



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 | 1 |
| WP-7357: Einführung in Best Practices zur Oracle-Datenbankbereitstellung auf EC2 und FSx | 1 |
| Lösungsarchitektur | 2 |
| Zu berücksichtigende Faktoren bei der Bereitstellung einer Oracle-Datenbank | 3 |
| VM-Leistung | 3 |
| Speicherlayout und -einstellungen | 3 |
| NFS-Konfiguration | 4 |
| Hochverfügbarkeit | 5 |
| Schrittweise Oracle-Bereitstellungsverfahren auf AWS EC2 und FSx | 5 |
| Stellen Sie eine EC2-Linux-Instance für Oracle über die EC2-Konsole bereit | 5 |
| Bereitstellen von FSx ONTAP -Dateisystemen für Oracle-Datenbankspeicher | 11 |
| Installieren und konfigurieren Sie Oracle auf einer EC2-Instance mit FSx-Datenbankvolumes | 21 |
| Einrichten von SnapMirror zwischen primärem und Standby-FSx-HA-Cluster | 23 |
| SnapCenter -Bereitstellung | 26 |
| EC2- und FSx-Oracle-Datenbankverwaltung | 31 |
| Einen Schnappschuss machen | 32 |
| Wiederherstellen zu einem bestimmten Zeitpunkt | 35 |
| Erstellen eines Datenbankklons | 45 |
| HA-Failover zum Standby und erneute Synchronisierung | 54 |
| Datenbankmigration von On-Premise in die Public Cloud | 55 |
| ONTAP -Speicher ist vor Ort verfügbar | 55 |
| ONTAP -Speicher ist vor Ort nicht verfügbar | 56 |
| Migrieren Sie lokale Oracle-Datenbanken mithilfe der PDB-Verlagerung mit maximaler Verfügbarkeit zu AWS FSx/EC2 | 56 |

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 anwendungsorientiert 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:

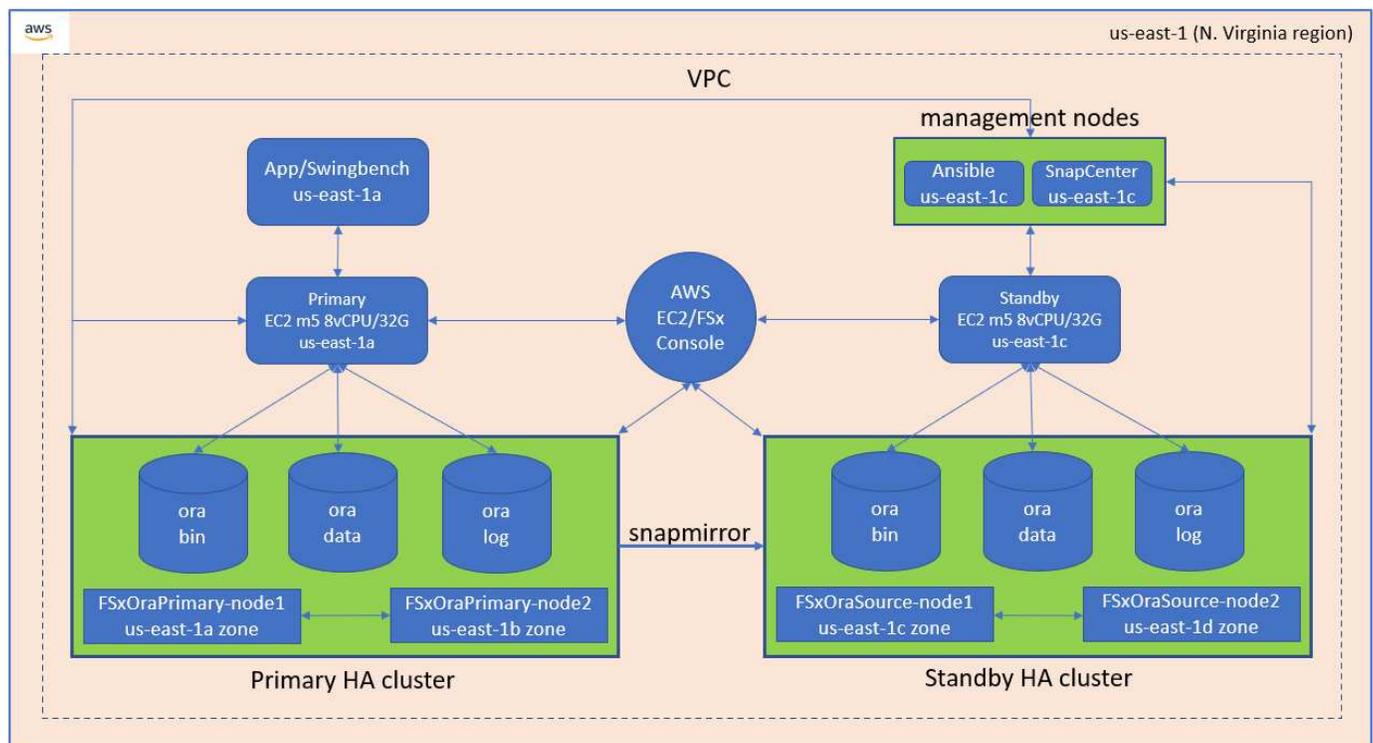
["Modernisieren Sie Ihre Oracle-Datenbank mit Hybrid Cloud in AWS und FSx ONTAP, Teil 1 – Anwendungsfall und Lösungsarchitektur"](#)

Lösungsarchitektur

Das folgende Architekturdiagramm veranschaulicht eine hochverfügbare Oracle-Datenbankbereitstellung auf einer AWS EC2-Instanz 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-Instanz 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-Instanz mit FSx-Speicher beschrieben.

VM-Leistung

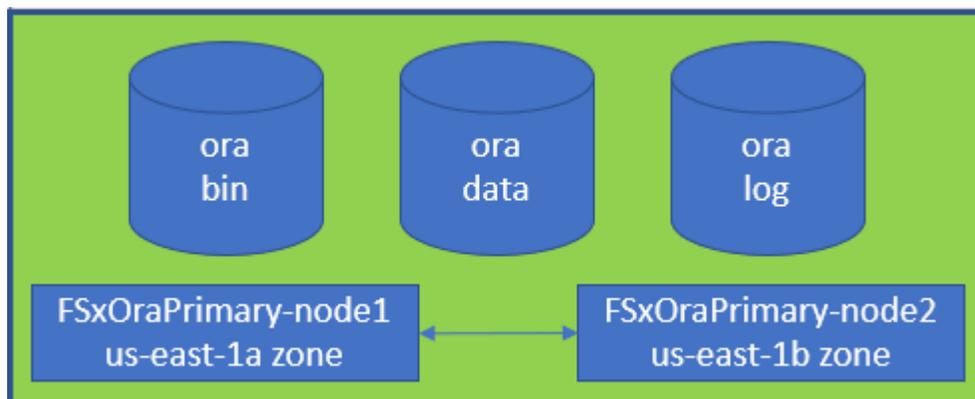
Die Auswahl der richtigen VM-Größe ist für die optimale Leistung einer relationalen Datenbank in einer öffentlichen Cloud wichtig. Für eine bessere Leistung empfiehlt NetApp die Verwendung einer Instanz der EC2 M5-Serie für die Oracle-Bereitstellung, die für Datenbank-Workloads optimiert ist. Derselbe 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.

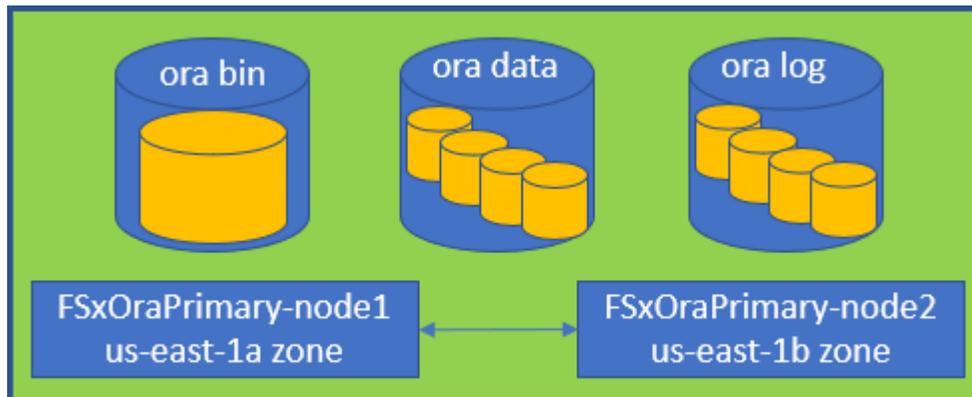
Speicherlayout und -einstellungen

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 |
|--|---|
| <ul style="list-style-type: none">• Control files• Data files• Redo logs | <code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536</code> |
| <ul style="list-style-type: none">• ORACLE_HOME• ORACLE_BASE | <code>rw,bg,hard,vers=3,proto=tcp,timeo=600,rsize=65536,wsiz=65536</code> |



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:

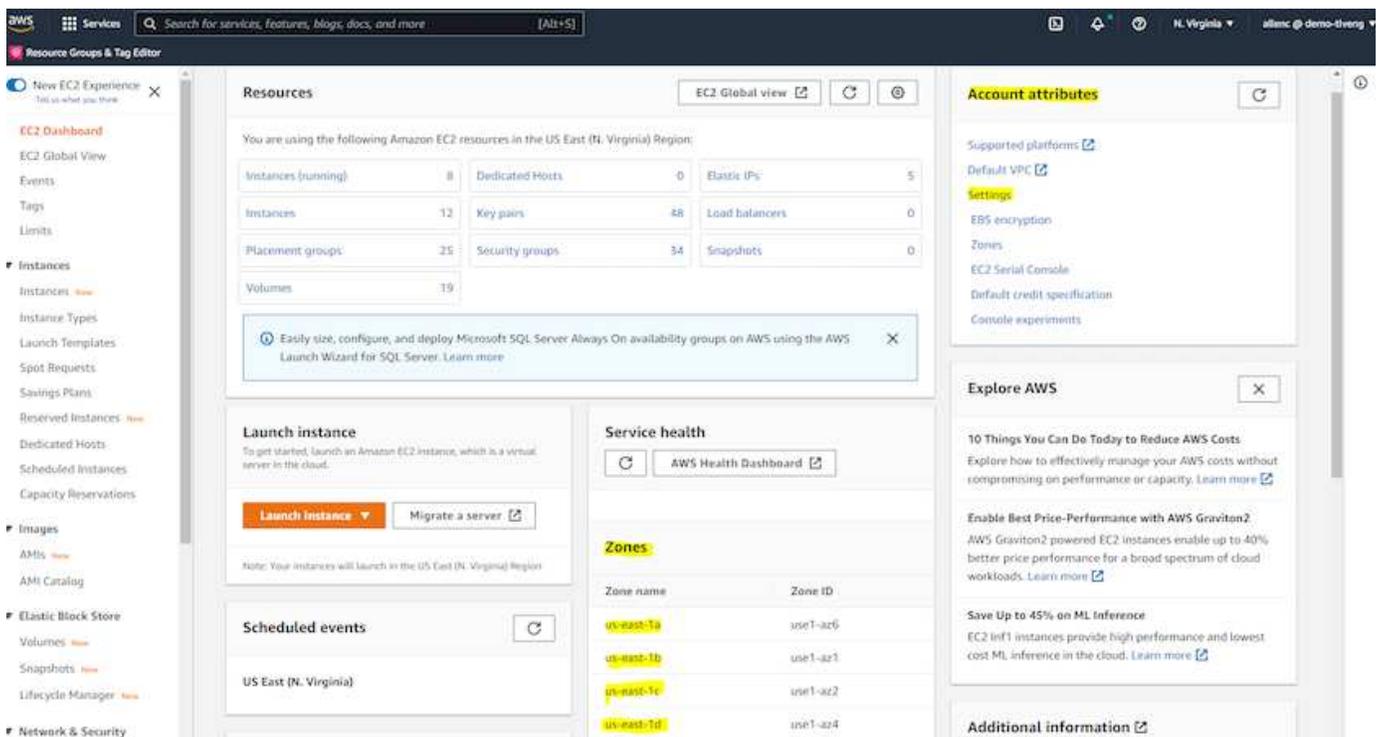
- ["Einrichten zur Verwendung von Amazon EC2"](#)

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

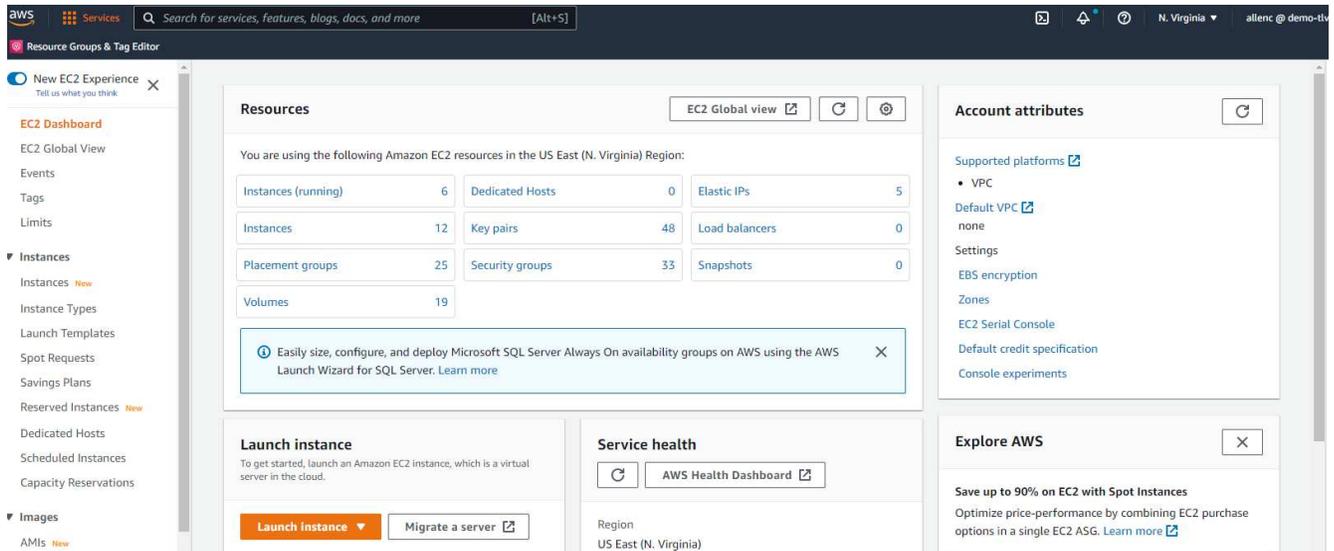
Sehen Sie sich das Tutorial an ["Erste Schritte mit Amazon EC2 Linux-Instances"](#) für schrittweise Bereitstellungsverfahren und Best Practices.

Schlüsselthemen:

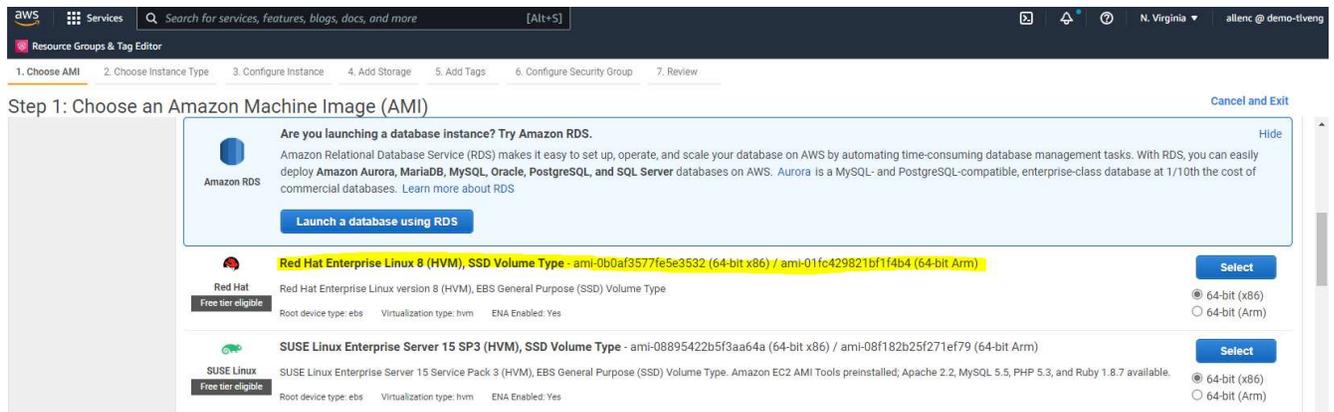
- Überblick.
- Voraussetzungen.
- Schritt 1: Starten Sie eine Instanz.
- Schritt 2: Stellen Sie eine Verbindung zu Ihrer Instanz her.
- Schritt 3: Bereinigen Sie Ihre Instanz.

Die folgenden Screenshots zeigen die Bereitstellung einer Linux-Instanz 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“.

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia allenc @ demo-tlven

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

| | | | | | | | | |
|-------------------------------------|----|-------------|----|-----|----------|-----|------------------|-----|
| <input type="checkbox"/> | m4 | m4.16xlarge | 64 | 256 | EBS only | Yes | 25 Gigabit | Yes |
| <input type="checkbox"/> | m5 | m5.large | 2 | 8 | EBS only | Yes | Up to 10 Gigabit | Yes |
| <input type="checkbox"/> | m5 | m5.xlarge | 4 | 16 | EBS only | Yes | Up to 10 Gigabit | Yes |
| <input checked="" type="checkbox"/> | m5 | m5.2xlarge | 8 | 32 | EBS only | Yes | Up to 10 Gigabit | Yes |
| <input type="checkbox"/> | m5 | m5.4xlarge | 16 | 64 | EBS only | Yes | Up to 10 Gigabit | Yes |
| <input type="checkbox"/> | m5 | m5.8xlarge | 32 | 128 | EBS only | Yes | 10 Gigabit | Yes |
| <input type="checkbox"/> | m5 | m5.12xlarge | 48 | 192 | EBS only | Yes | 10 Gigabit | Yes |
| <input type="checkbox"/> | m5 | m5.16xlarge | 64 | 256 | EBS only | Yes | 20 Gigabit | Yes |
| <input type="checkbox"/> | m5 | m5.24xlarge | 96 | 384 | EBS only | Yes | 25 Gigabit | Yes |
| <input type="checkbox"/> | 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“.

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia allenc @ demo-tlven

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

No default VPC found. Select another VPC, or create a new default VPC.

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances Launch into Auto Scaling Group

Purchasing option Request Spot instances

Network Create new VPC
No default VPC found. Create a new default VPC.

Subnet Create new subnet
250 IP Addresses available

Auto-assign Public IP

Hostname type

DNS Hostname Enable IP name IPv4 (A record) DNS requests
 Enable resource-based IPv4 (A record) DNS requests
 Enable resource-based IPv6 (AAAA record) DNS requests

Placement group Add instance to placement group

Capacity Reservation

Domain join directory Create new directory

IAM role Create new IAM role

Cancel Previous **Review and Launch** Next: Add Storage

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.

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia allenc @ demo-tveng

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

| Volume Type | Device | Snapshot | Size (GiB) | Volume Type | IOPS | Throughput (MB/s) | Delete on Termination | Encryption |
|-------------|-----------|------------------------|------------|---------------------------|------------|-------------------|-------------------------------------|---------------|
| Root | /dev/sda1 | snap-03a3ad00558b4d17c | 50 | General Purpose SSD (gp2) | 150 / 3000 | N/A | <input checked="" type="checkbox"/> | Not Encrypted |

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Shared file systems

You currently don't have any file systems on this instance. Select "Add file system" button below to add a file system.

[Add file system](#)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

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

aws Services Search for services, features, blogs, docs, and more [Alt+S] N. Virginia allenc @ demo-tveng

Resource Groups & Tag Editor

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

| Key (128 characters maximum) | Value (256 characters maximum) | Instances | Volumes | Network Interfaces |
|--|--------------------------------|-----------|---------|--------------------|
| <p><i>This resource currently has no tags</i></p> <p>Choose the Add tag button or click to add a Name tag.</p> <p>Make sure your IAM policy includes permissions to create tags.</p> | | | | |

[Add Tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

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.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

| Security Group ID | Name | Description | Actions |
|--|--|--|-----------------------------|
| <input type="checkbox"/> sg-0d746a0908bb97c48 | AviOcm03112021OCCM1635951256631-OCCMSecurityGroup-B3QFHUJRUUVW | NetApp OCCM Instance External Security Group | Copy to new |
| <input type="checkbox"/> sg-07b0625cd544aee16 | AVIOCCM0311OCCM1635943382952-OCCMSecurityGroup-1L8D4QX2SC945 | NetApp OCCM Instance External Security Group | Copy to new |
| <input type="checkbox"/> sg-0618122caef6c50e9 | AviOcm1103OCCM1635944222133-OCCMSecurityGroup-DX5PHX6CKVKC | NetApp OCCM Instance External Security Group | Copy to new |
| <input type="checkbox"/> sg-0d53ea8c78987e660 | AviOcm1209OCCM1631452667252-OCCMSecurityGroup-TSKVZ1Q4SH48 | NetApp OCCM Instance External Security Group | Copy to new |
| <input type="checkbox"/> sg-0aed9f8836b48c52d | AviOcmFSxOCCM1638110371156-OCCMSecurityGroup-N0ENZJW3TVYB | NetApp OCCM Instance External Security Group | Copy to new |
| <input type="checkbox"/> sg-083a6ea5cba912375 | connector1OCCM1631455604110-OCCMSecurityGroup-1790QV45PH3Z2W | NetApp OCCM Instance External Security Group | Copy to new |
| <input checked="" type="checkbox"/> sg-08148ca915189ac87 | default | default VPC security group | Copy to new |
| <input type="checkbox"/> sg-07f6c527620e3bb22 | fsx02OCCM1633339531669-OCCMSecurityGroup-1XZYC5WM15NP7 | NetApp OCCM Instance External Security Group | Copy to new |
| <input type="checkbox"/> sg-0f359d2ba38db749f | SG-Version10-0CEc6MEs-NetAppExternalSecurityGroup-N8B50KGTk8U | ONTAP Cloud firewall rules for management and data interface | Copy to new |

Inbound rules for sg-08148ca915189ac87 (Selected security groups: sg-08148ca915189ac87)

| Type | Protocol | Port Range | Source | Description |
|-------------|----------|------------|--------------------------------|-------------|
| All traffic | All | All | 192.168.1.0/24 | |
| All traffic | All | All | sg-08148ca915189ac87 (default) | |

[Cancel](#) [Previous](#) [Review and Launch](#)

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.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details [Edit AMI](#)

Red Hat Enterprise Linux 8 (HVM), SSD Volume Type - ami-0b0af3577fe5e3532
 Free tier eligible Red Hat Enterprise Linux version 8 (HVM), EBS General Purpose (SSD) Volume Type
 Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

| Instance Type | ECUs | vCPUs | Memory (GiB) | Instance Storage (GB) | EBS-Optimized Available | Network Performance |
|---------------|------|-------|--------------|-----------------------|-------------------------|---------------------|
| m5.2xlarge | - | 8 | 32 | EBS only | Yes | Up to 10 Gigabit |

Security Groups [Edit security groups](#)

| Security Group ID | Name | Description |
|----------------------|---------|----------------------------|
| sg-08148ca915189ac87 | default | default VPC security group |

All selected security groups inbound rules

| Type | Protocol | Port Range | Source | Description |
|-------------|----------|------------|--------------------------------|-------------|
| All traffic | All | All | 192.168.1.0/24 | |
| All traffic | All | All | sg-08148ca915189ac87 (default) | |

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

[Cancel](#) [Previous](#) [Launch](#)

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance. Amazon EC2 supports ED25519 and RSA key pair types.

Note: The selected key pair will be added to the set of keys authorized for this instance. [Learn more about removing existing key pairs from a public AMI.](#)

Choose an existing key pair ▼

Select a key pair

accesststkey | RSA ▼

I acknowledge that I have access to the corresponding private key file, and that without this file, I won't be able to log into my instance.

Cancel
Launch Instances

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-dblv2.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-Datenbankspeichervolumen, einschließlich der Oracle-Binär-, Daten- und Protokollvolumen. Die FSx-Speicher-NFS-Volumen können entweder über die AWS FSx-Konsole oder über die Oracle-Installation bereitgestellt werden. Außerdem gibt es eine Konfigurationsautomatisierung, die die Volumens gemäß der Konfiguration des Benutzers in einer Automatisierungsparameterdatei zuweist.

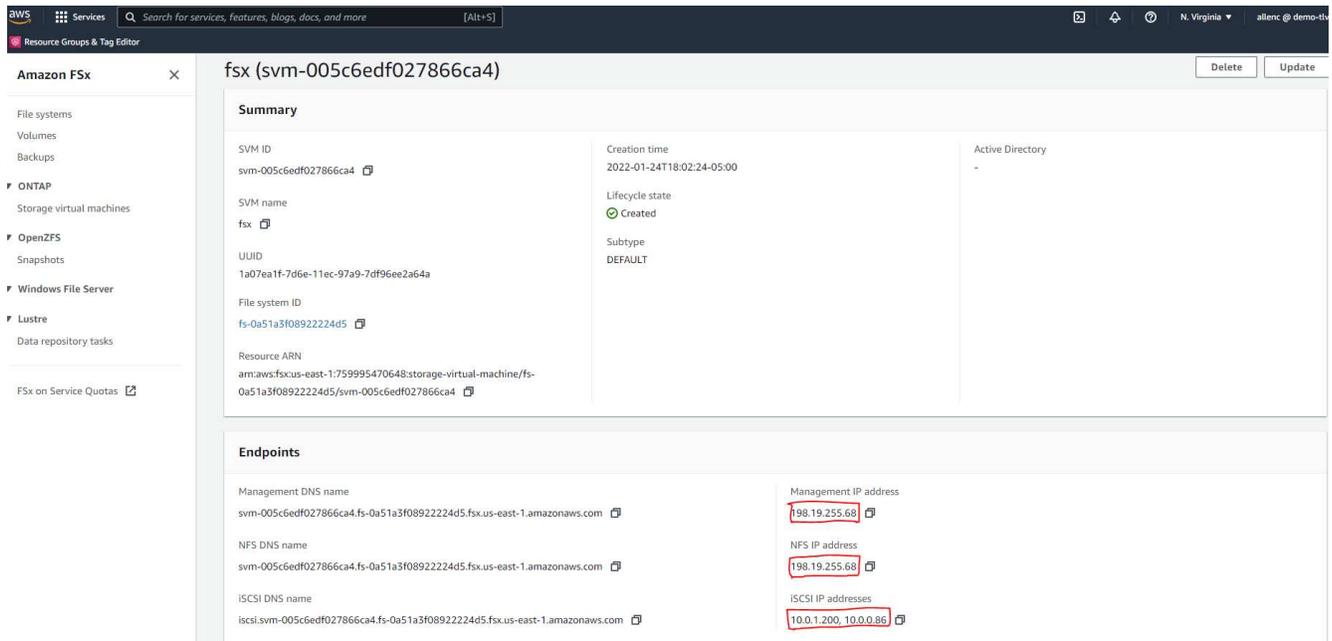
Erstellen von FSx ONTAP Dateisystemen

Auf diese Dokumentation verwiesen "[Verwalten von FSx ONTAP Dateisystemen](#)" zum Erstellen von FSx ONTAP Dateisystemen.

Wichtige Überlegungen:

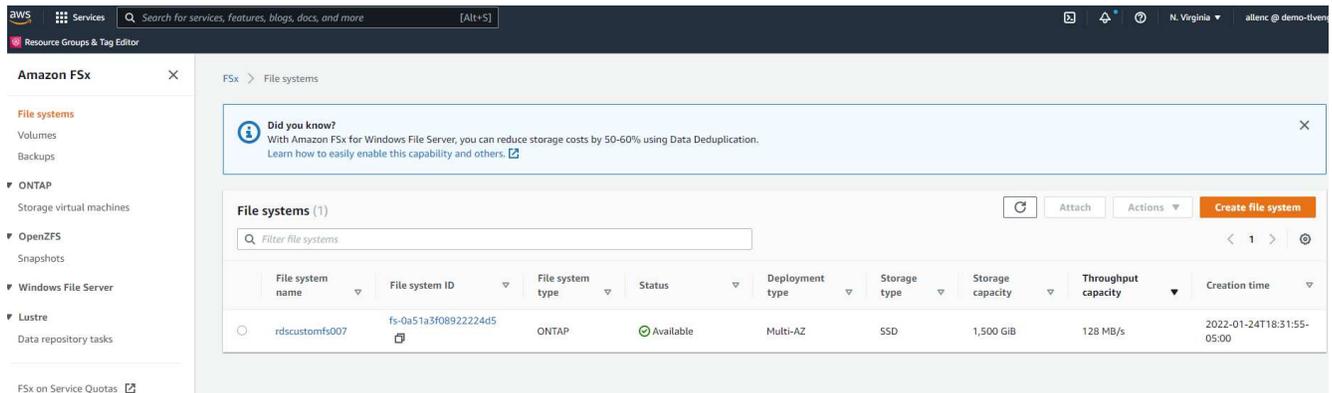
- SSD-Speicherkapazität. Mindestens 1024 GiB, maximal 192 TiB.
- Bereitgestellte SSD-IOPS. Basierend auf den Workload-Anforderungen maximal 80.000 SSD-IOPS pro Dateisystem.

- 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.

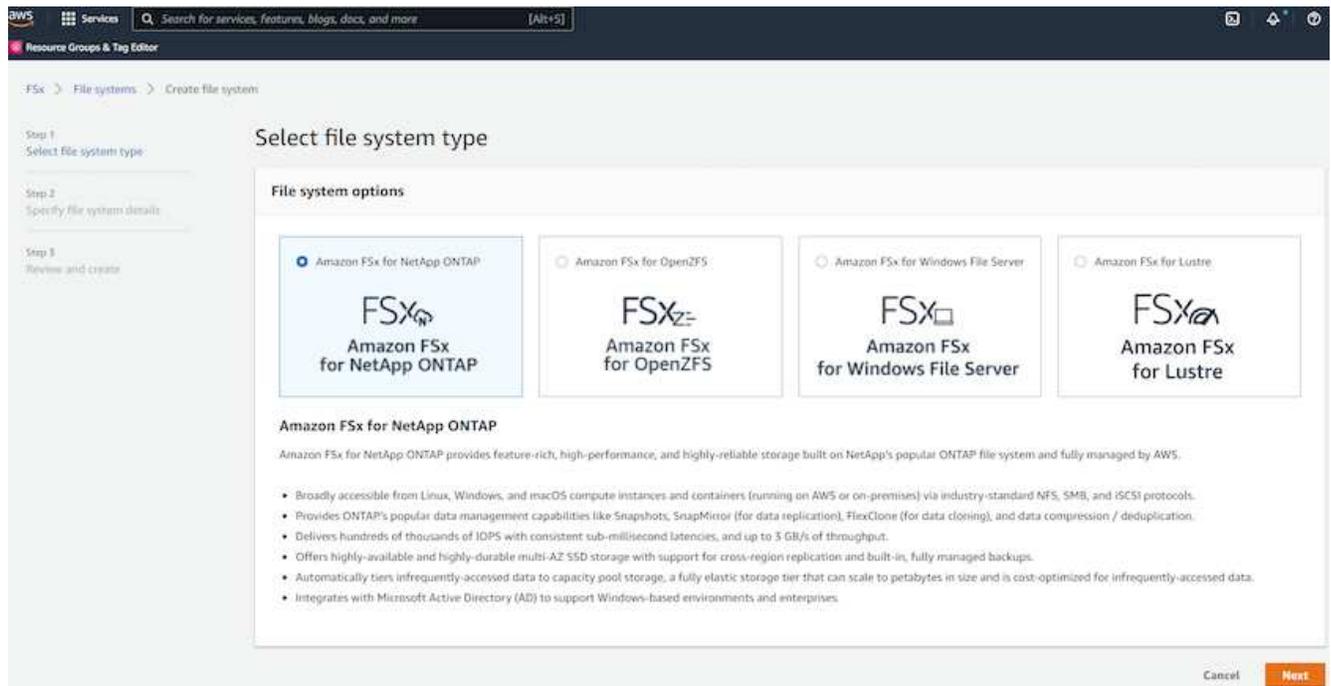


Sehen Sie sich die folgenden Schritt-für-Schritt-Anleitungen zum Einrichten eines primären oder Standby-HA-FSx-Clusters an.

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.

File system details

File system name - optional [Info](#)

Maximum of 256 Unicode letters, whitespace, and numbers, plus + - = . _ : /

Deployment type [Info](#)

Multi-AZ

Single-AZ

SSD storage capacity [Info](#)

Minimum 1024 GiB; Maximum 192 TiB.

Provisioned SSD IOPS

Amazon FSx provides 3 IOPS per GiB of storage capacity. You can also provision additional SSD IOPS as needed.

Automatic (3 IOPS per GiB of SSD storage)

User-provisioned

Maximum 80,000 IOPS

Throughput capacity [Info](#)

The sustained speed at which the file server hosting your file system can serve data. The file server can also burst to higher speeds for periods of time.

Recommended throughput capacity

128 MB/s

Specify throughput capacity

Throughput capacity

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.

Network & security

Virtual Private Cloud (VPC) [Info](#)

Specify the VPC from which your file system is accessible.

vpc-0474064fc537e5182 ▼

VPC Security Groups [Info](#)

Specify VPC Security Groups to associate with your file system's network interfaces.

Choose VPC security group(s) ▼

sg-08148ca915189ac87 (default) ✕

Preferred subnet [Info](#)

Specify the preferred subnet for your file system.

subnet-08c952541f4ab282d (us-east-1a) ▼

Standby subnet

subnet-0a84d6eeeb0f4e5c0 (us-east-1b) ▼

VPC route tables

Specify the VPC route tables associated with your file system.

VPC's default route table

Select one or more VPC route tables

Endpoint IP address range

Specify the IP address range in which the endpoints to access your file system will be created

No preference

Select an IP address range

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

Security & encryption

Encryption key [Info](#)
 AWS Key Management Service (KMS) encryption key that protects your file system data at rest.

aws/fsx (default) ▼

| Description | Account | KMS key ID |
|--|--------------|--------------------------------------|
| Default master key that protects my FSx resources when no other key is defined | 759995470648 | 5b31feff-6759-4306-a852-9c99a743982a |

File system administrative password
 Password for this file system's "fsxadmin" user, which you can use to access the ONTAP CLI or REST API.

Don't specify a password
 Specify a password

Password

Confirm password

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

Default storage virtual machine configuration

Storage virtual machine name

SVM administrative password
 Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.

Don't specify a password
 Specify a password

Password

Confirm password

Active Directory
 Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.

Do not join an Active Directory
 Join an Active Directory

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

Default volume configuration

Volume name

Maximum of 203 alphanumeric characters, plus _.

Junction path

The location within your file system where your volume will be mounted.

Volume size

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.

Cancel Back Next

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

aws Services Search for services, features, blogs, docs, and more [Alt+S]

Resource Groups & Tag Editor

Step 1 Select file system type

Step 2 Specify file system details

Step 3 Review and create

Create file system

Summary
Verify the following attributes before proceeding

| Attribute | Value | Editable after creation |
|-------------------------------|---|-------------------------|
| File system type | Amazon FSx for NetApp ONTAP | |
| File system name | aws_ora_prod | ✓ |
| Deployment type | Multi-AZ | |
| Storage type | SSD | |
| SSD storage capacity | 1,024 GiB | ✓ |
| Minimum SSD IOPS | 40000 IOPS | ✓ |
| Throughput capacity | 512 MB/s | ✓ |
| Virtual Private Cloud (VPC) | vpc-0474064fc537e5182 | |
| VPC Security Groups | sg-08148ca915189ac87 | ✓ |
| Preferred subnet | subnet-08c952541f4ab282d | |
| Standby subnet | subnet-0a84d6eeeb0f4e5c0 | |
| VPC route tables | VPC's default route table | |
| Endpoint IP address range | No preference | |
| KMS key ID | arn:aws:kms:us-east-1:759995470648:key/5b31feff-6759-4306-a852-9c99a743982a | |
| Daily automatic backup window | No preference | ✓ |
| Automatic backup | 7 day(s) | ✓ |

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

Create volume
✕

File system

ONTAP | fs-0a51a3f08922224d5 | rdscustomfs007 ▼

Storage virtual machine

svm-005c6edf027866ca4 | fsx ▼

Volume name

db1_log

Maximum of 203 alphanumeric characters, plus _.

Junction path

/db1_log

The location within your file system where your volume will be mounted.

Volume size

256000

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

Automatisierungsskript 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 Befehlsyntax 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-Instanz 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 `accesststkey.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-Instanz 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 accesststkey.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-addr 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
Vserver      Peer      Peer      Peer Cluster      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-Volumen 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
```

- 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 lgroup 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

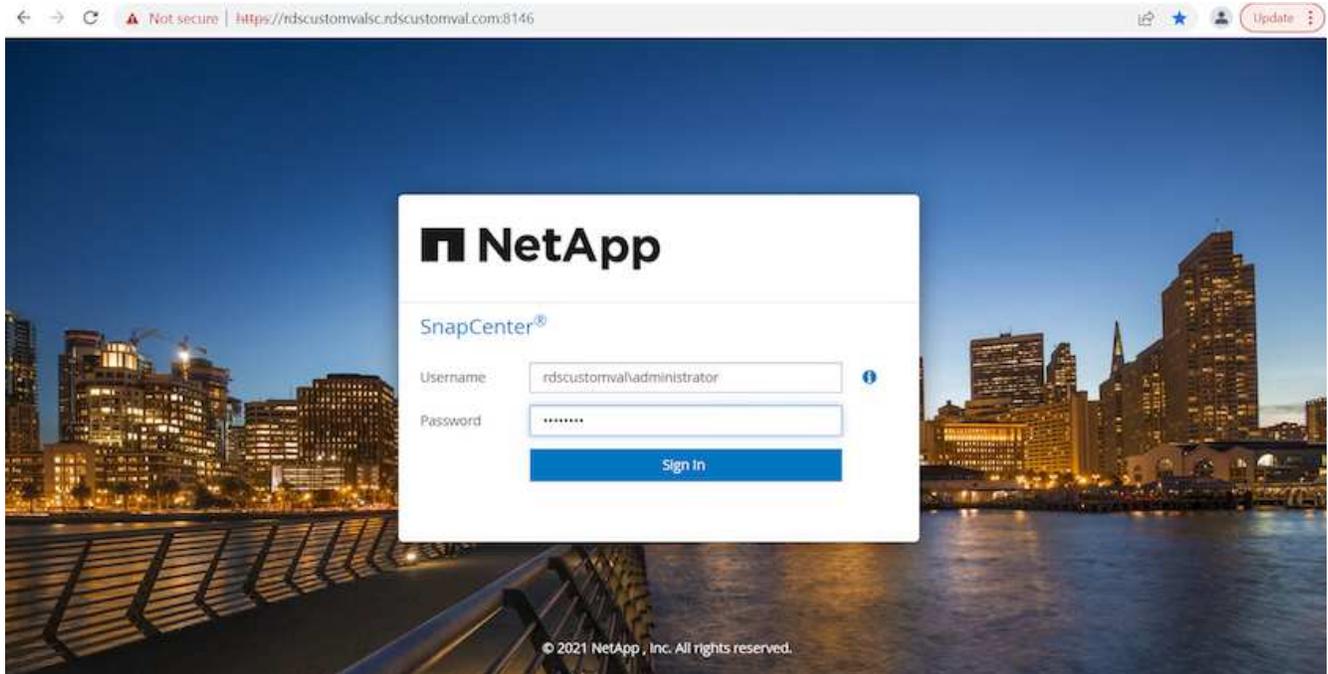
SnapCenter -Installation

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

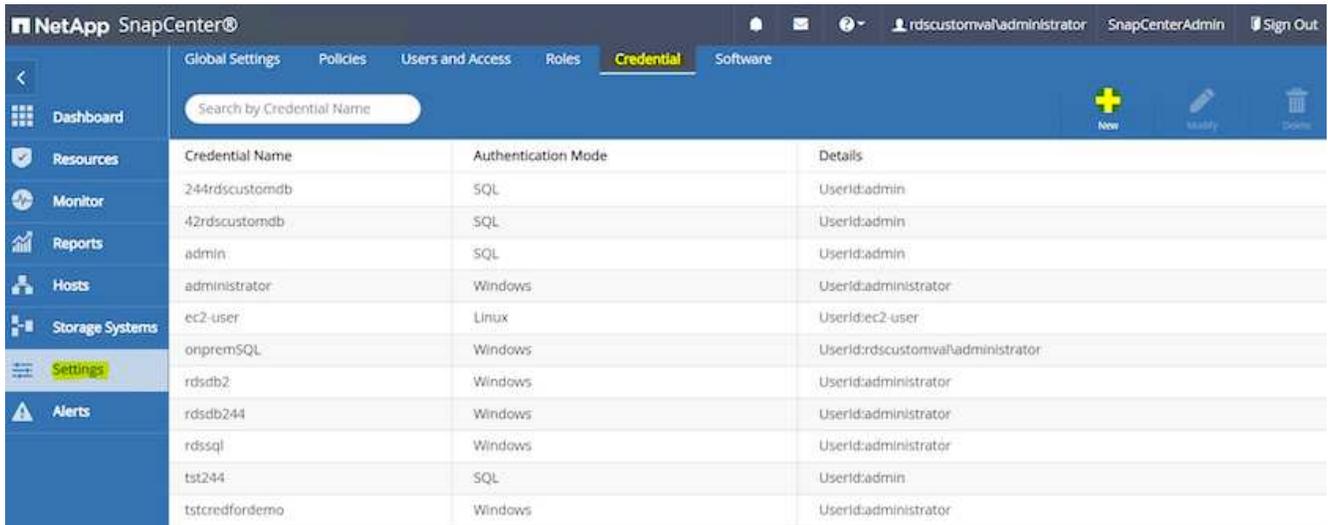
Version von SnapCenter befindet sich im Beta-Test und könnte in Kürze verfügbar sein. Erkundigen Sie sich bei Bedarf bei Ihrem NetApp -Vertreter nach der Verfügbarkeit.

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.

Credential ✕

Credential Name

Authentication Mode ▼

Username ⓘ

Password

Use sudo privileges ⓘ

- 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
```

- 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
```

- 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.

NetApp SnapCenter®

Managed Hosts | Disks | Shares | Initiator Groups | iSCSI Session

Search by Name

| Name | Type | System | Plug-in | Version | Overall Status |
|----------------------------------|---------|-------------|--|---------|----------------|
| RDSAMAZ-VJ0DQK0 | Windows | Stand-alone | Microsoft Windows Server, Microsoft SQL Server | 4.5 | Host down |
| rdscustommssql1.rdscustomval.com | Windows | Stand-alone | Microsoft Windows Server, Microsoft SQL Server | 4.5 | Running |

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

Add Host

Host Type: Linux

Host Name: 10.0.0.151

Credentials: ec2-user

Select Plug-ins to Install: SnapCenter Plug-ins Package 4.5 P2 for Linux

- Oracle Database
- SAP HANA

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

Submit | Cancel

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

More Options ✕

Port i

Installation Path i

Skip preinstall checks

Custom Plug-ins _____

Choose a File

No plug-ins found.

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

Confirm Fingerprint ✕

Authenticity of the host cannot be determined i

| Host name | Fingerprint | Valid |
|----------------------------|--|-------|
| ip-10-0-0-151.ec2.internal | ssh-rsa 2048 97:6F:3C:7D:38:42:F6:54:B7:AF:E3:61:61:BA:2E:6F | |

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

| Managed Hosts | | | | | | | |
|---|-------|-------------|-----------------------|---------|--|--|--|
| Search by Name <input style="width: 80px;" type="text"/> | | | | | | | |
| | | + | - | ↻ | ⋮ | | |
| | | Add | Remove | Refresh | More | | |
| Name | Type | System | Plug-in | Version | Overall Status | | |
| <input type="checkbox"/> ip-10-0-0-151.ec2.internal | Linux | Stand-alone | UNIX, Oracle Database | 4.5 | ● Running | | |

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 Sicherungsrichtlinie [Konfigurieren 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.

| Name | Oracle Database Type | Host/Cluster | Resource Group | Policies | Last Backup | Overall Status |
|------|----------------------|--------------------------|-------------------------------------|---|-----------------------|------------------|
| ORCL | Single Instance | ip-10-0-151.ec2.internal | orcl_full_backup orcl_log_backup | Oracle full backup Oracle log backup | 03/24/2022 8:40:08 PM | Backup succeeded |

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-Umgebungsconfiguration 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.

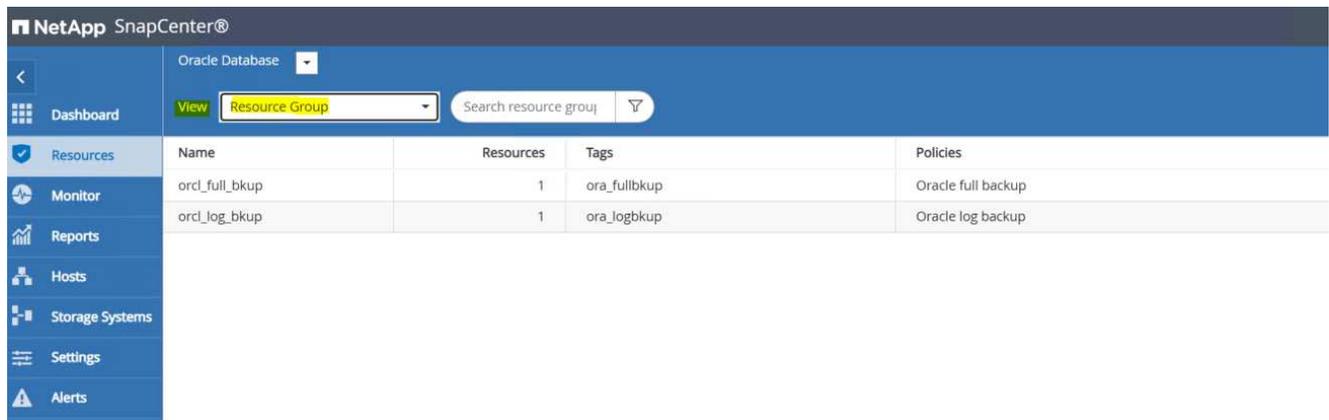
Einen Schnappschuss machen

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.

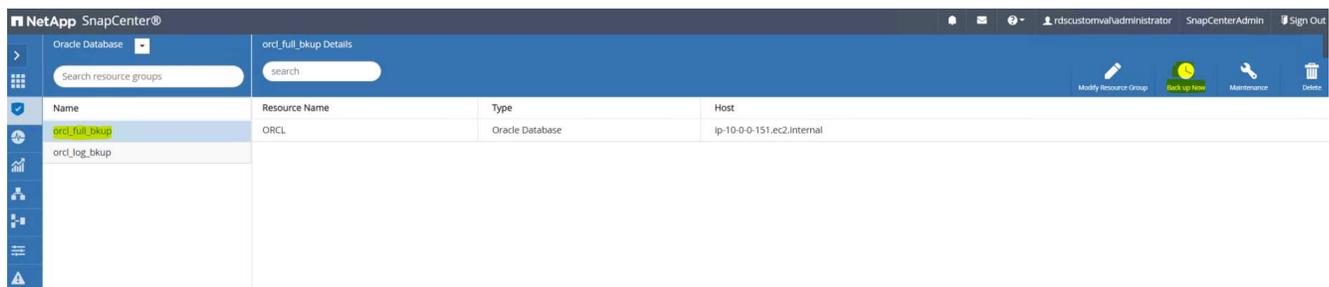
Erstellen eines vollständigen Datenbank-Snapshots

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

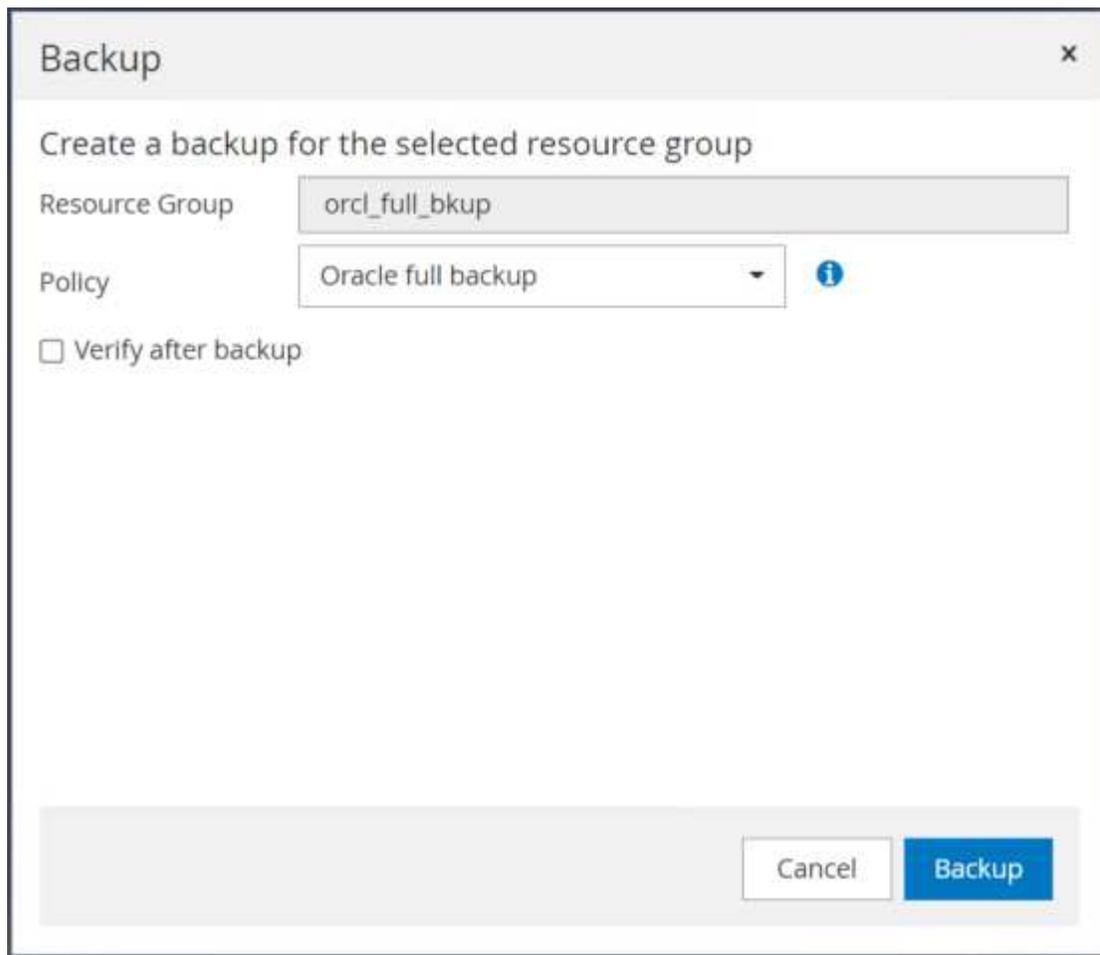
1. Melden Sie sich bei der SnapCenter -Benutzeroberfläche an und klicken Sie im Menü auf der linken Seite auf „Ressourcen“. Wechseln Sie im Dropdown-Menü „Ansicht“ zur Ansicht „Ressourcengruppe“.



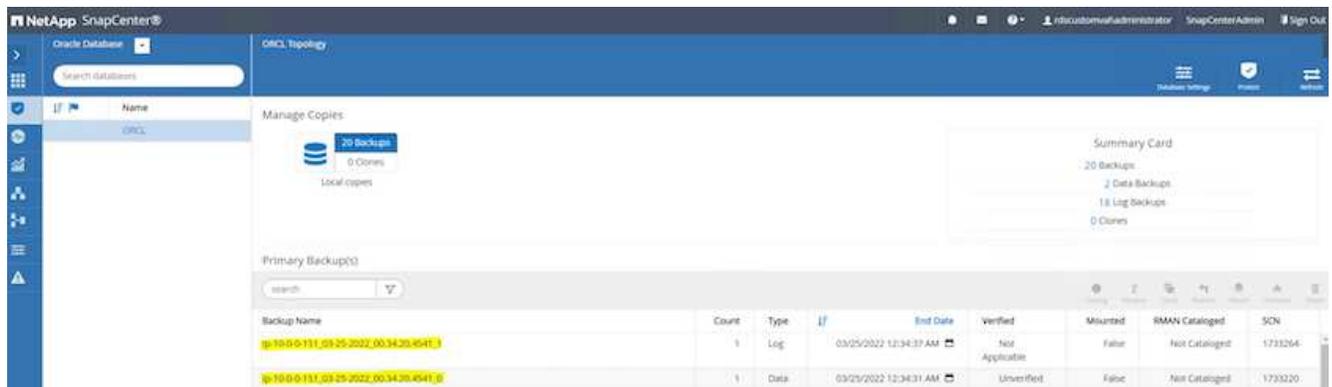
2. Klicken Sie auf den Namen der vollständigen Sicherungsressource und dann auf das Symbol „Jetzt sichern“, um eine Ad-hoc-Sicherung zu starten.



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



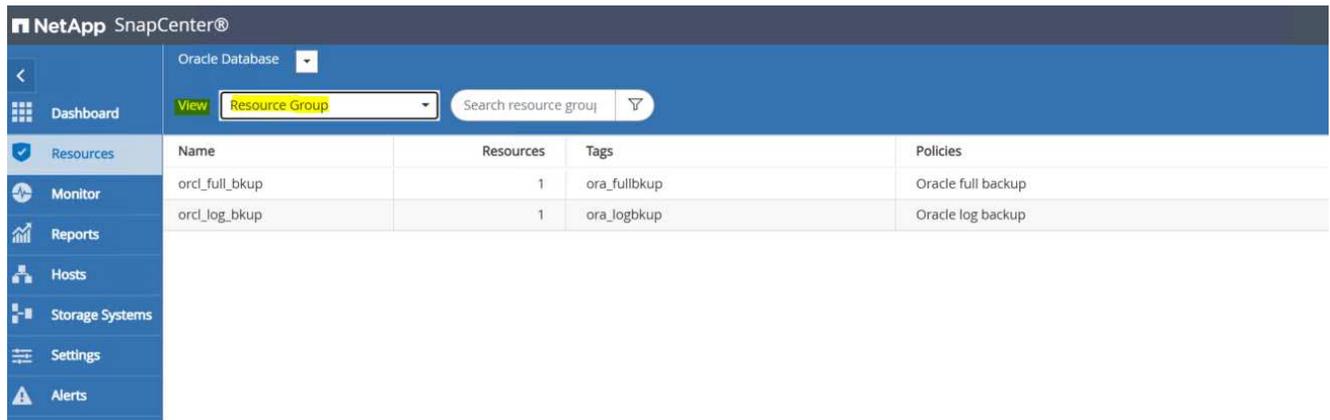
Öffnen Sie in der Ressourcenansicht der Datenbank die Seite „Verwaltete Sicherungskopien“ der Datenbank, um zu überprüfen, ob die einmalige Sicherung erfolgreich abgeschlossen wurde. Bei einer vollständigen Datenbanksicherung werden zwei Snapshots erstellt: einer für das Datenvolumen und einer für das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



Erstellen eines Archivprotokoll-Snapshots

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

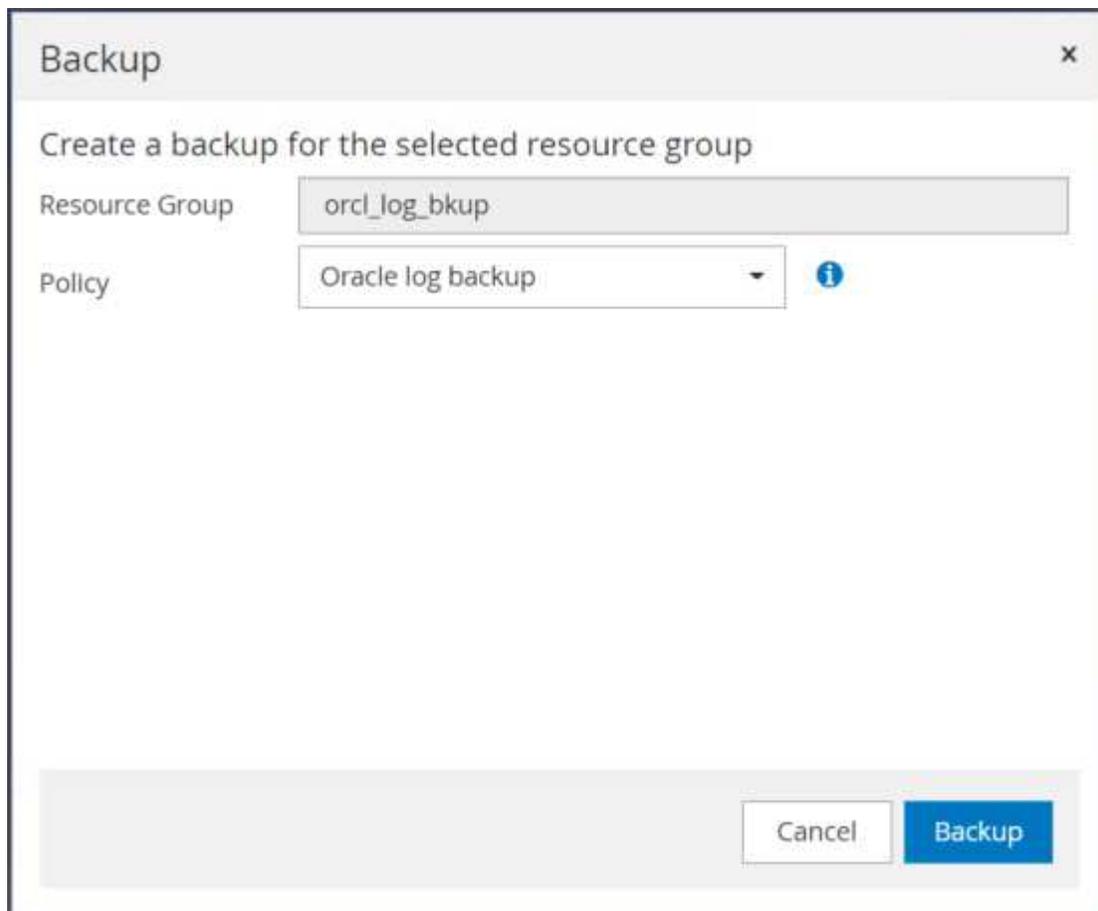
1. Melden Sie sich bei der SnapCenter -Benutzeroberfläche an und klicken Sie in der linken Menüleiste auf die Registerkarte „Ressourcen“. Wechseln Sie im Dropdown-Menü „Ansicht“ zur Ansicht „Ressourcengruppe“.



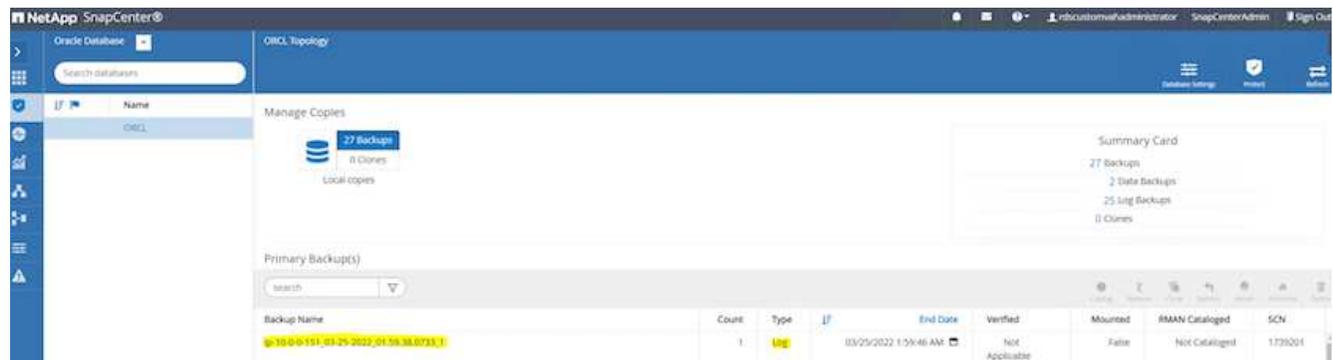
2. Klicken Sie auf den Ressourcennamen der Protokollsicherung und dann auf das Symbol „Jetzt sichern“, um eine Ad-hoc-Sicherung für Archivprotokolle zu starten.



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 Protokollvolumen 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.

NetApp SnapCenter®

Oracle Database | ORCL Topology

Search databases

Manage Copies

78 Backups
0 Clones
Local copies

Summary Card

78 Backups
5 Data Backups
73 Log Backups
0 Clones

Primary Backup(s)

| Backup Name | Count | Type | IF | End Date | Verified | Mounted | RMAN Cataloged | SCN |
|--|-------|------|----|------------------------|----------------|---------|----------------|---------|
| ip-10-0-0-151_03-25-2022_12:40:01.1098_1 | 1 | Log | | 03/25/2022 12:40:09 PM | Not Applicable | False | Not Cataloged | 1784293 |
| ip-10-0-0-151_03-25-2022_12:25:01.0080_1 | 1 | Log | | 03/25/2022 12:25:09 PM | Not Applicable | False | Not Cataloged | 1783383 |
| ip-10-0-0-151_03-25-2022_12:10:01.1097_1 | 1 | Log | | 03/25/2022 12:10:09 PM | Not Applicable | False | Not Cataloged | 1782417 |
| ip-10-0-0-151_03-25-2022_11:55:01.0500_1 | 1 | Log | | 03/25/2022 11:55:09 AM | Not Applicable | False | Not Cataloged | 1781160 |
| ip-10-0-0-151_03-25-2022_11:40:01.0323_1 | 1 | Log | | 03/25/2022 11:40:09 AM | Not Applicable | False | Not Cataloged | 1780268 |
| ip-10-0-0-151_03-25-2022_11:25:01.0430_1 | 1 | Log | | 03/25/2022 11:25:09 AM | Not Applicable | False | Not Cataloged | 1779368 |
| ip-10-0-0-151_03-25-2022_11:15:01.1503_1 | 1 | Log | | 03/25/2022 11:15:17 AM | Not Applicable | False | Not Cataloged | 1778546 |
| ip-10-0-0-151_03-25-2022_11:15:01.1503_0 | 1 | Data | | 03/25/2022 11:15:11 AM | Unverified | False | Not Cataloged | 1778504 |
| ip-10-0-0-151_03-25-2022_11:10:01.1834_1 | 1 | Log | | 03/25/2022 11:10:09 AM | Not Applicable | False | Not Cataloged | 1778184 |

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

Manage Copies

78 Backups
0 Clones
Local copies

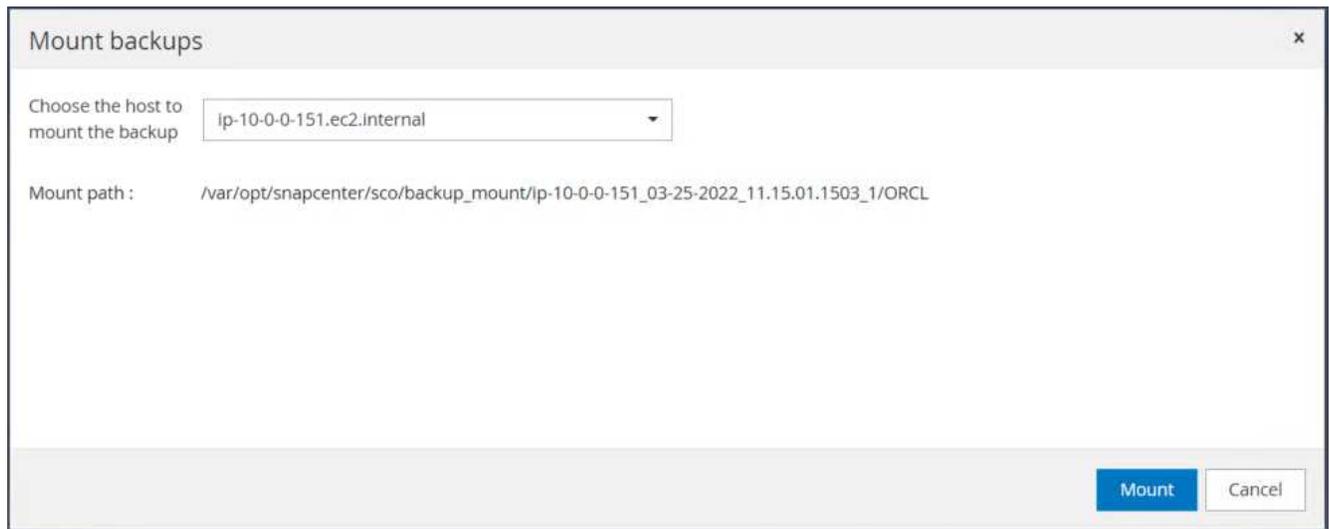
Summary Card

78 Backups
5 Data Backups
73 Log Backups
0 Clones

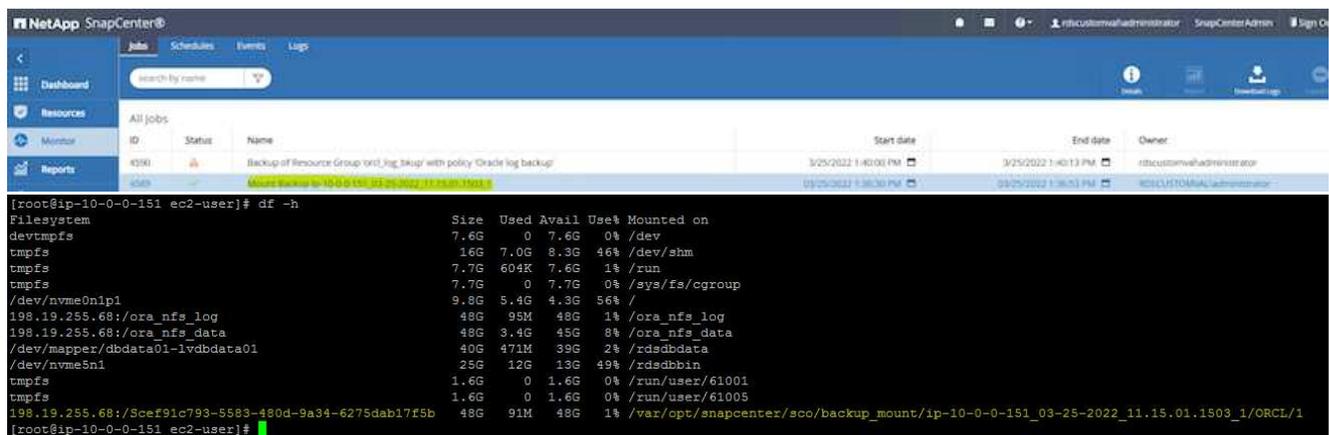
Primary Backup(s)

| Backup Name | Count | Type | IF | End Date | Verified | Mounted | RMAN Cataloged | SCN |
|--|-------|------|----|------------------------|----------------|---------|----------------|---------|
| ip-10-0-0-151_03-25-2022_12:40:01.1098_1 | 1 | Log | | 03/25/2022 12:40:09 PM | Not Applicable | False | Not Cataloged | 1784293 |
| ip-10-0-0-151_03-25-2022_12:25:01.0080_1 | 1 | Log | | 03/25/2022 12:25:09 PM | Not Applicable | False | Not Cataloged | 1783383 |
| ip-10-0-0-151_03-25-2022_12:10:01.1097_1 | 1 | Log | | 03/25/2022 12:10:09 PM | Not Applicable | False | Not Cataloged | 1782417 |
| ip-10-0-0-151_03-25-2022_11:55:01.0500_1 | 1 | Log | | 03/25/2022 11:55:09 AM | Not Applicable | False | Not Cataloged | 1781160 |
| ip-10-0-0-151_03-25-2022_11:40:01.0323_1 | 1 | Log | | 03/25/2022 11:40:09 AM | Not Applicable | False | Not Cataloged | 1780268 |
| ip-10-0-0-151_03-25-2022_11:25:01.0430_1 | 1 | Log | | 03/25/2022 11:25:09 AM | Not Applicable | False | Not Cataloged | 1779368 |
| ip-10-0-0-151_03-25-2022_11:15:01.1503_1 | 1 | Log | | 03/25/2022 11:15:17 AM | Not Applicable | False | Not Cataloged | 1778546 |
| ip-10-0-0-151_03-25-2022_11:15:01.1503_0 | 1 | Data | | 03/25/2022 11:15:11 AM | Unverified | False | Not Cataloged | 1778504 |
| ip-10-0-0-151_03-25-2022_11:10:01.1834_1 | 1 | Log | | 03/25/2022 11:10:09 AM | Not Applicable | False | Not Cataloged | 1778184 |

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



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



- Kopieren Sie die Archivprotokolle vom bereitgestellten Protokollträger 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/
```

- 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.

Manage Copies

80 Backups

0 Clones

Local copies

Summary Card

80 Backups

5 Data Backups

75 Log Backups

0 Clones

Primary Backup(s)

| Backup Name | Count | Type | End Date | Verified | Mounted | RMAN Cataloged | SCN |
|--|-------|------|------------------------|----------------|---------|----------------|---------|
| lp-10-0-0-151_03-25-2022_12.10.01.1097_1 | 1 | Log | 03/25/2022 12:10:09 PM | Not Applicable | False | Not Cataloged | 1782417 |
| lp-10-0-0-151_03-25-2022_11.55.01.0500_1 | 1 | Log | 03/25/2022 11:55:09 AM | Not Applicable | False | Not Cataloged | 1781160 |
| lp-10-0-0-151_03-25-2022_11.40.01.0323_1 | 1 | Log | 03/25/2022 11:40:09 AM | Not Applicable | False | Not Cataloged | 1780268 |
| lp-10-0-0-151_03-25-2022_11.25.01.0430_1 | 1 | Log | 03/25/2022 11:25:09 AM | Not Applicable | False | Not Cataloged | 1779368 |
| lp-10-0-0-151_03-25-2022_11.15.01.1503_1 | 1 | Log | 03/25/2022 11:15:17 AM | Not Applicable | True | Not Cataloged | 1778546 |
| lp-10-0-0-151_03-25-2022_11.15.01.1503_0 | 1 | Data | 03/25/2022 11:15:11 AM | Unverified | False | Not Cataloged | 1778504 |
| lp-10-0-0-151_03-25-2022_11.10.01.1834_1 | 1 | Log | 03/25/2022 11:10:09 AM | Not Applicable | False | Not Cataloged | 1778184 |

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

Restore ORCL

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Restore Scope

All Datafiles

Tablespaces

Control files

Database State

Change database state if needed for restore and recovery

Restore Mode

Force in place restore

If this check box is not selected and if any of the in place restore criteria is not met, restore will be performed using the connect and copy method. The connect and copy restore method might take time based on the files being restored.

Previous **Next**

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.

The screenshot shows the 'Restore ORCL' wizard window. On the left is a navigation pane with steps: 1 Restore Scope, 2 Recovery Scope (selected), 3 PreOps, 4 PostOps, 5 Notification, and 6 Summary. The main area is titled 'Choose Recovery Scope' and contains the following options:

- All Logs
- Until SCN (System Change Number)
- Date and Time
- No recovery

Below these options, there is a text input field for 'SCN' containing the value '1778546'. Underneath is a section 'Specify external archive log files locations' with a large empty text area and icons for adding, removing, and help. At the bottom right are 'Previous' and 'Next' buttons.

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

Restore ORCL x

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Specify optional scripts to run before performing a restore job ⓘ

Prescript full path

Arguments

Script timeout

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

Restore ORCL x

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Specify optional scripts to run after performing a restore job ⓘ

Postscript full path

Arguments

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

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

Restore ORCL x

- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification**
- 6 Summary

Provide email settings ?

Email preference:

From:

To:

Subject:

Attach job report

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

Restore ORCL
✕

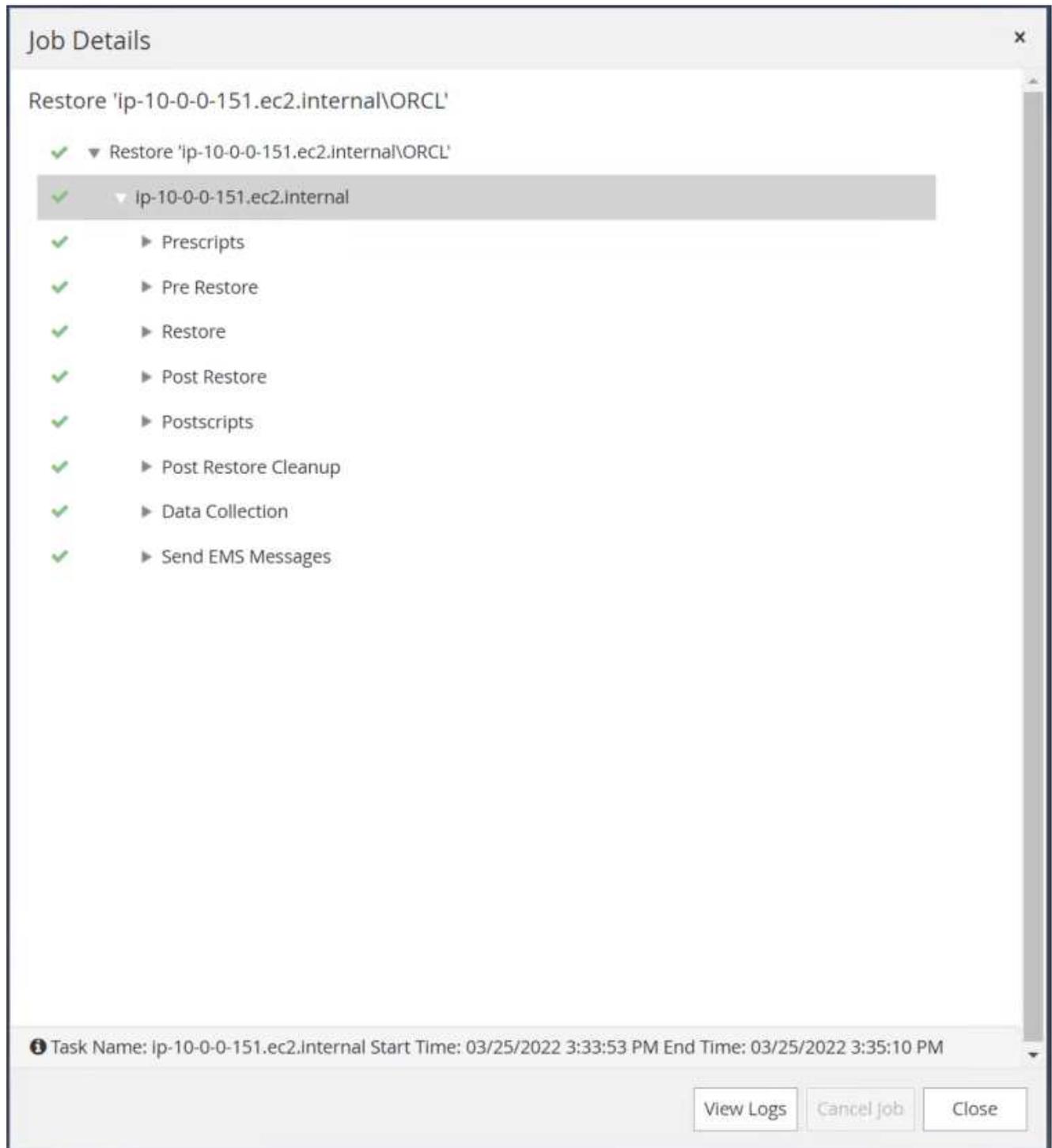
- 1 Restore Scope
- 2 Recovery Scope
- 3 PreOps
- 4 PostOps
- 5 Notification
- 6 Summary

Summary

| | |
|-----------------------|--|
| Backup name | ip-10-0-0-151_03-25-2022_11.15.01.1503_0 |
| Backup date | 03/25/2022 11:15:11 AM |
| Restore scope | All DataFiles |
| Recovery scope | Until SCN 1778546 |
| Auxiliary destination | |
| Options | Change database state if necessary , Open the database or container database in READ-WRITE mode after recovery |
| Prescript full path | None |
| Prescript arguments | |
| Postscript full path | None |
| Postscript arguments | |
| Send email | No |

Previous
Finish

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_TIME    OPEN_MODE
-----
ORCL          1778547 25-MAR-22  READ WRITE

SQL>

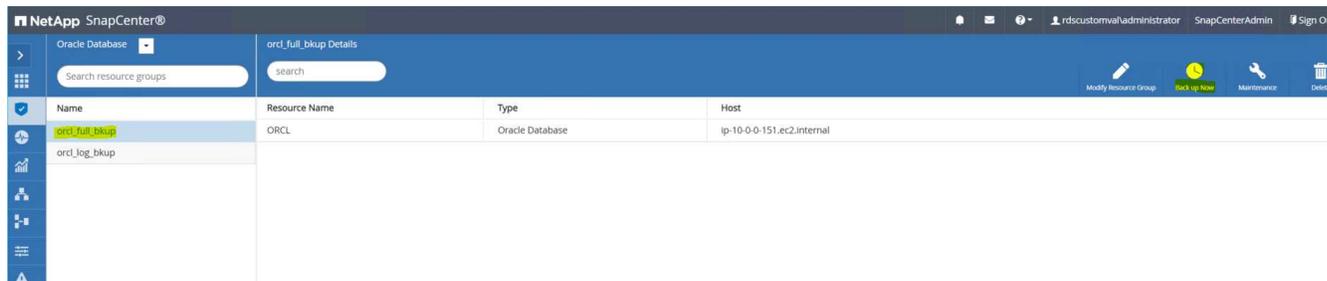
```

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

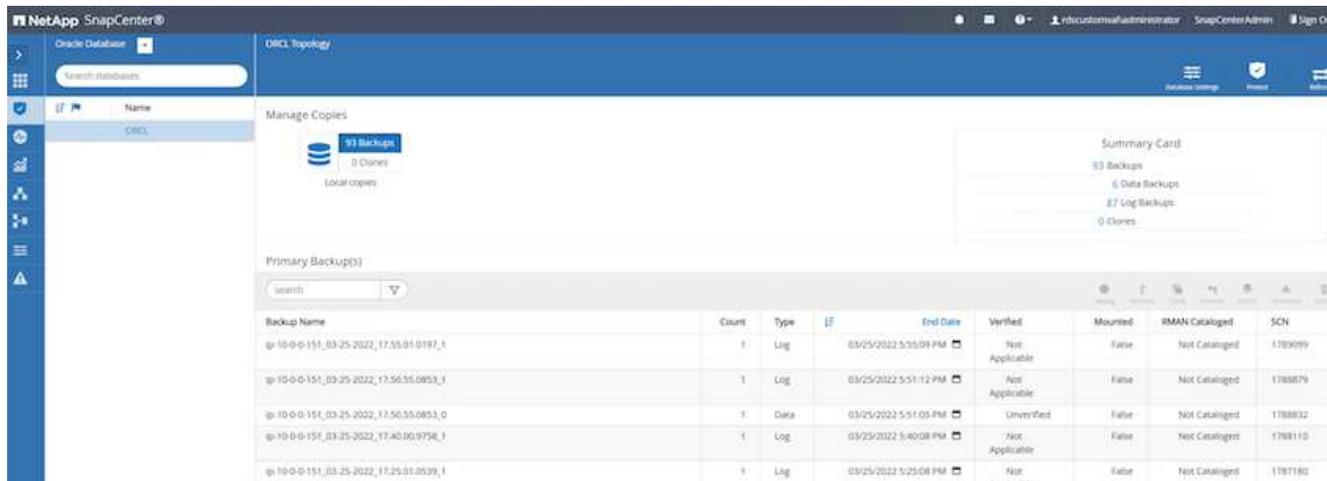
Erstellen eines Datenbankklons

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.



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

The screenshot shows the Oracle Cloud console interface for managing backups. At the top, there's a 'Manage Copies' section with '95 Backups' and '0 Clones'. A 'Summary Card' on the right shows '95 Backups', '6 Data Backups', '89 Log Backups', and '0 Clones'. Below this is a table of 'Primary Backup(s)'. One row is highlighted in blue, indicating it's selected for mounting.

| Backup Name | Count | Type | End Date | Verified | Mounted | RMAN Cataloged | SCN |
|--|-------|------|-----------------------|----------------|---------|----------------|---------|
| ip-10-0-0-151_03-25-2022_18.55.01.0309_1 | 1 | Log | 03/25/2022 6:55:09 PM | Not Applicable | False | Not Cataloged | 1892563 |
| ip-10-0-0-151_03-25-2022_18.40.00.9602_1 | 1 | Log | 03/25/2022 6:40:23 PM | Not Applicable | False | Not Cataloged | 1891375 |
| ip-10-0-0-151_03-25-2022_17.55.01.0197_1 | 1 | Log | 03/25/2022 5:55:09 PM | Not Applicable | False | Not Cataloged | 1789099 |
| ip-10-0-0-151_03-25-2022_17.50.55.0853_1 | 1 | Log | 03/25/2022 5:51:12 PM | Not Applicable | False | Not Cataloged | 1788079 |
| ip-10-0-0-151_03-25-2022_17.50.55.0853_0 | 1 | Data | 03/25/2022 5:51:05 PM | Unverified | False | Not Cataloged | 1788832 |
| ip-10-0-0-151_03-25-2022_17.40.00.9758_1 | 1 | Log | 03/25/2022 5:40:08 PM | Not | False | Not Cataloged | 1788110 |

The 'Mount backups' dialog is open, showing the selected backup and the host to mount it to. The mount path is automatically generated based on the backup name.

Choose the host to mount the backup:

Mount path: /var/opt/snapcenter/sco/backup_mount/ip-10-0-0-151_03-25-2022_17.50.55.0853_1/ORCL

Buttons: **Mount** (blue), Cancel (white)

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

ORCL Topology

Database Settings Protect Refresh

Manage Copies

93 Backups
0 Clones
Local copies

Summary Card

93 Backups
6 Data Backups
87 Log Backups
0 Clones

Primary Backup(s)

search

| Backup Name | Count | Type | IF | End Date | Verified | Mounted | RMAN Cataloged | SCN |
|--|-------|------|----|-----------------------|----------------|---------|----------------|---------|
| ip-10-0-0-151_03-25-2022_17:55:01.0197_1 | 1 | Log | | 03/25/2022 5:55:09 PM | Not Applicable | False | Not Cataloged | 1789099 |
| ip-10-0-0-151_03-25-2022_17:50:55.0853_1 | 1 | Log | | 03/25/2022 5:51:12 PM | Not Applicable | False | Not Cataloged | 1788879 |
| ip-10-0-0-151_03-25-2022_17:50:55.0853_0 | 1 | Data | | 03/25/2022 5:51:03 PM | Unverified | False | Not Cataloged | 1788832 |
| ip-10-0-0-151_03-25-2022_17:40:00.9758_1 | 1 | Log | | 03/25/2022 5:40:08 PM | Not Applicable | False | Not Cataloged | 1788110 |
| ip-10-0-0-151_03-25-2022_17:25:01.0539_1 | 1 | Log | | 03/25/2022 5:25:08 PM | Not Applicable | False | Not Cataloged | 1787180 |

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

Clone from ORCL

1 Name

Provide clone database SID

Clone SID

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Previous Next

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

Sie auf „Weiter“.

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Select the host to create a clone

Clone host: ip-10-0-0-47.ec2.internal

Datafile locations ⓘ

/ora_nfs_data_ORCLREAD

Reset

Control files ⓘ

/ora_nfs_data_ORCLREAD/ORCLREAD/control/control01.ctl

Reset

Redo logs ⓘ

| Group | Size | Unit | Number of files |
|--|------|------|-----------------|
| RedoGroup 1 | 128 | MB | 1 |
| /ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo04.log | | | |
| RedoGroup 2 | 128 | MB | 1 |

Previous Next

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“.

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user: None + i

Database port: 1521

Oracle Home Settings i

Oracle Home: /rdsdbbin/oracle

Oracle OS User: rdsdb

Oracle OS Group: database

Previous Next

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

Clone from ORCL

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

Recover Database

Until Cancel ⓘ

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

Until SCN (System Change Number) ⓘ

Specify external archive log locations ⓘ ⓘ ⓘ

Create new DBID ⓘ

Create tempfile for temporary tablespace ⓘ

Enter SQL queries to apply when clone is created

Enter scripts to run after clone operation ⓘ

Previous Next

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

Clone from ORCL x

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

Provide email settings ⓘ

Email preference

From

To

Subject

Attach job report

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

Clone from ORCL

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

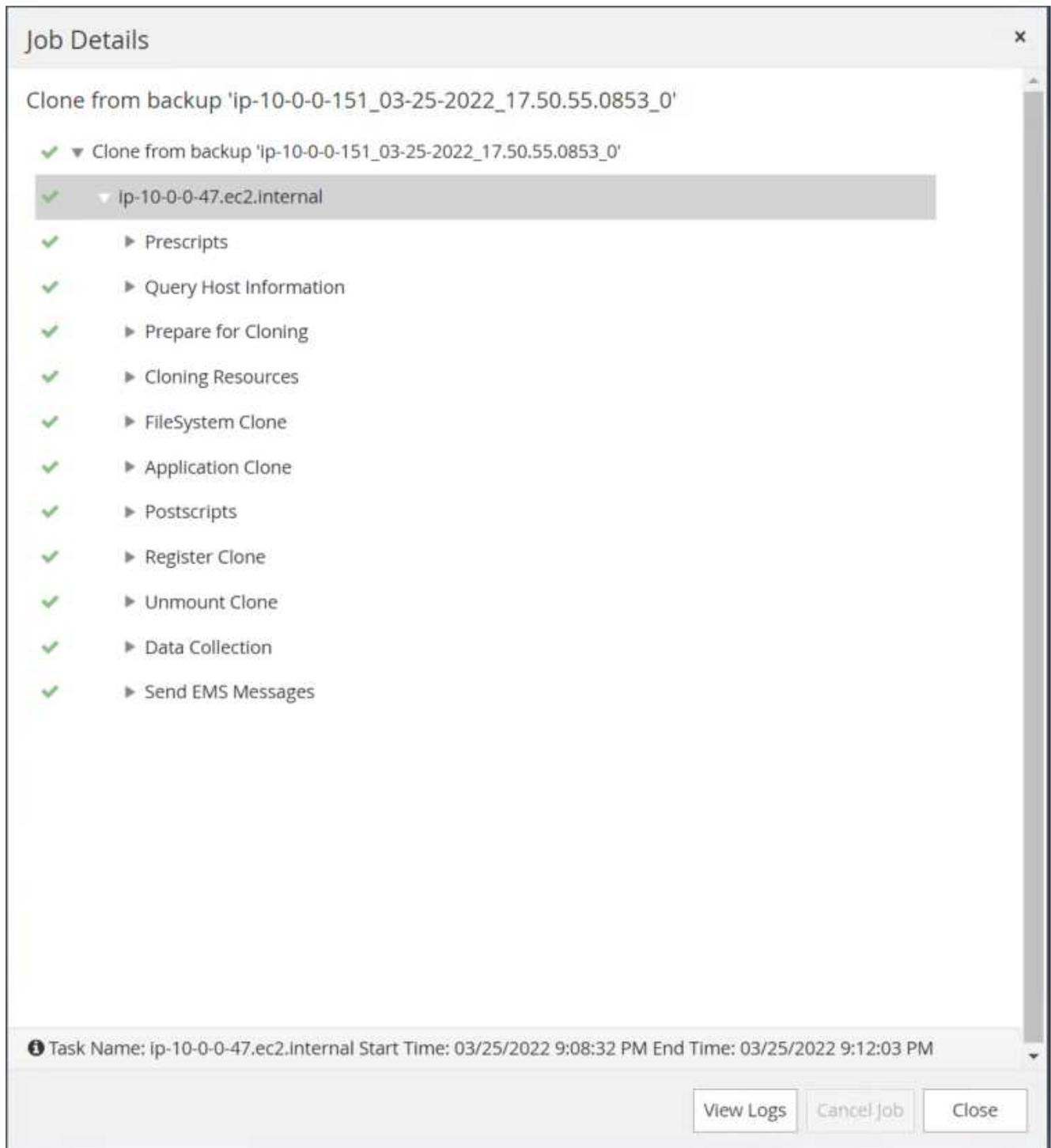
7 Summary

Summary

| | |
|----------------------|--|
| Clone from backup | ip-10-0-0-151_03-25-2022_17.50.55.0853_0 |
| Clone SID | ORCLREAD |
| Clone server | ip-10-0-0-47.ec2.internal |
| Oracle home | /rdsdbbin/oracle |
| Oracle OS user | rdsdb |
| Oracle OS group | database |
| Datafile mountpaths | /ora_nfs_data_ORCLREAD |
| Control files | /ora_nfs_data_ORCLREAD/ORCLREAD/control/control01.ctl |
| Redo groups | RedoGroup =1 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo04.log RedoGroup =2 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo03.log RedoGroup =3 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo02.log RedoGroup =4 TotalSize =128 Path =/ora_nfs_data_ORCLREAD/ORCLREAD/redolog/redo01.log |
| Recovery scope | Until SCN 1788879 |
| Prescript full path | none |
| Prescript arguments | |
| Postscript full path | none |
| Postscript arguments | |
| Send email | No |

Previous Finish

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 Abschnitt [Erstellen 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 Protokollvolumens 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 Datenbankvolumens können verwendet werden, um den ausgefallenen primären Standort mit der umgekehrten SnapMirror -Methode als neuen Standby-Standort neu aufzubauen.

- 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.

- Erstellen Sie eine EC2-Ziel-Compute-Instanz, die der lokalen Instanz entspricht.
- Stellen Sie passende, gleich große Datenbankvolumes über die FSx-Konsole bereit.
- Mounten Sie die FSx-Datenbankvolumes in der EC2-Instanz.
- 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.
- 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.
- Teilen Sie die gespiegelten Volumes auf, führen Sie die Oracle-Wiederherstellung auf dem Ziel aus und starten Sie die Datenbank für den Dienst.
- 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 Datenbankvolumen aus dem FSx-Speicher bereit und mounten Sie die Volumes in die EC2-Instanz.
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
```

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.