Best Practices für die Bereitstellung von Oracle-Datenbanken auf AWS EC2 und FSx

NetApp database solutions

NetApp
August 18, 2025

Inhalt

Best Practices für die Bereitstellung von Oracle-Datenbanken auf AWS EC2 und FSx

WP-7357: Einführung in Best Practices zur Oracle-Datenbankbereitstellung auf EC2 und FSx

Allen Cao, Niyaz Mohamed, Jeffrey Steiner, NetApp

Viele unternehmenskritische Oracle-Datenbanken werden immer noch vor Ort gehostet und viele Unternehmen möchten diese Oracle-Datenbanken in eine öffentliche Cloud migrieren. Diese Oracle-Datenbanken sind häufig anwendungszentriert und erfordern daher benutzerspezifische Konfigurationen, eine Funktion, die bei vielen Public-Cloud-Angeboten mit Datenbanken als Service fehlt. Daher erfordert die aktuelle Datenbanklandschaft eine Oracle-Datenbanklösung auf Basis der öffentlichen Cloud, die auf einem leistungsstarken, skalierbaren Rechen- und Speicherdienst basiert, der einzigartige Anforderungen erfüllen kann. AWS EC2-Recheninstanzen und der AWS FSx-Speicherdienst könnten die fehlenden Teile dieses Puzzles sein, die Sie zum Erstellen und Migrieren Ihrer unternehmenskritischen Oracle-Datenbank-Workloads in eine öffentliche Cloud nutzen können.

Amazon Elastic Compute Cloud (Amazon EC2) ist ein Webdienst, der sichere, skalierbare Rechenkapazität in der Cloud bereitstellt. Es wurde entwickelt, um Unternehmen das Cloud-Computing im Web-Maßstab zu erleichtern. Über die einfache Amazon EC2-Webdienstschnittstelle können Sie Kapazitäten mit minimalem Aufwand abrufen und konfigurieren. Es bietet Ihnen die vollständige Kontrolle über Ihre Computerressourcen und ermöglicht Ihnen die Ausführung in der bewährten Computerumgebung von Amazon.

Amazon FSx ONTAP ist ein AWS-Speicherdienst, der den branchenführenden NetApp ONTAP Block- und Dateispeicher verwendet, der NFS, SMB und iSCSI bereitstellt. Mit einer so leistungsstarken Speicher-Engine war es noch nie so einfach, unternehmenskritische Oracle-Datenbank-Apps mit Reaktionszeiten von unter einer Millisekunde, mehreren GBps Durchsatz und über 100.000 IOPS pro Datenbankinstanz auf AWS zu verlagern. Noch besser: Der FSx-Speicherdienst verfügt über eine native Replikationsfunktion, mit der Sie Ihre lokale Oracle-Datenbank problemlos zu AWS migrieren oder Ihre unternehmenskritische Oracle-Datenbank für HA oder DR in eine sekundäre AWS-Verfügbarkeitszone replizieren können.

Das Ziel dieser Dokumentation besteht darin, schrittweise Prozesse, Verfahren und Best-Practice-Anleitungen zur Bereitstellung und Konfiguration einer Oracle-Datenbank mit FSx-Speicher und einer EC2-Instance bereitzustellen, die eine ähnliche Leistung wie ein lokales System bietet. NetApp bietet außerdem ein Automatisierungs-Toolkit, das die meisten Aufgaben automatisiert, die für die Bereitstellung, Konfiguration und Verwaltung Ihrer Oracle-Datenbank-Workload in der AWS Public Cloud erforderlich sind.

Um mehr über die Lösung und den Anwendungsfall zu erfahren, sehen Sie sich das folgende Übersichtsvideo an:

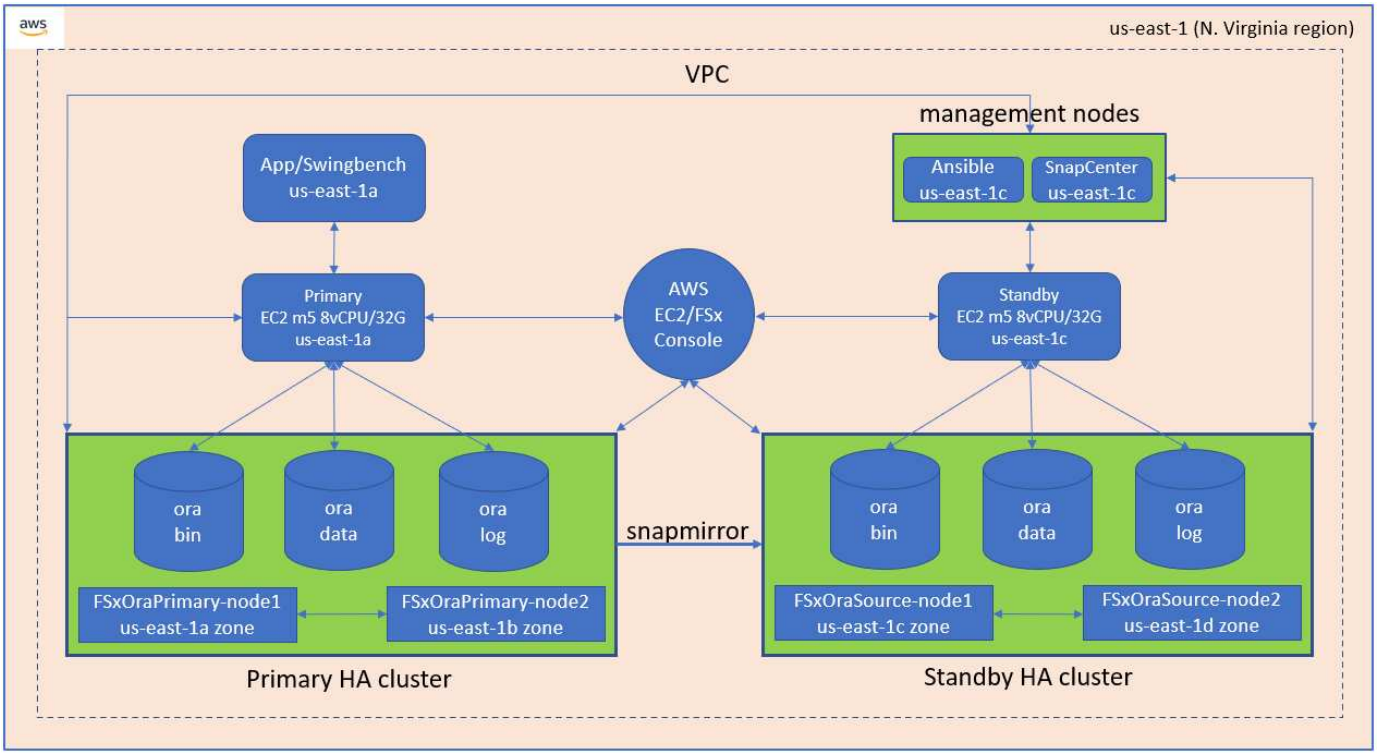
"Modernisieren Sie Ihre Oracle-Datenbank mit Hybrid Cloud in AWS und FSx ONTAP, Teil 1 – Anwendungsfall und Lösungsarchitektur"

Lösungsarchitektur

Das folgende Architekturdiagramm veranschaulicht eine hochverfügbare Oracle-Datenbankbereitstellung auf einer AWS EC2-Instance mit dem FSx-Speicherdienst. Für die Notfallwiederherstellung kann ein ähnliches Bereitstellungsschema eingerichtet werden, allerdings mit dem Standby in einer anderen Region.

Innerhalb der Umgebung wird die Oracle-Compute-Instanz über eine AWS EC2-Instanzkonsole bereitgestellt. Über die Konsole sind mehrere EC2-Instanztypen verfügbar. NetApp empfiehlt die Bereitstellung eines datenbankorientierten EC2-Instanztyps, beispielsweise eines m5 Ami-Images mit RedHat Enterprise Linux 8 und bis zu 10 Gps Netzwerkbandbreite.

Oracle-Datenbankspeicher auf FSx-Volumes wird dagegen mit der AWS FSx-Konsole oder CLI bereitgestellt. Anschließend werden die Oracle-Binär-, Daten- oder Protokollvolumes präsentiert und auf einem Linux-Host der EC2-Instance gemountet. Jedem Daten- oder Protokollvolume können je nach dem verwendeten zugrunde liegenden Speicherprotokoll mehrere LUNs zugewiesen werden.



Ein FSx-Speichercluster ist mit doppelter Redundanz konzipiert, sodass sowohl der primäre als auch der Standby-Speichercluster in zwei verschiedenen Verfügbarkeitszonen bereitgestellt werden. Datenbank-Volumes werden in einem vom Benutzer konfigurierbaren Intervall für alle Oracle-Binär-, Daten- und Protokoll-Volumes von einem primären FSx-Cluster auf einen Standby-FSx-Cluster repliziert.

Diese hochverfügbare Oracle-Umgebung wird mit einem Ansible-Controller-Knoten und einem SnapCenter -Backup-Server und UI-Tool verwaltet. Die Installation, Konfiguration und Replikation von Oracle werden mithilfe von auf Ansible-Playbooks basierenden Toolkits automatisiert. Alle Updates des Kernel-Betriebssystems der Oracle EC2-Instanz oder Oracle-Patches können parallel ausgeführt werden, um die Synchronisierung zwischen Primär- und Standby-Instanz aufrechtzuerhalten. Tatsächlich kann die anfängliche Automatisierungseinrichtung bei Bedarf problemlos erweitert werden, um einige sich täglich wiederholende Oracle-Aufgaben auszuführen.

SnapCenter bietet Workflows für die zeitpunktbezogene Wiederherstellung von Oracle-Datenbanken oder bei Bedarf für das Klonen von Datenbanken in der primären oder Standby-Zone. Über die SnapCenter -Benutzeroberfläche können Sie die Sicherung und Replikation von Oracle-Datenbanken auf den Standby-FSx-Speicher für hohe Verfügbarkeit oder Notfallwiederherstellung basierend auf Ihren RTO- oder RPO-Zielen konfigurieren.

Die Lösung bietet einen alternativen Prozess, der ähnliche Funktionen bietet wie die Bereitstellung von Oracle RAC und Data Guard.

Zu berücksichtigende Faktoren bei der Bereitstellung einer Oracle-Datenbank

Eine öffentliche Cloud bietet zahlreiche Möglichkeiten für die Datenverarbeitung und Speicherung. Die Verwendung der richtigen Art von Datenverarbeitungsinstanz und Speicher-Engine ist ein guter Ausgangspunkt für die Datenbankbereitstellung. Sie sollten außerdem Rechen- und Speicherkonfigurationen auswählen, die für Oracle-Datenbanken optimiert sind.

In den folgenden Abschnitten werden die wichtigsten Überlegungen beim Bereitstellen einer Oracle-Datenbank in einer öffentlichen AWS-Cloud auf einer EC2-Instance mit FSx-Speicher beschrieben.

VM-Leistung

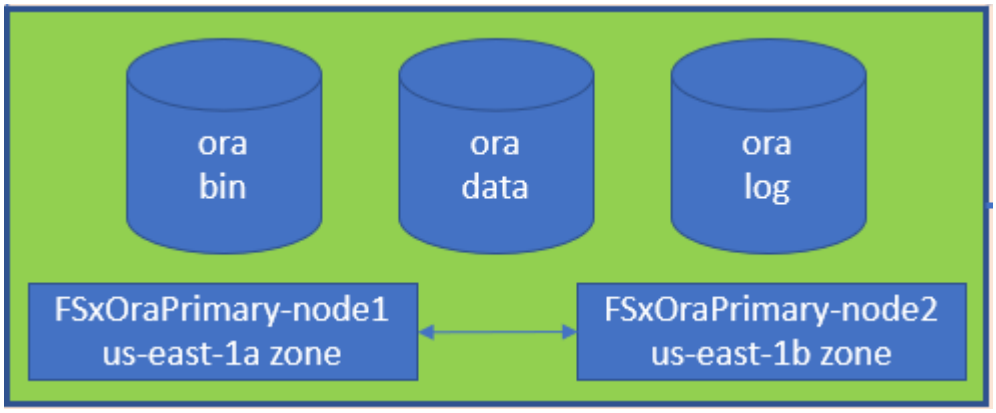
Die Auswahl der richtigen VM-Größe ist für die optimale Leistung einer relationalen Datenbank in einer öffentlichen Cloud wichtig. Für eine bessere Leistung empfiehlt NetApp die Verwendung einer Instanz der EC2 M5-Serie für die Oracle-Bereitstellung, die für Datenbank-Workloads optimiert ist. Derselbe Instanztyp wird auch verwendet, um eine RDS-Instanz für Oracle von AWS zu betreiben.

- Wählen Sie basierend auf den Arbeitslastmerkmalen die richtige vCPU- und RAM-Kombination.
- Fügen Sie einer VM Swap-Speicher hinzu. Bei der standardmäßigen Bereitstellung einer EC2-Instanz wird kein Swap-Speicherplatz erstellt, was für eine Datenbank nicht optimal ist.

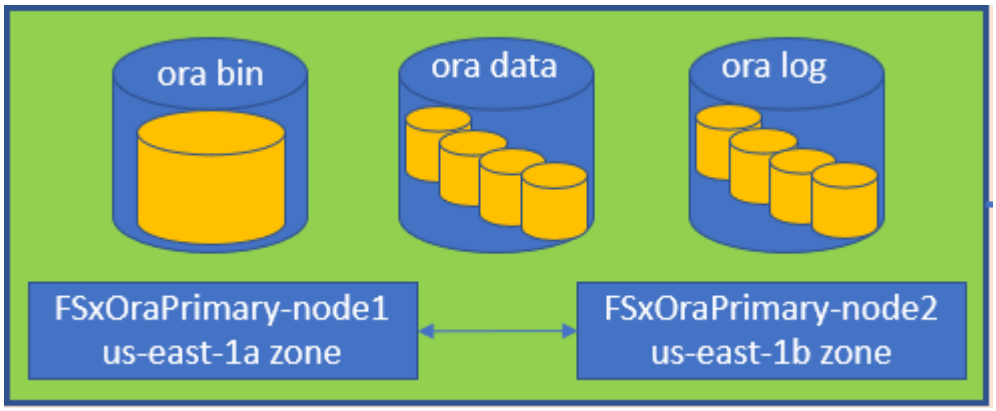
Speicherlayout und -einstellungen

NetApp empfiehlt das folgende Speicherlayout:

- Für die NFS-Speicherung wird ein Volume-Layout mit drei Volumes empfohlen: eines für die Oracle-Binärdatei, eines für Oracle-Daten und eine doppelte Steuerdatei und eines für das aktive Oracle-Protokoll, das archivierte Protokoll und die Steuerdatei.



- Für die iSCSI-Speicherung wird ein Volume-Layout mit drei Volumes empfohlen: eines für die Oracle-Binärdatei, eines für Oracle-Daten und eine doppelte Steuerdatei und eines für das aktive Oracle-Protokoll, das archivierte Protokoll und die Steuerdatei. Idealerweise sollte jedoch jedes Daten- und Protokollvolume vier LUNs enthalten. Die LUNs sind auf den HA-Clusterknoten ideal ausbalanciert.



- Für Speicher-IOPS und -Durchsatz können Sie den Schwellenwert für bereitgestellte IOPS und Durchsatz für den FSx-Speichercluster auswählen und diese Parameter können jederzeit im laufenden Betrieb angepasst werden, wenn sich die Arbeitslast ändert.
  - Die automatische IOPS-Einstellung beträgt drei IOPS pro GiB zugewiesener Speicherkapazität oder benutzerdefiniertem Speicher bis zu 80.000.
  - Der Durchsatz wird wie folgt erhöht: 128, 256, 512, 1024, 2045 MBps.

Überprüfen Sie die"Amazon FSx ONTAP -Leistung" Dokumentation zur Dimensionierung von Durchsatz und IOPS.

NFS-Konfiguration

Linux, das am weitesten verbreitete Betriebssystem, verfügt über native NFS-Funktionen. Oracle bietet den Direct NFS (dNFS)-Client an, der nativ in Oracle integriert ist. Oracle unterstützt NFSv3 seit über 20 Jahren. dNFS wird mit NFSv3 in allen Versionen von Oracle unterstützt. NFSv4 wird von allen Betriebssystemen unterstützt, die dem NFSv4-Standard folgen. dNFS-Unterstützung für NFSv4 erfordert Oracle 12.1.0.2 oder höher. NFSv4.1 erfordert spezielle Betriebssystemunterstützung. Informationen zu unterstützten Betriebssystemen finden Sie im NetApp Interoperability Matrix Tool (IMT). dNFS-Unterstützung für NFSv4.1 erfordert Oracle Version 19.3.0.0 oder höher.

Die automatisierte Oracle-Bereitstellung mit dem NetApp Automatisierungs-Toolkit konfiguriert dNFS automatisch auf NFSv3.

Weitere zu berücksichtigende Faktoren:

- TCP-Slot-Tabellen sind das NFS-Äquivalent zur Warteschlangentiefe des Host-Bus-Adapters (HBA). Diese Tabellen steuern die Anzahl der NFS-Operationen, die zu einem bestimmten Zeitpunkt ausstehen können. Der Standardwert liegt normalerweise bei 16, was für eine optimale Leistung viel zu niedrig ist. Bei neueren Linux-Kerneln tritt das gegenteilige Problem auf, da diese das TCP-Slot-Tabellenlimit automatisch auf ein Niveau erhöhen können, das den NFS-Server mit Anfragen überlastet.

  Um eine optimale Leistung zu erzielen und Leistungsprobleme zu vermeiden, passen Sie die Kernelparameter, die die TCP-Slot-Tabellen steuern, auf 128 an.

```
sysctl -a | grep tcp.*.slot_table
```

- Die folgende Tabelle enthält empfohlene NFS-Mount-Optionen für Linux NFSv3 – Einzelinstanz.

File Type	Mount Options
• Control files • Data files • Redo logs	rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsize=65536
• ORACLE_HOME • ORACLE_BASE	rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsize=65536

Überprüfen Sie vor der Verwendung von dNFS, ob die im Oracle-Dokument 1495104.1 beschriebenen Patches installiert sind. Die NetApp -Supportmatrix für NFSv3 und NFSv4 umfasst keine spezifischen Betriebssysteme. Alle Betriebssysteme, die dem RFC entsprechen, werden unterstützt. Wenn Sie im Online IMT nach NFSv3- oder NFSv4-Unterstützung suchen, wählen Sie kein bestimmtes Betriebssystem aus, da keine Übereinstimmungen angezeigt werden. Alle Betriebssysteme werden implizit durch die allgemeine Richtlinie unterstützt.

Hochverfügbarkeit

Wie in der Lösungsarchitektur angegeben, basiert HA auf der Replikation auf Speicherebene. Daher hängen der Start und die Verfügbarkeit von Oracle davon ab, wie schnell die Rechen- und Speicherkapazität hochgefahren und wiederhergestellt werden kann. Beachten Sie die folgenden Schlüsselfaktoren:

- Halten Sie eine Standby-Compute-Instanz bereit und synchronisieren Sie sie mit der primären über ein paralleles Ansible-Update auf beiden Hosts.
- Replizieren Sie das Binärvolume vom primären Volume für Standby-Zwecke, damit Sie Oracle nicht in letzter Minute installieren und herausfinden müssen, was installiert und gepatcht werden muss.
- Die Replikationshäufigkeit bestimmt, wie schnell die Oracle-Datenbank wiederhergestellt werden kann, um den Dienst wieder verfügbar zu machen. Es besteht ein Kompromiss zwischen Replikationshäufigkeit und Speicherverbrauch.
- Nutzen Sie die Automatisierung, um die Wiederherstellung und Umstellung auf Standby schnell und ohne menschliche Fehler durchzuführen. NetApp stellt hierfür ein Automatisierungs-Toolkit bereit.

Schrittweise Oracle-Bereitstellungsverfahren auf AWS EC2 und FSx

In diesem Abschnitt werden die Bereitstellungsverfahren für die Bereitstellung einer benutzerdefinierten Oracle RDS-Datenbank mit FSx-Speicher beschrieben.

Stellen Sie eine EC2-Linux-Instance für Oracle über die EC2-Konsole bereit

Wenn Sie neu bei AWS sind, müssen Sie zunächst eine AWS-Umgebung einrichten. Die Registerkarte „Dokumentation“ auf der Zielseite der AWS-Website bietet Links zu EC2-Anweisungen zum Bereitstellen einer Linux EC2-Instanz, die zum Hosten Ihrer Oracle-Datenbank über die AWS EC2-Konsole verwendet werden

kann. Der folgende Abschnitt ist eine Zusammenfassung dieser Schritte. Einzelheiten finden Sie in der verlinkten AWS EC2-spezifischen Dokumentation.

Einrichten Ihrer AWS EC2-Umgebung

Sie müssen ein AWS-Konto erstellen, um die erforderlichen Ressourcen zum Ausführen Ihrer Oracle-Umgebung auf dem EC2- und FSx-Dienst bereitzustellen. Die folgende AWS-Dokumentation liefert die notwendigen Details:

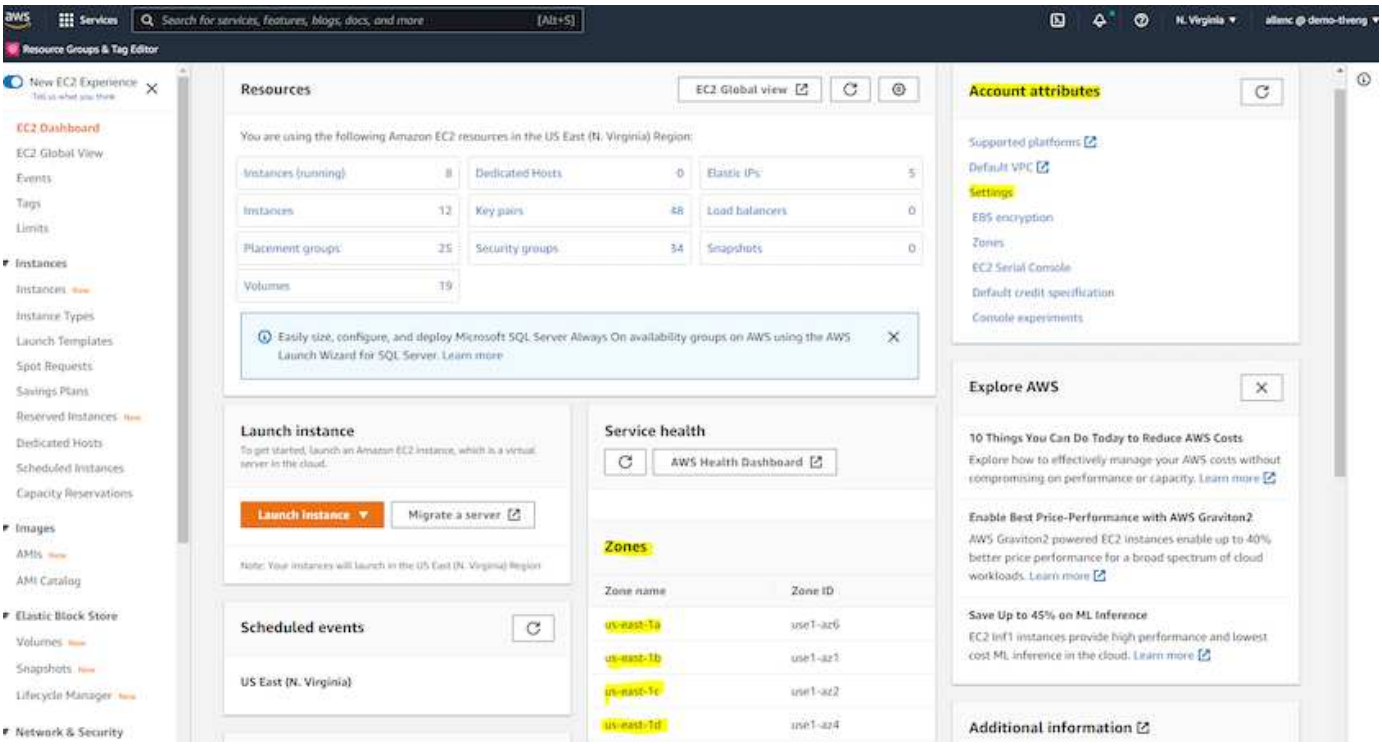
- "Einrichten zur Verwendung von Amazon EC2"

Schlüsselthemen:

- Registrieren Sie sich bei AWS.
- Erstellen Sie ein Schlüsselpaar.
- Erstellen Sie eine Sicherheitsgruppe.

Aktivieren mehrerer Verfügbarkeitszonen in AWS-Kontoattributen

Für eine Oracle-Hochverfügbarkeitskonfiguration, wie im Architekturdiagramm dargestellt, müssen Sie mindestens vier Verfügbarkeitszonen in einer Region aktivieren. Die mehreren Verfügbarkeitszonen können auch in verschiedenen Regionen liegen, um die erforderlichen Entfernungen für die Notfallwiederherstellung einzuhalten.



Erstellen und Verbinden mit einer EC2-Instance zum Hosten einer Oracle-Datenbank

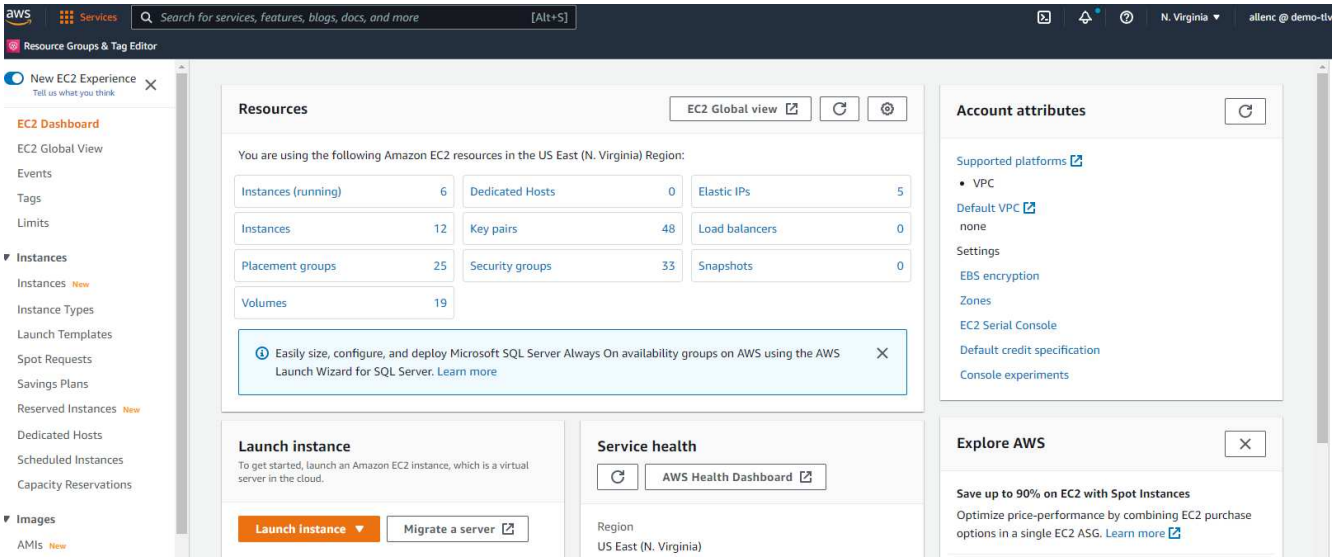
Sehen Sie sich das Tutorial an"Erste Schritte mit Amazon EC2 Linux-Instances" für schrittweise Bereitstellungsverfahren und Best Practices.

Schlüsselthemen:

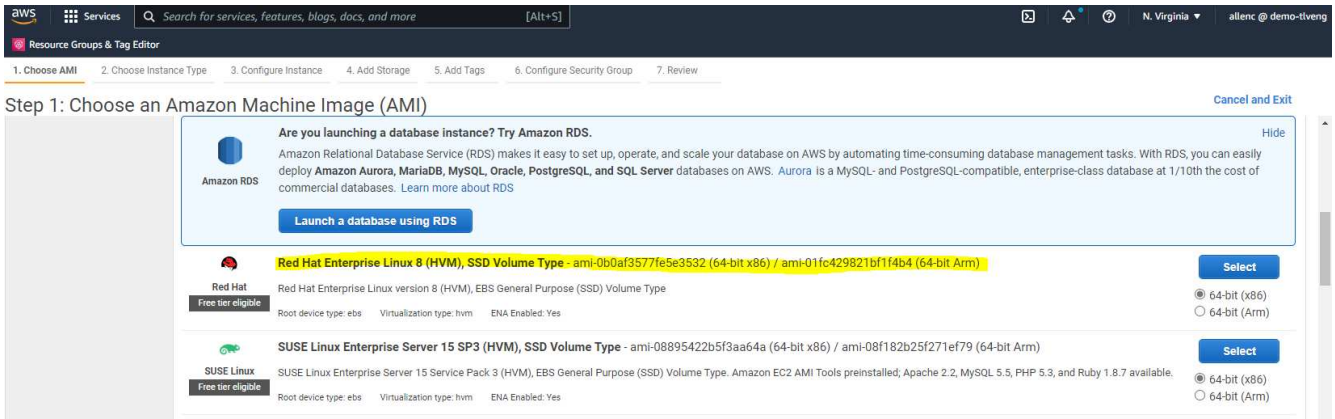
- Überblick.
- Voraussetzungen.
- Schritt 1: Starten Sie eine Instanz.
- Schritt 2: Stellen Sie eine Verbindung zu Ihrer Instanz her.
- Schritt 3: Bereinigen Sie Ihre Instanz.

Die folgenden Screenshots zeigen die Bereitstellung einer Linux-Instance vom Typ m5 mit der EC2-Konsole zum Ausführen von Oracle.

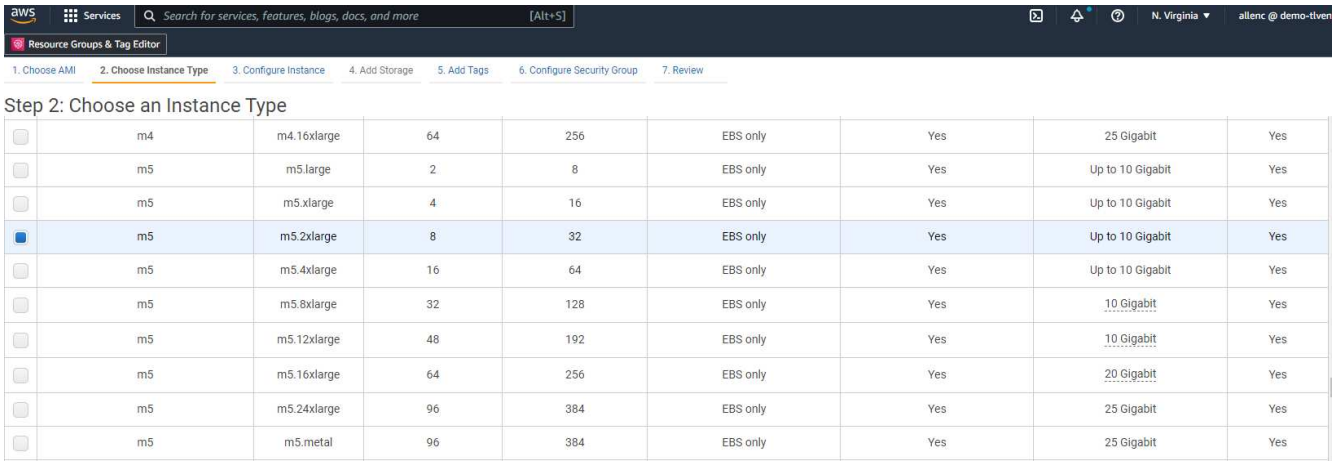
1. Klicken Sie im EC2-Dashboard auf die gelbe Schaltfläche „Instanz starten“, um den Bereitstellungsworkflow der EC2-Instanz zu starten.



2. Wählen Sie in Schritt 1 „Red Hat Enterprise Linux 8 (HVM), SSD-Volume-Typ – ami-0b0af3577fe5e3532 (64-Bit x86) / ami-01fc429821bf1f4b4 (64-Bit Arm)“ aus.

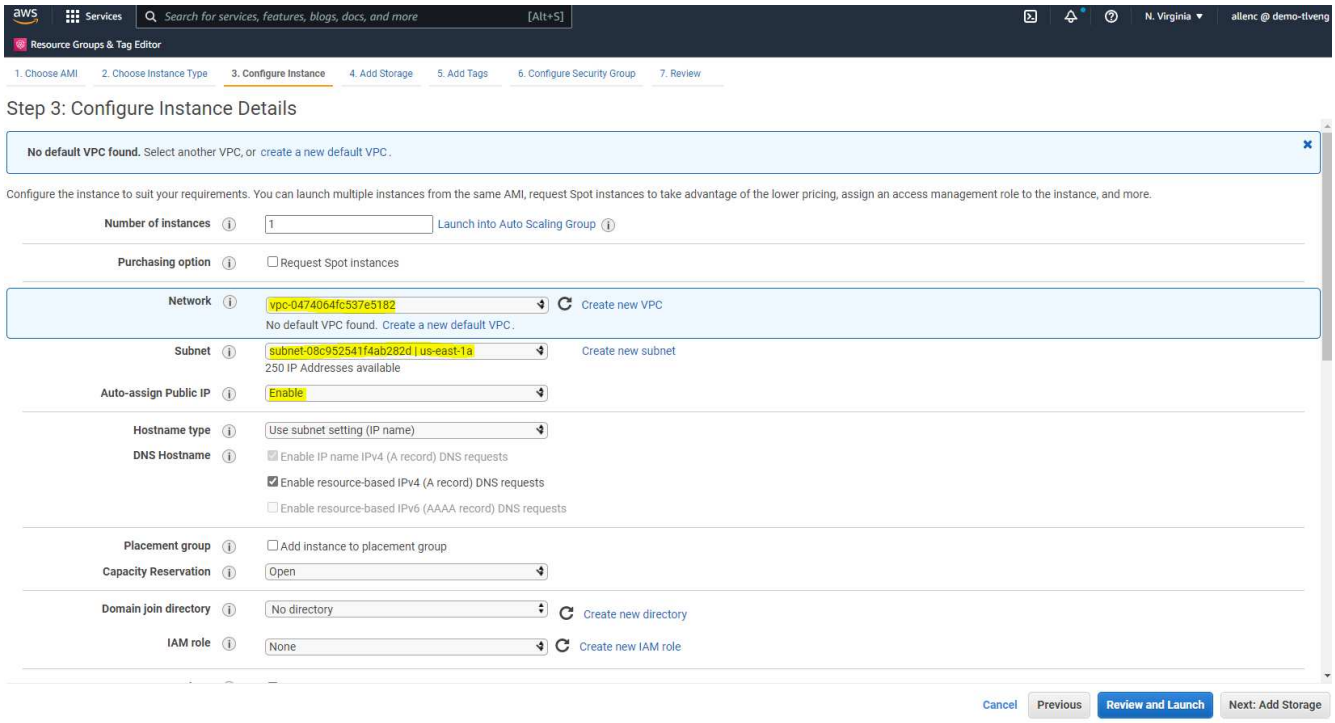


3. Wählen Sie in Schritt 2 einen m5-Instanztyp mit der entsprechenden CPU- und Speicherzuweisung basierend auf Ihrer Oracle-Datenbank-Workload aus. Klicken Sie auf „Weiter: Instanzdetails konfigurieren“.

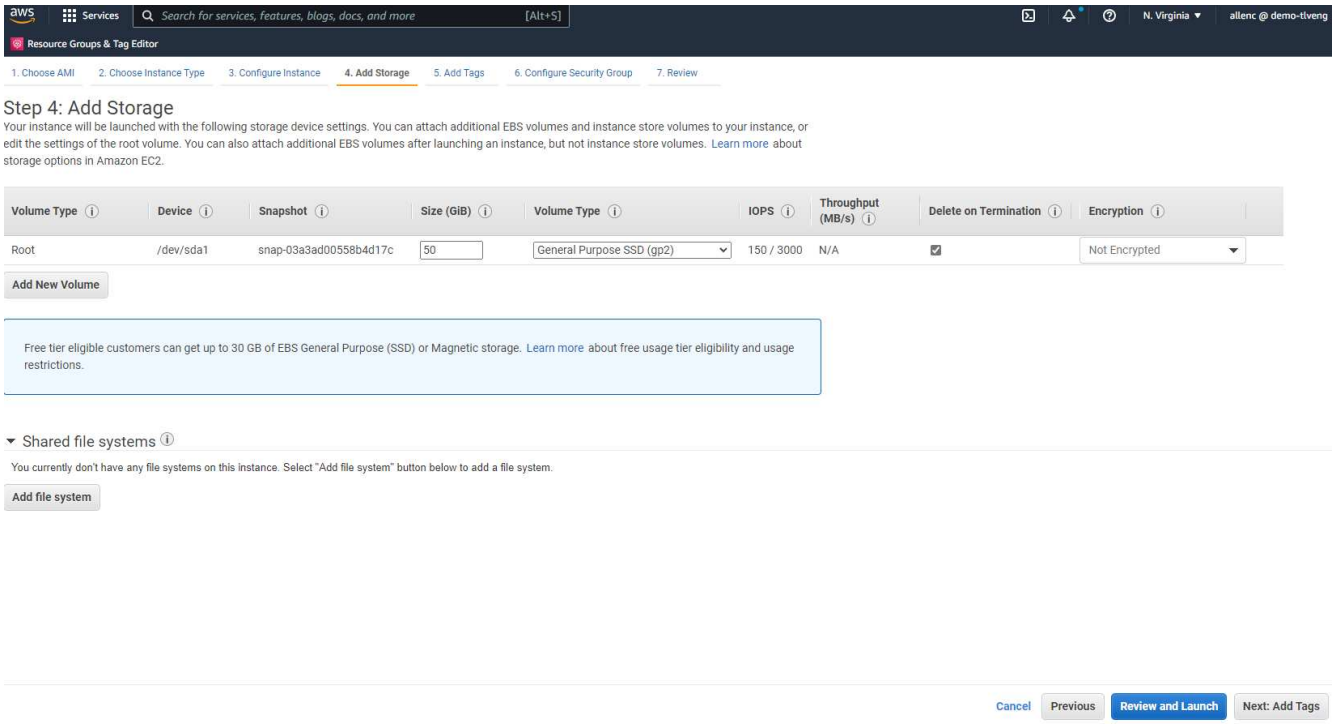


☐	m4	m4.16xlarge	64	256	EBS only	Yes	25 Gigabit	Yes
☐	m5	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
☐	m5	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
☑	m5	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
☐	m5	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
☐	m5	m5.8xlarge	32	128	EBS only	Yes	10 Gigabit	Yes
☐	m5	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
☐	m5	m5.16xlarge	64	256	EBS only	Yes	20 Gigabit	Yes
☐	m5	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
☐	m5	m5.metal	96	384	EBS only	Yes	25 Gigabit	Yes

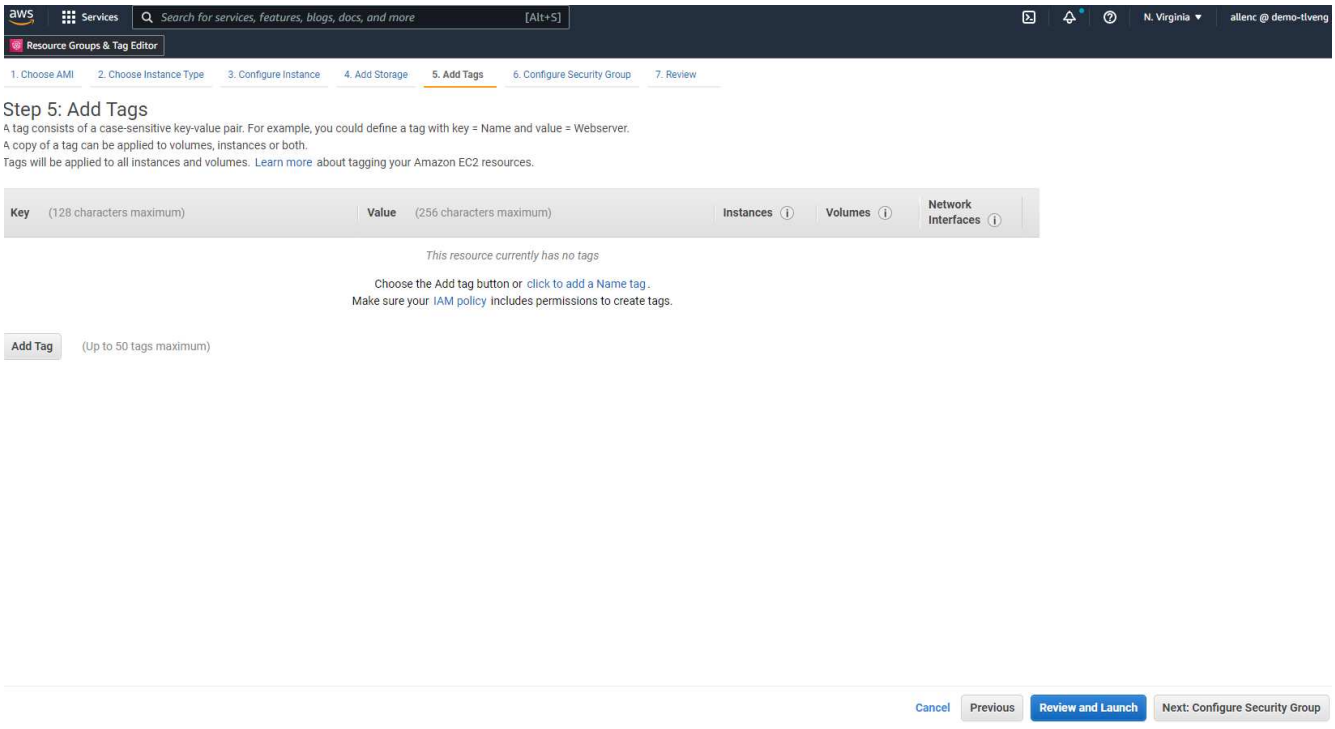
4. Wählen Sie in Schritt 3 die VPC und das Subnetz aus, in dem die Instanz platziert werden soll, und aktivieren Sie die öffentliche IP-Zuweisung. Klicken Sie auf „Weiter: Speicher hinzufügen“.



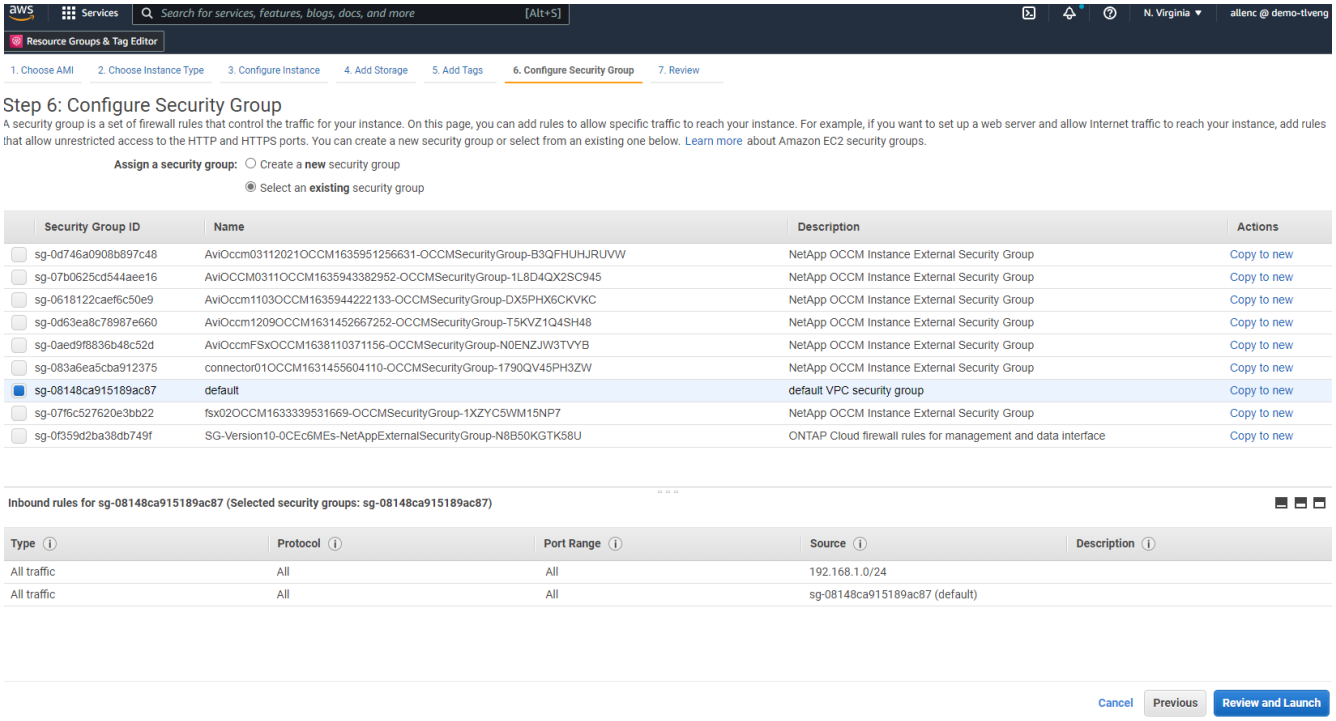
5. Weisen Sie in Schritt 4 genügend Speicherplatz für die Root-Festplatte zu. Möglicherweise benötigen Sie den Speicherplatz, um einen Swap hinzuzufügen. Standardmäßig wird der EC2-Instanz kein Swap-Speicher zugewiesen, was für die Ausführung von Oracle nicht optimal ist.



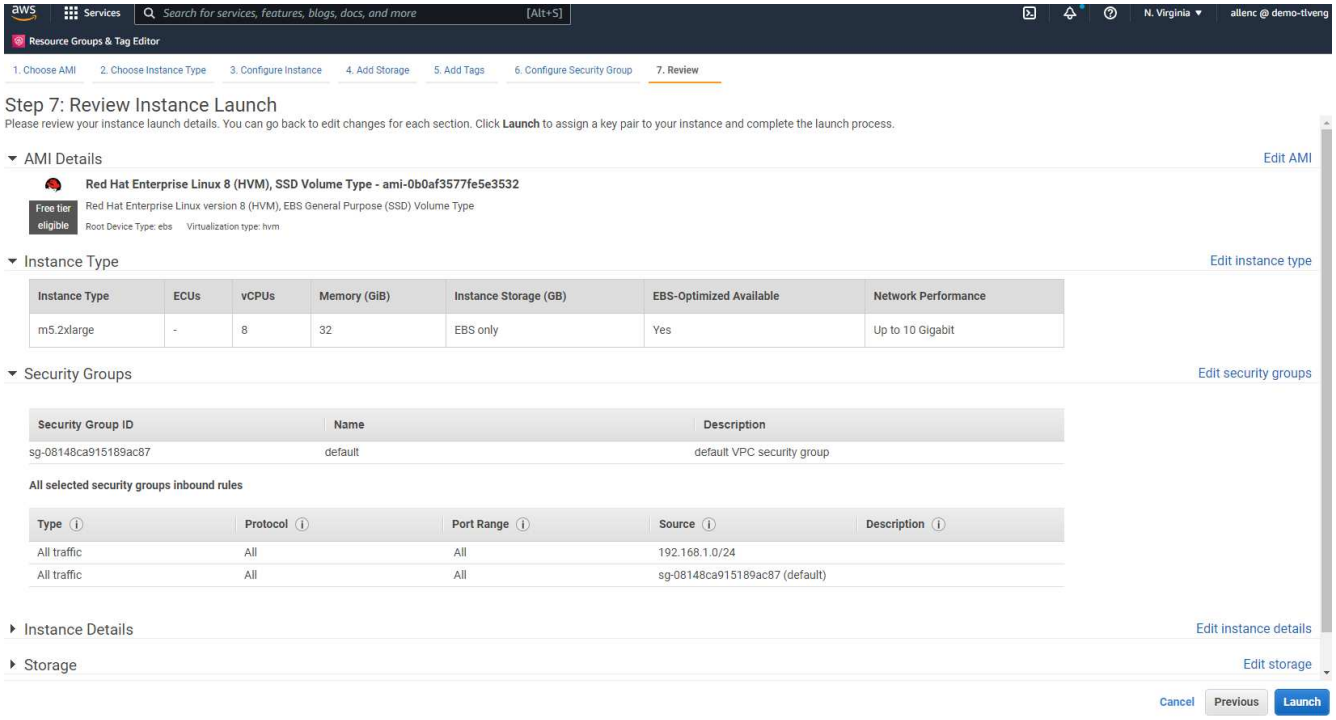
6. Fügen Sie in Schritt 5 bei Bedarf ein Tag zur Instanzidentifizierung hinzu.

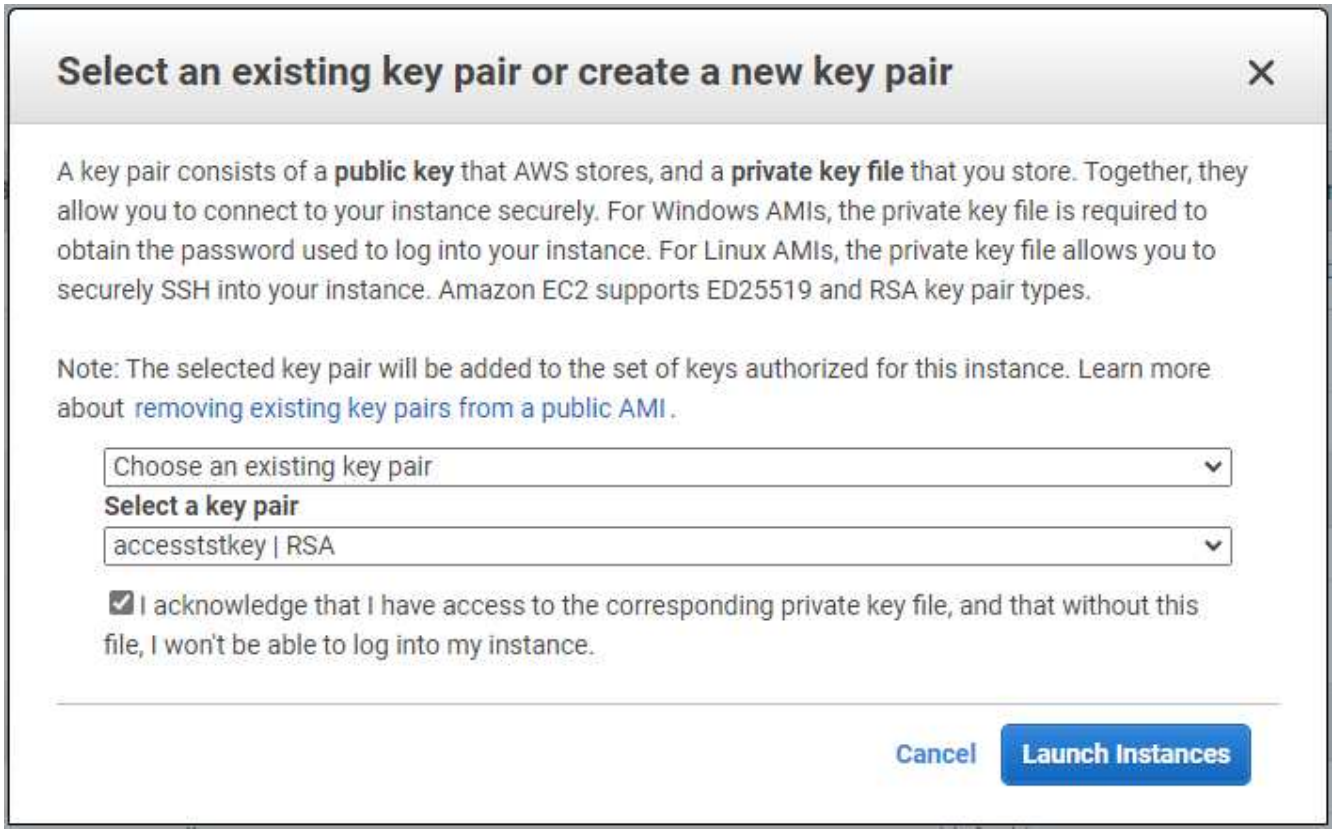


7. Wählen Sie in Schritt 6 eine vorhandene Sicherheitsgruppe aus oder erstellen Sie eine neue mit der gewünschten eingehenden und ausgehenden Richtlinie für die Instanz.



8. Überprüfen Sie in Schritt 7 die Zusammenfassung der Instanzkonfiguration und klicken Sie auf „Starten“, um die Instanzbereitstellung zu starten. Sie werden aufgefordert, ein Schlüsselpaar zu erstellen oder ein Schlüsselpaar für den Zugriff auf die Instanz auszuwählen.





9. Melden Sie sich mit einem SSH-Schlüsselpaar bei der EC2-Instanz an. Nehmen Sie gegebenenfalls Änderungen an Ihrem Schlüsselnamen und der IP-Adresse der Instanz vor.

```
ssh -i ora-db1v2.pem ec2-user@54.80.114.77
```

Sie müssen zwei EC2-Instanzen als primäre und Standby-Oracle-Server in ihrer vorgesehenen Verfügbarkeitszone erstellen, wie im Architekturdiagramm dargestellt.

Bereitstellen von FSx ONTAP -Dateisystemen für Oracle-Datenbankspeicher

Bei der Bereitstellung einer EC2-Instanz wird ein EBS-Stammvolume für das Betriebssystem zugewiesen. FSx ONTAP Dateisysteme bieten Oracle-Datenbankspeichervolumes, einschließlich der Oracle-Binär-, Daten- und Protokollvolumes. Die FSx-Speicher-NFS-Volumes können entweder über die AWS FSx-Konsole oder über die Oracle-Installation bereitgestellt werden. Außerdem gibt es eine Konfigurationsautomatisierung, die die Volumes gemäß der Konfiguration des Benutzers in einer Automatisierungsparameterdatei zuweist.

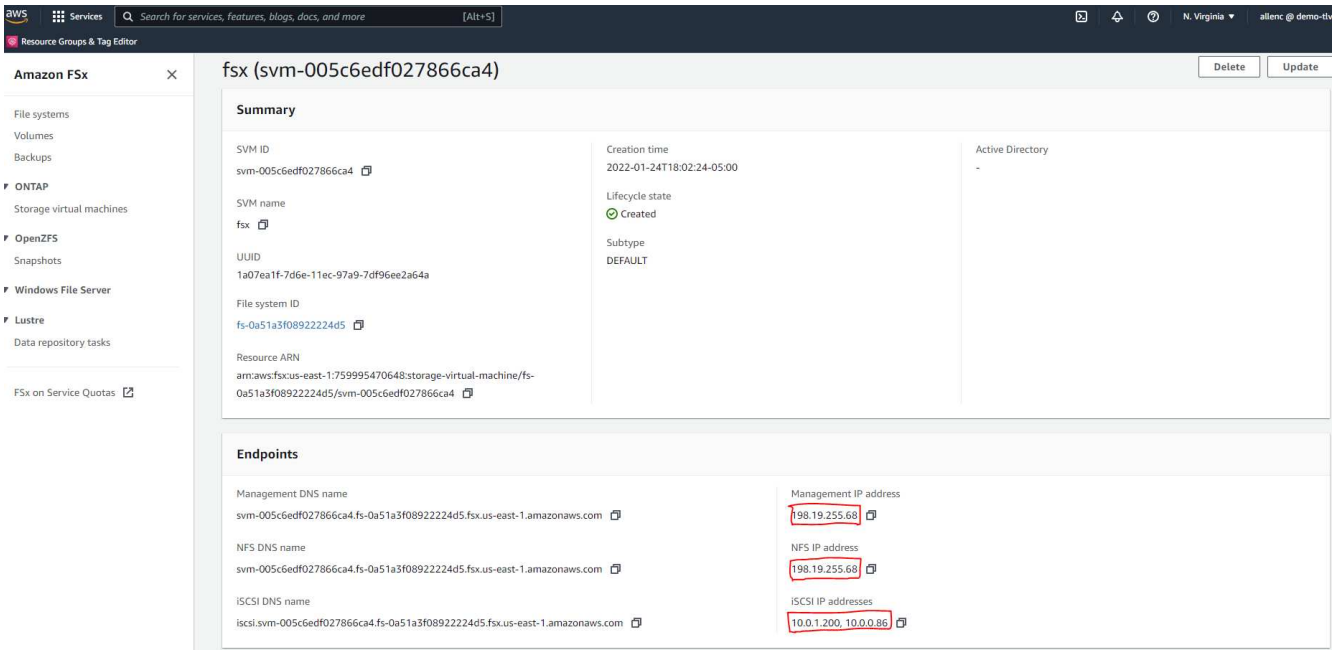
Erstellen von FSx ONTAP Dateisystemen

Auf diese Dokumentation verwiesen "Verwalten von FSx ONTAP Dateisystemen" zum Erstellen von FSx ONTAP Dateisystemen.

Wichtige Überlegungen:

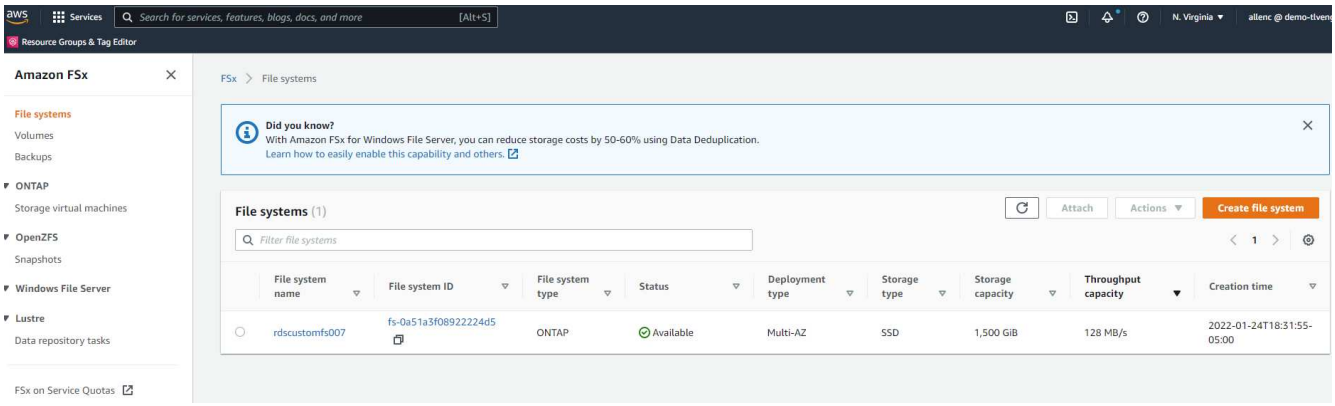
- SSD-Speicherkapazität. Mindestens 1024 GiB, maximal 192 TiB.
- Bereitgestellte SSD-IOPS. Basierend auf den Workload-Anforderungen maximal 80.000 SSD-IOPS pro Dateisystem.

- Durchsatzkapazität.
- Legen Sie das Administratorkennwort fsxadmin/vsadmin fest. Erforderlich für die FSx-Konfigurationsautomatisierung.
- Sicherung und Wartung. Deaktivieren Sie automatische tägliche Sicherungen. Die Sicherung des Datenbankspeichers wird über die SnapCenter -Planung ausgeführt.
- Rufen Sie die SVM-Verwaltungs-IP-Adresse sowie protokollspezifische Zugriffsadressen von der SVM-Detailseite ab. Erforderlich für die FSx-Konfigurationsautomatisierung.

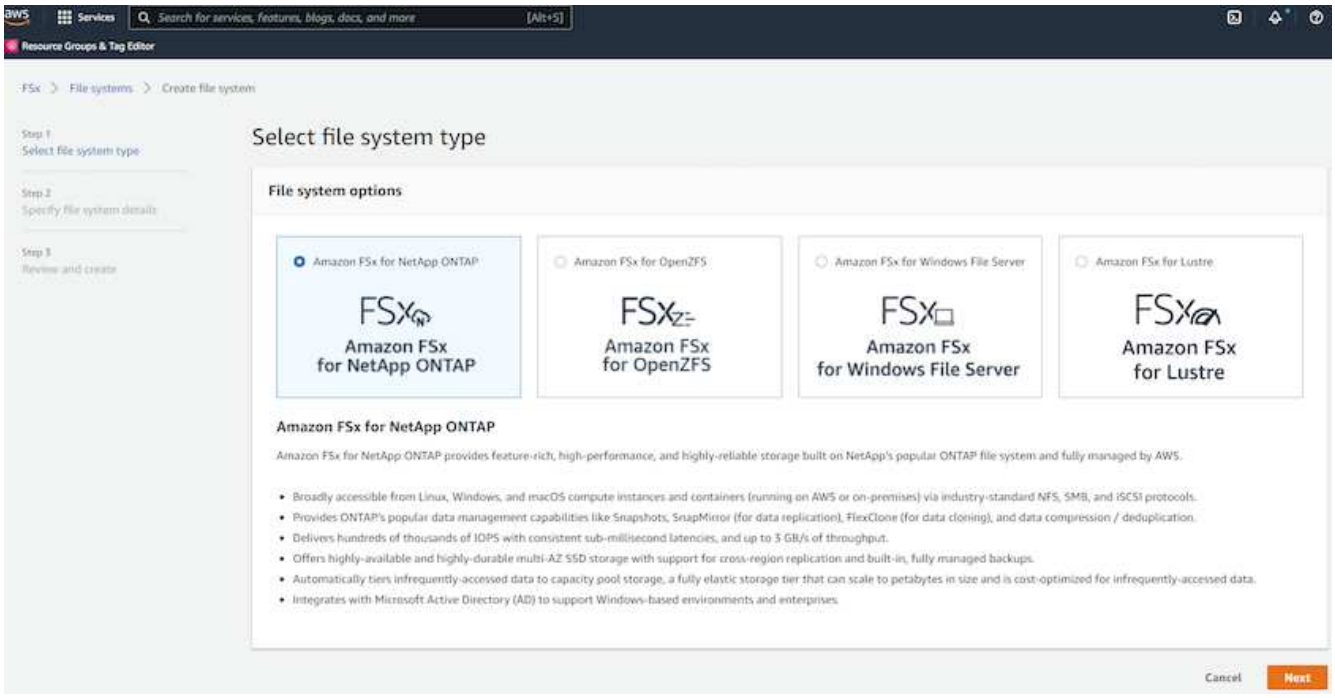


Sehen Sie sich die folgenden Schritt-für-Schritt-Anleitungen zum Einrichten eines primären oder Standby-HA-FSx-Clusters an.

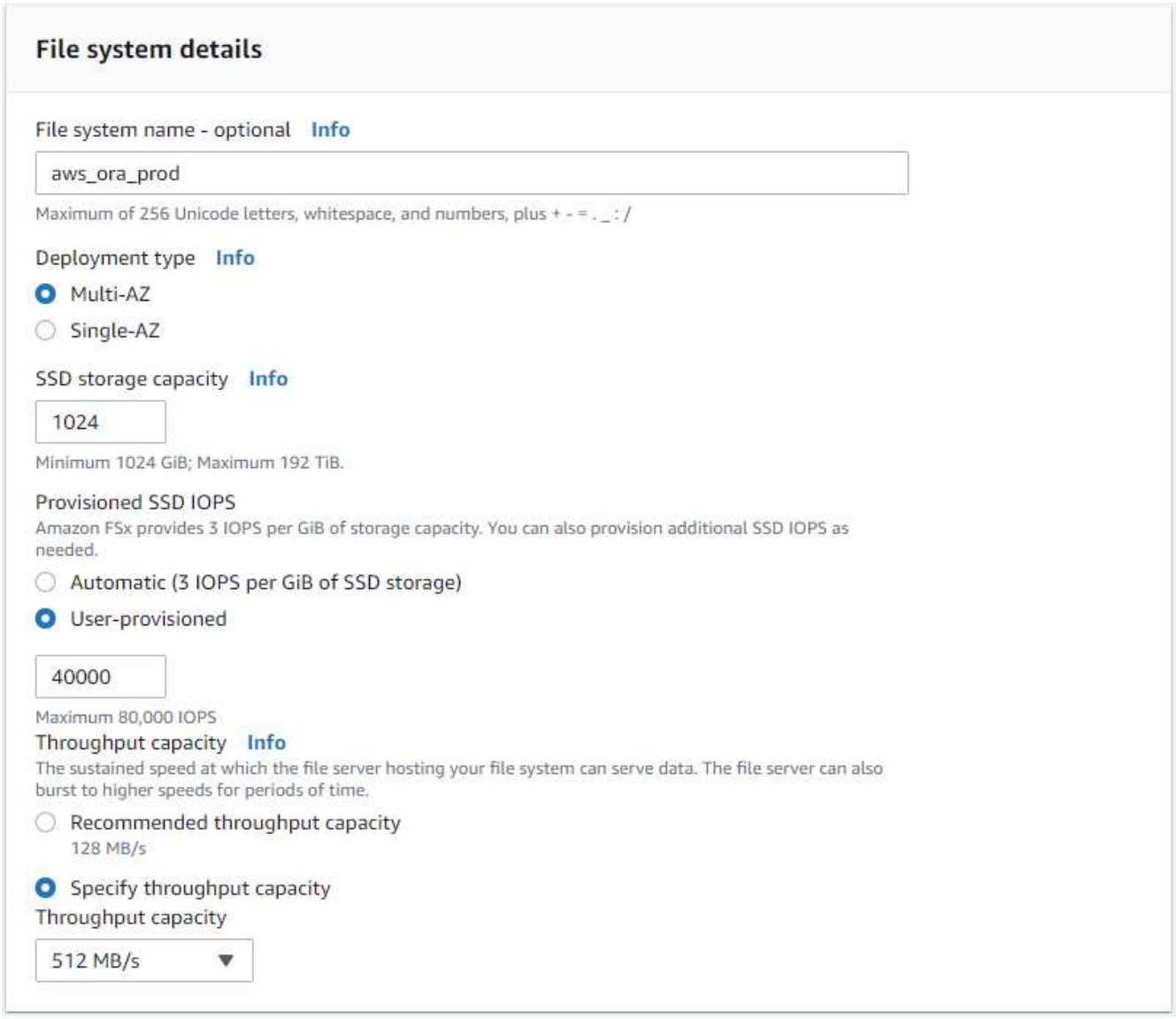
1. Klicken Sie in der FSx-Konsole auf „Dateisystem erstellen“, um den FSx-Bereitstellungsworkflow zu starten.



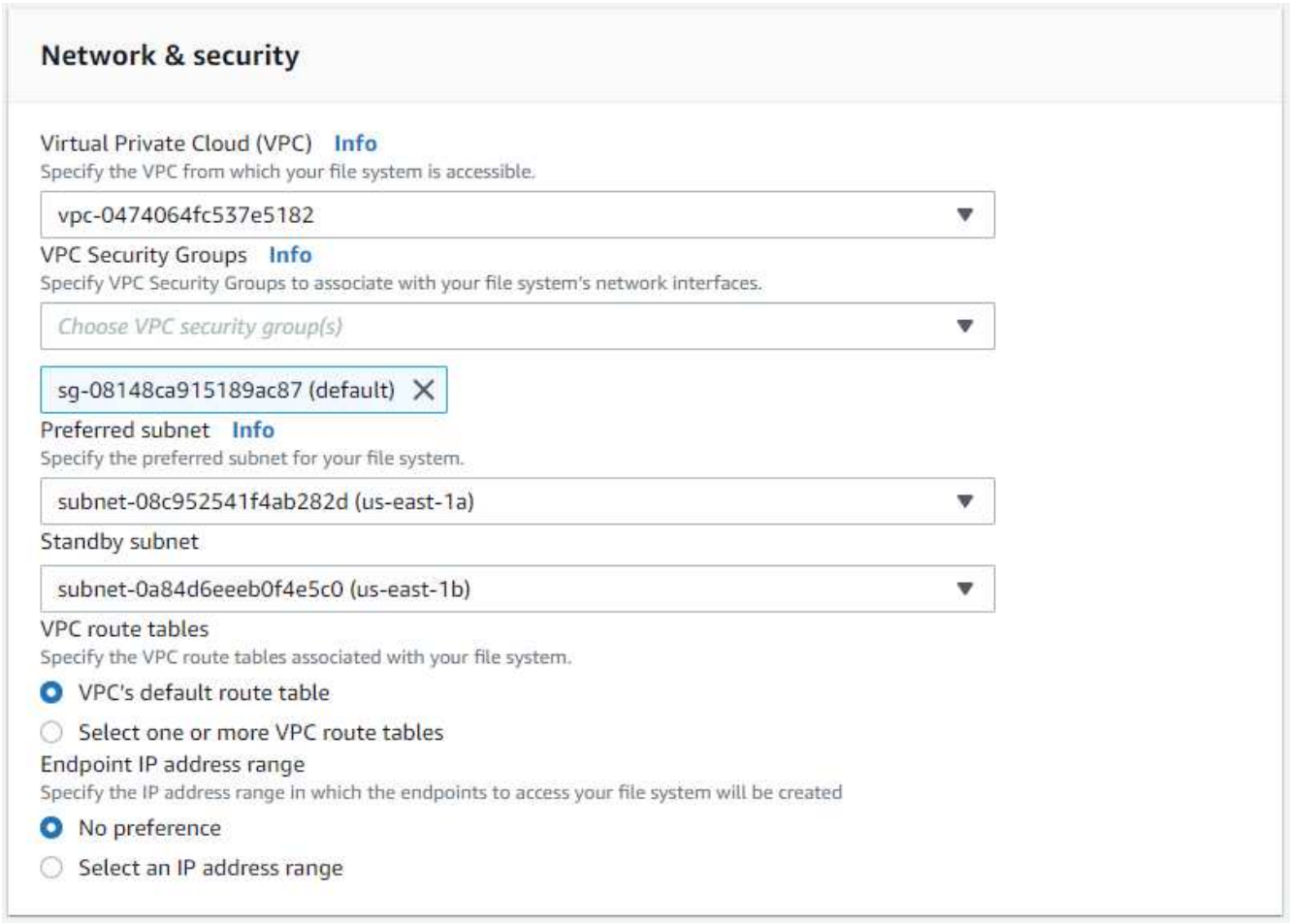
2. Wählen Sie Amazon FSx ONTAP aus. Klicken Sie dann auf Weiter.



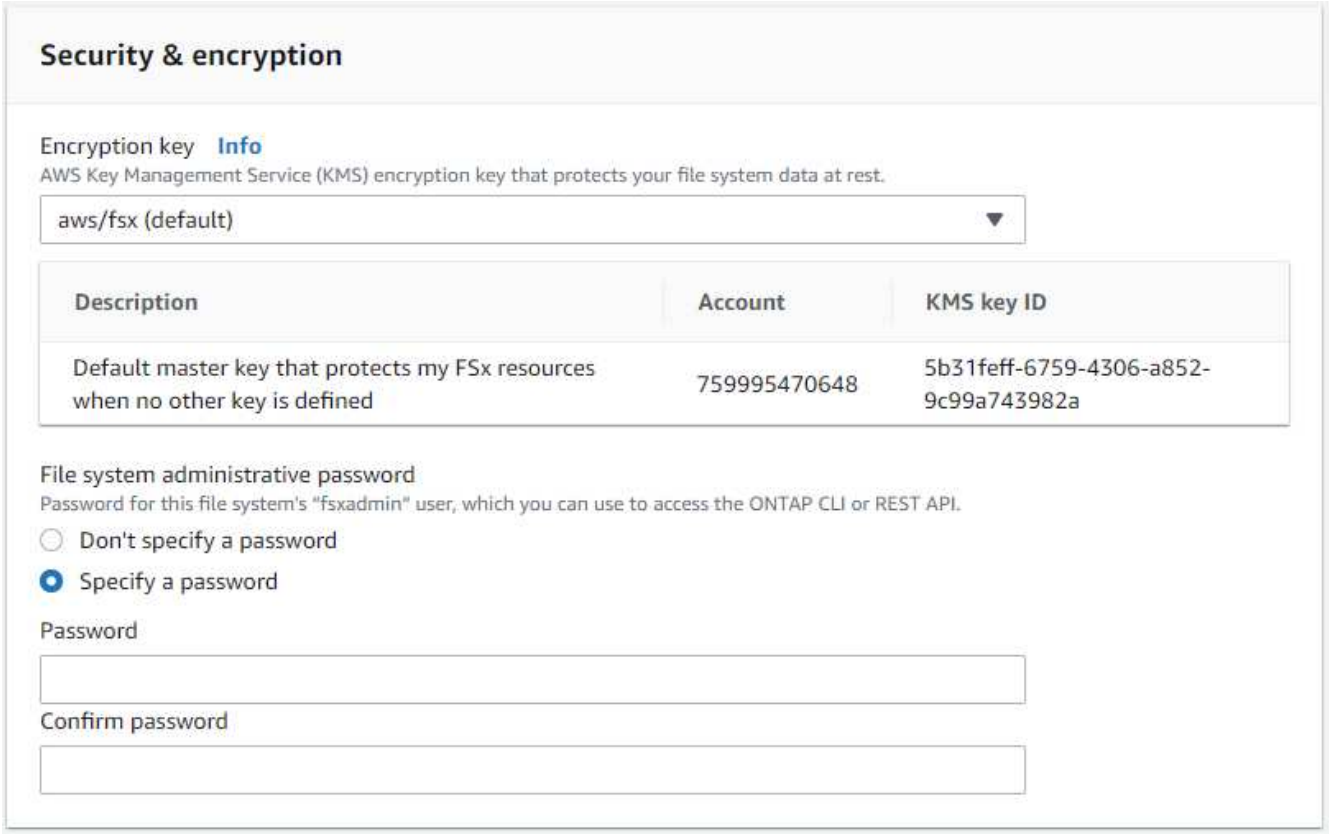
3. Wählen Sie „Standarderstellung“ und geben Sie Ihrem Dateisystem in den Dateisystemdetails den Namen „Multi-AZ HA“. Wählen Sie basierend auf Ihrer Datenbankarbeitslast entweder automatische oder vom Benutzer bereitgestellte IOPS mit bis zu 80.000 SSD-IOPS. Der FSx-Speicher verfügt über bis zu 2 TiB NVMe-Caching im Backend, das noch höhere gemessene IOPS liefern kann.



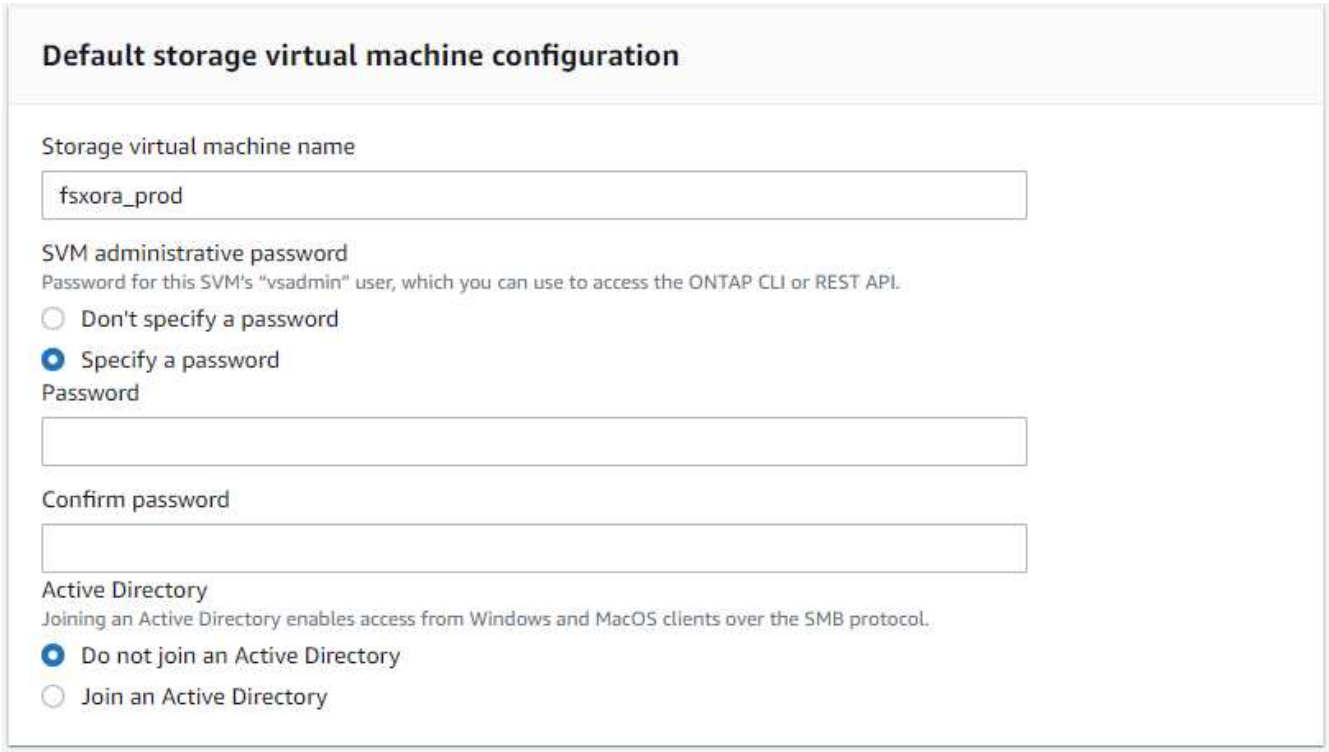
4. Wählen Sie im Abschnitt „Netzwerk und Sicherheit“ die VPC, die Sicherheitsgruppe und die Subnetze aus. Diese sollten vor der FSx-Bereitstellung erstellt werden. Platzieren Sie die FSx-Speicherknoten basierend auf der Rolle des FSx-Clusters (primär oder Standby) in den entsprechenden Zonen.



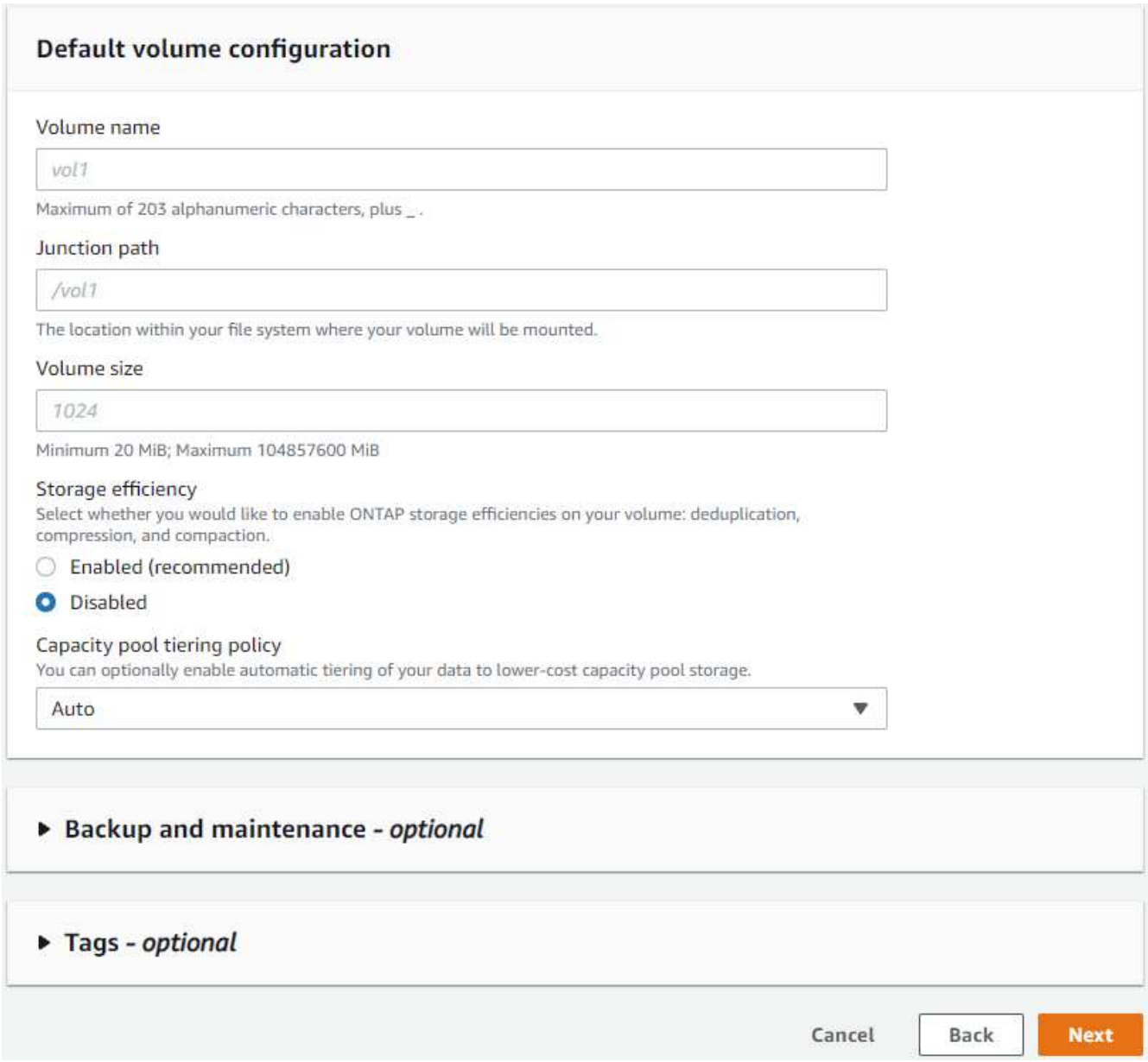
5. Akzeptieren Sie im Abschnitt „Sicherheit und Verschlüsselung“ die Standardeinstellung und geben Sie das fsxadmin-Passwort ein.



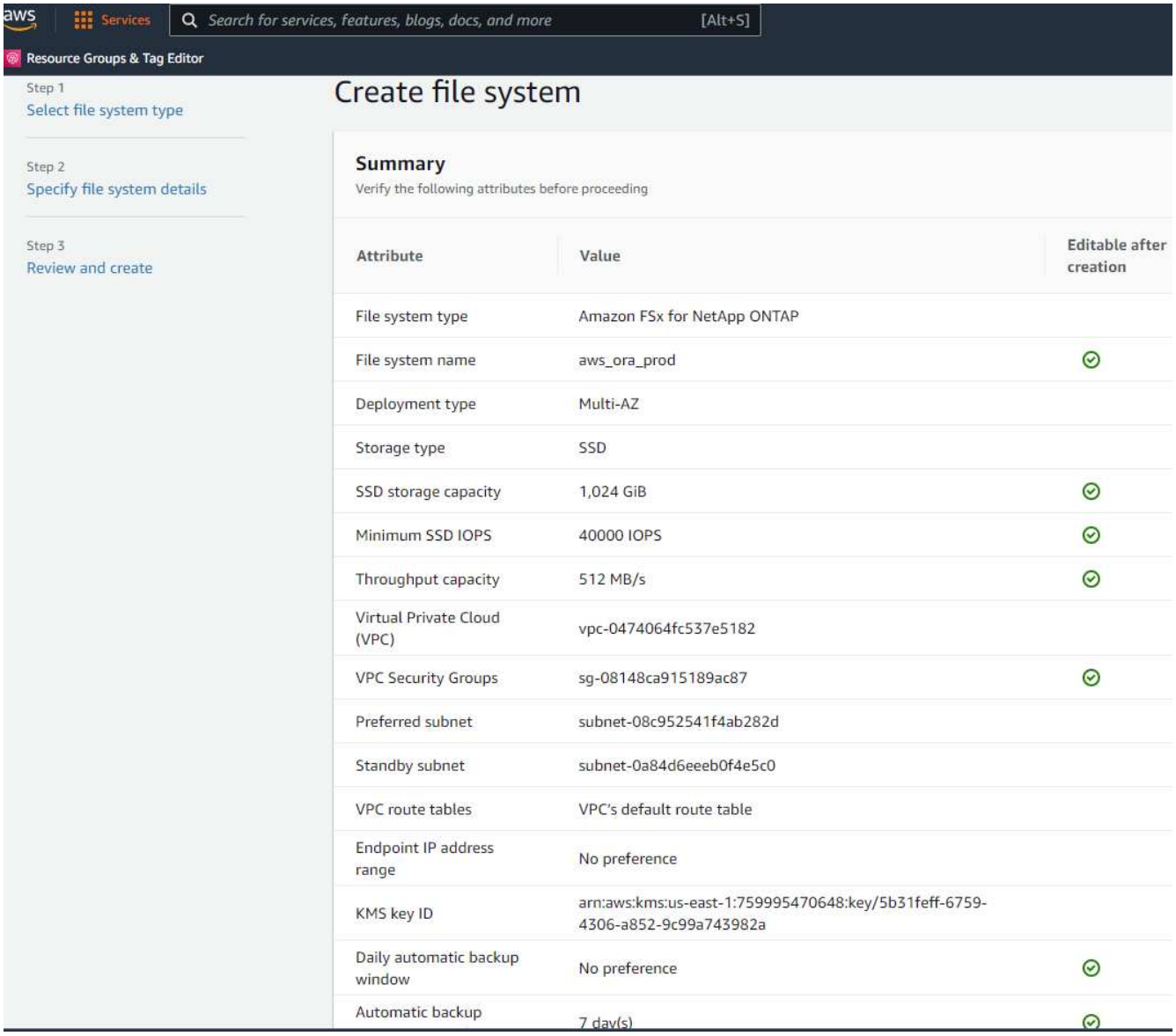
6. Geben Sie den SVM-Namen und das vsadmin-Passwort ein.



7. Lassen Sie die Volume-Konfiguration leer. Sie müssen an dieser Stelle kein Volume erstellen.



8. Überprüfen Sie die Seite „Zusammenfassung“ und klicken Sie auf „Dateisystem erstellen“, um die Bereitstellung des FSx-Dateisystems abzuschließen.



Bereitstellung von Datenbankvolumes für Oracle-Datenbanken

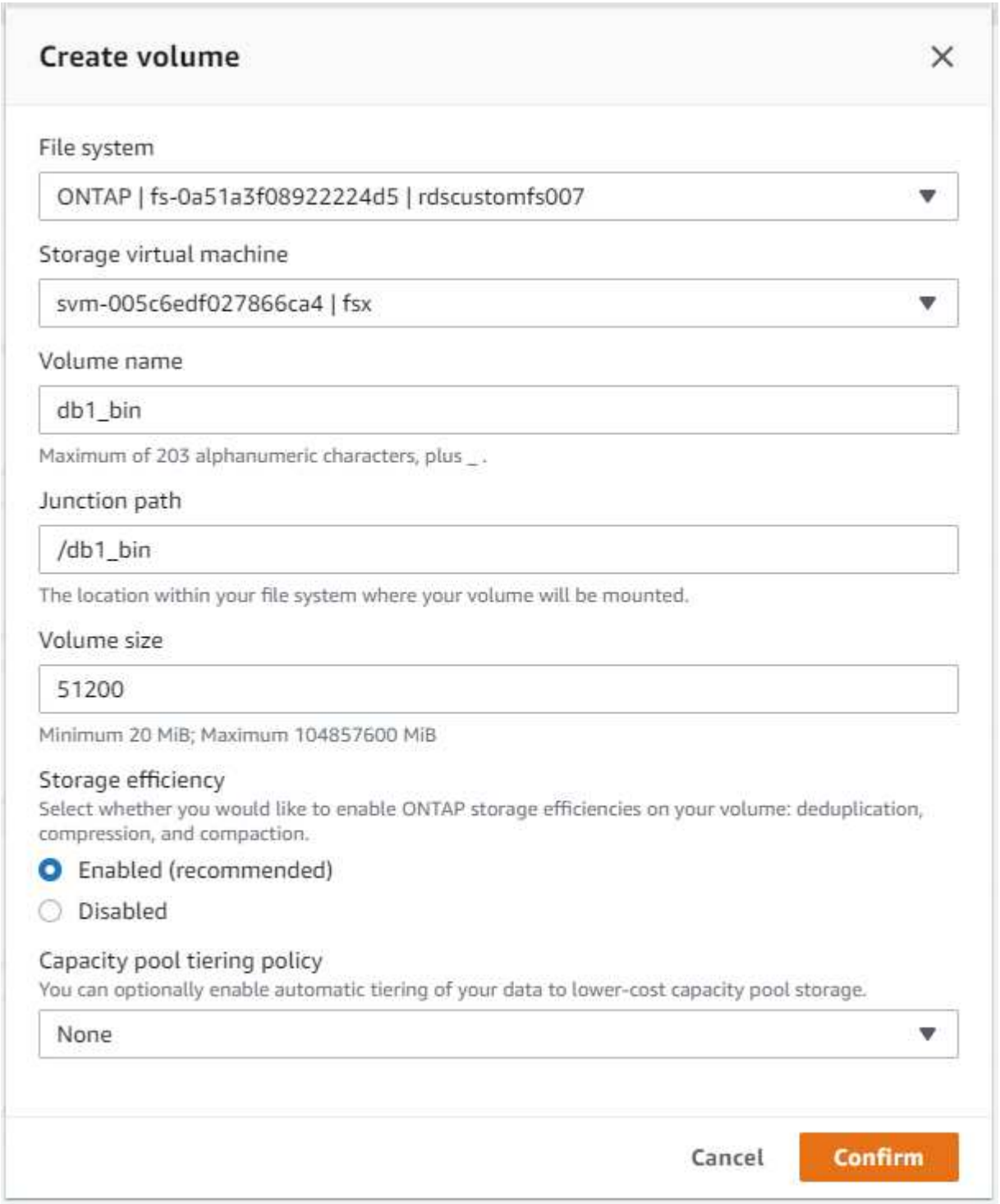
Sehen"Verwalten von FSx ONTAP -Volumes – Erstellen eines Volumes" für Details.

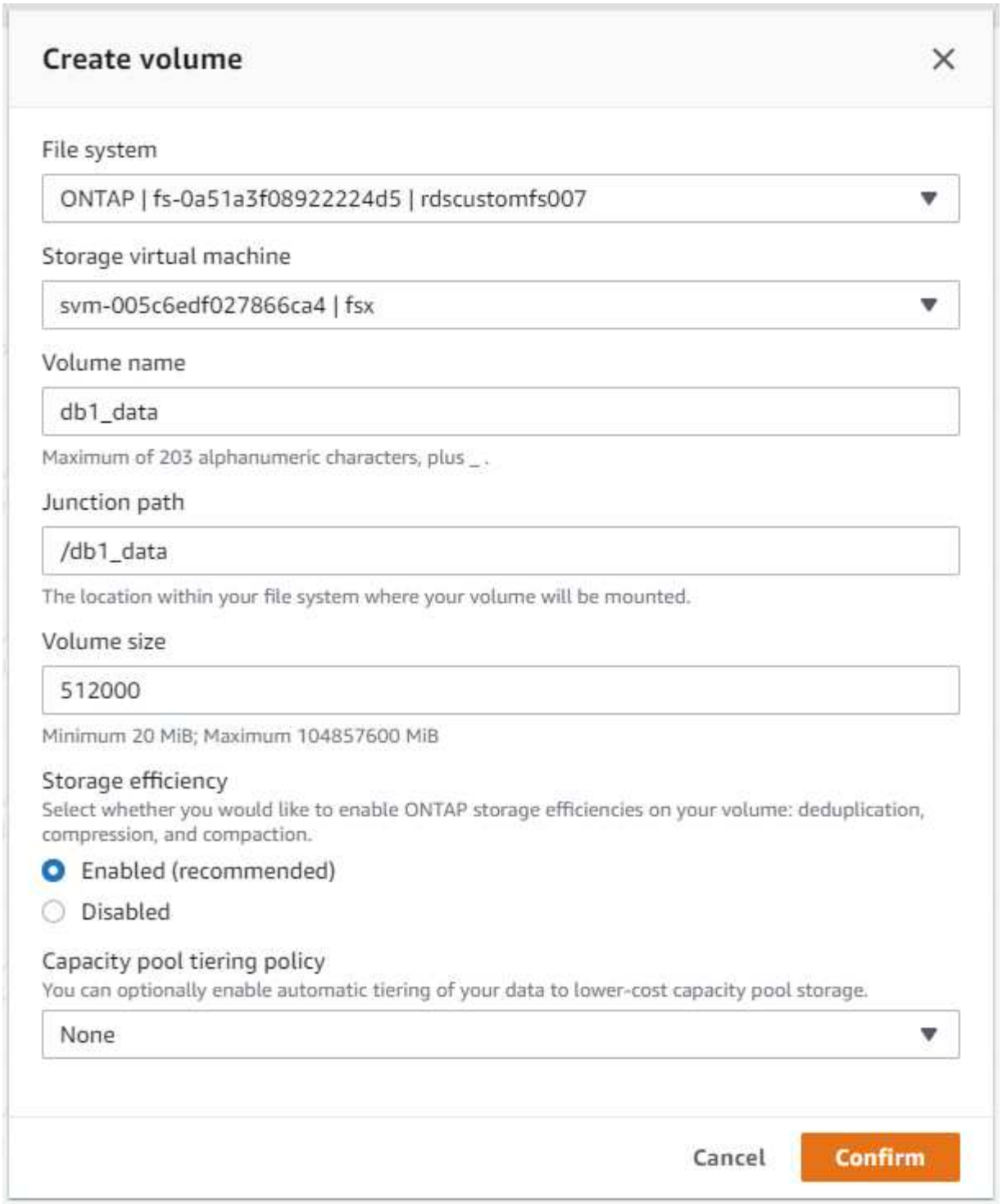
Wichtige Überlegungen:

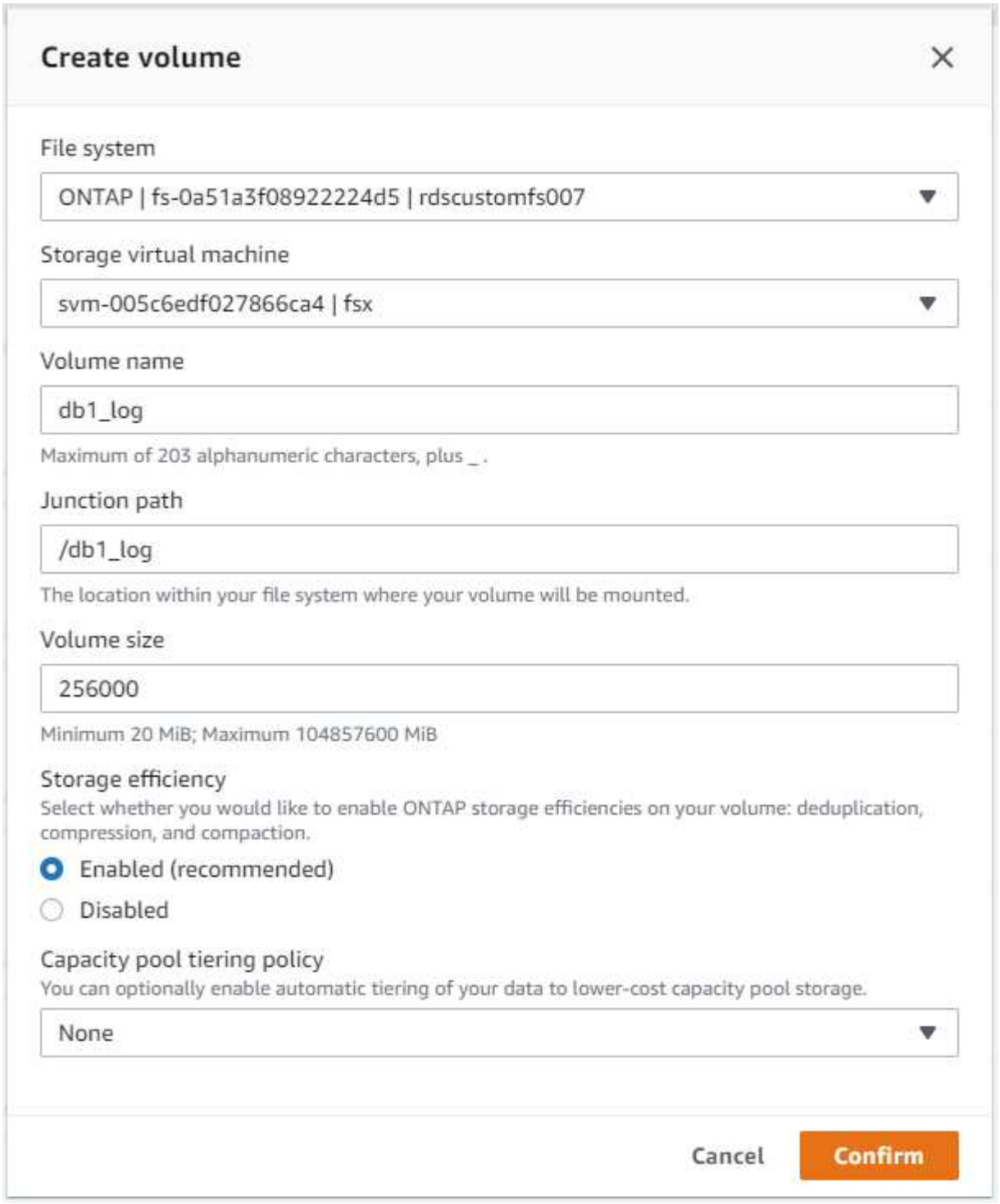
- Angemessene Dimensionierung der Datenbankvolumes.
- Deaktivieren der Kapazitätspool-Tiering-Richtlinie für die Leistungskonfiguration.
- Aktivieren von Oracle dNFS für NFS-Speichervolumes.
- Einrichten von Multipath für iSCSI-Speichervolumes.

Erstellen Sie ein Datenbankvolume über die FSx-Konsole

Über die AWS FSx-Konsole können Sie drei Volumes für die Oracle-Datenbankdateispeicherung erstellen: eines für die Oracle-Binärdatei, eines für die Oracle-Daten und eines für das Oracle-Protokoll. Stellen Sie zur ordnungsgemäßen Identifizierung sicher, dass die Volume-Benennung mit dem Oracle-Hostnamen (definiert in der Hosts-Datei im Automatisierungs-Toolkit) übereinstimmt. In diesem Beispiel verwenden wir db1 als EC2-Oracle-Hostnamen anstelle eines typischen IP-adressbasierten Hostnamens für eine EC2-Instanz.


Create volume
File system
ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007
Storage virtual machine
svm-005c6edf027866ca4 | fsx
Volume name
db1_bin
Maximum of 203 alphanumeric characters, plus _ .
Junction path
/db1_bin
The location within your file system where your volume will be mounted.
Volume size
51200
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
None
Cancel
Confirm


Create volume
File system
ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007
Storage virtual machine
svm-005c6edf027866ca4 | fsx
Volume name
db1_data
Maximum of 203 alphanumeric characters, plus _ .
Junction path
/db1_data
The location within your file system where your volume will be mounted.
Volume size
512000
Minimum 20 MiB; Maximum 104857600 MiB
Storage efficiency
Select whether you would like to enable ONTAP storage efficiencies on your volume: deduplication, compression, and compaction.
Enabled (recommended)
Disabled
Capacity pool tiering policy
You can optionally enable automatic tiering of your data to lower-cost capacity pool storage.
None
Cancel
Confirm



Das Erstellen von iSCSI-LUNs wird derzeit von der FSx-Konsole nicht unterstützt. Für die Bereitstellung von iSCSI-LUNs für Oracle können die Volumes und LUNs mithilfe der Automatisierung für ONTAP mit dem NetApp Automation Toolkit erstellt werden.

Installieren und konfigurieren Sie Oracle auf einer EC2-Instance mit FSx-Datenbankvolumes

Das NetApp Automatisierungsteam stellt ein Automatisierungskit bereit, um die Oracle-Installation und -Konfiguration auf EC2-Instanzen gemäß Best Practices auszuführen. Die aktuelle Version des Automatisierungskits unterstützt Oracle 19c auf NFS mit dem Standard-RU-Patch 19.8. Das

Automatisierungskit kann bei Bedarf problemlos für andere RU-Patches angepasst werden.

Bereiten Sie einen Ansible-Controller zum Ausführen der Automatisierung vor

Folgen Sie den Anweisungen im Abschnitt "Erstellen und Verbinden mit einer EC2-Instance zum Hosten einer Oracle-Datenbank ", um eine kleine EC2-Linux-Instanz bereitzustellen, um den Ansible-Controller auszuführen. Anstatt RedHat zu verwenden, sollte Amazon Linux t2.large mit 2vCPU und 8G RAM ausreichen.

Abrufen des NetApp Oracle Deployment Automation Toolkits

Melden Sie sich bei der in Schritt 1 bereitgestellten EC2 Ansible-Controller-Instanz als ec2-user an und führen Sie im Stammverzeichnis von ec2-user den folgenden Befehl aus: `git clone` Befehl zum Klonen einer Kopie des Automatisierungscodes.

```
git clone https://github.com/NetApp-Automation/na_oracle19c_deploy.git
```

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

Führen Sie eine automatisierte Oracle 19c-Bereitstellung mit dem Automatisierungs-Toolkit durch

Sehen Sie sich diese detaillierten Anweisungen an"CLI-Bereitstellung Oracle 19c-Datenbank" um Oracle 19c mit CLI-Automatisierung bereitzustellen. Es gibt eine kleine Änderung in der Befehlssyntax für die Playbook-Ausführung, da Sie für die Host-Zugriffsauthentifizierung ein SSH-Schlüsselpaar anstelle eines Kennworts verwenden. Die folgende Liste ist eine Zusammenfassung auf hoher Ebene:

1. Standardmäßig verwendet eine EC2-Instance ein SSH-Schlüsselpaar zur Zugriffsauthentifizierung. Aus den Stammverzeichnissen der Ansible-Controller-Automatisierung `/home/ec2-user/na_oracle19c_deploy` , Und `/home/ec2-user/na_rds_fsx_oranfs_config` , erstellen Sie eine Kopie des SSH-Schlüssels `accessstkey.pem` für den im Schritt "Erstellen und Verbinden mit einer EC2-Instance zum Hosten einer Oracle-Datenbank ."
2. Melden Sie sich als EC2-Benutzer beim DB-Host der EC2-Instanz an und installieren Sie die Python3-Bibliothek.

   ```
   sudo yum install python3
   ```

3. Erstellen Sie einen 16-GB-Auslagerungsbereich vom Root-Laufwerk. Standardmäßig erstellt eine EC2-Instance keinen Swap-Speicher. Befolgen Sie diese AWS-Dokumentation:"Wie ordne ich mithilfe einer Auslagerungsdatei Speicher zu, der als Auslagerungsspeicher in einer Amazon EC2-Instanz fungiert?" .
4. Zurück zum Ansible-Controller(`cd /home/ec2-user/na_rds_fsx_oranfs_config`), und führen Sie das Preclone-Playbook mit den entsprechenden Anforderungen aus und `linux_config` Tags.

   ```
   ansible-playbook -i hosts rds_preclone_config.yml -u ec2-user --private
   -key accessstkey.pem -e @vars/fsx_vars.yml -t requirements_config
   ```

```
ansible-playbook -i hosts rds_preclone_config.yml -u ec2-user --private
-key accesststkey.pem -e @vars/fsx_vars.yml -t linux_config
```

5. Wechseln Sie zum `/home/ec2-user/na_oracle19c_deploy-master` Verzeichnis, lesen Sie die README-Datei und füllen Sie die globale `vars.yml` Datei mit den relevanten globalen Parametern.
6. Füllen Sie die `host_name.yml` Datei mit den entsprechenden Parametern im `host_vars` Verzeichnis.
7. Führen Sie das Playbook für Linux aus und drücken Sie die Eingabetaste, wenn Sie zur Eingabe des vsadmin-Passworts aufgefordert werden.

```
ansible-playbook -i hosts all_playbook.yml -u ec2-user --private-key
accesststkey.pem -t linux_config -e @vars/vars.yml
```

8. Führen Sie das Playbook für Oracle aus und drücken Sie die Eingabetaste, wenn Sie zur Eingabe des vsadmin-Passworts aufgefordert werden.

```
ansible-playbook -i hosts all_playbook.yml -u ec2-user --private-key
accesststkey.pem -t oracle_config -e @vars/vars.yml
```

Ändern Sie bei Bedarf das Berechtigungsbit in der SSH-Schlüsseldatei auf 400. Ändern des Oracle-Hosts(`ansible_host` im `host_vars` Datei) IP-Adresse an die öffentliche Adresse Ihrer EC2-Instanz.

Einrichten von SnapMirror zwischen primärem und Standby-FSx-HA-Cluster

Für hohe Verfügbarkeit und Notfallwiederherstellung können Sie die SnapMirror Replikation zwischen dem primären und dem Standby-FSx-Speichercluster einrichten. Im Gegensatz zu anderen Cloud-Speicherdiensten ermöglicht FSx einem Benutzer, die Speicherreplikation mit der gewünschten Frequenz und dem gewünschten Replikationsdurchsatz zu steuern und zu verwalten. Darüber hinaus können Benutzer HA/DR testen, ohne dass dies Auswirkungen auf die Verfügbarkeit hat.

Die folgenden Schritte zeigen, wie Sie die Replikation zwischen einem primären und einem Standby-FSx-Speichercluster einrichten.

1. Richten Sie das Peering des primären und Standby-Clusters ein. Melden Sie sich als Benutzer fsxadmin beim primären Cluster an und führen Sie den folgenden Befehl aus. Dieser wechselseitige Erstellungsprozess führt den Erstellungsbefehl sowohl auf dem primären Cluster als auch auf dem Standby-Cluster aus. Ersetzen `standby_cluster_name` durch den passenden Namen für Ihre Umgebung.

```
cluster peer create -peer-addrs
standby_cluster_name,inter_cluster_ip_address -username fsxadmin
-initial-allowed-vserver-peers *
```

2. Richten Sie vServer-Peering zwischen dem primären und dem Standby-Cluster ein. Melden Sie sich als vsadmin-Benutzer beim primären Cluster an und führen Sie den folgenden Befehl aus. Ersetzen

`primary_vserver_name` , `standby_vserver_name` , `standby_cluster_name` mit den entsprechenden Namen für Ihre Umgebung.

```
vserver peer create -vserver primary_vserver_name -peer-vserver
standby_vserver_name -peer-cluster standby_cluster_name -applications
snapmirror
```

3. Überprüfen Sie, ob die Cluster- und VServer-Peerings richtig eingerichtet sind.

```
FsxId00164454fac5591e6::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
FsxId0b6a95149d07aa82e    1-80-000011           Available      ok

FsxId00164454fac5591e6::> vserver peer show
            Peer        Peer                           Peering        Remote
Vserver     Vserver     State        Peer Cluster      Applications   Vserver
----------- ----------- ------------ ----------------- -------------- ---------
svm_FSxOraSource
            svm_FSxOraTarget
                        peered       FsxId0b6a95149d07aa82e
                                                       snapmirror     svm_FSxOraTarget

FsxId00164454fac5591e6::>
```

4. Erstellen Sie Ziel-NFS-Volumes im Standby-FSx-Cluster für jedes Quell-Volume im primären FSx-Cluster. Ersetzen Sie den Datenträgernamen entsprechend Ihrer Umgebung.

```
vol create -volume dr_db1_bin -aggregate aggr1 -size 50G -state online
-policy default -type DP
```

```
vol create -volume dr_db1_data -aggregate aggr1 -size 500G -state online
-policy default -type DP
```

```
vol create -volume dr_db1_log -aggregate aggr1 -size 250G -state online
-policy default -type DP
```

5. Sie können auch iSCSI-Volumes und LUNs für die Oracle-Binärdatei, Oracle-Daten und das Oracle-Protokoll erstellen, wenn das iSCSI-Protokoll für den Datenzugriff verwendet wird. Lassen Sie in den Volumes etwa 10 % freien Speicherplatz für Snapshots.

```
vol create -volume dr_db1_bin -aggregate aggr1 -size 50G -state online
-policy default -unix-permissions ---rwxr-xr-x -type RW
```

```
lun create -path /vol/dr_db1_bin/dr_db1_bin_01 -size 45G -ostype linux
```

```
vol create -volume dr_db1_data -aggregate aggr1 -size 500G -state online
-policy default -unix-permissions ---rwxr-xr-x -type RW
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_01 -size 100G -ostype
linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_02 -size 100G -ostype
linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_03 -size 100G -ostype
linux
```

```
lun create -path /vol/dr_db1_data/dr_db1_data_04 -size 100G -ostype
linux
```

vol erstellen -volume dr_db1_log -aggregate aggr1 -size 250G -state online -policy default -unix -permissions ---rwxr-xr-x -type RW

```
lun create -path /vol/dr_db1_log/dr_db1_log_01 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_02 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_03 -size 45G -ostype linux
```

```
lun create -path /vol/dr_db1_log/dr_db1_log_04 -size 45G -ostype linux
```

6. Erstellen Sie für iSCSI-LUNs eine Zuordnung für den Oracle-Hostinitiator für jede LUN, wobei Sie die binäre LUN als Beispiel verwenden. Ersetzen Sie die Igroup durch einen passenden Namen für Ihre Umgebung und erhöhen Sie die LUN-ID für jede zusätzliche LUN.

```
lun mapping create -path /vol/dr_db1_bin/dr_db1_bin_01 -igroup ip-10-0-
1-136 -lun-id 0
```

```
lun mapping create -path /vol/dr_db1_data/dr_db1_data_01 -igroup ip-10-
0-1-136 -lun-id 1
```

7. Erstellen Sie eine SnapMirror -Beziehung zwischen den primären und Standby-Datenbankvolumes. Ersetzen Sie den entsprechenden SVM-Namen für Ihre Umgebung.

```
snapmirror create -source-path svm_FSxOraSource:db1_bin -destination
-path svm_FSxOraTarget:dr_db1_bin -vserver svm_FSxOraTarget -throttle
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

```
snapmirror create -source-path svm_FSxOraSource:db1_data -destination
-path svm_FSxOraTarget:dr_db1_data -vserver svm_FSxOraTarget -throttle
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

```
snapmirror create -source-path svm_FSxOraSource:db1_log -destination
-path svm_FSxOraTarget:dr_db1_log -vserver svm_FSxOraTarget -throttle
unlimited -identity-preserve false -policy MirrorAllSnapshots -type DP
```

Dieses SnapMirror Setup kann mit einem NetApp Automation Toolkit für NFS-Datenbankvolumes automatisiert werden. Das Toolkit steht auf der öffentlichen GitHub-Site von NetApp zum Download bereit.

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

Lesen Sie die README-Anweisungen sorgfältig durch, bevor Sie mit der Einrichtung und dem Failover-Test beginnen.

> Das Replizieren der Oracle-Binärdatei vom primären auf einen Standby-Cluster kann Auswirkungen auf die Oracle-Lizenz haben. Wenden Sie sich zur Klärung an Ihren Oracle-Lizenzvertreter. Die Alternative besteht darin, Oracle zum Zeitpunkt der Wiederherstellung und des Failovers zu installieren und zu konfigurieren.

SnapCenter -Bereitstellung

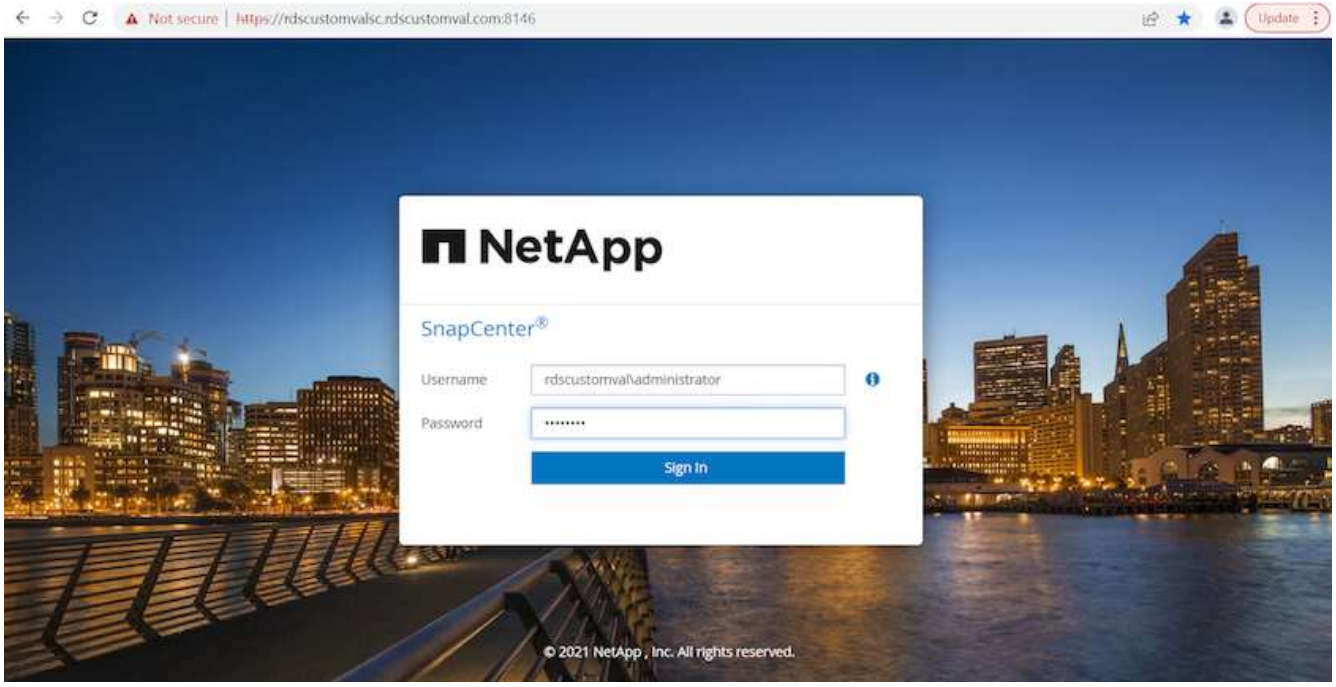
SnapCenter -Installation

Folgen"Installieren des SnapCenter -Servers" um den SnapCenter -Server zu installieren. In dieser Dokumentation wird die Installation eines eigenständigen SnapCenter -Servers beschrieben. Eine SaaS-

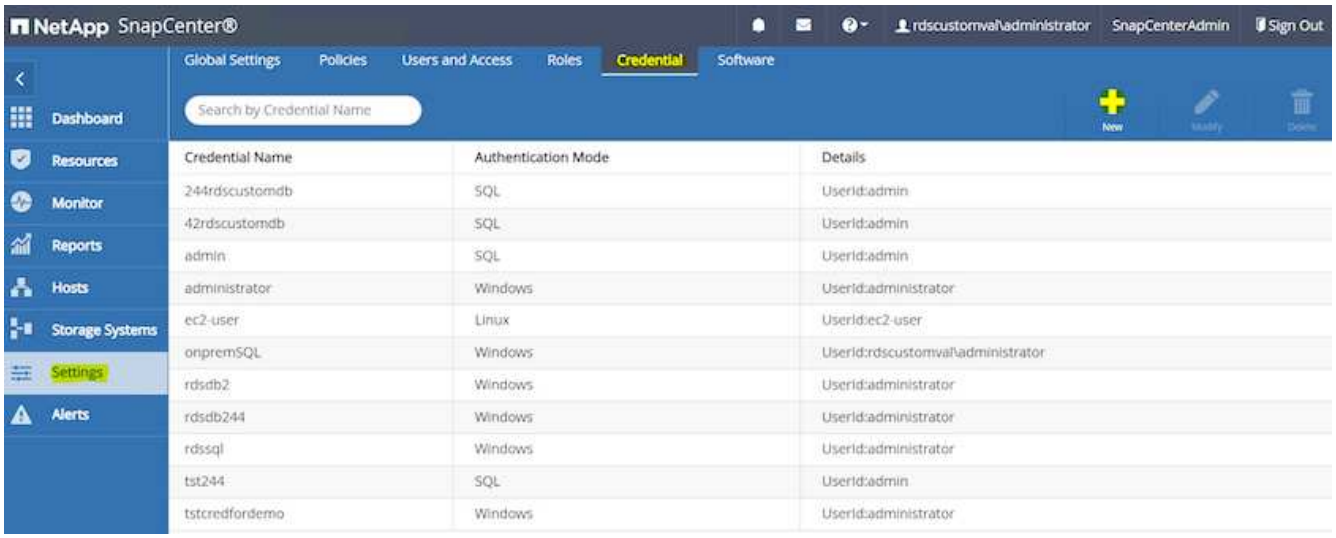
Version von SnapCenter befindet sich im Beta-Test und könnte in Kürze verfügbar sein. Erkundigen Sie sich bei Bedarf bei Ihrem NetApp -Vertreter nach der Verfügbarkeit.

Konfigurieren Sie das SnapCenter -Plugin für den EC2 Oracle-Host

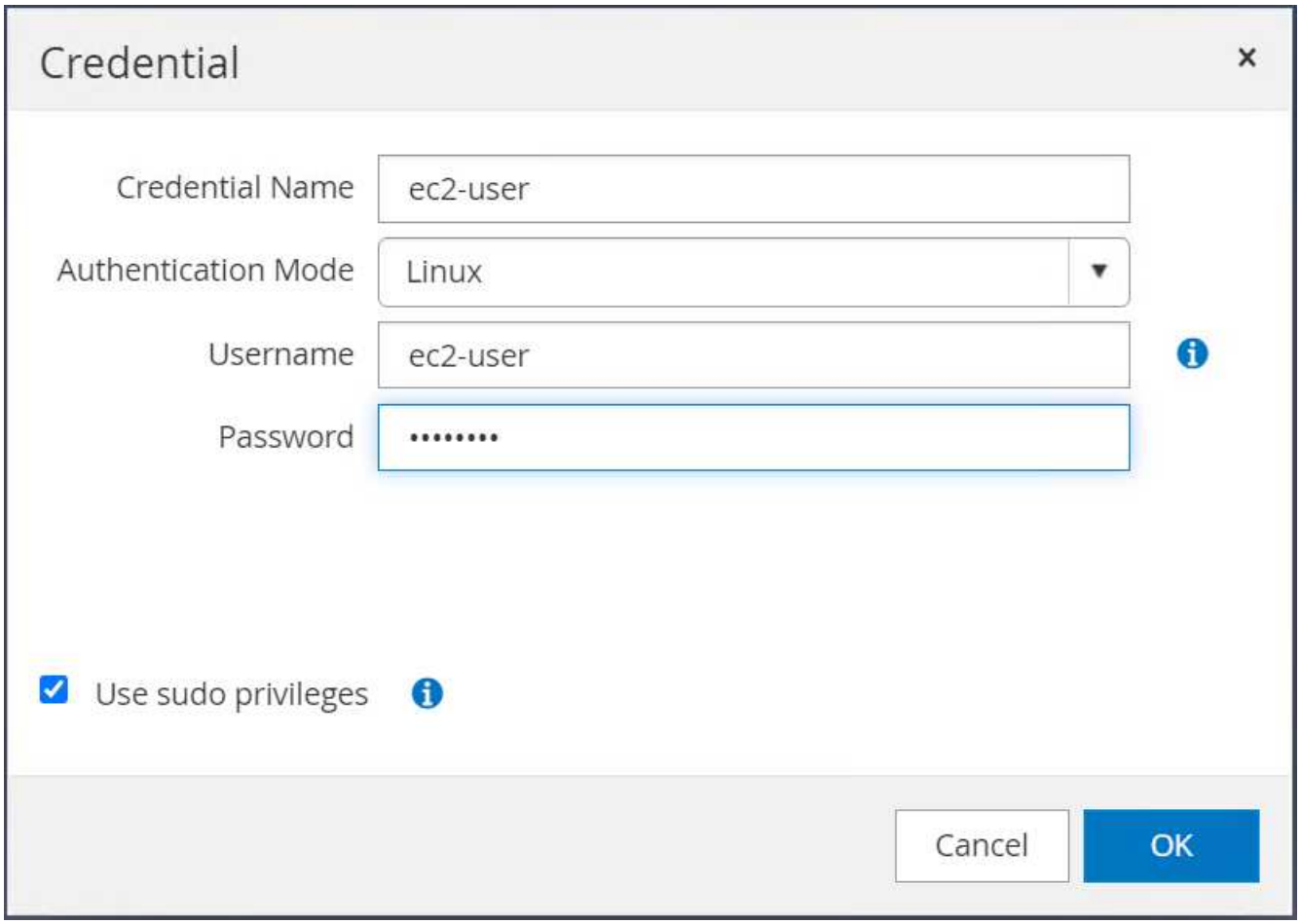
1. Melden Sie sich nach der automatisierten SnapCenter -Installation als Administratorbenutzer bei SnapCenter für den Windows-Host an, auf dem der SnapCenter -Server installiert ist.



2. Klicken Sie im Menü auf der linken Seite auf „Einstellungen“ und dann auf „Anmeldeinformationen“ und „Neu“, um EC2-Benutzeranmeldeinformationen für die Installation des SnapCenter -Plugins hinzuzufügen.



3. Setzen Sie das EC2-Benutzerkennwort zurück und aktivieren Sie die Kennwort-SSH-Authentifizierung, indem Sie das `/etc/ssh/sshd_config` Datei auf dem EC2-Instance-Host.
4. Stellen Sie sicher, dass das Kontrollkästchen „Sudo-Berechtigungen verwenden“ aktiviert ist. Sie haben im vorherigen Schritt einfach das EC2-Benutzerkennwort zurückgesetzt.



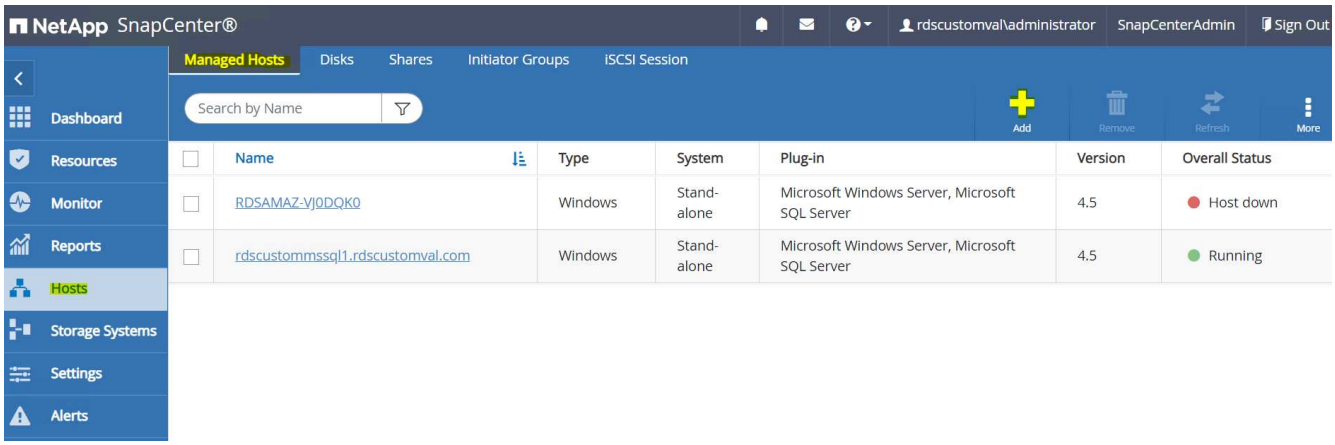
5. Fügen Sie den SnapCenter -Servernamen und die IP-Adresse zur Hostdatei der EC2-Instanz zur Namensauflösung hinzu.

```
[ec2-user@ip-10-0-0-151 ~]$ sudo vi /etc/hosts
[ec2-user@ip-10-0-0-151 ~]$ cat /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4
localhost4.localdomain4
::1         localhost localhost.localdomain localhost6
localhost6.localdomain6
10.0.1.233  rdscustomvalsc.rdscustomval.com rdscustomvalsc
```

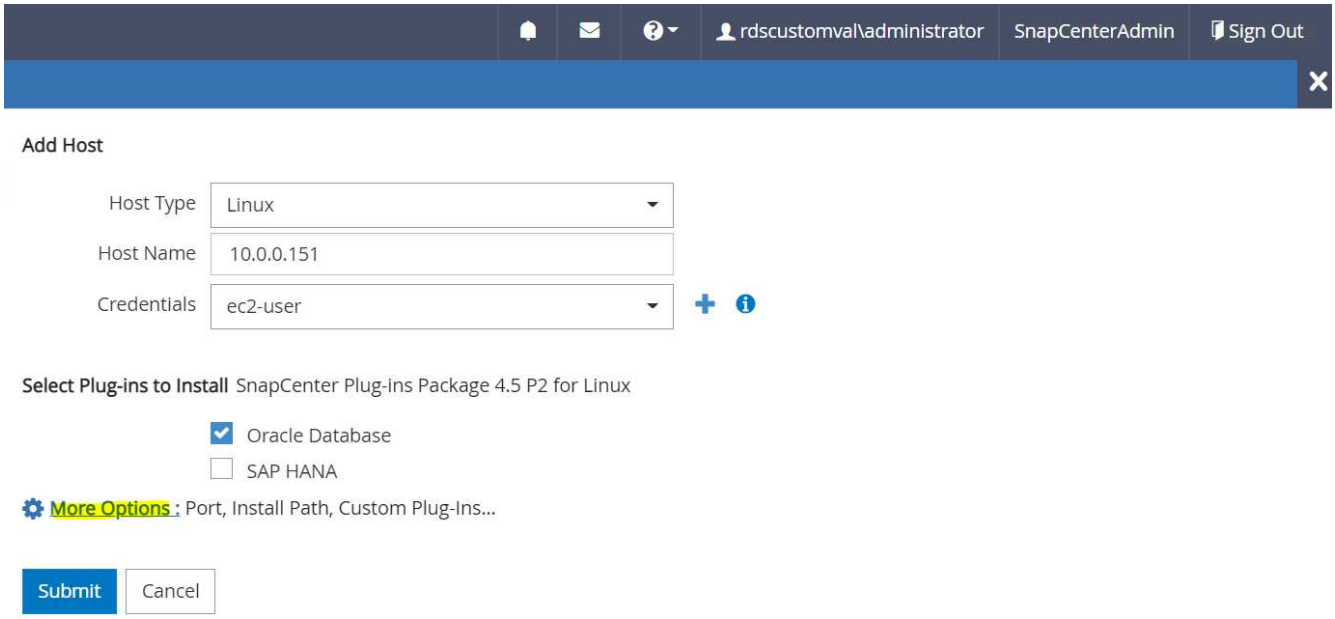
6. Fügen Sie auf dem Windows-Host des SnapCenter -Servers die IP-Adresse des EC2-Instance-Hosts zur Windows-Hostdatei hinzu `C:\Windows\System32\drivers\etc\hosts`.

```
10.0.0.151      ip-10-0-0-151.ec2.internal
```

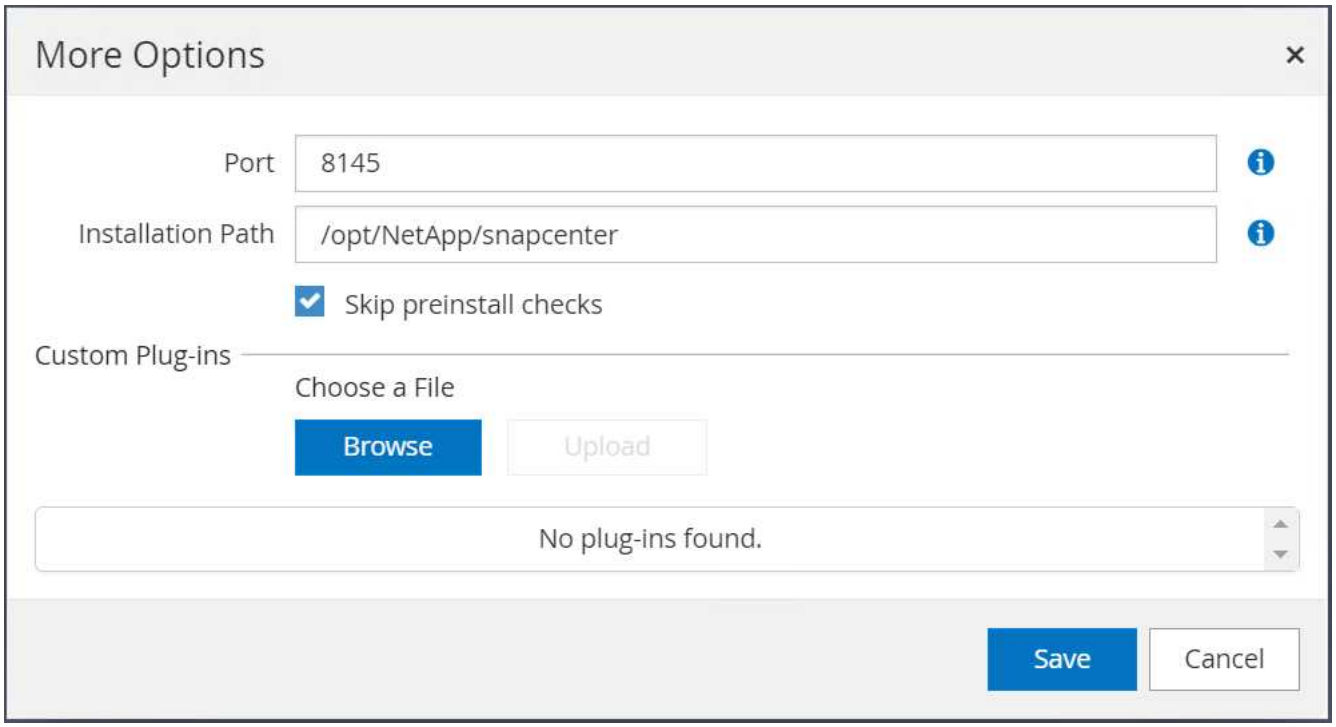
7. Wählen Sie im Menü auf der linken Seite „Hosts > Managed Hosts“ und klicken Sie dann auf „Hinzufügen“, um den EC2-Instance-Host zu SnapCenter hinzuzufügen.



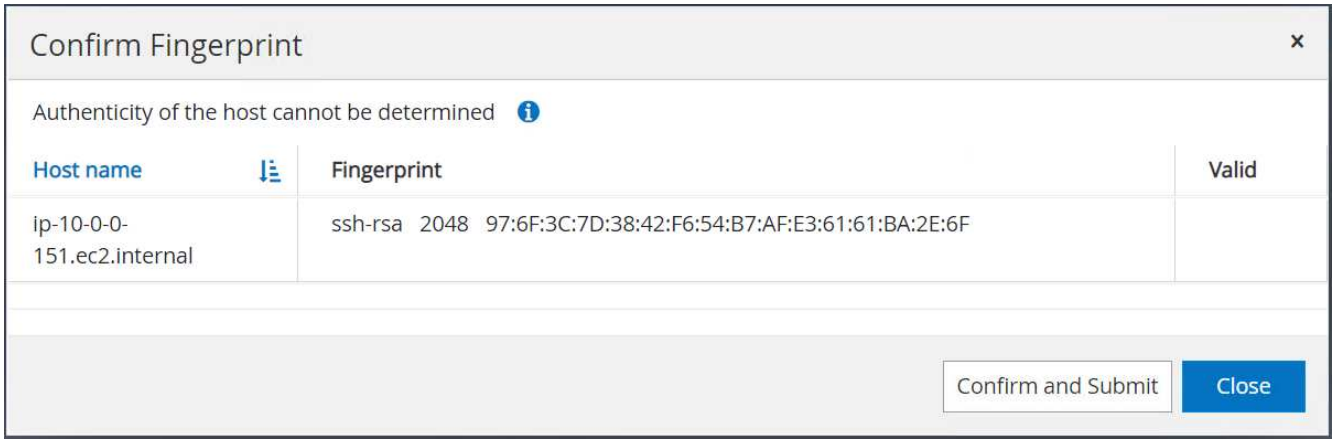
Aktivieren Sie die Oracle-Datenbank und klicken Sie vor dem Absenden auf „Weitere Optionen“.



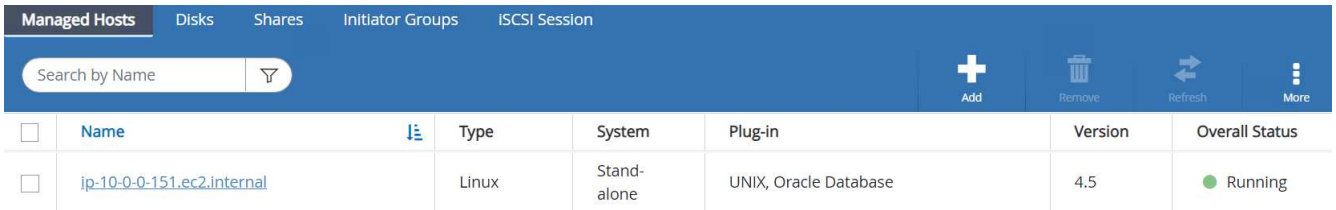
Aktivieren Sie „Vorinstallationsprüfungen überspringen“. Bestätigen Sie das Überspringen der Vorinstallationsprüfungen und klicken Sie dann auf „Nach dem Speichern senden“.



Sie werden aufgefordert, den Fingerabdruck zu bestätigen. Klicken Sie dann auf „Bestätigen und senden“.



Nach erfolgreicher Plugin-Konfiguration wird der Gesamtstatus des verwalteten Hosts als „Wird ausgeführt“ angezeigt.



Konfigurieren der Sicherungsrichtlinie für die Oracle-Datenbank

Siehe diesen Abschnitt"Richten Sie die Datenbanksicherungsrichtlinie in SnapCenter ein" Einzelheiten zum Konfigurieren der Oracle-Datenbank-Sicherungsrichtlinie.

Im Allgemeinen müssen Sie eine Richtlinie für die vollständige Snapshot-Sicherung der Oracle-Datenbank und

eine Richtlinie für die Snapshot-Sicherung nur des Oracle-Archivprotokolls erstellen.

> Sie können die Bereinigung des Oracle-Archivprotokolls in der Sicherungsrichtlinie aktivieren, um den Protokollarchivspeicherplatz zu steuern. Aktivieren Sie „ SnapMirror nach dem Erstellen einer lokalen Snapshot-Kopie aktualisieren“ unter „Sekundäre Replikationsoption auswählen“, da Sie für HA oder DR an einen Standby-Speicherort replizieren müssen.

Konfigurieren der Sicherung und Planung von Oracle-Datenbanken

Die Datenbanksicherung in SnapCenter ist benutzerkonfigurierbar und kann entweder einzeln oder als Gruppe in einer Ressourcengruppe eingerichtet werden. Das Sicherungsintervall hängt von den RTO- und RPO-Zielen ab. NetApp empfiehlt, alle paar Stunden eine vollständige Datenbanksicherung durchzuführen und die Protokollsicherung für eine schnelle Wiederherstellung häufiger, beispielsweise alle 10–15 Minuten, zu archivieren.

Weitere Informationen finden Sie im Oracle-Abschnitt von"Implementieren Sie eine Sicherungsrichtlinie zum Schutz der Datenbank" für eine detaillierte Schritt-für-Schritt-Anleitung zur Implementierung der im Abschnitt erstellten SicherungsrichtlinieKonfigurieren der Sicherungsrichtlinie für die Oracle-Datenbank und für die Planung von Sicherungsaufträgen.

Das folgende Bild zeigt ein Beispiel für die Ressourcengruppen, die zum Sichern einer Oracle-Datenbank eingerichtet werden.

EC2- und FSx-Oracle-Datenbankverwaltung

Zusätzlich zur AWS EC2- und FSx-Verwaltungskonsole werden in dieser Oracle-Umgebung der Ansible-Steuerknoten und das SnapCenter -UI-Tool für die Datenbankverwaltung eingesetzt.

Ein Ansible-Steuerknoten kann zum Verwalten der Oracle-Umgebungskonfiguration verwendet werden, mit parallelen Updates, die primäre und Standby-Instanzen für Kernel- oder Patch-Updates synchron halten. Failover, Resynchronisierung und Failback können mit dem NetApp Automation Toolkit automatisiert werden, um eine schnelle Anwendungswiederherstellung und -verfügbarkeit mit Ansible zu erreichen. Einige wiederholbare Datenbankverwaltungsaufgaben können mithilfe eines Playbooks ausgeführt werden, um menschliche Fehler zu reduzieren.

Das SnapCenter -UI-Tool kann mit dem SnapCenter -Plugin für Oracle-Datenbanken Datenbank-Snapshot-Backups, Point-in-Time-Wiederherstellungen, Datenbankklonen usw. durchführen. Weitere Informationen zu den Funktionen des Oracle-Plugins finden Sie im"Übersicht über das SnapCenter -Plug-in für Oracle-Datenbanken" .

Die folgenden Abschnitte enthalten Einzelheiten dazu, wie wichtige Funktionen der Oracle-Datenbankverwaltung mit der SnapCenter -Benutzeroberfläche erfüllt werden:

- Datenbank-Snapshot-Backups
- Datenbank-Point-in-Time-Wiederherstellung
- Datenbankklon erstellen

Beim Datenbankklonen wird eine Replik einer primären Datenbank auf einem separaten EC2-Host erstellt, um im Falle eines logischen Datenfehlers oder einer Beschädigung die Daten wiederherstellen zu können. Klone können außerdem zum Testen von Anwendungen, zum Debuggen, zur Patch-Validierung usw. verwendet werden.

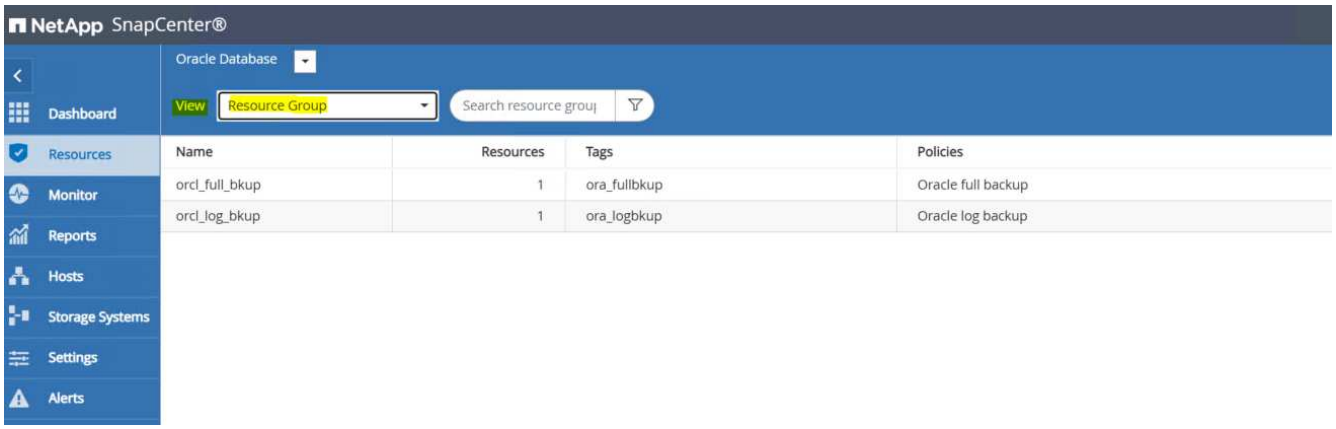
Einen Schnappschuss machen

Eine EC2/FSx Oracle-Datenbank wird regelmäßig in vom Benutzer konfigurierten Intervallen gesichert. Ein Benutzer kann außerdem jederzeit eine einmalige Snapshot-Sicherung durchführen. Dies gilt sowohl für Snapshot-Sicherungen der gesamten Datenbank als auch für Snapshot-Sicherungen nur des Archivprotokolls.

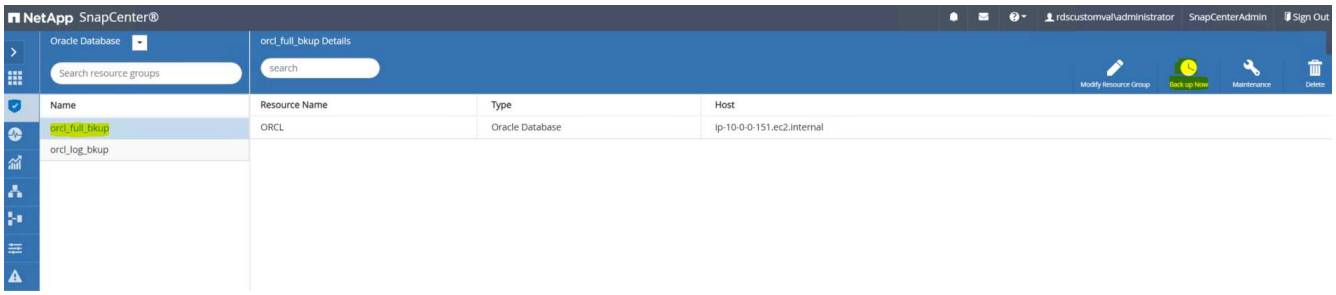
Erstellen eines vollständigen Datenbank-Snapshots

Ein vollständiger Datenbank-Snapshot umfasst alle Oracle-Dateien, einschließlich Datendateien, Steuerdateien und Archivprotokolldateien.

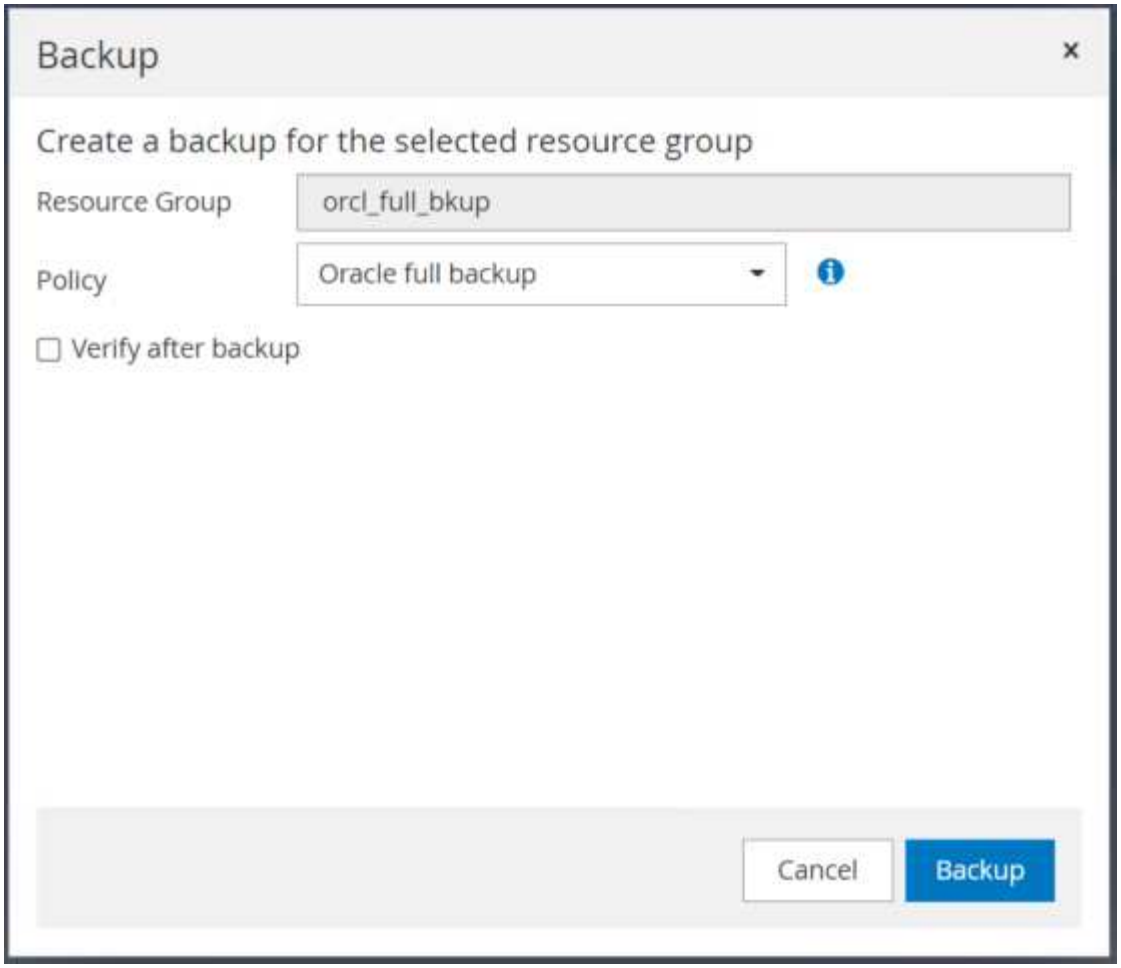
1. Melden Sie sich bei der SnapCenter -Benutzeroberfläche an und klicken Sie im Menü auf der linken Seite auf „Ressourcen“. Wechseln Sie im Dropdown-Menü „Ansicht“ zur Ansicht „Ressourcengruppe“.



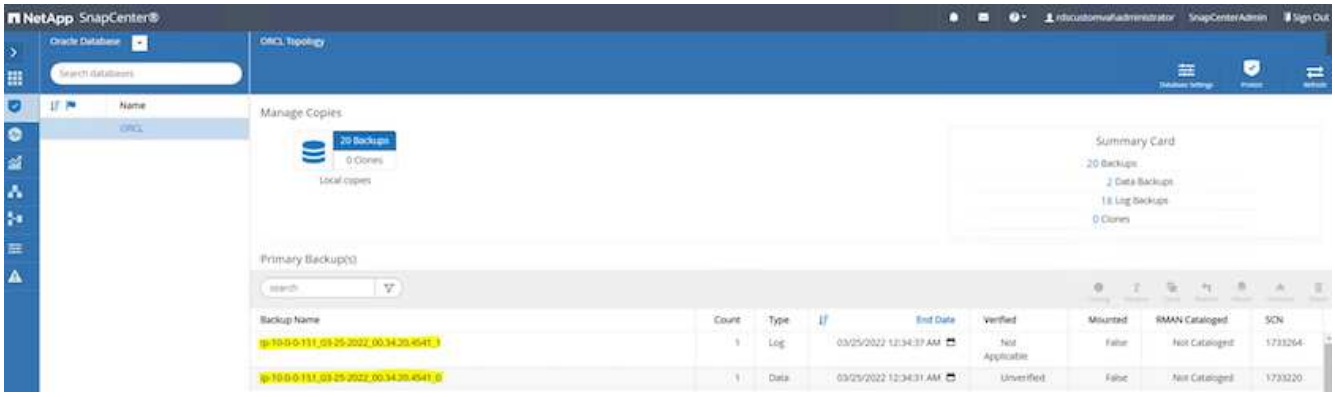
2. Klicken Sie auf den Namen der vollständigen Sicherungsressource und dann auf das Symbol „Jetzt sichern“, um eine Ad-hoc-Sicherung zu starten.



3. Klicken Sie auf „Sichern“ und bestätigen Sie anschließend die Sicherung, um eine vollständige Datenbanksicherung zu starten.



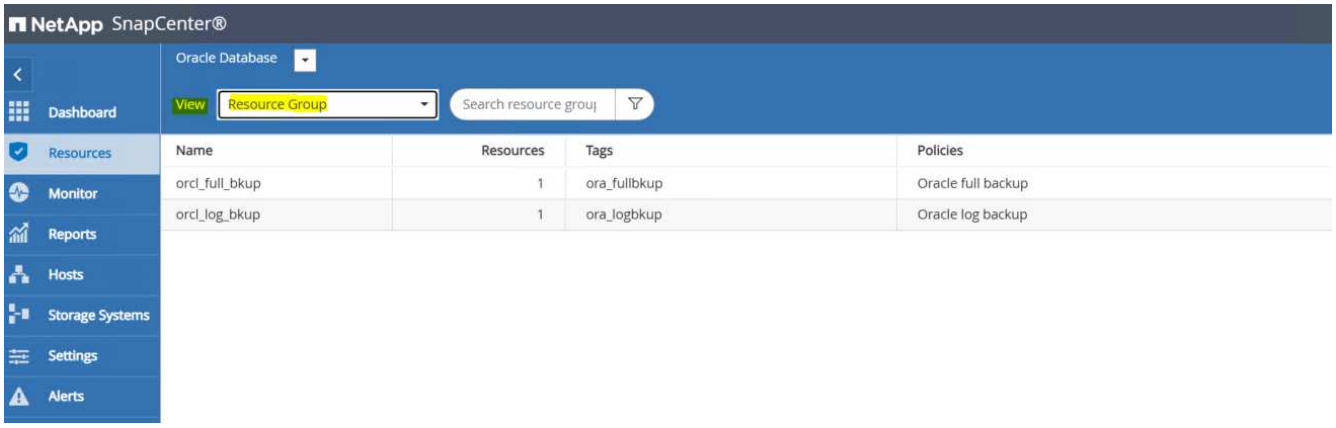
Öffnen Sie in der Ressourcenansicht der Datenbank die Seite „Verwaltete Sicherungskopien“ der Datenbank, um zu überprüfen, ob die einmalige Sicherung erfolgreich abgeschlossen wurde. Bei einer vollständigen Datenbanksicherung werden zwei Snapshots erstellt: einer für das Datenvolumen und einer für das Protokollvolumen.



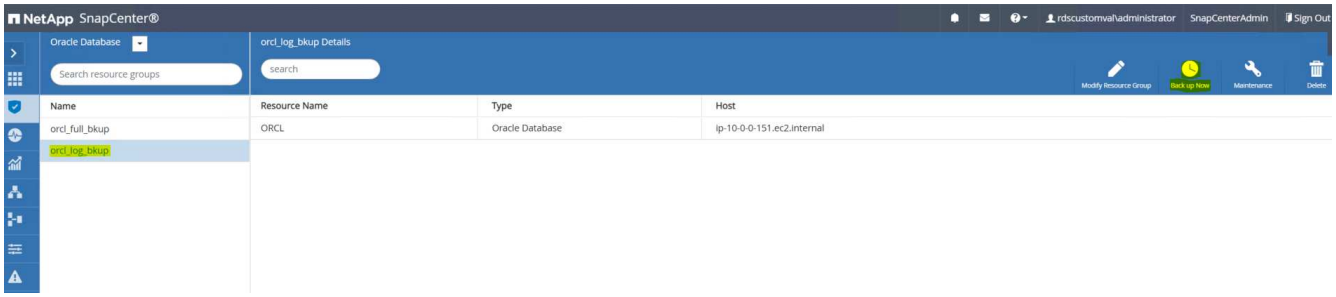
Erstellen eines Archivprotokoll-Snapshots

Ein Archivprotokoll-Snapshot wird nur für das Oracle-Archivprotokollvolume erstellt.

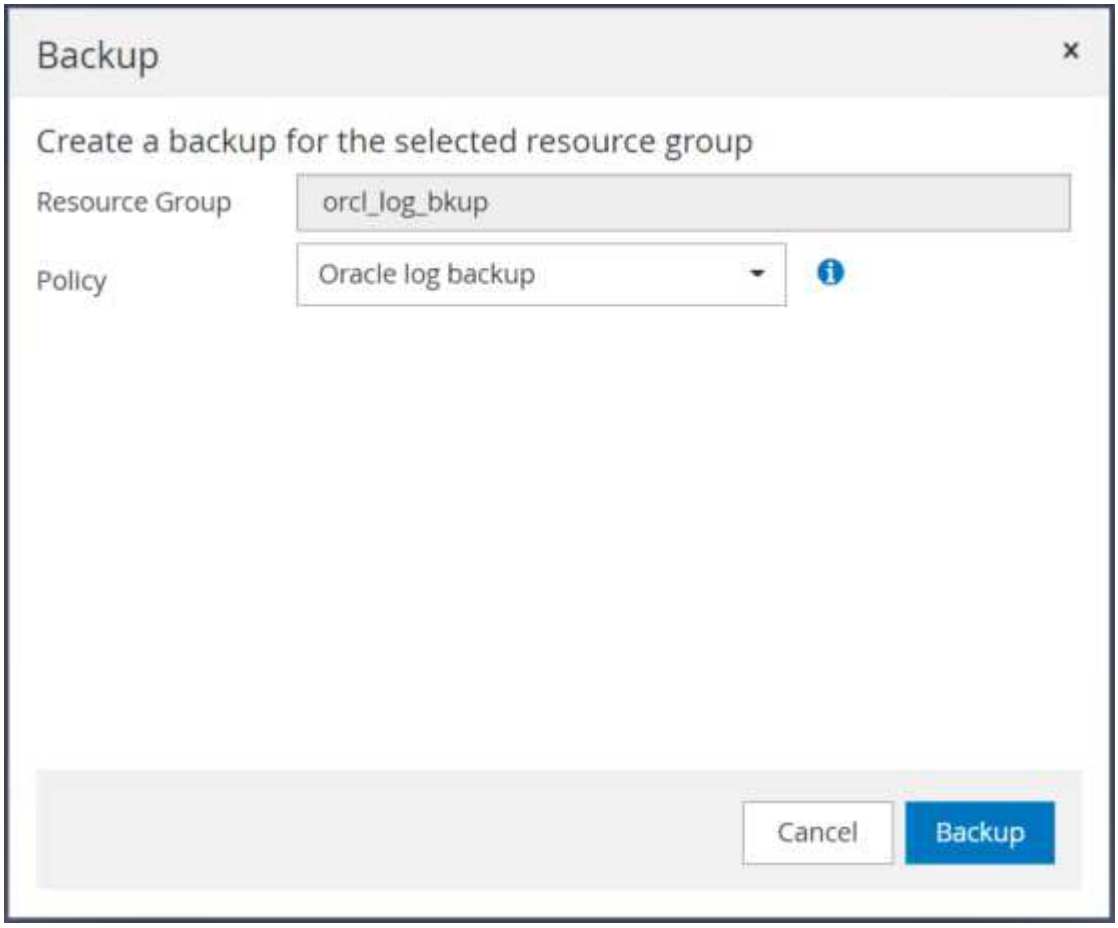
1. Melden Sie sich bei der SnapCenter -Benutzeroberfläche an und klicken Sie in der linken Menüleiste auf die Registerkarte „Ressourcen“. Wechseln Sie im Dropdown-Menü „Ansicht“ zur Ansicht „Ressourcengruppe“.



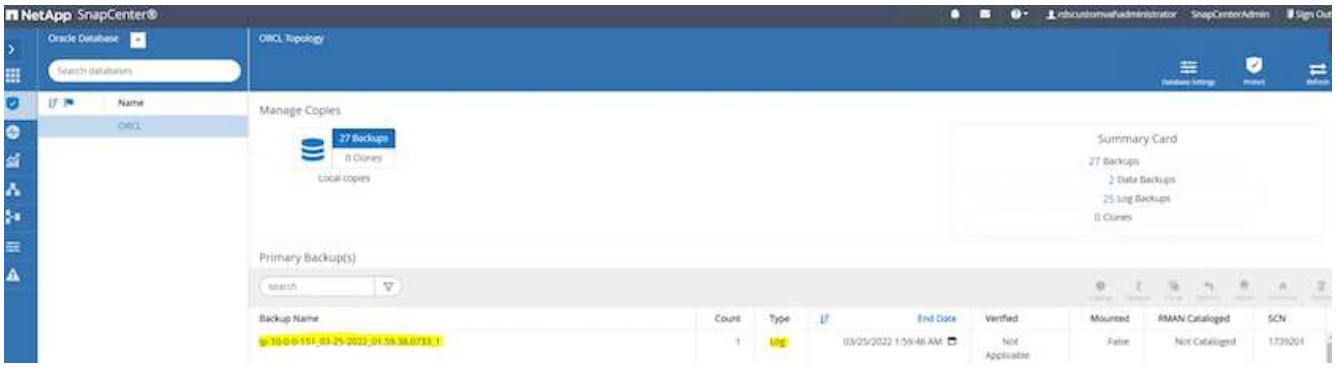
2. Klicken Sie auf den Ressourcennamen der Protokollsicherung und dann auf das Symbol „Jetzt sichern“, um eine Ad-hoc-Sicherung für Archivprotokolle zu starten.



3. Klicken Sie auf „Sichern“ und bestätigen Sie die Sicherung, um eine Archivprotokollsicherung zu starten.



Öffnen Sie in der Ressourcenansicht der Datenbank die Seite „Verwaltete Sicherungskopien“ der Datenbank, um zu überprüfen, ob die einmalige Sicherung des Archivprotokolls erfolgreich abgeschlossen wurde. Bei einer Archivprotokollsicherung wird ein Snapshot für das Protokollvolume erstellt.

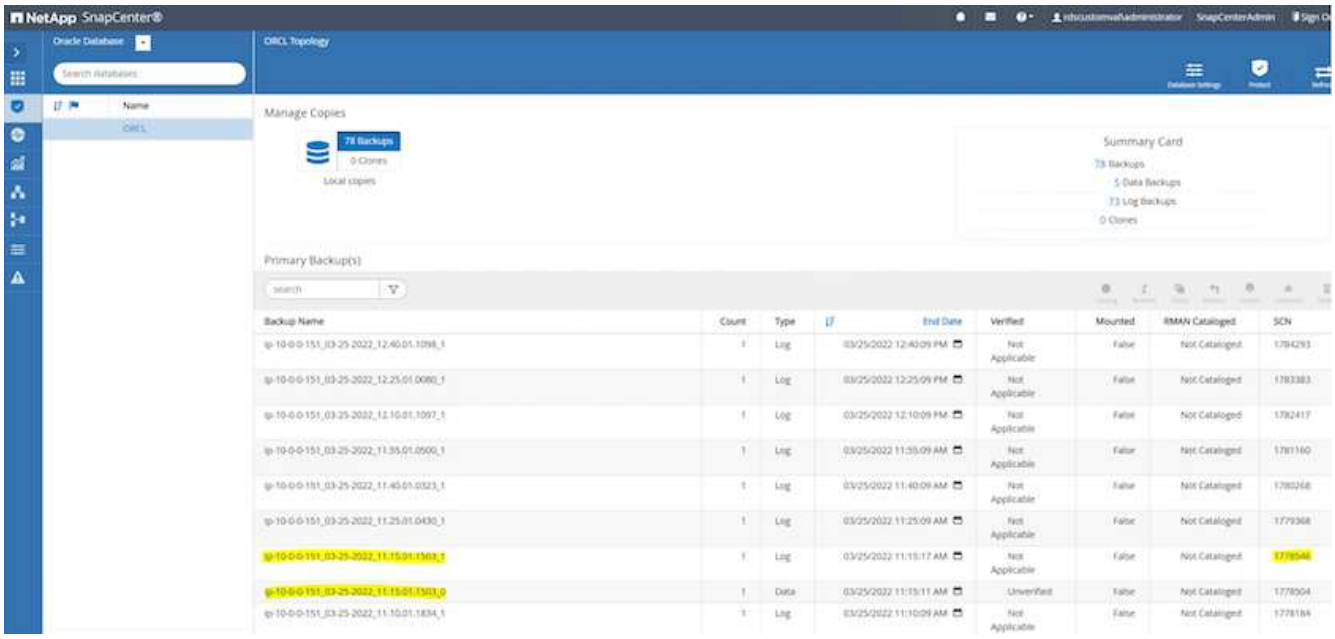


Wiederherstellen zu einem bestimmten Zeitpunkt

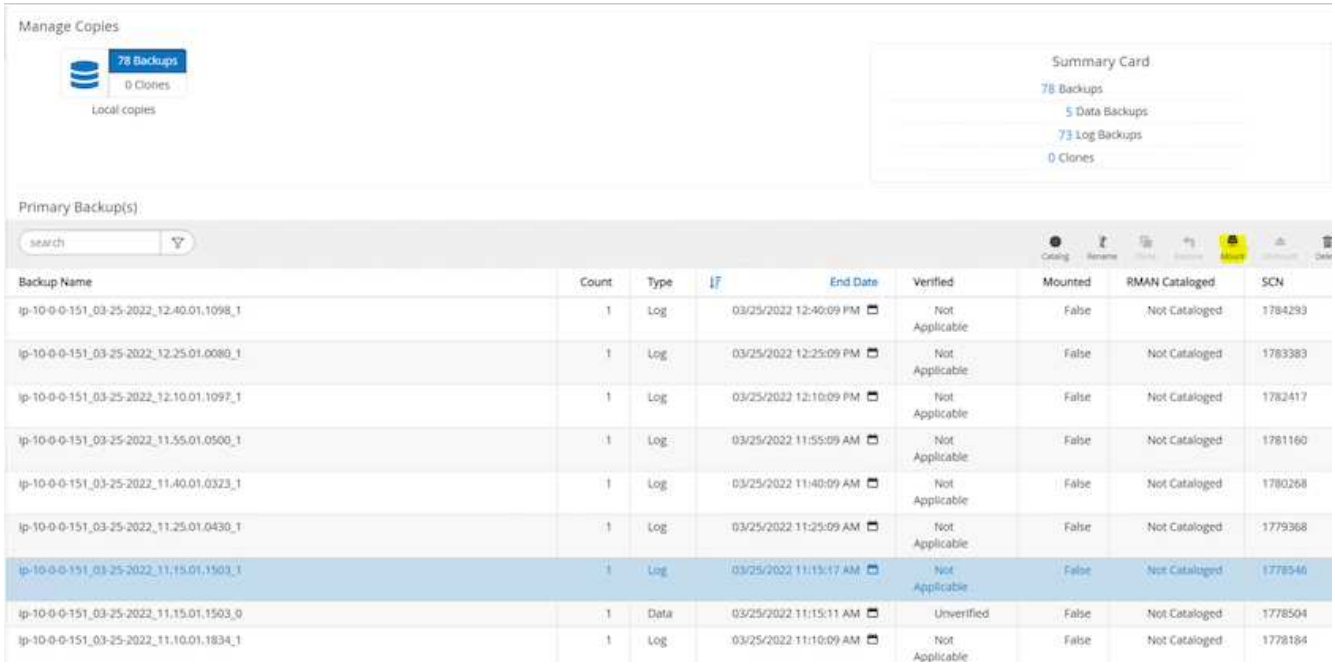
Die SnapCenter-basierte Wiederherstellung zu einem bestimmten Zeitpunkt wird auf demselben EC2-Instance-Host ausgeführt. Führen Sie die folgenden Schritte aus, um die Wiederherstellung durchzuführen:

1. Klicken Sie auf der Registerkarte „SnapCenter -Ressourcen“ > „Datenbankansicht“ auf den Datenbanknamen, um die Datenbanksicherung zu öffnen.

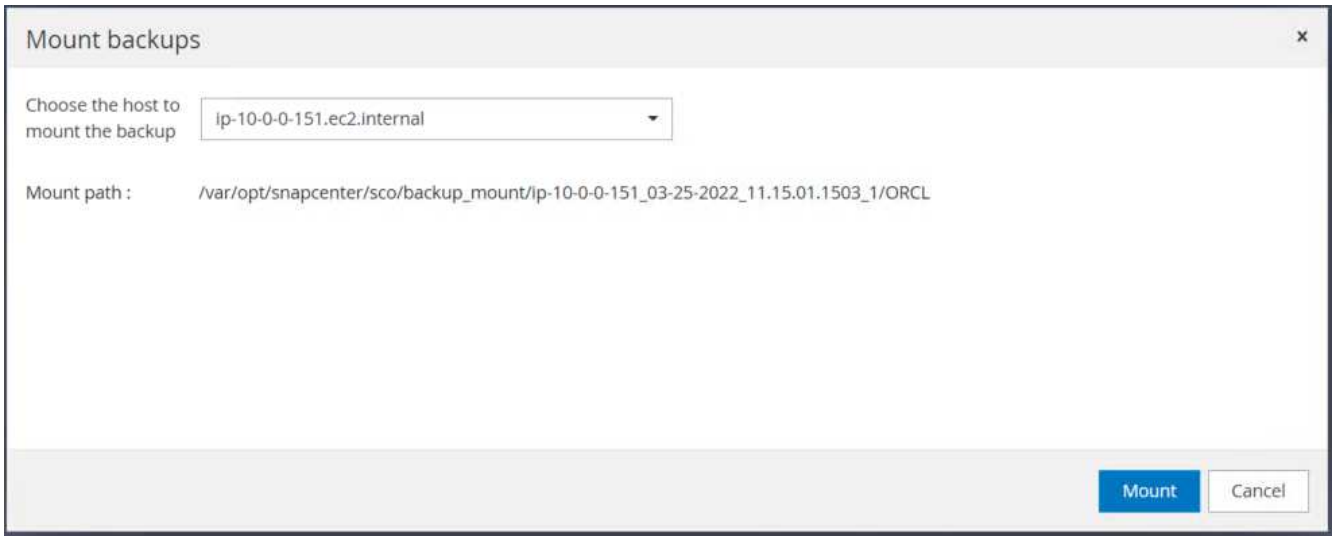
2. Wählen Sie die Datenbanksicherungskopie und den gewünschten Zeitpunkt zur Wiederherstellung aus. Notieren Sie sich auch die entsprechende SCN-Nummer zum Zeitpunkt. Die Point-in-Time-Wiederherstellung kann entweder anhand der Uhrzeit oder der SCN durchgeführt werden.



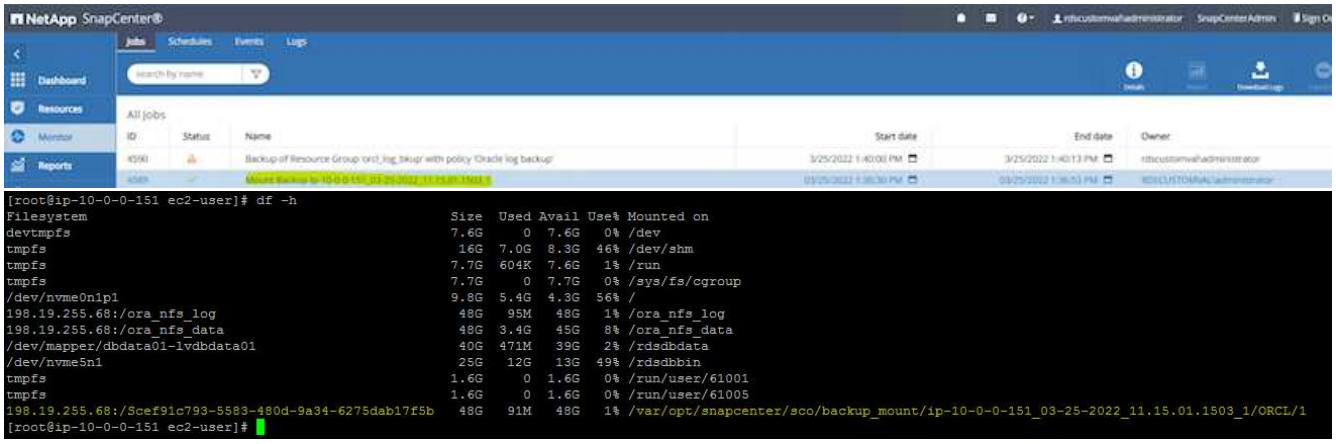
3. Markieren Sie den Snapshot des Protokollvolumes und klicken Sie auf die Schaltfläche „Mounten“, um das Volume zu mounten.



4. Wählen Sie die primäre EC2-Instanz zum Mounten des Protokolldatenträgers.



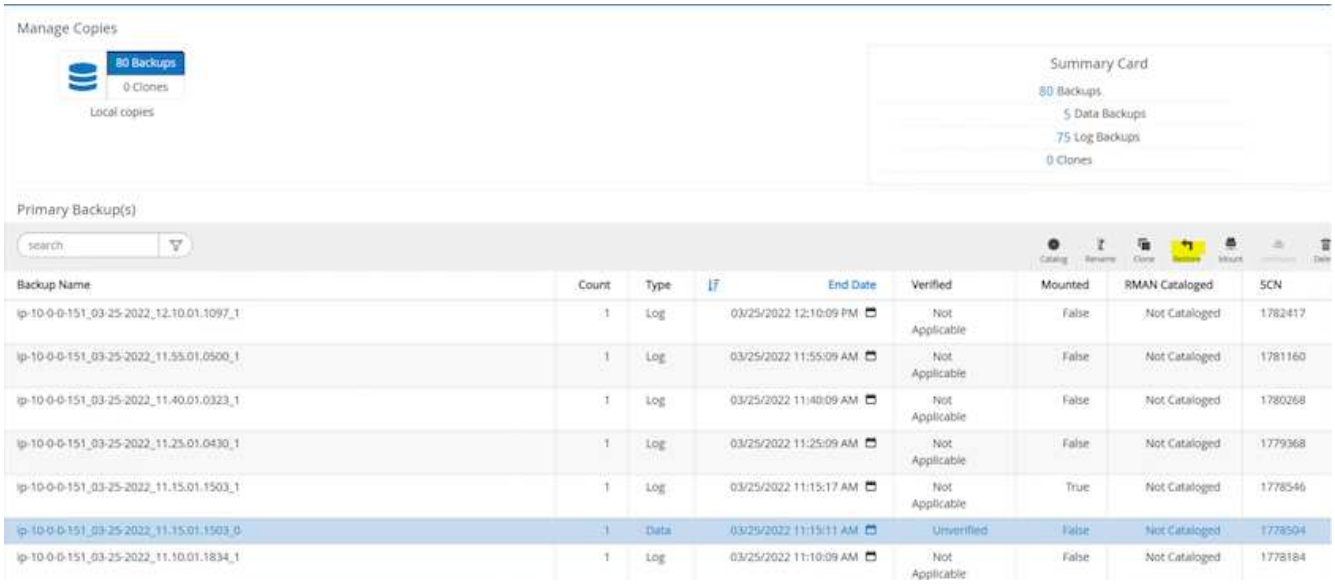
5. Überprüfen Sie, ob der Mount-Job erfolgreich abgeschlossen wurde. Überprüfen Sie auch den EC2-Instance-Host, um das bereitgestellte Protokollvolume und den Bereitstellungspunktpfad anzuzeigen.



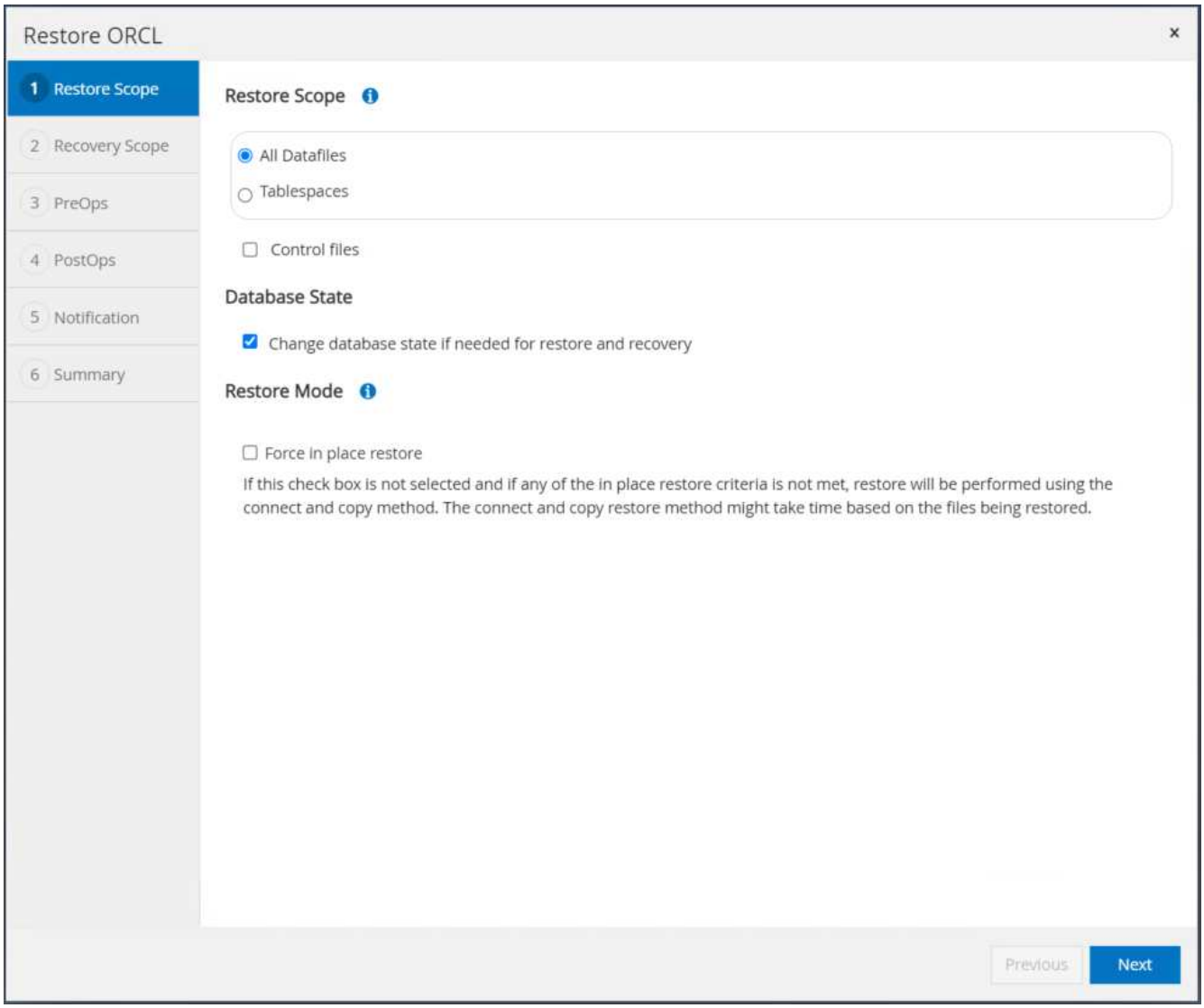
6. Kopieren Sie die Archivprotokolle vom bereitgestellten Protokolldatenträger in das aktuelle Archivprotokollverzeichnis.

```
[ec2-user@ip-10-0-0-151 ~]$ cp /var/opt/snapcenter/sco/backup_mount/ip-10-0-0-151_03-25-2022_11.15.01.1503_1/ORCL/1/db/ORCL_A/arch/*.arc /ora_nfs_log/db/ORCL_A/arch/
```

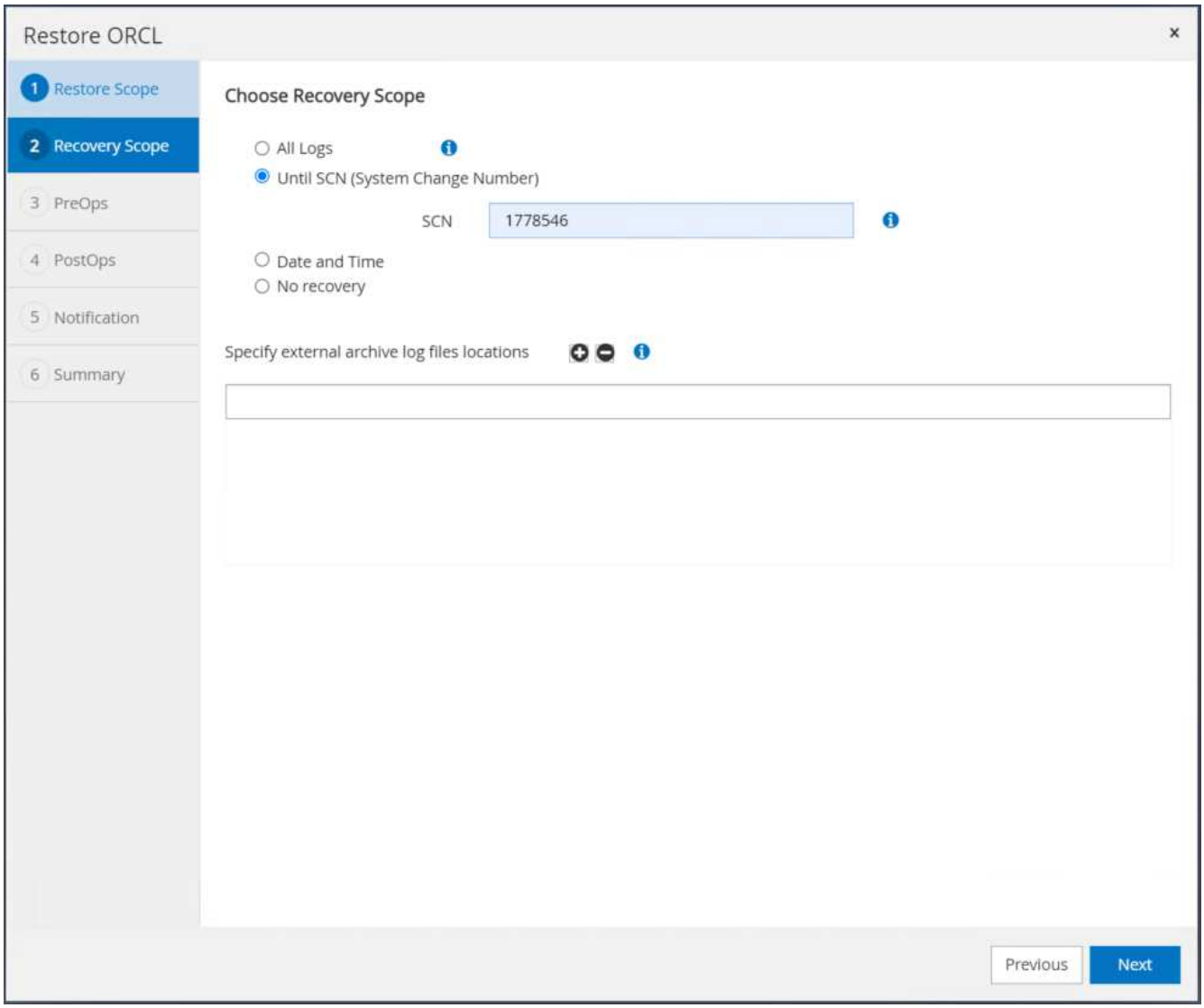
7. Kehren Sie zur Registerkarte „SnapCenter -Ressource“ > Seite „Datenbanksicherung“ zurück, markieren Sie die Daten-Snapshot-Kopie und klicken Sie auf die Schaltfläche „Wiederherstellen“, um den Workflow zur Datenbankwiederherstellung zu starten.



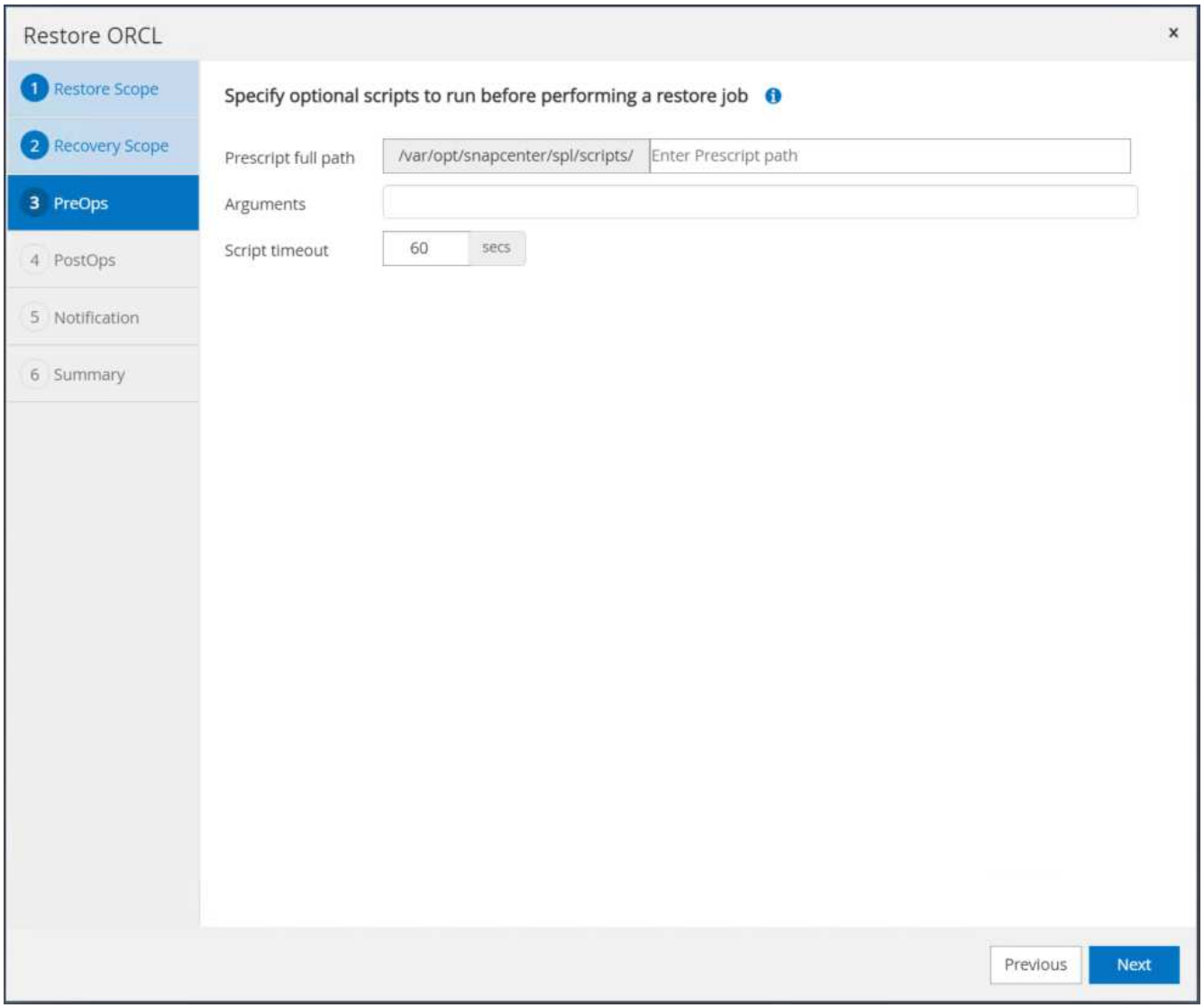
8. Aktivieren Sie „Alle Datendateien“ und „Datenbankstatus ändern, falls für Wiederherstellung und Wiederherstellung erforderlich“ und klicken Sie auf „Weiter“.



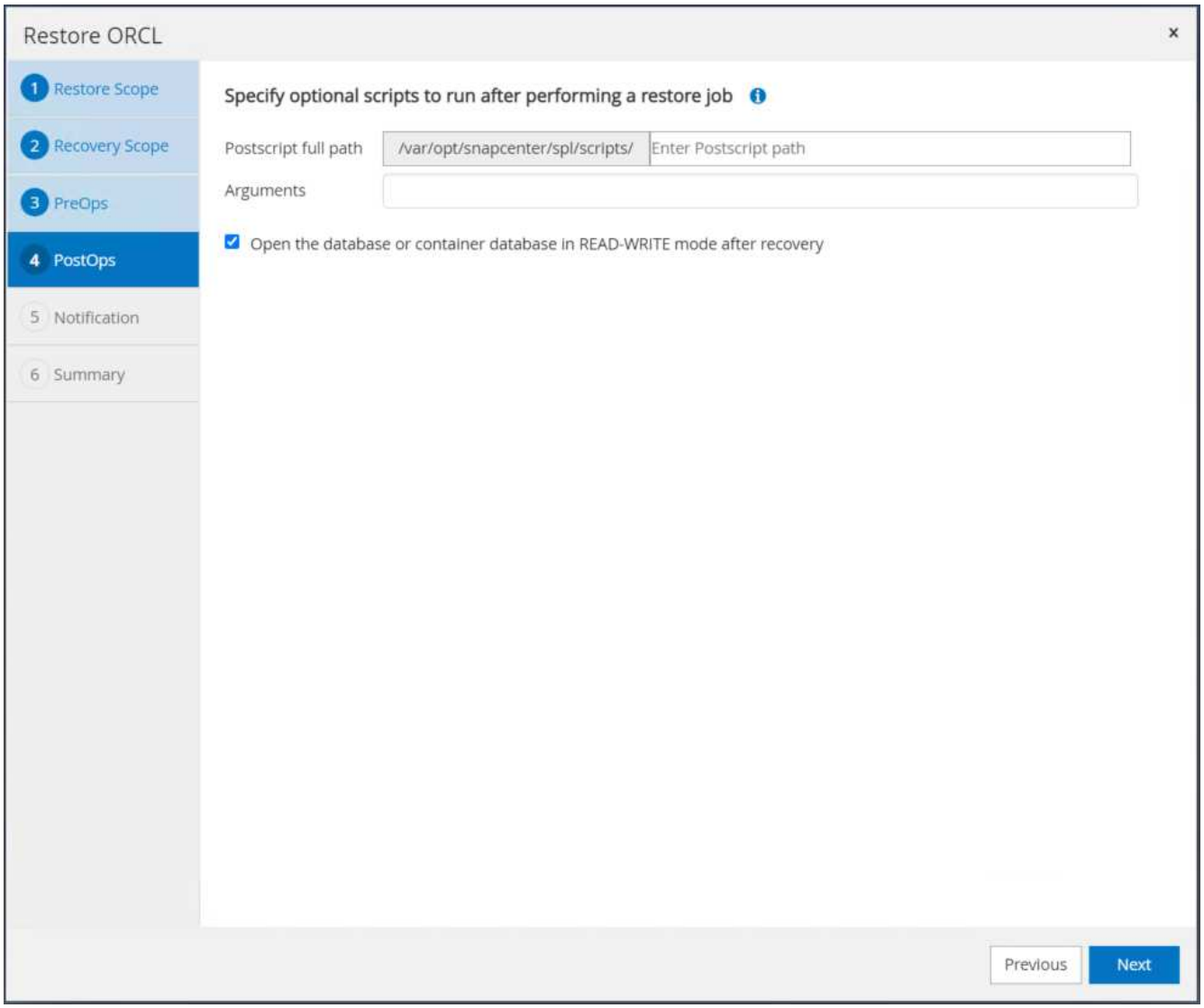
9. Wählen Sie den gewünschten Wiederherstellungsumfang entweder mithilfe von SCN oder Zeit. Anstatt die bereitgestellten Archivprotokolle in das aktuelle Protokollverzeichnis zu kopieren, wie in Schritt 6 gezeigt, kann der Pfad des bereitgestellten Archivprotokolls zur Wiederherstellung unter „Speicherorte für externe Archivprotokolldateien angeben“ aufgeführt werden.



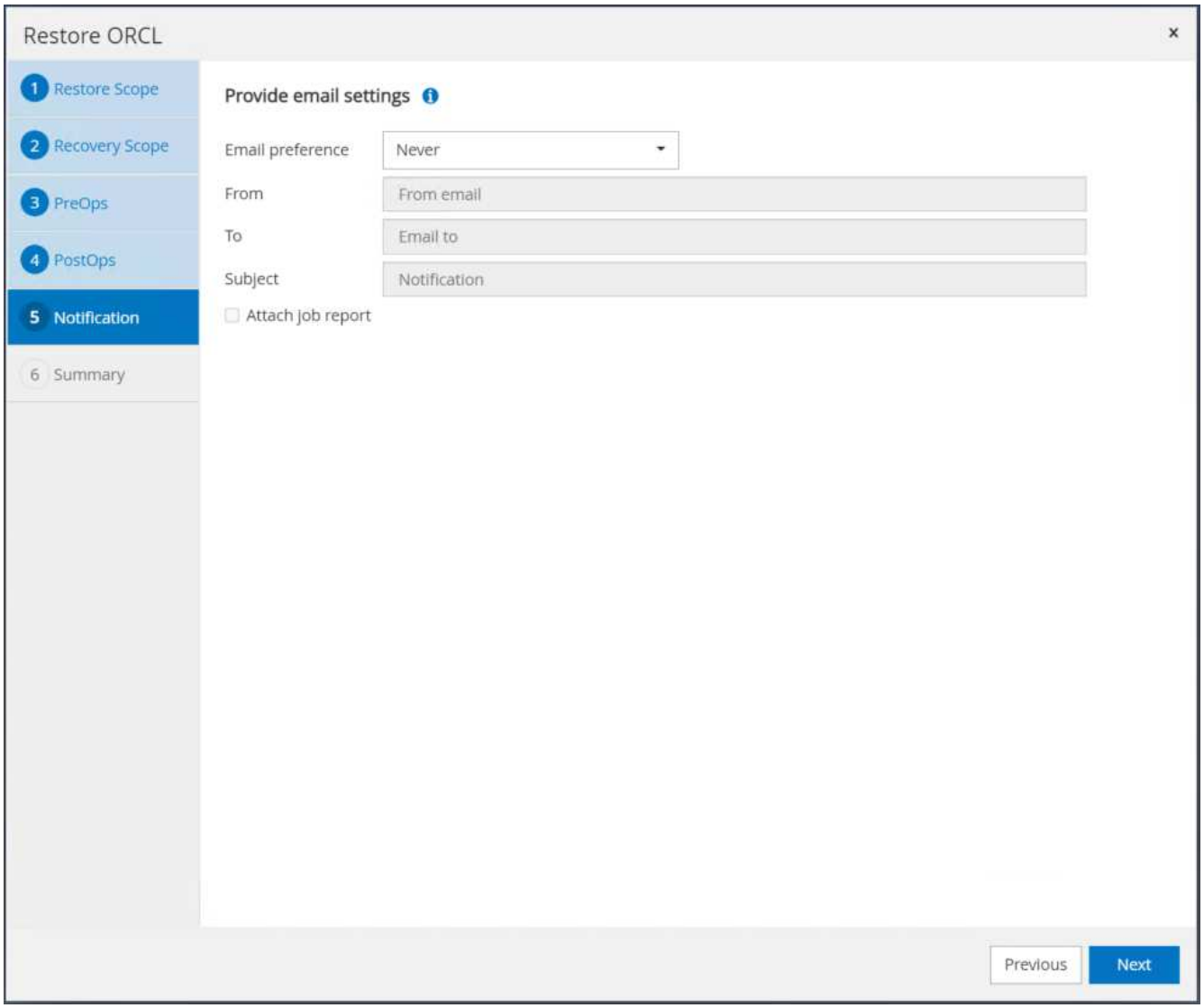
10. Geben Sie ein optionales Prescript an, das bei Bedarf ausgeführt werden soll.



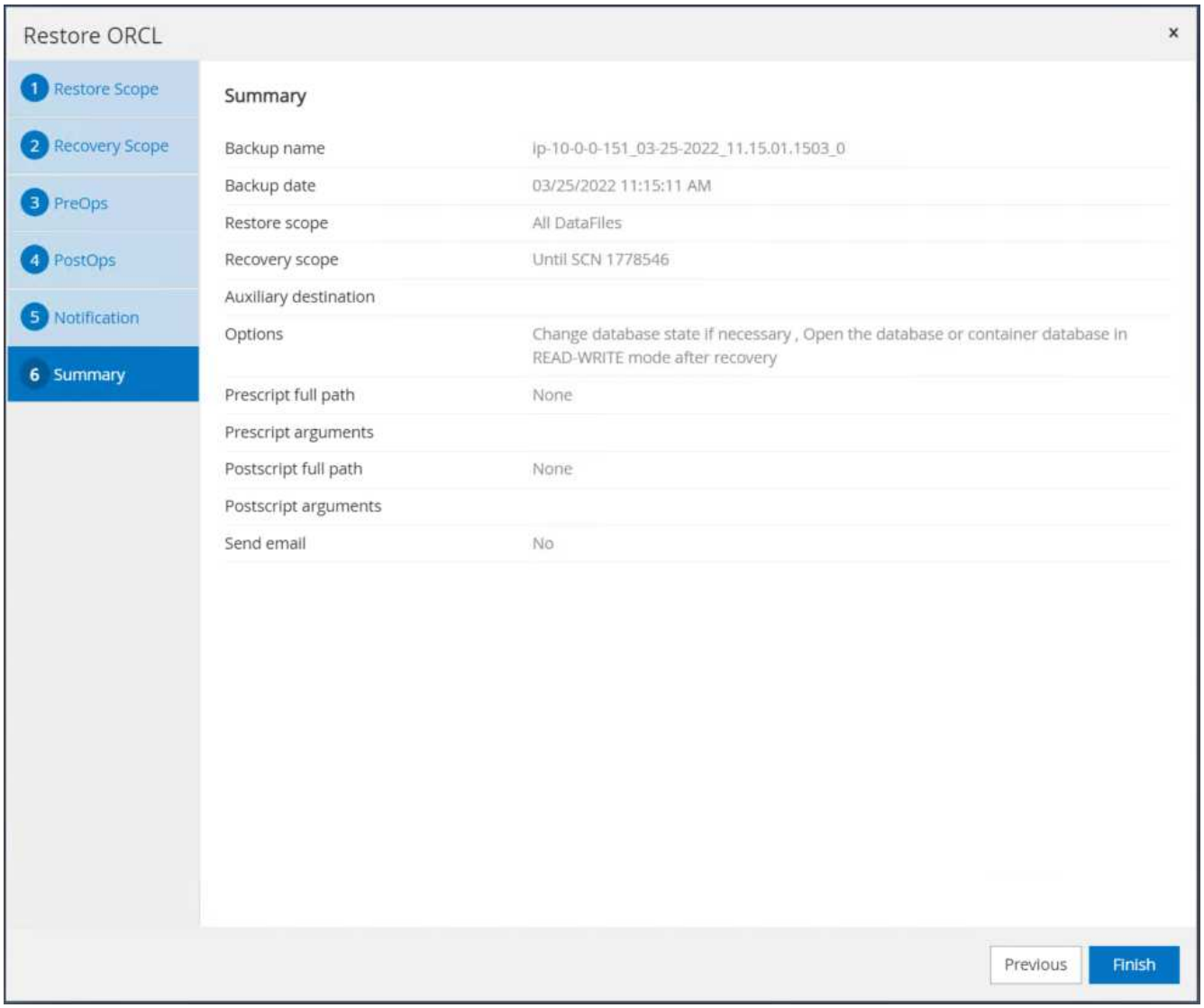
11. Geben Sie ein optionales Afterscript an, das bei Bedarf ausgeführt werden soll. Überprüfen Sie die geöffnete Datenbank nach der Wiederherstellung.



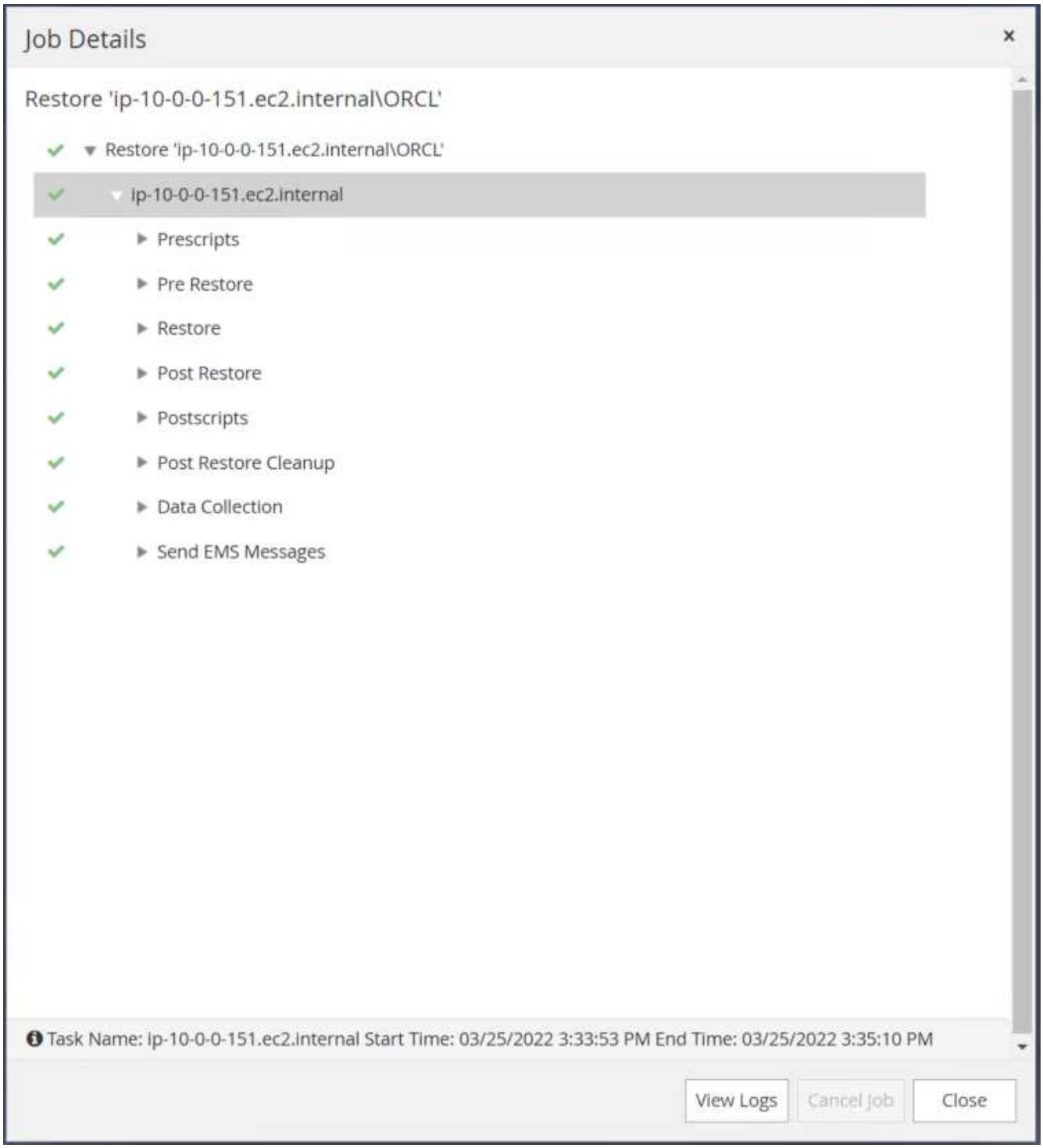
12. Geben Sie einen SMTP-Server und eine E-Mail-Adresse an, wenn eine Jobbenachrichtigung erforderlich ist.



13. Stellen Sie die Jobzusammenfassung wieder her. Klicken Sie auf „Fertig stellen“, um den Wiederherstellungsauftrag zu starten.



14. Bestätigen Sie die Wiederherstellung von SnapCenter.



15. Validieren Sie die Wiederherstellung vom EC2-Instance-Host.

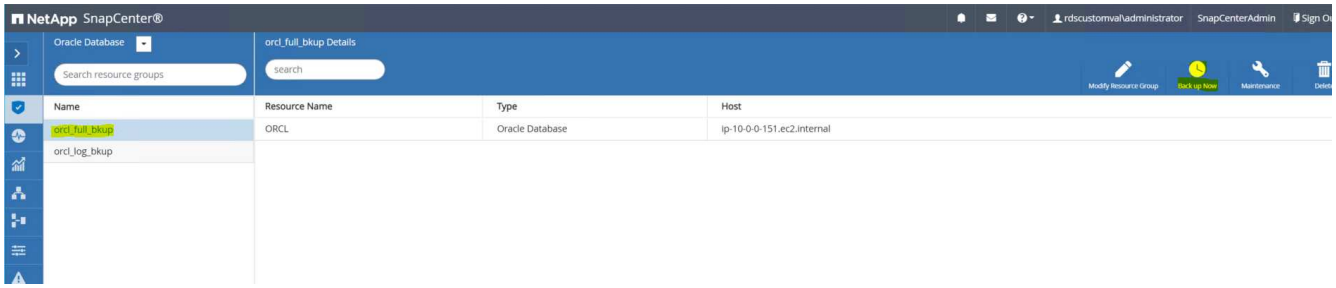
```
-bash-4.2$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Mar 25 15:44:08 2022
Version 19.8.0.0.0

Copyright (c) 1982, 2020, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.8.0.0.0

SQL> select name, RESETLOGS_CHANGE#, RESETLOGS_TIME, open_mode from v$database;

NAME      RESETLOGS_CHANGE# RESETLOGS OPEN_MODE
--------- ----------------- --------- --------------------
ORCL                1778547 25-MAR-22 READ WRITE

SQL>
```

16. Um das Wiederherstellungsprotokollvolume auszuhängen, führen Sie die Schritte in Schritt 4 in umgekehrter Reihenfolge aus.

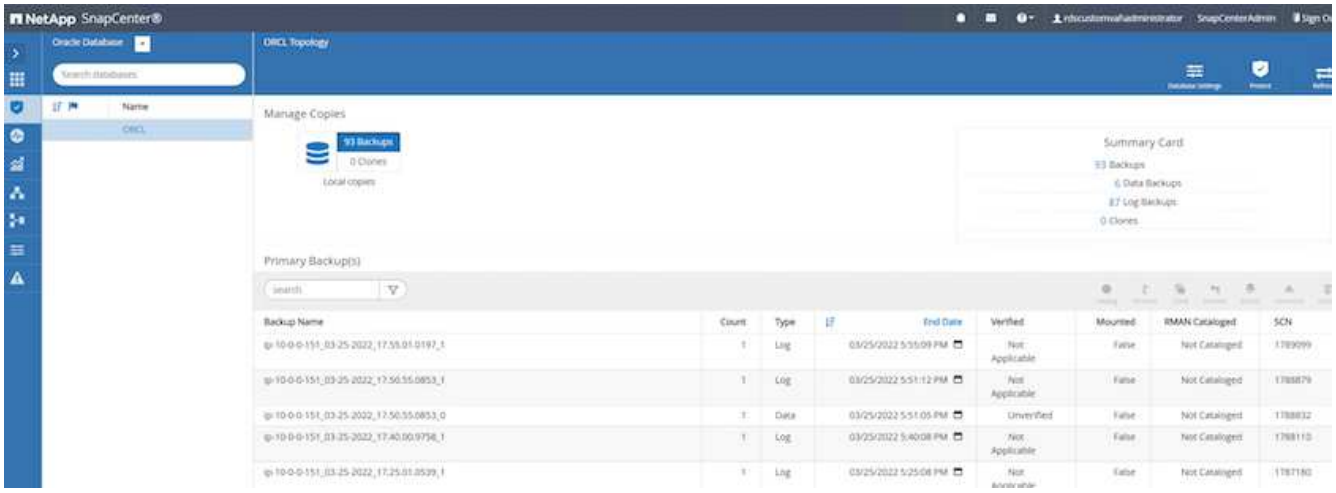
Erstellen eines Datenbankklons

Der folgende Abschnitt zeigt, wie Sie mit dem SnapCenter -Klon-Workflow einen Datenbankklon von einer primären Datenbank zu einer Standby-EC2-Instance erstellen.

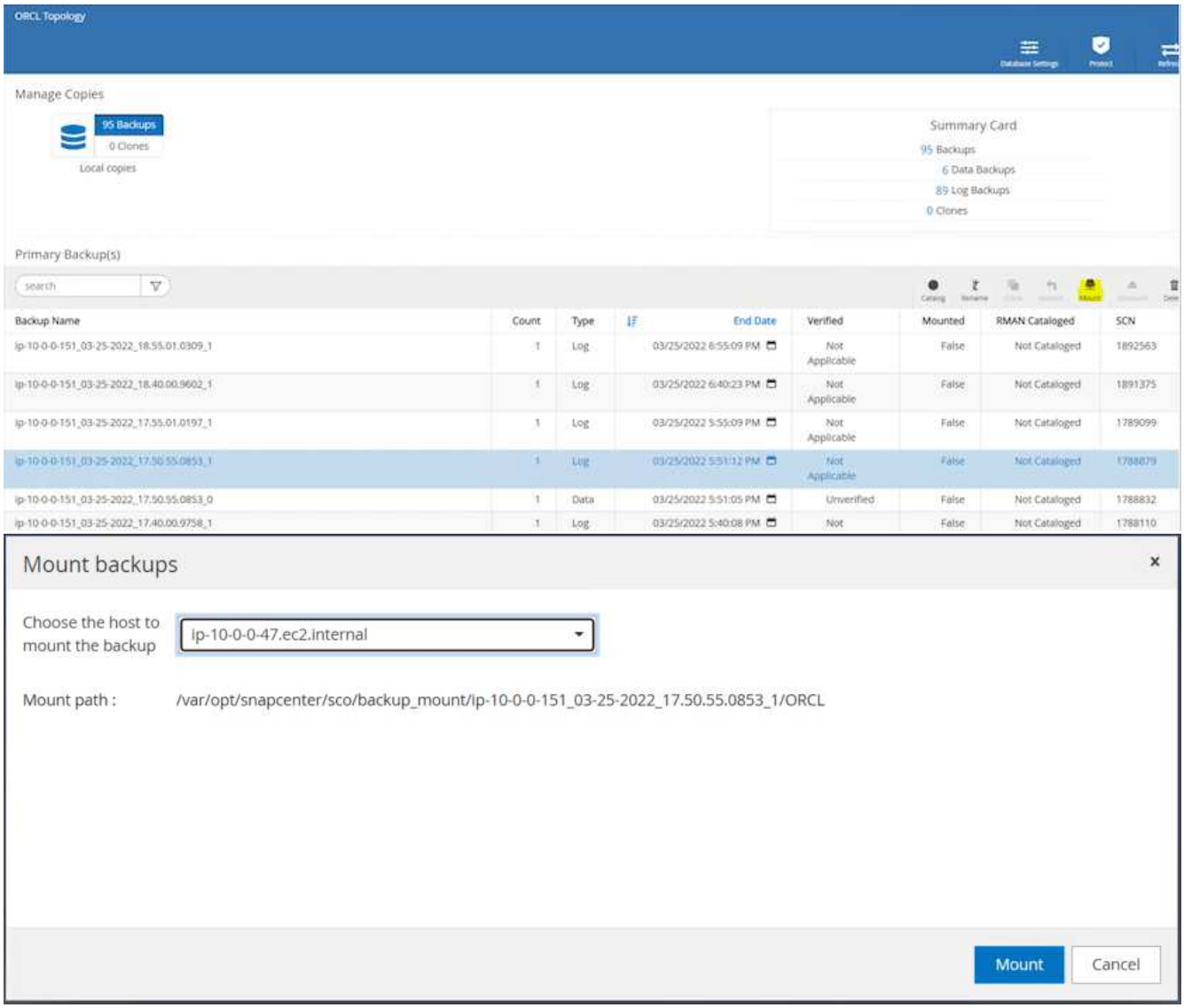
1. Erstellen Sie mithilfe der Ressourcengruppe „Vollständige Sicherung“ eine vollständige Snapshot-Sicherung der primären Datenbank von SnapCenter .



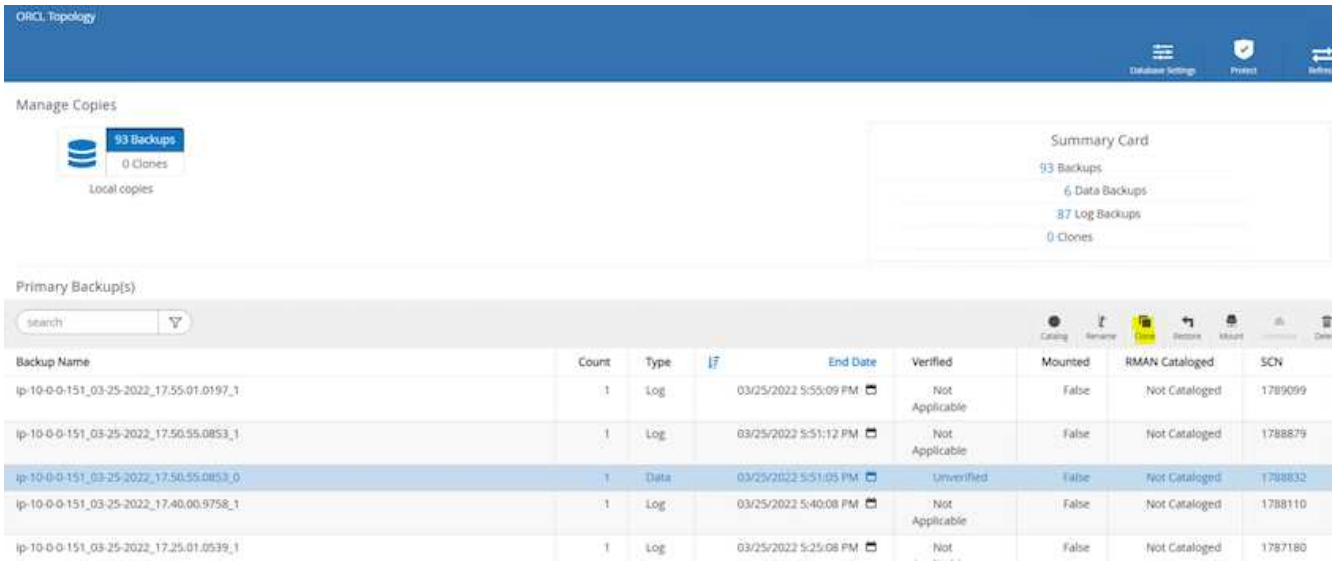
2. Öffnen Sie auf der Registerkarte „SnapCenter -Ressource“ > „Datenbankansicht“ die Seite „Datenbanksicherungsverwaltung“ für die primäre Datenbank, aus der die Replik erstellt werden soll.



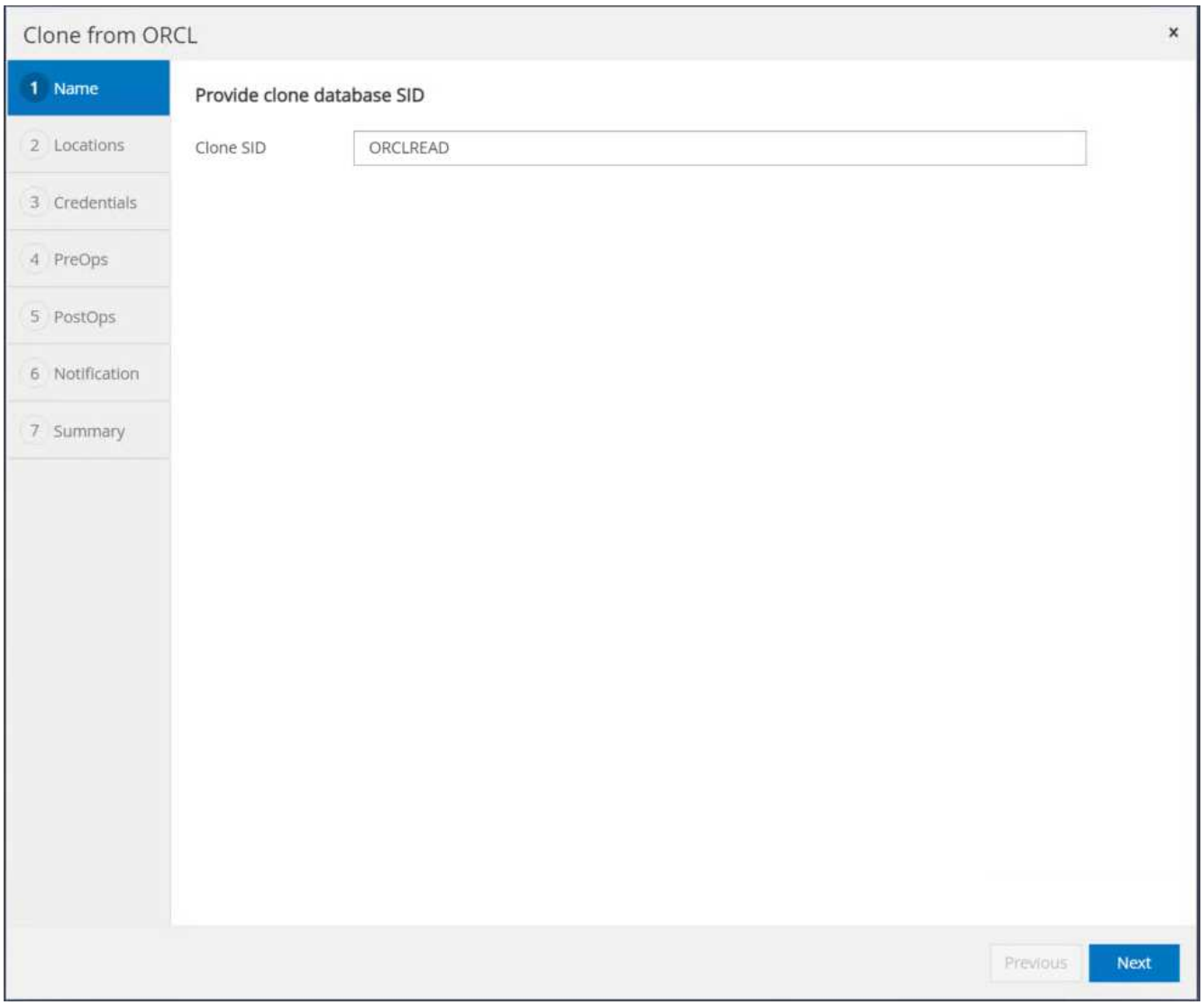
3. Hängen Sie den in Schritt 4 erstellten Snapshot des Protokollvolumes in den Standby-Host der EC2-Instance ein.



4. Markieren Sie die Snapshot-Kopie, die für die Replik geklont werden soll, und klicken Sie auf die Schaltfläche „Klonen“, um den Klonvorgang zu starten.

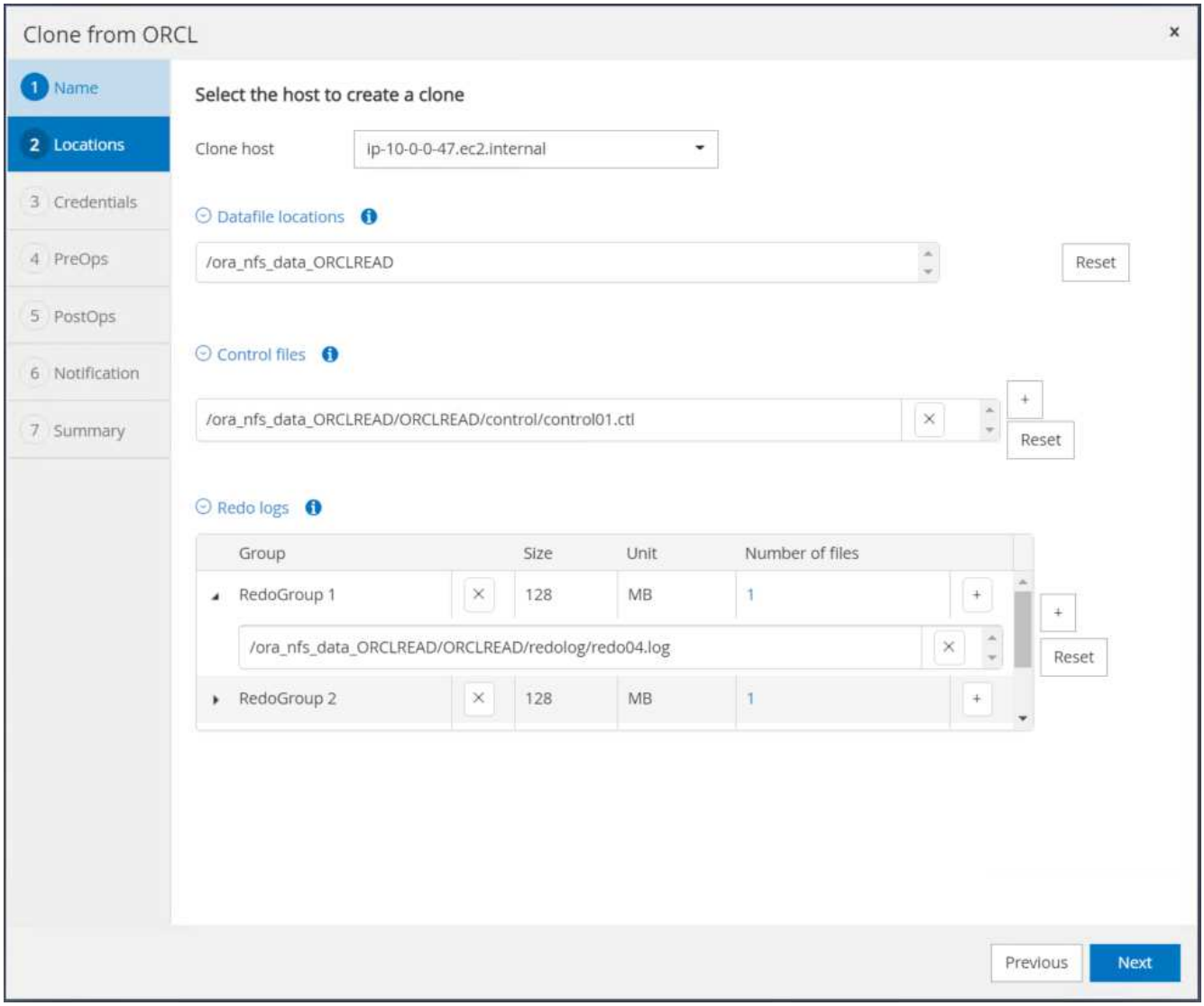


5. Ändern Sie den Namen der Replikatkopie, sodass er sich vom Namen der primären Datenbank unterscheidet. Klicken Sie auf Weiter.

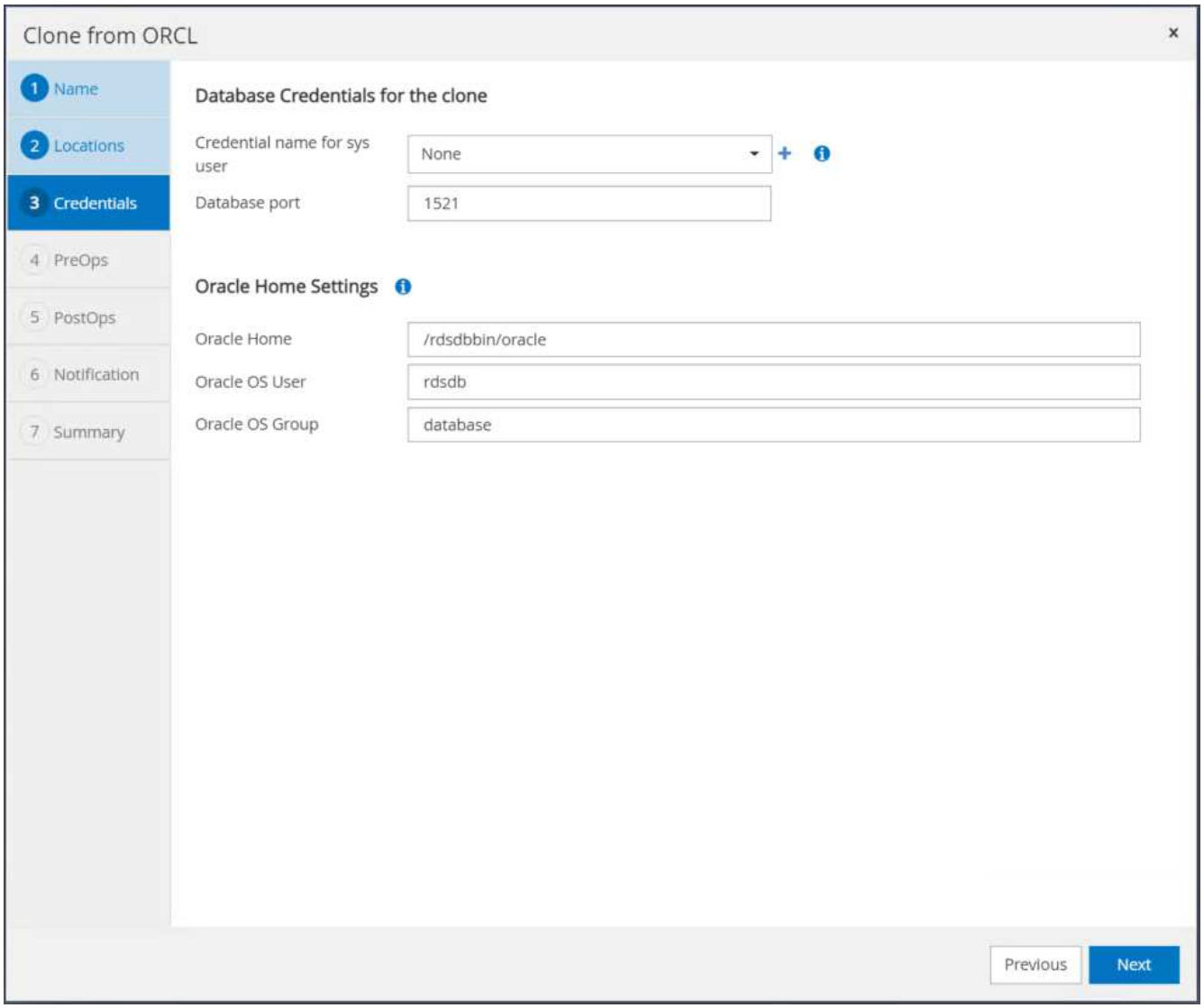


6. Ändern Sie den Klonhost in den Standby-EC2-Host, akzeptieren Sie die Standardbenennung und klicken

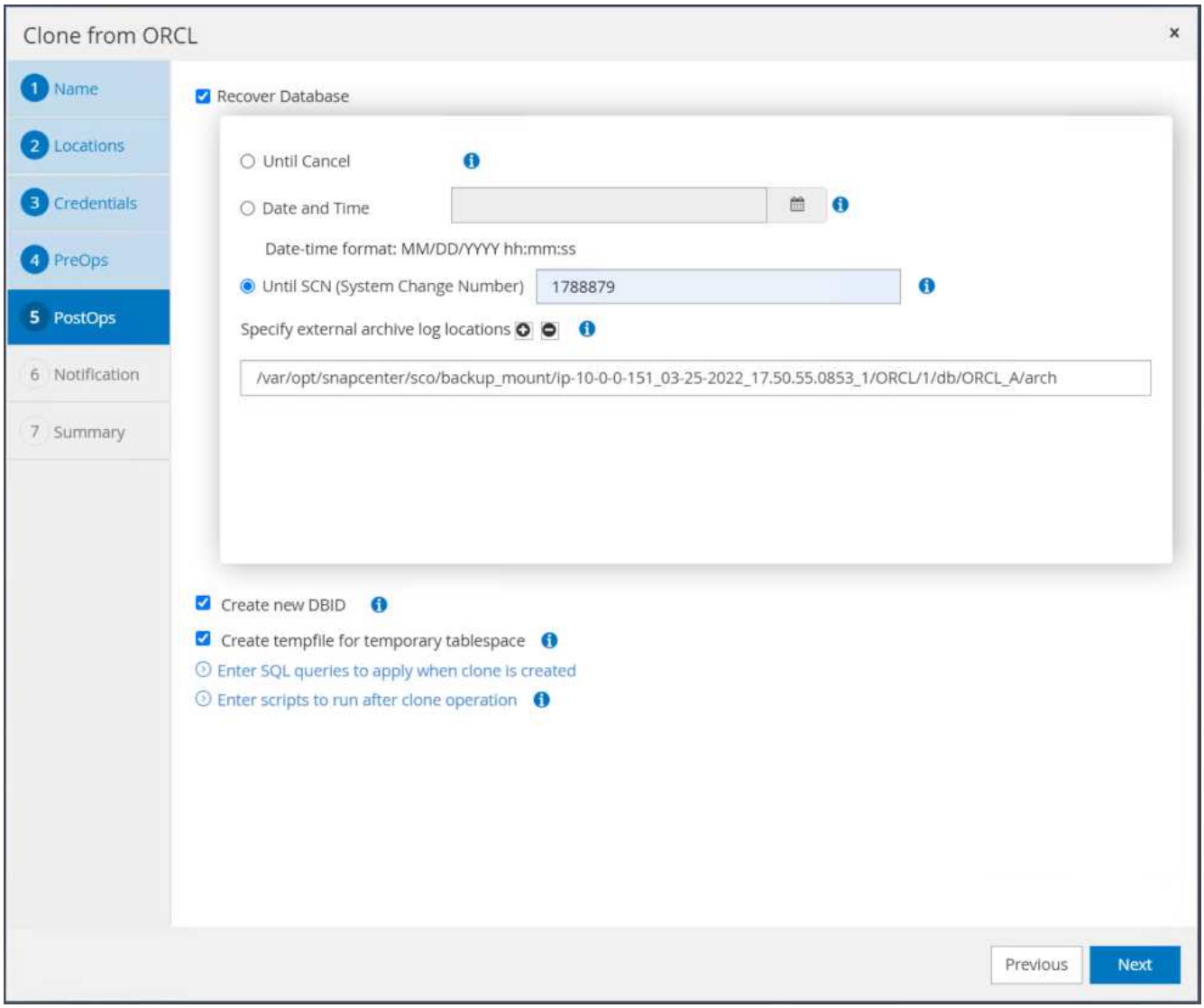
Sie auf „Weiter“.



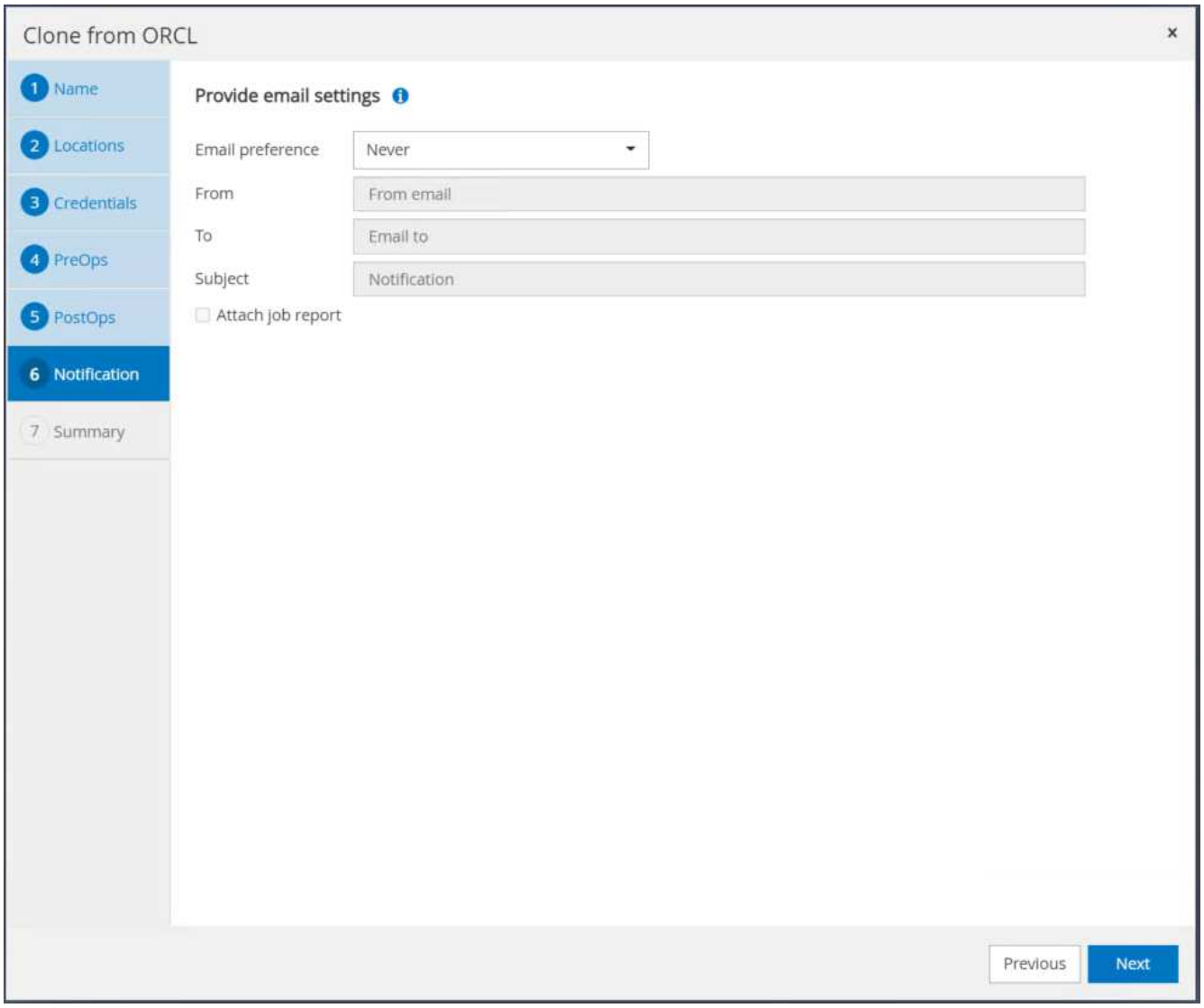
7. Ändern Sie Ihre Oracle-Home-Einstellungen so, dass sie mit den für den Ziel-Oracle-Server-Host konfigurierten Einstellungen übereinstimmen, und klicken Sie auf „Weiter“.



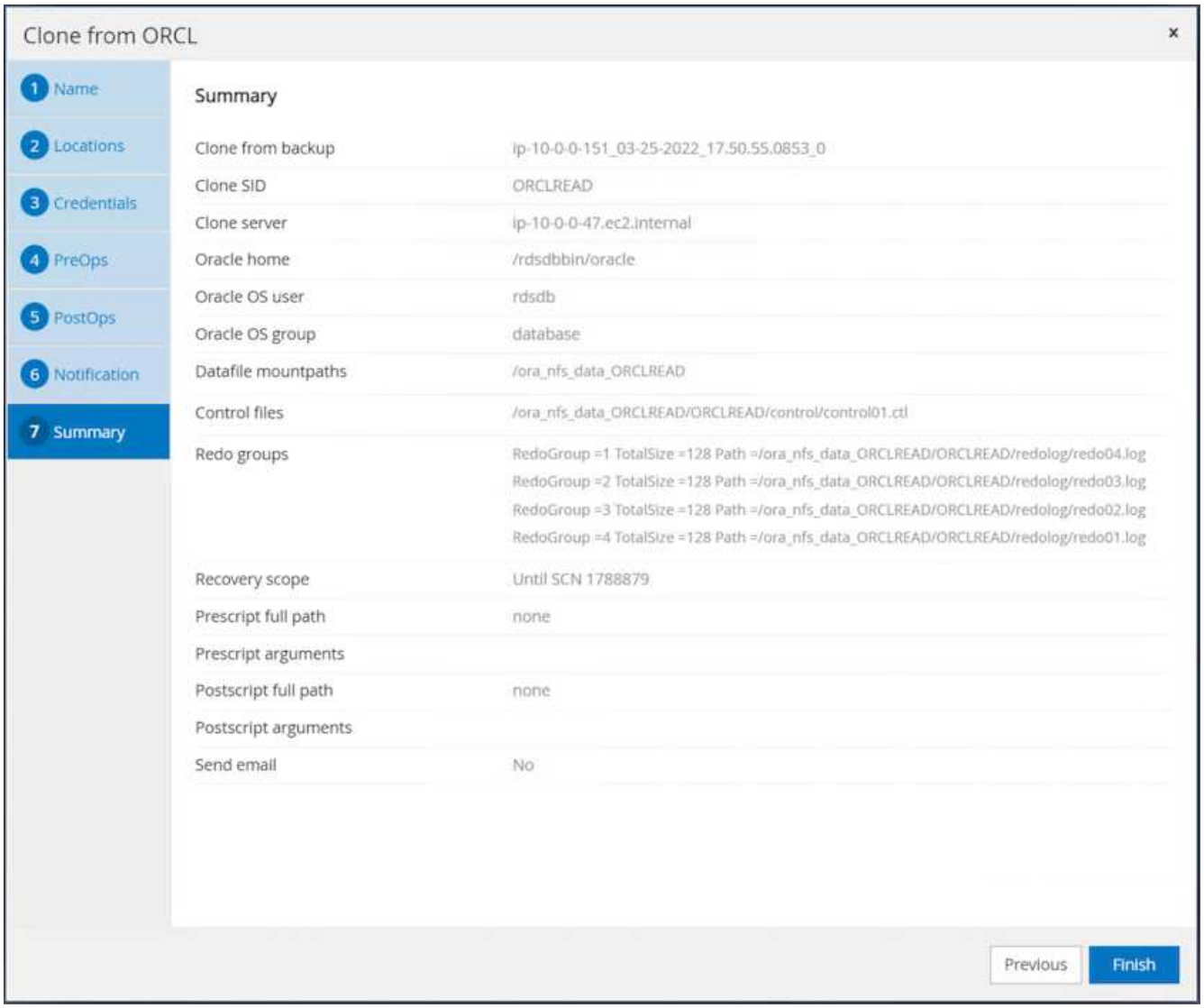
8. Geben Sie einen Wiederherstellungspunkt entweder mithilfe der Zeit oder der SCN und des bereitgestellten Archivprotokollpfads an.



9. Senden Sie bei Bedarf die SMTP-E-Mail-Einstellungen.

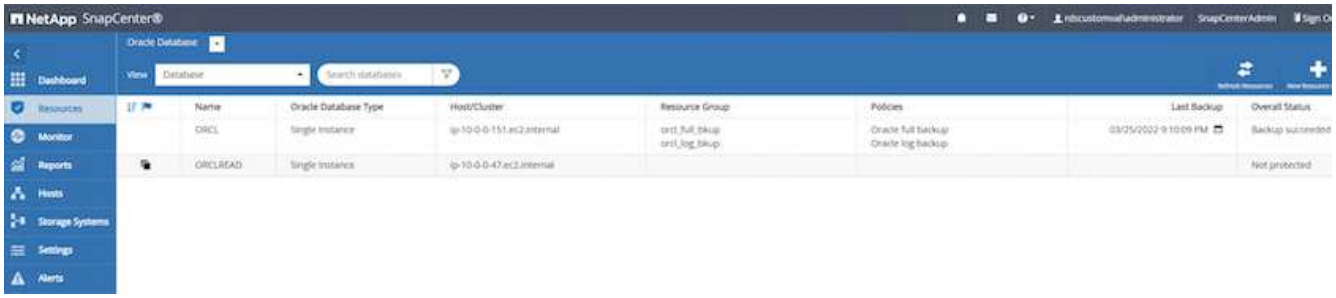


10. Klonen Sie die Auftragszusammenfassung und klicken Sie auf „Fertig“, um den Klonauftrag zu starten.



11. Validieren Sie den Replikatklon, indem Sie das Klonauftragsprotokoll überprüfen.

Die geklonte Datenbank wird sofort in SnapCenter registriert.



12. Deaktivieren Sie den Oracle-Archivprotokollmodus. Melden Sie sich als Oracle-Benutzer bei der EC2-Instanz an und führen Sie den folgenden Befehl aus:

```
sqlplus / as sysdba
```

```
shutdown immediate;
```

```
startup mount;
```

```
alter database noarchivelog;
```

```
alter database open;
```

Anstelle primärer Oracle-Sicherungskopien kann mit denselben Verfahren auch ein Klon aus replizierten sekundären Sicherungskopien auf dem Ziel-FSx-Cluster erstellt werden.

HA-Failover zum Standby und erneute Synchronisierung

Der Oracle HA-Standby-Cluster bietet hohe Verfügbarkeit im Falle eines Ausfalls am primären Standort, entweder in der Rechenschicht oder in der Speicherschicht. Ein wesentlicher Vorteil der Lösung besteht darin, dass ein Benutzer die Infrastruktur jederzeit und in beliebiger Häufigkeit testen und validieren kann. Das Failover kann vom Benutzer simuliert oder durch einen tatsächlichen Fehler ausgelöst werden. Die Failover-Prozesse sind identisch und können für eine schnelle Anwendungswiederherstellung automatisiert werden.

Sehen Sie sich die folgende Liste der Failover-Verfahren an:

1. Führen Sie für ein simuliertes Failover eine Protokoll-Snapshot-Sicherung aus, um die neuesten Transaktionen auf die Standby-Site zu übertragen, wie im AbschnittErstellen eines Archivprotokoll-Snapshots . Bei einem Failover, das durch einen tatsächlichen Fehler ausgelöst wird, werden die letzten wiederherstellbaren Daten mit der letzten erfolgreichen geplanten Sicherung des Protokollvolumes auf den Standby-Standort repliziert.
2. Unterbrechen Sie den SnapMirror zwischen dem primären und dem Standby-FSx-Cluster.
3. Mounten Sie die replizierten Standby-Datenbank-Volumes auf dem Standby-Host der EC2-Instance.
4. Verknüpfen Sie die Oracle-Binärdatei erneut, wenn die replizierte Oracle-Binärdatei für die Oracle-Wiederherstellung verwendet wird.
5. Stellen Sie die Standby-Oracle-Datenbank auf das letzte verfügbare Archivprotokoll wieder her.
6. Öffnen Sie die Standby-Oracle-Datenbank für den Anwendungs- und Benutzerzugriff.
7. Bei einem tatsächlichen Ausfall des primären Standorts übernimmt die Standby-Oracle-Datenbank nun die Rolle des neuen primären Standorts und Datenbankvolumes können verwendet werden, um den ausgefallenen primären Standort mit der umgekehrten SnapMirror -Methode als neuen Standby-Standort neu aufzubauen.

8. Um einen Ausfall des primären Standorts zu Test- oder Validierungszwecken zu simulieren, fahren Sie die Standby-Oracle-Datenbank nach Abschluss der Testübungen herunter. Hängen Sie dann die Standby-Datenbankvolumes vom Standby-EC2-Instance-Host aus und synchronisieren Sie die Replikation vom primären Standort erneut mit dem Standby-Standort.

Diese Verfahren können mit dem NetApp Automation Toolkit durchgeführt werden, das auf der öffentlichen NetApp GitHub-Site zum Download bereitsteht.

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

Lesen Sie die README-Anweisung sorgfältig durch, bevor Sie mit der Einrichtung und dem Failover-Test beginnen.

Datenbankmigration von On-Premise in die Public Cloud

Die Datenbankmigration ist in jedem Fall ein anspruchsvolles Unterfangen. Die Migration einer Oracle-Datenbank von einem lokalen Standort in die Cloud ist keine Ausnahme.

In den folgenden Abschnitten werden die wichtigsten Faktoren beschrieben, die bei der Migration von Oracle-Datenbanken in die öffentliche AWS-Cloud mit der AWS EC2-Rechen- und FSx-Speicherplattform zu berücksichtigen sind.

ONTAP -Speicher ist vor Ort verfügbar

Wenn sich die lokale Oracle-Datenbank auf einem ONTAP -Speicherarray befindet, ist es einfacher, die Replikation für die Datenbankmigration mithilfe der in den AWS FSx ONTAP -Speicher integrierten NetApp SnapMirror -Technologie einzurichten. Der Migrationsprozess kann mithilfe der NetApp BlueXP Konsole orchestriert werden.

1. Erstellen Sie eine EC2-Ziel-Compute-Instanz, die der lokalen Instanz entspricht.
2. Stellen Sie passende, gleich große Datenbankvolumes über die FSx-Konsole bereit.
3. Mounten Sie die FSx-Datenbankvolumes in der EC2-Instance.
4. Richten Sie die SnapMirror Replikation zwischen den lokalen Datenbankvolumes und den Ziel-FSx-Datenbankvolumes ein. Die erste Synchronisierung zum Verschieben der primären Quelldaten kann einige Zeit in Anspruch nehmen, alle nachfolgenden inkrementellen Aktualisierungen erfolgen jedoch viel schneller.
5. Beenden Sie zum Zeitpunkt der Umschaltung die primäre Anwendung, um alle Transaktionen zu stoppen. Führen Sie über die Oracle sqlplus CLI-Schnittstelle einen Oracle-Online-Protokollwechsel aus und lassen Sie SnapMirror Sync das letzte archivierte Protokoll auf das Zielvolume übertragen.
6. Teilen Sie die gespiegelten Volumes auf, führen Sie die Oracle-Wiederherstellung auf dem Ziel aus und starten Sie die Datenbank für den Dienst.
7. Richten Sie Anwendungen auf die Oracle-Datenbank in der Cloud aus.

Das folgende Video zeigt, wie Sie eine Oracle-Datenbank mithilfe der NetApp BlueXP -Konsole und der SnapMirror Replikation von vor Ort zu AWS FSx/EC2 migrieren.

Migrieren Sie lokale Oracle-Datenbanken zu AWS

ONTAP -Speicher ist vor Ort nicht verfügbar

Wenn die lokale Oracle-Datenbank auf einem anderen Speicher eines Drittanbieters als ONTAP gehostet wird, basiert die Datenbankmigration auf der Wiederherstellung einer Sicherungskopie der Oracle-Datenbank. Sie müssen das Archivprotokoll abspielen, um es vor dem Umschalten auf den neuesten Stand zu bringen.

AWS S3 kann als Staging-Speicherbereich für die Datenbankverschiebung und -migration verwendet werden. Beachten Sie die folgenden allgemeinen Schritte für diese Methode:

1. Stellen Sie eine neue, passende EC2-Instanz bereit, die mit der lokalen Instanz vergleichbar ist.
2. Stellen Sie gleiche Datenbankvolumes aus dem FSx-Speicher bereit und mounten Sie die Volumes in die EC2-Instance.
3. Erstellen Sie eine Oracle-Sicherungskopie auf Festplattenebene.
4. Verschieben Sie die Sicherungskopie in den AWS S3-Speicher.
5. Erstellen Sie die Oracle-Steuerdatei neu und stellen Sie die Datenbank wieder her, indem Sie Daten und das Archivprotokoll aus dem S3-Speicher abrufen.
6. Synchronisieren Sie die Ziel-Oracle-Datenbank mit der lokalen Quelldatenbank.
7. Fahren Sie beim Umschalten die Anwendung und die Oracle-Quelldatenbank herunter. Kopieren Sie die letzten Archivprotokolle und wenden Sie sie auf die Ziel-Oracle-Datenbank an, um sie auf den neuesten Stand zu bringen.
8. Starten Sie die Zieldatenbank für den Benutzerzugriff.
9. Leiten Sie die Anwendung zur Zieldatenbank um, um die Umstellung abzuschließen.

Migrieren Sie lokale Oracle-Datenbanken mithilfe der PDB-Verlagerung mit maximaler Verfügbarkeit zu AWS FSx/EC2

Dieser Migrationsansatz eignet sich am besten für Oracle-Datenbanken, die bereits im PDB/CDB-Multitenant-Modell bereitgestellt werden und für die vor Ort kein ONTAP Speicher verfügbar ist. Die PDB-Verlagerungsmethode nutzt die Oracle PDB-Hot-Clone-Technologie, um PDBs zwischen einer Quell-CDB und einer Ziel-CDB zu verschieben und dabei die Dienstunterbrechung zu minimieren.

Erstellen Sie zunächst eine CDB in AWS FSx/EC2 mit ausreichend Speicherplatz, um PDBs zu hosten, die von vor Ort migriert werden sollen. Mehrere lokale PDBs können einzeln verschoben werden.

1. Wenn die lokale Datenbank in einer einzelnen Instanz und nicht im mehrinstanzenfähigen PDB/CDB-Modell bereitgestellt wird, befolgen Sie die Anweisungen in"Konvertieren einer einzelnen Instanz einer Nicht-CDB in eine PDB in einer Multitenant-CDB" um die einzelne Instanz in eine Multitenant-PDB/CDB zu konvertieren. Folgen Sie dann dem nächsten Schritt, um das konvertierte PDB in AWS FSx/EC2 in CDB zu migrieren.
2. Wenn die lokale Datenbank bereits im Multitenant-PDB/CDB-Modell bereitgestellt ist, folgen Sie den Anweisungen in"Migrieren Sie lokale Oracle-Datenbanken mit PDB-Verlagerung in die Cloud" um die Migration durchzuführen.

Das folgende Video zeigt, wie eine Oracle-Datenbank (PDB) mithilfe der PDB-Relocation mit maximaler Verfügbarkeit nach FSx/EC2 migriert werden kann.

"Migrieren Sie lokale Oracle PDBs mit maximaler Verfügbarkeit zu AWS CDB"

Obwohl die Anweisungen in Schritt 1 und 2 im Kontext der öffentlichen Azure-Cloud dargestellt werden, sind die Verfahren ohne Änderungen auf die AWS-Cloud anwendbar.

Das NetApp Solutions Automation-Team bietet ein Migrations-Toolkit, das die Migration von Oracle-Datenbanken von lokalen Standorten in die AWS-Cloud erleichtern kann. Verwenden Sie den folgenden Befehl, um das Oracle-Datenbankmigrations-Toolkit für die PDB-Verschiebung herunterzuladen.

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