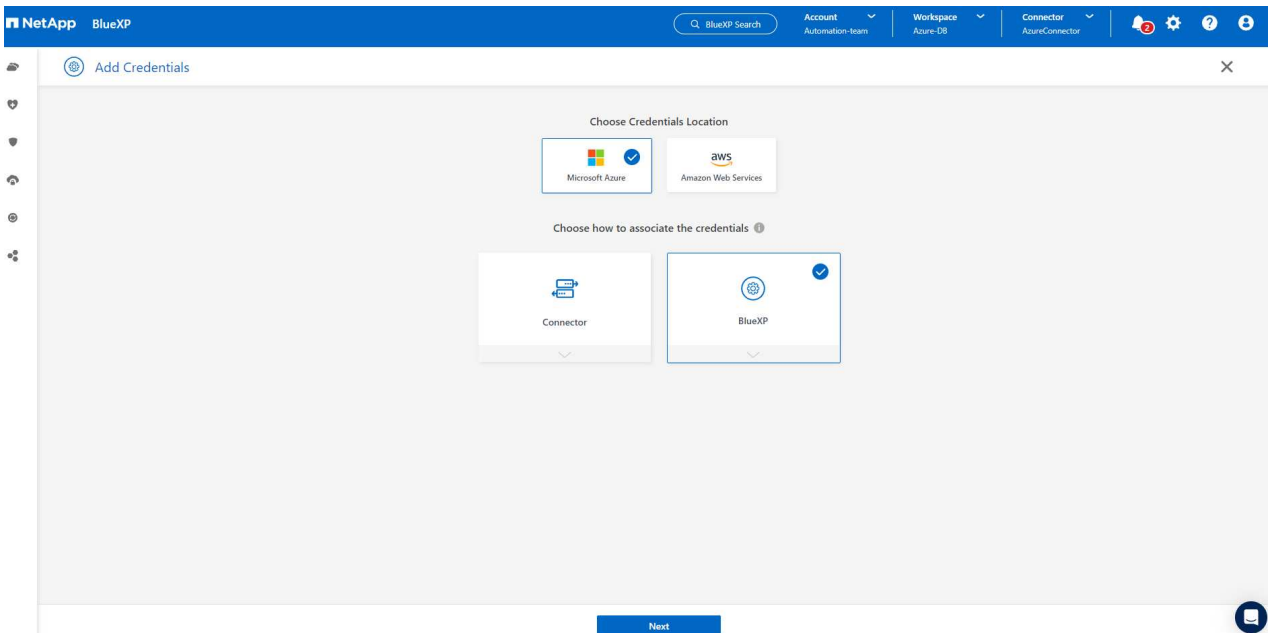
Azure Blob Storage 20 Storage Accounts

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 2 ? !

Add Credentials 1 Credentials Type 2 Define Credentials 3 Marketplace Subscription 4 Review X

Define Microsoft Azure Credentials
Learn more about Azure application credentials

Credentials Name ? Client Secret

Azure_Hybrid_TME

Application (client) ID Directory (tenant) ID

2fbc9be5-a259-4539-bb57-036b176f5cc7 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 2 ? !

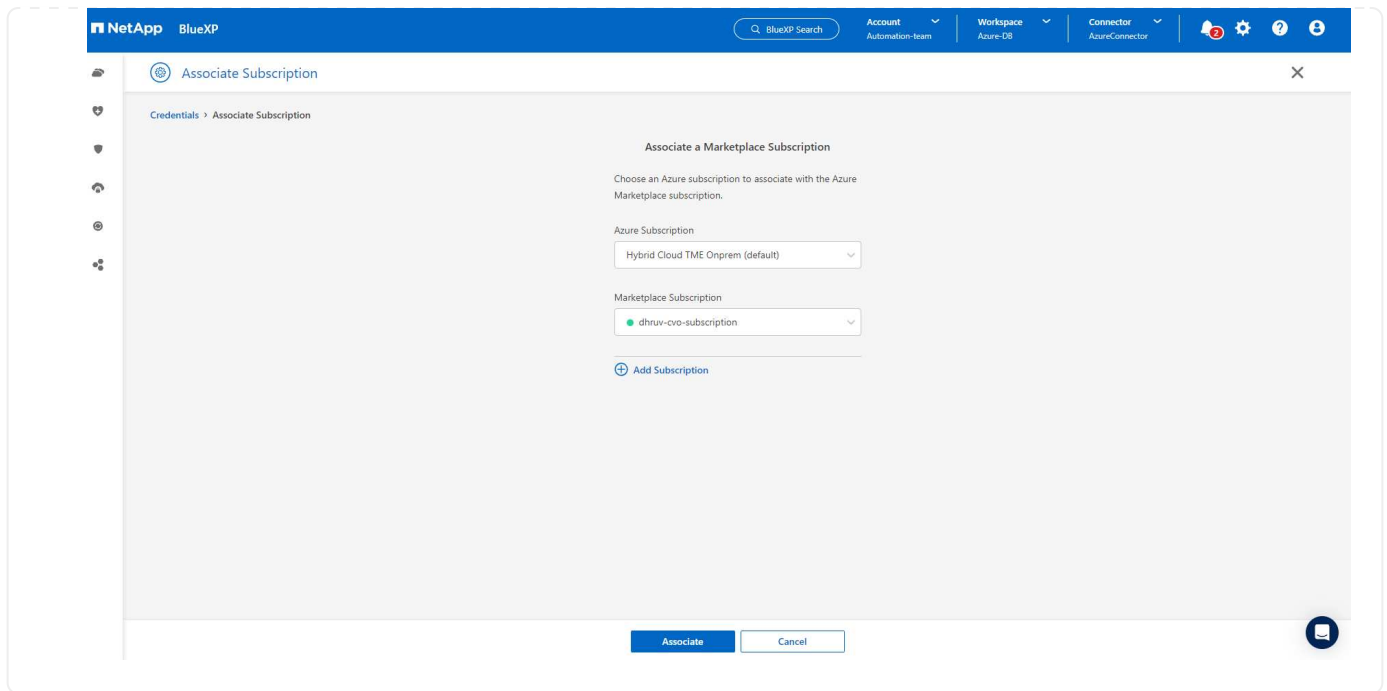
Add Credentials 1 Credentials Type 2 Define Credentials 3 Review X

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 !

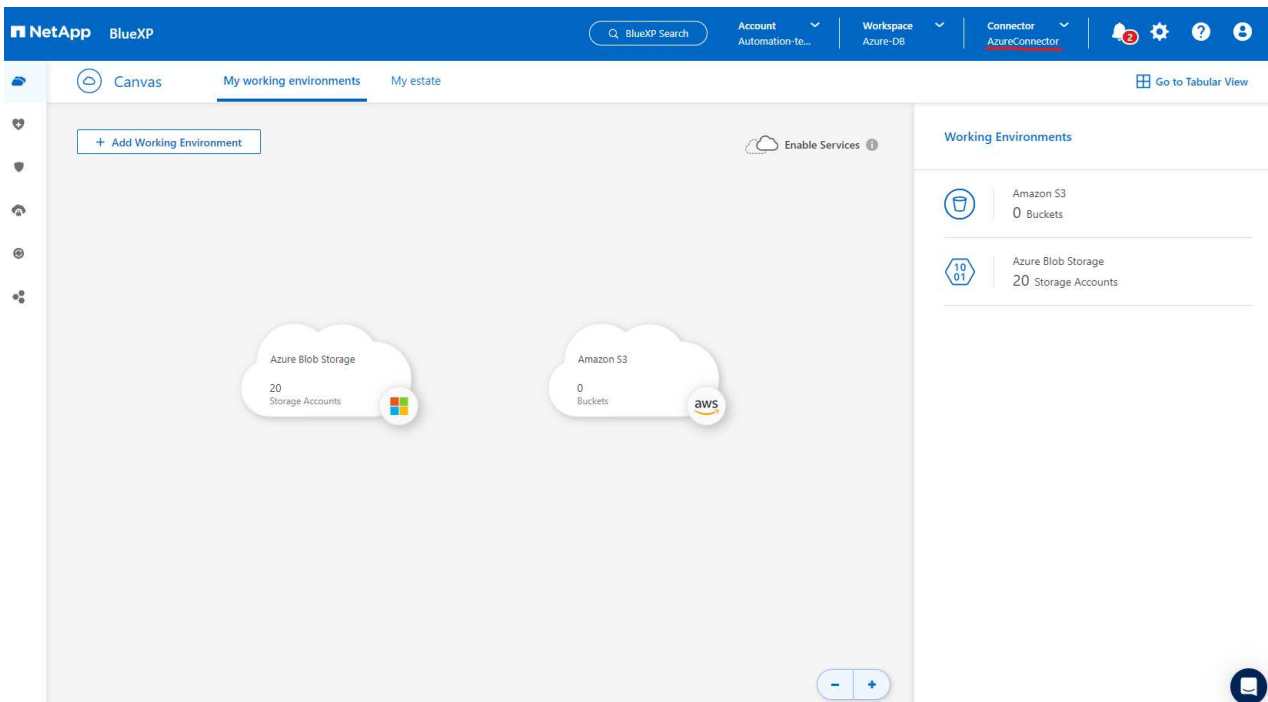
5. Möglicherweise müssen Sie auch ein **Marketplace-Abonnement** mit den Zugangsdaten verknüpfen.



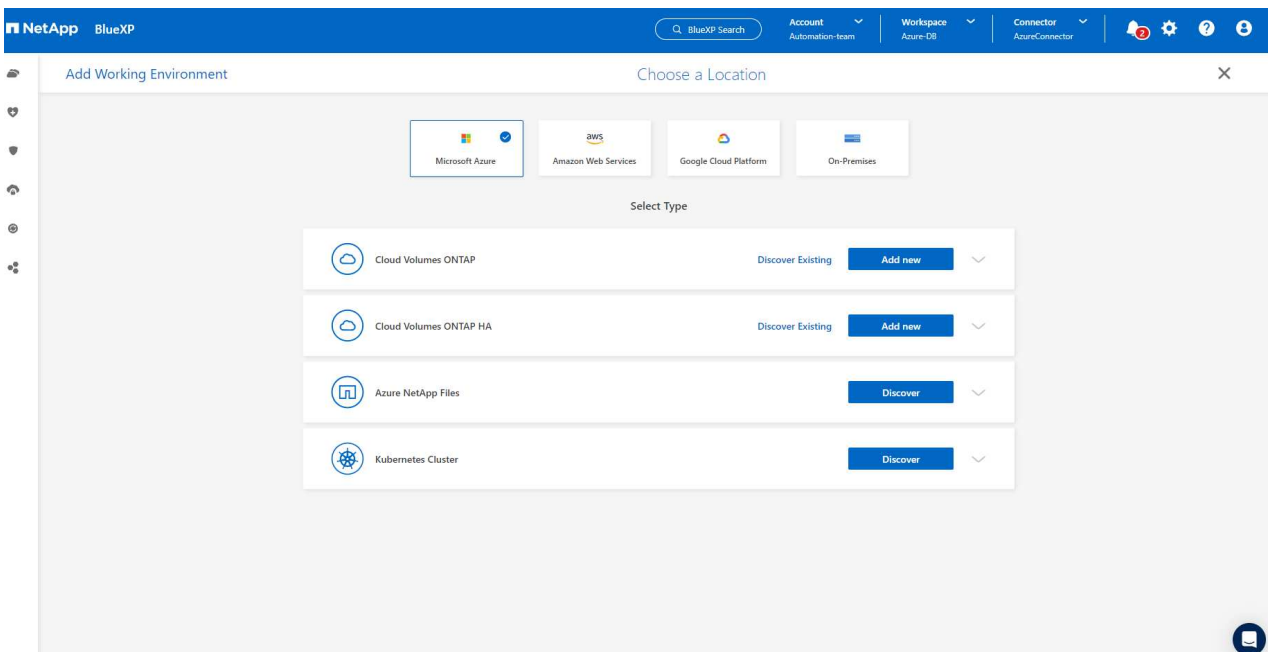
Einrichtung der SnapCenter Services

Wenn die Azure-Zugangsdaten konfiguriert sind, können SnapCenter-Services jetzt wie folgt eingerichtet werden:

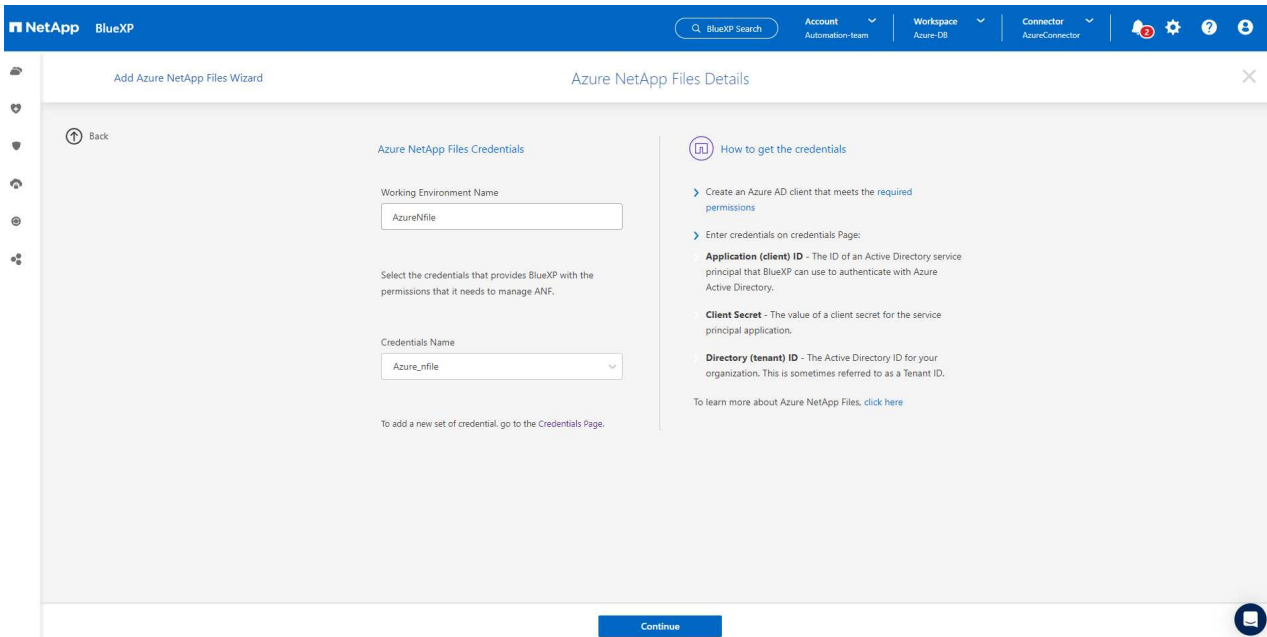
1. Zurück zur Bildschirmseite, von **Meine Arbeitsumgebung** Klicken Sie auf **Arbeitsumgebung hinzufügen**, um Azure NetApp Files in Azure zu entdecken.



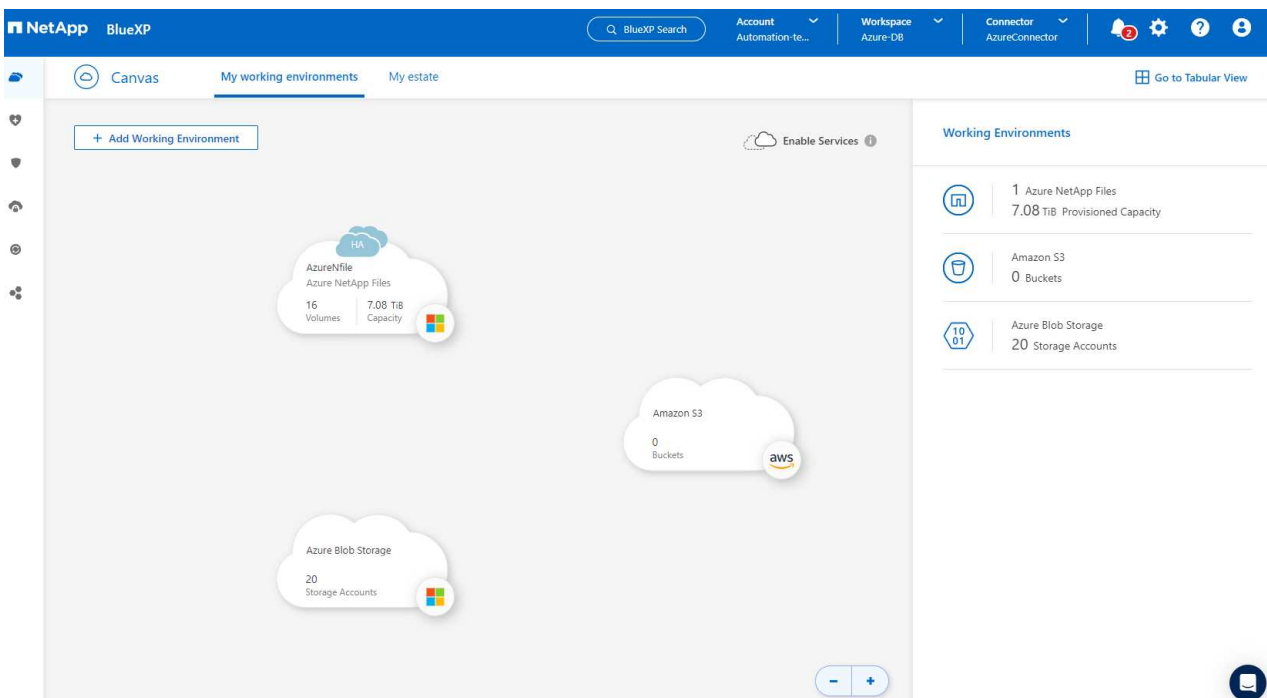
2. Wählen Sie **Microsoft Azure** als Speicherort und klicken Sie auf **Discover**.



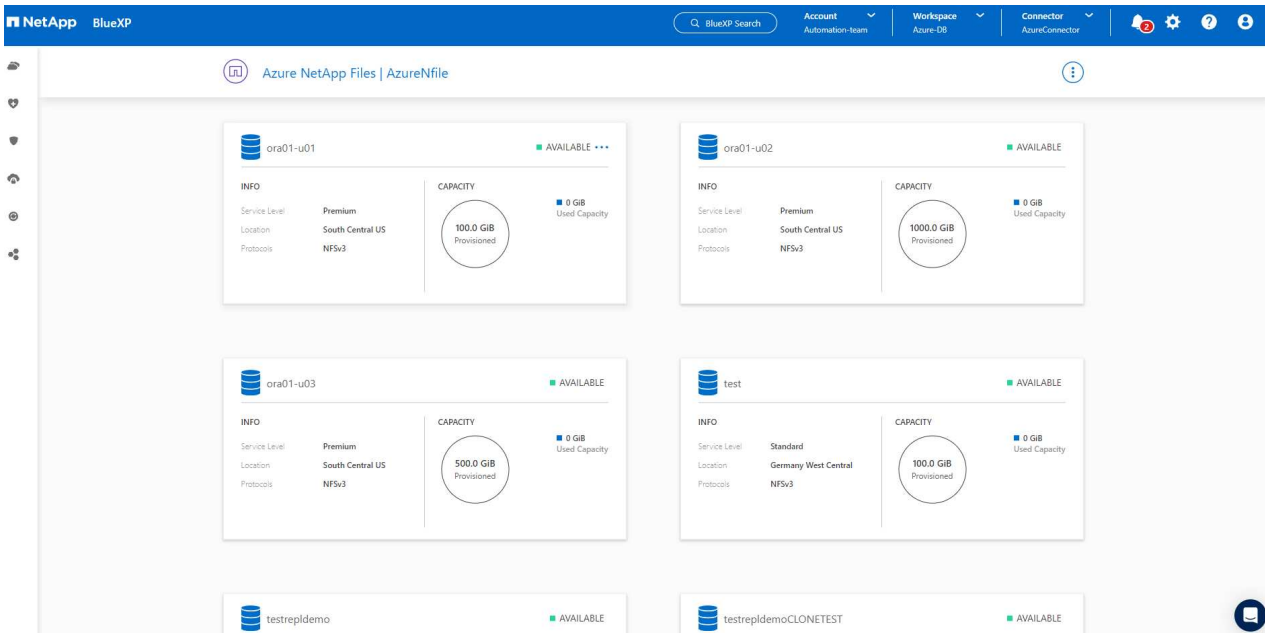
3. Name **Arbeitsumgebung** und wählen Sie **Credential Name** erstellt im vorherigen Abschnitt, und klicken Sie auf **Weiter**.



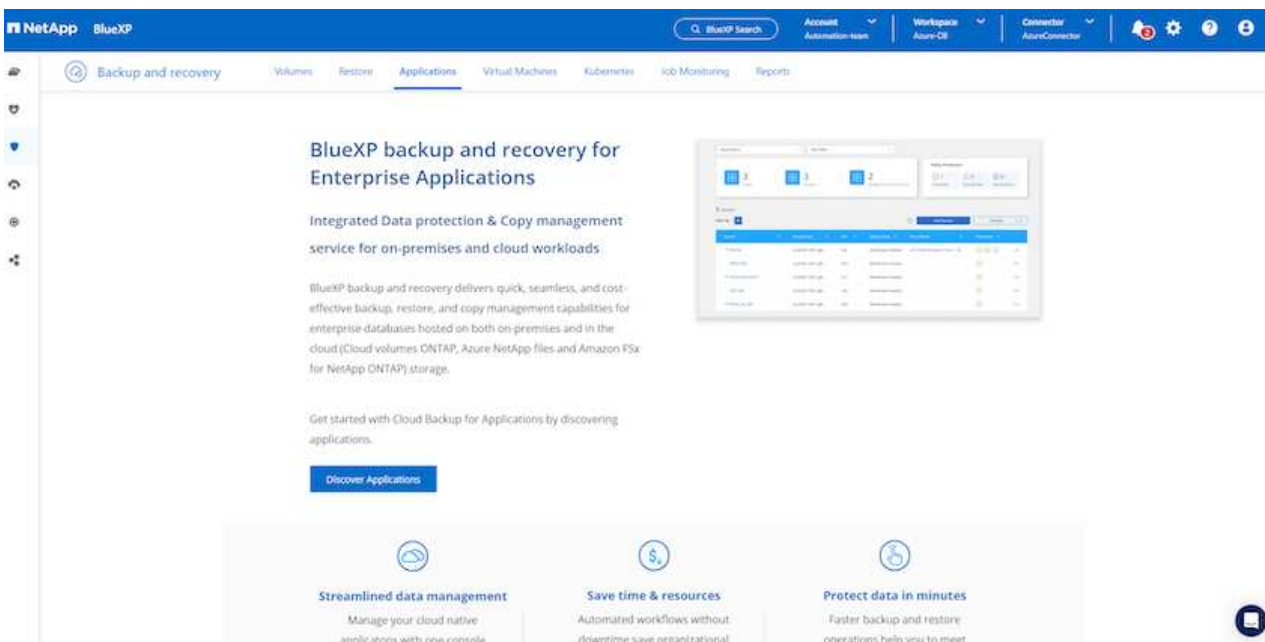
4. BlueXP-Konsole kehrt zu **Meine Arbeitsumgebungen** zurück und entdeckte Azure NetApp Files aus Azure erscheint jetzt auf **Leinwand**.



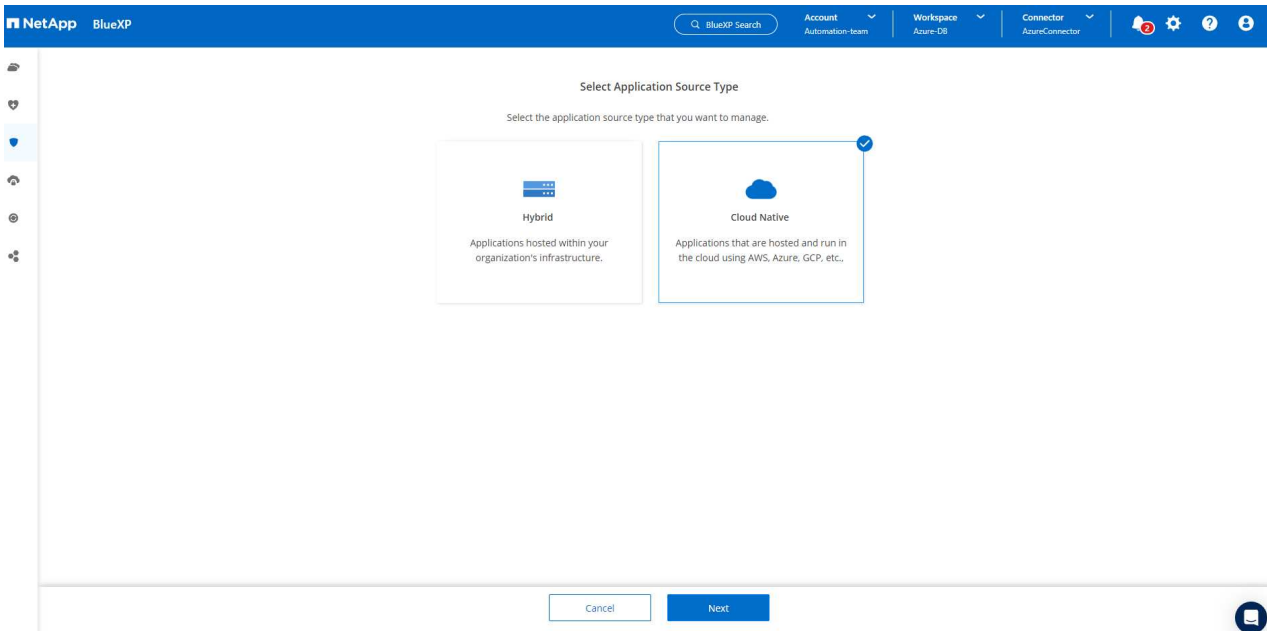
5. Klicken Sie auf das Symbol **Azure NetApp Files** und dann auf **Arbeitsumgebung eingeben**, um die im Azure NetApp Files-Speicher bereitgestellten Oracle-Datenbank-Volumes anzuzeigen.



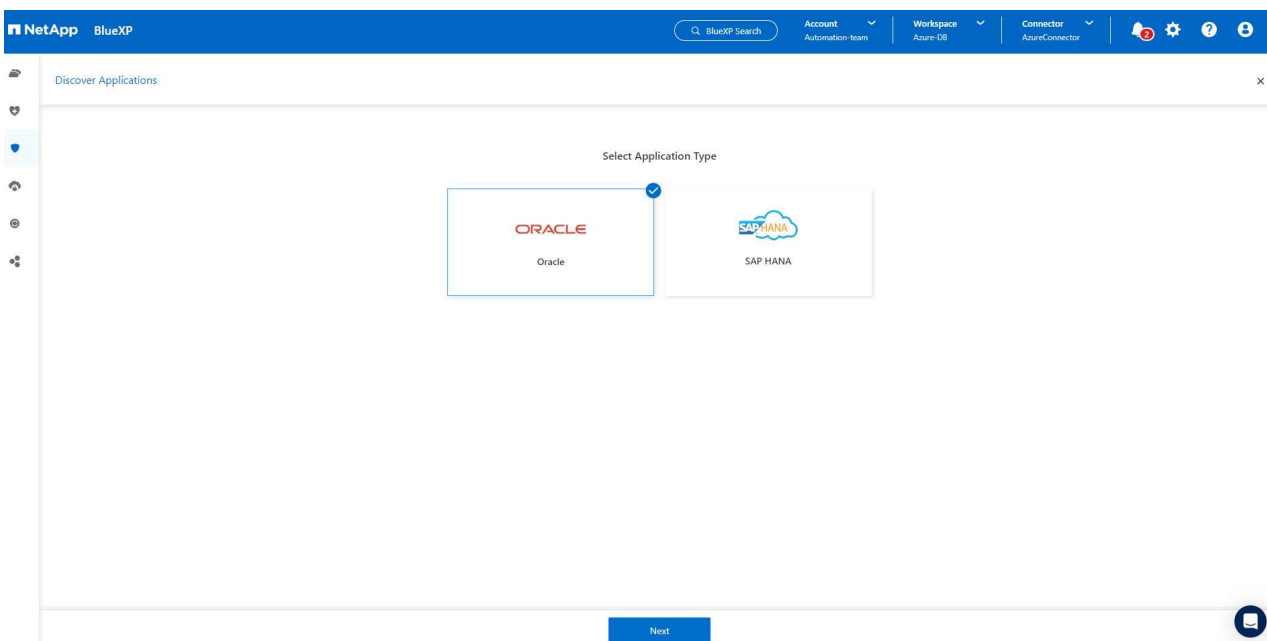
6. Bewegen Sie in der linken Seitenleiste der Konsole Ihre Maus über das Schutzsymbol und klicken Sie dann auf **Schutz > Anwendungen**, um die Startseite der Anwendungen zu öffnen. Klicken Sie Auf **Anwendungen Entdecken**.



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

1 Host Details 2 Configuration 3 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

1 Host Details 2 Configuration 3 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

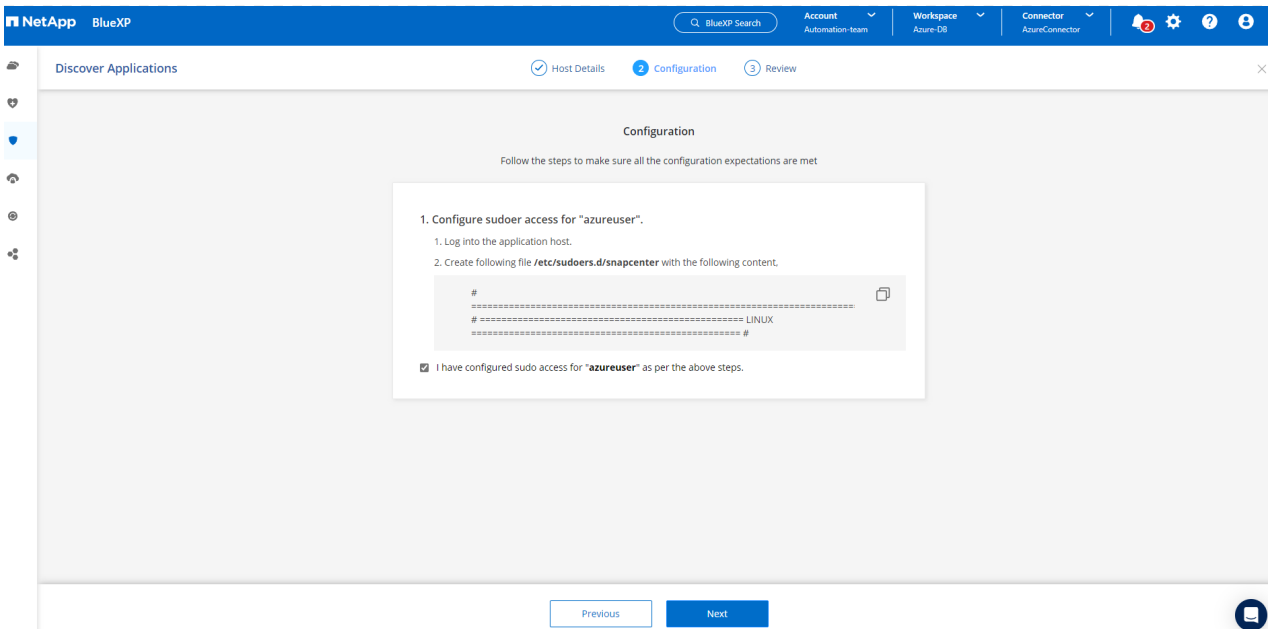
Fingerprint: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAAB...

☒ By proceeding further, I confirm that the above fingerprint for host is valid.

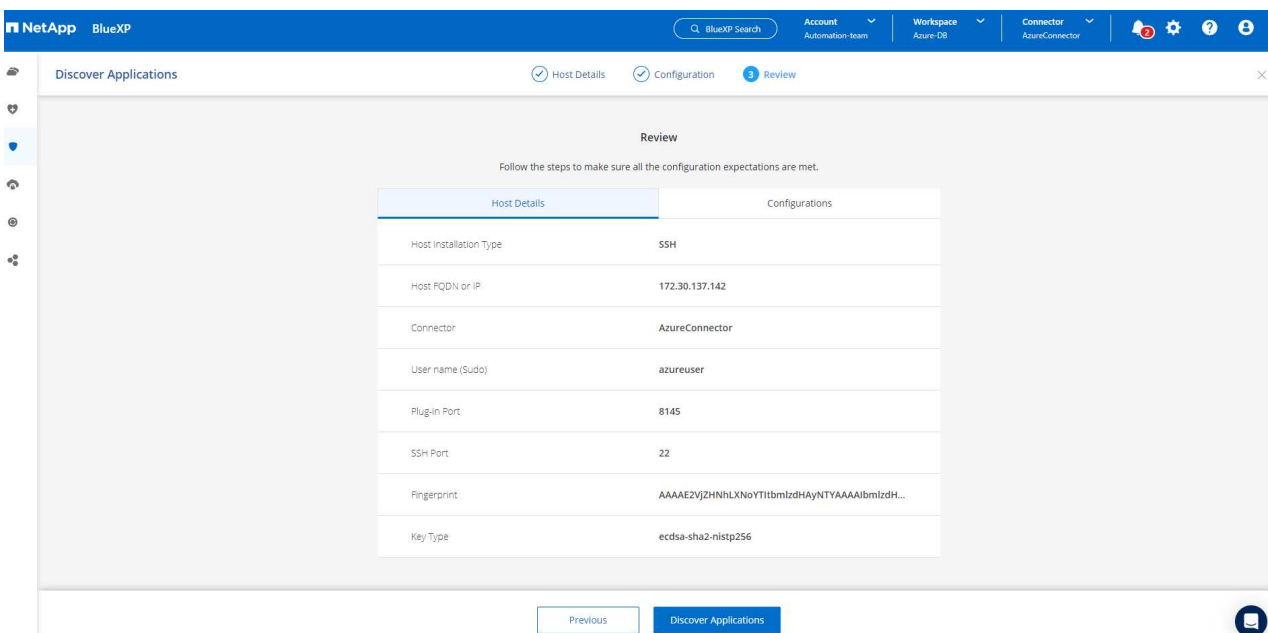
Proceed Cancel

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.

NetApp BlueXP

Backup and recovery | Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring | Reports

Cloud Native | Oracle

3 Hosts | 3 ORACLE | 0 Clone

Application Protection

0 Protected | 3 Unprotected

3 Databases

Filter By +

Manage Databases | Settings

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

1 - 3 of 3

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.

NetApp BlueXP

Backup and recovery | Volumes | Restore | **Applications** | Virtual Machines | Kubernetes | Job Monitoring | Reports

Cloud Native | Oracle

4 Hosts | 3 ORACLE | 0 Clone

Application Protection

0 Protected | 3 Unprotected

3 Databases

Filter By +

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1tst	172.30.15.124		Unprotected

1 - 3 of 3

2. Wenn Sie mit der Richtlinienkonfiguration zufrieden sind, können Sie dann **Assign** Ihre Richtlinie Ihrer Wahl zuweisen, um die Datenbank zu schützen.

NetApp BlueXP

Backup and recovery | Volumes | Restore | **Applications** | Virtual Machines | Kubernetes | Job Monitoring | Reports

Applications > Assign Policy

Assign Policy

Assign a policy to start taking backups of the database "NTAP"

4 Policies

Policy Name	Backup Type	Schedules
<input type="radio"/> Oracle Full Backup for Bronze	FullBackup	Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input type="radio"/> Oracle Full Backup for Gold	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 16 copies Daily: Repeats Every 1 Day, Keeps 30 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input type="radio"/> Oracle Full Backup for Silver	FullBackup	Hourly: Repeats Every 12 Hrs, Keeps 6 copies Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input checked="" type="radio"/> my_full_bkup	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 3 Days

1 - 4 of 4

Cancel Assign

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.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. The 'Applications' section displays a summary for 'Cloud Native' and 'Oracle' hosts. Below this, a table lists databases with their protection status. A context menu is open for the 'NTAP' database, showing options like 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore'.

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99		Unprotected
db1tst	172.30.15.124		Unprotected

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.

The screenshot shows the NetApp BlueXP 'Job Monitoring' page. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', 'Job Monitoring' (selected), and 'Reports'. The page displays details for a specific backup job: 'Backup of NTAP oracle database on host 172.30.137.142 with policy my_full_bkup and schedule H...'. Below this, a summary card shows the job type, start time, end time, and status. A table lists the sub-jobs, including the main backup and subsequent cleanup steps. The duration of the main backup is highlighted as '4 Minutes'.

Job Name	Job ID	Start Time	End Time	Duration
Backup of NTAP oracle database on host 172.30...	61a12139-330e-4390-bc...	Jul 11 2023, 2:17:53 pm	Jul 11 2023, 2:21:38 pm	4 Minutes
Applying Retention	27f9d5f-68f0-4880-a48...	Jul 11 2023, 2:21:38 pm	Jul 11 2023, 2:21:38 pm	0 Second
Performing cleanup after backup	074c0689-097e-41aa-ac...	Jul 11 2023, 2:21:36 pm	Jul 11 2023, 2:21:38 pm	2 Seconds
Finalizing Oracle database log backup	348189d3-90b5-4cce-97...	Jul 11 2023, 2:21:36 pm	Jul 11 2023, 2:21:36 pm	0 Second

5. Im drei-Punkt-Dropdown-Menü **Details anzeigen** können Sie die aus Snapshot-Backups erstellten Backup-Sets anzeigen.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring Reports

Cloud Native Oracle

4 Hosts 3 ORACLE 0 Clone

Application Protection 2 Protected 1 Unprotected

3 Databases

Filter By +

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

Manage Databases Settings

View Details On-Demand Backup Assign Policy Un-assign Policy Restore

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-Volume bzw. Protokoll-Volume. Ein Snapshot eines Protokollvolumes erfolgt direkt nach einem Snapshot eines Datenbank-Datenvolumes. Sie können einen Filter anwenden, wenn Sie nach einem bestimmten Backup in der Sicherungsliste suchen.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring Reports

Applications > Database Details

Database Details

NTAP Database Name	Protected Protection	my_full_bkup Policy Names	Database Type
172.30.137.142 Host Name	ANF Host Storage	Unreachable Database Version	zEHlu7vkdya8nujcxllbkKELKVXToyNcllents Connector Id
- Clones	- Parent Database	Disabled RMAN Catalog	- RMAN catalog repository

14 Backups

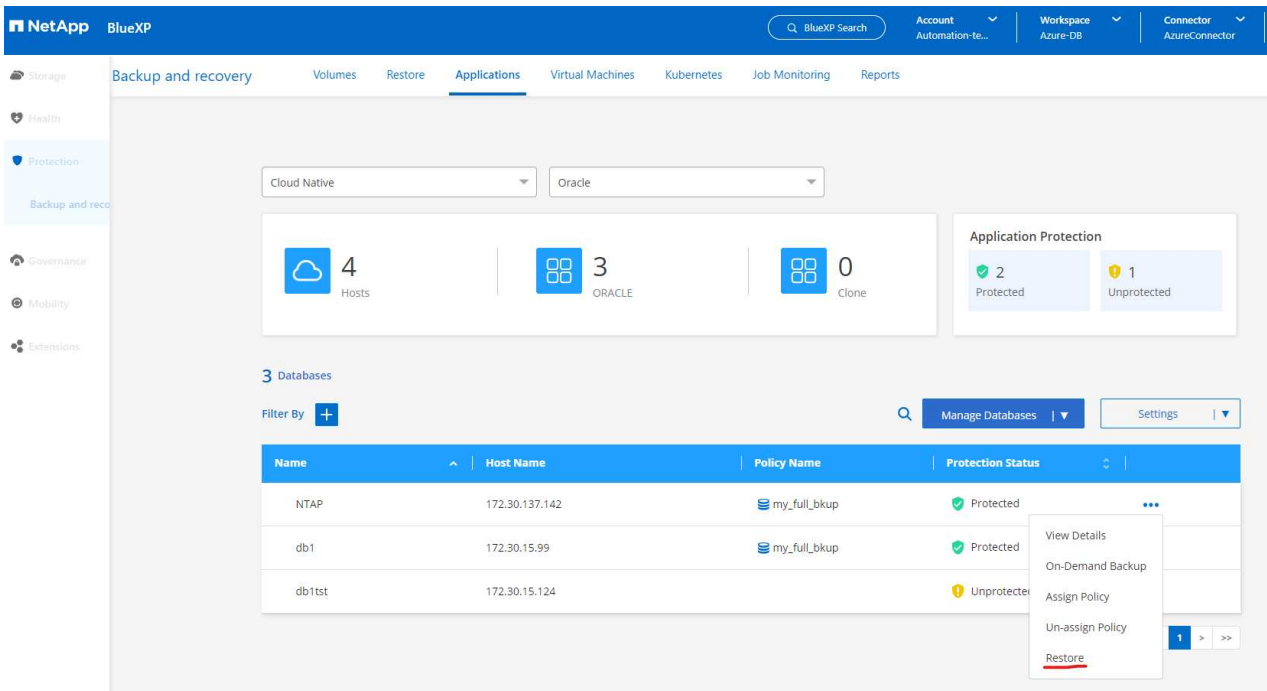
Filter By +

Select Timeframe

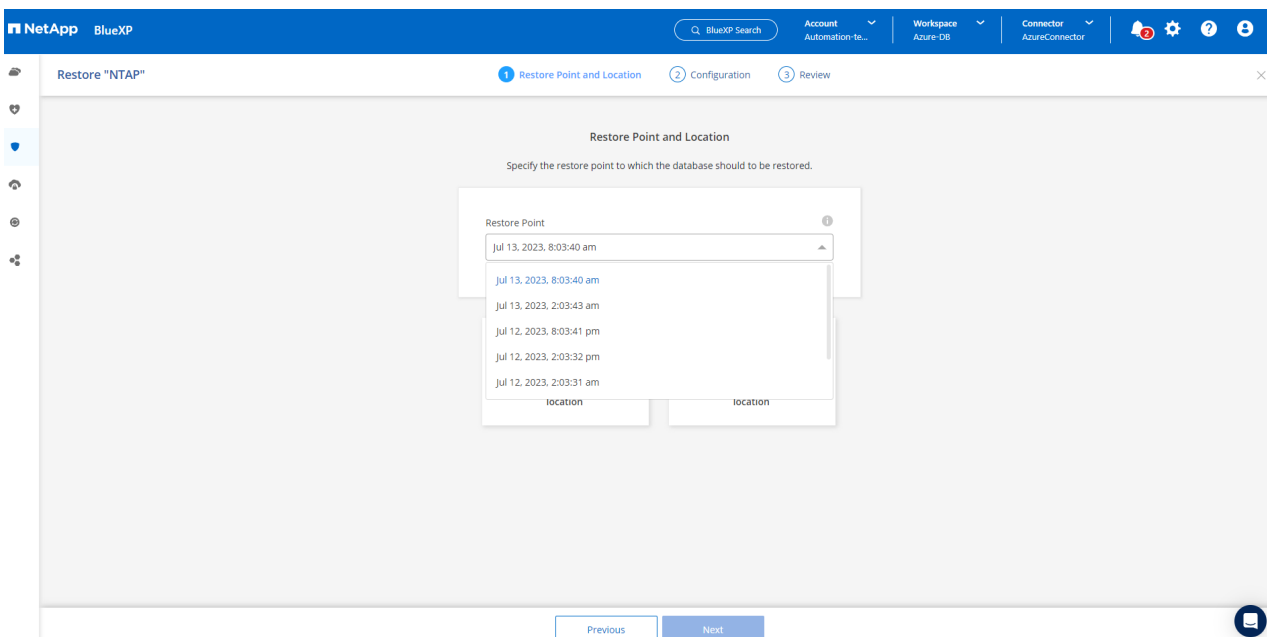
Backup Name	Backup Type	SCN	RMAN Catalog	Backup Time	
my_full_bkup_Hourly_NTAP_2023_07_13_12_04_28_8376...	Log	29192187	Not Cataloged	Jul 13, 2023, 8:06:22 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_4363...	Data	29192136	Not Cataloged	Jul 13, 2023, 8:03:40 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_04_28_5618...	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.

NetApp BlueXP

Restore "NTAP"

1 Restore Point and Location 2 Configuration 3 Review

Restore Point and Location

Specify the restore point to which the database should be restored.

Restore Point
Jul 13, 2023, 8:03:40 am

Restore to original location

Restore to alternate location

Previous Next

4. Definieren Sie Ihren Bereich *** Wiederherstellung*** und *** Wiederherstellungsumfang***. Alle Protokolle bedeuten eine vollständige Wiederherstellung auf dem neuesten Stand, einschließlich der aktuellen Protokolle.

NetApp BlueXP

Restore "NTAP"

1 Restore Point and Location 2 Configuration 3 Review

Restore Scope

☒ All Data Files
Data Files Restore

☐ Control Files
Control Files Restore

Database state will be changed if needed for restore and recovery.

Recovery Scope

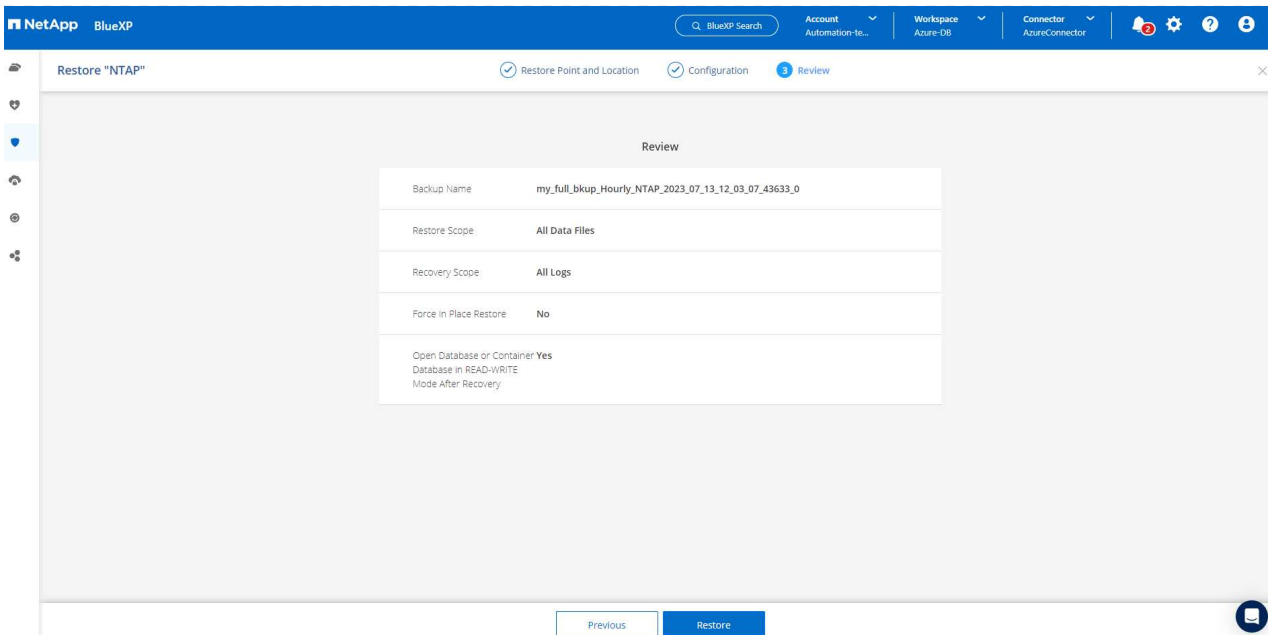
☒ All Logs ☐ Until System Change Number ☐ Date and Time ☐ No Recovery

External Archive log locations

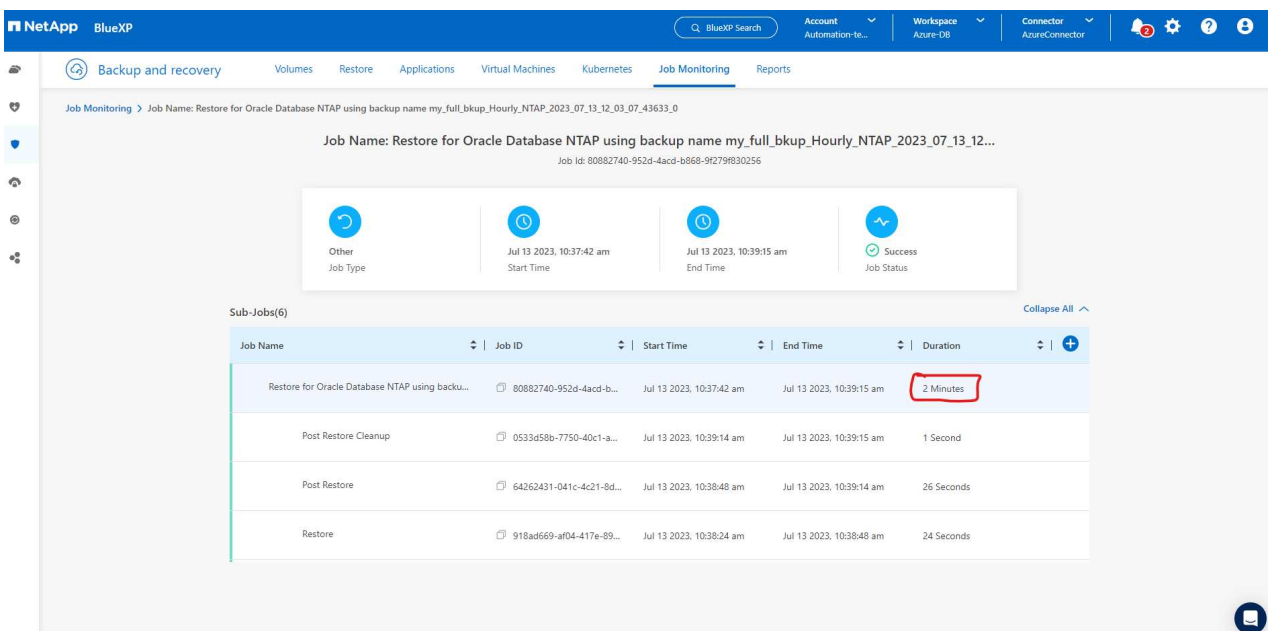
☒ Open the database or the container database in READ-WRITE mode after recovery.

Previous Next

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 links for 'Account', 'Workspace', and 'Connector'. The left sidebar shows various categories like 'Storage', 'Health', 'Protection', 'Governance', 'Mobility', and 'Extensions'. The main content area is titled 'Applications' and shows a summary of resources: 4 Cloud Native Hosts, 3 ORACLE, and 0 Clones. Below this, there's a section for '3 Databases' with a table listing them. The table has columns for Name, Host Name, Policy Name, and Protection Status. The databases listed are NTAP, db1, and db1tst. The 'db1tst' database is marked as '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).

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

2. Wählen Sie den **Wiederherstellungspunkt** und aktivieren Sie die Option **an alternativen Speicherort wiederherstellen**.

The screenshot shows the 'Restore "NTAP"' configuration page 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' shows 'Jul 13, 2023, 8:03:40 am'. Below this, there are two options: 'Restore to original location' and 'Restore to alternate location'. The 'Restore to alternate location' option is selected, indicated by a blue checkmark. At the bottom, there are 'Previous' and 'Next' buttons.

3. Legen Sie auf der nächsten Seite **Configuration** alternative **Host**, neue Datenbank **SID** und **Oracle Home** wie bei einer alternativen Azure VM konfiguriert fest.

The screenshot shows the 'Configuration' step in the NetApp BlueXP interface for restoring a database. The page title is 'Restore "NTAP"'. The navigation bar includes 'Restore Point and Location', 'Configuration' (active), and 'Review'. The main content area is titled 'Configuration' and contains a form with the following fields:

- Host:** 172.30.137.147
- SID:** NTAP1
- Oracle Home:** /u01/app/oracle/product/19.0.0/clone
- Database Credentials:** Optional, with a link to 'Add Credential'.
- Maximum storage throughput (MiB/s):** Optional, with a field 'Enter throughput (1-4500)'.

At the bottom, there are 'Previous' and 'Next' buttons.

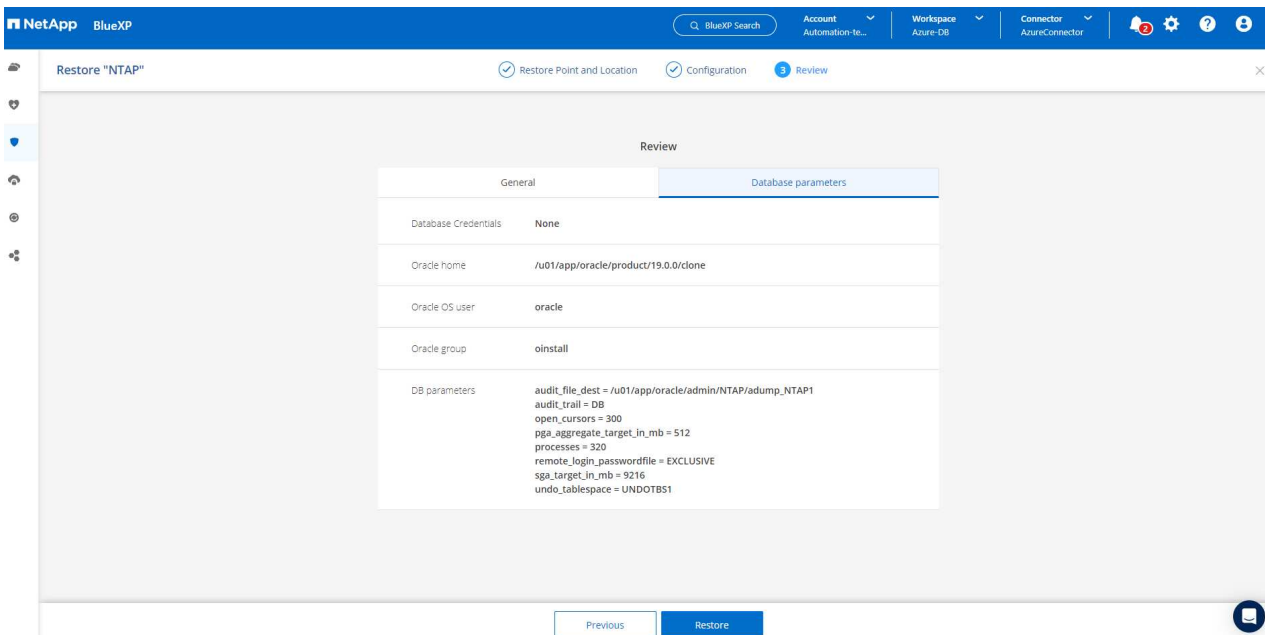
4. Die Seite Review **General** zeigt die Details der geklonten Datenbank wie SID, alternativer Host, Speicherort der Datendateien, Wiederherstellungsumfang usw.

The screenshot shows the 'Review' step in the NetApp BlueXP interface. The page title is 'Restore "NTAP"'. The navigation bar includes 'Restore Point and Location', 'Configuration', and 'Review' (active). The main content area is titled 'Review' and contains a table with the following data:

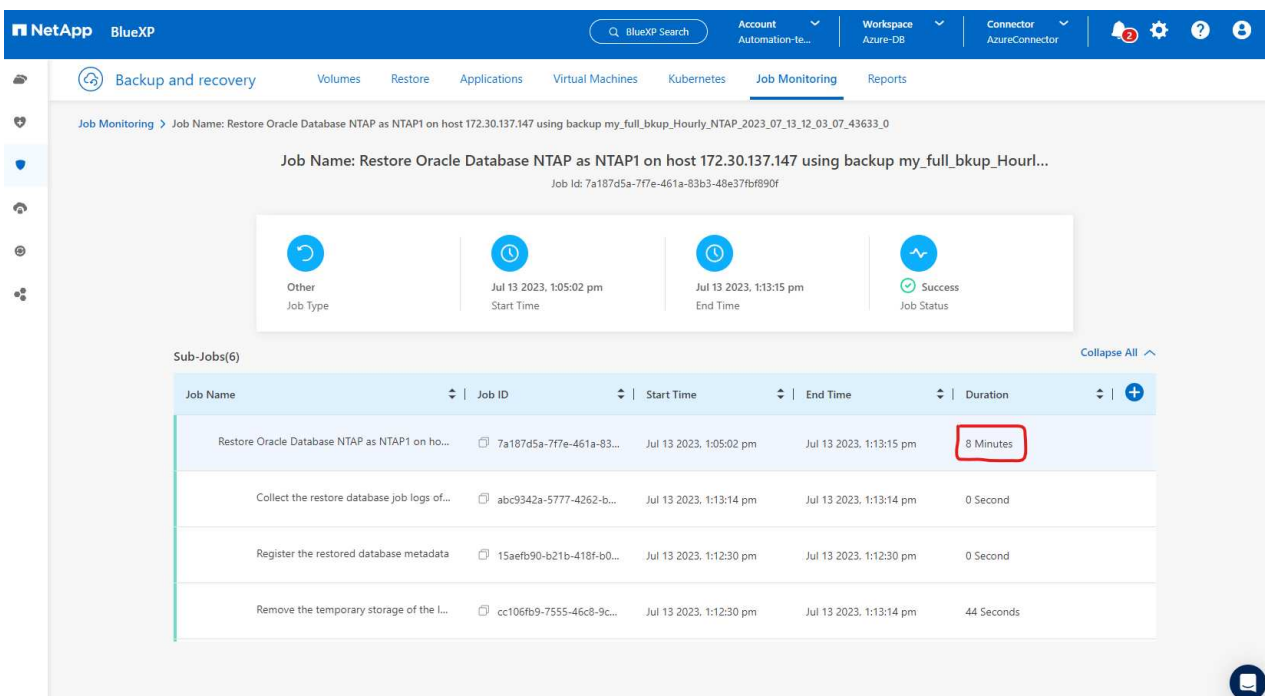
General	Database parameters
Backup Name	my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_43633_0
SID	NTAP1
Host	172.30.137.147
Datafile locations	/u02_NTAP1
Control files	/u02_NTAP1/NTAP1/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo03_01.log
Recovery scope	Until cancel using selected backup's archive logs
Recovery Point	Jul 13, 2023, 8:03:40 am
Location	Alternate Location

At the bottom, there are 'Previous' and 'Restore' buttons.

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 +

Manage Databases Settings

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 $ORACLE_SID are not allowed.
#
#
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
NTAP1:/u01/app/oracle/product/19.0.0/clone:N
[oracle@acao-ora02 admin]$ export ORACLE_SID=NTAP1
[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$database;

NAME          OPEN_MODE          LOG_MODE
-----
NTAP1         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 Konsoleneinstellung hinzugefügt.** um Amazon FSX for ONTAP zur BlueXP Arbeitsumgebung hinzuzufügen, sind in der BlueXP Konsoleneinstellung 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.

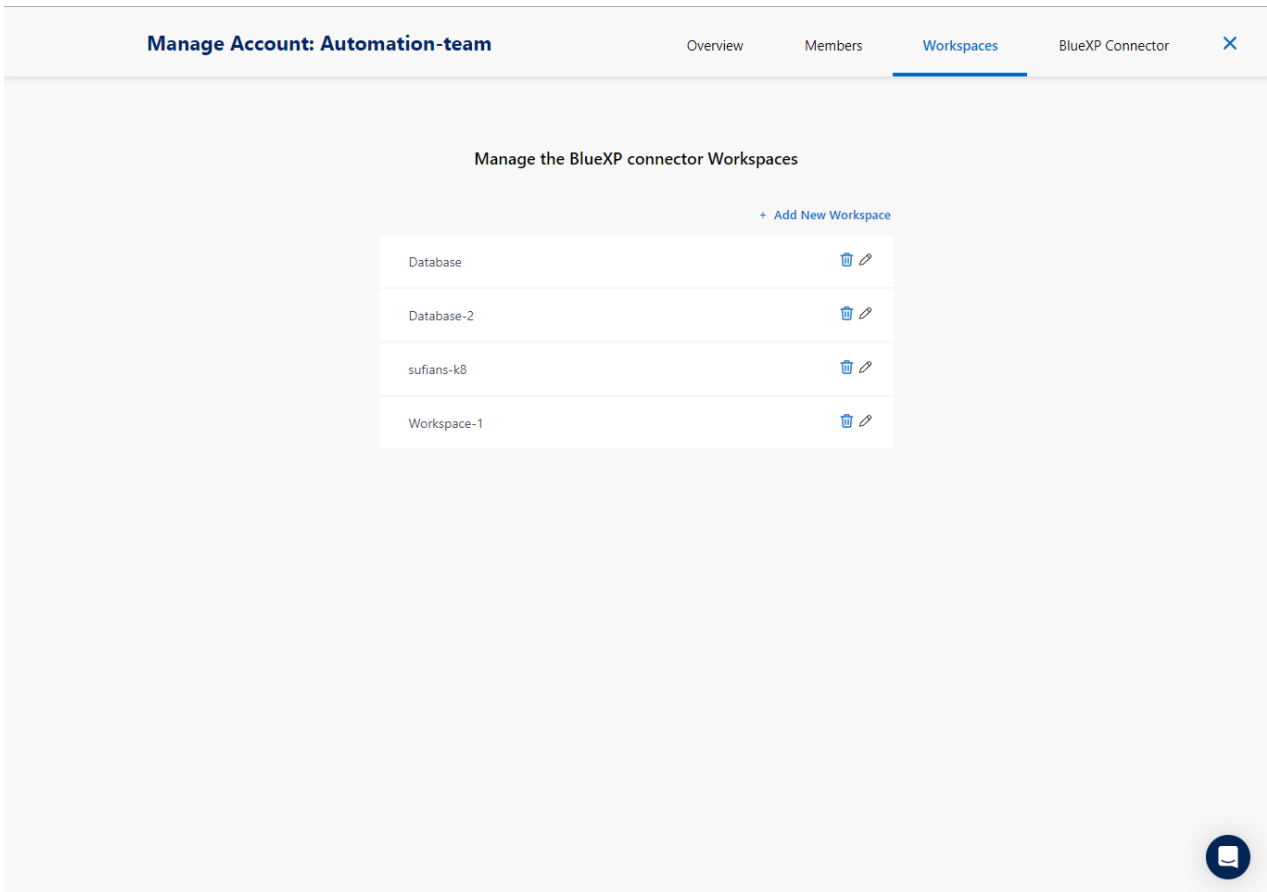
The screenshot displays the AWS IAM console interface. On the left, the 'Identity and Access Management (IAM)' sidebar is visible, with 'Policies' selected. The main content area shows the 'Summary' for the 'snapcenter' policy. The policy's ARN is 'arn:aws:iam::541696183547:policy/snapcenter' and its description is 'Policy to grant snapcenter service permission to create connector in AWS.' Below this, the 'Permissions' tab is active, showing a JSON string for the policy's statement. The JSON defines a policy with version '2012-10-17' and a single statement that allows a list of IAM and EC2 actions. The actions listed include iam:CreateRole, iam:DeleteRole, iam:PutRolePolicy, iam:CreateInstanceProfile, iam:DeleteRolePolicy, iam:AddRoleToInstanceProfile, iam:RemoveRoleFromInstanceProfile, iam:DeleteInstanceProfile, iam:PassRole, iam:ListRoles, ec2:DescribeInstanceStatus, ec2:RunInstances, ec2:ModifyInstanceAttribute, ec2:CreateSecurityGroup, ec2:DeleteSecurityGroup, ec2:DescribeSecurityGroups, ec2:RevokeSecurityGroupEgress, ec2:AuthorizeSecurityGroupEgress, ec2:AuthorizeSecurityGroupIngress, ec2:RevokeSecurityGroupIngress, ec2:CreateNetworkInterface, and 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.



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
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

- 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.

Add Connector - AWS

[More Information](#)

- 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

AKIA6JRXA6ZVGVF5HMO3

AWS Secret Key

.....

Want to launch an instance without AWS Credentials? [v](#)

[Previous](#)[Next](#)

2. Benennen Sie die Connector-Instanz und wählen Sie unter **Details** *Rolle erstellen.

Add Connector - AWS

[More Information](#)

- ✓ 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 - AWSMore Information ×

✓ AWS Credentials ✓ Details 3 Network 4 Security Group 5 Review

Network

Connectivity
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)
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
Example: http://172.16.254.1:8080
Define Credentials for this Proxy
Upload a root certificate

Previous Next

2. Stellen Sie die **Sicherheitsgruppe** für den Konnektor ein.

Add BlueXP Connector - AWS

More Information

✓ AWS Credentials

✓ Details

✓ Network

4 Security Group

5 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.

Add BlueXP Connector - AWS

More Information

✓ AWS Credentials

✓ Details

✓ Network

✓ Security Group

5 Review

Review

[Code for Terraform Automation](#)

BlueXP Connector Name	aws-snapctr-us-east
AWS Access Key	AKIAH4H43ZT56IWWR3TI
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.

The screenshot shows the AWS IAM console. On the left, the 'Identity and Access Management (IAM)' menu is open, and 'Roles' is selected. The main area displays a list of roles. The 'Create role' button is in the top right corner.

Role name	Trusted entities	Last activity
AmazonEC2RoleforAWSUser	AWS Service: ec2	-
AmazonSSMRoleforInstancesQuickSetup	AWS Service: ec2	156 days ago
aws-controltower-AdministratorExecutionRole	Account: 982617961887	-
aws-controltower-ConfigRecorderRole	AWS Service: config	-
aws-controltower-ForwardNotificationRole	AWS Service: lambda	2 days ago
aws-controltower-ReadOnlyExecutionRole	Account: 982617961887	-
AWS-QuickSetup-StackSet-Local-AdministrationRole	AWS Service: cloudformation	154 days ago
AWS-QuickSetup-StackSet-Local-ExecutionRole	Account: 541696183547	154 days ago
AWSControlTowerExecution	Account: 292306980405	232 days ago
AWSReservedSSO_AWSAdministratorAccess_3d8eb05a699802fa	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	26 days ago
AWSReservedSSO_AWSOrganizationalAccess_Mock3e725667e253	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_AWSPowerUserAccess_509f0a0f6a4ed1	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_AWSReadOnlyAccess_23434b7b71bb11d	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_SAA-Dev-ReadOnly_Ib8e11a983e811e7	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-

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.

The screenshot shows the 'Select trusted entity' page in the AWS IAM console. The 'Trusted entity type' section has 'AWS account' selected. Under 'An AWS account', 'Another AWS account' is selected, and the 'Account ID' is '992013314444'. The 'Options' section has 'Require external ID' and 'Require MFA' checked.

Trusted entity type

- ☐ AWS service: Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☒ AWS account: Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web Identity: Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation: Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy: Create a custom trust policy to enable others to perform actions in this account.

An AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- ☐ This account (541696183547)
- ☒ Another AWS account
 - Account ID:
 - Identifier of the account that can use this role
 - Account ID is a 12-digit number.

Options

- ☒ Require external ID (Best practice when a third party will assume this role)
- ☒ Require MFA: Requires that the assuming entity use multi-factor authentication.

Cancel Next

3. Filtern Sie Berechtigungsrichtlinien nach fsx und fügen Sie der Rolle **Berechtigungsrichtlinien** hinzu.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (Selected 1/889) Info
Choose one or more policies to attach to your new role.

Q Filter policies by property or policy name and press enter. 4 matches

'fsx' X Clear filters

	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.

Cancel Previous **Next**

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**.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
fsxn_bluexp
Maximum 64 characters. Use alphanumeric and "+-,@,_" characters.

Description
Add a short explanation for this role.
Grant permission for BlueXP access to FSxN in AWS.
Maximum 1000 characters. Use alphanumeric and "+-,@,_" characters.

Step 1: Select trusted entities Edit

```

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.

NetApp BlueXP

BlueXP Search Account Automation-te... Workspace Database-2 Connector acio-aws conn...

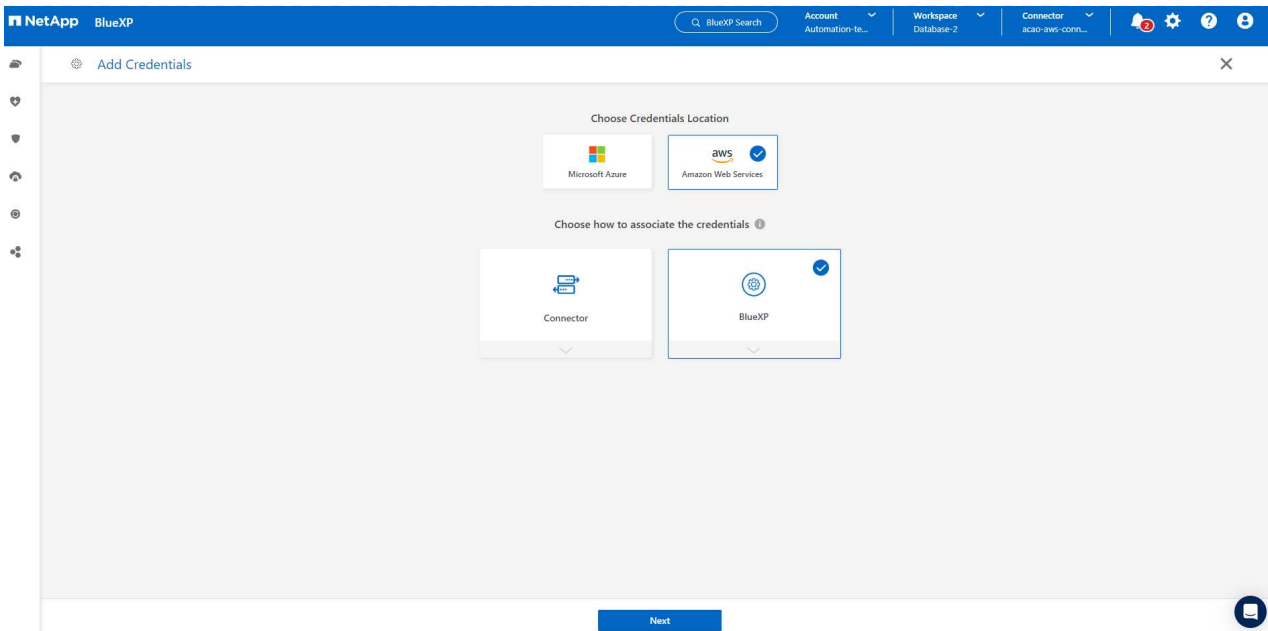
Credentials **Account credentials** User credentials

BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.

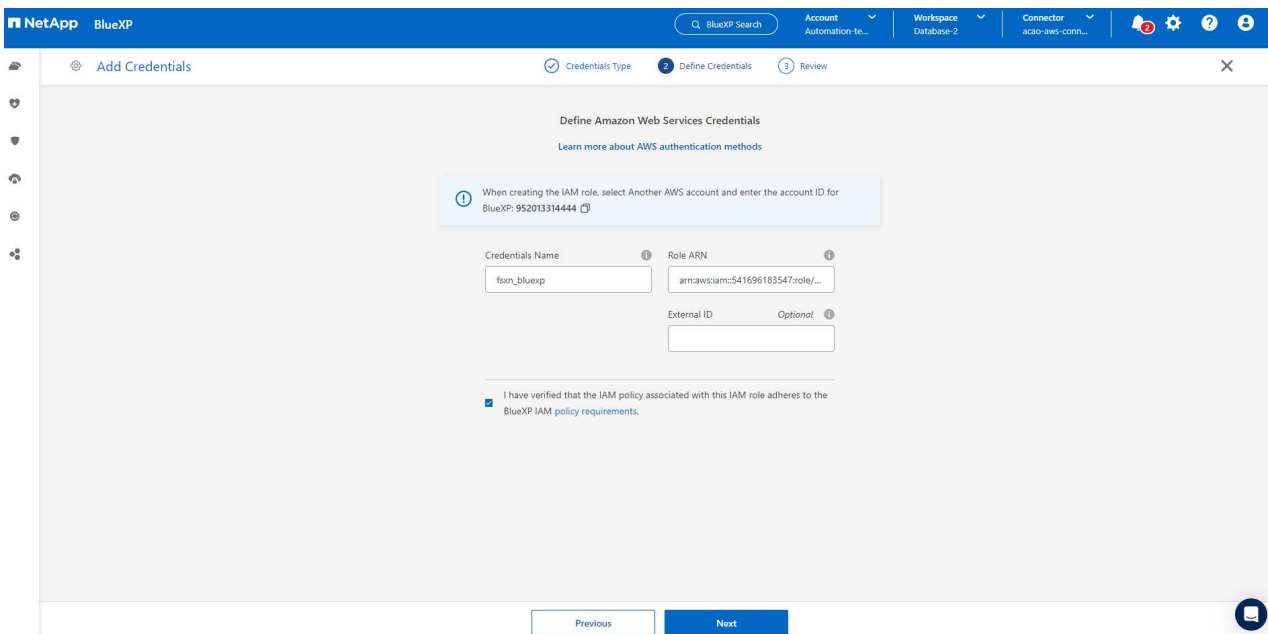
5 Credentials Add credentials

Account	Type	Role
shantanucreds	Assume Role	BlueXP
210811600188	AWS Account ID	nkanthik_kafka_mfs_role_FSxN
		Assume Role

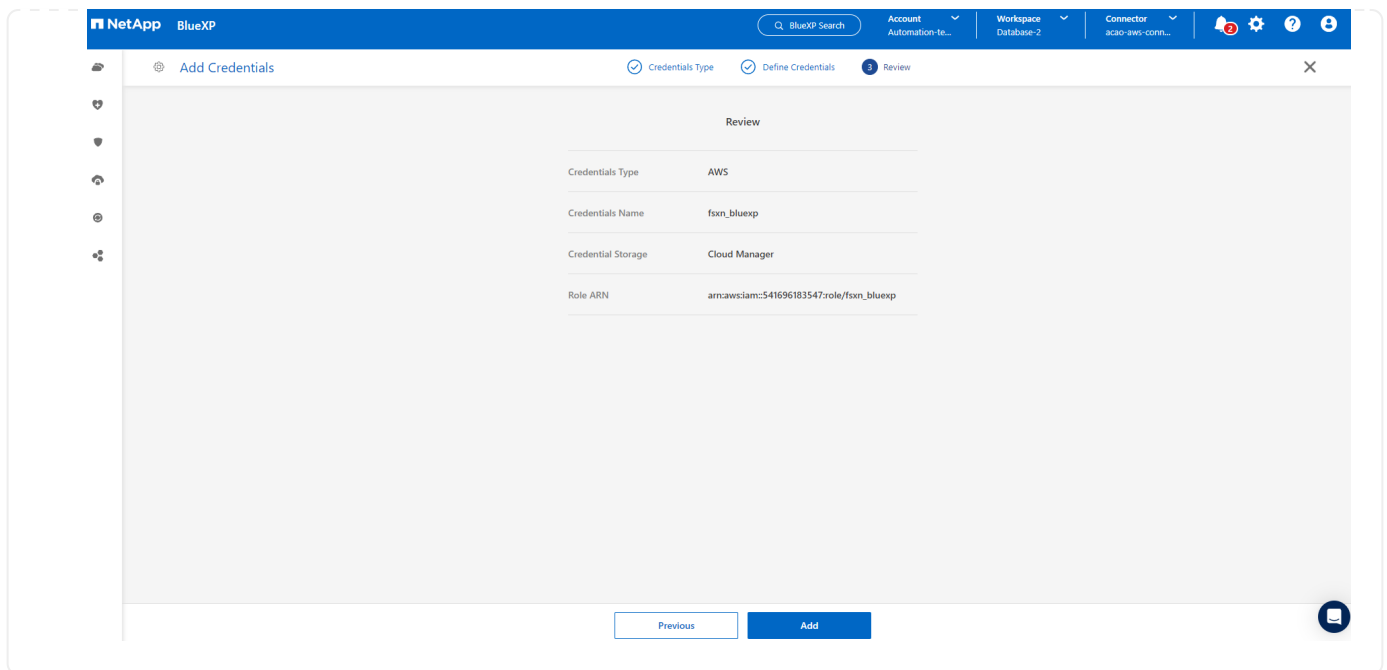
6. Wählen Sie den Anmeldeinformationsspeicherort als **- Amazon Web Services - BlueXP**.



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.



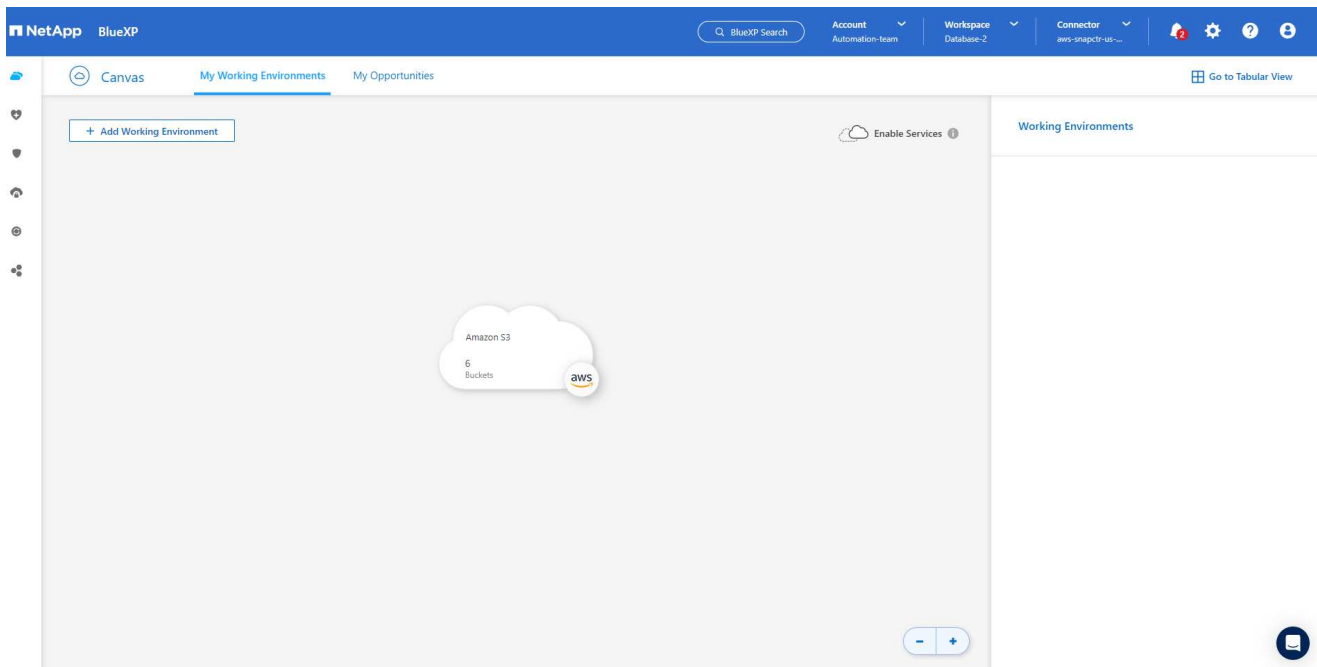
8. Bewertung und **Hinzufügen**.



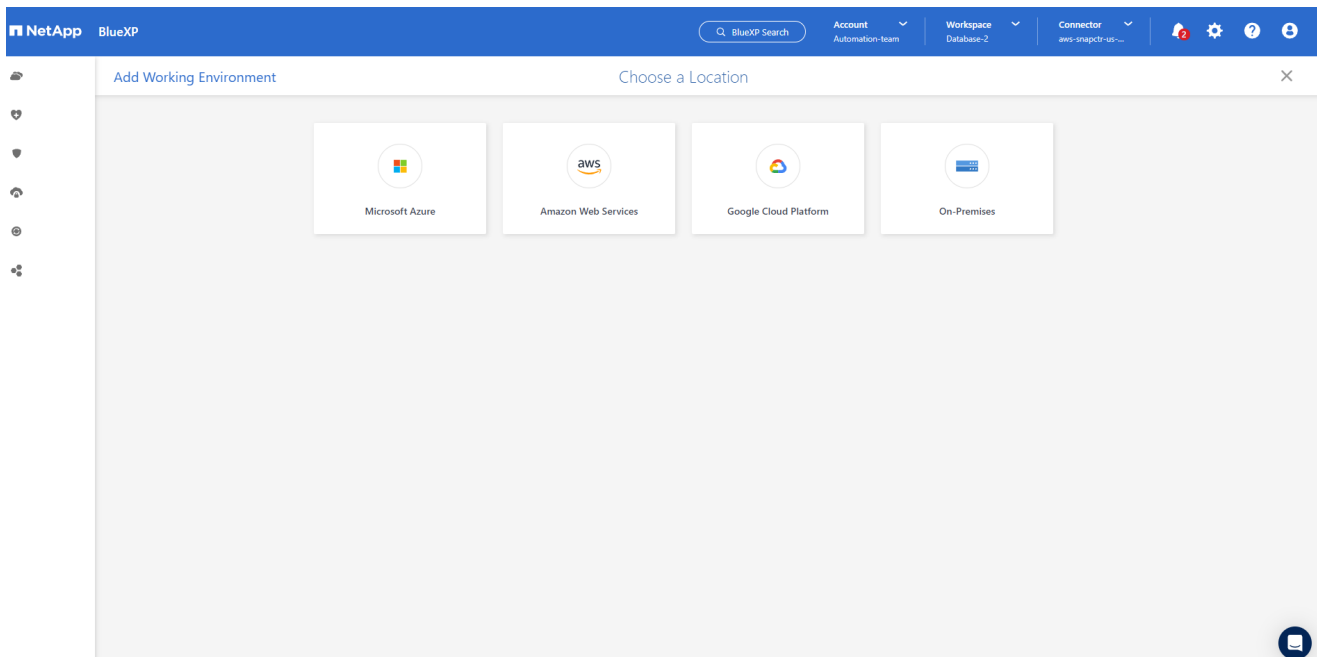
Einrichtung der SnapCenter Services

Wenn der Connector bereitgestellt und die Zugangsdaten hinzugefügt wurden, können SnapCenter-Services jetzt wie folgt eingerichtet werden:

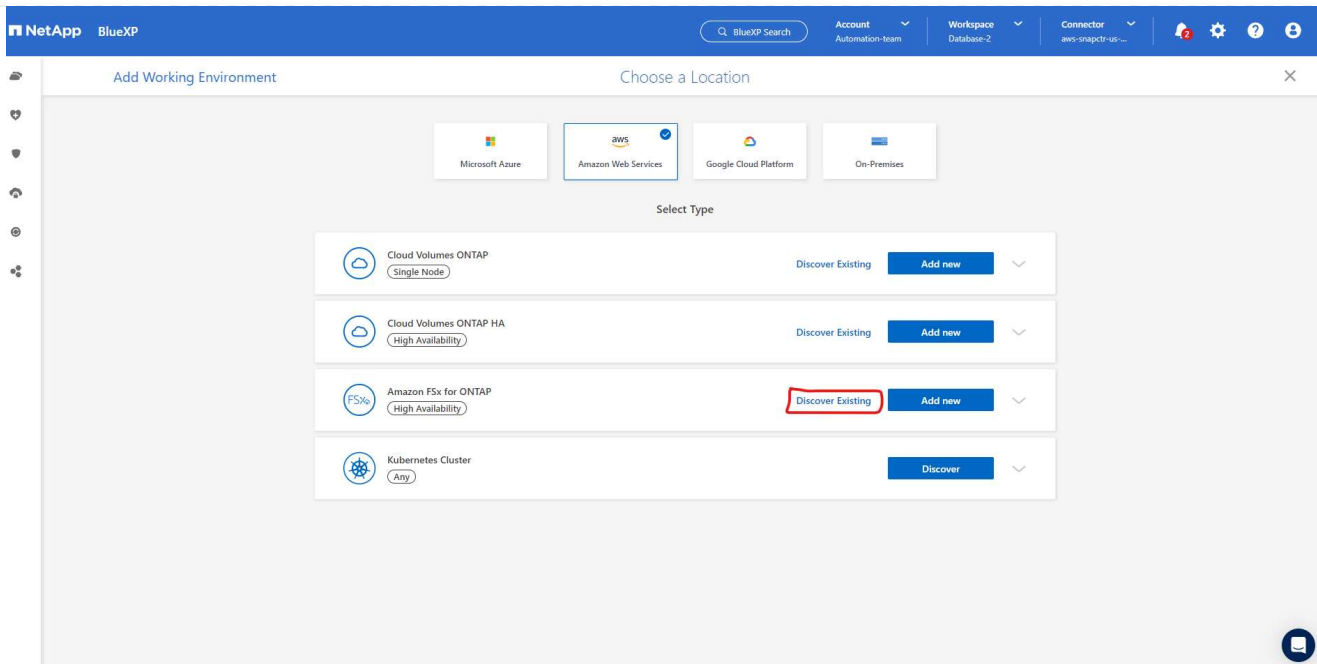
1. Klicken Sie unter **Meine Arbeitsumgebung** auf **Arbeitsumgebung hinzufügen**, um FSX in AWS bereitzustellen.



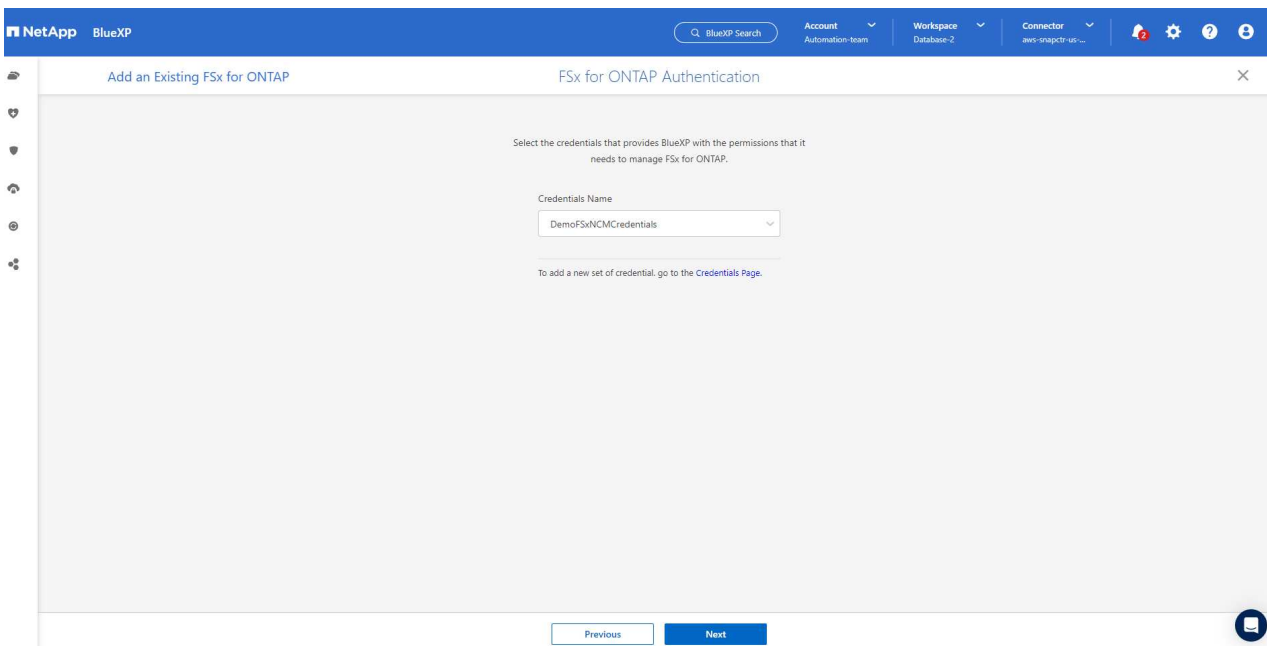
1. Wählen Sie **Amazon Web Services** als Speicherort.



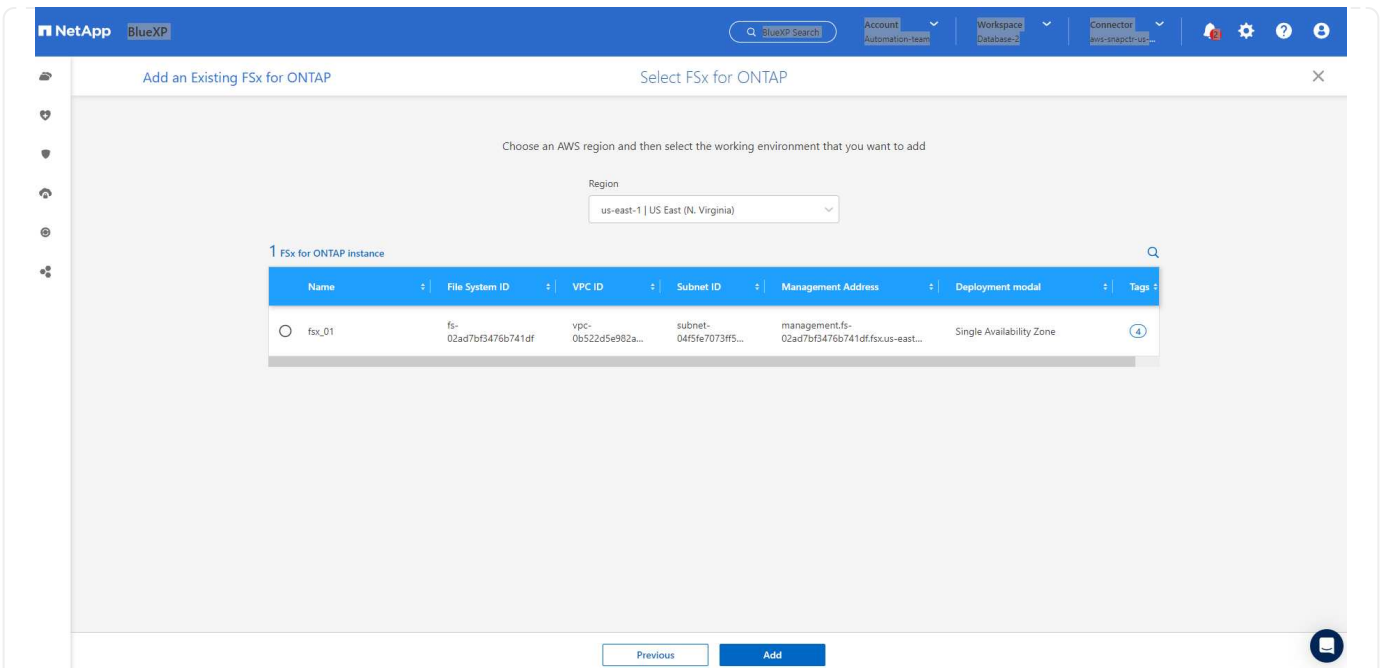
1. Klicken Sie neben **Amazon FSX for ONTAP** auf **existing** entdecken.



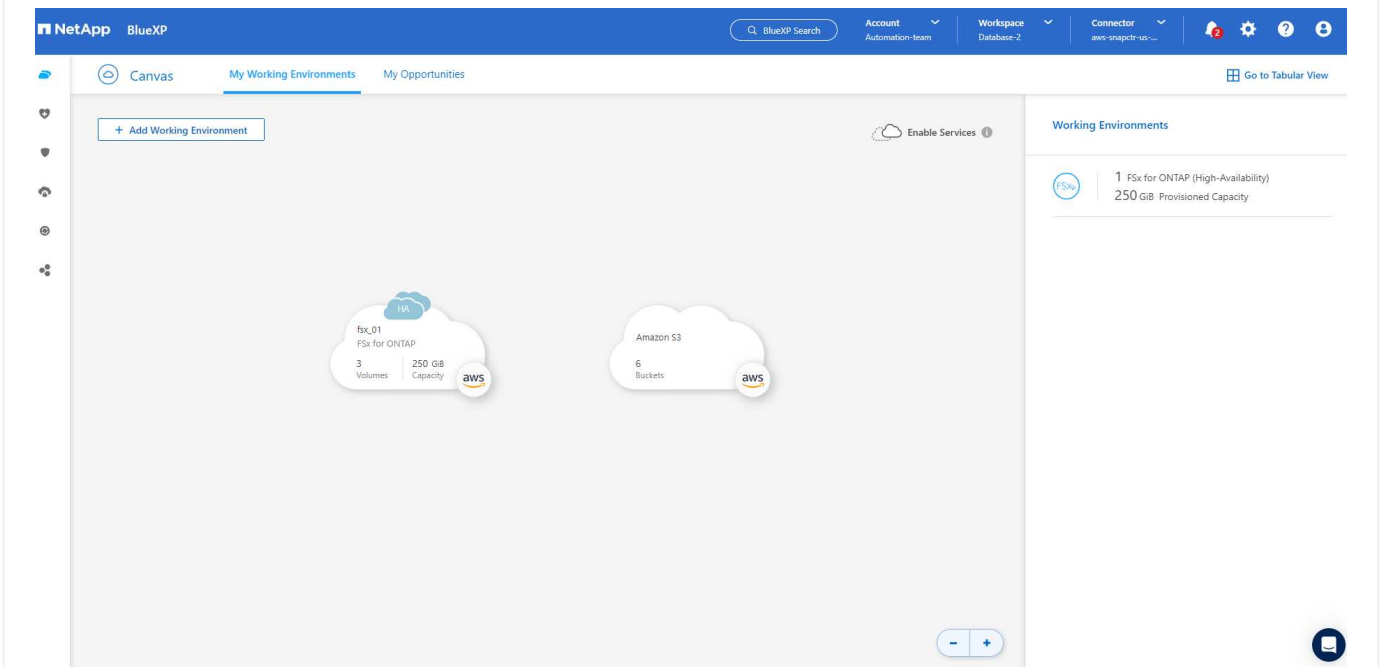
1. Wählen Sie den **Zugangsdaten-Namen** aus, den Sie im vorherigen Abschnitt erstellt haben, um BlueXP die Berechtigungen zu erteilen, die es benötigt, um FSx for ONTAP zu verwalten. Wenn Sie keine Zugangsdaten hinzugefügt haben, können Sie diese über das Menü **Einstellungen** oben rechts in der BlueXP Konsole hinzufügen.



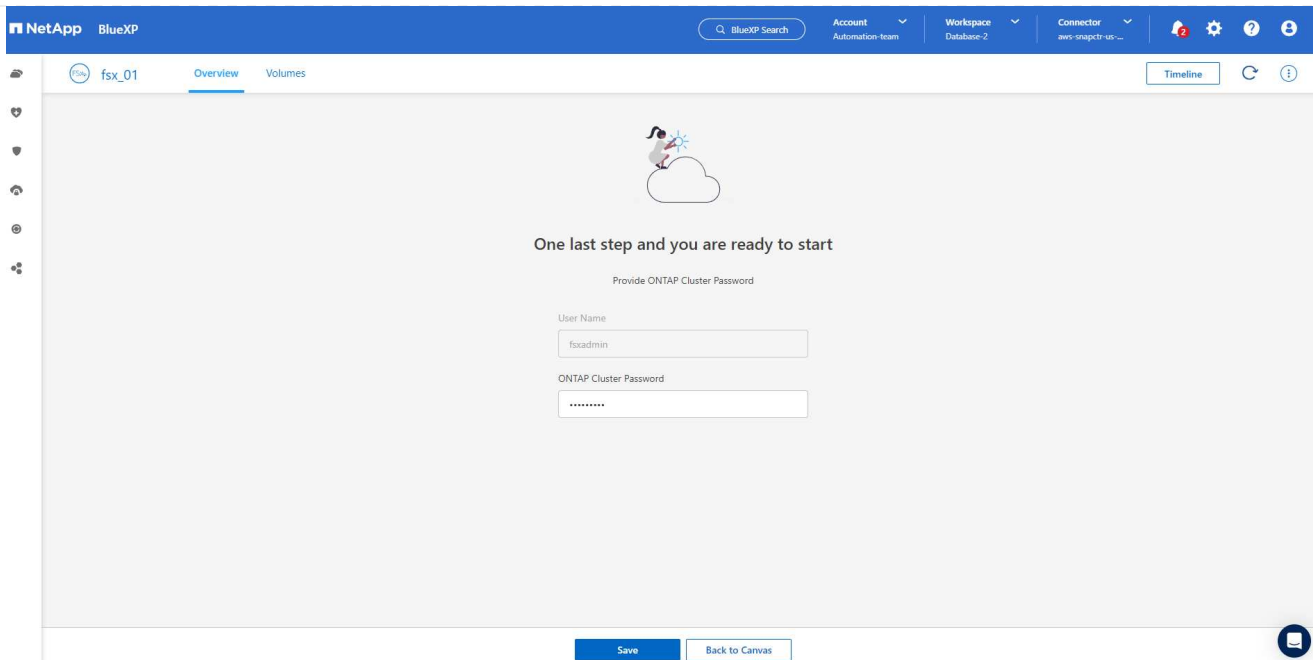
2. Wählen Sie die AWS-Region aus, in der Amazon FSX for ONTAP bereitgestellt wird, wählen Sie den FSX-Cluster aus, der die Oracle-Datenbank hostet, und klicken Sie auf Hinzufügen.



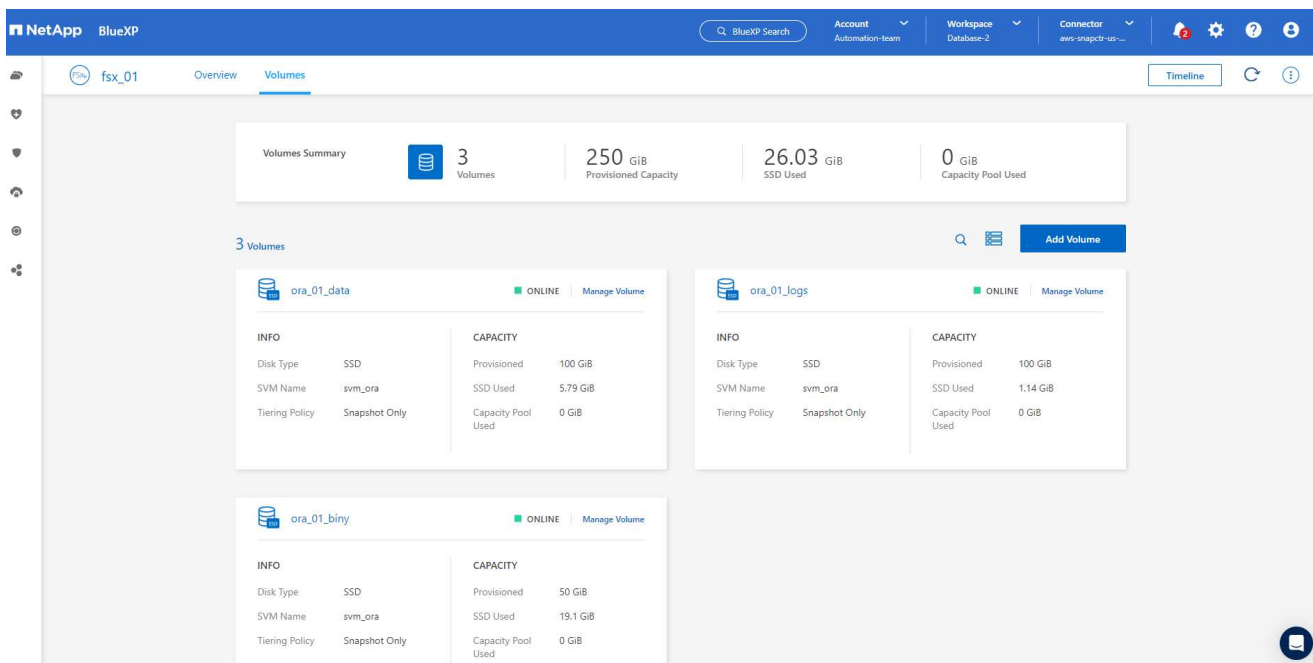
1. Die entdeckte Amazon FSX for ONTAP-Instanz erscheint jetzt in der Arbeitsumgebung.



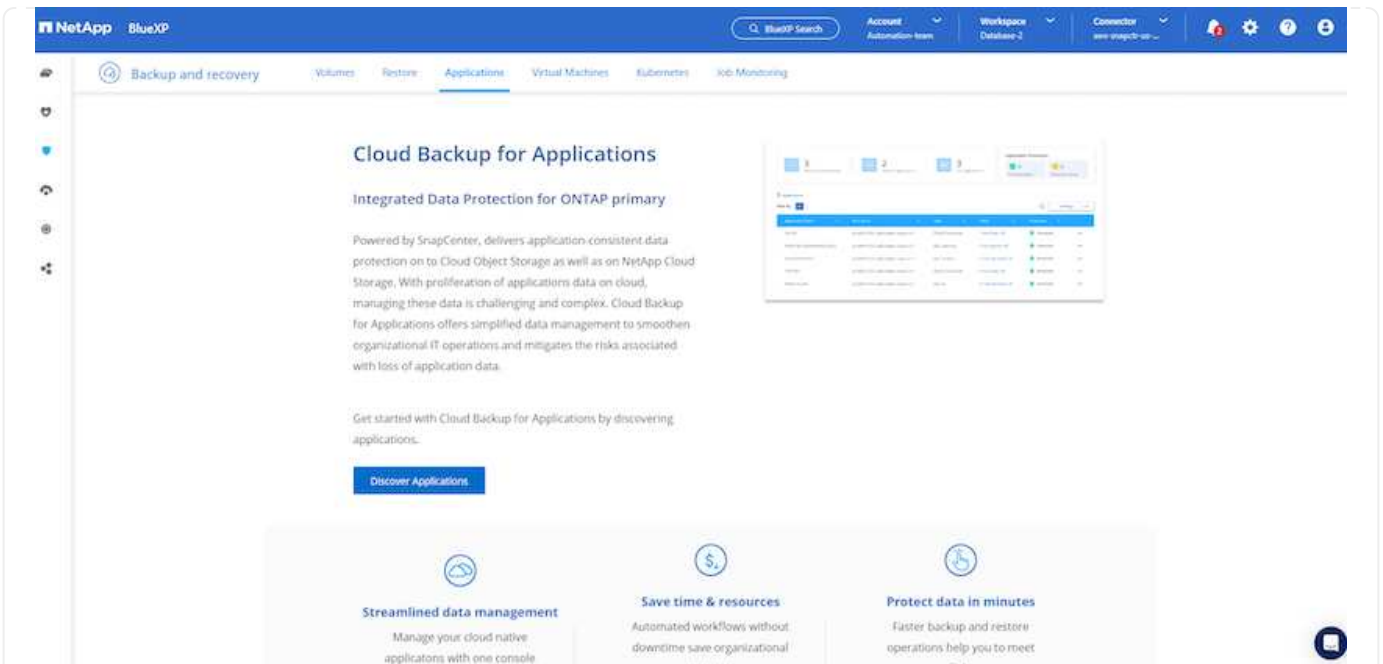
1. Sie können sich mit Ihren fsxadmin-Anmeldeinformationen im FSX-Cluster anmelden.



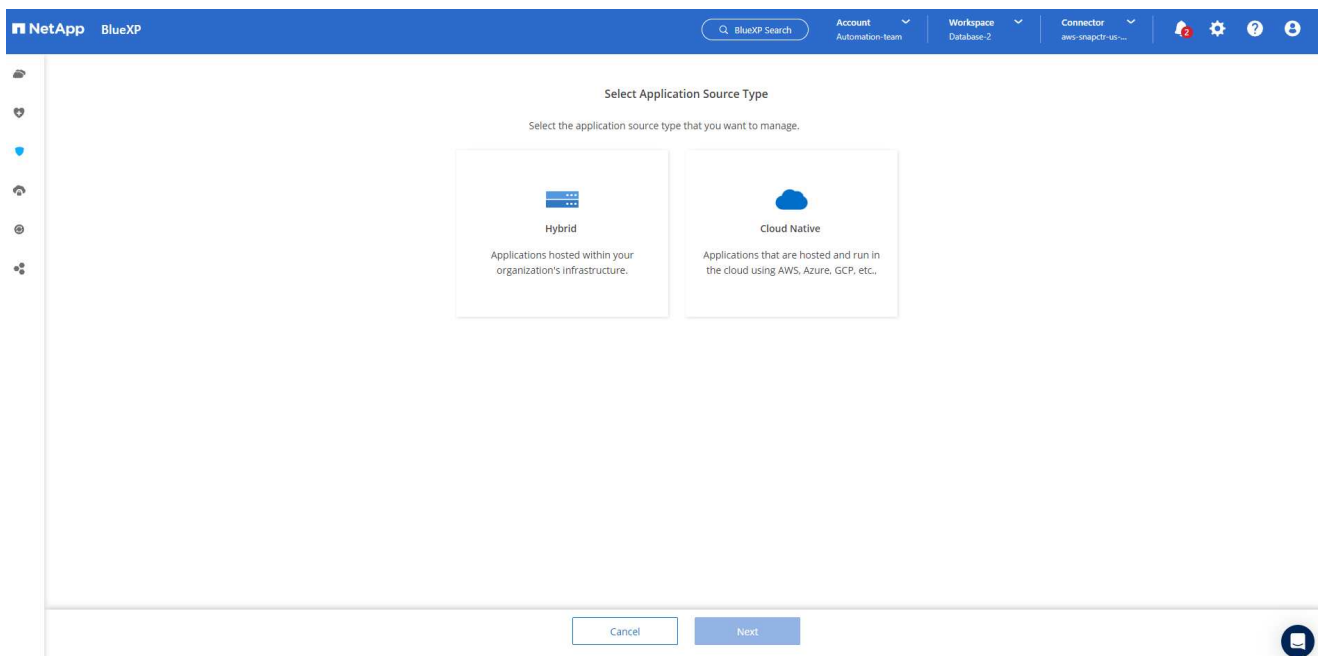
1. Nachdem Sie sich bei Amazon FSX for ONTAP angemeldet haben, prüfen Sie Ihre Informationen zum Datenbank-Storage (z. B. Datenbank-Volumes).



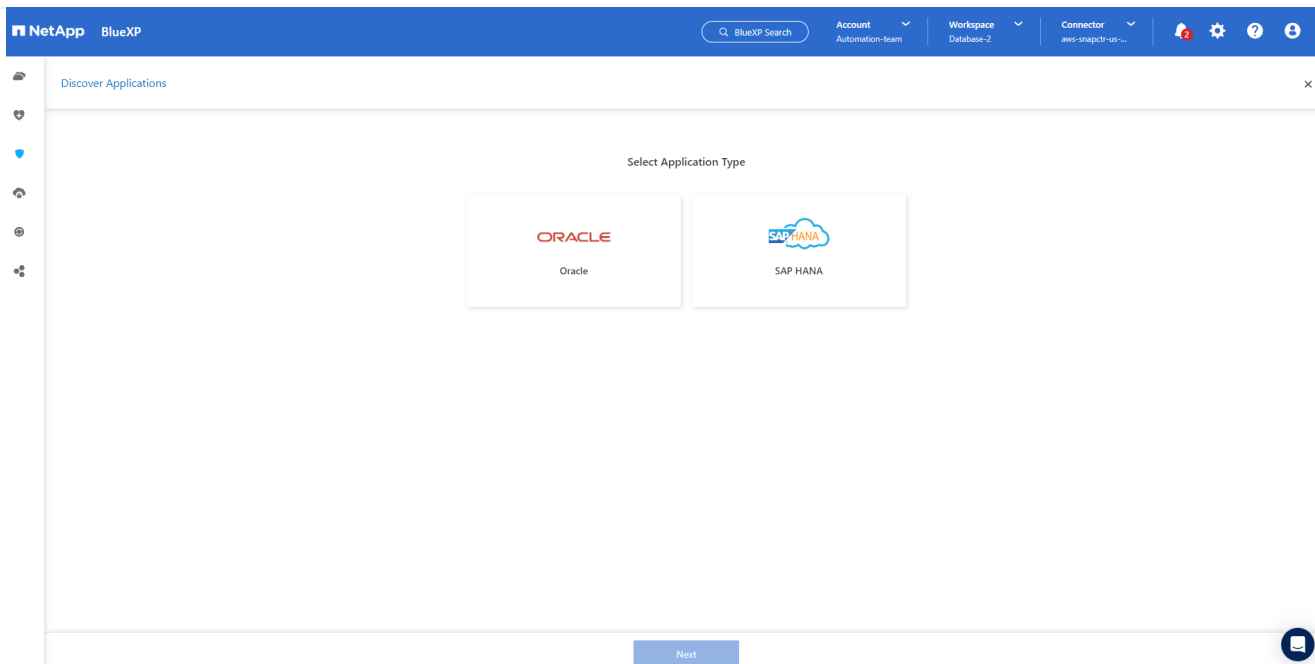
1. Bewegen Sie in der linken Seitenleiste der Konsole Ihre Maus über das Schutzsymbol und klicken Sie dann auf **Schutz > Anwendungen**, um die Startseite der Anwendungen zu öffnen. Klicken Sie Auf **Anwendungen Entdecken**.



1. Wählen Sie **Cloud Native** als Quelltyp der Anwendung aus.

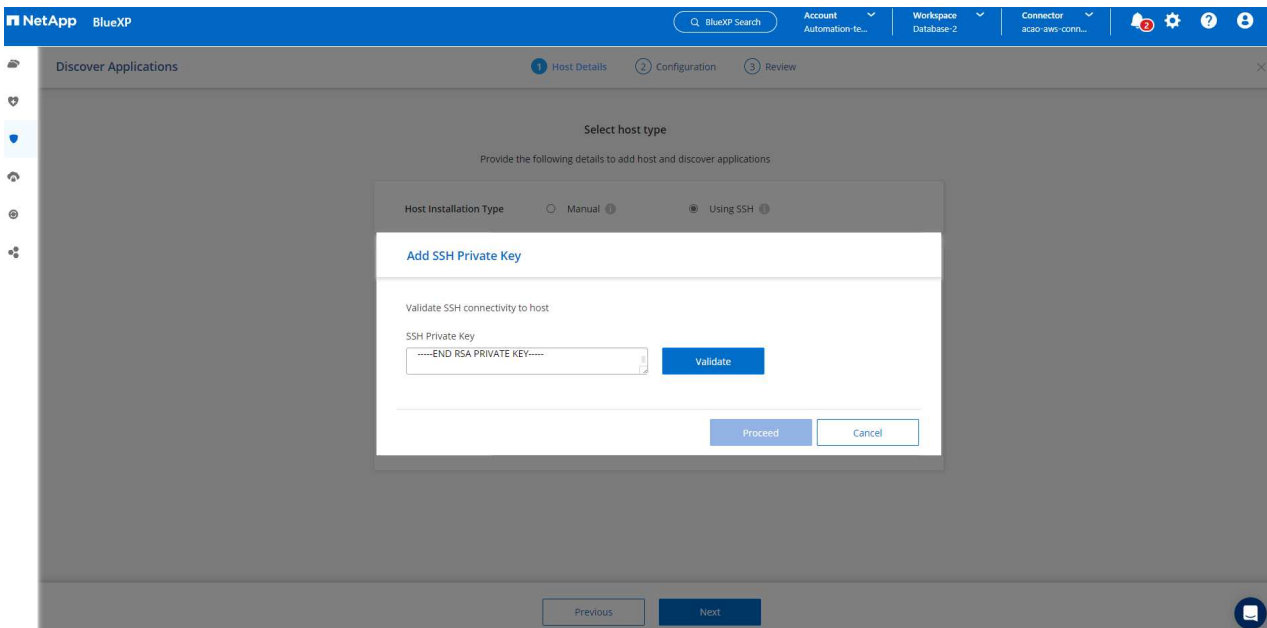


1. Wählen Sie **Oracle** für den Anwendungstyp.

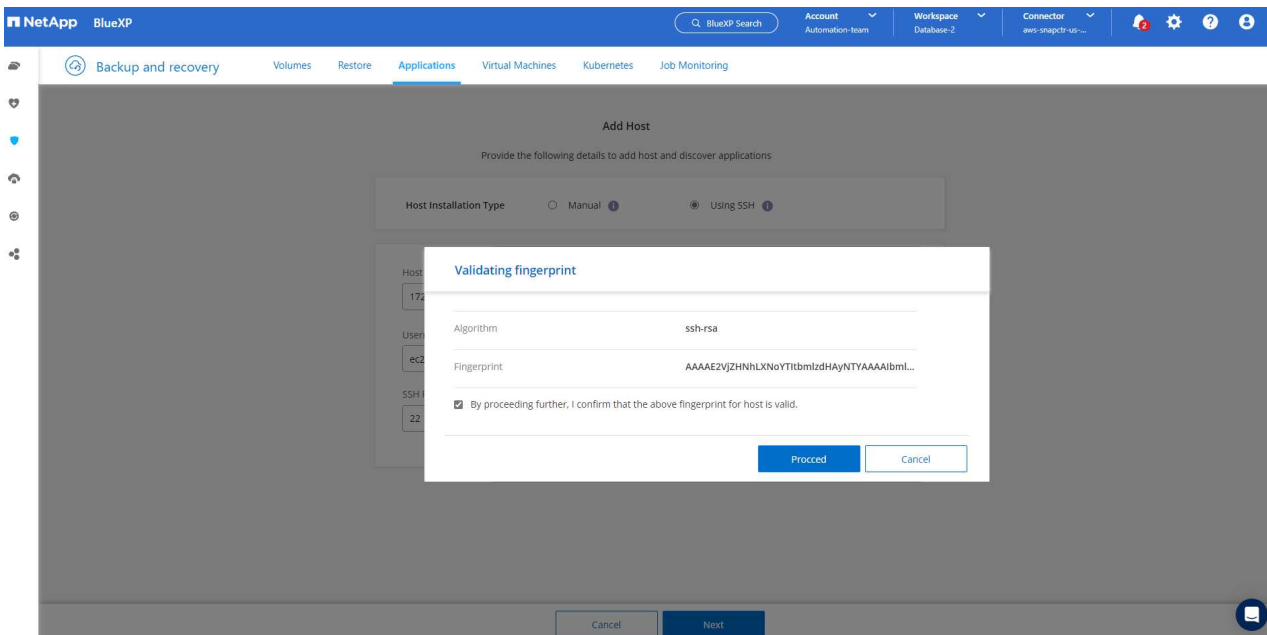


1. Geben Sie Details zum Host der AWS EC2 Oracle Applikation ein. Wählen Sie **mit SSH** als **Host-Installationstyp** für eine schrittweise Plugin-Installation und Datenbankerkennung. Klicken Sie dann auf **SSH Private Key** hinzufügen.

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.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

Cloud Native Oracle

1 Hosts 1 ORACLE 0 Clone

Application Protection

0 Protected 1 Unprotected

1 Databases

Filter By +

Manage Databases Settings

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

1 - 1 of 1

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. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. Below the navigation bar, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows '1 Hosts', '1 ORACLE', and '0 Clone'. An 'Application Protection' section shows '0 Protected' and '1 Unprotected'. A table lists databases with columns: 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: Policies, About, and Hosts.

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

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 'Policies' page. The top navigation bar is the same as the previous screenshot. Below the navigation bar, there are filters for 'Cloud Native' and 'Oracle'. A 'Create Policy' button is visible. A table lists policies with columns: Policy Name, Backup Type, and Schedules and Retention. The table shows four policies: 'Oracle Full Backup for Bronze', 'Oracle Full Backup for Gold', 'Oracle Full Backup for Silver', and 'my_full_bkup'. Each policy has a 'FullBackup' type and specific schedules and retention settings. A 'Settings' dropdown menu is open, showing options: Policies, About, and Hosts.

Policy Name	Backup Type	Schedules and Retention
Oracle Full Backup for Bronze	FullBackup	Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov
Oracle Full Backup for Gold	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 16 copies Daily: Repeats Every 1 Day, Keeps 30 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov
Oracle Full Backup for Silver	FullBackup	Hourly: Repeats Every 12 Hrs, Keeps 6 copies Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov
my_full_bkup	FullBackup	Hourly: Repeats Every 1 Hr, Keeps 3 Days

1. Wenn Sie mit der Richtlinienkonfiguration zufrieden sind, können Sie die gewünschte Richtlinie zum Schutz der Datenbank zuweisen.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' section displays a summary for 'Cloud Native' and 'Oracle' environments. Below this, a table lists databases. The database 'db1' is shown with a protection status of 'Unprotected'. A context menu is open over the 'Unprotected' status, with the 'Assign Policy' option highlighted.

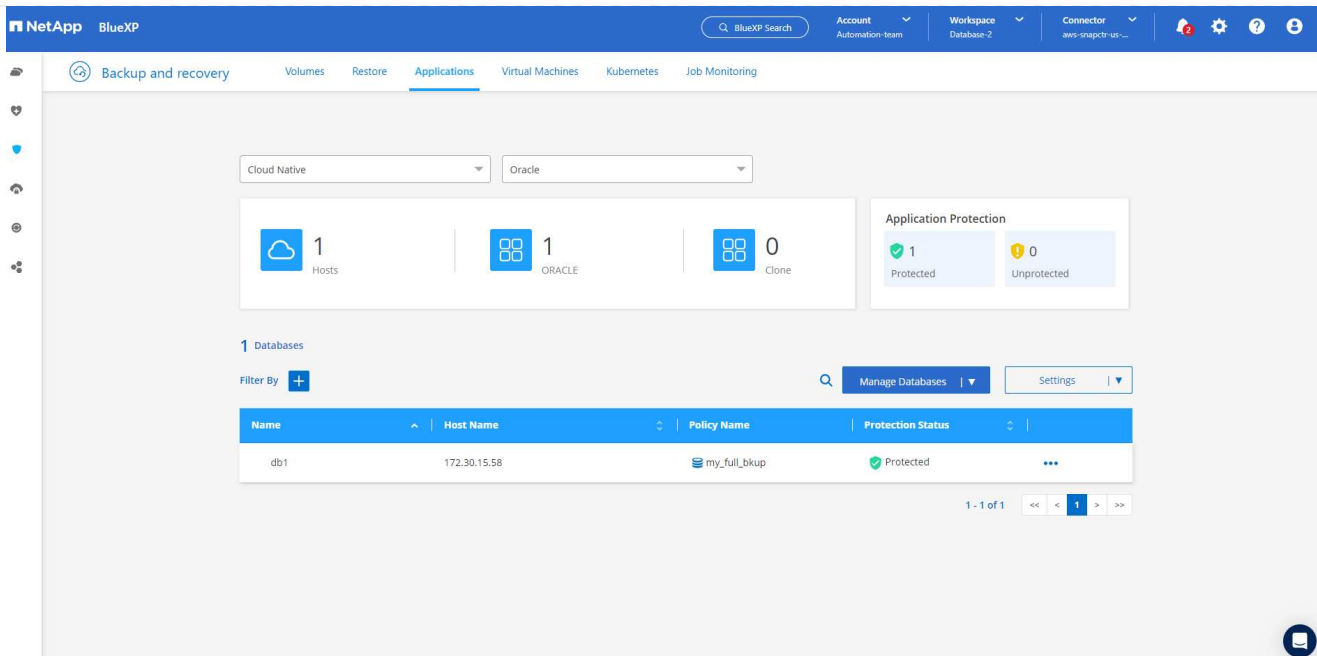
Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

1. Wählen Sie die Richtlinie aus, die der Datenbank zugewiesen werden soll.

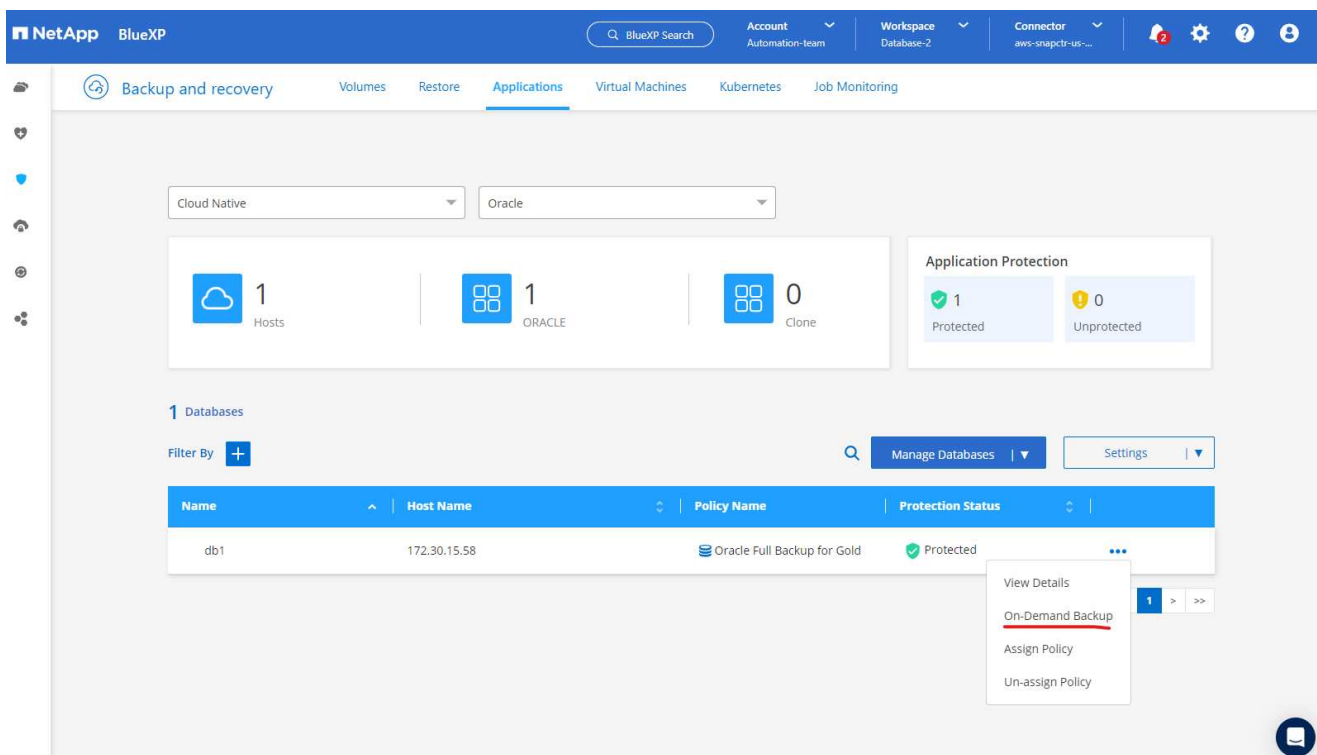
The screenshot shows the 'Assign Policy' dialog in the NetApp BlueXP interface. The dialog title is 'Assign Policy' with a subtitle 'Assign a policy to start taking backups of the database "db1"'. It displays a list of 4 policies. The policy 'my_full_bkup' is selected with a blue checkmark. At the bottom, there are 'Cancel' and 'Assign' buttons.

Policy Name	Backup Type	Schedules
<input type="radio"/> Oracle Full Backup for Bronze	FullBackup	Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input type="radio"/> Oracle Full Backup for Gold	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 16 copies Daily: Repeats Every 1 Day, Keeps 30 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input type="radio"/> Oracle Full Backup for Silver	FullBackup	Hourly: Repeats Every 12 Hrs, Keeps 6 copies Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
<input checked="" type="radio"/> my_full_bkup	FullBackup	Hourly: Repeats Every 1 Hr, Keeps 3 Days

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-Volume als auch für Protokoll-Volume ab. Ein Snapshot eines Protokollvolumes erfolgt direkt nach einem Snapshot eines Datenbank-Volumes. Sie können einen Filter anwenden, wenn Sie nach einem bestimmten Backup in einer langen Liste suchen.

NetApp
BlueXP

BlueXP Search

Account
Automation-team

Workspace
Database-2

Connector
aws-snapctr-us-...

Backup and recovery
Volumes
Restore
Applications
Virtual Machines
Kubernetes
Job Monitoring

Applications > 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.

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		

6 Backups

Filter By + Select Timeframe

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.

Restore "db1"

1 Restore Settings 2 Review

Restore Settings

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

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

Previous Next

1. Überprüfen und starten Sie die Datenbank-Wiederherstellung und -Wiederherstellung.

NetApp BlueXP

Q BlueXP Search

Account Automation-team

Workspace Database-2

Connector aws-snapctr-us...

2

⚙

?

👤

Restore "db1"

Restore Settings

2 Review

Review

Backup Name

Oracle_Full_Backup_for_Gold_Weekl
y_db1_2023_03_24_19_11_51_51476_
0

Restore Scope

All Data Files

Recovery Scope

All Logs

Force In Place Restore

Yes

Open Database or Container
Database in READ-WRITE Mode
After Recovery

Yes

Previous

Restore

1. Auf der Registerkarte **Job-Überwachung** können Sie den Status des Wiederherstellungsjobs sowie alle Details anzeigen, während er ausgeführt wird.

NetApp BlueXP

Q BlueXP Search

Account Automation-team

Workspace Database-2

Connector aws-snapctr-us...

2

⚙

?

👤

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Job Monitoring

⌂

Last Updated

March 24 2023, 15:25:33

Advanced Search & Filtering

Timeframe: Last 24 Hours

Jobs(30)

Job ID

Type

Resource Name

Status

Job Name

Start Time

1fdca0bd-a9c8-45aa...

--

--

Success

Restore for Oracle Database db1 ...

Mar 24 2023, 3:16:28 pr

f6f4fe2d-3040-497f...

--

--

Success

Backup of db1 oracle database o...

Mar 24 2023, 3:11:51 pr

5e3299f5-29db-4dcc...

--

--

Success

Backup of db1 oracle database o...

Mar 24 2023, 2:10:03 pr

6da5e51e-1a79-4e7e...

--

--

Success

Initialize FullBackup backup of po...

Mar 24 2023, 2:10:01 pr

NetAppBlueXP

BlueXP Search

AccountAutomation team

WorkspaceDatabase-2

Connectoraws-snapctr-us-...

2

?

3

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

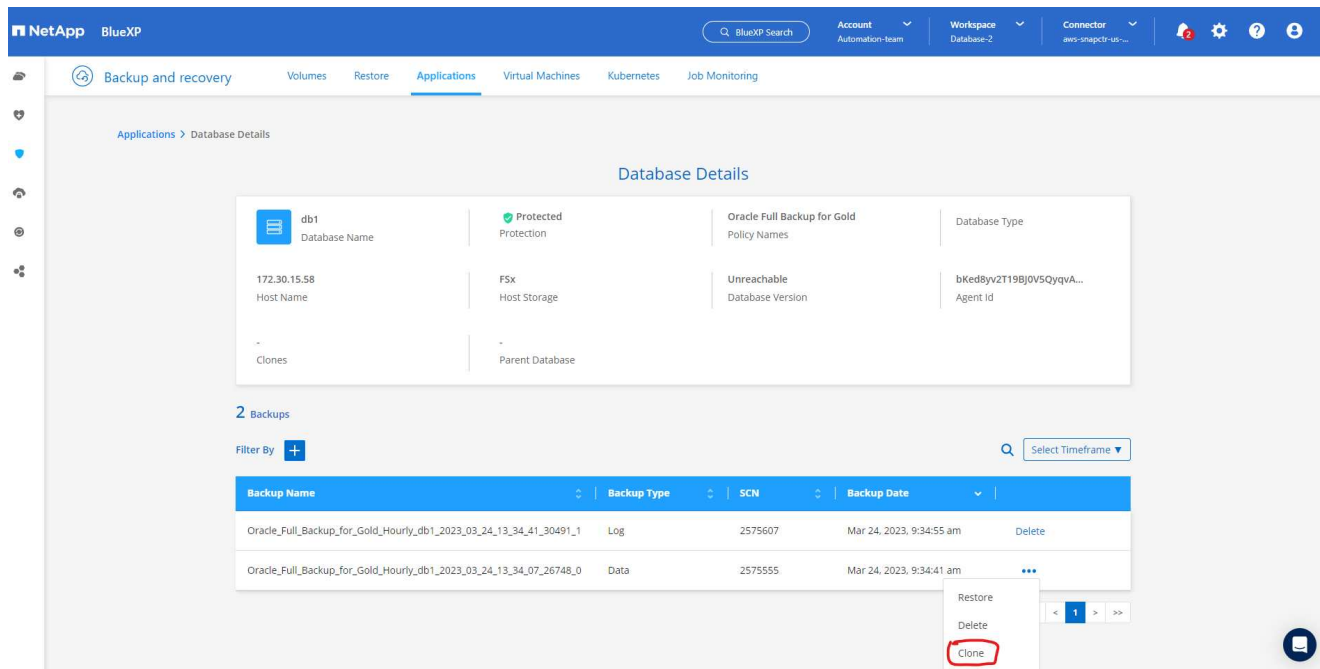
Sub-Jobs(6)

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	fb7b1171-9f6f-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

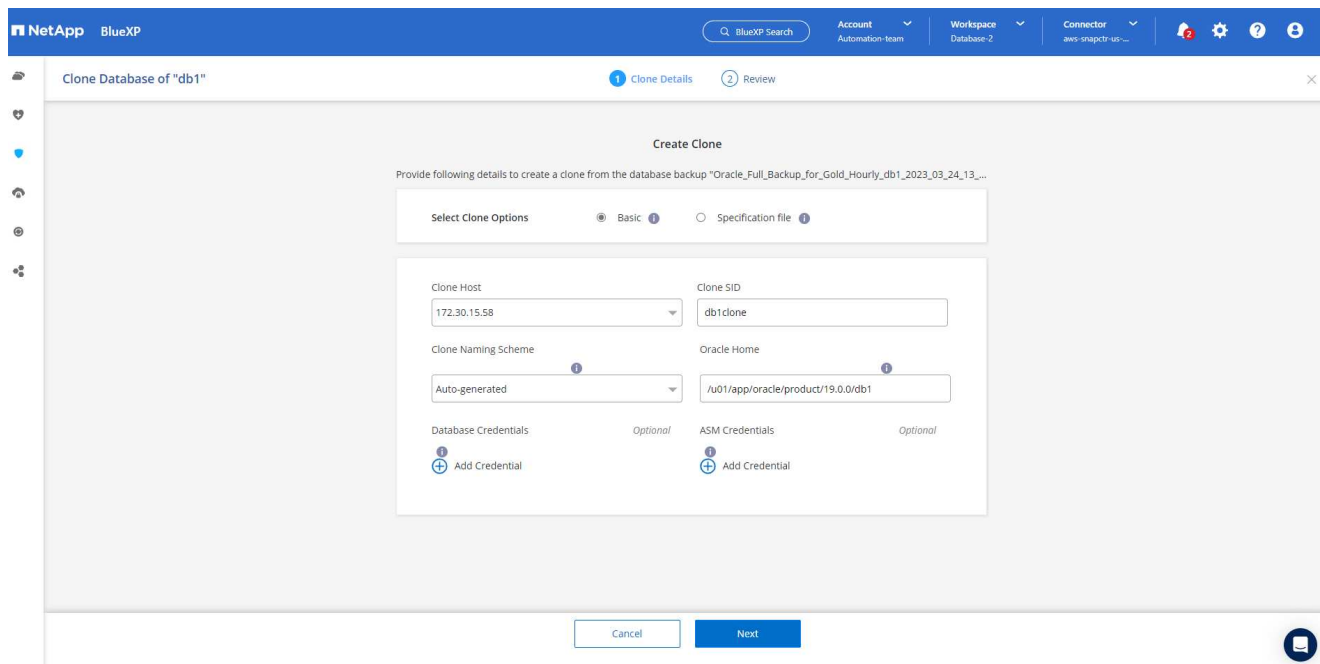
Klon einer Oracle Datenbank

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.

NetApp BlueXP

BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...

Clone Database of "db1"

1 Clone Details

2 Review

Create Clone

Provide following details to create a clone from the database backup "Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19..."

Select Clone Options

☐ Basic
 ☒ Specification file

Generate specification file to modify input parameters and use for clone.

Download File

Specification File

db1_3_24_2023_10_14_spec.json

Browse

Clone Host

172.30.15.58

Clone SID

db1clone

Database Credentials

Optional

Add Credential

ASM Credentials

Optional

Add Credential

Cancel

Next

1. Überprüfen und starten Sie den Job.

NetApp BlueXP

BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...

Clone Database of "db1"

1 Clone Details

2 Review

Review

General	Database parameters
Backup Name	Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_34_07_26748_0
Clone SID	db1clone
Clone Host	172.30.15.58
Datafile locations	DATA_db1clone
Control files	+DATA_db1clone/db1clone/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redolog/redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redolog/redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redolog/redo03_01.log
Recovery scope	Until cancel using selected backup's archive logs

Previous

Clone

1. Überwachen Sie den Status des Klonjobs über die Registerkarte **Job Monitoring**.

111

NetAppBlueXP

BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapc1r-18-...

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Job Monitoring

Job Id: cd30abaf-fbe2-4052-a6db-4bf965a8d29b

Job Details

Job Id: cd30abaf-fbe2-4052-a6db-4bf965a8d29b

Expand All

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	51f152c1-853a-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-8225-4784bcd9843&sc_channel=ps&s_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqWQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwid=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

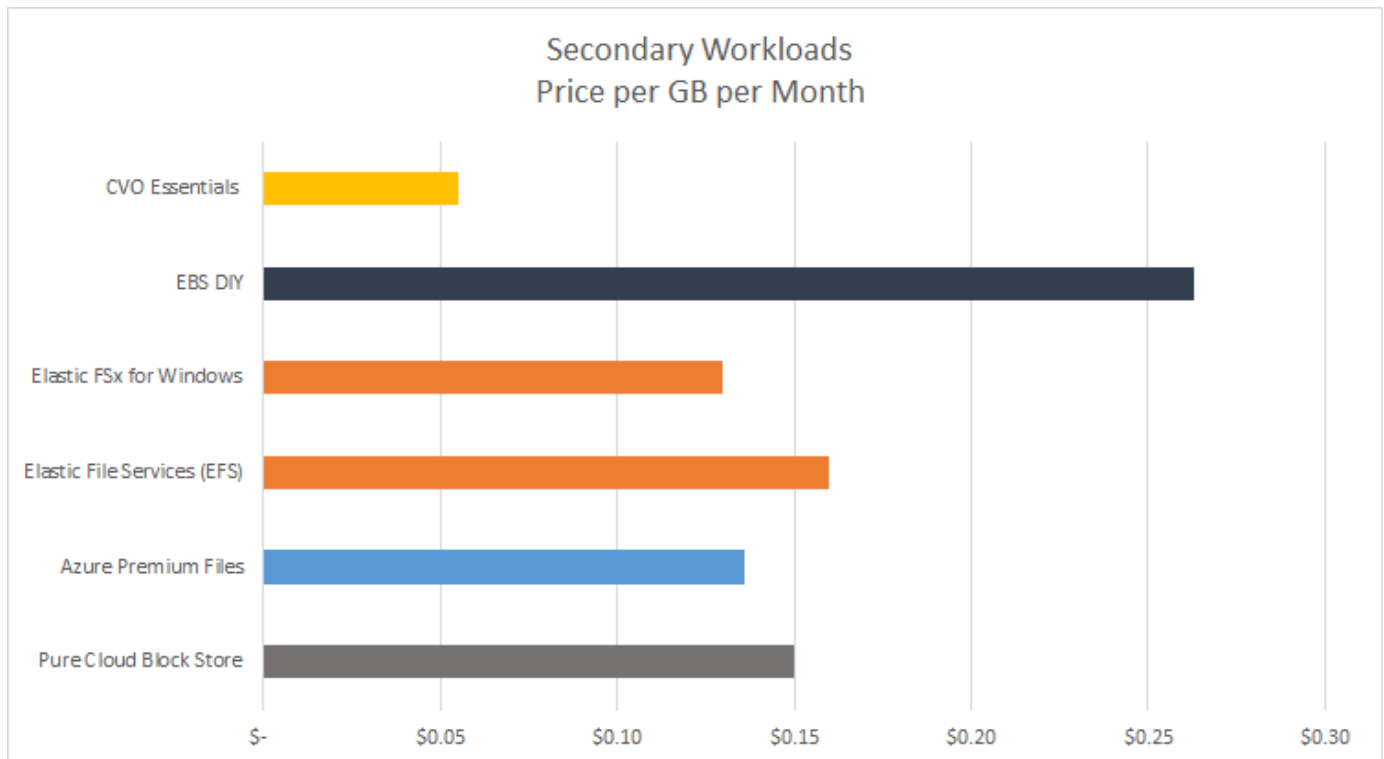
Heute befinden sich viele Enterprise-Datenbanken aus Performance-, Sicherheits- und anderen Gründen immer noch in privaten Datacentern eines Unternehmens. Diese Hybrid-Cloud-Datenbanklösung ermöglicht Unternehmen, ihre primären Datenbanken vor Ort zu betreiben und gleichzeitig eine Public Cloud für Test- 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:

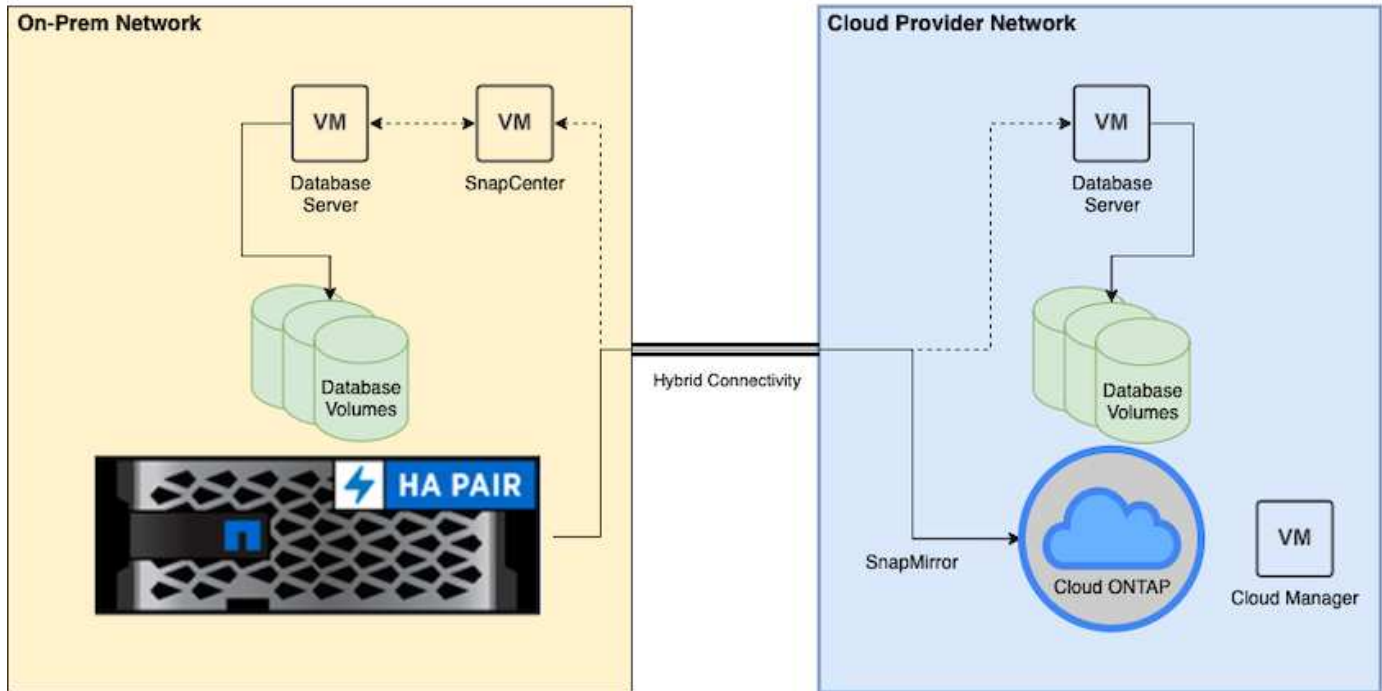
- ["Backup einer Oracle-Datenbank in einer Hybrid Cloud mit SnapCenter"](#)
- ["SnapCenter – KLONEN SIE ENTWICKLUNG/TEST für eine Oracle Datenbank in AWS Cloud"](#)

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:

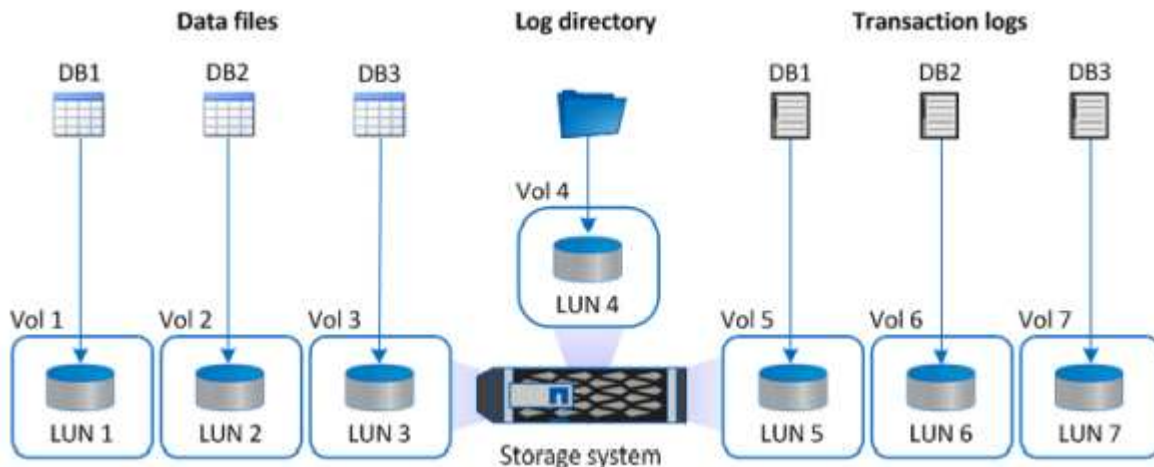
- **Single Instance oder HA-Bereitstellung.** HA-Bereitstellung bietet Redundanz bei Ausfall eines SnapCenter-Instanz-Servers.
- **Namensauflösung.** DNS muss auf dem SnapCenter-Server konfiguriert sein, um alle Datenbank-Hosts sowie auf der Speicher-SVM aufzulösen, damit die Suche vorwärts und rückwärts 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.

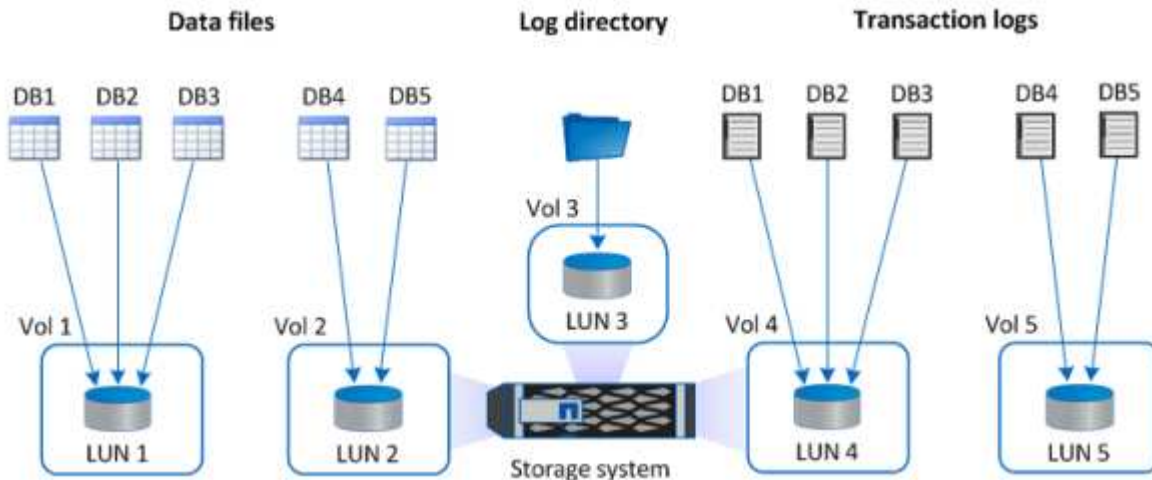
Storage-Konfiguration des lokalen Datenbankservers

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:

["SnapCenter-Standard-kapazitätsbasierte Lizenzen"](#)

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 temporelem 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

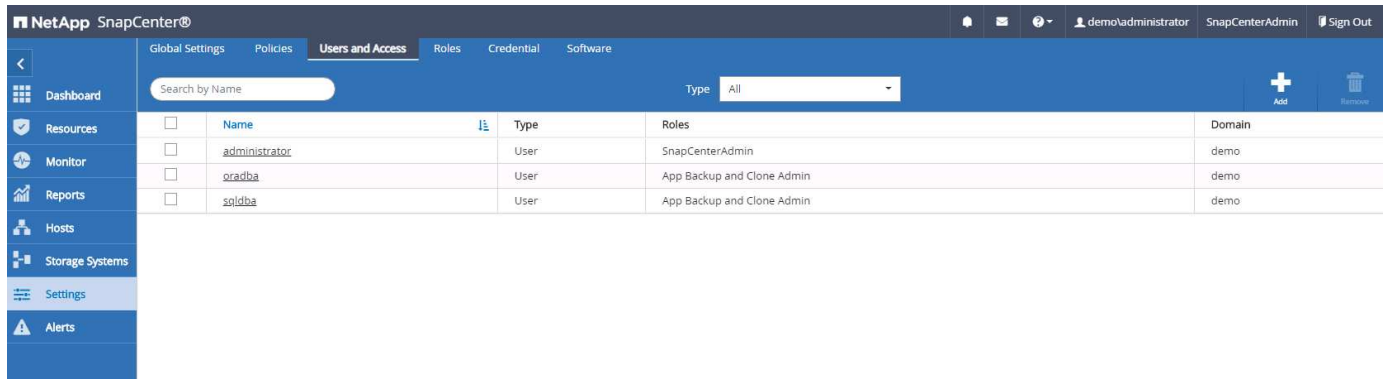
Es ist sinnvoll, eine dedizierte Admin-Benutzer-ID für jede von SnapCenter unterstützte Datenbankplattform zur Sicherung, Wiederherstellung und/oder Disaster Recovery von Datenbanken zu haben. Sie können auch eine einzige ID zum Managen aller Datenbanken verwenden. In unseren Test-Cases und Demos haben 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.



Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oradba	User	App Backup and Clone Admin	demo
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

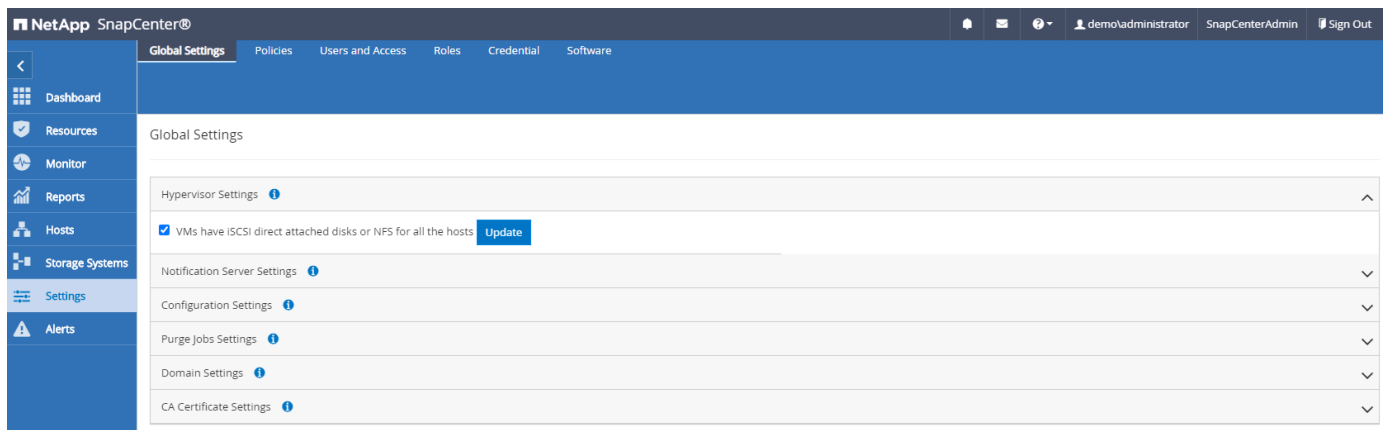


Bevor Sie versuchen, SnapCenter-Plugins auf Cloud-DB-Serverinstanzen zu installieren, stellen Sie sicher, dass alle Konfigurationsschritte wie im entsprechenden Cloud-Abschnitt für die Bereitstellung von Computing-Instanzen aufgeführt abgeschlossen wurden.

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.

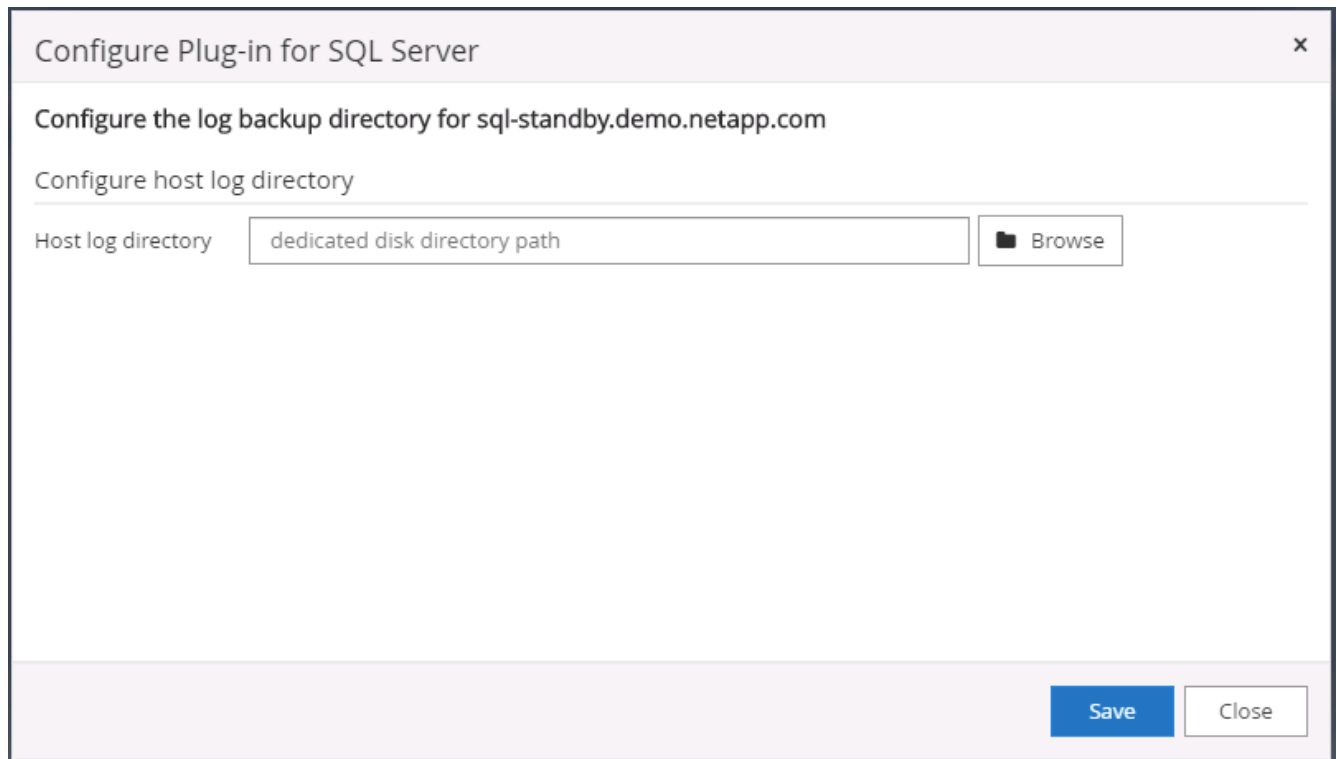
- Klicken Sie im linken Menü auf die Registerkarte Hosts und dann auf Hinzufügen, um den Host-Workflow hinzuzufügen zu öffnen.
- Wählen Sie Windows für den Hosttyp. Der Hostname kann entweder ein Hostname oder eine IP-Adresse sein. Der Hostname muss vom SnapCenter-Host auf die richtige Host-IP-Adresse 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.

- Nach der Installation des Plug-ins auf einem Windows-Host wird sein Gesamtstatus als „Protokollverzeichnis konfigurieren“ angezeigt.

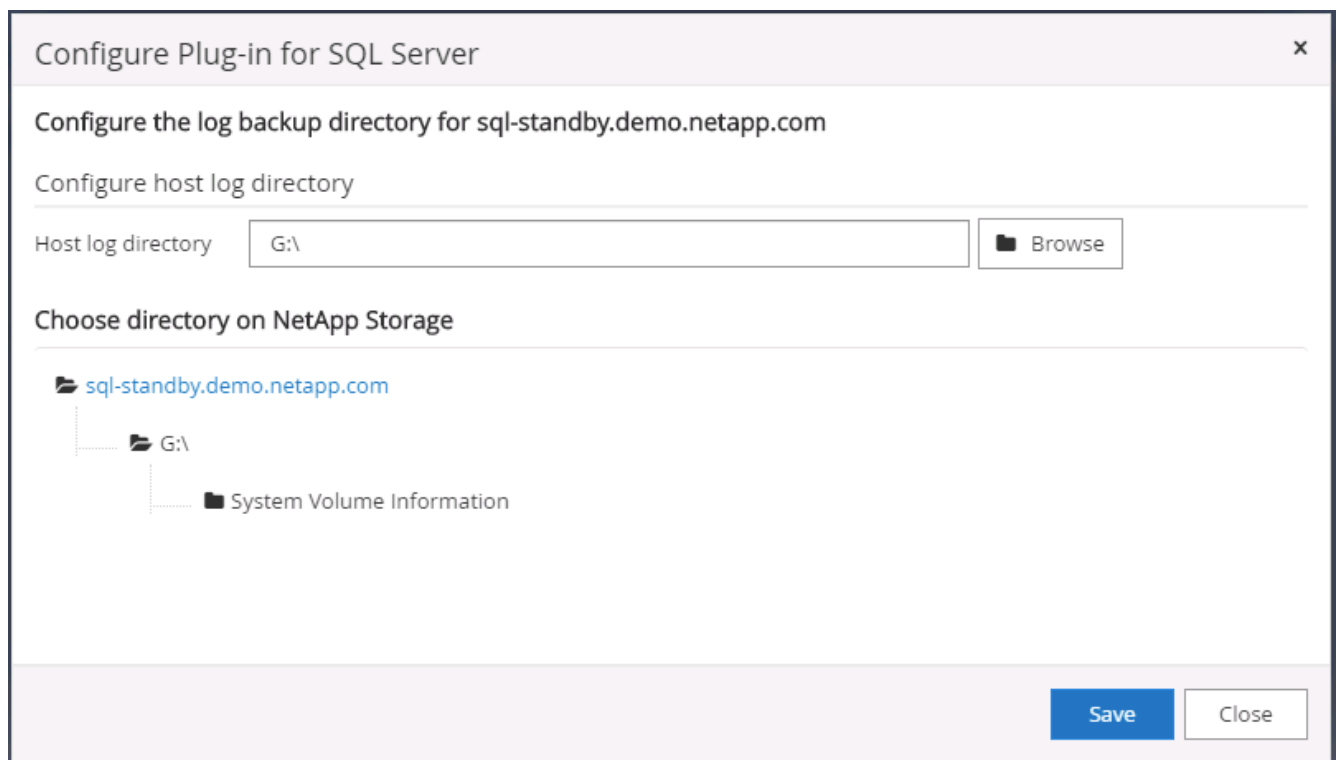
Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Configure log directory

- Klicken Sie auf den Hostnamen, um die Konfiguration des SQL Server-Protokollverzeichnisses zu öffnen.

- Klicken Sie auf „Protokollverzeichnis konfigurieren“, um „Plug-in für SQL Server konfigurieren“ zu öffnen.

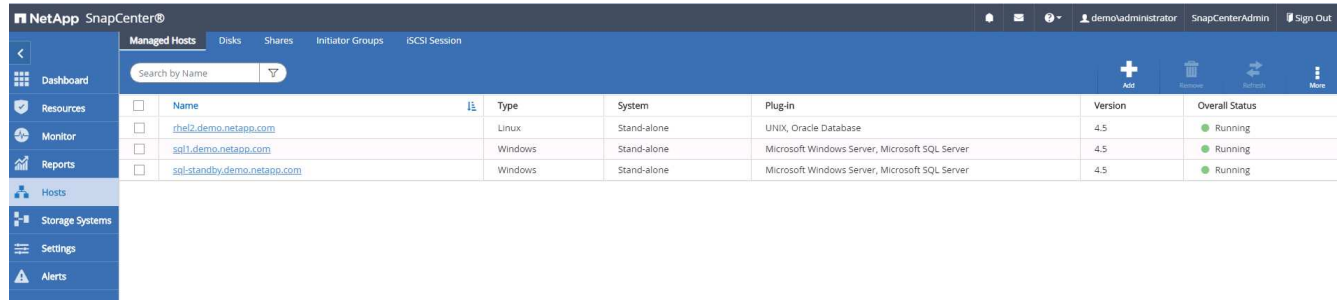


7. Klicken Sie auf Browse, um NetApp Storage zu entdecken, so dass ein Log-Verzeichnis eingestellt werden kann; SnapCenter verwendet dieses Log-Verzeichnis, um die Transaktions-Log-Dateien für SQL Server zu öffnen. Klicken Sie dann auf Speichern.



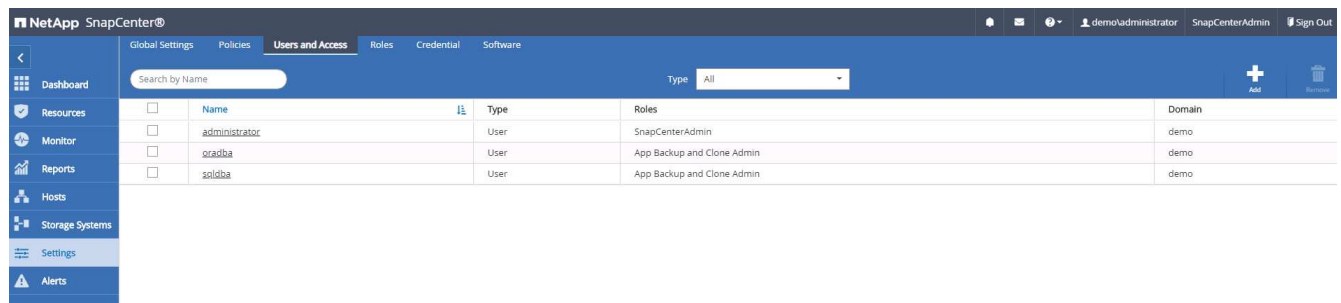
Wenn NetApp Storage, der einem DB-Host zur Ermittlung bereitgestellt wird, hinzugefügt werden soll, muss der Storage (On-Prem oder CVO) zum SnapCenter hinzugefügt werden, wie in Schritt 6 für CVO als Beispiel dargestellt.

8. Nach der Konfiguration des Protokollverzeichnisses wird der Gesamtstatus des Windows-Host-Plug-ins in „Ausführen“ geändert.

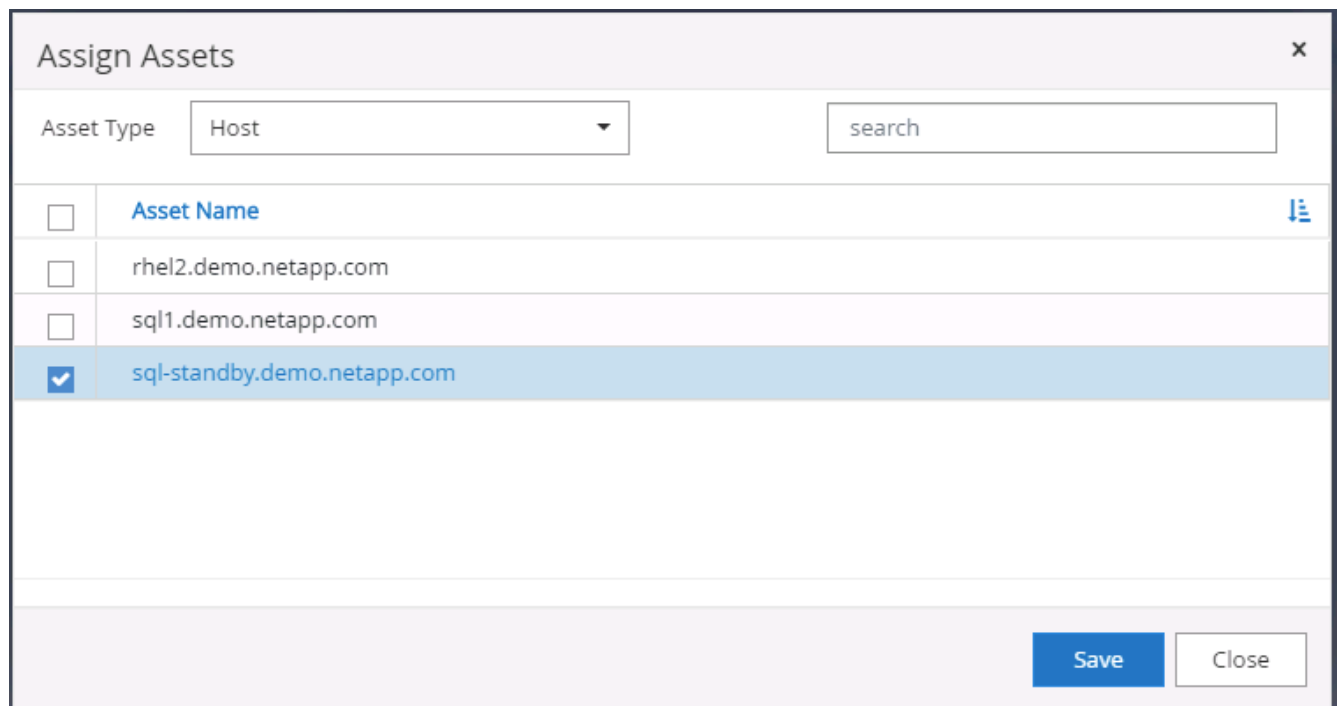


Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft 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

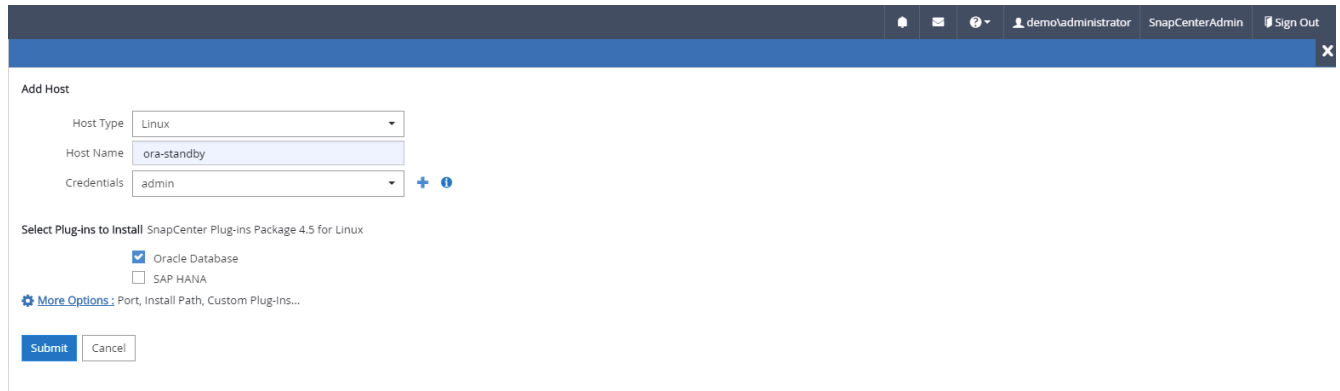
Save Close

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.



Add Host

Host Type: Linux

Host Name: ora-standby

Credentials: admin

Select Plug-ins to Install: SnapCenter Plug-ins Package 4.5 for Linux

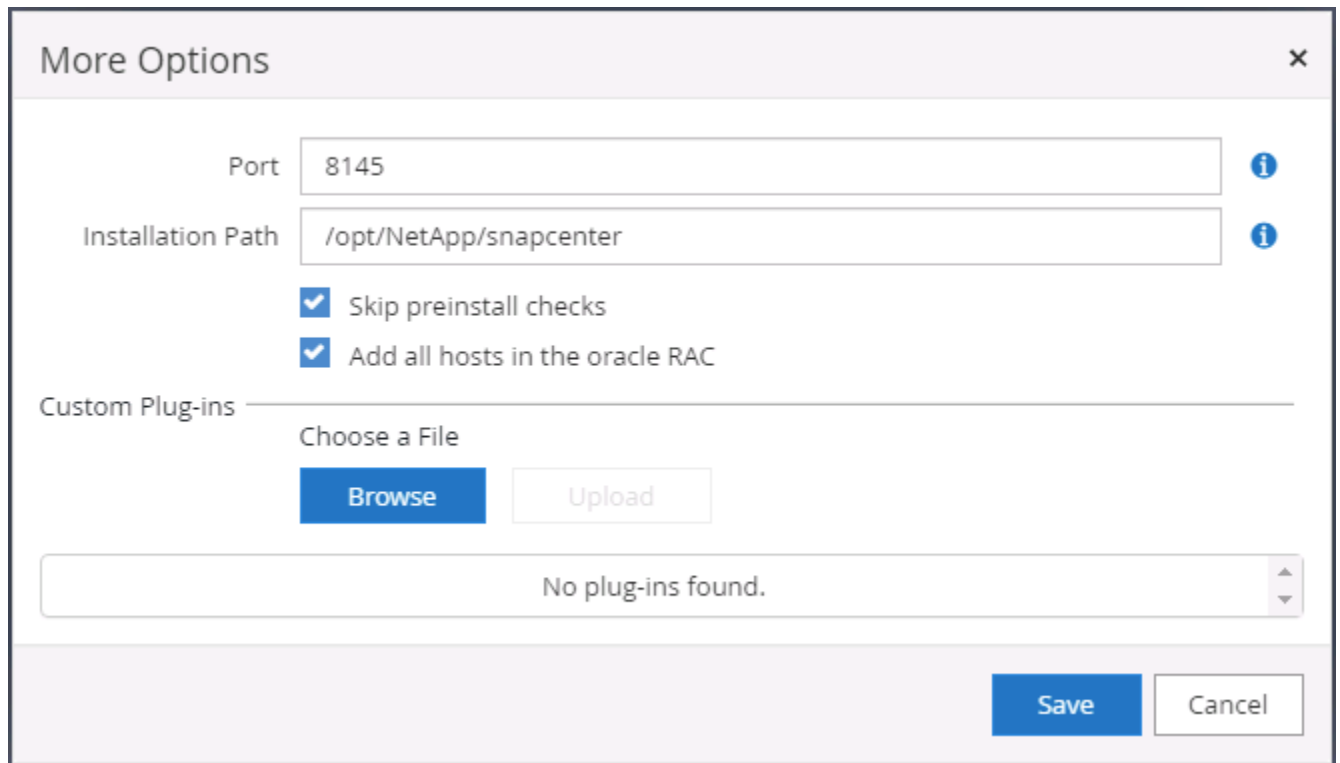
☒ Oracle Database

☐ SAP HANA

[More Options](#): Port, Install Path, Custom Plug-ins...

Submit Cancel

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.



More Options

Port: 8145

Installation Path: /opt/NetApp/snapcenter

☒ Skip preinstall checks

☒ Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse Upload

No plug-ins found.

Save Cancel

5. Klicken Sie auf Senden, um die Plugin-Installation zu starten. Sie werden wie unten gezeigt aufgefordert, den Fingerabdruck zu bestätigen.

Confirm Fingerprint
✕

Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
ora-standby.demo.netapp.com	ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

Confirm and Submit
Close

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.

NetApp SnapCenter®							
<div> Managed Hosts Disks Shares Initiator Groups iSCSI Session </div>							
<div> Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts </div>							
<div> Search by Name </div>							
<input type="checkbox"/>	Name	Type	System	Plug-in	Version	Overall Status	
<input type="checkbox"/>	ora-standby.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
<input type="checkbox"/>	rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
<input type="checkbox"/>	sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	
<input type="checkbox"/>	sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	

7. Weisen Sie den neu hinzugefügten Host der korrekten Datenbank-Management-Benutzer-ID zu (in unserem Fall oradba).

NetApp SnapCenter®

Users and Access
Users/Groups Details

Search by Name

☐ Name
☐ administrator
☒ oradba
☐ sqlidba

User Name
Domain
Roles

oradba
demo
App Backup and Clone Admin

Assign Assets

☐ Asset Name
☐ 10.0.0.1
☐ 192.168.0.101
☐ admin
☐ Linux Admin
☐ Oracle Archive Log Backup
☐ Oracle Full Online Backup
☐ rhel2.demo.netapp.com

☐ Type
☐ DataOntapCluster
☐ DataOntapCluster
☐ Credentials
☐ Credentials
☐ Policy
☐ Policy
☐ host

☐ Asset Type
☐ Storage Connection
☐ Storage Connection
☐ Credentials
☐ Credentials
☐ Policy
☐ Policy
☐ host

Submit
Cancel

Assign Assets

Asset Type
Host
search

<input type="checkbox"/>	Asset Name
<input checked="" type="checkbox"/>	ora-standby.demo.netapp.com
<input type="checkbox"/>	rhel2.demo.netapp.com
<input type="checkbox"/>	sql1.demo.netapp.com
<input type="checkbox"/>	sql-standby.demo.netapp.com

Save
Close

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.

NetApp SnapCenter®

Oracle Database

View
Database
Search databases

Refresh Resources
New Resource Group

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

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.

NetApp SnapCenter®

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

Microsoft SQL Server

View

Database

search by name

Refresh Resources

New Resource Group

	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 Datenbankanmeldeinformationen neu konfiguriert werden, um die rote Sperre zu entsperren.

NetApp SnapCenter®

demo/sqldba

App Backup and Clone Admin

Sign Out

<

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

Microsoft SQL Server

View Instance search by name

Refresh Resources

New Resource Group

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)

NetApp SnapCenter®							
Microsoft SQL Server							
Instance - Credentials							
search by name							
Add Credential							
Name							
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.

NetApp SnapCenter®

</

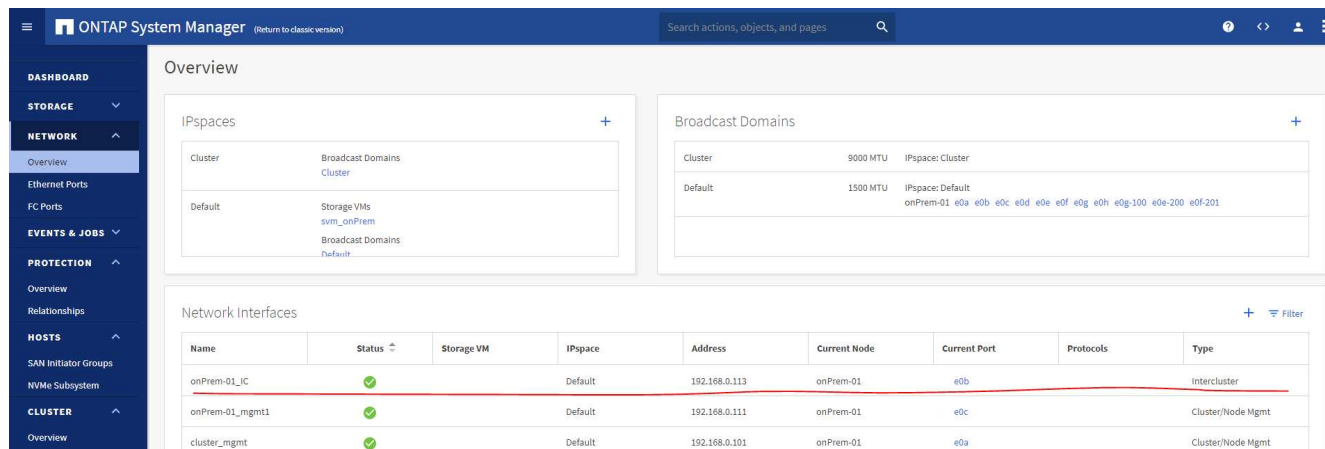
5. Storage Cluster-Peering und DB Volumes Replication einrichten

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.

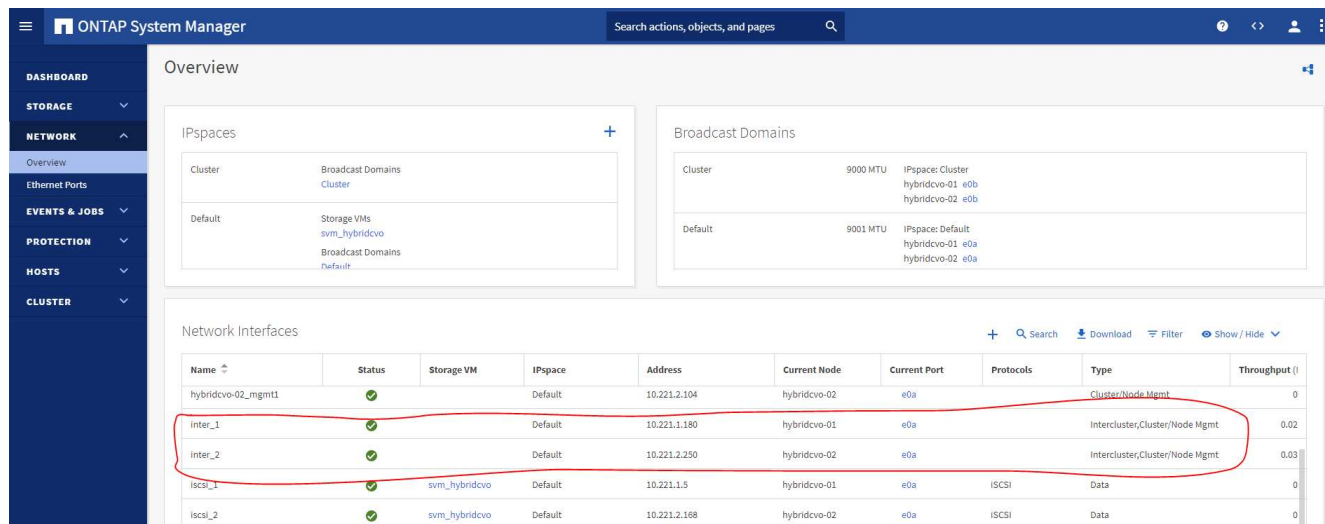
1. Konfigurieren Sie Intercluster LIFs für Cluster-Peering sowohl auf dem On-Premises-Cluster als auch auf der CVO-Cluster-Instanz. Dieser Schritt kann mit ONTAP System Manager ausgeführt werden. In einer CVO-Standardimplementierung werden automatisch Inter-Cluster-LIFs konfiguriert.

On-Premises-Cluster:



Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type
onPrem-01_IC	✓		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	10.221.1.5	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.

ONTAP System Manager (Return to classic version)

Search actions, objects, and pages

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

Overview

Relationships

HOSTS

CLUSTER

Overview

Settings

UI Settings

LOG LEVEL
DEBUG

INACTIVITY TIMEOUT
30 minutes

Intercluster Settings

Network Interfaces

IP ADDRESS
✓ 192.168.0.113

Cluster Peers

PEERED CLUSTER NAME
✓ hybridcvo

Peer Cluster

Generate Passphrase

Manage Cluster Peers

Storage VM Peers

PEERED STORAGE VMs
✓ 1

4. Wechseln Sie zur Registerkarte Volumes. Wählen Sie das zu replizierende Datenbank-Volume aus, und klicken Sie auf „Schützen“.

ONTAP System Manager (Return to classic version)

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Volumes

+ Add Delete Protect More

Name	rhel2_u03 All Volumes
onPrem_data	
rhel2_u01	
rhel2_u02	
✓ rhel2_u03	
rhel2_u0309232119421203118	
sql1_data	
sql1_log	
sql1_snapctr	
svm_onPrem_root	

Overview Snapshot Copies Clone Hierarchy SnapMirror (Local or Remote)

STATUS
✓ Online

STYLE
FlexVol

MOUNT PATH
/rhel2_u03

STORAGE VM
svm_onPrem

LOCAL TIER
onPrem_01_SSD_1

SNAPSHOT POLICY
default

QUOTA
Off

TYPE
Read Write

SPACE RESERVATION

Capacity

0% 10% 20% 30% 40% 50%

SNAPSHOT CAPACITY

0 Bytes Available | 2.36 GB Used | 2.36 GB Overflow

Performance

Hour Day Week

Latency

1.5

1

5. Legen Sie die Schutzrichtlinie auf Asynchronus fest. Wählen Sie das Ziel-Cluster und die Storage-SVM

aus.

ONTAP System Manager

(Return to classic version)

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Protect Volumes

PROTECTION POLICY

Asynchronous

Source

CLUSTER

onPrem

STORAGE VM

svm_onPrem

SELECTED VOLUMES

rhel2_u03

Destination

CLUSTER

hybridcvo

STORAGE VM

svm_hybridcvo

Destination Settings

2 matching labels

VOLUME NAME

PREFIX

vol_

SUFFIX

<SourceVolumeName>_dest

Override default storage service name

Configuration Details

Initialize relationship

Enable FabricPool

Save

Cancel

6. Überprüfen Sie, ob das Volume zwischen Quelle und Ziel synchronisiert wird und ob die Replikationsbeziehung ordnungsgemäß ist.

Volumes

+ Add

Delete

Protect

More

rhel2_u03

All Volumes

Edit

More

onPrem_data

rhel2_u01

rhel2_u02

rhel2_u03

rhel2_u0309232119421203118

Overview

Snapshot Copies

Clone Hierarchy

SnapMirror (Local or Remote)

Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag
svm_onPremorhel2_u03	svm_hybridcvoorhel2_u03_dr	MirrorAllSnapshots	Healthy	Mirrored	12 seconds

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](#).

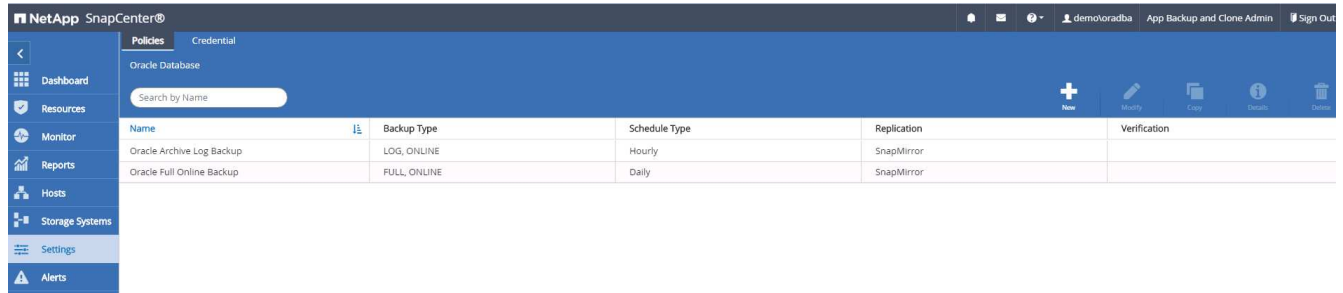
Name	IP	Cluster Name	User Name	Platform	Controller License
svm_hybridv	10.0.0.1			CVO	⊘
svm_onPrem	192.168.0.101			CVO	✓

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.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

Previous

Next

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

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

7

Keep Snapshot copies for

14

days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

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

Daily ⓘ

Error retry count

3 ⓘ

Previous

Next

6. Geben Sie ein optionales Skript an, das vor und nach einer Sicherungsfahrt ausgeführt werden soll.

Modify Oracle Database Backup Policy

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

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Führen Sie bei Bedarf eine Backup-Überprüfung durch.

141

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

60

secs

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Choose optional arguments...

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Choose optional arguments...

Previous

Next

8. Zusammenfassung.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	Oracle Full Online Backup
Details	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

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

Oracle Archive Log Backup

Backup Oracle archive logs

Previous

Next

3. Wählen Sie den Sicherungstyp und die Zeitplanfrequenz aus.

144

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

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 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

7

Keep Snapshot copies for

14 days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

7 days

Previous

Next

5. Aktivieren Sie die Replizierung an einen sekundären Standort in der Public Cloud.

146

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

Hourly

Error retry count

3

Previous

Next

6. Geben Sie alle optionalen Skripts an, die vor und nach der Protokollsicherung ausgeführt werden sollen.

New Oracle Database Backup Policy

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

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Geben Sie alle Skripts für die Backup-Überprüfung an.

148

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

60secs

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Choose optional arguments...

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Choose optional arguments...

Previous

Next

8. Zusammenfassung.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

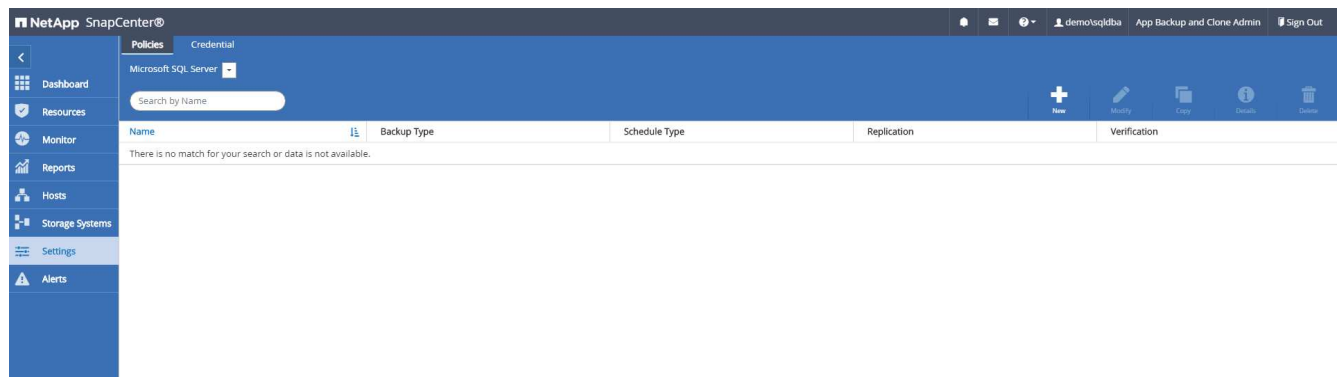
Policy name	Oracle Archive Log Backup
Details	Backup Oracle archive logs
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive 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

Previous

Finish

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

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

SQL Server Full Backup

Details

Backup all data and log files

Previous

Next

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

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

4. Legen Sie den Aufbewahrungszeitraum für Backups fest.

152

New SQL Server Backup Policy

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

7

full backups

☐ Keep log backups applicable to last

14

days

Full backup retention settings ⓘ

Daily

☒ Total Snapshot copies to keep

7

☐ Keep Snapshot copies for

14

days

Previous

Next

5. Replizierung von Backup-Kopien an einen sekundären Standort in der Cloud aktivieren

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

Daily

Error retry count

3

Previous

Next

6. 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

Choose optional arguments...

Choose optional arguments...

60secs

Previous

Next

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.

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 all data and log files
Backup type	Full backup and log backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Daily
UTM retention	Total backup copies to retain : 7
Daily Full backup retention	Total backup copies to retain : 7
Replication	SnapMirror enabled , Secondary policy label: Daily , 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

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

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

SQL Server Log Backup

Backup SQL server log

Previous

Next

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:

100

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.

New SQL Server Backup Policy

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

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

Choose optional arguments...

Choose optional arguments...

60secs

Previous

Next

6. Zusammenfassung.

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.

NetApp SnapCenter®						
<div> <div>Oracle Database</div> <div>View Database Search databases</div> </div>						
Resources	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup Overall Status
	cdb2	Single instance (Multitenant)	rhe12.demo.netapp.com			Not protected

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.

NetApp SnapCenter®

Oracle Database

Search databases

1 2 3 4 5 6
Name Resources Policies Verification Notification Summary

Provide a name and tags for the resource group

Name

Tags

☒ Use custom name format for Snapshot copy

\$CustomText

Backup settings

Exclude archive log destinations from backup

3. Fügen Sie der Ressourcengruppe Datenbankressourcen hinzu.

NetApp SnapCenter®

Oracle Database

Search databases

1 2 3 4 5 6
Name Resources Policies Verification Notification Summary

Add resources to Resource Group

Host

Available Resources

search available resources

Selected Resources

cdb2 (rhe12.demo.netapp.com)

4. Wählen Sie aus der Dropdown-Liste eine vollständige Backup Policy aus, die in Abschnitt 7 erstellt wurde.

NetApp SnapCenter®

Oracle Database

Search databases

1 2 3 4 5 6
Name Resources Policies Verification Notification Summary

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

5. Klicken Sie auf das Pluszeichen (+), um den gewünschten Backup-Zeitplan zu konfigurieren.

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.

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhei2_cdb2	1	orafullbkup	Oracle Full Online Backup		

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.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhe12_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name rhe12_cdb2_log

Tags oralogbkup

☒ Use custom name format for Snapshot copy

\$CustomText rhe12_cdb2_log

Backup settings

Exclude archive log destinations from backup

3. Fügen Sie der Ressourcengruppe Datenbankressourcen hinzu.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhe12_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host All

Available Resources

search available resources

Selected Resources

cdb2 (rhe12.demo.netapp.com)

Total 1

Previous Next

4. Wählen Sie aus der Dropdown-Liste eine Protokoll-Backup-Richtlinie aus, die in Abschnitt 7 erstellt wurde.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhe12_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

Oracle Archive Log Backup

Oracle Full Online Backup

Oracle Archive Log Backup

Policy

Applied Schedules

Configure Schedules

None

Total 1

Previous Next

5. Klicken Sie auf das Pluszeichen (+), um den gewünschten Backup-Zeitplan zu konfigurieren.

Add schedules for policy Oracle Archive Log Backup

Hourly

Start date

09/10/2021 3:00 PM

☒ Expires on

12/31/2021 3:00 PM

Repeat every

1

hours

0

mins

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

Cancel

OK

6. Wenn die Backup-Überprüfung konfiguriert ist, wird sie hier angezeigt.

NetApp SnapCenter®
demolordba
App Backup and Clone Admin
Sign Out

Oracle Database

Search resource groups

Name

rhel2_cdb2

Total 1

New Resource Group

1

2

3

4

5

6

Name

Resources

Policies

Verification

Notification

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.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

Total 1

New Resource Group

If you want to send notifications for scheduled or on demand 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.

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.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: rhel2_cdb2_log

Tags: oralogbkup

Policy: Oracle Archive Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Oracle Database

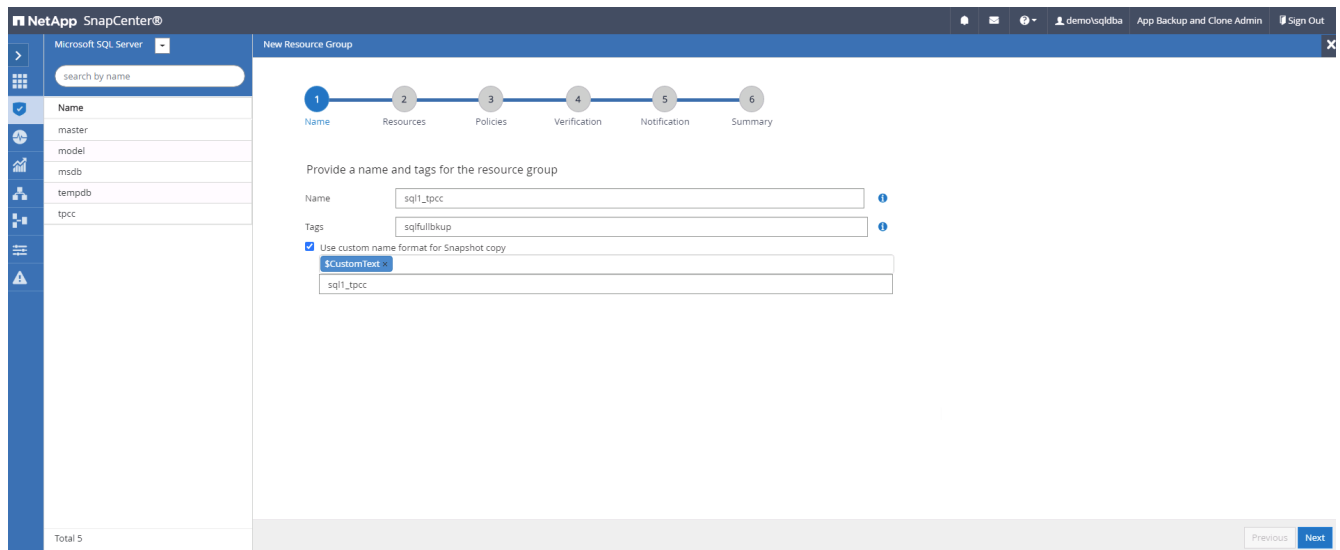
Verification enabled for policy: None

Send email: No

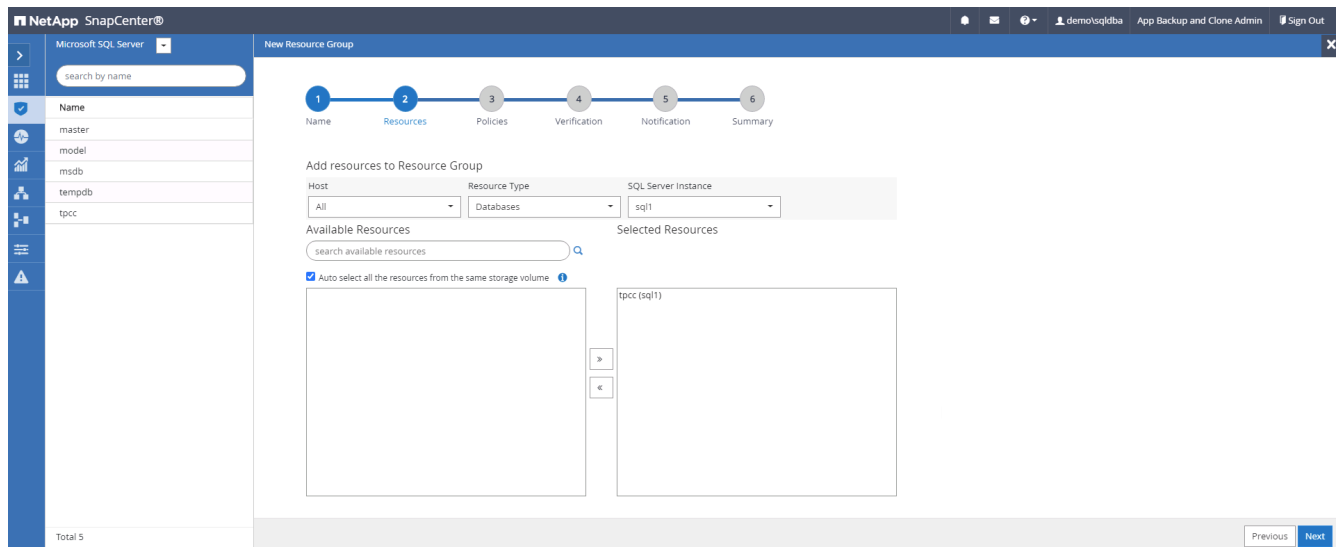
Previous Finish

Erstellen Sie eine Ressourcengruppe für die vollständige Sicherung von SQL Server

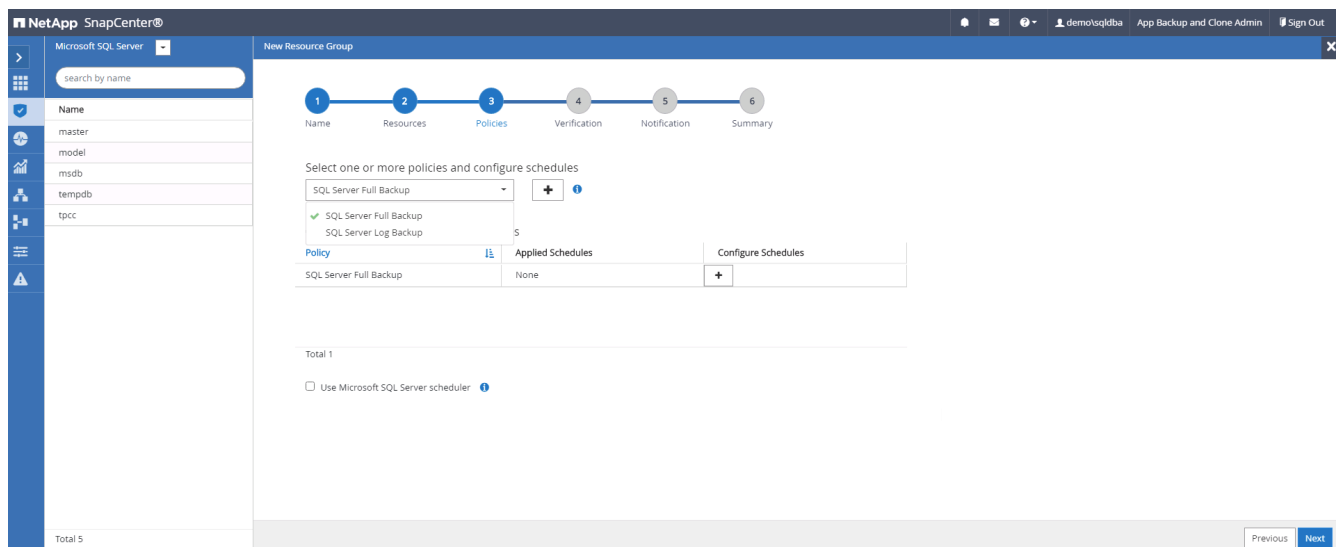
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdown-Liste Ansicht entweder eine Datenbank oder eine Ressourcengruppe aus, um den Arbeitsablauf für die Erstellung von Ressourcengruppen zu starten. 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

☒ Expires on

Repeat every 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

Search by name

Name

master

model

msdb

tempdb

tpcc

New Resource Group

1 Name

2 Resources

3 Policies

4 Verification

5 Notification

6 Summary

Select the verification servers

Verification server

Load secondary locators to verify backups on secondary

Secondary storage location: SnapVault or SnapMirror

Source Volume

Destination Volume

svm_onPremsql1_data

svm_hybridvsql1_data_dr

svm_onPremsql1_log

svm_hybridvsql1_log_dr

Configure verification schedules

Policy

Schedule Type

Applied Schedules

Configure Schedules

There is no match for your search or data is not available.

Total 5

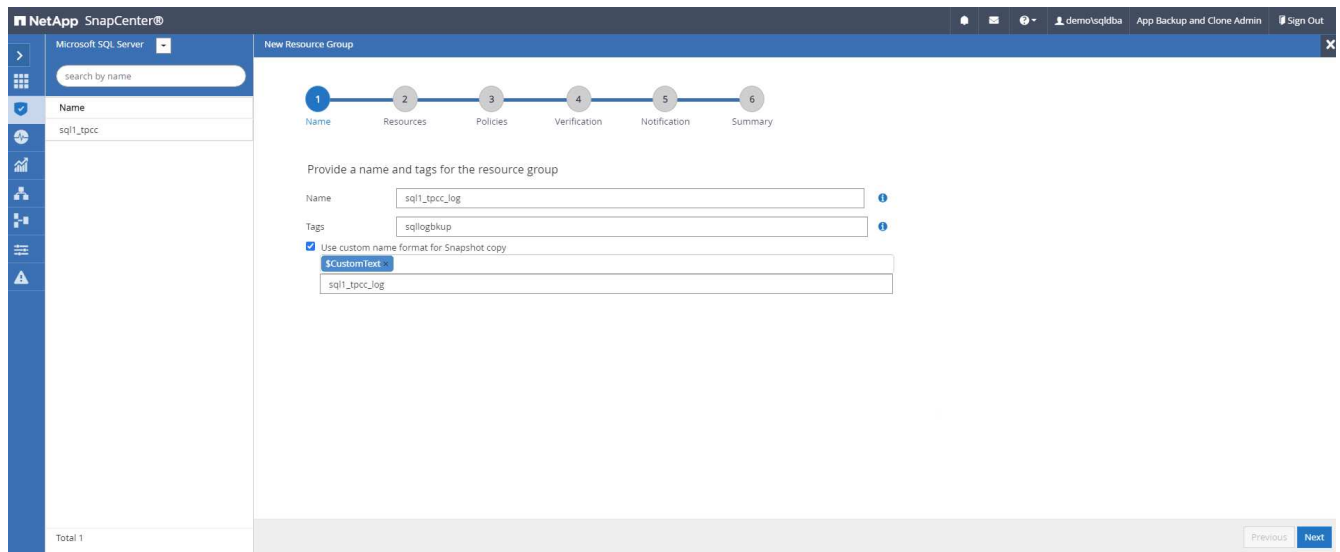
Previous Next

6. Konfigurieren Sie bei Bedarf den SMTP-Server für E-Mail-Benachrichtigungen.

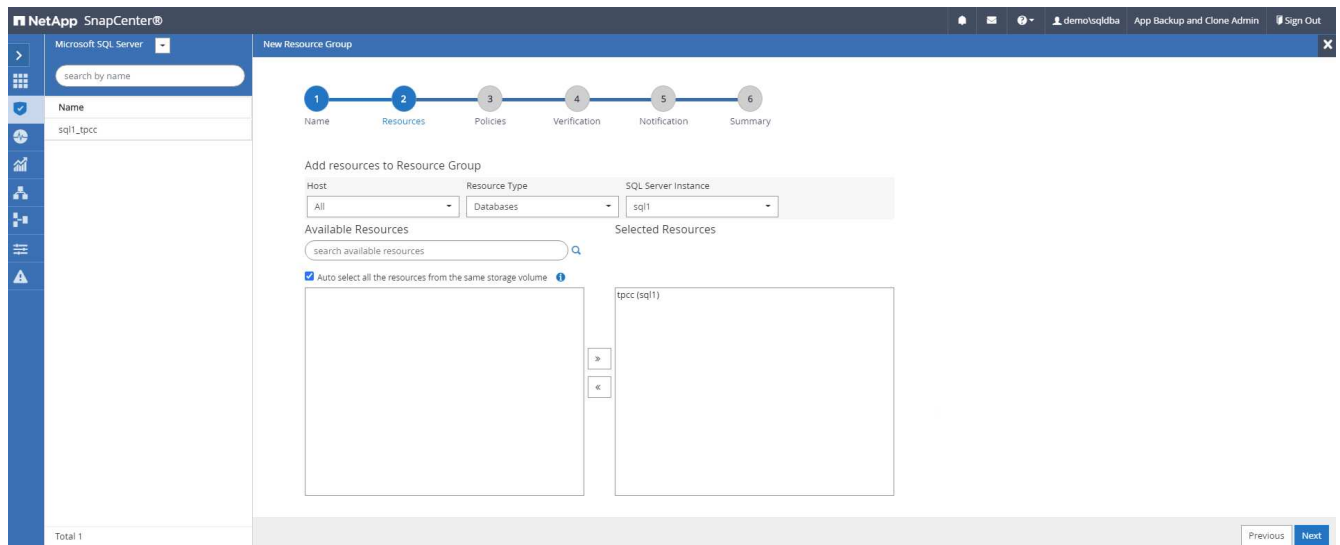
7. Zusammenfassung.

Erstellen Sie eine Ressourcengruppe für die Protokollsicherung von SQL Server

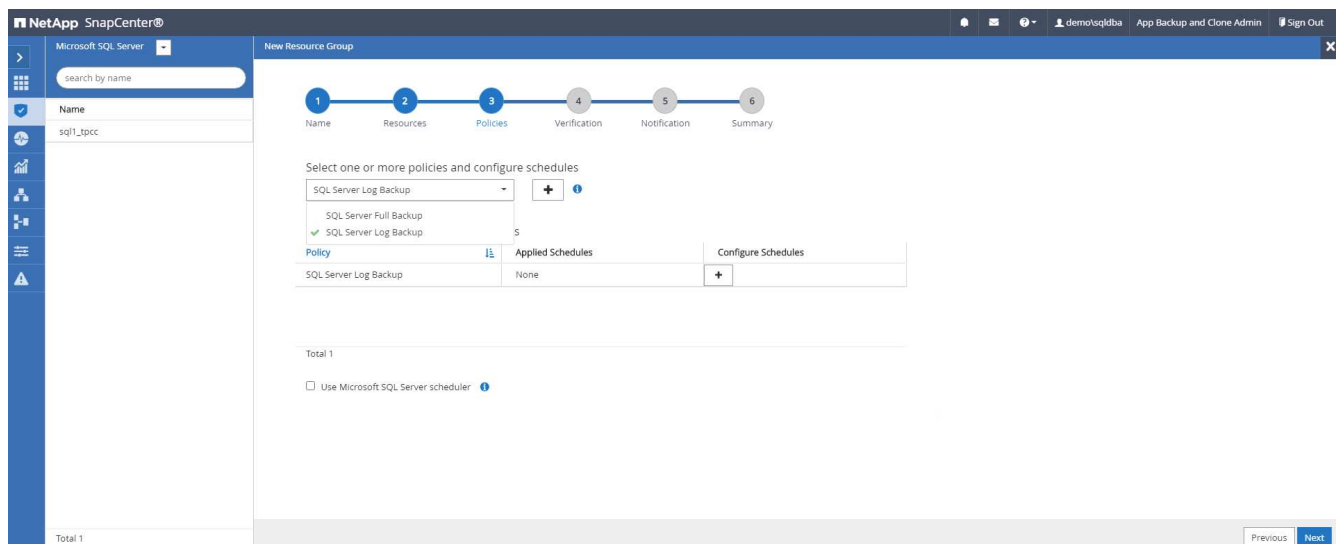
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdown-Liste Ansicht entweder eine Datenbank oder eine Ressourcengruppe aus, um den Arbeitsablauf für die Erstellung von Ressourcengruppen zu starten. 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.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

SQL Server Log Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
SQL Server Log Backup	Hourly: Repeat every 1 hours	✎ ✕

Total 1

☐ Use Microsoft SQL Server scheduler

[Previous](#) [Next](#)

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

search by name

Name

sql1_tpcc

Total 1

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_onPrem:sql1_data	svm_hybridcv:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcv:sql1_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.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1_tpcc

Total 1

New Resource Group

If you want to send notifications for scheduled or on demand 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.

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

7. Zusammenfassung.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: sql1_tpcc_log

Tags: sqllogbkup

Policy: SQL Server Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Microsoft SQL Server

Verification Server: None

Verification enabled for policy: None

Send email: No

Previous Finish

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.

NetApp SnapCenter®

Jobs Schedules Events Logs

search by name

Jobs - Filter

ID	Status	Name	Start date	End date	Owner
532	✓	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/sqldba
528	✓	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/sqldba
524	✓	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/sqldba
521	✓	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/sqldba
517	✓	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/sqldba
513	✓	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/sqldba
509	✓	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/sqldba
503	✓	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/sqldba

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.

The screenshot shows the NetApp SnapCenter web interface. On the left is a navigation sidebar with icons for databases, backups, clones, and alerts. The main area is titled 'cdb2 Topology' and 'Manage Copies'. It displays a diagram with 'Local copies' (197 Backups, 0 Clones) and 'Mirror copies' (197 Backups, 3 Clones). A 'Summary Card' on the right shows: 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. Below this is a table of 'Primary Backup(s)'.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhel2_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhel2_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

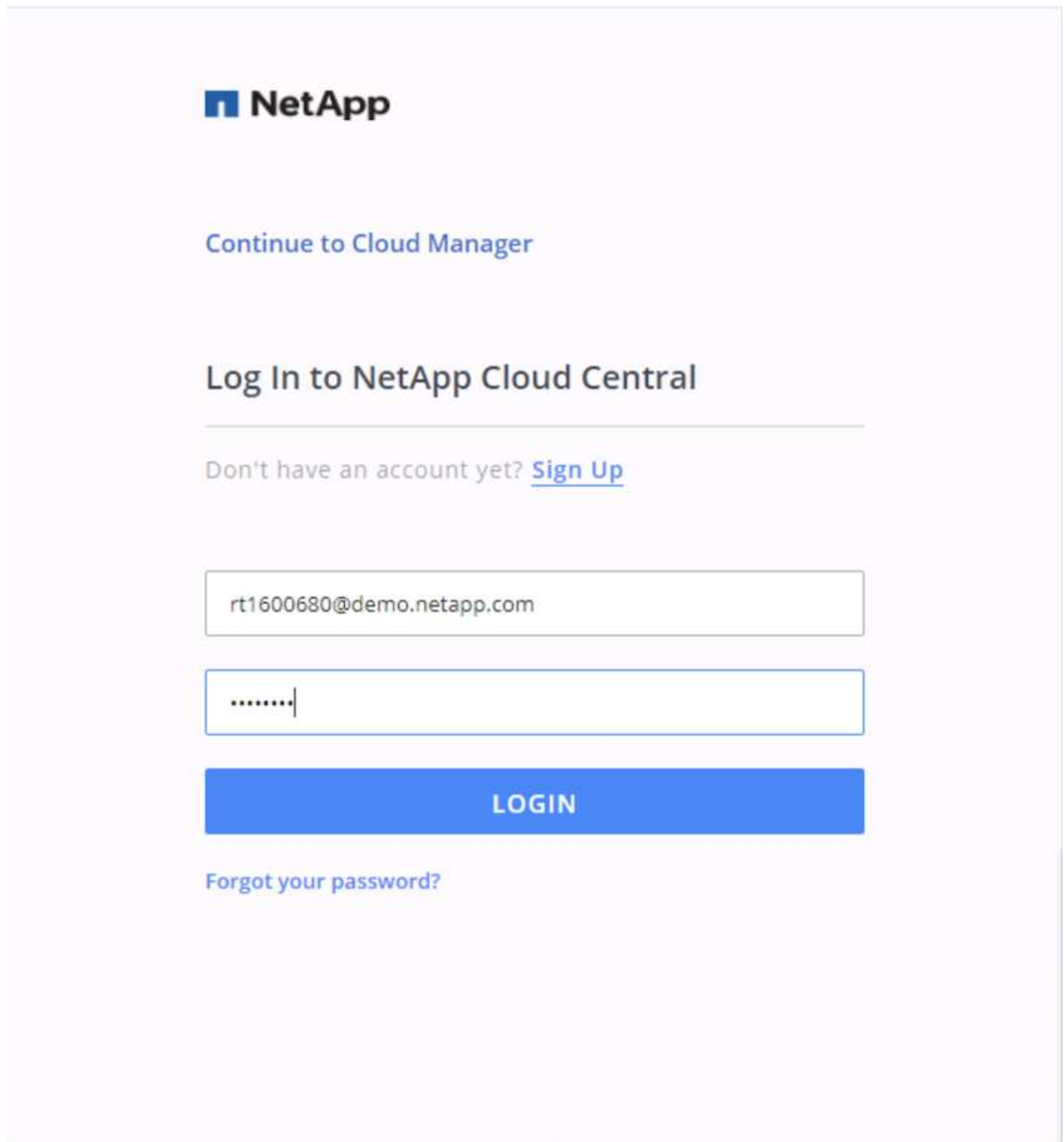
2. Schritte zur Implementierung von Cloud Manager und Cloud Volumes ONTAP in AWS



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.



The image shows the NetApp Cloud Central login page. At the top is the NetApp logo. Below it is a link to "Continue to Cloud Manager". The main heading is "Log In to NetApp Cloud Central". Below this heading is a link for users who don't have an account: "Don't have an account yet? [Sign Up](#)". There are two input fields: the first for the email address, which contains "rt1600680@demo.netapp.com", and the second for the password, which is masked with dots. Below the password field is a blue "LOGIN" button. At the bottom of the login section is a link: "Forgot your password?".

NetApp

[Continue to Cloud Manager](#)

Log In to NetApp Cloud Central

Don't have an account yet? [Sign Up](#)

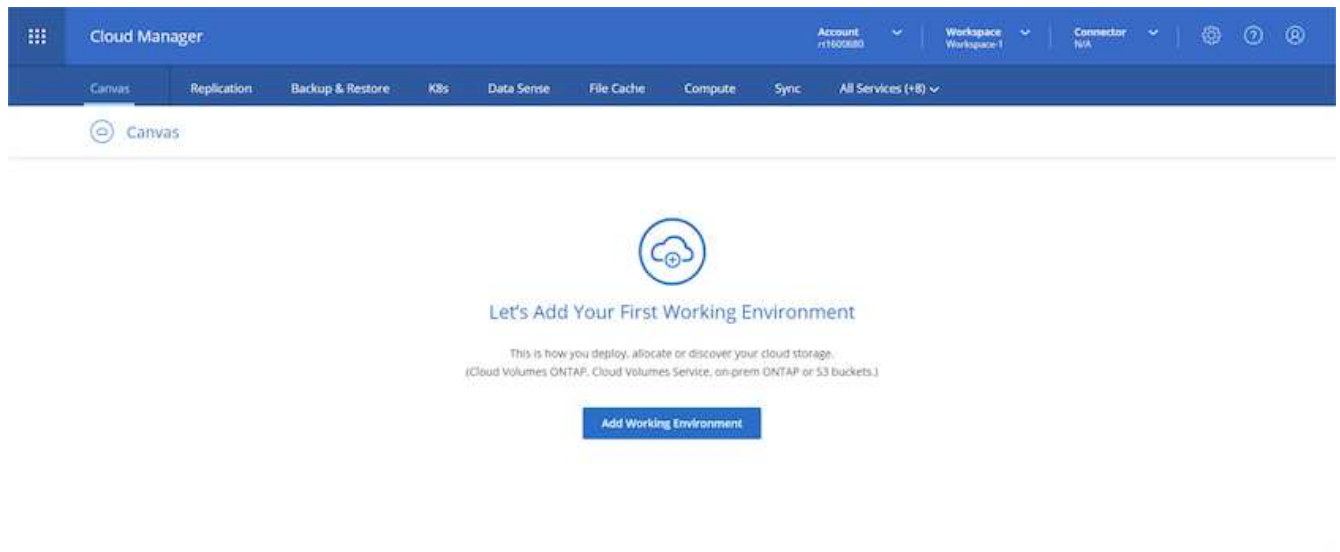
rt1600680@demo.netapp.com

.....|

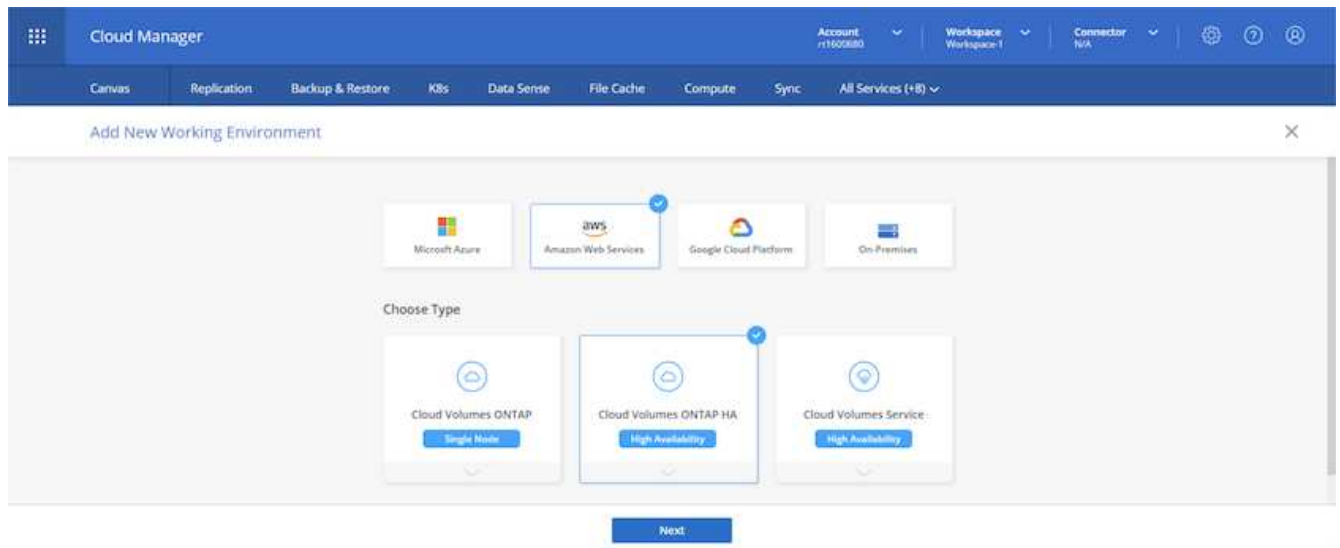
LOGIN

[Forgot your password?](#)

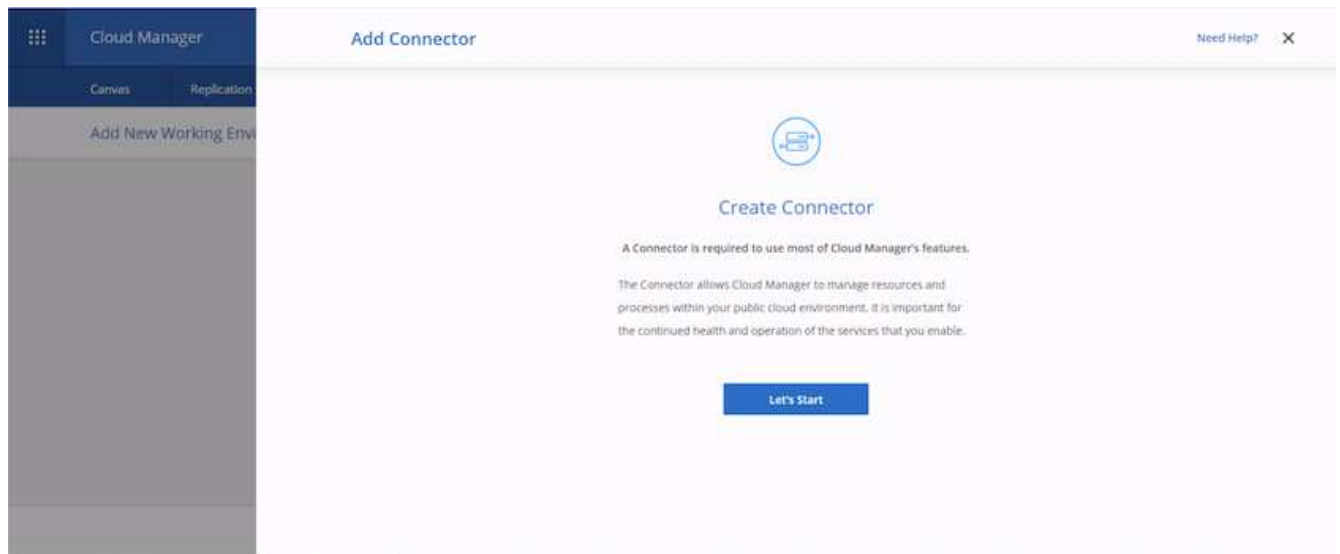
2. Nach der Anmeldung sollten Sie auf den Bildschirm gebracht werden.



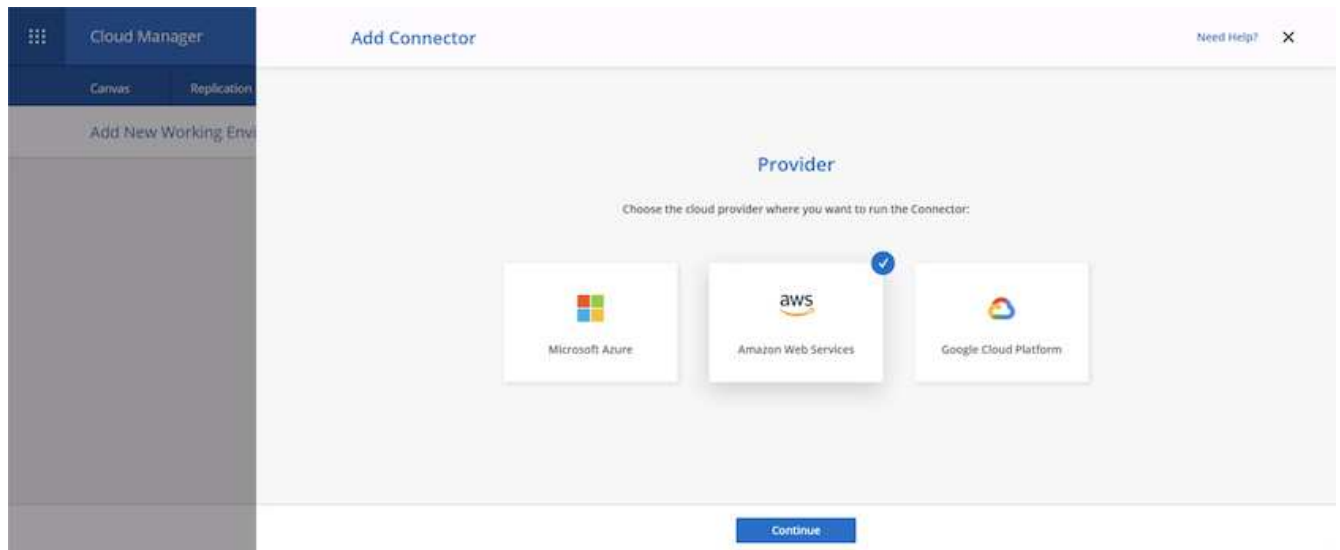
3. Klicken Sie auf „Arbeitsumgebung hinzufügen“ und wählen Sie Cloud Volumes ONTAP in AWS. Hier haben Sie außerdem die Wahl, ob Sie ein Single Node-System oder ein Hochverfügbarkeitspaar implementieren möchten. Ich habe mich entschieden, ein Hochverfügbarkeitspaar bereitzustellen.



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](#)".

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

AWS Credentials

AWS Access Key

AWS Access Key is required

AWS Secret Key

Region

us-east-1 | US East (N. Virginia)

Want to launch an instance without AWS Credentials?

Previous Next

7. Geben Sie dem Konnektor einen Namen und verwenden Sie entweder eine vordefinierte Rolle, wie auf der beschrieben ["Die NetApp Richtlinien"](#) Oder Fragen Sie Cloud Manager, welche Rolle Sie dabei spielen sollten.

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

Details

Connector Instance Name

awscloudmanager

Add Tags to Connector Instance

Connector Role

Create Role Select an existing Role

Role Name

Cloud-Manager-Operator-IBnt24j

Previous Next

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

Cloud Manager

Canvas Replication

Add New Working Environment

Add Connector

Need Help? X

Get Ready AWS Credentials Details **4 Network** 5 Security Group 6 Review

Connectivity

VPC: vpc-083fcbd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN_us-east-1a_r11600...

Key Pair: r11600680

Public IP: Enable

Proxy Configuration (Optional)

HTTP Proxy: Example: https://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

Previous Next

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.

Cloud Manager

Canvas Replication

Add New Working Environment

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network **5 Security Group** 6 Review

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

HTTP (Port 80)	HTTPS (Port 443)	SSH (Port 22)
Source Type: My IP	Source Type: My IP	Source Type: My IP
Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32

Previous Next

10. Überprüfen Sie die Informationen auf der Übersichtsseite, und klicken Sie auf Hinzufügen, um den Connector bereitzustellen.

Cloud Manager

Canvas Replication

Add New Working Environment

Add Connector Need Help? X

Get Ready AWS Credentials Details Network Security Group **Review**

Code for Terraform Automation

Connector Name	awscloudmanager
Region	us-east-1
VPC	vpc-083fcbd79f75dfb6e - 10.221.0.0/16
Subnet	10.221.4.0/24 publicSN-us-east-1a-rt1600680
Key Pair	rt1600680
Public IP	Enable
Proxy	None
Security Group	HTTP: 216.240.31.145/32, HTTPS: 216.240.31.145/32, SSH: 216.240.31.145/32

[Previous](#) [Add](#)

11. Der Connector wird nun mit einem Cloud-Formierung-Stack implementiert. Sie können den Fortschritt von Cloud Manager oder über AWS überwachen.

Cloud Manager

Canvas Replication

Add New Working Environment

Deploying a Connector

Show Details

- Keep this wizard open until the deployment process is complete. It usually takes about 7 minutes.
- No other Cloud Manager features are available during deployment.
- When the process is complete, you can continue the operation that you started.

12. Wenn die Bereitstellung abgeschlossen ist, wird eine Seite mit dem Erfolg angezeigt.

Cloud Manager

Canvas Replication

Add New Working Environment

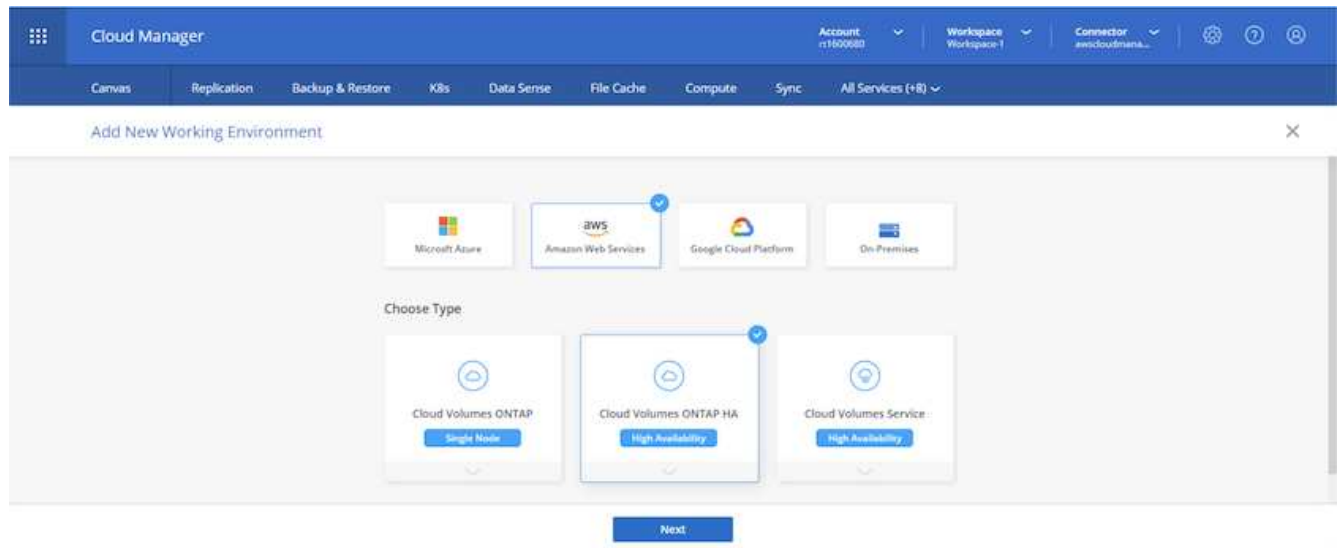
Connector Successfully Created

The Connector was created successfully.

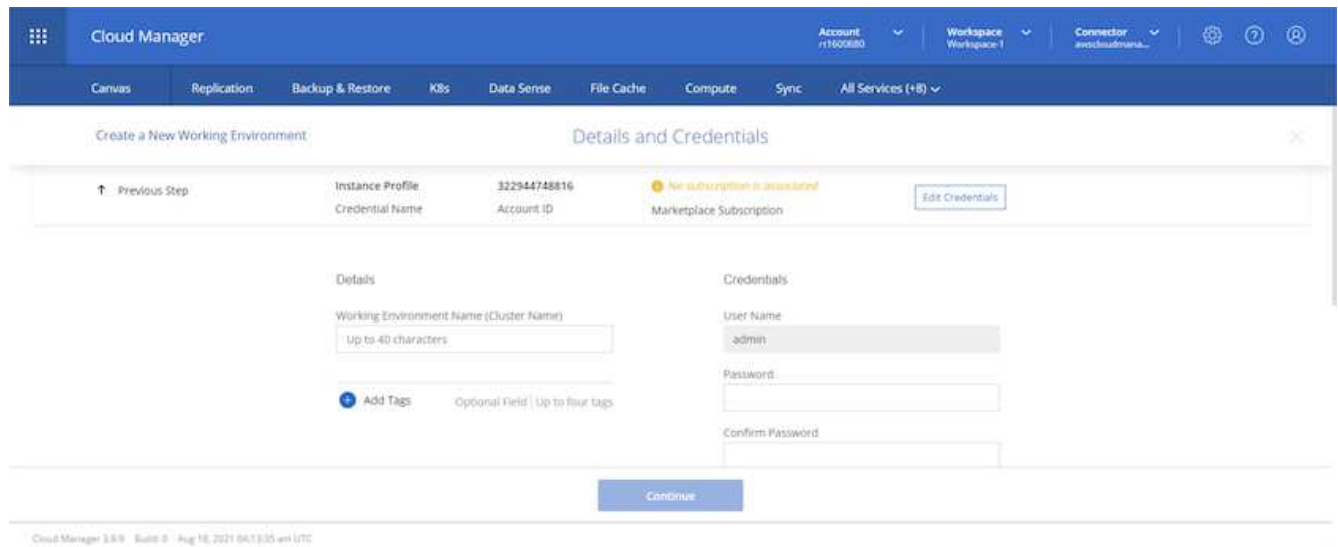
[Continue](#)

Implementieren Sie Cloud Volumes ONTAP

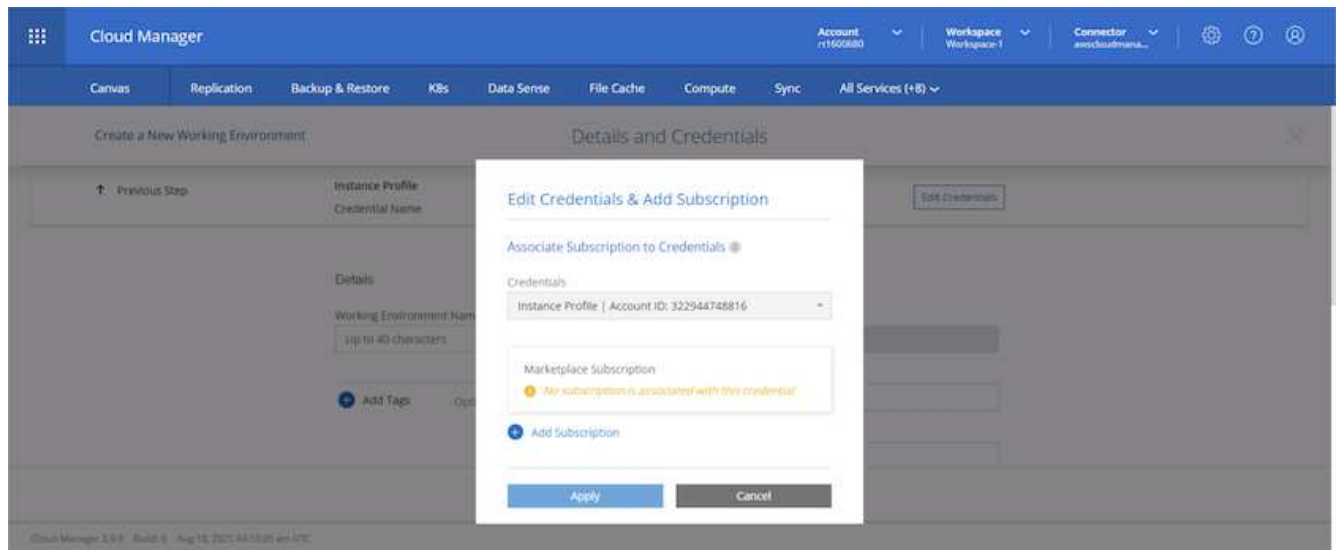
1. Wählen Sie AWS und die Art der Implementierung auf der Grundlage Ihrer Anforderungen aus.



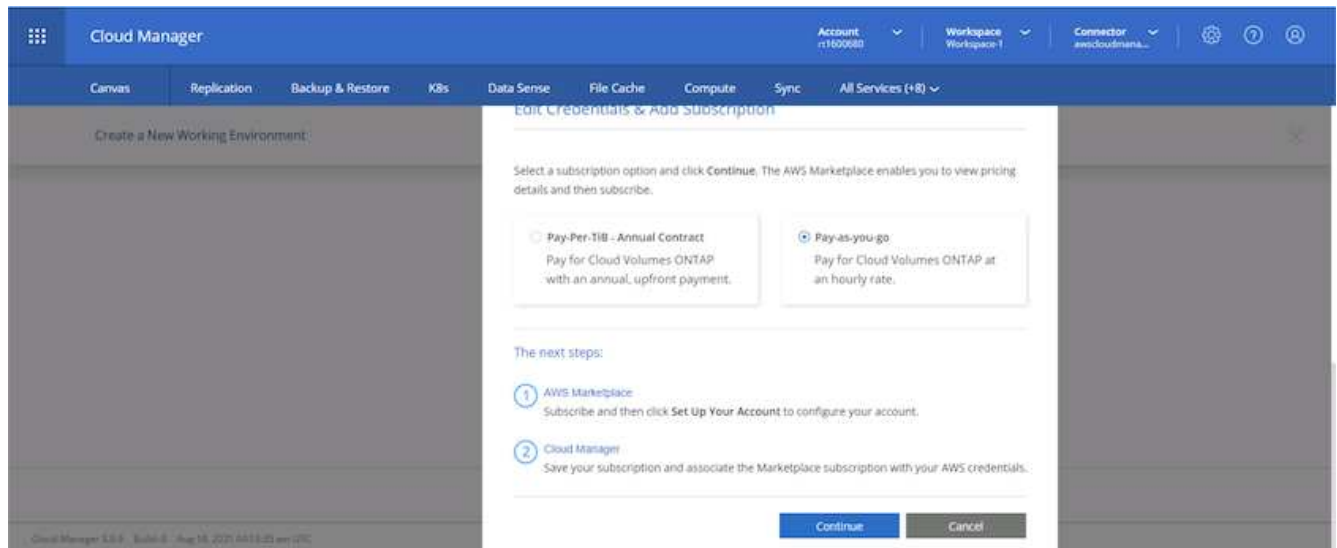
2. Wenn kein Abonnement zugewiesen wurde und Sie mit PAYGO kaufen möchten, wählen Sie Anmeldedaten bearbeiten.



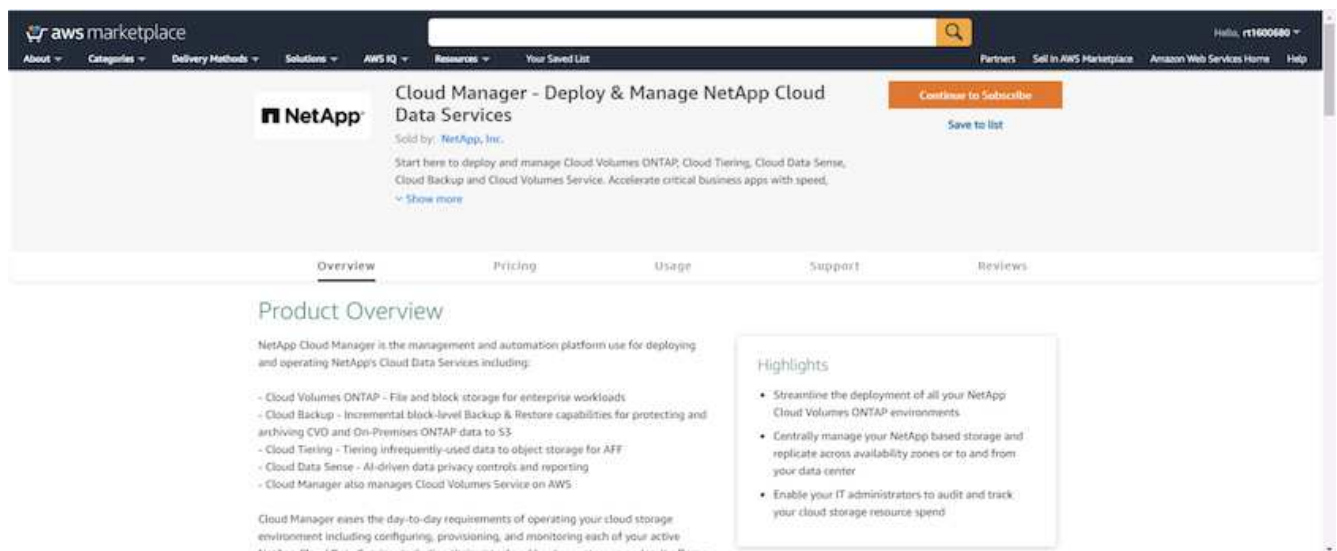
3. Wählen Sie Abonnement Hinzufügen.



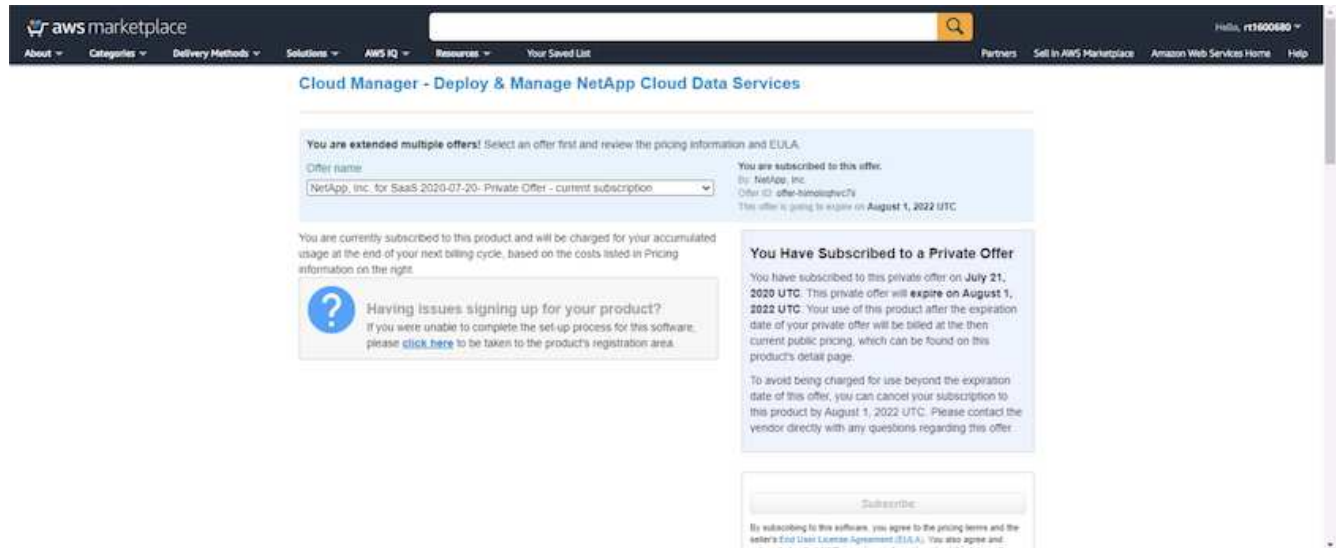
4. Wählen Sie den Vertrag aus, den Sie abonnieren möchten. Ich entschied mich für Pay-as-you-go.



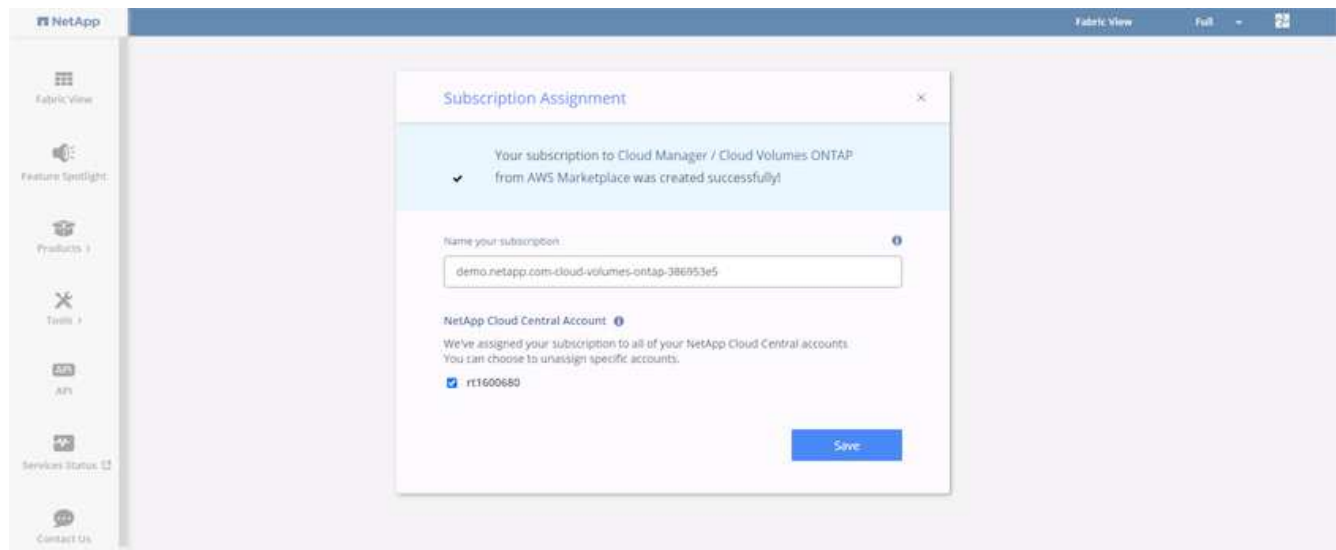
5. Sie werden zu AWS umgeleitet und wählen Sie „Weiter“, um sich Abonnieren zu öffnen.



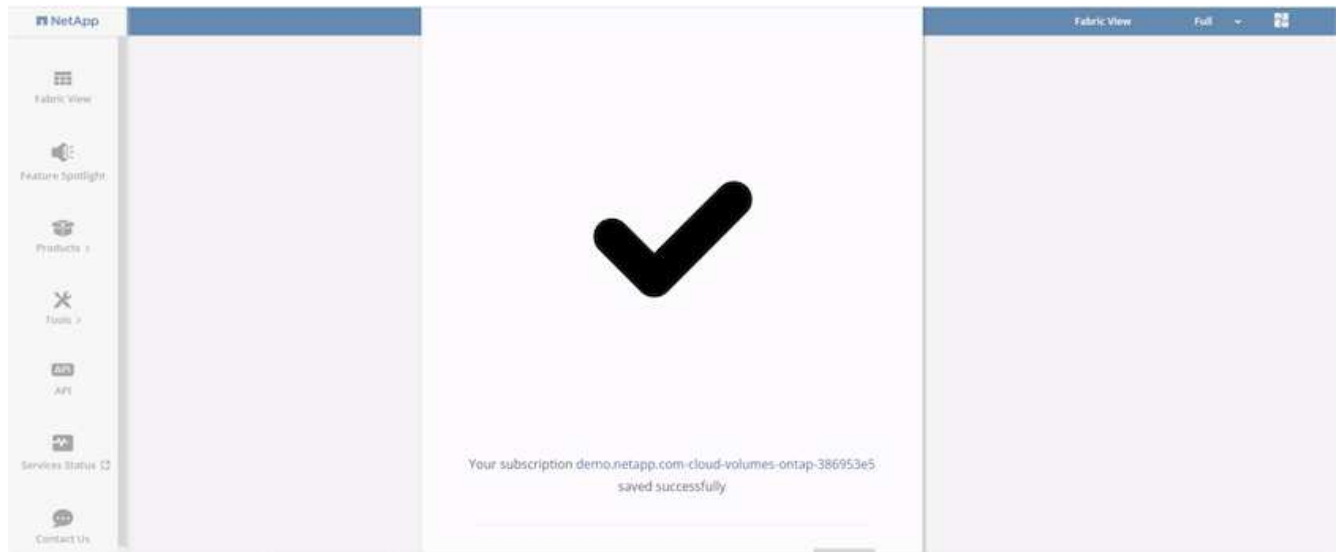
6. Melden Sie sich an und Sie werden zurück auf NetApp Cloud Central umgeleitet. Wenn Sie bereits abonniert haben und nicht umgeleitet werden, klicken Sie auf den Link "Hier klicken".



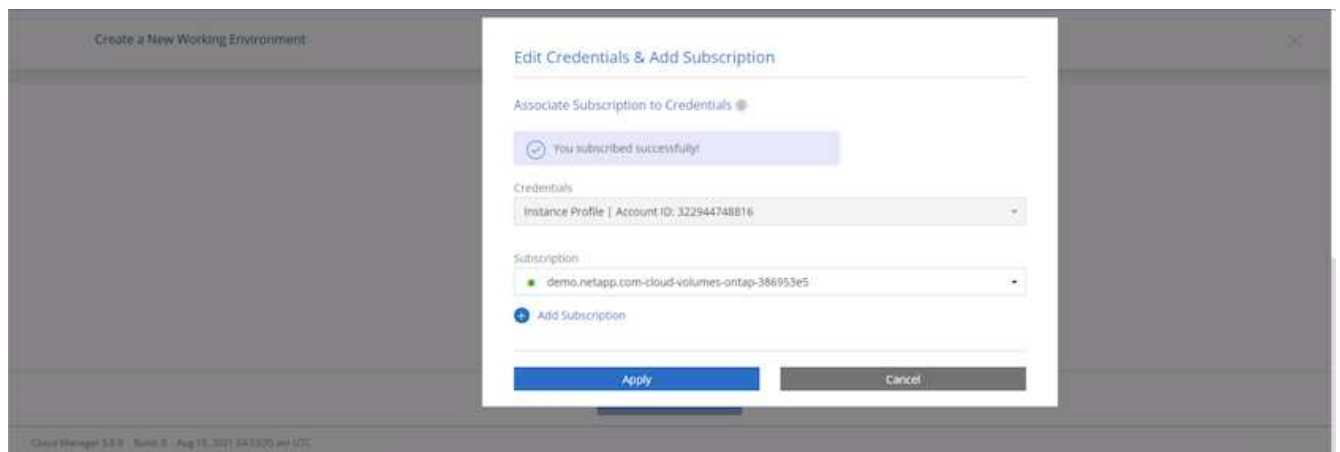
7. Sie werden zu Cloud Central umgeleitet. Dort müssen Sie die Namen Ihres Abonnements benennen und es Ihrem Cloud Central Konto zuweisen.



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.:

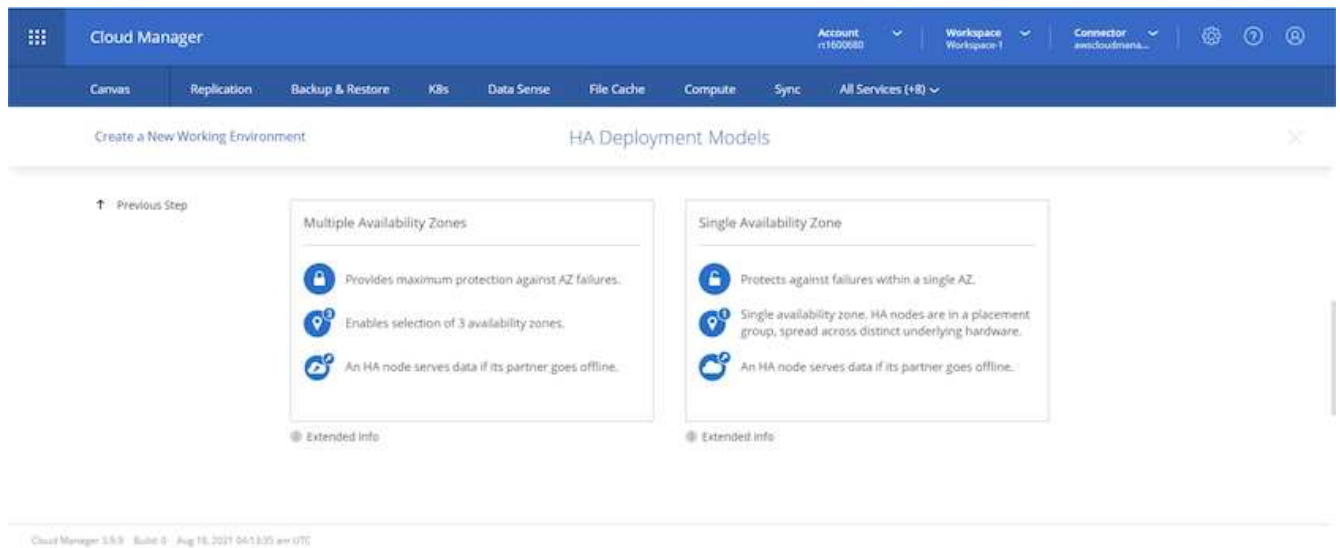
- a. Cluster-Name
- b. Cluster-Passwort
- c. AWS Tags (optional)

The screenshot shows the 'Details and Credentials' step in the 'Create a New Working Environment' wizard. The top navigation bar includes 'Cloud Manager' and various service tabs like 'Canvas', 'Replication', 'Backup & Restore', etc. The main content area is divided into 'Details' and 'Credentials' sections. In the 'Details' section, the 'Working Environment Name (Cluster Name)' is set to 'hybridawsco'. In the 'Credentials' section, the 'User Name' is 'admin', and the 'Password' and 'Confirm Password' fields are filled with masked characters. A 'Continue' button is at the bottom.

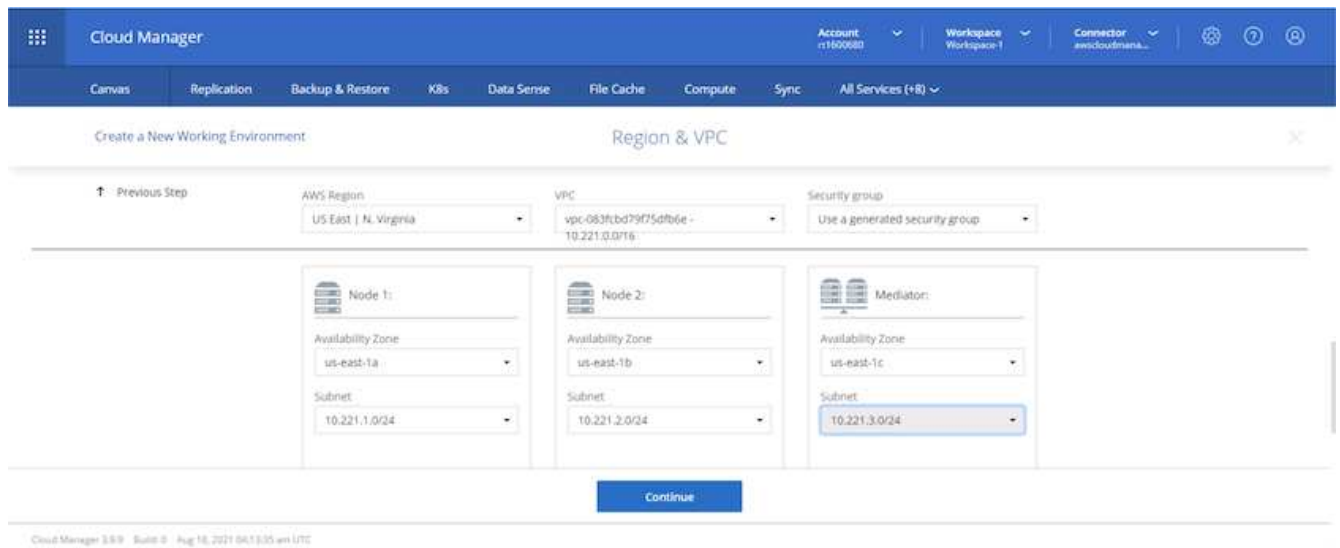
11. Wählen Sie aus, welche zusätzlichen Services Sie bereitstellen möchten. Weitere Informationen zu diesen Services finden Sie auf der ["NetApp Cloud Homepage"](#).

The screenshot shows the 'Services' step in the 'Create a New Working Environment' wizard. The top navigation bar is the same as the previous screenshot. The main content area lists three services: 'Data Sense & Compliance', 'Backup to Cloud', and 'Monitoring'. Each service has a toggle switch and a dropdown arrow, all of which are currently turned on. A 'Continue' button is at the bottom.

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.

Cloud Manager

Account: rt1600680 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Connectivity & SSH Authentication

Previous Step

Nodes

SSH Authentication Method: Password

Mediator

Security Group: Use a generated security group

Key Pair Name: rt1600680

Internet Connection Method: Public IP address

Continue

Cloud Manager 3.8.9 | Build 2 | Aug 18, 2021 06:13:35 am UTC



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"](#).

Cloud Manager

Account: rt1618349 | Workspace: Workspace-1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Floating IPs

Previous Step

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an AWS transit gateway.

You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.

Floating IP address for cluster management: 10.222.0.200

Floating IP address 1 for NFS and CIFS data: 10.222.0.201

Floating IP address 2 for NFS and CIFS data: 10.222.0.202

Floating IP address for SVM management (Optional): Enter Floating IP Address

Continue

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: #wicloudmana...

Canvas Replication Backup & Restore K8s 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-0e46720d0da10c593	1 Subnets	1 Tags

2 Route Tables | The main route table is the default for the VPC

Continue

Cloud Manager 3.8.9 Build 0 Aug 18, 2021 06:13:35 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: #wicloudmana...

Canvas Replication Backup & Restore K8s Data Sense File Cache Compute Sync All Services (+8)

Create a New Working Environment Data Encryption

Previous Step

 AWS Managed Encryption

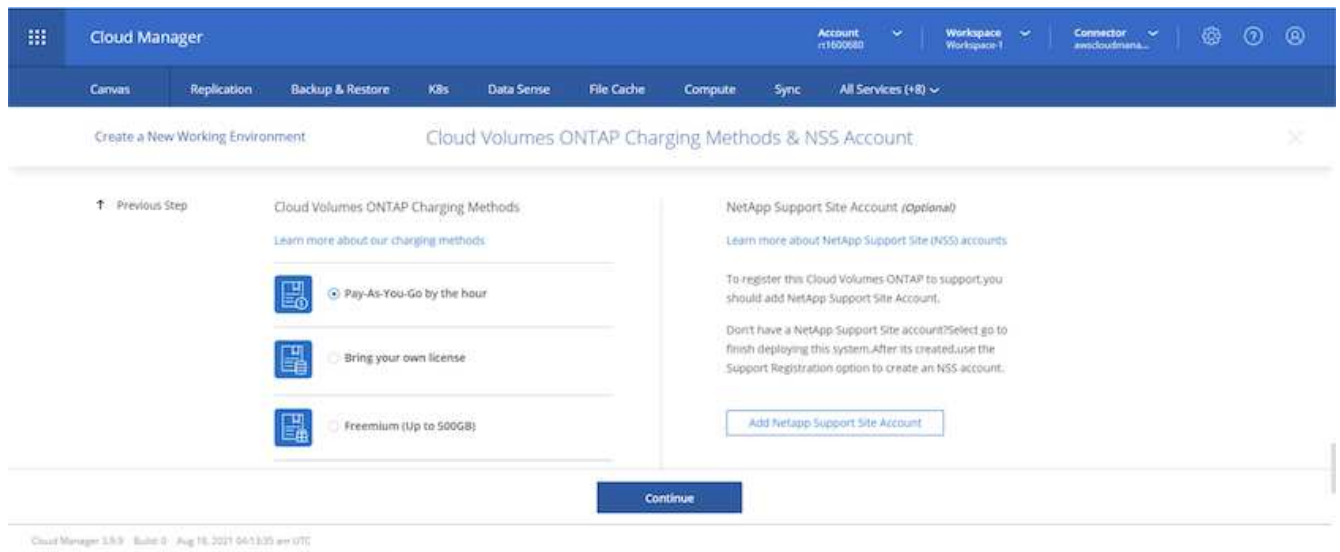
AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

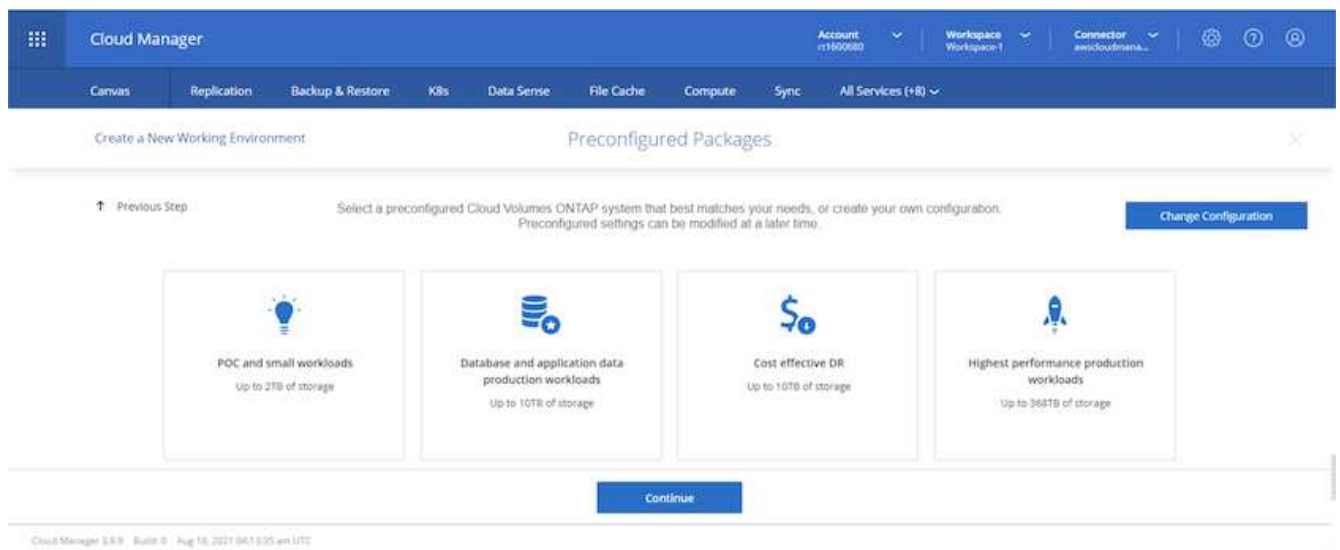
Continue

Cloud Manager 3.8.9 Build 0 Aug 18, 2021 06:13:35 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.

Cloud Manager

Account: r1600880 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Create Volume

↑ Previous Step

Details & Protection

Volume Name: | Size (GiB): | Volume size:

Snapshot Policy: | ☐ Default Policy

Protocol

NFS | CIFS | iSCSI

Access Control:

Custom export policy:

Advanced options:

Continue | Skip

Cloud Manager 3.8.9 | Build: 9 | Aug 18, 2021 04:13:35 am UTC

7. 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 Manager

Account: r1600880 | Workspace: Workspace 1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8)

Create a New Working Environment | Review & Approve

↑ Previous Step | hybridawscvo | Show API request

aws | us-east-1 | HA

☒ I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. [More information >](#)

☒ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. [More information >](#)

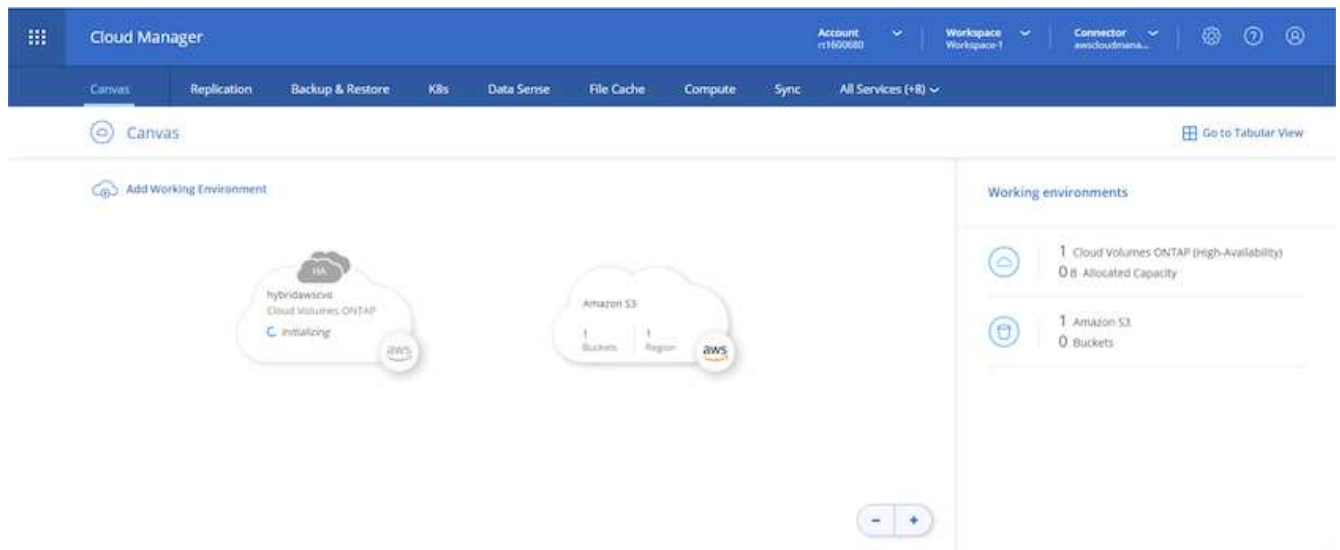
Overview | Networking | Storage

Storage System:	Cloud Volumes ONTAP HA	HA Deployment Model:	Multiple Availability Zones
License Type:	Cloud Volumes ONTAP Standard	Encryption:	AWS Managed
Capacity Limit:	10TB	Customer Master Key:	aws/ebc

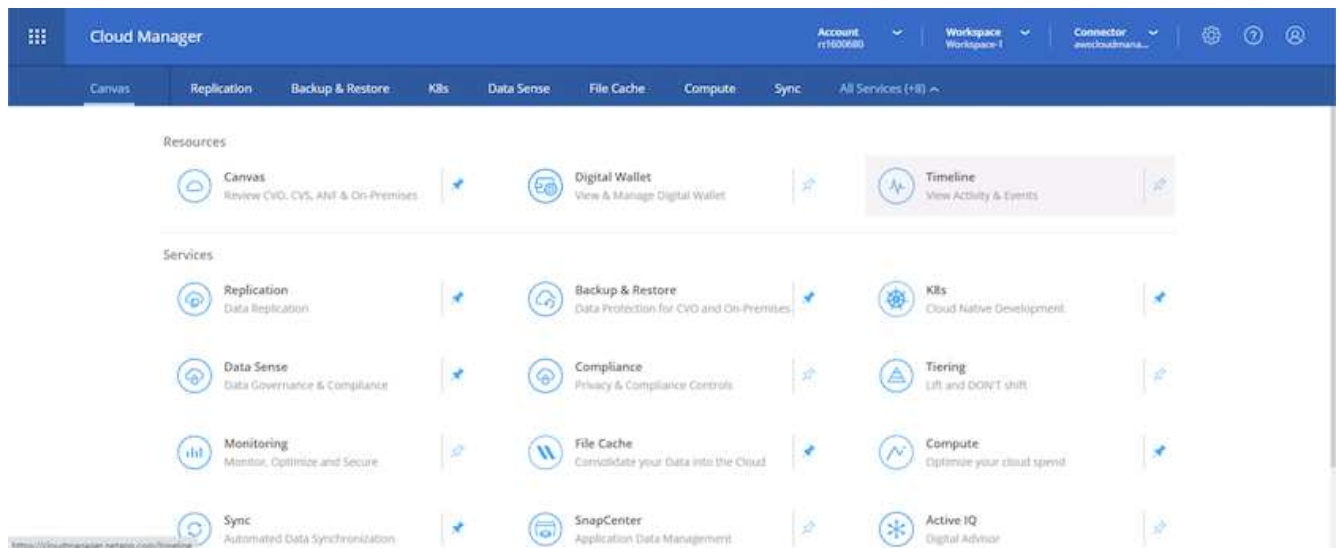
Go

Cloud Manager 3.8.9 | Build: 9 | Aug 18, 2021 04:13:35 am UTC

8. 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.

Cloud Manager Account: r1600680 Workspace: Workspace-1 Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) v

Timeline

Filters: Time (1) Service Action Agent (1) Resource User Status Reset

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudman...	hybridawsco	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawsco	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 18 2021, 10:00:53 pm	Describe Operation Status					Success

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.

Cloud Manager Account: r1600680 Workspace: Workspace-1 Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) v

Canvas

Add Working Environment

Working environments

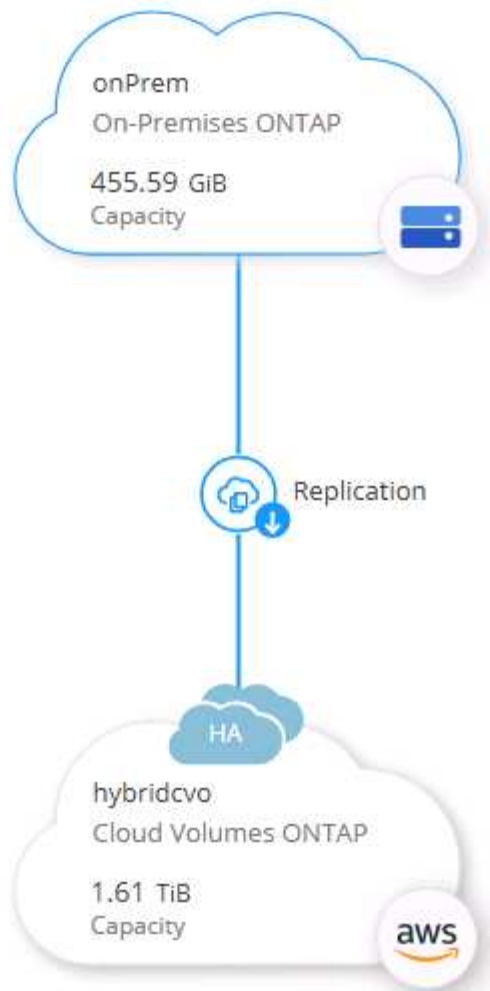
- 1 Cloud Volumes ONTAP (High-Availability) 1 GB Allocated Capacity
- 1 Amazon S3 0 Buckets

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



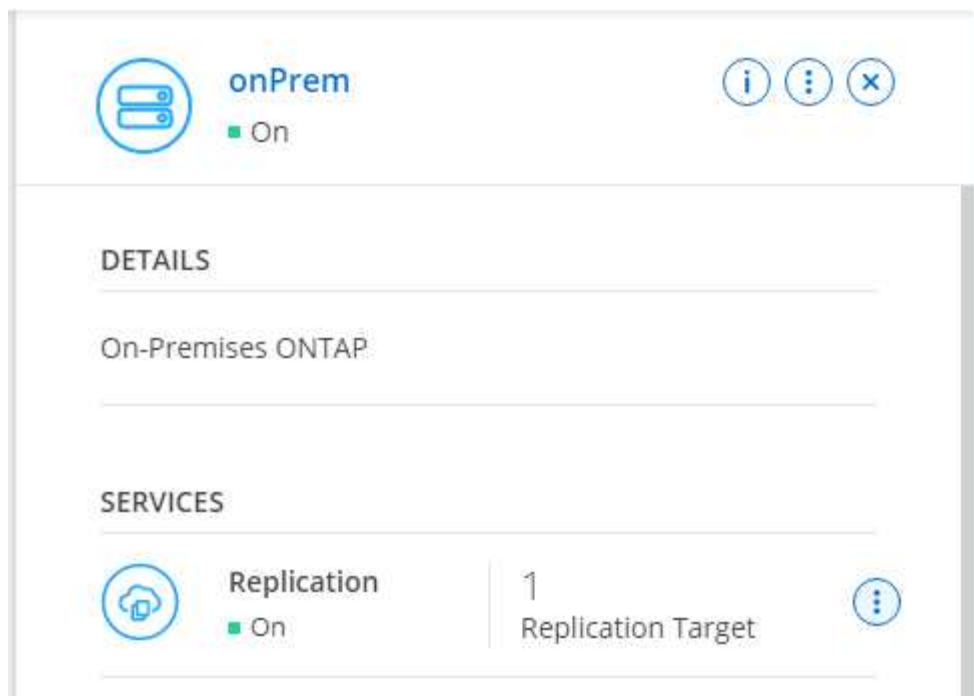
Replication

■ Off

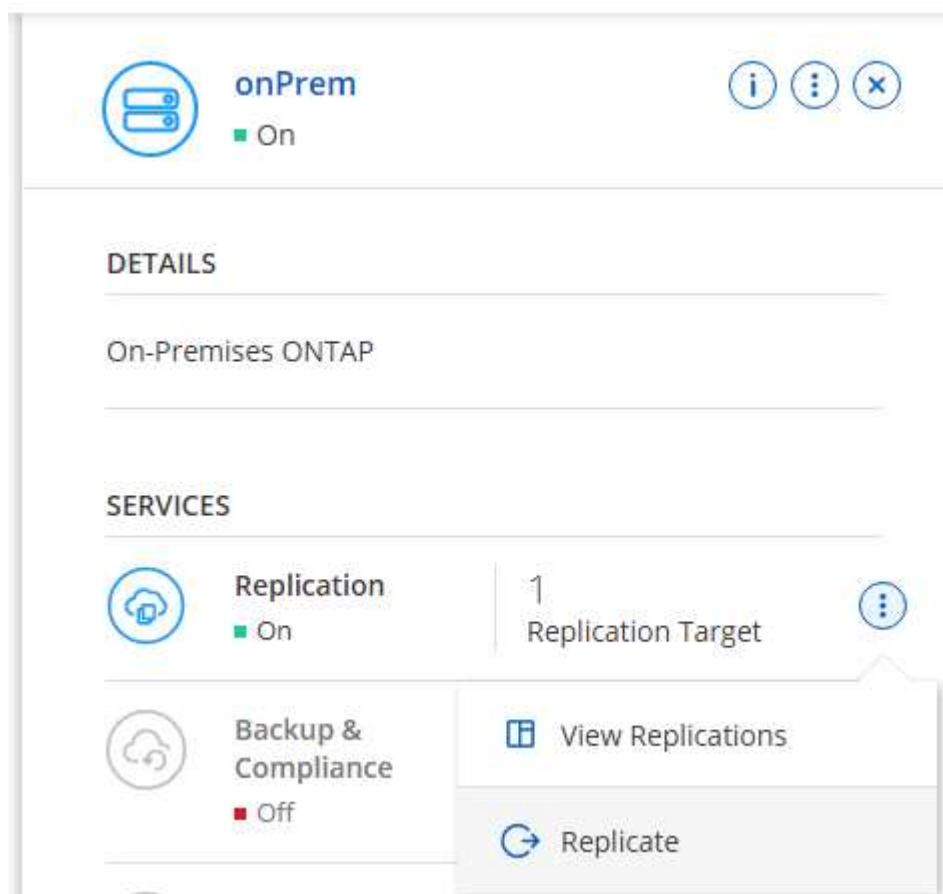
Enable



Oder Optionen.



Replizierung:



2. Wenn Sie keine Drag-and-Drop-Option haben, wählen Sie das Ziel-Cluster aus, zu dem Sie replizieren möchten.

Replicate Data

From: onPrem

To: select the Working Environment to which you want to replicate data

Replication Target

hybridcvo (Cloud Volumes ONTAP)

Start Replication Wizard

Cancel

- Wählen Sie das Volume aus, das Sie replizieren möchten. Wir haben die Daten und alle Log-Volumes repliziert.

Replication Setup
Source Volume Selection
✕

rhel2_u03
■ ONLINE

INFO

Storage VM Name: svm_onPrem

Tiering Policy: None

Volume Type: RW

CAPACITY

100 GB
Allocated

■ 7.29 GB
Disk Used

rhel2_u0309232119421203118
■ ONLINE

INFO

Storage VM Name: svm_onPrem

Tiering Policy: None

Volume Type: RW

CAPACITY

100 GB
Allocated

■ 35.83 MB
Disk Used

sql1_data
■ ONLINE

INFO

Storage VM Name: svm_onPrem

Tiering Policy: None

Volume Type: RW

CAPACITY

53.37 GB
Allocated

■ 45.09 GB
Disk Used

sql1_log
■ ONLINE

INFO

Storage VM Name: svm_onPrem

Tiering Policy: None

Volume Type: RW

CAPACITY

21.35 GB
Allocated

■ 18.16 GB
Disk Used

sql1_snapctr
■ ONLINE

INFO

Storage VM Name: svm_onPrem

Tiering Policy: None

Volume Type: RW

CAPACITY

24.87 GB
Allocated

■ 21.23 GB
Disk Used

Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC

- 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.

Replication Setup Destination Disk Type and Tiering ×


[↑ Previous Step](#)

Destination Disk Type

General Purpose SSD

General Purpose SSD - Dynamic Performance

Throughput Optimized HDD

 S3 Tiering [What are storage tiers?](#)

☒ Enabled ☐ Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

[Continue](#)

Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC

5. Wählen Sie den Zielvolumennamen: Wir haben ausgewählt `[source_volume_name]_dr`.

Destination Volume Name

Destination Volume Name

sql1_data_dr

Destination Aggregate

Automatically select the best aggregate

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-Volume 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-Volume und einen „stündlichen“ Zeitplan für die Log-Volumes, wobei diese jedoch je nach Anforderungen geändert werden können.

Replication Setup

Schedule

Previous Step

Select a replication schedule

One-time copy

No schedule

10min

Every hour
Minutes: 0th, 10th, 20th, 3...

12-hourly

Every day
Hours: 12 AM and 12 PM
Minutes: 15th minute

5min

Every hour
Minutes: 0th, 5th, 10th, 15t...

6-hourly

Every day
Hours: 12 AM, 6 AM, 12 PM...
Minutes: 15th minute

8hour

Every day
Hours: 2 AM, 10 AM and 6 ...
Minutes: 15th minute

daily

Every day
Hours: 12 AM
Minutes: 10th minute

hourly

Every hour
Minutes: 5th minute

monthly

Every month
Days: 2nd
Hours: 12 AM
Minutes: 20th minute

pg-15-minutely

Every hour

pg-6-hourly

Every day

pg-daily

Every day

pg-daily-set2

Every day

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.

Replication Setup

Review & Approve

Previous Step

Review your selection and start the replication process

Source

onPrem

sql1_data

Destination

hybridcvo

sql1_data_copy

☒ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements.
 [More information >](#)

Source Volume Allocated Size:

53.37 GB

Source Volume Used Size:

45.09 GB

Source Thin Provisioning:

Yes

Destination Volume Allocated Size:

53.37 GB

Destination Volume Disk Type:

General Purpose SSD (...)

Capacity Tiering:

S3

Destination Thin Provisioning:

Yes

Destination Aggregate:

aggr1 (Automatically s...

Destination Storage VM:

svm_hybridcvo

Max Transfer Rate:

100 MB/s

SnapMirror Policy:

Mirror

Replication Schedule:

daily

10. Setzen Sie diesen Prozess für Datenvolumen und Protokoll-Volumes 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.

Replication

7 Volume Relationships

153.32 GiB Replicated Capacity

0 Currently Transferring

7 Healthy

0 Failed

7 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	
✓	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AI 19.73 MiB	...
✓	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB	...
✓	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB	...
✓	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AI 24.56 KiB	...

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.

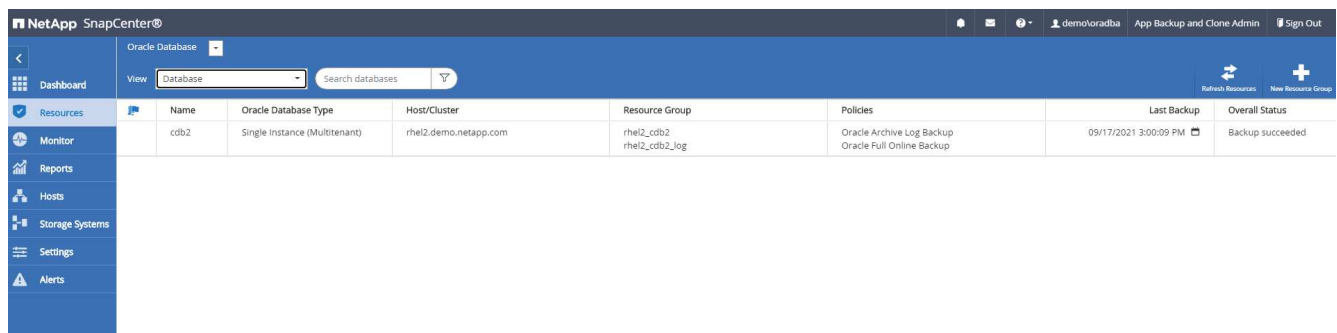
1. Rufen Sie das Windows-Administratorpasswort ab, um sich über RDP bei einer Instanz anzumelden.
2. Deaktivieren Sie die Windows-Firewall, treten Sie der Windows SnapCenter-Domäne des Hosts bei und fügen Sie die Instanz zum DNS-Server zur Namensauflösung hinzu.
3. Bereitstellen eines SnapCenter-Protokollvolumens 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

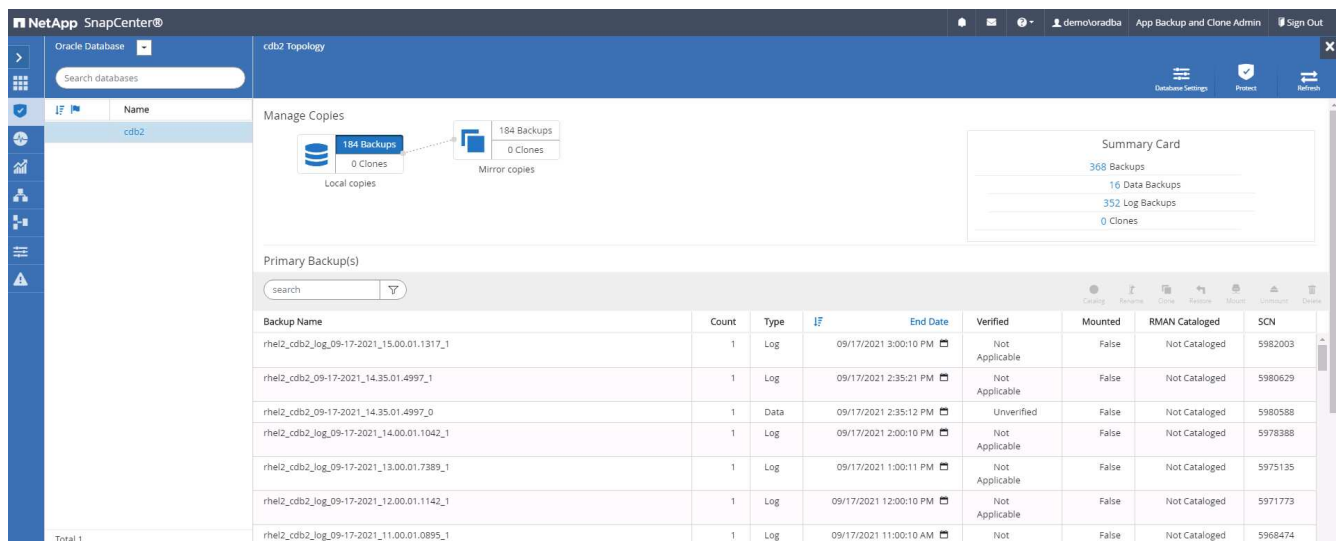
Die Agilität der Public Cloud, die Amortisierung und die Kosteneinsparungen sind sinnvolle Vorteile für Unternehmen, die sich für die Entwicklung und das Testen von Datenbankapplikationen durch die Public Cloud entscheiden. Es gibt kein besseres Werkzeug als SnapCenter, um dies Wirklichkeit werden zu 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.

NetApp SnapCenter®

Oracle Database

Search databases

cdb2

Manage Copies

184 Backups
0 Clones
Local copies

184 Backups
0 Clones
Mirror copies

Summary Card

368 Backups
16 Data Backups
352 Log Backups
0 Clones

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	IF	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
Total 1								

4. 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.

Mount backups

Choose the host to mount the backup: ora-standby.demo.netapp.com

Mount path: /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2

Secondary storage location: Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

Mount Cancel

NetApp SnapCenter®

Oracle Database

Search databases

cdb2 Topology

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)

search

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_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
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_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_log_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



Wenn die Protokollbeschneidung aktiviert ist und der Wiederherstellungspunkt über den letzten Protokollschnitt hinaus erweitert wird, müssen möglicherweise mehrere Archiv-Log-Backups eingebunden werden.

- 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
rhel2_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
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_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_log_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

- 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

cdb2test

Exclude PDBs

Type to find PDBs

☐ PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume

svm_onPrem:rhel2_u02

Destination Volume

svm_hybridcvo:rhel2_u02_dr

Logs

Source Volume

svm_onPrem:rhel2_u03

Destination Volume

svm_hybridcvo:rhel2_u03_dr

Previous

Next

- 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

5

6

7

Select the host to create a clone

Clone host
ora-standby.demo.netapp.com

Datafile locations ⓘ

/u02_cdb2test
Reset

Control files ⓘ

/u02_cdb2test/cdb2test/control/control01.ctl
/u02_cdb2test/cdb2test/control/control02.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
<div> <div> RedoGroup 1 </div> <div> </div> </div>	200	MB	1
/u02_cdb2test/cdb2test/redolog/redo03.log			
<div> <div> RedoGroup 2 </div> <div> </div> </div>	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

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

/u01/app/oracle/product/19800/cdb2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

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

5

6

7

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/
Enter Prescript path

Arguments

Script timeout

60
secs

Database Parameter settings

Previous
Next

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

☐ Date and Time

☒ Until SCN (System Change Number)

5980629

Date-time format: MM/DD/YYYY hh:mm:ss

Specify external archive log locations

/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/

☒ 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

```

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

Never

From

From email

To

Email to

Subject

Notification

☐ 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.

✕

Previous

Next

12. Zusammenfassung des Klons:

Clone from cdb2

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

Summary

Clone from backup	rhel2_cdb2_09-17-2021_14.35.01.4997_0
Clone SID	cdb2test
Clone server	ora-standby.demo.netapp.com
Exclude PDBs	none
Oracle home	/u01/app/oracle/product/19800/cdb2
Oracle OS user	oracle
Oracle OS group	oinstall
Datafile mountpaths	/u02_cdb2test
Control files	/u02_cdb2test/cdb2test/control/control01.ctl /u02_cdb2test/cdb2test/control/control02.ctl
Redo groups	RedoGroup =1 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo03.log RedoGroup =2 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo02.log RedoGroup =3 TotalSize =200 Path =/u02_cdb2test/cdb2test/redolog/redo01.log
Recovery scope	Until SCN 5980629
Prescript full path	none
Prescript arguments	
Postscript full path	none
Postscript arguments	

Previous

Finish

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

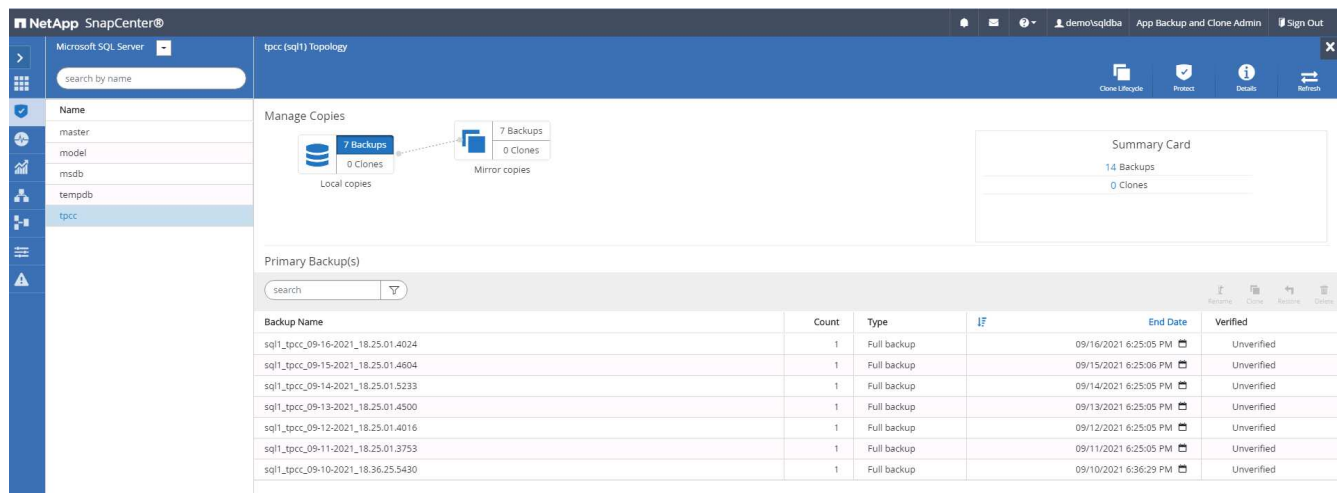
1. Melden Sie sich mit einer Datenbank-Management-Benutzer-ID für SQL Server bei SnapCenter an. Navigieren Sie zur Registerkarte Ressourcen, die die SQL Server-Benutzerdatenbanken anzeigt, die durch SnapCenter geschützt sind, und eine Ziel-Standby-SQL-Instanz in der Public Cloud.



The screenshot shows the NetApp SnapCenter interface for Microsoft SQL Server. The left sidebar contains navigation options: Dashboard, Resources, Monitor, Reports, Hosts, Storage Systems, Settings, and Alerts. The main area displays a table of databases with columns: Name, Instance, Host, Last Backup, Overall Status, and Type. The table lists several databases including master, model, msdb, tempdb, and their standby instances.

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 diagram with 'Local copies' (7 Backups, 0 Clones) and 'Mirror copies' (7 Backups, 0 Clones). Below the diagram is a table of primary backups with columns: Backup Name, Count, Type, End Date, and Verified. The table lists several full backup entries with their respective dates and verification status.

Backup Name	Count	Type	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

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

search by name

Clone Library | Protect | Details | Backup

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	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_09-15-2021_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

search by name

Clone Library | Protect | Details | Backup

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	if	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
Choose

Clone instance
Nothing selected

Clone name
tpcc

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

- 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

sql-standby.demo.netapp.com

Clone instance

sql-standby

Clone name

tpcc_clone

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. 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

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

☐ All log backups

☒ By log backups until

9/17/2021 6:25:10 PM

☐ By specific date until

09/17/2021 6:25:05 PM

☐ None

Previous

Next

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

Choose optional arguments...

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

8. Konfigurieren Sie einen SMTP-Server, wenn eine E-Mail-Benachrichtigung gewünscht wird.

217

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ 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.

✕

Previous

Next

9. Zusammenfassung Klonen.

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_dev

Mount option

Auto assign volume mount point under custom path

Prescript full path

None

Prescript arguments

Postscript full path

None

Postscript arguments

Send email

No

Previous

Finish

- Überwachen Sie den Job-Status und überprüfen Sie, ob die vorgesehene Benutzerdatenbank mit einer Ziel-SQL-Instanz im Cloud-Klon-Server verbunden wurde.

NetApp SnapCenter®						
Jobs - Filter						
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:sqlqdba	
763	✓	Discover resources for all hosts	09/16/2021 7:56:49 PM	09/16/2021 7:56:54 PM	demo:sqlqdba	
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:sqlqdba	
760	⚠	Discover resources for all hosts	09/16/2021 7:19:05 PM	09/16/2021 7:19:09 PM	demo:sqlqdba	
759	⚠	Discover resources for all hosts	09/16/2021 7:18:43 PM	09/16/2021 7:18:48 PM	demo:sqlqdba	
756	⚠	Discover resources for all hosts	09/16/2021 6:59:51 PM	09/16/2021 6:59:56 PM	demo:sqlqdba	
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:sqlqdba	
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:sqlqdba	
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:sqlqdba	

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?

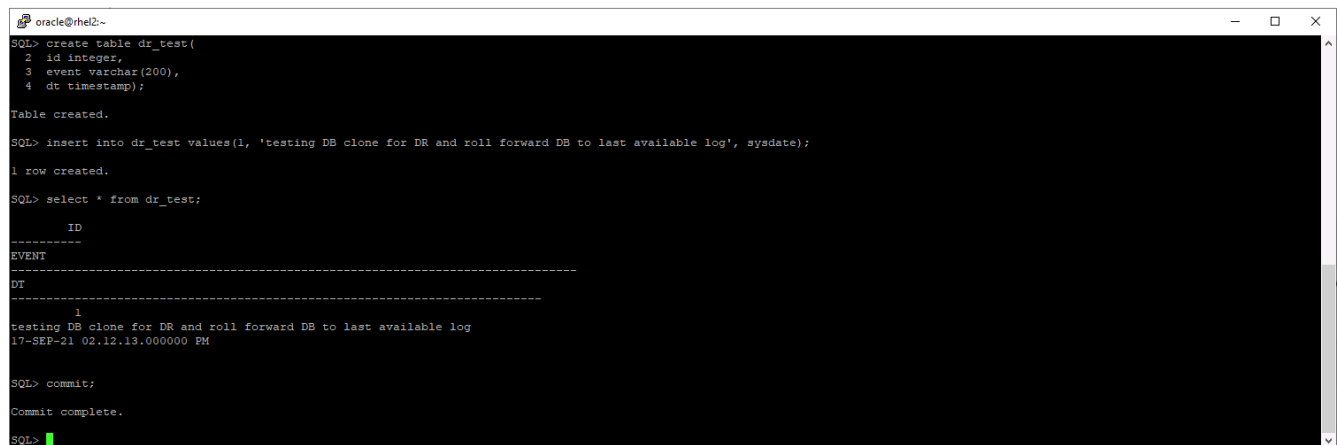
Wenn Sie Hilfe bei dieser Lösung und bei den Anwendungsfällen benötigen, treten Sie dem bei ["NetApp Solution Automation Community unterstützt Slack-Channel"](#) Und suchen Sie den Kanal zur Lösungsautomatisierung, um Ihre Fragen zu stellen oder zu fragen.

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.

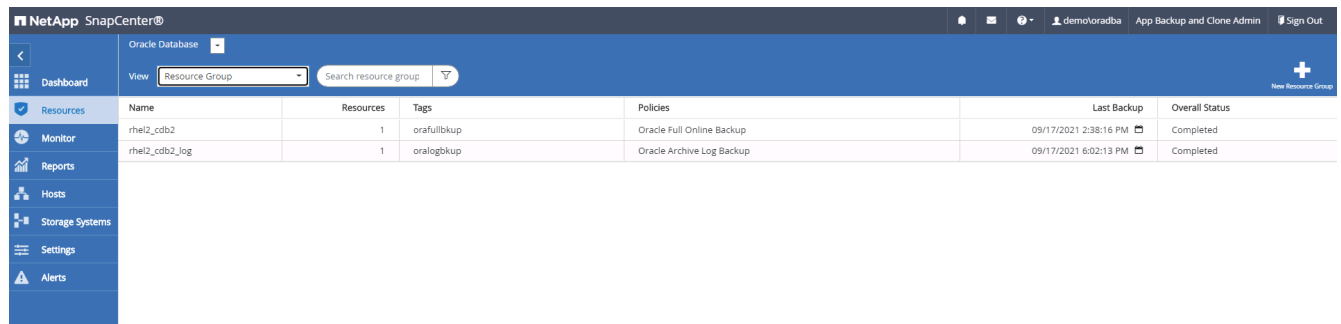
SQL> select * from dr_test;

      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.



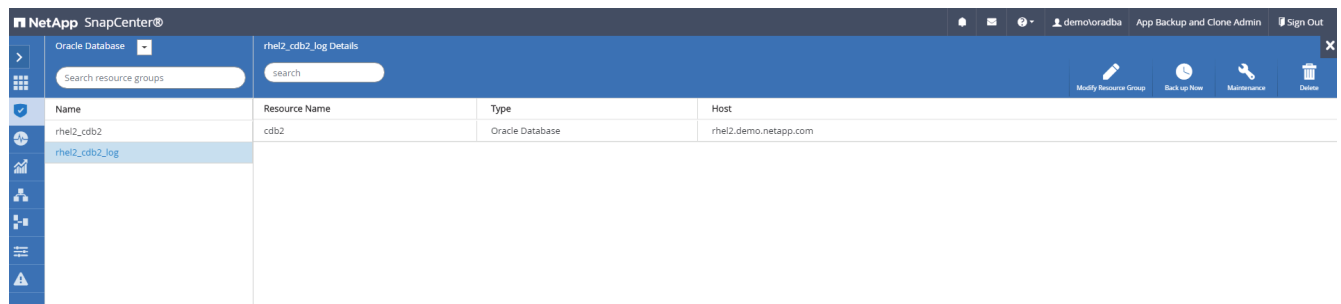
NetApp SnapCenter® Oracle Database

View: Resource Group Search resource group

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

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

- 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.



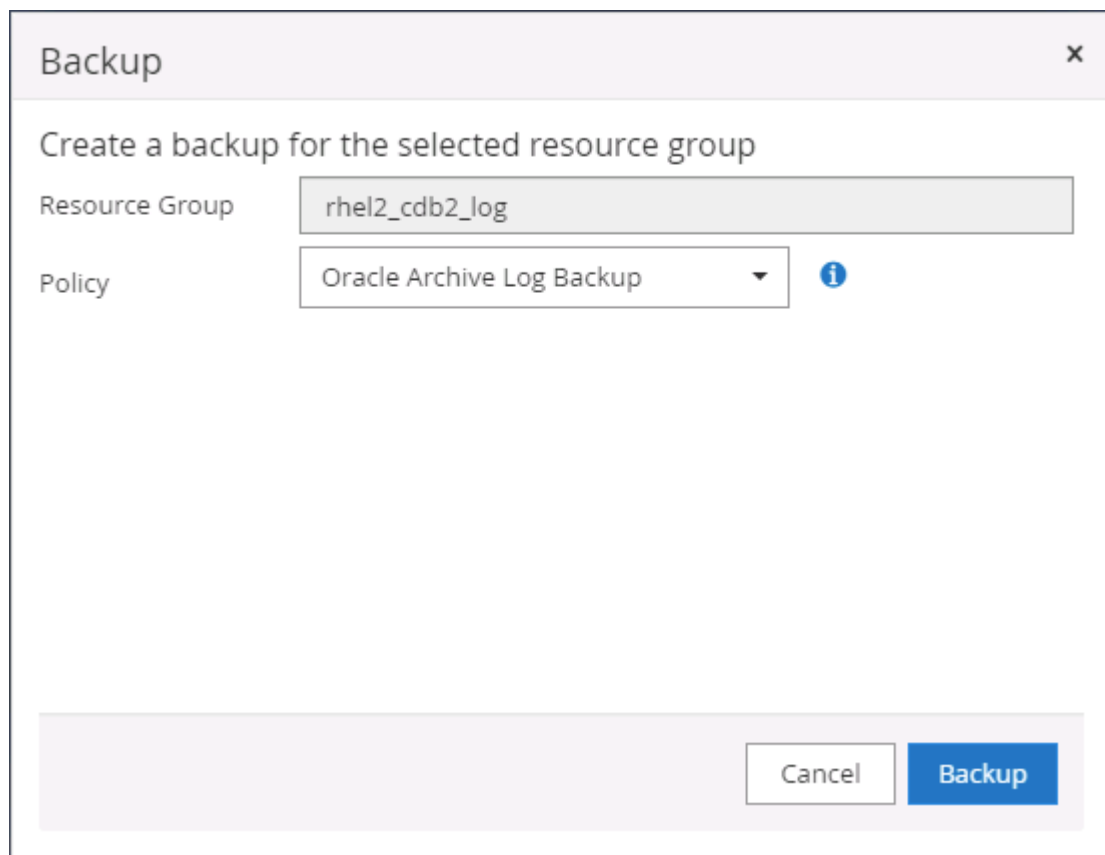
NetApp SnapCenter® Oracle Database

Search resource groups

rhel2_cdb2_log Details

Name	Resource Name	Type	Host
rhel2_cdb2	cdb2	Oracle Database	rhel2.demo.netapp.com
rhel2_cdb2_log			

Modify Resource Group Back up Now Maintenance Delete



Backup

Create a backup for the selected resource group

Resource Group: rhel2_cdb2_log

Policy: Oracle Archive Log Backup

Cancel Backup



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 an Oracle Database. The left sidebar contains navigation icons. The main area displays the 'cdb2 Topology' with a 'Manage Copies' section showing 'Local copies' (185 Backups, 0 Clones) and 'Mirror copies' (185 Backups, 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. Three backup entries are listed, all with a count of 1 and type 'Log'.

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 'Mount backups' dialog box is shown. It has a title bar with a close button. The first section is 'Choose the host to mount the backup' with a dropdown menu showing 'ora-standby.demo.netapp.com'. The second section is 'Mount path : /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2'. The third section is 'Secondary storage location : Snap Vault / Snap Mirror'. It contains two columns: 'Source Volume' and 'Destination Volume'. Under 'Source Volume' is 'svm_onPrem:rhel2_u03'. Under 'Destination Volume' is a dropdown menu showing 'svm_hybridcvo:rhel2_u03_dr'. At the bottom right are 'Mount' and 'Cancel' buttons.

5. Wählen Sie das letzte vollständige Datenbank-Backup aus und klicken Sie auf Klonen, um den Klon-Workflow zu initiieren.

NetApp SnapCenter®

Oracle Database

Search databases

cdb2 Topology

Manage Copies

Local copies: 185 Backups, 0 Clones

Mirror copies: 185 Backups, 2 Clones

Summary Card

- 370 Backups
- 16 Data Backups
- 354 Log Backups
- 2 Clones

Secondary Mirror Backup(s)

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	True	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
rhel2_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
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_log_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

Total 3

6. Wählen Sie eine eindeutige Clone-DB-ID auf dem Host aus.

Clone from cdb2

1 Name

Complete Database Clone

Clone SID:

Exclude PDBs:

PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume: svm_onPrem:rhel2_u02

Destination Volume:

Logs

Source Volume: svm_onPrem:rhel2_u03

Destination Volume:

Previous Next

7. Stellen Sie ein Protokoll-Volume 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

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

EVENTS & JOBS

PROTECTION

HOSTS

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$ 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/nvme0nlp2             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:/Sc39c05df8-4b00-4b3a-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-Volume 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.

224

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
ora-standby.demo.netapp.com

Datafile locations ⓘ

/u02_cdb2dr
Reset

Control files ⓘ

/u02_cdb2dr/cdb2dr/control/control01.ctl
/u03_cdb2dr/cdb2dr/control/control02.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
<div> RedoGroup 1 </div>	200	MB	1
/u03_cdb2dr/cdb2dr/redolog/redo03.log			
<div> RedoGroup 2 </div>	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

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

/u01/app/oracle/product/19800/cdb2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

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

5

6

7

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

+
Reset

Previous

Next

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

/var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1/orareco/CDB2/archivelog/

☒ Create new DBID*i*

☒ Create tempfile for temporary tablespace*i*

i

Previous

Next

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

Never

From

From email

To

Email to

Subject

Notification

☐ 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.

✕

Previous

Next

13. Zusammenfassung DES DR-Klons:

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Summary

Clone from backup

rhe12_cdb2_09-17-2021_14.35.01.4997_0

Clone SID

cdb2dr

Clone server

ora-standby.demo.netapp.com

Exclude PDBs

none

Oracle home

/u01/app/oracle/product/19800/cdb2

Oracle OS user

oracle

Oracle OS group

oinstall

Datafile mountpaths

/u02_cdb2dr

Control files

/u02_cdb2dr/cdb2dr/control/control01.ctl
/u03_cdb2dr/cdb2dr/control/control02.ctl

Redo groups

RedoGroup =1 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo03.log
RedoGroup =2 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo02.log
RedoGroup =3 TotalSize =200 Path =/u03_cdb2dr/cdb2dr/redolog/redo01.log

Recovery scope

Until Cancel

Prescript full path

none

Prescript arguments

Postscript full path

none

Postscript arguments

Previous

Finish

- Geklonte DBs sind sofort nach Abschluss des Klon mit SnapCenter registriert und sind dann für den Backup-Schutz verfügbar.

NetApp SnapCenter®							
<div> <div>Oracle Database</div> <div>View Database</div> <div>Search databases</div> </div>							
	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

- 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-Volume.
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 rekonstruiert 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.

```

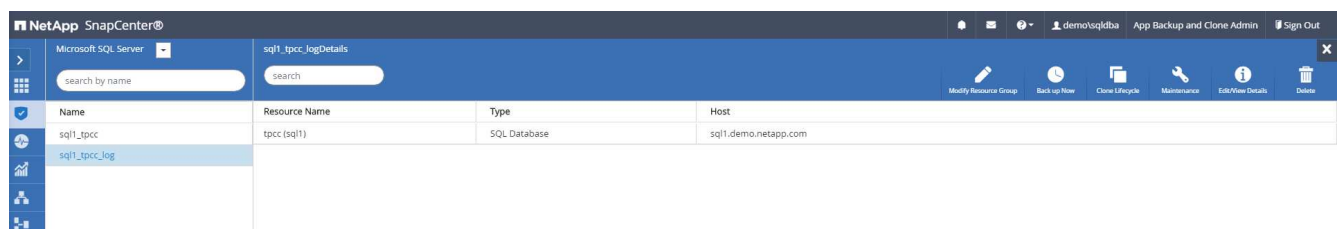
Administrator Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

-----
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>

```

2. 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.



3. Führen Sie ein Protokoll-Backup manuell aus, um die letzte Transaktion auszuführen, die in den sekundären Storage in der Public Cloud repliziert werden soll.

Backup

Create a backup for the selected resource group

Resource Group

Policy

4. Wählen Sie das letzte vollständige SQL Server-Backup für den Klon aus.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

search by name

Clone Lifecycle Protect Details Refresh

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 2 Clones

Summary Card

14 Backups

2 Clones

Secondary Mirror Backup(s)

search

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 Klonnamen und die Mount-Option. Der sekundäre Storage-Standort, an dem das Klonen durchgeführt wird, ist automatisch gefüllt.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

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

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

☒ All log backups

☐ By log backups until

9/19/2021 6:25:10 PM

☐ By specific date until

09/19/2021 6:25:05 PM

☐ None

Previous

Next

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

Choose optional arguments...

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

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

Never

From

From email

To

Email to

Subject

Notification

☐ 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.

✕

Previous

Next

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	
Monitor	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	
Storage Systems	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	
Alerts	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	

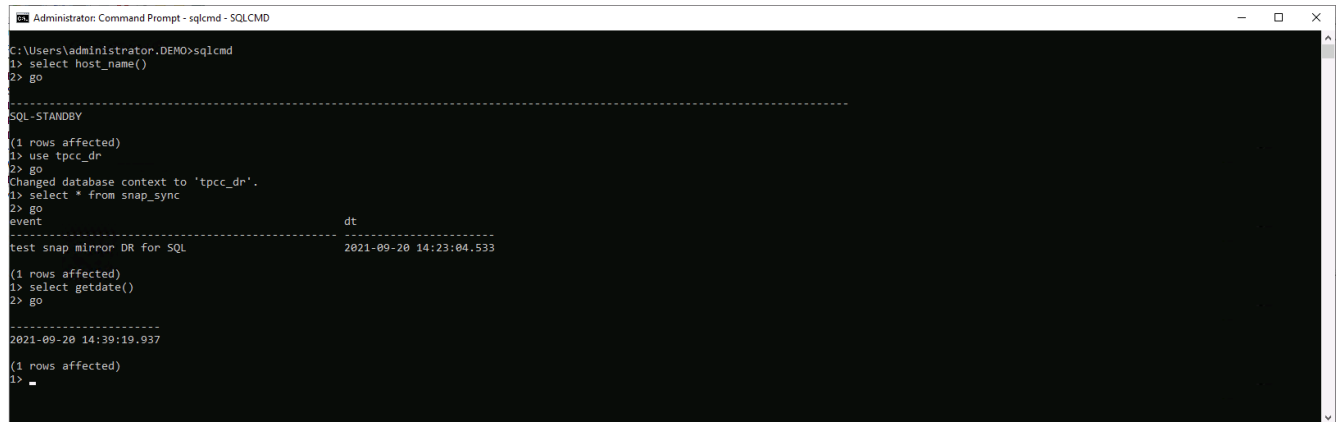
Validierung und Konfiguration von SQL-Klonen nach dem DR-Verfahren

- Überwachen des Auftragsstatus von Klonen.

NetApp SnapCenter®							
Jobs Schedules Events Logs							
search by name							
Jobs - Filter	ID	Status	Name	Start date	End date	Owner	
Monitor	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 2:28:17 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	

- 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-Volume.
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.

Copyright-Informationen

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

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

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