Hybride Cloud-Datenbanklösungen mit SnapCenter

NetApp database solutions

NetApp
August 18, 2025

Inhalt

Hybride Cloud-Datenbanklösungen mit SnapCenter

TR-4908: Hybrid Cloud-Datenbanklösungen mit SnapCenter – Übersicht

Alan Cao, Felix Melligan, NetApp

Diese Lösung bietet NetApp -Mitarbeitern und Kunden Anweisungen und Anleitungen zum Konfigurieren, Betreiben und Migrieren von Datenbanken in eine Hybrid-Cloud-Umgebung mithilfe des GUI-basierten Tools NetApp SnapCenter und des NetApp Storage-Dienstes CVO in öffentlichen Clouds für die folgenden Anwendungsfälle:

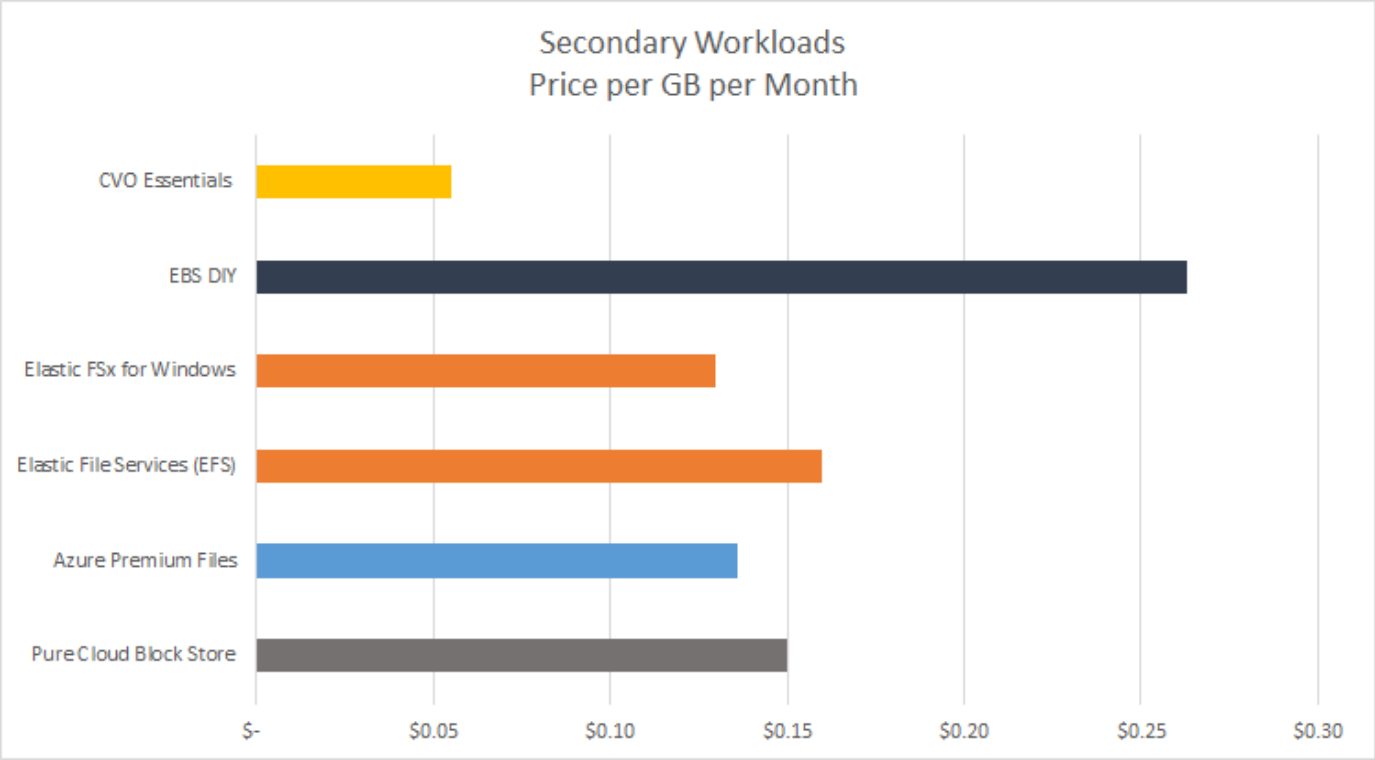
- Datenbank-Entwicklungs-/Testvorgänge in der Hybrid Cloud
- Datenbank-Notfallwiederherstellung in der Hybrid Cloud

Heutzutage befinden sich viele Unternehmensdatenbanken aus Leistungs-, Sicherheits- und/oder anderen Gründen noch immer in privaten Unternehmensrechenzentren. Diese Hybrid-Cloud-Datenbanklösung ermöglicht es Unternehmen, ihre primären Datenbanken vor Ort zu betreiben und gleichzeitig eine öffentliche Cloud für Entwicklungs-/Test-Datenbankvorgänge sowie für die Notfallwiederherstellung zu verwenden, um Lizenz- und Betriebskosten zu senken.

Viele Unternehmensdatenbanken wie Oracle, SQL Server, SAP HANA usw. sind mit hohen Lizenz- und Betriebskosten verbunden. Viele Kunden zahlen eine einmalige Lizenzgebühr sowie jährliche Supportkosten, die auf der Anzahl der Rechenkerne in ihrer Datenbankumgebung basieren, unabhängig davon, ob die Kerne für Entwicklung, Tests, Produktion oder Notfallwiederherstellung verwendet werden. Viele dieser Umgebungen werden während des gesamten Anwendungslebenszyklus möglicherweise nicht vollständig genutzt.

Die Lösungen bieten Kunden die Möglichkeit, die Anzahl ihrer lizenzierbaren Kerne potenziell zu reduzieren, indem sie ihre Datenbankumgebungen, die für Entwicklung, Tests oder Notfallwiederherstellung vorgesehen sind, in die Cloud verschieben. Durch die Nutzung der Skalierbarkeit, Redundanz, Hochverfügbarkeit und eines verbrauchsbasierten Abrechnungsmodells der öffentlichen Cloud können erhebliche Kosteneinsparungen bei Lizenzierung und Betrieb erzielt werden, ohne dass dabei die Benutzerfreundlichkeit oder Verfügbarkeit der Anwendung beeinträchtigt wird.

Neben potenziellen Einsparungen bei den Datenbanklizenzkosten ermöglicht das kapazitätsbasierte CVO-Lizenzmodell von NetApp den Kunden, Speicherkosten pro GB einzusparen und bietet ihnen gleichzeitig ein hohes Maß an Datenbankverwaltungsfreundlichkeit, das bei konkurrierenden Speicherdiensten nicht verfügbar ist. Das folgende Diagramm zeigt einen Vergleich der Speicherkosten beliebter Speicherdienste, die in der öffentlichen Cloud verfügbar sind.



Diese Lösung zeigt, dass sich Hybrid-Cloud-Datenbankvorgänge mithilfe des GUI-basierten Softwaretools SnapCenter und der NetApp SnapMirror Technologie einfach einrichten, implementieren und betreiben lassen.

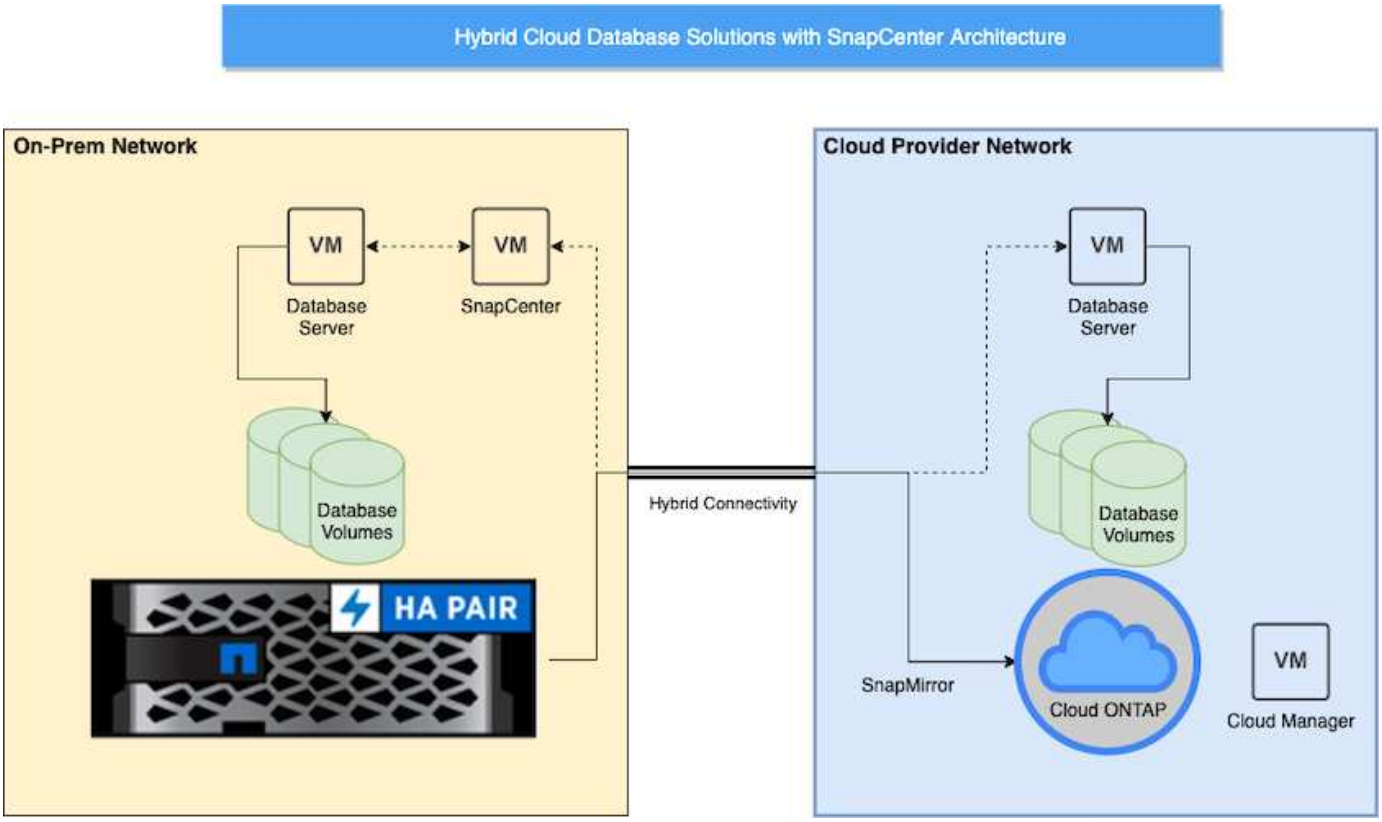
Die folgenden Videos zeigen SnapCenter in Aktion:

- "Sicherung einer Oracle-Datenbank über eine Hybrid Cloud mit SnapCenter"
- "SnapCenter– DEV/TEST für eine Oracle-Datenbank in die AWS Cloud klonen"

Obwohl die Abbildungen in diesem Dokument CVO als Zielspeicherinstanz in der öffentlichen Cloud zeigen, ist die Lösung auch für die neue Version der FSx ONTAP -Speicher-Engine für AWS vollständig validiert.

Lösungsarchitektur

Das folgende Architekturdiagramm veranschaulicht eine typische Implementierung des Unternehmensdatenbankbetriebs in einer Hybrid Cloud für Entwicklungs-/Test- und Notfallwiederherstellungsvorgänge.



Im normalen Geschäftsbetrieb können synchronisierte Datenbankvolumes in der Cloud geklont und zur Anwendungsentwicklung oder zum Testen in Dev/Test-Datenbankinstanzen eingebunden werden. Im Falle eines Ausfalls können dann die synchronisierten Datenbankvolumes in der Cloud zur Notfallwiederherstellung aktiviert werden.

SnapCenter Anforderungen

Diese Lösung ist für eine Hybrid-Cloud-Umgebung konzipiert, um lokale Produktionsdatenbanken zu unterstützen, die für Entwicklungs-/Test- und Notfallwiederherstellungsvorgänge auf alle gängigen öffentlichen Clouds übertragen werden können.

Diese Lösung unterstützt alle Datenbanken, die derzeit von SnapCenter unterstützt werden, obwohl hier nur Oracle- und SQL Server-Datenbanken demonstriert werden. Diese Lösung wird mit virtualisierten Datenbank-Workloads validiert, obwohl auch Bare-Metal-Workloads unterstützt werden.

Wir gehen davon aus, dass Produktionsdatenbankserver vor Ort gehostet werden und DB-Volumes den DB-Hosts von einem ONTAP Speichercluster bereitgestellt werden. Die SnapCenter software wird vor Ort für die Datenbanksicherung und Datenreplikation in die Cloud installiert. Ein Ansible-Controller wird empfohlen, ist aber für die Automatisierung der Datenbankbereitstellung oder die Synchronisierung des Betriebssystemkernels und der Datenbankkonfiguration mit einer Standby-DR-Instanz oder Entwicklungs-/Testinstanzen in der öffentlichen Cloud nicht erforderlich.

Anforderungen

Umfeld	Anforderungen
Vor Ort	Alle von SnapCenter unterstützten Datenbanken und Versionen
	SnapCenter v4.4 oder höher
	Ansible v2.09 oder höher
	ONTAP Cluster 9.x
	Intercluster-LIFs konfiguriert
	Konnektivität von lokalen Standorten zu einem Cloud-VPC (VPN, Interconnect usw.)
	Netzwerkports geöffnet – SSH 22 – TCP 8145, 8146, 10000, 11104, 11105
Cloud – AWS	"Cloud Manager-Connector"
	"Cloud Volumes ONTAP"
	Abgleichen von DB OS EC2-Instanzen mit On-Prem
Cloud – Azure	"Cloud Manager-Connector"
	"Cloud Volumes ONTAP"
	Abgleich von DB OS Azure Virtual Machines mit On-Prem
Cloud – GCP	"Cloud Manager-Connector"
	"Cloud Volumes ONTAP"
	Abgleichen von DB OS Google Compute Engine-Instanzen mit lokalen

Voraussetzungen für die Konfiguration

Voraussetzungen für die Konfiguration

Vor der Ausführung von Hybrid-Cloud-Datenbank-Workloads müssen bestimmte Voraussetzungen sowohl vor Ort als auch in der Cloud konfiguriert werden. Der folgende Abschnitt bietet eine allgemeine Zusammenfassung dieses Prozesses und die folgenden Links bieten weitere Informationen zur erforderlichen Systemkonfiguration.

Vor Ort

- Installation und Konfiguration von SnapCenter
- Speicherkonfiguration des lokalen Datenbankservers
- Lizenzanforderungen
- Vernetzung und Sicherheit
- Automatisierung

Öffentliche Cloud

- Ein NetApp Cloud Central-Login
- Netzwerkzugriff von einem Webbrowser auf mehrere Endpunkte

- Ein Netzwerkstandort für einen Connector
- Cloud-Anbieter-Berechtigungen
- Vernetzung für einzelne Dienste

Wichtige Überlegungen:

1. Wo soll der Cloud Manager Connector bereitgestellt werden?
2. Dimensionierung und Architektur von Cloud Volume ONTAP
3. Einzelknoten oder Hochverfügbarkeit?

Weitere Einzelheiten finden Sie unter den folgenden Links:

"Vor Ort"

"Öffentliche Cloud"

Voraussetzungen vor Ort

Die folgenden Aufgaben müssen vor Ort abgeschlossen werden, um die SnapCenter Hybrid-Cloud-Datenbank-Workloadumgebung vorzubereiten.

Installation und Konfiguration von SnapCenter

Das NetApp SnapCenter -Tool ist eine Windows-basierte Anwendung, die normalerweise in einer Windows-Domänenumgebung ausgeführt wird, obwohl auch eine Bereitstellung in Arbeitsgruppen möglich ist. Es basiert auf einer mehrschichtigen Architektur, die einen zentralen Verwaltungsserver (den SnapCenter -Server) und ein SnapCenter Plug-In auf den Datenbankserver-Hosts für Datenbank-Workloads umfasst. Hier sind einige wichtige Überlegungen zur Hybrid-Cloud-Bereitstellung.

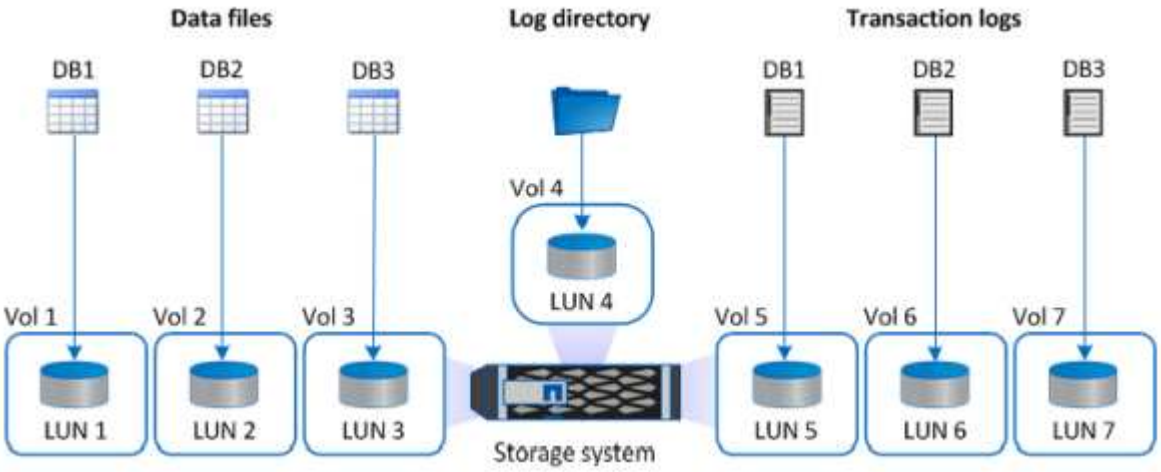
- **Einzelinstanz oder HA-Bereitstellung.** Die HA-Bereitstellung bietet Redundanz für den Fall, dass ein einzelner SnapCenter -Instanzserver ausfällt.
- **Namensauflösung.** DNS muss auf dem SnapCenter -Server konfiguriert werden, um alle Datenbankhosts aufzulösen, sowie auf dem Speicher-SVM für die Vorwärts- und Rückwärtssuche. DNS muss auch auf Datenbankservern konfiguriert werden, um den SnapCenter -Server und die Speicher-SVM sowohl für die Vorwärts- als auch für die Rückwärtssuche aufzulösen.
- **Konfiguration der rollenbasierten Zugriffskontrolle (RBAC).** Bei gemischten Datenbank-Workloads möchten Sie möglicherweise RBAC verwenden, um die Verwaltungsverantwortung für verschiedene DB-Plattformen zu trennen, z. B. einen Administrator für die Oracle-Datenbank oder einen Administrator für SQL Server. Dem DB-Admin-Benutzer müssen die erforderlichen Berechtigungen erteilt werden.
- **Aktivieren Sie eine richtlinienbasierte Sicherungsstrategie.** Um die Konsistenz und Zuverlässigkeit der Sicherung zu gewährleisten.
- **Öffnen Sie die erforderlichen Netzwerkports in der Firewall.** Damit der lokale SnapCenter -Server mit im Cloud-DB-Host installierten Agenten kommunizieren kann.
- **Ports müssen geöffnet sein, um SnapMirror Verkehr zwischen On-Premise und der öffentlichen Cloud zu ermöglichen.** Der SnapCenter -Server verwendet ONTAP SnapMirror , um Snapshot-Backups vor Ort auf Cloud-CVO-Speicher-SVMs zu replizieren.

Nach sorgfältiger Planung und Überlegung vor der Installation klicken Sie auf diese"Voraussetzungen für die SnapCenter -Installation" für Details zur Installation und Konfiguration von SnapCenter .

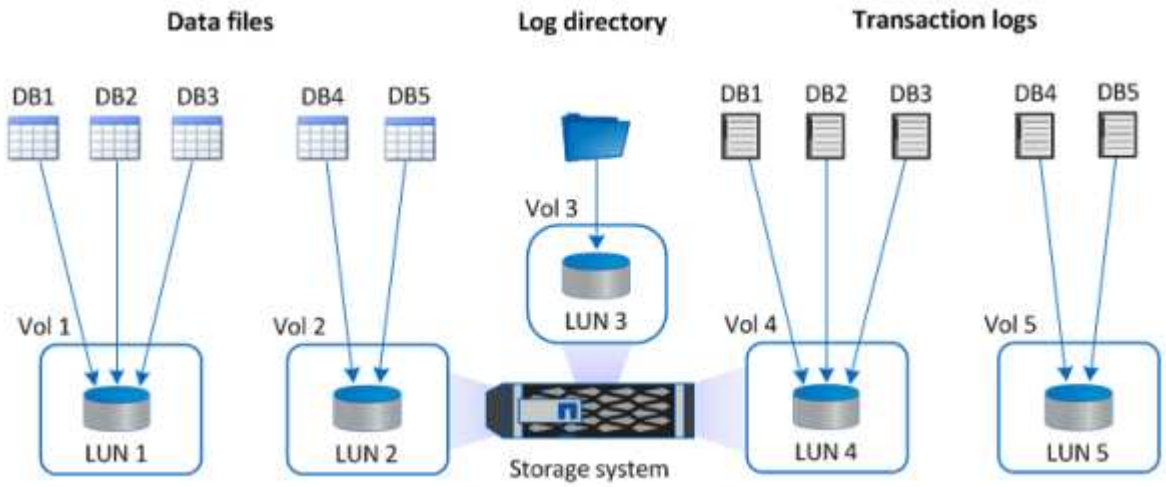
Speicherkonfiguration des lokalen Datenbankservers

Die Speicherleistung spielt eine wichtige Rolle für die Gesamtleistung von Datenbanken und Anwendungen. Ein gut konzipiertes Speicherlayout kann nicht nur die DB-Leistung verbessern, sondern auch die Verwaltung der Datenbanksicherung und -wiederherstellung vereinfachen. Bei der Definition Ihres Speicherlayouts sollten Sie mehrere Faktoren berücksichtigen, darunter die Größe der Datenbank, die erwartete Datenänderungsrate für die Datenbank und die Häufigkeit, mit der Sie Sicherungen durchführen.

Das direkte Anschließen von Speicher-LUNs an die Gast-VM über NFS oder iSCSI für virtualisierte Datenbank-Workloads bietet im Allgemeinen eine bessere Leistung als die Speicherzuweisung über VMDK. NetApp empfiehlt das in der folgenden Abbildung dargestellte Speicherlayout für eine große SQL Server-Datenbank auf LUNs.



Die folgende Abbildung zeigt das von NetApp empfohlene Speicherlayout für kleine oder mittlere SQL Server-Datenbanken auf LUNs.



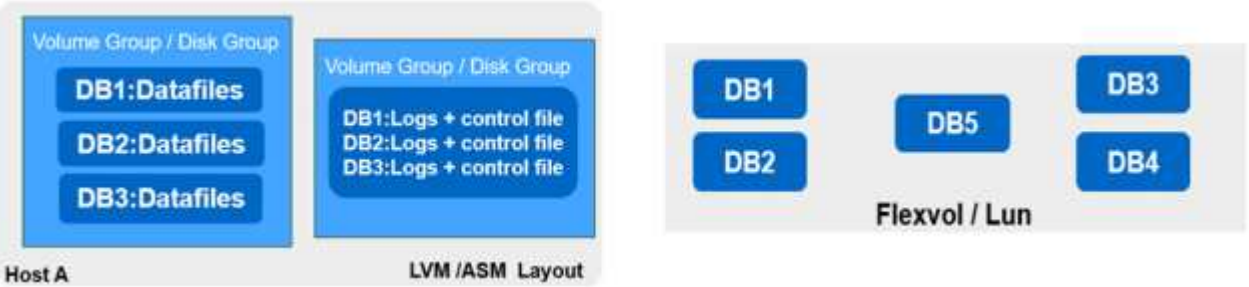
Das Protokollverzeichnis ist SnapCenter vorbehalten, um das Transaktionsprotokoll-Rollup für die Datenbankwiederherstellung durchzuführen. Bei einer besonders großen Datenbank können einem Volume mehrere LUNs zugewiesen werden, um die Leistung zu verbessern.

Für Oracle-Datenbank-Workloads unterstützt SnapCenter Datenbankumgebungen, die von ONTAP -Speicher unterstützt werden und als physische oder virtuelle Geräte auf dem Host bereitgestellt werden. Sie können die gesamte Datenbank je nach Kritikalität der Umgebung auf einem oder mehreren Speichergeräten hosten.

Normalerweise isolieren Kunden Datendateien auf dediziertem Speicher von allen anderen Dateien wie Steuerdateien, Redo-Dateien und Archivprotokolldateien. Dies hilft Administratoren, mithilfe der Snapshot-Technologie innerhalb weniger Sekunden bis Minuten eine große kritische Datenbank (im Petabyte-Bereich) schnell wiederherzustellen (ONTAP Single-File SnapRestore) oder zu klonen.

Für geschäftskritische Workloads, die empfindlich auf Latenz reagieren, sollte ein dediziertes Speichervolume für verschiedene Arten von Oracle-Dateien bereitgestellt werden, um die bestmögliche Latenz zu erreichen. Bei einer großen Datenbank sollten den Datendateien mehrere LUNs (NetApp empfiehlt bis zu acht) pro Volume zugewiesen werden.

Für kleinere Oracle-Datenbanken unterstützt SnapCenter gemeinsam genutzte Speicherlayouts, in denen Sie mehrere Datenbanken oder Teile einer Datenbank auf demselben Speichervolume oder LUN hosten können. Als Beispiel für dieses Layout können Sie Datendateien für alle Datenbanken auf einer +DATA ASM-Datenträgergruppe oder einer Datenträgergruppe hosten. Die restlichen Dateien (Redo-, Archivprotokoll- und Steuerdateien) können auf einer anderen dedizierten Datenträgergruppe oder Volumegruppe (LVM) gehostet werden. Ein solches Bereitstellungsszenario wird unten veranschaulicht.



Um die Verlagerung von Oracle-Datenbanken zu erleichtern, sollte die Oracle-Binärdatei auf einer separaten LUN installiert werden, die in der regulären Sicherungsrichtlinie enthalten ist. Dadurch wird sichergestellt, dass im Falle einer Datenbankverschiebung auf einen neuen Serverhost der Oracle-Stack zur Wiederherstellung gestartet werden kann, ohne dass aufgrund einer nicht synchronisierten Oracle-Binärdatei potenzielle Probleme auftreten.

Lizenzanforderungen

SnapCenter ist eine lizenzierte Software von NetApp. Es ist im Allgemeinen in einer lokalen ONTAP -Lizenz enthalten. Für die Hybrid-Cloud-Bereitstellung ist jedoch auch eine Cloud-Lizenz für SnapCenter erforderlich, um CVO als Ziel für die Datenreplikation zu SnapCenter hinzuzufügen. Weitere Informationen zur kapazitätsbasierten Standardlizenz von SnapCenter finden Sie unter den folgenden Links:

"SnapCenter Standard-Kapazitätslizenzen"

Vernetzung und Sicherheit

Bei einem hybriden Datenbankbetrieb, der eine lokale Produktionsdatenbank erfordert, die für Entwicklung/Test und Notfallwiederherstellung in die Cloud ausgelagert werden kann, sind Vernetzung und Sicherheit wichtige Faktoren, die beim Einrichten der Umgebung und beim Herstellen einer Verbindung mit der öffentlichen Cloud von einem lokalen Rechenzentrum aus berücksichtigt werden müssen.

Öffentliche Clouds verwenden normalerweise eine virtuelle private Cloud (VPC), um verschiedene Benutzer innerhalb einer öffentlichen Cloud-Plattform zu isolieren. Innerhalb einer einzelnen VPC wird die Sicherheit mithilfe von Maßnahmen wie Sicherheitsgruppen gesteuert, die je nach Benutzeranforderungen für die Sperrung einer VPC konfigurierbar sind.

Die Konnektivität vom lokalen Rechenzentrum zum VPC kann durch einen VPN-Tunnel gesichert werden. Auf dem VPN-Gateway kann die Sicherheit mithilfe von NAT- und Firewall-Regeln erhöht werden, die Versuche blockieren, Netzwerkverbindungen von Hosts im Internet zu Hosts im Unternehmensrechenzentrum herzustellen.

Überprüfen Sie aus Netzwerk- und Sicherheitsgründen die relevanten CVO-Regeln für eingehenden und ausgehenden Datenverkehr für die öffentliche Cloud Ihrer Wahl:

- "Sicherheitsgruppenregeln für CVO – AWS"
- "Sicherheitsgruppenregeln für CVO – Azure"
- "Firewall-Regeln für CVO – GCP"

Verwenden der Ansible-Automatisierung zum Synchronisieren von DB-Instances zwischen lokalen Standorten und der Cloud – optional

Um die Verwaltung einer Hybrid-Cloud-Datenbankumgebung zu vereinfachen, empfiehlt NetApp dringend, einen Ansible-Controller einzusetzen, um einige Verwaltungsaufgaben zu automatisieren, beispielsweise die Synchronisierung von Compute-Instanzen vor Ort und in der Cloud. Dies ist jedoch nicht zwingend erforderlich. Dies ist besonders wichtig, da eine nicht synchronisierte Compute-Instanz in der Cloud die wiederhergestellte Datenbank in der Cloud aufgrund fehlender Kernel-Pakete und anderer Probleme fehleranfällig machen kann.

Die Automatisierungsfunktion eines Ansible-Controllers kann auch verwendet werden, um SnapCenter für bestimmte Aufgaben zu erweitern, z. B. das Aufteilen der SnapMirror Instanz, um die DR-Datenkopie für die Produktion zu aktivieren.

Befolgen Sie diese Anweisungen, um Ihren Ansible-Steuerknoten für RedHat- oder CentOS-Maschinen einzurichten:

1. Anforderungen für den Ansible-Steuerknoten:
    a. Eine RHEL/CentOS-Maschine mit den folgenden installierten Paketen:
        i. Python3
        ii. Pip3
        iii. Ansible (Version größer als 2.10.0)
        iv. Git

Wenn Sie über eine neue RHEL/CentOS-Maschine verfügen, auf der die oben genannten Anforderungen nicht installiert sind, führen Sie die folgenden Schritte aus, um diese Maschine als Ansible-Steuerknoten einzurichten:

1. Aktivieren Sie das Ansible-Repository für RHEL-8/RHEL-7
   a. Für RHEL-8 (führen Sie den folgenden Befehl als Root aus)

```
subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-
rpms
```

   b. Für RHEL-7 (führen Sie den folgenden Befehl als Root aus)

```
subscription-manager repos --enable rhel-7-server-ansible-2.9-rpms
```

2. Fügen Sie den folgenden Inhalt in das Terminal ein

```
sudo yum -y install python3 >> install.log
sudo yum -y install python3-pip >> install.log
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
install.log
sudo yum -y install git >> install.log
```

Befolgen Sie diese Anweisungen, um Ihren Ansible-Steuerknoten für Ubuntu- oder Debian-Maschinen einzurichten:

1. Anforderungen für den Ansible-Steuerknoten:
   a. Eine Ubuntu/Debian-Maschine mit den folgenden installierten Paketen:
      i. Python3
      ii. Pip3
      iii. Ansible (Version größer als 2.10.0)
      iv. Git

Wenn Sie über eine neue Ubuntu/Debian-Maschine verfügen, auf der die oben genannten Anforderungen nicht installiert sind, führen Sie die folgenden Schritte aus, um diese Maschine als Ansible-Steuerknoten einzurichten:

1. Fügen Sie den folgenden Inhalt in das Terminal ein

```
sudo apt-get -y install python3 >> outputlog.txt
sudo apt-get -y install python3-pip >> outputlog.txt
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
outputlog.txt
sudo apt-get -y install git >> outputlog.txt
```

Voraussetzungen für die Public Cloud

Bevor wir den Cloud Manager-Connector und Cloud Volumes ONTAP installieren und SnapMirror konfigurieren, müssen wir einige Vorbereitungen für unsere Cloud-Umgebung treffen. Auf dieser Seite werden die erforderlichen Arbeiten sowie die Überlegungen zur Bereitstellung von Cloud Volumes ONTAP beschrieben.

Checkliste für die Bereitstellungsvoraussetzungen für Cloud Manager und Cloud Volumes ONTAP

- Ein NetApp Cloud Central-Login
- Netzwerkzugriff von einem Webbrowser auf mehrere Endpunkte
- Ein Netzwerkstandort für einen Connector
- Cloud-Anbieter-Berechtigungen
- Vernetzung für einzelne Dienste

Weitere Informationen zu den Voraussetzungen für den Einstieg finden Sie auf unserer "Cloud-Dokumentation" .

Überlegungen

1. Was ist ein Cloud Manager-Connector?

In den meisten Fällen muss ein Cloud Central-Kontoadministrator einen Connector in Ihrer Cloud oder Ihrem lokalen Netzwerk bereitstellen. Der Connector ermöglicht Cloud Manager die Verwaltung von Ressourcen und Prozessen innerhalb Ihrer öffentlichen Cloud-Umgebung.

Weitere Informationen zu Connectors finden Sie auf unserer "Cloud-Dokumentation" .

2. Dimensionierung und Architektur von Cloud Volumes ONTAP

Beim Bereitstellen von Cloud Volumes ONTAP haben Sie die Wahl zwischen einem vordefinierten Paket oder der Erstellung einer eigenen Konfiguration. Obwohl viele dieser Werte später ohne Unterbrechung geändert werden können, müssen vor der Bereitstellung einige wichtige Entscheidungen basierend auf den in der Cloud bereitzustellenden Workloads getroffen werden.

Jeder Cloud-Anbieter bietet unterschiedliche Bereitstellungsoptionen und fast jede Arbeitslast hat ihre eigenen einzigartigen Eigenschaften. NetApp verfügt über eine "TCO-Rechner" Dies kann dabei helfen, die Größe von Bereitstellungen anhand von Kapazität und Leistung richtig festzulegen. Es basiert jedoch auf einigen grundlegenden Konzepten, die es wert sind, berücksichtigt zu werden:

- Erforderliche Kapazität
- Netzwerkfähigkeit der virtuellen Cloud-Maschine
- Leistungsmerkmale von Cloud-Speicher

Der Schlüssel liegt darin, eine Konfiguration zu planen, die nicht nur die aktuellen Kapazitäts- und Leistungsanforderungen erfüllt, sondern auch zukünftiges Wachstum berücksichtigt. Dies wird allgemein als Kapazitätsspielraum und Leistungsspielraum bezeichnet.

Wenn Sie weitere Informationen wünschen, lesen Sie die Dokumentation zur richtigen Planung für "AWS" , "Azurblau" , Und "GCP" .

3. Einzelknoten oder Hochverfügbarkeit?

In allen Clouds besteht die Möglichkeit, CVO entweder in einem einzelnen Knoten oder in einem Cluster-Hochverfügbarkeitspaar mit zwei Knoten bereitzustellen. Je nach Anwendungsfall möchten Sie möglicherweise einen einzelnen Knoten bereitstellen, um Kosten zu sparen, oder ein HA-Paar, um zusätzliche Verfügbarkeit und Redundanz zu gewährleisten.

Für einen DR-Anwendungsfall oder das Hochfahren eines temporären Speichers für Entwicklung und Tests werden häufig einzelne Knoten verwendet, da die Auswirkungen eines plötzlichen Zonen- oder Infrastrukturausfalls geringer sind. Für alle Produktionsanwendungsfälle, bei denen sich die Daten nur an einem einzigen Ort befinden oder bei denen der Datensatz über mehr Redundanz und Verfügbarkeit verfügen muss, wird jedoch eine hohe Verfügbarkeit empfohlen.

Weitere Informationen zur Architektur der Hochverfügbarkeitsversionen der einzelnen Clouds finden Sie in der Dokumentation für "AWS" , "Azurblau" Und "GCP" .

Erste Schritte – Übersicht

Erste Schritte – Übersicht

Dieser Abschnitt enthält eine Zusammenfassung der Aufgaben, die abgeschlossen werden müssen, um die im vorherigen Abschnitt beschriebenen Voraussetzungen zu erfüllen. Der folgende Abschnitt enthält eine allgemeine Aufgabenliste für lokale und öffentliche Cloud-Vorgänge. Die detaillierten Prozesse und Verfahren können durch Anklicken der entsprechenden Links abgerufen werden.

Vor Ort

- Richten Sie den Datenbankadministratorbenutzer in SnapCenter ein
- Voraussetzungen für die Installation des SnapCenter -Plugins
- Installation des SnapCenter Host-Plugins
- DB-Ressourcenerkennung
- Einrichten von Storage-Cluster-Peering und DB-Volume-Replikation
- Fügen Sie SnapCenter CVO-Datenbankspeicher-SVM hinzu
- Richten Sie die Datenbanksicherungsrichtlinie in SnapCenter ein
- Implementieren Sie eine Sicherungsrichtlinie zum Schutz der Datenbank
- Sicherung validieren

Öffentliche AWS-Cloud

- Vorflugkontrolle
- Schritte zum Bereitstellen von Cloud Manager und Cloud Volumes ONTAP in AWS
- EC2-Compute-Instanz für Datenbank-Workload bereitstellen

Klicken Sie für weitere Informationen auf die folgenden Links:

"Vor Ort","Öffentliche Cloud – AWS"

Erste Schritte vor Ort

Das NetApp SnapCenter -Tool verwendet eine rollenbasierte Zugriffskontrolle (RBAC), um den Zugriff auf Benutzerressourcen und die Erteilung von Berechtigungen zu verwalten. Bei der SnapCenter -Installation werden vorab ausgefüllte Rollen erstellt. Sie können auch benutzerdefinierte Rollen basierend auf Ihren Anforderungen oder Anwendungen erstellen.

Vor Ort

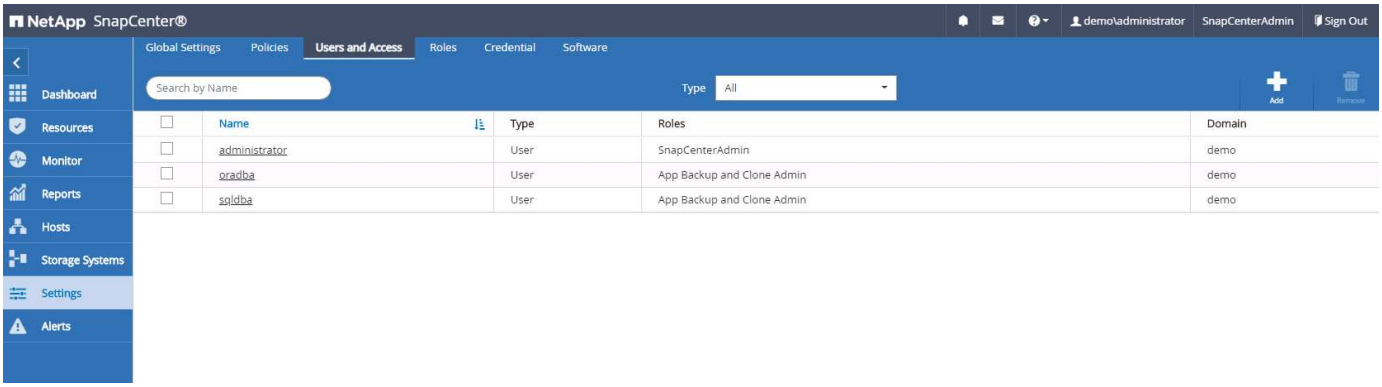
1. Richten Sie den Datenbankadministratorbenutzer in SnapCenter ein

Es ist sinnvoll, für jede von SnapCenter unterstützte Datenbankplattform eine dedizierte Administrator-Benutzer-ID für die Datenbanksicherung, -wiederherstellung und/oder -notfallwiederherstellung zu haben. Sie können auch eine einzige ID verwenden, um alle Datenbanken zu verwalten. In unseren Testfällen und Demonstrationen haben wir jeweils einen dedizierten Administratorbenutzer für Oracle und SQL Server erstellt.

Bestimmte SnapCenter -Ressourcen können nur mit der Rolle „SnapCenterAdmin“ bereitgestellt werden. Anschließend können Ressourcen anderen Benutzerkennungen für den Zugriff zugewiesen werden.

In einer vorinstallierten und konfigurierten SnapCenter Umgebung vor Ort wurden die folgenden Aufgaben möglicherweise bereits abgeschlossen. Wenn nicht, erstellen Sie mit den folgenden Schritten einen Datenbankadministratorbenutzer:

1. Fügen Sie den Administratorbenutzer zu Windows Active Directory hinzu.
2. Melden Sie sich bei SnapCenter mit einer ID an, die Ihnen mit der Rolle SnapCenterAdmin zugewiesen wurde.
3. Navigieren Sie unter „Einstellungen“ und „Benutzer“ zur Registerkarte „Zugriff“ und klicken Sie auf „Hinzufügen“, um einen neuen Benutzer hinzuzufügen. Die neue Benutzer-ID wird mit dem in Schritt 1 in Windows Active Directory erstellten Administratorbenutzer verknüpft. . Weisen Sie dem Benutzer nach Bedarf die richtige Rolle zu. Weisen Sie dem Administratorbenutzer gegebenenfalls Ressourcen zu.



2. Voraussetzungen für die Installation des SnapCenter -Plugins

SnapCenter führt Backup-, Wiederherstellungs-, Klon- und andere Funktionen mithilfe eines Plugin-Agenten durch, der auf den DB-Hosts ausgeführt wird. Es stellt über die auf der Registerkarte „Einstellungen und Anmeldeinformationen“ konfigurierten Anmeldeinformationen eine Verbindung zum Datenbankhost und zur Datenbank für die Plug-in-Installation und andere Verwaltungsfunktionen her. Es gibt spezifische Berechtigungsanforderungen, die auf dem Zielhosttyp (z. B. Linux oder Windows) sowie dem Datenbanktyp basieren.

Die Anmeldeinformationen des DB-Hosts müssen vor der Installation des SnapCenter -Plugins konfiguriert werden. Im Allgemeinen möchten Sie ein Administratorbenutzerkonto auf dem DB-Host als Ihre Host-Verbindungsdaten für die Plugin-Installation verwenden. Sie können dieselbe Benutzer-ID auch für den Datenbankzugriff mithilfe der betriebssystembasierten Authentifizierung gewähren. Andererseits können Sie für den DB-Verwaltungszugriff auch eine Datenbankauthentifizierung mit unterschiedlichen Datenbankbenutzer-IDs verwenden. Wenn Sie sich für die Verwendung der betriebssystembasierten Authentifizierung entscheiden, muss der Benutzer-ID des Betriebssystemadministrators DB-Zugriff gewährt werden. Bei der domänenbasierten SQL Server-Installation von Windows kann ein Domänenadministratorkonto zum Verwalten aller SQL Server innerhalb der Domäne verwendet werden.

Windows-Host für SQL-Server:

1. Wenn Sie Windows-Anmeldeinformationen zur Authentifizierung verwenden, müssen Sie Ihre Anmeldeinformationen einrichten, bevor Sie Plugins installieren.
2. Wenn Sie zur Authentifizierung eine SQL Server-Instanz verwenden, müssen Sie die Anmeldeinformationen nach der Installation der Plug-Ins hinzufügen.
3. Wenn Sie beim Einrichten der Anmeldeinformationen die SQL-Authentifizierung aktiviert haben, wird die erkannte Instanz oder Datenbank mit einem roten Schlosssymbol angezeigt. Wenn das Schlosssymbol angezeigt wird, müssen Sie die Anmeldeinformationen der Instanz oder Datenbank angeben, um die Instanz oder Datenbank erfolgreich zu einer Ressourcengruppe hinzuzufügen.
4. Sie müssen die Anmeldeinformationen einem RBAC-Benutzer ohne Systemadministratorzugriff 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-Administratorbenutzer muss sowohl über die Ressourcengruppen- als auch über die Sicherungsberechtigungen verfügen.

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 auf der 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 Anmeldeinformationen mit dem Linux-Authentifizierungsmodus für den Installationsbenutzer.
4. Sie müssen Java 1.8.x (64-Bit) auf Ihrem Linux-Host installieren.
5. Durch die Installation des Oracle-Datenbank-Plugins wird auch das SnapCenter -Plugin für Unix installiert.

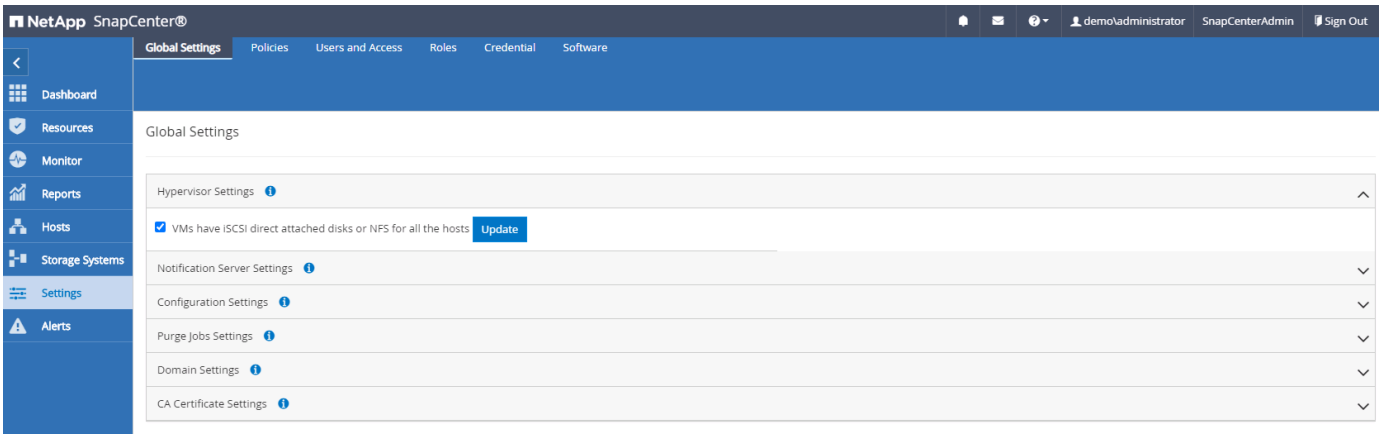
3. Installation des SnapCenter Host-Plugins

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

Die folgenden Schritte veranschaulichen, wie ein Datenbankhost zu SnapCenter hinzugefügt wird, während ein SnapCenter -Plugin auf dem Host installiert ist. Das Verfahren gilt sowohl für das Hinzufügen von lokalen Hosts als auch von Cloud-Hosts. Die folgende Demonstration fügt einen Windows- oder Linux-Host hinzu, der sich in AWS befindet.

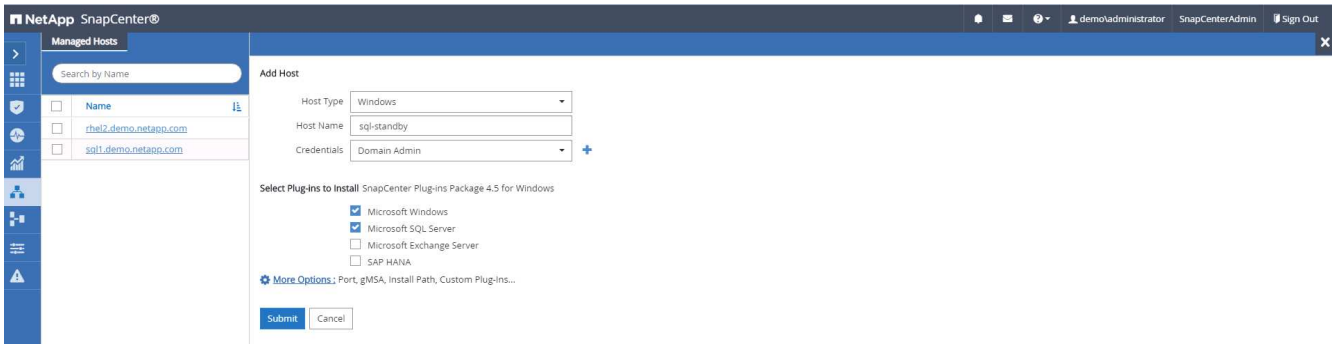
Konfigurieren der globalen SnapCenter VMware-Einstellungen

Navigieren Sie zu Einstellungen > Globale Einstellungen. Wählen Sie unter „Hypervisor-Einstellungen“ die Option „VMs haben iSCSI-Direktanschlussdatenträger oder NFS für alle Hosts“ und klicken Sie auf „Aktualisieren“.



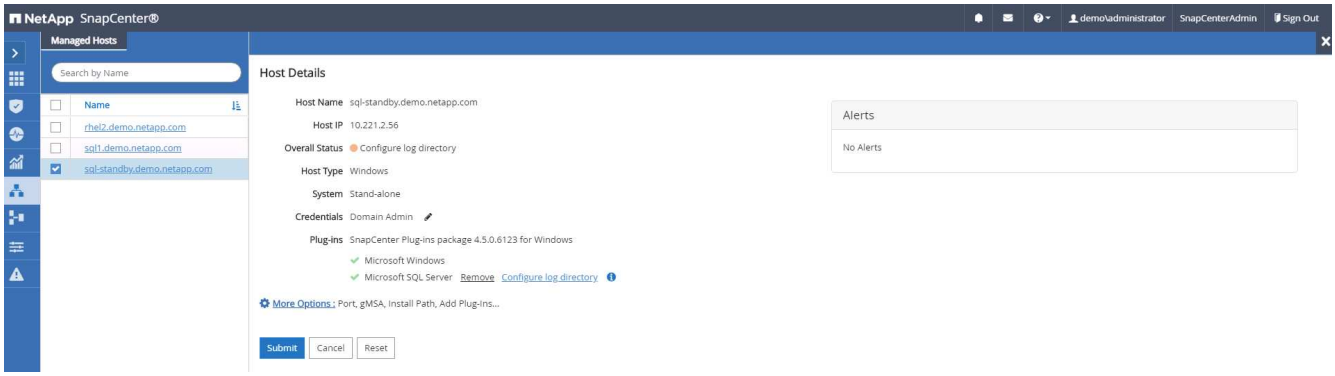
Windows-Host hinzufügen und Plugin auf dem Host installieren

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

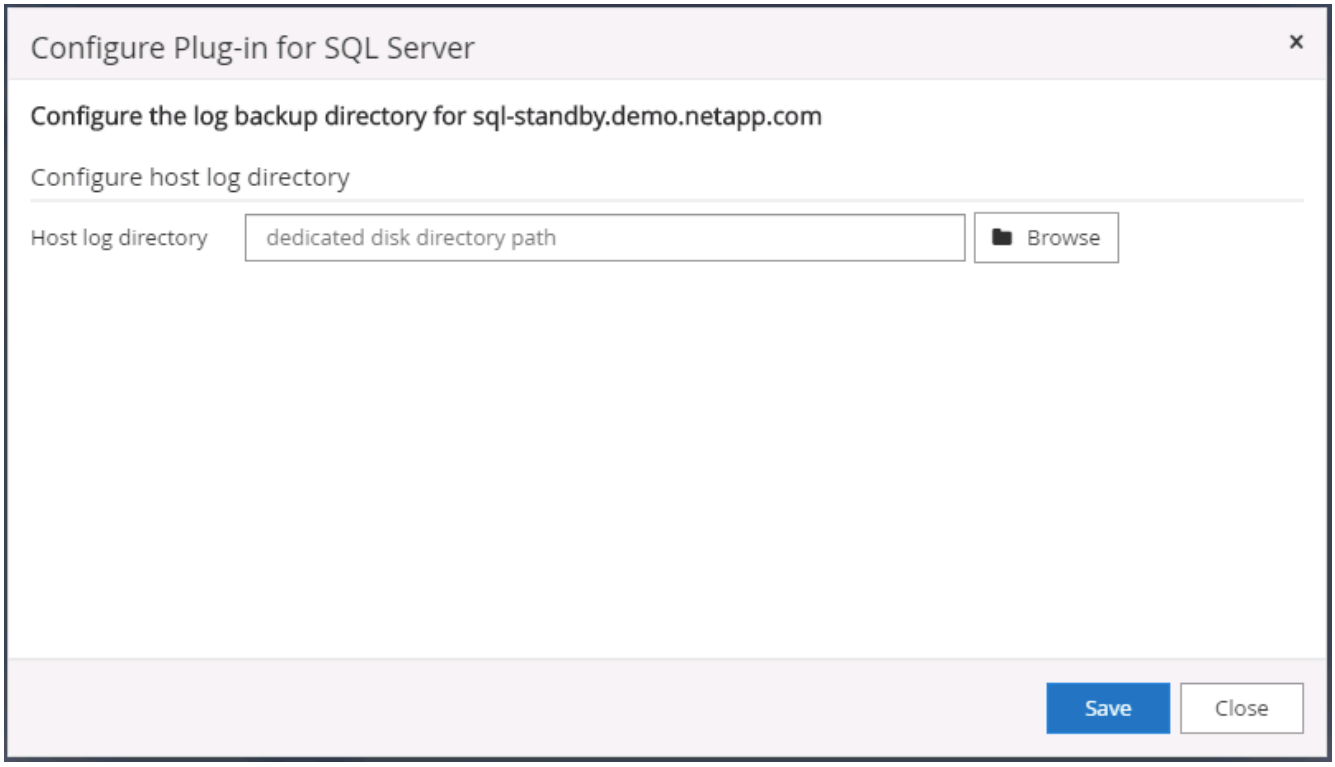


4. Nachdem das Plug-In auf einem Windows-Host installiert wurde, wird sein Gesamtstatus als „Protokollverzeichnis konfigurieren“ angezeigt.

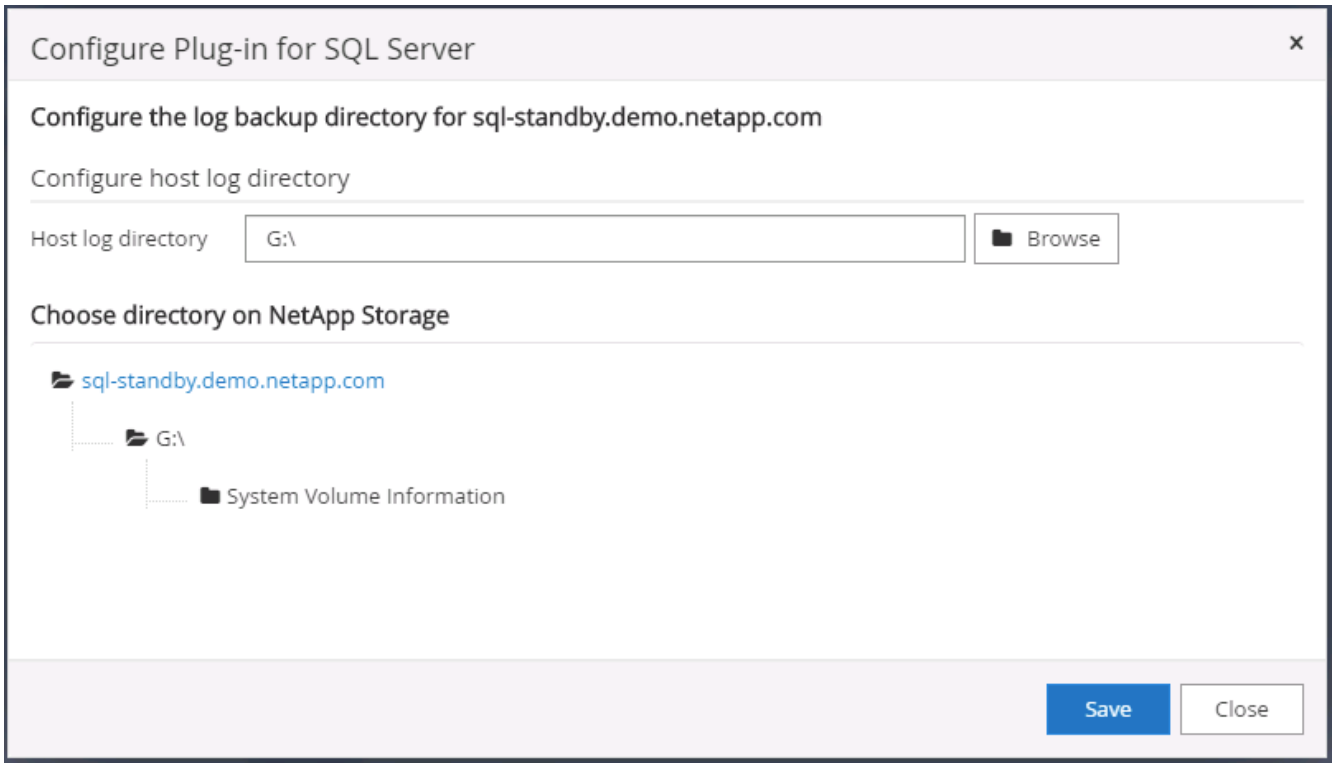
5. Klicken Sie auf den Hostnamen, um die Konfiguration des SQL Server-Protokollverzeichnisses zu öffnen.



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

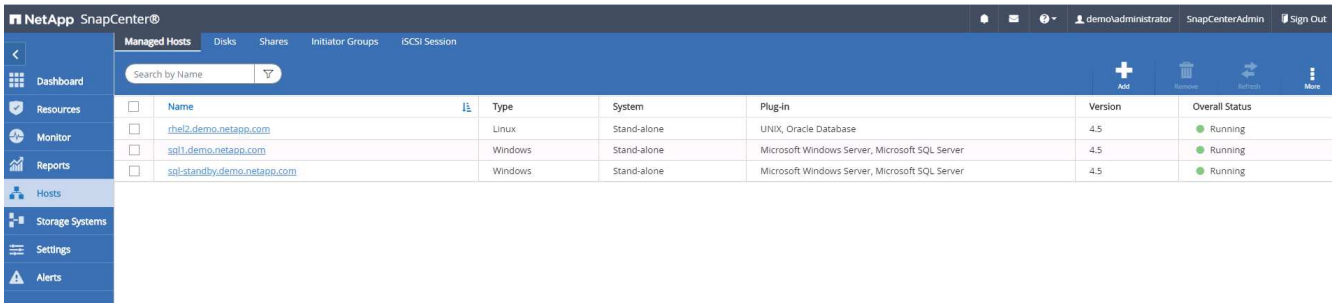


7. Klicken Sie auf „Durchsuchen“, um den NetApp -Speicher zu ermitteln, sodass ein Protokollverzeichnis festgelegt werden kann. SnapCenter verwendet dieses Protokollverzeichnis, um die Transaktionsprotokolldateien des SQL-Servers zusammenzufassen. Klicken Sie dann auf Speichern.

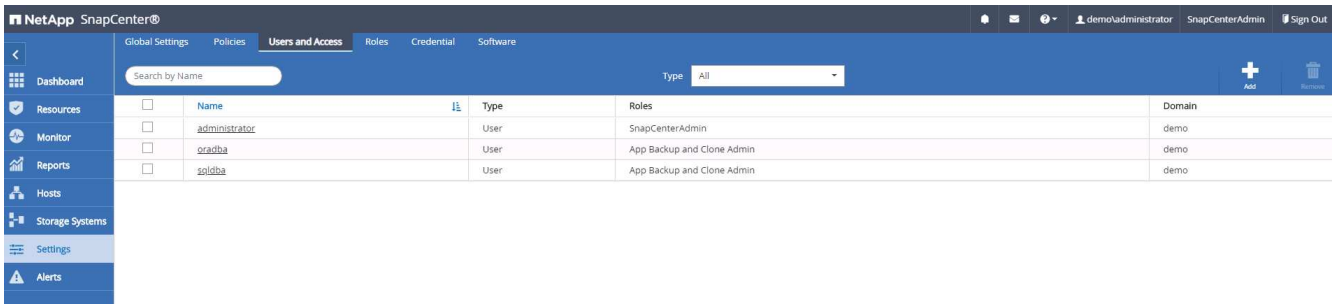


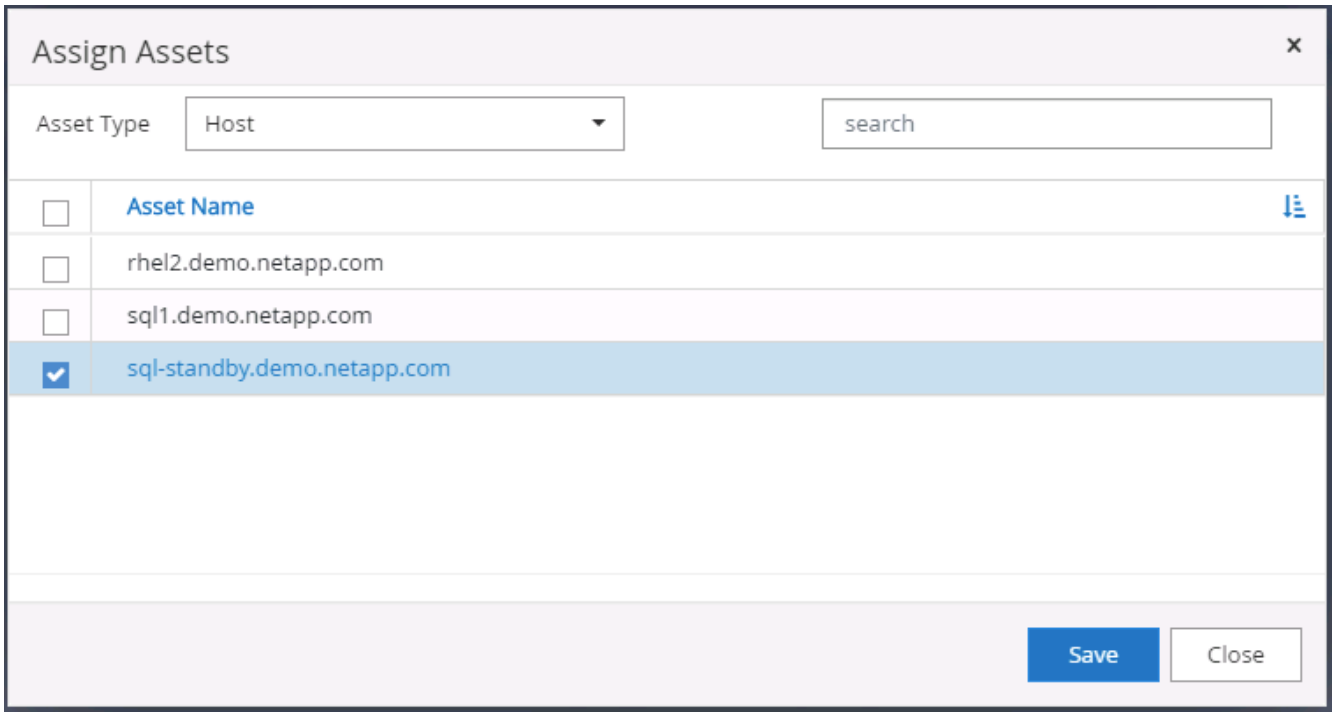
Damit auf einem DB-Host bereitgestellter NetApp Speicher erkannt werden kann, muss der Speicher (vor Ort oder CVO) zu SnapCenter hinzugefügt werden, wie in Schritt 6 für CVO als Beispiel dargestellt.

8. Nachdem das Protokollverzeichnis konfiguriert wurde, wird der Gesamtstatus des Windows-Host-Plugins in „Wird ausgeführt“ geändert.



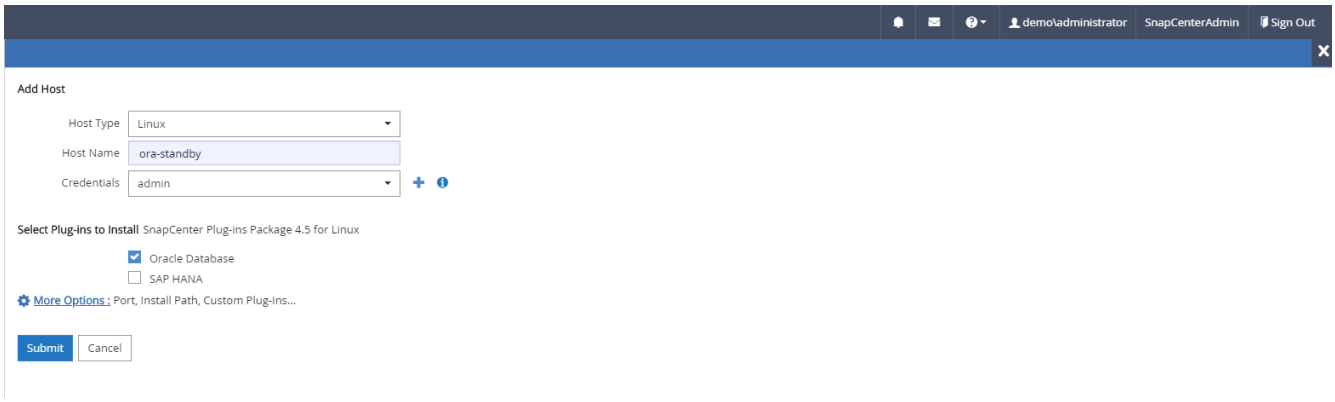
9. Um den Host der Benutzer-ID für die Datenbankverwaltung zuzuweisen, navigieren Sie zur Registerkarte „Zugriff“ unter „Einstellungen“ und „Benutzer“, klicken Sie auf die Benutzer-ID für die Datenbankverwaltung (in unserem Fall die sqldba, der der Host zugewiesen werden muss) und klicken Sie auf „Speichern“, um die Host-Ressourcenzuweisung abzuschließen.



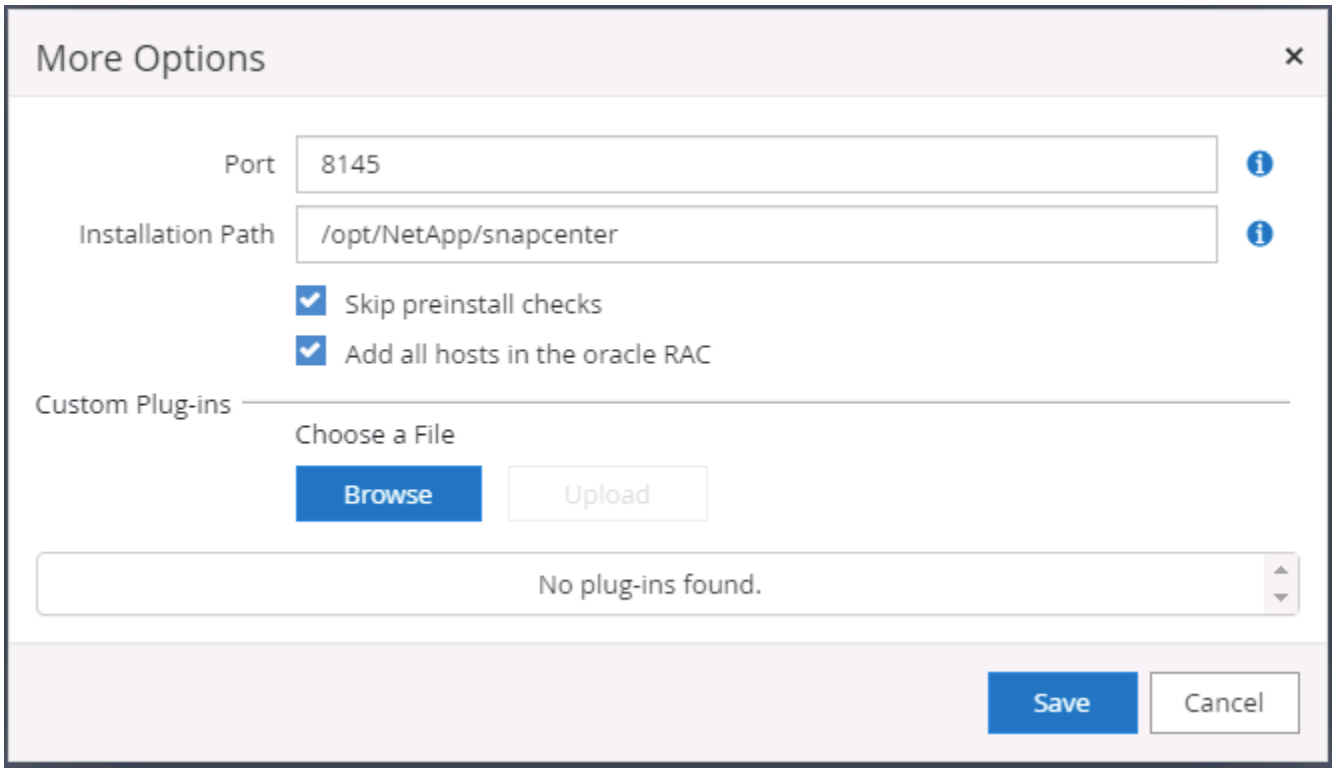


Unix-Host hinzufügen und Plugin auf dem Host installieren

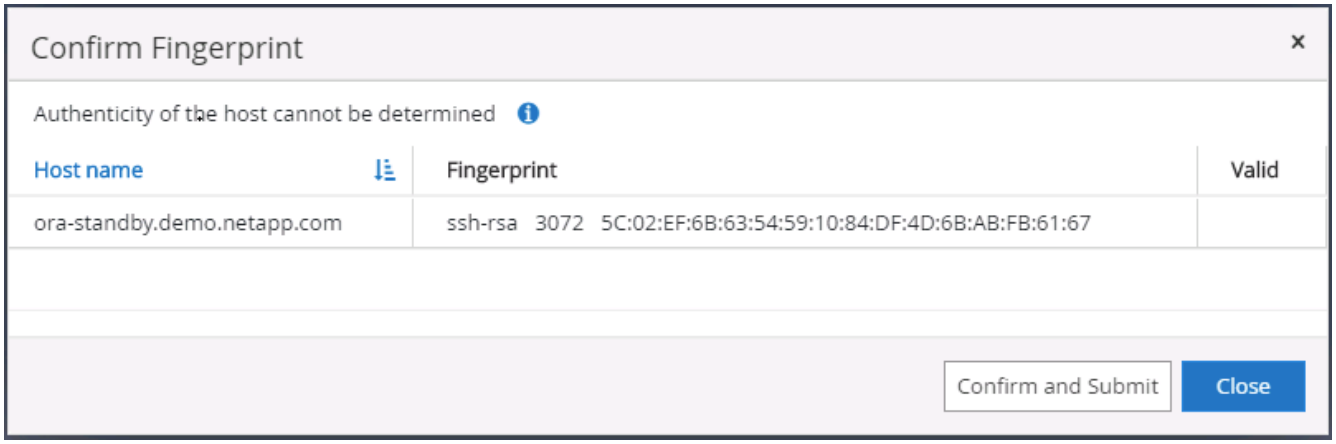
1. Melden Sie sich bei SnapCenter mit einer Benutzer-ID mit SnapCenterAdmin-Berechtigungen an.
2. Klicken Sie im linken Menü auf die Registerkarte „Hosts“ und dann auf „Hinzufügen“, um den Workflow „Host hinzufügen“ zu öffnen.
3. Wählen Sie Linux als Hosttyp. Der Hostname kann entweder der Hostname oder eine IP-Adresse sein. Der Hostname muss jedoch aufgelöst werden, um die Host-IP-Adresse vom SnapCenter -Host zu korrigieren. Wählen Sie die in Schritt 2 erstellten Host-Anmeldeinformationen. Für die Host-Anmeldeinformationen sind Sudo-Berechtigungen erforderlich. Aktivieren Sie „Oracle Database“ als zu installierendes Plug-In, wodurch sowohl Oracle- als auch Linux-Host-Plug-Ins installiert werden.



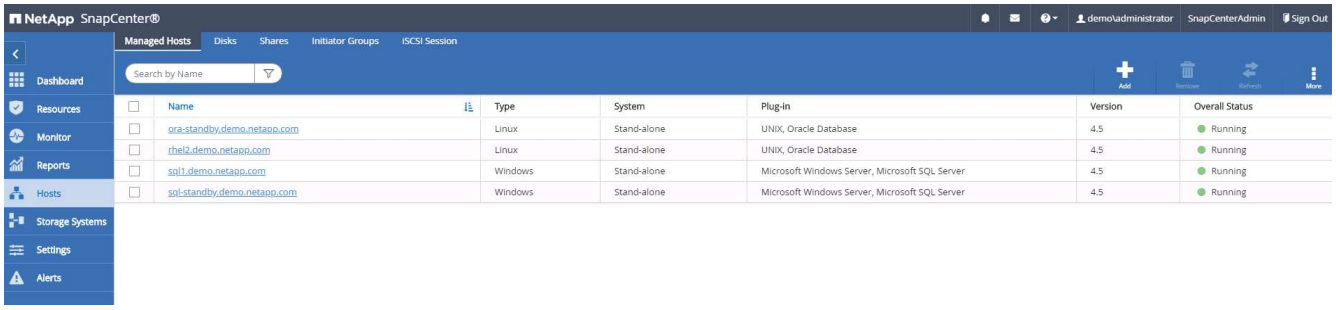
4. Klicken Sie auf „Weitere Optionen“ und wählen Sie „Überprüfungen vor der Installation überspringen“. Sie werden aufgefordert, das Überspringen der Vorinstallationsprüfung zu bestätigen. Klicken Sie auf „Ja“ und dann auf „Speichern“.



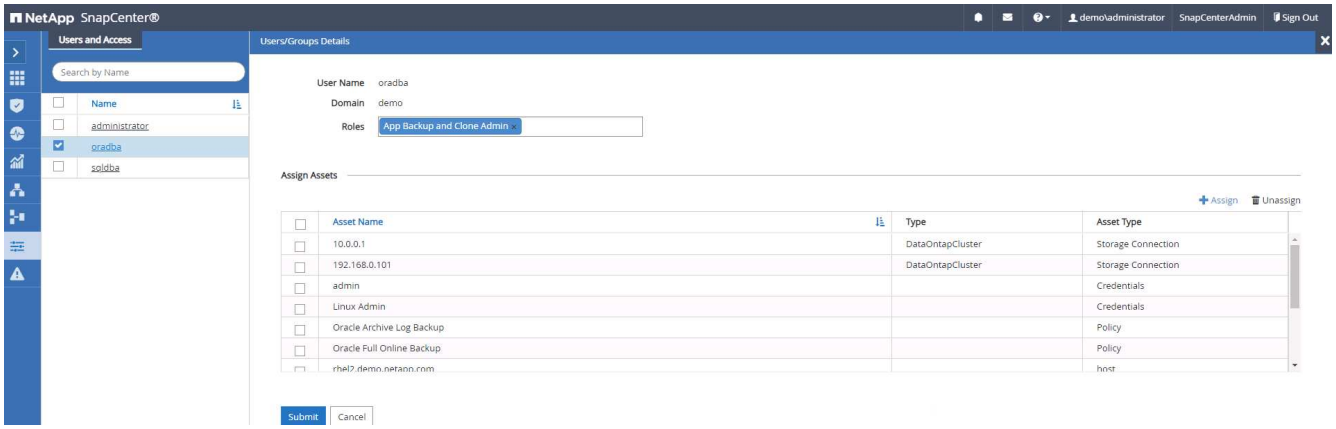
5. Klicken Sie auf „Senden“, um die Installation des Plugins zu starten. Sie werden aufgefordert, den Fingerabdruck wie unten gezeigt zu bestätigen.

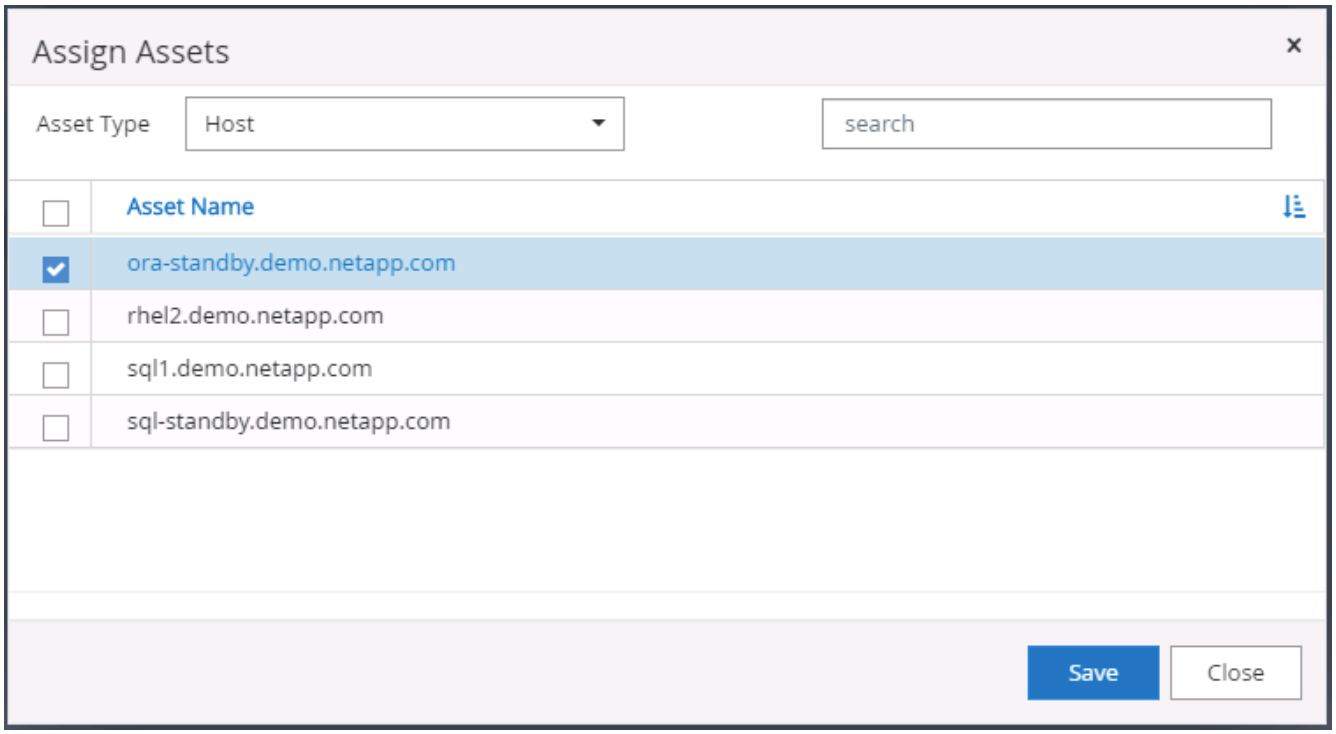


6. SnapCenter führt die Hostvalidierung und -registrierung durch und anschließend wird das Plug-In auf dem Linux-Host installiert. Der Status wird von „Plugin wird installiert“ in „Wird ausgeführt“ geändert.



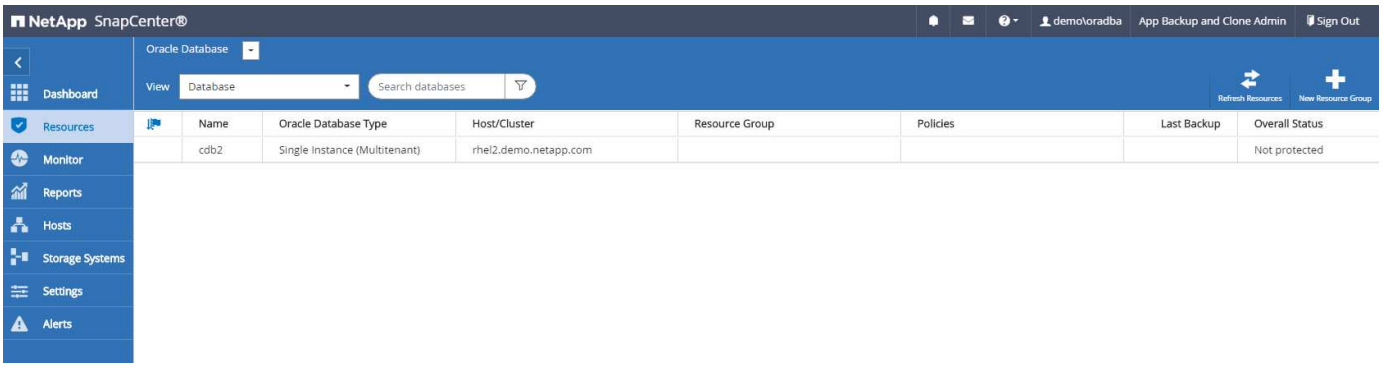
7. Weisen Sie dem neu hinzugefügten Host die richtige Benutzer-ID für die Datenbankverwaltung zu (in unserem Fall oradba).





4. Datenbankressourcenerkennung

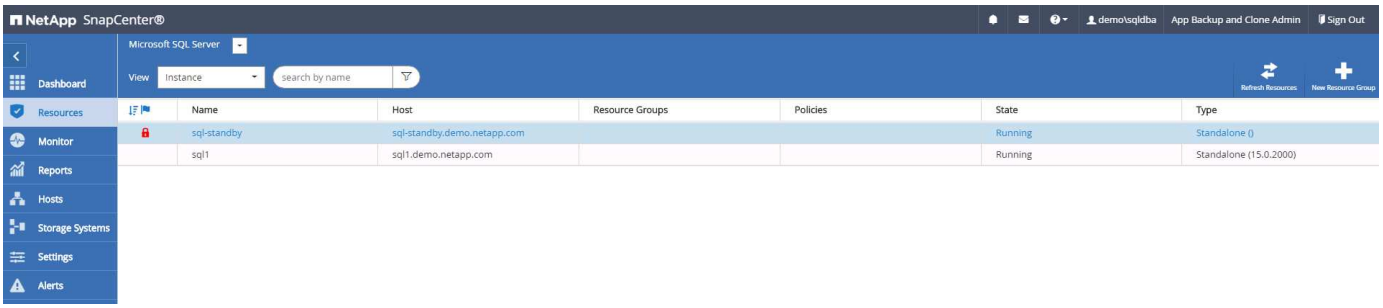
Bei erfolgreicher Plugin-Installation können die Datenbankressourcen auf dem Host sofort erkannt werden. Klicken Sie im linken Menü auf die Registerkarte „Ressourcen“. Je nach Art der Datenbankplattform stehen verschiedene Ansichten zur Verfügung, beispielsweise die Datenbank, die Ressourcengruppe usw. Möglicherweise müssen Sie auf die Registerkarte „Ressourcen aktualisieren“ klicken, wenn die Ressourcen auf dem Host nicht erkannt und angezeigt werden.

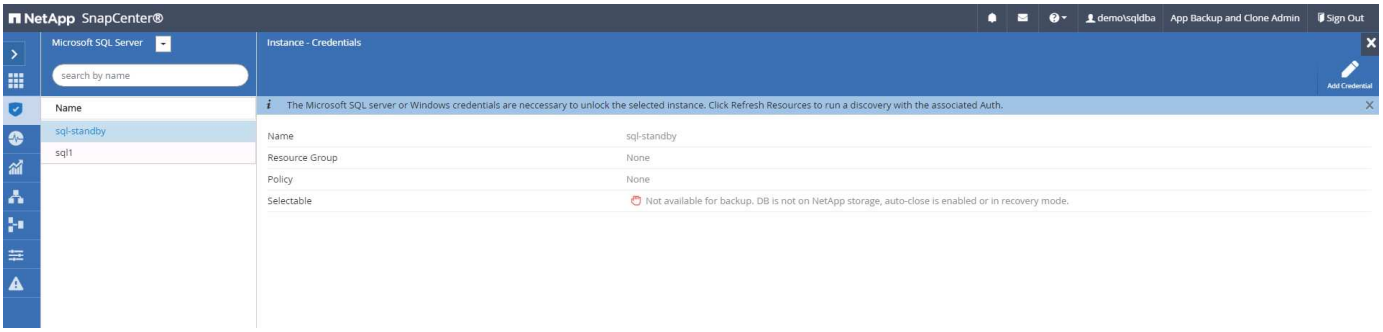


Wenn die Datenbank zum ersten Mal erkannt wird, wird der Gesamtstatus als „Nicht geschützt“ angezeigt. Der vorherige Screenshot zeigt eine Oracle-Datenbank, die noch nicht durch eine Sicherungsrichtlinie geschützt ist.

Wenn eine Sicherungskonfiguration oder -richtlinie eingerichtet ist und eine Sicherung ausgeführt wurde, zeigt der Gesamtstatus für die Datenbank den Sicherungsstatus als „Sicherung erfolgreich“ und den Zeitstempel der letzten Sicherung an. Der folgende Screenshot zeigt den Sicherungsstatus einer SQL Server-Benutzerdatenbank.

Wenn die Anmeldeinformationen für den Datenbankzugriff nicht richtig eingerichtet sind, zeigt eine rote Sperrschaltfläche an, dass auf die Datenbank nicht zugegriffen werden kann. Wenn beispielsweise Windows-Anmeldeinformationen keinen Systemadministratorzugriff auf eine Datenbankinstanz gewähren, müssen die Datenbankanmeldeinformationen neu konfiguriert werden, um das rote Schloss zu entsperren.





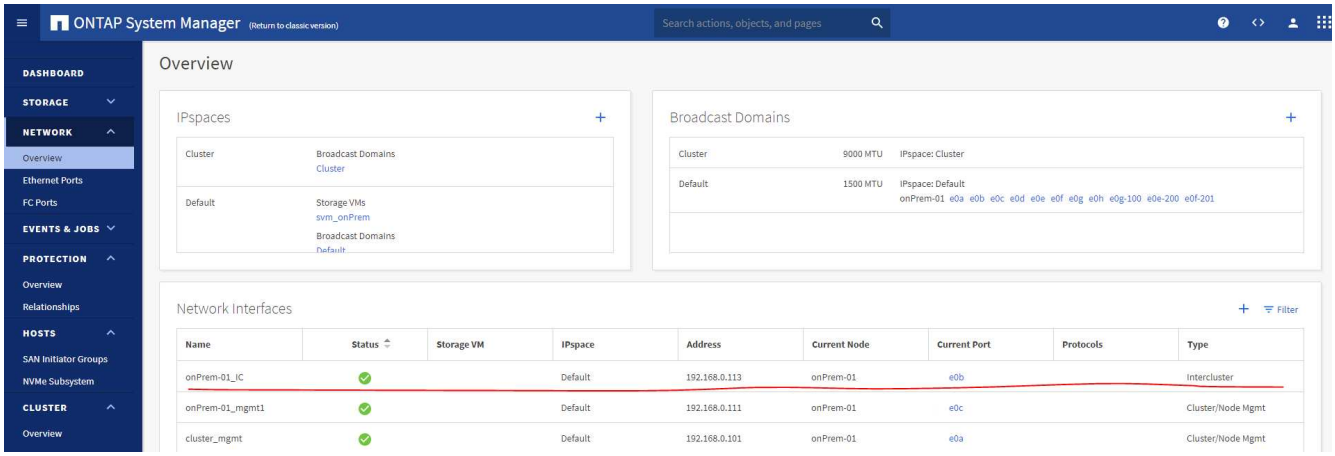
Nachdem die entsprechenden Anmeldeinformationen entweder auf Windows- oder Datenbankebene konfiguriert wurden, verschwindet das rote Schloss und die Informationen zum SQL Server-Typ werden erfasst und überprüft.

5. Einrichten von Storage-Cluster-Peering und DB-Volume-Replikation

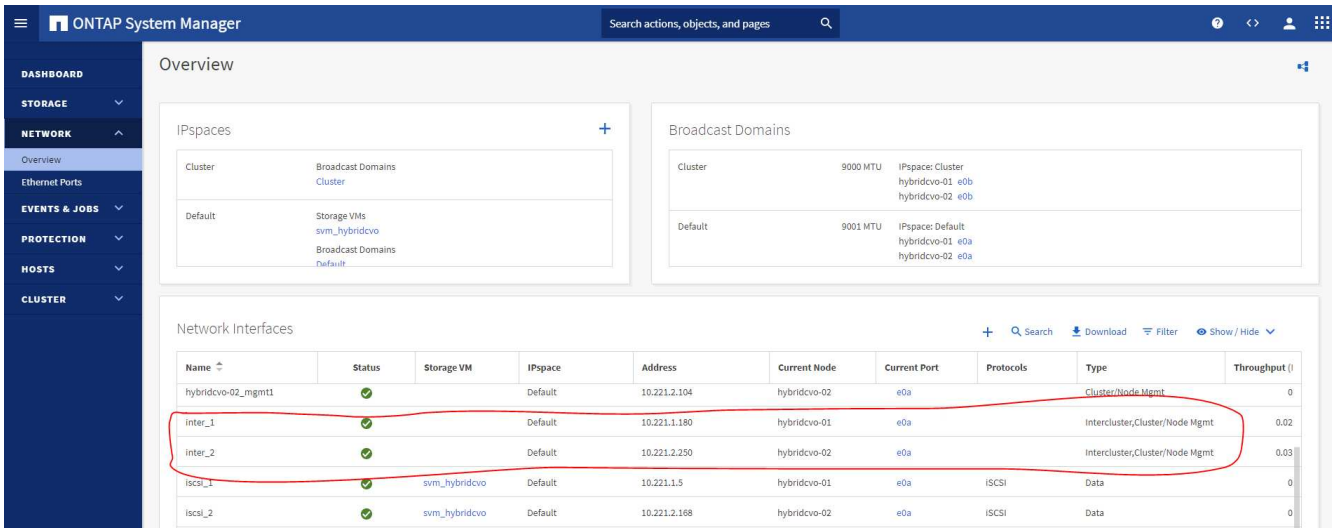
Um Ihre lokalen Datenbankdaten mit einer öffentlichen Cloud als Ziel zu schützen, werden lokale ONTAP Cluster-Datenbankvolumes mithilfe der NetApp SnapMirror -Technologie in das Cloud-CVO repliziert. Die replizierten Zielvolumes können dann für DEV/OPS oder Disaster Recovery geklont werden. Mit den folgenden allgemeinen Schritten können Sie Cluster-Peering und die Replikation von DB-Volumes einrichten.

1. Konfigurieren Sie Intercluster-LIFs für Cluster-Peering sowohl auf dem lokalen Cluster als auch auf der CVO-Clusterinstanz. Dieser Schritt kann mit ONTAP System Manager durchgeführt werden. Bei einer standardmäßigen CVO-Bereitstellung werden LIFs zwischen Clustern automatisch konfiguriert.

   Lokaler Cluster:



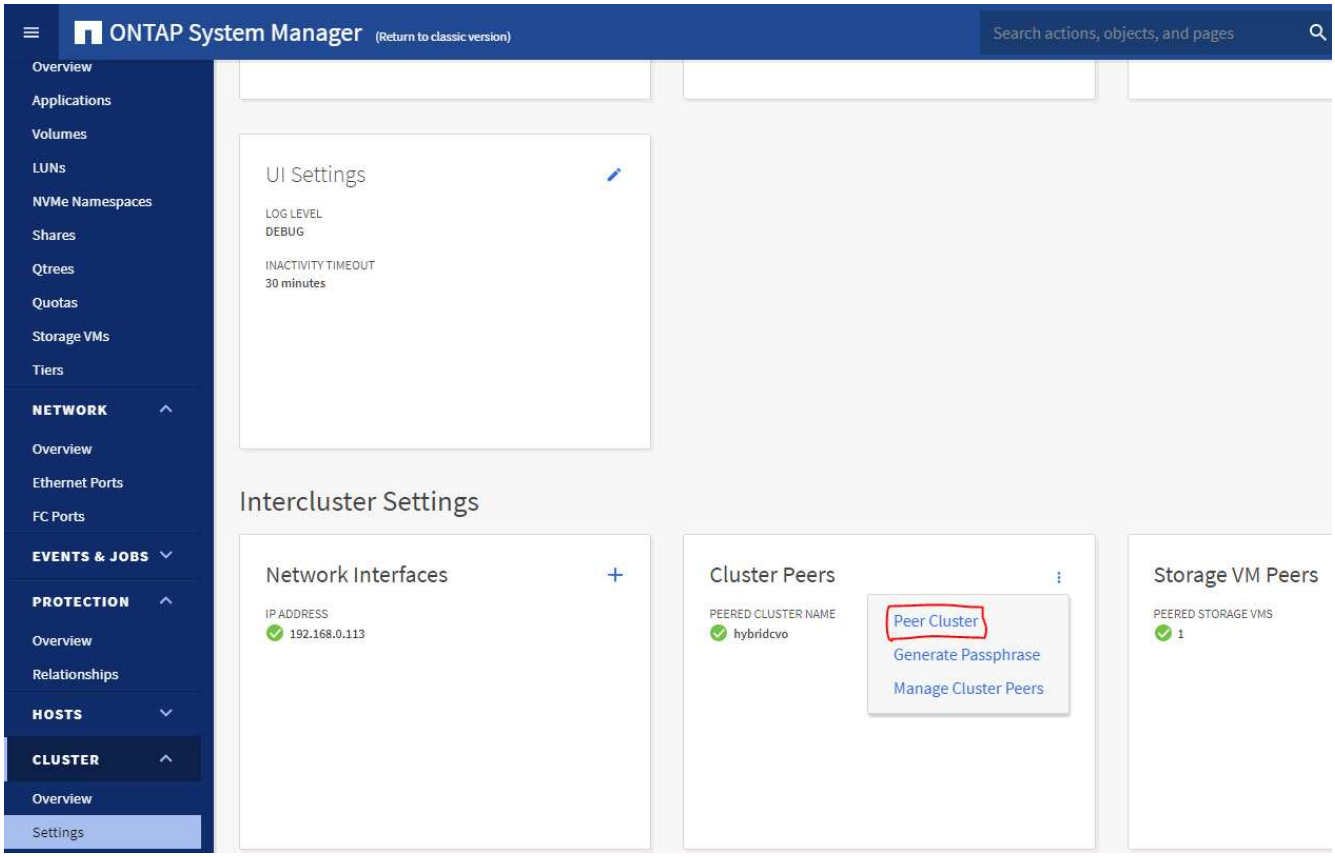
   Ziel-CVO-Cluster:



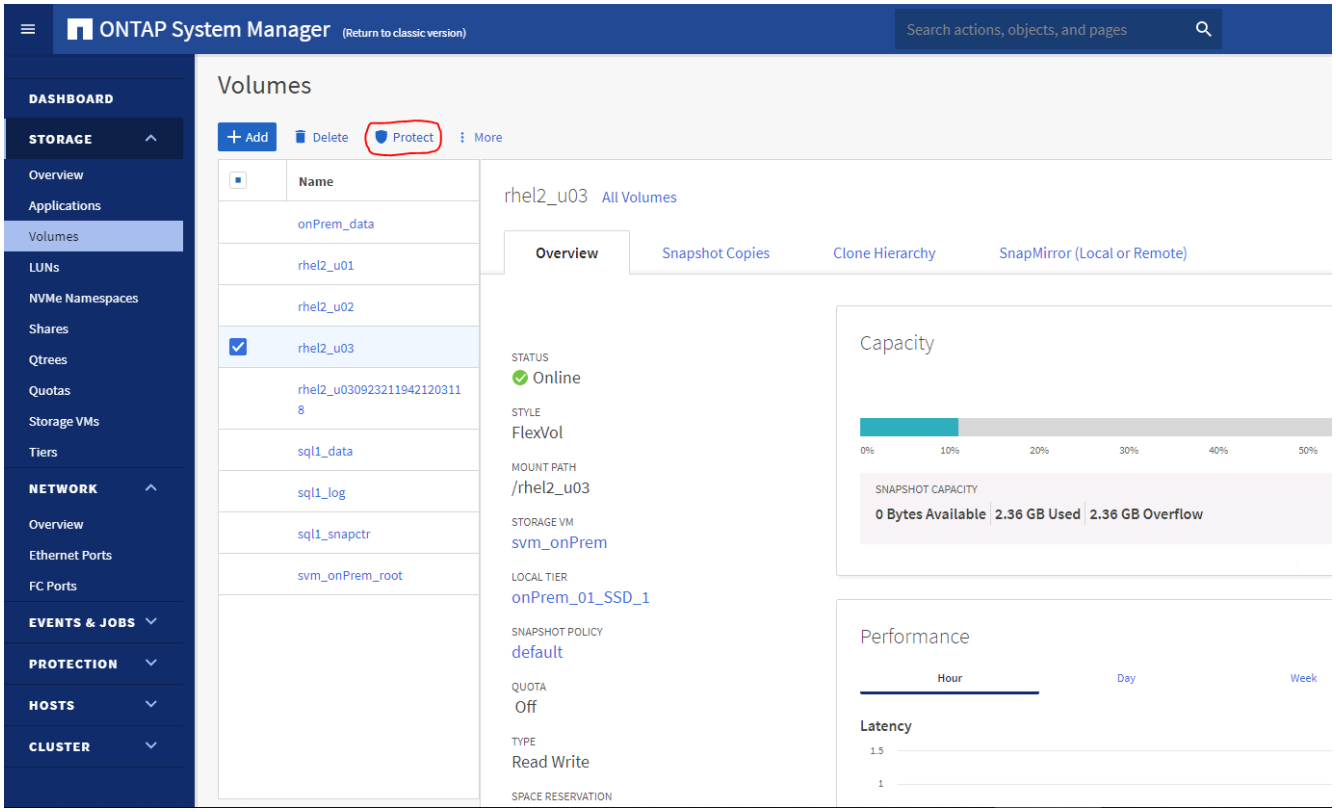
2. Wenn die Intercluster-LIFs konfiguriert sind, können Cluster-Peering und Volume-Replikation per Drag-and-Drop im NetApp Cloud Manager eingerichtet werden. Sehen"Erste Schritte – AWS Public Cloud" für Details.

   Alternativ können Cluster-Peering und DB-Volume-Replikation mithilfe von ONTAP System Manager wie folgt durchgeführt werden:

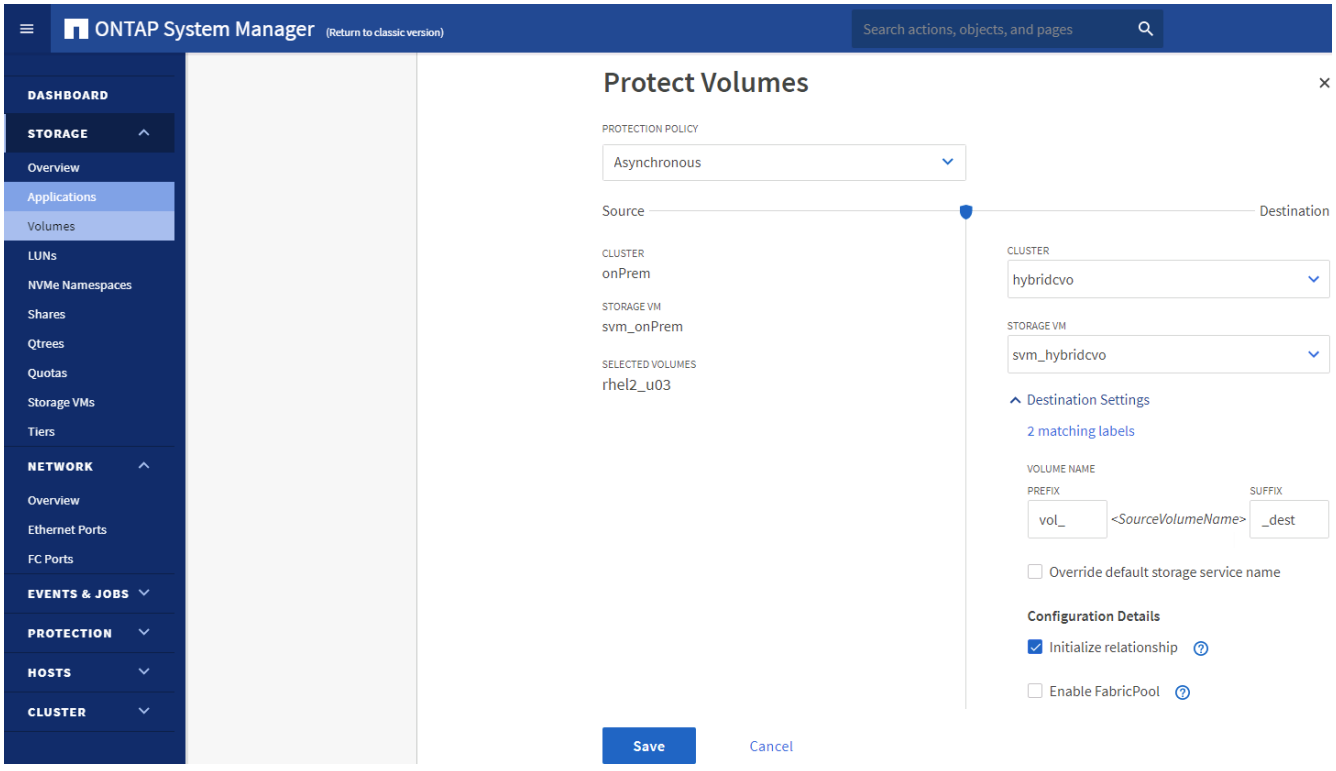
3. Melden Sie sich beim ONTAP System Manager an. Navigieren Sie zu Cluster > Einstellungen und klicken Sie auf Peer-Cluster, um das Cluster-Peering mit der CVO-Instanz in der Cloud einzurichten.



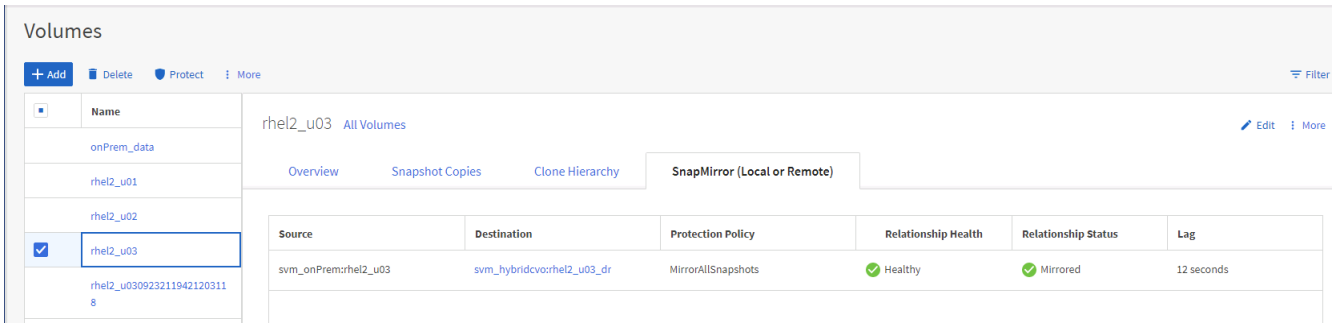
4. Gehen Sie zur Registerkarte „Volumes“. Wählen Sie das zu replizierende Datenbankvolume aus und klicken Sie auf „Schützen“.



5. Legen Sie die Schutzrichtlinie auf „Asynchron“ fest. Wählen Sie den Zielcluster und die Speicher-SVM aus.

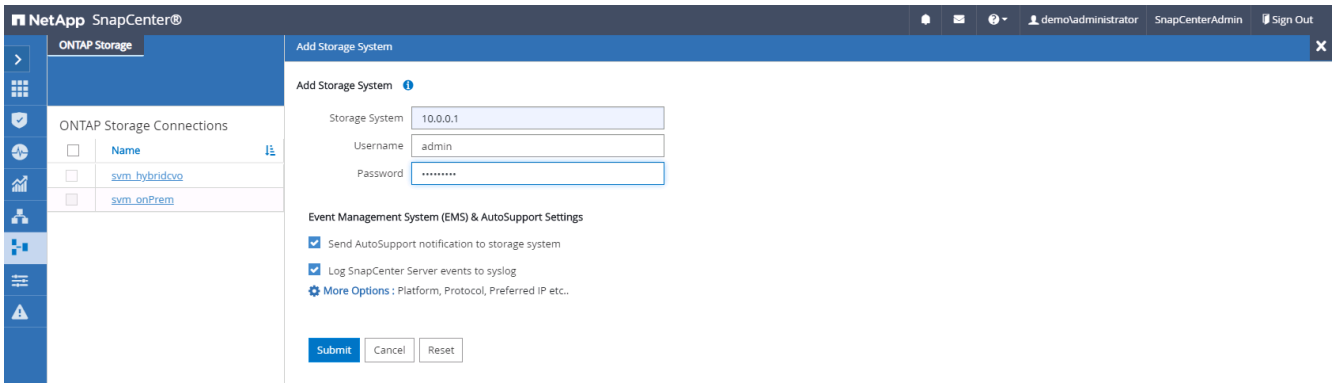


6. Überprüfen Sie, ob das Volume zwischen Quelle und Ziel synchronisiert ist und ob die Replikationsbeziehung fehlerfrei ist.

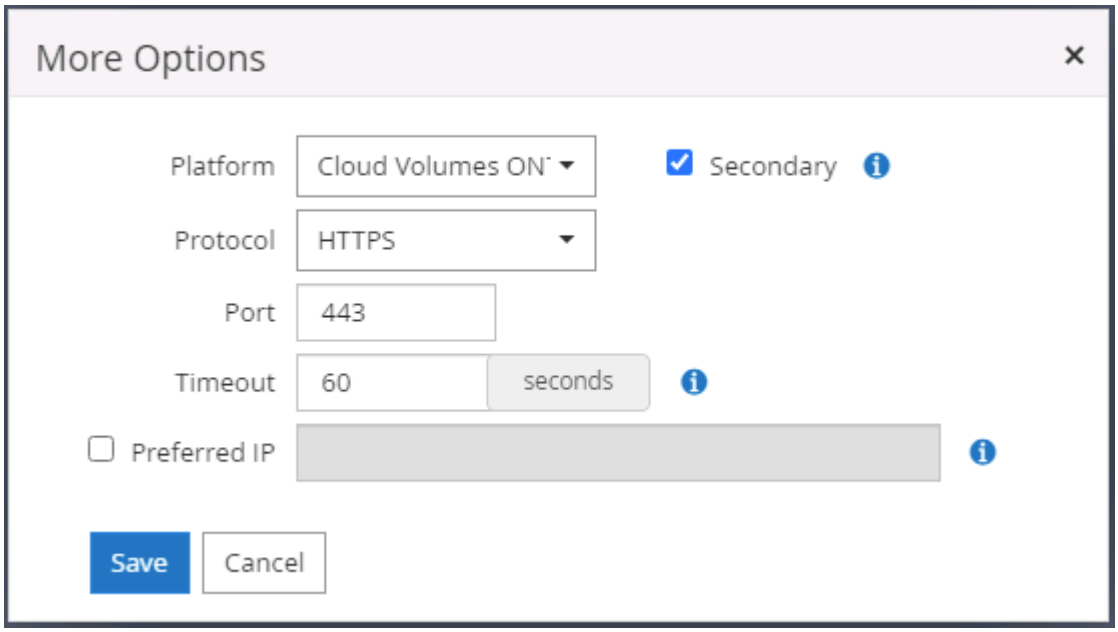


6. Fügen Sie SnapCenter CVO-Datenbankspeicher-SVM hinzu

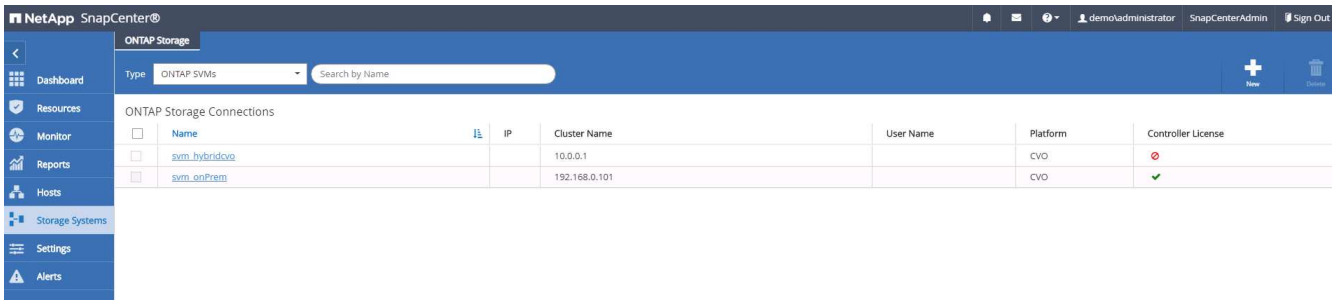
1. Melden Sie sich bei SnapCenter mit einer Benutzer-ID mit SnapCenterAdmin-Berechtigungen an.
2. Klicken Sie im Menü auf die Registerkarte „Speichersystem“ und dann auf „Neu“, um SnapCenter eine CVO-Speicher-SVM hinzuzufügen, die replizierte Zieldatenbank-Volumes hostet. Geben Sie die Cluster-Verwaltungs-IP in das Feld „Speichersystem“ ein und geben Sie den entsprechenden Benutzernamen und das entsprechende Kennwort ein.



3. Klicken Sie auf „Weitere Optionen“, um zusätzliche Speicherkonfigurationsoptionen zu öffnen. Wählen Sie im Feld „Plattform“ Cloud Volumes ONTAP aus, aktivieren Sie „Sekundär“ und klicken Sie dann auf „Speichern“.



4. Weisen Sie den Speichersystemen die Benutzer-IDs für die SnapCenter Datenbankverwaltung zu, wie in3. Installation des SnapCenter Host-Plugins .

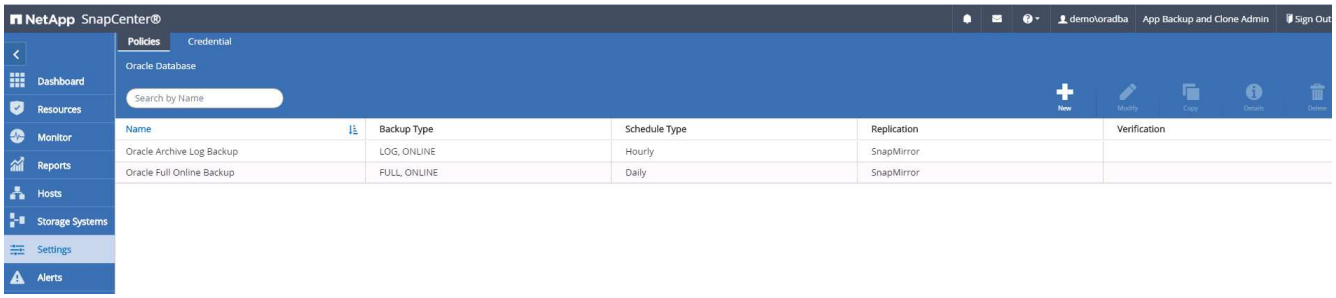


7. Richten Sie die Datenbanksicherungsrichtlinie in SnapCenter ein

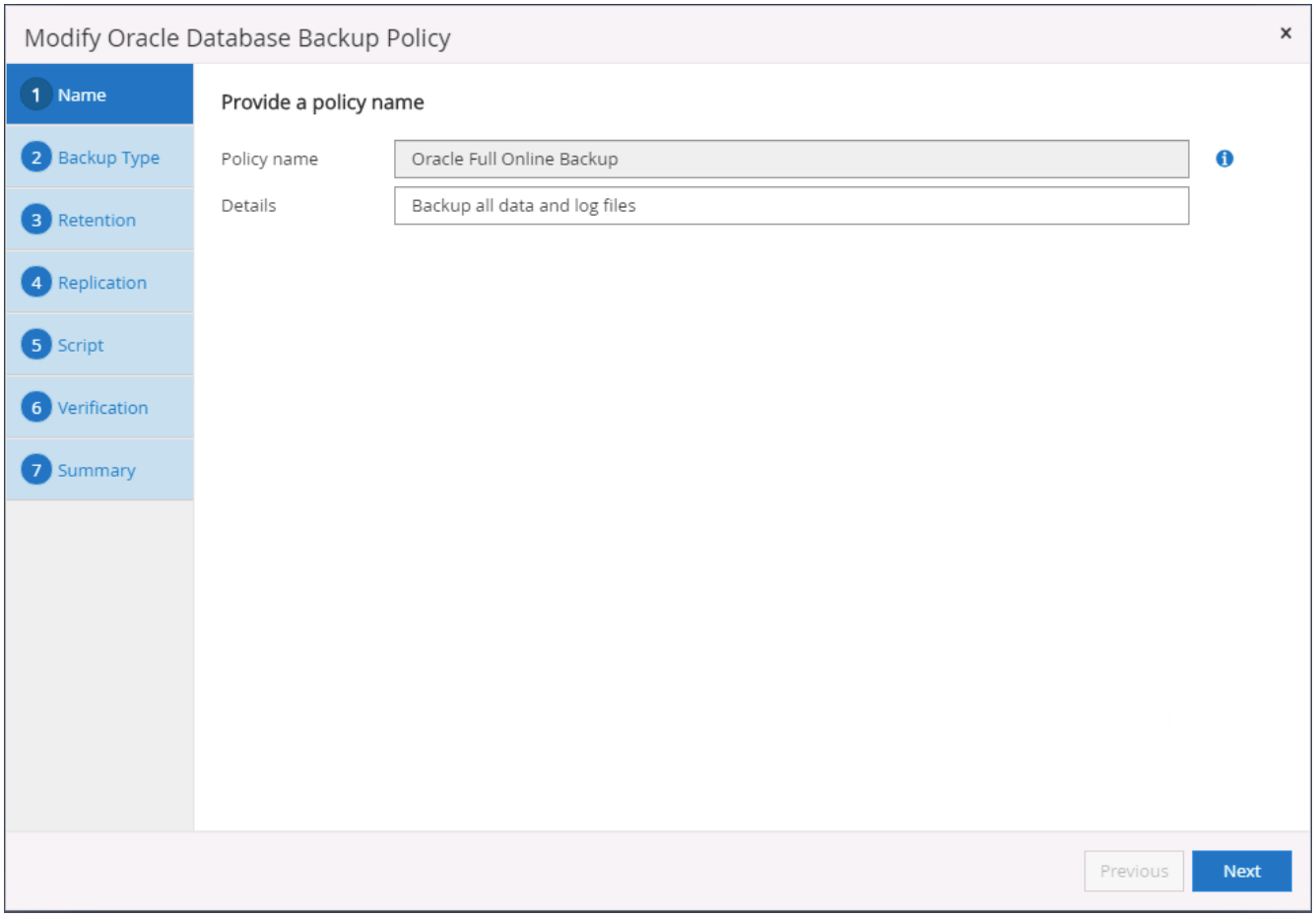
Die folgenden Verfahren veranschaulichen, wie Sie eine vollständige Sicherungsrichtlinie für Datenbanken oder Protokolldateien erstellen. Die Richtlinie kann dann zum Schutz der Datenbankressourcen implementiert werden. Das Recovery Point Objective (RPO) oder Recovery Time Objective (RTO) bestimmt die Häufigkeit von Datenbank- und/oder Protokollsicherungen.

Erstellen einer vollständigen Datenbanksicherungsrichtlinie für Oracle

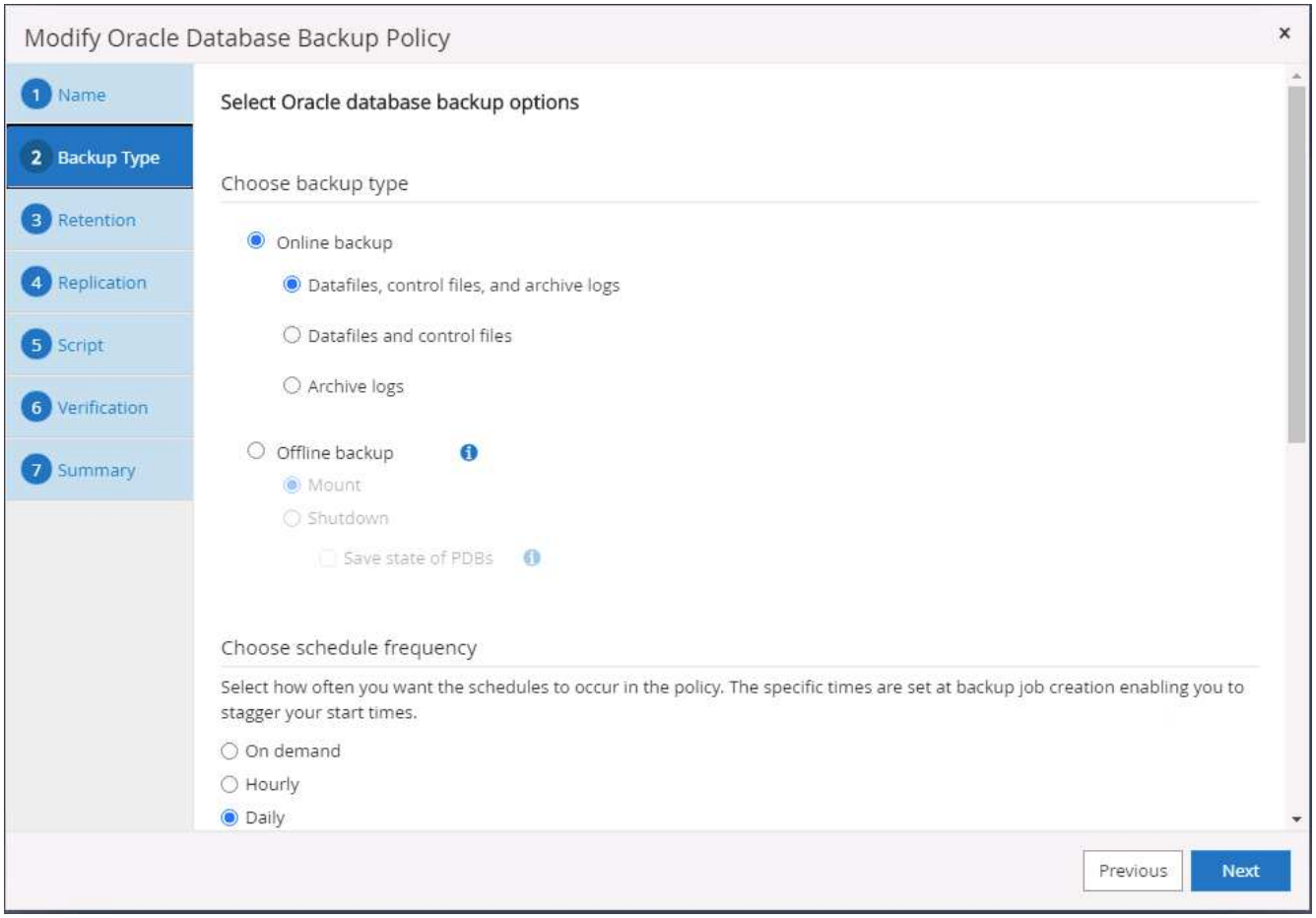
1. Melden Sie sich bei SnapCenter mit einer Benutzer-ID für die Datenbankverwaltung an, klicken Sie auf „Einstellungen“ und dann auf „Richtlinien“.



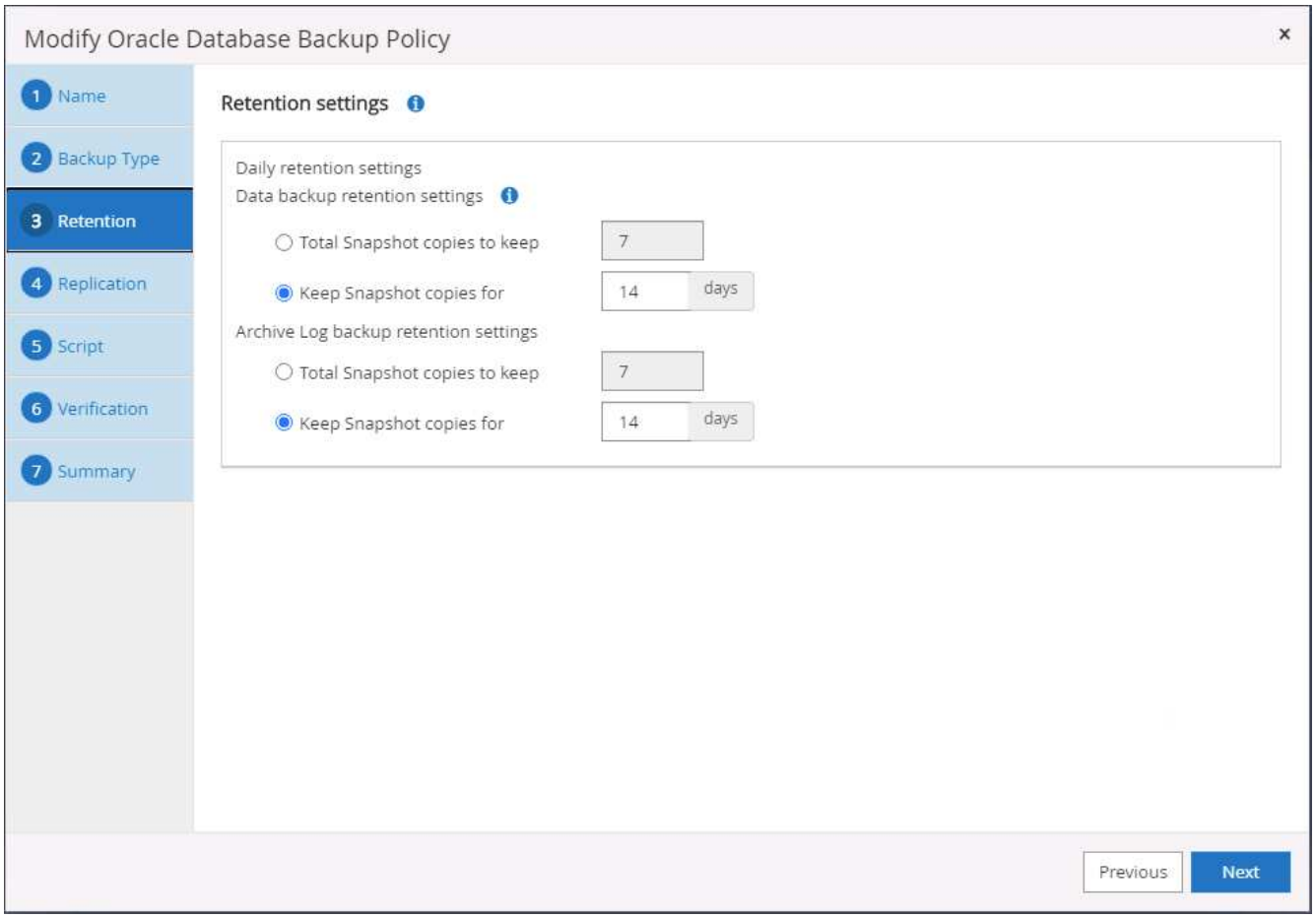
2. Klicken Sie auf „Neu“, um einen neuen Workflow zur Erstellung einer Sicherungsrichtlinie zu starten, oder wählen Sie eine vorhandene Richtlinie zur Änderung aus.



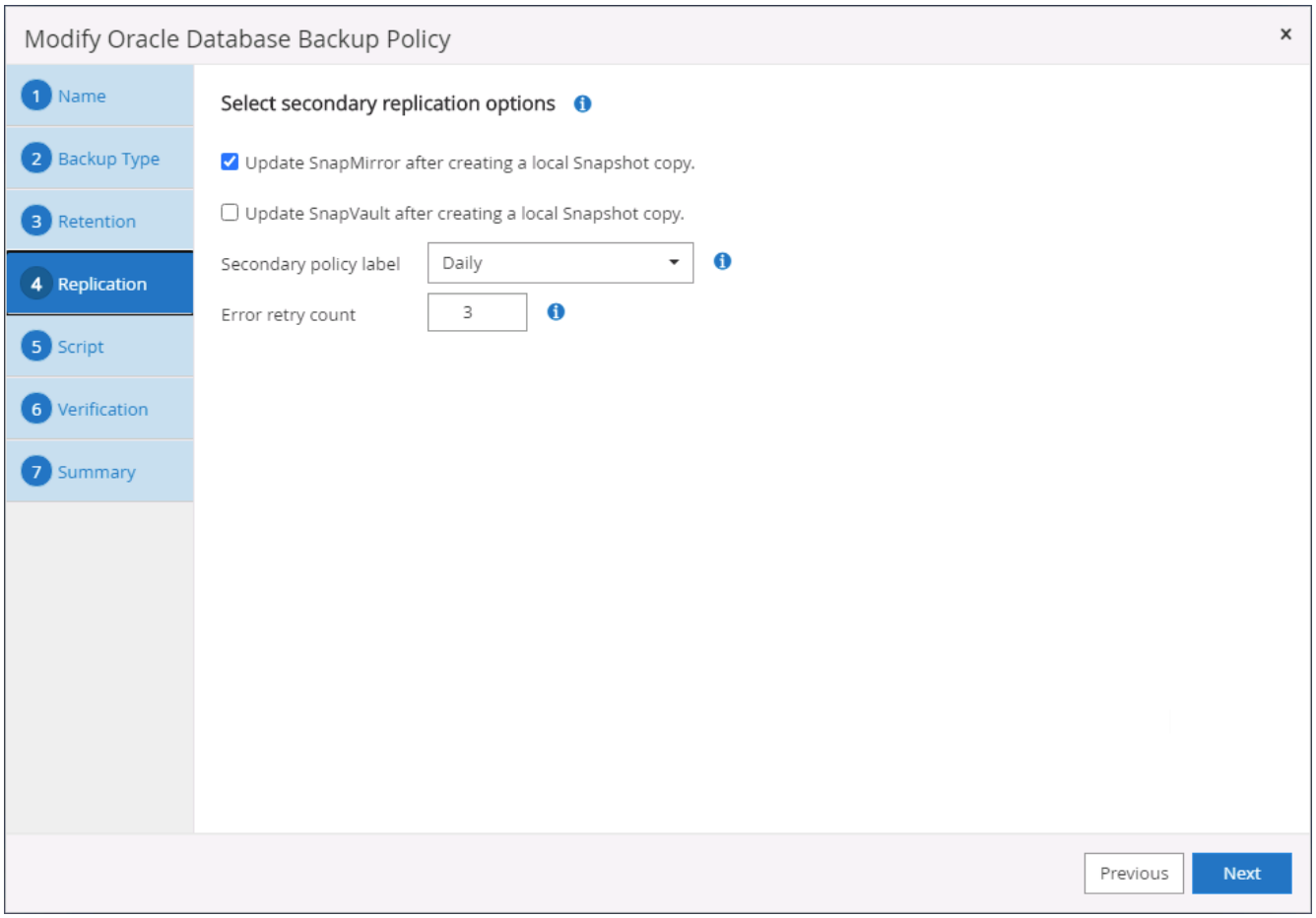
3. Wählen Sie den Sicherungstyp und die geplante Häufigkeit aus.



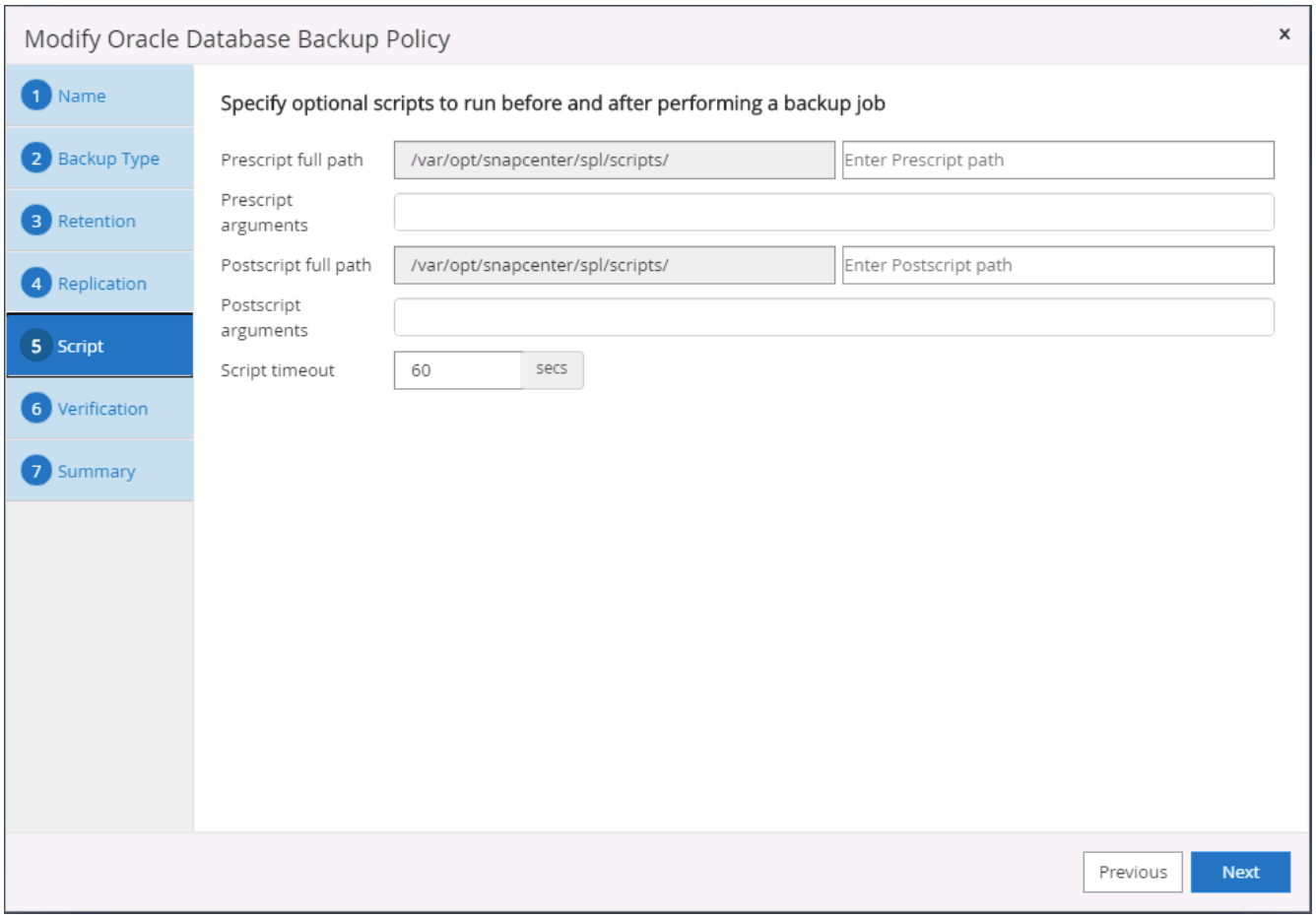
4. Legen Sie die Einstellung für die Sicherungsaufbewahrung fest. Dadurch wird festgelegt, wie viele vollständige Datenbanksicherungskopien aufbewahrt werden sollen.



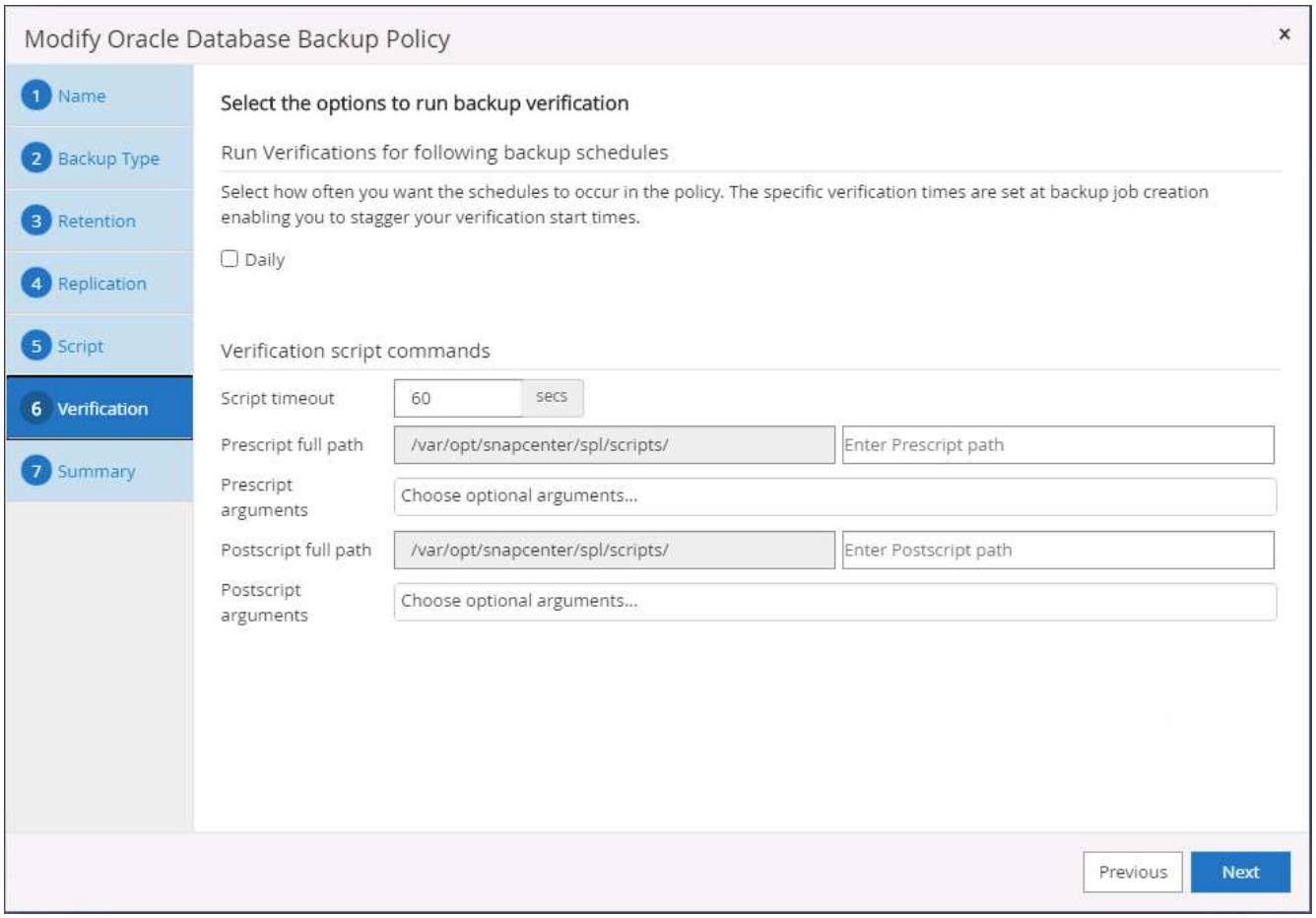
5. Wählen Sie die sekundären Replikationsoptionen aus, um lokale primäre Snapshot-Sicherungen an einen sekundären Speicherort in der Cloud zu replizieren.



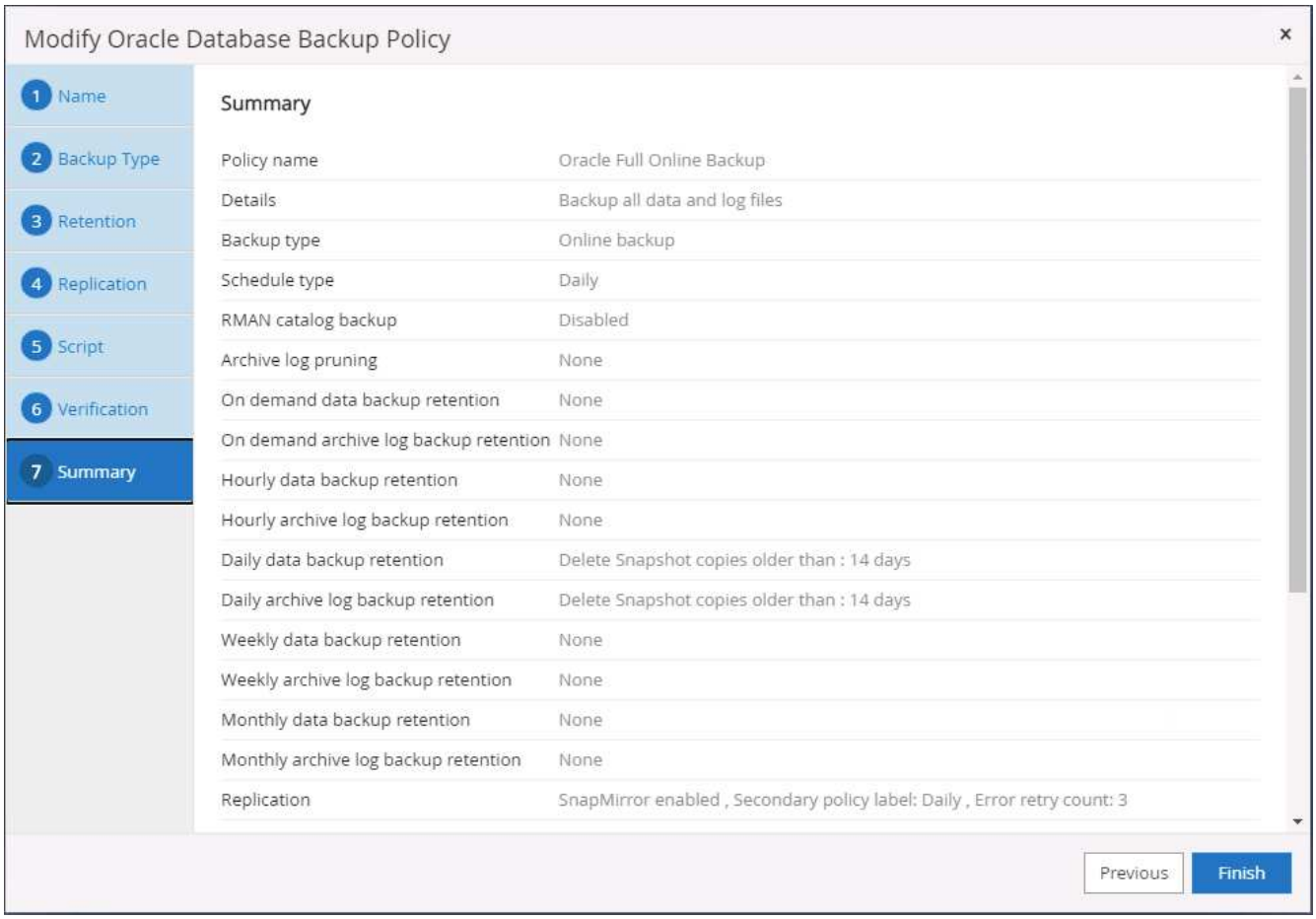
6. Geben Sie optionale Skripts an, die vor und nach einem Sicherungslauf ausgeführt werden sollen.



7. Führen Sie bei Bedarf eine Sicherungsüberprüfung durch.

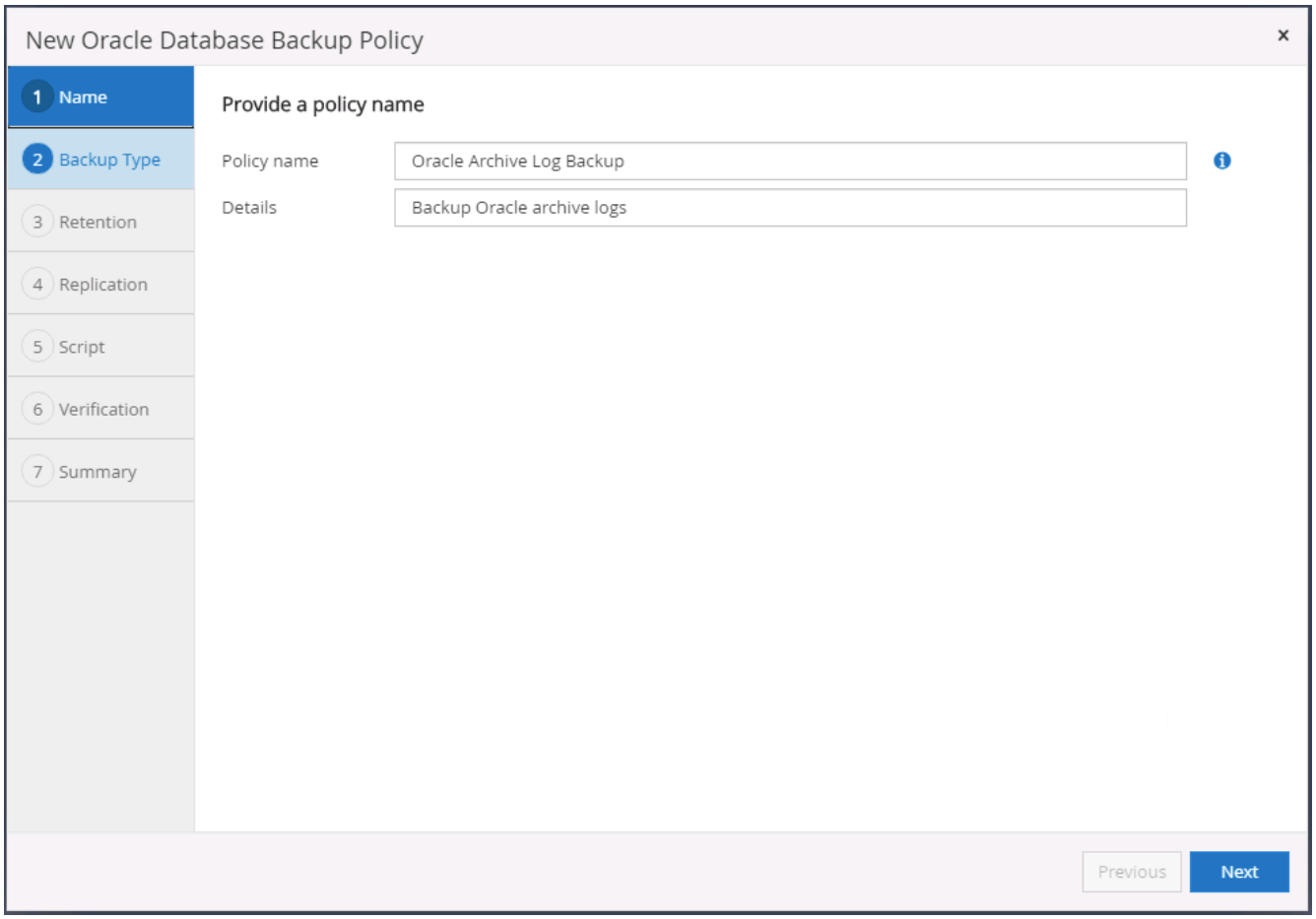


8. Zusammenfassung.

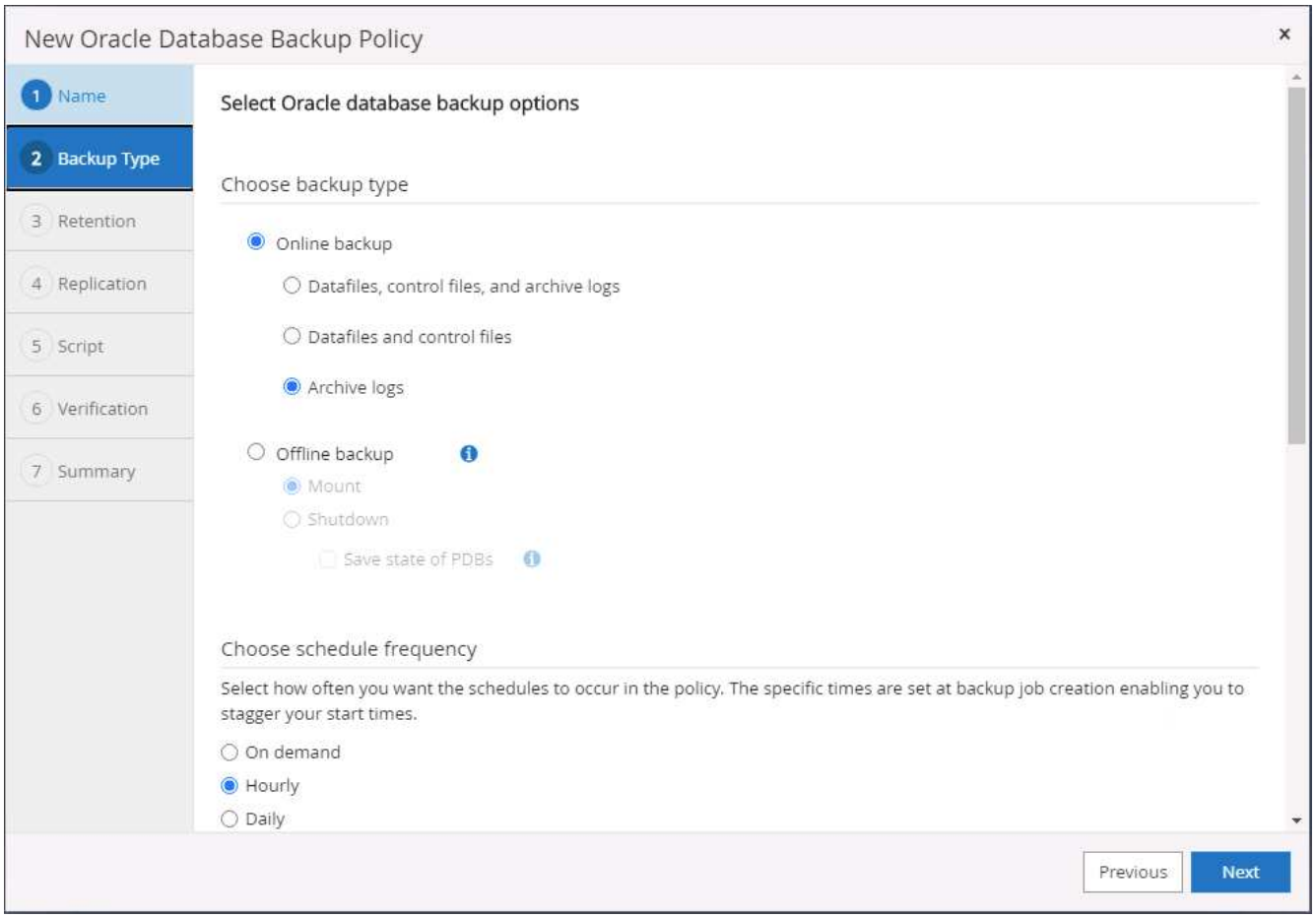


Erstellen einer Richtlinie zur Datenbankprotokollsicherung für Oracle

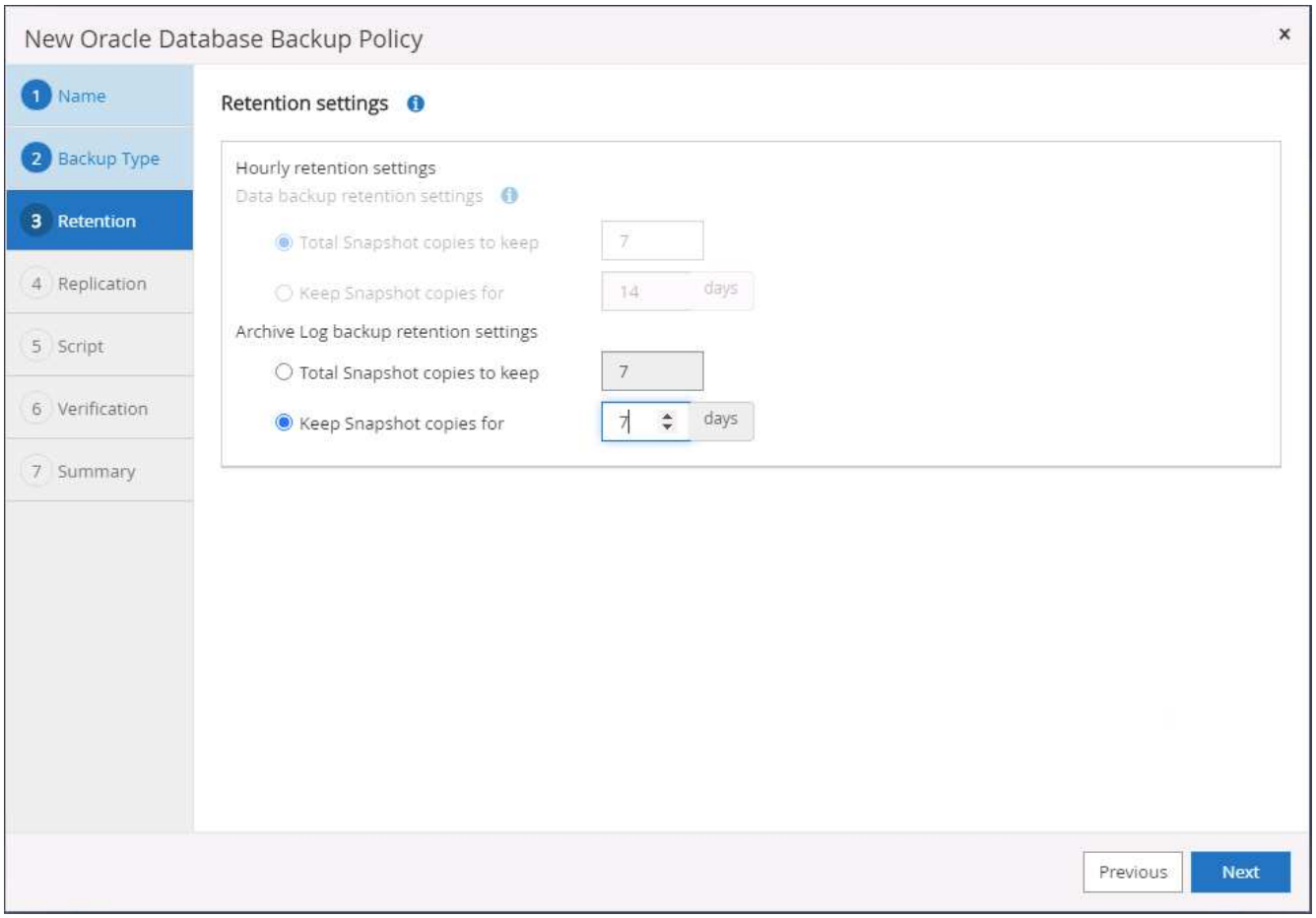
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an, klicken Sie auf „Einstellungen“ und dann auf „Richtlinien“.
2. Klicken Sie auf „Neu“, um einen neuen Workflow zum Erstellen einer Sicherungsrichtlinie zu starten, oder wählen Sie eine vorhandene Richtlinie zur Änderung aus.



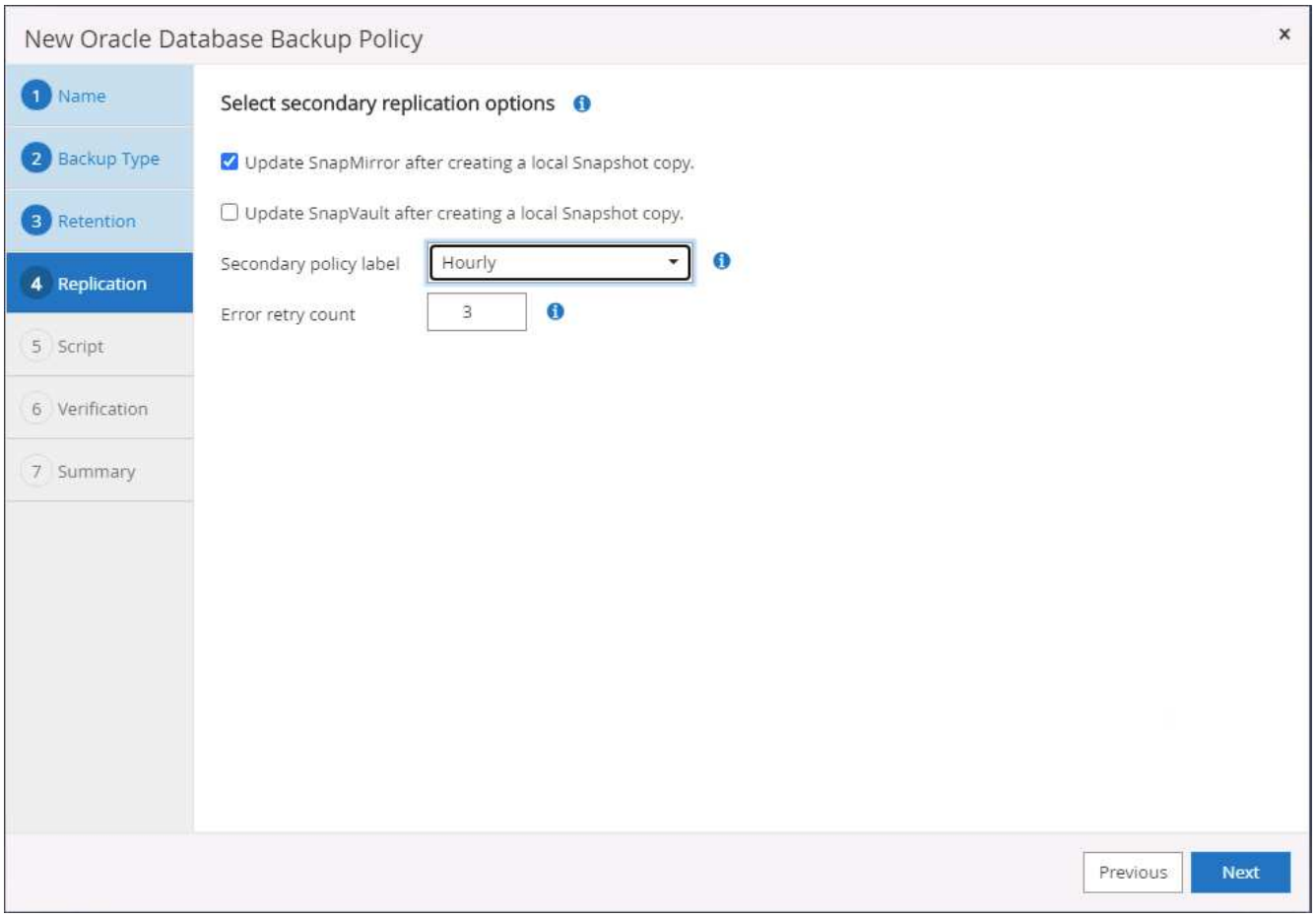
3. Wählen Sie den Sicherungstyp und die geplante Häufigkeit aus.



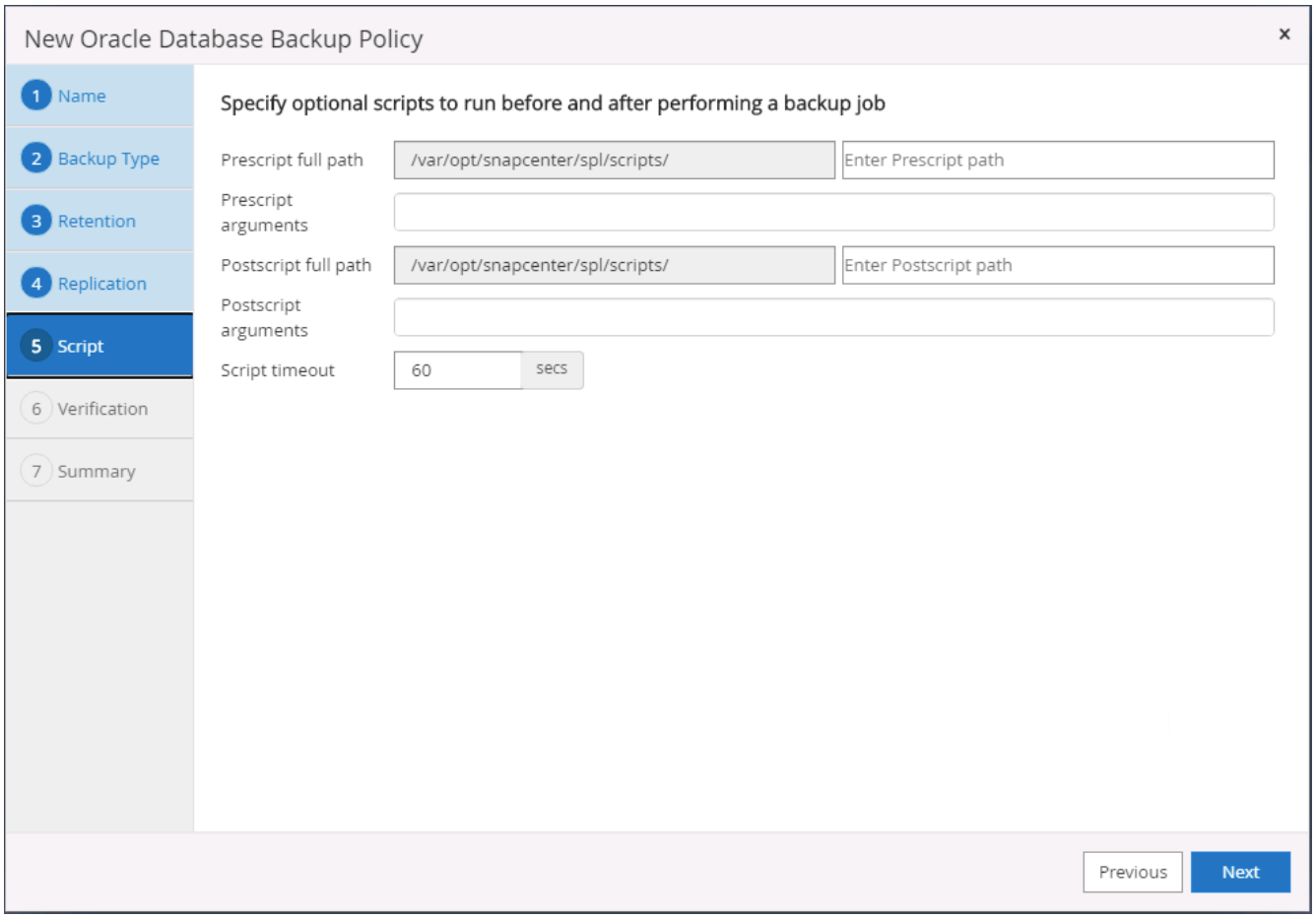
4. Legen Sie den Aufbewahrungszeitraum für das Protokoll fest.



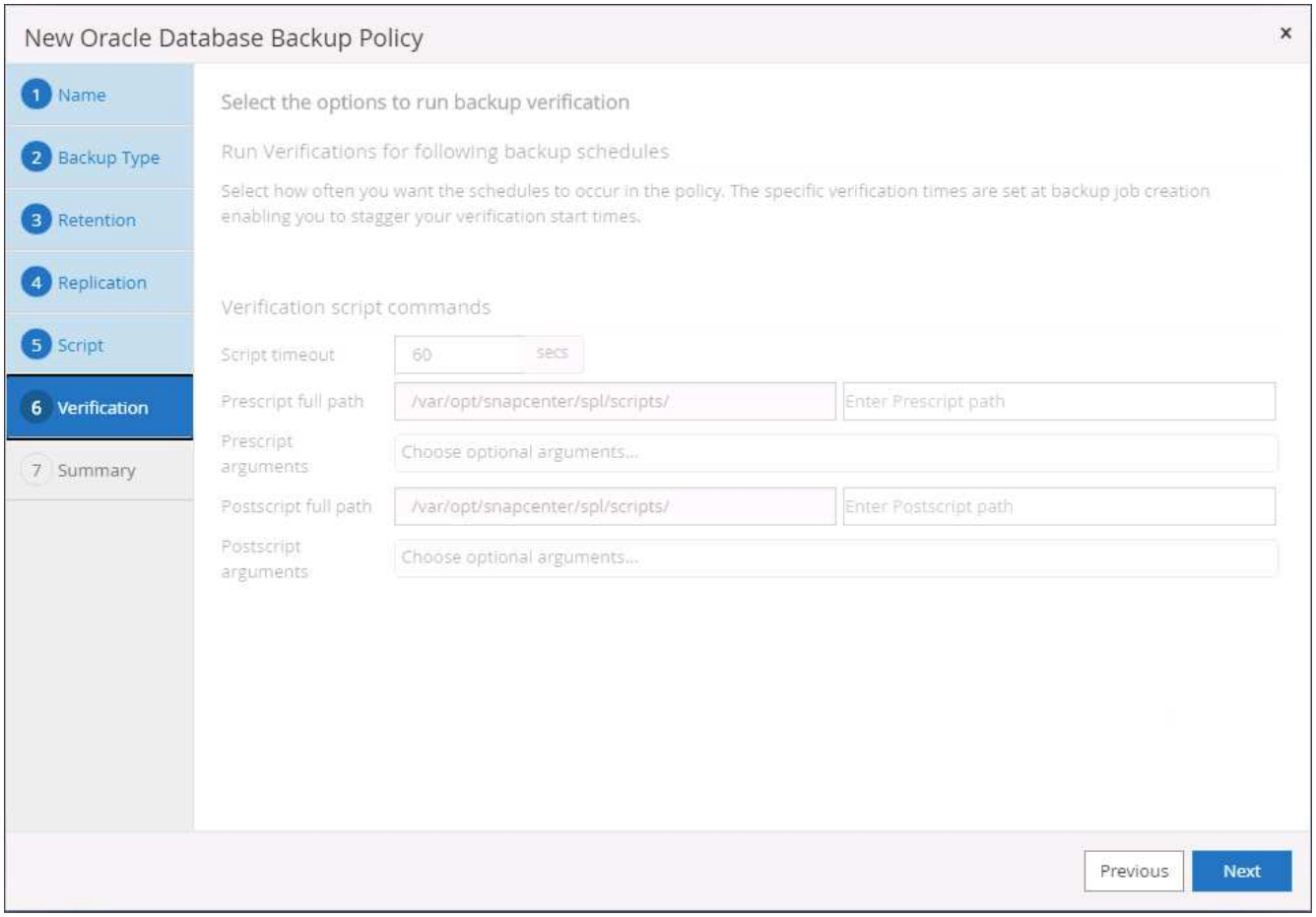
5. Aktivieren Sie die Replikation an einem sekundären Standort in der öffentlichen Cloud.



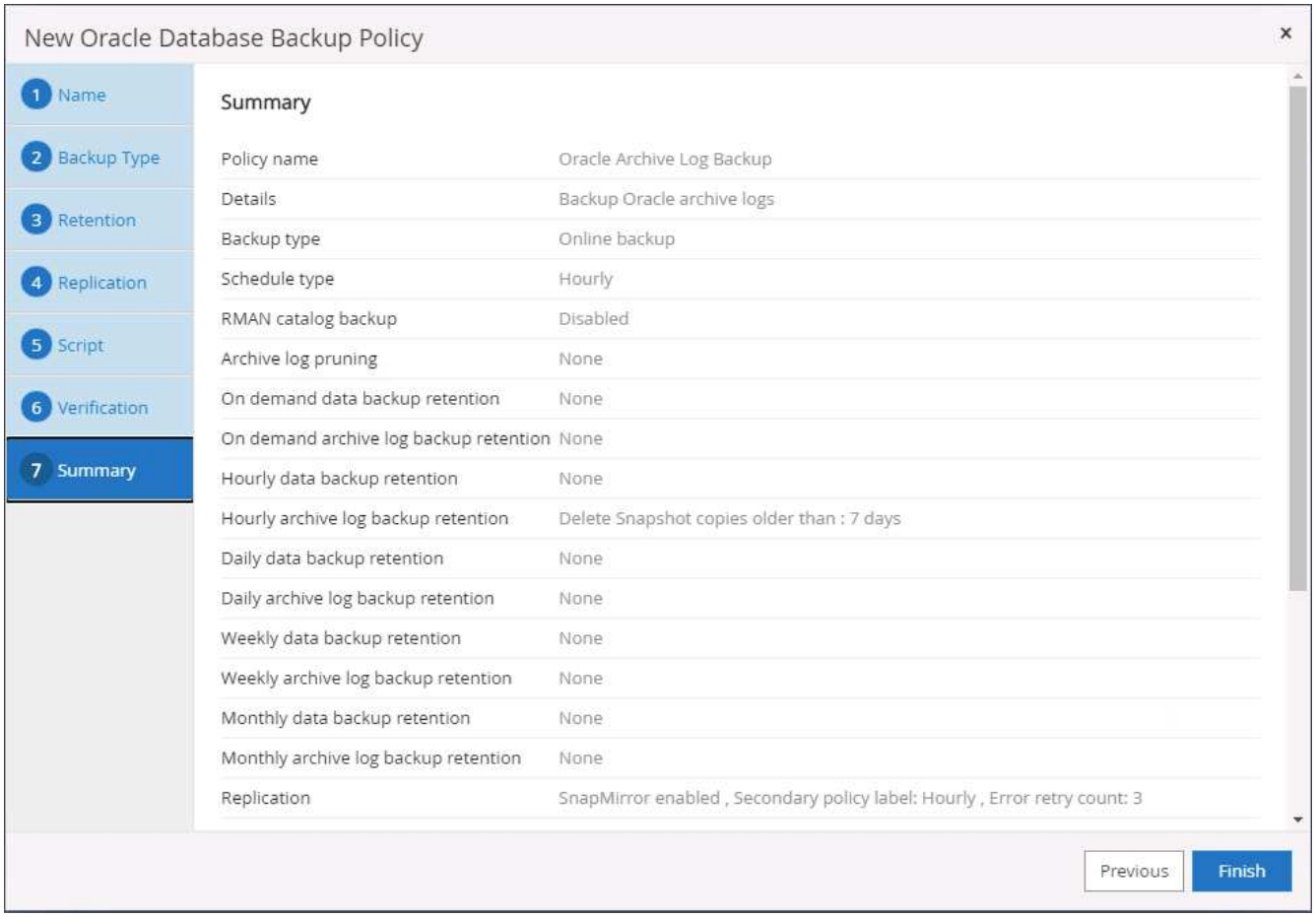
6. Geben Sie optionale Skripts an, die vor und nach der Protokollsicherung ausgeführt werden sollen.



7. Geben Sie alle Sicherungsüberprüfungsskripte an.

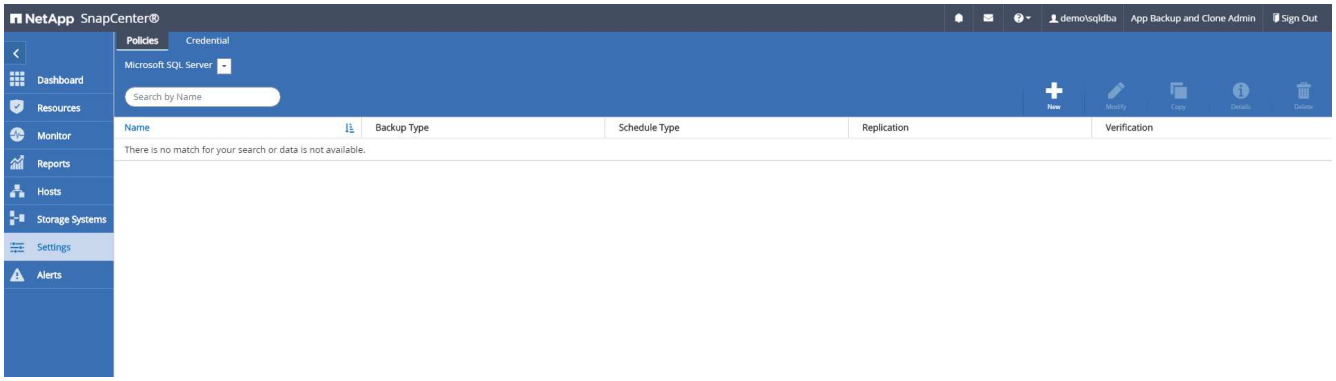


8. Zusammenfassung.

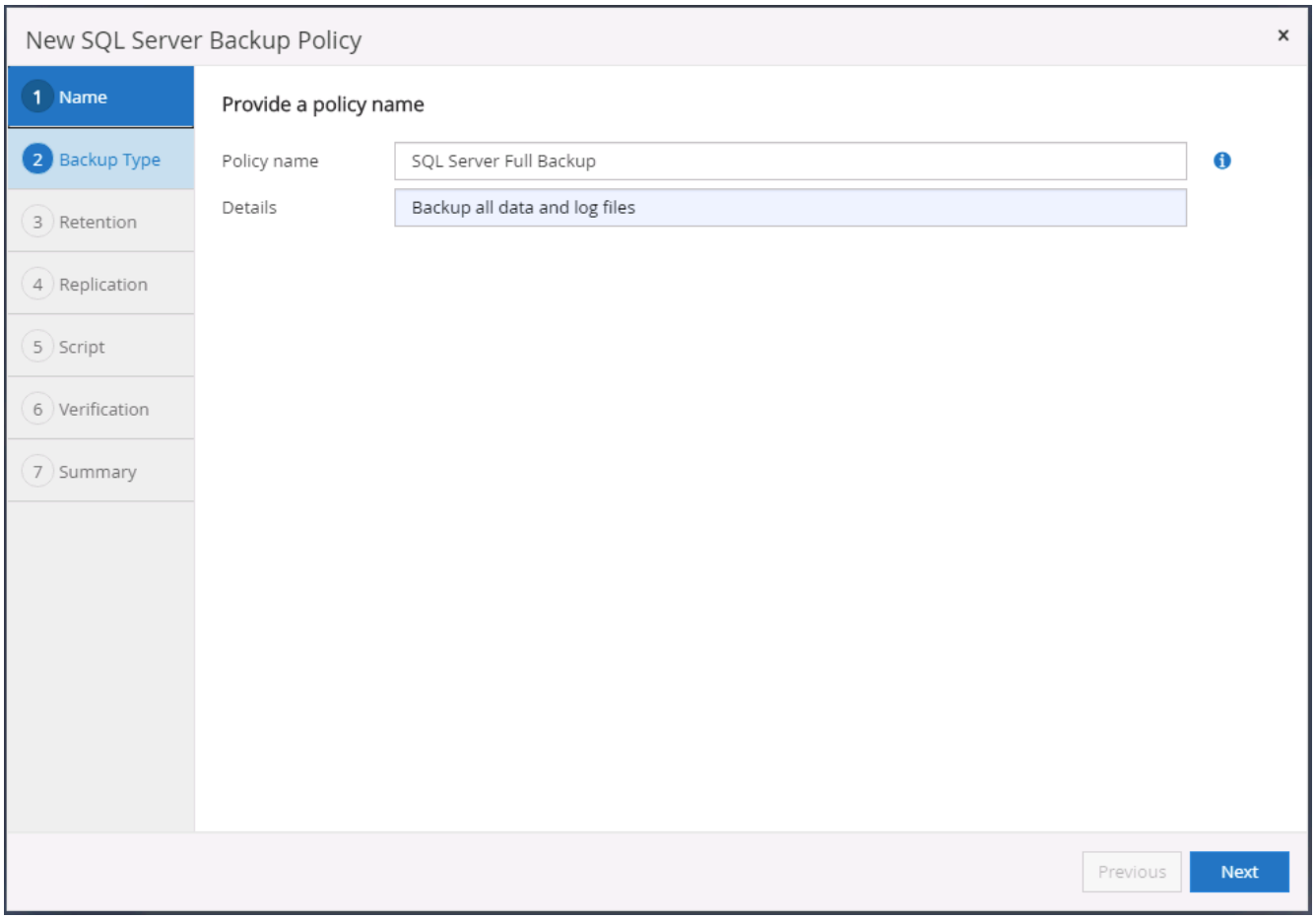


Erstellen einer vollständigen Datenbanksicherungsrichtlinie für SQL

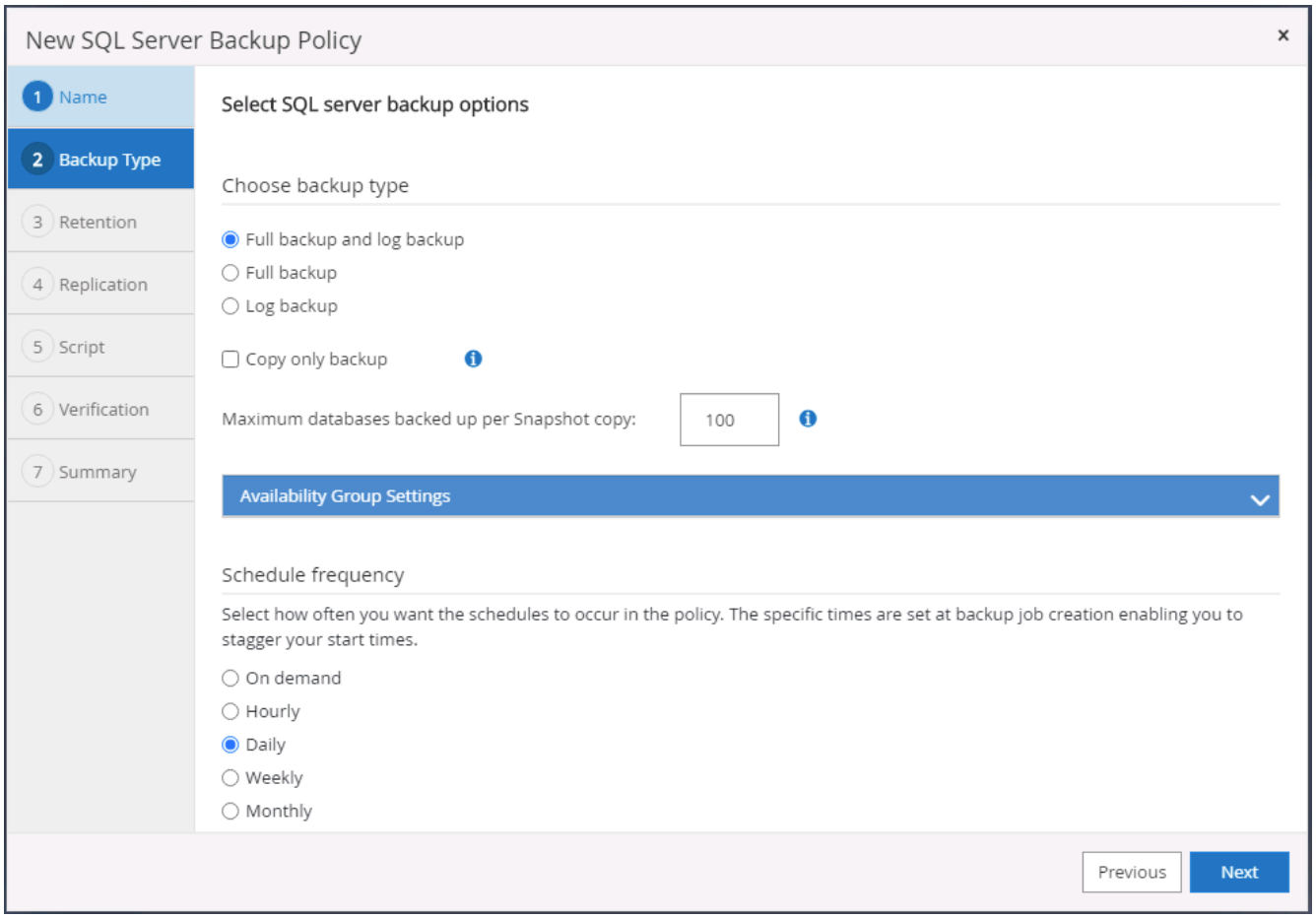
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an, klicken Sie auf „Einstellungen“ und dann auf „Richtlinien“.



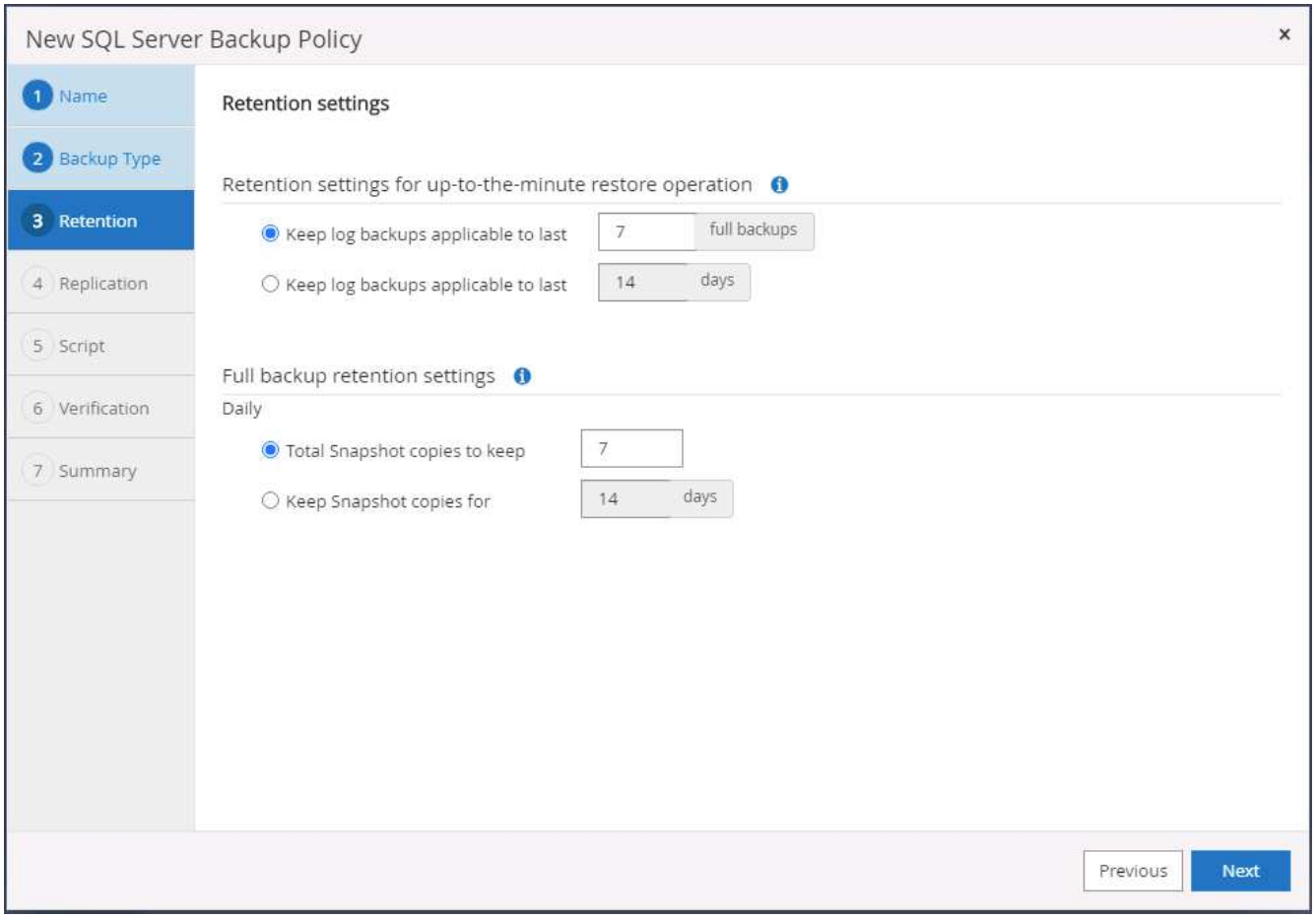
2. Klicken Sie auf „Neu“, um einen neuen Workflow zum Erstellen einer Sicherungsrichtlinie zu starten, oder wählen Sie eine vorhandene Richtlinie zur Änderung aus.



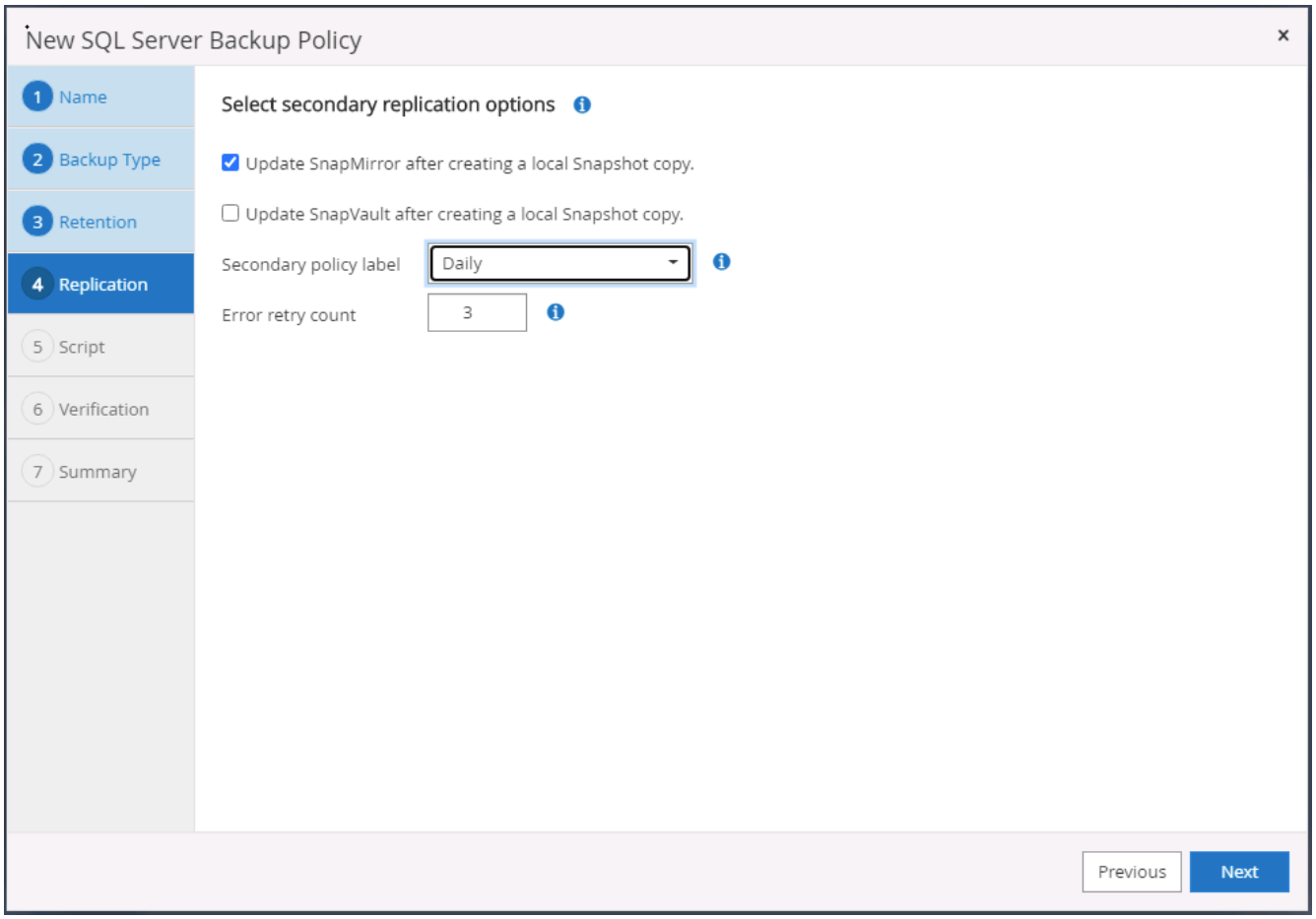
3. Definieren Sie die Sicherungsoption und die geplante Häufigkeit. Für SQL Server, der mit einer Verfügbarkeitsgruppe konfiguriert ist, kann ein bevorzugtes Sicherungsreplikat festgelegt werden.



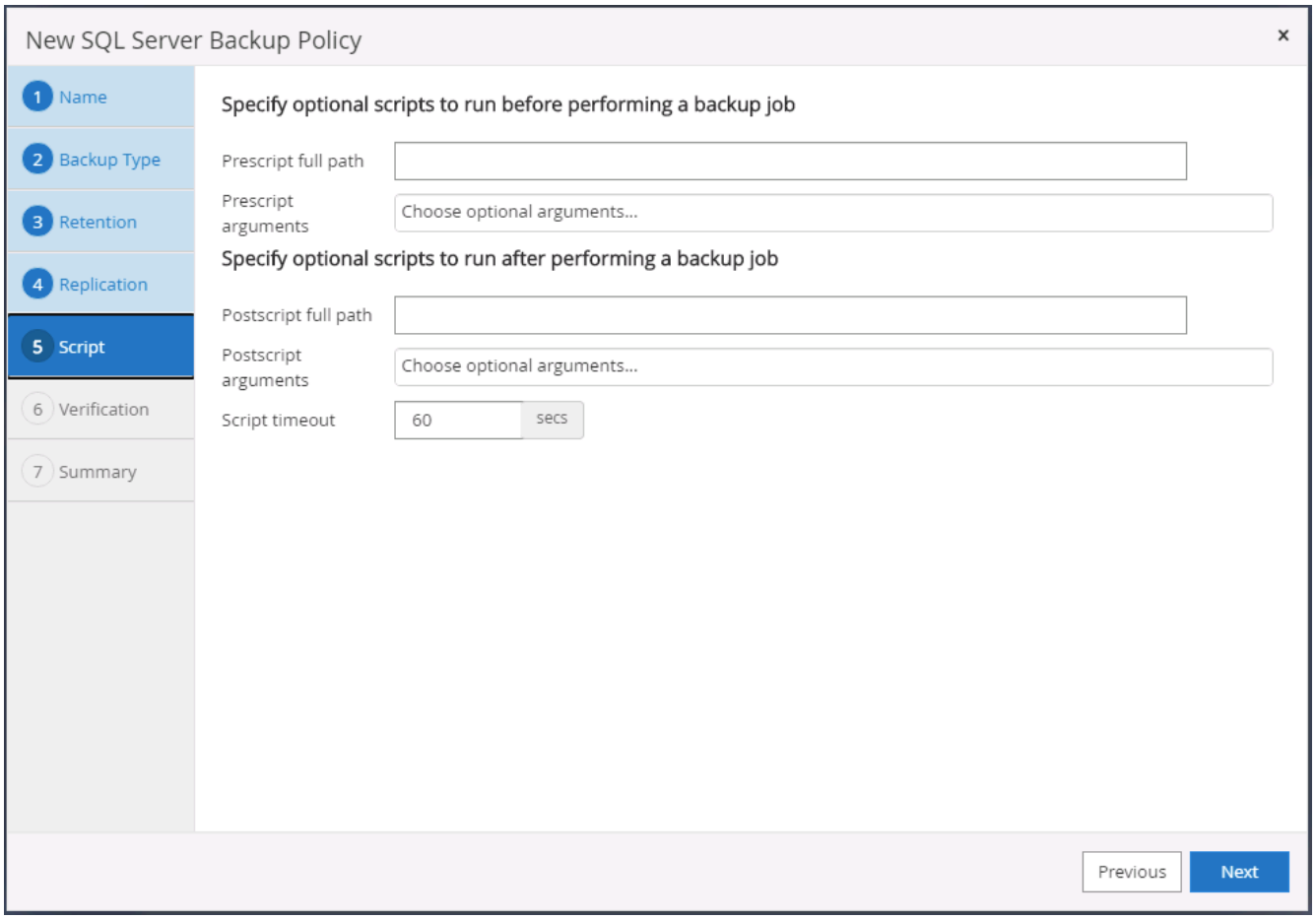
4. Legen Sie den Aufbewahrungszeitraum für die Sicherung fest.



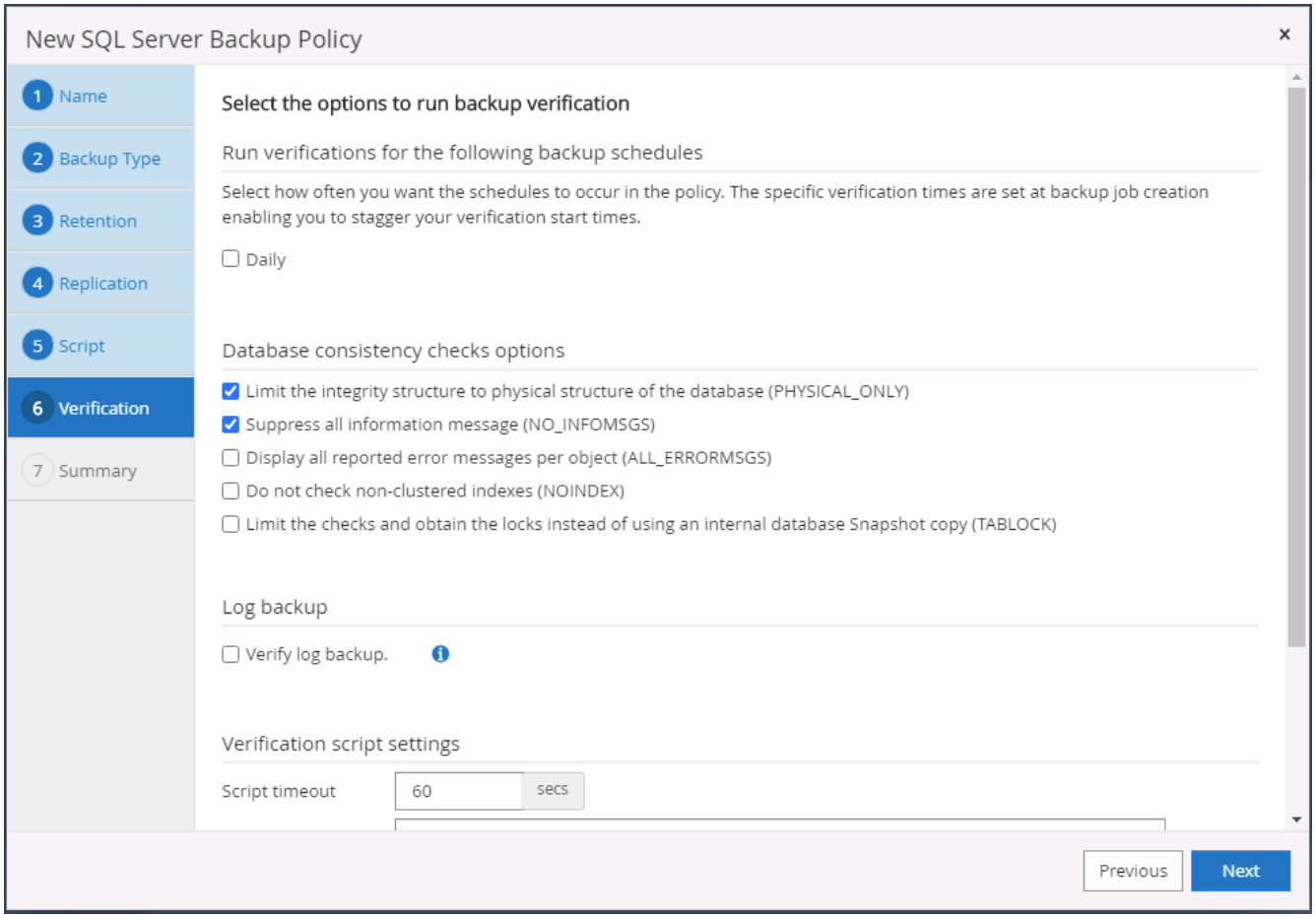
5. Aktivieren Sie die Replikation von Sicherungskopien an einem sekundären Speicherort in der Cloud.



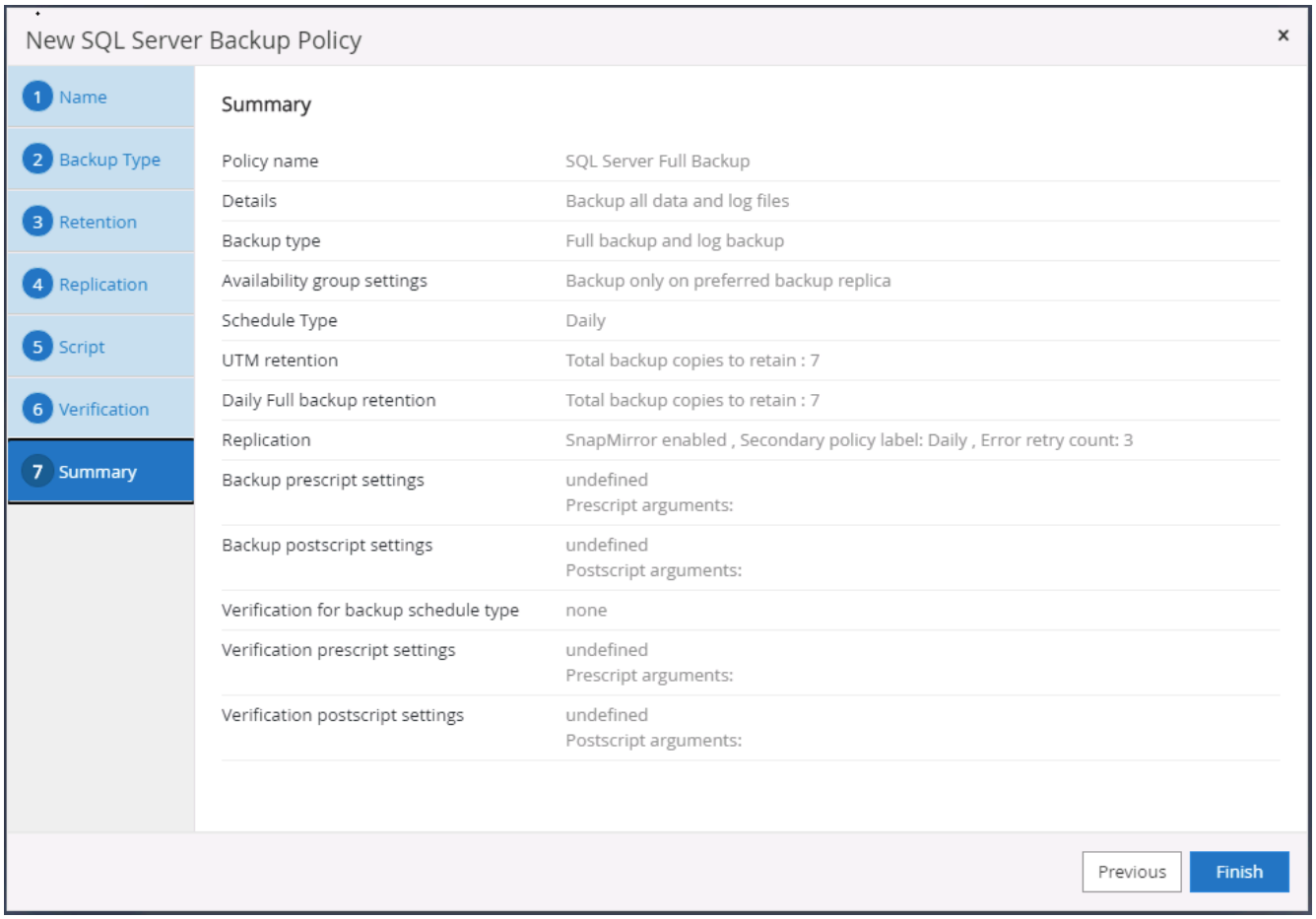
6. Geben Sie optionale Skripts an, die vor oder nach einem Sicherungsauftrag ausgeführt werden sollen.



7. Geben Sie die Optionen zum Ausführen der Sicherungsüberprüfung an.

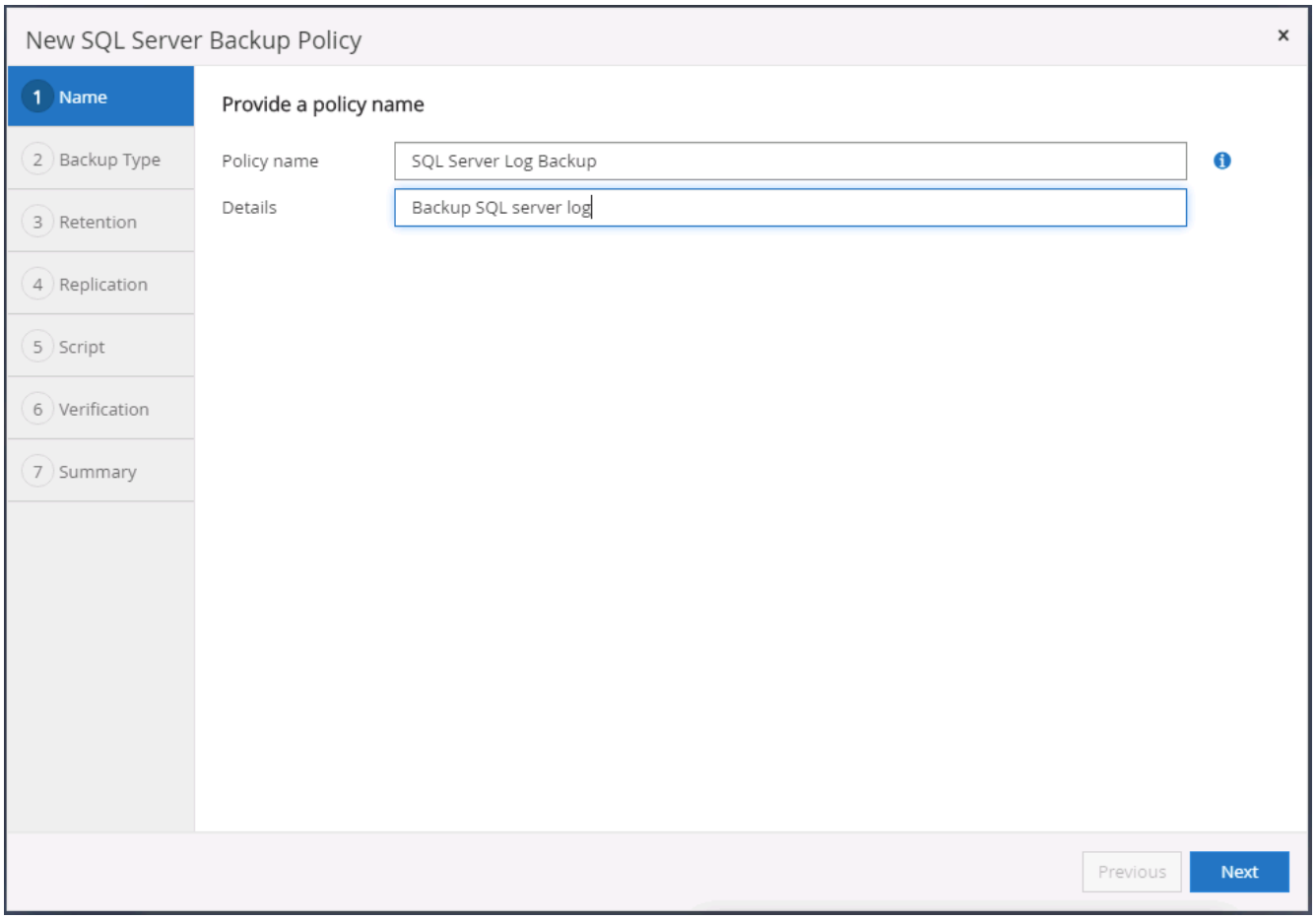


8. Zusammenfassung.

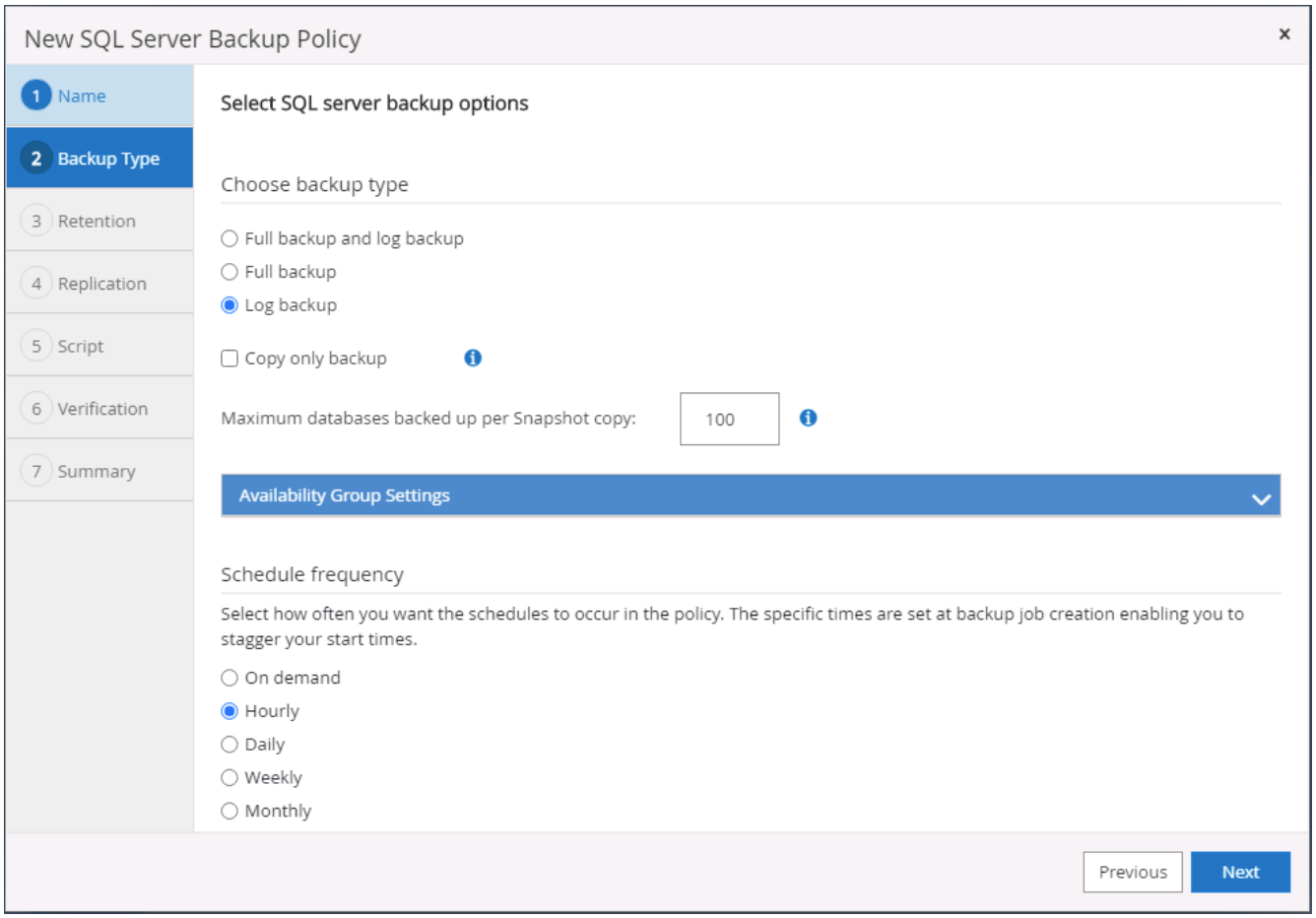


Erstellen Sie eine Datenbankprotokoll-Sicherungsrichtlinie für SQL.

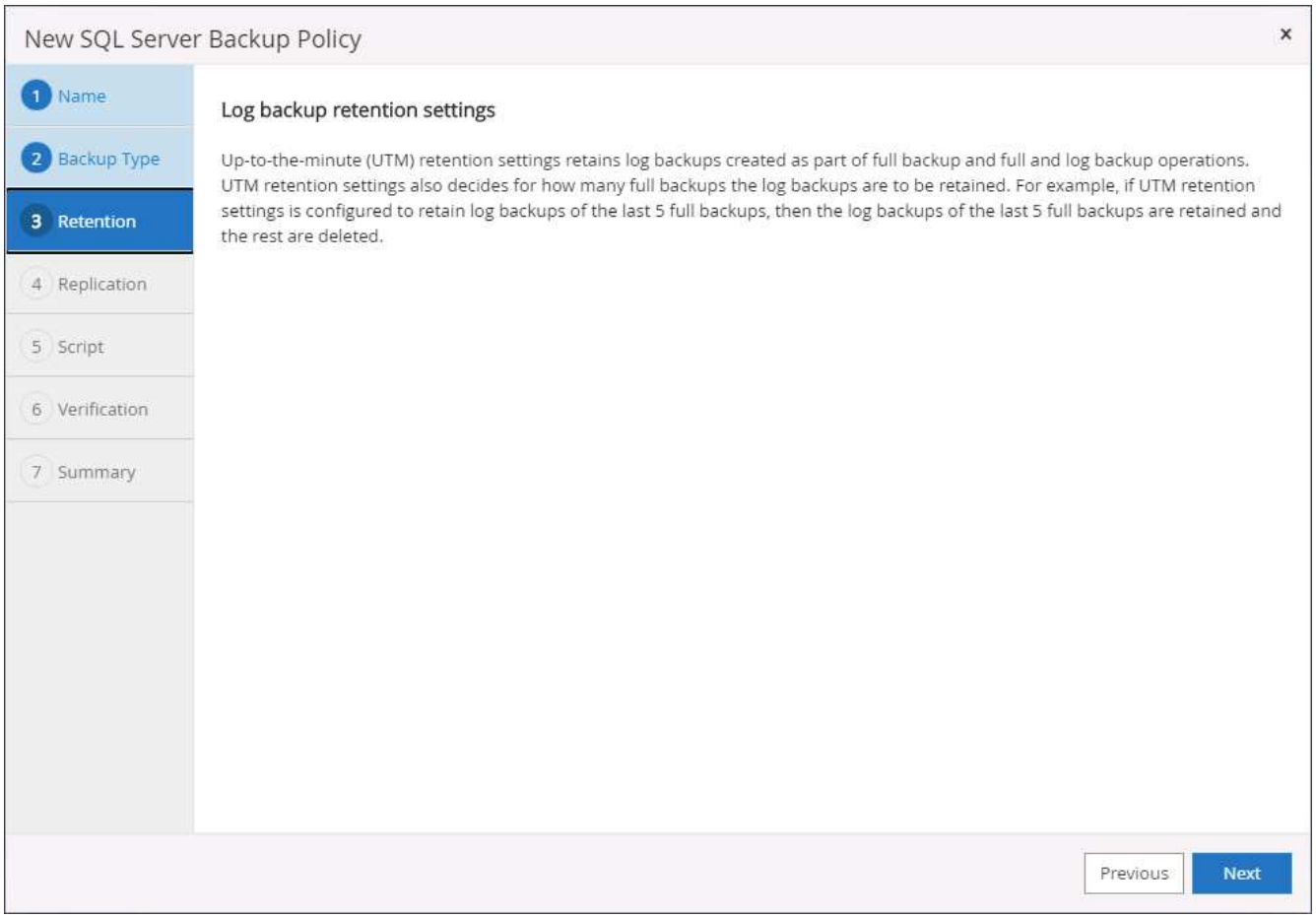
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an, klicken Sie auf „Einstellungen“ > „Richtlinien“ und dann auf „Neu“, um einen neuen Workflow zur Richtlinienerstellung zu starten.



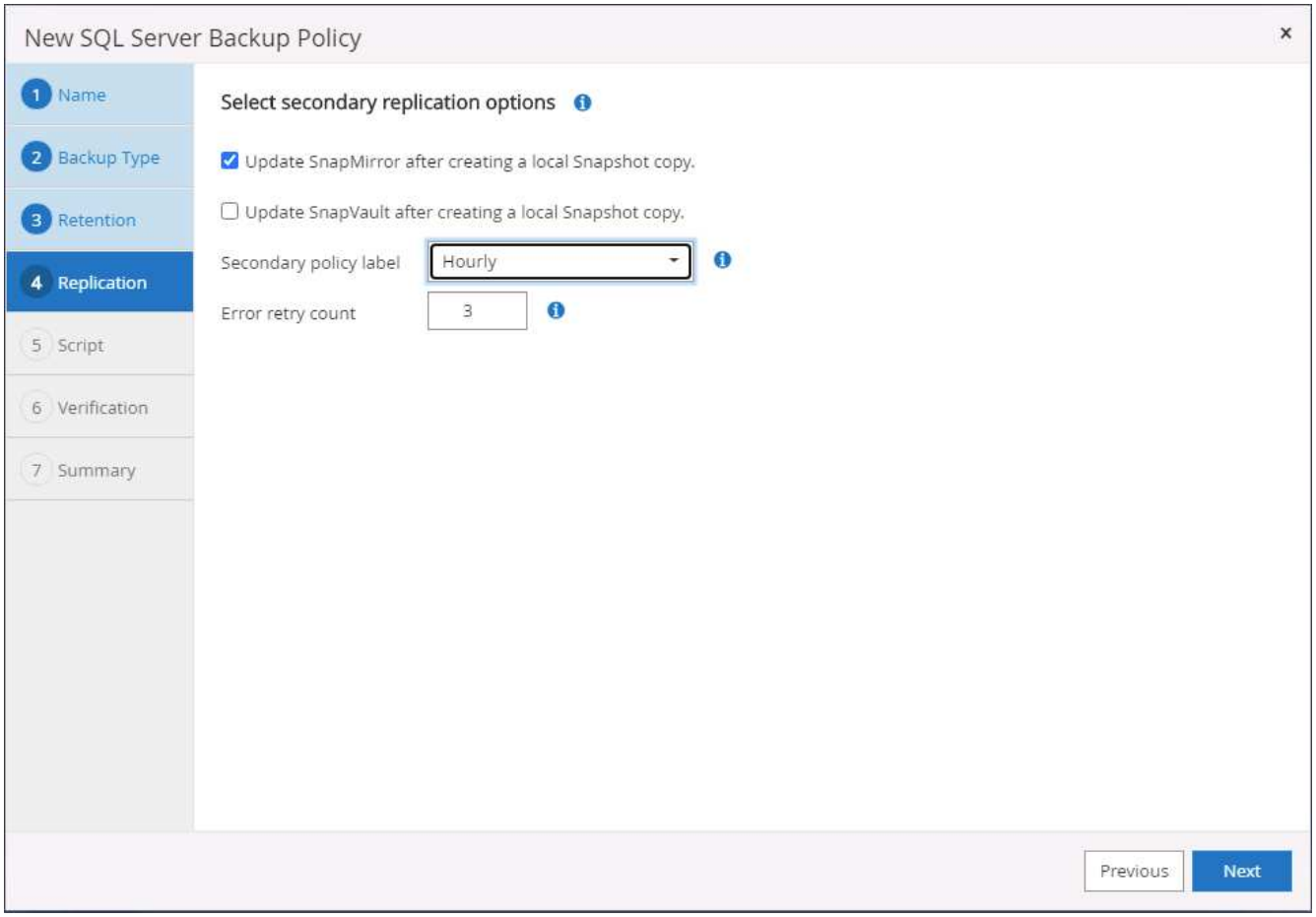
2. Definieren Sie die Protokollsicherungsoption und die geplante Häufigkeit. Für SQL Server, der mit einer Verfügbarkeitsgruppe konfiguriert ist, kann ein bevorzugtes Sicherungsreplikat festgelegt werden.



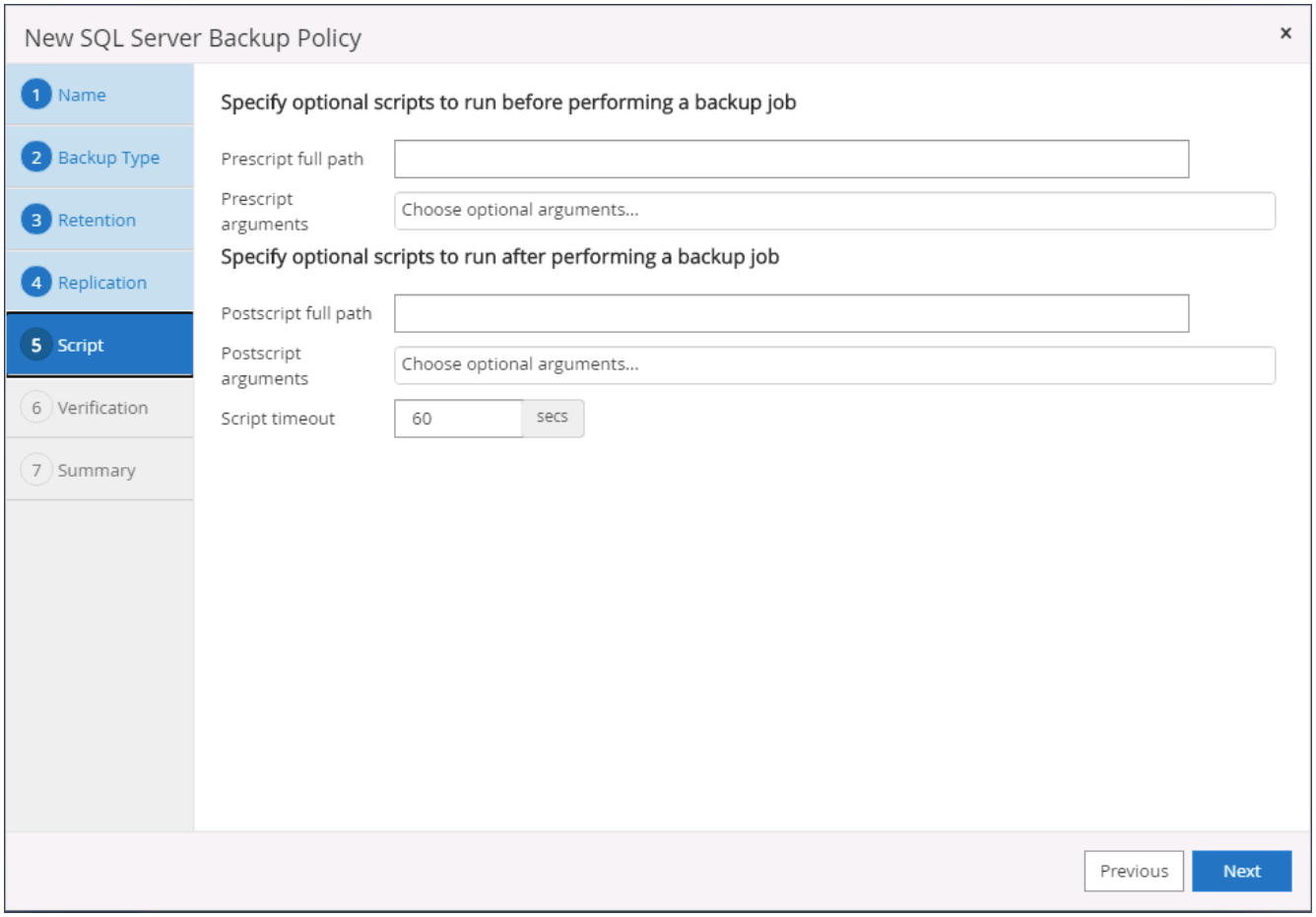
3. Die Datensicherungsrichtlinie des SQL-Servers definiert die Aufbewahrungsdauer der Protokollsicherung. Übernehmen Sie hier die Standardwerte.



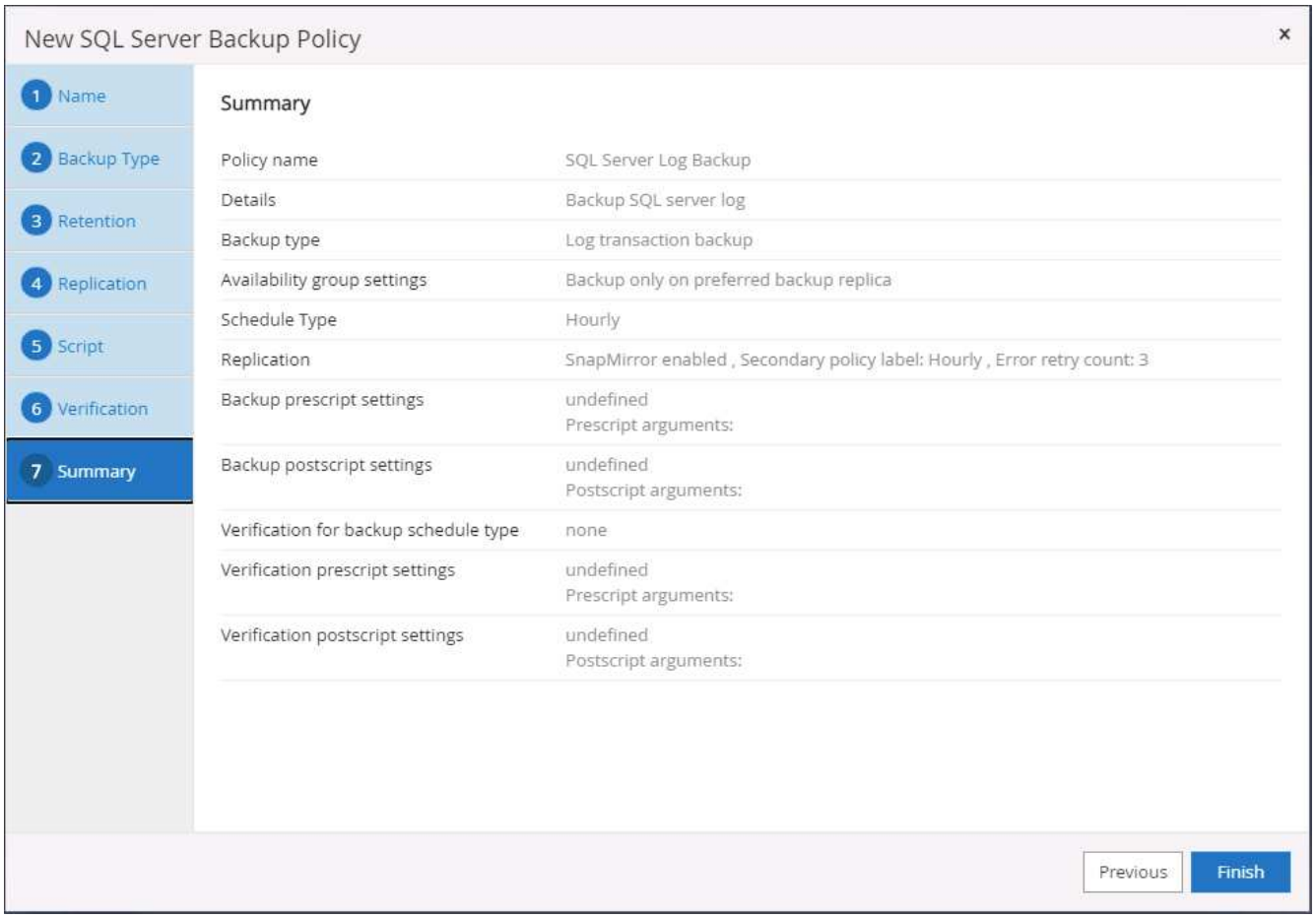
4. Aktivieren Sie die Protokollsicherungsreplikation auf sekundäre Server in der Cloud.



5. Geben Sie optionale Skripts an, die vor oder nach einem Sicherungsauftrag ausgeführt werden sollen.



6. Zusammenfassung.

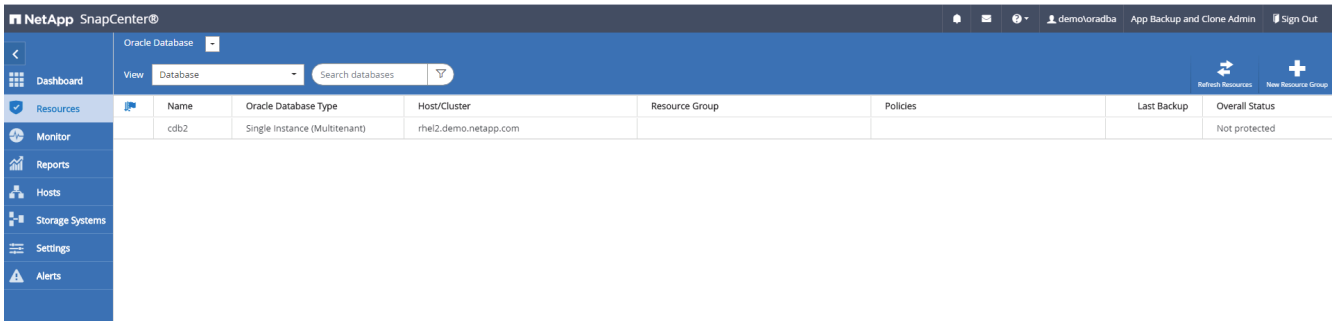


8. Implementieren Sie eine Sicherungsrichtlinie zum Schutz der Datenbank

SnapCenter verwendet eine Ressourcengruppe, um eine Datenbank in einer logischen Gruppierung von Datenbankressourcen zu sichern, z. B. mehrere auf einem Server gehostete Datenbanken, eine Datenbank, die dieselben Speichervolumes gemeinsam nutzt, mehrere Datenbanken, die eine Geschäftsanwendung unterstützen usw. Durch den Schutz einer einzelnen Datenbank wird eine eigene Ressourcengruppe erstellt. Die folgenden Verfahren zeigen, wie Sie eine in Abschnitt 7 erstellte Sicherungsrichtlinie zum Schutz von Oracle- und SQL Server-Datenbanken implementieren.

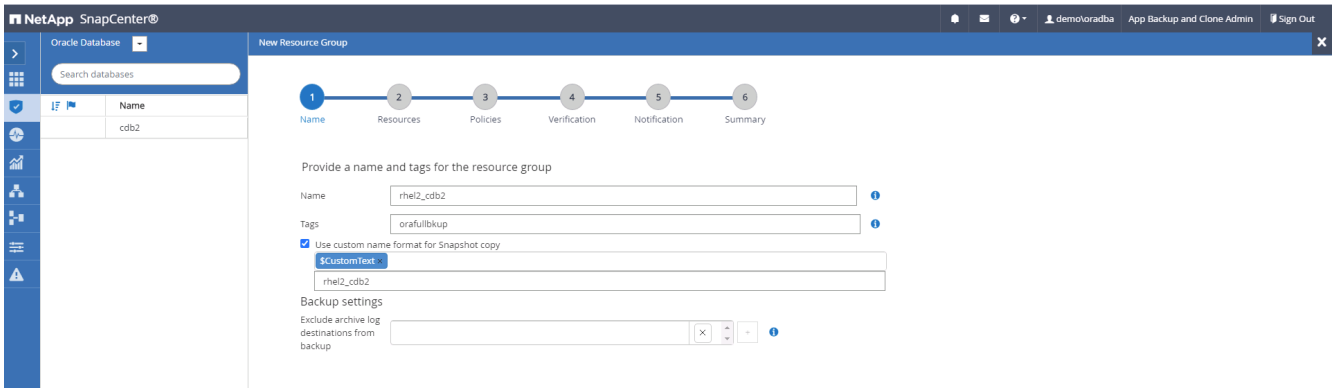
Erstellen Sie eine Ressourcengruppe für die vollständige Sicherung von Oracle

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

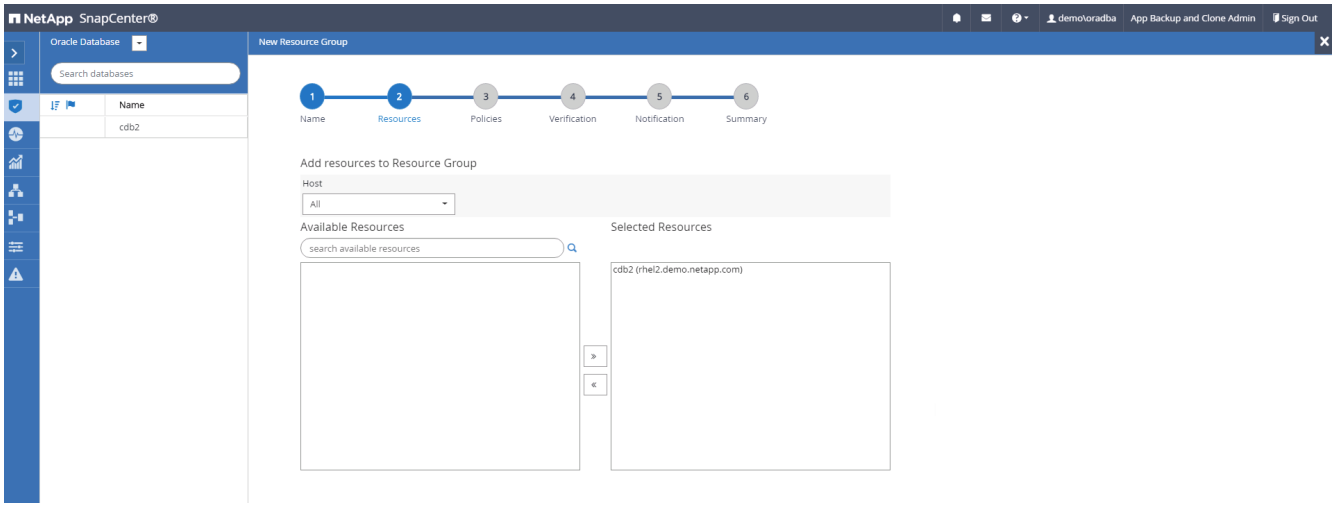


2. Geben Sie einen Namen und Tags für die Ressourcengruppe an. Sie können ein Benennungsformat für

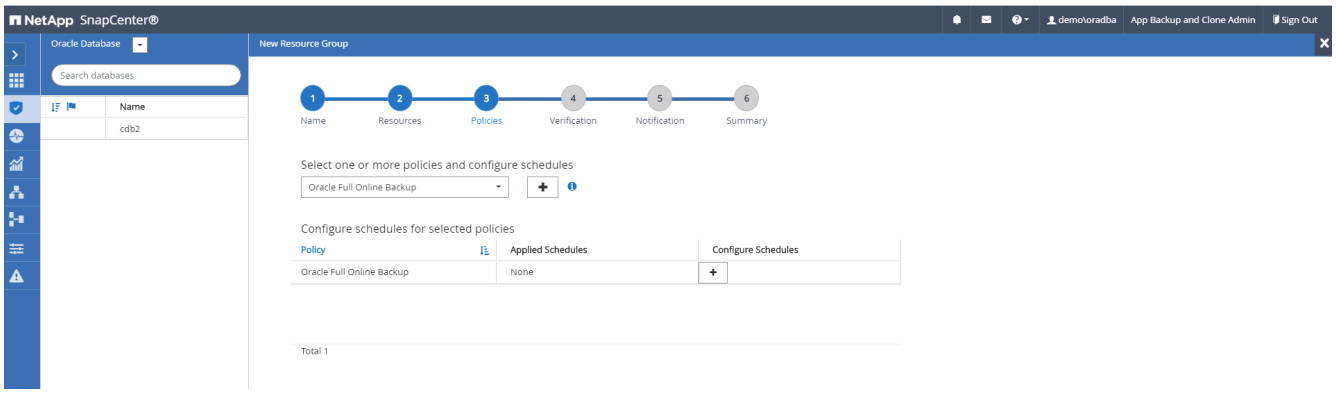
die Snapshot-Kopie definieren und das redundante Archivprotokollziel umgehen, falls konfiguriert.



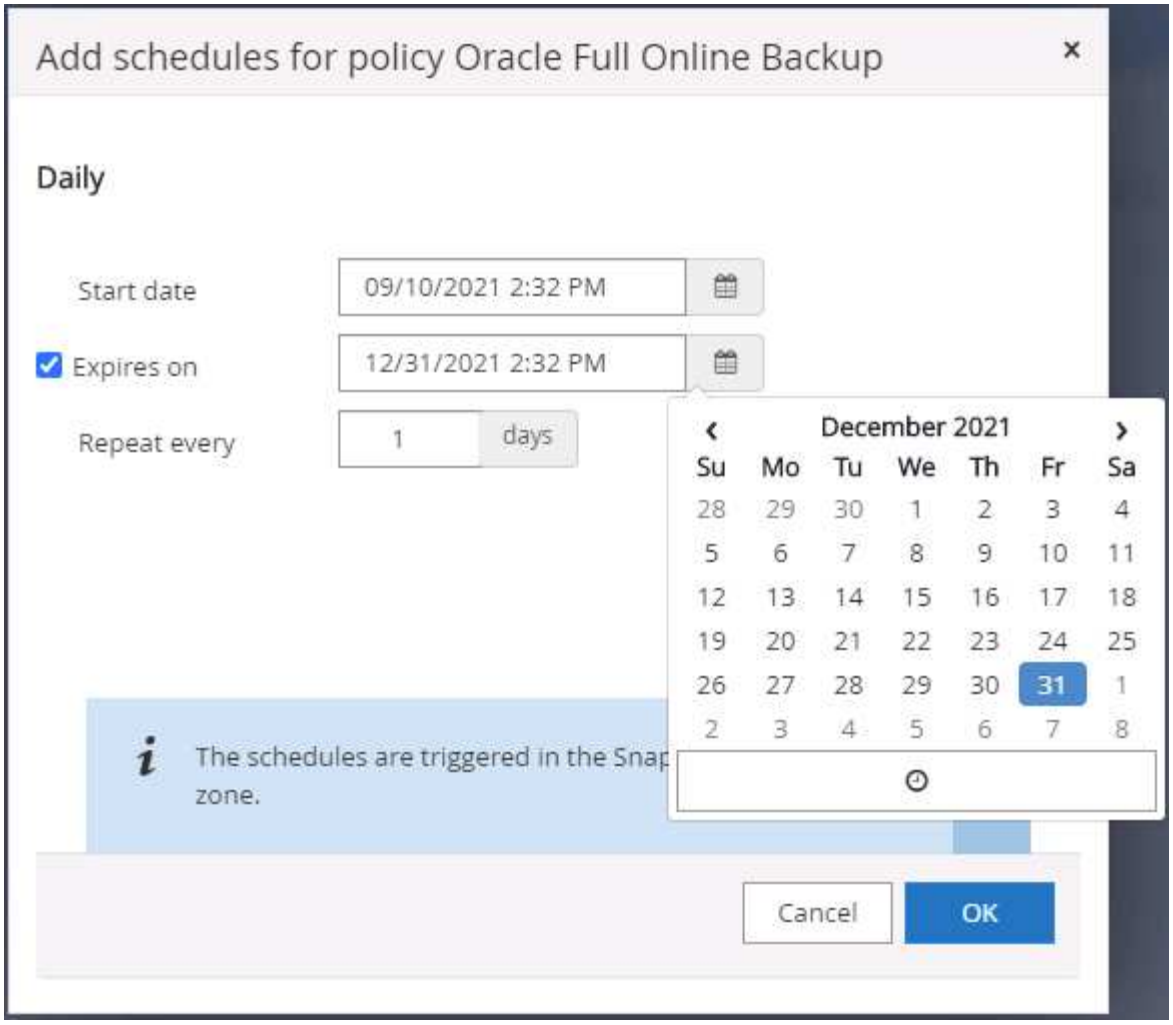
3. Fügen Sie der Ressourcengruppe Datenbankressourcen hinzu.



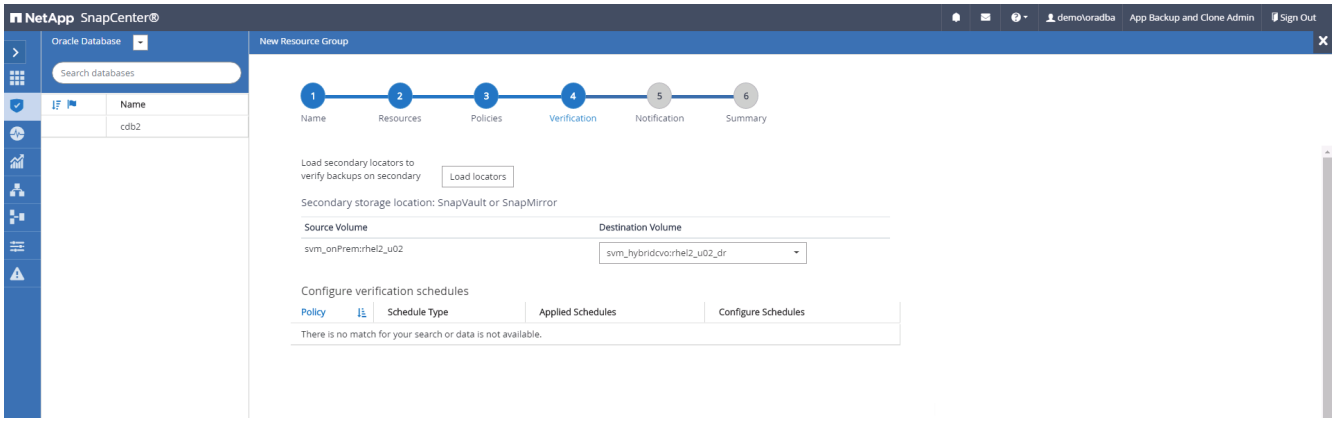
4. Wählen Sie aus der Dropdown-Liste eine in Abschnitt 7 erstellte vollständige Sicherungsrichtlinie aus.



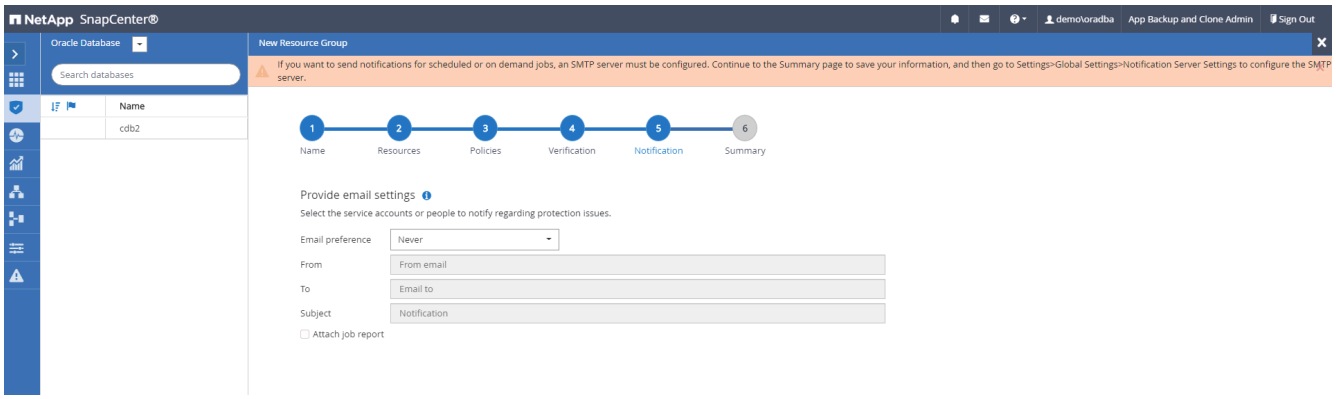
5. Klicken Sie auf das (+)-Zeichen, um den gewünschten Sicherungszeitplan zu konfigurieren.



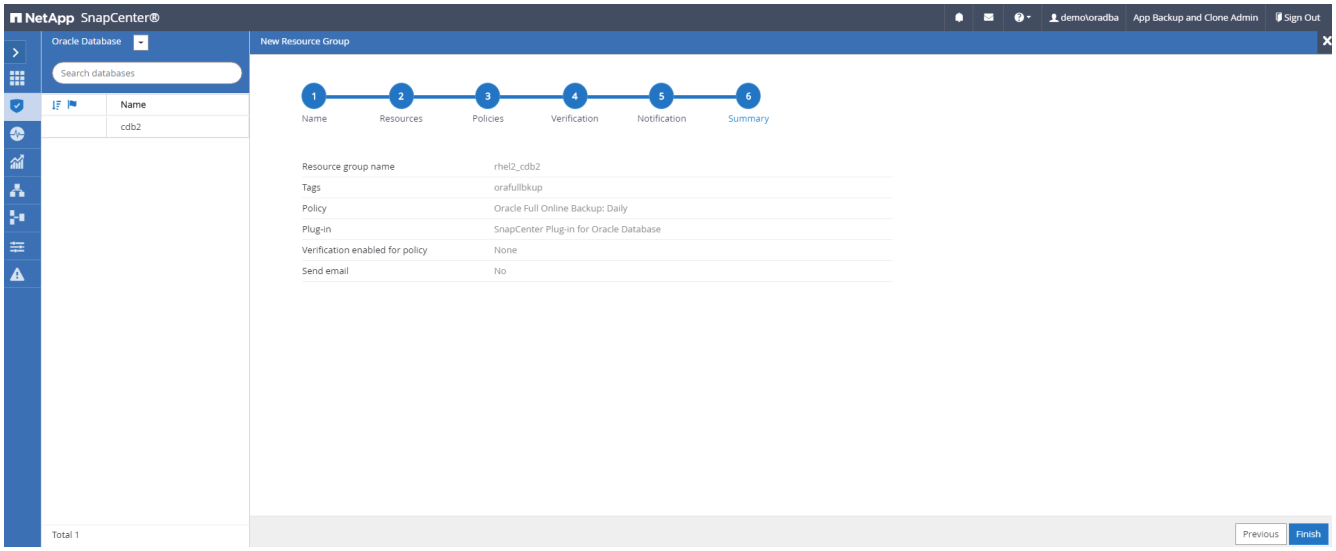
6. Klicken Sie auf „Lokalisierer laden“, um das Quell- und Zielvolume zu laden.



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

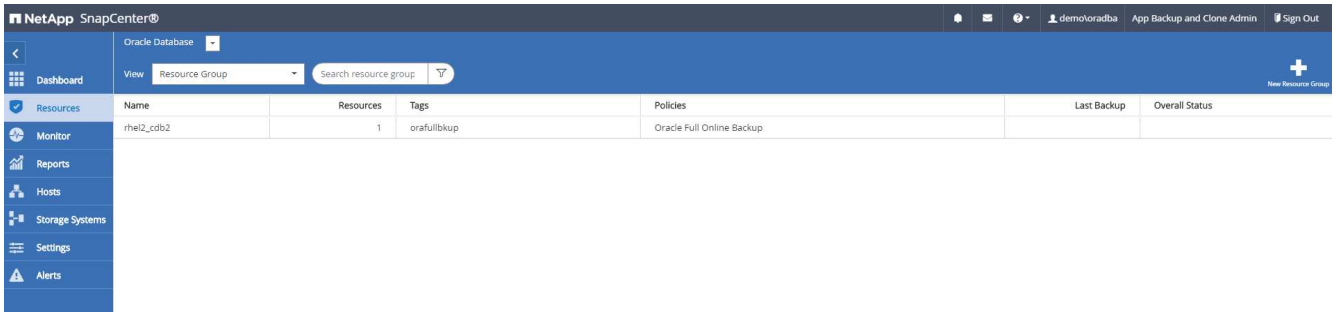


8. Zusammenfassung.

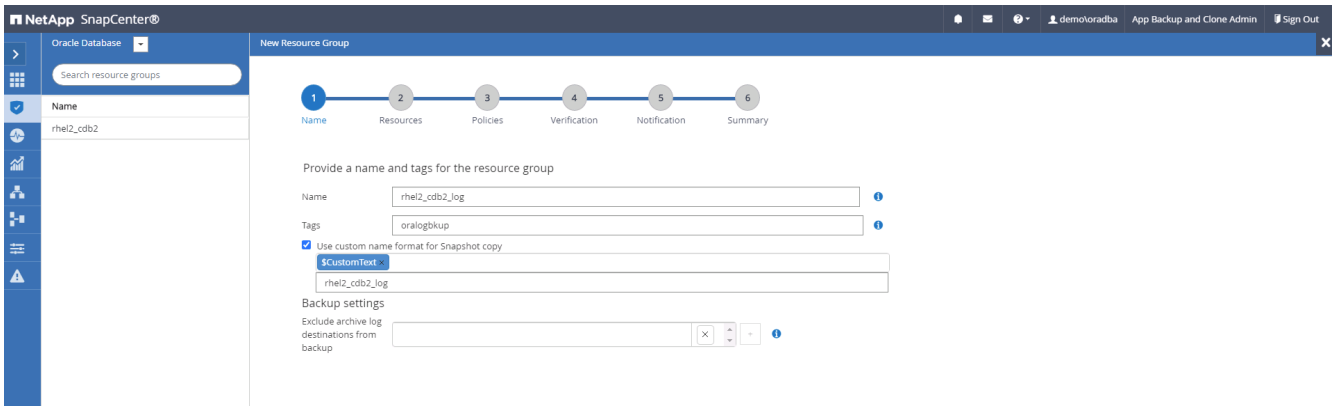


Erstellen einer Ressourcengruppe für die Protokollsicherung von Oracle

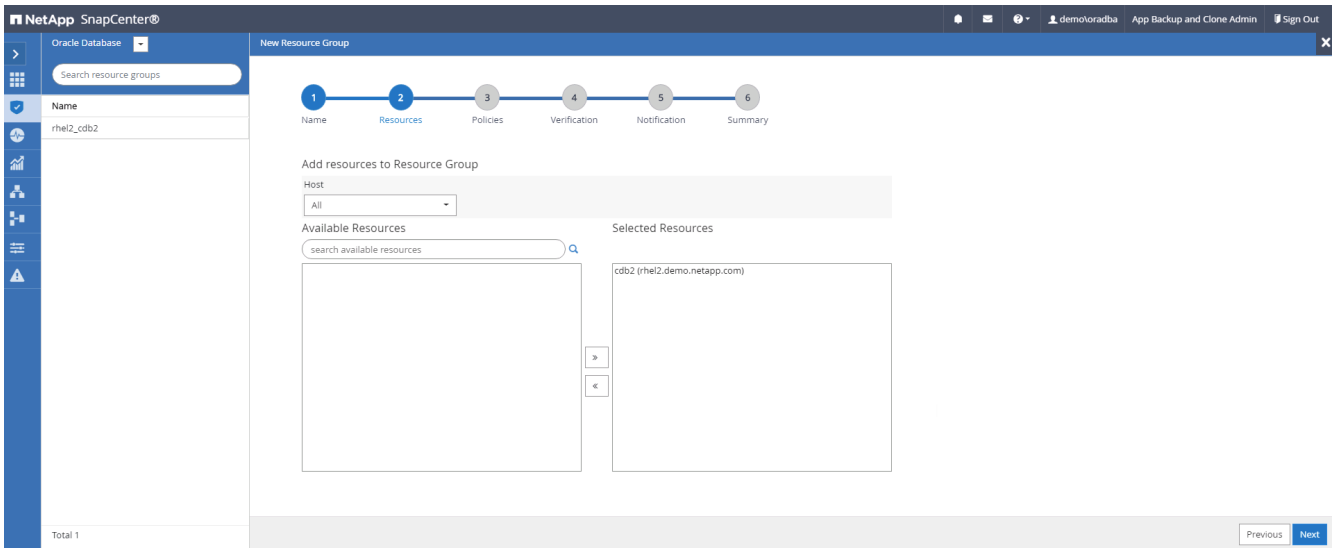
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdownliste „Ansicht“ entweder „Datenbank“ oder „Ressourcengruppe“ aus, um den Workflow zur Erstellung der Ressourcengruppe zu starten.



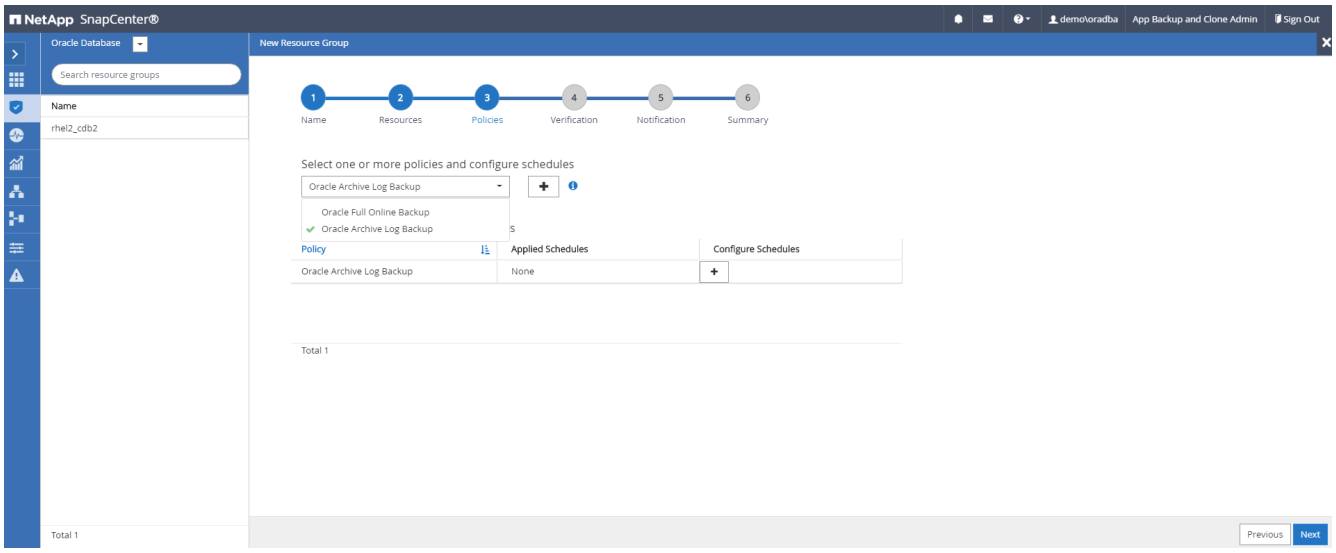
2. Geben Sie einen Namen und Tags für die Ressourcengruppe an. Sie können ein Benennungsformat für die Snapshot-Kopie definieren und das redundante Archivprotokollziel umgehen, falls konfiguriert.



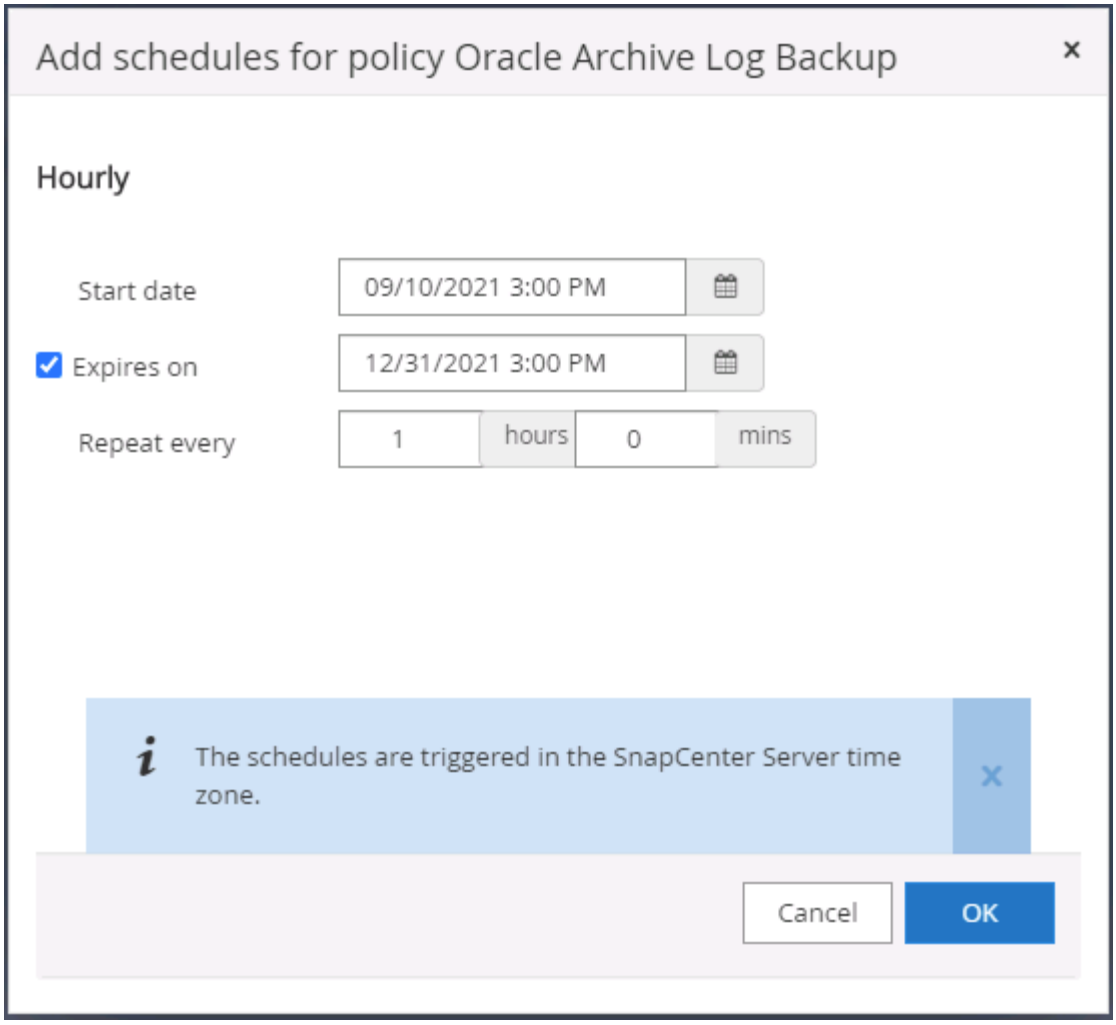
3. Fügen Sie der Ressourcengruppe Datenbankressourcen hinzu.



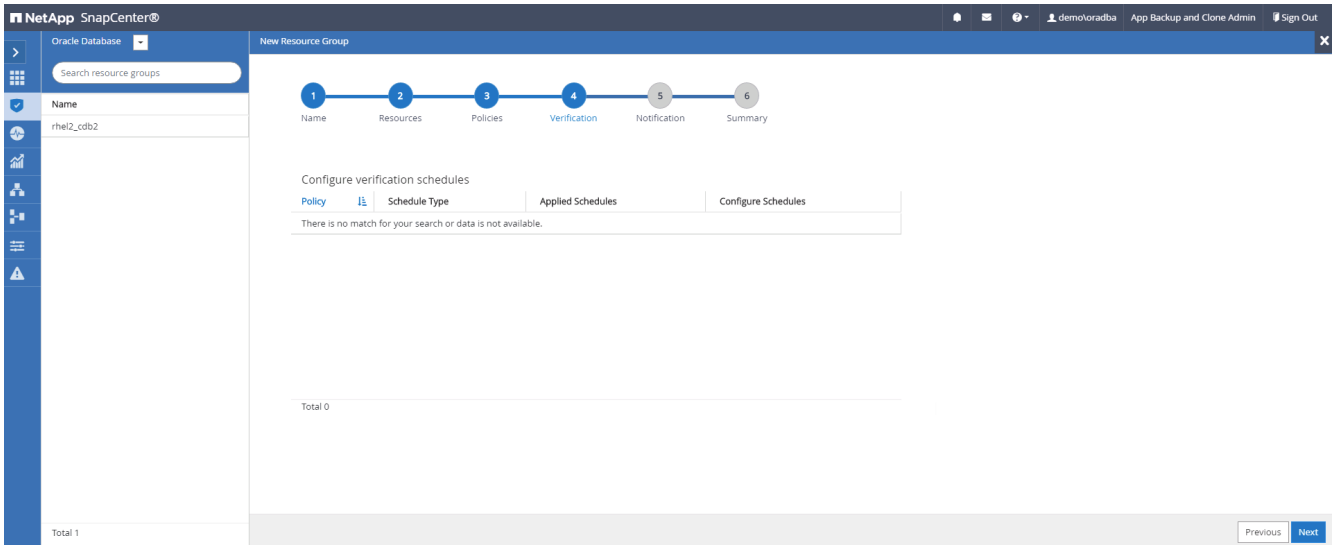
4. Wählen Sie aus der Dropdownliste eine in Abschnitt 7 erstellte Protokollsicherungsrichtlinie aus.



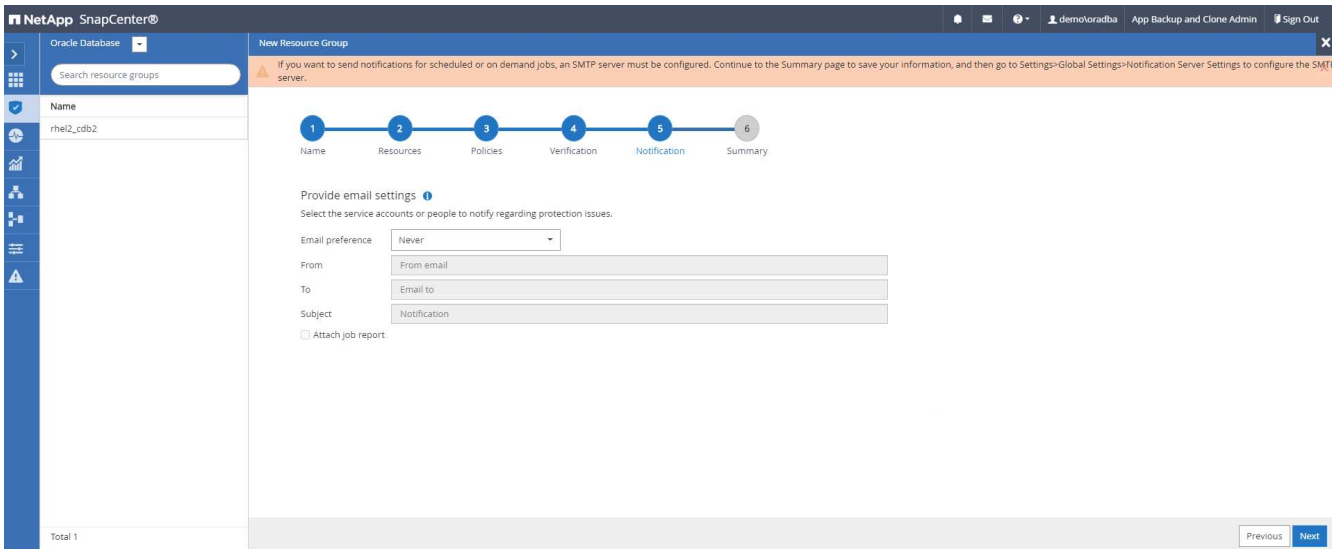
5. Klicken Sie auf das (+)-Zeichen, um den gewünschten Sicherungszeitplan zu konfigurieren.



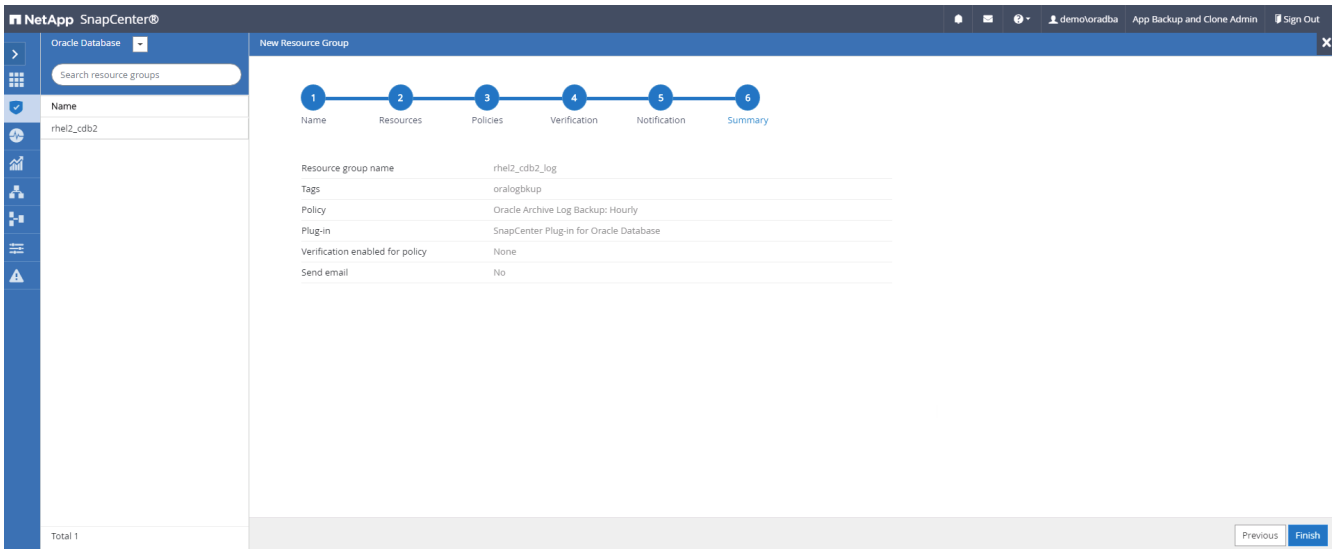
6. Wenn die Sicherungsüberprüfung konfiguriert ist, wird sie hier angezeigt.



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

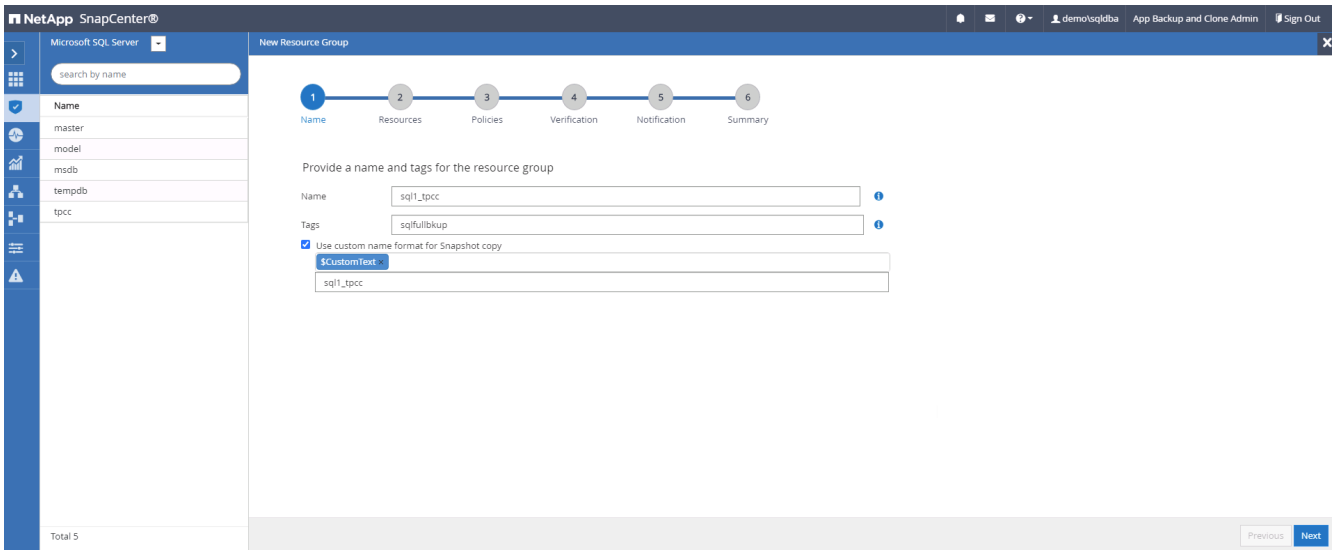


8. Zusammenfassung.

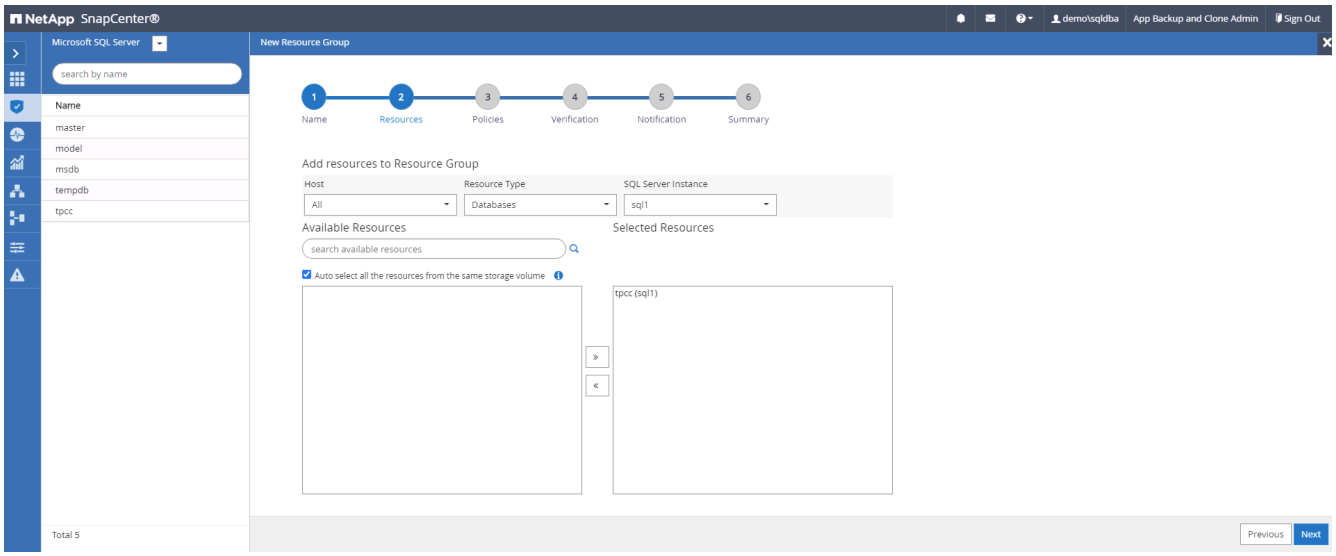


Erstellen einer Ressourcengruppe für die vollständige Sicherung von SQL Server

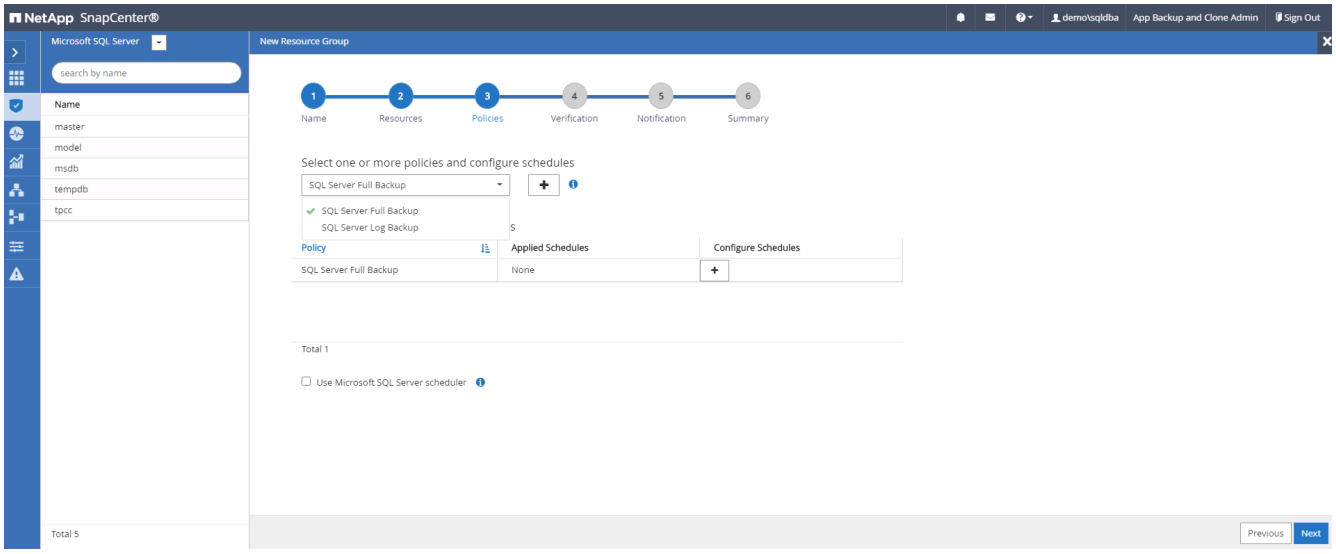
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdownliste „Ansicht“ entweder eine Datenbank oder eine Ressourcengruppe aus, um den Workflow zum Erstellen der Ressourcengruppe zu starten. Geben Sie einen Namen und Tags für die Ressourcengruppe an. Sie können ein Benennungsformat für die Snapshot-Kopie definieren.



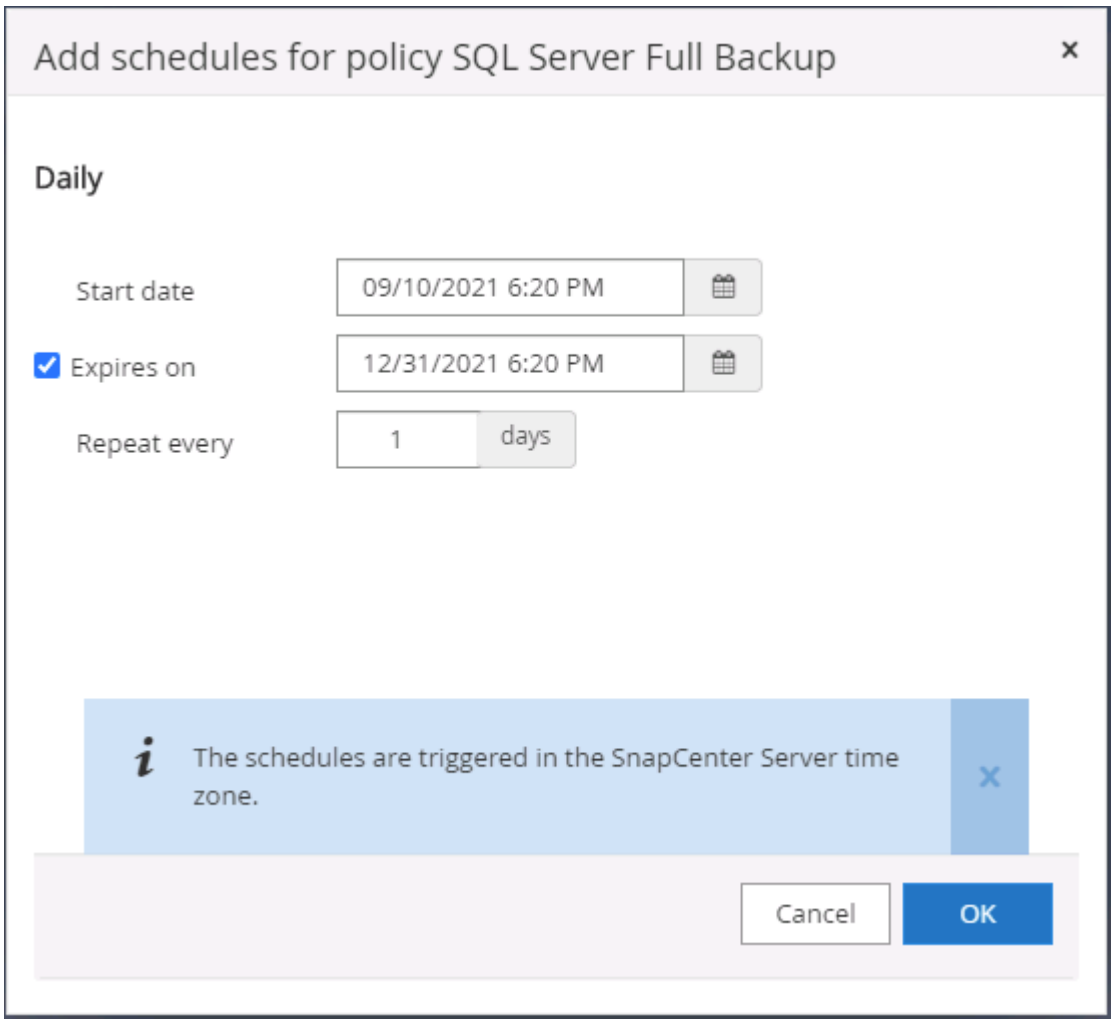
2. Wählen Sie die zu sichernden Datenbankressourcen aus.



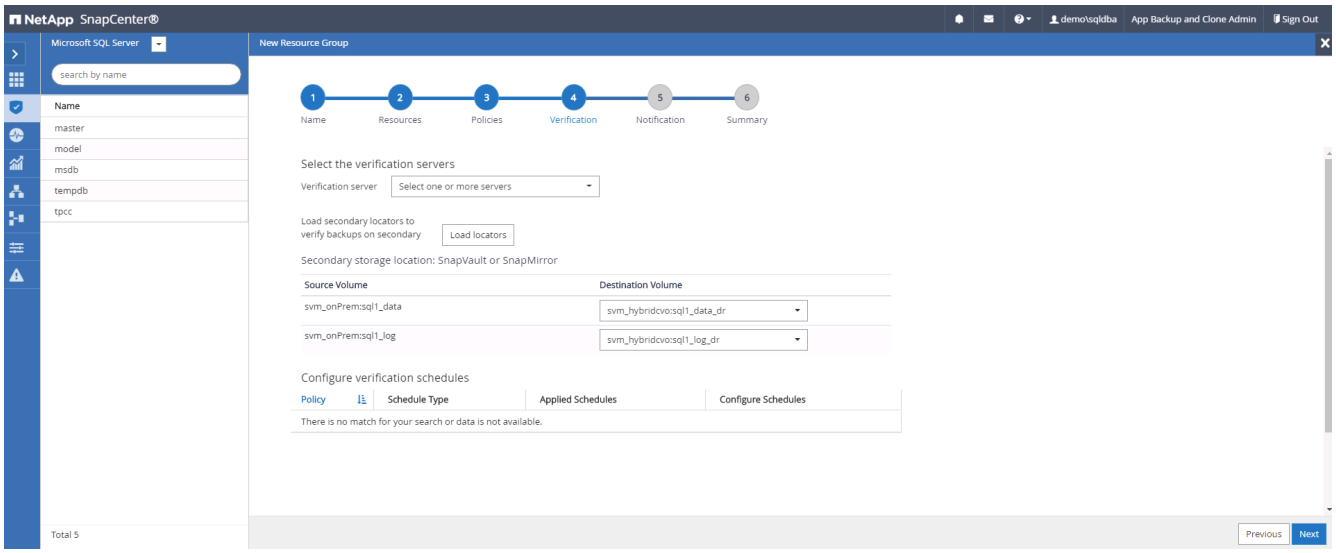
3. Wählen Sie eine vollständige SQL-Sicherungsrichtlinie aus, die in Abschnitt 7 erstellt wurde.



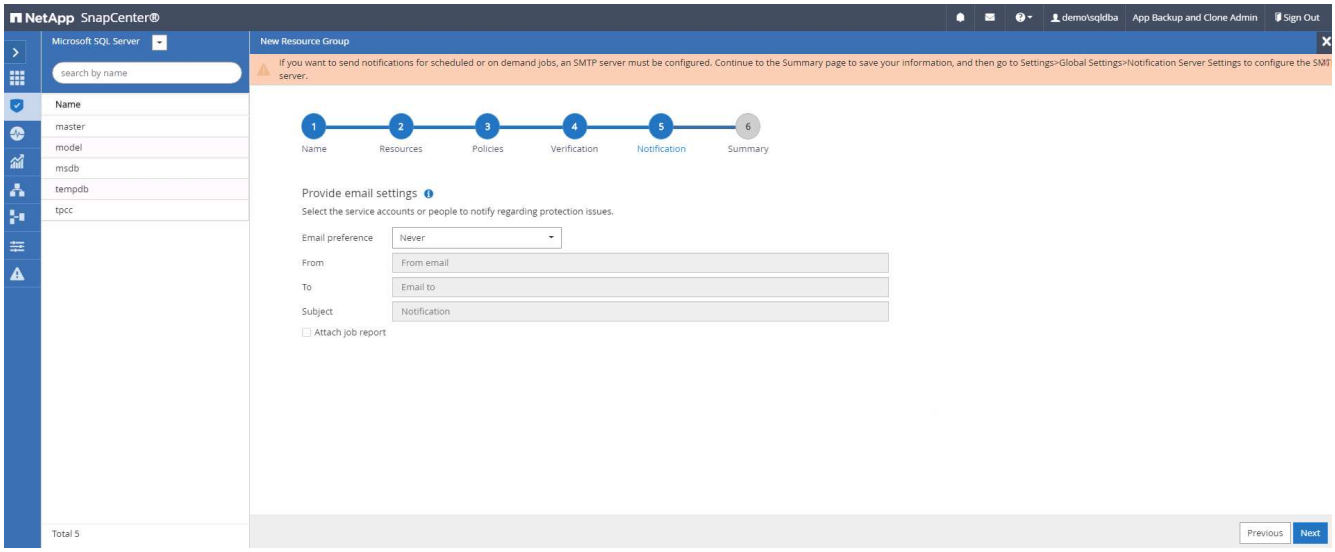
4. Fügen Sie genaue Zeitpunkte und Häufigkeiten für Sicherungen hinzu.



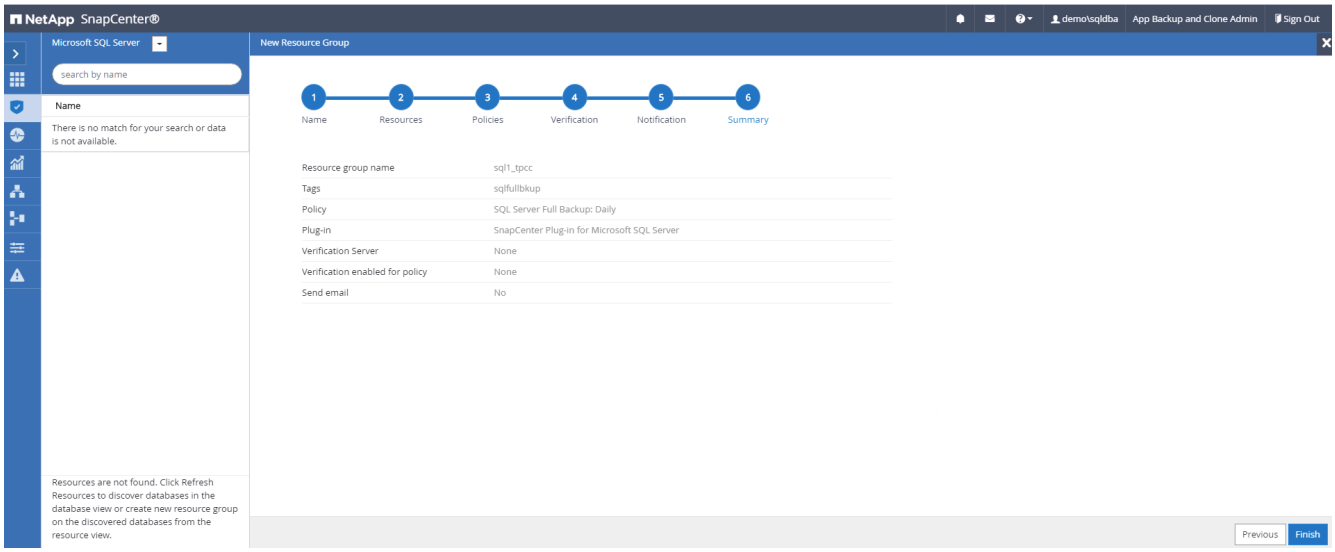
5. Wählen Sie den Überprüfungsserver für die Sicherung auf dem sekundären Server aus, wenn eine Sicherungsüberprüfung durchgeführt werden soll. Klicken Sie auf „Localor laden“, um den sekundären Speicherort zu füllen.



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

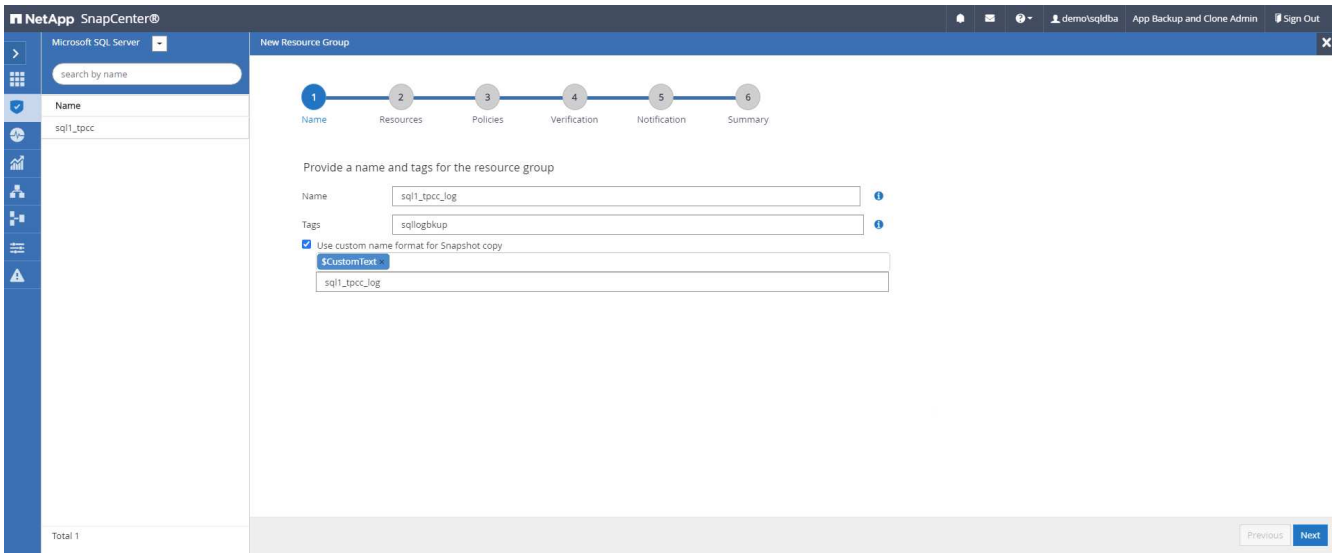


7. Zusammenfassung.

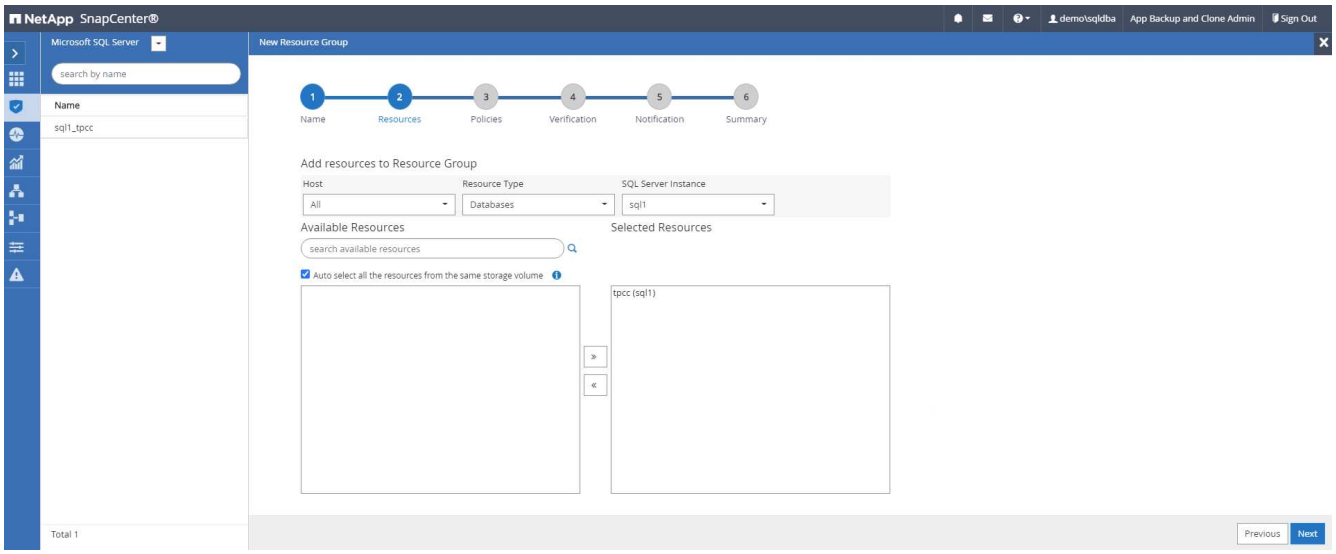


Erstellen einer Ressourcengruppe für die Protokollsicherung von SQL Server

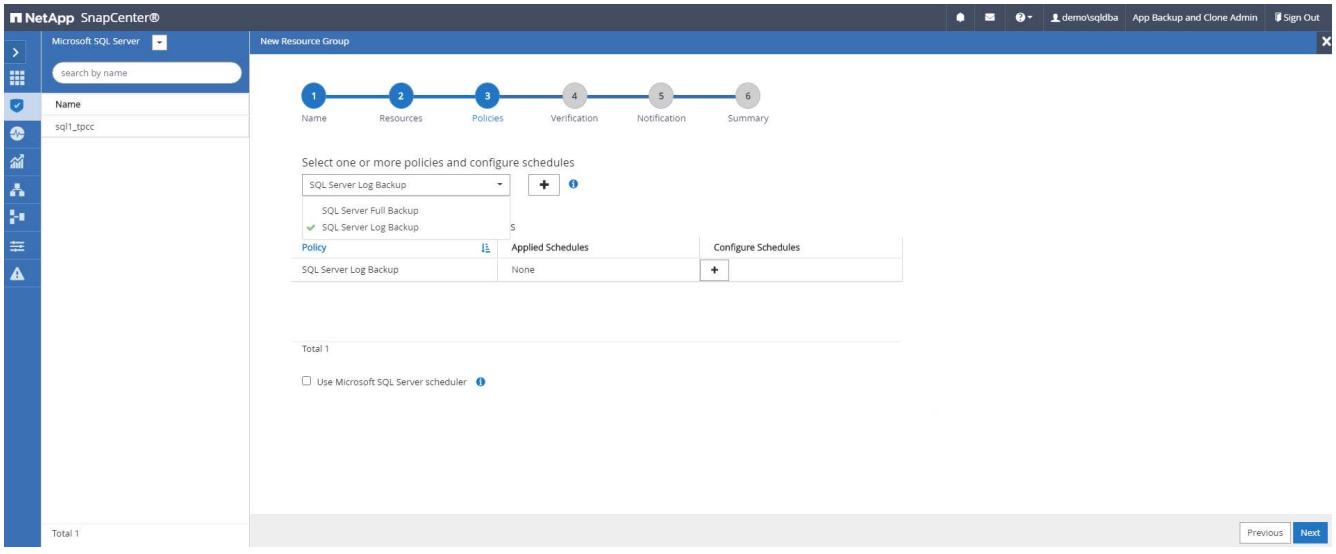
1. Melden Sie sich mit einer Benutzer-ID für die Datenbankverwaltung bei SnapCenter an und navigieren Sie zur Registerkarte „Ressourcen“. Wählen Sie in der Dropdownliste „Ansicht“ entweder eine Datenbank oder eine Ressourcengruppe aus, um den Workflow zum Erstellen der Ressourcengruppe zu starten. Geben Sie den Namen und die Tags für die Ressourcengruppe an. Sie können ein Benennungsformat für die Snapshot-Kopie definieren.



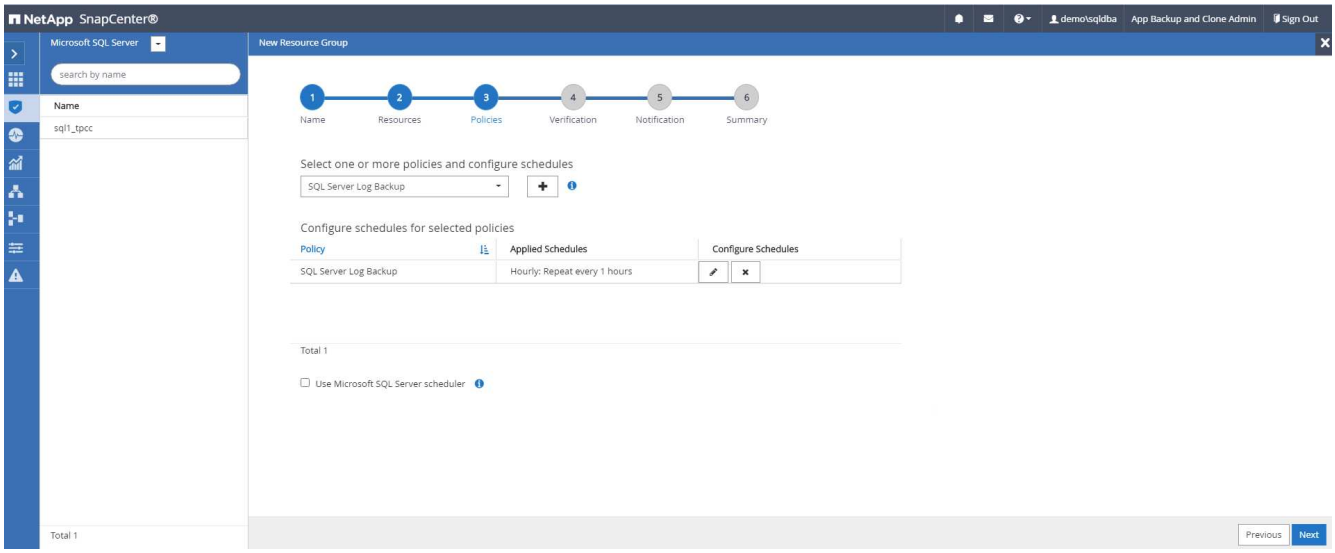
2. Wählen Sie die zu sichernden Datenbankressourcen aus.



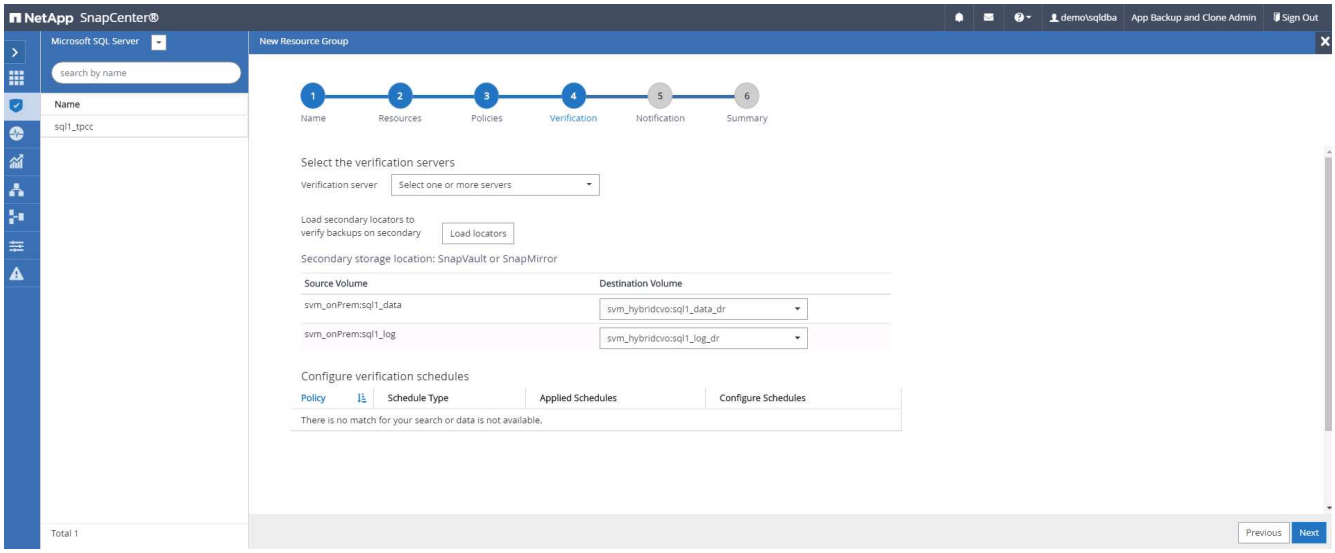
3. Wählen Sie eine in Abschnitt 7 erstellte SQL-Protokollsicherungsrichtlinie aus.



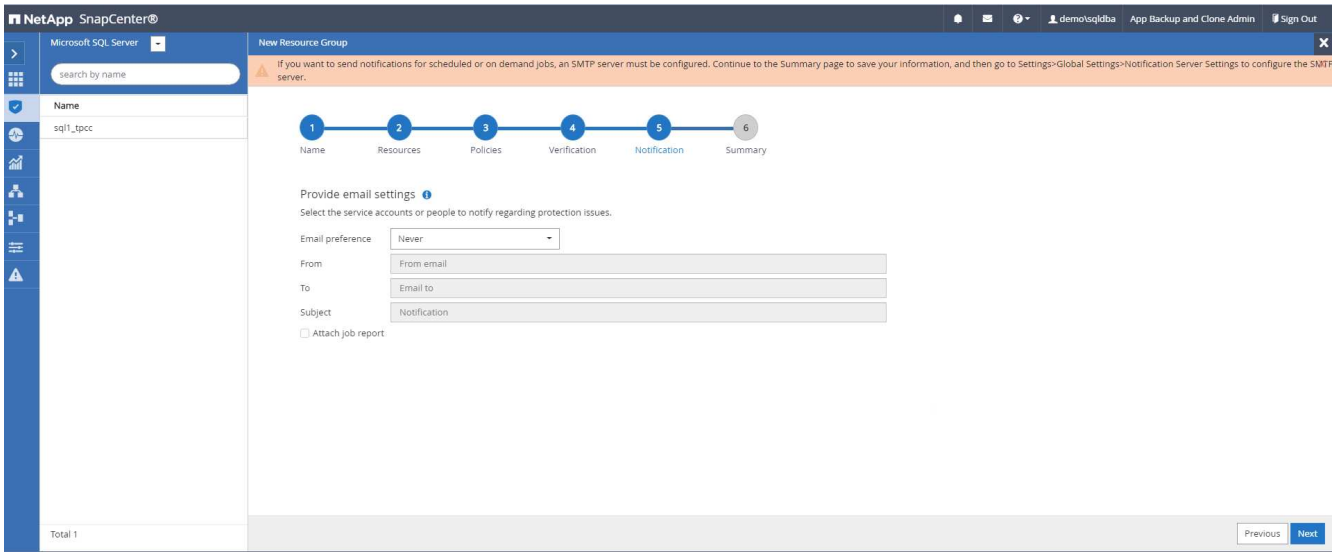
4. Fügen Sie den genauen Zeitpunkt für die Sicherung sowie die Häufigkeit hinzu.



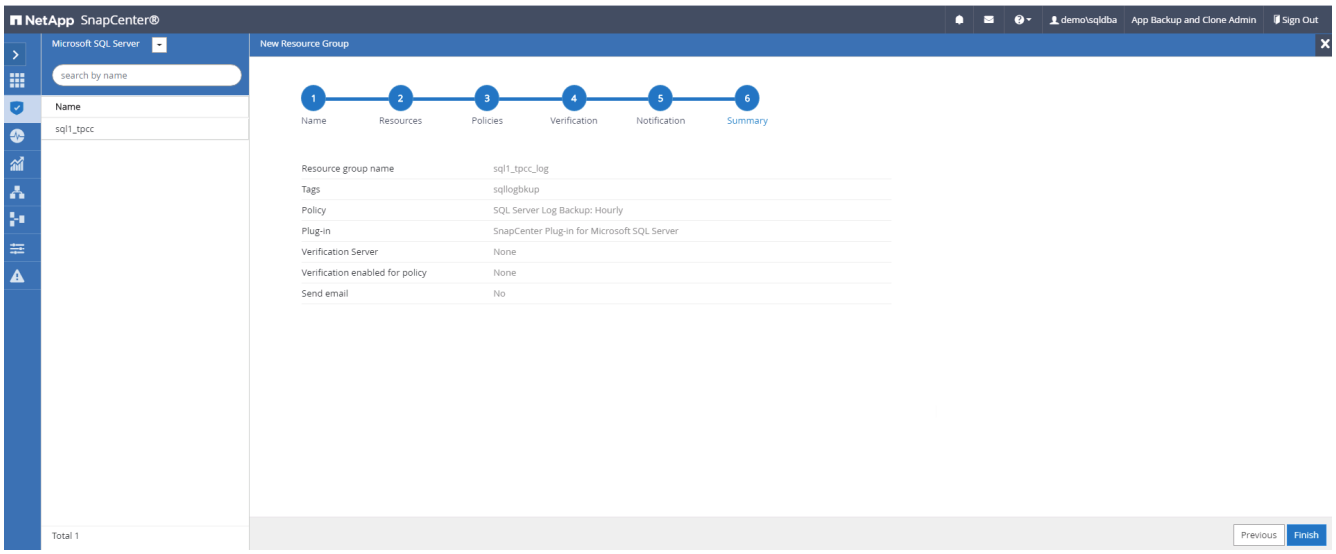
5. Wählen Sie den Überprüfungsserver für die Sicherung auf dem sekundären Server aus, wenn eine Sicherungsüberprüfung durchgeführt werden soll. Klicken Sie auf den Load Locator, um den sekundären Speicherort zu füllen.



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



7. Zusammenfassung.

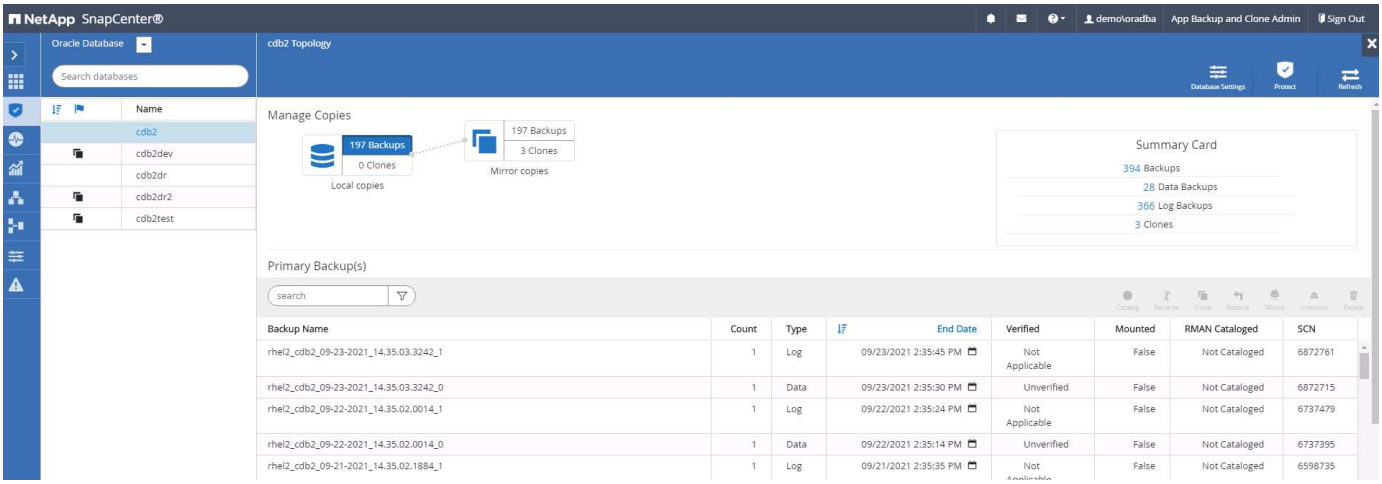


9. Sicherung validieren

Nachdem zum Schutz der Datenbankressourcen Ressourcengruppen für die Datenbanksicherung erstellt wurden, werden die Sicherungsaufträge gemäß dem vordefinierten Zeitplan ausgeführt. Überprüfen Sie den Status der Auftragsausführung auf der Registerkarte „Überwachen“.

Gehen Sie zur Registerkarte „Ressourcen“, klicken Sie auf den Datenbanknamen, um Details zur Datenbanksicherung anzuzeigen, und wechseln Sie zwischen lokalen Kopien und Spiegelkopien, um zu

überprüfen, ob Snapshot-Sicherungen an einen sekundären Speicherort in der öffentlichen Cloud repliziert werden.



An diesem Punkt stehen Datenbank-Sicherungskopien in der Cloud zum Klonen bereit, um Entwicklungs-/Testprozesse auszuführen oder im Falle eines primären Fehlers eine Notfallwiederherstellung durchzuführen.

Erste Schritte mit der AWS Public Cloud

In diesem Abschnitt wird der Prozess der Bereitstellung von Cloud Manager und Cloud Volumes ONTAP in AWS beschrieben.

Öffentliche AWS-Cloud

Um die Übersichtlichkeit zu verbessern, haben wir dieses Dokument auf Grundlage einer Bereitstellung in AWS erstellt. Der Prozess ist für Azure und GCP jedoch sehr ähnlich.

1. Vorflugkontrolle

Stellen Sie vor der Bereitstellung sicher, dass die Infrastruktur vorhanden ist, um die Bereitstellung in der nächsten Phase zu ermöglichen. Hierzu gehört Folgendes:

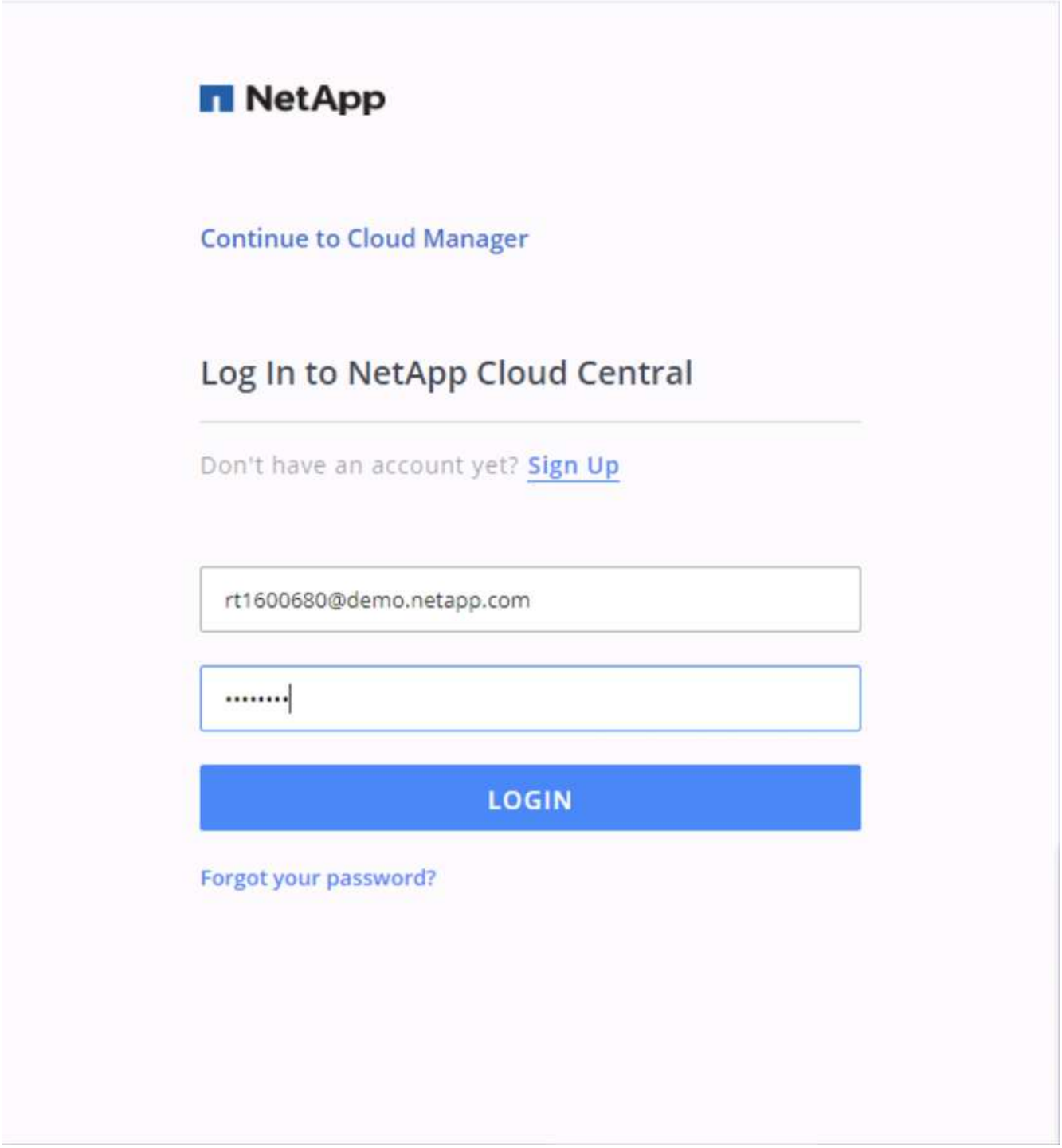
- AWS-Konto
- VPC in der Region Ihrer Wahl
- Subnetz mit Zugang zum öffentlichen Internet
- Berechtigungen zum Hinzufügen von IAM-Rollen zu Ihrem AWS-Konto
- Ein geheimer Schlüssel und Zugriffsschlüssel für Ihren AWS-Benutzer

2. Schritte zum Bereitstellen von Cloud Manager und Cloud Volumes ONTAP in AWS

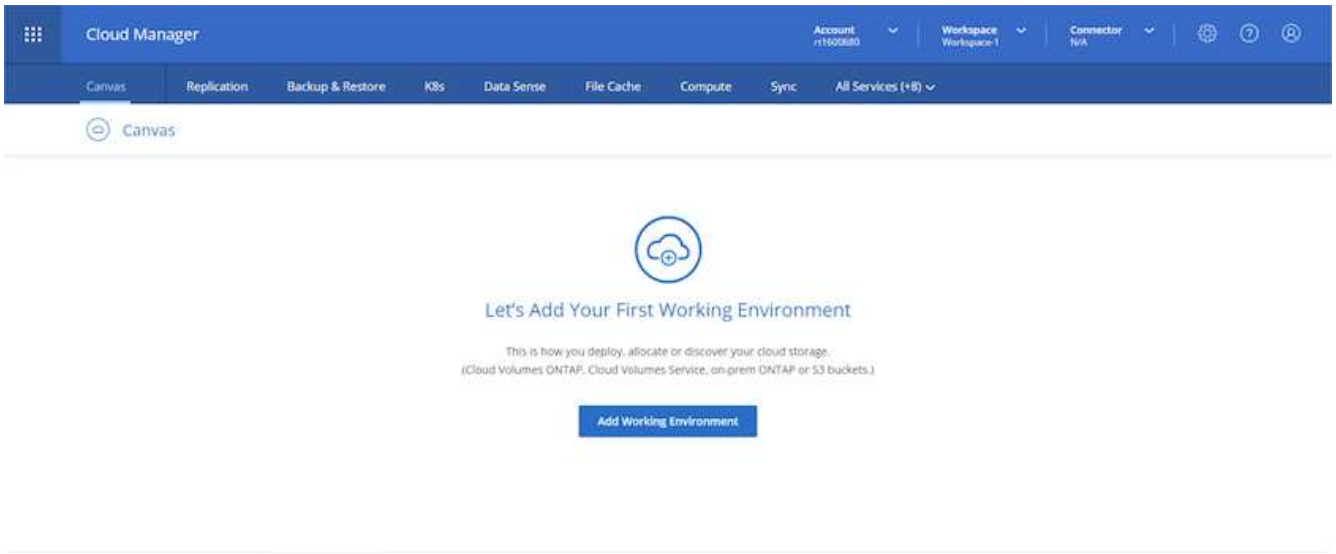
Es gibt viele Methoden zum Bereitstellen von Cloud Manager und Cloud Volumes ONTAP. Diese Methode ist die einfachste, erfordert jedoch die meisten Berechtigungen. Wenn diese Methode für Ihre AWS-Umgebung nicht geeignet ist, konsultieren Sie bitte die "NetApp Cloud-Dokumentation" .

Bereitstellen des Cloud Manager-Connectors

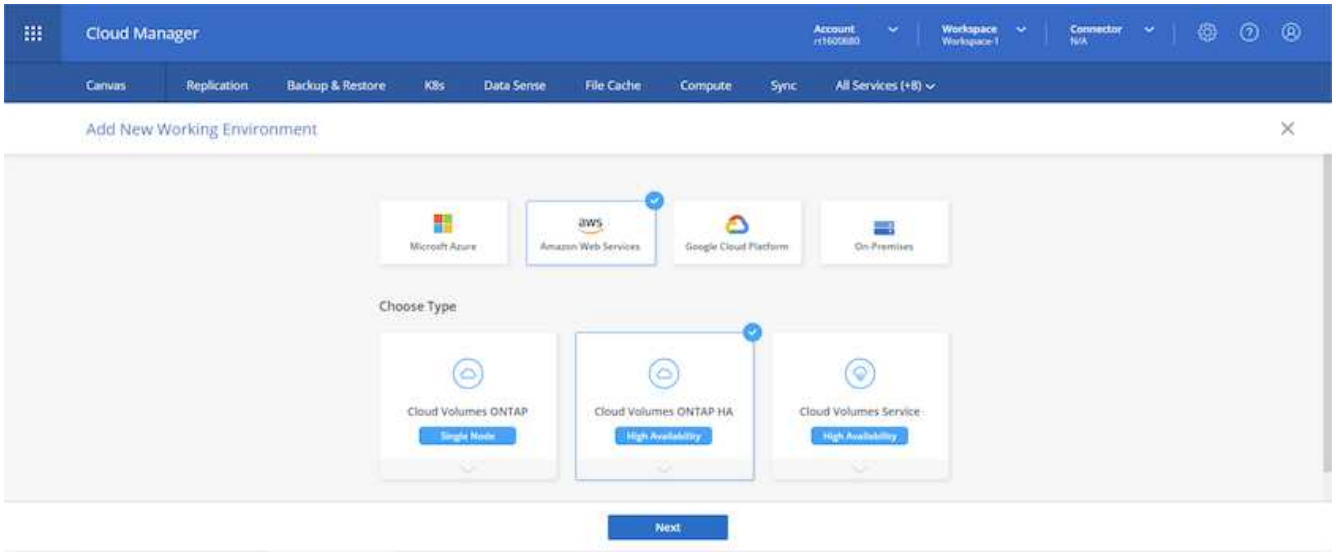
1. Navigieren Sie zu "NetApp BlueXP" und melden Sie sich an oder registrieren Sie sich.



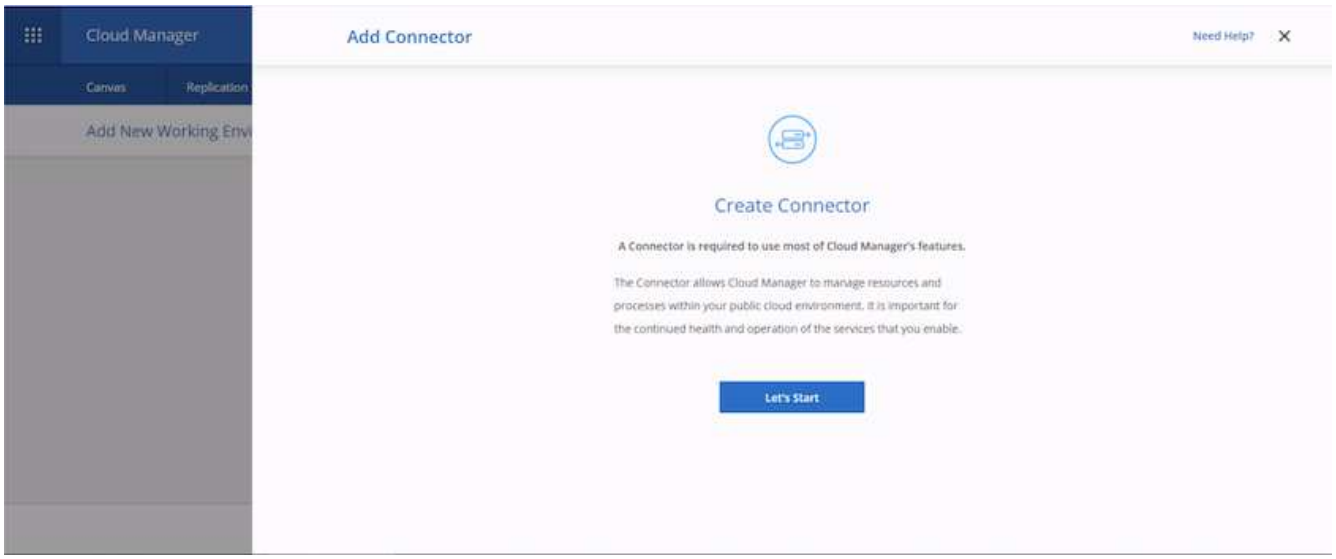
2. Nach der Anmeldung sollten Sie zum Canvas weitergeleitet werden.



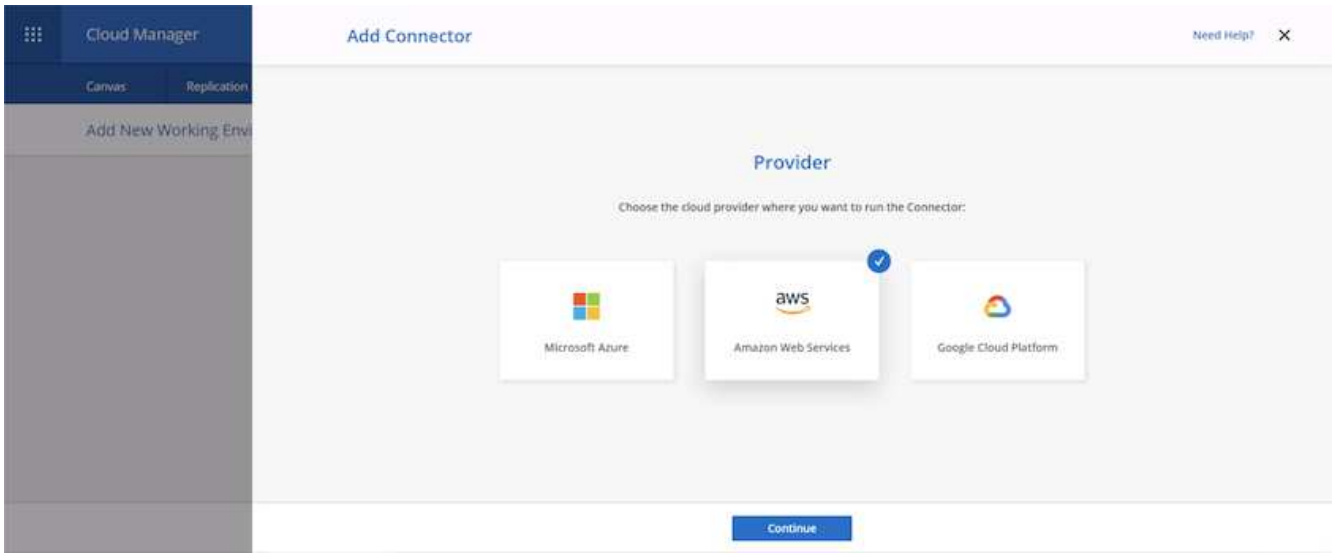
3. Klicken Sie auf „Arbeitsumgebung hinzufügen“ und wählen Sie Cloud Volumes ONTAP in AWS. Hier wählen Sie auch aus, ob Sie ein Einzelknotensystem oder ein Hochverfügbarkeitspaar einsetzen möchten. Ich habe mich für die Bereitstellung eines Hochverfügbarkeitspaars entschieden.



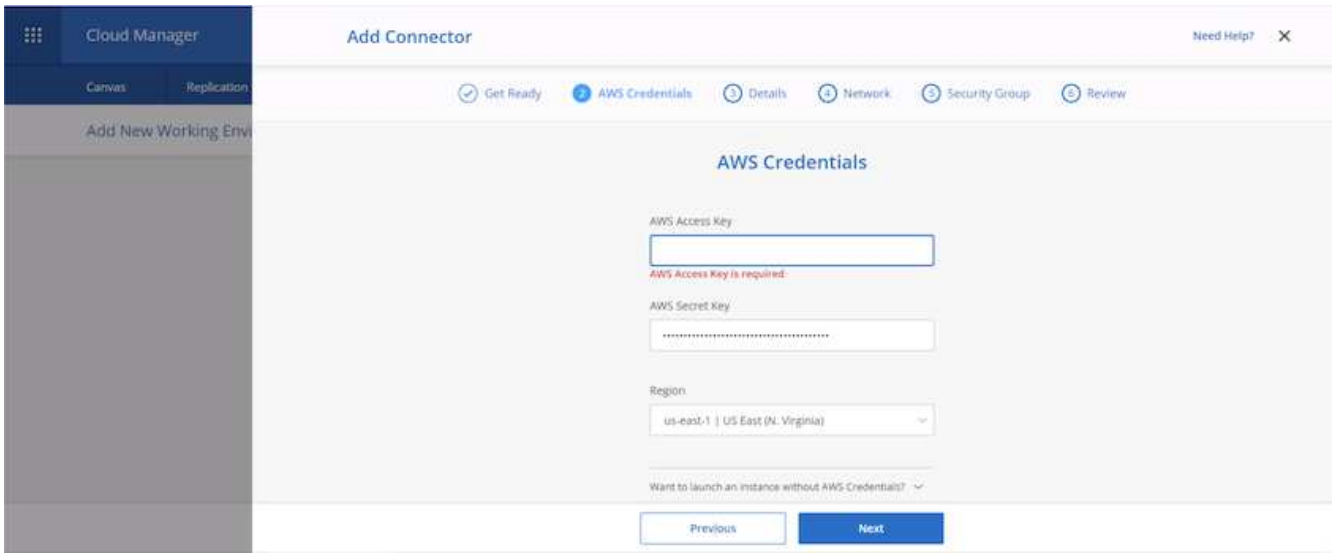
4. Wenn kein Connector erstellt wurde, wird ein Popup-Fenster mit der Aufforderung angezeigt, einen Connector zu erstellen.



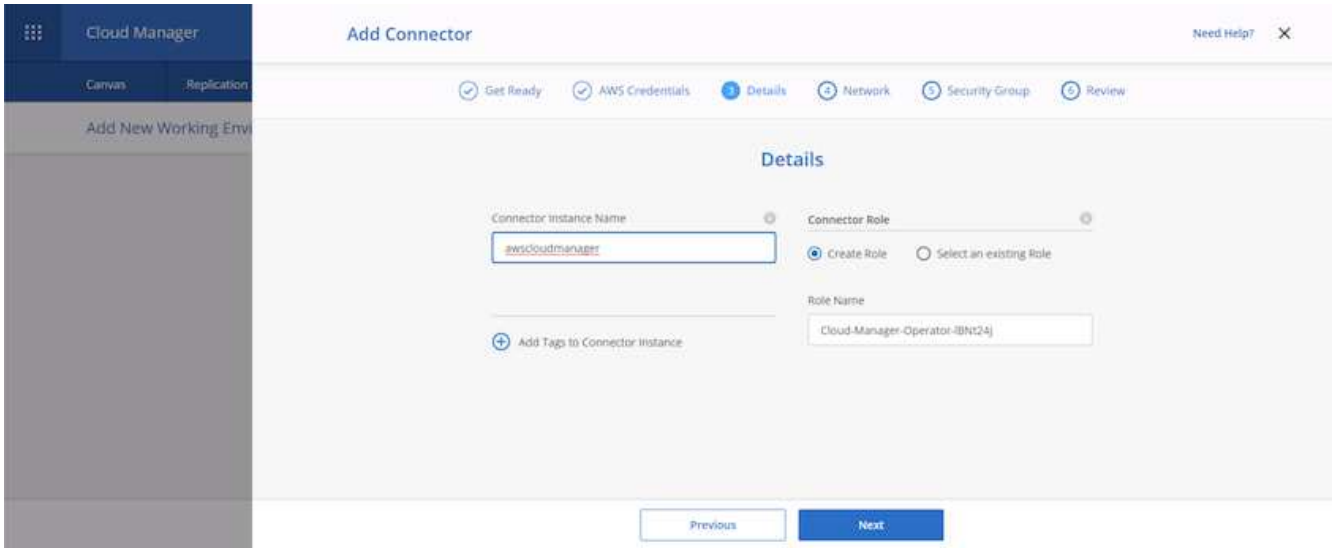
5. Klicken Sie auf „Los geht‘s“ und wählen Sie dann „AWS“ aus.



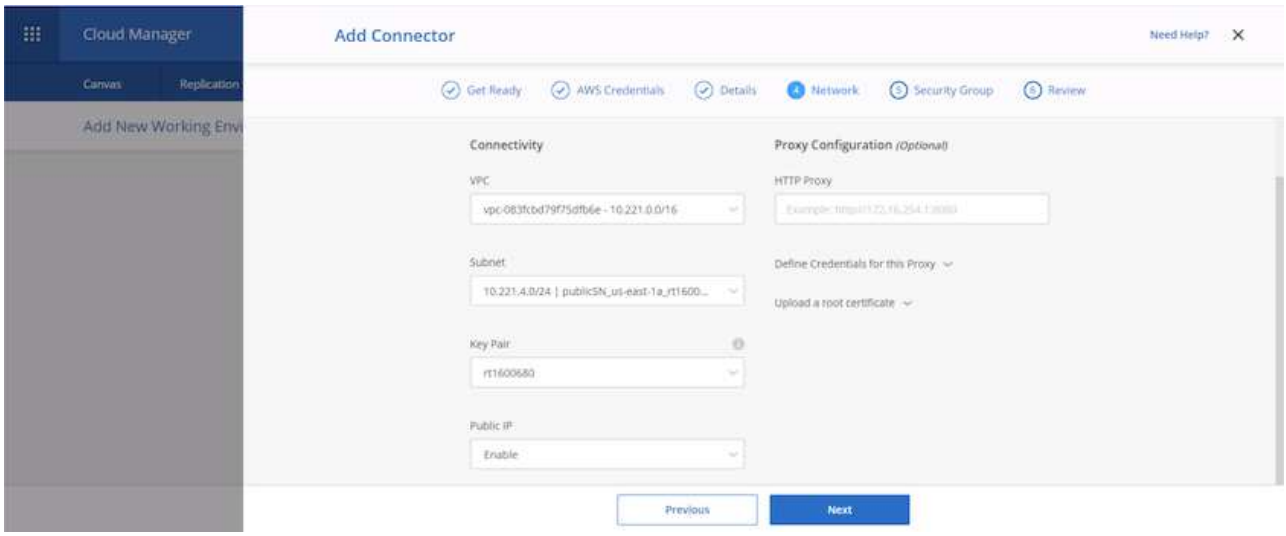
6. Geben Sie Ihren geheimen Schlüssel und Zugriffsschlüssel ein. Stellen Sie sicher, dass Ihr Benutzer über die richtigen Berechtigungen verfügt, die auf der "NetApp -Richtlinienseite" .



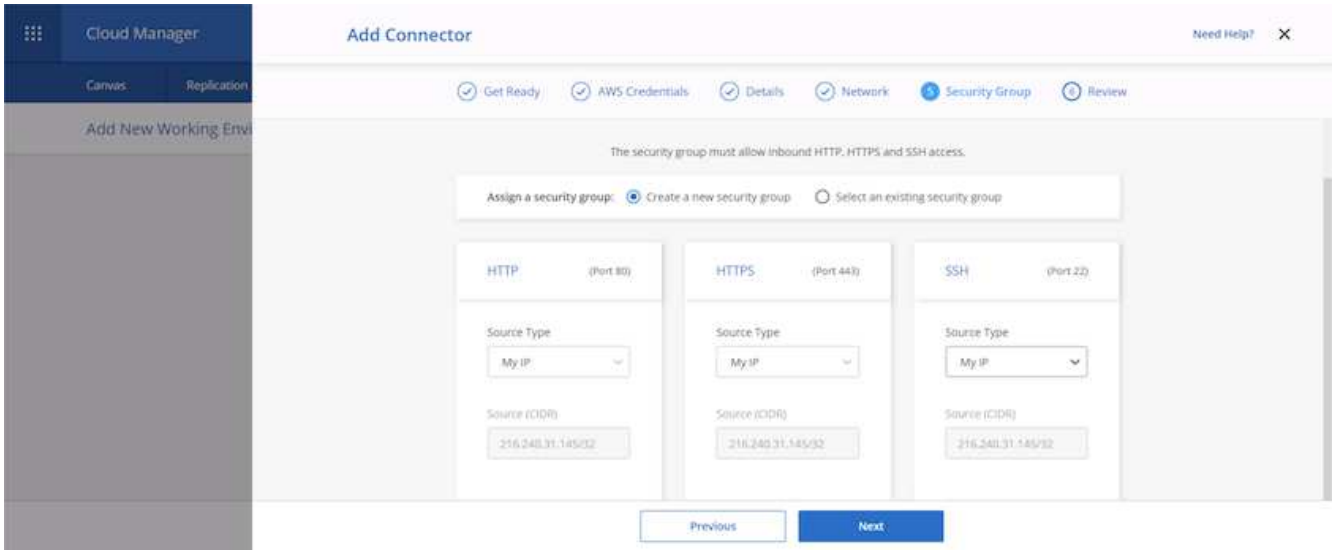
7. Geben Sie dem Connector einen Namen und verwenden Sie entweder eine vordefinierte Rolle, wie auf der "NetApp -Richtlinienseite" oder bitten Sie Cloud Manager, die Rolle für Sie zu erstellen.



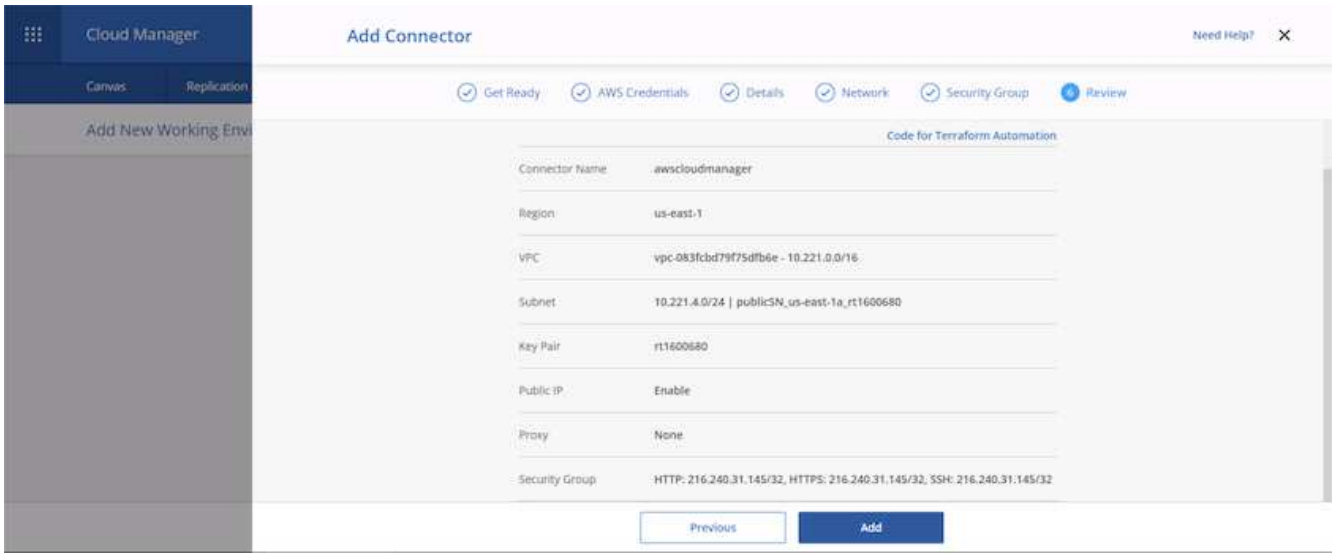
8. Geben Sie die Netzwerkinformationen an, die zum Bereitstellen des Connectors erforderlich sind. Überprüfen Sie, ob der ausgehende Internetzugriff aktiviert ist, indem Sie:
   a. Dem Connector eine öffentliche IP-Adresse zuweisen
   b. Dem Connector einen Proxy zum Arbeiten geben
   c. Dem Connector eine Route zum öffentlichen Internet über ein Internet-Gateway geben



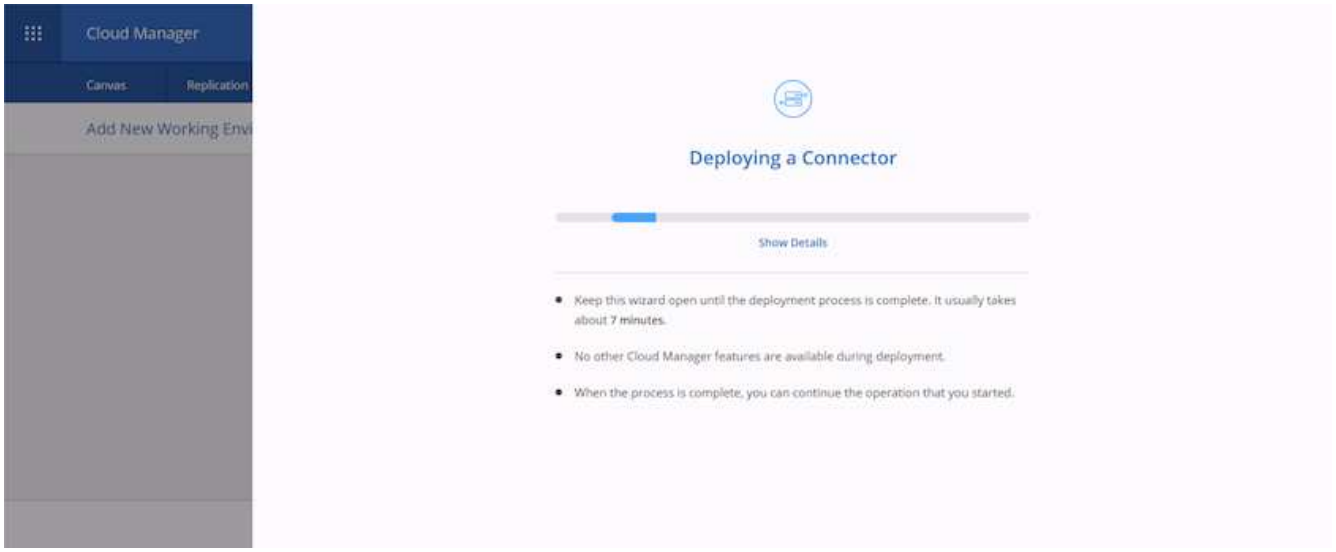
9. Stellen Sie die Kommunikation mit dem Connector über SSH, HTTP und HTTPs bereit, indem Sie entweder eine Sicherheitsgruppe bereitstellen oder eine neue Sicherheitsgruppe erstellen. Ich habe den Zugriff auf den Connector nur von meiner IP-Adresse aus aktiviert.



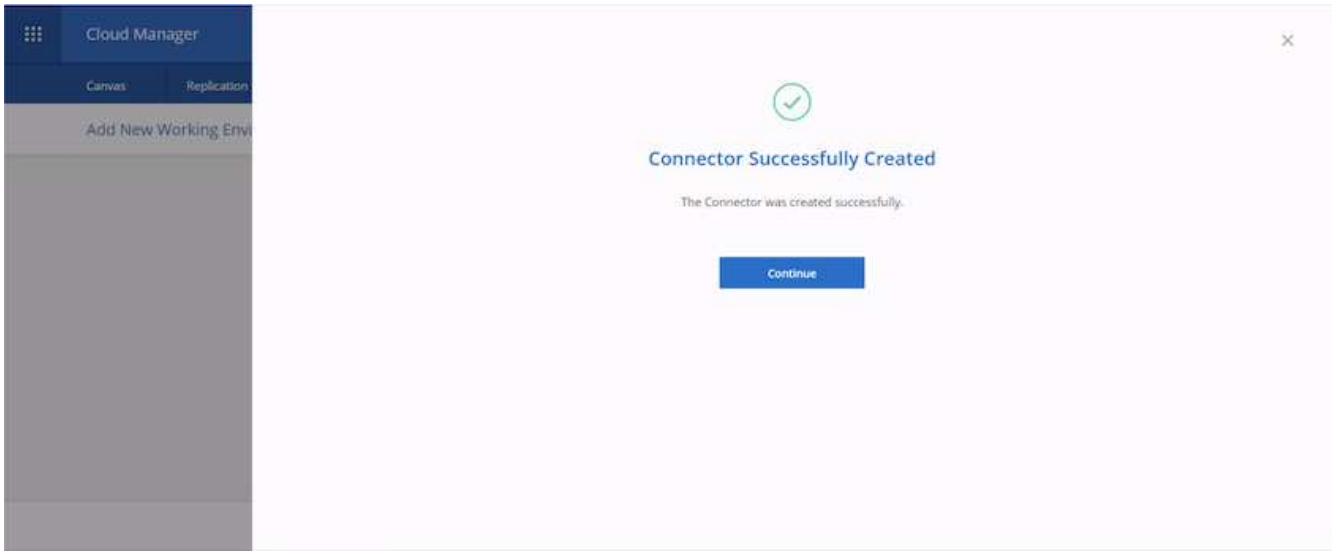
10. Überprüfen Sie die Informationen auf der Übersichtsseite und klicken Sie auf „Hinzufügen“, um den Connector bereitzustellen.



11. Der Connector wird jetzt mithilfe eines Cloud-Formation-Stacks bereitgestellt. Sie können den Fortschritt über Cloud Manager oder AWS überwachen.

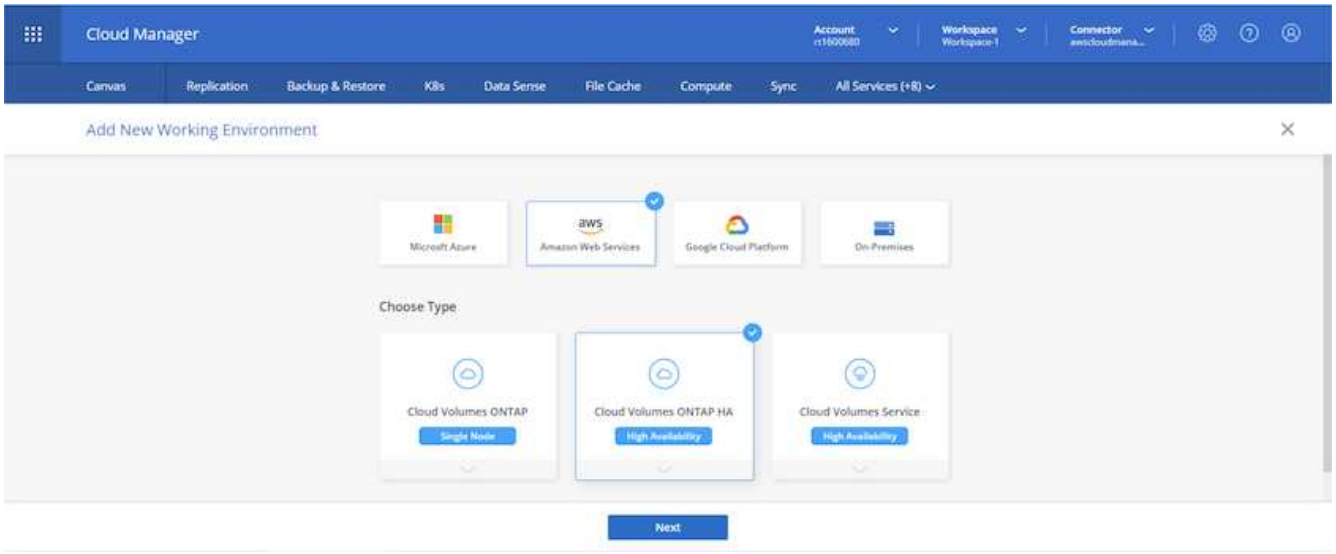


12. Wenn die Bereitstellung abgeschlossen ist, wird eine Erfolgsseite angezeigt.

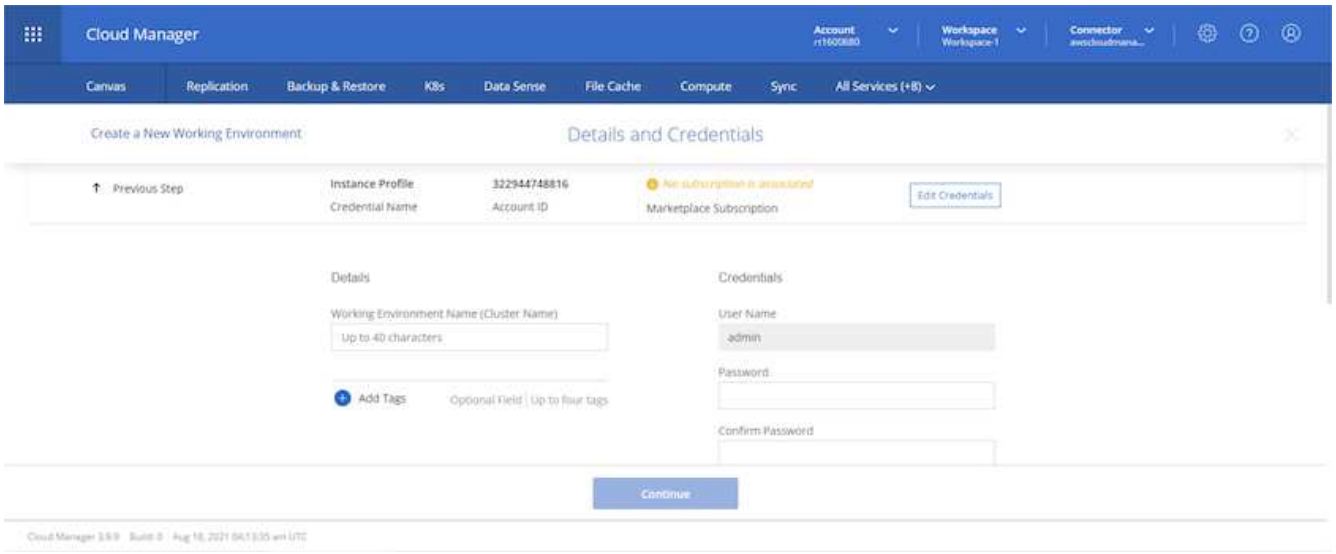


Bereitstellen von Cloud Volumes ONTAP

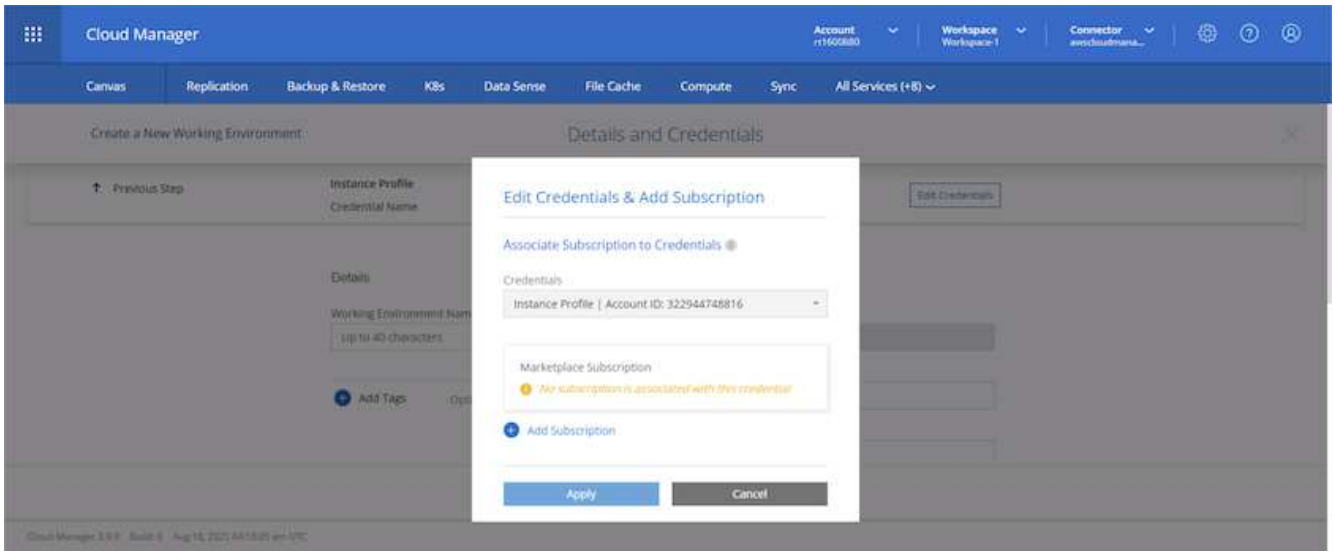
1. Wählen Sie AWS und den Bereitstellungstyp entsprechend Ihren Anforderungen aus.



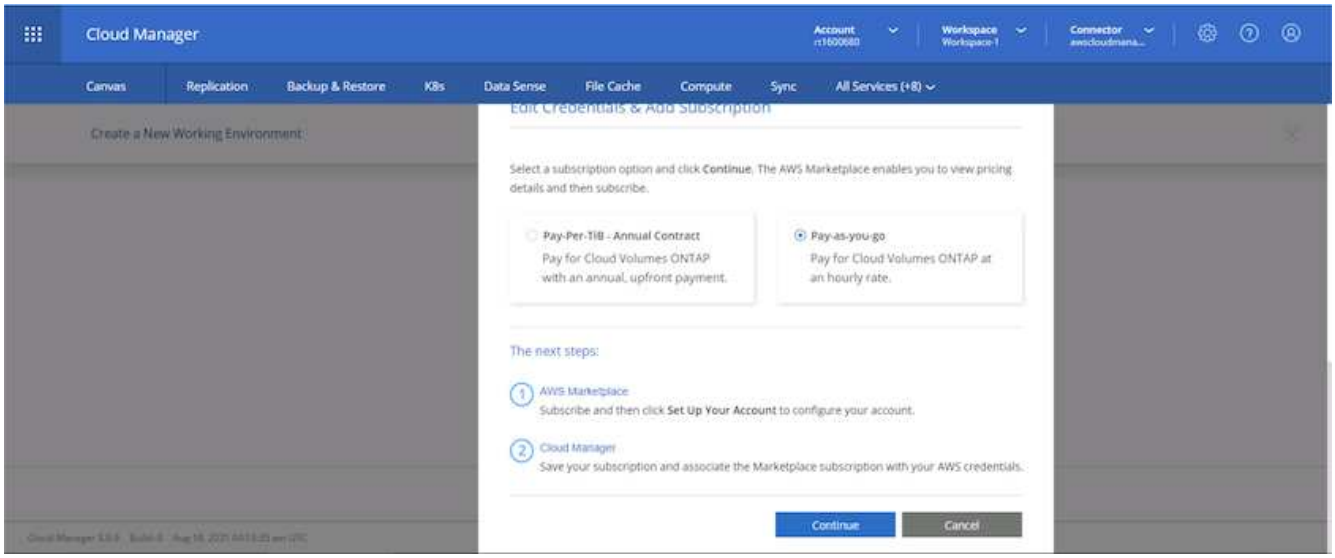
2. Wenn kein Abonnement zugewiesen wurde und Sie mit PAYGO kaufen möchten, wählen Sie „Anmeldeinformationen bearbeiten“.



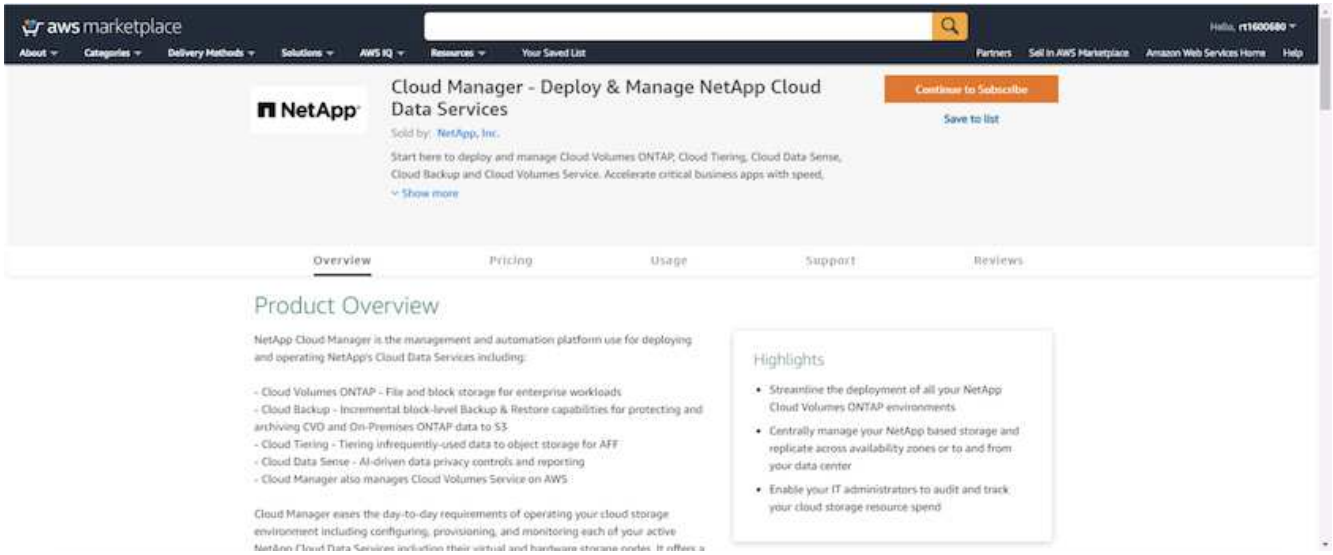
3. Wählen Sie Abonnement hinzufügen.



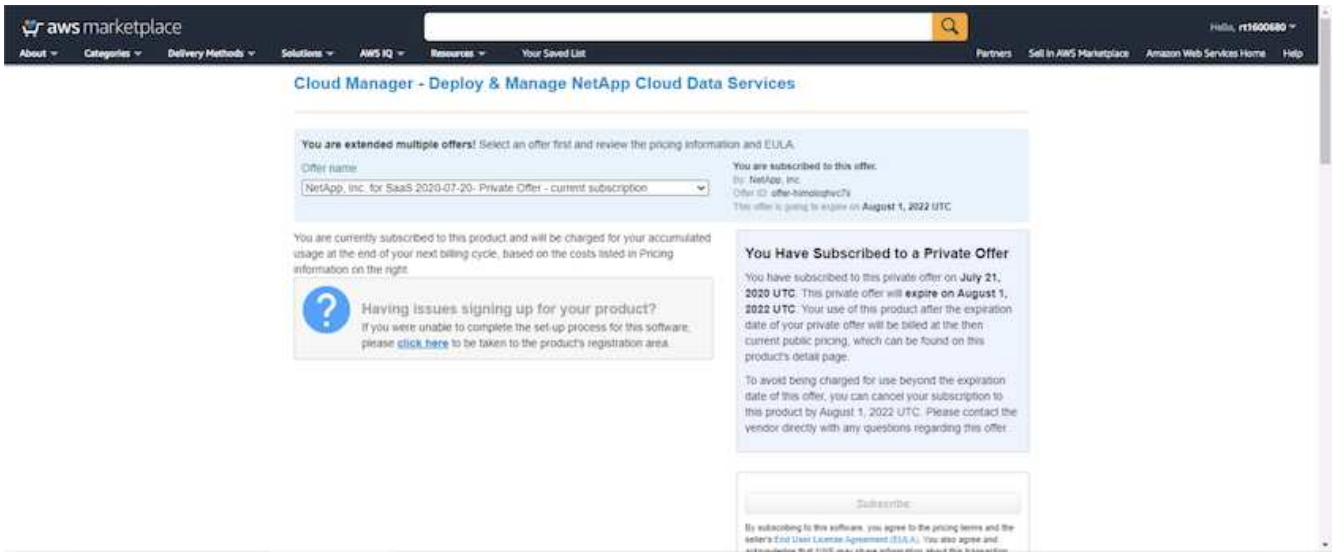
4. Wählen Sie die Art des Vertrags, den Sie abonnieren möchten. Ich habe mich für Pay-as-you-go entschieden.



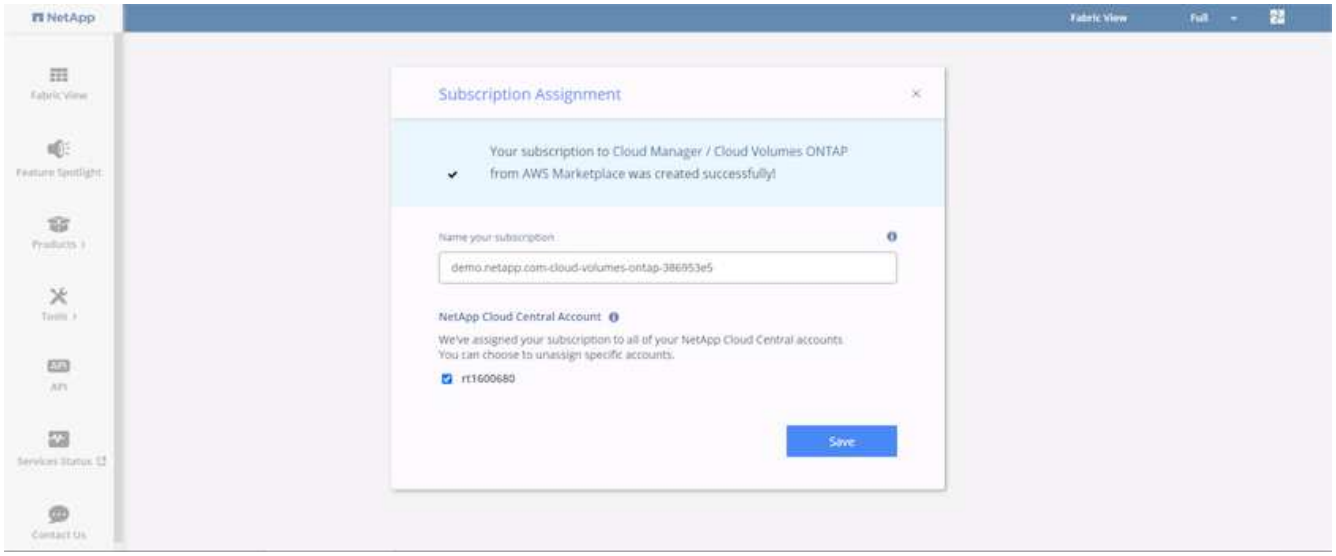
5. Sie werden zu AWS weitergeleitet. Wählen Sie „Weiter zum Abonnieren“ aus.



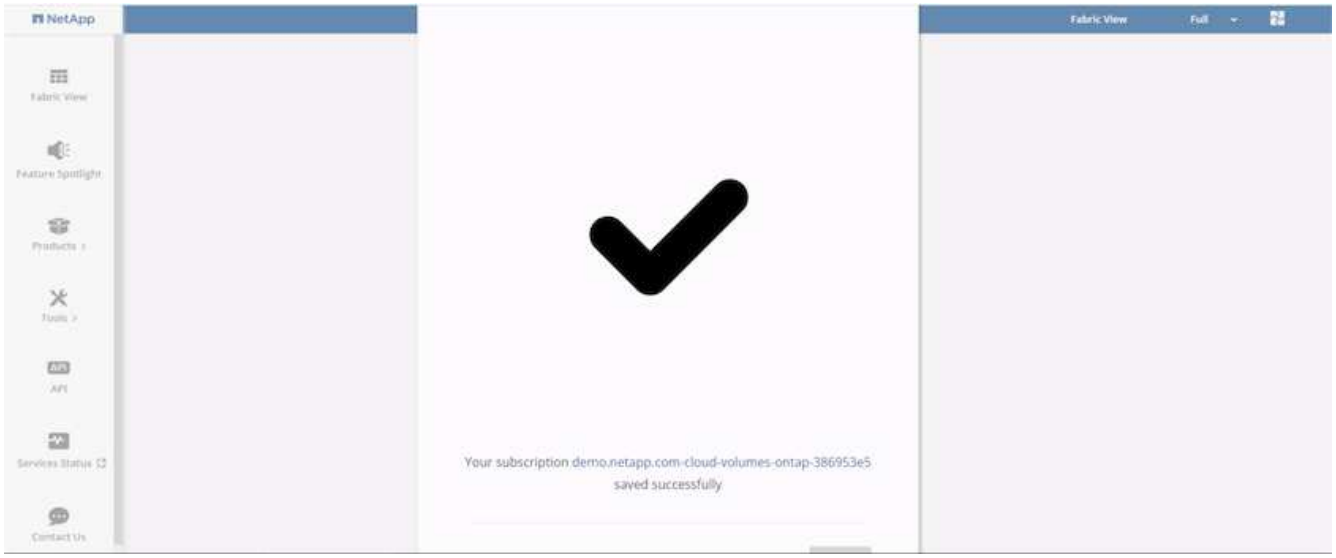
6. Abonnieren Sie und Sie werden zurück zu NetApp Cloud Central weitergeleitet. Wenn Sie bereits abonniert haben und nicht weitergeleitet werden, wählen Sie den Link „Hier klicken“.



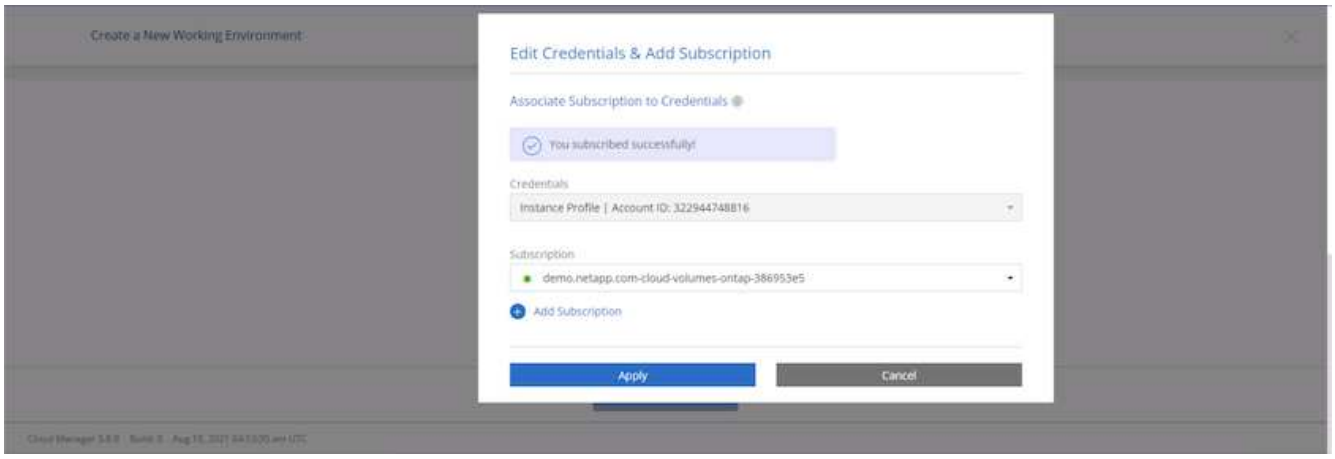
7. Sie werden zu Cloud Central weitergeleitet, wo Sie Ihrem Abonnement einen Namen geben und es Ihrem Cloud Central-Konto zuordnen müssen.



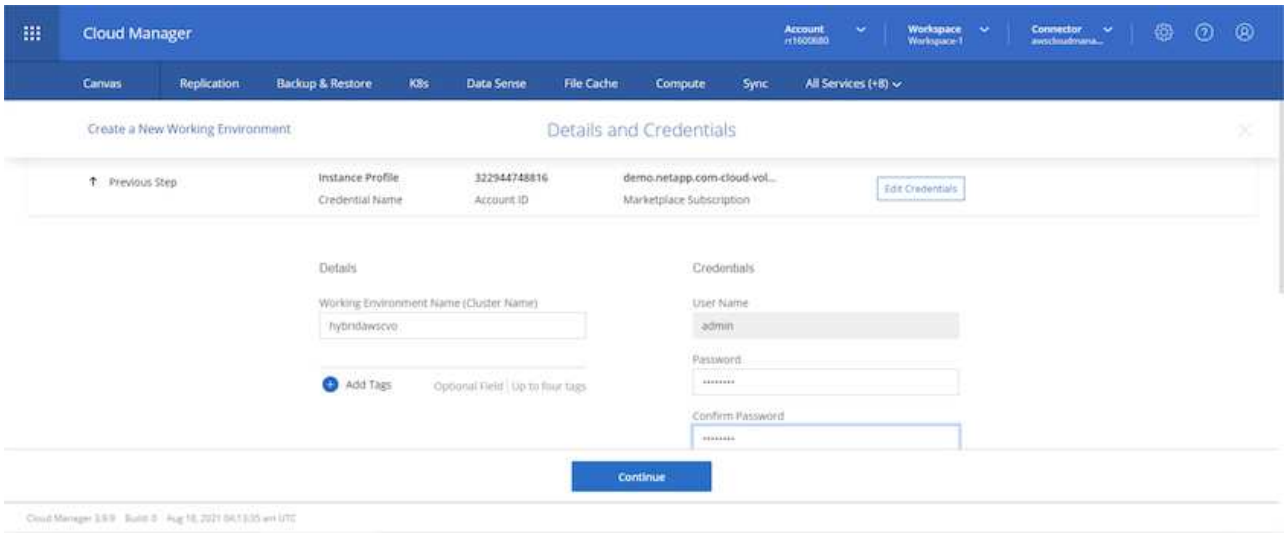
8. Bei erfolgreichem Abschluss wird eine Seite mit einem Häkchen angezeigt. Navigieren Sie zurück zu Ihrer Registerkarte „Cloud Manager“.



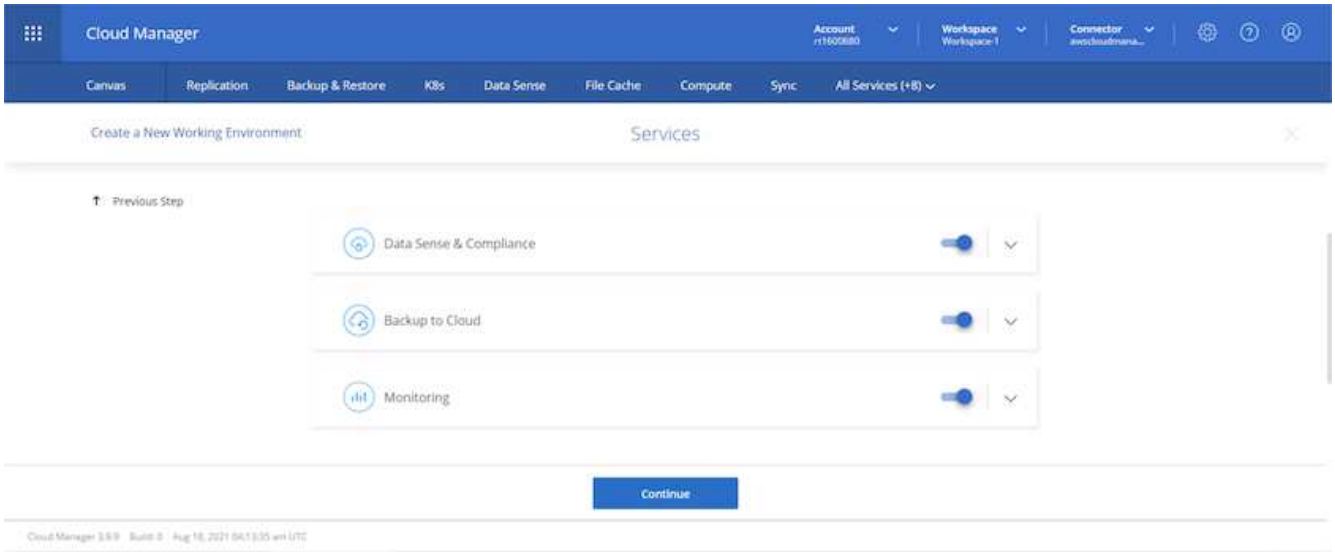
9. Das Abonnement wird jetzt in Cloud Central angezeigt. Klicken Sie auf „Übernehmen“, um fortzufahren.



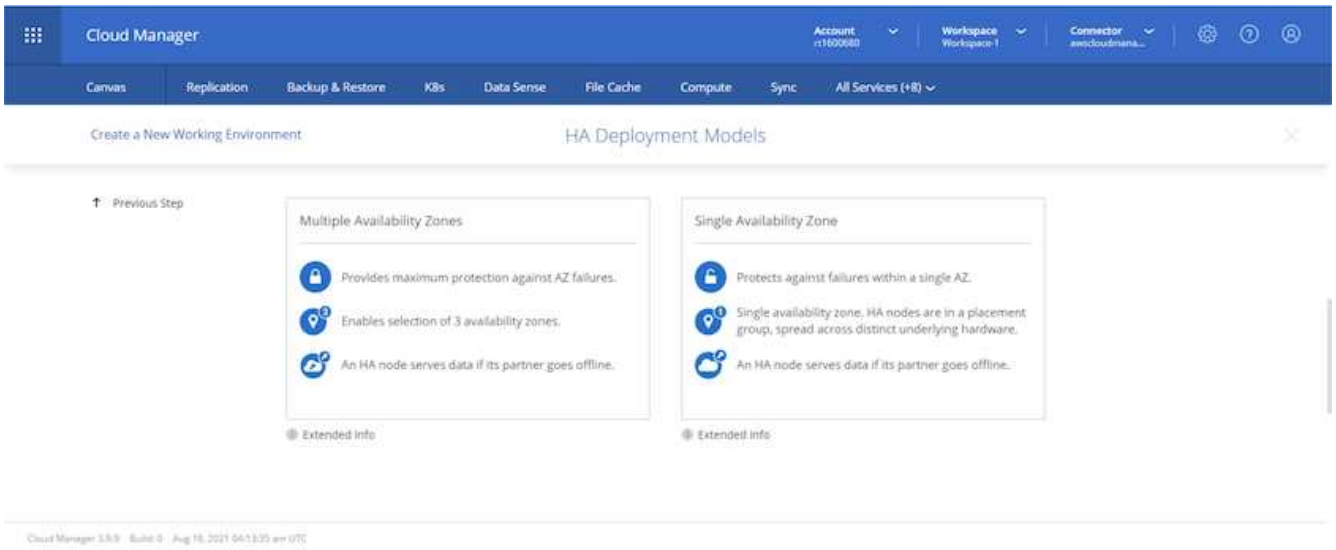
10. Geben Sie die Details der Arbeitsumgebung ein, beispielsweise:
    a. Clustername
    b. Clusterkennwort
    c. AWS-Tags (optional)



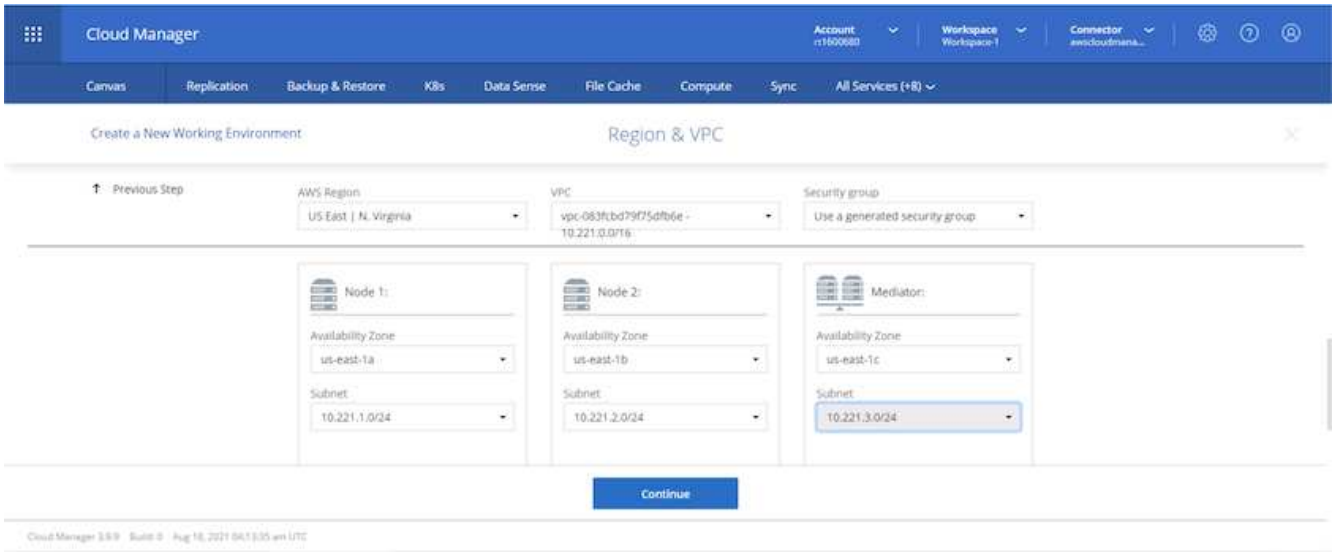
11. Wählen Sie aus, welche zusätzlichen Dienste Sie bereitstellen möchten. Um mehr über diese Dienste zu erfahren, besuchen Sie die "BlueXP: Moderne Datenverwaltung leicht gemacht" .



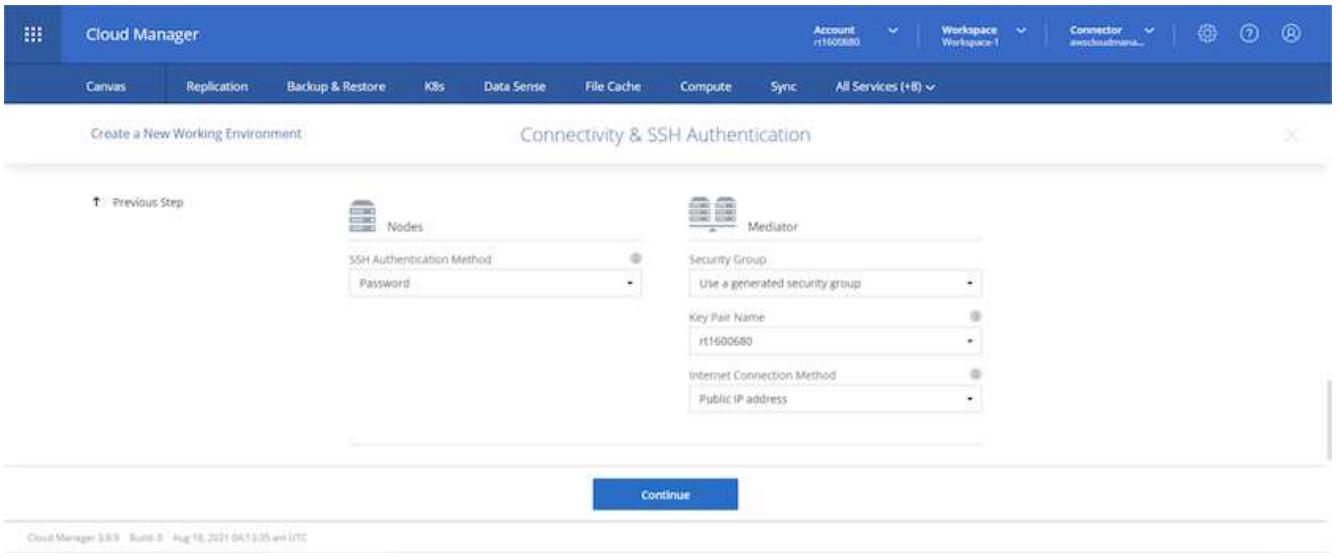
12. Wählen Sie, ob die Bereitstellung in mehreren Verfügbarkeitszonen (erfordert drei Subnetze, jedes in einer anderen AZ) oder in einer einzigen Verfügbarkeitszone erfolgen soll. Ich habe mehrere AZs ausgewählt.



13. Wählen Sie die Region, VPC und Sicherheitsgruppe für den Cluster aus, in dem er bereitgestellt werden soll. In diesem Abschnitt weisen Sie auch die Verfügbarkeitszonen pro Knoten (und Mediator) sowie die von ihnen belegten Subnetze zu.

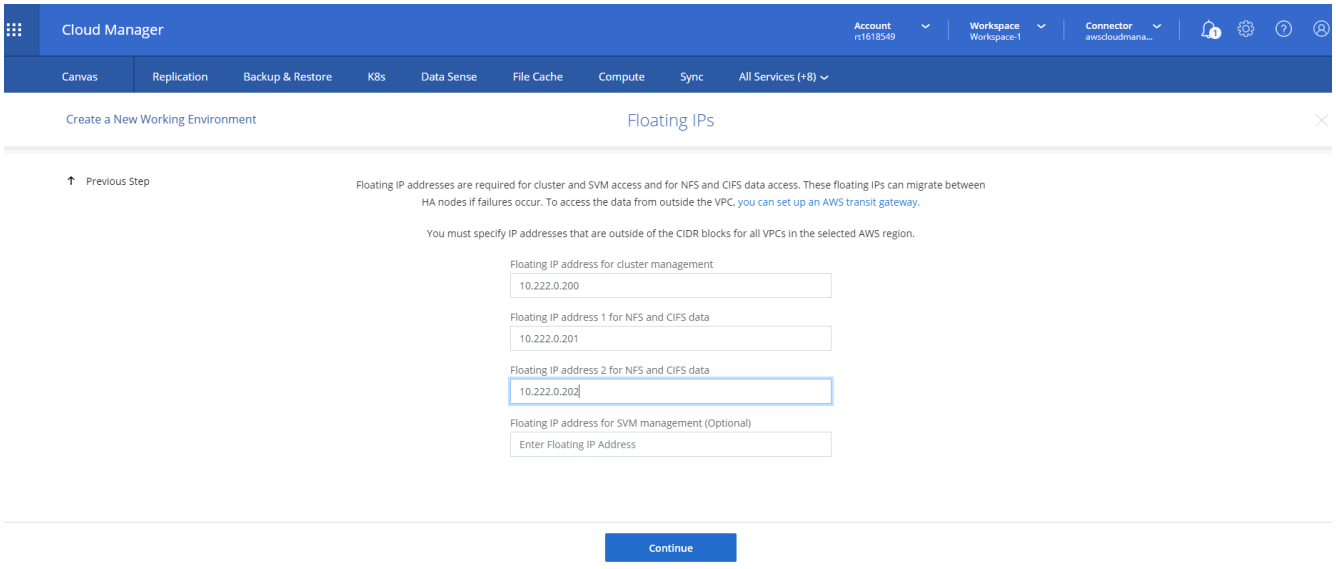


14. Wählen Sie die Verbindungsmethoden für die Knoten sowie den Mediator.

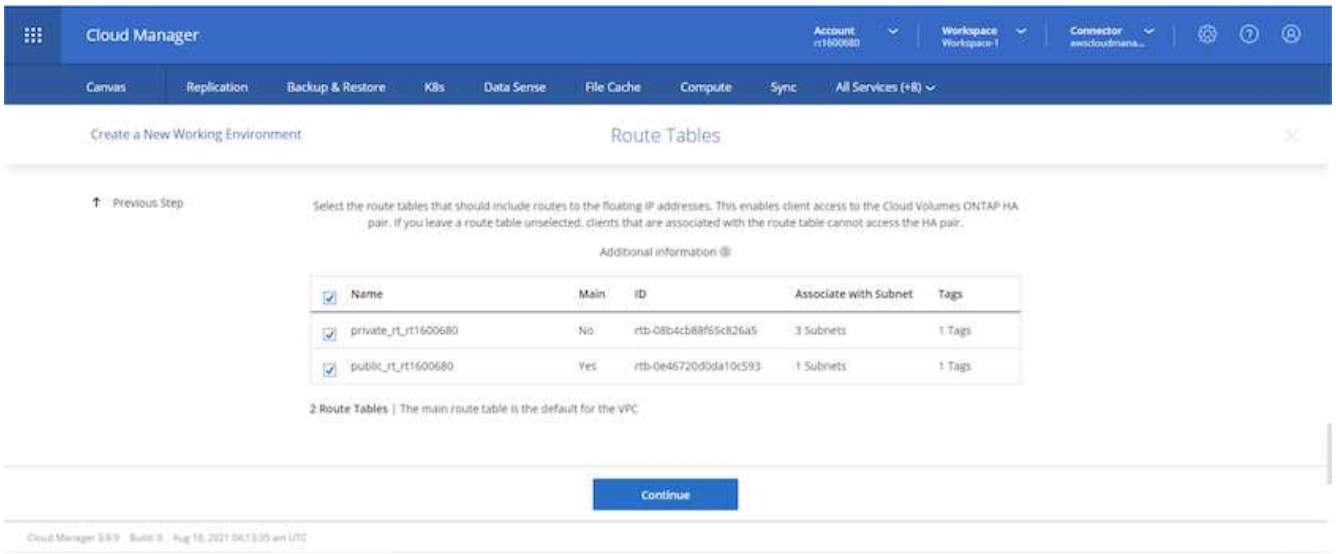


Der Mediator erfordert die Kommunikation mit den AWS-APIs. Eine öffentliche IP-Adresse ist nicht erforderlich, solange die APIs nach der Bereitstellung der Mediator-EC2-Instanz erreichbar sind.

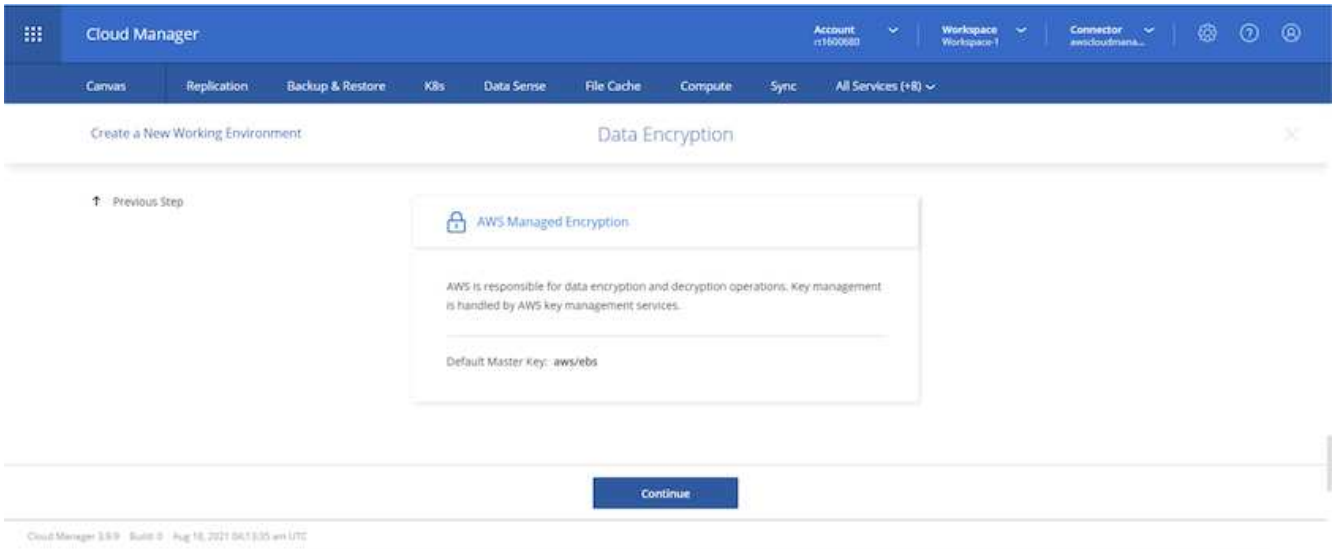
1. Floating-IP-Adressen werden verwendet, um den Zugriff auf die verschiedenen IP-Adressen zu ermöglichen, die Cloud Volumes ONTAP verwendet, einschließlich Cluster-Management und Datenbereitstellungs-IPs. Dabei muss es sich um Adressen handeln, die in Ihrem Netzwerk noch nicht geroutet werden können und zu Routentabellen in Ihrer AWS-Umgebung hinzugefügt werden. Diese sind erforderlich, um während des Failovers konsistente IP-Adressen für ein HA-Paar zu aktivieren. Weitere Informationen zu Floating IP-Adressen finden Sie in der "NetApp Cloud-Dokumentation" .



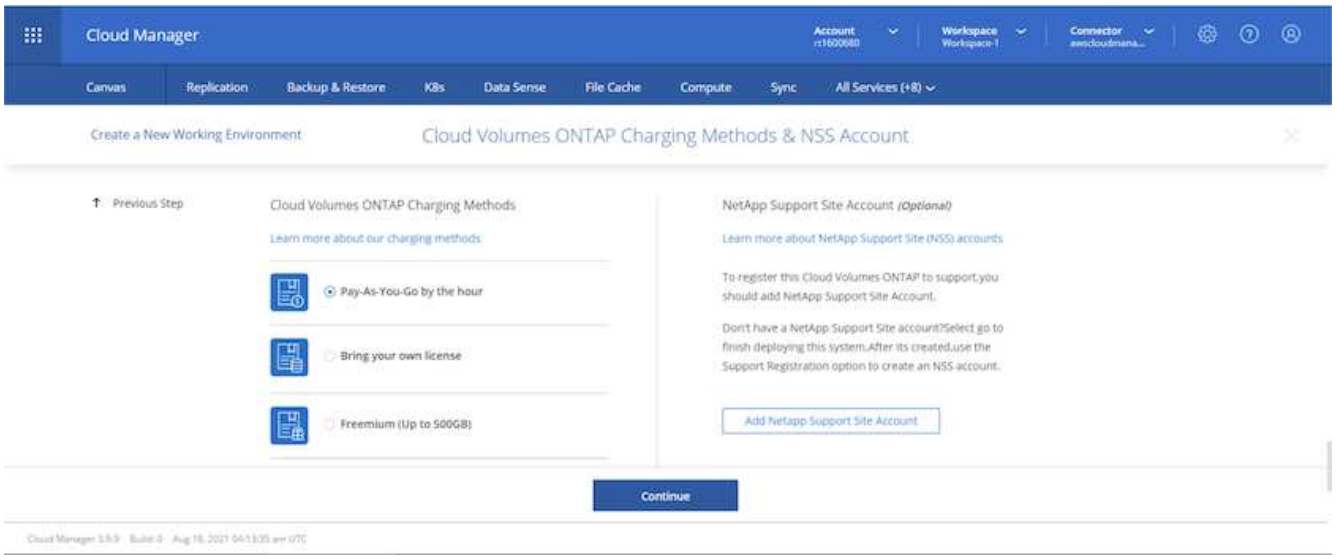
2. Wählen Sie aus, zu welchen Routentabellen die Floating-IP-Adressen hinzugefügt werden. Diese Routentabellen werden von Clients zur Kommunikation mit Cloud Volumes ONTAP verwendet.



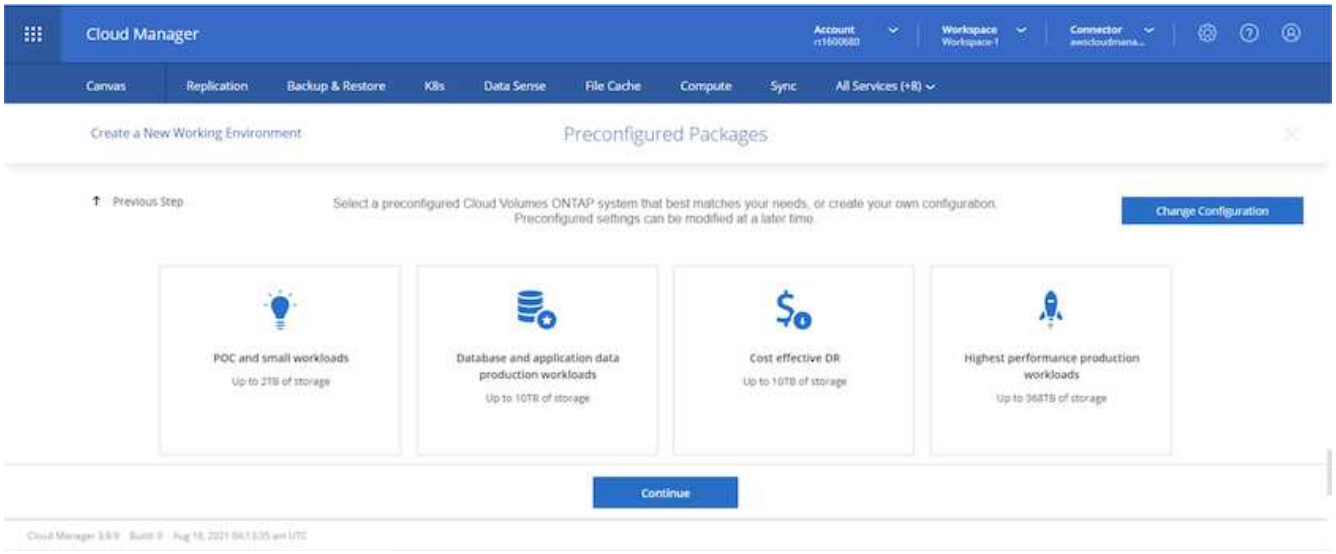
3. Wählen Sie, ob Sie die von AWS verwaltete Verschlüsselung oder AWS KMS aktivieren möchten, um die ONTAP -Root-, Boot- und Datenfestplatten zu verschlüsseln.



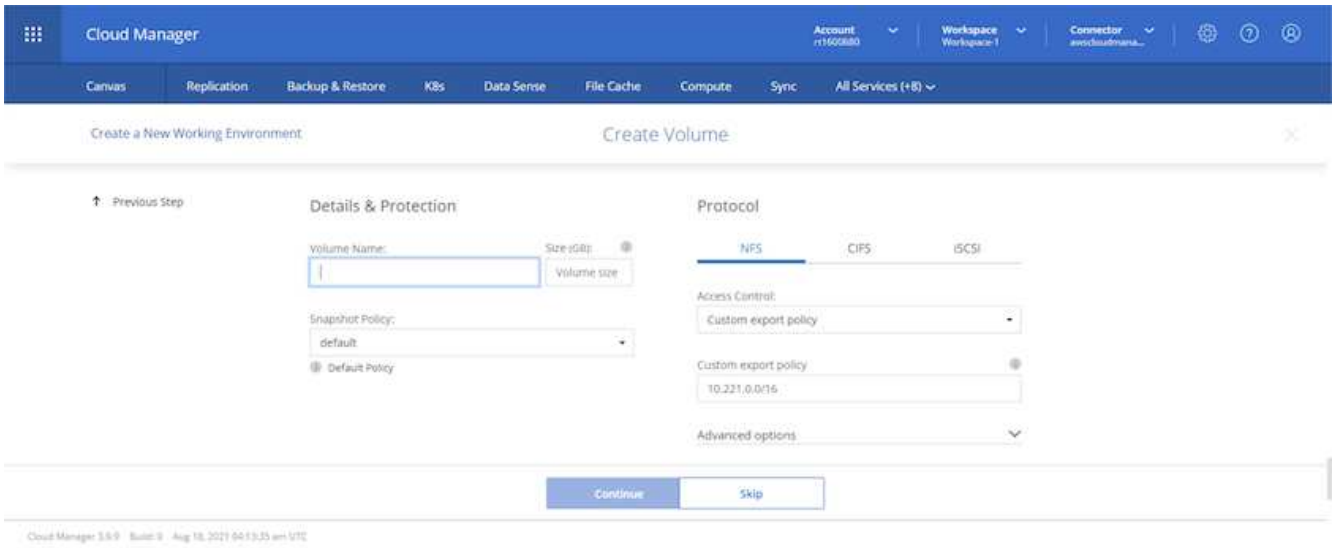
4. Wählen Sie Ihr Lizenzmodell. Wenn Sie nicht wissen, welche Option Sie wählen sollen, wenden Sie sich an Ihren NetApp Vertreter.



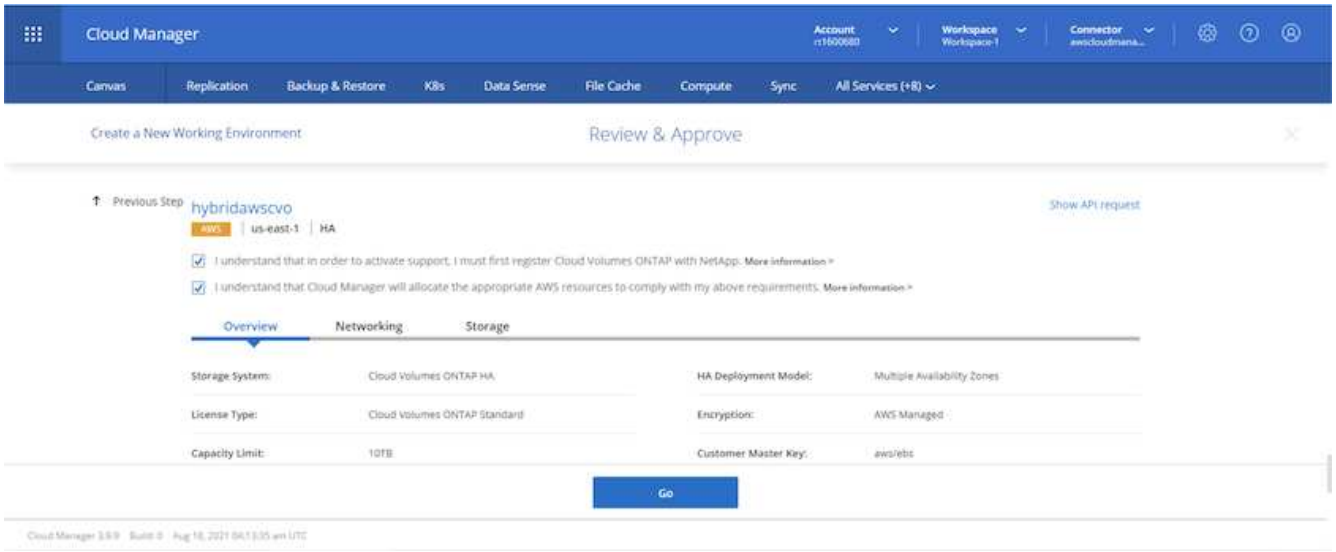
5. Wählen Sie die Konfiguration aus, die am besten zu Ihrem Anwendungsfall passt. Dies hängt mit den Größenüberlegungen zusammen, die auf der Seite mit den Voraussetzungen behandelt werden.



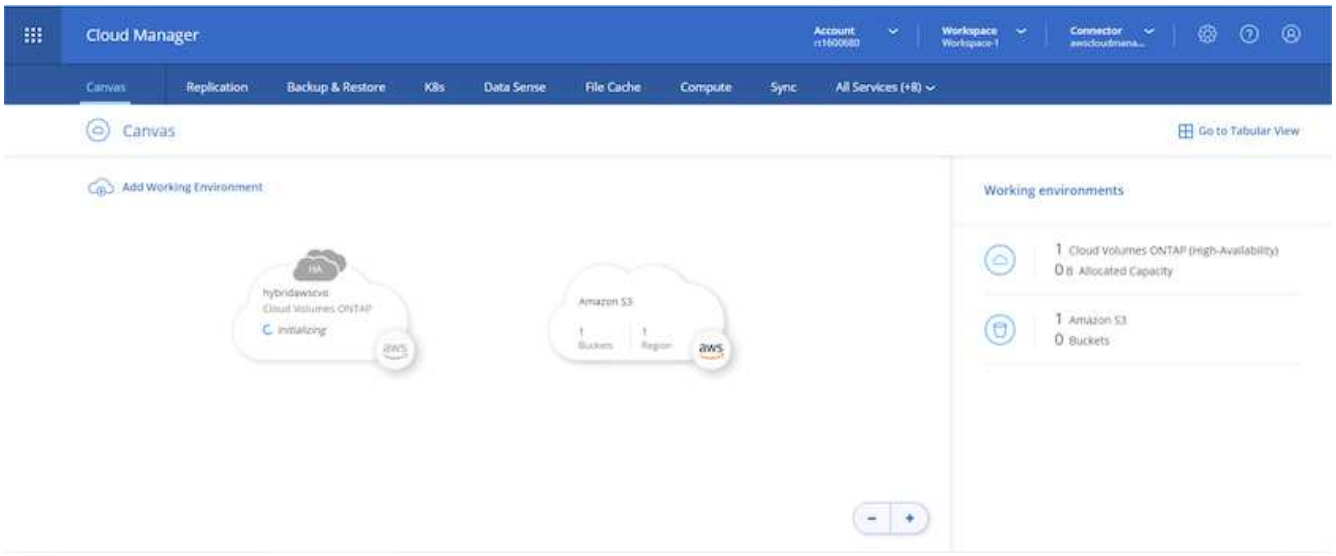
6. Erstellen Sie optional ein Volume. Dies ist nicht erforderlich, da in den nächsten Schritten SnapMirror verwendet wird, das die Volumes für uns erstellt.



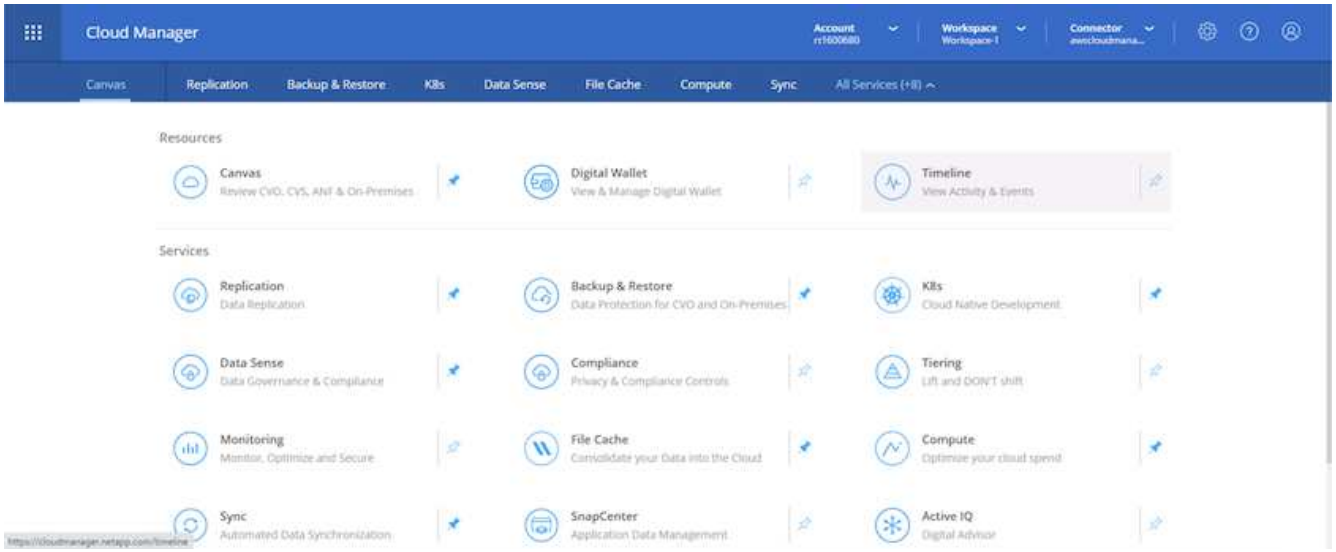
7. Überprüfen Sie die getroffene Auswahl und aktivieren Sie die Kontrollkästchen, um zu bestätigen, dass Sie verstehen, dass Cloud Manager Ressourcen in Ihrer AWS-Umgebung bereitstellt. Wenn Sie fertig sind, klicken Sie auf „Los“.



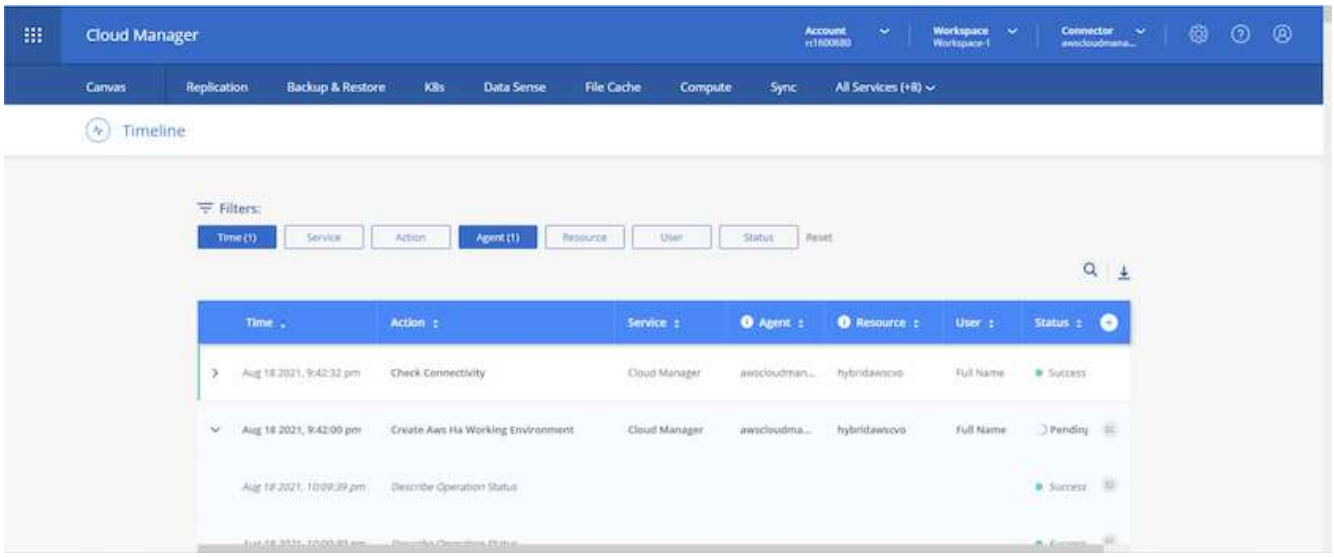
8. Cloud Volumes ONTAP startet jetzt seinen Bereitstellungsprozess. Cloud Manager verwendet AWS-APIs und Cloud-Formationsstapel, um Cloud Volumes ONTAP bereitzustellen. Anschließend wird das System gemäß Ihren Vorgaben konfiguriert, sodass Sie ein sofort einsatzbereites System erhalten, das Sie sofort nutzen können. Der Zeitrahmen für diesen Vorgang variiert je nach getroffener Auswahl.



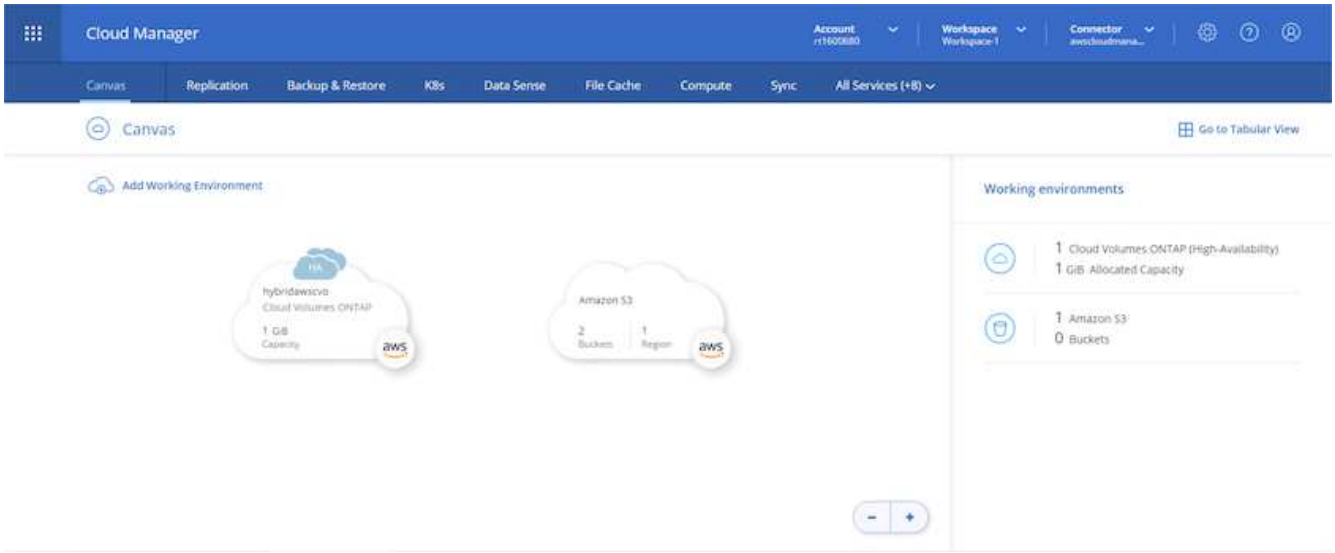
9. Sie können den Fortschritt überwachen, indem Sie zur Zeitleiste navigieren.



10. Die Zeitleiste dient als Überprüfung aller im Cloud Manager durchgeführten Aktionen. Sie können alle API-Aufrufe anzeigen, die von Cloud Manager während der Einrichtung sowohl an AWS als auch an den ONTAP Cluster getätigt werden. Dies kann auch effektiv zur Behebung aller auftretenden Probleme verwendet werden.



11. Nach Abschluss der Bereitstellung wird der CVO-Cluster mit der aktuellen Kapazität auf der Leinwand angezeigt. Der ONTAP Cluster ist in seinem aktuellen Zustand vollständig konfiguriert, um ein echtes Out-of-the-Box-Erlebnis zu ermöglichen.

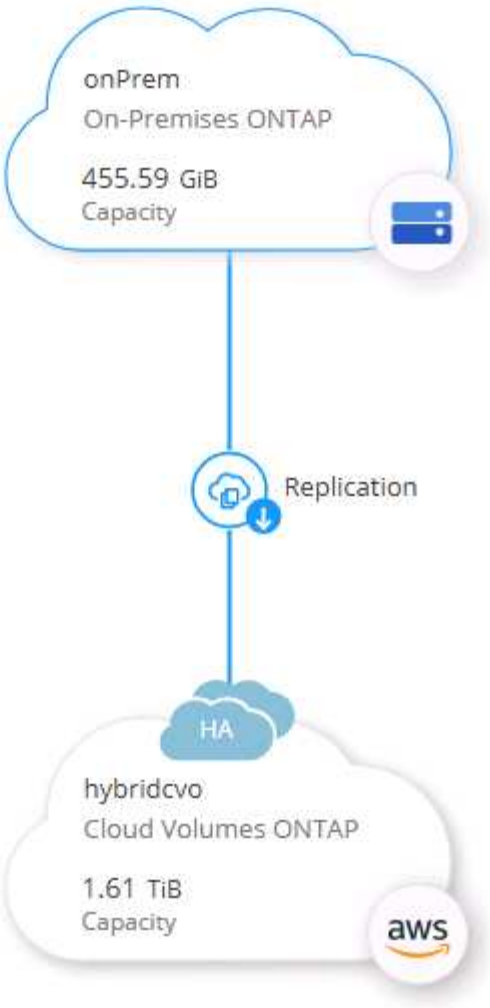


Konfigurieren Sie SnapMirror von On-Premises in die Cloud

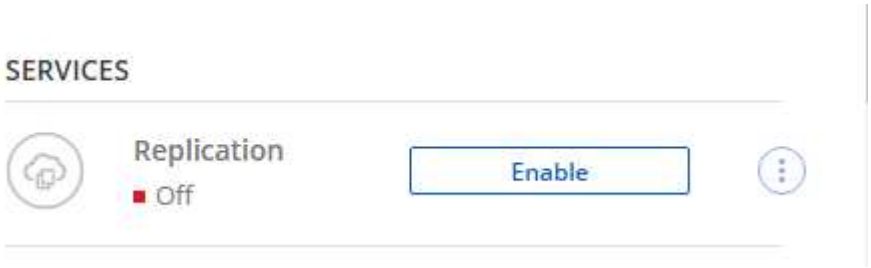
Nachdem Sie nun ein Quell- ONTAP -System und ein Ziel- ONTAP -System bereitgestellt haben, können Sie Volumes mit Datenbankdaten in die Cloud replizieren.

Eine Anleitung zu kompatiblen ONTAP Versionen für SnapMirror finden Sie im "SnapMirror -Kompatibilitätsmatrix" .

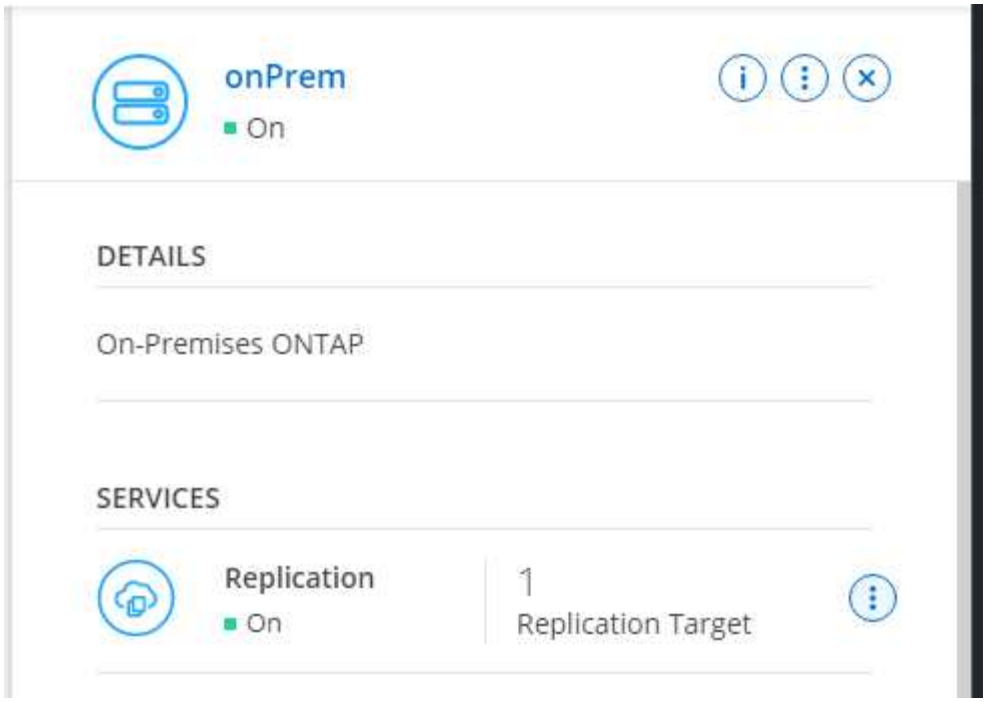
1. Klicken Sie auf das Quell ONTAP -System (vor Ort) und ziehen Sie es per Drag & Drop zum Ziel, wählen Sie Replikation > Aktivieren oder wählen Sie Replikation > Menü > Replizieren.



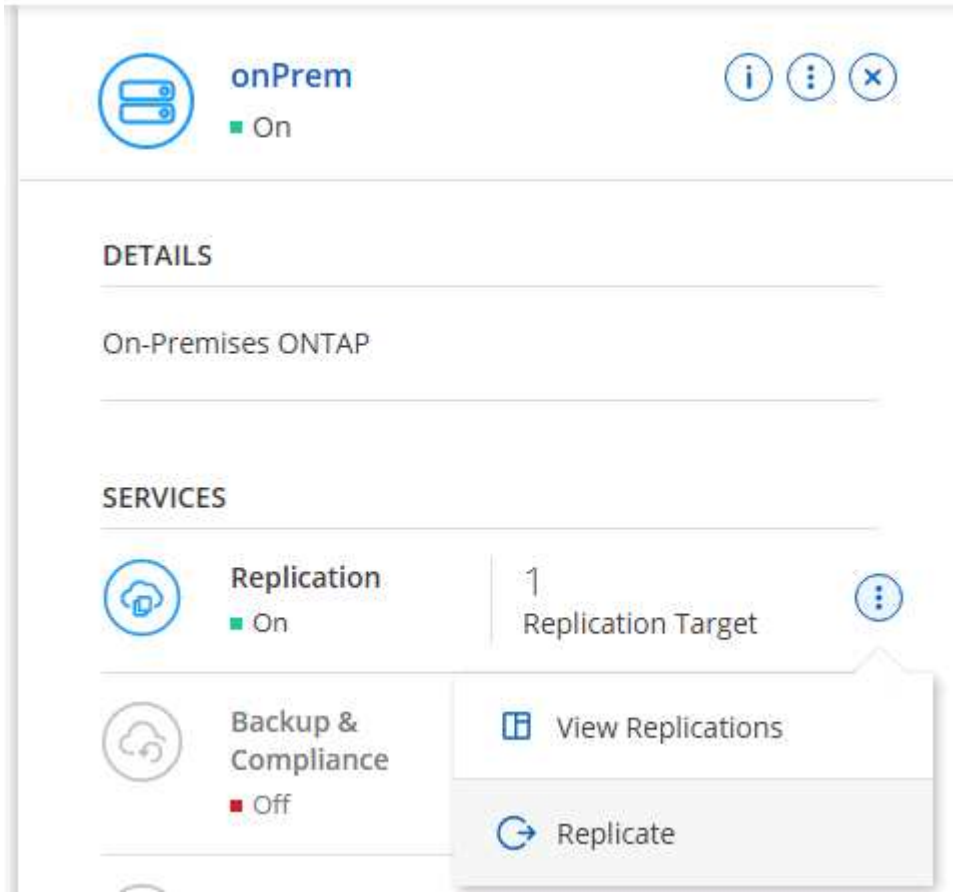
Wählen Sie Aktivieren.



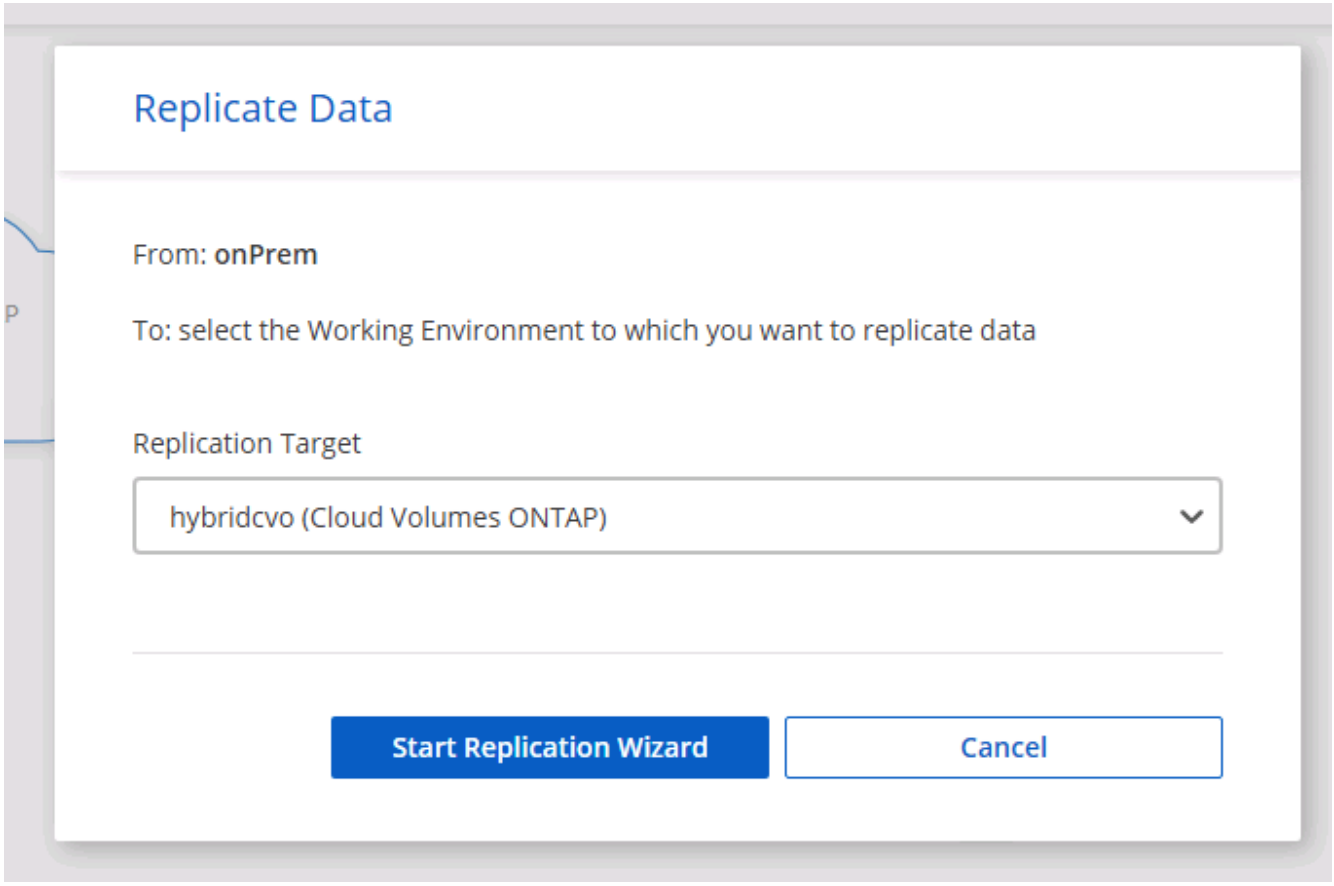
Oder Optionen.



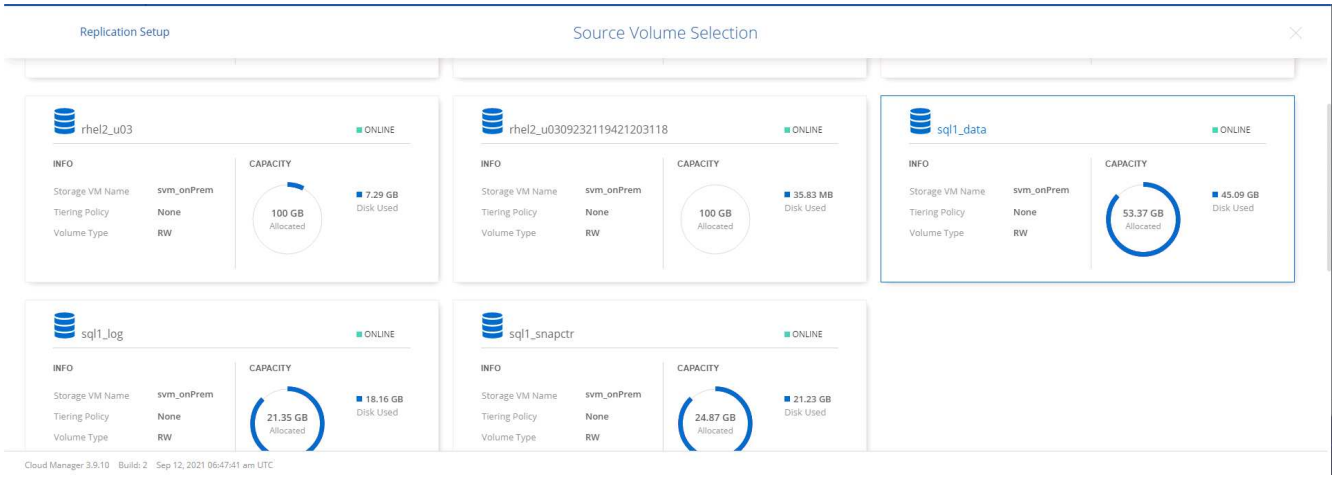
Replizieren.



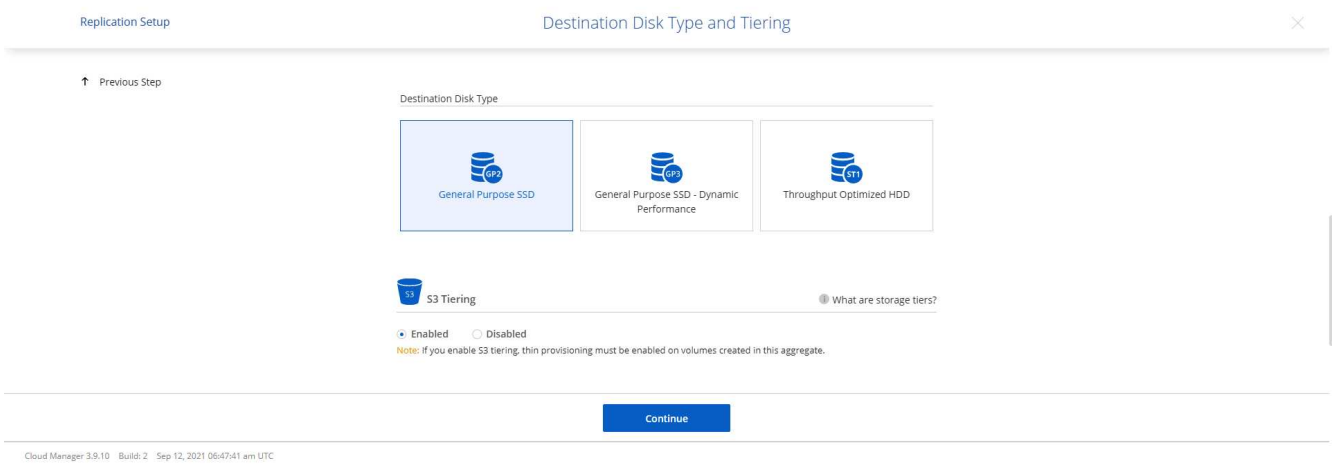
2. Wenn Sie nicht per Drag & Drop verschoben haben, wählen Sie den Zielcluster für die Replikation aus.



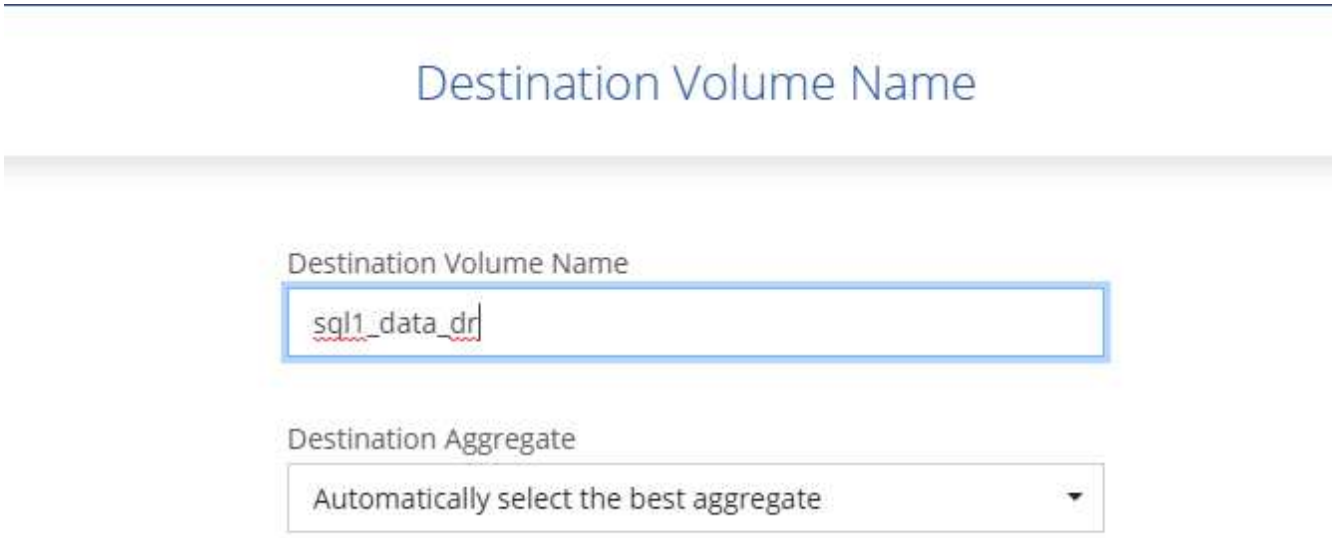
3. Wählen Sie das Volume aus, das Sie replizieren möchten. Wir haben die Daten und alle Protokollvolumes repliziert.



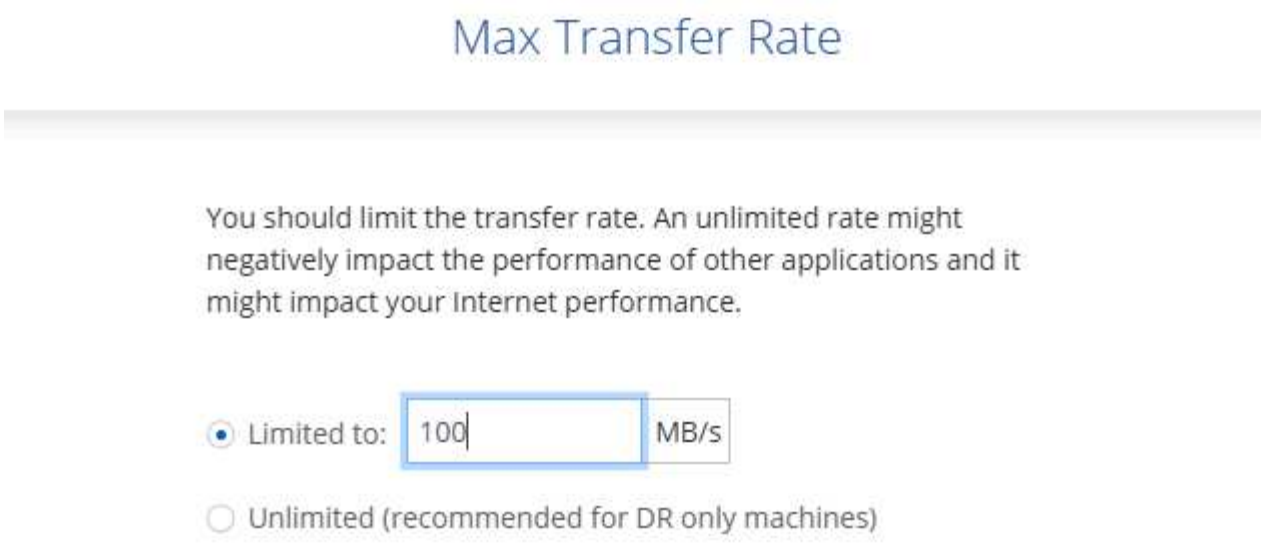
4. Wählen Sie den Zieldatenträgertyp und die Tiering-Richtlinie aus. Für die Notfallwiederherstellung empfehlen wir eine SSD als Datenträgertyp und zur Aufrechterhaltung der Datenschichtung. Durch Data Tiering werden die gespiegelten Daten in kostengünstigen Objektspeicher verschoben, wodurch Sie Geld für lokale Festplatten sparen. Wenn Sie die Beziehung trennen oder das Volume klonen, verwenden die Daten den schnellen, lokalen Speicher.



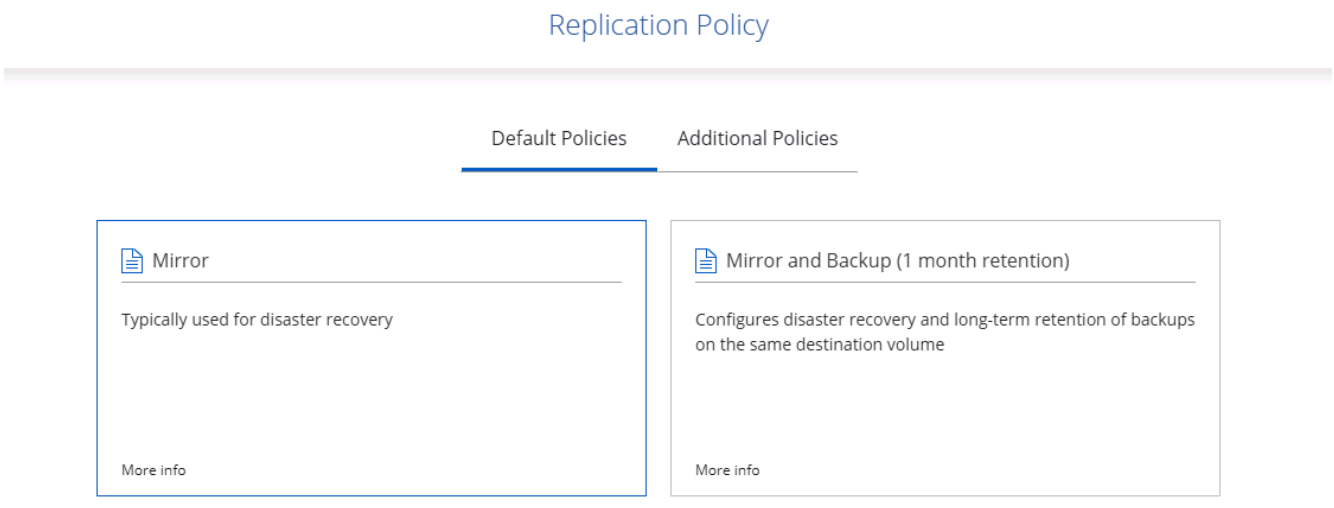
5. Wählen Sie den Namen des Zielvolumes aus: Wir haben gewählt `[source_volume_name]_dr`.



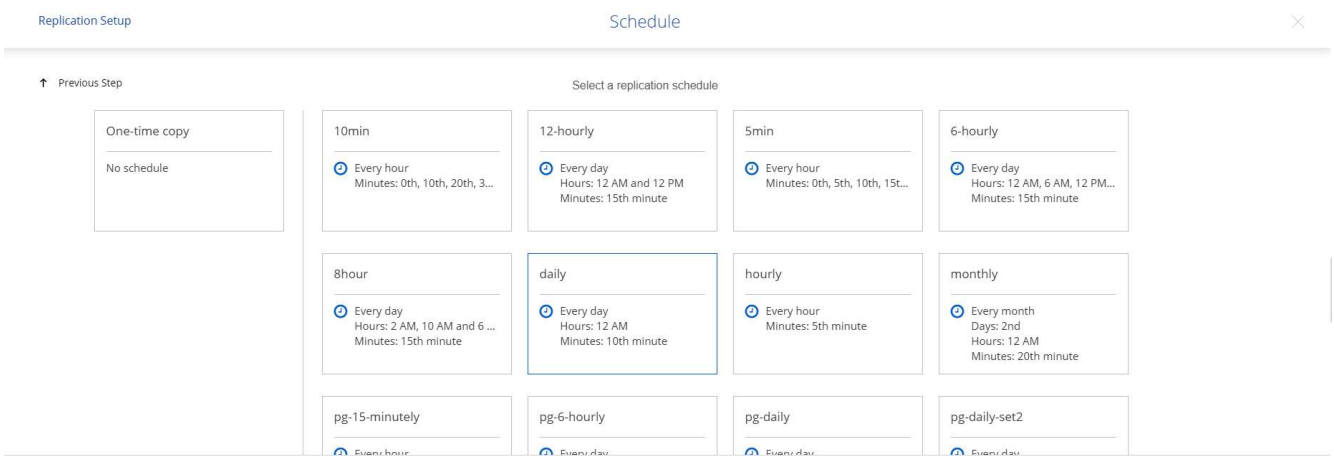
6. Wählen Sie die maximale Übertragungsrate für die Replikation. Dadurch können Sie Bandbreite sparen, wenn Sie über eine Verbindung zur Cloud mit geringer Bandbreite, beispielsweise ein VPN, verfügen.



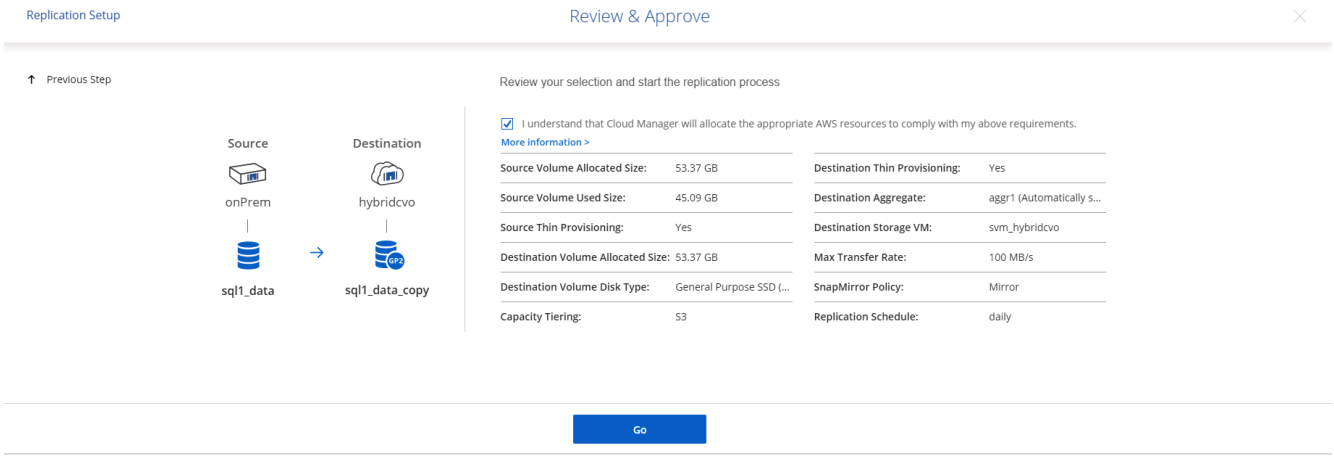
7. Definieren Sie die Replikationsrichtlinie. Wir haben uns für einen Mirror entschieden, der den aktuellsten Datensatz nimmt und diesen auf das Zielvolume repliziert. Sie können je nach Ihren Anforderungen auch eine andere Police wählen.



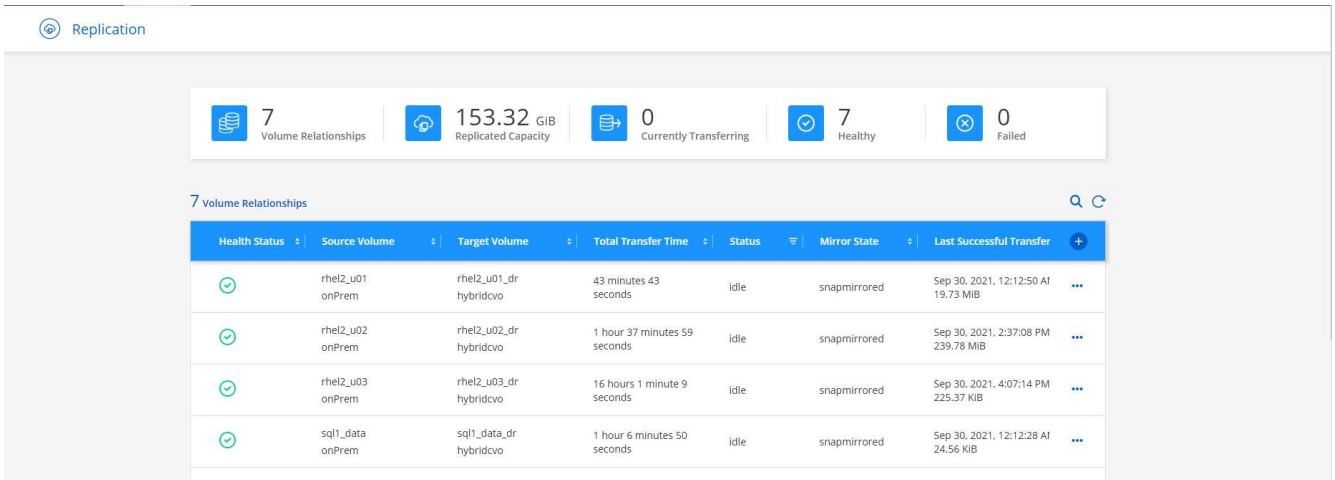
8. Wählen Sie den Zeitplan zum Auslösen der Replikation. NetApp empfiehlt, einen „täglichen“ Zeitplan für das Datenvolumen und einen „stündlichen“ Zeitplan für die Protokollvolumes festzulegen, obwohl dieser je nach Bedarf geändert werden kann.



9. Überprüfen Sie die eingegebenen Informationen, klicken Sie auf „Los“, um den Cluster-Peer und den SVM-Peer auszulösen (wenn Sie zum ersten Mal zwischen den beiden Clustern replizieren), und implementieren und initialisieren Sie dann die SnapMirror Beziehung.



10. Setzen Sie diesen Vorgang für Datenvolumes und Protokollvolumes fort.
11. Um alle Ihre Beziehungen zu überprüfen, navigieren Sie zur Registerkarte „Replikation“ im Cloud Manager. Hier können Sie Ihre Beziehungen verwalten und deren Status überprüfen.



12. Nachdem alle Volumes repliziert wurden, befinden Sie sich in einem stabilen Zustand und sind bereit, mit den Disaster Recovery- und Dev/Test-Workflows fortzufahren.

3. EC2-Compute-Instanz für Datenbank-Workload bereitstellen

AWS verfügt über vorkonfigurierte EC2-Recheninstanzen für verschiedene Workloads. Die Wahl des Instanztyps bestimmt die Anzahl der CPU-Kerne, die Speicherkapazität, den Speichertyp und die Speicherkapazität sowie die Netzwerkleistung. Für die Anwendungsfälle wird der Hauptspeicher zum Ausführen der Datenbank-Workload, mit Ausnahme der Betriebssystempartition, von CVO oder der FSx ONTAP -Speicher-Engine zugewiesen. Daher sind die wichtigsten zu berücksichtigenden Faktoren die Wahl der CPU-Kerne, des Speichers und der Netzwerkleistungsstufe. Typische AWS EC2-Instanztypen finden Sie hier: "EC2-Instanztyp" .

Dimensionierung der Compute-Instanz

1. Wählen Sie den richtigen Instanztyp basierend auf der erforderlichen Arbeitslast aus. Zu den zu berücksichtigenden Faktoren zählen die Anzahl der zu unterstützenden Geschäftstransaktionen, die Anzahl gleichzeitiger Benutzer, die Größe des Datensatzes usw.
2. Die Bereitstellung einer EC2-Instanz kann über das EC2-Dashboard gestartet werden. Die genauen Bereitstellungsverfahren gehen über den Rahmen dieser Lösung hinaus. Sehen "Amazon EC2" für Details.

Linux-Instanzkonfiguration für Oracle-Workload

Dieser Abschnitt enthält zusätzliche Konfigurationsschritte nach der Bereitstellung einer EC2-Linux-Instance.

1. Fügen Sie dem DNS-Server eine Oracle-Standby-Instanz zur Namensauflösung innerhalb der SnapCenter -Verwaltungsdomäne hinzu.
2. Fügen Sie eine Linux-Verwaltungsbenutzer-ID als SnapCenter OS-Anmeldeinformationen mit Sudo-Berechtigungen ohne Kennwort hinzu. Aktivieren Sie die ID mit SSH-Passwortauthentifizierung auf der EC2-Instanz. (Standardmäßig sind die SSH-Passwortauthentifizierung und das passwortlose Sudo auf EC2-Instanzen deaktiviert.)
3. Konfigurieren Sie die Oracle-Installation so, dass sie mit der lokalen Oracle-Installation übereinstimmt, z. B. mit Betriebssystem-Patches, Oracle-Versionen und -Patches usw.
4. NetApp Ansible DB-Automatisierungsrollen können genutzt werden, um EC2-Instanzen für Anwendungsfälle in den Bereichen Datenbankentwicklung/-test und Notfallwiederherstellung zu konfigurieren. Der Automatisierungscode kann von der öffentlichen GitHub-Site von NetApp heruntergeladen werden: "Automatisierte Bereitstellung von Oracle 19c" . Das Ziel besteht darin, einen Datenbanksoftware-Stack auf einer EC2-Instanz zu installieren und zu konfigurieren, um ihn an die lokalen Betriebssystem- und Datenbankkonfigurationen anzupassen.

Windows-Instanzkonfiguration für SQL Server-Workload

In diesem Abschnitt werden zusätzliche Konfigurationsschritte nach der ersten Bereitstellung einer EC2-Windows-Instance aufgeführt.

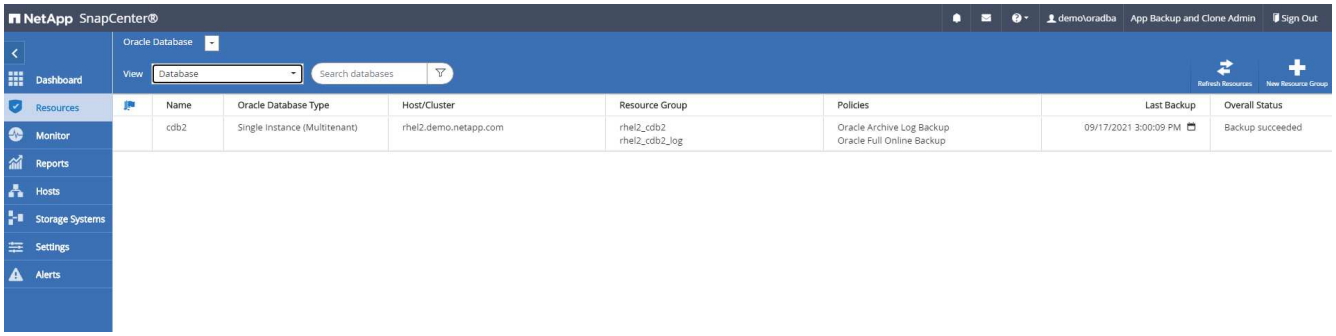
1. Rufen Sie das Windows-Administratorkennwort ab, um sich über RDP bei einer Instanz anzumelden.
2. Deaktivieren Sie die Windows-Firewall, fügen Sie den Host der Windows SnapCenter -Domäne hinzu und fügen Sie die Instanz zur Namensauflösung dem DNS-Server hinzu.
3. Stellen Sie ein SnapCenter -Protokollvolume bereit, um SQL Server-Protokolldateien zu speichern.
4. Konfigurieren Sie iSCSI auf dem Windows-Host, um das Volume zu mounten und das Festplattenlaufwerk zu formatieren.
5. Auch hier können viele der vorherigen Aufgaben mit der NetApp -Automatisierungslösung für SQL Server automatisiert werden. Suchen Sie auf der öffentlichen GitHub-Site zur NetApp Automatisierung nach neu veröffentlichten Rollen und Lösungen: "NetApp Automatisierung" .

Workflow für Dev/Test Bursting in die Cloud

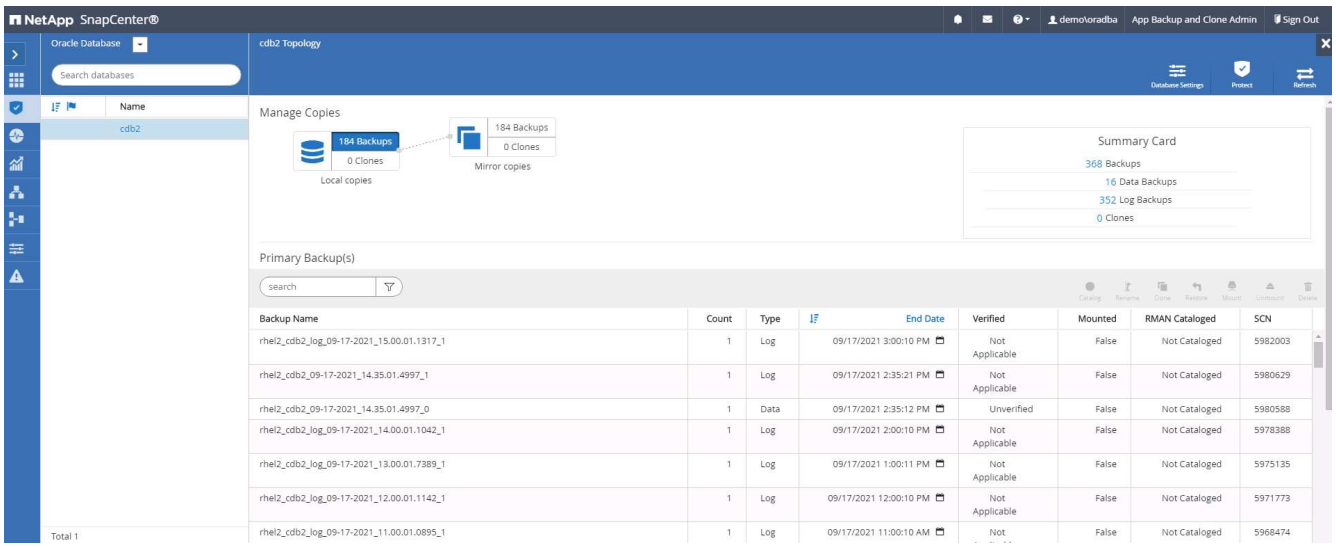
Die Agilität der öffentlichen Cloud, die schnelle Wertschöpfung und die Kosteneinsparungen sind allesamt bedeutende Wertversprechen für Unternehmen, die die öffentliche Cloud für die Entwicklung und das Testen von Datenbankanwendungen nutzen. Um dies zu verwirklichen, gibt es kein besseres Tool als SnapCenter . SnapCenter kann nicht nur Ihre Produktionsdatenbank vor Ort schützen, sondern auch schnell eine Kopie für die Anwendungsentwicklung oder Codetests in der öffentlichen Cloud klonen und verbraucht dabei nur sehr wenig zusätzlichen Speicherplatz. Nachfolgend finden Sie eine schrittweise Anleitung zur Verwendung dieses Tools.

Klonen Sie eine Oracle-Datenbank für Entwicklung/Test aus einer replizierten Snapshot-Sicherung

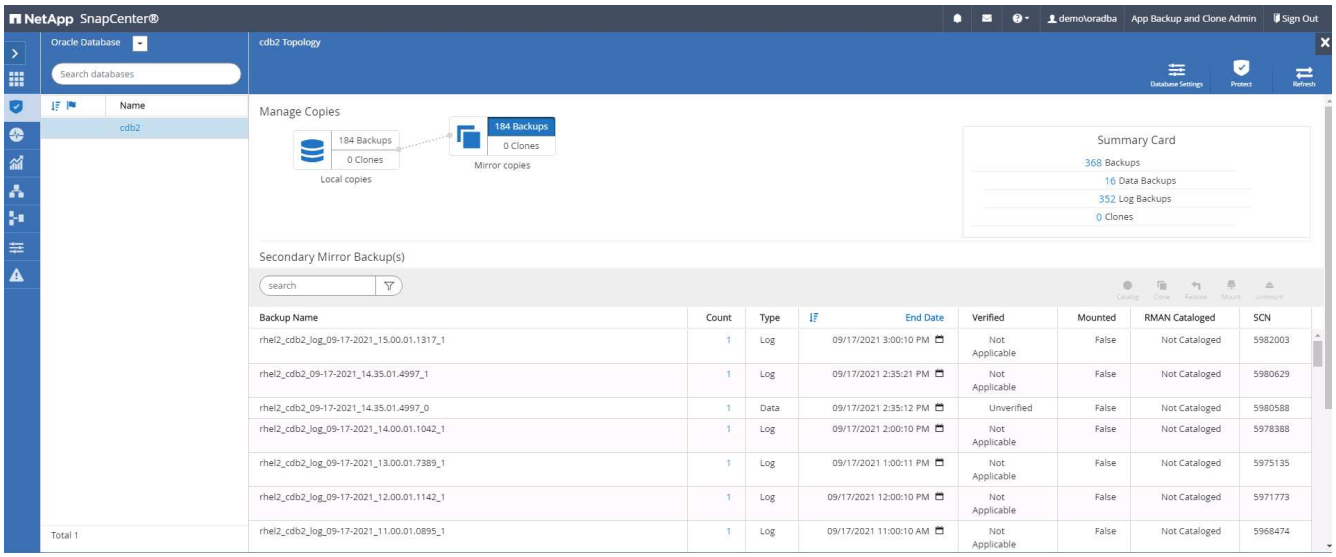
1. Melden Sie sich bei SnapCenter mit einer Datenbankverwaltungs-Benutzer-ID für Oracle an. Navigieren Sie zur Registerkarte „Ressourcen“, auf der die von SnapCenter geschützten Oracle-Datenbanken angezeigt werden.



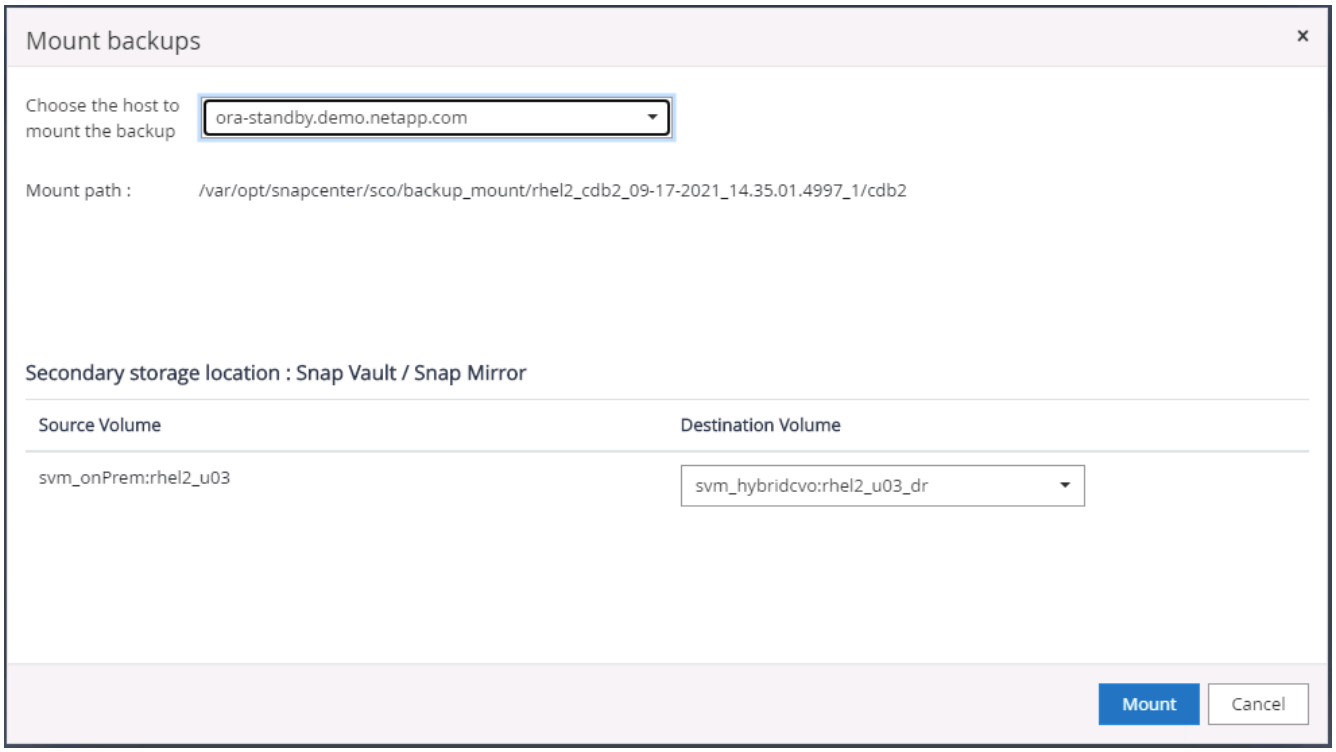
2. Klicken Sie auf den gewünschten lokalen Datenbanknamen für die Sicherungstopologie und die Detailansicht. Wenn ein sekundärer Replikationsstandort aktiviert ist, werden verknüpfte Spiegelsicherungen angezeigt.

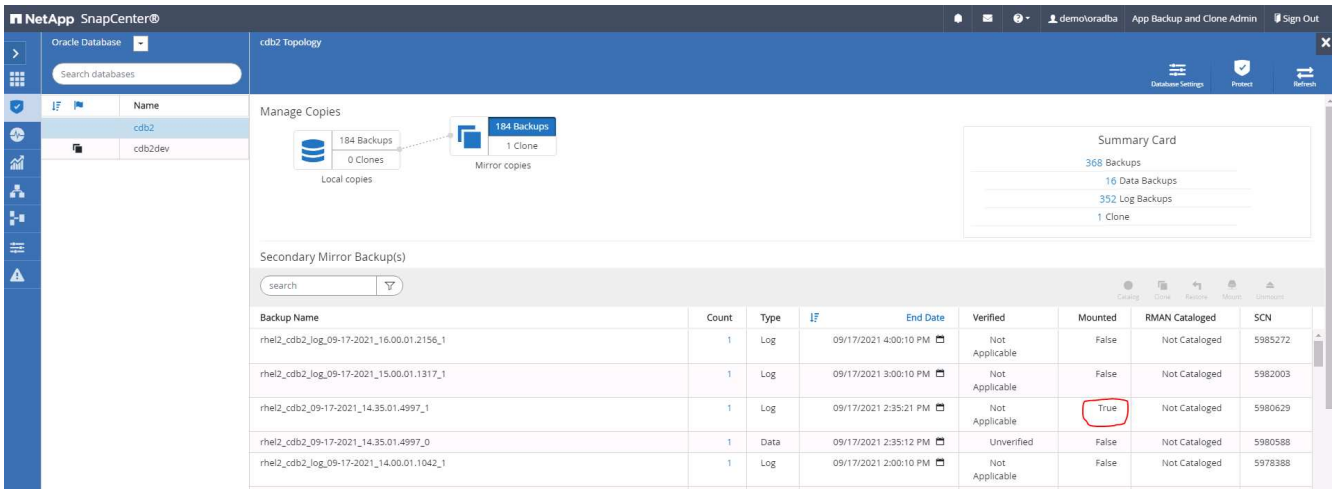


3. Durch Klicken auf „Gespiegelte Backups“ können Sie zur Ansicht „Gespiegelte Backups“ wechseln. Anschließend werden die sekundären Spiegelsicherungen angezeigt.



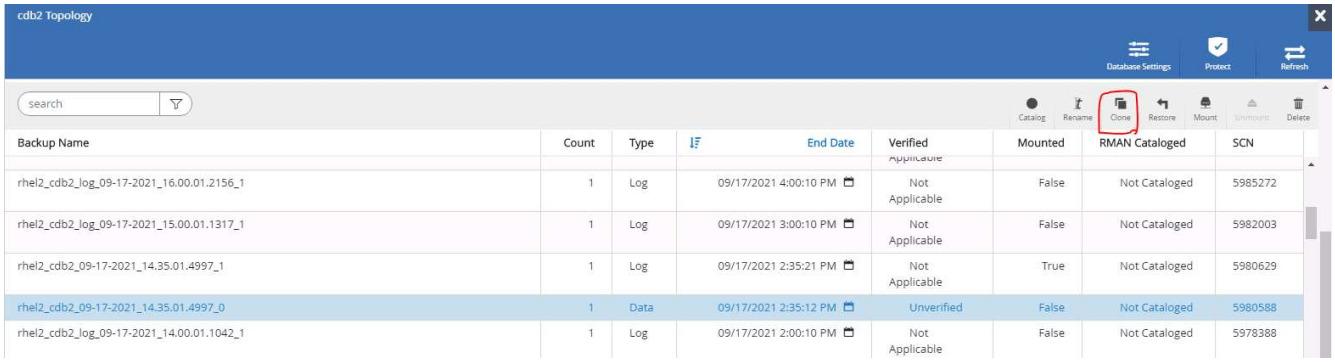
4. Wählen Sie eine gespiegelte sekundäre Datenbanksicherungskopie zum Klonen aus und bestimmen Sie einen Wiederherstellungspunkt entweder nach Zeit und Systemänderungsnummer oder nach SCN. Im Allgemeinen sollte der Wiederherstellungspunkt hinter der vollständigen Datenbanksicherungszeit oder dem zu klonenden SCN liegen. Nachdem ein Wiederherstellungspunkt festgelegt wurde, muss die erforderliche Protokolldateisicherung zur Wiederherstellung bereitgestellt werden. Die Protokolldateisicherung sollte auf dem Ziel-DB-Server bereitgestellt werden, auf dem die Klondatenbank gehostet werden soll.



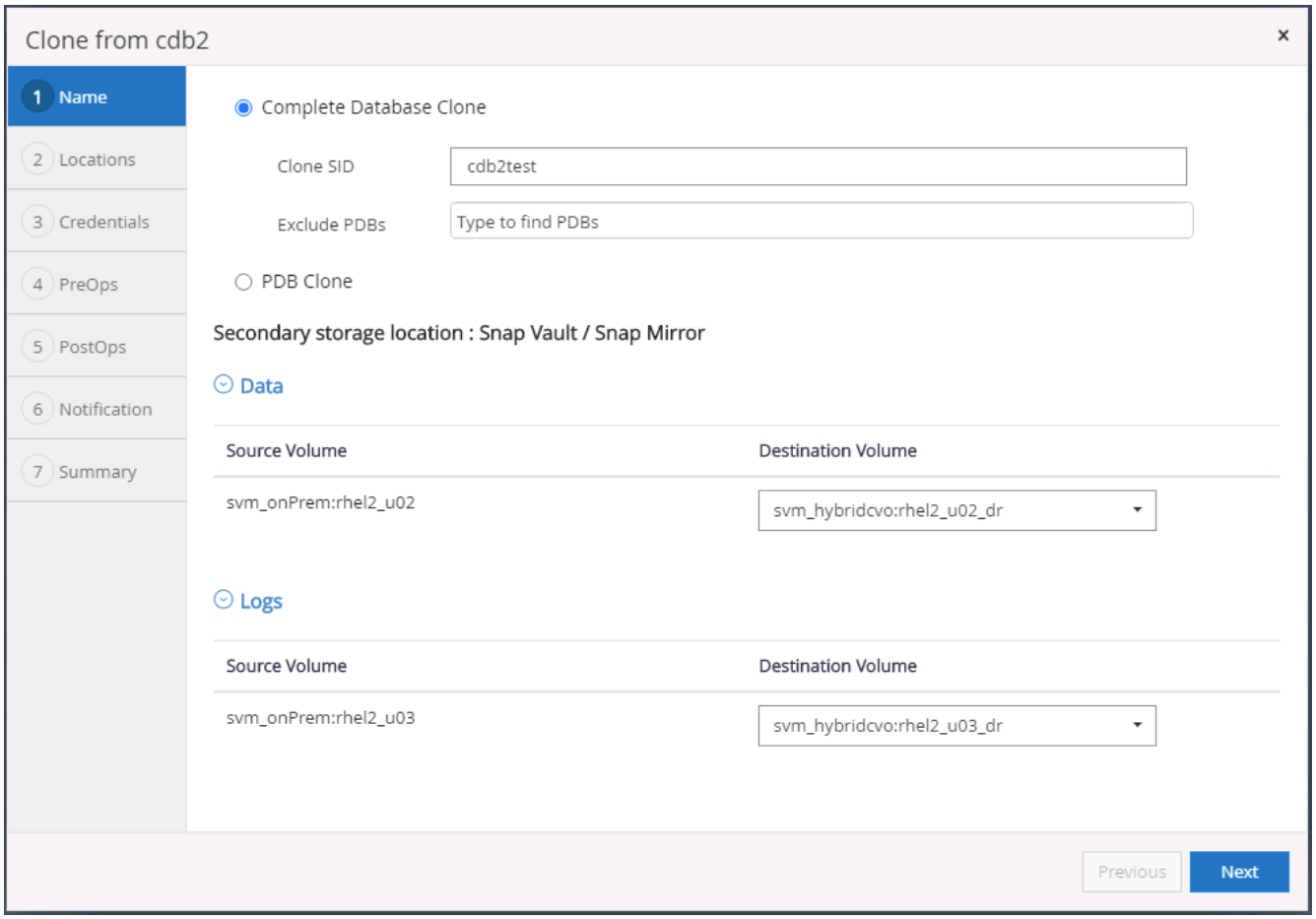


Wenn die Protokollbereinigung aktiviert ist und der Wiederherstellungspunkt über die letzte Protokollbereinigung hinaus erweitert wird, müssen möglicherweise mehrere Archivprotokollsicherungen bereitgestellt werden.

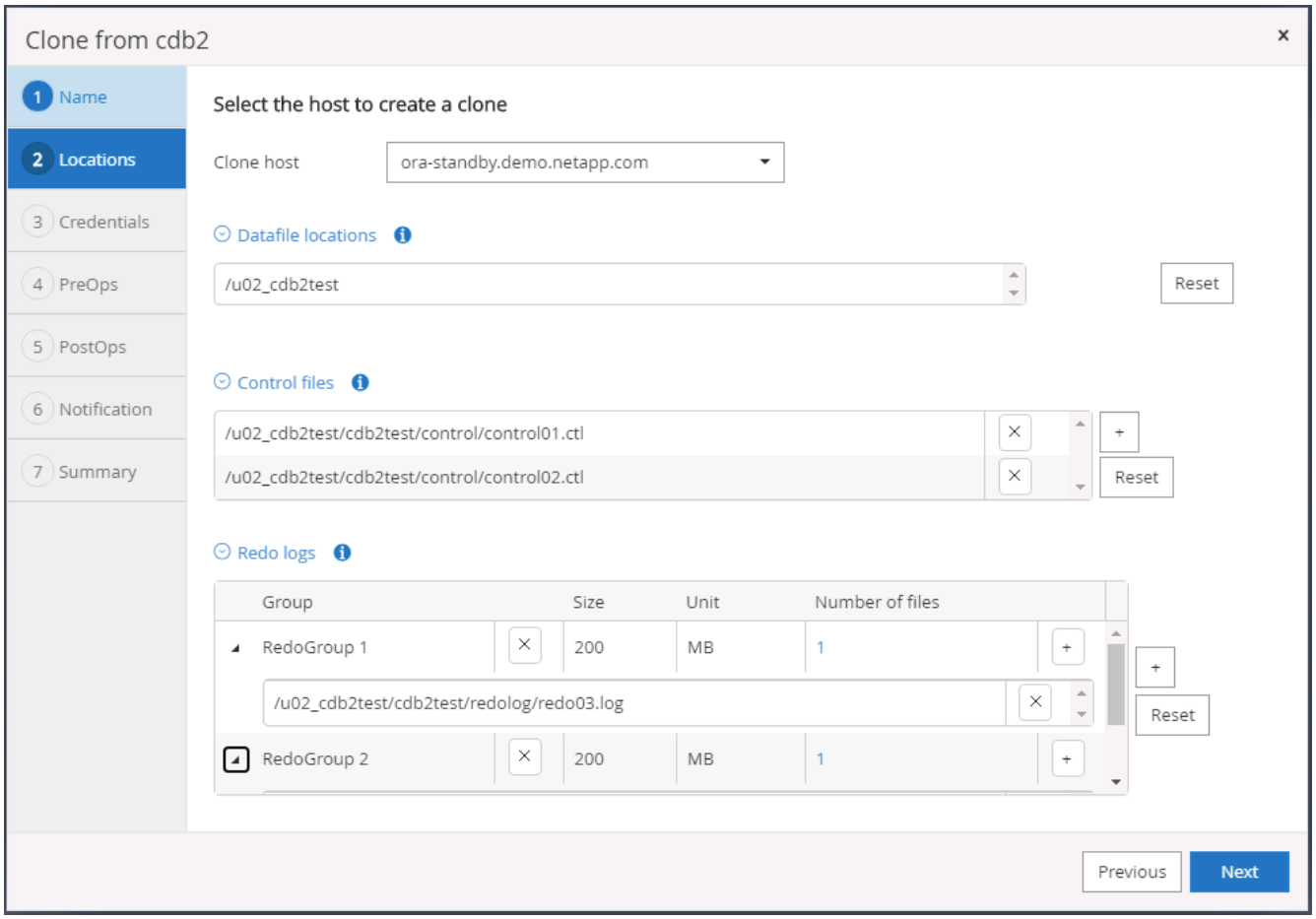
5. Markieren Sie die vollständige Datenbanksicherungskopie, die geklont werden soll, und klicken Sie dann auf die Schaltfläche „Klonen“, um den DB-Klon-Workflow zu starten.



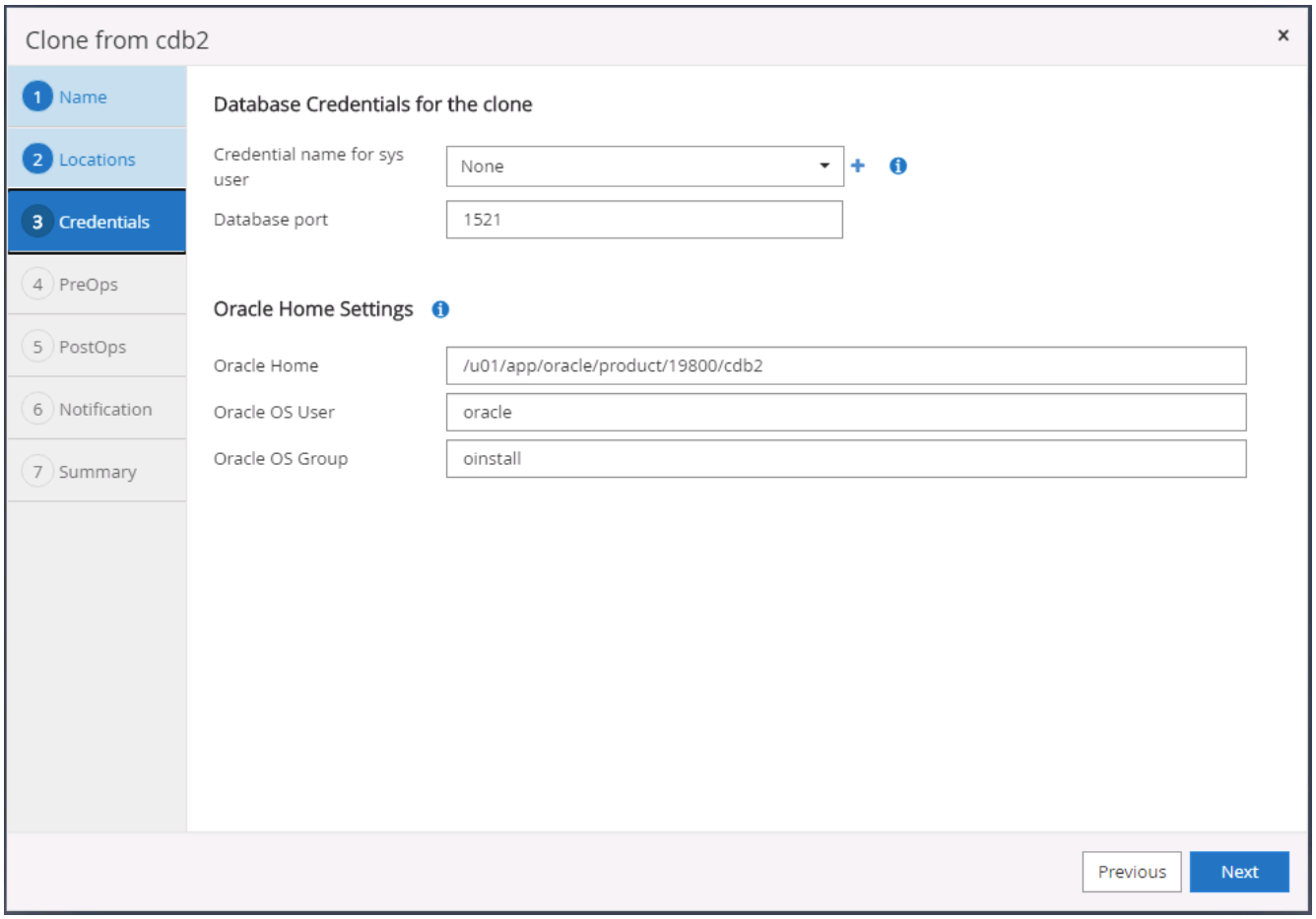
6. Wählen Sie eine geeignete Klon-DB-SID für eine vollständige Containerdatenbank oder einen CDB-Klon.



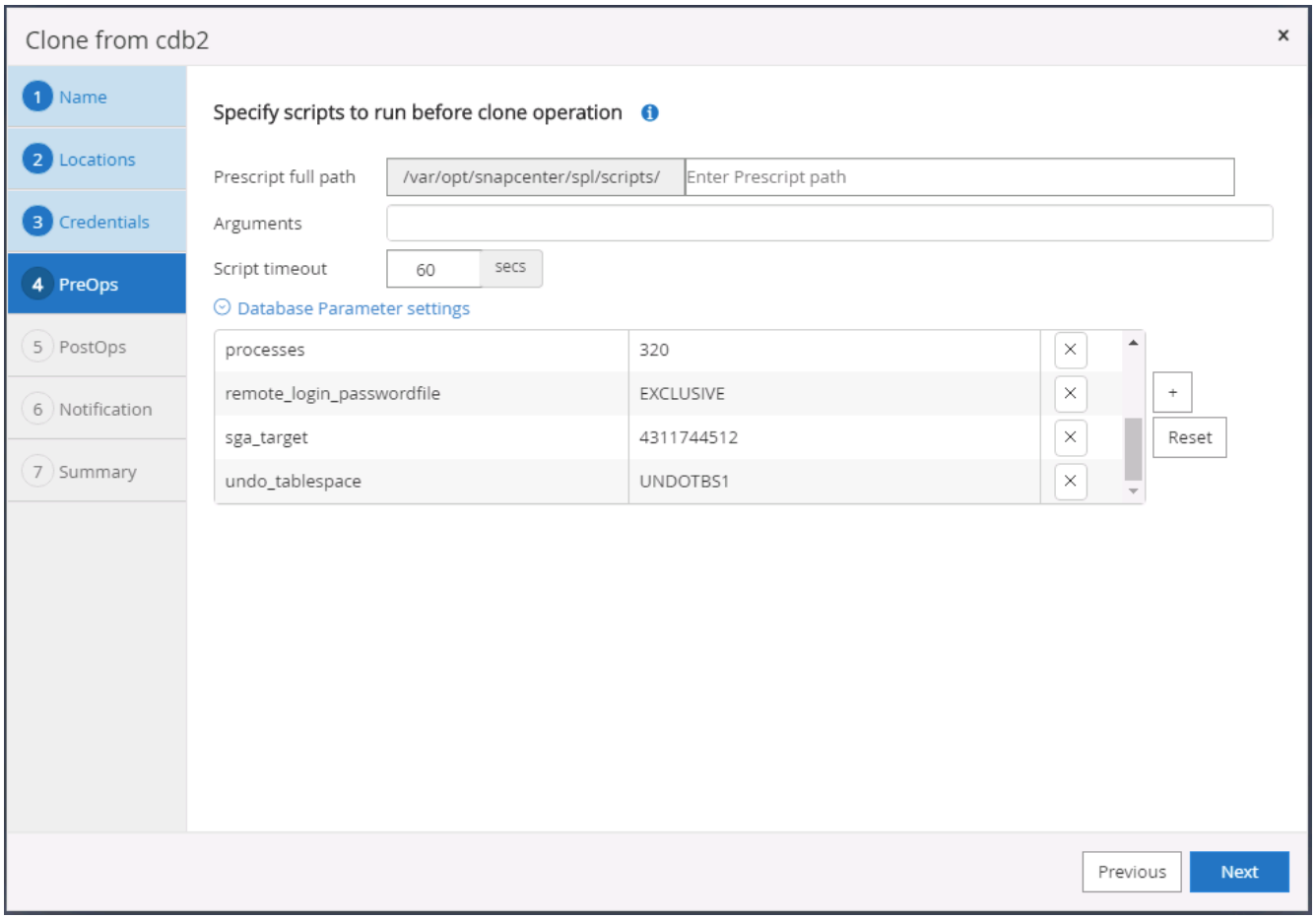
7. Wählen Sie den Ziel-Klonhost in der Cloud aus, und durch den Klon-Workflow werden Datendatei-, Steuerdatei- und Redo-Log-Verzeichnisse erstellt.



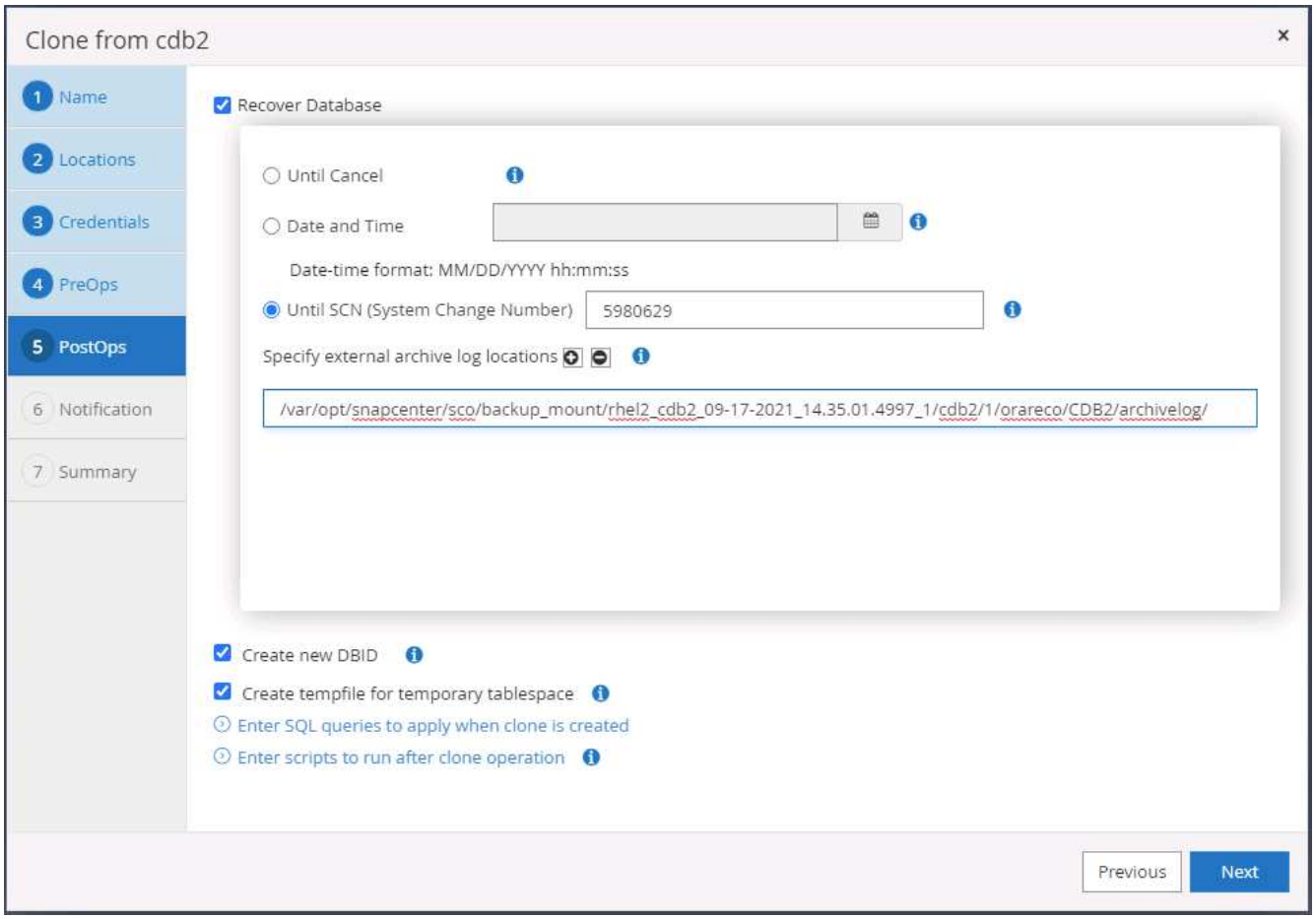
8. Der Anmeldeinformationsname „Keine“ wird für die betriebssystembasierte Authentifizierung verwendet, wodurch der Datenbankport irrelevant wird. Geben Sie das richtige Oracle Home, den Oracle OS-Benutzer und die Oracle OS-Gruppe ein, wie sie im Ziel-Klon-DB-Server konfiguriert sind.

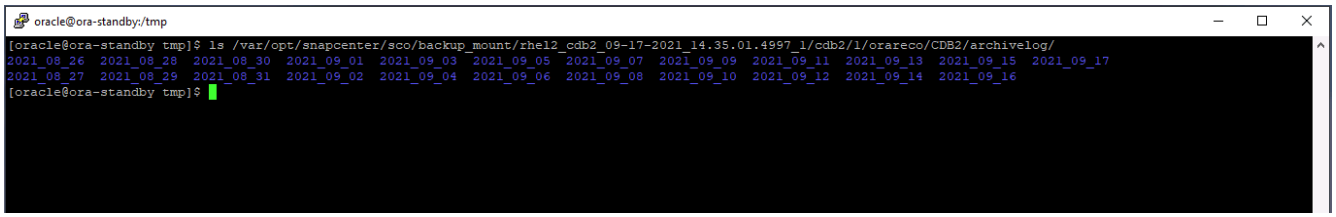


9. Geben Sie die Skripte an, die vor dem Klonvorgang ausgeführt werden sollen. Noch wichtiger ist, dass hier die Datenbankinstanzparameter angepasst oder definiert werden können.

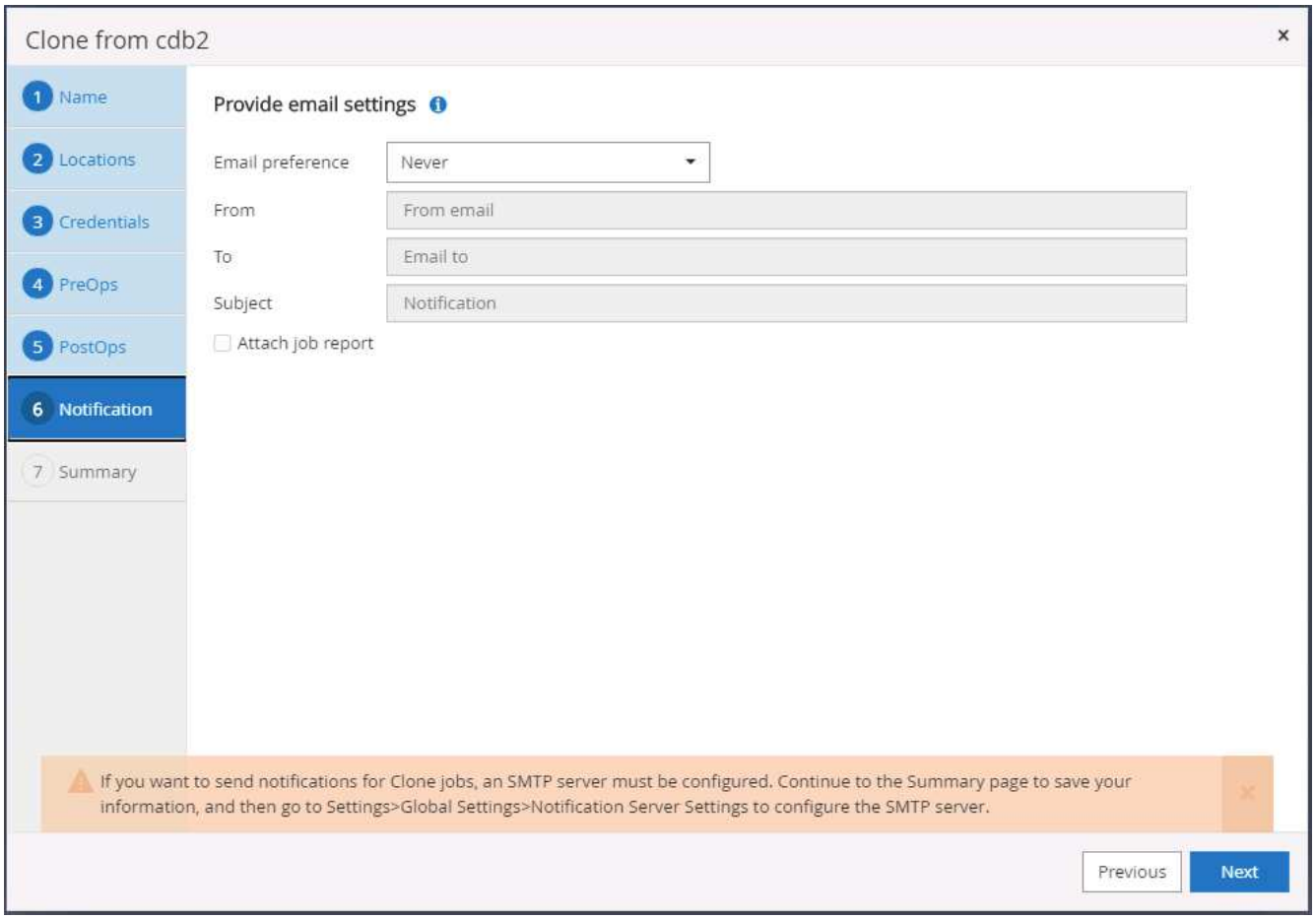


10. Geben Sie den Wiederherstellungspunkt entweder nach Datum und Uhrzeit oder nach SCN an. „Bis zum Abbrechen“ stellt die Datenbank bis zu den verfügbaren Archivprotokollen wieder her. Geben Sie den externen Speicherort des Archivprotokolls vom Zielhost an, auf dem das Archivprotokollvolume bereitgestellt ist. Wenn der Oracle-Besitzer des Zielservers nicht mit dem lokalen Produktionsserver identisch ist, überprüfen Sie, ob das Archivprotokollverzeichnis vom Oracle-Besitzer des Zielservers gelesen werden kann.

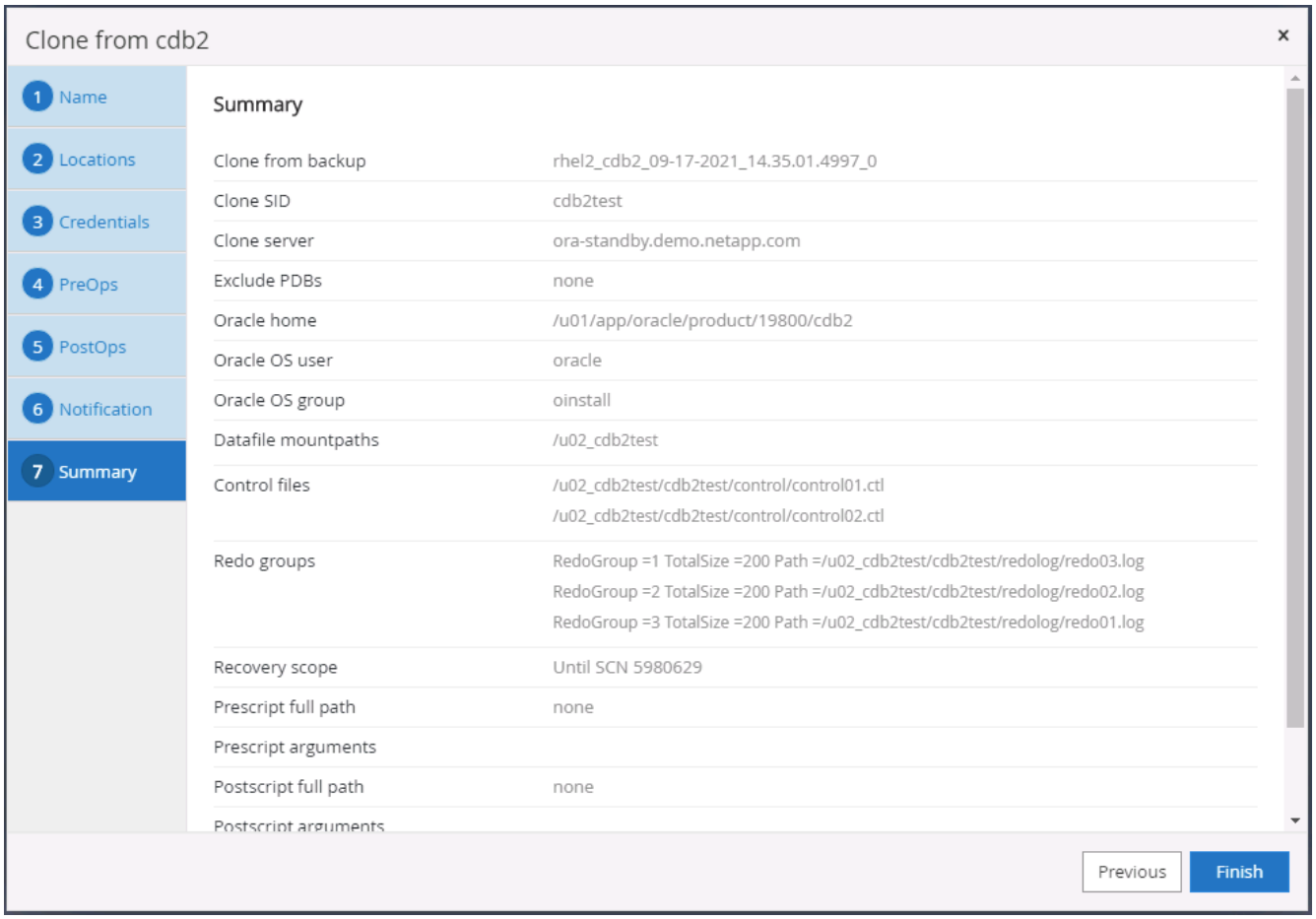




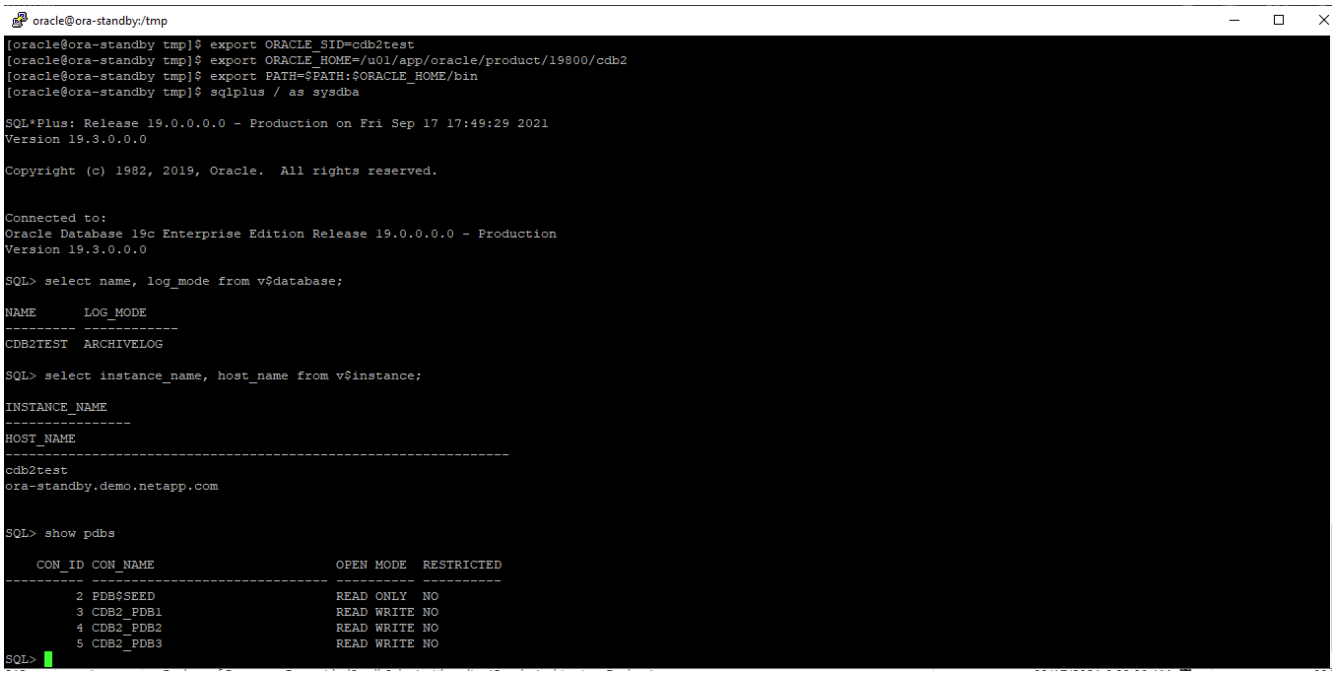
11. Konfigurieren Sie den SMTP-Server bei Bedarf für E-Mail-Benachrichtigungen.



12. Klonzusammenfassung.

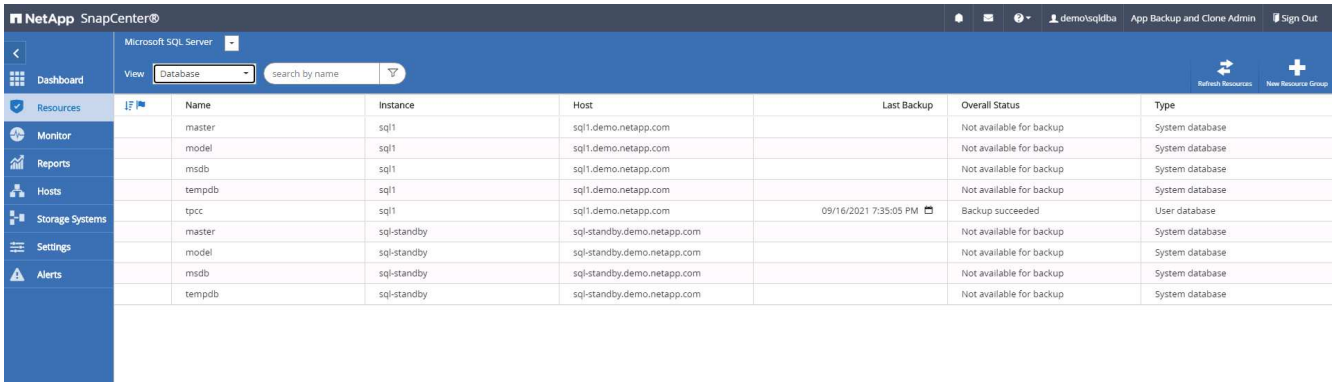


13. Sie sollten nach dem Klonen eine Validierung durchführen, um sicherzustellen, dass die geklonte Datenbank betriebsbereit ist. Einige zusätzliche Aufgaben, wie das Starten des Listeners oder das Deaktivieren des DB-Protokollarchivmodus, können in der Dev/Test-Datenbank ausgeführt werden.

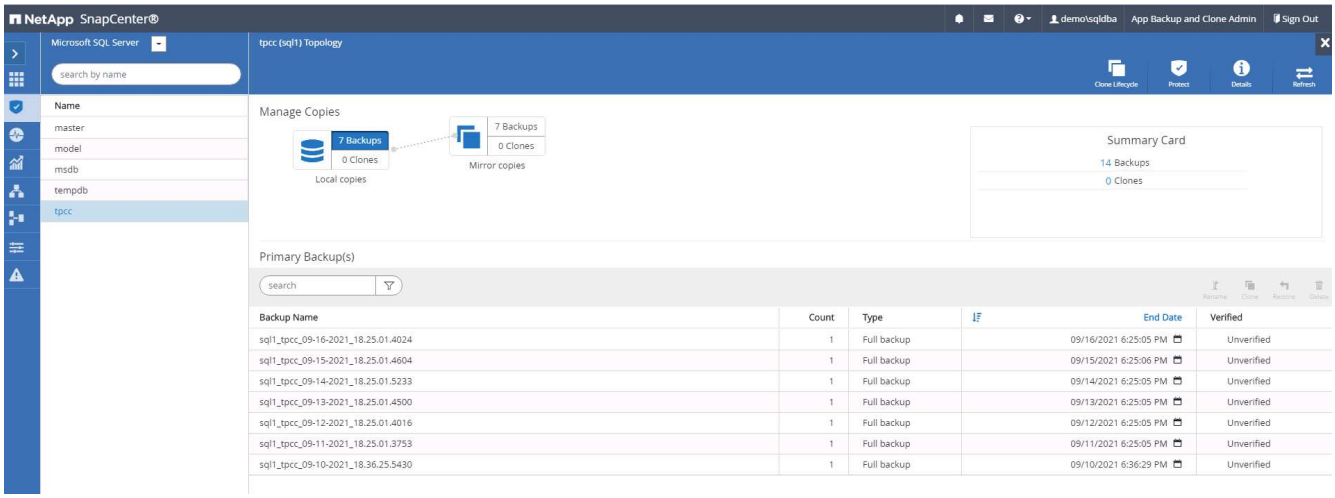


Klonen Sie eine SQL-Datenbank für Entwicklung/Test aus einer replizierten Snapshot-Sicherung

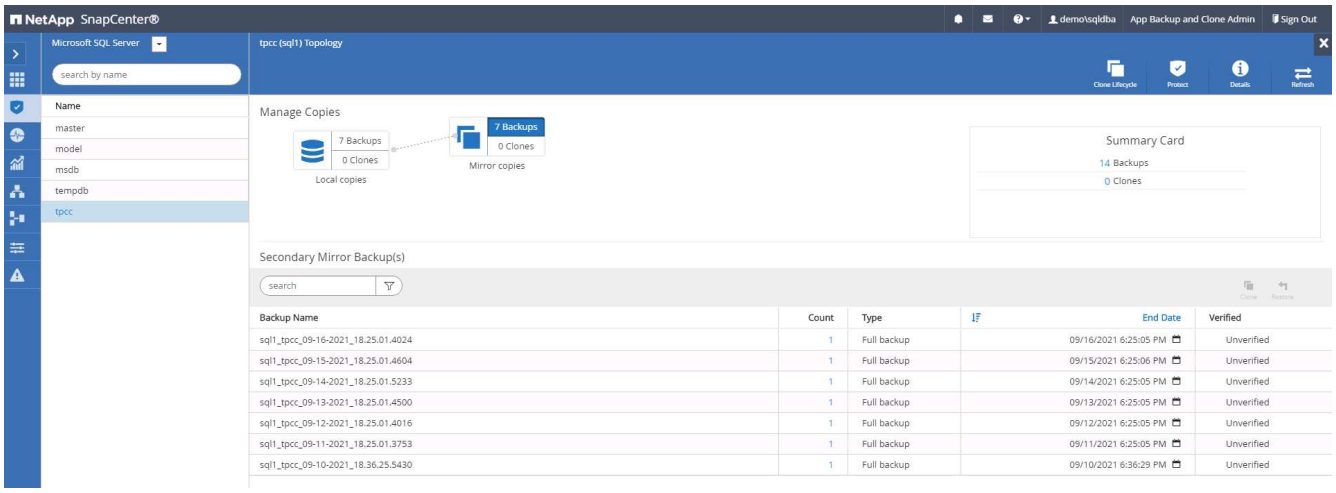
1. Melden Sie sich bei SnapCenter mit einer Datenbankverwaltungs-Benutzer-ID für SQL Server an. Navigieren Sie zur Registerkarte „Ressourcen“, auf der die von SnapCenter geschützten SQL Server-Benutzerdatenbanken und eine Ziel-Standby-SQL-Instanz in der öffentlichen Cloud angezeigt werden.



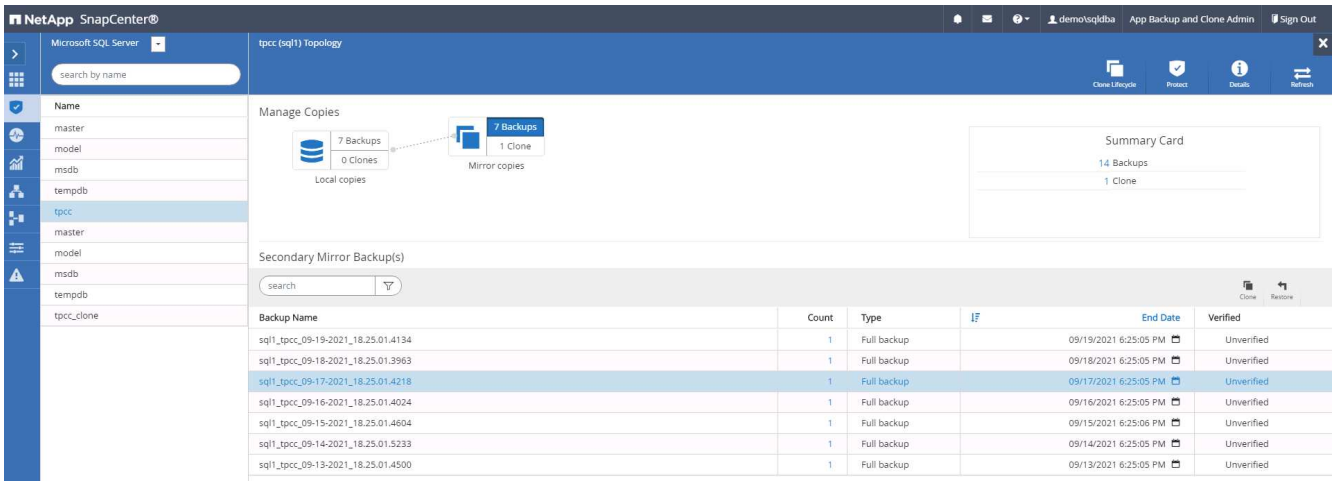
2. Klicken Sie auf den gewünschten lokalen SQL Server-Benutzerdatenbanknamen, um die Sicherungstopologie und die Detailansicht anzuzeigen. Wenn ein sekundärer replizierter Speicherort aktiviert ist, werden verknüpfte Spiegelsicherungen angezeigt.

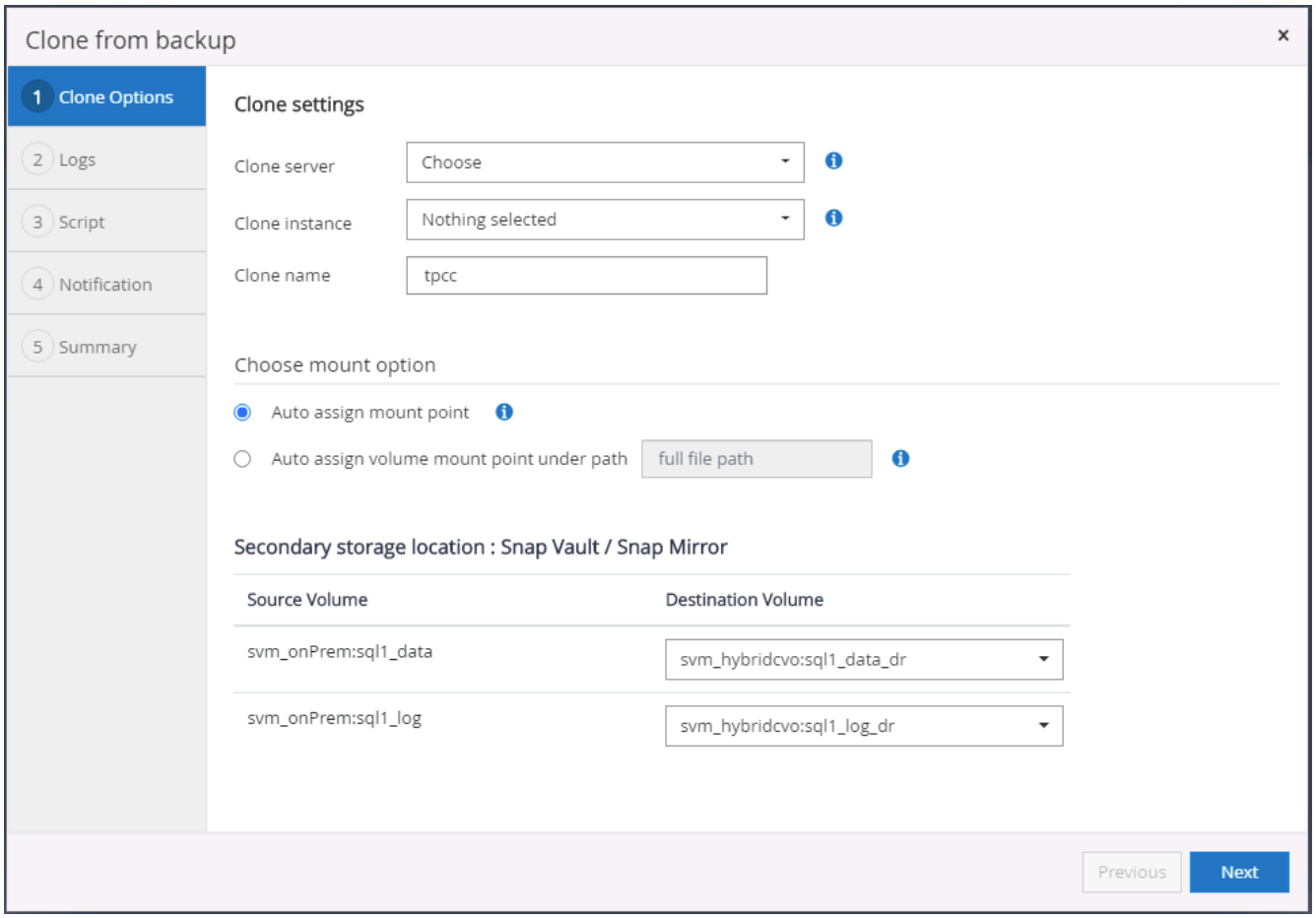


3. Wechseln Sie zur Ansicht „Gespiegelte Sicherungen“, indem Sie auf „Gespiegelte Sicherungen“ klicken. Anschließend werden sekundäre Spiegelsicherungen angezeigt. Da SnapCenter das SQL Server-Transaktionsprotokoll zur Wiederherstellung auf einem dedizierten Laufwerk sichert, werden hier nur vollständige Datenbanksicherungen angezeigt.

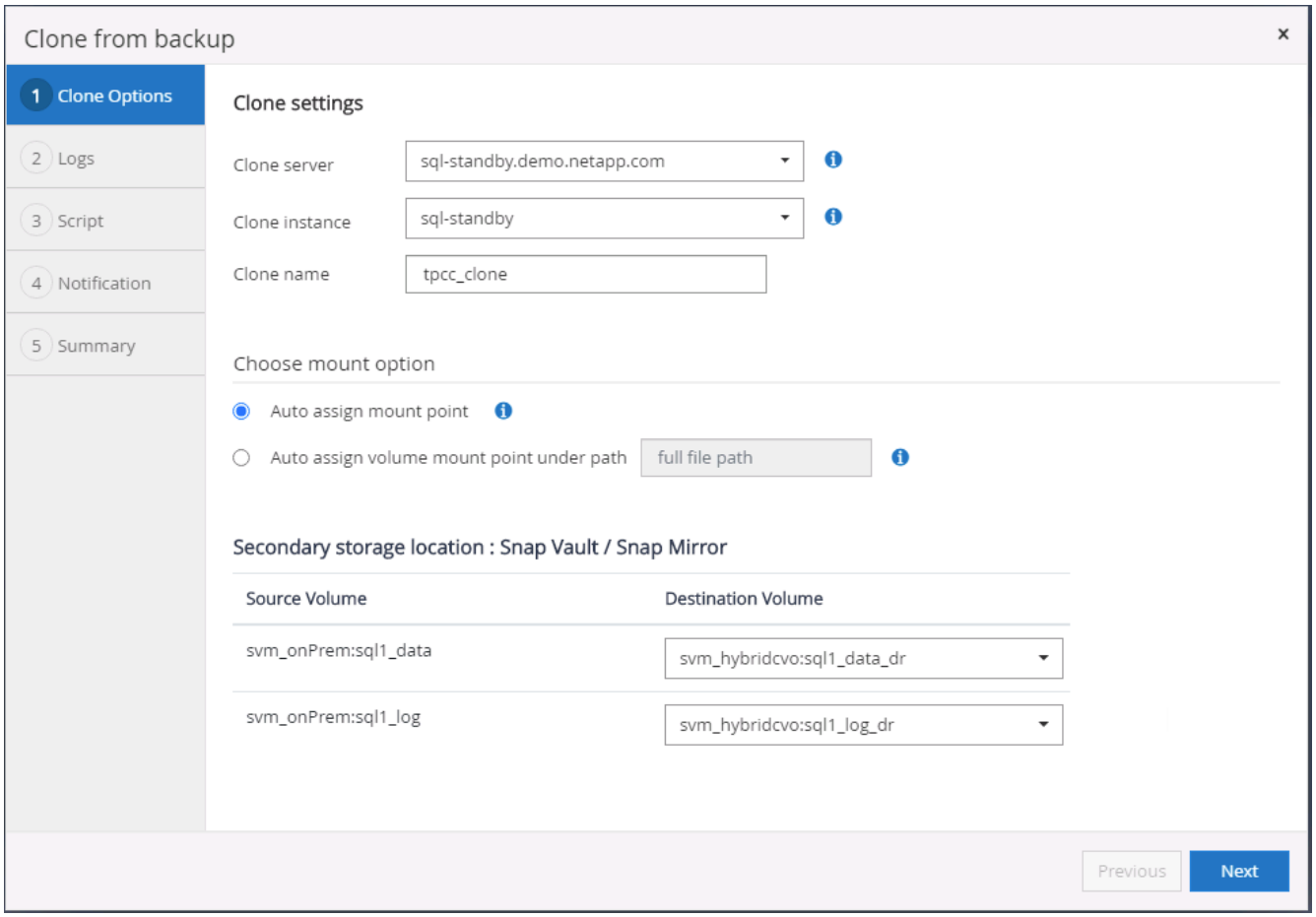


4. Wählen Sie eine Sicherungskopie aus und klicken Sie dann auf die Schaltfläche „Klonen“, um den Arbeitsablauf „Aus Sicherung klonen“ zu starten.

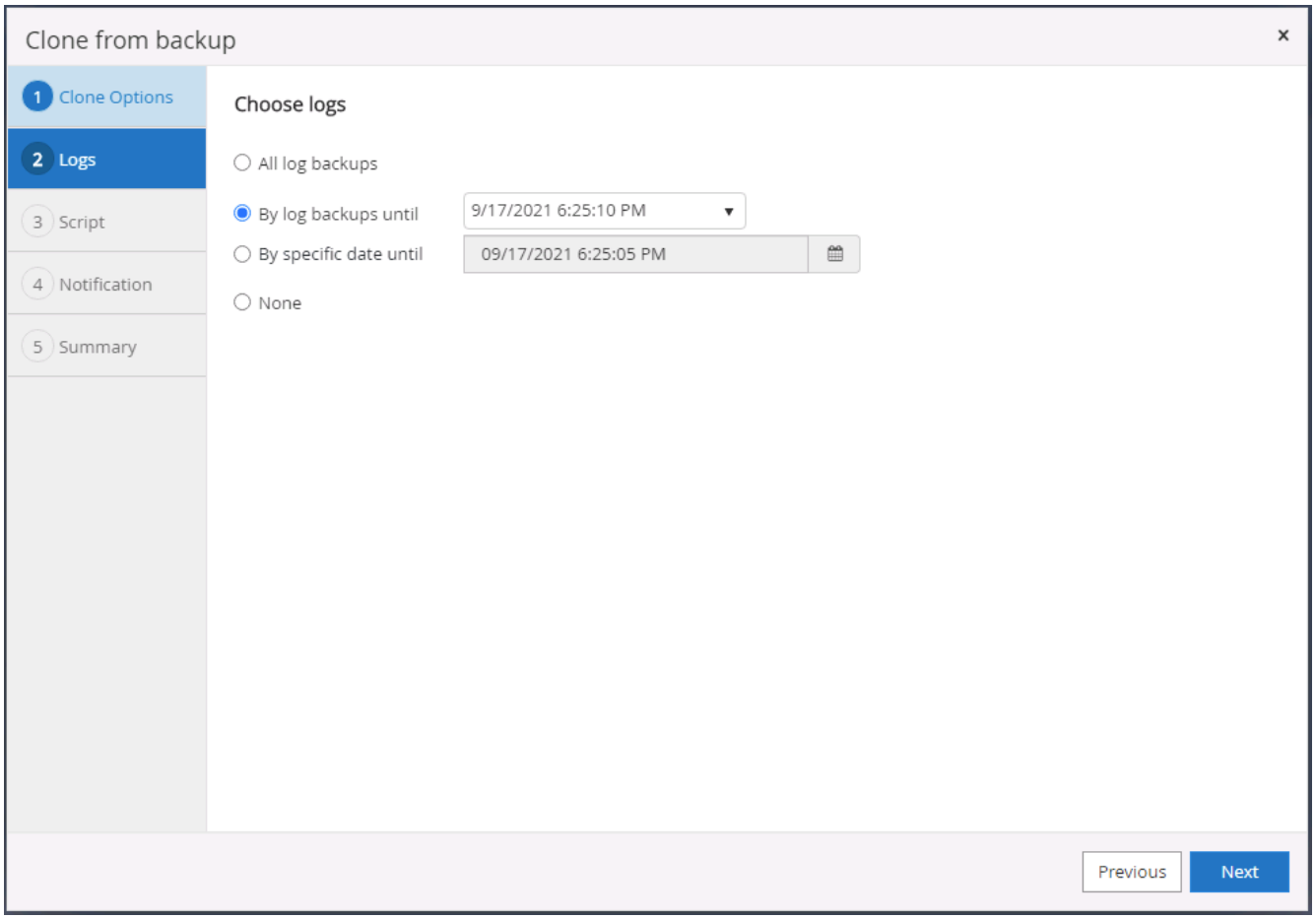




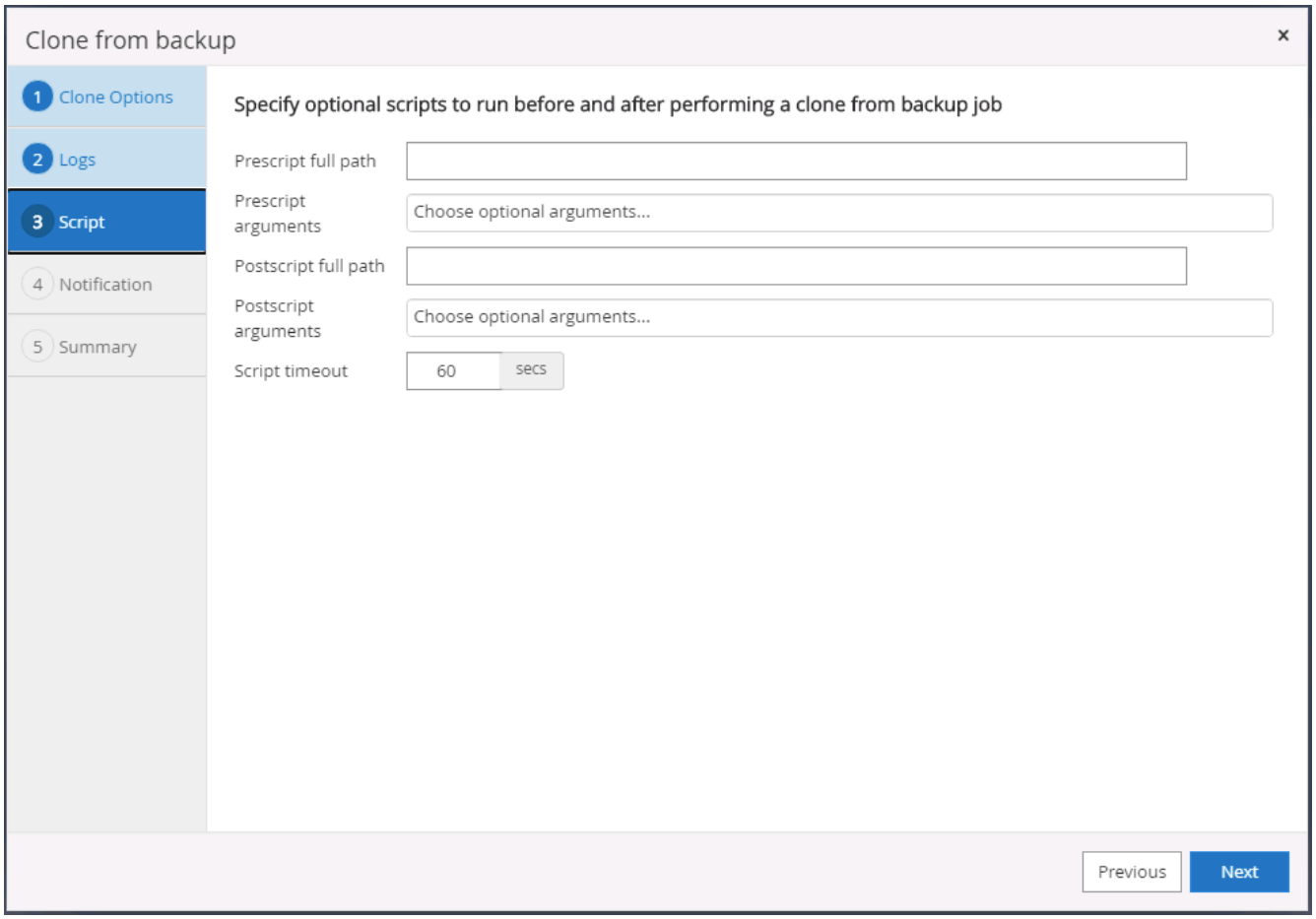
5. Wählen Sie einen Cloud-Server als Zielklonserver, den Namen der Kloninstanz und den Namen der Klondatenbank aus. Wählen Sie entweder einen automatisch zugewiesenen Einhängepunkt oder einen benutzerdefinierten Einhängepunktpfad.



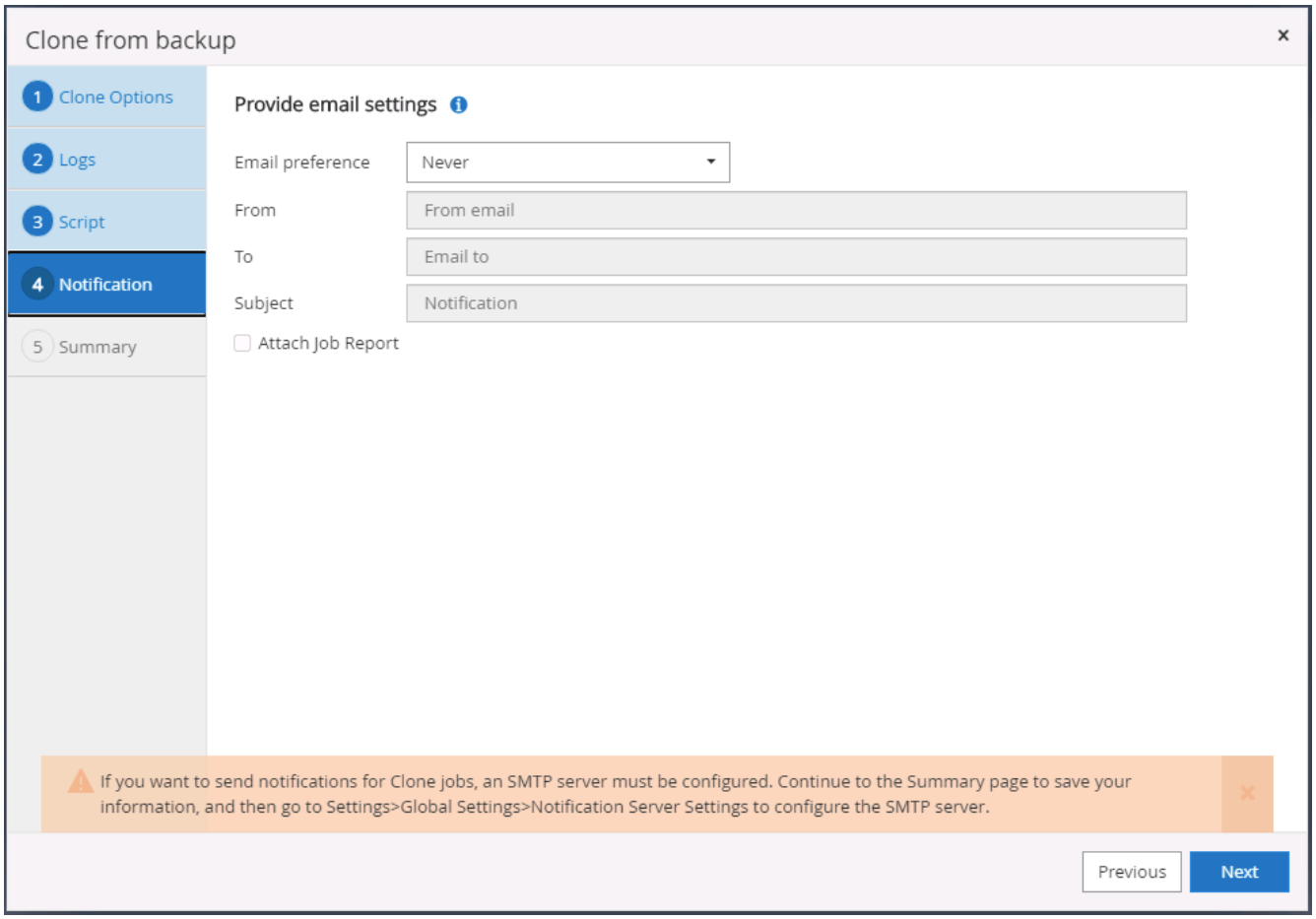
6. Bestimmen Sie einen Wiederherstellungspunkt entweder anhand der Sicherungszeit eines Protokolls oder anhand eines bestimmten Datums und einer bestimmten Uhrzeit.



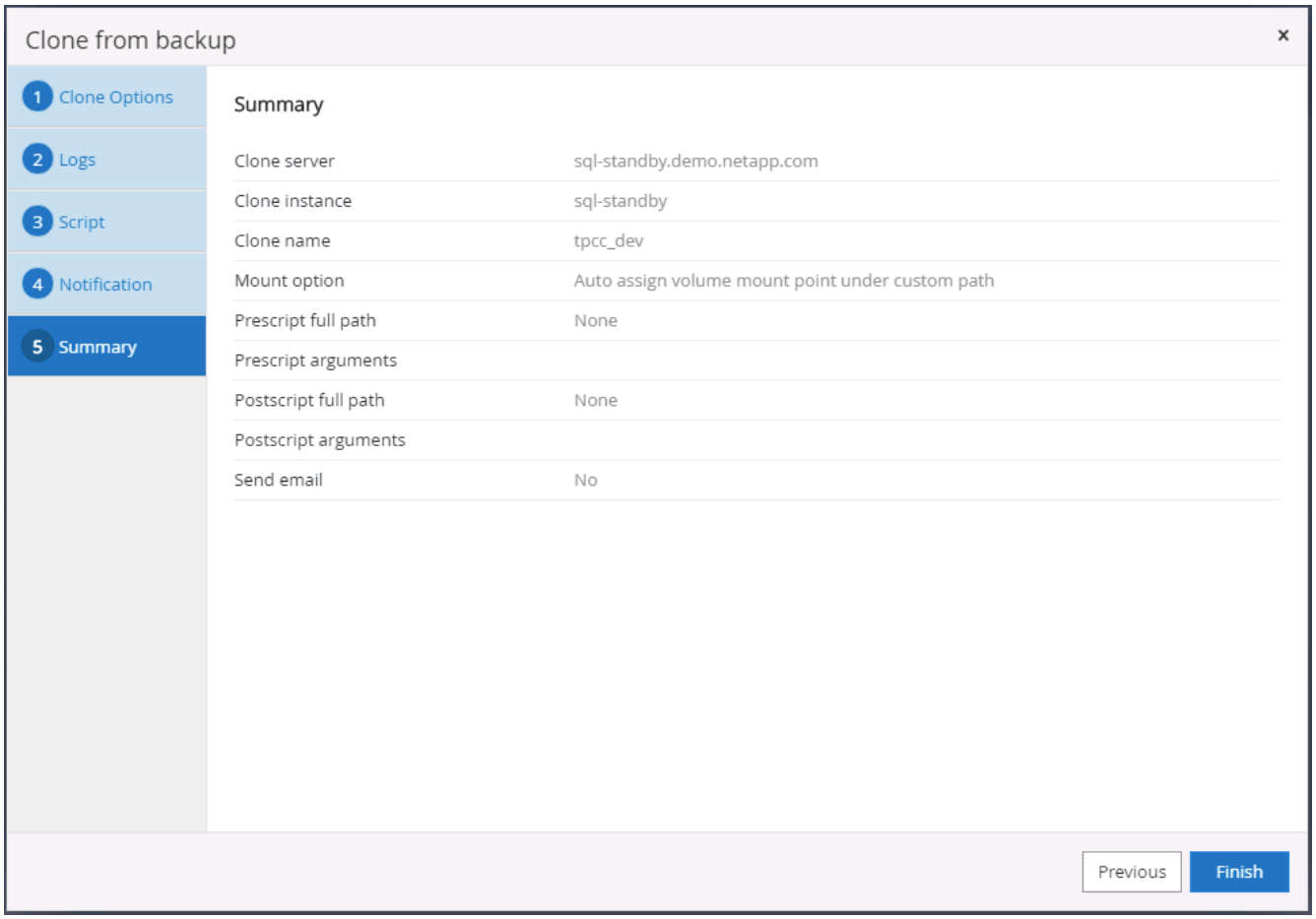
7. Geben Sie optionale Skripts an, die vor und nach dem Klonvorgang ausgeführt werden sollen.



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



9. Klonzusammenfassung.



10. Überwachen Sie den Auftragsstatus und überprüfen Sie, ob die gewünschte Benutzerdatenbank an eine SQL-Zielinstanz im Cloud-Klonserver angehängt wurde.

Konfiguration nach dem Klonen

1. Eine lokale Oracle-Produktionsdatenbank wird normalerweise im Protokollarchivmodus ausgeführt. Dieser Modus ist für eine Entwicklungs- oder Testdatenbank nicht erforderlich. Um den Protokollarchivierungsmodus zu deaktivieren, melden Sie sich als sysdba bei der Oracle-Datenbank an, führen Sie einen Befehl zum Ändern des Protokollmodus aus und starten Sie die Datenbank für den Zugriff.
2. Konfigurieren Sie einen Oracle-Listener oder registrieren Sie die neu geklonte Datenbank mit einem vorhandenen Listener für den Benutzerzugriff.
3. Ändern Sie für SQL Server den Protokollmodus von „Vollständig“ in „Einfach“, damit die Entwicklungs-/Testprotokolldatei von SQL Server problemlos verkleinert werden kann, wenn sie das Protokollvolumen

füllt.

Klondatenbank aktualisieren

1. Löschen Sie geklonte Datenbanken und bereinigen Sie die Cloud-DB-Serverumgebung. Befolgen Sie dann die vorherigen Verfahren, um eine neue Datenbank mit neuen Daten zu klonen. Das Klonen einer neuen Datenbank dauert nur wenige Minuten.
2. Fahren Sie die Klondatenbank herunter und führen Sie mithilfe der CLI einen Befehl zum Aktualisieren des Klons aus. Weitere Informationen finden Sie in der folgenden SnapCenter -Dokumentation:"Aktualisieren eines Klons" .

Wo bekomme ich Hilfe?

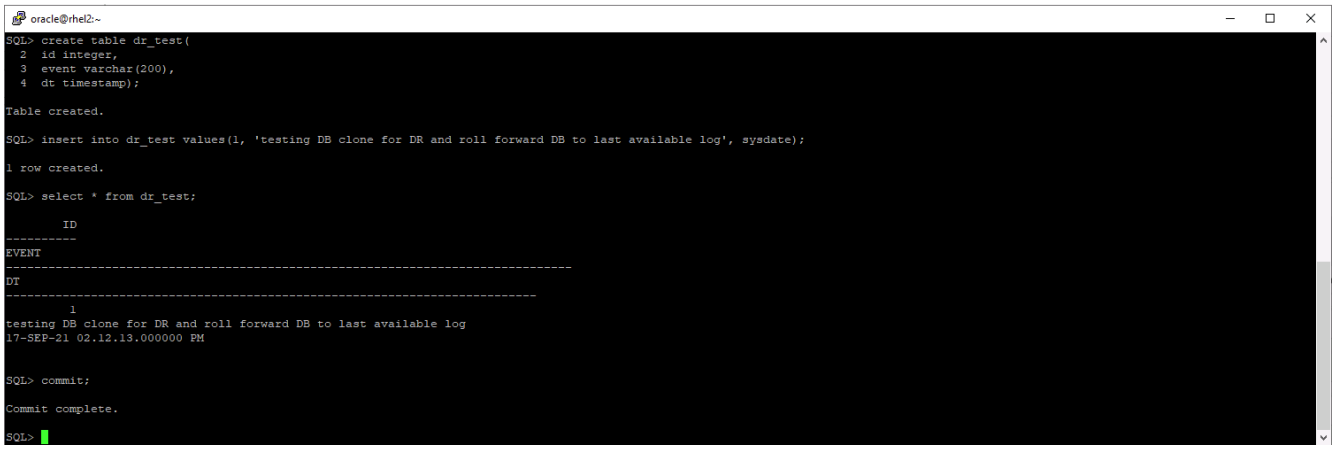
Wenn Sie Hilfe bei dieser Lösung und den Anwendungsfällen benötigen, treten Sie dem"Slack-Kanal für den Support der NetApp Solution Automation-Community" und suchen Sie nach dem Kanal zur Lösungsautomatisierung, um Ihre Fragen oder Anfragen zu posten.

Workflow zur Notfallwiederherstellung

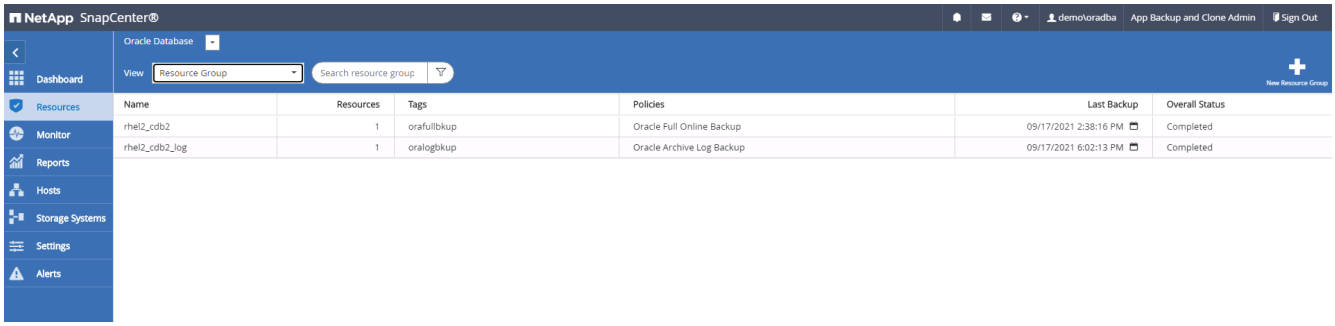
Unternehmen haben die öffentliche Cloud als praktikable Ressource und Ziel für die Notfallwiederherstellung angenommen. SnapCenter gestaltet diesen Prozess so nahtlos wie möglich. Dieser Notfallwiederherstellungs-Workflow ist dem Klon-Workflow sehr ähnlich, allerdings wird bei der Datenbankwiederherstellung das letzte verfügbare Protokoll verwendet, das in die Cloud repliziert wurde, um alle möglichen Geschäftstransaktionen wiederherzustellen. Es gibt jedoch zusätzliche Schritte vor und nach der Konfiguration, die speziell für die Notfallwiederherstellung erforderlich sind.

Klonen Sie eine lokale Oracle-Produktionsdatenbank für die Notfallwiederherstellung in die Cloud

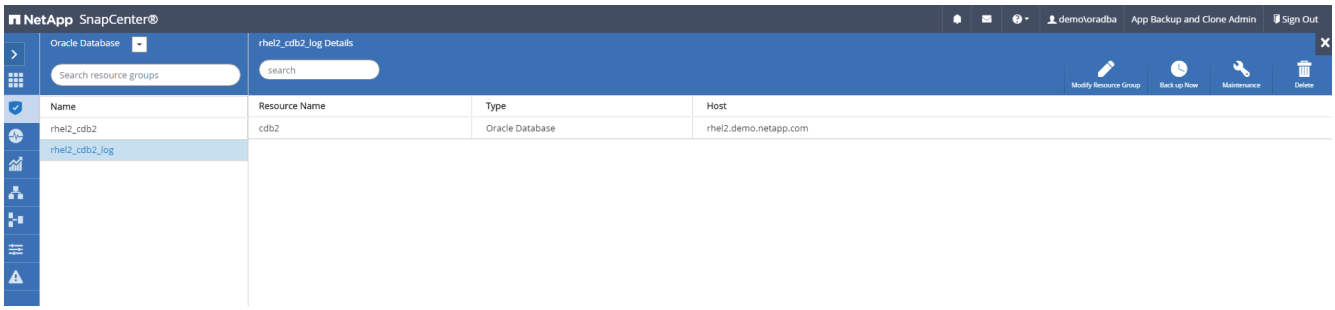
1. Um zu überprüfen, ob die Klonwiederherstellung über das letzte verfügbare Protokoll läuft, haben wir eine kleine Testtabelle erstellt und eine Zeile eingefügt. Die Testdaten würden nach einer vollständigen Wiederherstellung des letzten verfügbaren Protokolls wiederhergestellt.

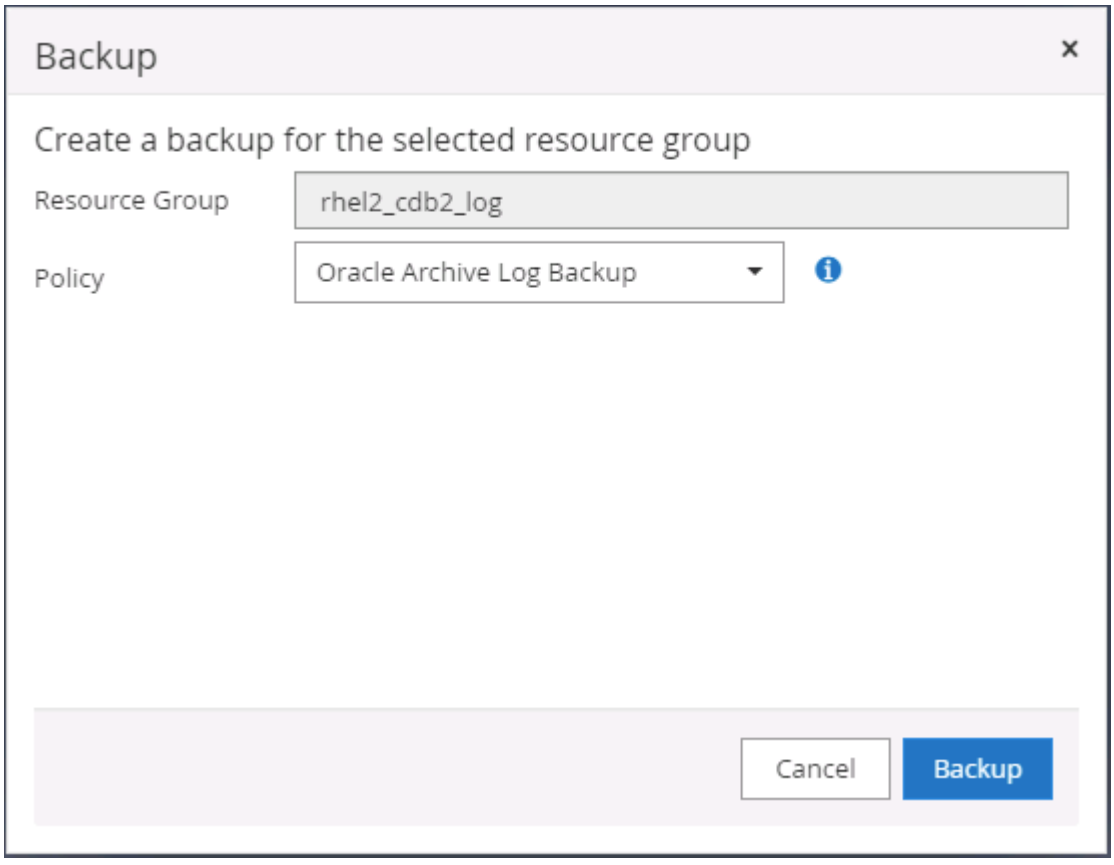


2. Melden Sie sich bei SnapCenter mit einer Datenbankverwaltungs-Benutzer-ID für Oracle an. Navigieren Sie zur Registerkarte „Ressourcen“, auf der die von SnapCenter geschützten Oracle-Datenbanken angezeigt werden.



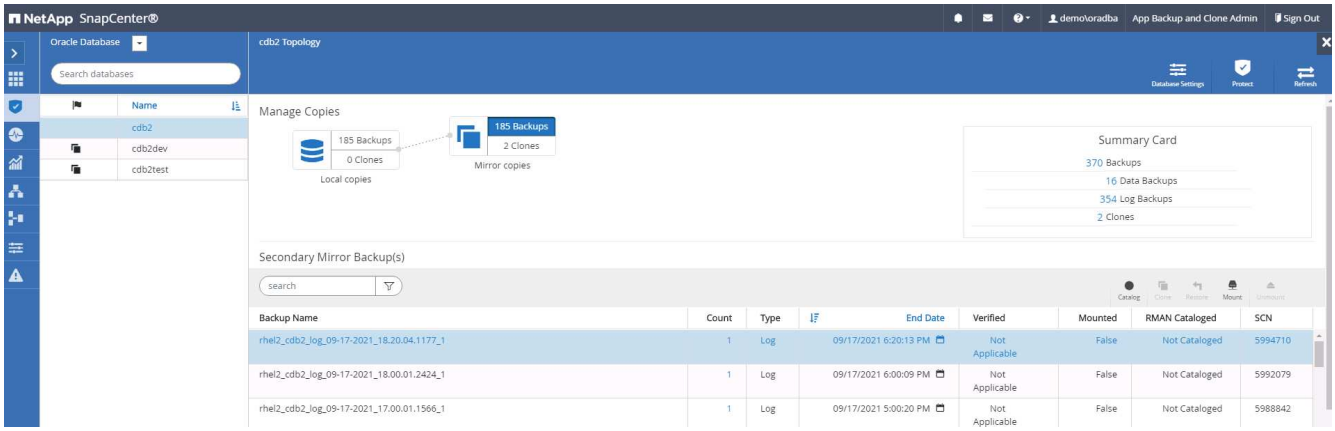
3. Wählen Sie die Oracle-Protokollressourcengruppe aus und klicken Sie auf „Jetzt sichern“, um manuell eine Oracle-Protokollsicherung auszuführen und die letzte Transaktion an das Ziel in der Cloud zu übertragen. In einem echten DR-Szenario hängt die letzte wiederherstellbare Transaktion von der Replikationshäufigkeit des Datenbankprotokollvolumens in die Cloud ab, die wiederum von der RTO- oder RPO-Richtlinie des Unternehmens abhängt.

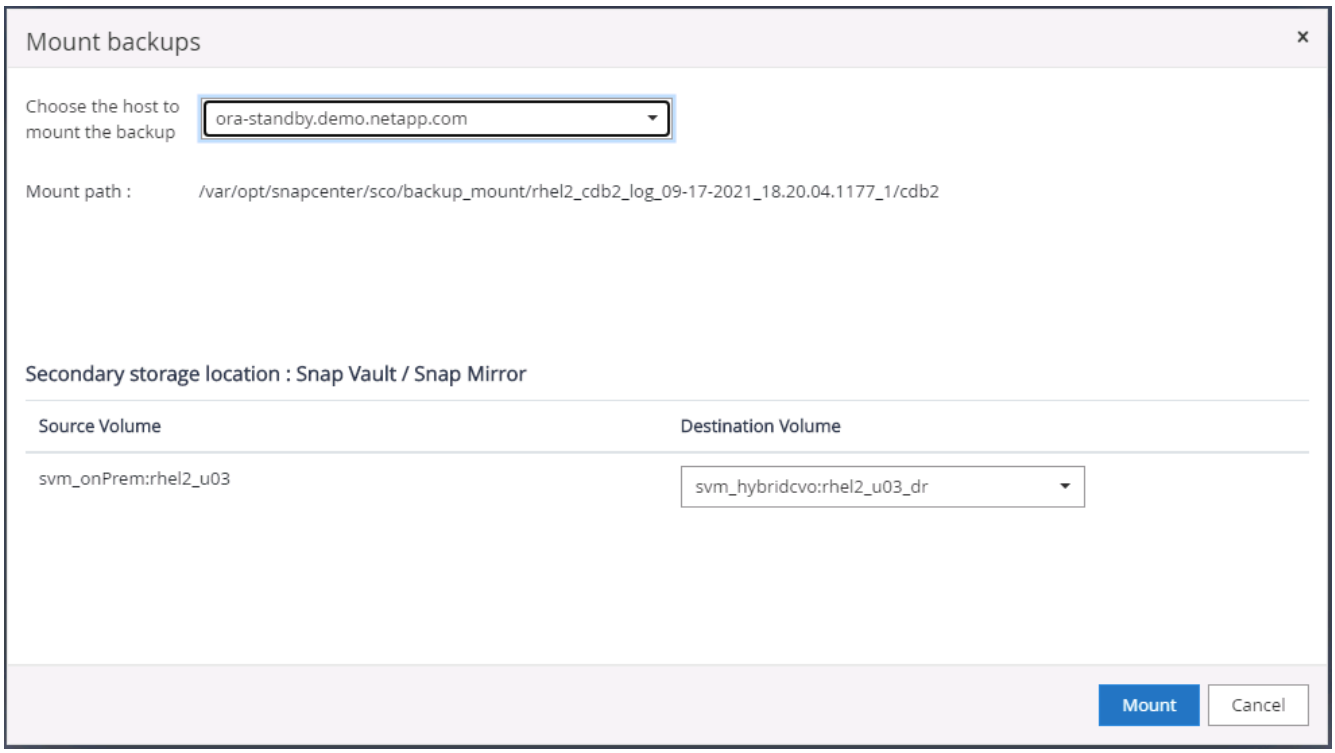




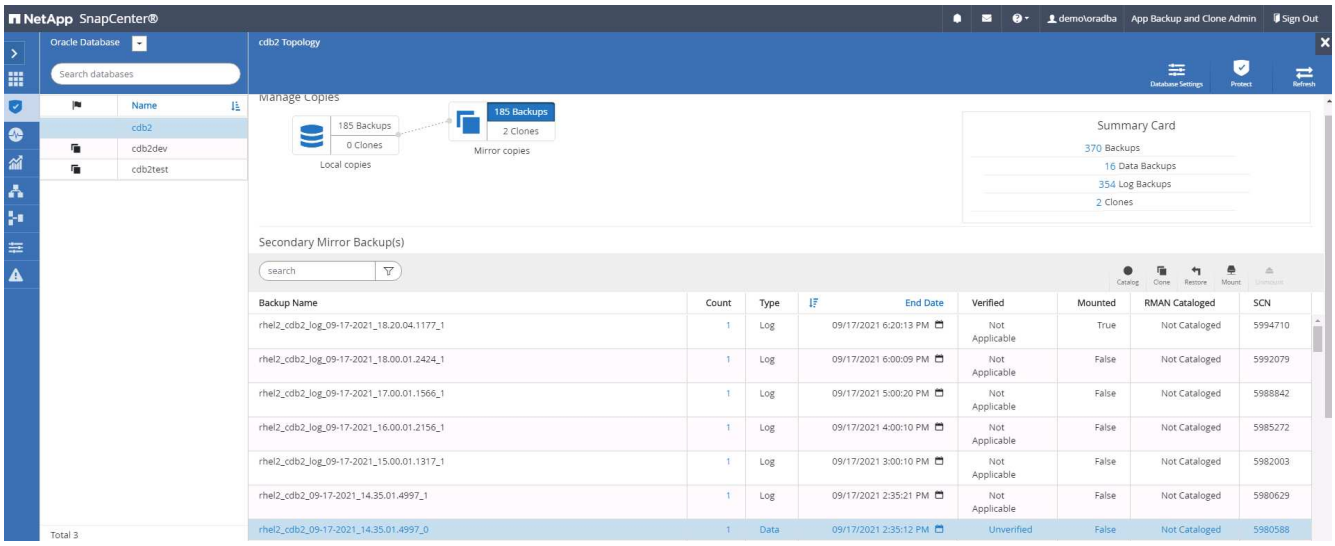
Beim asynchronen SnapMirror gehen in einem Notfallwiederherstellungsszenario Daten verloren, die es im Intervall der Datenbankprotokollsicherung nicht zum Cloud-Ziel geschafft haben. Um Datenverluste zu minimieren, können häufigere Protokollsicherungen geplant werden. Allerdings gibt es eine technisch erreichbare Grenze für die Häufigkeit der Protokollsicherung.

4. Wählen Sie die letzte Protokollsicherung auf den sekundären Spiegelsicherungen aus und mounten Sie die Protokollsicherung.

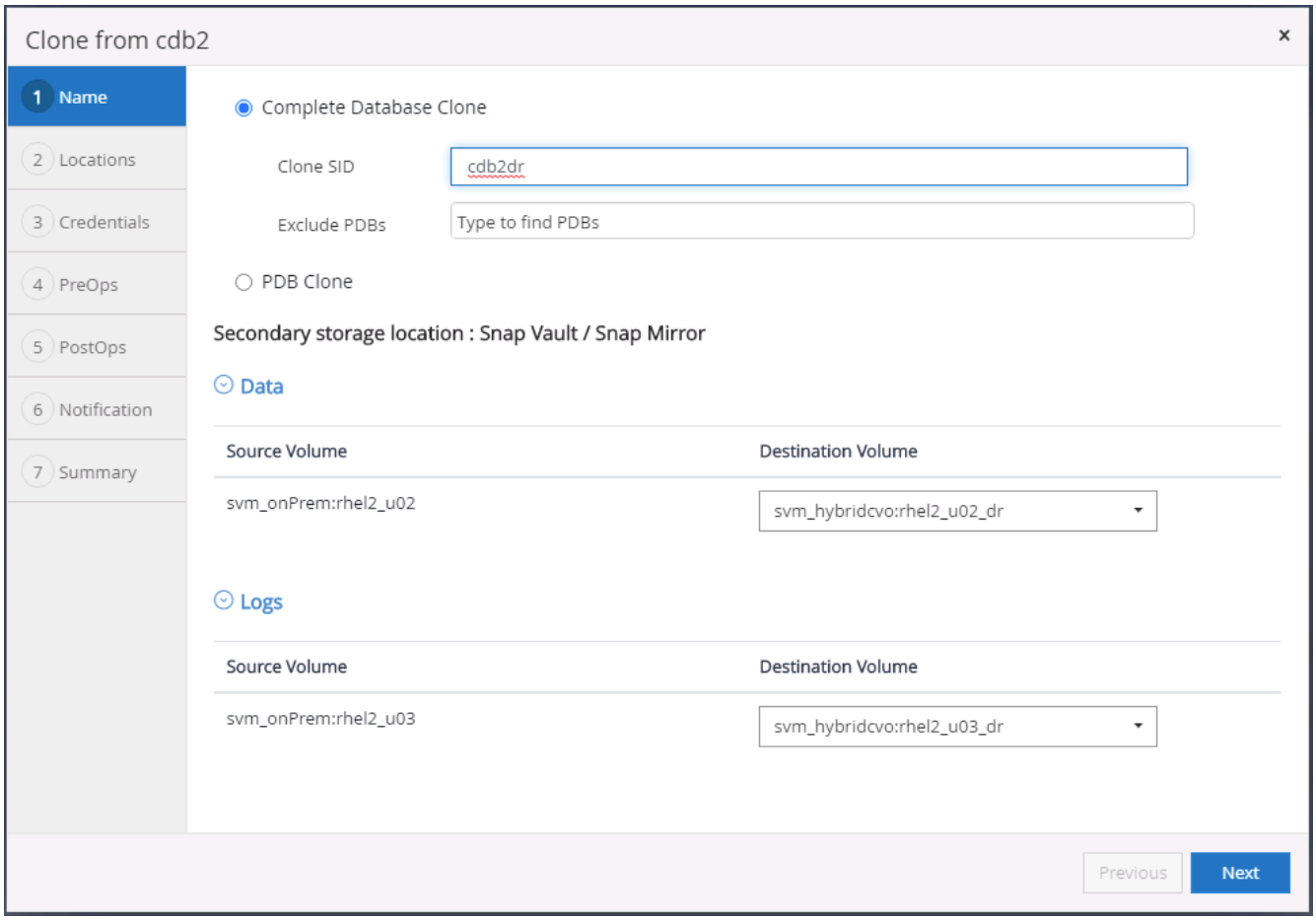




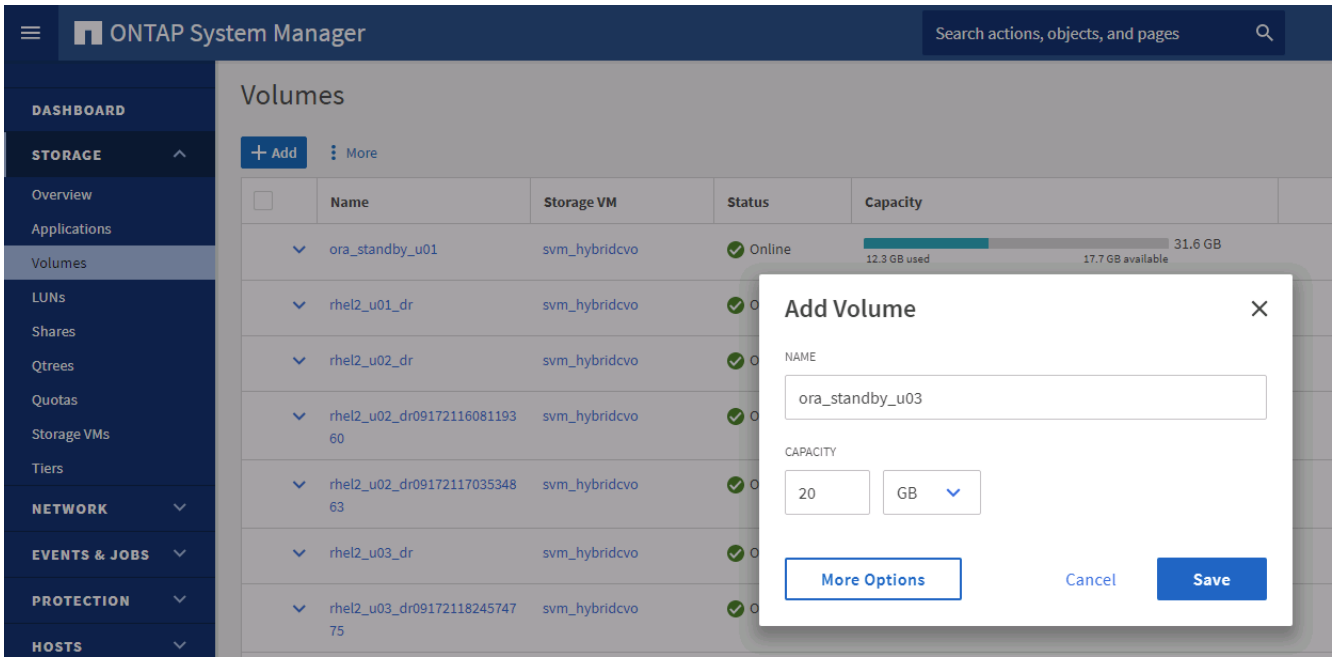
5. Wählen Sie die letzte vollständige Datenbanksicherung aus und klicken Sie auf „Klonen“, um den Klon-Workflow zu starten.

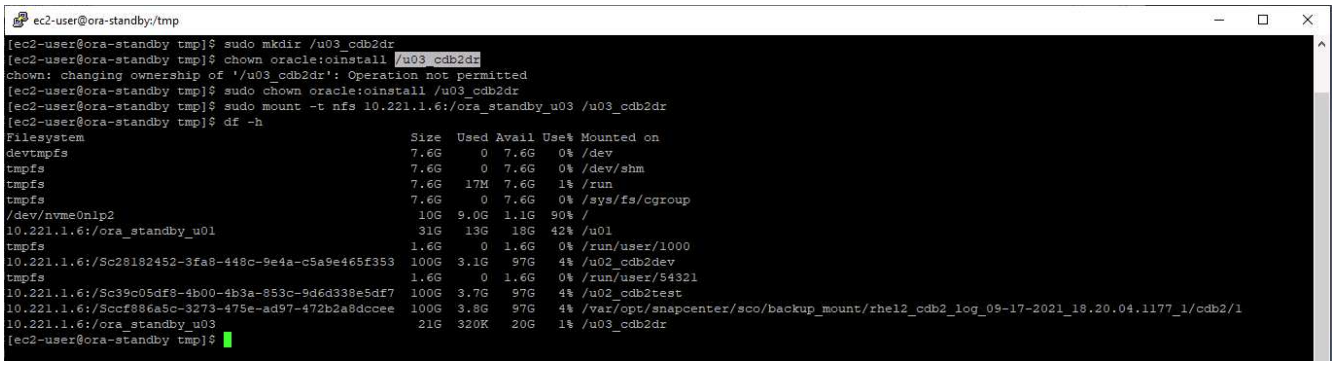


6. Wählen Sie eine eindeutige Klon-DB-ID auf dem Host aus.



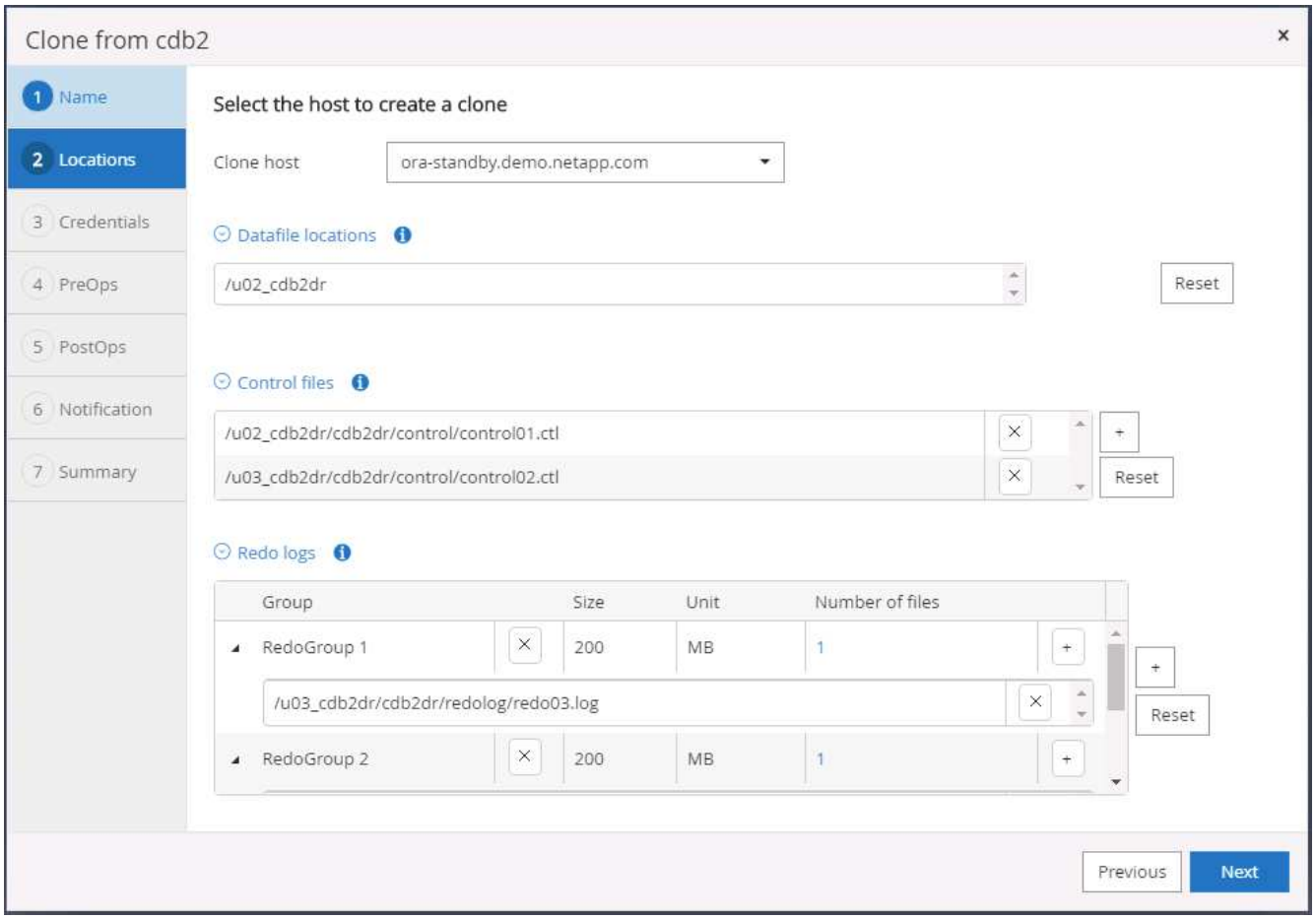
7. Stellen Sie ein Protokollvolume bereit und mounten Sie es auf dem Ziel-DR-Server für den Oracle-Flash-Wiederherstellungsbereich und die Online-Protokolle.



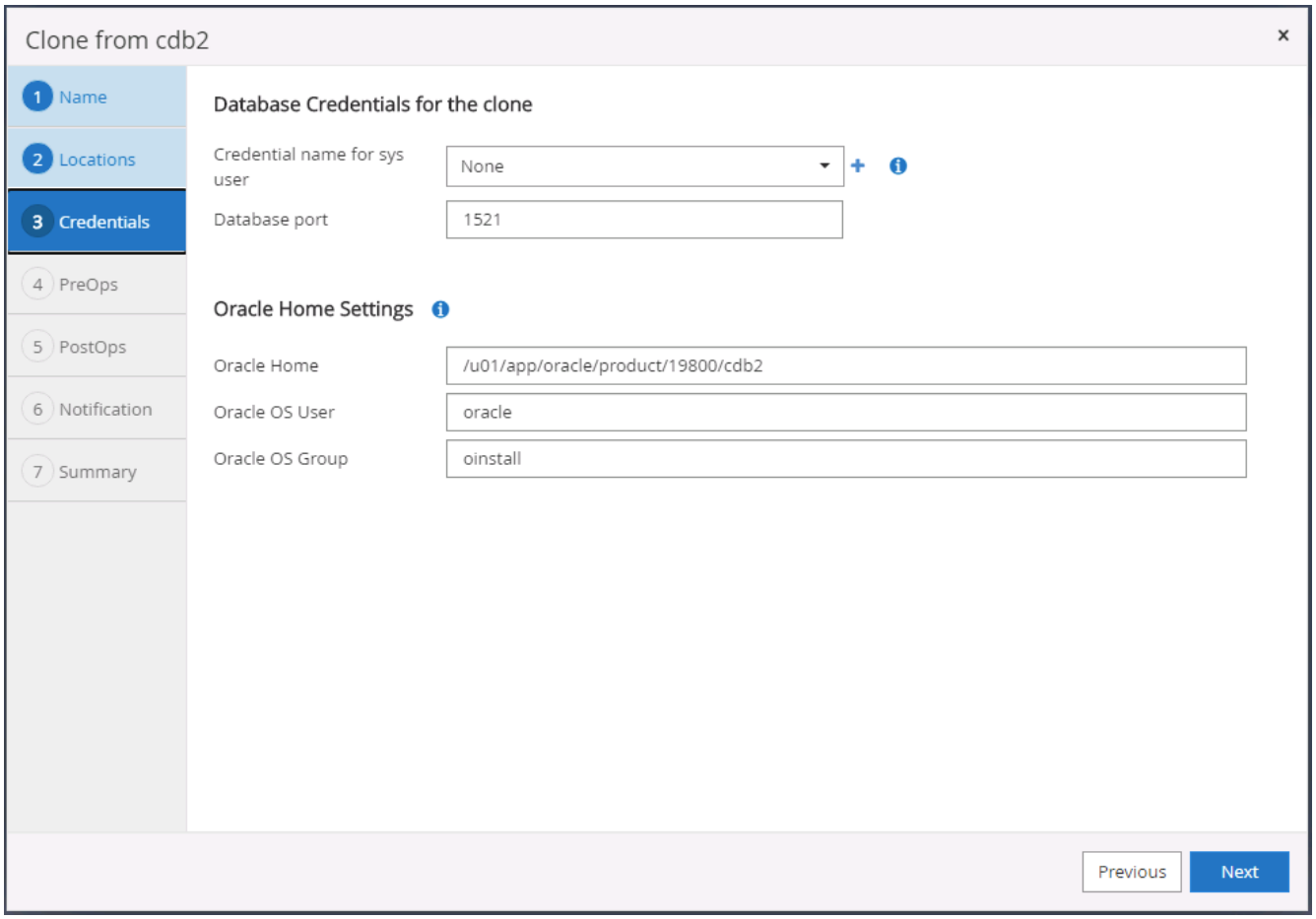


Beim Oracle-Klonvorgang wird kein Protokollvolume erstellt, das vor dem Klonen auf dem DR-Server bereitgestellt werden muss.

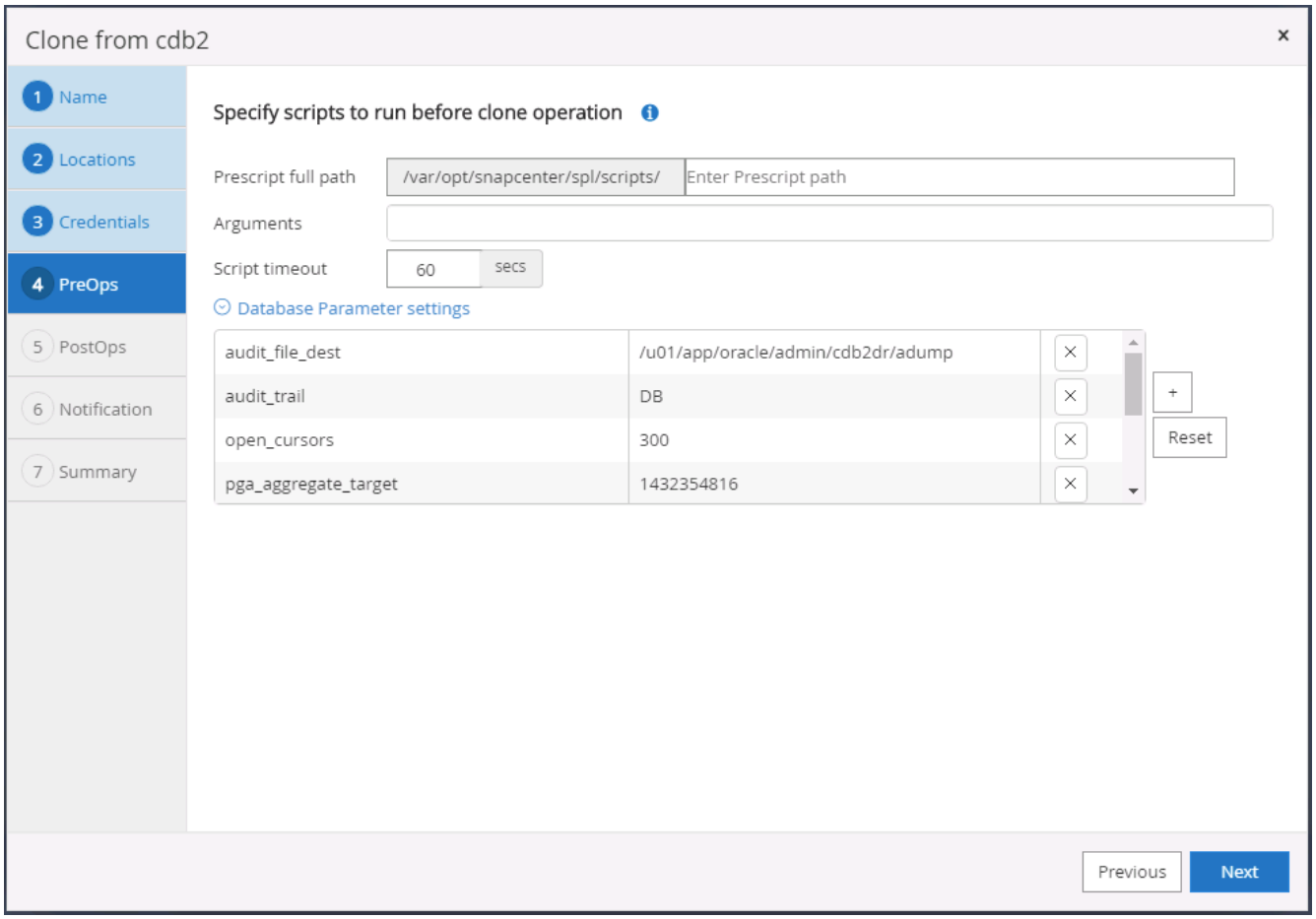
8. Wählen Sie den Ziel-Klonhost und den Speicherort für die Datendateien, Steuerdateien und Redo-Protokolle aus.



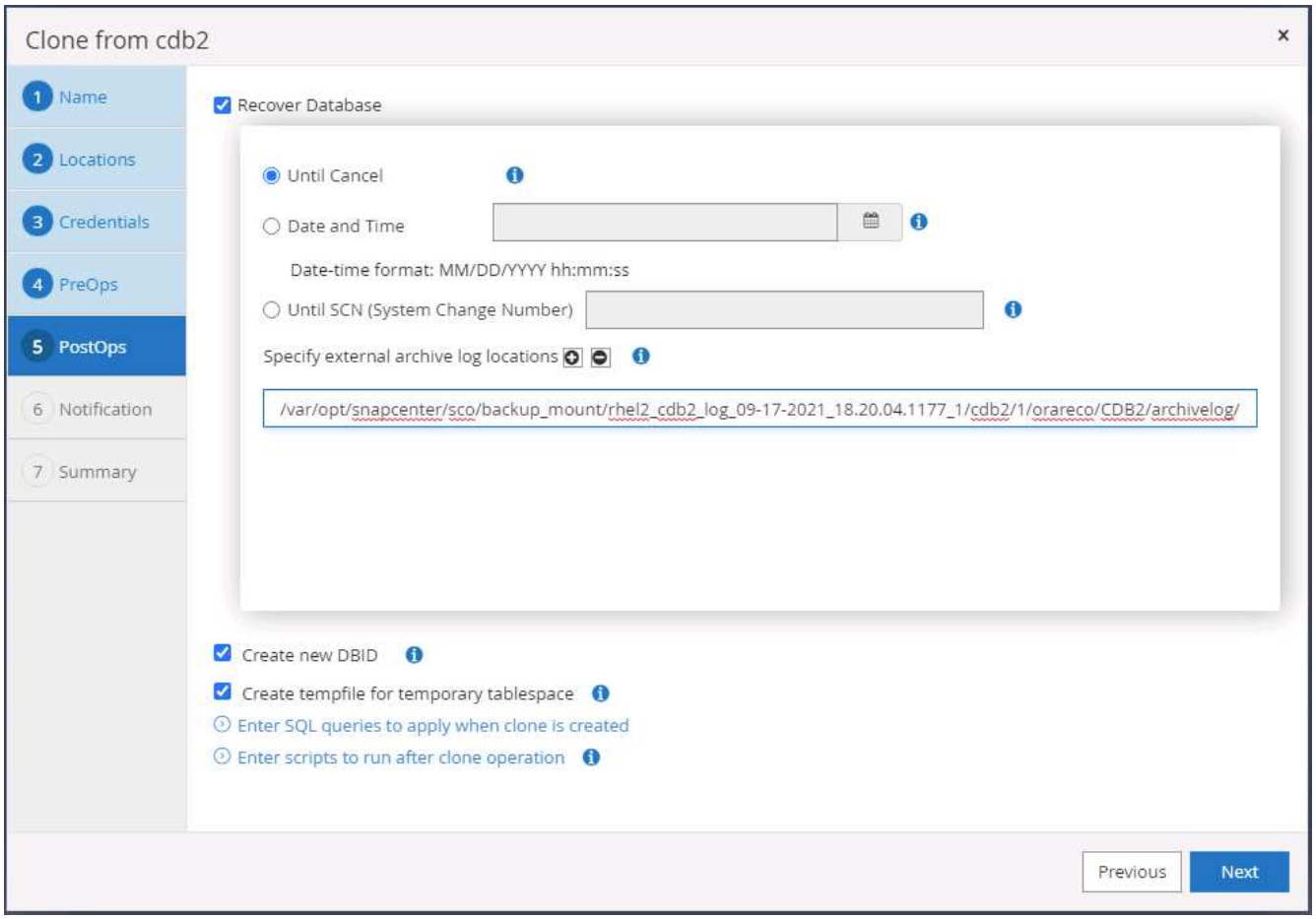
9. Wählen Sie die Anmeldeinformationen für den Klon aus. Geben Sie die Details der Oracle-Home-Konfiguration auf dem Zielserver ein.



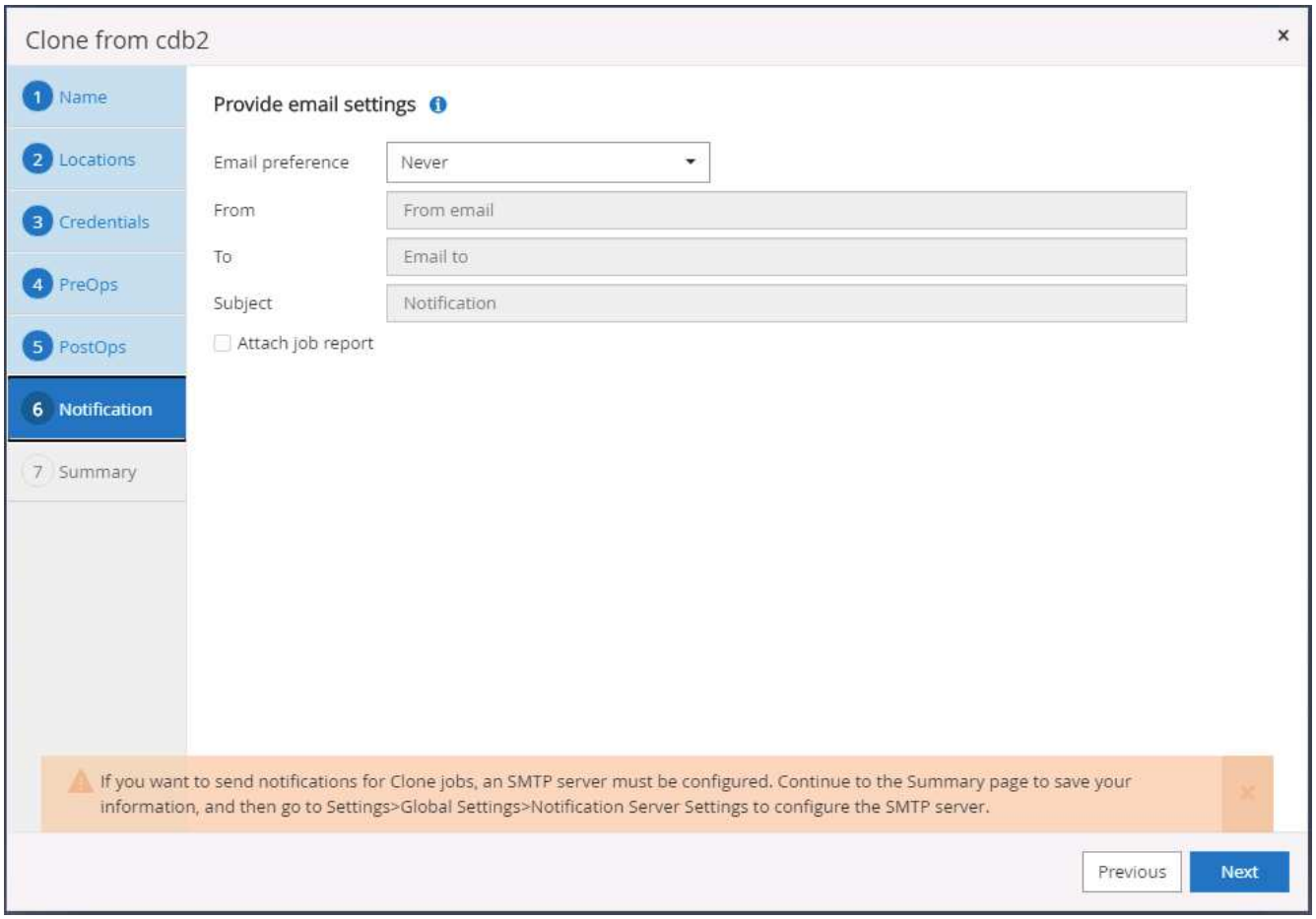
10. Geben Sie die Skripte an, die vor dem Klonen ausgeführt werden sollen. Datenbankparameter können bei Bedarf angepasst werden.



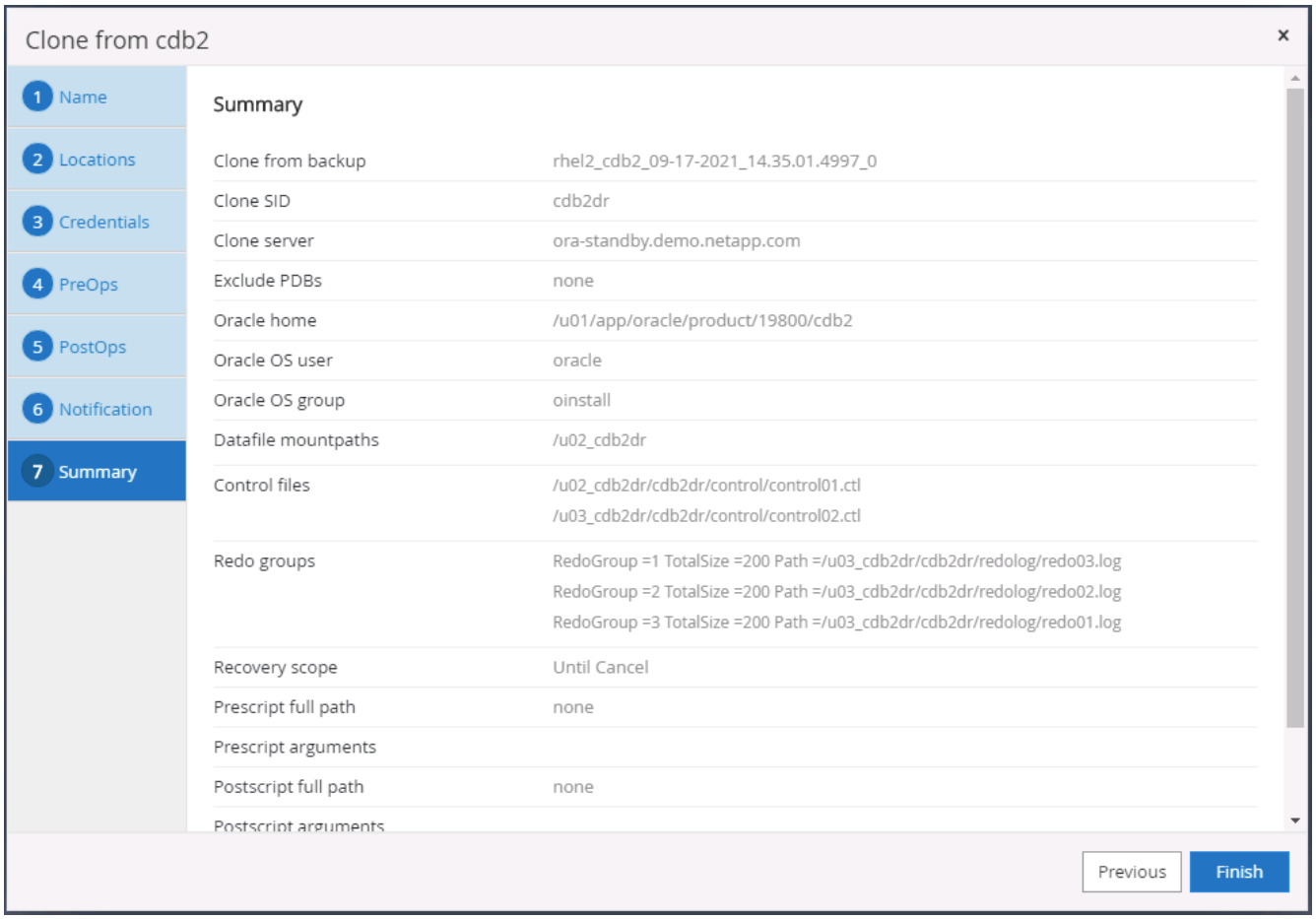
11. Wählen Sie „Bis zum Abbrechen“ als Wiederherstellungsoption aus, damit die Wiederherstellung alle verfügbaren Archivprotokolle durchläuft, um die letzte an den sekundären Cloud-Speicherort replizierte Transaktion wiederherzustellen.



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



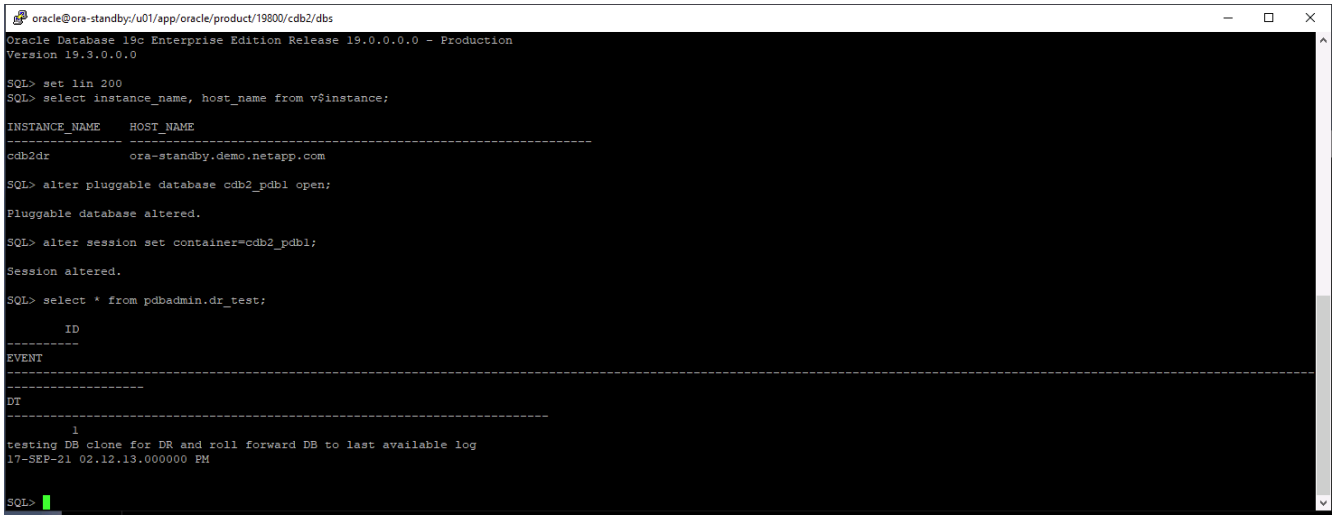
13. Zusammenfassung des DR-Klons.



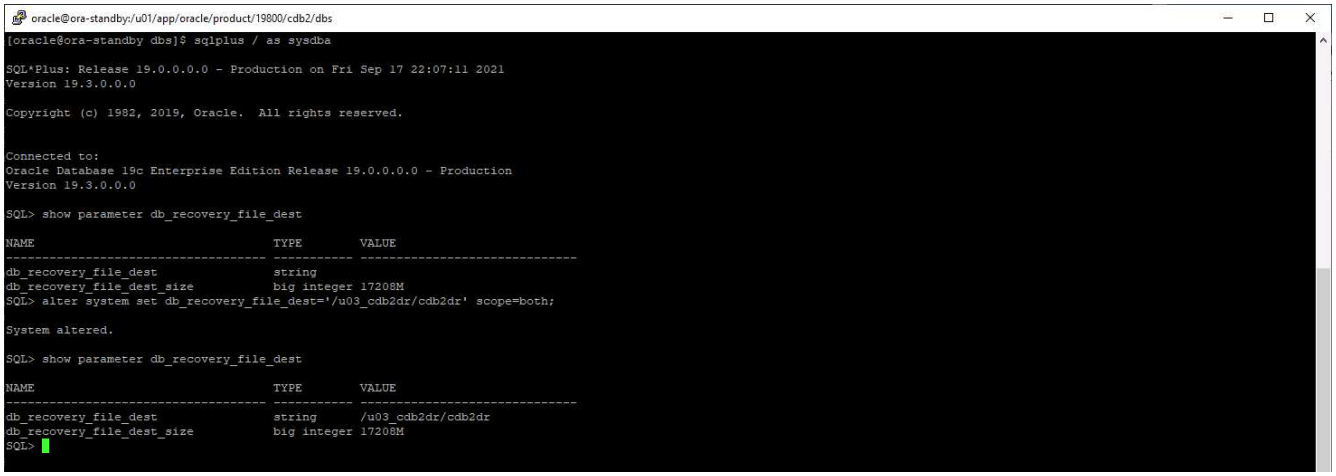
14. Geklonte Datenbanken werden unmittelbar nach Abschluss des Klonvorgangs bei SnapCenter registriert und stehen dann für den Backup-Schutz zur Verfügung.

Validierung und Konfiguration des Post-DR-Klons für Oracle

1. Validieren Sie die letzte Testtransaktion, die am DR-Standort in der Cloud gelöscht, repliziert und wiederhergestellt wurde.



2. Konfigurieren Sie den Flash-Wiederherstellungsbereich.

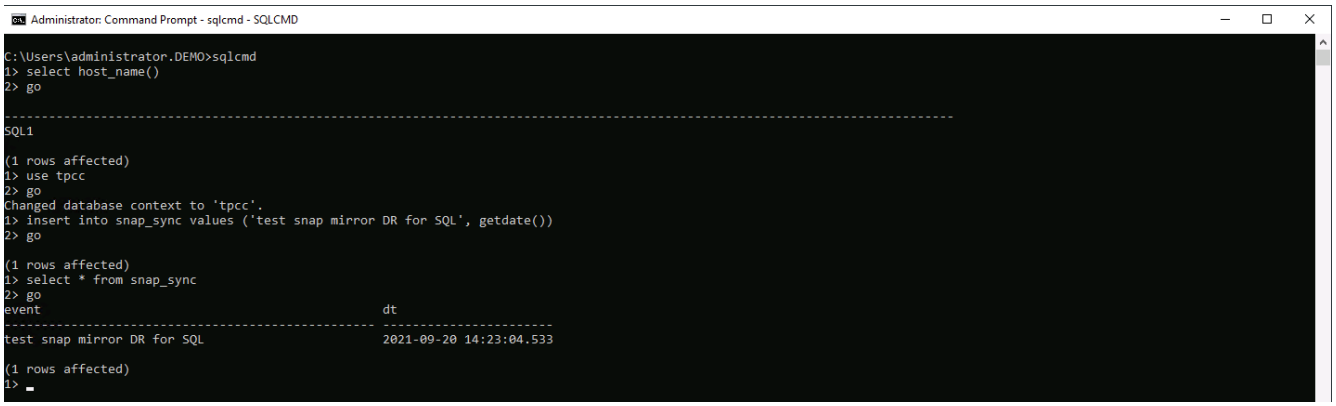


3. Konfigurieren Sie den Oracle-Listener für den Benutzerzugriff.
4. Trennen Sie das geklonte Volume vom replizierten Quellvolume.
5. Führen Sie eine umgekehrte Replikation von der Cloud zum lokalen Server durch und erstellen Sie den ausgefallenen lokalen Datenbankserver neu.

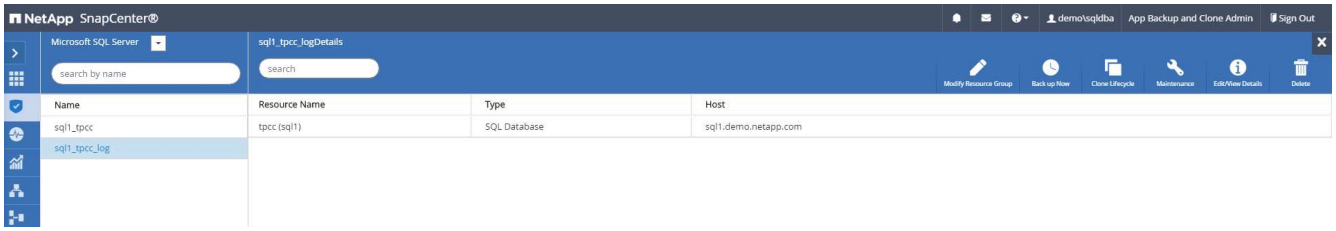
Durch die Klonaufteilung kann es zu einer deutlich höheren temporären Speicherplatzauslastung als im Normalbetrieb kommen. Nach dem Neuaufbau des lokalen DB-Servers kann jedoch zusätzlicher Speicherplatz freigegeben werden.

Klonen Sie eine lokale SQL-Produktionsdatenbank zur Notfallwiederherstellung in die Cloud.

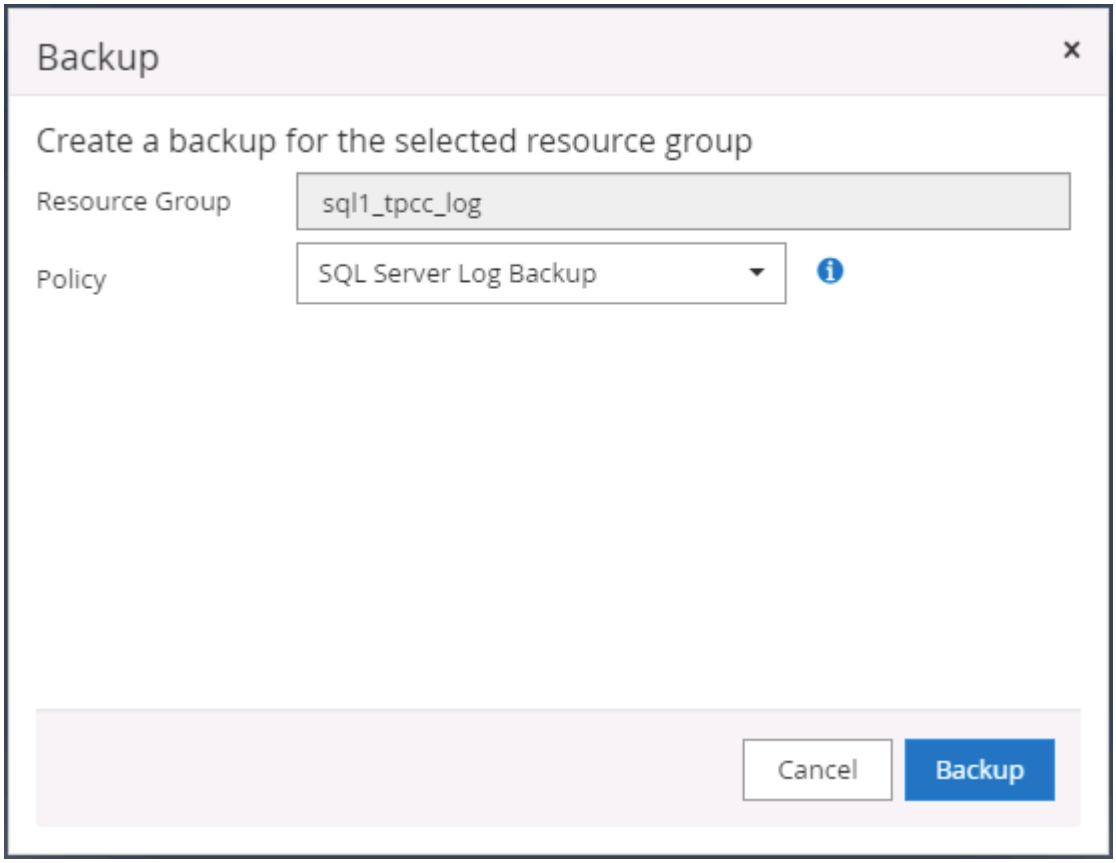
1. Um zu überprüfen, ob die SQL-Klonwiederherstellung das letzte verfügbare Protokoll durchlaufen hat, haben wir eine kleine Testtabelle erstellt und eine Zeile eingefügt. Die Testdaten würden nach einer vollständigen Wiederherstellung bis zum letzten verfügbaren Protokoll wiederhergestellt.



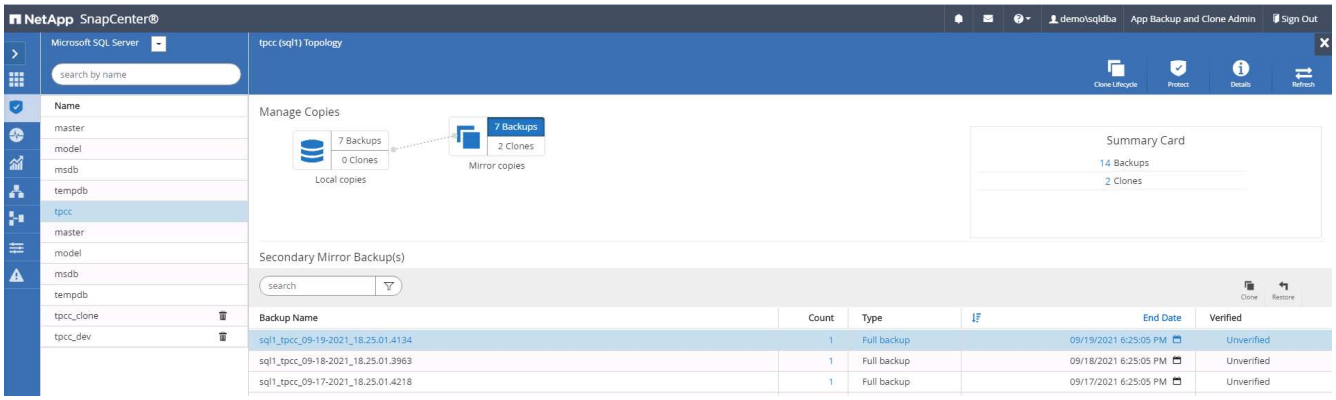
2. Melden Sie sich bei SnapCenter mit einer Datenbankverwaltungs-Benutzer-ID für SQL Server an. Navigieren Sie zur Registerkarte „Ressourcen“, auf der die SQL Server-Schutzressourcengruppe angezeigt wird.



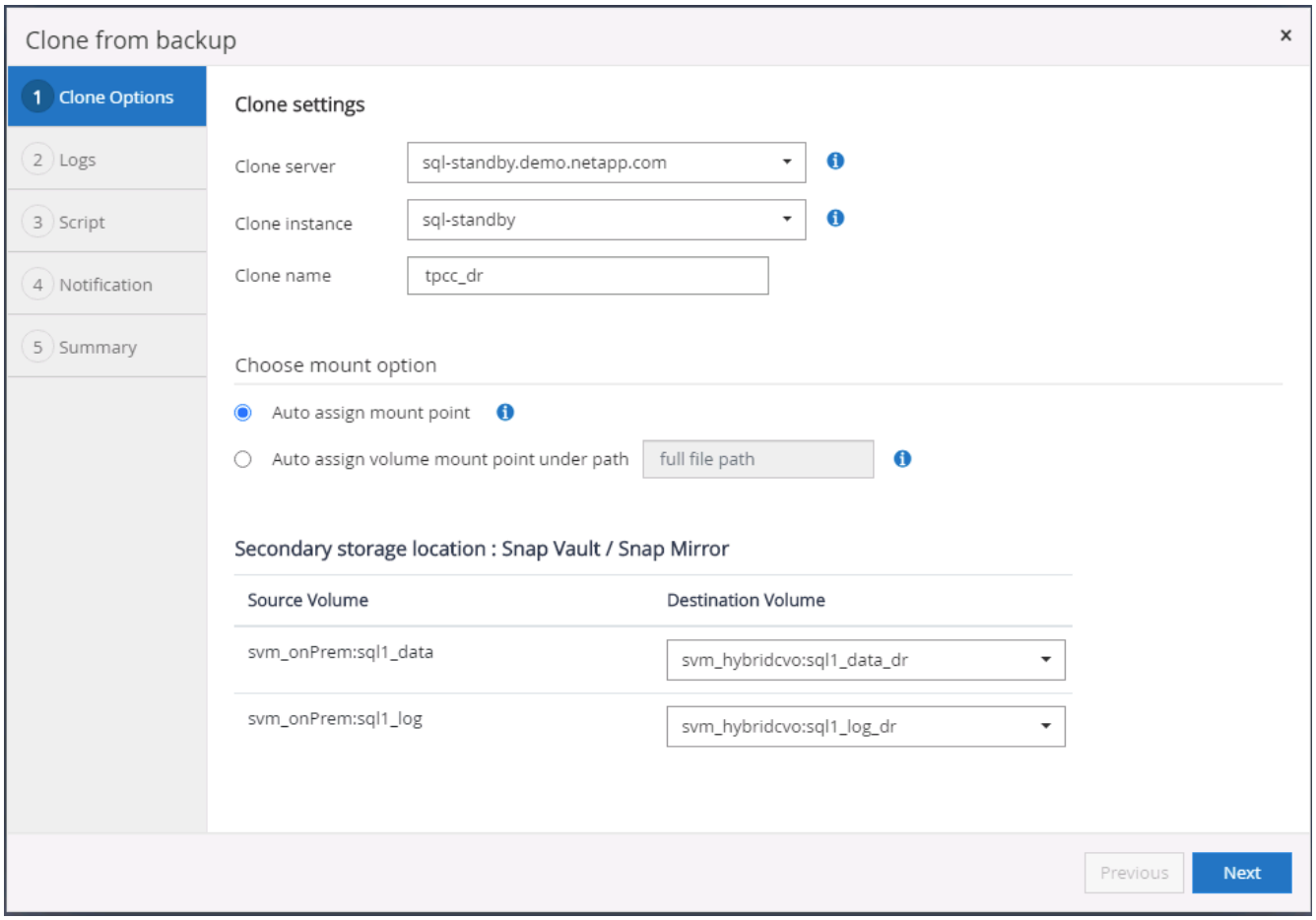
3. Führen Sie manuell eine Protokollsicherung aus, um die letzte zu replizierende Transaktion in den sekundären Speicher in der öffentlichen Cloud zu übertragen.



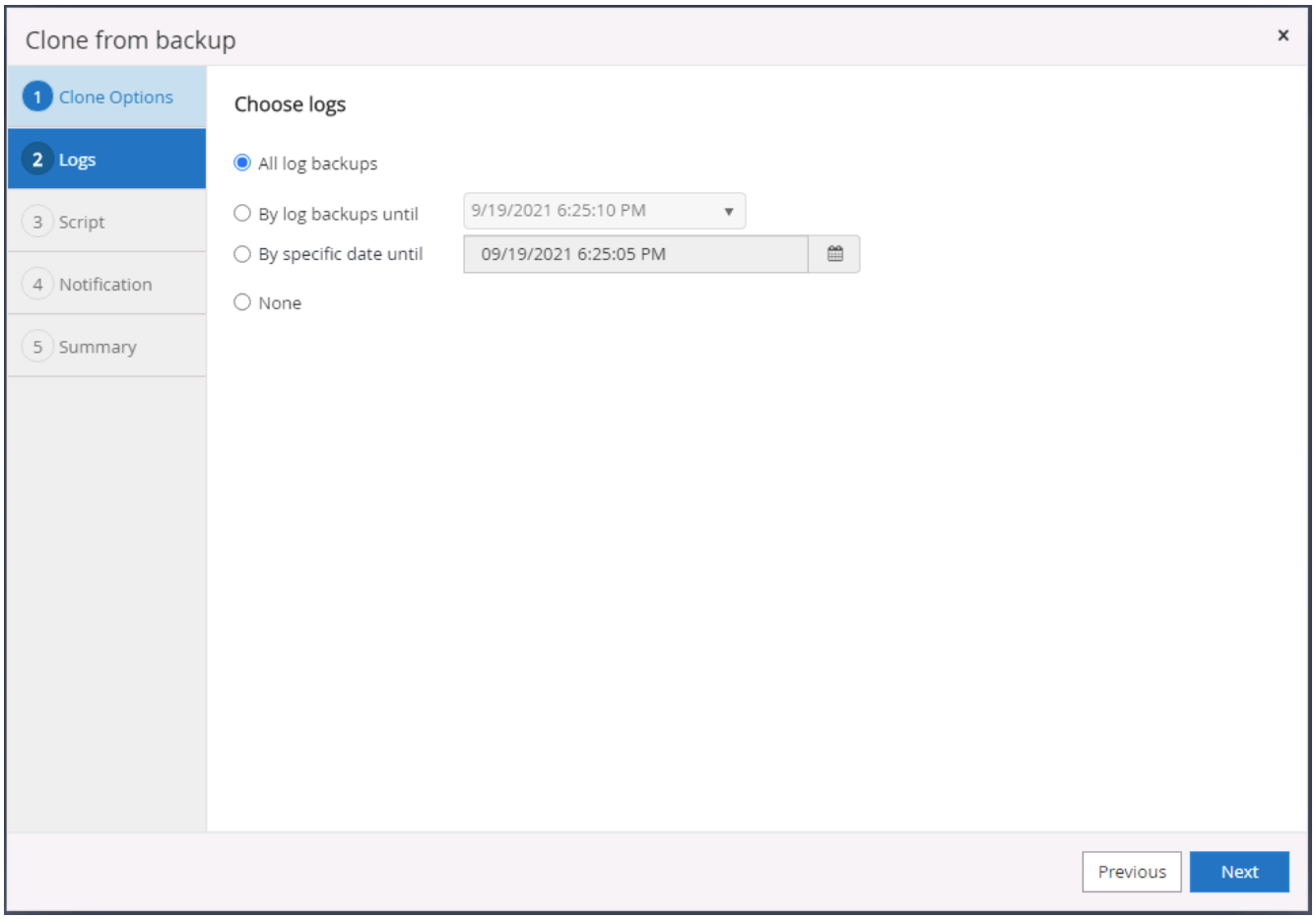
4. Wählen Sie die letzte vollständige SQL Server-Sicherung für den Klon aus.



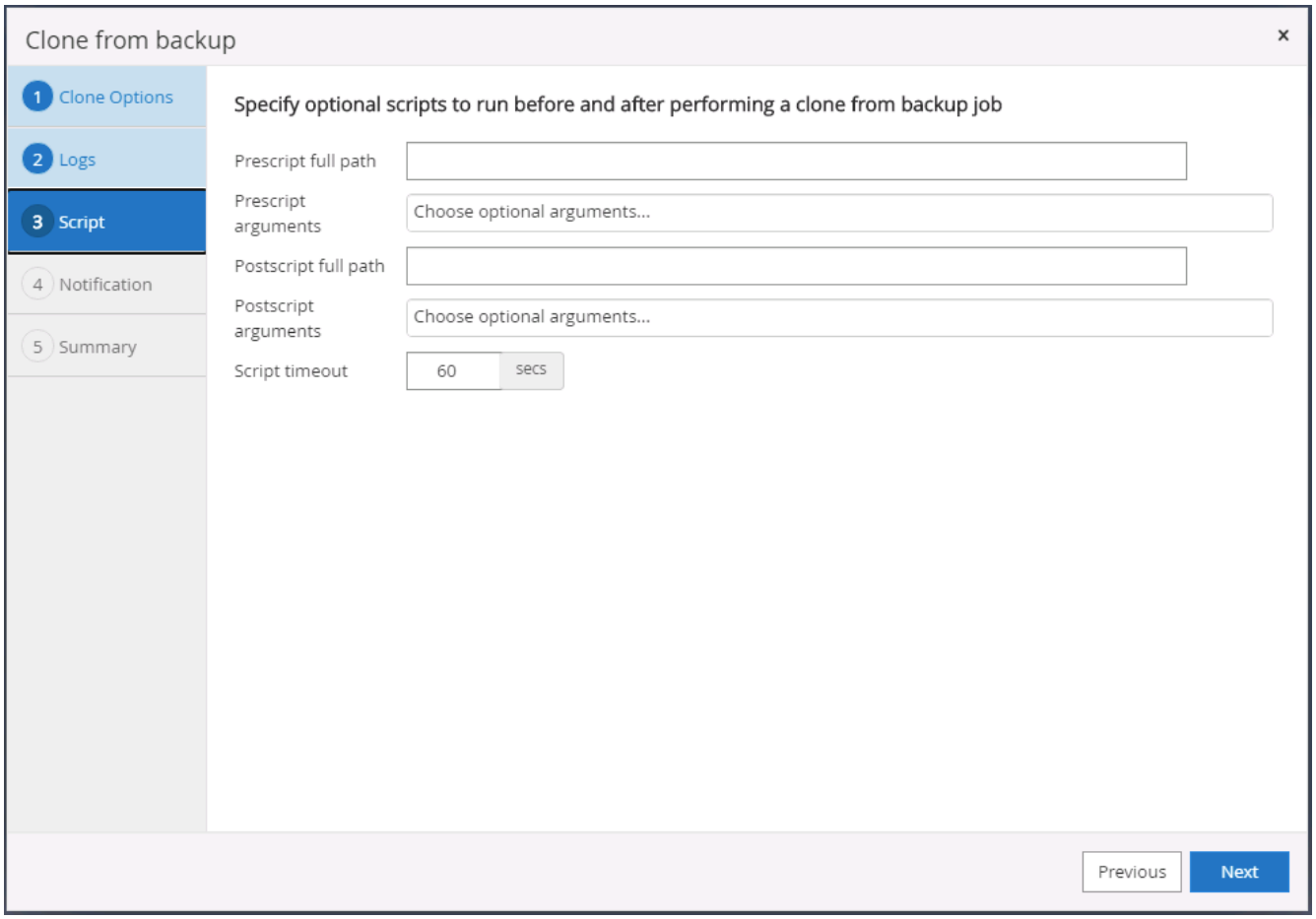
5. Legen Sie die Kloneinstellungen fest, z. B. Klonserver, Kloninstanz, Klonname und Mount-Option. Der sekundäre Speicherort, an dem das Klonen durchgeführt wird, wird automatisch ausgefüllt.



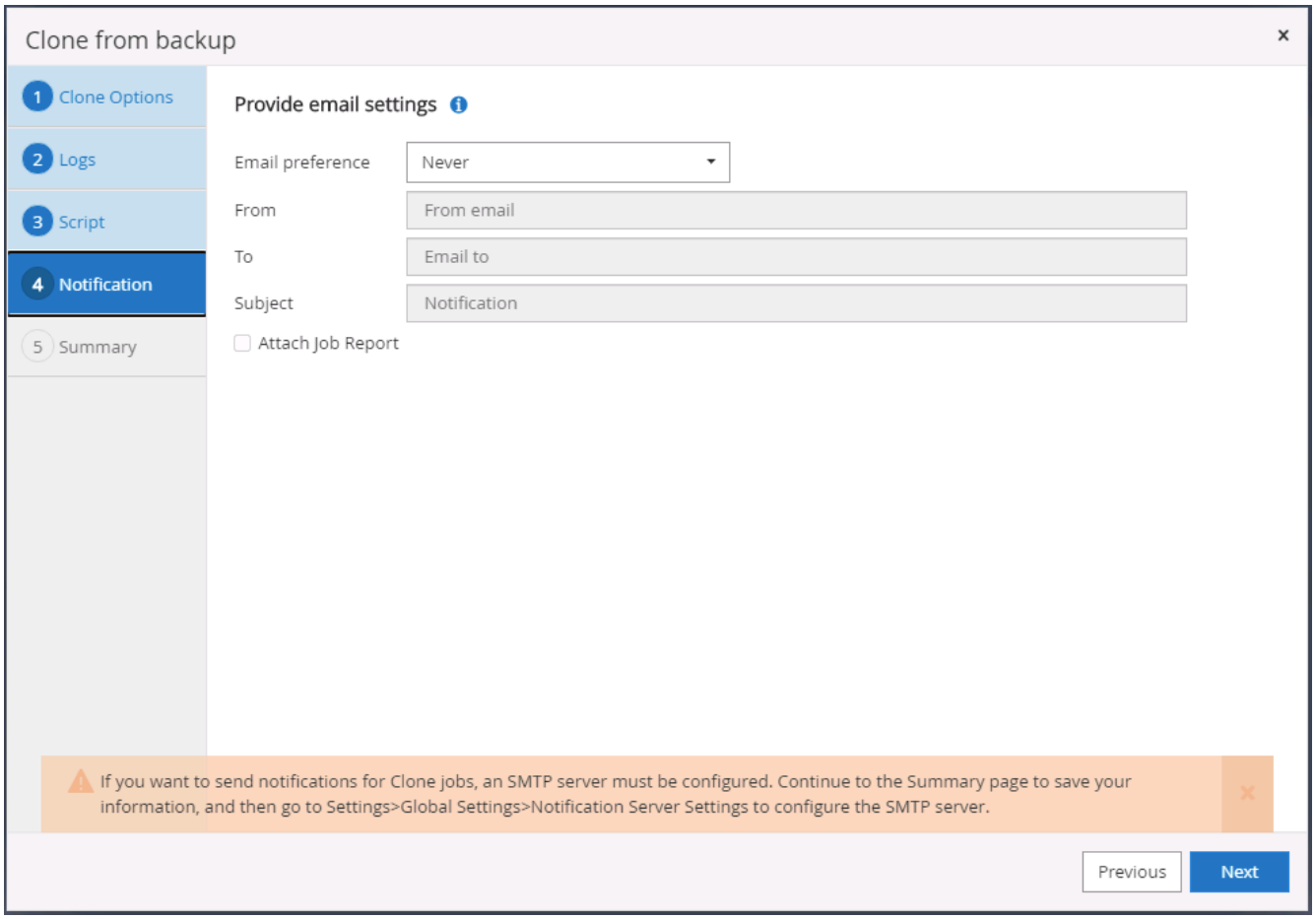
6. Wählen Sie alle anzuwendenden Protokollsicherungen aus.



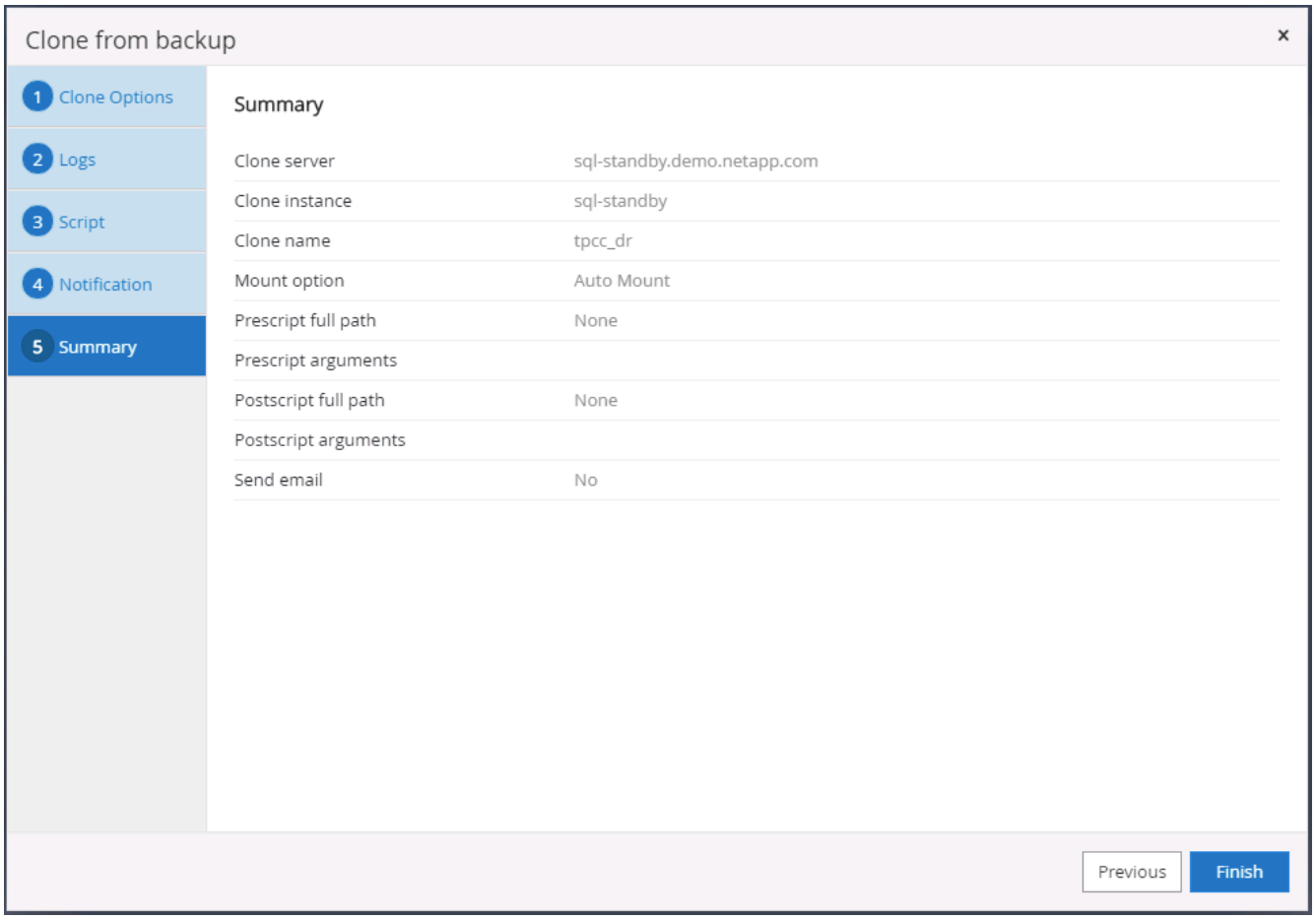
7. Geben Sie optionale Skripts an, die vor oder nach dem Klonen ausgeführt werden sollen.

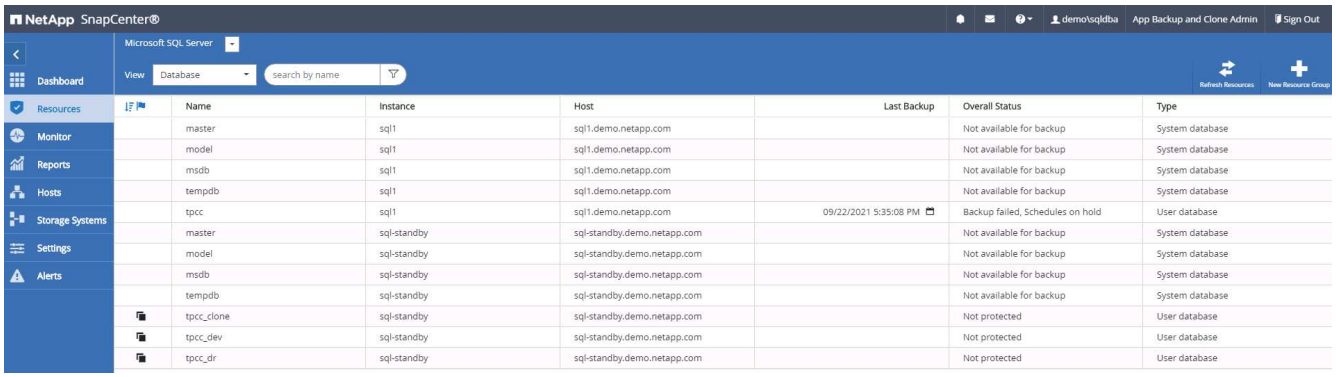


8. Geben Sie einen SMTP-Server an, wenn eine E-Mail-Benachrichtigung gewünscht ist.



9. Zusammenfassung des DR-Klons. Geklonte Datenbanken werden sofort bei SnapCenter registriert und stehen für den Backup-Schutz zur Verfügung.



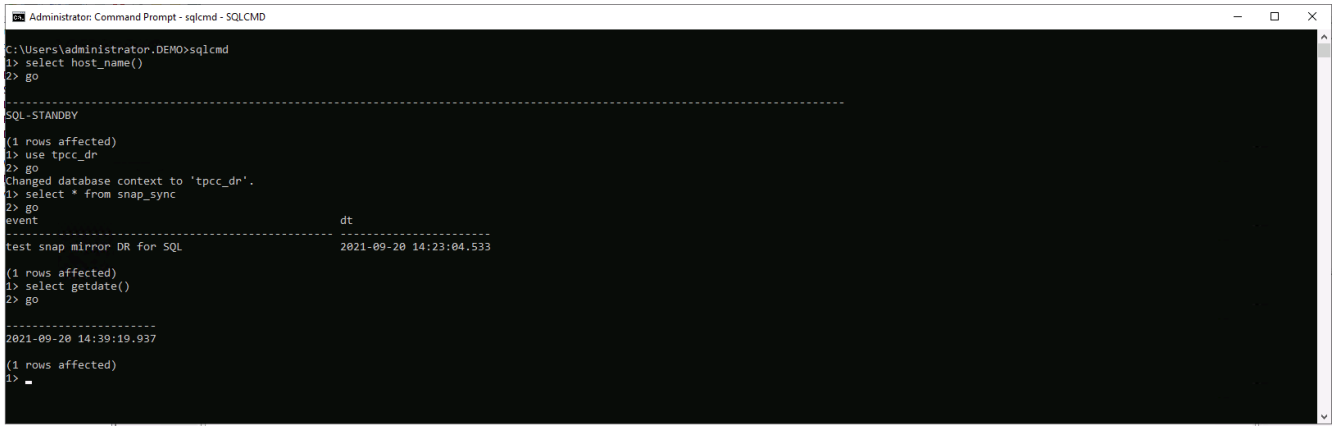


Validierung und Konfiguration des Post-DR-Klons für SQL

1. Überwachen Sie den Status des Klonauftrags.

2. Überprüfen Sie, ob die letzte Transaktion mit allen Protokolldateiklonen und -wiederherstellungen repliziert

und wiederhergestellt wurde.



3. Konfigurieren Sie ein neues SnapCenter -Protokollverzeichnis auf dem DR-Server für die SQL Server-Protokollsicherung.
4. Trennen Sie das geklonte Volume vom replizierten Quellvolume.
5. Führen Sie eine umgekehrte Replikation von der Cloud zum lokalen Server durch und erstellen Sie den ausgefallenen lokalen Datenbankserver neu.

Wo bekomme ich Hilfe?

Wenn Sie Hilfe bei dieser Lösung und den Anwendungsfällen benötigen, treten Sie bitte dem"Slack-Kanal für den Support der NetApp Solution Automation-Community" und suchen Sie nach dem Kanal zur Lösungsautomatisierung, um Ihre Fragen oder Anfragen zu posten.