TR-4964: Sichern, Wiederherstellen und Klonen von Oracle-Datenbanken mit SnapCenter Services – AWS

NetApp database solutions

NetApp
August 18, 2025

Inhalt

TR-4964: Sichern, Wiederherstellen und Klonen von Oracle-Datenbanken mit SnapCenter Services – AWS

Diese Lösung bietet einen Überblick und Details zum Sichern, Wiederherstellen und Klonen von Oracle-Datenbanken mithilfe von NetApp SnapCenter SaaS und der BlueXP -Konsole in der Azure-Cloud.

Allen Cao, Niyaz Mohamed, NetApp

Zweck

SnapCenter Services ist die SaaS-Version des klassischen SnapCenter -Datenbankverwaltungs-UI-Tools, das über die NetApp BlueXP -Cloud-Verwaltungskonsole verfügbar ist. Es ist ein integraler Bestandteil des NetApp Cloud-Backup- und Datenschutzangebots für Datenbanken wie Oracle und HANA, die auf NetApp Cloud-Speicher ausgeführt werden. Dieser SaaS-basierte Dienst vereinfacht die herkömmliche Bereitstellung eigenständiger SnapCenter -Server, für die im Allgemeinen ein Windows-Server erforderlich ist, der in einer Windows-Domänenumgebung ausgeführt wird.

In dieser Dokumentation zeigen wir, wie Sie SnapCenter Services zum Sichern, Wiederherstellen und Klonen von Oracle-Datenbanken einrichten, die auf Amazon FSx ONTAP -Speicher- und EC2-Recheninstanzen bereitgestellt werden. Obwohl die Einrichtung und Verwendung viel einfacher ist, bieten SnapCenter Services wichtige Funktionen, die im alten SnapCenter -UI-Tool verfügbar sind.

Diese Lösung ist für die folgenden Anwendungsfälle geeignet:

- Datenbanksicherung mit Snapshots für Oracle-Datenbanken, die in Amazon FSx ONTAP gehostet werden
- Oracle-Datenbankwiederherstellung im Falle eines Ausfalls
- Schnelles und speichereffizientes Klonen von Primärdatenbanken für eine Entwicklungs-/Testumgebung oder andere Anwendungsfälle

Publikum

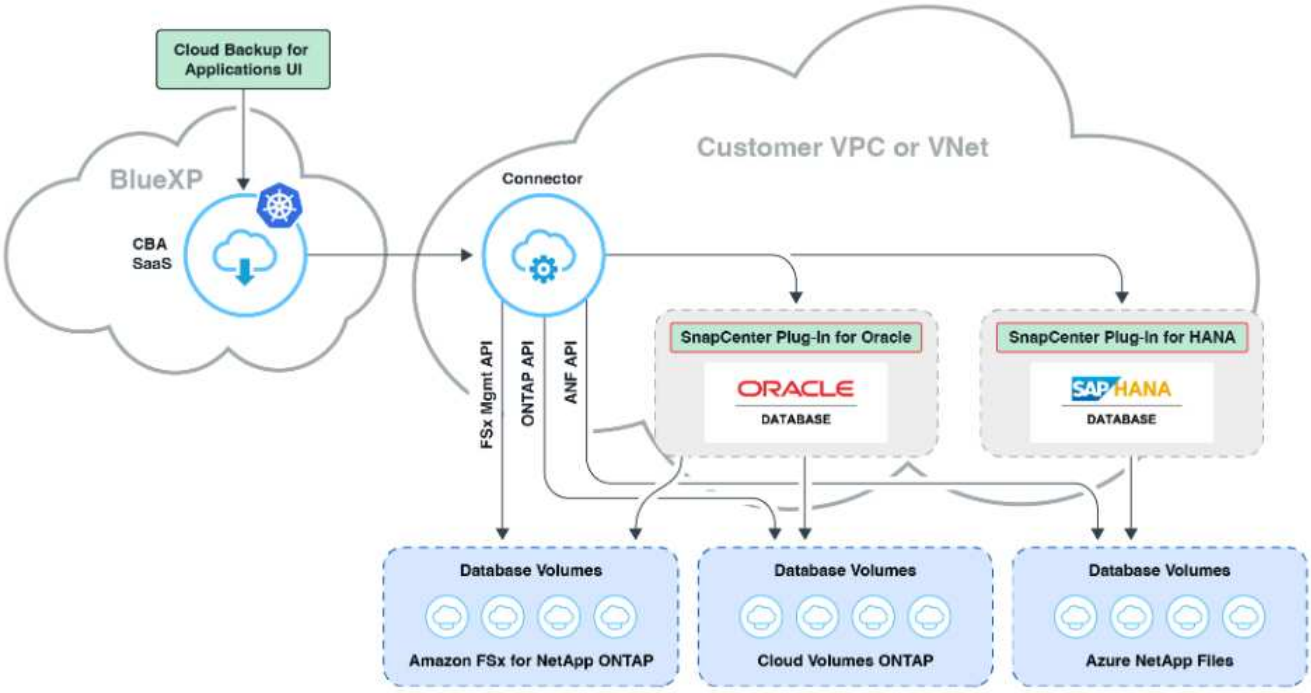
Diese Lösung ist für die folgenden Zielgruppen gedacht:

- Der DBA, der Oracle-Datenbanken verwaltet, die auf Amazon FSx ONTAP -Speicher ausgeführt werden
- Der Lösungsarchitekt, der daran interessiert ist, die Sicherung, Wiederherstellung und das Klonen von Oracle-Datenbanken in der öffentlichen AWS-Cloud zu testen
- Der Speicheradministrator, der den Amazon FSx ONTAP Speicher unterstützt und verwaltet
- Der Anwendungseigentümer, dem die Anwendungen gehören, die im Amazon FSx ONTAP -Speicher bereitgestellt werden

Test- und Validierungsumgebung für Lösungen

Das Testen und Validieren dieser Lösung wurde in einer AWS FSx- und EC2-Umgebung durchgeführt, die möglicherweise nicht der endgültigen Bereitstellungsumgebung entspricht. Weitere Informationen finden Sie im Abschnitt Wichtige Faktoren für die Bereitstellungsüberlegungen .

Architektur



Dieses Bild bietet eine detaillierte Darstellung der BlueXP backup and recovery für Anwendungen innerhalb der BlueXP Konsole, einschließlich der Benutzeroberfläche, des Connectors und der von ihm verwalteten Ressourcen.

Hardware- und Softwarekomponenten

Hardware

FSx ONTAP Speicher	Aktuelle von AWS angebotene Version	Ein FSx HA-Cluster in derselben VPC und Verfügbarkeitszone
EC2-Instanz für Compute	t2.xlarge/4vCPU/16G	Zwei EC2 T2 xlarge EC2-Instanzen, eine als primärer DB-Server und die andere als Klon-DB-Server

Software

RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	RedHat-Abonnement zum Testen bereitgestellt
Oracle Grid-Infrastruktur	Version 19.18	RU-Patch p34762026_190000_Linux-x86-64.zip angewendet
Oracle-Datenbank	Version 19.18	RU-Patch p34765931_190000_Linux-x86-64.zip angewendet

Oracle OPatch	Version 12.2.0.1.36	Neuester Patch p6880880_190000_Linux-x86-64.zip
SnapCenter -Dienst	Version	v2.3.1.2324

Wichtige Faktoren für die Bereitstellungsüberlegungen

- **Connector muss im selben VPC wie Datenbank und FSx bereitgestellt werden.** Wenn möglich, sollte der Connector im selben AWS VPC bereitgestellt werden, wodurch die Verbindung zum FSx-Speicher und der EC2-Recheninstanz ermöglicht wird.
- **Eine für den SnapCenter Connector erstellte AWS IAM-Richtlinie.** Die Richtlinie im JSON-Format ist in der ausführlichen SnapCenter -Dienstdokumentation verfügbar. Wenn Sie die Connector-Bereitstellung mit der BlueXP Konsole starten, werden Sie auch aufgefordert, die Voraussetzungen mit Details zu den erforderlichen Berechtigungen im JSON-Format einzurichten. Die Richtlinie sollte dem AWS-Benutzerkonto zugewiesen werden, dem der Connector gehört.
- **Der AWS-Kontozugriffsschlüssel und das im AWS-Konto erstellte SSH-Schlüsselpaar.** Das SSH-Schlüsselpaar wird dem EC2-Benutzer zugewiesen, um sich beim Connector-Host anzumelden und dann ein Datenbank-Plug-In auf dem EC2-DB-Server-Host bereitzustellen. Der Zugriffsschlüssel erteilt die Berechtigung zur Bereitstellung des erforderlichen Connectors mit der oben genannten IAM-Richtlinie.
- **Ein Anmeldeinformationselement, das der BlueXP Konsoleneinstellung hinzugefügt wurde.** Um Amazon FSx ONTAP zur BlueXP -Arbeitsumgebung hinzuzufügen, wird in den BlueXP -Konsoleneinstellungen eine Anmeldeinformation eingerichtet, die BlueXP die Berechtigung zum Zugriff auf Amazon FSx ONTAP erteilt.
- **java-11-openjdk auf dem EC2-Datenbankinstanz-Host installiert.** Für die Installation des SnapCenter -Dienstes ist Java Version 11 erforderlich. Es muss vor dem Versuch der Plug-In-Bereitstellung auf dem Anwendungshost installiert werden.

Lösungsbereitstellung

Es gibt eine umfassende NetApp -Dokumentation mit einem breiteren Anwendungsbereich, die Ihnen beim Schutz Ihrer Cloud-nativen Anwendungsdaten hilft. Das Ziel dieser Dokumentation besteht darin, schrittweise Verfahren bereitzustellen, die die Bereitstellung des SnapCenter -Dienstes mit der BlueXP Konsole abdecken, um Ihre auf Amazon FSx ONTAP und einer EC2-Recheninstanz bereitgestellte Oracle-Datenbank zu schützen. Dieses Dokument ergänzt bestimmte Details, die in allgemeineren Anweisungen möglicherweise fehlen.

Führen Sie zunächst die folgenden Schritte aus:

- Lesen Sie die allgemeinen Hinweise"Schützen Sie die Daten Ihrer Cloud-nativen Anwendungen" und die Abschnitte zu Oracle und Amazon FSx ONTAP.
- Sehen Sie sich die folgende Video-Komplettlösung an.

Lösungsbereitstellung

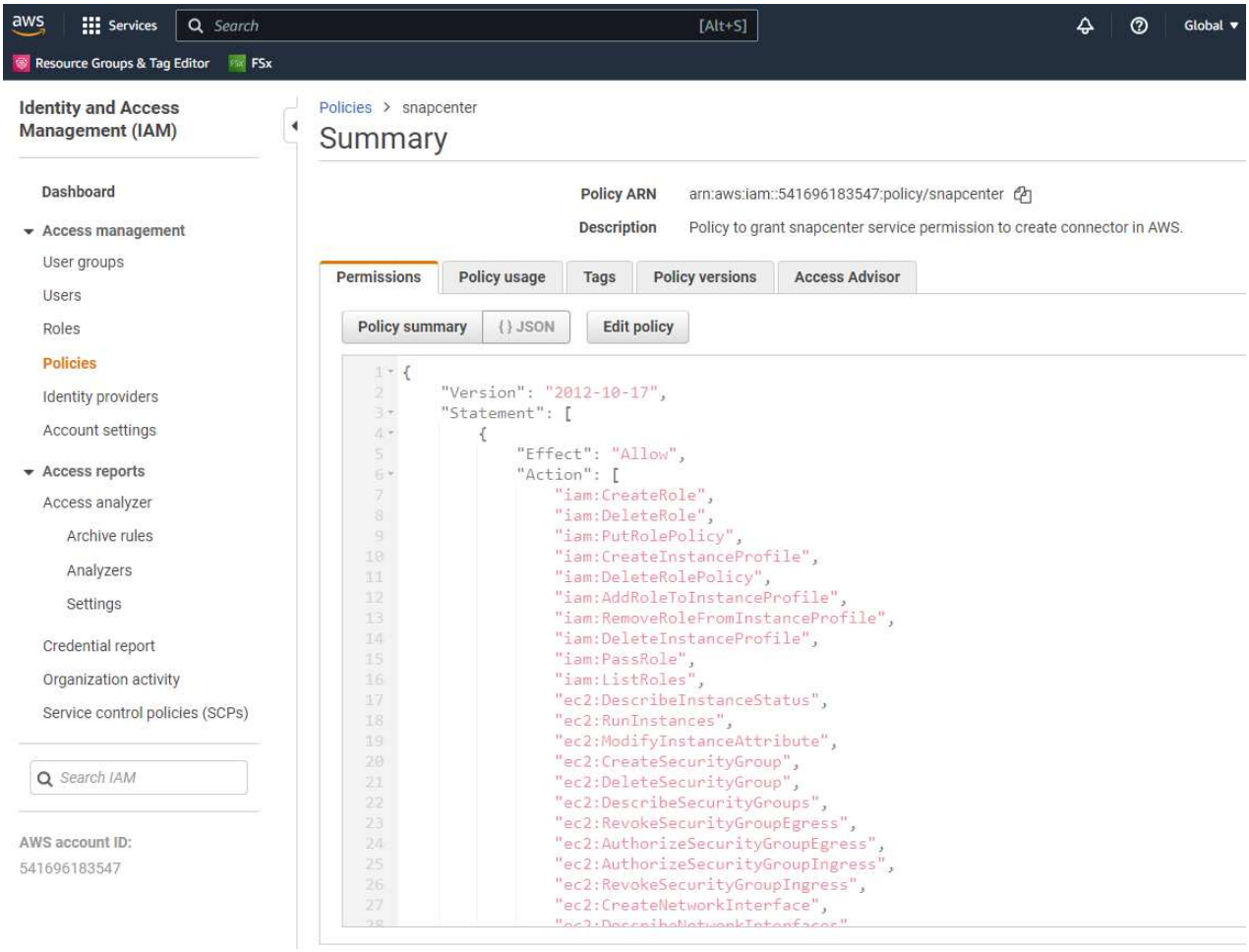
Voraussetzungen für die Bereitstellung des SnapCenter -Dienstes

Für die Bereitstellung sind die folgenden Voraussetzungen erforderlich.

1. Ein primärer Oracle-Datenbankserver auf einer EC2-Instance mit einer vollständig bereitgestellten und laufenden Oracle-Datenbank.
2. Ein in AWS bereitgestellter Amazon FSx ONTAP -Cluster, der die oben genannten Datenbank-Volumes hostet.
3. Ein optionaler Datenbankserver auf einer EC2-Instance, der zum Testen des Klonens einer Oracle-Datenbank auf einen alternativen Host verwendet werden kann, um eine Entwicklungs-/Test-Workload oder beliebige Anwendungsfälle zu unterstützen, die einen vollständigen Datensatz einer Produktions-Oracle-Datenbank erfordern.
4. Wenn Sie Hilfe benötigen, um die oben genannten Voraussetzungen für die Oracle-Datenbankbereitstellung auf Amazon FSx ONTAP und EC2-Compute-Instance zu erfüllen, lesen Sie"Bereitstellung und Schutz von Oracle-Datenbanken in AWS FSx/EC2 mit iSCSI/ASM" oder Whitepaper"Best Practices für die Oracle-Datenbankbereitstellung auf EC2 und FSx"

Onboarding zur BlueXP -Vorbereitung

1. Verwenden Sie den Link"NetApp BlueXP" um sich für den Zugriff auf die BlueXP -Konsole anzumelden.
2. Melden Sie sich bei Ihrem AWS-Konto an, um eine IAM-Richtlinie mit den entsprechenden Berechtigungen zu erstellen und die Richtlinie dem AWS-Konto zuzuweisen, das für die Bereitstellung des BlueXP Connectors verwendet wird.

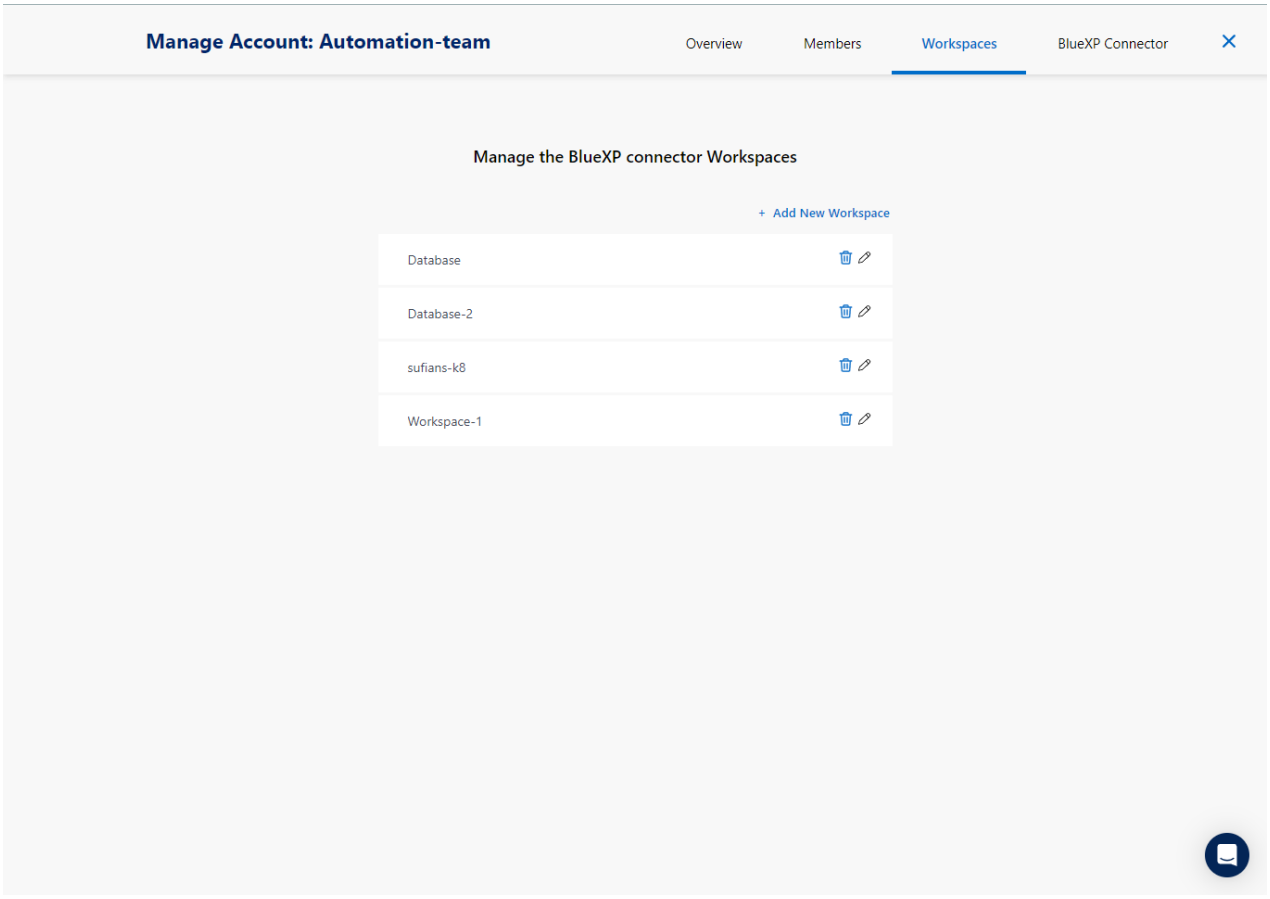


Die Richtlinie sollte mit einer JSON-Zeichenfolge konfiguriert werden, die in der NetApp Dokumentation verfügbar ist. Die JSON-Zeichenfolge kann auch von der Seite abgerufen werden, wenn die Connector-Bereitstellung gestartet wird und Sie zur Zuweisung der erforderlichen Berechtigungen aufgefordert werden.

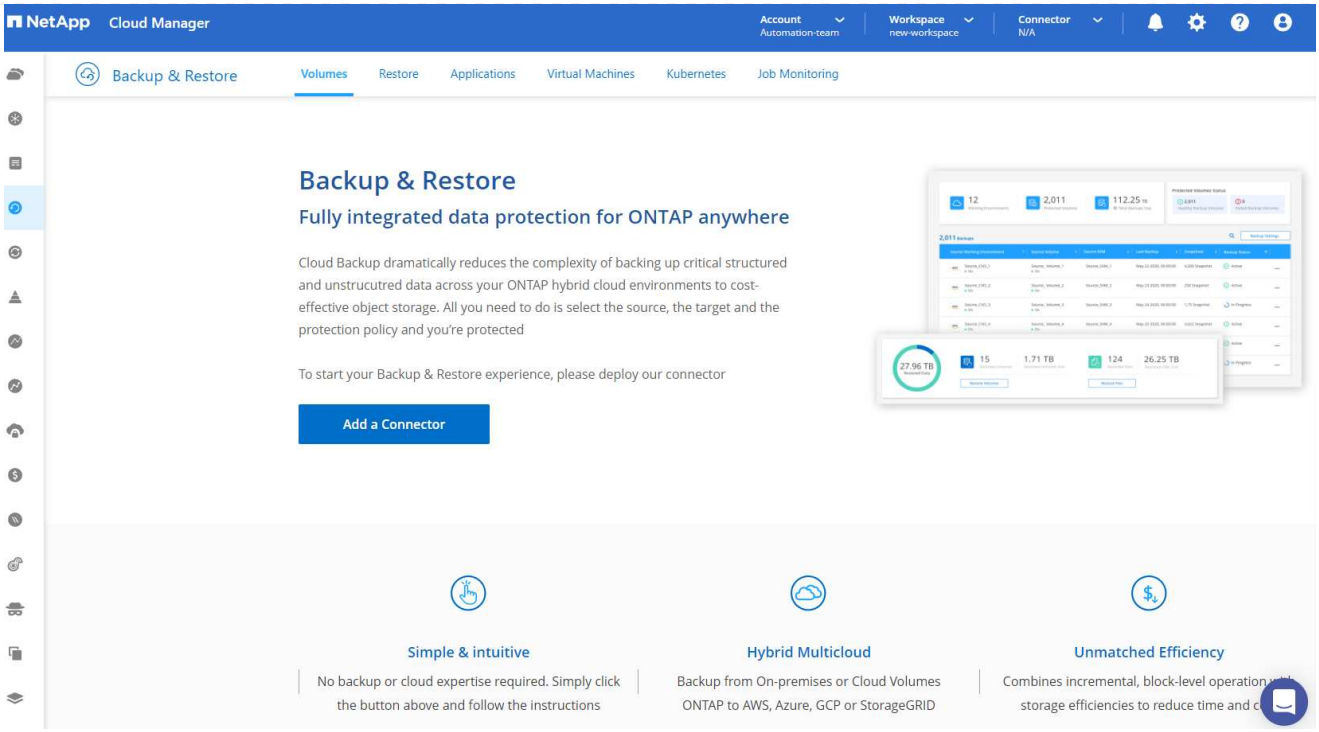
3. Sie benötigen außerdem AWS VPC, Subnetz, Sicherheitsgruppe, einen Zugriffsschlüssel und Geheimnisse für das AWS-Benutzerkonto, einen SSH-Schlüssel für den EC2-Benutzer usw., die für die Bereitstellung des Connectors bereit sind.

Bereitstellen eines Connectors für SnapCenter -Dienste

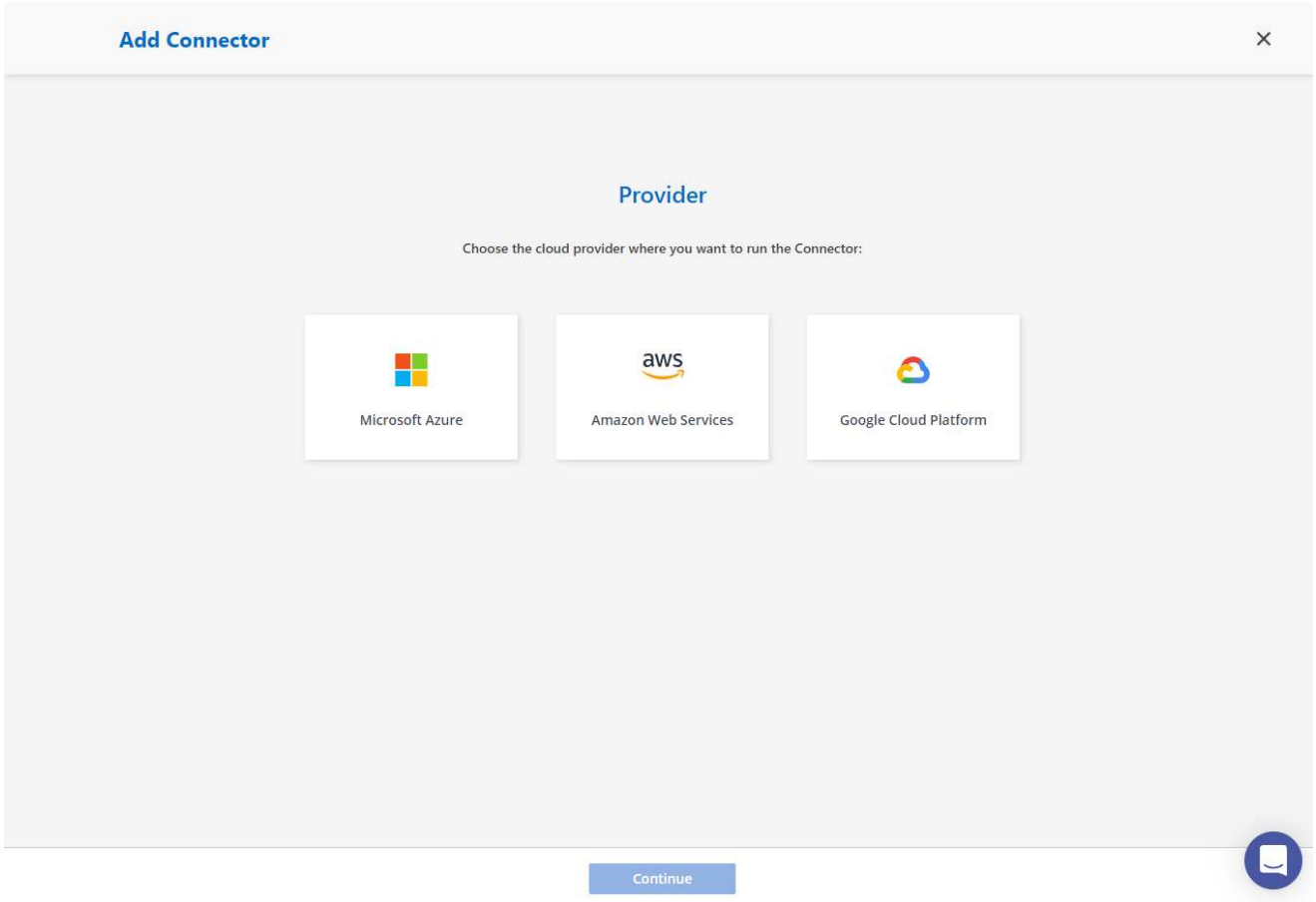
1. Melden Sie sich bei der BlueXP -Konsole an. Bei einem gemeinsam genutzten Konto empfiehlt es sich, einen individuellen Arbeitsbereich zu erstellen, indem Sie auf **Konto** > **Konto verwalten** > **Arbeitsbereich** klicken, um einen neuen Arbeitsbereich hinzuzufügen.



2. Klicken Sie auf **Connector hinzufügen**, um den Workflow zur Connector-Bereitstellung zu starten.

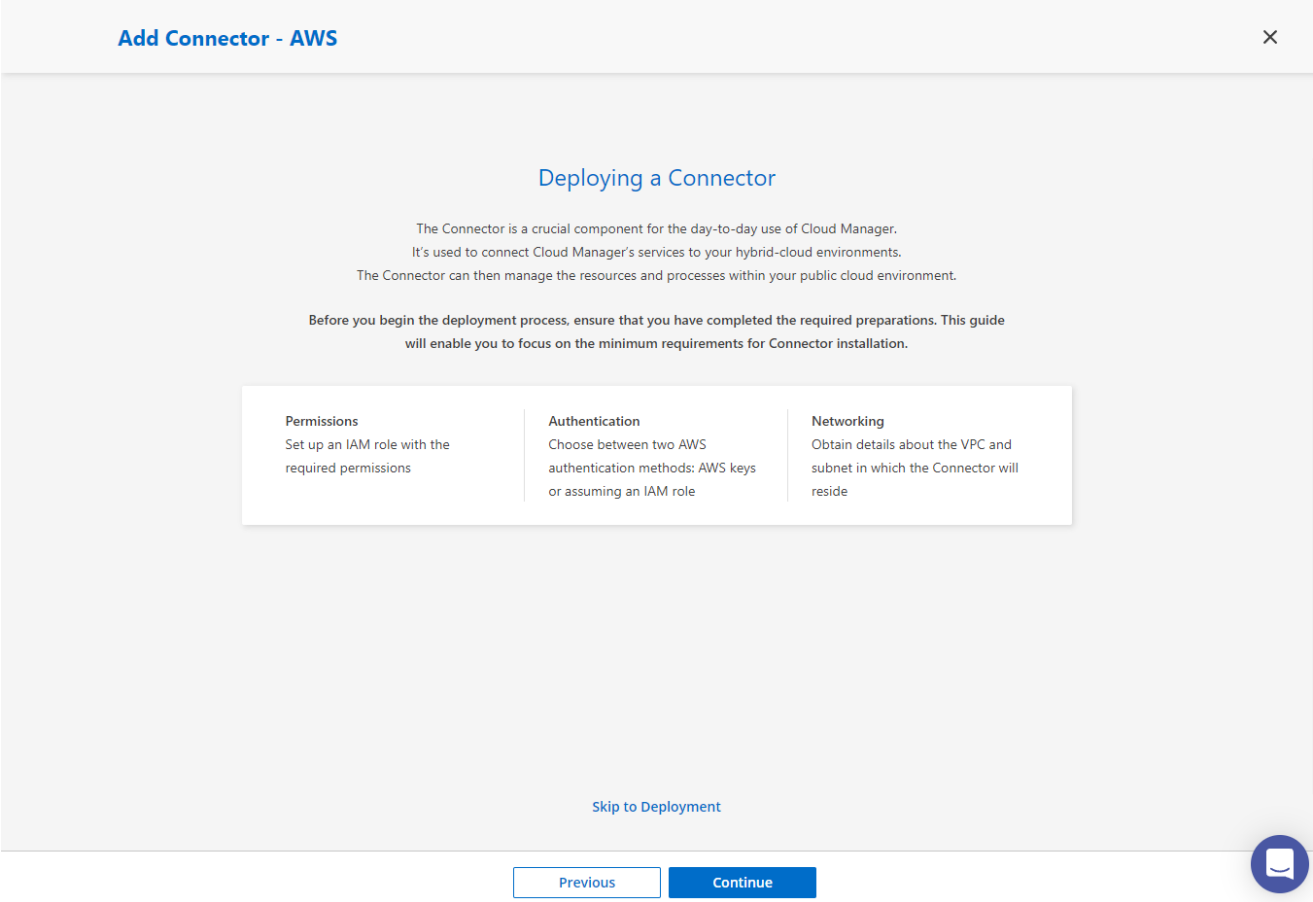


1. Wählen Sie Ihren Cloud-Anbieter (in diesem Fall **Amazon Web Services**).

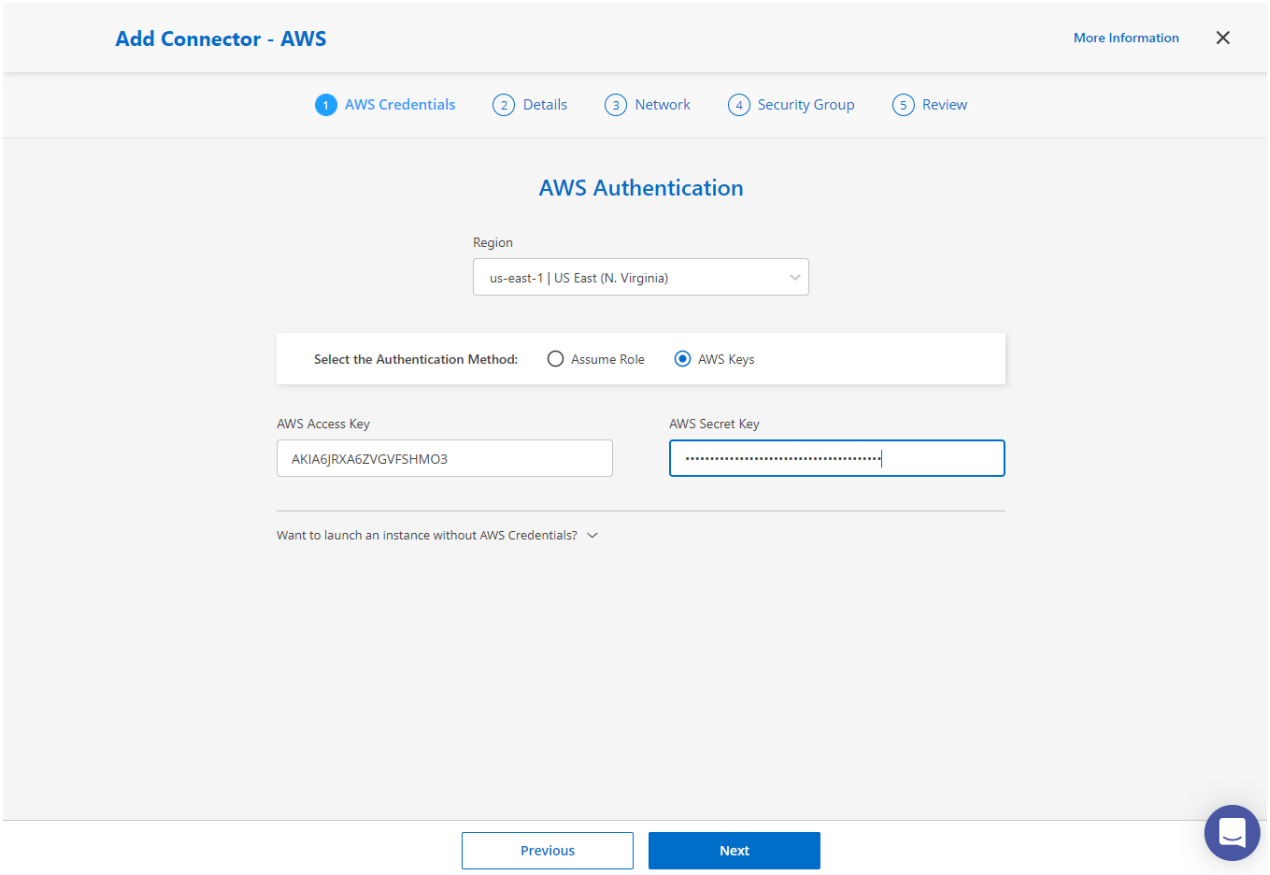


1. Überspringen Sie die Schritte **Berechtigung**, **Authentifizierung** und **Netzwerk**, wenn Sie diese bereits in Ihrem AWS-Konto eingerichtet haben. Wenn nicht, müssen Sie diese konfigurieren, bevor Sie fortfahren. Von hier aus können Sie auch die Berechtigungen für die AWS-Richtlinie abrufen, auf

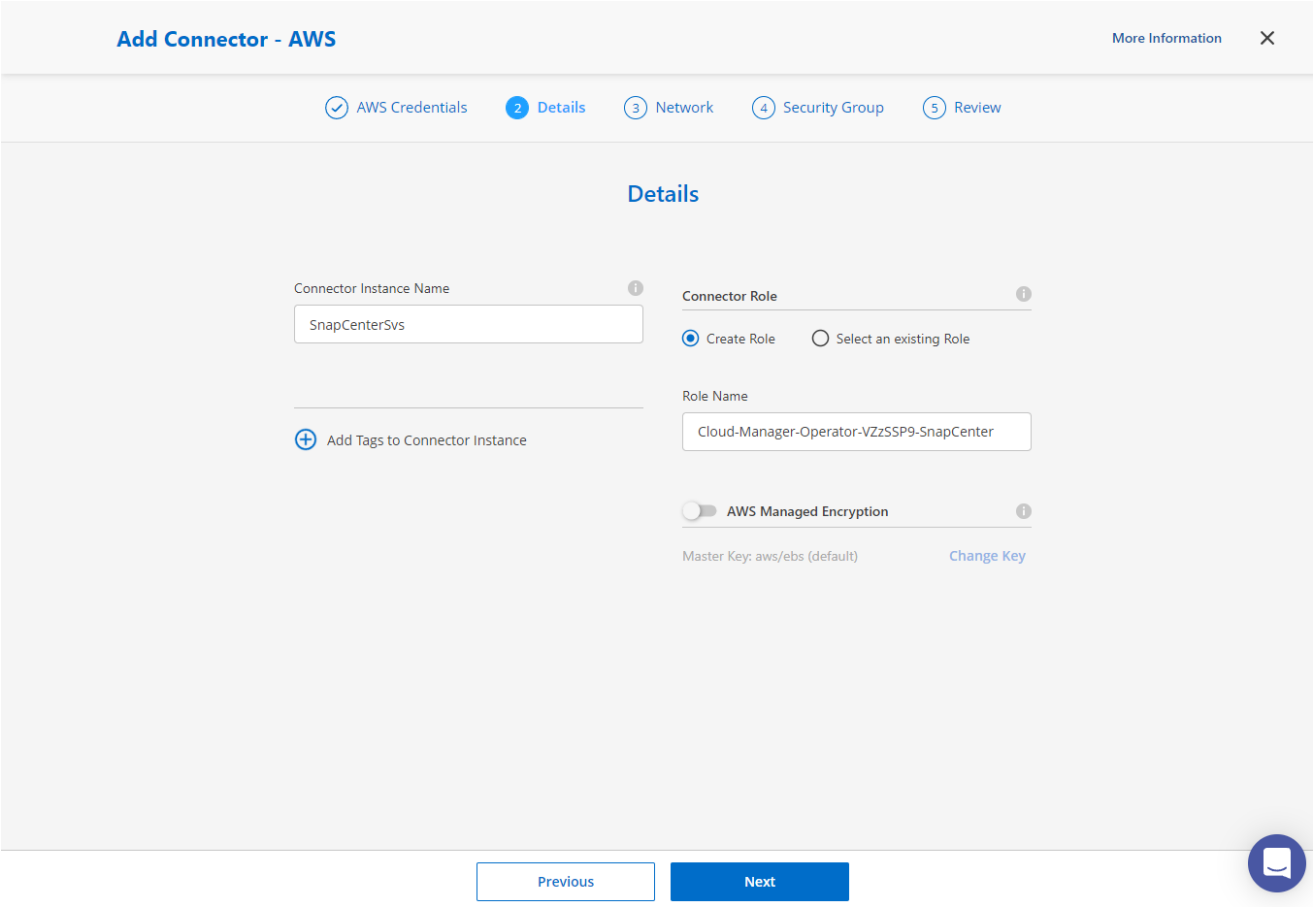
die im vorherigen Abschnitt verwiesen wird.Onboarding zur BlueXP -Vorbereitung ."



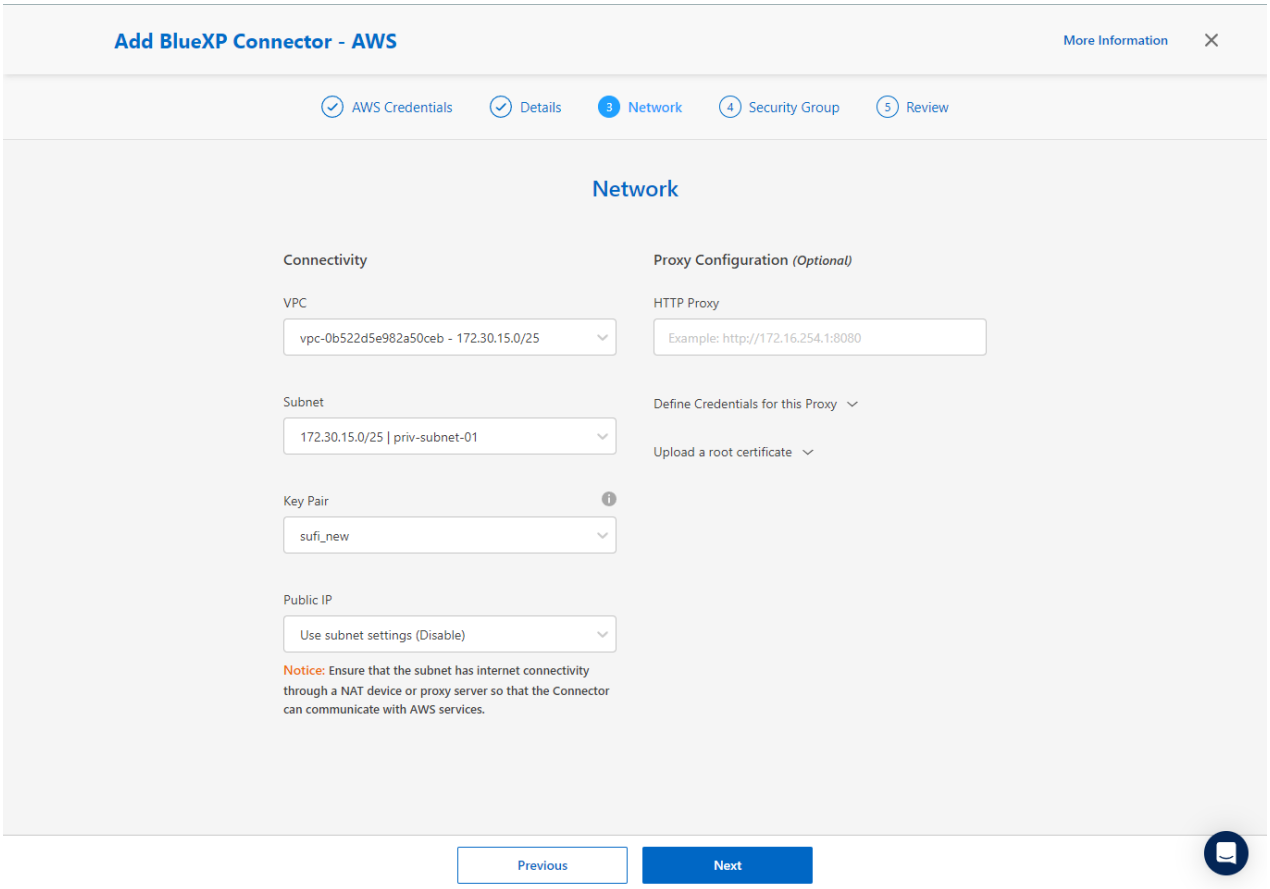
1. Geben Sie Ihre AWS-Kontoauthentifizierung mit **Zugriffsschlüssel** und **Geheimschlüssel** ein.



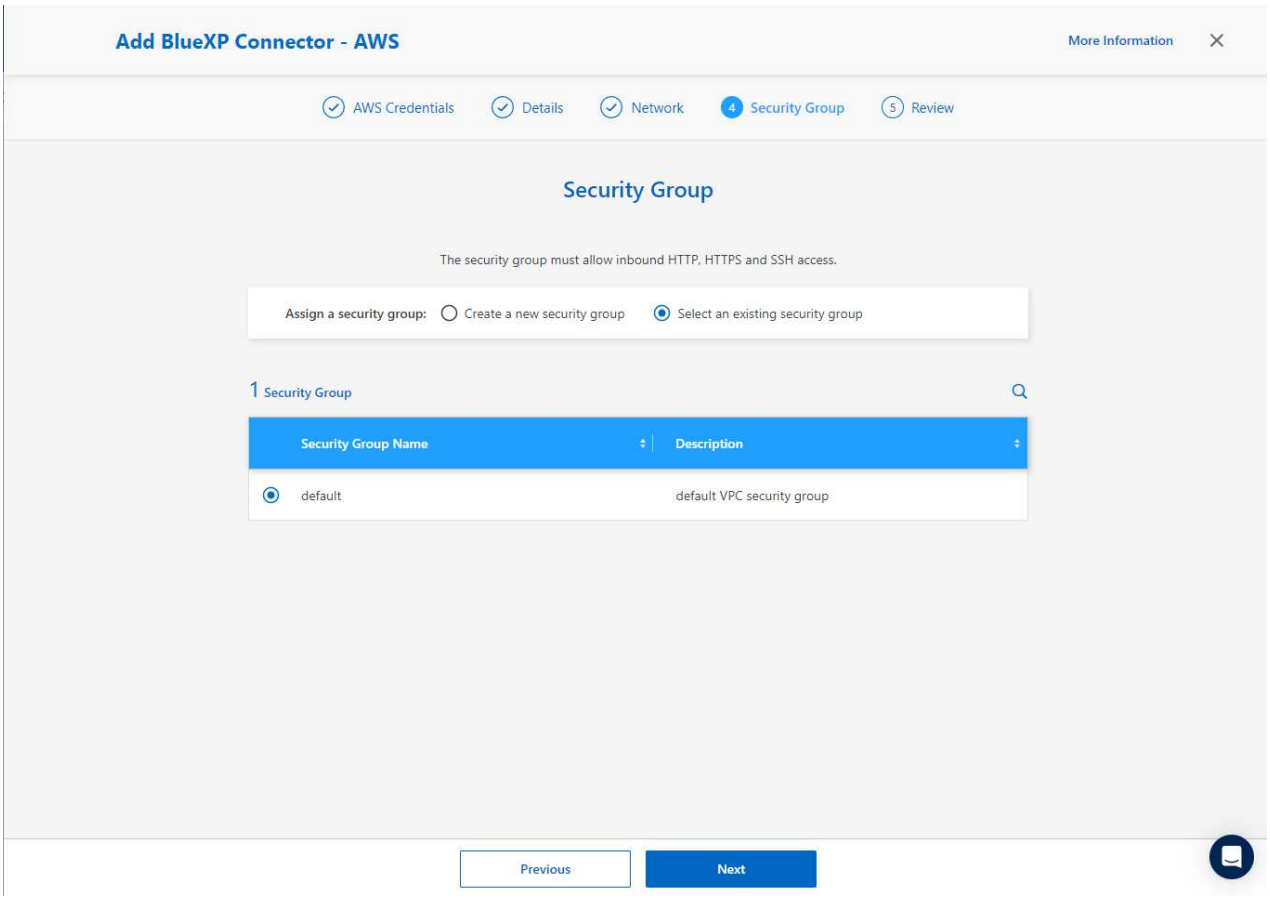
2. Benennen Sie die Connector-Instanz und wählen Sie unter **Details Rolle erstellen** aus.



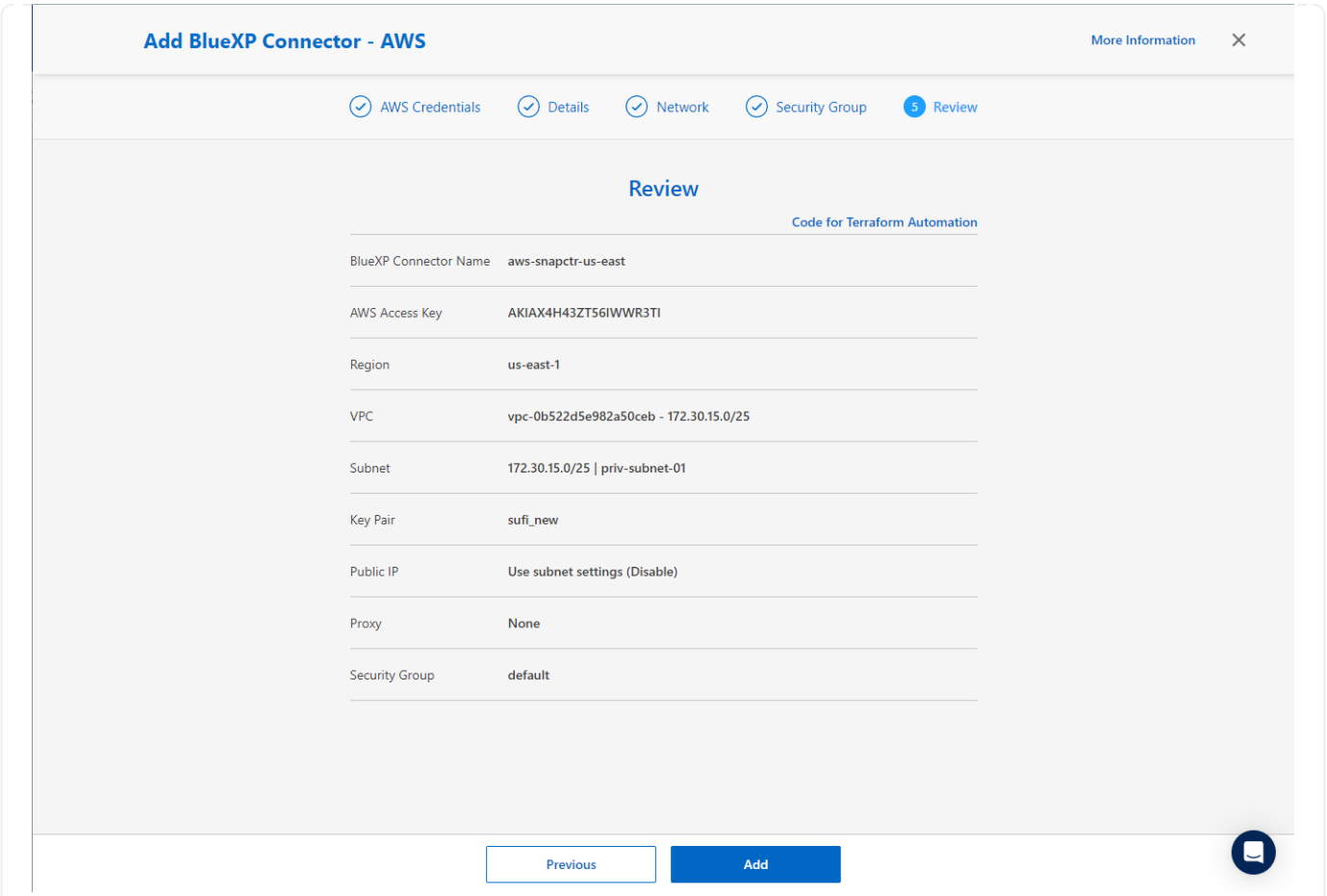
1. Konfigurieren Sie das Netzwerk mit dem richtigen **VPC**, **Subnetz** und SSH-**Schlüsselpaar** für den Connector-Zugriff.



2. Legen Sie die **Sicherheitsgruppe** für den Connector fest.

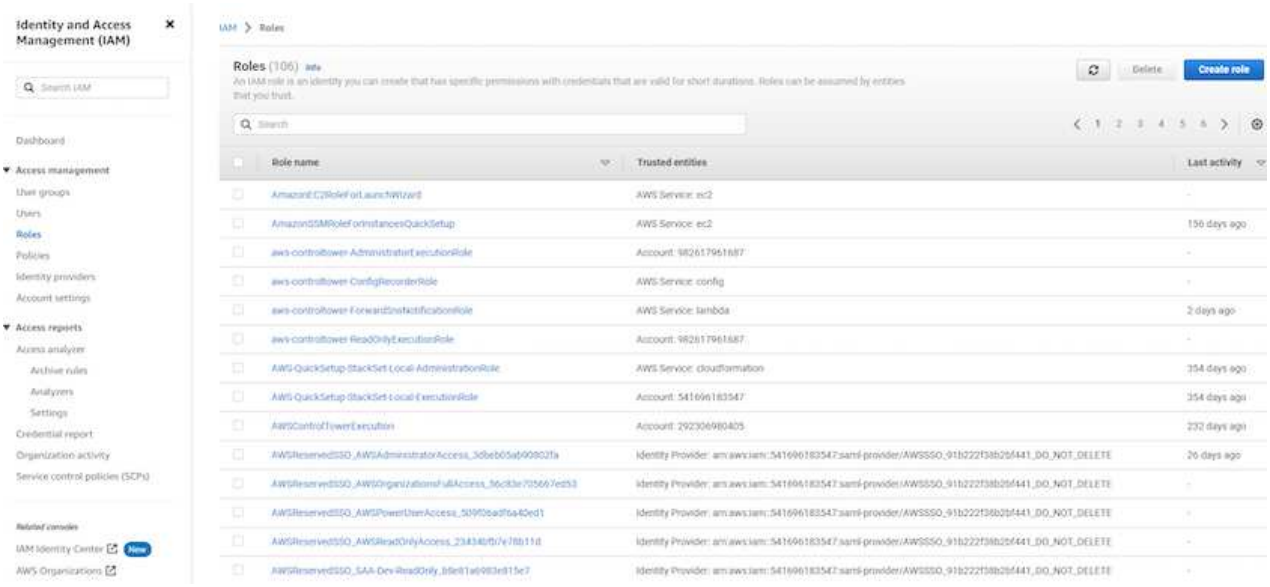


3. Überprüfen Sie die Übersichtsseite und klicken Sie auf **Hinzufügen**, um mit der Connector-Erstellung zu beginnen. Die Bereitstellung dauert in der Regel etwa 10 Minuten. Nach Abschluss wird die Connector-Instanz im AWS EC2-Dashboard angezeigt.

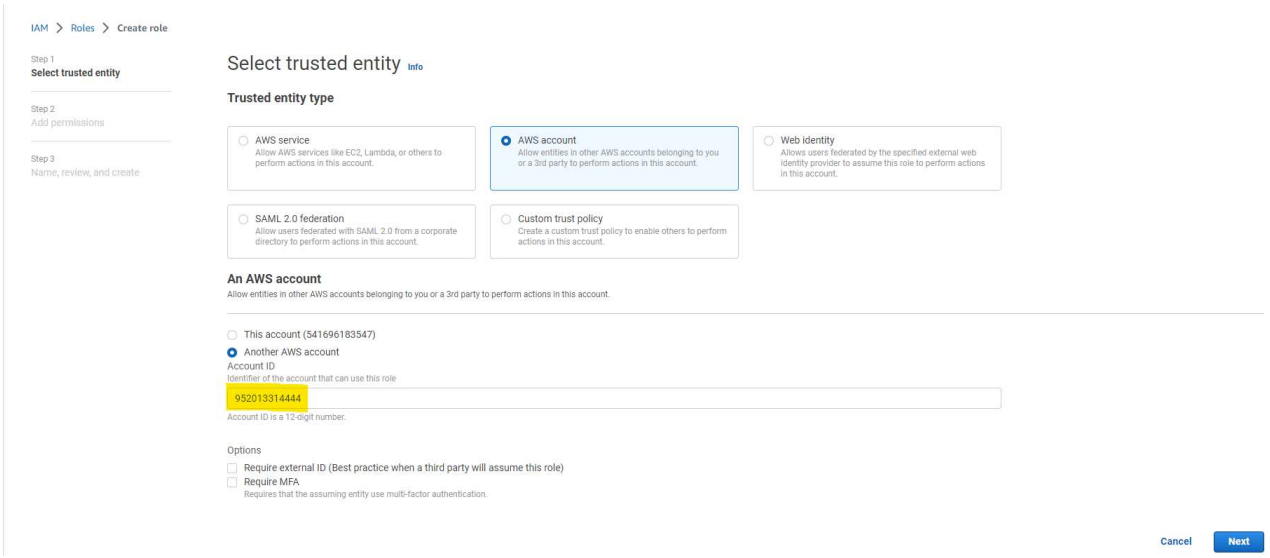


Definieren Sie in BlueXP eine Anmeldeinformation für den Zugriff auf AWS-Ressourcen

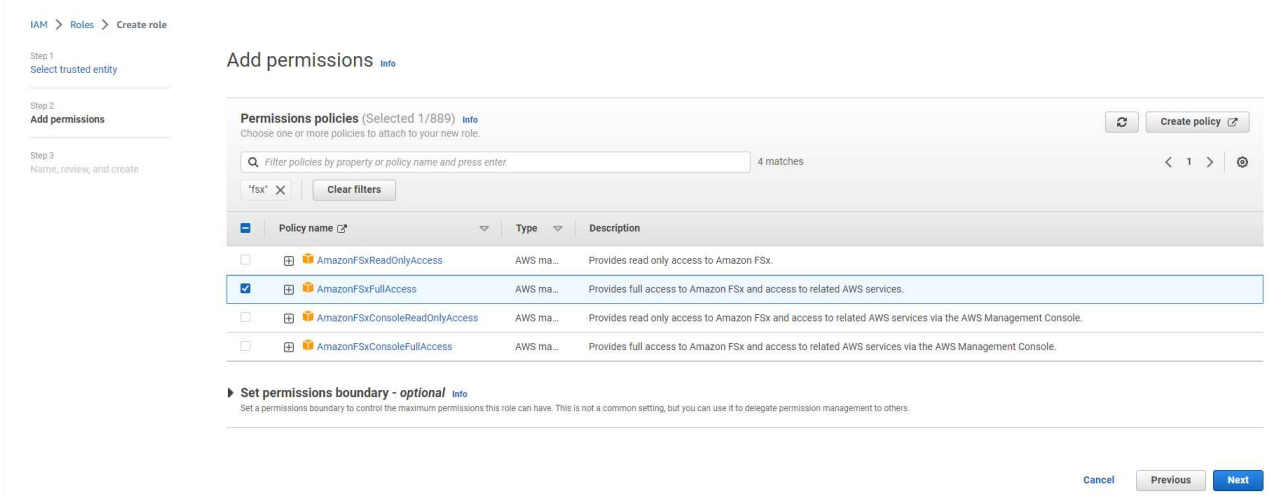
1. Erstellen Sie zunächst in der AWS EC2-Konsole eine Rolle im Menü **Rollen** von **Identity and Access Management (IAM)** und dann **Rolle erstellen**, um den Workflow zur Rollenerstellung zu starten.



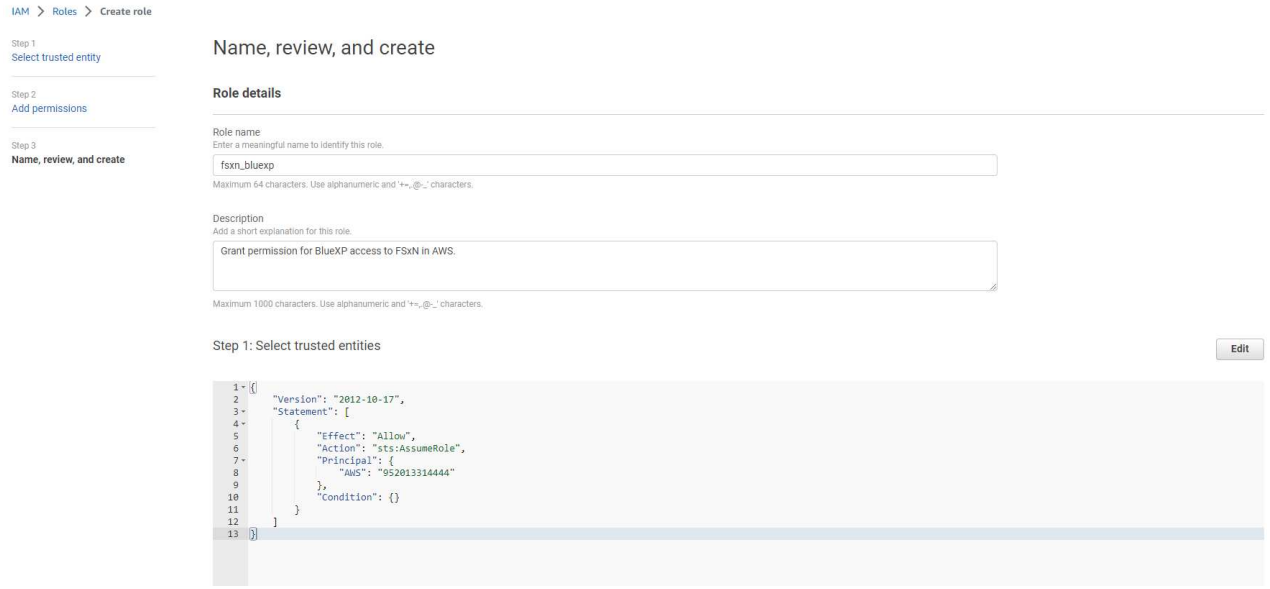
2. Wählen Sie auf der Seite **Vertrauenswürdige Entität auswählen AWS-Konto**, **Anderes AWS-Konto** und fügen Sie die BlueXP -Konto-ID ein, die von der BlueXP Konsole abgerufen werden kann.



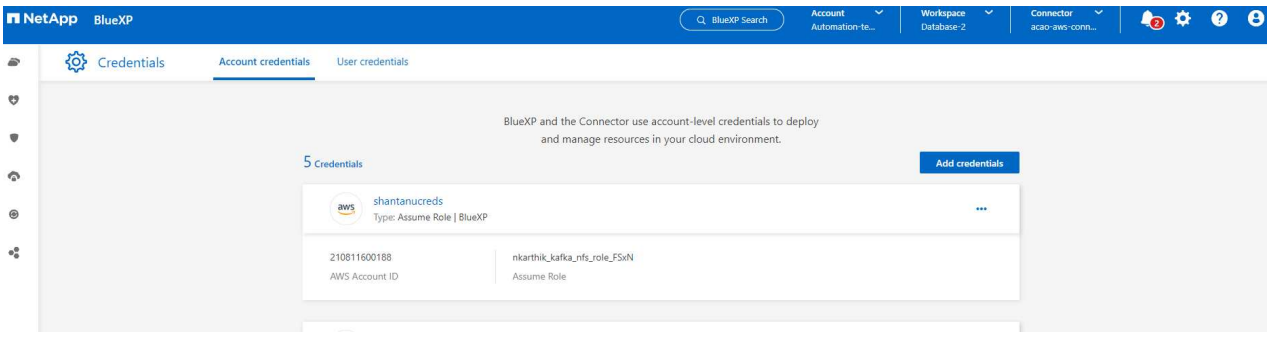
3. Filtern Sie Berechtigungsrichtlinien nach fsx und fügen Sie der Rolle **Berechtigungsrichtlinien** hinzu.



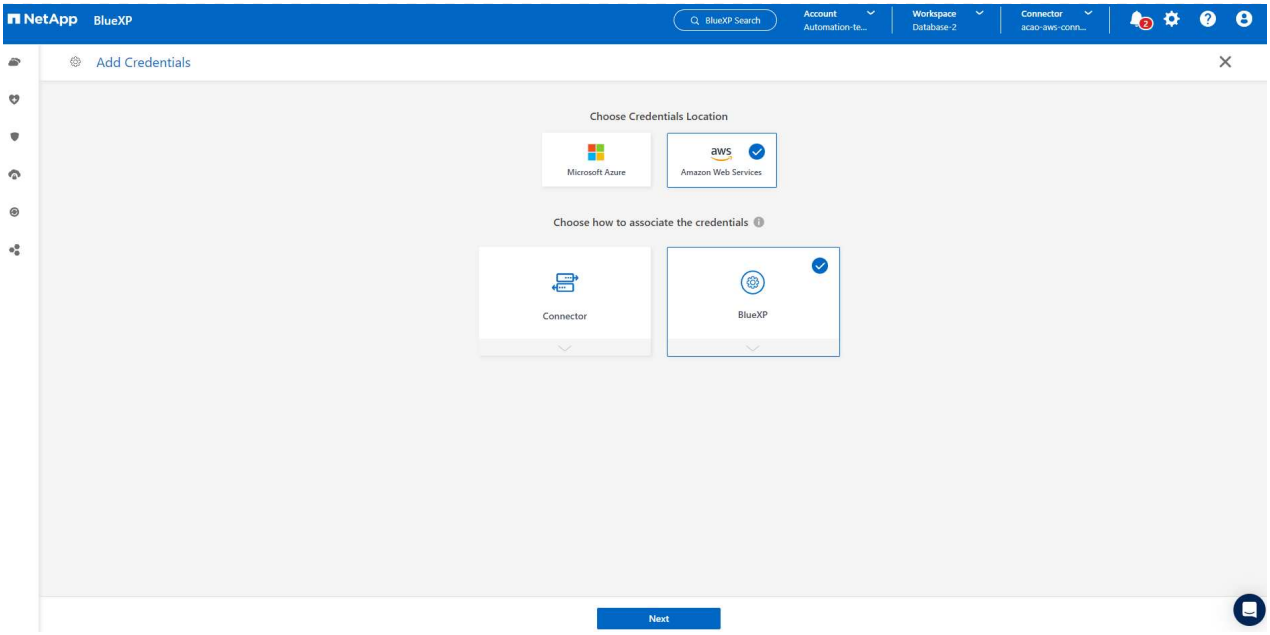
4. Geben Sie auf der Seite **Rollendetails** der Rolle einen Namen, fügen Sie eine Beschreibung hinzu und klicken Sie dann auf **Rolle erstellen**.



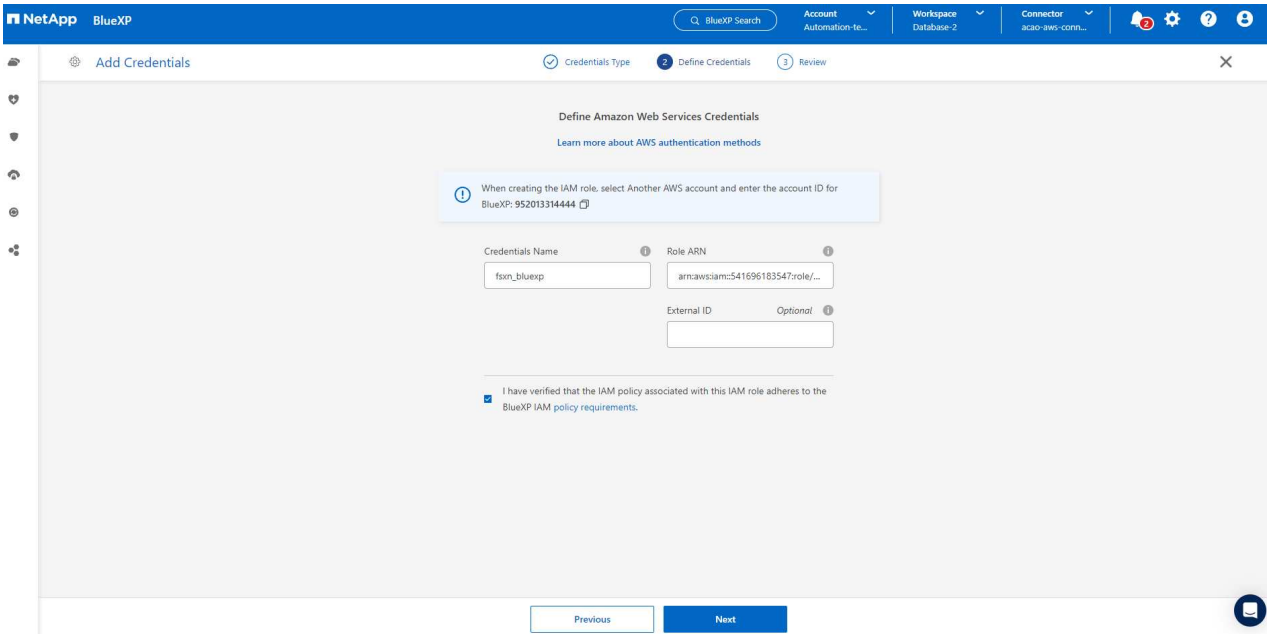
5. Zurück zur BlueXP -Konsole: Klicken Sie auf das Einstellungssymbol in der oberen rechten Ecke der Konsole, um die Seite **Kontoanmeldeinformationen** zu öffnen. Klicken Sie auf **Anmeldeinformationen hinzufügen**, um den Workflow zur Anmeldeinformationskonfiguration zu starten.



6. Wählen Sie den Anmeldeinformationsort als **Amazon Web Services – BlueXP**.

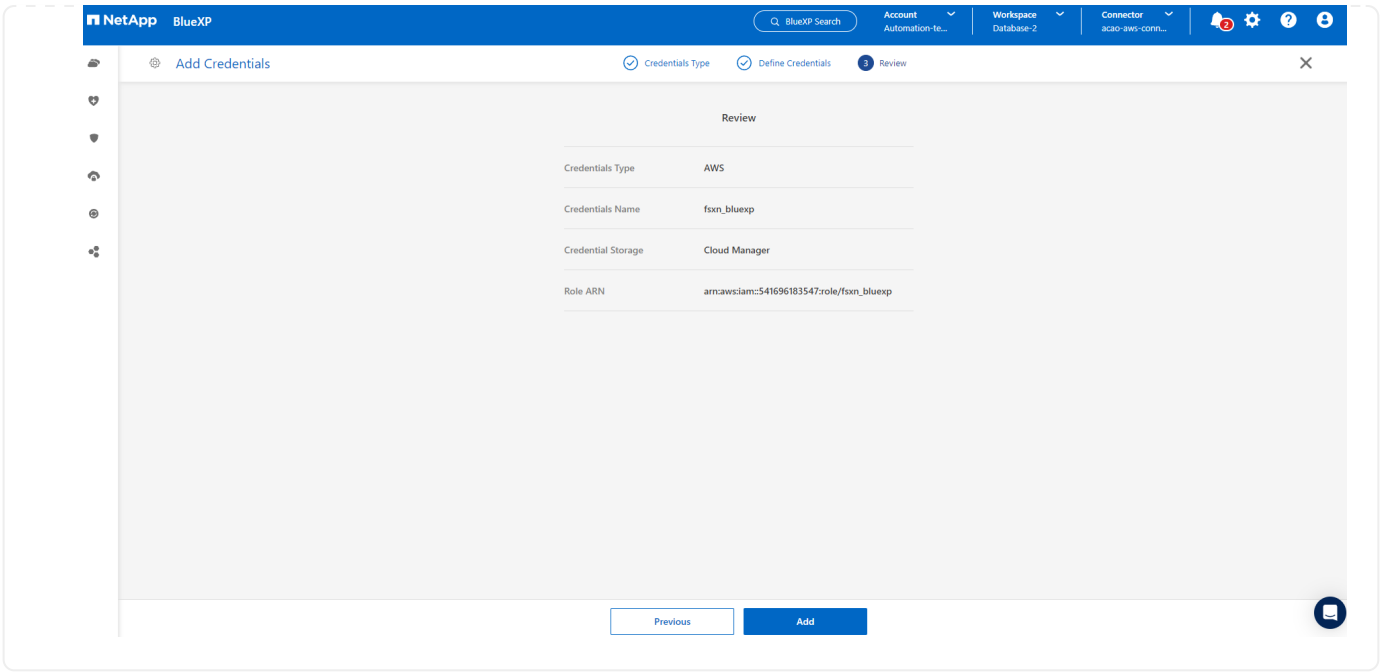


7. Definieren Sie AWS-Anmeldeinformationen mit der richtigen **Rollen-ARN**, die aus der im ersten Schritt oben erstellten AWS-IAM-Rolle abgerufen werden kann. BlueXP **Konto-ID**, die zum Erstellen der AWS IAM-Rolle in Schritt 1 verwendet wird.



8. Überprüfen und **Hinzufügen**

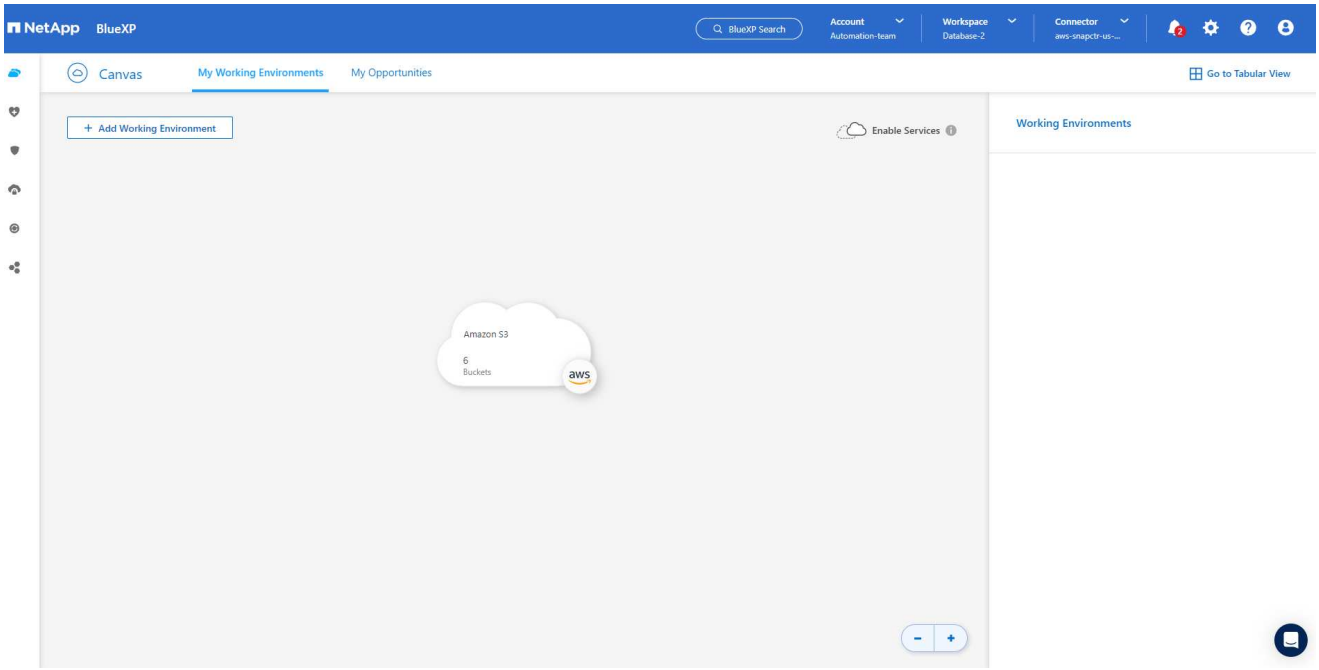
.



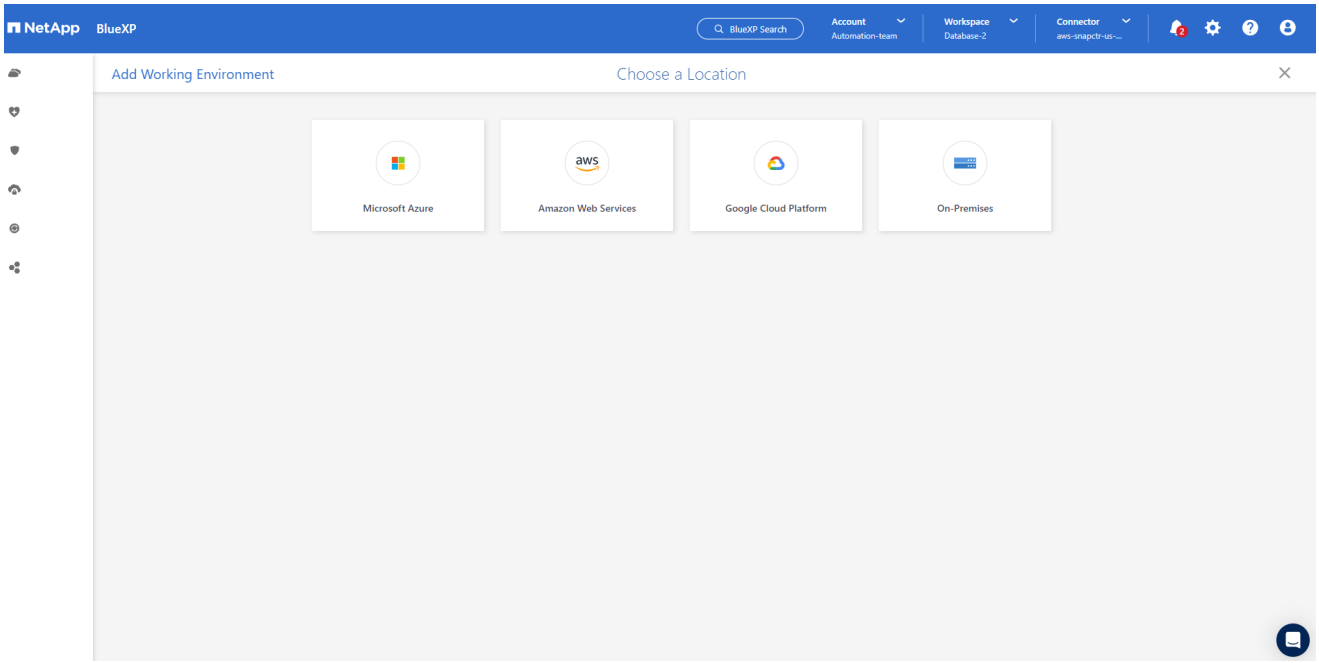
Einrichtung der SnapCenter -Dienste

Nachdem der Connector bereitgestellt und die Anmeldeinformationen hinzugefügt wurden, können die SnapCenter -Dienste nun mit dem folgenden Verfahren eingerichtet werden:

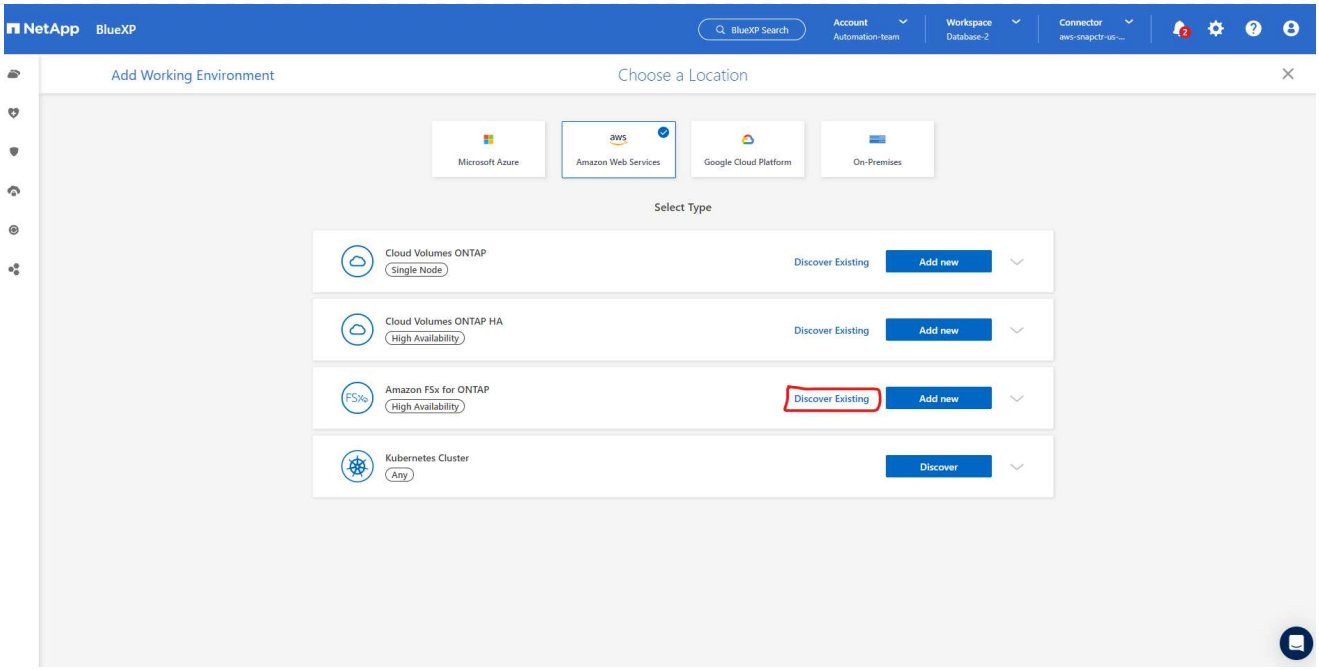
1. Klicken Sie unter **Meine Arbeitsumgebung** auf **Arbeitsumgebung hinzufügen**, um in AWS bereitgestelltes FSx zu entdecken.



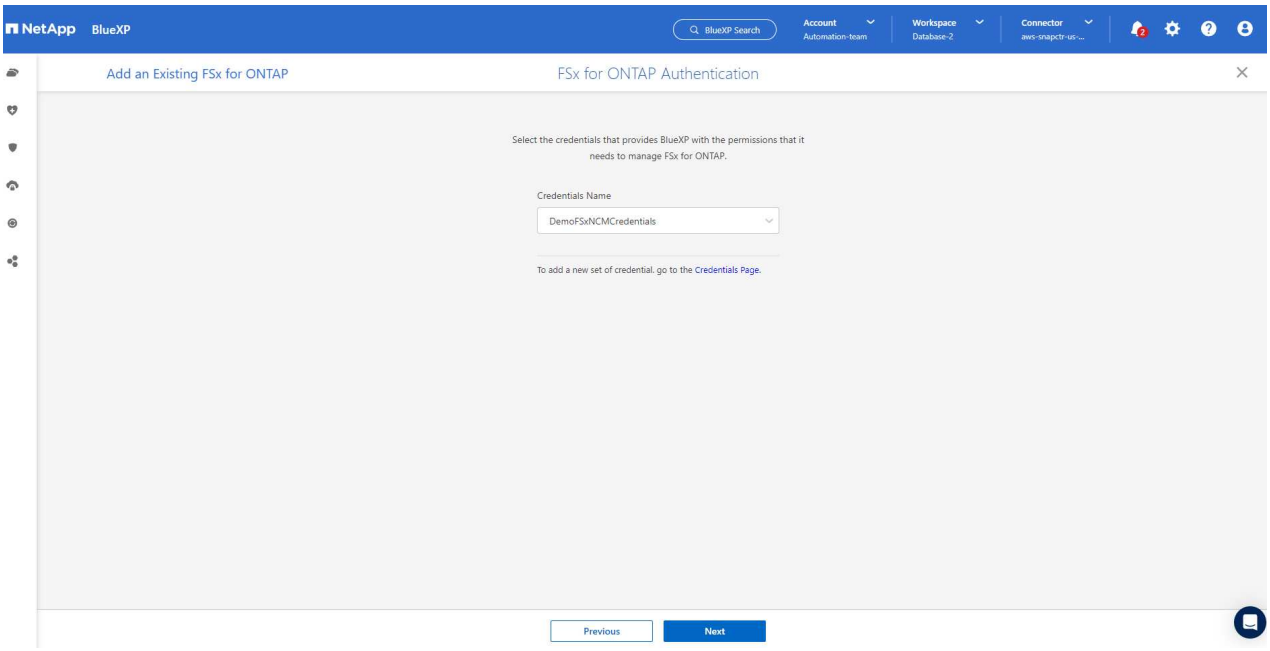
1. Wählen Sie als Standort **Amazon Web Services**.



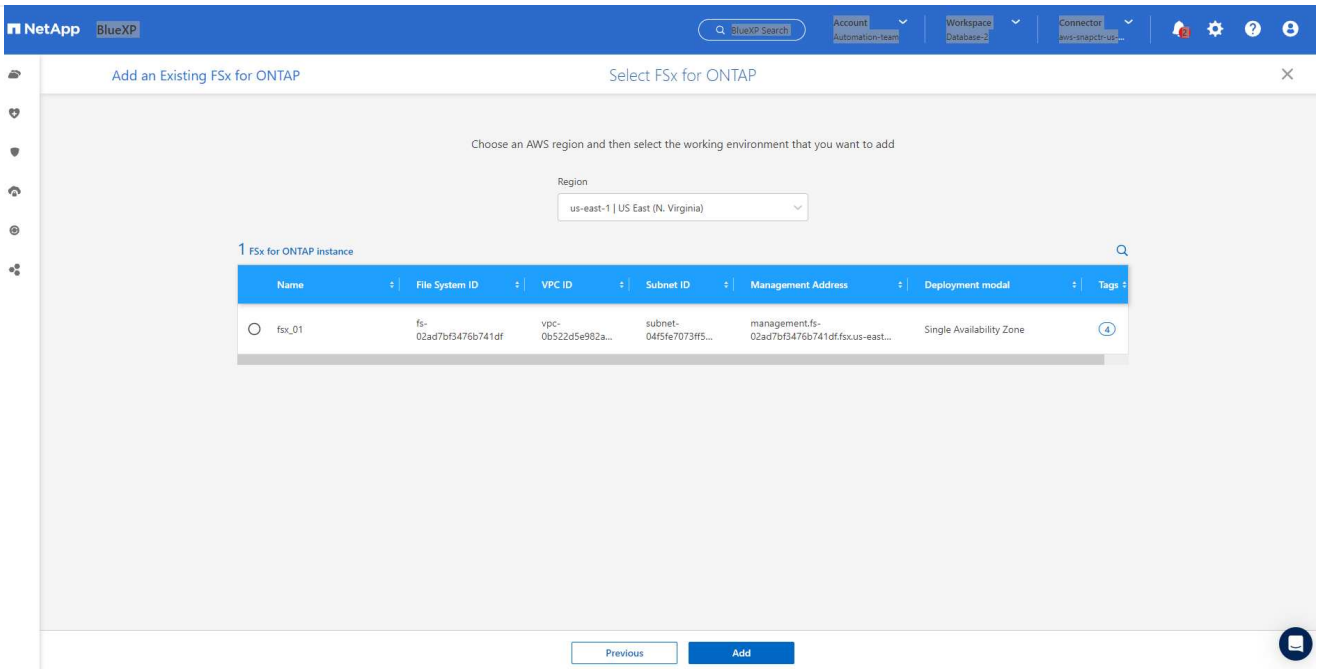
1. Klicken Sie neben * Amazon FSx ONTAP* auf **Vorhandenes erkennen**.



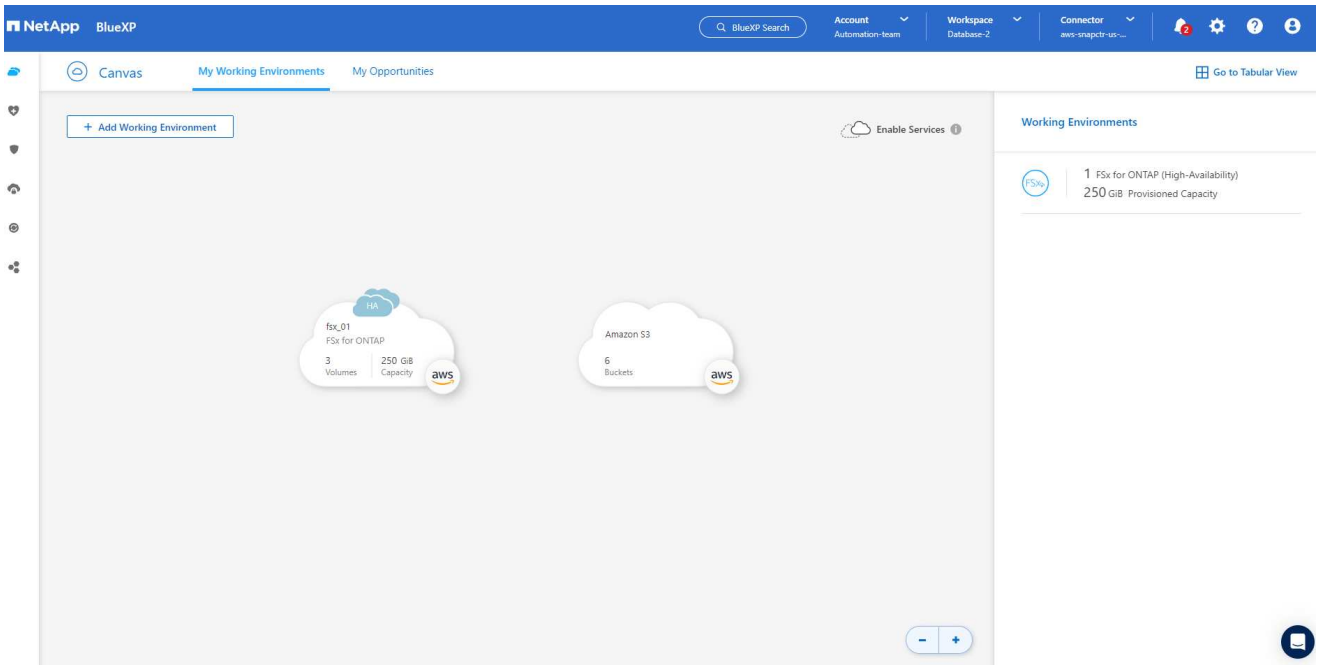
1. Wählen Sie den **Anmeldeinformationsnamen** aus, den Sie im vorherigen Abschnitt erstellt haben, um BlueXP die Berechtigungen zu erteilen, die es zum Verwalten von FSx ONTAP benötigt. Wenn Sie keine Anmeldeinformationen hinzugefügt haben, können Sie diese über das Menü **Einstellungen** in der oberen rechten Ecke der BlueXP -Konsole hinzufügen.



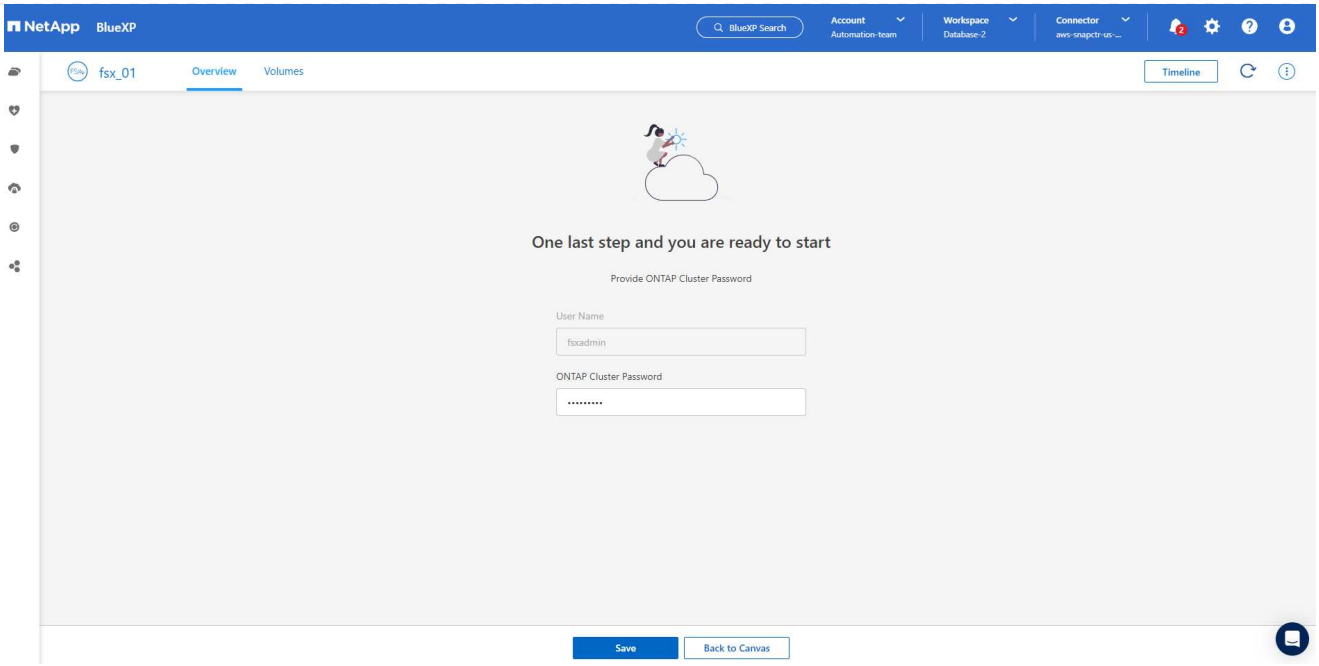
2. Wählen Sie die AWS-Region aus, in der Amazon FSx ONTAP bereitgestellt wird, wählen Sie den FSx-Cluster aus, der die Oracle-Datenbank hostet, und klicken Sie auf „Hinzufügen“.



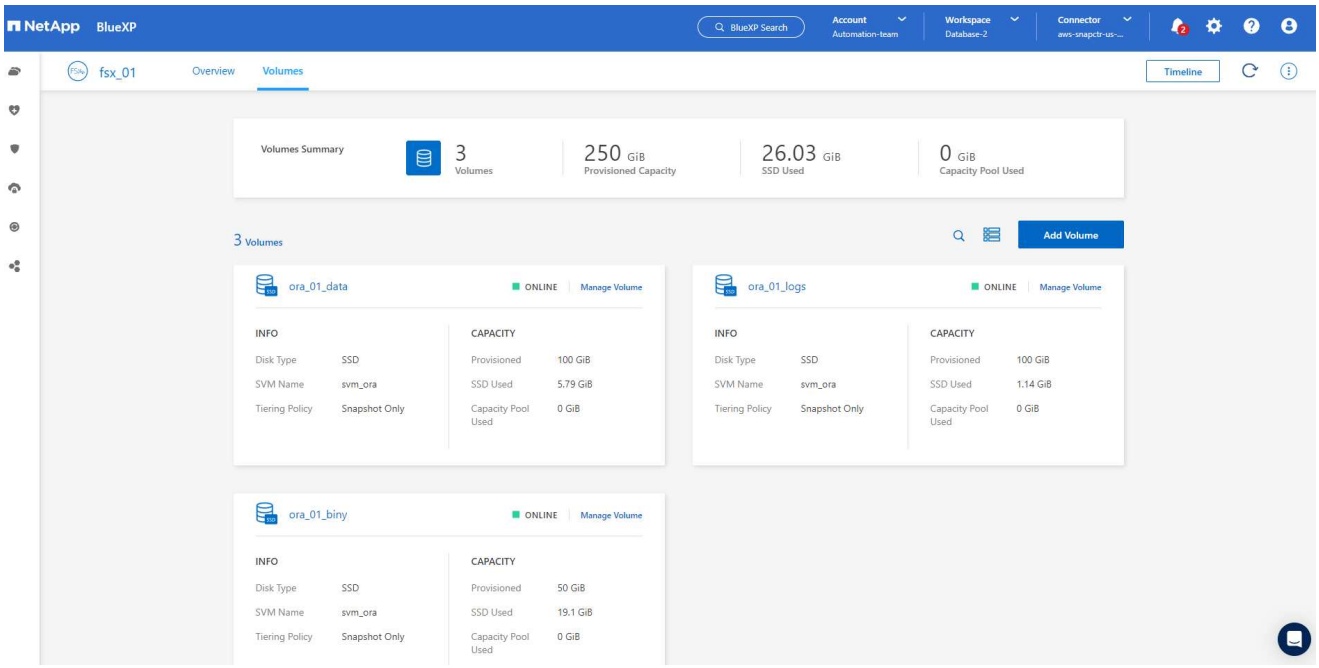
1. Die erkannte Amazon FSx ONTAP -Instanz wird jetzt in der Arbeitsumgebung angezeigt.



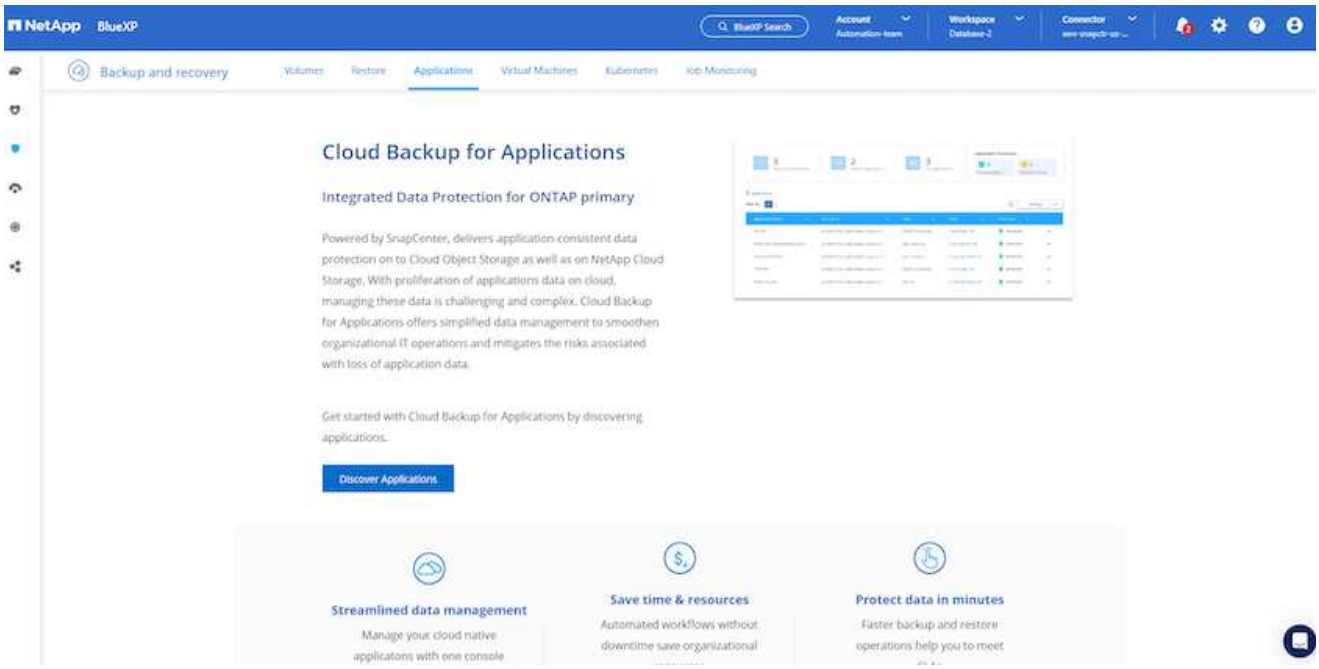
1. Sie können sich mit den Anmeldeinformationen Ihres fsxadmin-Kontos beim FSx-Cluster anmelden.



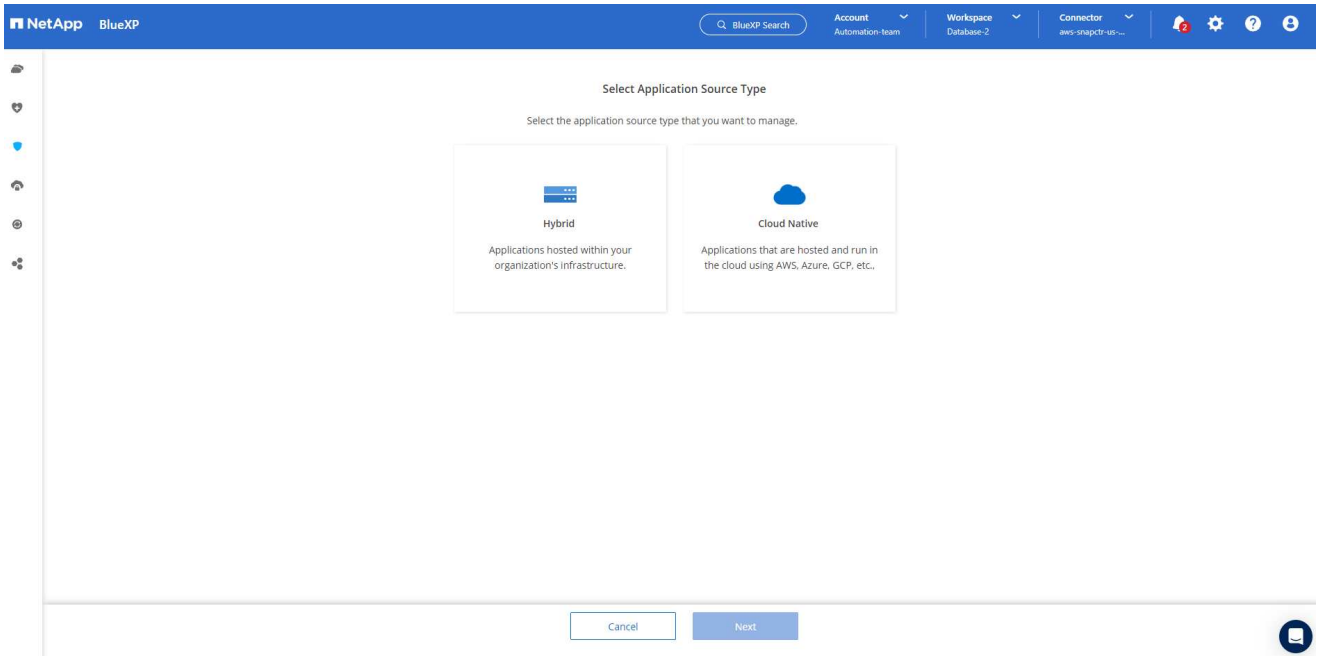
1. Nachdem Sie sich bei Amazon FSx ONTAP angemeldet haben, überprüfen Sie Ihre Datenbankspeicherinformationen (z. B. Datenbankvolumes).



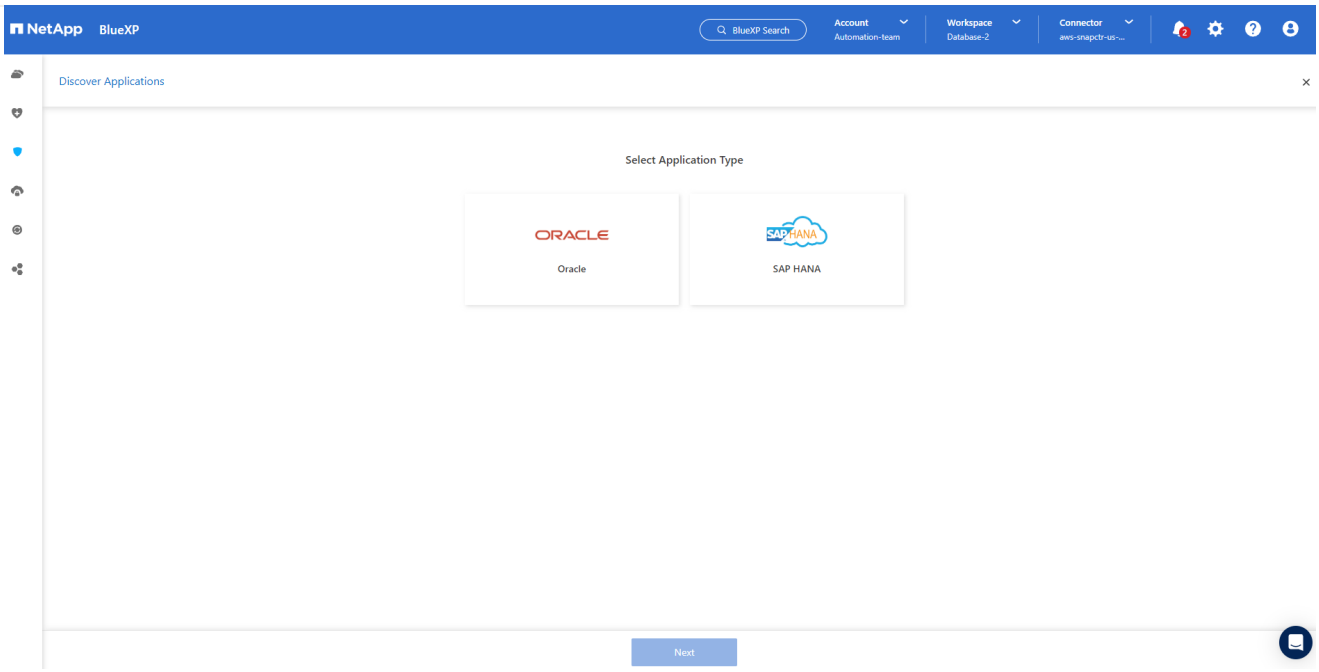
1. Bewegen Sie in der linken Seitenleiste der Konsole den Mauszeiger über das Schutzsymbol und klicken Sie dann auf **Schutz** > **Anwendungen**, um die Startseite „Anwendungen“ zu öffnen. Klicken Sie auf **Anwendungen erkennen**.



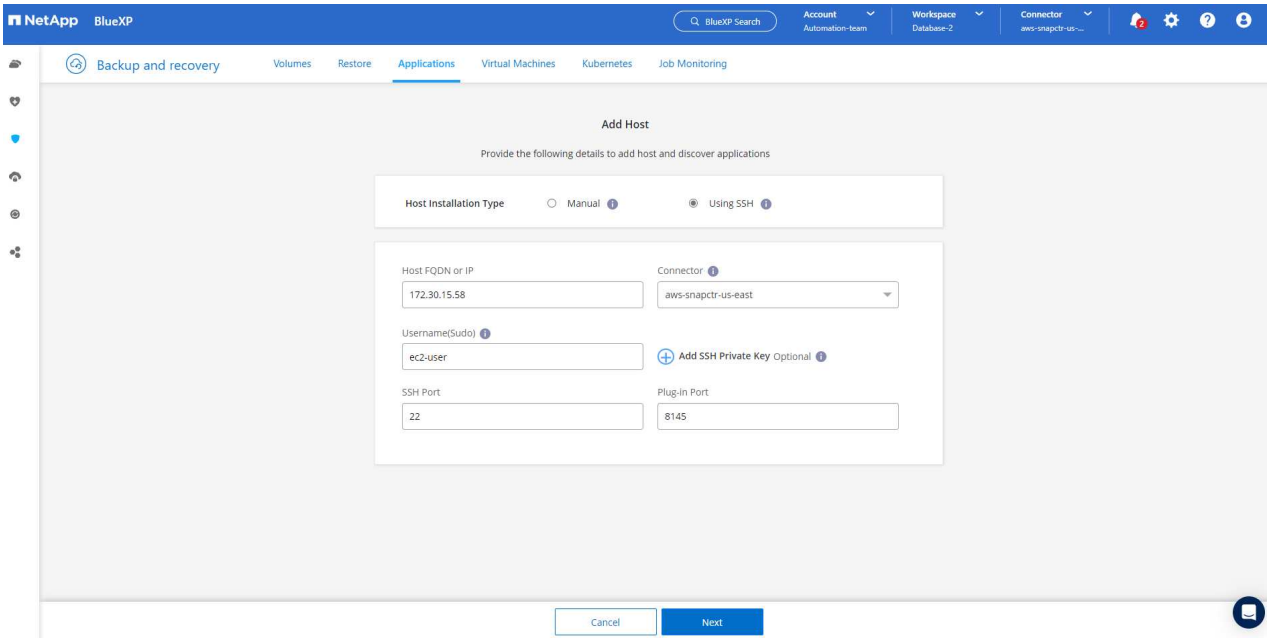
1. Wählen Sie **Cloud Native** als Anwendungsquelltyp.



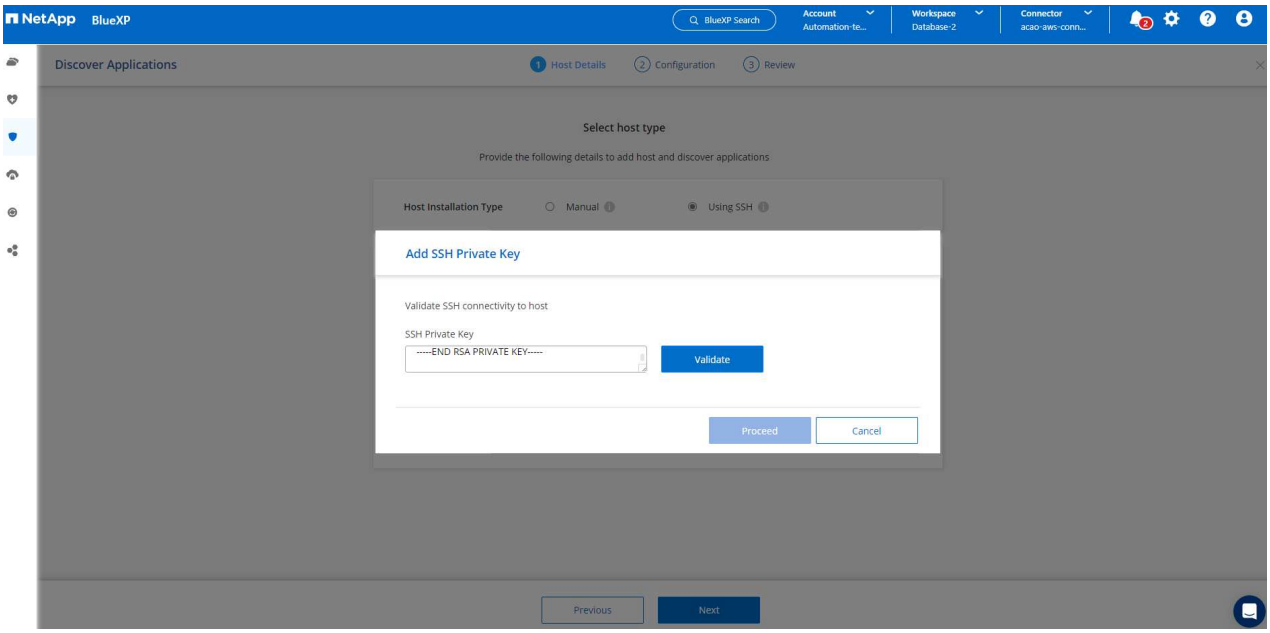
1. Wählen Sie **Oracle** als Anwendungstyp.



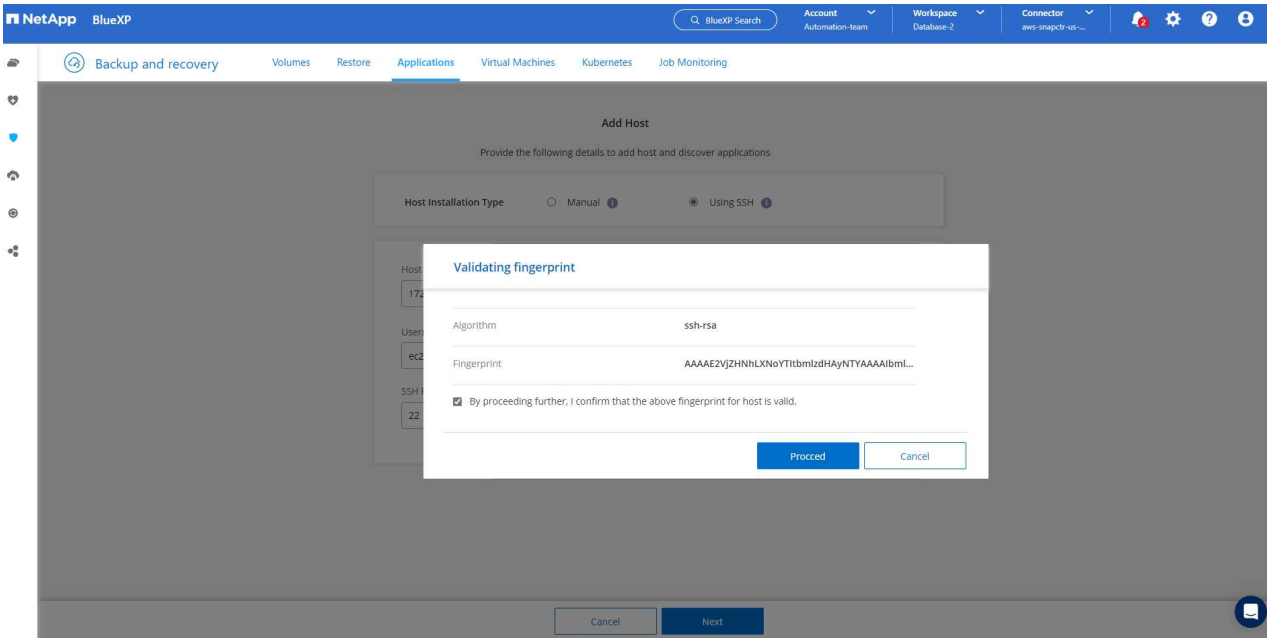
1. Geben Sie die Hostdetails der AWS EC2 Oracle-Anwendung ein. Wählen Sie **SSH verwenden** als **Host-Installationstyp** für die Plug-in-Installation und Datenbankerkennung in einem Schritt. Klicken Sie dann auf **Privaten SSH-Schlüssel hinzufügen**.



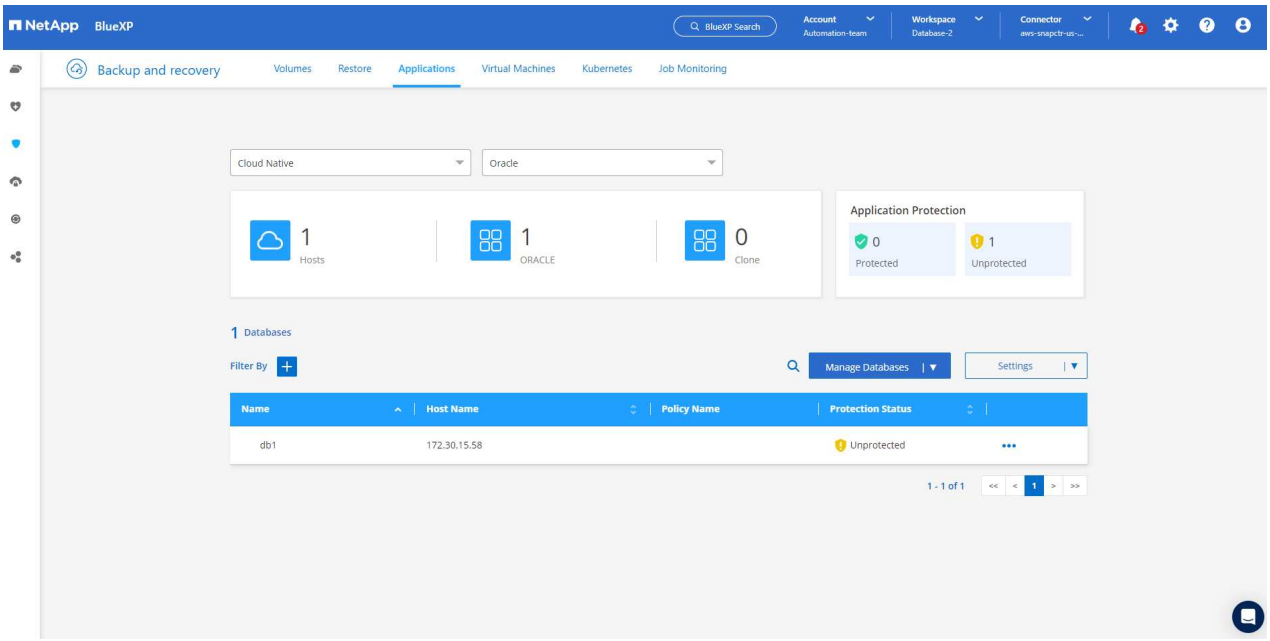
2. Fügen Sie Ihren EC2-Benutzer-SSH-Schlüssel für den EC2-Datenbankhost ein und klicken Sie auf **Validieren**, um fortzufahren.



3. Um fortzufahren, werden Sie aufgefordert, den **Fingerabdruck zu validieren**.



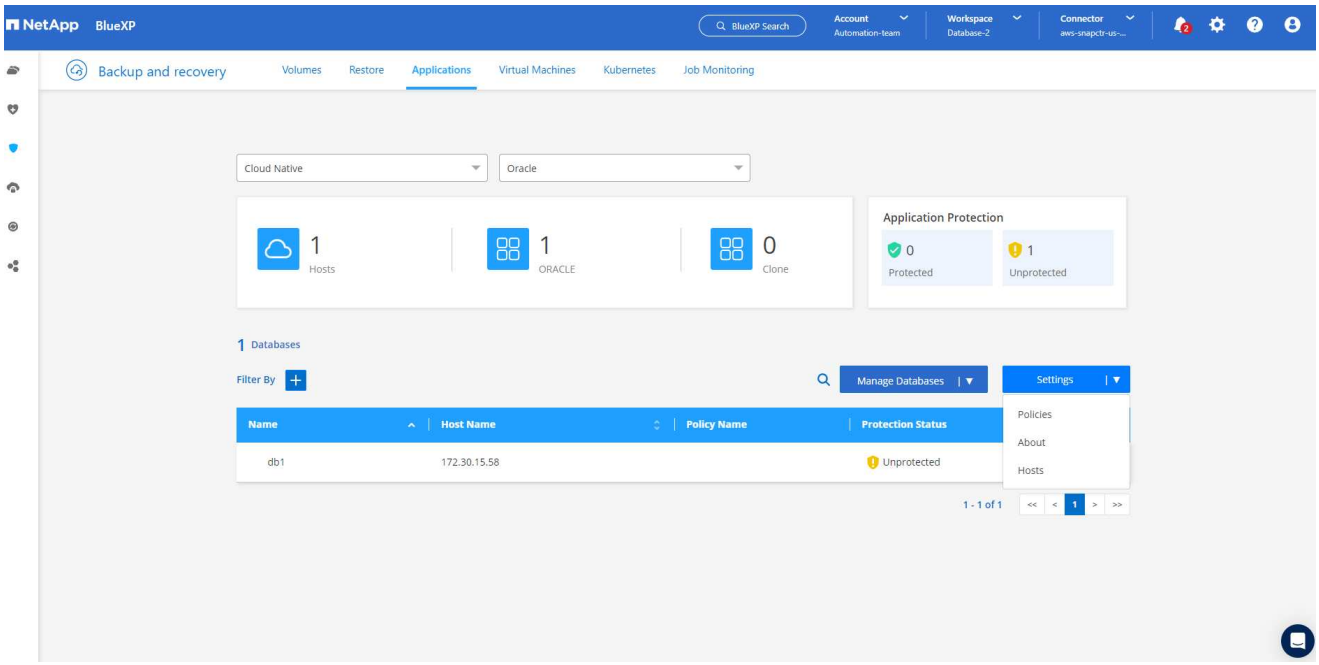
4. Klicken Sie auf **Weiter**, um ein Oracle-Datenbank-Plugin zu installieren und die Oracle-Datenbanken auf dem EC2-Host zu ermitteln. Erkannte Datenbanken werden zu **Anwendungen** hinzugefügt. Der **Schutzstatus** der Datenbank wird bei der ersten Erkennung als **Ungeschützt** angezeigt.



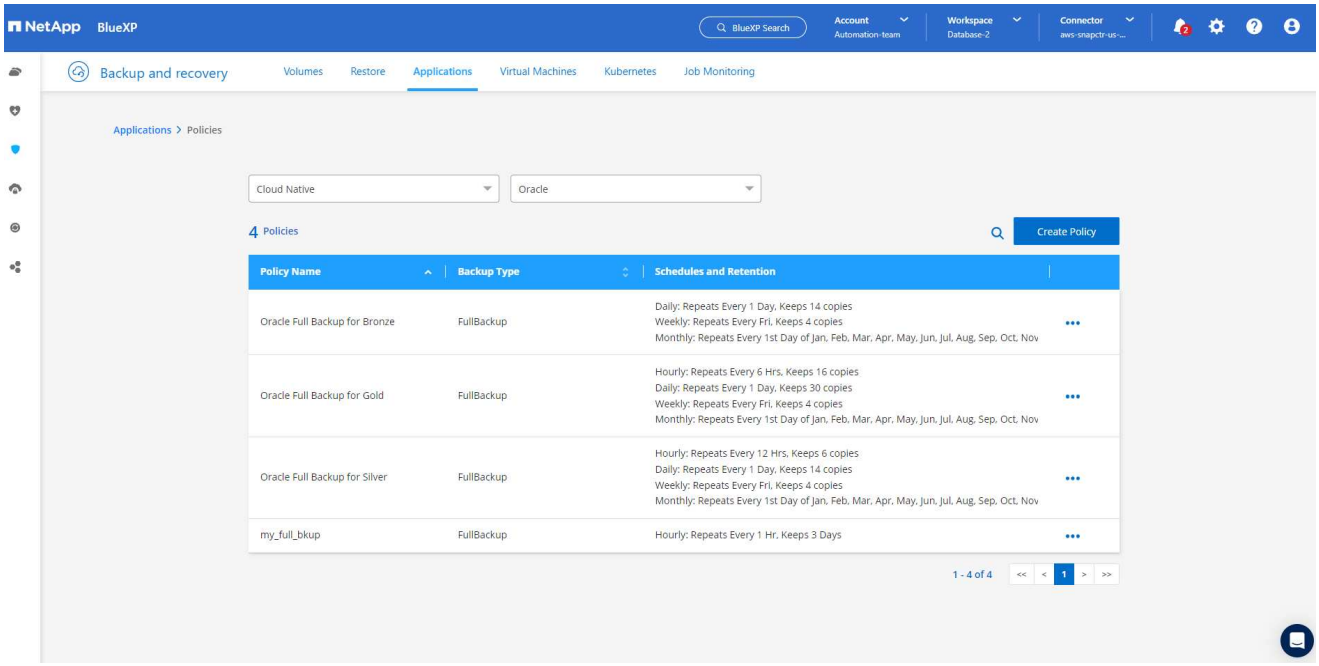
Damit ist die Ersteinrichtung der SnapCenter -Dienste für Oracle abgeschlossen. In den nächsten drei Abschnitten dieses Dokuments werden Sicherungs-, Wiederherstellungs- und Klonvorgänge für Oracle-Datenbanken beschrieben.

Oracle-Datenbanksicherung

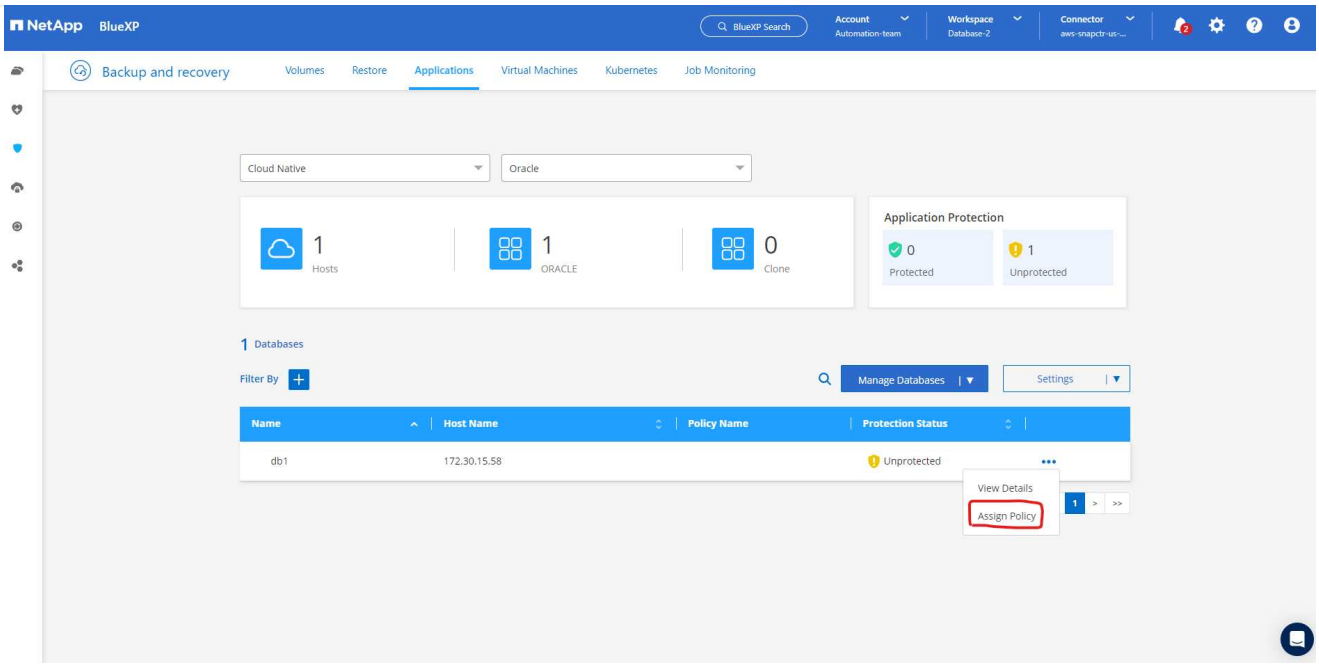
1. Klicken Sie auf die drei Punkte neben dem **Schutzstatus** der Datenbank und dann auf **Richtlinien**, um die standardmäßig vorinstallierten Datenbankschutzrichtlinien anzuzeigen, die zum Schutz Ihrer Oracle-Datenbanken angewendet werden können.



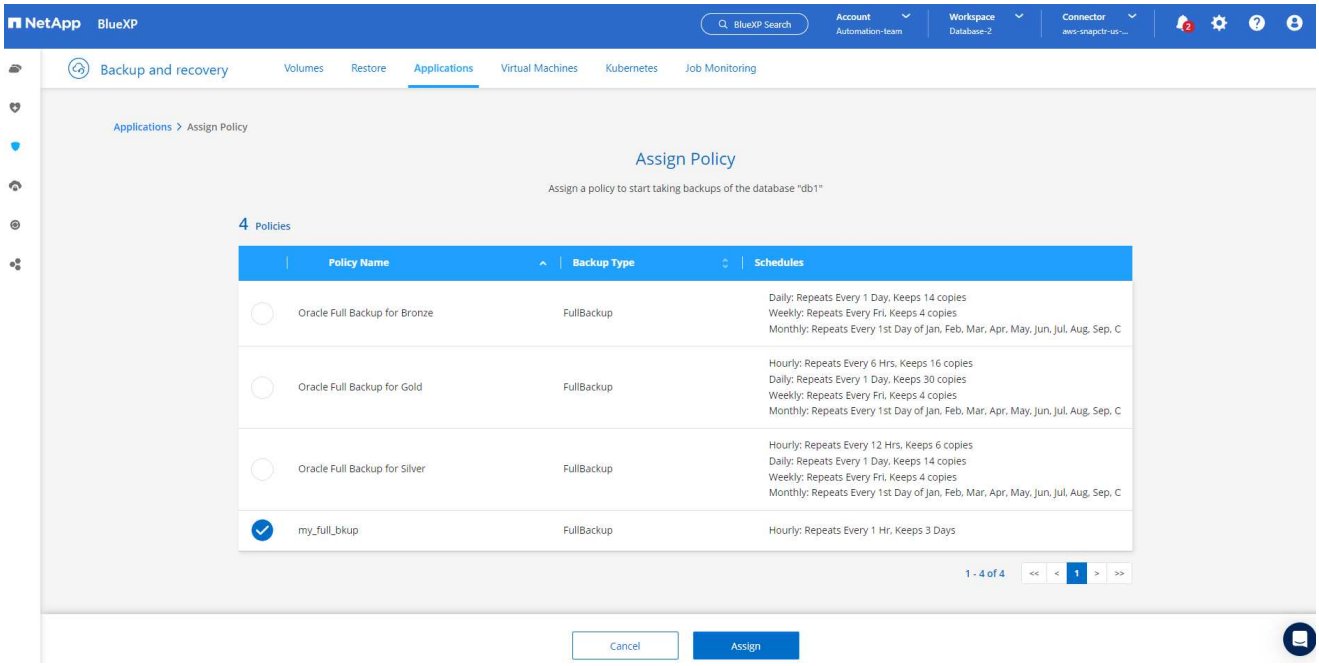
1. Sie können auch Ihre eigene Richtlinie mit einer benutzerdefinierten Sicherungshäufigkeit und einem benutzerdefinierten Aufbewahrungsfenster für Sicherungsdaten erstellen.



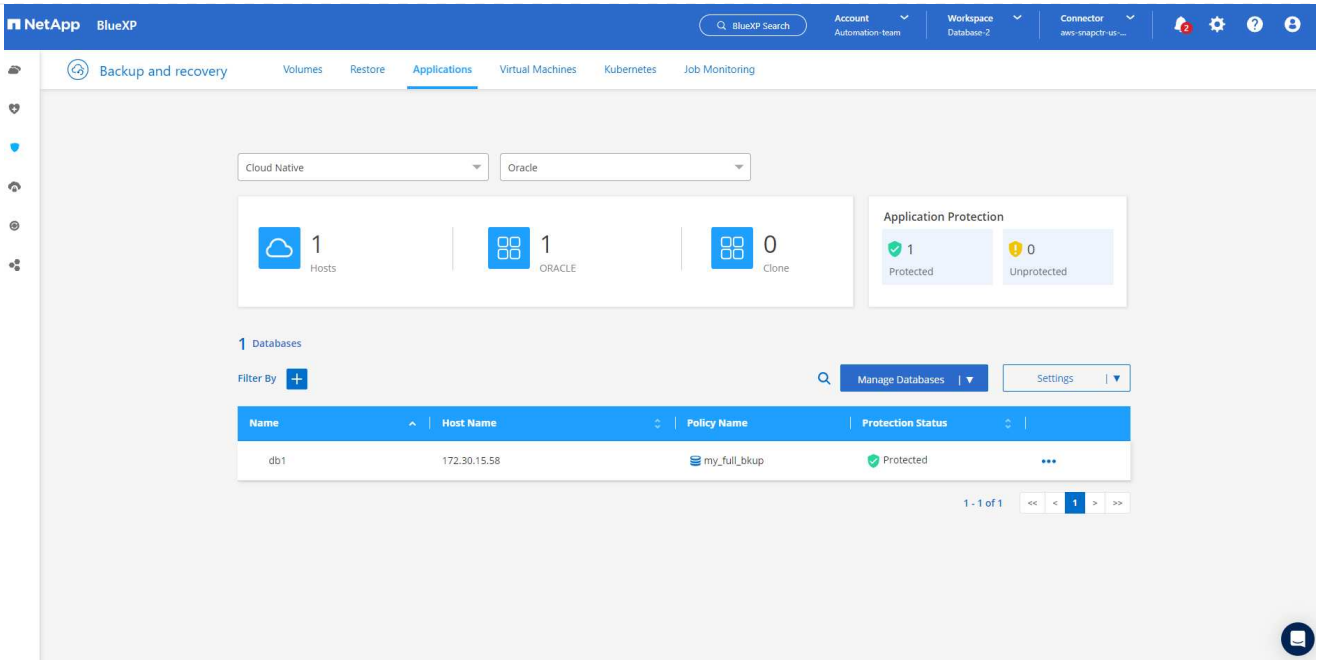
1. Wenn Sie mit der Richtlinienkonfiguration zufrieden sind, können Sie die gewünschte Richtlinie zum Schutz der Datenbank zuweisen.



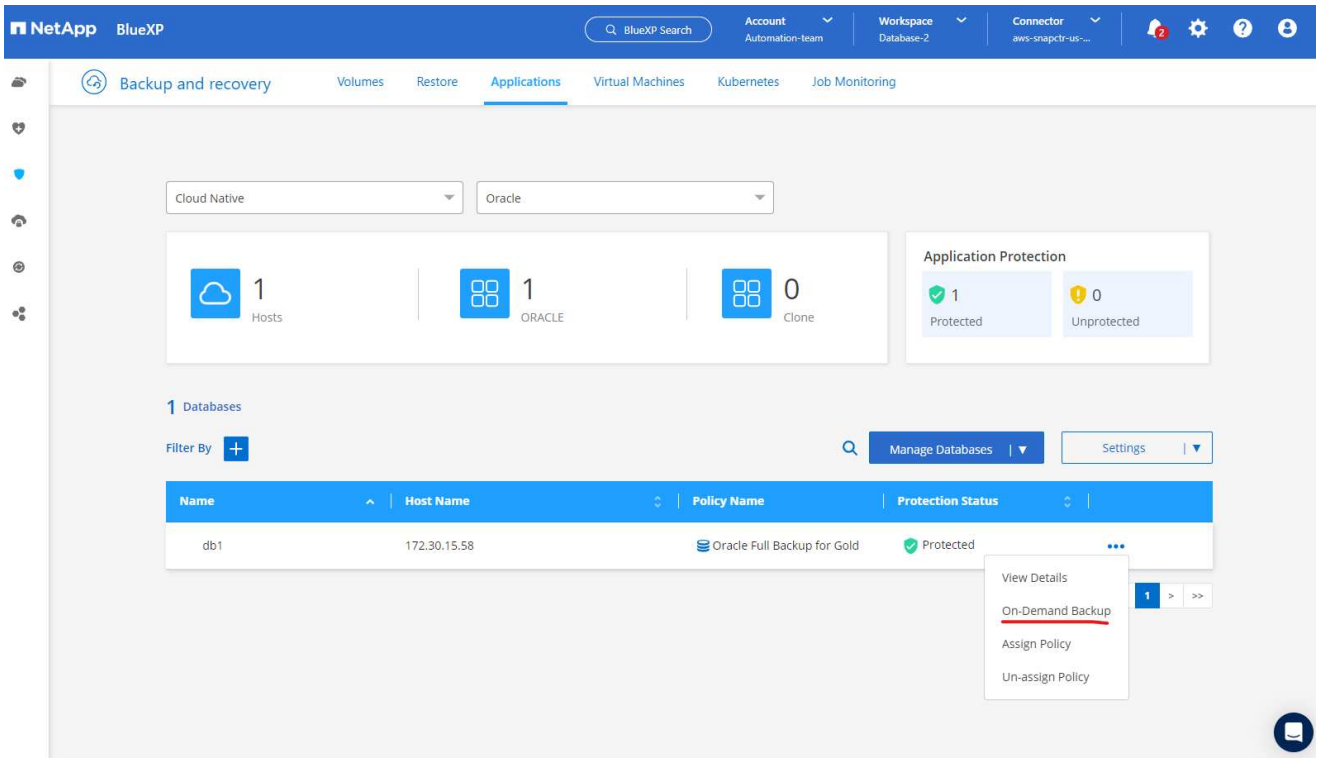
1. Wählen Sie die Richtlinie aus, die der Datenbank zugewiesen werden soll.



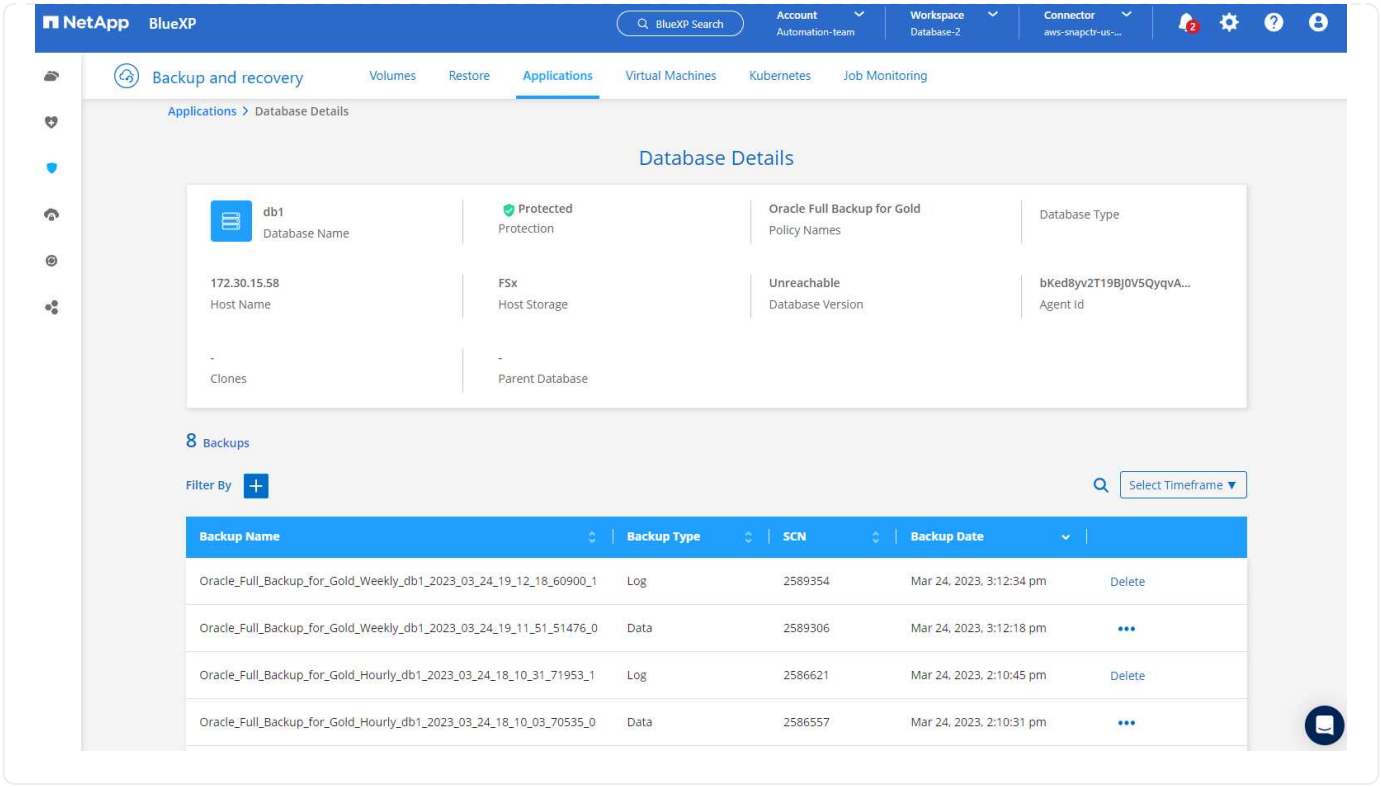
1. Nachdem die Richtlinie angewendet wurde, ändert sich der Datenbankschutzstatus in **Geschützt** mit einem grünen Häkchen.



1. Die Datenbanksicherung wird nach einem vordefinierten Zeitplan ausgeführt. Sie können auch eine einmalige On-Demand-Sicherung ausführen, wie unten gezeigt.

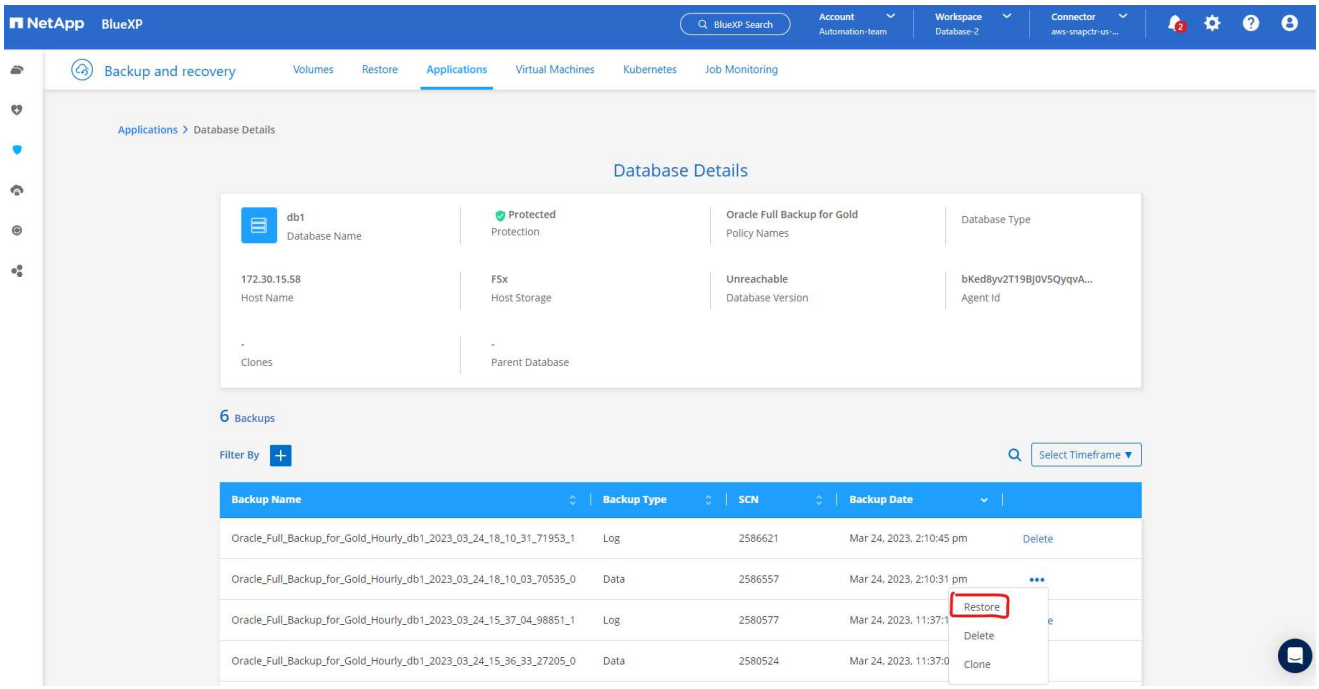


1. Die Details der Datenbanksicherungen können angezeigt werden, indem Sie in der Menüliste auf **Details anzeigen** klicken. Dazu gehören der Sicherungsname, der Sicherungstyp, die SCN und das Sicherungsdatum. Ein Sicherungssatz umfasst einen Snapshot sowohl für das Datenvolumen als auch für das Protokollvolumen. Ein Protokollvolume-Snapshot wird direkt nach einem Datenbankvolume-Snapshot durchgeführt. Sie können einen Filter anwenden, wenn Sie in einer langen Liste nach einem bestimmten Backup suchen.

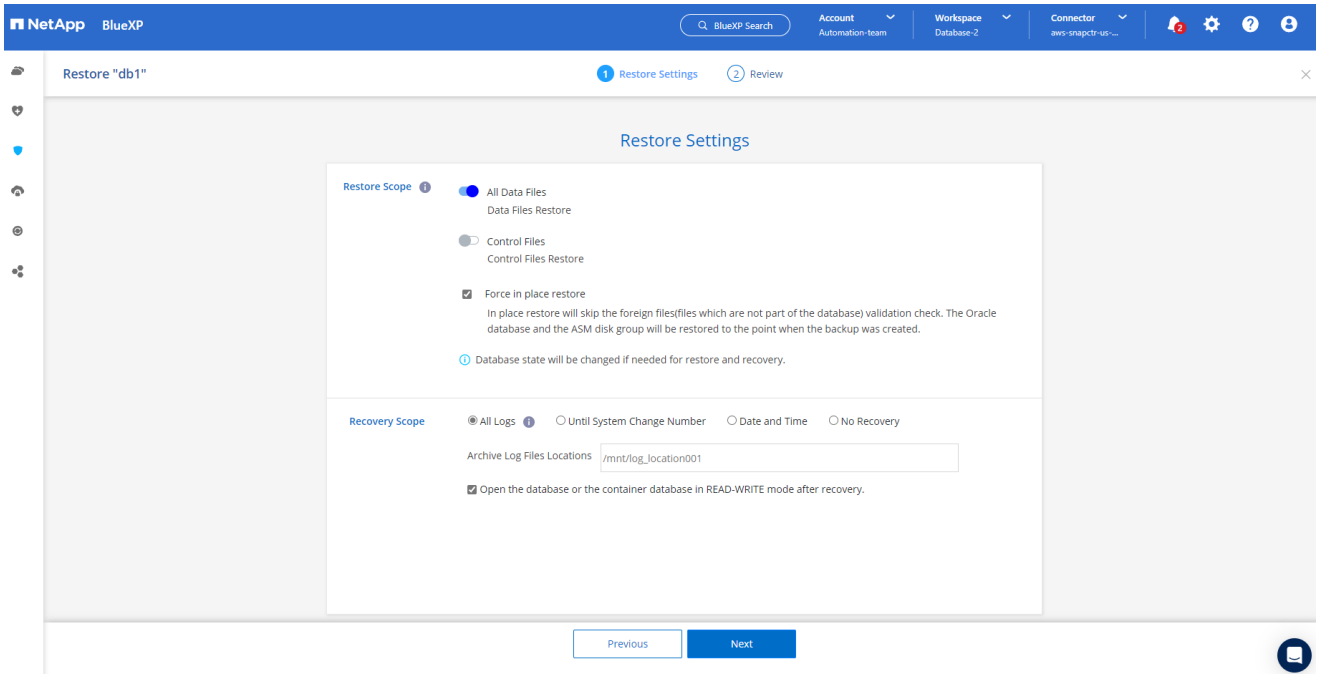


Wiederherstellung und Wiederherstellung von Oracle-Datenbanken

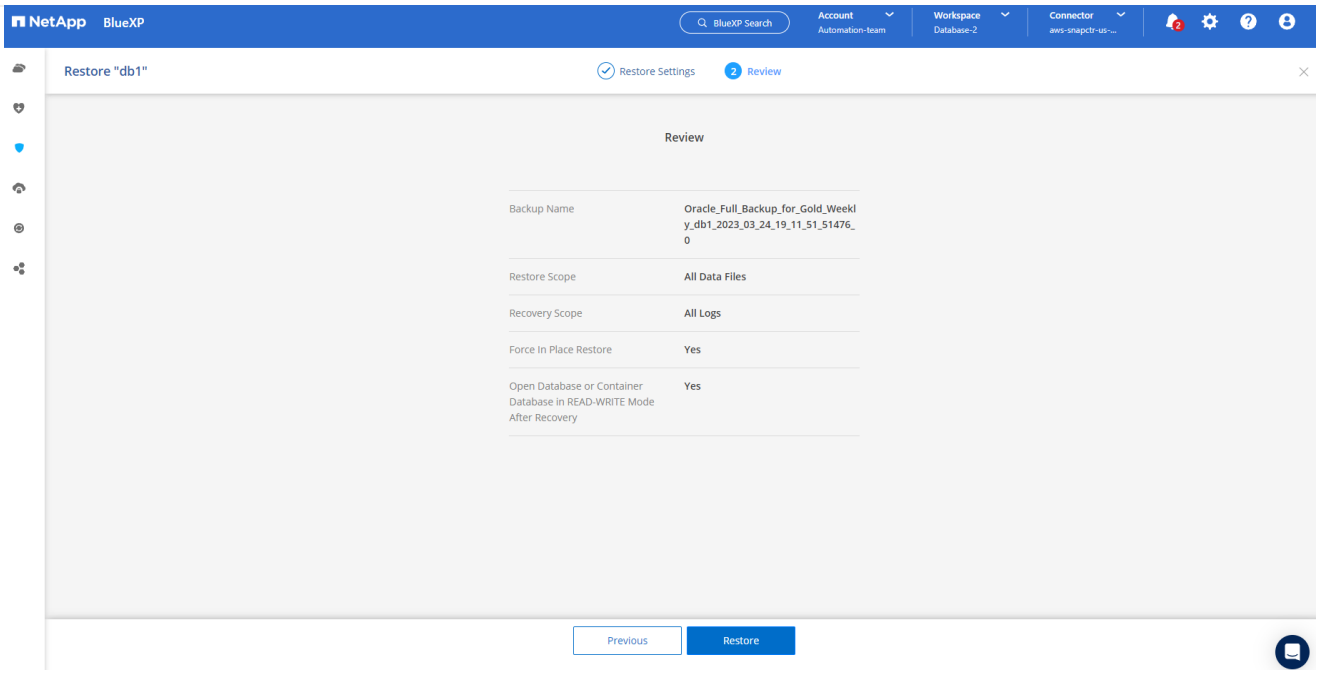
1. Wählen Sie für eine Datenbankwiederherstellung das richtige Backup, entweder nach SCN oder Backup-Zeit. Klicken Sie auf die drei Punkte in der Datenbankdatensicherung und dann auf **Wiederherstellen**, um die Wiederherstellung und Wiederherstellung der Datenbank zu starten.



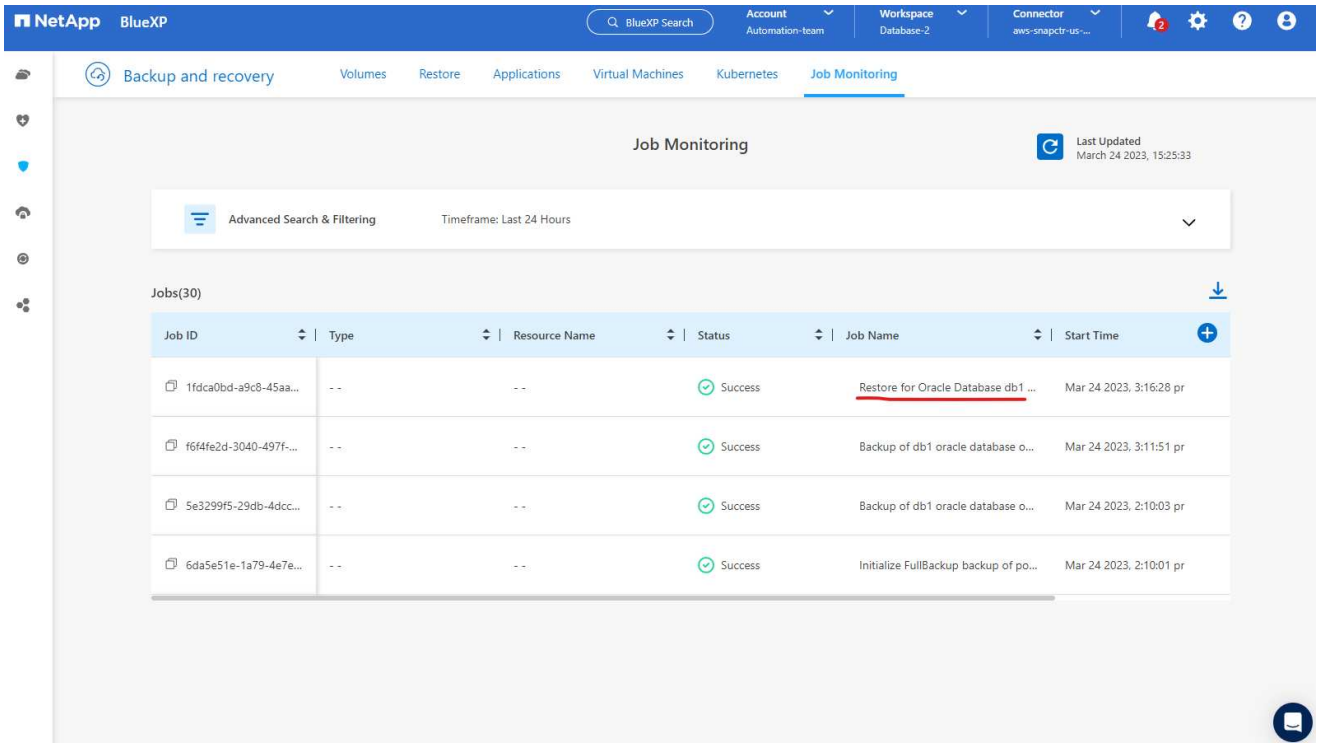
1. Wählen Sie Ihre Wiederherstellungseinstellung. Wenn Sie sicher sind, dass sich nach der Sicherung nichts an der physischen Datenbankstruktur geändert hat (z. B. das Hinzufügen einer Datendatei oder einer Datenträgergruppe), können Sie die Option **Force in place restore** verwenden, die im Allgemeinen schneller ist. Andernfalls aktivieren Sie dieses Kontrollkästchen nicht.

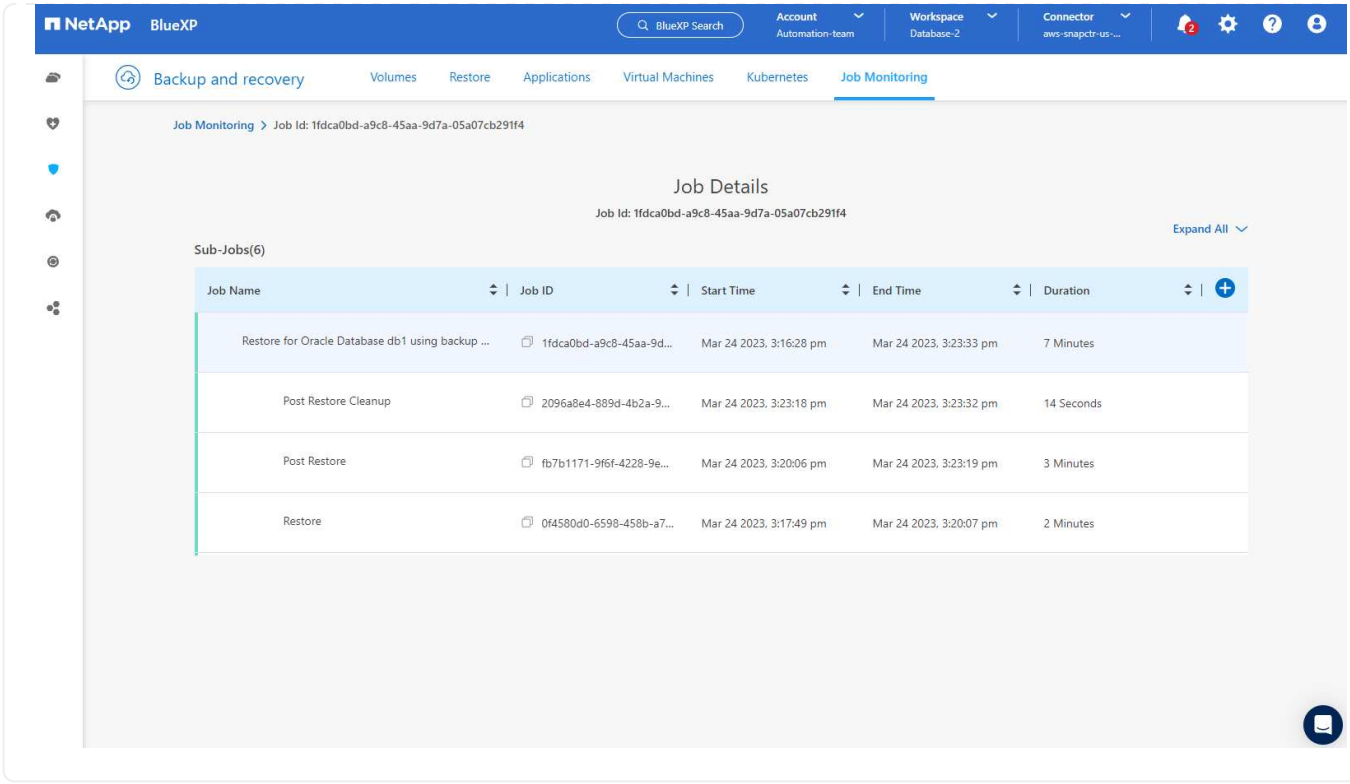


1. Überprüfen und starten Sie die Wiederherstellung und Wiederherstellung der Datenbank.



1. Auf der Registerkarte **Jobüberwachung** können Sie den Status des Wiederherstellungsjobs sowie alle Details während der Ausführung anzeigen.

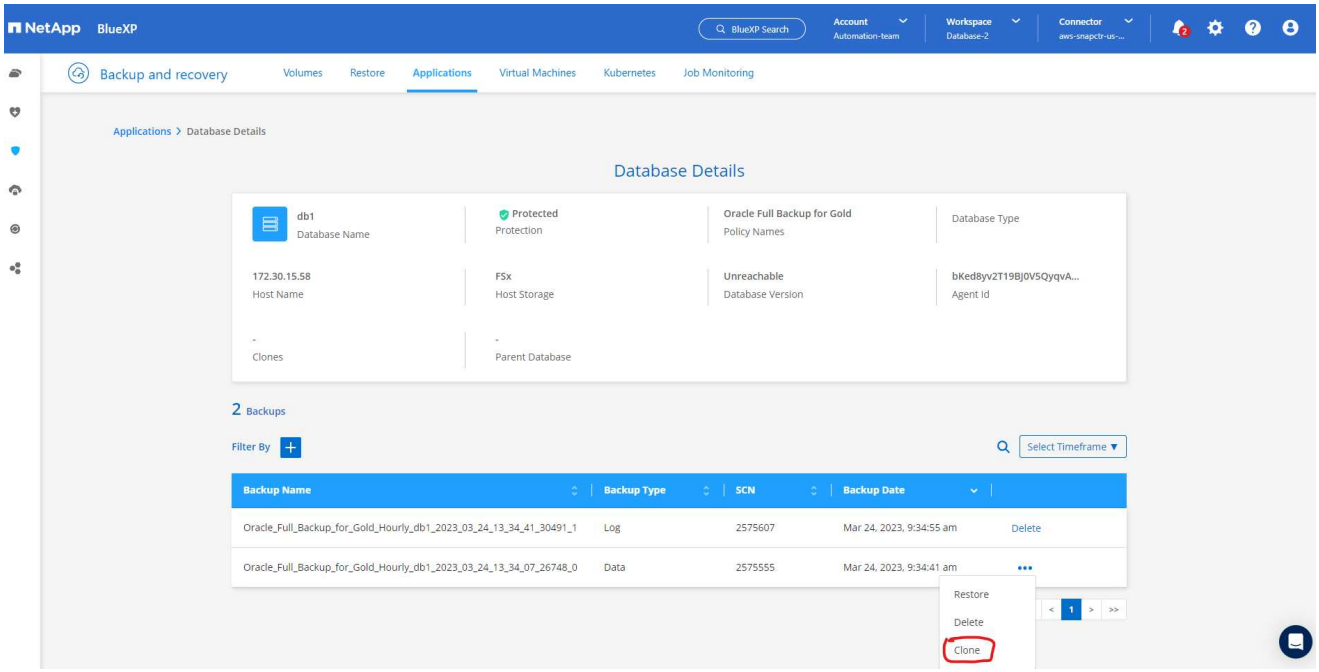




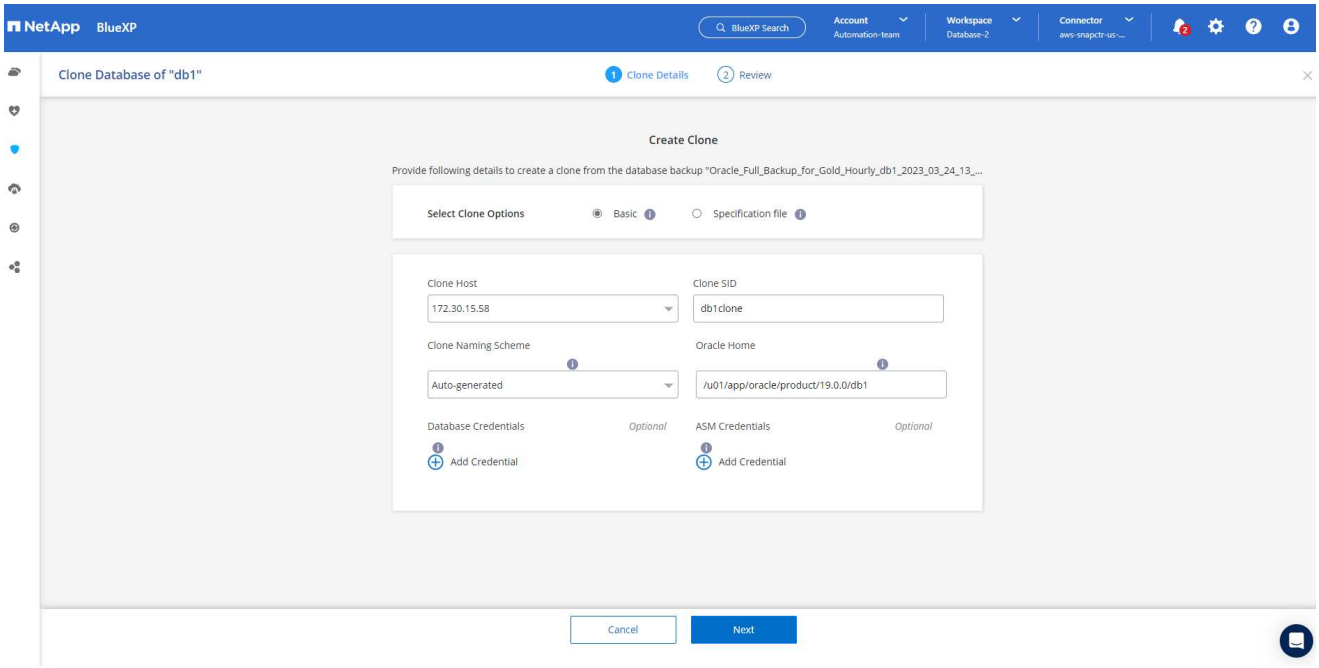
Oracle-Datenbankklon

Um eine Datenbank zu klonen, starten Sie den Klon-Workflow von derselben Detailseite der Datenbanksicherung.

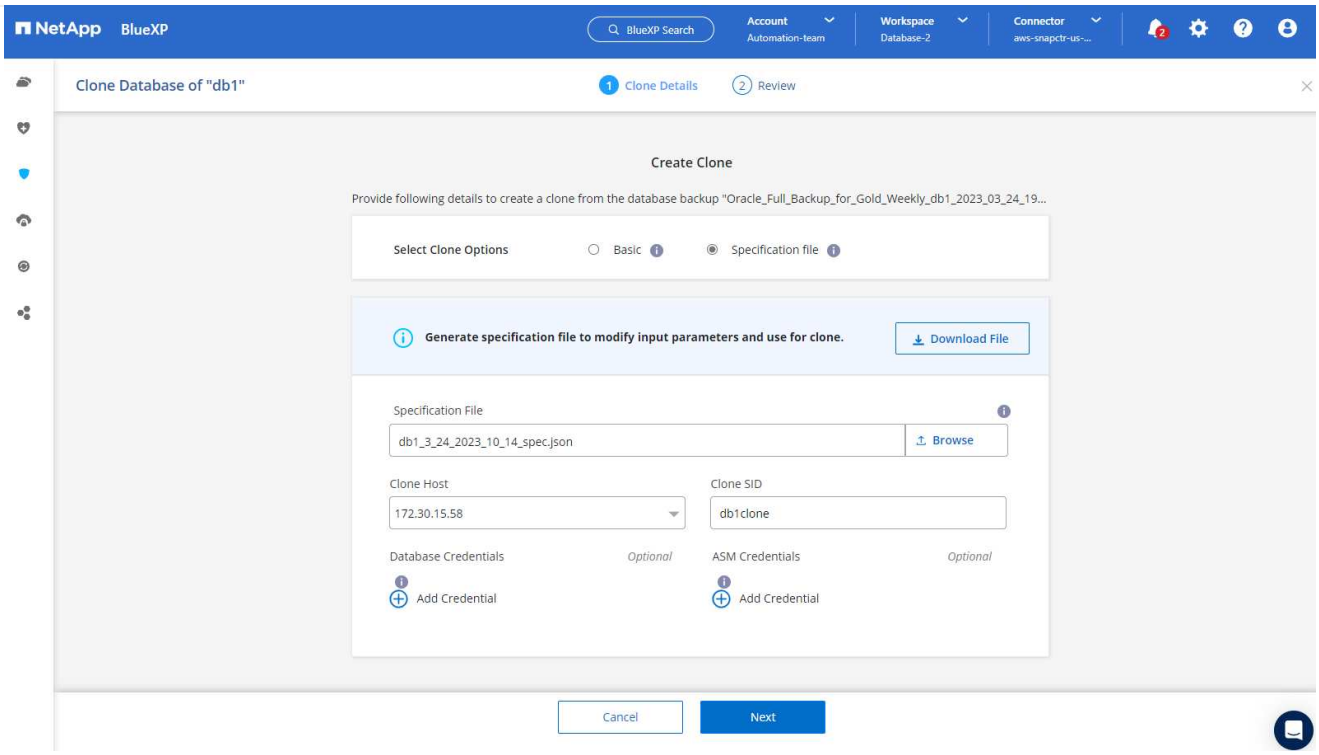
1. Wählen Sie die richtige Datenbanksicherungskopie aus, klicken Sie auf die drei Punkte, um das Menü anzuzeigen, und wählen Sie die Option **Klonen**.



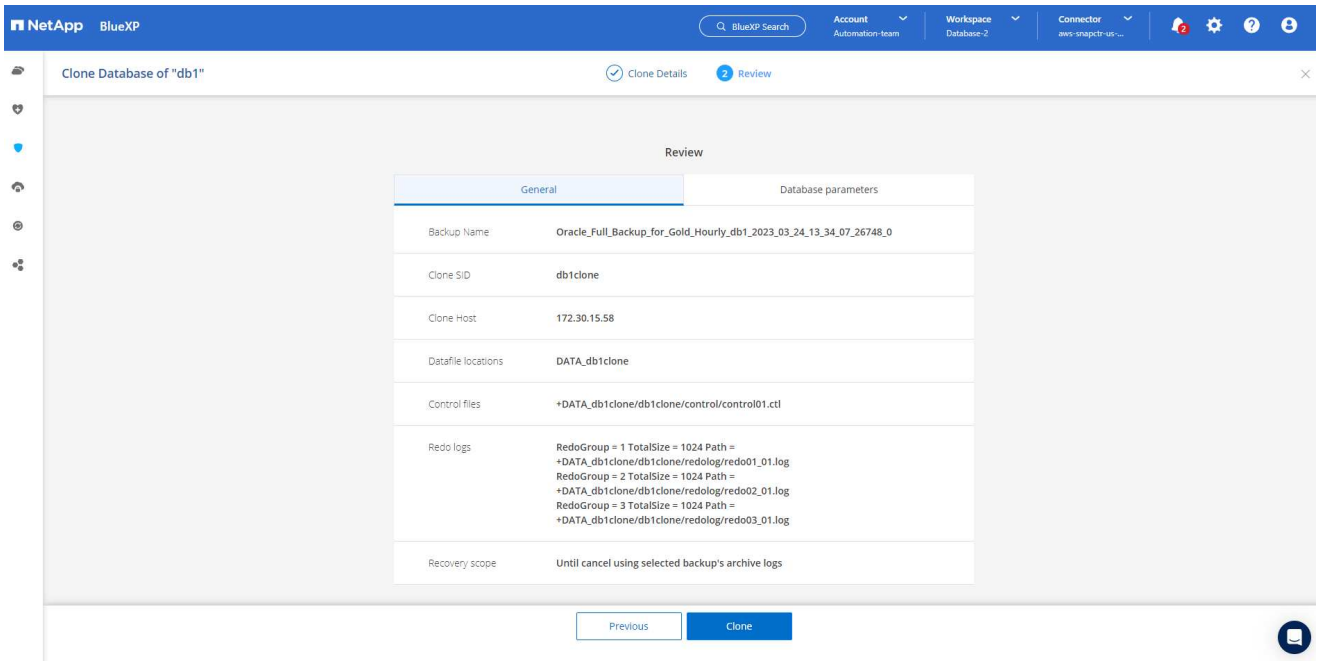
1. Wählen Sie die Option **Basic**, wenn Sie keine Parameter der geklonten Datenbank ändern müssen.



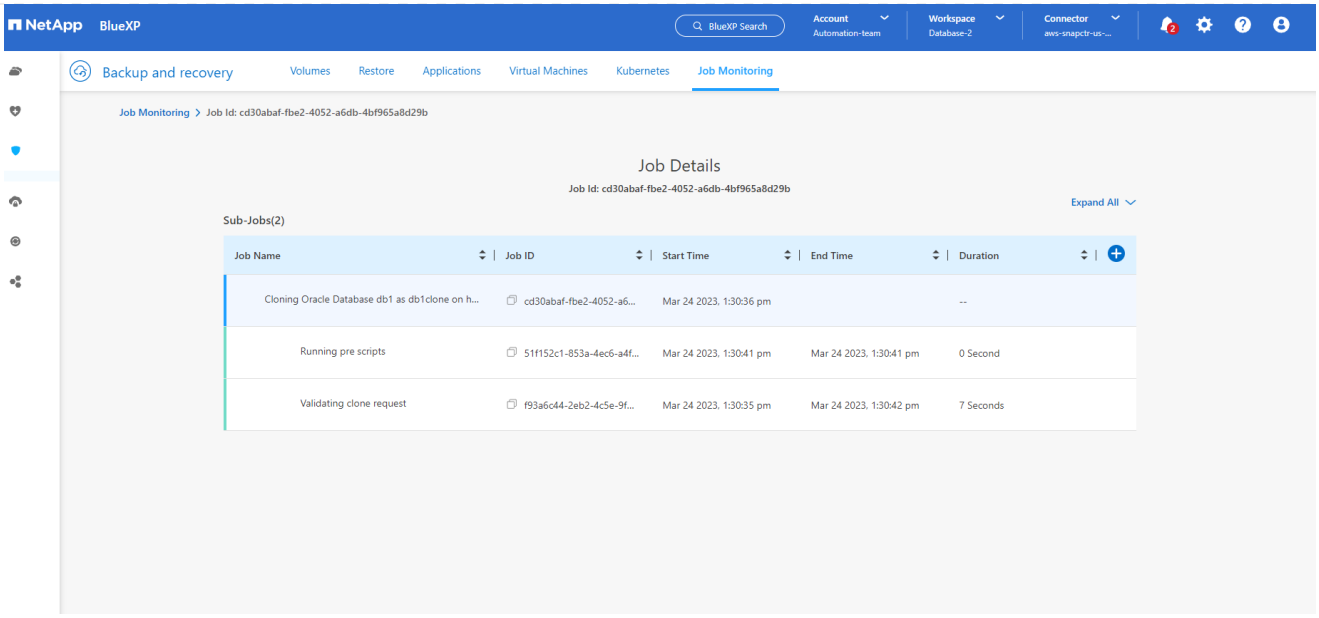
1. Alternativ können Sie **Spezifikationsdatei** auswählen. Dadurch haben Sie die Möglichkeit, die aktuelle Init-Datei herunterzuladen, Änderungen vorzunehmen und sie dann wieder in den Job hochzuladen.



1. Überprüfen und starten Sie den Job.



1. Überwachen Sie den Status des Klonauftrags auf der Registerkarte **Auftragsüberwachung**.



1. Validieren Sie die geklonte Datenbank auf dem EC2-Instance-Host.

```
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
+ASM:/u01/app/oracle/product/19.0.0/grid:N
db1:/u01/app/oracle/product/19.0.0/db1:N
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
db1clone:/u01/app/oracle/product/19.0.0/db1:N
[oracle@ip-172-30-15-58 ~]$ crsctl stat res -t
--------------------------------------------------------------------------------
Name           Target  State        Server                   State details
--------------------------------------------------------------------------------
Local Resources
--------------------------------------------------------------------------------
ora.DATA.dg
               ONLINE  ONLINE       ip-172-30-15-58          STABLE
ora.DATA_DB1CLONE.dg
               ONLINE  ONLINE       ip-172-30-15-58          STABLE
ora.LISTENER.lsnr
               ONLINE  ONLINE       ip-172-30-15-58          STABLE
ora.LOGS.dg
               ONLINE  ONLINE       ip-172-30-15-58          STABLE
ora.LOGS_SCO_2748138658.dg
               ONLINE  ONLINE       ip-172-30-15-58          STABLE
ora.asm
               ONLINE  ONLINE       ip-172-30-15-58          Started,STABLE
ora.ons
               OFFLINE OFFLINE      ip-172-30-15-58          STABLE
--------------------------------------------------------------------------------
Cluster Resources
--------------------------------------------------------------------------------
ora.cssd
      1        ONLINE  ONLINE       ip-172-30-15-58          STABLE
ora.db1.db
      1        ONLINE  ONLINE       ip-172-30-15-58          Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /db1,STABLE
ora.db1clone.db
      1        ONLINE  ONLINE       ip-172-30-15-58          Open,HOME=/u01/app/o
                                                             racle/product/19.0.0
                                                             /db1,STABLE
ora.diskmon
      1        OFFLINE OFFLINE                               STABLE
ora.driver.afd
      1        ONLINE  ONLINE       ip-172-30-15-58          STABLE
ora.evmd
      1        ONLINE  ONLINE       ip-172-30-15-58          STABLE
--------------------------------------------------------------------------------
[oracle@ip-172-30-15-58 ~]$
```

```
[oracle@ip-172-30-15-58 ~]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/db1
[oracle@ip-172-30-15-58 ~]$ export ORACLE_SID=db1clone
[oracle@ip-172-30-15-58 ~]$ export PATH=$ORACLE_HOME/bin:$PATH
[oracle@ip-172-30-15-58 ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Mar 24 18:32:21 2023
Version 19.18.0.0.0

Copyright (c) 1982, 2022, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.18.0.0.0

SQL> select name, open_mode from v$database;

NAME      OPEN_MODE
--------- --------------------
DB1CLONE  READ WRITE

SQL>
```

Weitere Informationen

Weitere Informationen zu den in diesem Dokument beschriebenen Informationen finden Sie in den folgenden Dokumenten und/oder auf den folgenden Websites:

- BlueXP einrichten und verwalten

"https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html"

- BlueXP backup and recovery

"https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html"

- Amazon FSx ONTAP

"https://aws.amazon.com/fsx/netapp-ontap/"

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2