



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	1
Zweck	1
Publikum	1
Test- und Validierungsumgebung für Lösungen	1
Architektur	2
Hardware- und Softwarekomponenten	2
Wichtige Faktoren für die Bereitstellungsüberlegungen	3
Lösungsbereitstellung	3
Voraussetzungen für die Bereitstellung des SnapCenter -Dienstes	3
Onboarding zur BlueXP -Vorbereitung	4
Bereitstellen eines Connectors für SnapCenter -Dienste	5
Definieren Sie in BlueXP eine Anmeldeinformation für den Zugriff auf AWS-Ressourcen	12
Einrichtung der SnapCenter -Dienste	16
Oracle-Datenbanksicherung	24
Wiederherstellung und Wiederherstellung von Oracle-Datenbanken	28
Oracle-Datenbankklon	31
Weitere Informationen	36

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 Datenschutzes 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

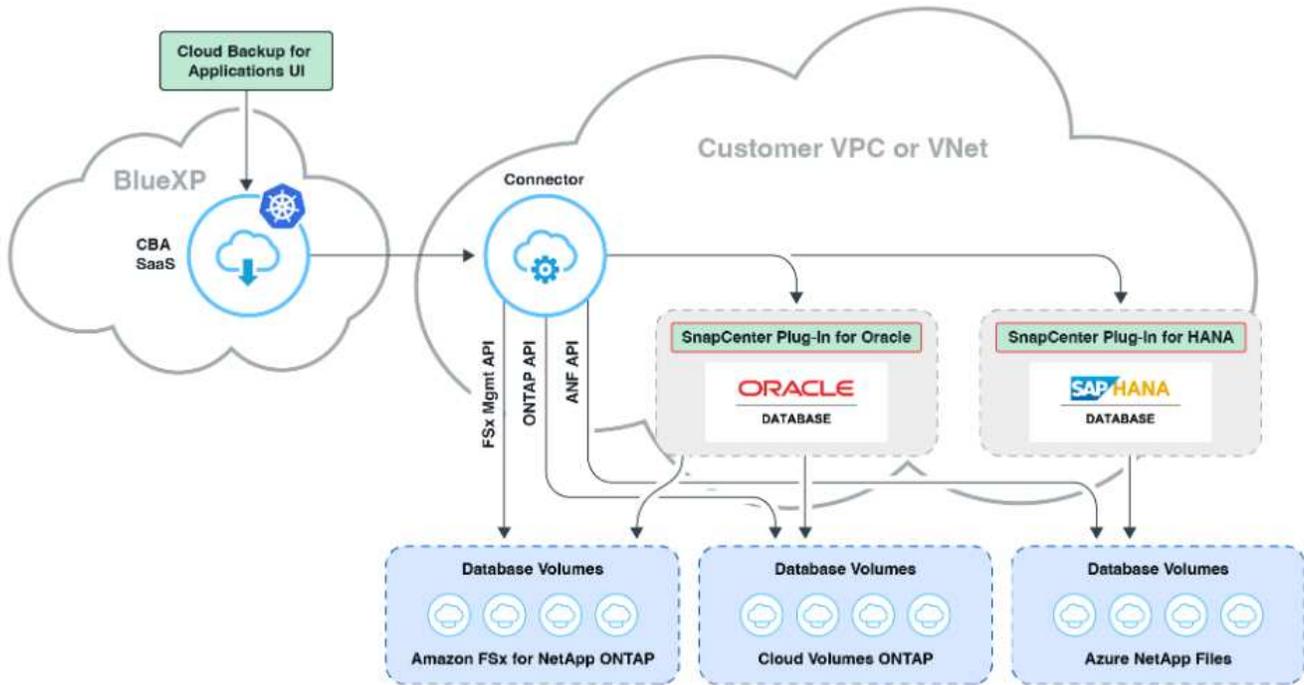
Diese Lösung ist für die folgenden Zielgruppen gedacht:

- 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 -Dienstokumentation 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 Konsoleinstellung hinzugefügt wurde.** Um Amazon FSx ONTAP zur BlueXP -Arbeitsumgebung hinzuzufügen, wird in den BlueXP -Konsoleinstellungen 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.

The screenshot shows the AWS IAM console interface. On the left is a navigation menu for Identity and Access Management (IAM). The main content area is titled 'Policies > snapcenter Summary'. It shows the Policy ARN as 'arn:aws:iam::541696183547:policy/snapcenter' and the Description as 'Policy to grant snapcenter service permission to create connector in AWS.'. Below this are tabs for 'Permissions', 'Policy usage', 'Tags', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is active, showing a 'Policy summary' button and a 'JSON' button. The JSON policy document is displayed in a code editor, showing a version of '2012-10-17' and a list of actions including IAM and EC2 actions.

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.

The screenshot shows the 'Workspaces' management interface in the BlueXP console. At the top, there is a navigation bar with the account name 'Automation-team' and tabs for 'Overview', 'Members', 'Workspaces' (which is active), and 'BlueXP Connector'. Below the navigation bar, the main heading is 'Manage the BlueXP connector Workspaces'. To the right of this heading is a '+ Add New Workspace' button. Below this, there is a table listing existing workspaces:

Workspace Name	Actions
Database	
Database-2	
sufians-k8	
Workspace-1	

In the bottom right corner of the interface, there is a circular icon containing a document symbol.

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

NetApp Cloud Manager Account Automation-team Workspace new-workspace Connector N/A

Backup & Restore Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

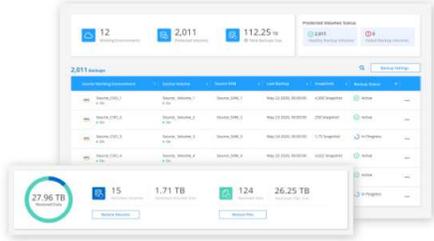
Backup & Restore

Fully integrated data protection for ONTAP anywhere

Cloud Backup dramatically reduces the complexity of backing up critical structured and unstructured data across your ONTAP hybrid cloud environments to cost-effective object storage. All you need to do is select the source, the target and the protection policy and you're protected

To start your Backup & Restore experience, please deploy our connector

[Add a Connector](#)



Simple & intuitive
No backup or cloud expertise required. Simply click the button above and follow the instructions

Hybrid Multicloud
Backup from On-premises or Cloud Volumes ONTAP to AWS, Azure, GCP or StorageGRID

Unmatched Efficiency
Combines incremental, block-level operation storage efficiencies to reduce time and cost

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

Add Connector ✕

Provider

Choose the cloud provider where you want to run the Connector:



Microsoft Azure



Amazon Web Services



Google Cloud Platform

[Continue](#) 

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](#) ."

Add Connector - AWS

Deploying a Connector

The Connector is a crucial component for the day-to-day use of Cloud Manager. It's used to connect Cloud Manager's services to your hybrid-cloud environments. The Connector can then manage the resources and processes within your public cloud environment.

Before you begin the deployment process, ensure that you have completed the required preparations. This guide will enable you to focus on the minimum requirements for Connector installation.

Permissions Set up an IAM role with the required permissions	Authentication Choose between two AWS authentication methods: AWS keys or assuming an IAM role	Networking Obtain details about the VPC and subnet in which the Connector will reside
--	--	---

[Skip to Deployment](#)

[Previous](#) [Continue](#)

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

- 1 AWS Credentials
- 2 Details
- 3 Network
- 4 Security Group
- 5 Review

AWS Authentication

Region
us-east-1 | US East (N. Virginia)

Select the Authentication Method: Assume Role AWS Keys

AWS Access Key
AKIA6JRXA6ZVGVFUSHMO3

AWS Secret Key
.....

Want to launch an instance without AWS Credentials? v

Previous

Next



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

- 1 AWS Credentials
- 2 Details
- 3 Network
- 4 Security Group
- 5 Review

Details

Connector Instance Name
SnapCenterSvs

Connector Role
 Create Role Select an existing Role

+ Add Tags to Connector Instance

Role Name
Cloud-Manager-Operator-VZzSSP9-SnapCenter

AWS Managed Encryption
Master Key: aws/ebs (default) [Change Key](#)

Previous

Next



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

Add BlueXP Connector - AWS More Information ×

✓ AWS Credentials ✓ Details **3 Network** 4 Security Group 5 Review

Network

Connectivity

VPC
vpc-0b522d5e982a50ceb - 172.30.15.0/25

Subnet
172.30.15.0/25 | priv-subnet-01

Key Pair ?
sufi_new

Public IP
Use subnet settings (Disable)

Notice: Ensure that the subnet has internet connectivity through a NAT device or proxy server so that the Connector can communicate with AWS services.

Proxy Configuration (Optional)

HTTP Proxy
Example: http://172.16.254.1:8080

Define Credentials for this Proxy ∨

Upload a root certificate ∨

Previous Next



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

 AWS Credentials  Details  Network ** Security Group**  Review

Security Group

The security group must allow inbound HTTP, HTTPS and SSH access.

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

1 Security Group 

Security Group Name	Description
<input checked="" type="radio"/> default	default VPC security group

Previous

Next 

- 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.

Add BlueXP Connector - AWS More Information ✕

✓ AWS Credentials ✓ Details ✓ Network ✓ Security Group **5** Review

Review [Code for Terraform Automation](#)

BlueXP Connector Name	aws-snapctr-us-east
AWS Access Key	AKIAX4H43ZT5GIWWR3TI
Region	us-east-1
VPC	vpc-0b522d5e982a50ceb - 172.30.15.0/25
Subnet	172.30.15.0/25 priv-subnet-01
Key Pair	sufi_new
Public IP	Use subnet settings (Disable)
Proxy	None
Security Group	default

Previous Add ✉

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

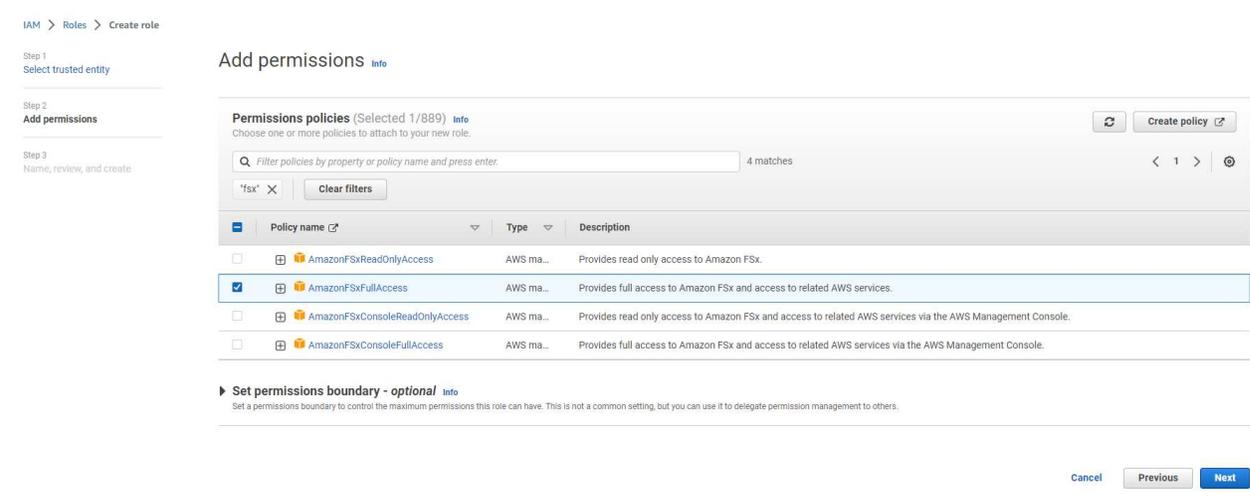
1. Erstellen Sie zunächst in der AWS EC2-Konsole eine Rolle im Menü **Rollen** von **Identity and Access Management (IAM)** und dann **Rolle erstellen**, um den Workflow zur Rollenerstellung zu starten.

The screenshot shows the AWS IAM console interface. On the left, there is a navigation sidebar with 'Identity and Access Management (IAM)' at the top and a search bar. Below the search bar, there are sections for 'Dashboard', 'Access management' (with 'Roles' selected), 'Access reports', and 'Related consoles'. The main area shows the 'Roles' page with a title 'Roles (106)' and a description: 'An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.' Below this is a search bar and a table of roles. The table has columns for 'Role name', 'Trusted entities', and 'Last activity'. The 'Create role' button is in the top right corner.

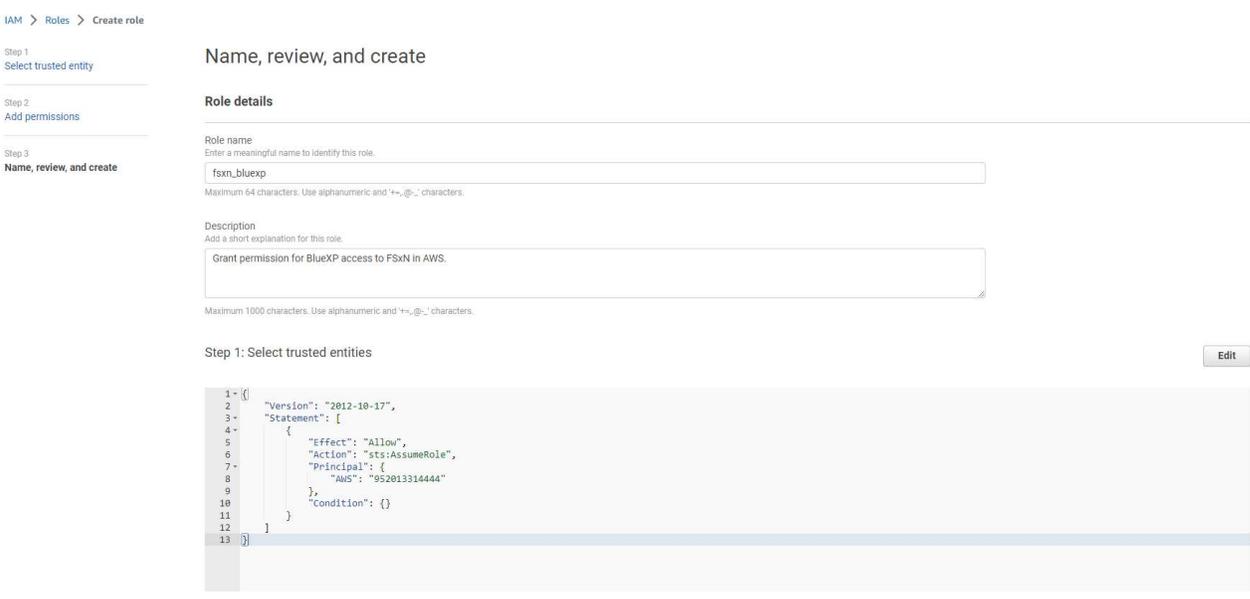
2. Wählen Sie auf der Seite **Vertrauenswürdige Entität auswählen** **AWS-Konto**, **Anderes AWS-Konto** und fügen Sie die BlueXP -Konto-ID ein, die von der BlueXP Konsole abgerufen werden kann.

The screenshot shows the 'Create role' wizard in the AWS IAM console, specifically Step 1: 'Select trusted entity'. The left sidebar shows the progress: Step 1 (selected), Step 2: 'Add permissions', and Step 3: 'Name, review, and create'. The main area is titled 'Select trusted entity' and has a sub-section 'Trusted entity type' with five radio button options: 'AWS service', 'AWS account' (selected), 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Below this is the 'An AWS account' section with two radio button options: 'This account (541696183547)' and 'Another AWS account' (selected). The 'Account ID' field is filled with '952013314444'. There are also 'Options' for 'Require external ID' and 'Require MFA'. The 'Next' button is highlighted in blue.

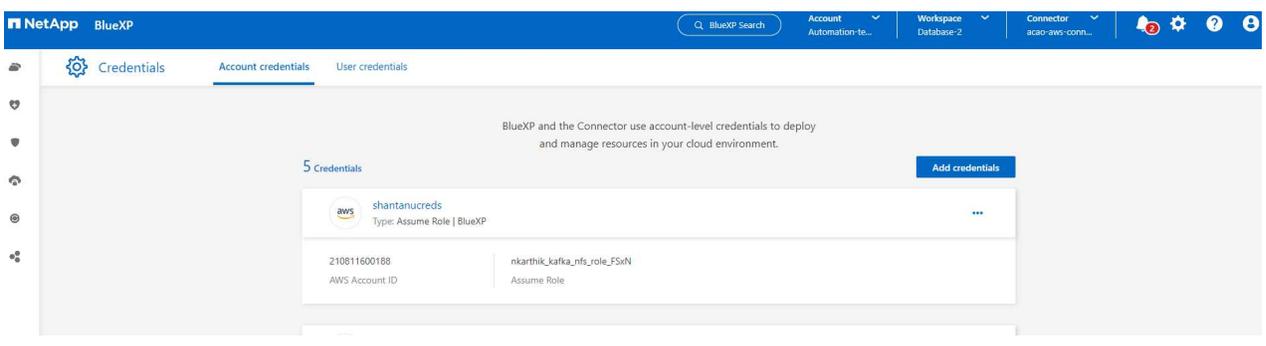
3. Filtern Sie Berechtigungsrichtlinien nach fsx und fügen Sie der Rolle **Berechtigungsrichtlinien** hinzu.



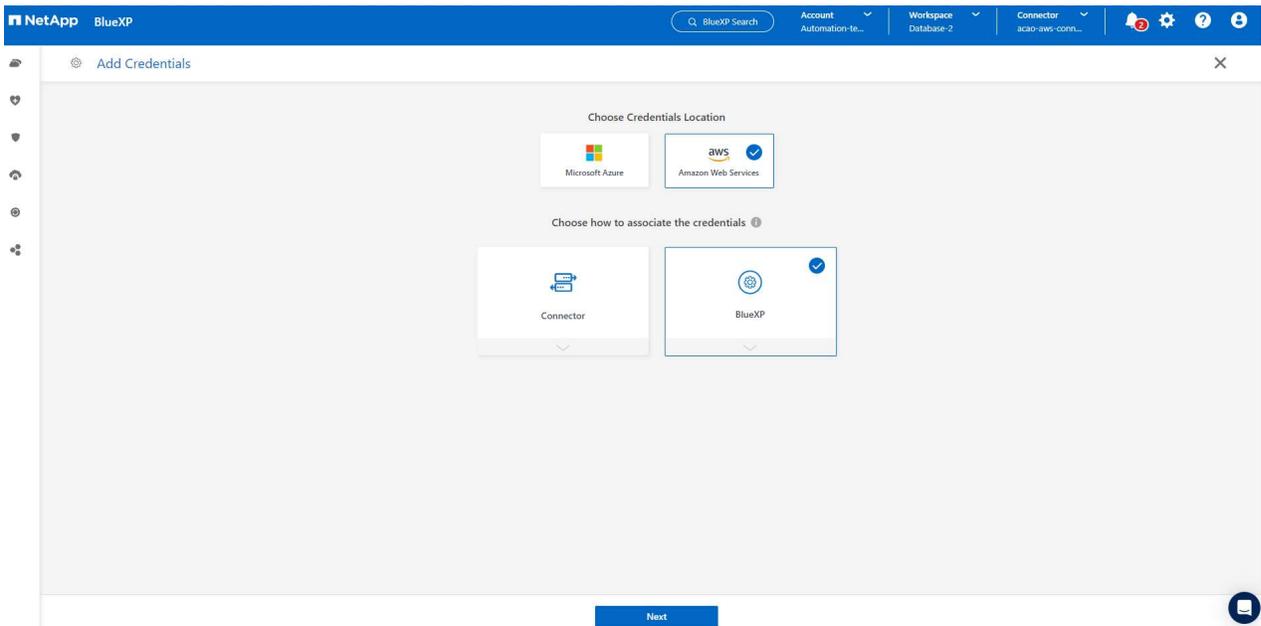
4. Geben Sie auf der Seite **Rollendetails** der Rolle einen Namen, fügen Sie eine Beschreibung hinzu und klicken Sie dann auf **Rolle erstellen**.



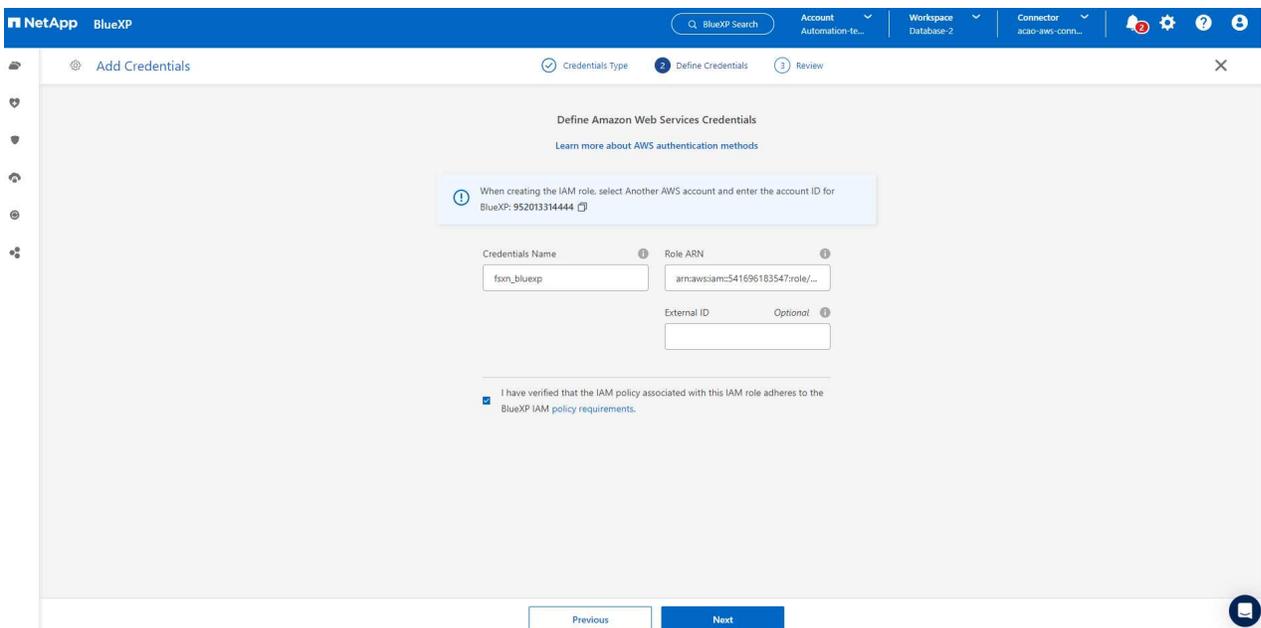
5. Zurück zur BlueXP -Konsole: Klicken Sie auf das Einstellungssymbol in der oberen rechten Ecke der Konsole, um die Seite **Kontoanmeldeinformationen** zu öffnen. Klicken Sie auf **Anmeldeinformationen hinzufügen**, um den Workflow zur Anmeldeinformationskonfiguration zu starten.



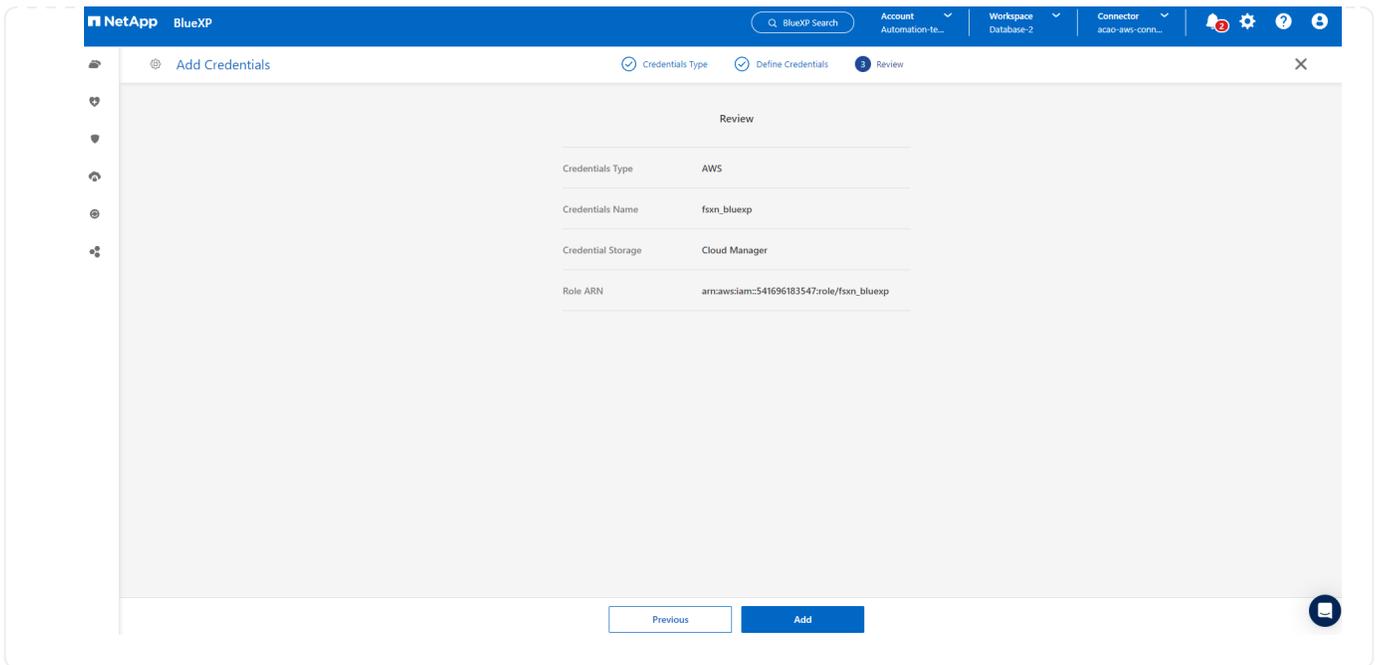
6. Wählen Sie den Anmeldeinformationsort als **Amazon Web Services – BlueXP**.



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.



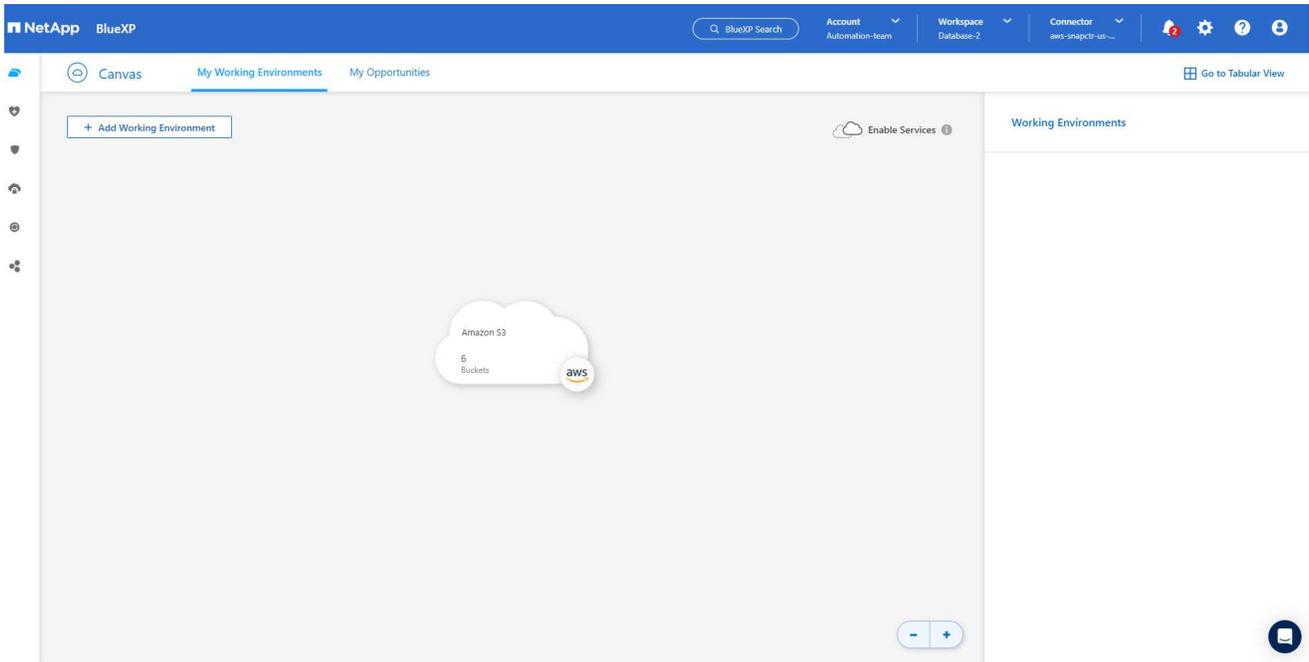
8. Überprüfen und **Hinzufügen**



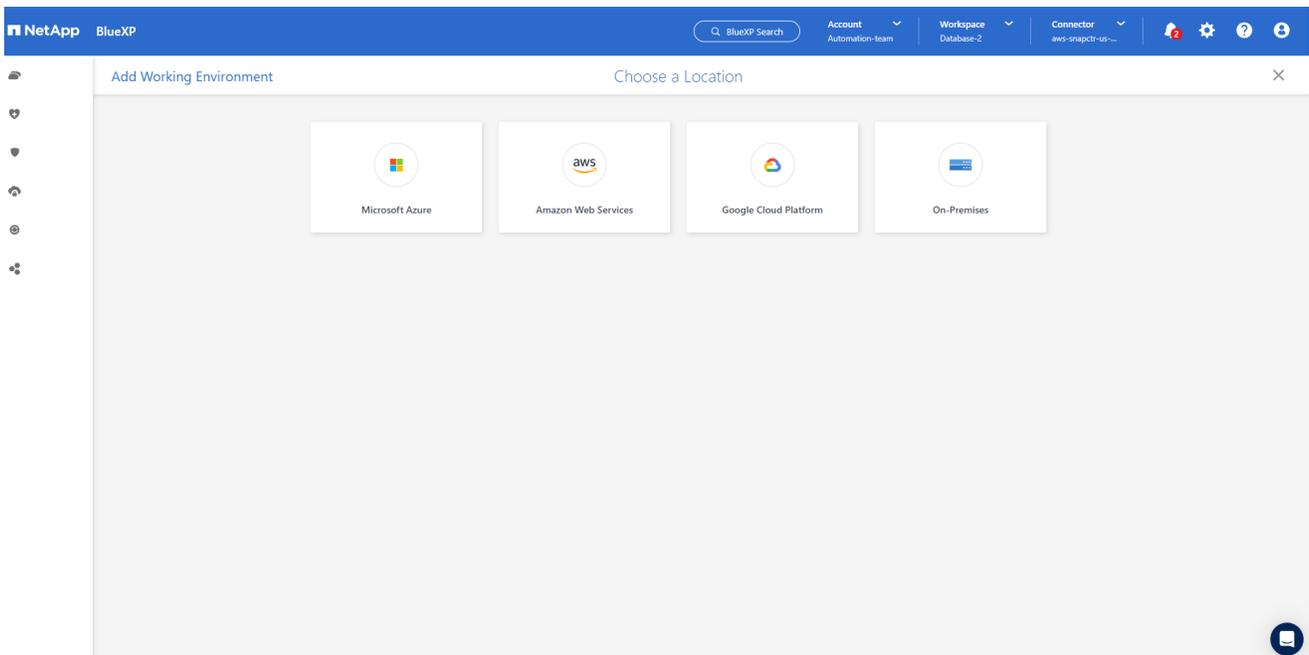
Einrichtung der SnapCenter -Dienste

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

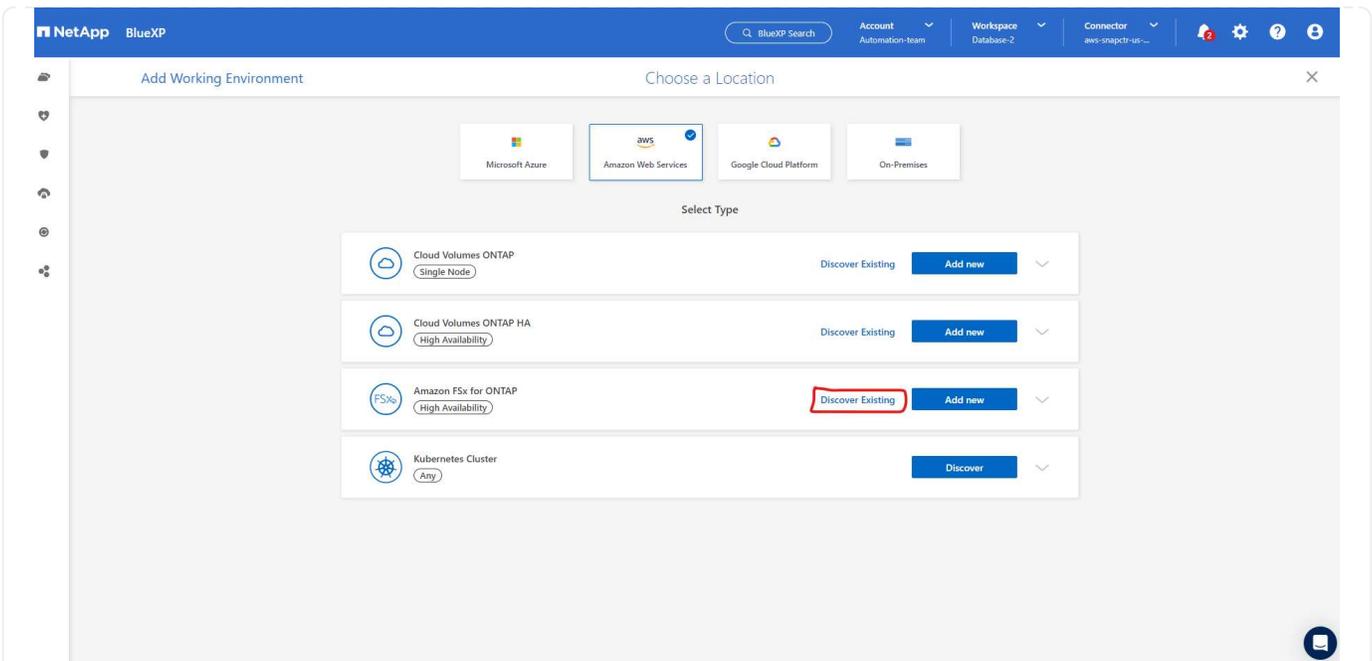
1. Klicken Sie unter **Meine Arbeitsumgebung** auf **Arbeitsumgebung hinzufügen**, um in AWS bereitgestelltes FSx zu entdecken.



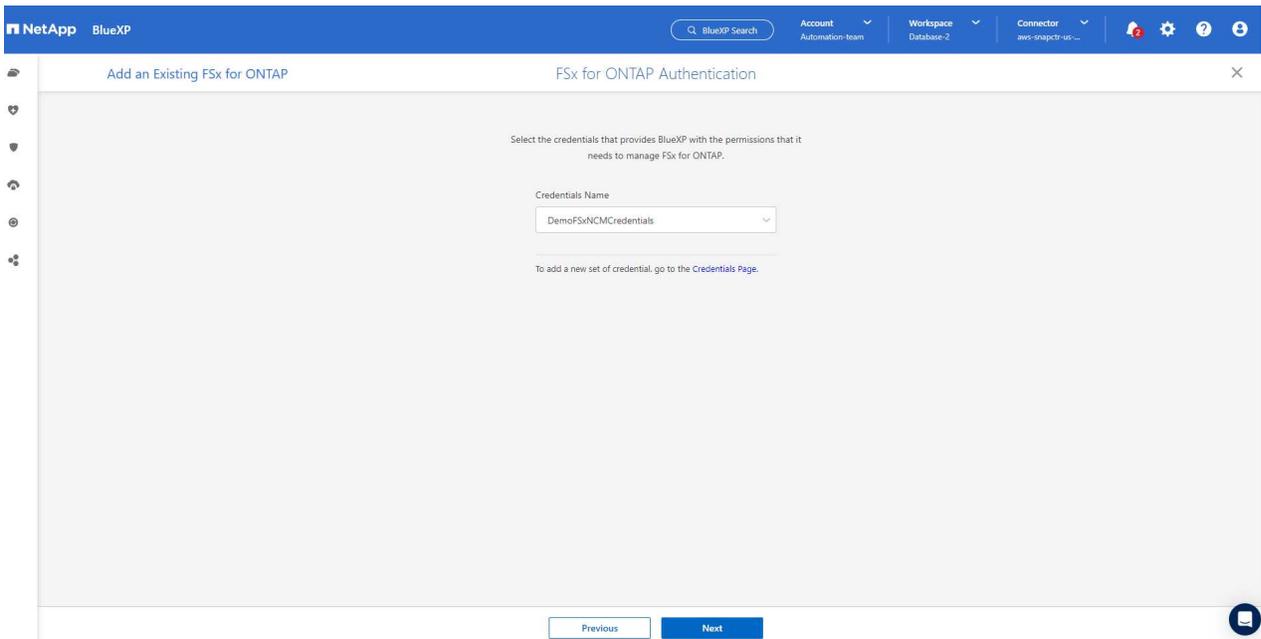
1. Wählen Sie als Standort **Amazon Web Services**.



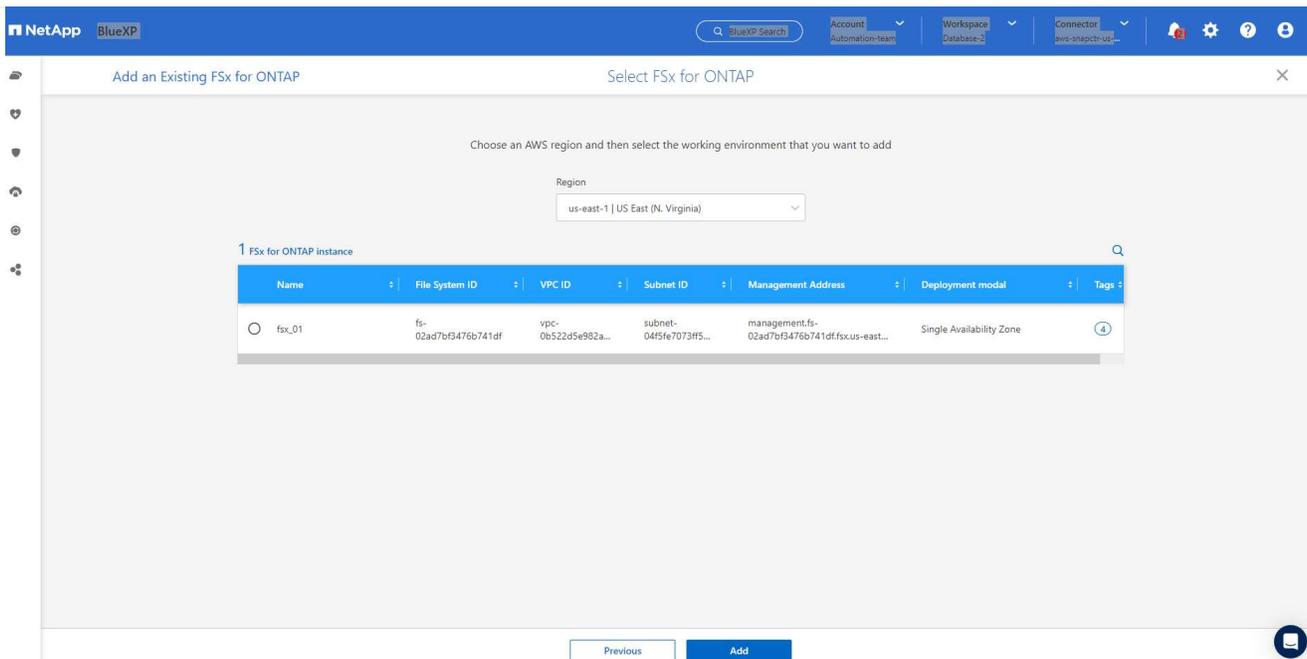
1. Klicken Sie neben * Amazon FSx ONTAP* auf **Vorhandenes erkennen**.



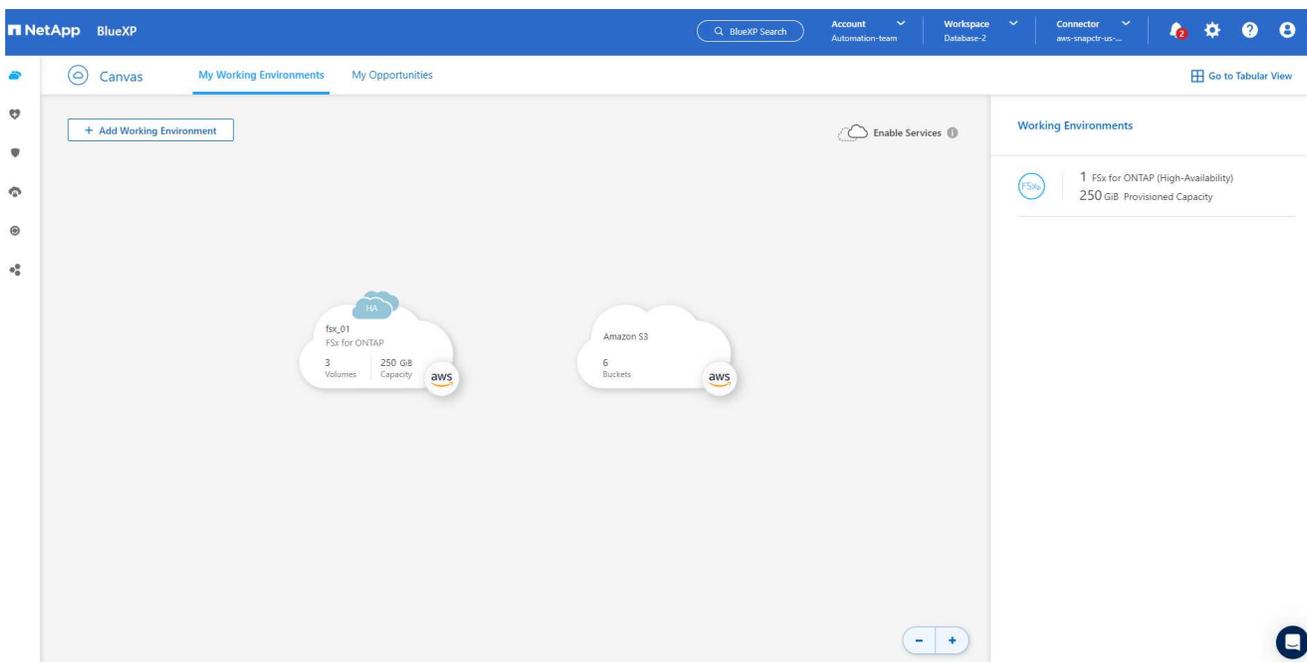
1. Wählen Sie den **Anmeldeinformationsnamen** aus, den Sie im vorherigen Abschnitt erstellt haben, um BlueXP die Berechtigungen zu erteilen, die es zum Verwalten von FSx ONTAP benötigt. Wenn Sie keine Anmeldeinformationen hinzugefügt haben, können Sie diese über das Menü **Einstellungen** in der oberen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



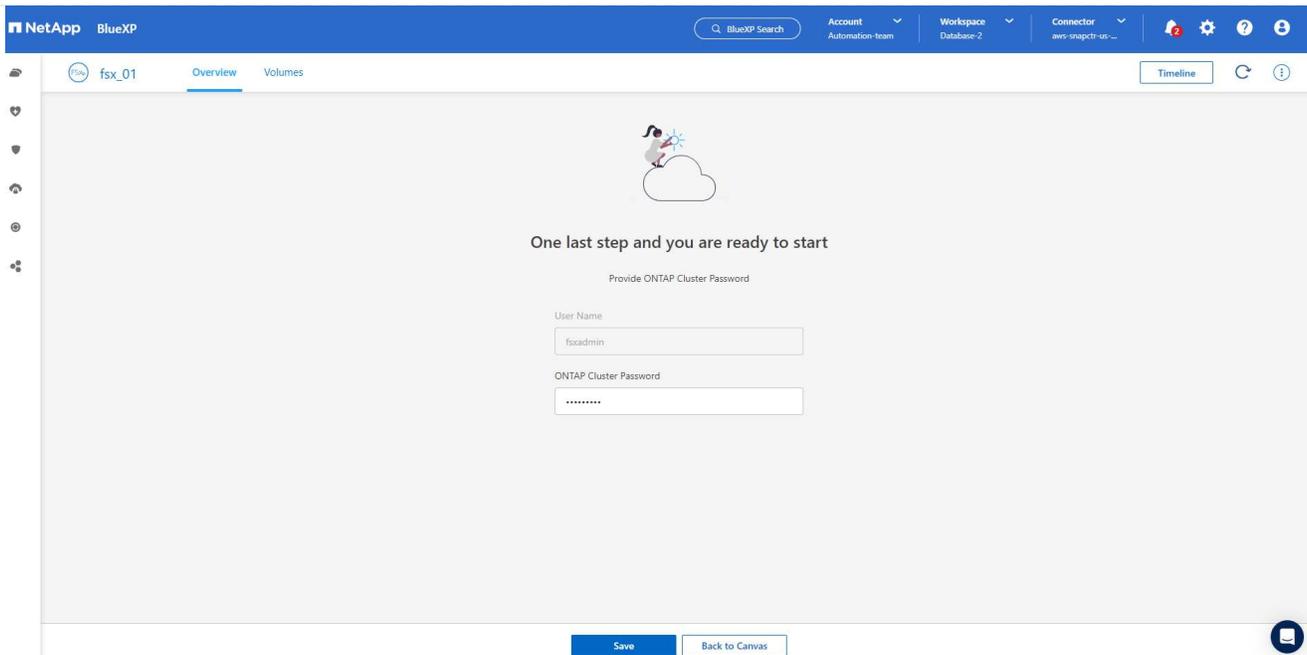
2. Wählen Sie die AWS-Region aus, in der Amazon FSx ONTAP bereitgestellt wird, wählen Sie den FSx-Cluster aus, der die Oracle-Datenbank hostet, und klicken Sie auf „Hinzufügen“.



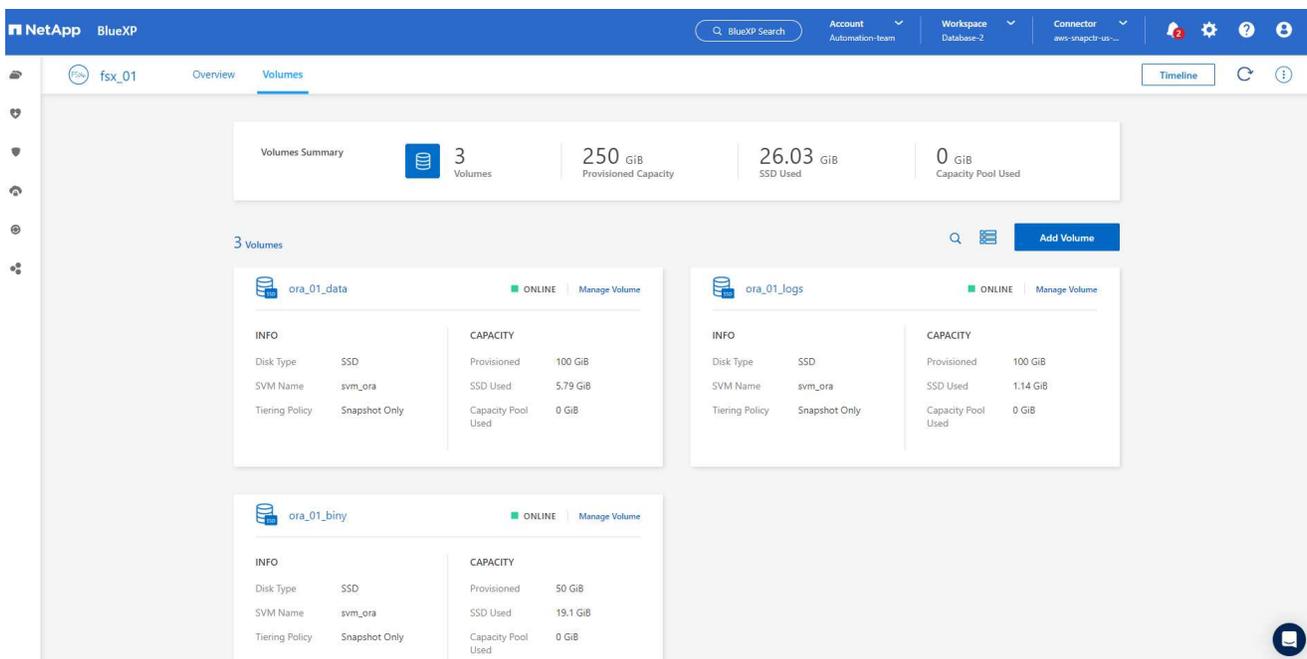
1. Die erkannte Amazon FSx ONTAP -Instanz wird jetzt in der Arbeitsumgebung angezeigt.



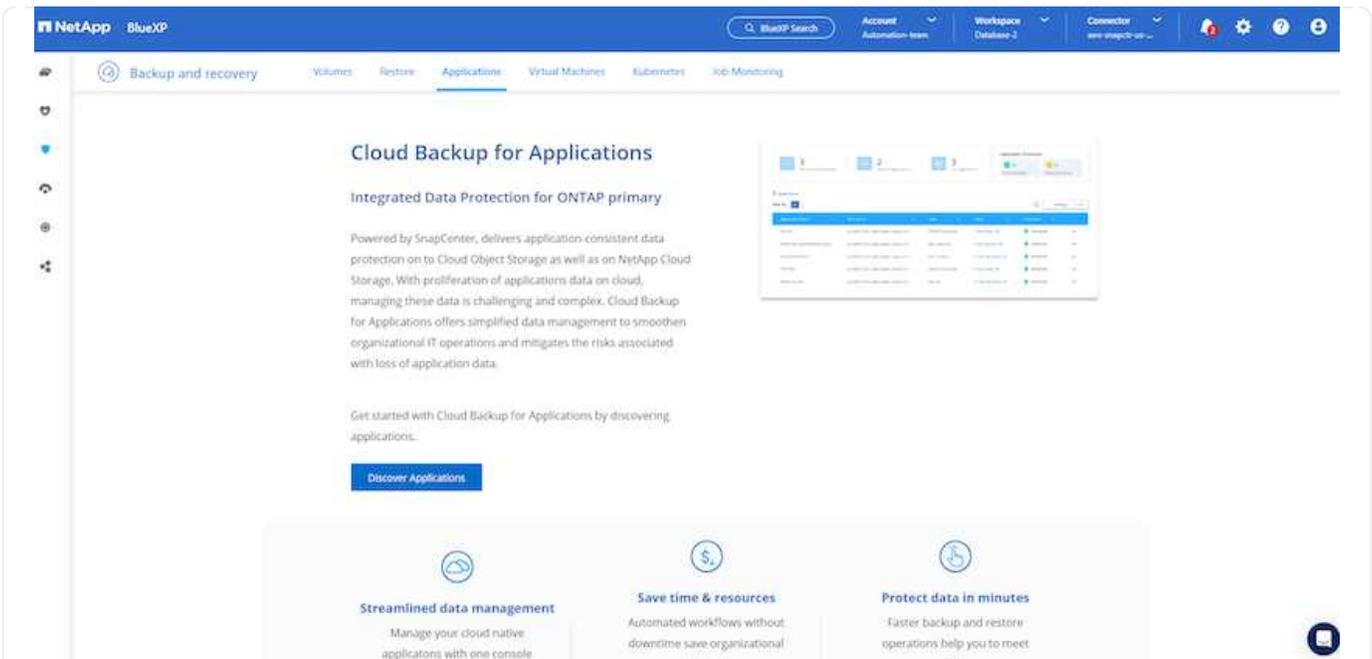
1. Sie können sich mit den Anmeldeinformationen Ihres fsxadmin-Kontos beim FSx-Cluster anmelden.



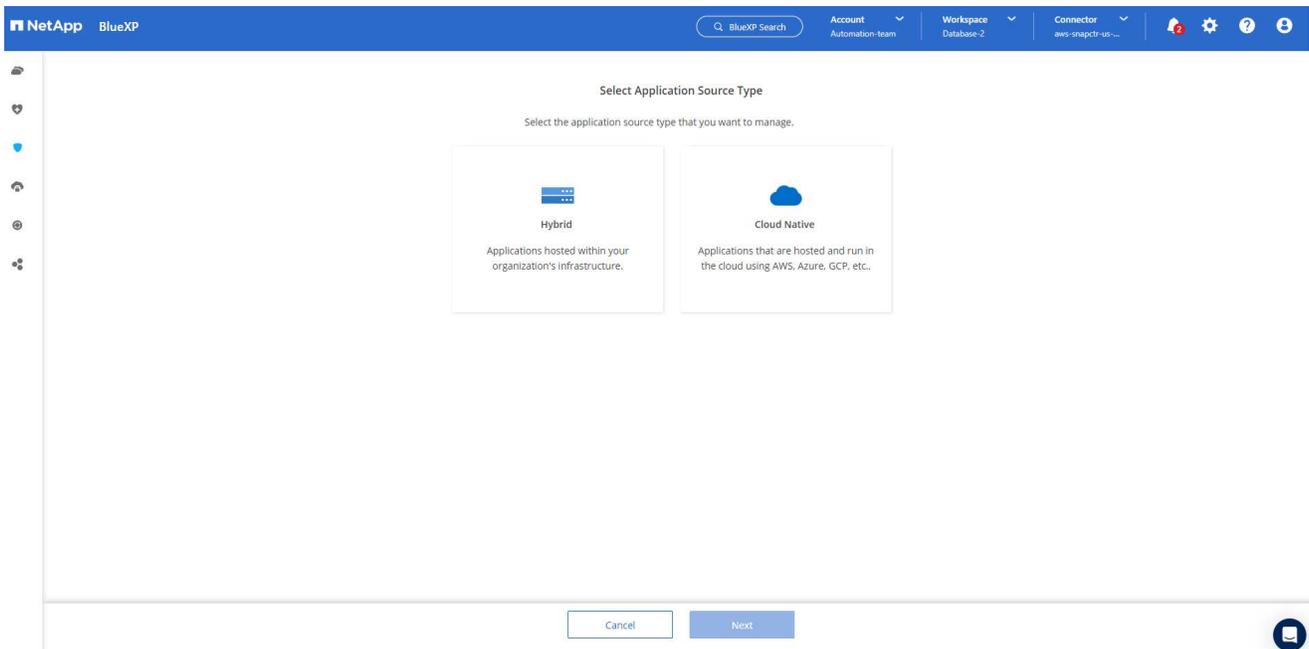
1. Nachdem Sie sich bei Amazon FSx ONTAP angemeldet haben, überprüfen Sie Ihre Datenbankspeicherinformationen (z. B. Datenbankvolumes).



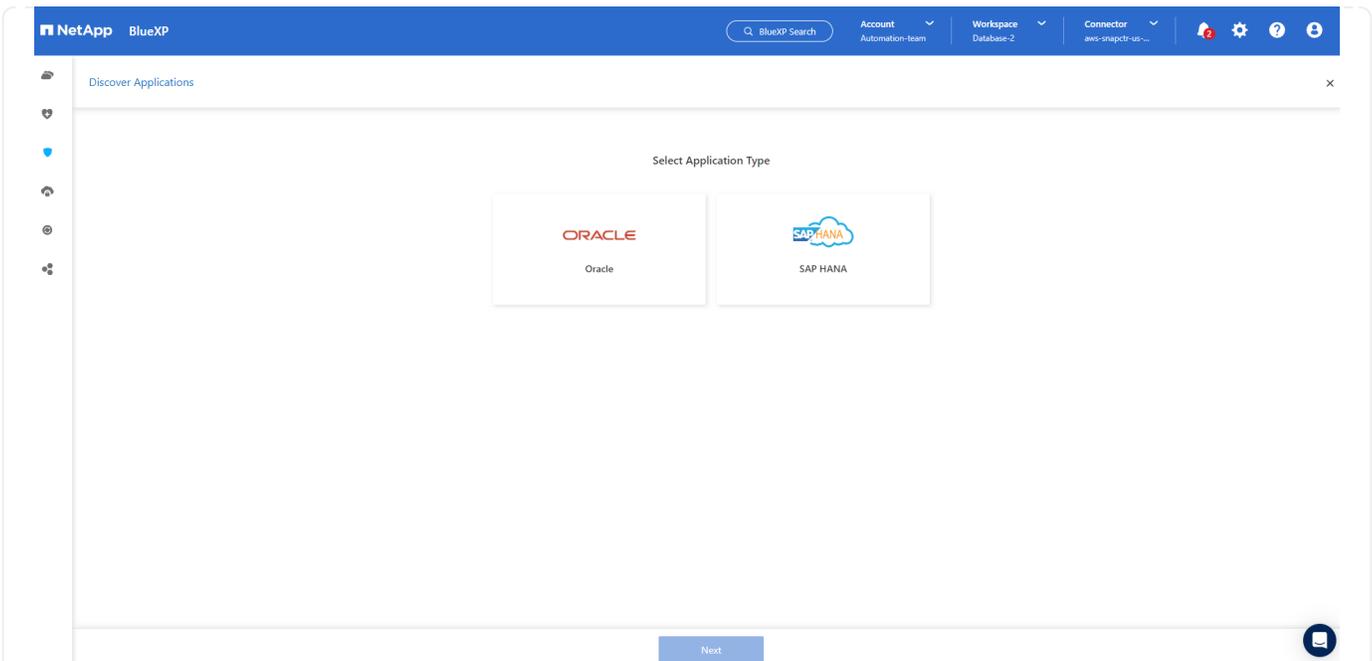
1. Bewegen Sie in der linken Seitenleiste der Konsole den Mauszeiger über das Schutzsymbol und klicken Sie dann auf **Schutz > Anwendungen**, um die Startseite „Anwendungen“ zu öffnen. Klicken Sie auf **Anwendungen erkennen**.



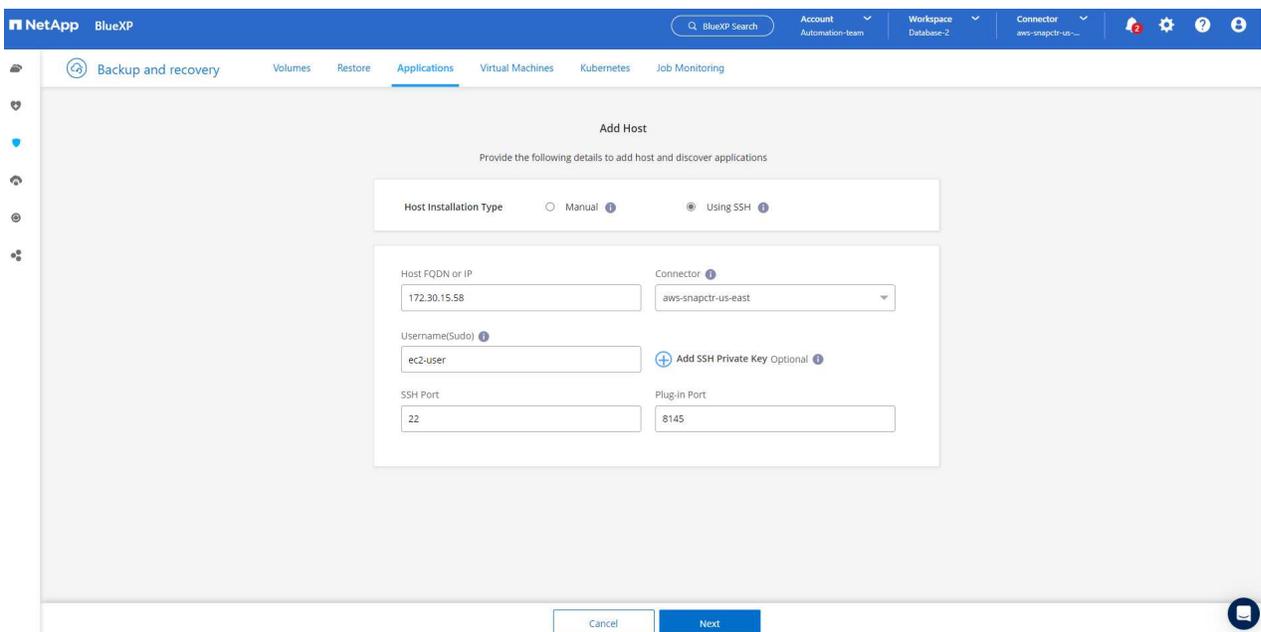
1. Wählen Sie **Cloud Native** als Anwendungsquellentyp.



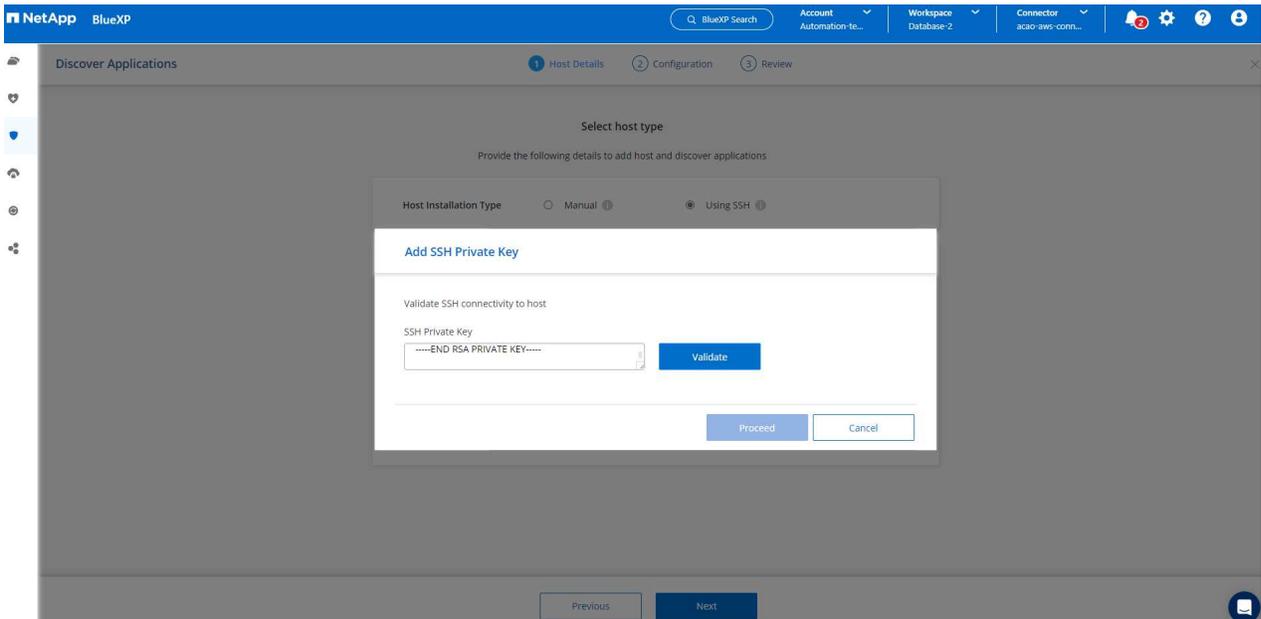
1. Wählen Sie **Oracle** als Anwendungstyp.



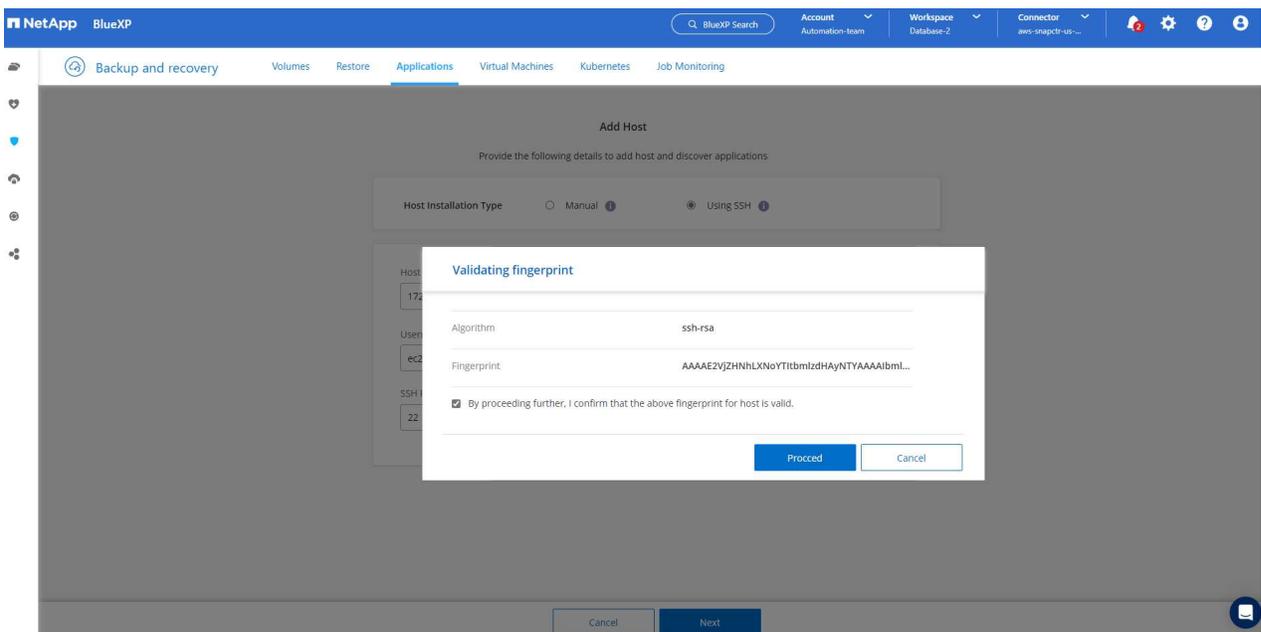
1. Geben Sie die Hostdetails der AWS EC2 Oracle-Anwendung ein. Wählen Sie **SSH verwenden** als **Host-Installationstyp** für die Plug-in-Installation und Datenbankerkennung in einem Schritt. Klicken Sie dann auf **Privaten SSH-Schlüssel hinzufügen**.



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.

The screenshot shows the NetApp BlueXP console interface. At the top, there's a navigation bar with 'NetApp BlueXP' and a search bar. Below the navigation bar, there are tabs for 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' tab is selected. The main content area shows a summary of resources: 'Cloud Native' (1 Hosts), 'Oracle' (1 ORACLE), and 'Clone' (0 Clones). To the right, there's an 'Application Protection' summary showing 0 Protected and 1 Unprotected. Below this, there's a section for '1 Databases' with a 'Filter By' button and a search bar. A table lists the database details:

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

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

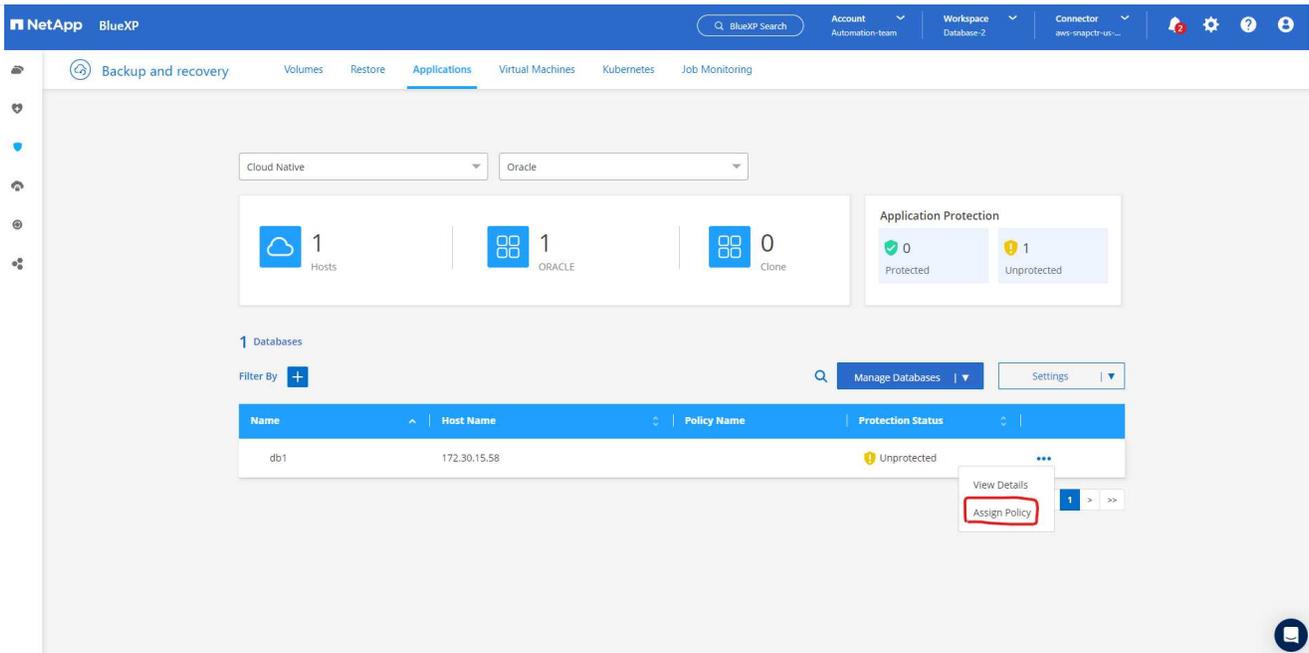
1. Klicken Sie auf die drei Punkte neben dem **Schutzstatus** der Datenbank und dann auf **Richtlinien**, um die standardmäßig vorinstallierten Datenbankschutzrichtlinien anzuzeigen, die zum Schutz Ihrer Oracle-Datenbanken angewendet werden können.

The screenshot shows the NetApp BlueXP interface. At the top, there's a navigation bar with 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. Below this, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows '1 Hosts', '1 ORACLE', and '0 Clone'. An 'Application Protection' section indicates '0 Protected' and '1 Unprotected'. A table lists databases with columns for Name, Host Name, Policy Name, and Protection Status. The table shows one database named 'db1' with host '172.30.15.58' and status 'Unprotected'. A 'Settings' dropdown menu is open, showing options for Policies, About, and Hosts.

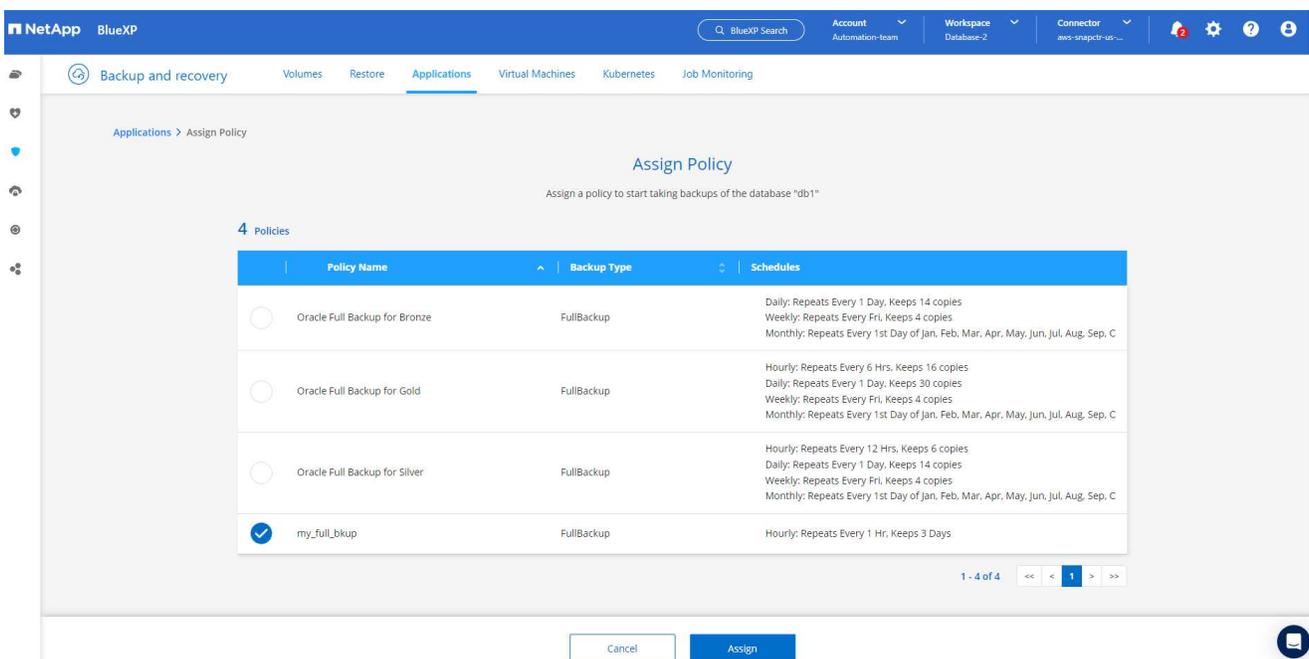
1. Sie können auch Ihre eigene Richtlinie mit einer benutzerdefinierten Sicherungshäufigkeit und einem benutzerdefinierten Aufbewahrungsfenster für Sicherungsdaten erstellen.

The screenshot shows the NetApp BlueXP interface for 'Applications > Policies'. It features filters for 'Cloud Native' and 'Oracle'. A 'Create Policy' button is visible. A table lists four policies with columns for Policy Name, Backup Type, and Schedules and Retention. The policies are: 'Oracle Full Backup for Bronze', 'Oracle Full Backup for Gold', 'Oracle Full Backup for Silver', and 'my_full_bkup'. Each policy row includes details about backup frequency and retention, and a three-dot menu icon for further actions.

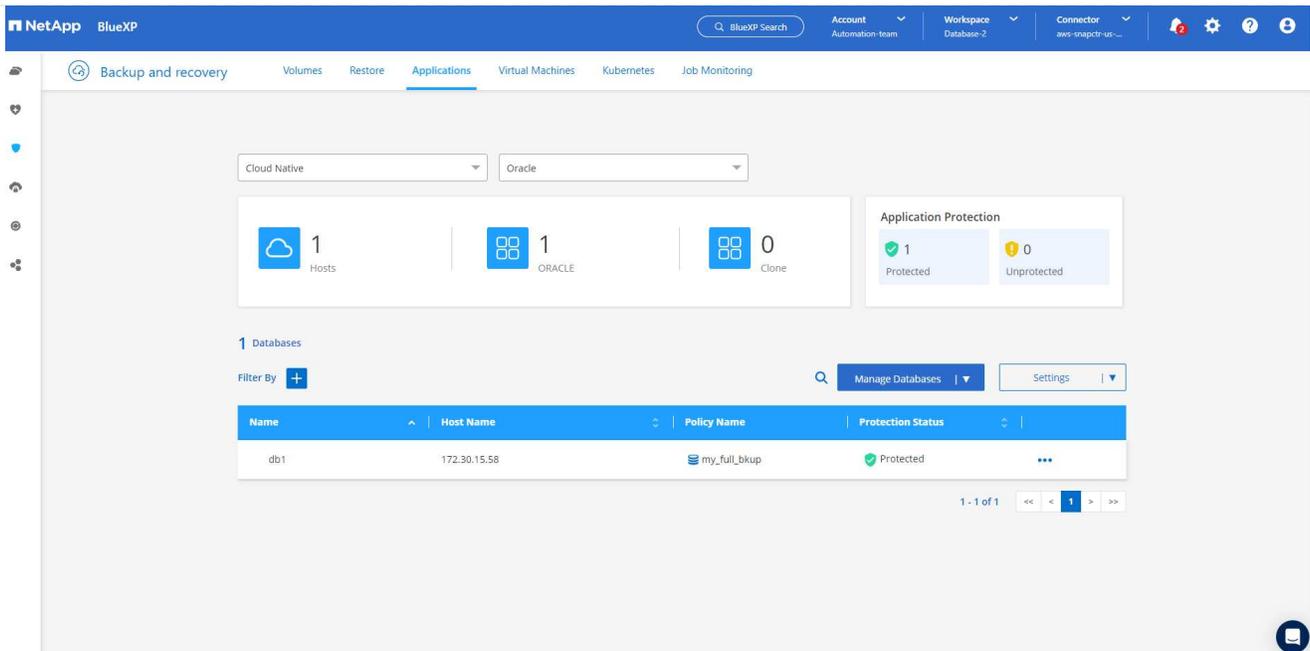
1. Wenn Sie mit der Richtlinienkonfiguration zufrieden sind, können Sie die gewünschte Richtlinie zum Schutz der Datenbank zuweisen.



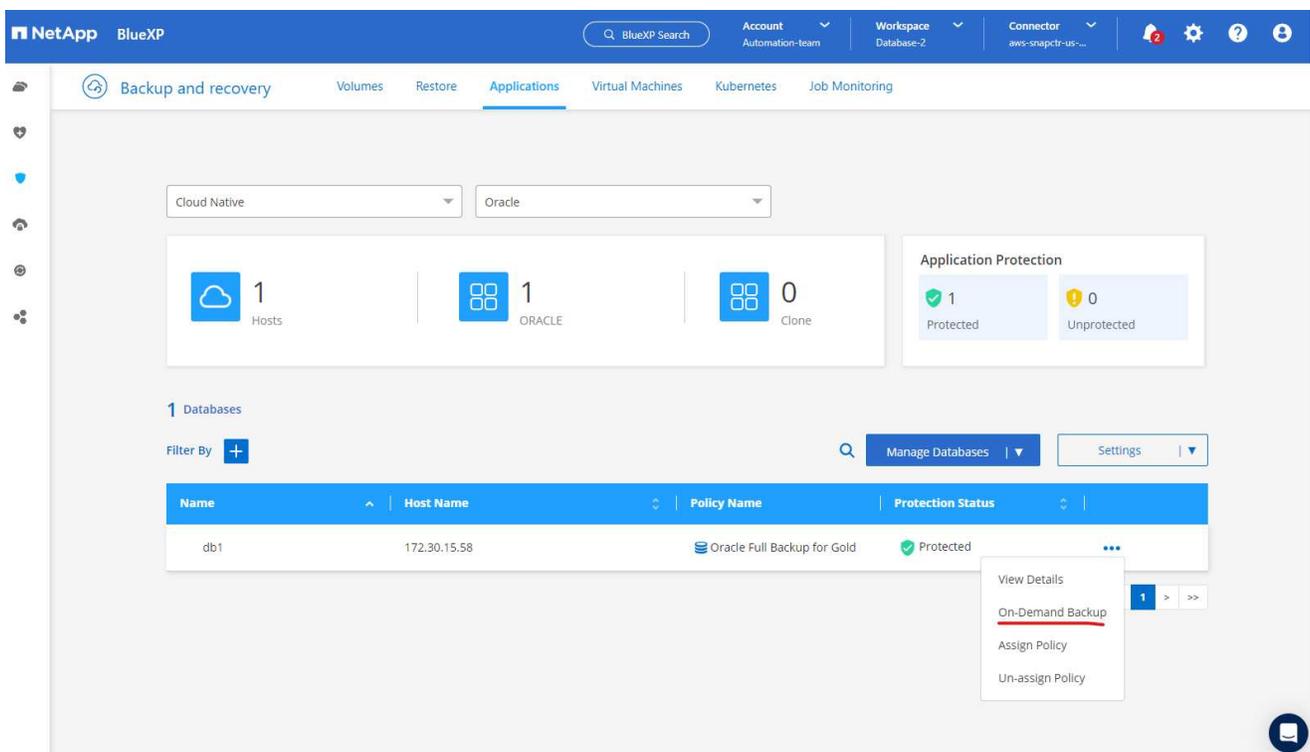
1. Wählen Sie die Richtlinie aus, die der Datenbank zugewiesen werden soll.



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 Protokollvolumen-Snapshot wird direkt nach einem Datenbankvolumen-Snapshot durchgeführt. Sie können einen Filter anwenden, wenn Sie in einer langen Liste nach einem bestimmten Backup suchen.

NetApp BlueXP

Account Automation-team | Workspace Database-2 | Connector aws-snapctr-us...

Backup and recovery | Volumes | Restore | **Applications** | Virtual Machines | Kubernetes | Job Monitoring

Applications > Database Details

Database Details

db1 Database Name	Protected Protection	Oracle Full Backup for Gold Policy Names	Database Type
172.30.15.58 Host Name	FSx Host Storage	Unreachable Database Version	bKed8yv2T19Bj0V5Qyqva... Agent Id
- Clones	- Parent Database		

8 Backups

Filter By +

Select Timeframe

Backup Name	Backup Type	SCN	Backup Date	
Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_12_18_60900_1	Log	2589354	Mar 24, 2023, 3:12:34 pm	Delete
Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19_11_51_51476_0	Data	2589306	Mar 24, 2023, 3:12:18 pm	...
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1	Log	2586621	Mar 24, 2023, 2:10:45 pm	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_03_70535_0	Data	2586557	Mar 24, 2023, 2:10:31 pm	...

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.

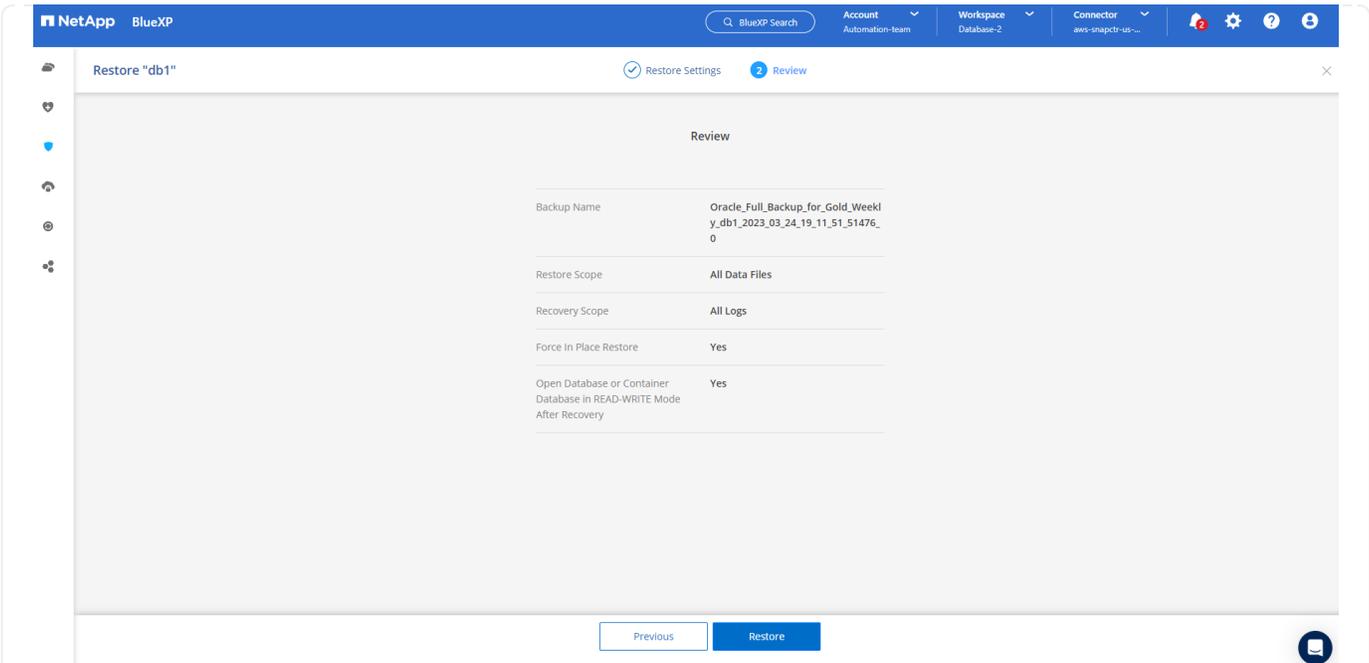
The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The main content area is titled 'Database Details' and shows information for a database named 'db1'. Below this, there is a section for 'Backups' with a table listing backup details. The table has columns for 'Backup Name', 'Backup Type', 'SCN', and 'Backup Date'. The third row in the table has a 'Restore' button highlighted with a red box. Other buttons like 'Delete' and 'Clone' are also visible in a dropdown menu.

Backup Name	Backup Type	SCN	Backup Date	
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_31_71953_1	Log	2586621	Mar 24, 2023, 2:10:45 pm	Delete
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_18_10_03_70535_0	Data	2586557	Mar 24, 2023, 2:10:31 pm	...
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_37_04_98851_1	Log	2580577	Mar 24, 2023, 11:37:1	Restore
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_36_33_27205_0	Data	2580524	Mar 24, 2023, 11:37:0	Delete Clone

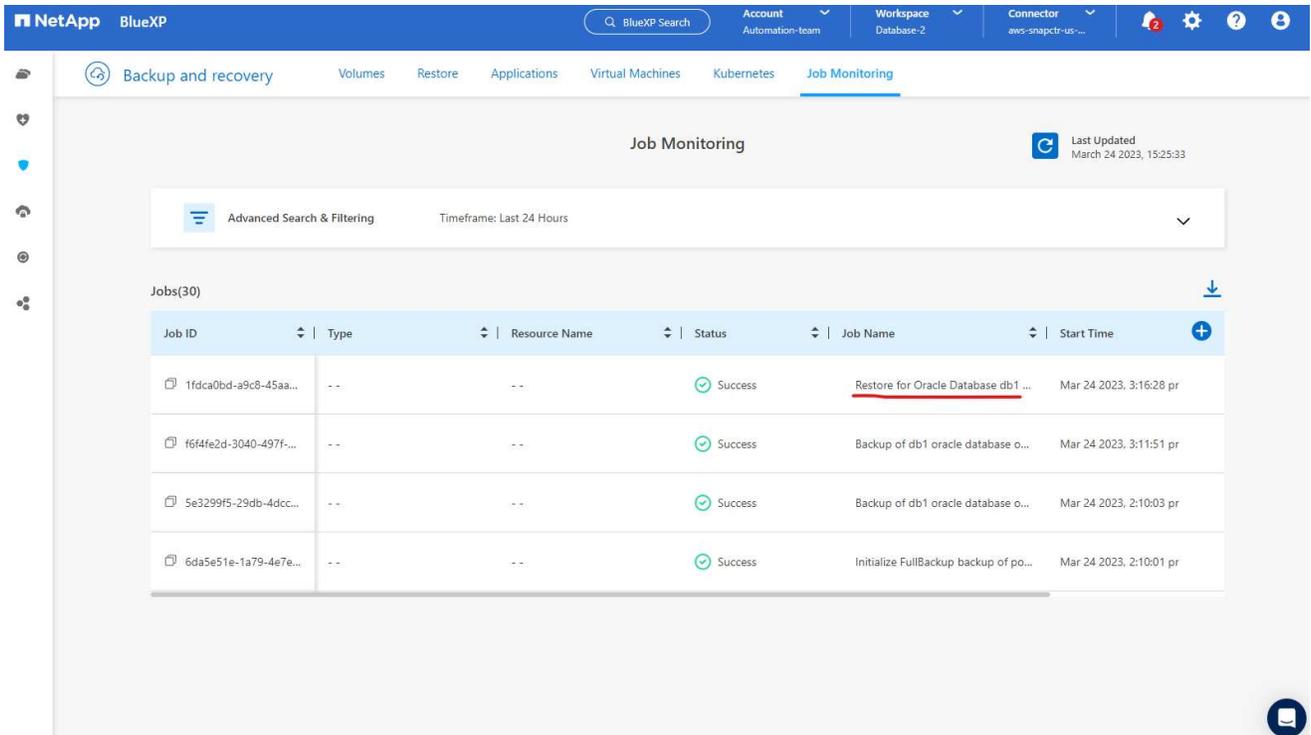
1. Wählen Sie Ihre Wiederherstellungseinstellung. Wenn Sie sicher sind, dass sich nach der Sicherung nichts an der physischen Datenbankstruktur geändert hat (z. B. das Hinzufügen einer Datendatei oder einer Datenträgergruppe), können Sie die Option **Force in place restore** verwenden, die im Allgemeinen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

The screenshot shows the 'Restore Settings' dialog for 'db1'. It is divided into 'Restore Scope' and 'Recovery Scope' sections. Under 'Restore Scope', the 'All Data Files' option is selected, and the 'Force in place restore' checkbox is checked. Under 'Recovery Scope', the 'All Logs' option is selected. The 'Archive Log Files Locations' field contains '/mnt/log_location001'. There are 'Previous' and 'Next' buttons at the bottom.

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.



NetApp BlueXP Account Automation-team Workspace Database-2 Connector aws-snapctr-us-...

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

Job Monitoring > Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4

Job Details

Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4 Expand All

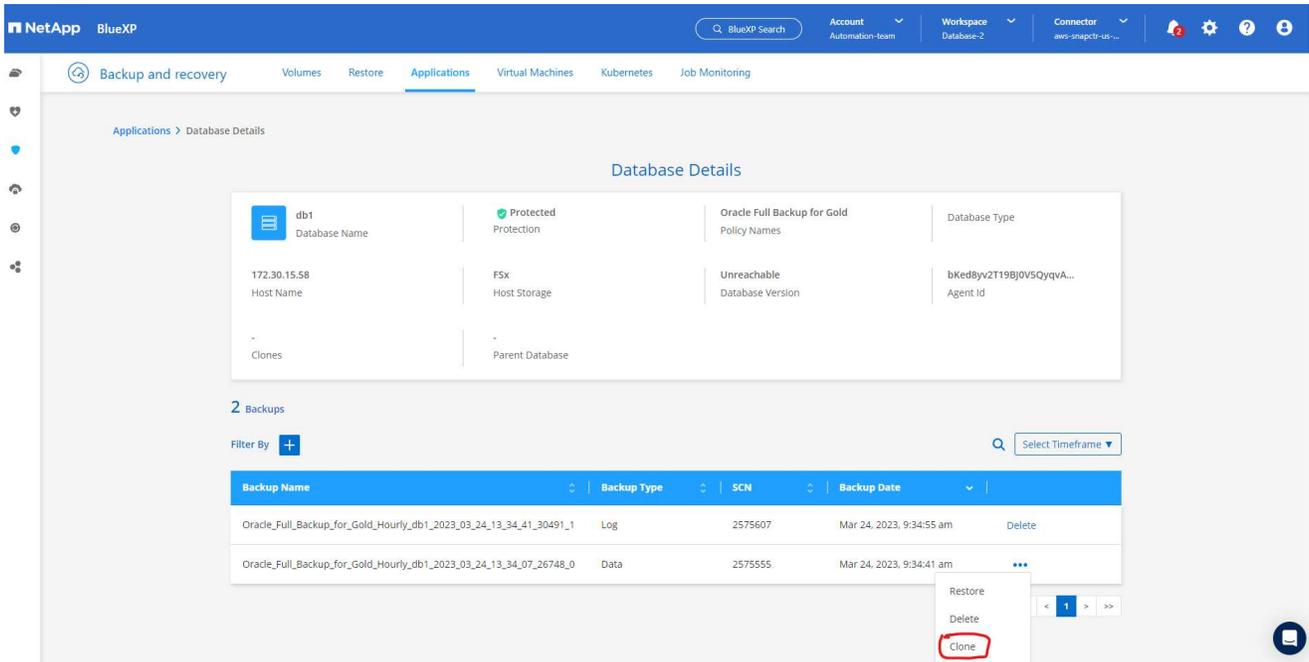
Sub-Jobs(6)

Job Name	Job ID	Start Time	End Time	Duration
Restore for Oracle Database db1 using backup ...	1fdca0bd-a9c8-45aa-9d...	Mar 24 2023, 3:16:28 pm	Mar 24 2023, 3:23:33 pm	7 Minutes
Post Restore Cleanup	2096a8e4-889d-4b2a-9...	Mar 24 2023, 3:23:18 pm	Mar 24 2023, 3:23:32 pm	14 Seconds
Post Restore	fb7b1171-966f-4228-9e...	Mar 24 2023, 3:20:06 pm	Mar 24 2023, 3:23:19 pm	3 Minutes
Restore	0f4580d0-6598-458b-a7...	Mar 24 2023, 3:17:49 pm	Mar 24 2023, 3:20:07 pm	2 Minutes

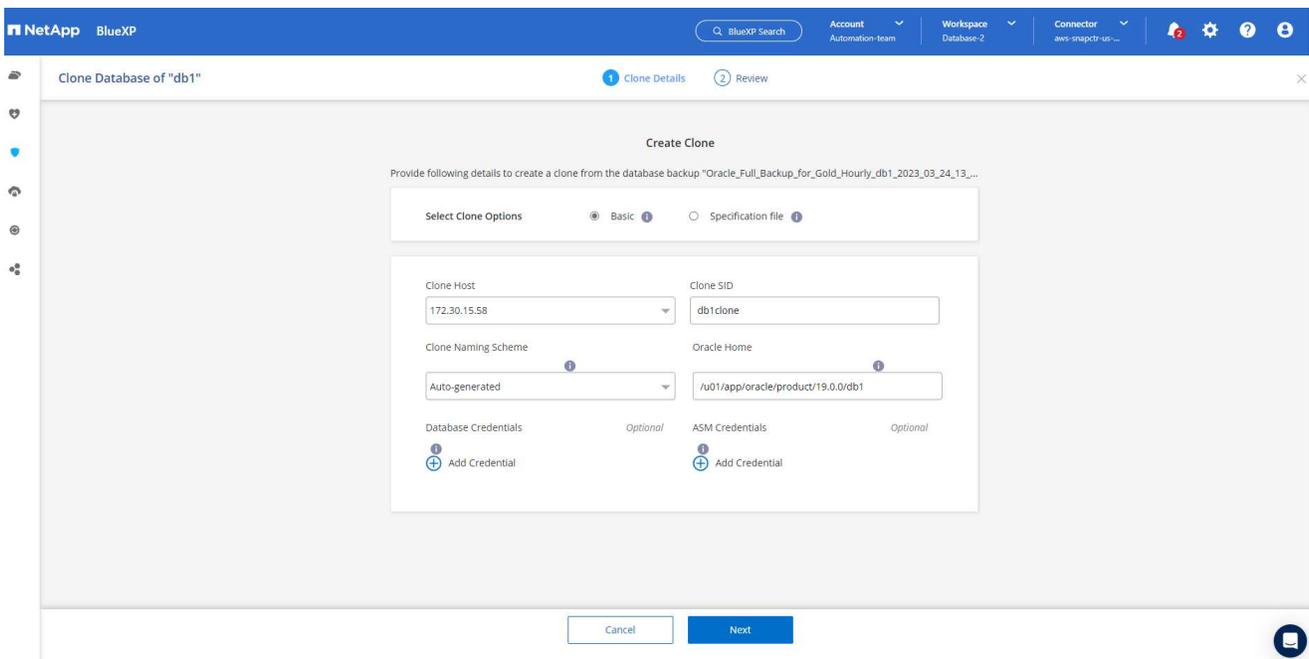
Oracle-Datenbankklon

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.

The screenshot shows the 'Create Clone' configuration screen in the NetApp BlueXP interface. The title is 'Clone Database of "db1"'. The interface is divided into two steps: '1 Clone Details' and '2 Review'. The 'Create Clone' section prompts the user to provide details for creating a clone from a database backup. The backup name is 'Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19...'. Under 'Select Clone Options', the 'Specification file' option is selected. A button 'Download File' is available. The 'Specification File' field contains 'db1_3_24_2023_10_14_specjson' with a 'Browse' button. The 'Clone Host' is set to '172.30.15.58' and the 'Clone SID' is 'db1clone'. There are sections for 'Database Credentials' and 'ASM Credentials', both marked as 'Optional', with 'Add Credential' buttons. At the bottom, there are 'Cancel' and 'Next' buttons.

1. Überprüfen und starten Sie den Job.

The screenshot shows the 'Review' screen in the NetApp BlueXP interface. The title is 'Clone Database of "db1"'. The interface is divided into two steps: '1 Clone Details' and '2 Review'. The 'Review' section displays the configuration details for the clone job. The details are organized into two columns: 'General' and 'Database parameters'. The 'General' column includes Backup Name, Clone SID, Clone Host, Datafile locations, Control files, Redo logs, and Recovery scope. The 'Database parameters' column includes the Backup Name, Clone SID, Clone Host, and Datafile locations. The 'Redo logs' section lists three Redo Groups with their TotalSize and Path. At the bottom, there are 'Previous' and 'Clone' buttons.

General	Database parameters
Backup Name	Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_34_07_26748_0
Clone SID	db1clone
Clone Host	172.30.15.58
Datafile locations	DATA_db1clone
Control files	+DATA_db1clone/db1clone/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redo/redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redo/redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redo/redo03_01.log
Recovery scope	Until cancel using selected backup's archive logs

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

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and dropdown menus for 'Account Automation-team', 'Workspace Database-2', and 'Connector aws-snapc1r-1b...'. The main menu has 'Backup and recovery' selected, with sub-menus for 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Job Monitoring' page displays 'Job Details' for Job ID: cd30abaf-fbe2-4052-a6db-4bf965a8d29b. It lists 'Sub-Jobs(2)' in a table:

Job Name	Job ID	Start Time	End Time	Duration
Cloning Oracle Database db1 as db1clone on h...	cd30abaf-fbe2-4052-a6...	Mar 24 2023, 1:30:36 pm		--
Running pre scripts	511f52c1-853a-4ec6-a4f...	Mar 24 2023, 1:30:41 pm	Mar 24 2023, 1:30:41 pm	0 Second
Validating clone request	f93a6c44-2eb2-4c5e-9f...	Mar 24 2023, 1:30:35 pm	Mar 24 2023, 1:30:42 pm	7 Seconds

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/oracle/product/19.0.0/db1,STABLE
ora.db1clone.db
      1        ONLINE  ONLINE      ip-172-30-15-58          Open,HOME=/u01/app/oracle/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$databases;

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

- Amazon FSx ONTAP

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

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.