



TR-4977: Sichern, Wiederherstellen und Klonen von Oracle-Datenbanken mit SnapCenter Services – Azure

NetApp database solutions

NetApp
August 18, 2025

Inhalt

TR-4977: Sichern, Wiederherstellen und Klonen von Oracle-Datenbanken mit SnapCenter Services –

Azure	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	4
Definieren Sie in BlueXP eine Anmeldeinformation für den Zugriff auf Azure-Ressourcen	12
Einrichtung der SnapCenter -Dienste	15
Oracle-Datenbanksicherung	22
Wiederherstellung und Wiederherstellung von Oracle-Datenbanken	26
Oracle-Datenbankklon	29
Weitere Informationen	34

TR-4977: Sichern, Wiederherstellen und Klonen von Oracle-Datenbanken mit SnapCenter Services – Azure

Allen Cao, Niyaz Mohamed, NetApp

Diese Lösung bietet einen Überblick und Details zum Sichern, Wiederherstellen und Klonen von Oracle-Datenbanken mit NetApp SnapCenter SaaS unter Verwendung der BlueXP -Konsole.

Zweck

SnapCenter Services ist die SaaS-Version des klassischen SnapCenter -Datenbankverwaltungs-UI-Tools, das über die NetApp BlueXP -Cloud-Verwaltungskontrolle verfügbar ist. Es ist ein integraler Bestandteil des NetApp Cloud-Backup- und Datenschutzangebots für Datenbanken wie Oracle und HANA, die auf Azure NetApp Files 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 Azure NetApp Files Volumes und Azure-Compute-Instanzen bereitgestellt sind. Mit der webbasierten BlueXP -Benutzeroberfläche ist es sehr einfach, den Datenschutz für eine auf Azure NetApp Files bereitgestellte Oracle-Datenbank einzurichten.

Diese Lösung ist für die folgenden Anwendungsfälle geeignet:

- Datenbanksicherung mit Snapshots für Oracle-Datenbanken, die in Azure NetApp Files und Azure VMs gehostet werden
- Oracle-Datenbankwiederherstellung im Falle eines Ausfalls
- Schnelles Klonen von Primärdatenbanken für Entwicklungs-, Testumgebungen oder andere Anwendungsfälle

Publikum

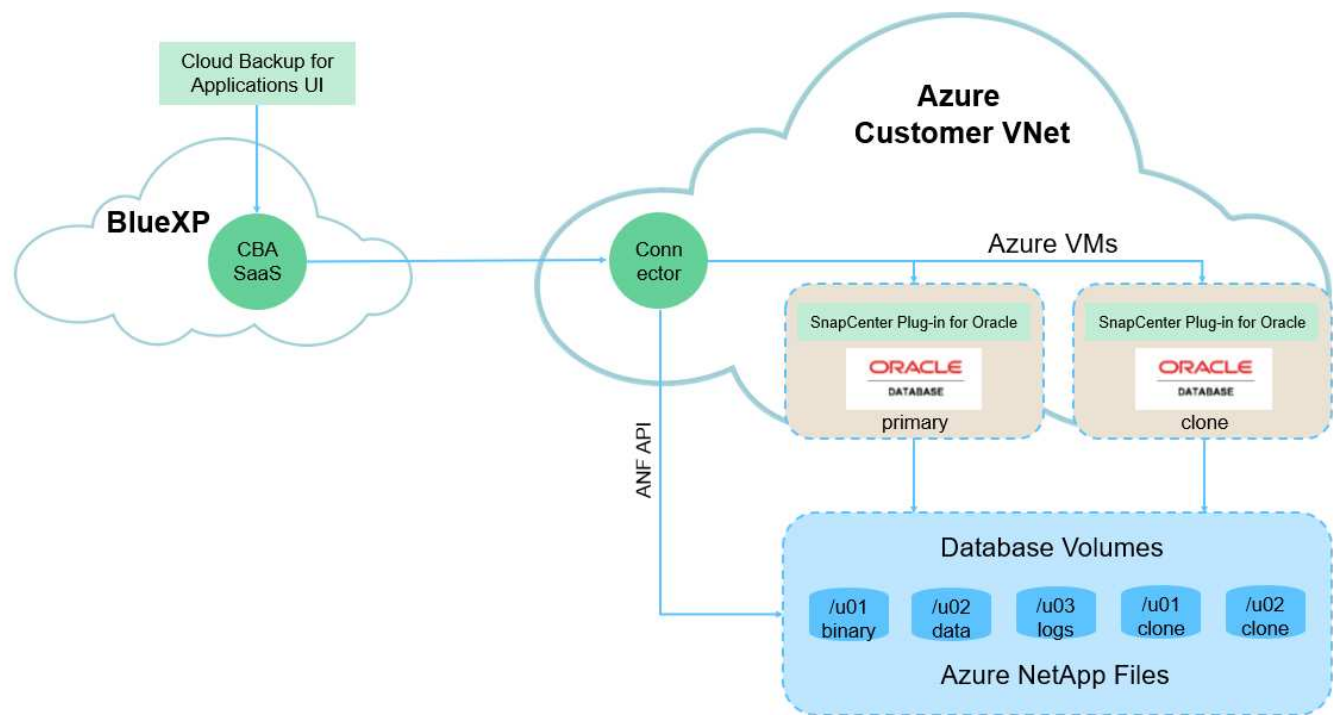
Diese Lösung ist für die folgenden Zielgruppen gedacht:

- Der DBA, der Oracle-Datenbanken verwaltet, die auf Azure NetApp Files -Speicher ausgeführt werden
- Der Lösungsarchitekt, der daran interessiert ist, die Sicherung, Wiederherstellung und das Klonen von Oracle-Datenbanken in Azure zu testen
- Der Speicheradministrator, der den Azure NetApp Files Speicher unterstützt und verwaltet
- Der Anwendungsbesitzer, dem die Anwendungen gehören, die im Azure NetApp Files Speicher und auf Azure-VMs bereitgestellt werden

Test- und Validierungsumgebung für Lösungen

Das Testen und Validieren dieser Lösung wurde in einer Laborumgebung durchgeführt, die möglicherweise nicht der endgültigen Bereitstellungsumgebung entspricht. Weitere Informationen finden Sie im Abschnitt

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

Azure NetApp Files Speicher	Premium-Service-Level	Auto-QoS-Typ und 4 TB Speicherkapazität im Test
Azure-Instanz für Compute	Standard B4ms (4 vcpus, 16 GiB Speicher)	Zwei Instanzen bereitgestellt, eine als primärer DB-Server und die andere als Klon-DB-Server

Software

RedHat Linux	Red Hat Enterprise Linux 8.7 (LVM) – x64 Gen2	RedHat-Abonnement zum Testen bereitgestellt
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 v2.5.0-2822	Agentenversion v2.5.0-2822

Wichtige Faktoren für die Bereitstellungsüberlegungen

- **Connector muss im selben virtuellen Netzwerk/Subnetz wie Datenbanken und Azure NetApp Files bereitgestellt werden.** Wenn möglich, sollte der Connector in denselben virtuellen Azure-Netzwerken und Ressourcengruppen bereitgestellt werden, wodurch die Konnektivität zum Azure NetApp Files -Speicher und den Azure-Compute-Instanzen ermöglicht wird.
- **Ein Azure-Benutzerkonto oder Active Directory-Dienstprinzipal, das im Azure-Portal für den SnapCenter Connector erstellt wurde.** Für die Bereitstellung eines BlueXP -Connectors sind bestimmte Berechtigungen zum Erstellen und Konfigurieren einer virtuellen Maschine und anderer Rechenressourcen, zum Konfigurieren des Netzwerks und zum Zugriff auf das Azure-Abonnement erforderlich. Außerdem sind Berechtigungen erforderlich, um später Rollen und Berechtigungen für den Betrieb des Connectors zu erstellen. Erstellen Sie in Azure eine benutzerdefinierte Rolle mit Berechtigungen und weisen Sie sie dem Benutzerkonto oder Dienstprinzipal zu. Weitere Einzelheiten finden Sie unter dem folgenden Link: "[Einrichten von Azure-Berechtigungen](#)".
- **Ein in der Azure-Ressourcengruppe erstelltes SSH-Schlüsselpaar.** Das SSH-Schlüsselpaar wird dem Azure-VM-Benutzer für die Anmeldung beim Connector-Host und dem Datenbank-VM-Host für die Bereitstellung und Ausführung eines Plug-Ins zugewiesen. Die BlueXP Konsolen-Benutzeroberfläche verwendet den SSH-Schlüssel, um das SnapCenter -Dienst-Plug-In auf dem Datenbank-Host bereitzustellen und so die Plug-In-Installation und Datenbankerkennung des Anwendungshosts in einem Schritt zu ermöglichen.
- **Ein Anmeldeinformationselement, das der BlueXP Konsoleinstellung hinzugefügt wurde.** Um Azure NetApp Files Speicher zur BlueXP Arbeitsumgebung hinzuzufügen, muss in den BlueXP -Konsoleinstellungen eine Anmeldeinformation eingerichtet werden, die Berechtigungen für den Zugriff auf Azure NetApp Files von der BlueXP -Konsole aus erteilt.
- **java-11-openjdk auf dem Azure VM-Datenbankinstanzhost 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 Oracle-Datenbank zu schützen, die auf einem Azure NetApp Files -Speicher und einer Azure-Compute-Instanz bereitgestellt wird.

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 Azure NetApp Files.
- Sehen Sie sich die folgende Video-Komplettlösung an

[Video zur Bereitstellung von Oracle und ANF](#)

Voraussetzungen für die Bereitstellung des SnapCenter -Dienstes

Für die Bereitstellung sind die folgenden Voraussetzungen erforderlich.

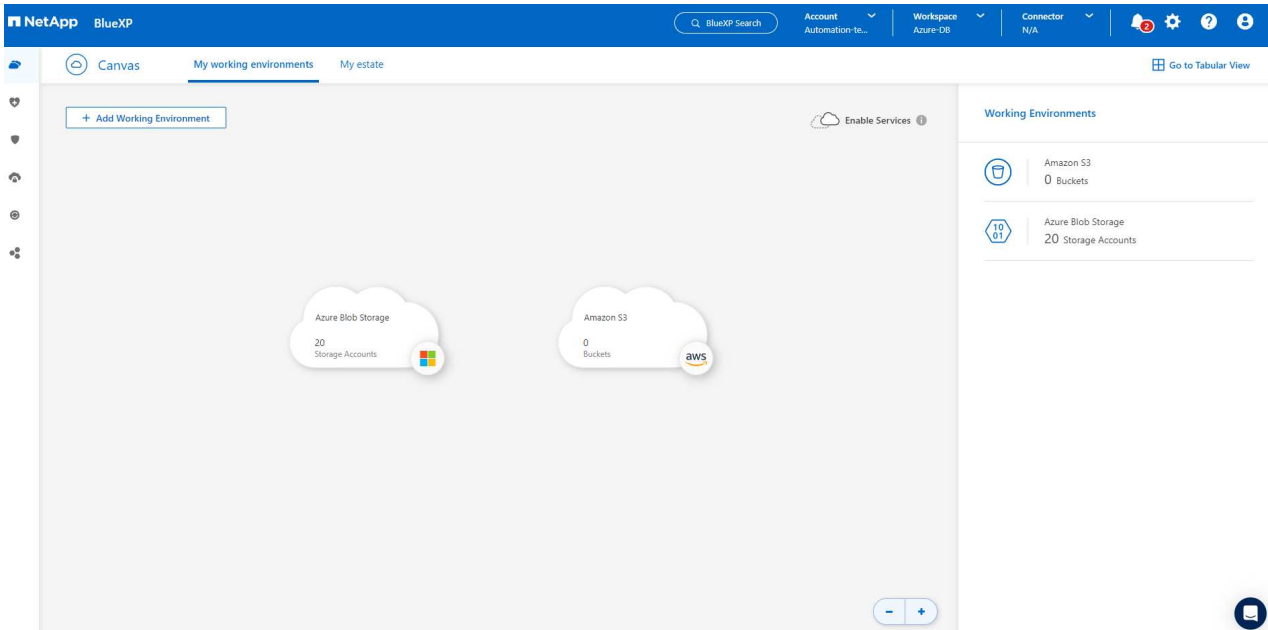
1. Ein primärer Oracle-Datenbankserver auf einer Azure-VM-Instanz mit einer vollständig bereitgestellten und laufenden Oracle-Datenbank.
2. Ein in Azure bereitgestellter Kapazitätspool des Azure NetApp Files -Speicherdienstes, der über die Kapazität verfügt, den im Abschnitt „Hardwarekomponenten“ aufgeführten Datenbankspeicherbedarf zu erfüllen.
3. Ein sekundärer Datenbankserver auf einer Azure-VM-Instanz, 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 Oracle-Produktionsdatenbank erfordern.
4. Weitere Informationen zur Oracle-Datenbankbereitstellung auf Azure NetApp Files und Azure Compute-Instanzen finden Sie unter ["Bereitstellung und Schutz von Oracle-Datenbanken auf Azure NetApp Files"](#) .

Onboarding zur BlueXP -Vorbereitung

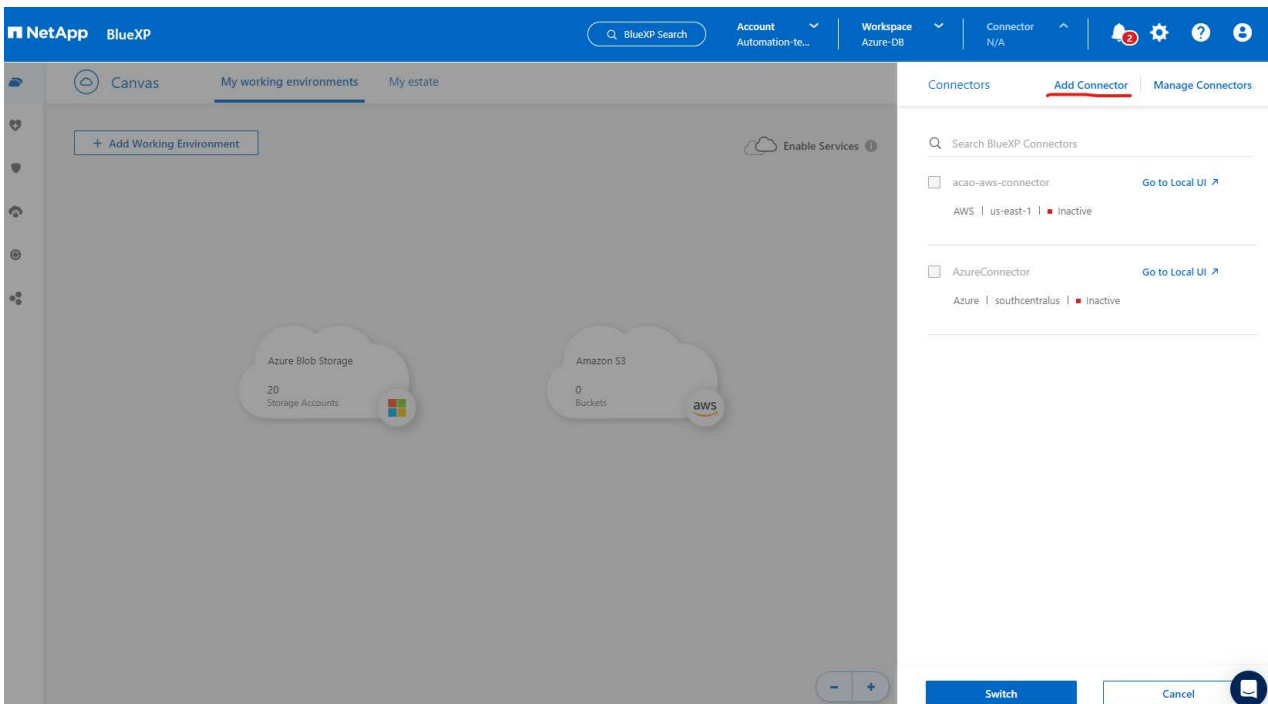
1. Verwenden Sie den Link ["NetApp BlueXP"](#) um sich für den Zugriff auf die BlueXP -Konsole anzumelden.
2. Erstellen Sie ein Azure-Benutzerkonto oder einen Active Directory-Dienstprinzipal und erteilen Sie Berechtigungen mit Rolle im Azure-Portal für die Bereitstellung des Azure-Connectors.
3. Um BlueXP für die Verwaltung von Azure-Ressourcen einzurichten, fügen Sie eine BlueXP -Anmeldeinformation mit Details eines Active Directory-Dienstprinzipals hinzu, den BlueXP zur Authentifizierung bei Azure Active Directory verwenden kann (App-Client-ID), ein Clientgeheimnis für die Dienstprinzipalanwendung (Clientgeheimnis) und die Active Directory-ID für Ihre Organisation (Mandanten-ID).
4. Sie benötigen außerdem das virtuelle Azure-Netzwerk, die Ressourcengruppe, die Sicherheitsgruppe, einen SSH-Schlüssel für den VM-Zugriff usw., die für die Bereitstellung des Connectors und die Installation des Datenbank-Plugins bereit sind.

Bereitstellen eines Connectors für SnapCenter -Dienste

1. Melden Sie sich bei der BlueXP -Konsole an.



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



3. Wählen Sie Ihren Cloud-Anbieter (in diesem Fall **Microsoft Azure**).

Provider

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



[Deploy the Connector on your premises](#) 

Continue



- Überspringen Sie die Schritte **Berechtigung**, **Authentifizierung** und **Netzwerk**, wenn Sie diese bereits in Ihrem Azure-Konto eingerichtet haben. Wenn nicht, müssen Sie diese konfigurieren, bevor Sie fortfahren. Von hier aus können Sie auch die Berechtigungen für die Azure-Richtlinie abrufen, auf die im vorherigen Abschnitt verwiesen wird. [Onboarding zur BlueXP -Vorbereitung](#) ."

Deploying a BlueXP Connector

The BlueXP Connector is a crucial component for the day-to-day use of BlueXP.

It's used to connect BlueXP's services to your hybrid-cloud environments.

The BlueXP 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 BlueXP Connector installation.

Permissions

Ensure that the Azure user or service principal you've provided has sufficient permissions

Authentication

Choose between two methods: an

[Azure user account](#) or an

[Active Directory service principal](#)

Networking

Ensure that you have details on the VNet and subnet in which the BlueXP Connector will reside

[Skip to Deployment](#)

[Previous](#)

[Continue](#)



5. Klicken Sie auf **Zur Bereitstellung springen**, um Ihren Connector **Virtual Machine Authentication** zu konfigurieren. Fügen Sie das SSH-Schlüsselpaar, das Sie während des Onboardings in der Azure-Ressourcengruppe erstellt haben, zur BlueXP -Vorbereitung für die Connector-OS-Authentifizierung hinzu.

1

VM Authentication

2

Details

3

Network

4

Security Group

5

Review

Virtual Machine Authentication

You are logged in with Azure user: [acao@netapp.com](#)

Tenant: Hybrid Cloud TME

Subscription

Hybrid Cloud TME Onprem

Location

South Central US

Resource Group

☐ Create New ☒ Use Existing

Resource Group

ANFAVSRG

Authentication Method

☐ Password ☒ Public Key

User Name

azureuser

Enter SSH Public Key

-----BEGIN RSA PRIVATE KEY----- MIIGSAIBAAKCA...

[Previous](#)[Next](#)

6. Geben Sie einen Namen für die Connector-Instanz ein, wählen Sie **Erstellen** aus, akzeptieren Sie den Standard-**Rollennamen** unter **Details** und wählen Sie das Abonnement für das Azure-Konto aus.

Add BlueXP Connector - Azure

More Information

✓ VM Authentication

2 Details

3 Network

4 Security Group

5 Review

Details

Connector Instance Name

AzureConnector

Connector Role

Create

Attach existing

Manual

Role Name

BlueXP Operator-5519248

Subscriptions to apply with the role

Hybrid Cloud TME Onprem

Add Tags to Connector Instance

Previous

Next

7. Konfigurieren Sie das Netzwerk mit dem richtigen **VNet**, **Subnetz** und deaktivieren Sie die **öffentliche IP**, stellen Sie jedoch sicher, dass der Connector in Ihrer Azure-Umgebung über Internetzugang verfügt.

Add BlueXP Connector - Azure
More Information

VM Authentication
Details
3 Network
4 Security Group
5 Review

Network

Connectivity

VNet

Subnet

Public IP

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

Proxy Configuration (Optional)

HTTP Proxy

Define Credentials for this Proxy

Upload a root certificate

Previous
Next

8. Konfigurieren Sie die **Sicherheitsgruppe** für den Connector, der HTTP-, HTTPS- und SSH-Zugriff zulässt.

Add BlueXP Connector - Azure
More Information

VM Authentication
Details
Network
4 Security Group
5 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

HTTP (Port 80)

Source Type

Source (CIDR)

HTTPS (Port 443)

Source Type

Source (CIDR)

SSH (Port 22)

Source Type

Source (CIDR)

Previous
Next

9. 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-VM im Azure-Portal angezeigt.

Add BlueXP Connector - Azure

[More Information](#)

✓ VM Authentication

✓ Details

✓ Network

✓ Security Group

5 Review

Review

Code for Terraform Automation

BlueXP Connector Name	AzureConnector
Subscription	Hybrid Cloud TME Onprem
Location	South Central US
Resource Group	Existing - ANFAVSRG
Role	New - BlueXP Operator-5519248
Authentication Method	Password (user: azureuser)
VNet	ANFAVVal
Subnet	VM_Sub
Public IP	Enable
Proxy	None
Security Group	HTTP: 0.0.0.0/0, HTTPS: 0.0.0.0/0, SSH: 0.0.0.0/0

[Previous](#)[Add](#)

10. Nachdem der Connector bereitgestellt wurde, wird der neu erstellte Connector im Dropdown-Menü **Connector** angezeigt.

NetApp BlueXP

Q BlueXP Search

Account Automation-to...

Workspace Azure-DB

Connector AzureConnector

2

?

Canvas

My working environments

My estate

+ Add Working Environment

Enable Services

Azure Blob Storage

20 Storage Accounts

Amazon S3

0 Buckets

Working Environments

Amazon S3

0 Buckets

Azure Blob Storage

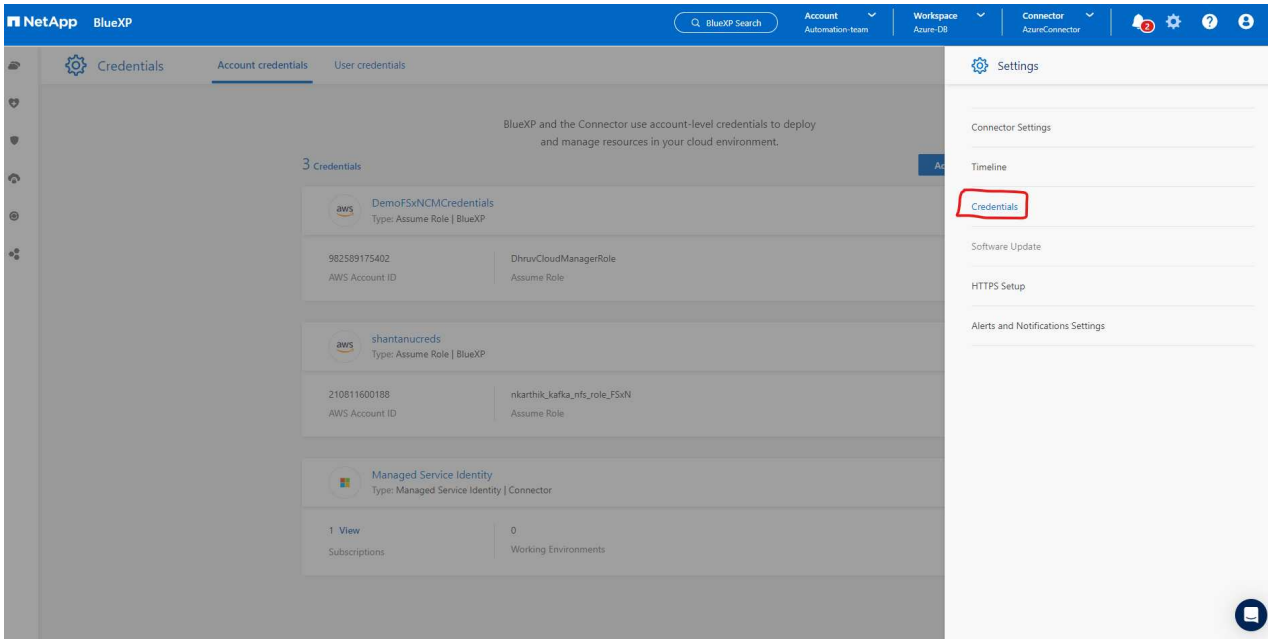
20 Storage Accounts

-

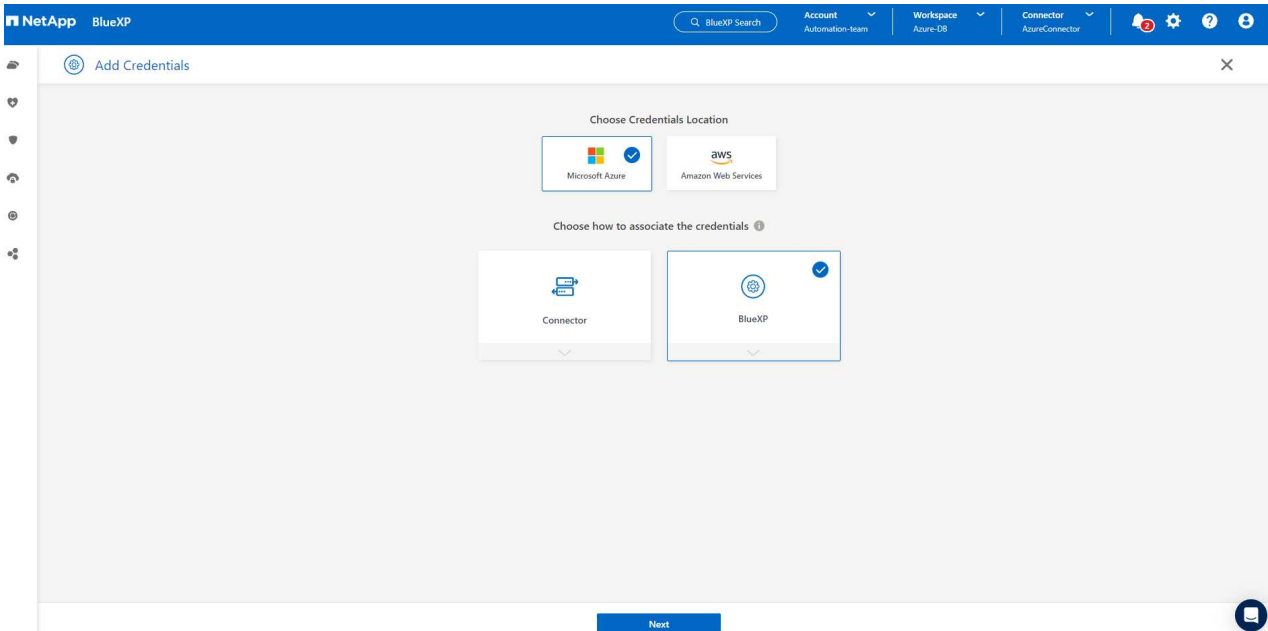
+

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

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



2. Wählen Sie als Speicherort der Anmeldeinformationen „**Microsoft Azure – BlueXP**“.



3. Definieren Sie Azure-Anmeldeinformationen mit dem richtigen **Client Secret**, **Client ID** und **Tenant ID**, die während des vorherigen BlueXP -Onboarding-Prozesses erfasst worden sein sollten.

NetApp BlueXP Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector 2 ? !

Add Credentials ✓ Credentials Type 2 Define Credentials 3 Marketplace Subscription 4 Review ✕

Define Microsoft Azure Credentials
Learn more about Azure application credentials

Credentials Name ? Client Secret

Azure_Hybrid_TME

Application (client) ID Directory (tenant) ID

2fbc9be5-a259-4539-bb57-036b176f5cc7 9bb0aab6-5c98-419b-9cfd-7a38bd496...

☒ I have verified that the Azure role assigned to the Active Directory service principal matches BlueXP policy requirements.

Previous Next !

4. Überprüfen und **Hinzufügen**

NetApp BlueXP Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector 2 ? !

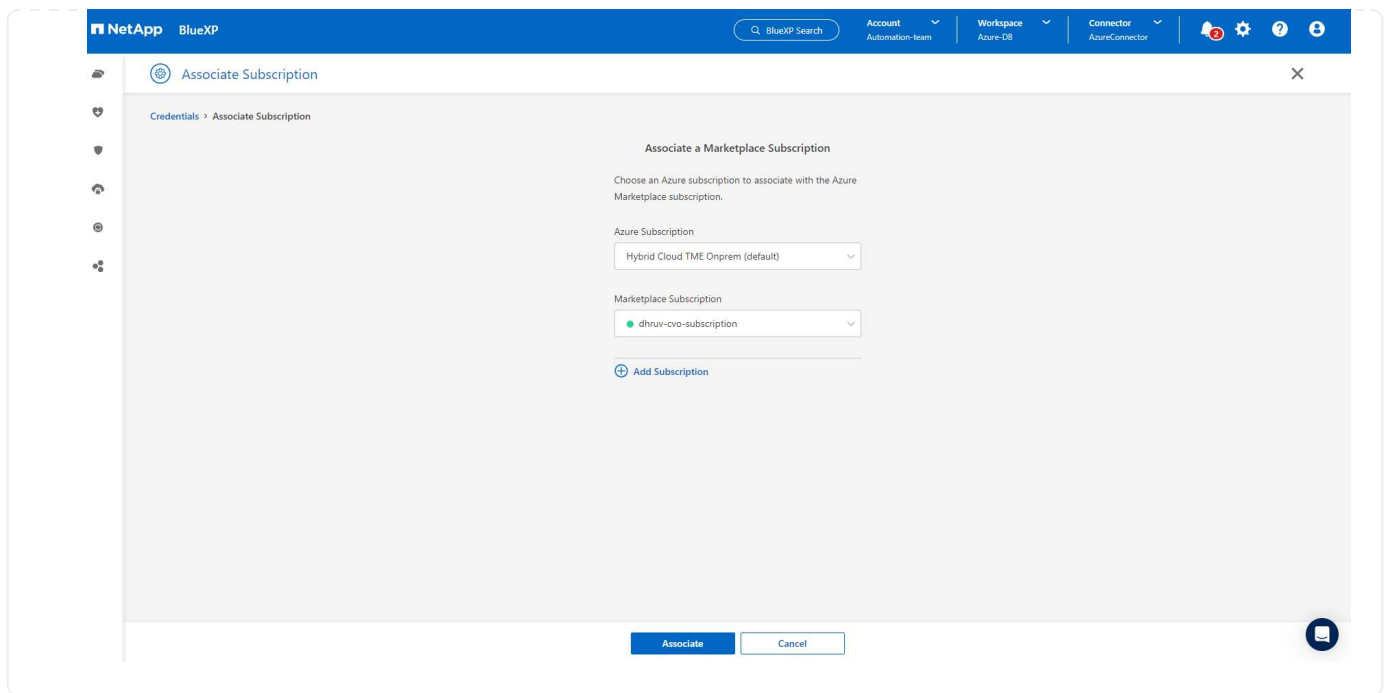
Add Credentials ✓ Credentials Type ✓ Define Credentials 3 Review ✕

Review

Credentials Type	Azure
Credentials Name	Azure_Hybrid_TME
Credential Storage	Cloud Manager
Application (client) ID	2fbc9be5-a259-4539-bb57-036b176f5cc7
Directory (tenant) ID	9bb0aab6-5c98-419b-9cfd-7a38bd496e1f

Previous Add !

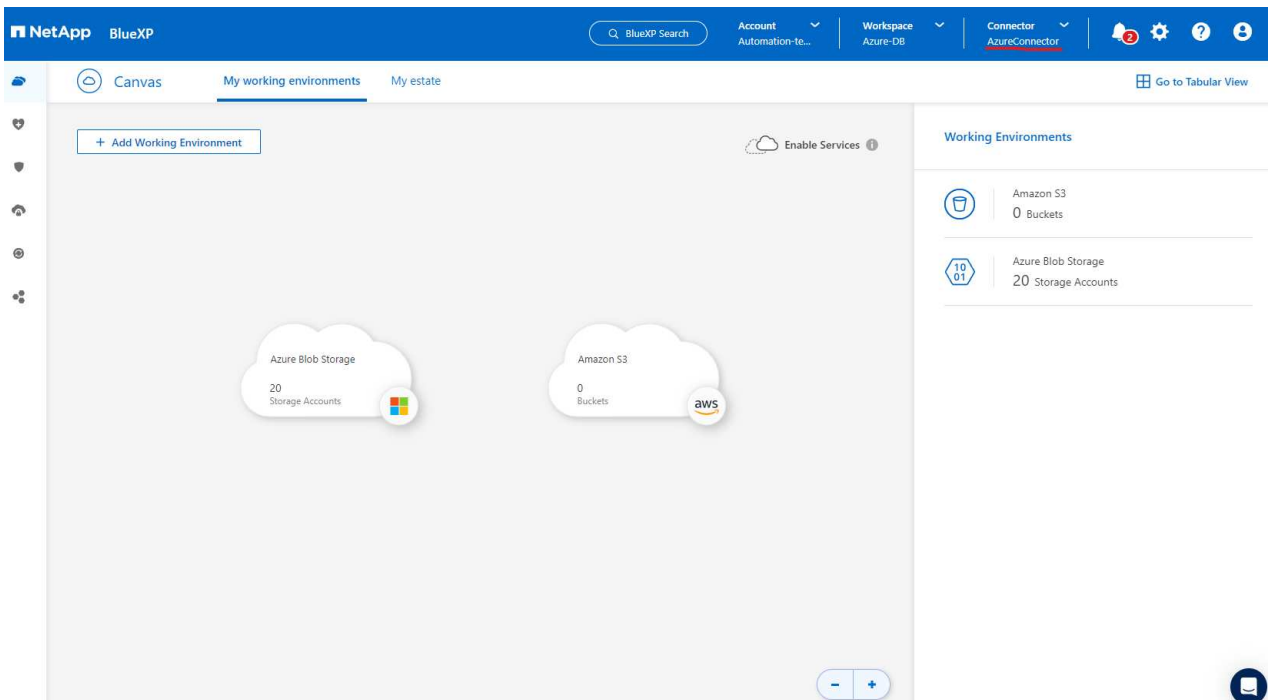
5. Möglicherweise müssen Sie den Anmeldeinformationen auch ein **Marketplace-Abonnement** zuordnen.



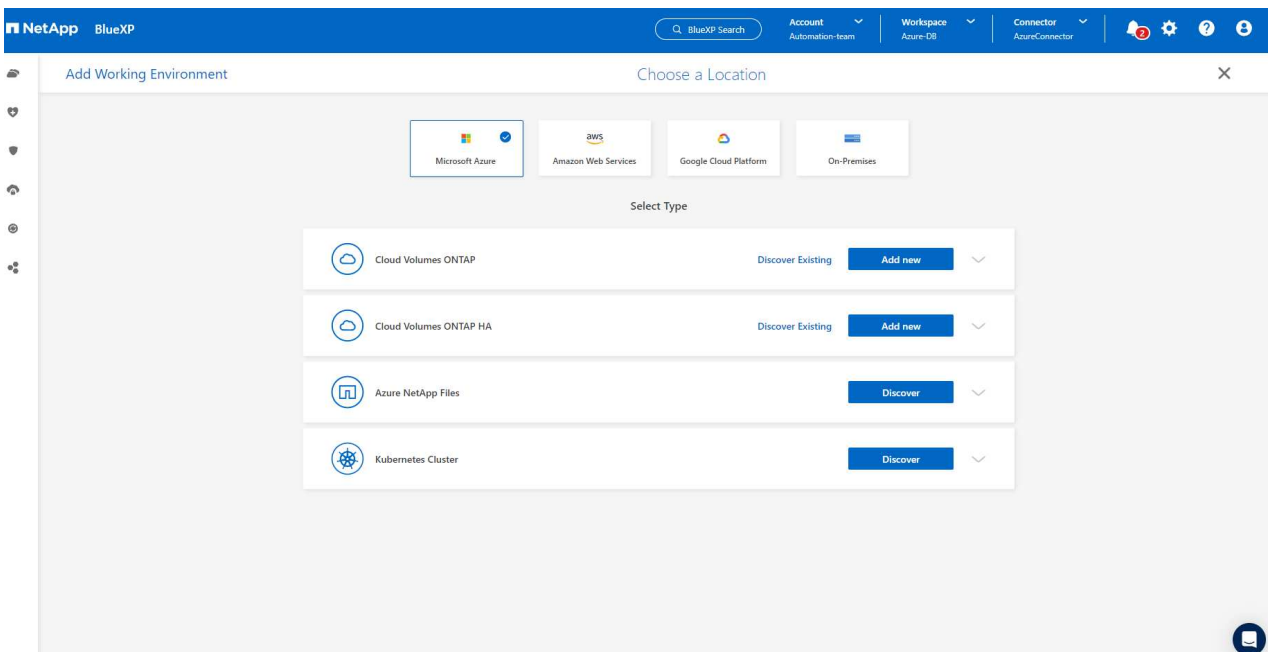
Einrichtung der SnapCenter -Dienste

Nachdem die Azure-Anmeldeinformationen konfiguriert wurden, können die SnapCenter -Dienste nun mit den folgenden Verfahren eingerichtet werden:

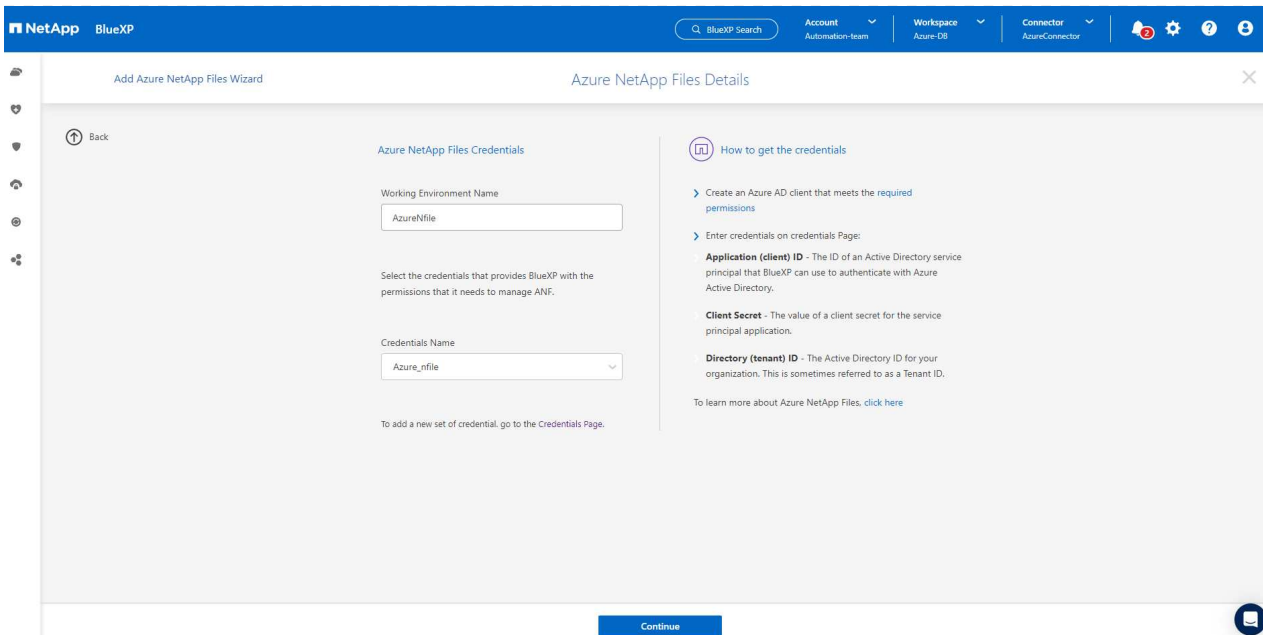
1. Zurück zur Canvas-Seite: Klicken Sie unter **Meine Arbeitsumgebung** auf **Arbeitsumgebung hinzufügen**, um die in Azure bereitgestellten Azure NetApp Files zu ermitteln.



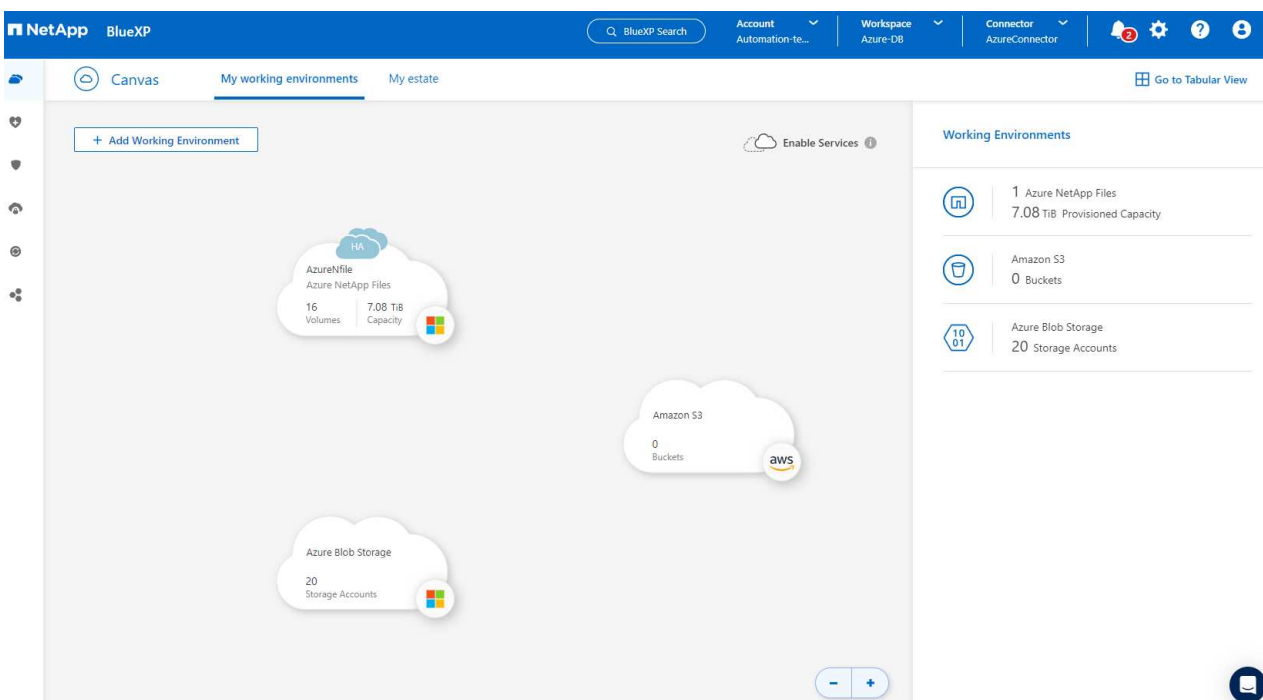
2. Wählen Sie als Speicherort **Microsoft Azure** und klicken Sie auf **Erkennen**.



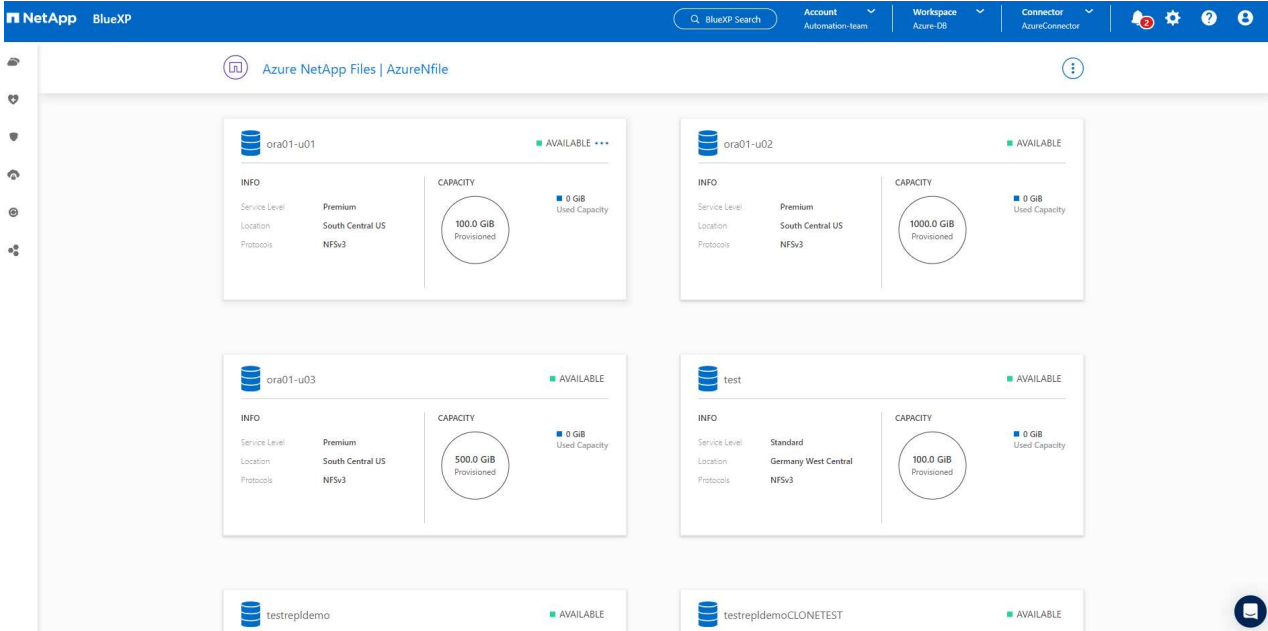
3. Benennen Sie **Arbeitsumgebung**, wählen Sie den im vorherigen Abschnitt erstellten **Anmeldeinformationsnamen** und klicken Sie auf **Weiter**.



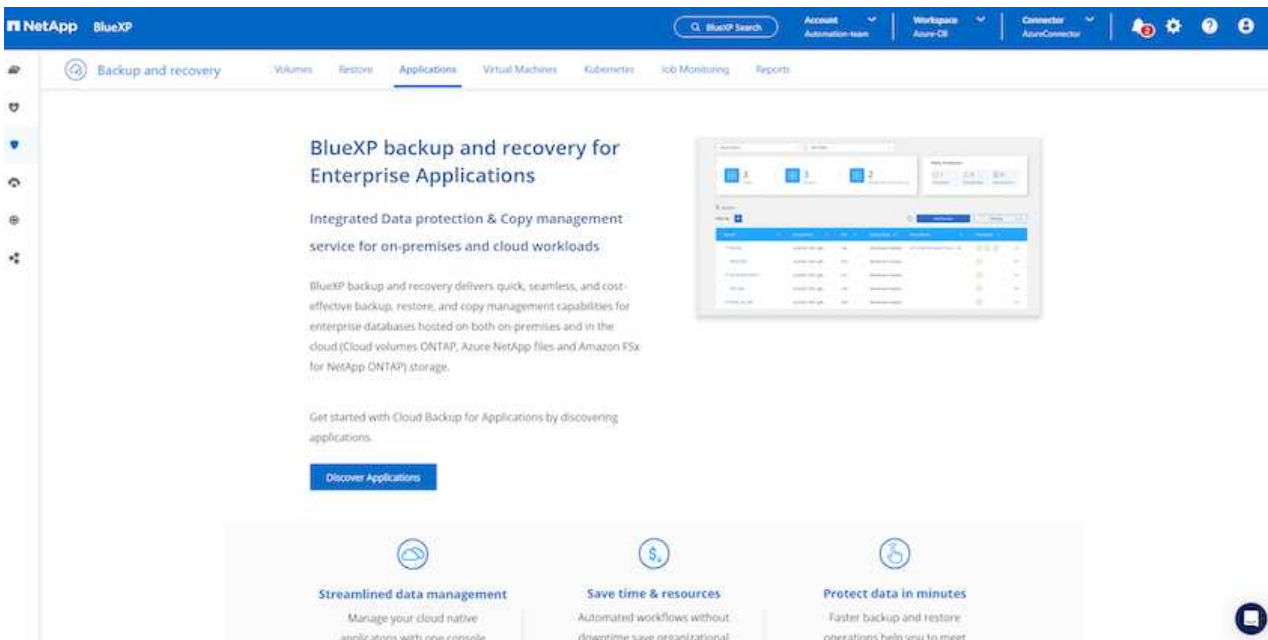
4. Die BlueXP Konsole kehrt zu **Meine Arbeitsumgebungen** zurück und hat festgestellt, dass Azure NetApp Files von Azure jetzt auf **Canvas** angezeigt werden.



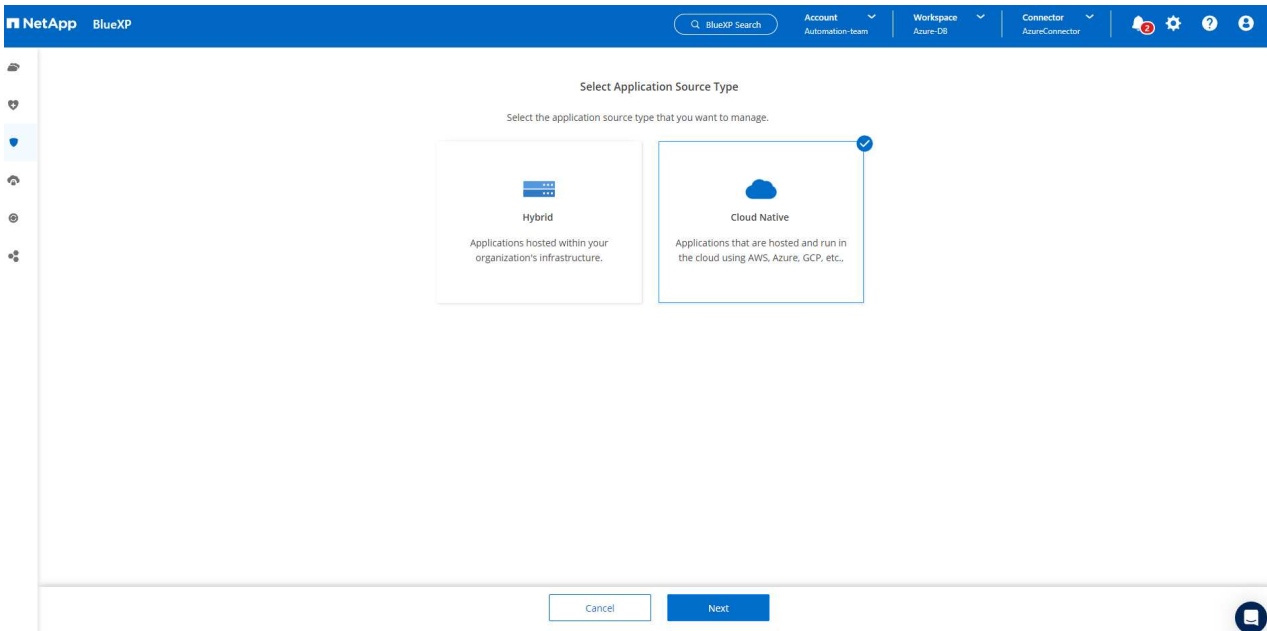
5. Klicken Sie auf das Symbol * Azure NetApp Files* und dann auf **Arbeitsumgebung aufrufen**, um die im Azure NetApp Files -Speicher bereitgestellten Oracle-Datenbankvolumes anzuzeigen.



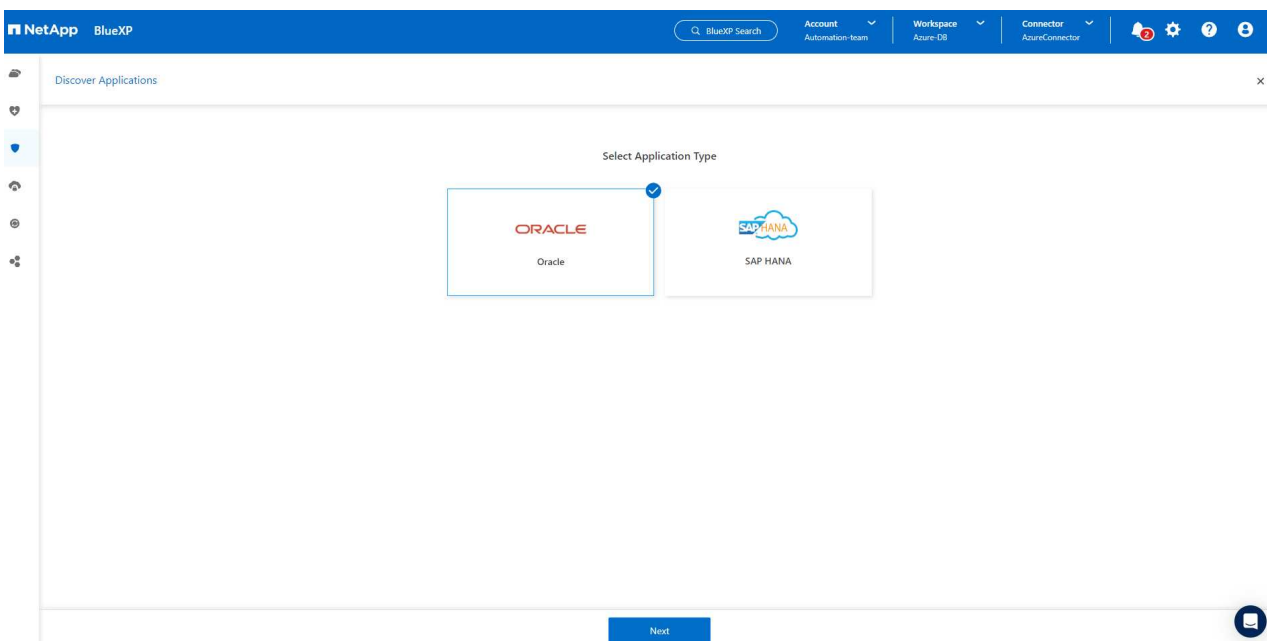
6. Bewegen Sie in der linken Seitenleiste der Konsole den Mauszeiger über das Schutzsymbol und klicken Sie dann auf **Schutz > Anwendungen**, um die Startseite „Anwendungen“ zu öffnen. Klicken Sie auf **Anwendungen erkennen**.



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



8. Wählen Sie **Oracle** als Anwendungstyp und klicken Sie auf **Weiter**, um die Seite mit den Hostdetails zu öffnen.



9. Wählen Sie **SSH verwenden** und geben Sie die Oracle Azure VM-Details an, z. B. **IP-Adresse**, **Connector**, **Benutzername** für die Azure VM-Verwaltung, z. B. „azureuser“. Klicken Sie auf **Privaten SSH-Schlüssel hinzufügen**, um das SSH-Schlüsselpaar einzufügen, das Sie zum Bereitstellen der Oracle Azure-VM verwendet haben. Sie werden außerdem aufgefordert, den Fingerabdruck zu bestätigen.

NetApp BlueXP Q BlueXP Search Account Automation team Workspace Azure DB Connector AzureConnector 🔔 ⚙️ ?

Discover Applications 1 Host Details 2 Configuration 3 Review

Select host type
Provide the following details to add host and discover applications

Host Installation Type ☐ Manual ☒ Using SSH

Host FQDN or IP Connector

Username [Add SSH Private Key Optional](#)

SSH Port Plug-in Port

[Previous](#) [Next](#)

Discover Applications 1 Host Details 2 Configuration 3 Review

Select host type
Provide the following details to add host and discover applications

Host Installation Type ☐ Manual ☒ Using SSH

Validate fingerprint

Algorithm

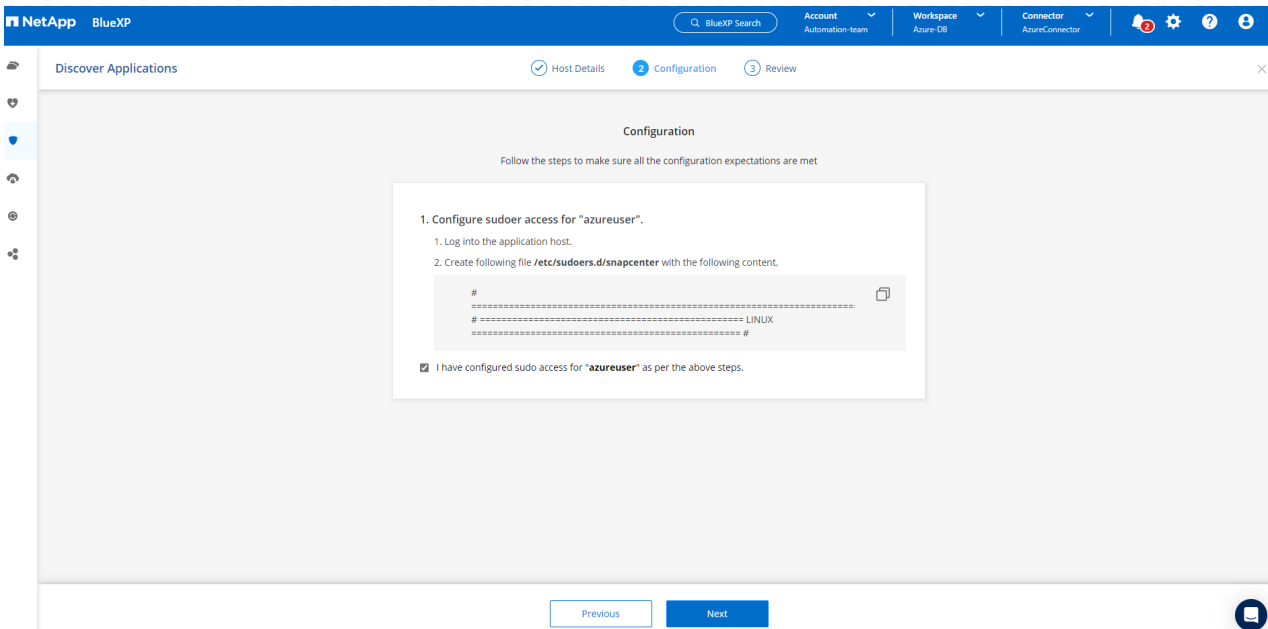
Fingerprint [📋](#)

☒ By proceeding further, I confirm that the above fingerprint for host is valid.

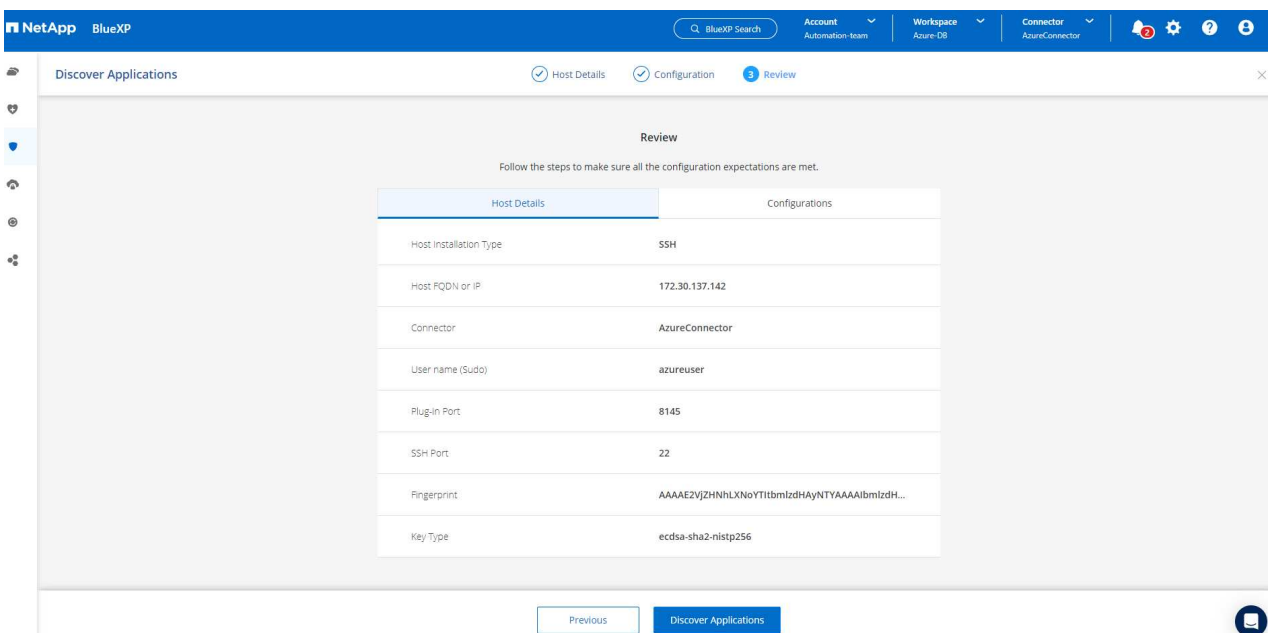
[Proceed](#) [Cancel](#)

[Previous](#) [Next](#)

10. Fahren Sie mit der nächsten **Konfigurationsseite** fort, um den Sudoer-Zugriff auf die Oracle Azure VM einzurichten.



11. Überprüfen Sie dies und klicken Sie auf **Anwendungen erkennen**, um ein Plug-In auf der Oracle Azure-VM zu installieren und die Oracle-Datenbank auf der VM in einem Schritt zu erkennen.



12. Erkannte Oracle-Datenbanken auf Azure-VM werden zu **Anwendungen** hinzugefügt und auf der Seite **Anwendungen** wird die Anzahl der Hosts und Oracle-Datenbanken innerhalb der Umgebung aufgelistet. Der **Schutzstatus** der Datenbank wird zunächst als **Ungeschützt** angezeigt.

NetApp
BlueXP

BlueXP Search

Account Automation-te...

Workspace Azure-DB

Connector AzureConnector

Backup and recovery
Volumes
Restore
Applications
Virtual Machines
Kubernetes
Job Monitoring
Reports

Cloud Native
Oracle

3 Hosts

3 ORACLE

0 Clone

Application Protection

0 Protected

3 Unprotected

3 Databases

Filter By

Manage Databases

Settings

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1st	172.30.15.124		Unprotected

1 - 3 of 3

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. Unsere Test-Oracle-Datenbank in Azure VM ist mit drei Volumes mit einem Gesamtspeicher von etwa 1,6 TiB konfiguriert. Dies gibt einen Kontext zum Zeitpunkt der Snapshot-Sicherung, Wiederherstellung und des Klonens einer Datenbank dieser Größe.

```
[oracle@acao-ora01 ~]$ df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  7.9G         0  7.9G   0% /dev
tmpfs                     7.9G         0  7.9G   0% /dev/shm
tmpfs                     7.9G      17M  7.9G   1% /run
tmpfs                     7.9G         0  7.9G   0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv 40G       23G     15G  62% /
/dev/mapper/rootvg-usrlv  9.8G      1.6G    7.7G  18% /usr
/dev/sda2                 496M     115M   381M  24% /boot
/dev/mapper/rootvg-varlv  7.9G     787M    6.7G  11% /var
/dev/mapper/rootvg-homelv 976M     323M    586M  36% /home
/dev/mapper/rootvg-optlv  2.0G      9.6M    1.8G   1% /opt
/dev/mapper/rootvg-tmplv  2.0G      22M    1.8G   2% /tmp
/dev/sda1                 500M      6.8M   493M   2% /boot/efi
172.30.136.68:/ora01-u01 100G       23G     78G  23% /u01
172.30.136.68:/ora01-u03 500G     117G    384G  24% /u03
172.30.136.68:/ora01-u02 1000G     804G    197G  81% /u02
tmpfs                     1.6G         0  1.6G   0% /run/user/1000
[oracle@acao-ora01 ~]$
```

1. Um die Datenbank zu schützen, klicken Sie auf die drei Punkte neben dem **Schutzstatus** der Datenbank und dann auf **Richtlinie zuweisen**, um die standardmäßig vorinstallierten oder benutzerdefinierten Datenbankschutzrichtlinien anzuzeigen, die auf Ihre Oracle-Datenbanken angewendet werden können. Unter **Einstellungen – Richtlinien** haben Sie die Möglichkeit, Ihre eigene Richtlinie mit einer benutzerdefinierten Sicherungshäufigkeit und einem benutzerdefinierten Aufbewahrungsfenster für Sicherungsdaten zu erstellen.

NetApp BlueXP

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

Cloud Native | Oracle

4 Hosts | 3 ORACLE | 0 Clone

Application Protection: 0 Protected, 3 Unprotected

3 Databases

Filter By +

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1tst	172.30.15.124		Unprotected

1 - 3 of 3

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

NetApp BlueXP

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

Applications > Assign Policy

Assign Policy

Assign a policy to start taking backups of the database "NTAP"

4 Policies

Policy Name	Backup Type	Schedules
☐ Oracle Full Backup for Bronze	FullBackup	Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
☐ Oracle Full Backup for Gold	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 16 copies Daily: Repeats Every 1 Day, Keeps 30 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
☐ Oracle Full Backup for Silver	FullBackup	Hourly: Repeats Every 12 Hrs, Keeps 6 copies Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
☒ my_full_bkup	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 3 Days

1 - 4 of 4

Cancel Assign

3. Nachdem die Richtlinie angewendet wurde, ändert sich der Datenbankschutzstatus in **Geschützt** mit einem grünen Häkchen. BlueXP führt die Snapshot-Sicherung gemäß dem definierten Zeitplan aus. Darüber hinaus ist **ON-Demand Backup** über das Dropdown-Menü mit den drei Punkten verfügbar, wie unten gezeigt.

The screenshot shows the NetApp BlueXP interface with the 'Applications' tab selected. It displays a summary of protection for Cloud Native (3 Hosts), Oracle (3), and Clone (0). Below this, a table lists databases with their protection status. A dropdown menu is open for the 'db1' entry, showing options like 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore'.

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99		Unprotected
db1st	172.30.15.124		Unprotected

4. Auf der Registerkarte **Jobüberwachung** können Details zum Sicherungsauftrag angezeigt werden. Unsere Testergebnisse zeigten, dass das Sichern einer Oracle-Datenbank mit etwa 1,6 TiB etwa 4 Minuten dauerte.

The screenshot shows the NetApp BlueXP 'Job Monitoring' page. It displays a specific backup job for the NTAP oracle database. Below the job summary, a table lists sub-jobs with their durations. The duration for the main backup job is highlighted as '4 Minutes'.

Job Name	Job ID	Start Time	End Time	Duration
Backup of NTAP oracle database on host 172.30...	61a12139-330e-4390-bc...	Jul 11 2023, 2:17:53 pm	Jul 11 2023, 2:21:38 pm	4 Minutes
Applying Retention	27f9d5f-68f0-4880-a48...	Jul 11 2023, 2:21:38 pm	Jul 11 2023, 2:21:38 pm	0 Second
Performing cleanup after backup	074c0689-097e-41aa-ac...	Jul 11 2023, 2:21:36 pm	Jul 11 2023, 2:21:38 pm	2 Seconds
Finalizing Oracle database log backup	348189d3-90b5-4cce-97...	Jul 11 2023, 2:21:36 pm	Jul 11 2023, 2:21:36 pm	0 Second

5. Über das Dropdown-Menü mit den drei Punkten **Details anzeigen** können Sie die aus der Snapshot-Sicherung erstellten Sicherungssätze anzeigen.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring Reports

Cloud Native Oracle

4 Hosts 3 ORACLE 0 Clone

Application Protection 2 Protected 1 Unprotected

3 Databases

Filter By +

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

View Details On-Demand Backup Assign Policy Un-assign Policy Restore

6. Zu den Details der Datenbanksicherung gehören **Sicherungsname**, **Sicherungstyp**, **SCN**, **RMAN-Katalog** und **Sicherungszeit**. Ein Sicherungssatz enthält anwendungskonsistente Snapshots für das Datenvolumen bzw. das Protokollvolumen. Ein Protokollvolume-Snapshot wird direkt nach einem Datenbankdatenvolume-Snapshot durchgeführt. Sie können einen Filter anwenden, wenn Sie in der Sicherungsliste nach einer bestimmten Sicherung suchen.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring Reports

Applications > Database Details

Database Details

NTAP Database Name	Protected Protection	my_full_bkup Policy Names	Database Type
172.30.137.142 Host Name	ANF Host Storage	Unreachable Database Version	zEHlu7vkdyabnujcxllbkKELKVXTToyNcllents Connector Id
- Clones	- Parent Database	Disabled RMAN Catalog	- RMAN catalog repository

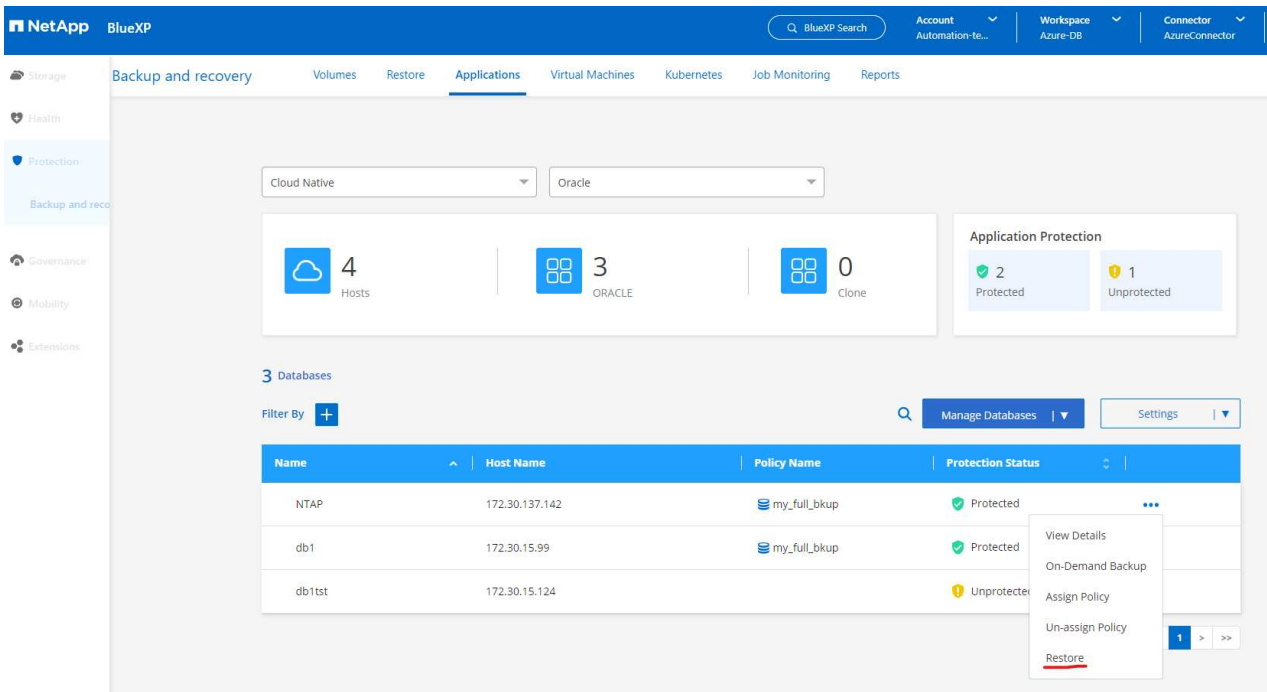
14 Backups

Filter By +

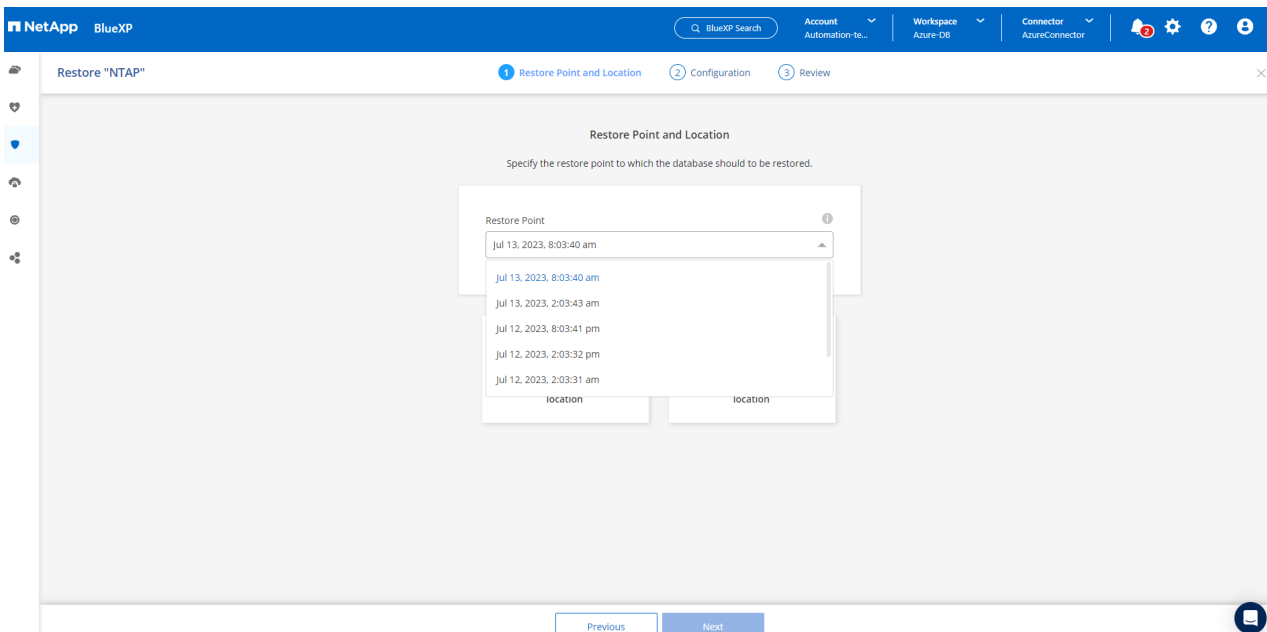
Backup Name	Backup Type	SCN	RMAN Catalog	Backup Time	
my_full_bkup_Hourly_NTAP_2023_07_13_12_04_28_8376...	Log	29192187	Not Cataloged	Jul 13, 2023, 8:06:22 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_4363...	Data	29192136	Not Cataloged	Jul 13, 2023, 8:03:40 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_04_28_5618...	Log	29178022	Not Cataloged	Jul 13, 2023, 2:05:50 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_03_03_6371...	Data	29177972	Not Cataloged	Jul 13, 2023, 2:03:43 am	Delete

Wiederherstellung und Wiederherstellung von Oracle-Datenbanken

1. Klicken Sie für eine Datenbankwiederherstellung in **Anwendungen** auf das Dropdown-Menü mit den drei Punkten für die wiederherzustellende Datenbank und dann auf **Wiederherstellen**, um den Arbeitsablauf zur Datenbankwiederherstellung und -wiederherstellung zu starten.



2. Wählen Sie Ihren **Wiederherstellungspunkt** anhand des Zeitstempels. Jeder Zeitstempel in der Liste stellt einen verfügbaren Datenbanksicherungssatz dar.



3. Wählen Sie für die Wiederherstellung und Wiederherstellung einer Oracle-Datenbank vor Ort den **ursprünglichen Speicherort** als **Wiederherstellungsort** aus.

NetApp BlueXP

Restore "NTAP"

1 Restore Point and Location 2 Configuration 3 Review

Restore Point and Location

Specify the restore point to which the database should be restored.

Restore Point
Jul 13, 2023, 8:03:40 am

Restore to original location

Restore to alternate location

Previous Next

4. Definieren Sie Ihren **Wiederherstellungsumfang** und **Wiederherstellungsumfang**. „Alle Protokolle“ bedeutet eine vollständige Wiederherstellung auf dem neuesten Stand, einschließlich der aktuellen Protokolle.

NetApp BlueXP

Restore "NTAP"

Restore Point and Location 2 Configuration 3 Review

Restore Scope

☒ All Data Files
Data Files Restore

☐ Control Files
Control Files Restore

Database state will be changed if needed for restore and recovery.

Recovery Scope

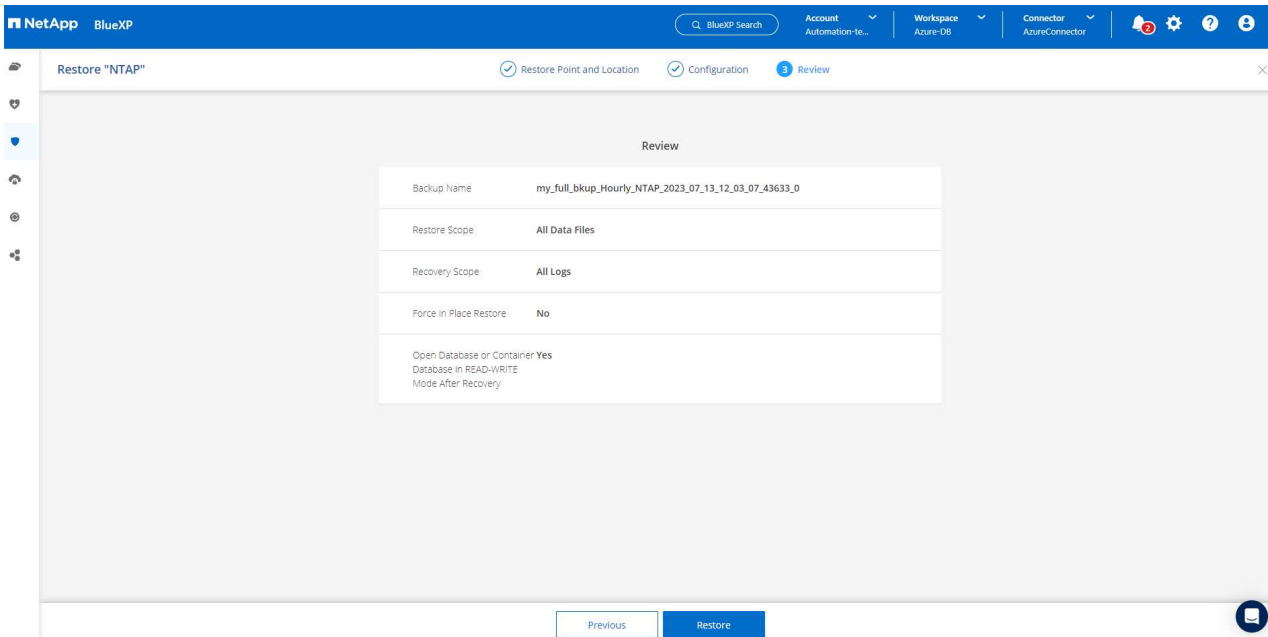
☒ All Logs ☐ Until System Change Number ☐ Date and Time ☐ No Recovery

External Archive log locations

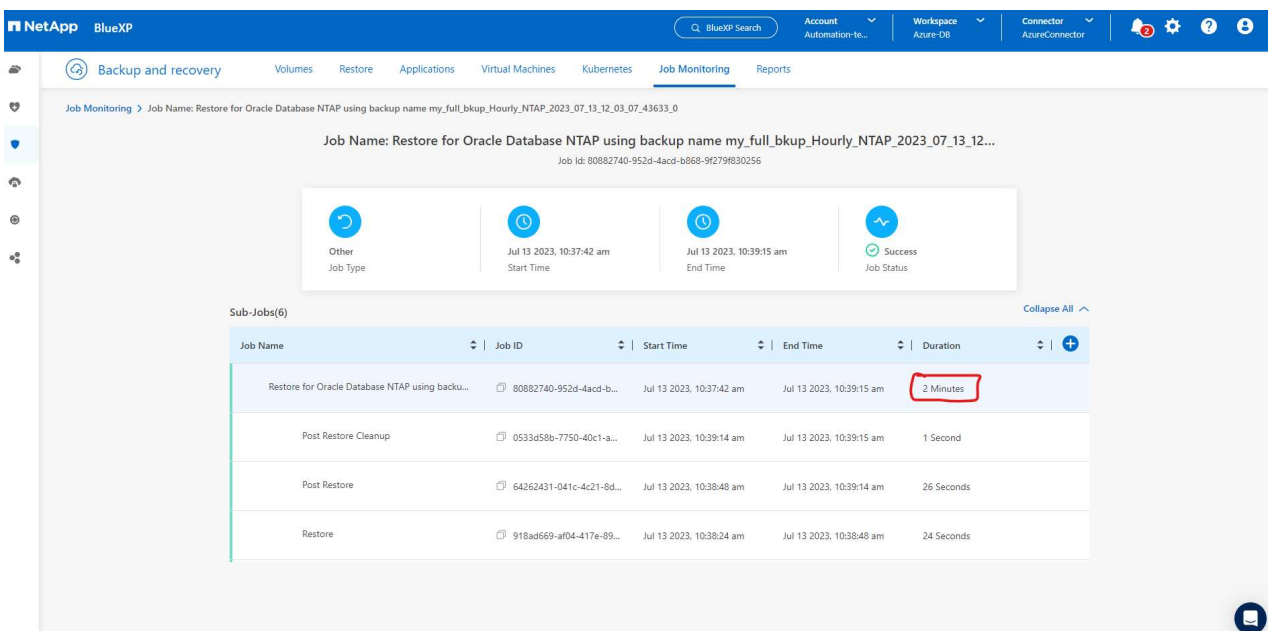
☒ Open the database or the container database in READ-WRITE mode after recovery.

Previous Next

5. Überprüfen und **Wiederherstellen**, um die Wiederherstellung und Wiederherstellung der Datenbank zu starten.



6. Auf der Registerkarte „Jobüberwachung“ haben wir festgestellt, dass die vollständige Wiederherstellung und Aktualisierung der Datenbank 2 Minuten dauerte.



Oracle-Datenbankklon

Die Verfahren zum Klonen von Datenbanken ähneln denen zur Wiederherstellung, jedoch auf einer alternativen Azure-VM mit identischem, vorinstalliertem und konfiguriertem Oracle-Software-Stack.



Stellen Sie sicher, dass Ihr Azure NetApp File-Speicher über ausreichend Kapazität für eine geklonte Datenbank derselben Größe wie die zu klonende primäre Datenbank verfügt. Die alternative Azure-VM wurde zu **Anwendungen** hinzugefügt.

1. Klicken Sie in **Anwendungen** auf das Dropdown-Menü mit den drei Punkten für die jeweilige Datenbank, die geklont werden soll, und klicken Sie dann auf **Wiederherstellen**, um den Klon-Workflow zu starten.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and links for 'Account', 'Workspace', and 'Connector'. The left sidebar lists various categories like 'Storage', 'Health', 'Protection', 'Governance', 'Mobility', and 'Extensions'. The main content area is titled 'Applications' and shows a summary of resources: 4 Cloud Native Hosts, 3 ORACLE instances, and 0 Clones. Below this, there's a section for '3 Databases' with a table listing them. The table has columns for Name, Host Name, Policy Name, and Protection Status. The databases listed are NTAP, db1, and db1tst. The 'db1tst' database is marked as 'Unprotected'. A dropdown menu is open for the 'db1tst' row, showing options: 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore' (which is highlighted with a red underline).

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

2. Wählen Sie den **Wiederherstellungspunkt** und aktivieren Sie **An einem anderen Speicherort wiederherstellen**.

NetApp BlueXP

Q BlueXP Search Account Automation-te... Workspace Azure-DB Connector AzureConnector

Restore "NTAP"

1 Restore Point and Location 2 Configuration 3 Review

Restore Point and Location

Specify the restore point to which the database should be restored.

Restore Point
Jul 13, 2023, 8:03:40 am

Restore to original location

Restore to alternate location

Previous Next

3. Legen Sie auf der nächsten **Konfigurationsseite** den alternativen **Host**, die neue Datenbank-**SID** und **Oracle Home** wie auf der alternativen Azure-VM konfiguriert fest.

NetApp BlueXP

Q BlueXP Search Account Automation-te... Workspace Azure-DB Connector AzureConnector

Restore "NTAP"

Restore Point and Location 2 Configuration 3 Review

Configuration

Specify the alternate host details on which the database will be restored and throughput.

Host
172.30.137.147

SID
NTAP1

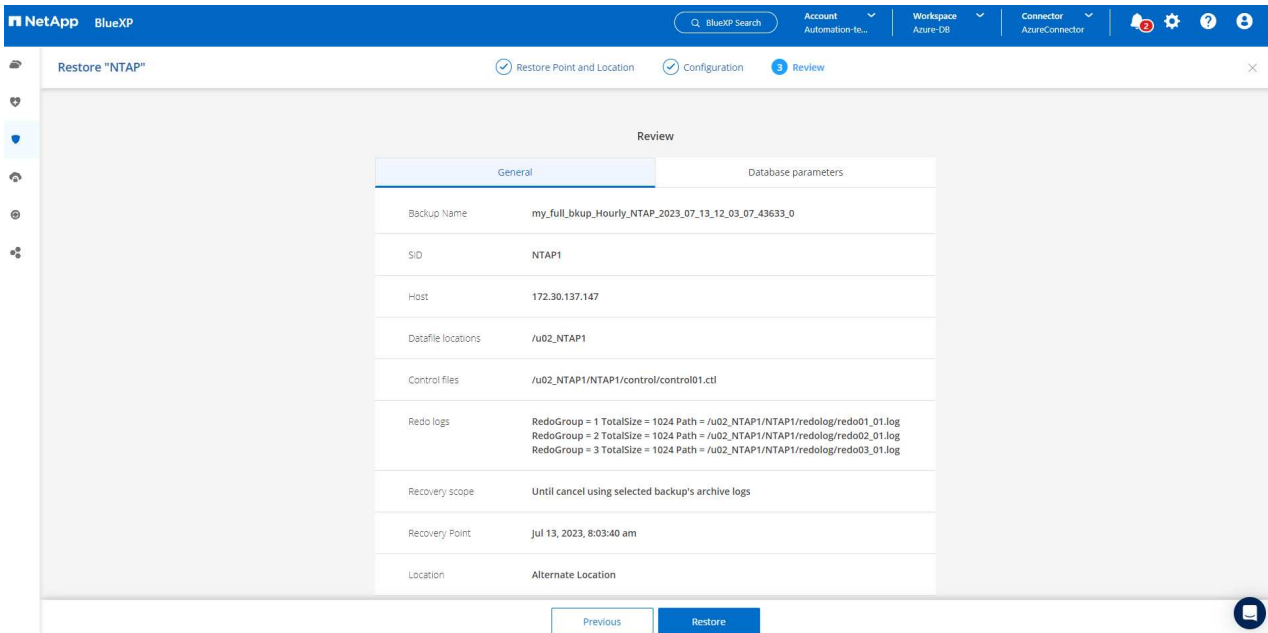
Oracle Home
/u01/app/oracle/product/19.0.0/clone

Database Credentials
Optional
Add Credential

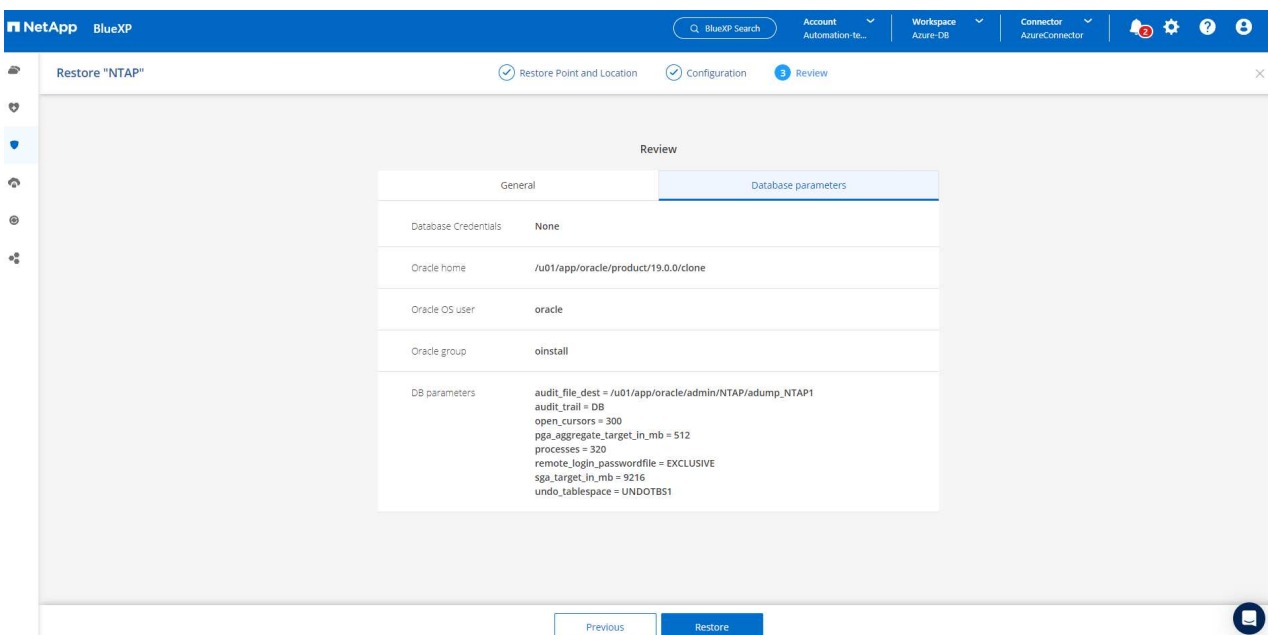
Maximum storage throughput (MiB/s)
Optional
Enter throughput (1-4500)

Previous Next

4. Auf der Seite „Allgemein“ werden die Details der geklonten Datenbank angezeigt, z. B. SID, alternativer Host, Speicherorte der Datendateien, Wiederherstellungsumfang usw.



5. Auf der Seite „Datenbankparameter überprüfen“ werden die Details der geklonten Datenbankkonfiguration sowie einige Datenbankparametereinstellungen angezeigt.



6. Überwachen Sie den Status des Klonauftrags auf der Registerkarte **Auftragsüberwachung**. Wir haben festgestellt, dass das Klonen einer 1,6 TiB großen Oracle-Datenbank 8 Minuten dauerte.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring Reports

Job Monitoring > Job Name: Restore Oracle Database NTAP as NTAP1 on host 172.30.137.147 using backup my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_43633_0
Job ID: 7a187d5a-7f7e-461a-83b3-48e37fb890f

Job Name: Restore Oracle Database NTAP as NTAP1 on host 172.30.137.147 using backup my_full_bkup_Hourl...

Other Job Type Jul 13 2023, 1:05:02 pm Start Time Jul 13 2023, 1:13:15 pm End Time Success Job Status

Sub-Jobs(6)

Job Name	Job ID	Start Time	End Time	Duration
Restore Oracle Database NTAP as NTAP1 on ho...	7a187d5a-7f7e-461a-83...	Jul 13 2023, 1:05:02 pm	Jul 13 2023, 1:13:15 pm	8 Minutes
Collect the restore database job logs of...	abc9342a-5777-4262-b...	Jul 13 2023, 1:13:14 pm	Jul 13 2023, 1:13:14 pm	0 Second
Register the restored database metadata	15aefb90-b21b-418f-b0...	Jul 13 2023, 1:12:30 pm	Jul 13 2023, 1:12:30 pm	0 Second
Remove the temporary storage of the l...	cc106fb9-7555-46c8-9c...	Jul 13 2023, 1:12:30 pm	Jul 13 2023, 1:13:14 pm	44 Seconds

7. Validieren Sie die geklonte Datenbank auf der BlueXP Seite **Anwendungen**, die anzeigt, dass die geklonte Datenbank sofort bei BlueXP registriert wurde.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring Reports

Cloud Native Oracle

4 Hosts 4 ORACLE 0 Clone

Application Protection 2 Protected 2 Unprotected

4 Databases

Filter By +

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
NTAP1	172.30.137.147	my_full_bkup	Unprotected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124	my_full_bkup	Unprotected

1 - 4 of 4

8. Überprüfen Sie die geklonte Datenbank auf der Oracle Azure-VM, die zeigte, dass die geklonte Datenbank wie erwartet ausgeführt wurde.

```

[oracle@acao-ora02 admin]$ cat /etc/oratab
#

# This file is used by ORACLE utilities.  It is created by root.sh
# and updated by either Database Configuration Assistant while creating
# a database or ASM Configuration Assistant while creating ASM instance.

# A colon, ':', is used as the field terminator.  A new line terminates
# the entry.  Lines beginning with a pound sign, '#', are comments.
#
# Entries are of the form:
#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:
#
# The first and second fields are the system identifier and home
# directory of the database respectively.  The third field indicates
# to the dbstart utility that the database should , "Y", or should not,
# "N", be brought up at system boot time.
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
NTAP1:/u01/app/oracle/product/19.0.0/clone:N
[oracle@acao-ora02 admin]$ export ORACLE_SID=NTAP1
[oracle@acao-ora02 admin]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/clone
[oracle@acao-ora02 admin]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@acao-ora02 admin]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Jul 13 17:16:31 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, log_mode from v$database;

NAME          OPEN_MODE          LOG_MODE
-----
NTAP1         READ WRITE         NOARCHIVELOG

```

Damit ist die Demonstration einer Sicherung, Wiederherstellung und eines Klons einer Oracle-Datenbank in Azure mit der NetApp BlueXP -Konsole unter Verwendung des SnapCenter -Dienstes abgeschlossen.

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)

- Azure NetApp Files

["https://azure.microsoft.com/en-us/products/netapp"](https://azure.microsoft.com/en-us/products/netapp)

- Erste Schritte mit Azure

["https://azure.microsoft.com/en-us/get-started/"](https://azure.microsoft.com/en-us/get-started/)

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.