



# Erste Schritte – Übersicht

## NetApp Solutions

NetApp  
April 25, 2024

This PDF was generated from [https://docs.netapp.com/de-de/netapp-solutions/databases/hybrid\\_dbops\\_snapcenter\\_getting\\_started\\_onprem.html](https://docs.netapp.com/de-de/netapp-solutions/databases/hybrid_dbops_snapcenter_getting_started_onprem.html) on April 25, 2024. Always check docs.netapp.com for the latest.

# Inhalt

- Erste Schritte – Übersicht ..... 1
  - On-Premises ..... 1
  - AWS Public Cloud ..... 1
  - Erste Schritte vor Ort ..... 1
  - Erste Schritte mit der AWS Public Cloud ..... 54

# 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

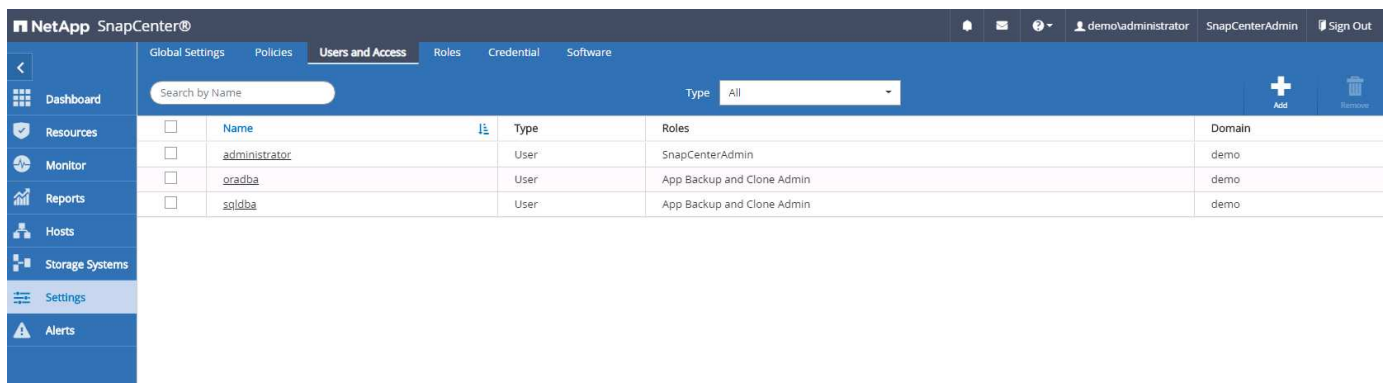
Es ist sinnvoll, eine dedizierte Admin-Benutzer-ID für jede von SnapCenter unterstützte Datenbankplattform zur Sicherung, Wiederherstellung und/oder Disaster Recovery von Datenbanken zu haben. Sie können auch eine einzige ID zum Managen aller Datenbanken verwenden. In unseren Test-Cases und Demos haben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



## 2. Installationsvoraussetzungen für das SnapCenter Plugin

SnapCenter führt Backup, Wiederherstellung, Klonen und weitere Funktionen mithilfe eines Plug-in-Agenten aus, der auf den DB-Hosts ausgeführt wird. Er verbindet sich mit dem Datenbank-Host und der Datenbank über Anmeldeinformationen, die unter der Registerkarte Einstellungen und Anmeldeinformationen für die Plugin-Installation und andere Verwaltungsfunktionen konfiguriert sind. Es gibt spezielle Berechtigungsanforderungen auf der Grundlage des Ziel-Host-Typs, wie Linux oder Windows, sowie der Datenbanktyp.

DB Hosts die Zugangsdaten müssen vor der SnapCenter Plugin-Installation konfiguriert werden. In der Regel möchten Sie ein Administrator-Benutzerkonto auf dem DB-Host als Ihre Host-Verbindungsdaten für die Plugin-Installation verwenden. Sie können auch dieselbe Benutzer-ID für den Datenbankzugriff über die BS-basierte Authentifizierung gewähren. Auf der anderen Seite können Sie auch Datenbank-Authentifizierung mit verschiedenen Datenbank-Benutzer-IDs für DB-Management-Zugriff. Wenn Sie sich für die Verwendung der OS-basierten Authentifizierung entscheiden, muss der BS-Admin-Benutzer-ID DB-Zugriff gewährt werden. Für die Windows-domänenbasierte SQL Server-Installation kann ein Domain-Administratorkonto verwendet werden, um alle SQL-Server innerhalb der Domäne zu verwalten.

Windows Host für SQL Server:

1. Wenn Sie Windows-Anmeldeinformationen zur Authentifizierung verwenden, müssen Sie die Anmeldedaten vor dem Installieren von Plug-ins einrichten.
2. Wenn Sie eine SQL Server-Instanz zur Authentifizierung verwenden, müssen Sie die Anmeldeinformationen nach der Installation von Plugins hinzufügen.
3. Wenn Sie die SQL-Authentifizierung beim Einrichten der Anmeldeinformationen aktiviert haben, wird die

erkannte Instanz oder Datenbank mit einem roten Sperrsymbol angezeigt. Wenn das Sperrsymbol angezeigt wird, müssen Sie die Instanz oder die Datenbankanmeldeinformationen angeben, um die Instanz oder Datenbank einer Ressourcengruppe erfolgreich hinzuzufügen.

4. Sie müssen die Anmeldedaten einem RBAC-Benutzer ohne sysadmin-Zugriff zuweisen, wenn die folgenden Bedingungen erfüllt sind:
  - Die Anmeldeinformationen werden einer SQL-Instanz zugewiesen.
  - Die SQL Instanz oder der Host wird einem RBAC-Benutzer zugewiesen.
  - Der RBAC-DB-Admin-Benutzer muss sowohl die Gruppen- als auch die Backup-Rechte besitzen.

#### UNIX Host für Oracle:

1. Sie müssen die passwortbasierte SSH-Verbindung für den Root- oder nicht-Root-Benutzer aktiviert haben, indem Sie sshd.conf bearbeiten und den sshd-Dienst neu starten. Die passwortbasierte SSH-Authentifizierung für die AWS-Instanz ist standardmäßig deaktiviert.
2. Konfigurieren Sie die Sudo-Berechtigungen für den nicht-Root-Benutzer, um den Plug-in-Prozess zu installieren und zu starten. Nach der Installation des Plugins werden die Prozesse als effektiver Root-Benutzer ausgeführt.
3. Erstellen Sie Anmeldedaten im Linux-Authentifizierungsmodus für den Installationsbenutzer.
4. Sie müssen Java 1.8.x (64-bit) auf Ihrem Linux-Host installieren.
5. Die Installation des Oracle Database Plugins installiert auch das SnapCenter Plugin für Unix.

### 3. SnapCenter Host Plugin Installation

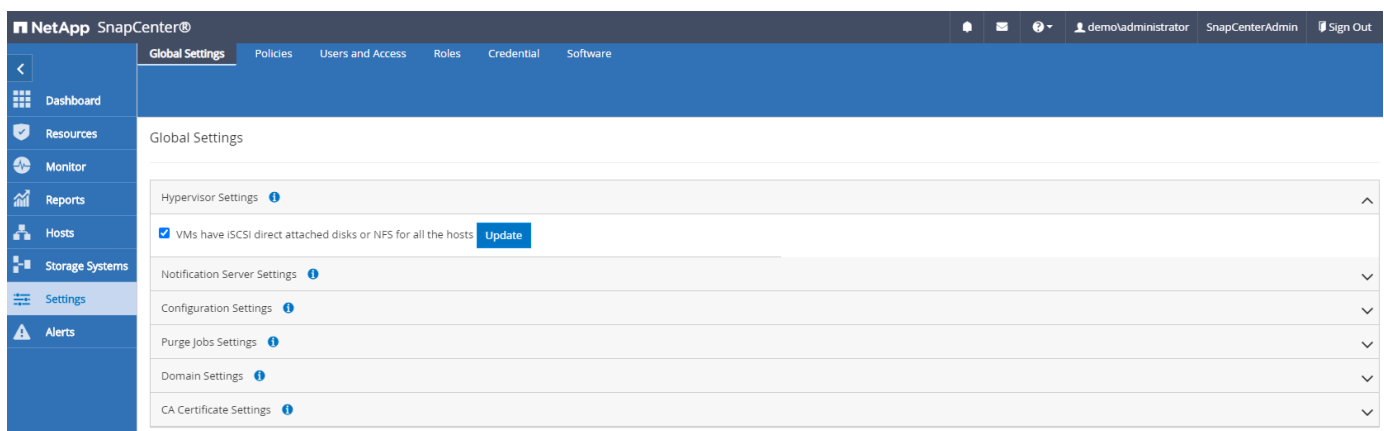


Bevor Sie versuchen, SnapCenter-Plugins auf Cloud-DB-Serverinstanzen zu installieren, stellen Sie sicher, dass alle Konfigurationsschritte wie im entsprechenden Cloud-Abschnitt für die Bereitstellung von Computing-Instanzen aufgeführt abgeschlossen wurden.

Die folgenden Schritte veranschaulichen, wie ein Datenbank-Host zu SnapCenter hinzugefügt wird, während ein SnapCenter-Plugin auf dem Host installiert ist. Das Verfahren gilt für das Hinzufügen von On-Premises-Hosts und Cloud-Hosts. Die folgende Demonstration führt zu einem Windows- oder Linux-Host in AWS.

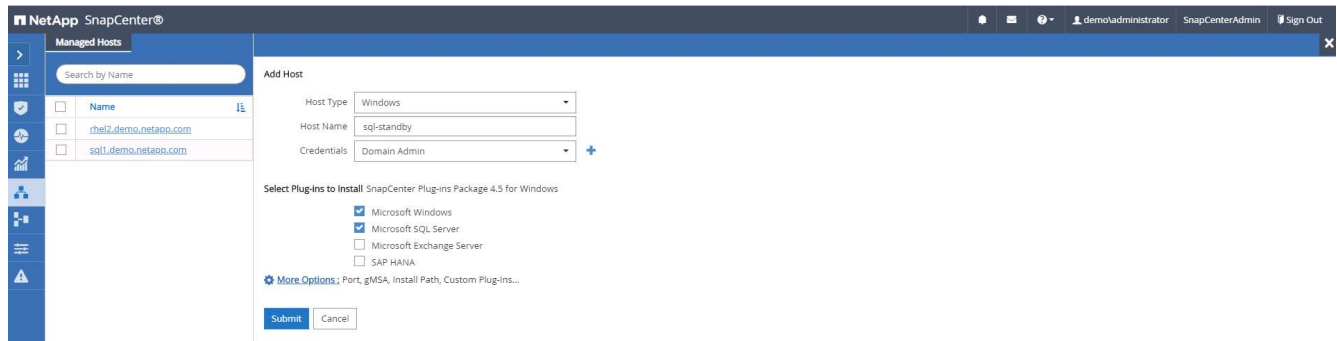
#### Konfigurieren Sie die globalen Einstellungen von SnapCenter VMware

Navigieren Sie zu Einstellungen > Globale Einstellungen. Wählen Sie unter Hypervisor-Einstellungen „VMs verfügen über direkt verbundene iSCSI-Festplatten oder NFS für alle Hosts“ aus und klicken Sie auf „Update“.

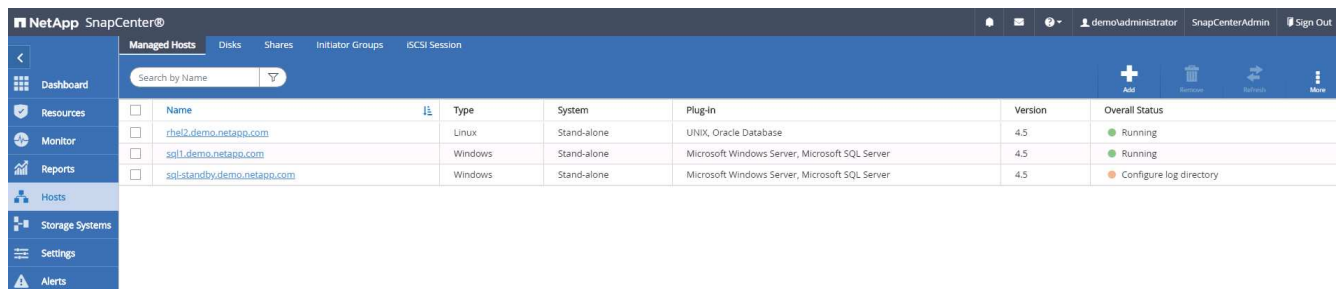


## Fügen Sie den Windows-Host und die Installation des Plugins auf dem Host hinzu

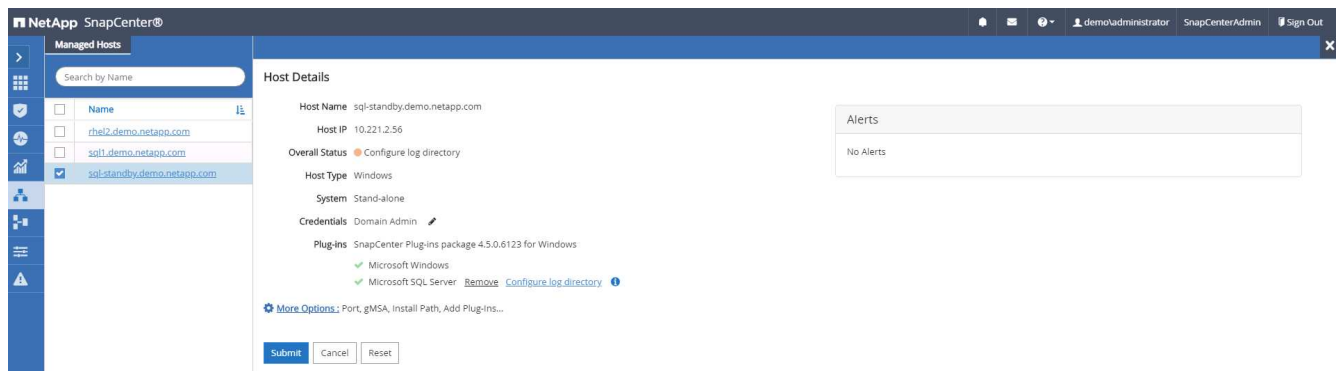
1. Melden Sie sich mit einer Benutzer-ID mit SnapCenterAdmin-Berechtigungen beim SnapCenter an.
2. Klicken Sie im linken Menü auf die Registerkarte Hosts und dann auf Hinzufügen, um den Host-Workflow hinzuzufügen zu öffnen.
3. Wählen Sie Windows für den Hosttyp. Der Hostname kann entweder ein Hostname oder eine IP-Adresse sein. Der Hostname muss vom SnapCenter-Host auf die richtige Host-IP-Adresse aufgelöst werden. Wählen Sie die in Schritt 2 erstellten Hostanmeldeinformationen aus. Wählen Sie Microsoft Windows und Microsoft SQL Server als die zu installierenden Plugin-Pakete.



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



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



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

Configure Plug-in for SQL Server

Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

Host log directory

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.


Configure Plug-in for SQL Server



Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

Host log directory

Choose directory on NetApp Storage

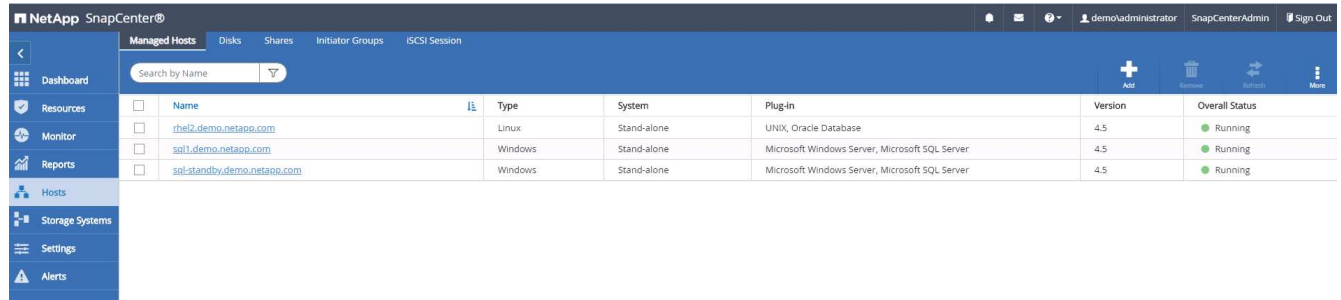
 sql-standby.demo.netapp.com

-  G:\
  -  System Volume Information



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.

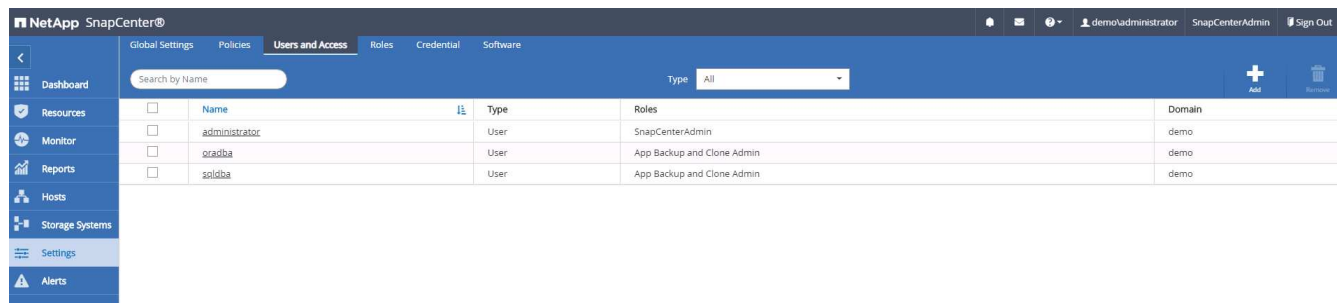
8. Nach der Konfiguration des Protokollverzeichnisses wird der Gesamtstatus des Windows-Host-Plug-ins in „Ausführen“ geändert.



The screenshot shows the NetApp SnapCenter interface. The 'Managed Hosts' tab is selected. The table lists three hosts: 'rhel2.demo.netapp.com' (Linux, Stand-alone, UNIX, Oracle Database, Version 4.5, Running), 'sql1.demo.netapp.com' (Windows, Stand-alone, Microsoft Windows Server, Microsoft SQL Server, Version 4.5, Running), and 'sql-standby.demo.netapp.com' (Windows, Stand-alone, Microsoft Windows Server, Microsoft SQL Server, Version 4.5, Running). The 'Overall Status' for all hosts is 'Running'.

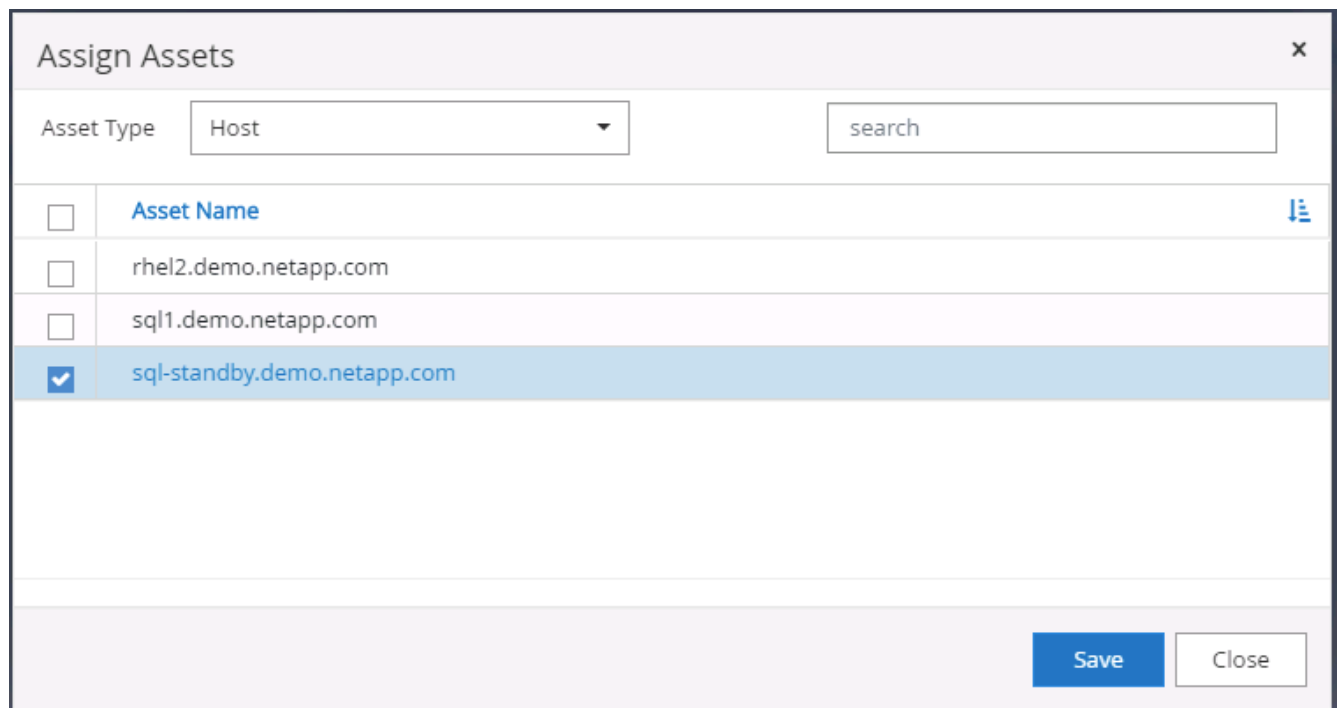
Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft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



The screenshot shows the NetApp SnapCenter interface. The 'Users and Access' tab is selected. The table lists three users: 'administrator' (User, SnapCenterAdmin, demo), 'oraoba' (User, App Backup and Clone Admin, demo), and 'sqldba' (User, App Backup and Clone Admin, demo).

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



The screenshot shows the 'Assign Assets' dialog box. The 'Asset Type' is set to 'Host'. The search bar is empty. The table lists three assets: 'rhel2.demo.netapp.com', 'sql1.demo.netapp.com', and 'sql-standby.demo.netapp.com'. The 'sql-standby.demo.netapp.com' asset is selected with a checkmark.

Asset Name
rhel2.demo.netapp.com
sql1.demo.netapp.com
sql-standby.demo.netapp.com

Save Close

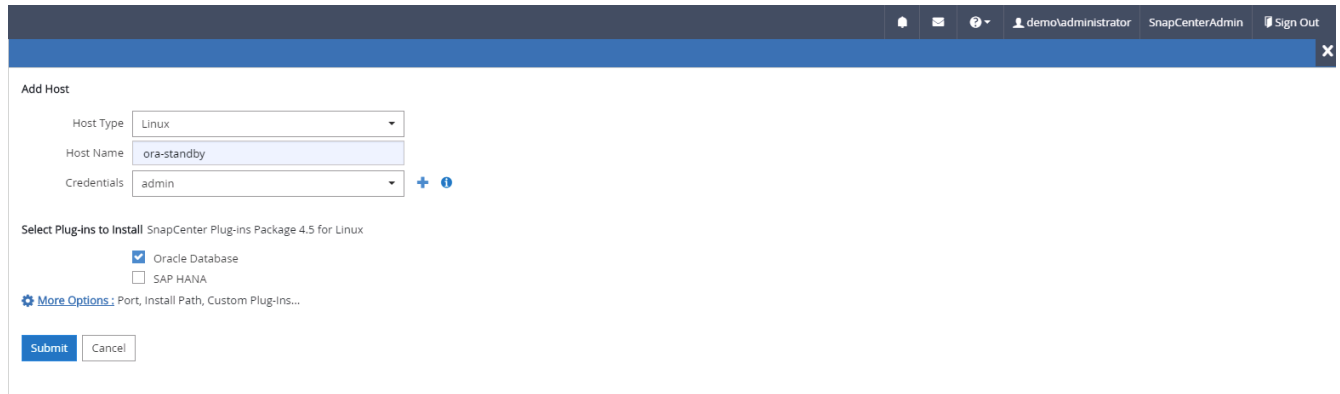
**Fügen Sie den Unix-Host hinzu und installieren Sie das Plugin auf dem Host**

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

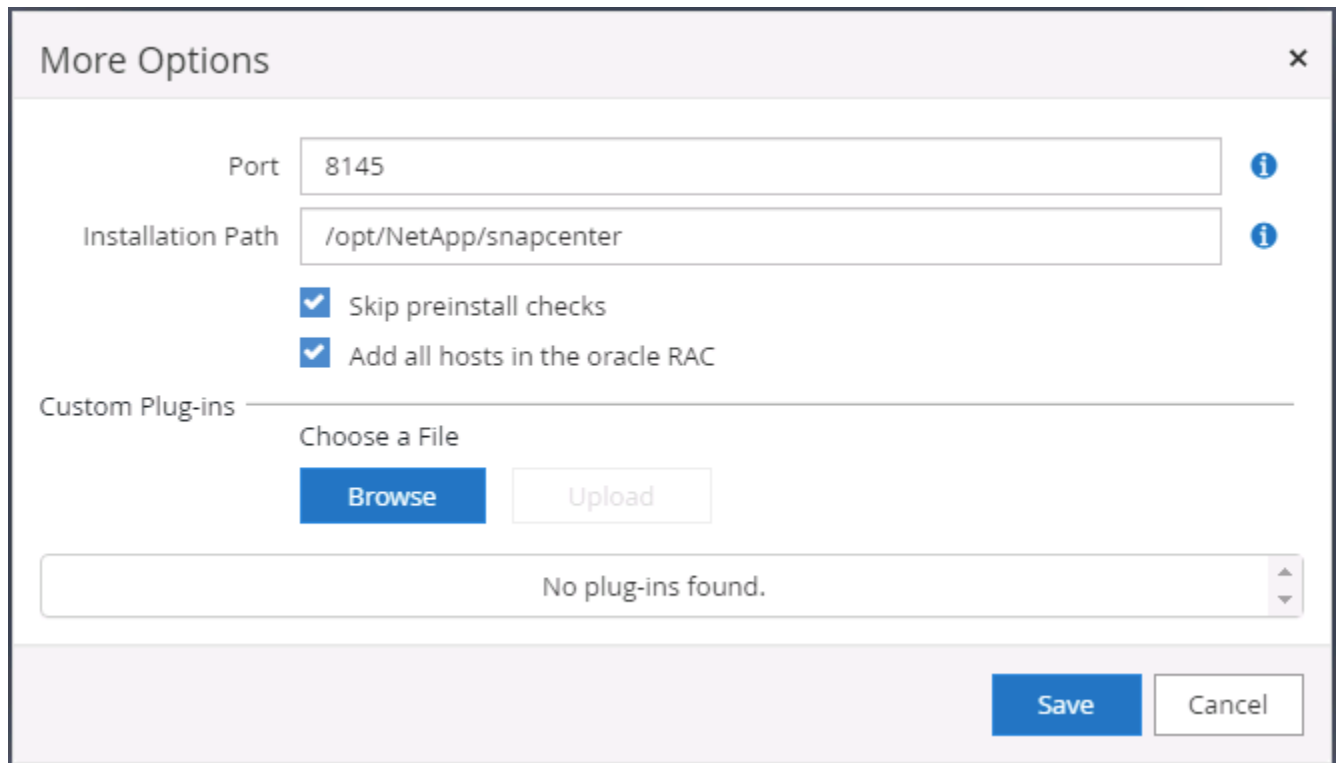
☒ Oracle Database

☐ 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> <div>Managed Hosts</div> <div>Disks</div> <div>Shares</div> <div>Initiator Groups</div> <div>ISCSI Session</div> </div> <div> <div>Search by Name</div> <div>+</div> <div>+</div> <div>+</div> <div>+</div> </div>							
	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	Type	Asset Type
10.0.0.1	DataOntapCluster	Storage Connection
192.168.0.101	DataOntapCluster	Storage Connection
admin		Credentials
Linux Admin		Credentials
Oracle Archive Log Backup		Policy
Oracle Full Online Backup		Policy
rhel2.demo.netapp.com		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®
demoloradba
App Backup and Clone Admin
Sign Out

Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

Oracle Database
View Database
Search databases

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

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®

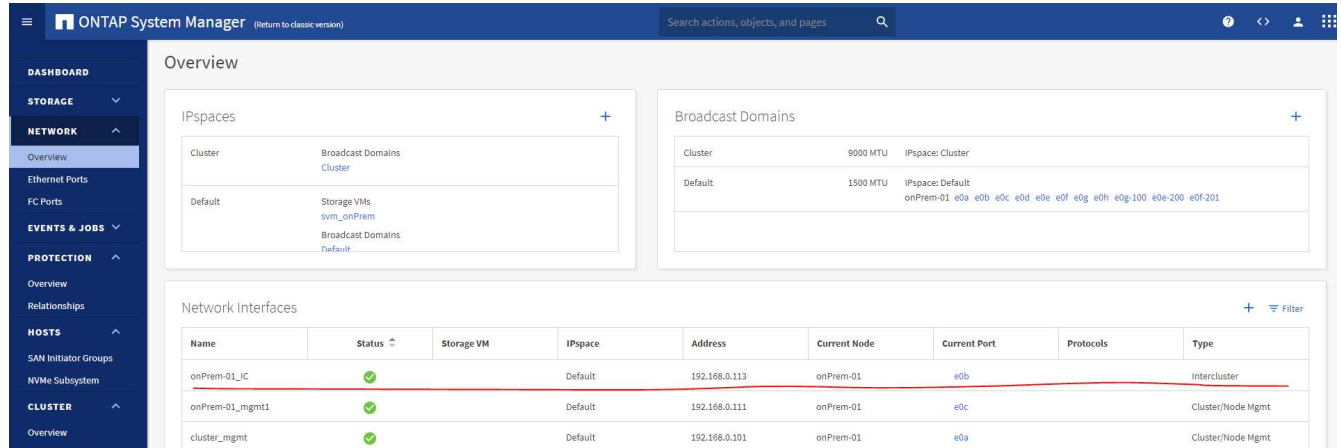
## 5. Storage Cluster-Peering und DB Volumes Replication einrichten

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.

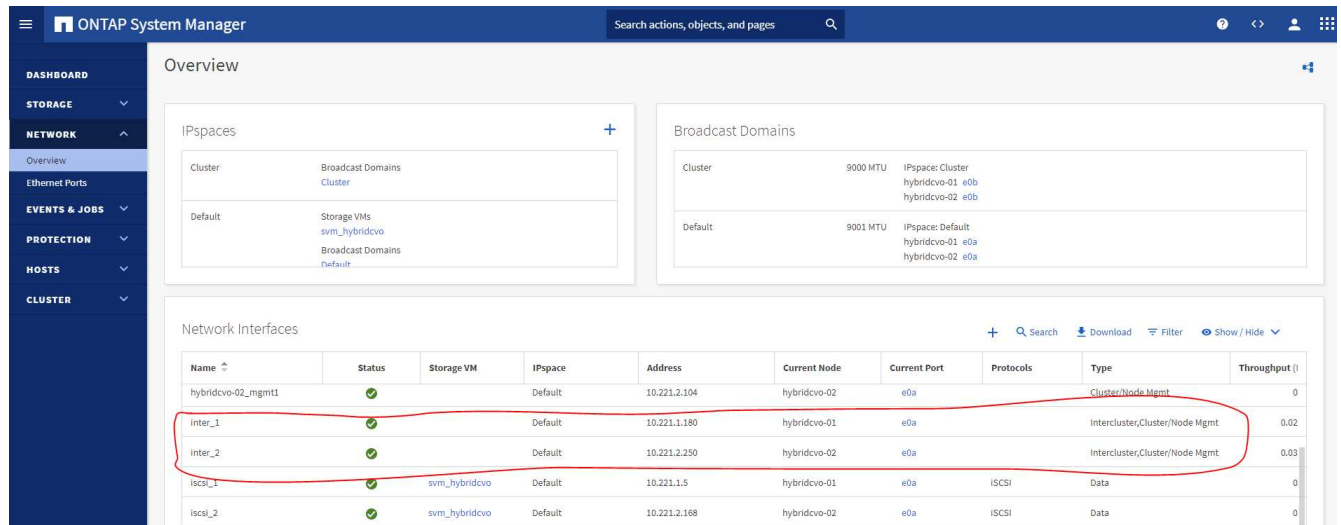
1. Konfigurieren Sie Intercluster LIFs für Cluster-Peering sowohl auf dem On-Premises-Cluster als auch auf der CVO-Cluster-Instanz. Dieser Schritt kann mit ONTAP System Manager ausgeführt werden. In einer CVO-Standardimplementierung werden automatisch Inter-Cluster-LIFs konfiguriert.

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
onPrem_data	
rhel2_u01	
rhel2_u02	
✓ rhel2_u03	
rhel2_u0309232119421203118	
sql1_data	
sql1_log	
sql1_snapctr	
svm_onPrem_root	

rhel2\_u03 All Volumes

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\_

<SourceVolumeName>

SUFFIX

\_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

Name

rhel2\_u03 All Volumes

onPrem\_data

rhel2\_u01

rhel2\_u02

☒ rhel2\_u03

rhel2\_u0309232119421203118

Filter

Edit

More

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.

13

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_hybridv0	10.0.0.1			CVO	⊗
svm_onPrem	192.168.0.101			CVO	✓

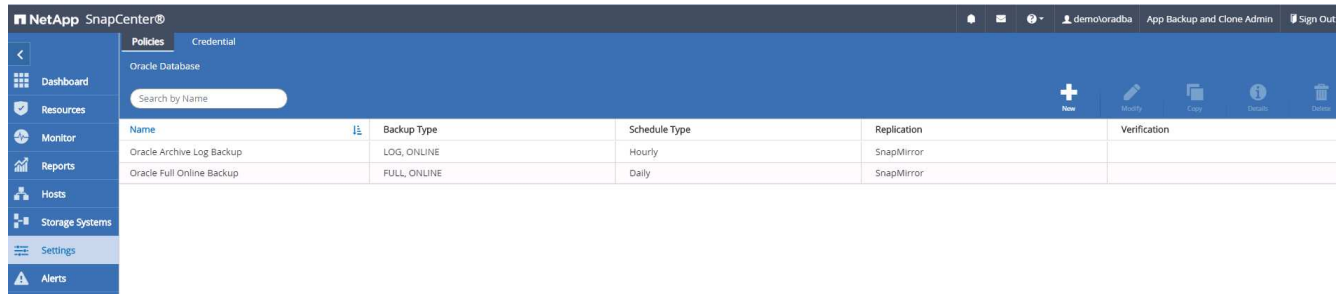
## 7. Einrichten der Datenbank Backup Policy in SnapCenter

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.

The screenshot shows a dialog box titled 'Modify Oracle Database Backup Policy'. On the left is a vertical list of steps: 1 Name, 2 Backup Type, 3 Retention, 4 Replication, 5 Script, 6 Verification, and 7 Summary. The 'Name' step is currently selected. The main area is titled 'Provide a policy name' and contains two input fields: 'Policy name' with the value 'Oracle Full Online Backup' and 'Details' with the value 'Backup all data and log files'. At the bottom right are 'Previous' and 'Next' buttons.

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.

16

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.

19

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.

22



New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☐ Datafiles, control files, and archive logs

☐ Datafiles and control files

☒ Archive logs

☐ Offline backup

☒ Mount

☐ Shutdown

☐ Save state of PDBs

Choose schedule frequency

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

☐ On demand

☒ Hourly

☐ Daily

Previous

Next

4. Legen Sie den Aufbewahrungszeitraum für das Protokoll fest.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Hourly retention settings

Data backup retention settings

Total Snapshot copies to keep

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.

24

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.

26

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

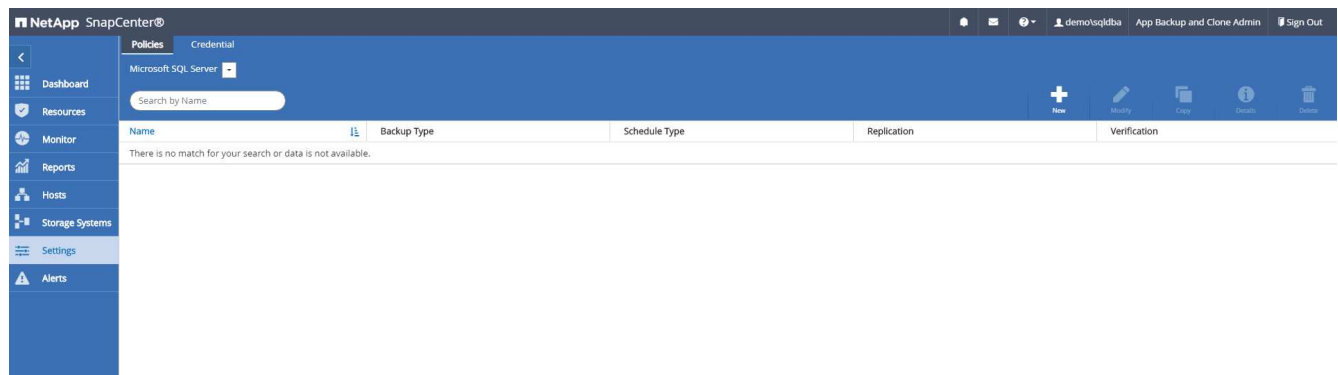
Policy name	Oracle Archive Log Backup
Details	Backup Oracle archive logs
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive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

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.



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\_ERRORMSGSGS)

☐ 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.

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.

36

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☐ Full backup and log backup

☐ Full backup

☒ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

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

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

☐ Monthly

Previous

Next

3. Die SQL Server Daten-Backup-Richtlinie definiert die Backup-Aufbewahrung für Protokolle. Akzeptieren Sie hier die Standardeinstellungen.

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®

Oracle Database

View Database Search databases

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

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 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name: rhe12\_cdb2

Tags: orafullbkup

☒ Use custom name format for Snapshot copy

\$CustomText: rhe12\_cdb2

Backup settings

Exclude archive log destinations from backup: [dropdown]

3. Fügen Sie der Ressourcengruppe Datenbankressourcen hinzu.

NetApp SnapCenter®

Oracle Database

Search databases

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

Add resources to Resource Group

Host: All

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 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 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	orafulbkup	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

Oracle Archive Log Backup

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
rhe2\_cdb2
Total 1

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

Configure verification schedules
Policy Schedule Type Applied Schedules Configure Schedules

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

Total 0

Previous Next

7. Konfigurieren Sie bei Bedarf einen SMTP-Server für E-Mail-Benachrichtigungen.



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

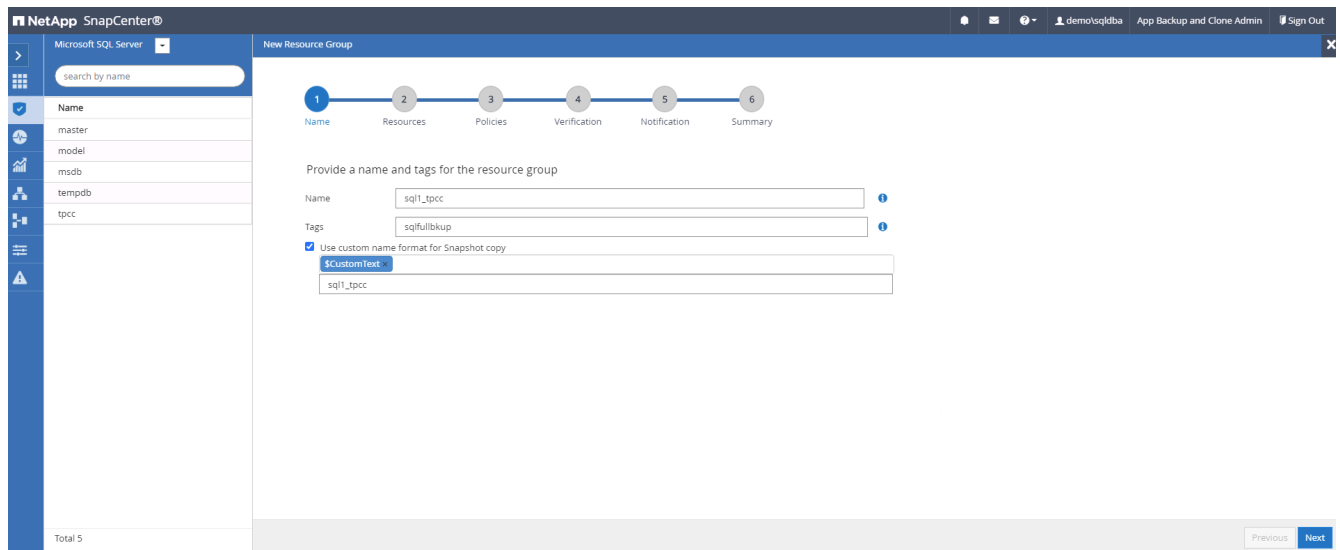
Verification enabled for policy: None

Send email: No

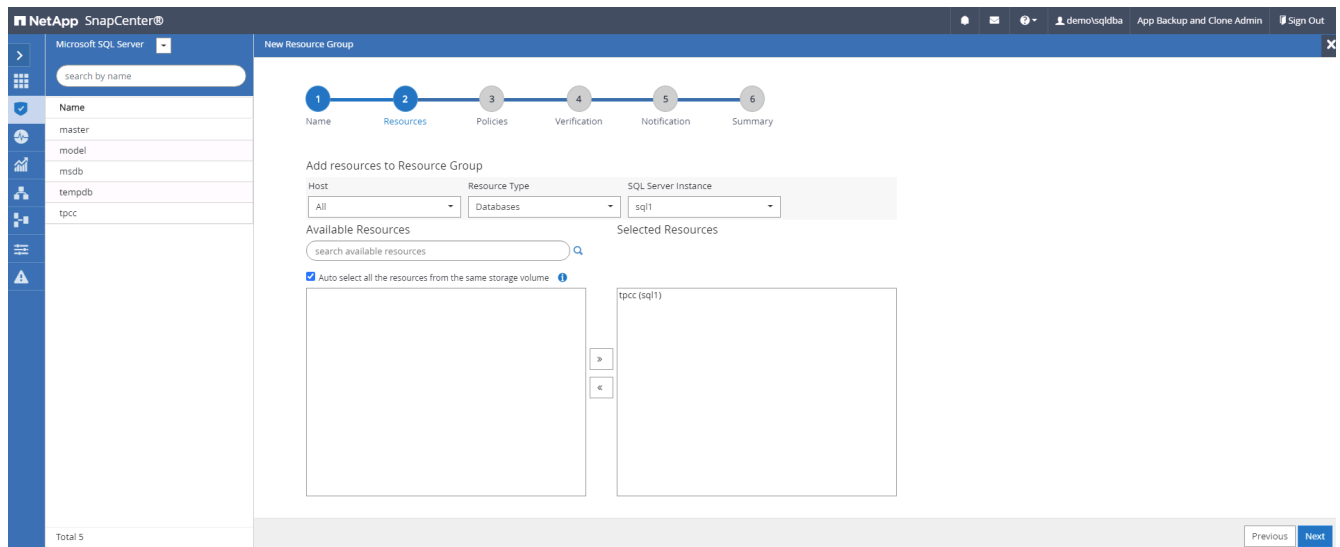
Previous Finish

## Erstellen Sie eine Ressourcengruppe für die vollständige Sicherung von SQL Server

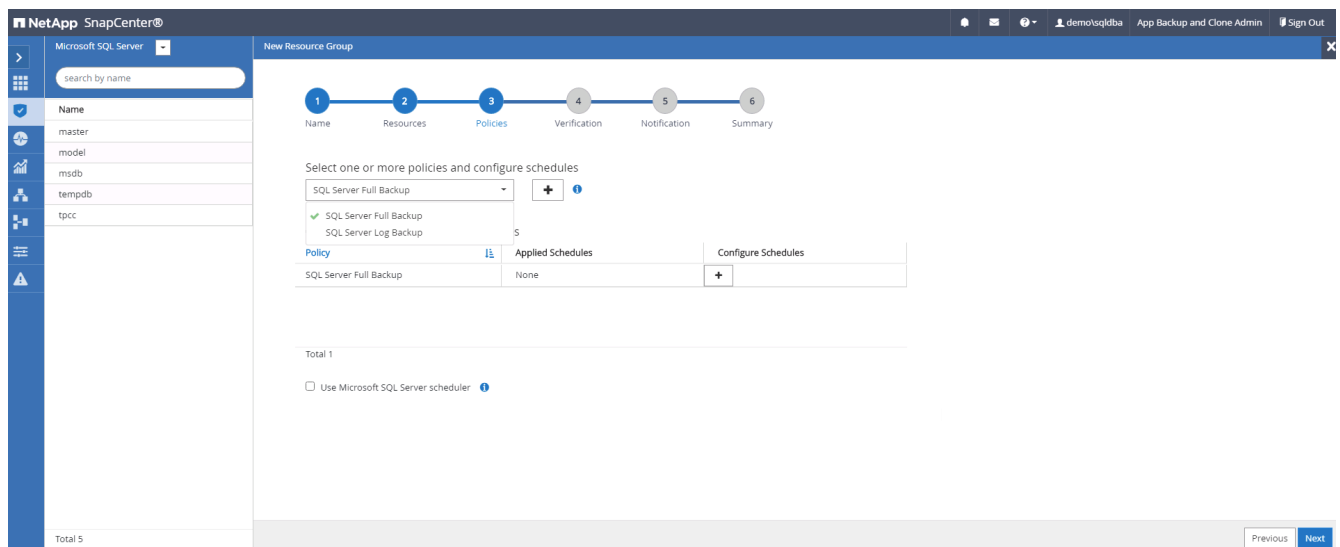
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdown-Liste Ansicht entweder eine Datenbank oder eine Ressourcengruppe aus, um den Arbeitsablauf für die Erstellung von Ressourcengruppen zu starten.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

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

Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume

Destination Volume

svm\_onPremsql1\_data

svm\_hybridvostsql1\_data\_dr

svm\_onPremsql1\_log

svm\_hybridvostsql1\_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

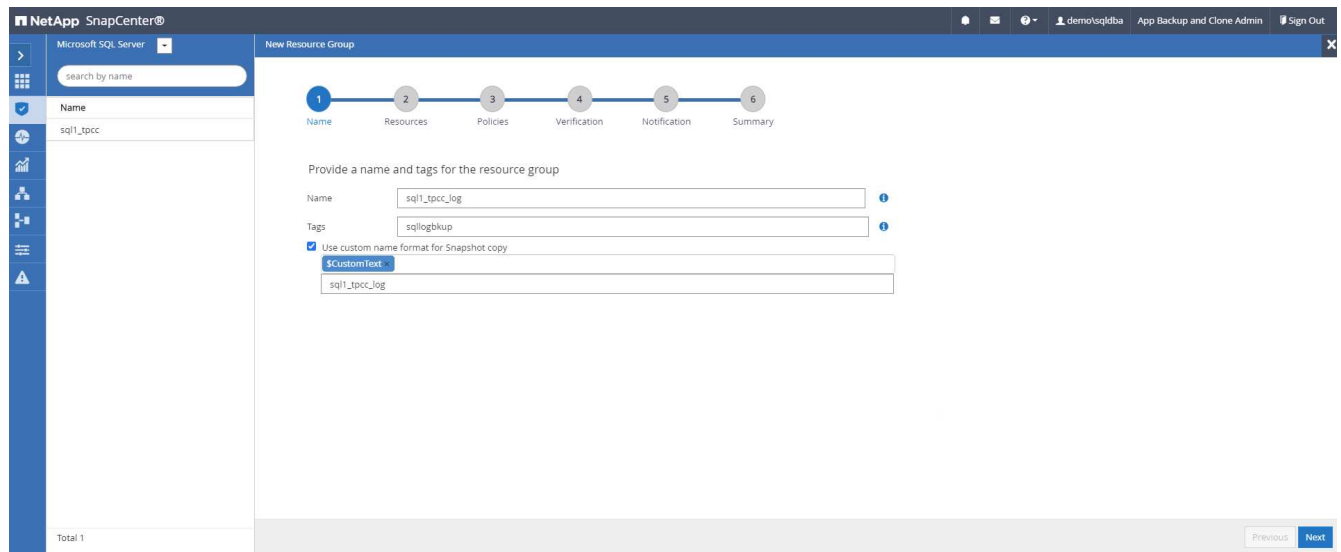
6. Konfigurieren Sie bei Bedarf den SMTP-Server für E-Mail-Benachrichtigungen.

49

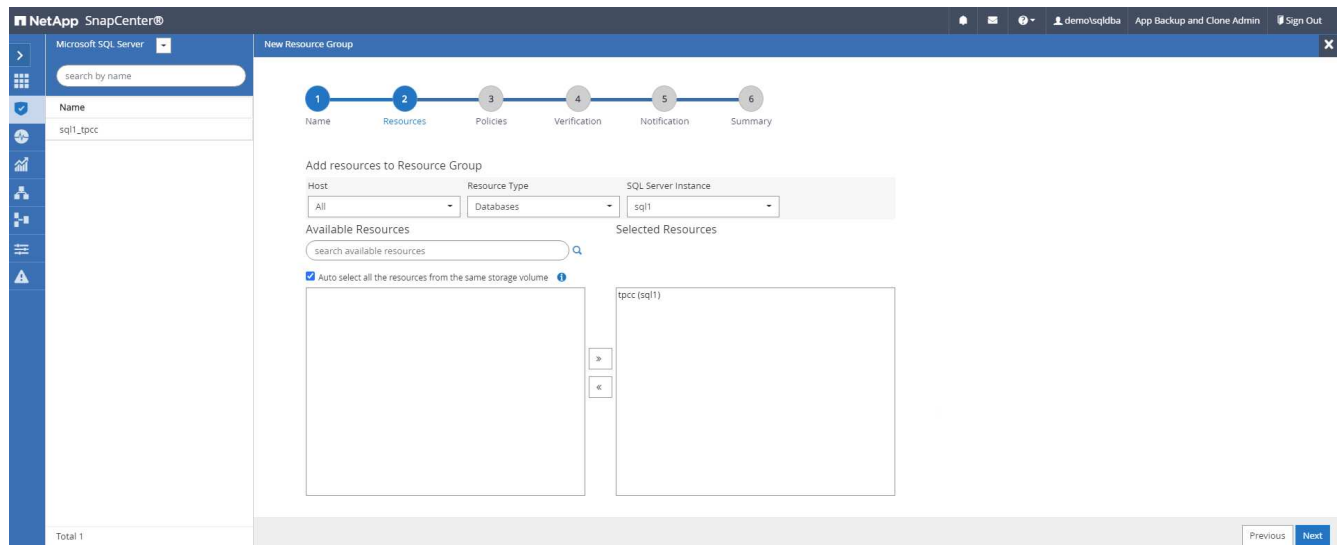
## 7. Zusammenfassung.

### Erstellen Sie eine Ressourcengruppe für die Protokollsicherung von SQL Server

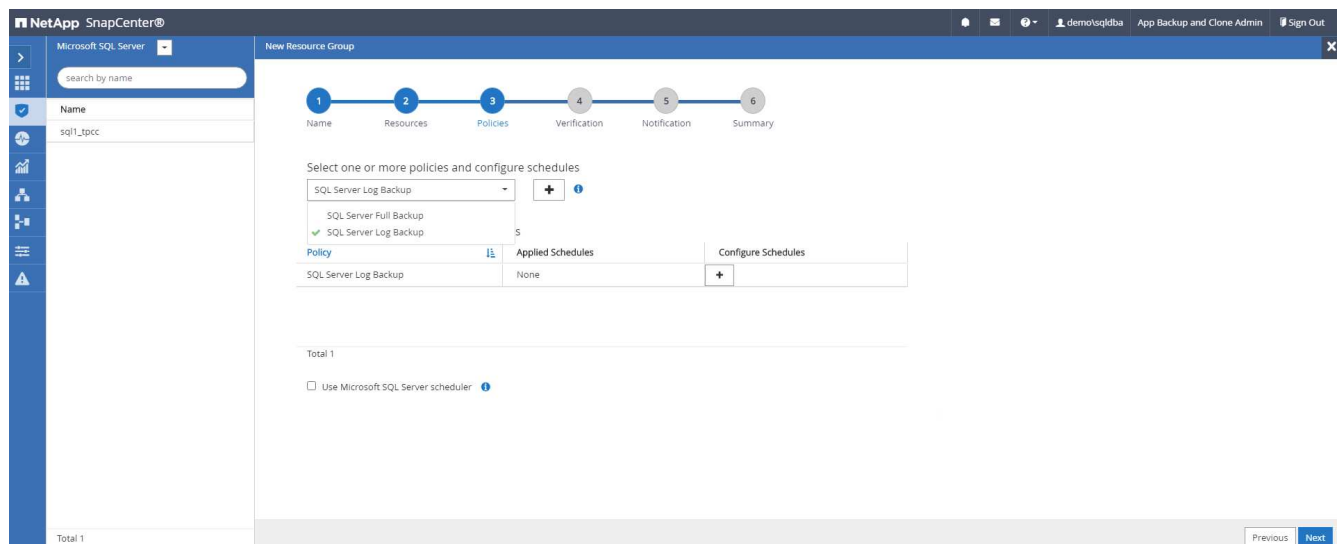
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdown-Liste Ansicht entweder eine Datenbank oder eine Ressourcengruppe aus, um den Arbeitsablauf für die Erstellung von Ressourcengruppen zu starten. 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 other functions. The main area is titled 'cdb2 Topology' and 'Manage Copies'. It displays a summary card with statistics: 394 Backups (28 Data Backups, 366 Log Backups, 3 Clones), 197 Backups (0 Clones) for Local copies, and 197 Backups (3 Clones) for Mirror copies. Below this is a table of Primary Backup(s) with columns: Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The table lists five backup entries with their respective details.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-29-2021_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

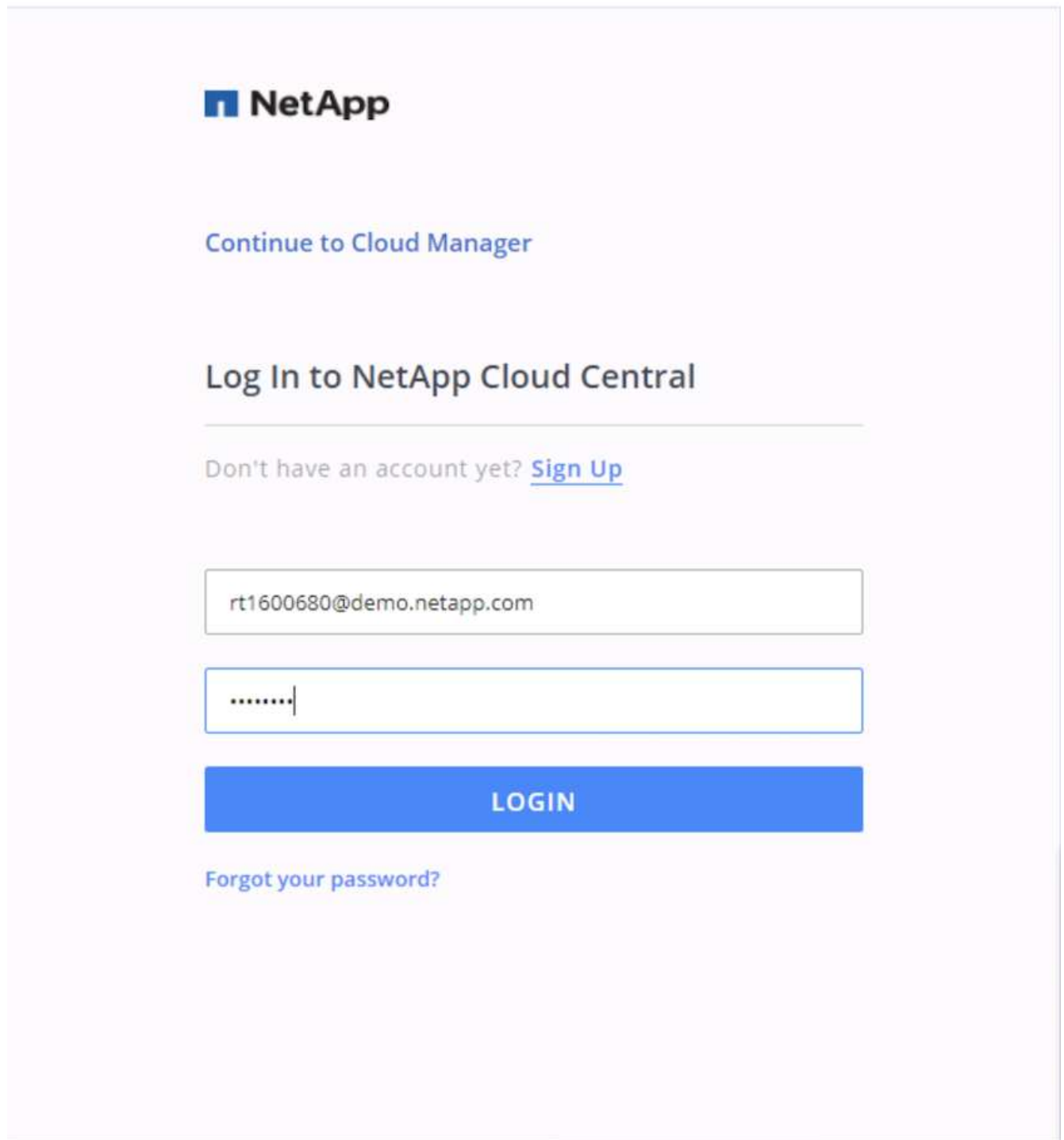


Für die Implementierung von Cloud Manager und Cloud Volumes ONTAP gibt es viele Methoden. Diese Methode ist die einfachste, erfordert jedoch die meisten Berechtigungen. Falls diese Methode für Ihre AWS-Umgebung nicht geeignet ist, schlagen Sie bitte in nach "[NetApp Cloud-Dokumentation](#)".



## 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 the heading is a link for users who don't have an account yet to "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 for "Forgot your password?".

**NetApp**

[Continue to Cloud Manager](#)

### Log In to NetApp Cloud Central

---

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

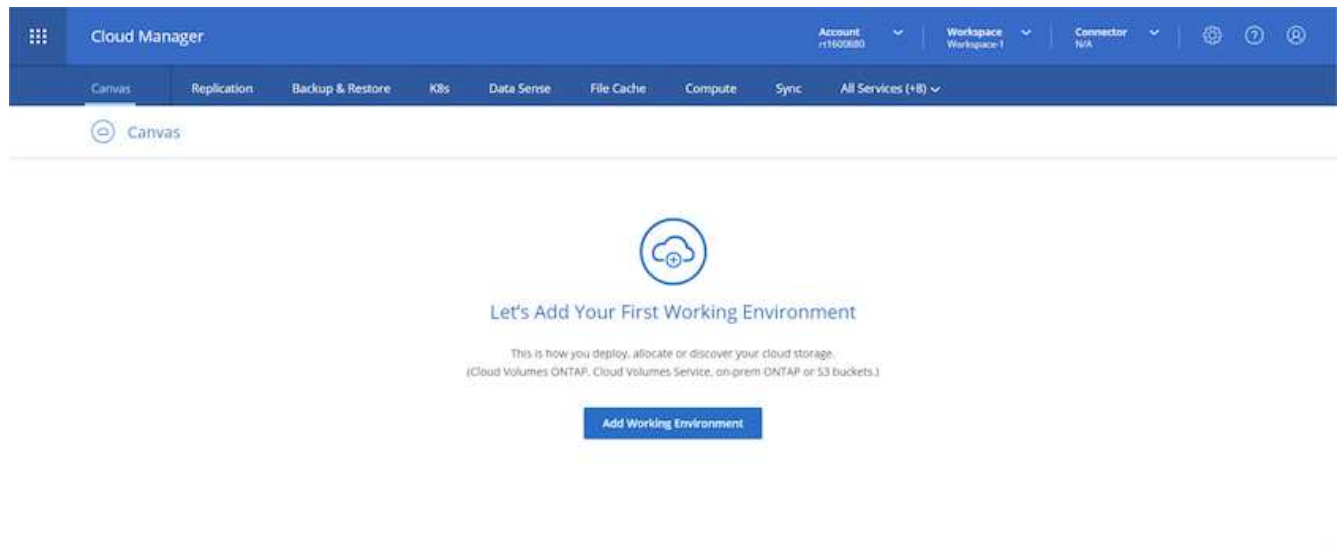
rt1600680@demo.netapp.com

.....|

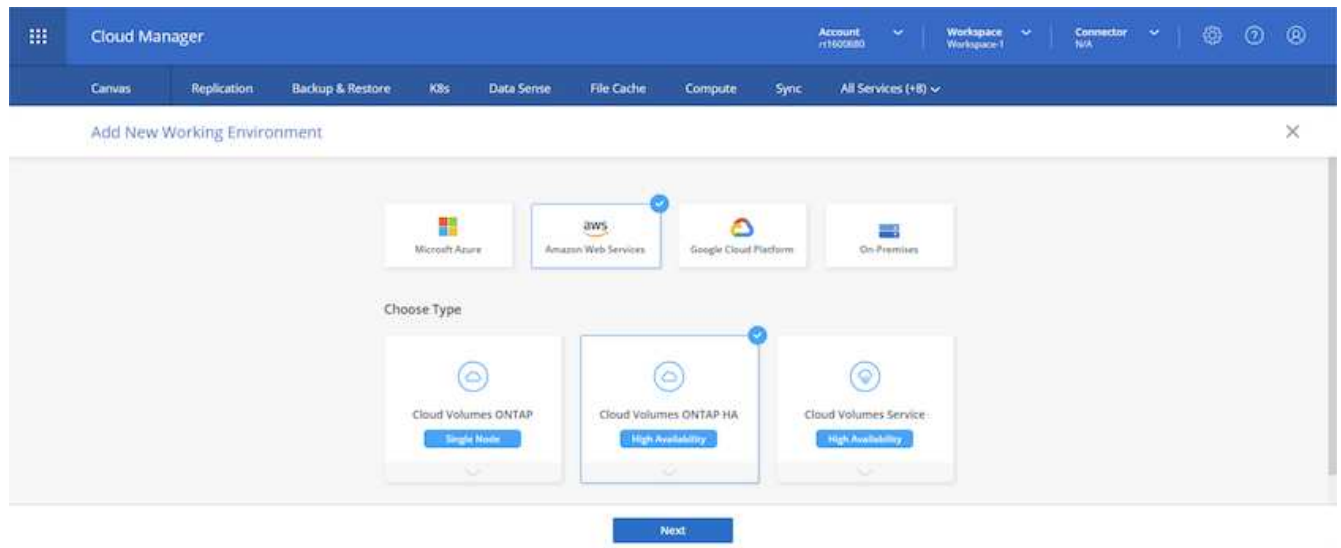
**LOGIN**

[Forgot your password?](#)

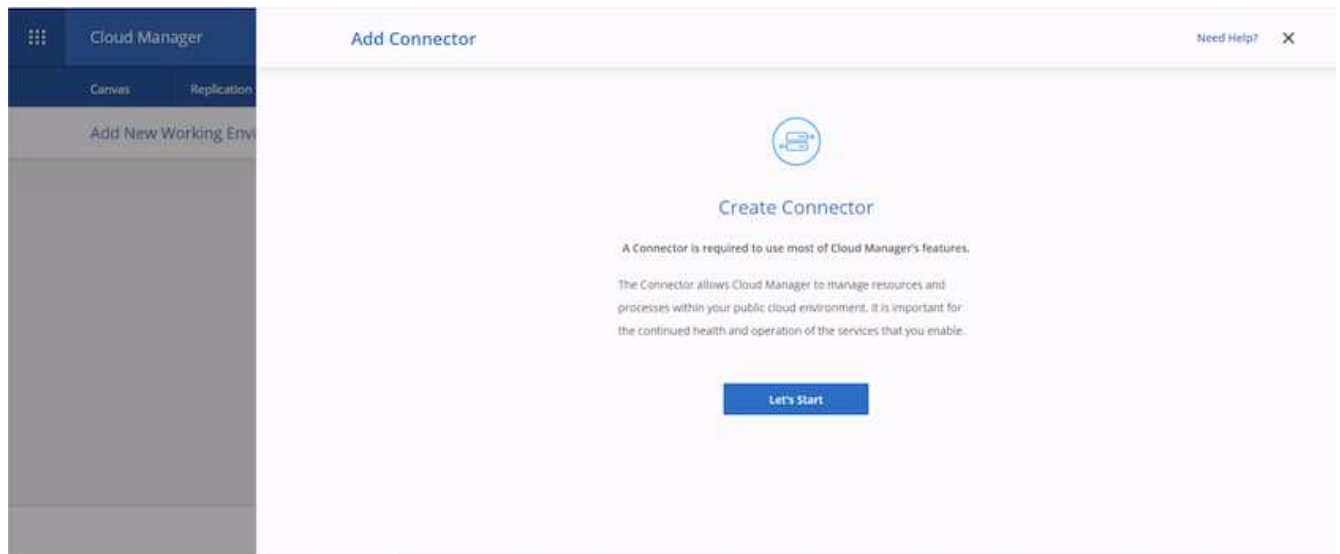
2. Nach der Anmeldung sollten Sie auf den Bildschirm gebracht werden.



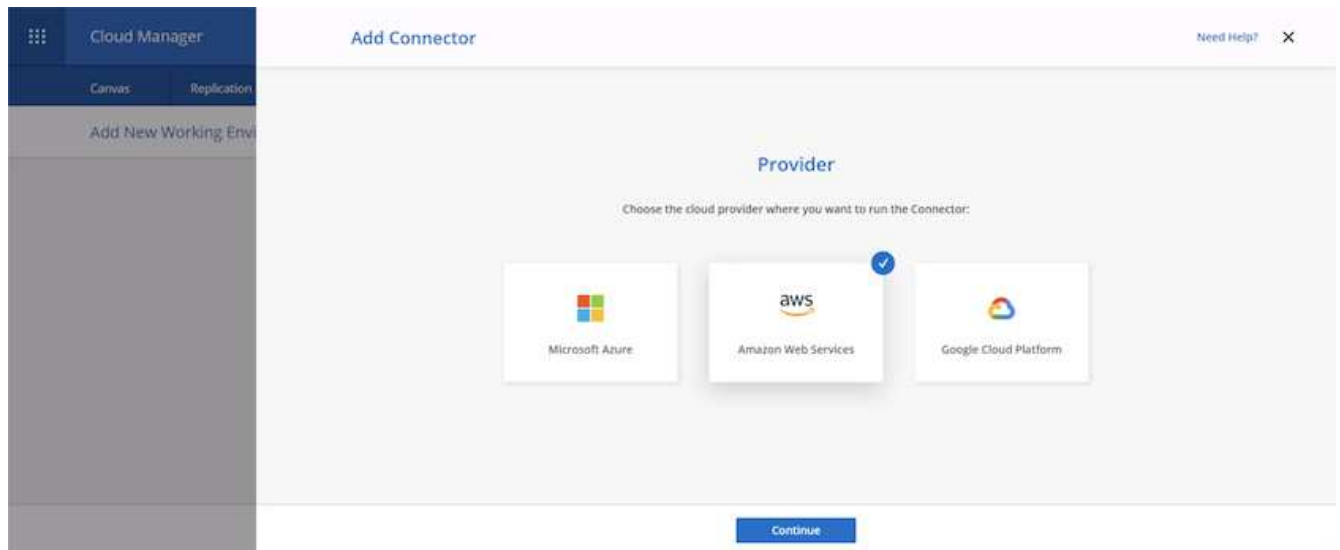
3. Klicken Sie auf „Arbeitsumgebung hinzufügen“ und wählen Sie Cloud Volumes ONTAP in AWS. Hier haben Sie außerdem die Wahl, ob Sie ein Single Node-System oder ein Hochverfügbarkeitspaar implementieren möchten. Ich habe mich entschieden, ein Hochverfügbarkeitspaar bereitzustellen.



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** | Add Connector | Need Help? X

Canvas | Replication

Add New Working Environment

Get Ready | AWS Credentials | Details | **4 Network** | Security Group | 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://11.22.16.254:12345

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** | Add Connector | Need Help? X

Canvas | Replication

Add New Working Environment

Get Ready | AWS Credentials | Details | Network | **5 Security Group** | 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

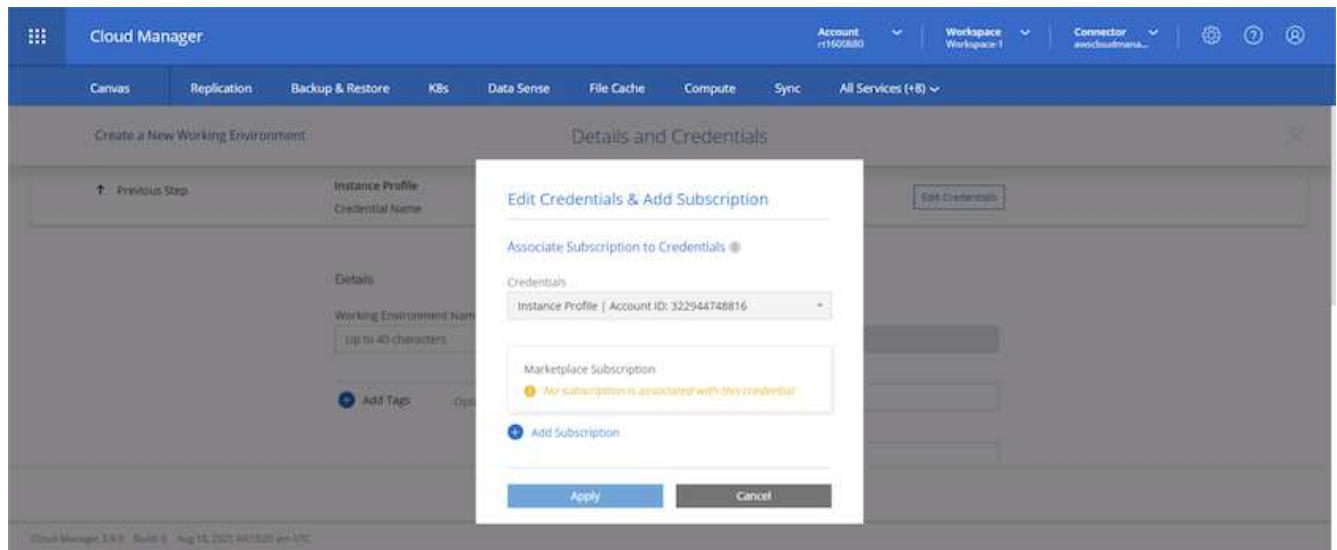
1. Wählen Sie AWS und die Art der Implementierung auf der Grundlage Ihrer Anforderungen aus.

The screenshot shows the 'Add New Working Environment' dialog in the Cloud Manager interface. The top navigation bar includes 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The main content area displays four cloud providers: Microsoft Azure, Amazon Web Services (selected with a blue checkmark), Google Cloud Platform, and On-Premises. Below this, the 'Choose Type' section shows three options: 'Cloud Volumes ONTAP Single Node', 'Cloud Volumes ONTAP HA High Availability' (selected with a blue checkmark), and 'Cloud Volumes Service High Availability'. A 'Next' button is located at the bottom center.

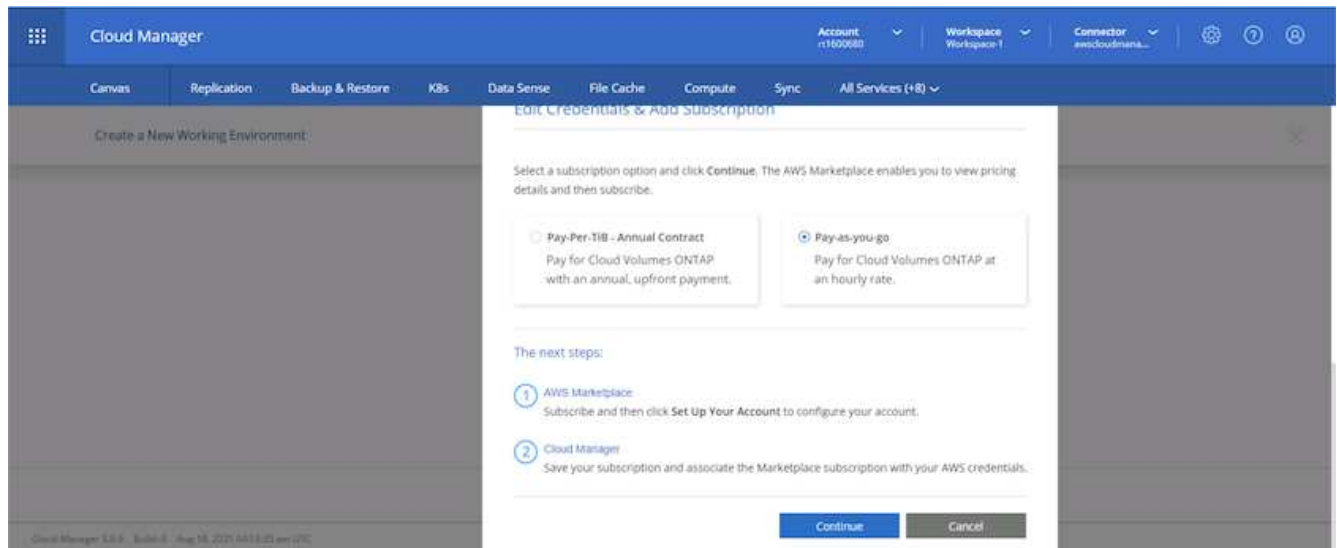
2. Wenn kein Abonnement zugewiesen wurde und Sie mit PAYGO kaufen möchten, wählen Sie Anmeldedaten bearbeiten.

The screenshot shows the 'Details and Credentials' dialog in the Cloud Manager interface. The top navigation bar is the same as the previous screenshot. The main content area is divided into two sections: 'Details' and 'Credentials'. The 'Details' section includes a 'Previous Step' link, a table with 'Instance Profile' (322944748816), 'Credential Name', and 'Account ID', and a 'Marketplace Subscription' section with a warning 'No subscription is associated' and an 'Edit Credentials' button. Below this, there are input fields for 'Working Environment Name (Cluster Name)' (up to 40 characters) and 'Add Tags' (optional field, up to four tags). The 'Credentials' section includes input fields for 'User Name' (admin), 'Password', and 'Confirm Password'. A 'Continue' button is located at the bottom center.

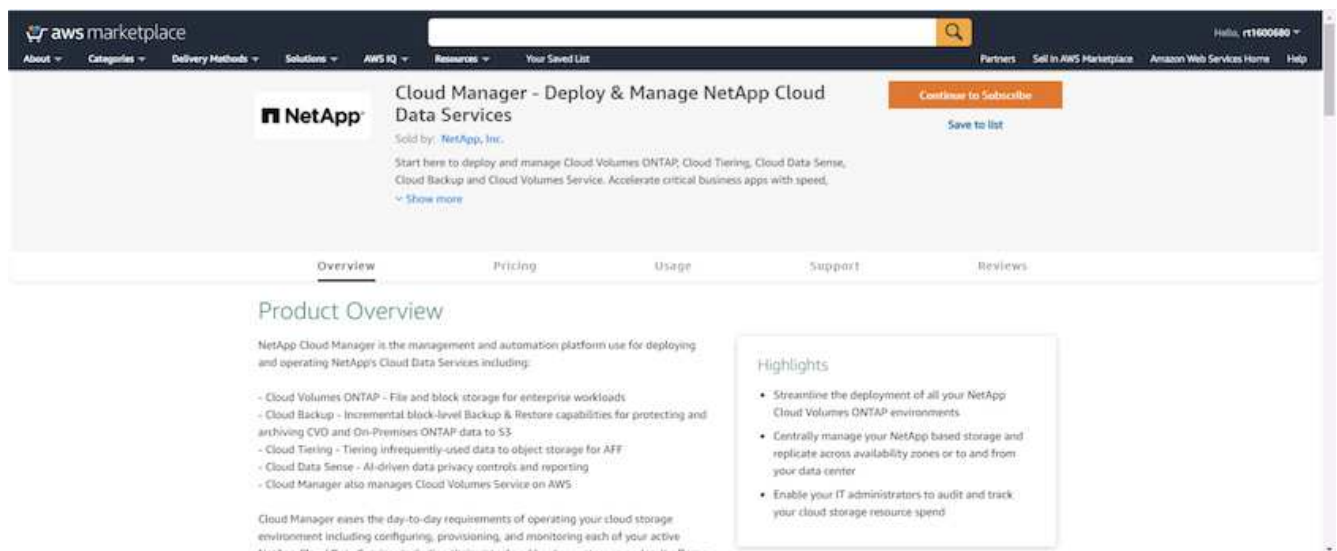
3. Wählen Sie Abonnement Hinzufügen.



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

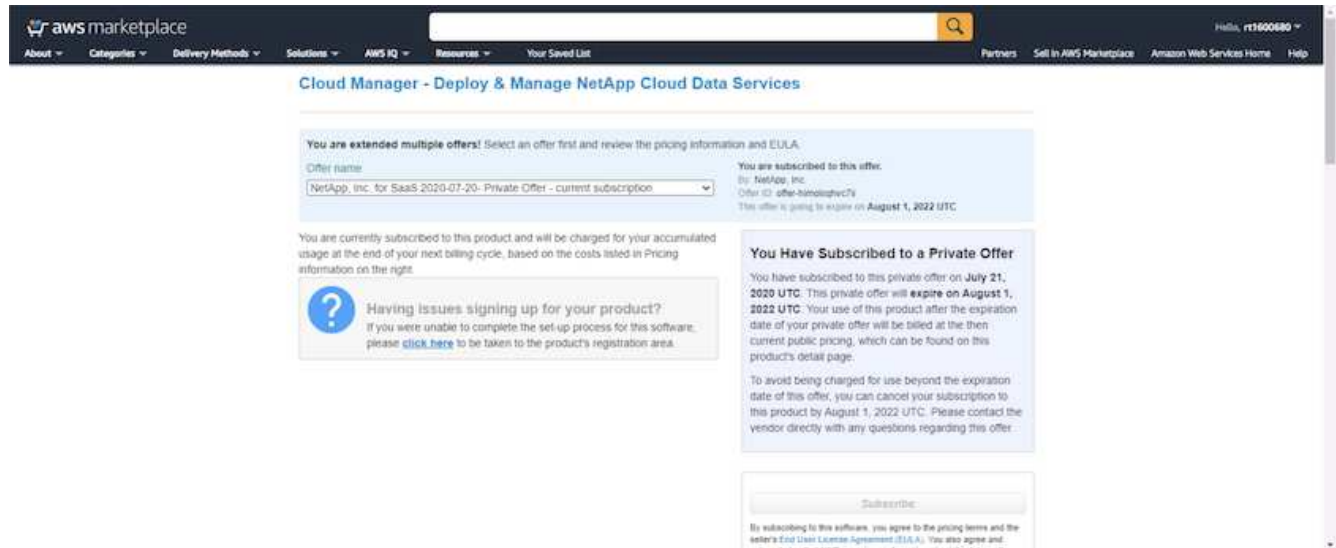


5. Sie werden zu AWS umgeleitet und wählen Sie „Weiter“, um sich Abonnieren zu öffnen.

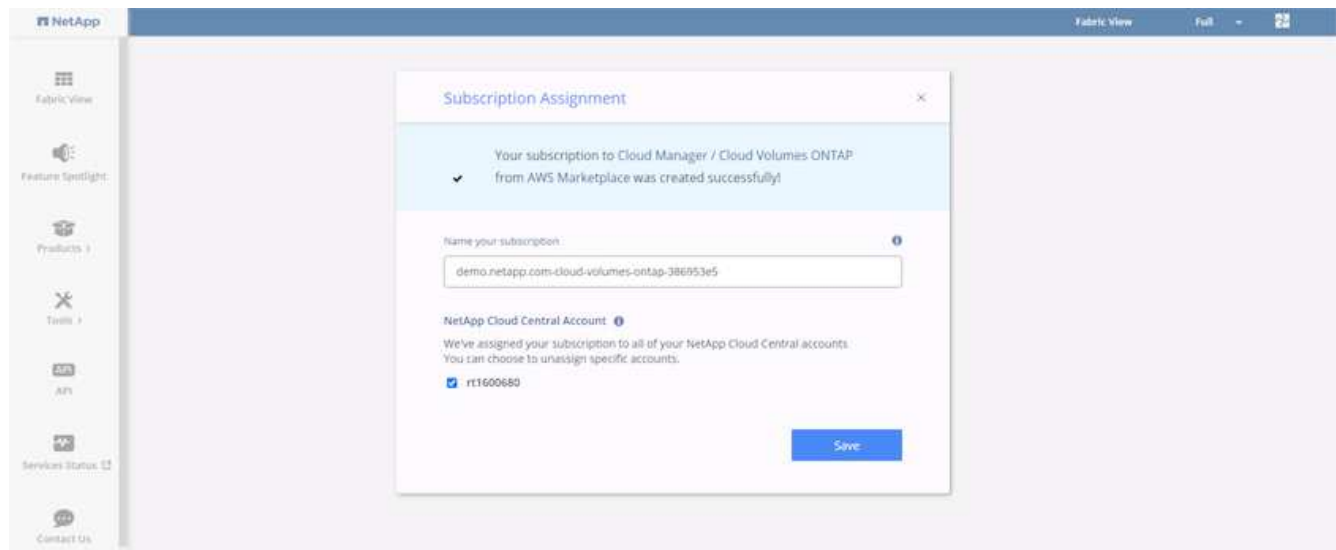




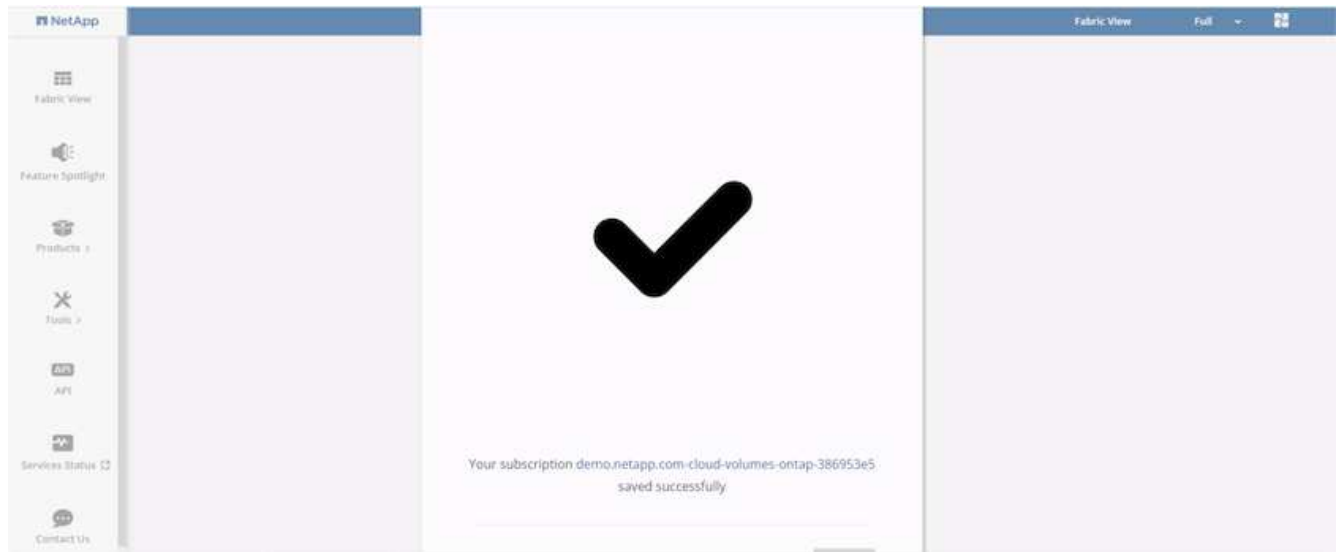
6. Melden Sie sich an und Sie werden zurück auf NetApp Cloud Central umgeleitet. Wenn Sie bereits abonniert haben und nicht umgeleitet werden, klicken Sie auf den Link "Hier klicken".



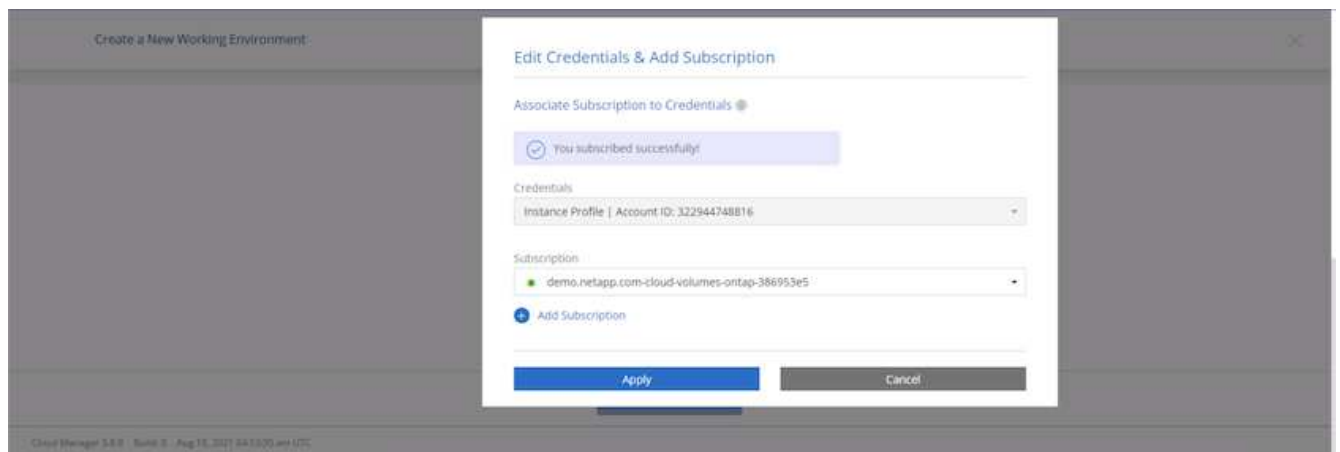
7. Sie werden zu Cloud Central umgeleitet. Dort müssen Sie die Namen Ihres Abonnements benennen und es Ihrem Cloud Central Konto zuweisen.



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.:

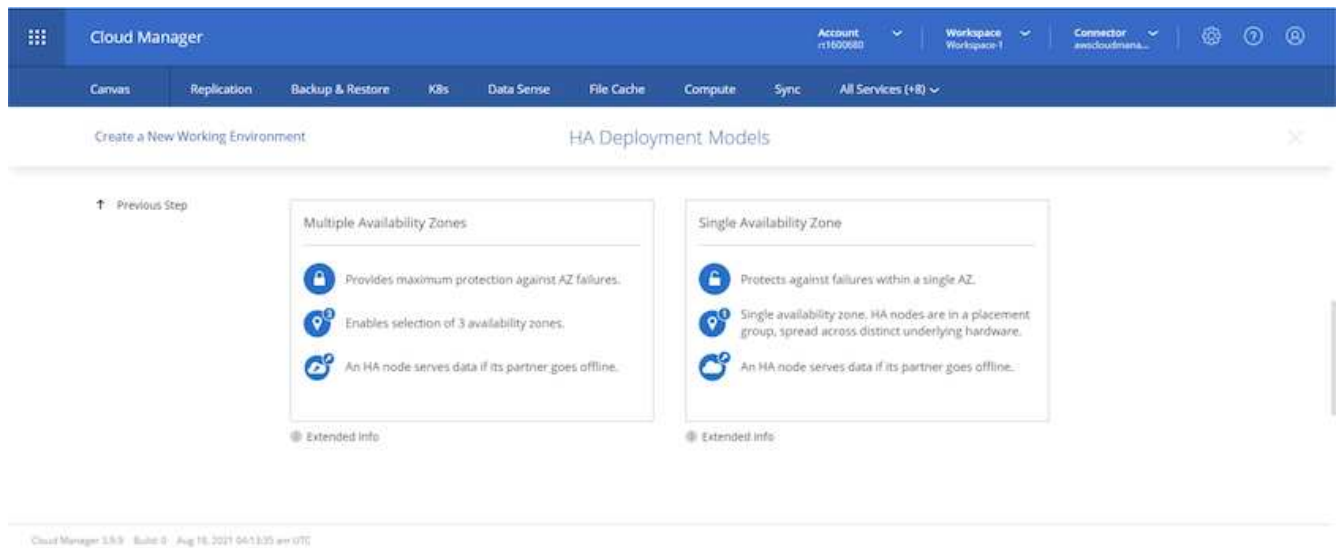
- a. Cluster-Name
- b. Cluster-Passwort
- c. AWS Tags (optional)

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 right.

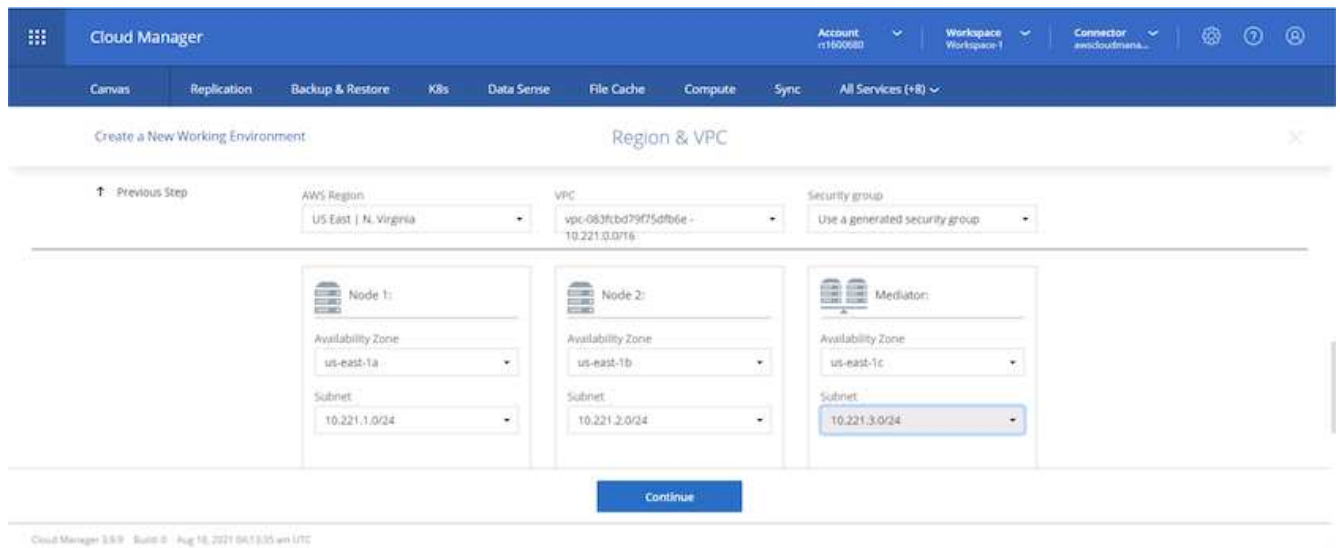
11. Wählen Sie aus, welche zusätzlichen Services Sie bereitstellen möchten. Weitere Informationen zu diesen Services finden Sie auf der ["NetApp Cloud Homepage"](#).

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 right.

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 5.8.9 | Build 2 | Aug 18, 2021 06:13:05 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: r1600680 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_r1600680	No	rtb-08b4cb88f5c826a5	3 Subnets	1 Tags
<input checked="" type="checkbox"/>	public_rt_r1600680	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: r1600680 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

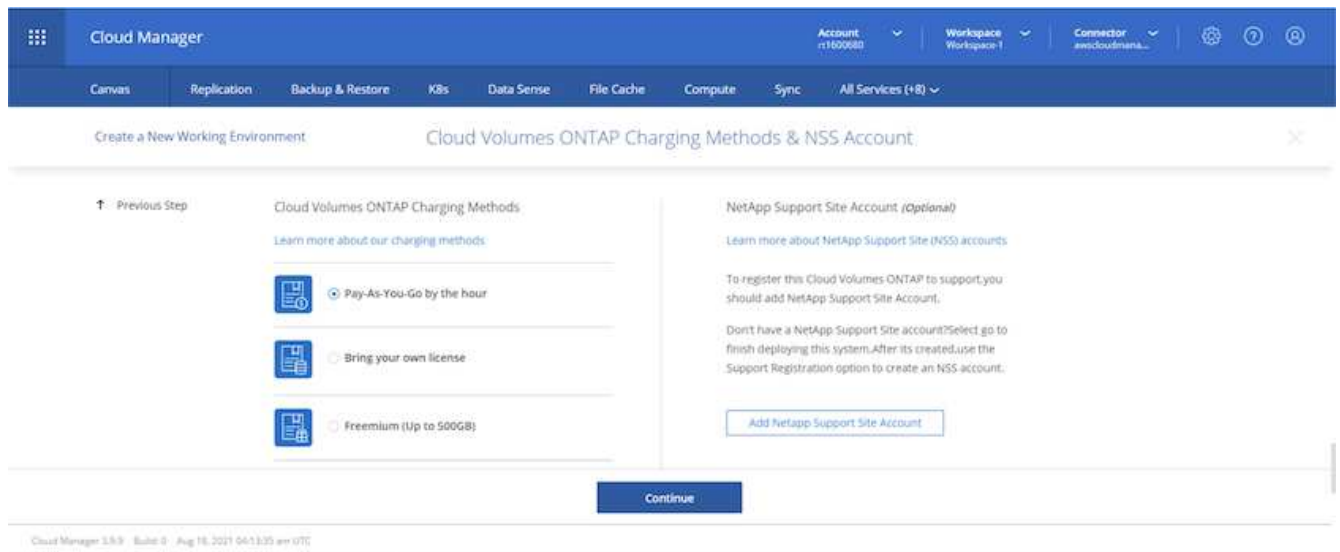
AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

Default Master Key: aws/ebs

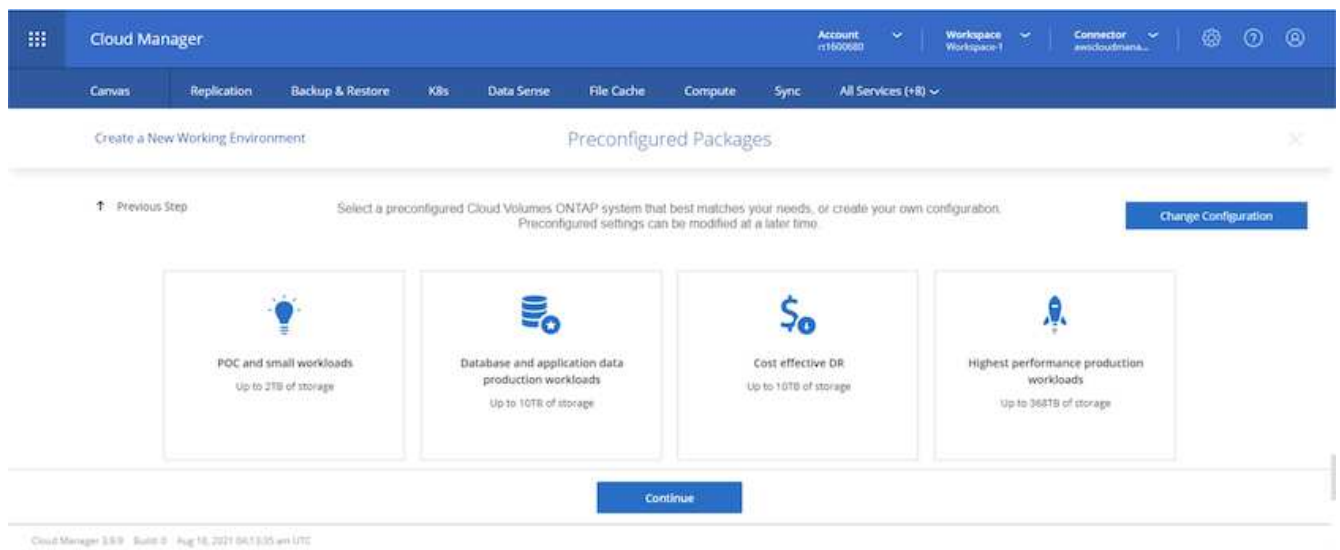
Continue

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.

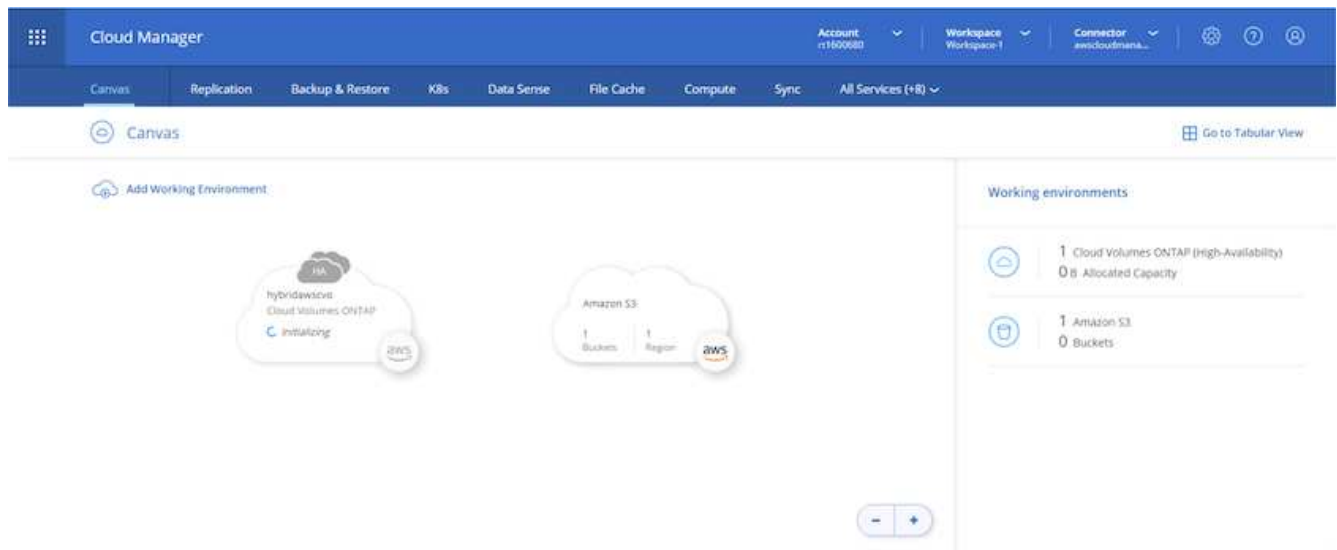
Cloud Manager 3.8.9 Build 9 Aug 18, 2021 04:13:35 am UTC

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“.

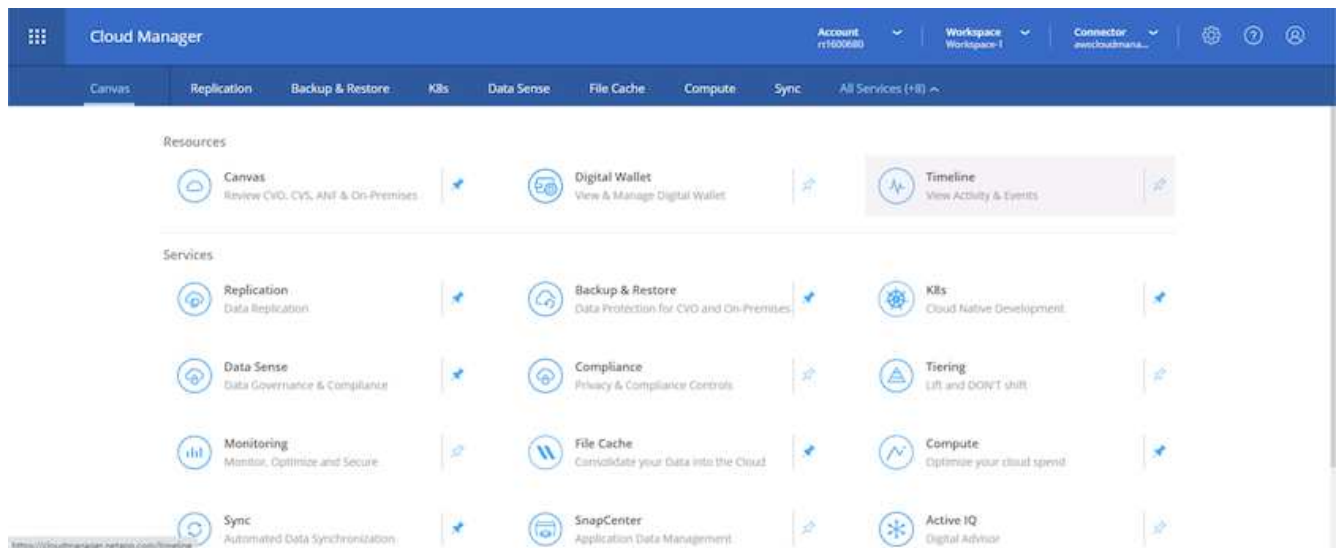
Cloud Manager 3.8.9 Build 9 Aug 18, 2021 04:13:35 am UTC

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	awscloudmana...	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, 10:09:39 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

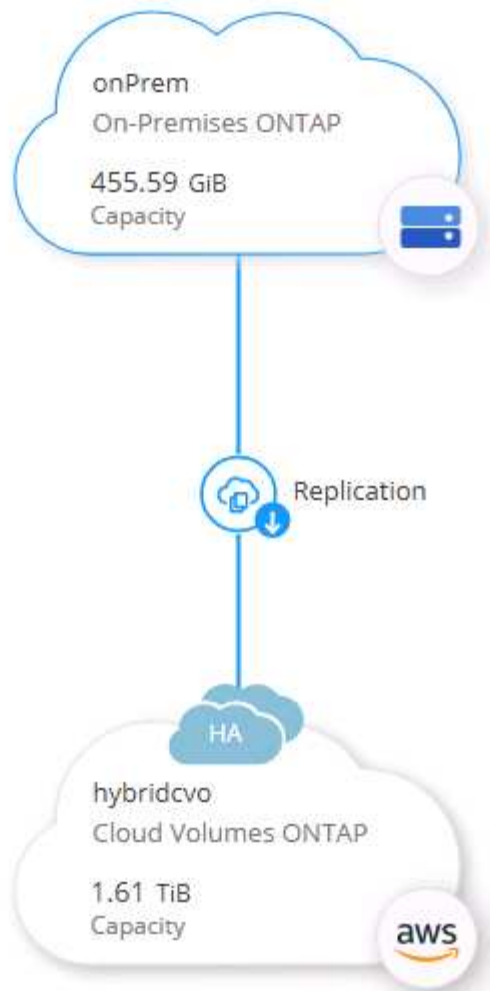
- 1 Cloud Volumes ONTAP (High-Availability) 1 GB Allocated Capacity
- 1 Amazon S3 0 Buckets

### 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



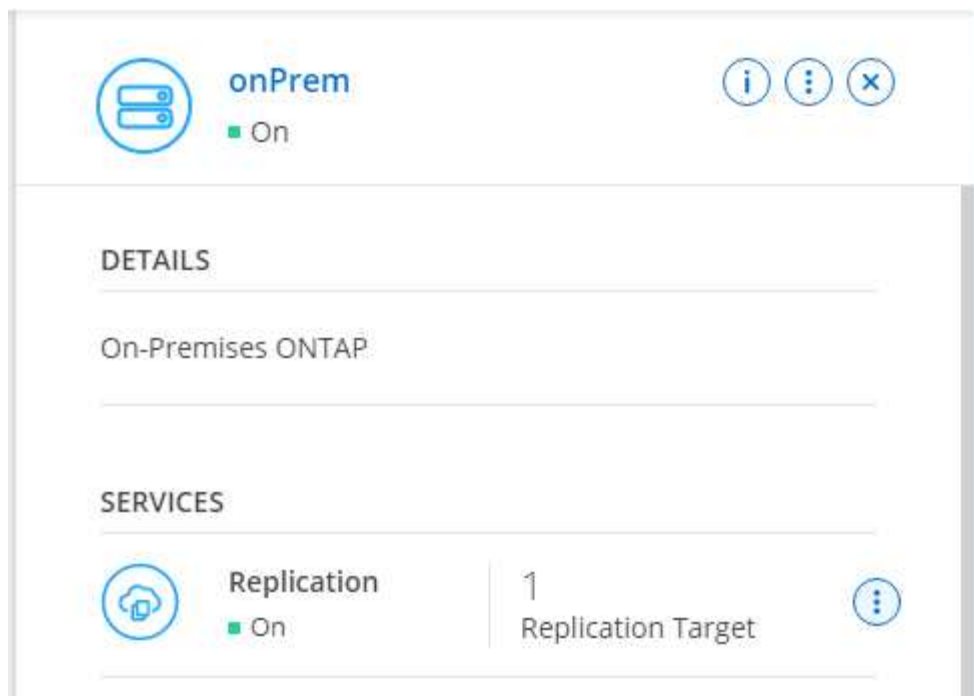
Replication

■ Off

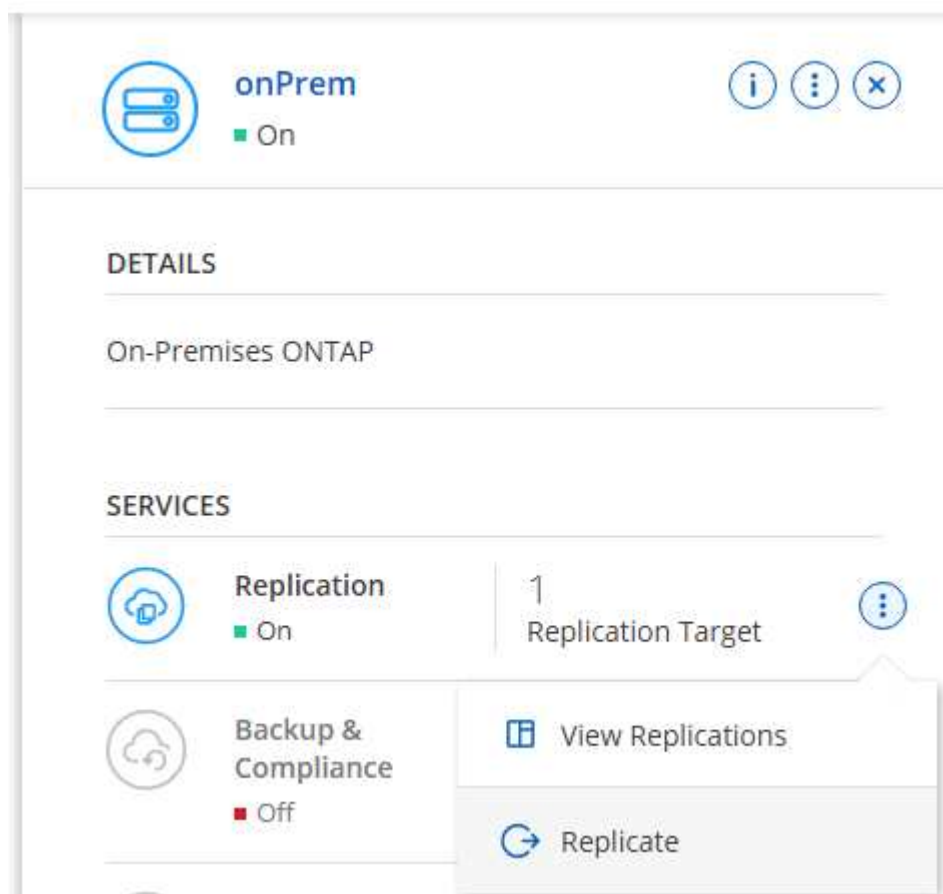
Enable



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 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-Volumen repliziert. Sie können auch eine andere Richtlinie auf Basis Ihrer Anforderungen wählen.

## Replication Policy


Default Policies

Additional Policies

 Mirror

Typically used for disaster recovery

More info

 Mirror and Backup (1 month retention)

Configures disaster recovery and long-term retention of backups on the same destination volume

More info

8. Wählen Sie den Zeitplan für das Auslösen der Replikation aus. NetApp empfiehlt die Festlegung eines „täglichen“ Zeitplans für das Daten-Volumen und einen „stündlichen“ Zeitplan für die Log-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	Destination Thin Provisioning:	Yes
Source Volume Used Size:	45.09 GB	Destination Aggregate:	aggr1 (Automatically s...
Source Thin Provisioning:	Yes	Destination Storage VM:	svm_hybridcvo
Destination Volume Allocated Size:	53.37 GB	Max Transfer Rate:	100 MB/s
Destination Volume Disk Type:	General Purpose SSD (...)	SnapMirror Policy:	Mirror
Capacity Tiering:	S3	Replication Schedule:	daily

Go

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"](#).

## 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.