



TR-4977: Copia de seguridad, restauración y clonación de bases de datos de Oracle con SnapCenter Services - Azure

NetApp database solutions

NetApp
August 18, 2025

Tabla de contenidos

TR-4977: Copia de seguridad, restauración y clonación de bases de datos de Oracle con SnapCenter

Services - Azure 1

 Objetivo 1

 Audiencia 1

 Entorno de prueba y validación de soluciones 1

 Arquitectura 2

 Componentes de hardware y software 2

 Factores clave a considerar en la implementación 3

Implementación de la solución 3

 Requisitos previos para la implementación del servicio SnapCenter 3

 Preparación para la incorporación a BlueXP 4

 Implementar un conector para los servicios de SnapCenter 4

 Definir una credencial en BlueXP para acceder a recursos de Azure 12

 Configuración de los servicios de SnapCenter 15

 Copia de seguridad de la base de datos de Oracle 22

 Restauración y recuperación de bases de datos de Oracle 27

 Clon de base de datos de Oracle 30

Información adicional 35

TR-4977: Copia de seguridad, restauración y clonación de bases de datos de Oracle con SnapCenter Services - Azure

Allen Cao, Niyaz Mohamed, NetApp

Esta solución proporciona una descripción general y detalles para la copia de seguridad, restauración y clonación de bases de datos de Oracle mediante NetApp SnapCenter SaaS usando la consola BlueXP .

Objetivo

SnapCenter Services es la versión SaaS de la clásica herramienta de interfaz de usuario de administración de bases de datos SnapCenter que está disponible a través de la consola de administración en nube NetApp BlueXP . Es una parte integral de la oferta de protección de datos y respaldo en la nube de NetApp para bases de datos como Oracle y HANA que se ejecutan en Azure NetApp Files. Este servicio basado en SaaS simplifica la implementación tradicional del servidor independiente SnapCenter que generalmente requiere un servidor Windows que funcione en un entorno de dominio Windows.

En esta documentación, demostramos cómo configurar los servicios de SnapCenter para realizar copias de seguridad, restaurar y clonar bases de datos de Oracle implementadas en volúmenes de Azure NetApp Files e instancias de cómputo de Azure. Es muy fácil configurar la protección de datos para la base de datos Oracle implementada en Azure NetApp Files con la interfaz de usuario BlueXP basada en web.

Esta solución aborda los siguientes casos de uso:

- Copia de seguridad de bases de datos con instantáneas para bases de datos Oracle alojadas en Azure NetApp Files y máquinas virtuales de Azure
- Recuperación de la base de datos Oracle en caso de fallo
- Clonación rápida de bases de datos primarias para entornos de desarrollo, prueba u otros casos de uso

Audiencia

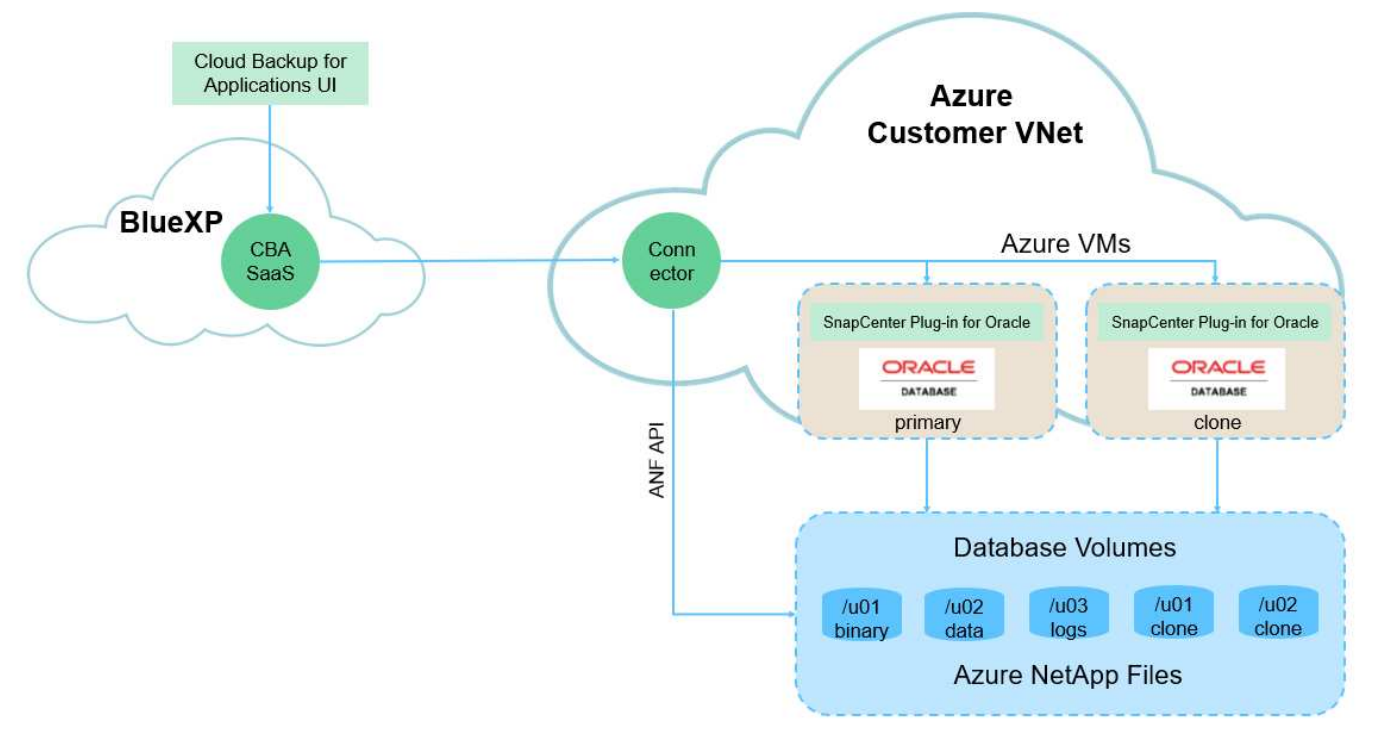
Esta solución está destinada a los siguientes públicos:

- El DBA que administra las bases de datos de Oracle que se ejecutan en el almacenamiento de Azure NetApp Files
- El arquitecto de soluciones que está interesado en probar la copia de seguridad, la restauración y la clonación de bases de datos de Oracle en Azure
- El administrador de almacenamiento que admite y administra el almacenamiento de Azure NetApp Files
- El propietario de la aplicación que posee las aplicaciones que se implementan en el almacenamiento de Azure NetApp Files y las máquinas virtuales de Azure

Entorno de prueba y validación de soluciones

La prueba y validación de esta solución se realizó en un entorno de laboratorio que podría no coincidir con el entorno de implementación final. Para más información, consulte la sección [Factores clave a considerar en la](#)

Arquitectura



Esta imagen proporciona una imagen detallada de la BlueXP backup and recovery para las aplicaciones dentro de la consola BlueXP , incluida la interfaz de usuario, el conector y los recursos que administra.

Componentes de hardware y software

Hardware

Almacenamiento de Azure NetApp Files	Nivel de servicio Premium	Tipo de QoS automático y 4 TB de capacidad de almacenamiento en prueba
Instancia de Azure para computación	B4ms estándar (4 vcpu, 16 GiB de memoria)	Se implementaron dos instancias, una como servidor de base de datos principal y la otra como servidor de base de datos clonado

Software

Red Hat Linux	Red Hat Enterprise Linux 8.7 (LVM) - x64 Gen2	Se implementó una suscripción a RedHat para realizar pruebas
Base de datos Oracle	Versión 19.18	Parche RU aplicado p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Versión 12.2.0.1.36	Último parche p6880880_190000_Linux-x86-64.zip
Servicio SnapCenter	Versión v2.5.0-2822	Versión del agente v2.5.0-2822

Factores clave a considerar en la implementación

- **Conector que se implementará en la misma red virtual/subred que las bases de datos y Azure NetApp Files.** Cuando sea posible, el conector se debe implementar en las mismas redes virtuales y grupos de recursos de Azure, lo que permite la conectividad con el almacenamiento de Azure NetApp Files y las instancias de cómputo de Azure.
- **Una cuenta de usuario de Azure o un principio de servicio de Active Directory creado en el portal de Azure para el conector de SnapCenter .** La implementación de un conector BlueXP requiere permisos específicos para crear y configurar una máquina virtual y otros recursos informáticos, para configurar la red y para obtener acceso a la suscripción de Azure. También se requieren permisos para crear posteriormente roles y permisos para que el Conector funcione. Cree un rol personalizado en Azure con permisos y asígnelo a la cuenta de usuario o al principio de servicio. Revise el siguiente enlace para más detalles: "[Configurar permisos de Azure](#)".
- **Un par de claves ssh creado en el grupo de recursos de Azure.** El par de claves SSH se asigna al usuario de la máquina virtual de Azure para iniciar sesión en el host del conector y también al host de la máquina virtual de la base de datos para implementar y ejecutar un complemento. La interfaz de usuario de la consola de BlueXP usa la clave SSH para implementar el complemento de servicio de SnapCenter en el host de la base de datos, lo que permite la instalación del complemento en un solo paso y la detección de la base de datos del host de la aplicación.
- **Se agregó una credencial a la configuración de la consola BlueXP .** Para agregar almacenamiento de Azure NetApp Files al entorno de trabajo de BlueXP , es necesario configurar una credencial que otorgue permisos para acceder a Azure NetApp Files desde la consola de BlueXP en la configuración de la consola de BlueXP .
- **java-11-openjdk instalado en el host de la instancia de base de datos de Azure VM.** La instalación del servicio SnapCenter requiere la versión 11 de Java. Debe instalarse en el host de la aplicación antes de intentar implementar el complemento.

Implementación de la solución

Existe una extensa documentación de NetApp con un alcance más amplio para ayudarlo a proteger los datos de sus aplicaciones nativas de la nube. El objetivo de esta documentación es proporcionar procedimientos paso a paso que cubren la implementación del servicio SnapCenter con la consola BlueXP para proteger su base de datos Oracle implementada en un almacenamiento de Azure NetApp Files y una instancia de cómputo de Azure.

Para comenzar, complete los siguientes pasos:

- Lea las instrucciones generales "[Proteja los datos de sus aplicaciones nativas de la nube](#)" y las secciones relacionadas con Oracle y Azure NetApp Files.
- Mira el siguiente video tutorial

[Vídeo de la implementación de Oracle y ANF](#)

Requisitos previos para la implementación del servicio SnapCenter

La implementación requiere los siguientes requisitos previos.

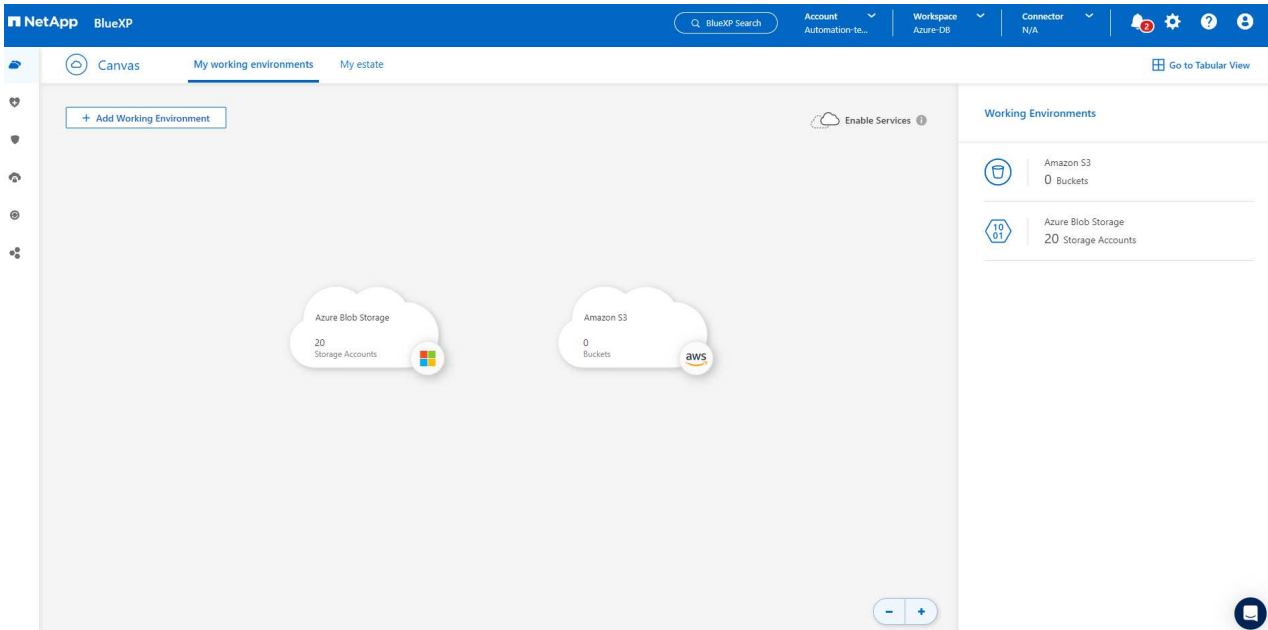
1. Un servidor de base de datos Oracle principal en una instancia de máquina virtual de Azure con una base de datos Oracle completamente implementada y en funcionamiento.
2. Un grupo de capacidad del servicio de almacenamiento de Azure NetApp Files implementado en Azure que tiene la capacidad de satisfacer las necesidades de almacenamiento de base de datos enumeradas en la sección de componentes de hardware.
3. Un servidor de base de datos secundario en una instancia de máquina virtual de Azure que se puede usar para probar la clonación de una base de datos de Oracle en un host alternativo con el fin de soportar una carga de trabajo de desarrollo/prueba o cualquier caso de uso que requiera un conjunto de datos completo de una base de datos de Oracle de producción.
4. Para obtener información adicional sobre la implementación de la base de datos de Oracle en Azure NetApp Files y la instancia de cómputo de Azure, consulte ["Implementación y protección de bases de datos de Oracle en Azure NetApp Files"](#) .

Preparación para la incorporación a BlueXP

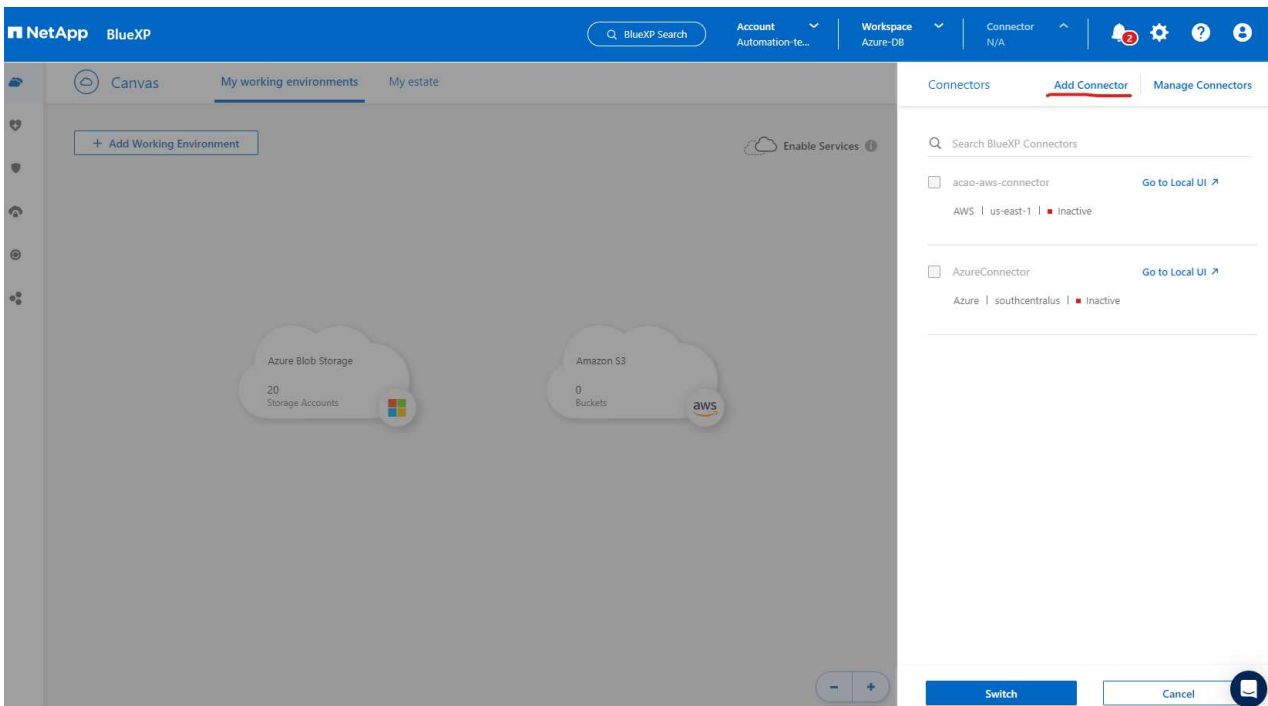
1. Utilice el enlace ["NetApp BlueXP"](#) para registrarse y obtener acceso a la consola BlueXP .
2. Cree una cuenta de usuario de Azure o un principio de servicio de Active Directory y otorgue permisos con rol en el portal de Azure para la implementación del conector de Azure.
3. Para configurar BlueXP para administrar recursos de Azure, agregue una credencial de BlueXP con detalles de una entidad de servicio de Active Directory que BlueXP pueda usar para autenticarse con Azure Active Directory (ID de cliente de la aplicación), un secreto de cliente para la aplicación de la entidad de servicio (secreto de cliente) y la ID de Active Directory para su organización (ID de inquilino).
4. También necesita la red virtual de Azure, el grupo de recursos, el grupo de seguridad, una clave SSH para el acceso a la máquina virtual, etc., listos para el aprovisionamiento del conector y la instalación del complemento de base de datos.

Implementar un conector para los servicios de SnapCenter

1. Inicie sesión en la consola BlueXP .



2. Haga clic en la flecha desplegable **Conector** y en **Agregar conector** para iniciar el flujo de trabajo de aprovisionamiento de conectores.



3. Elija su proveedor de nube (en este caso, **Microsoft Azure**).

Provider

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



[Deploy the Connector on your premises](#)

Continue

- Omita los pasos de **Permiso**, **Autenticación** y **Redes** si ya los tiene configurados en su cuenta de Azure. De lo contrario, deberá configurarlos antes de continuar. Desde aquí, también puede recuperar los permisos para la política de Azure a la que se hace referencia en la sección anterior "[Preparación para la incorporación a BlueXP](#)".

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. Haga clic en **Ir a implementación** para configurar su conector **Autenticación de máquina virtual**. Agregue el par de claves SSH que ha creado en el grupo de recursos de Azure durante la incorporación a la preparación de BlueXP para la autenticación del sistema operativo del conector.

Add BlueXP Connector - Azure

More Information

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. Proporcione un nombre para la instancia del conector, seleccione **Crear** y acepte el **Nombre de rol** predeterminado en **Detalles**, y elija la suscripción para la cuenta de Azure.

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. Configure la red con la **VNet** y la **Subred** adecuadas y deshabilite la **IP pública**, pero asegúrese de que el conector tenga acceso a Internet en su entorno de Azure.

Add BlueXP Connector - Azure

More Information

✓ VM Authentication

✓ Details

3 Network

4 Security Group

5 Review

Network

Connectivity

VNet

ANFAVSVal

Subnet

VM_Sub

Public IP

Disable

Proxy Configuration (Optional)

HTTP Proxy

Example: http://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

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

Previous

Next

8. Configure el **Grupo de seguridad** para el conector que permite el acceso HTTP, HTTPS y SSH.

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)	HTTPS (Port 443)	SSH (Port 22)
Source Type Anywhere	Source Type Anywhere	Source Type Anywhere
Source (CIDR) 0.0.0.0/0	Source (CIDR) 0.0.0.0/0	Source (CIDR) 0.0.0.0/0

Previous Next 📧

9. Revise la página de resumen y haga clic en **Agregar** para comenzar la creación del conector. Generalmente, la implementación completa demora unos 10 minutos. Una vez completado, la instancia del conector VM aparece en el portal de Azure.

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	ANFAVSub
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. Una vez implementado el conector, el conector recién creado aparece en el menú desplegable **Conector**.

NetApp BlueXP

BlueXP Search

Account Automation-to...

Workspace Azure-DB

Connector AzureConnector

2

Settings

Help

User

Canvas

My working environments

My estate

+ Add Working Environment

Enable Services

Azure Blob Storage 20 Storage Accounts

Amazon S3 0 Buckets

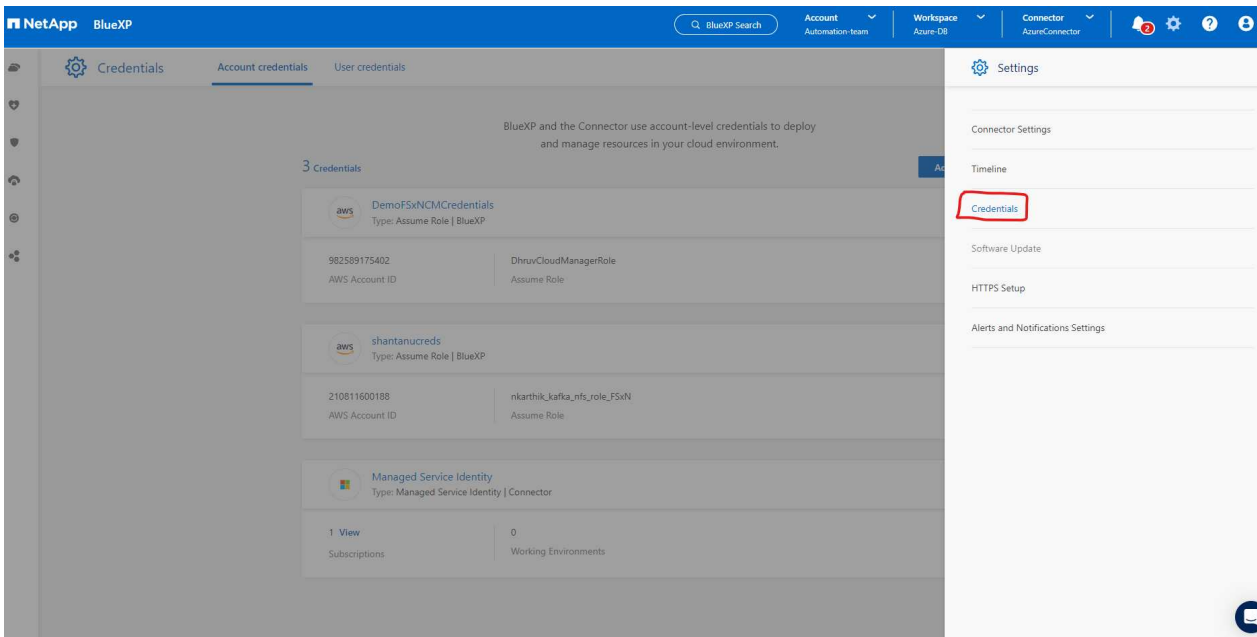
Working Environments

Amazon S3 0 Buckets

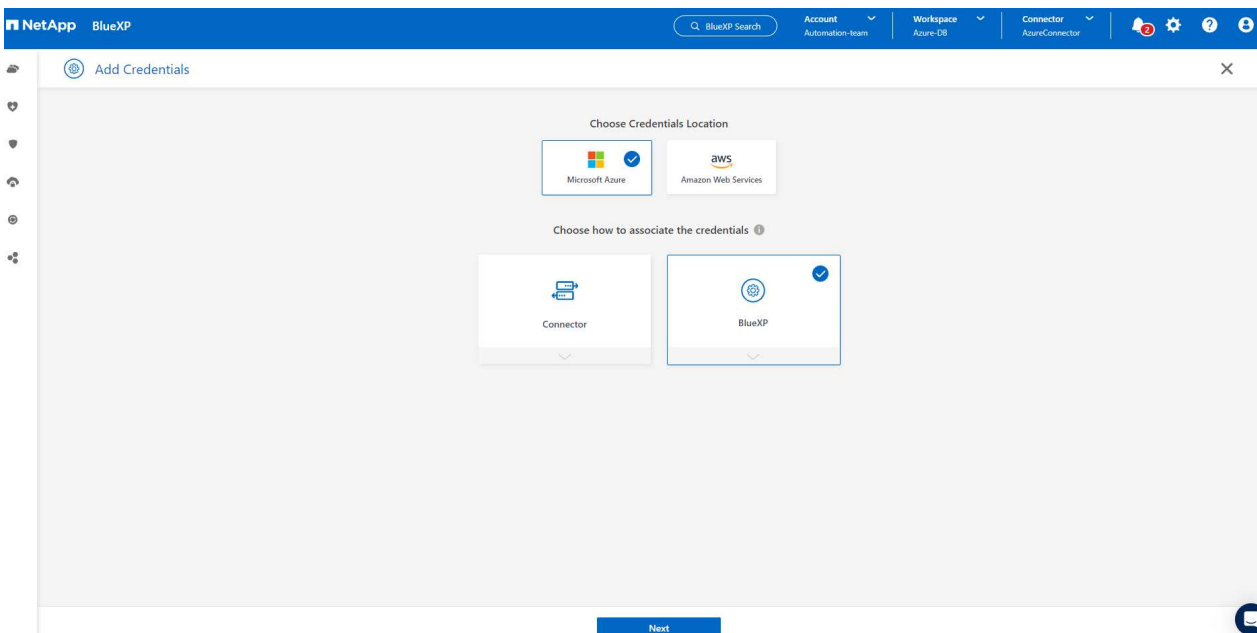
Azure Blob Storage 20 Storage Accounts

Definir una credencial en BlueXP para acceder a recursos de Azure

1. Haga clic en el ícono de configuración en la esquina superior derecha de la consola BlueXP para abrir la página **Credenciales de la cuenta**, haga clic en **Agregar credenciales** para iniciar el flujo de trabajo de configuración de credenciales.



2. Elija la ubicación de las credenciales como - **Microsoft Azure - BlueXP**.



3. Defina las credenciales de Azure con el **Secreto de cliente**, el **ID de cliente** y el **ID de inquilino** adecuados, que deberían haberse recopilado durante el proceso de incorporación de BlueXP anterior.

NetApp BlueXP

Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector

Add Credentials Credentials Type Define Credentials Marketplace Subscription 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. Revisar y Agregar

NetApp BlueXP

Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector

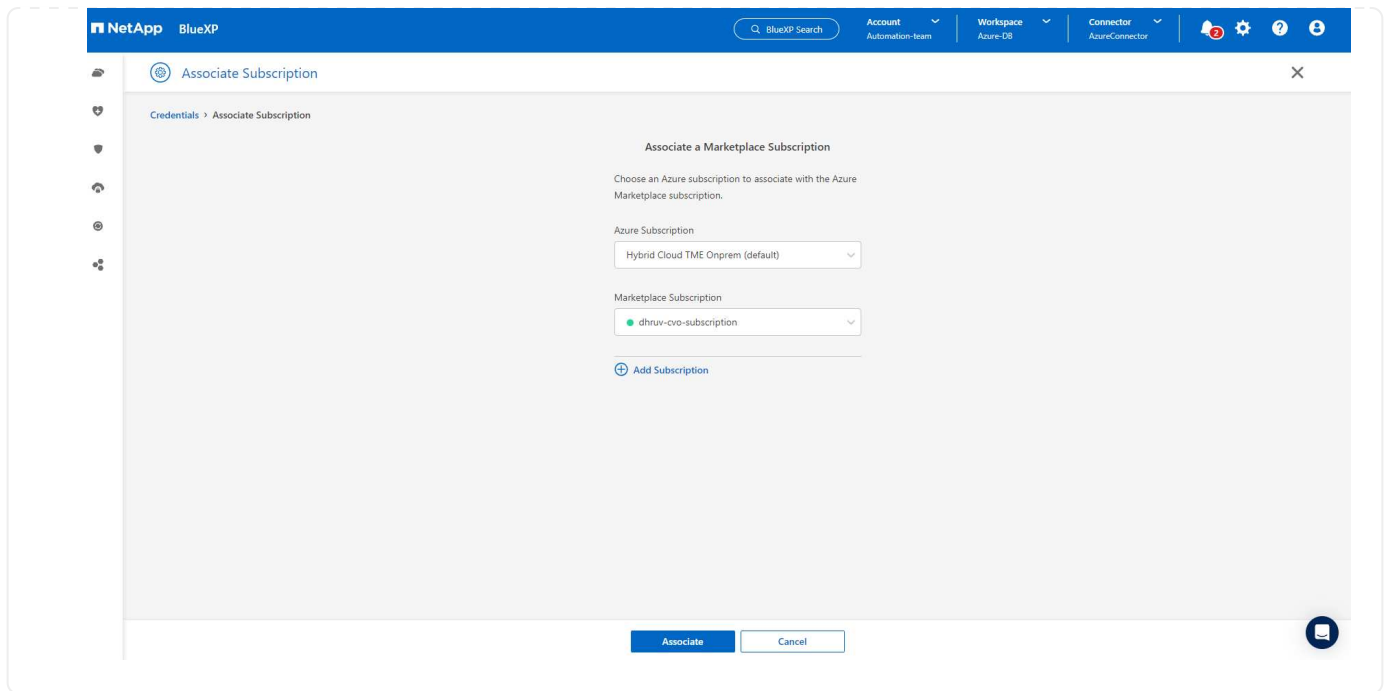
Add Credentials Credentials Type Define Credentials Review

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

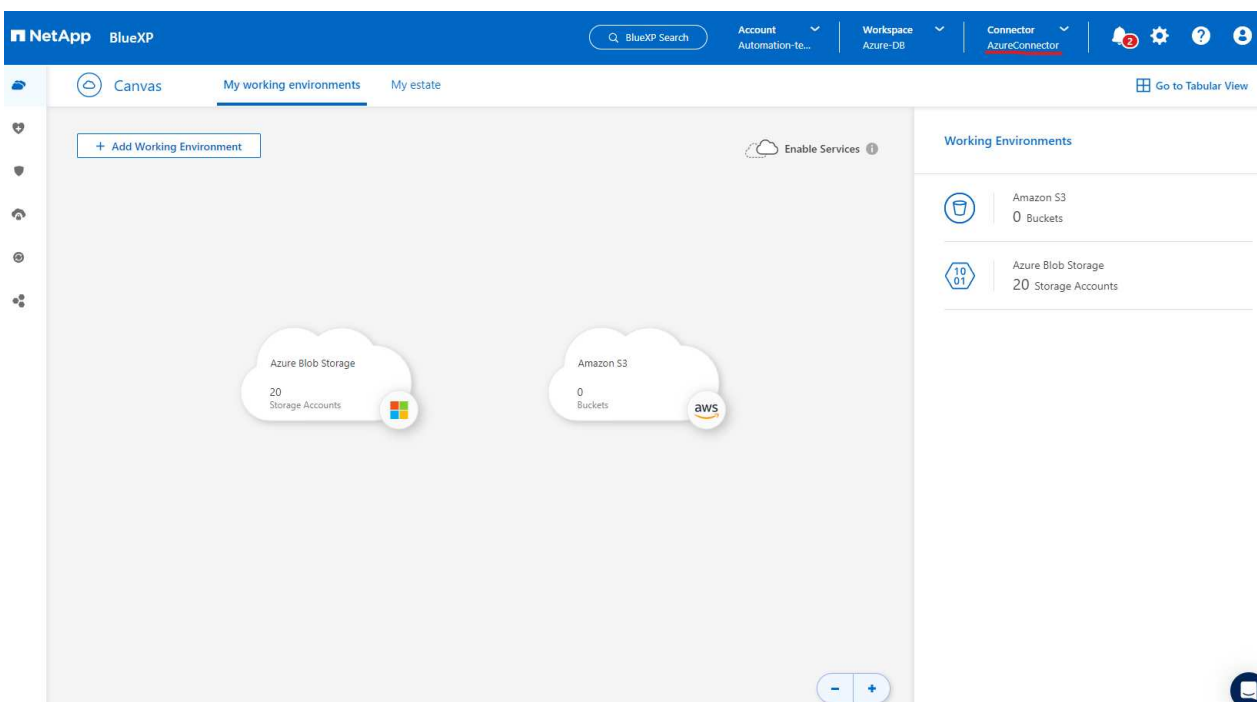
5. Es posible que también necesites asociar una **Suscripción al Marketplace** con la credencial.



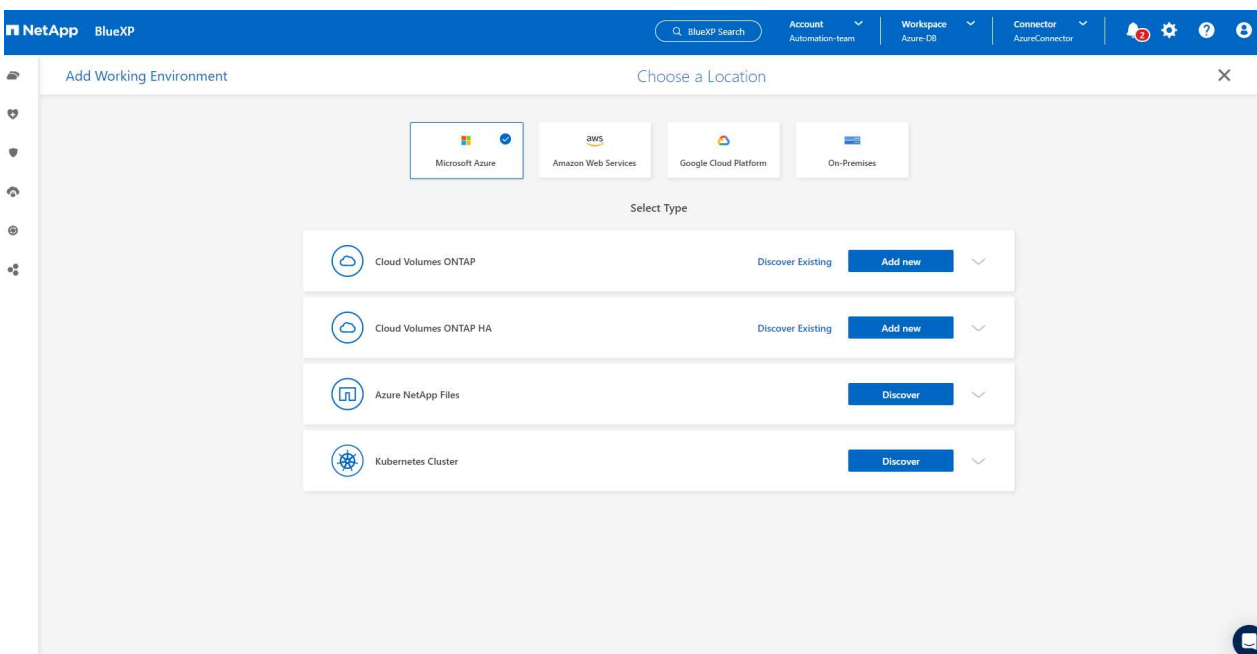
Configuración de los servicios de SnapCenter

Con las credenciales de Azure configuradas, los servicios de SnapCenter ahora se pueden configurar con los siguientes procedimientos:

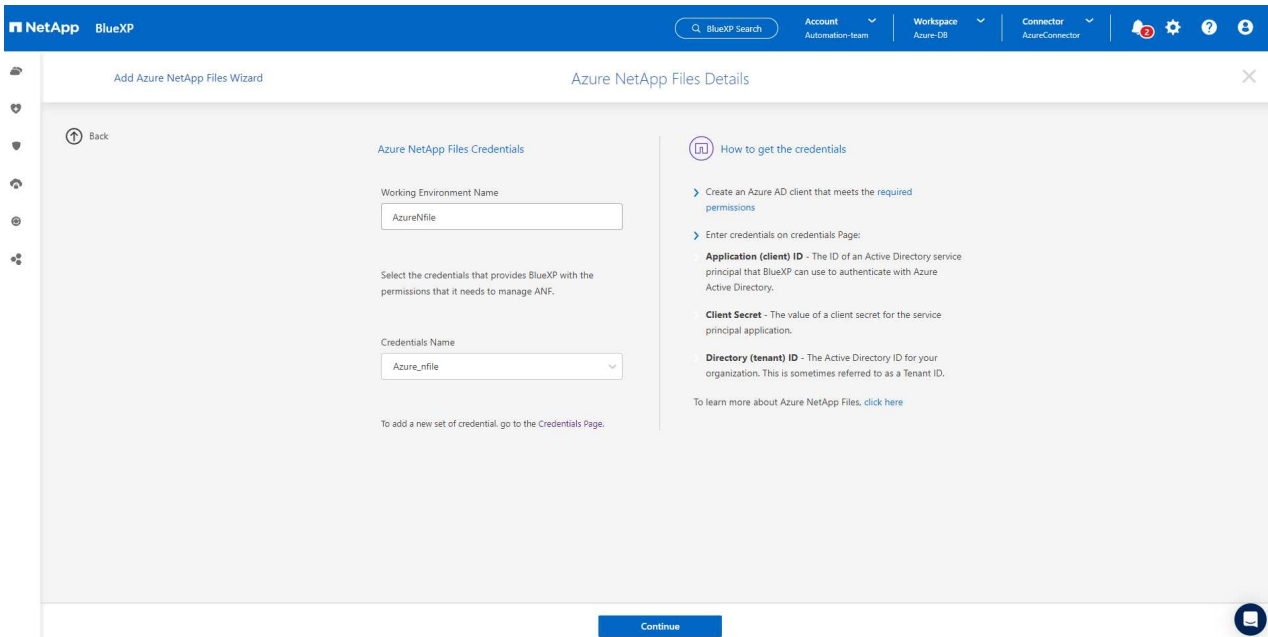
1. Regrese a la página Lienzo, desde **Mi entorno de trabajo**, haga clic en **Agregar entorno de trabajo** para descubrir Azure NetApp Files implementados en Azure.



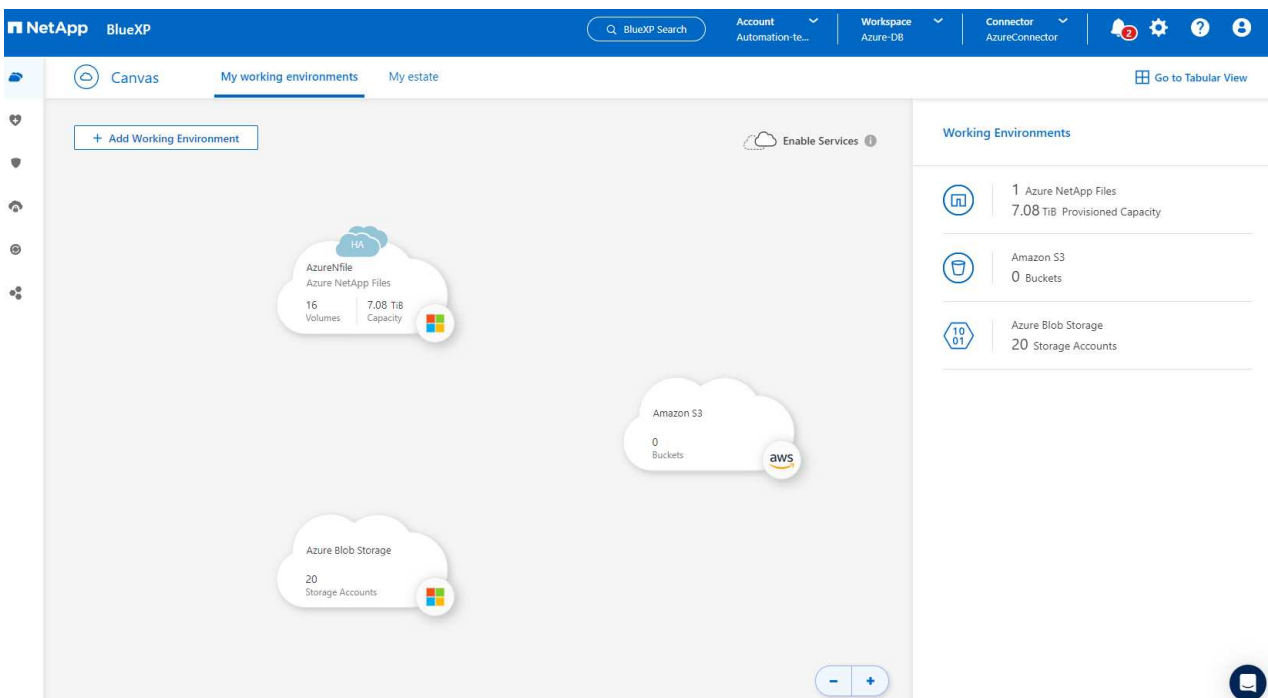
2. Elija **Microsoft Azure** como ubicación y haga clic en **Descubrir**.



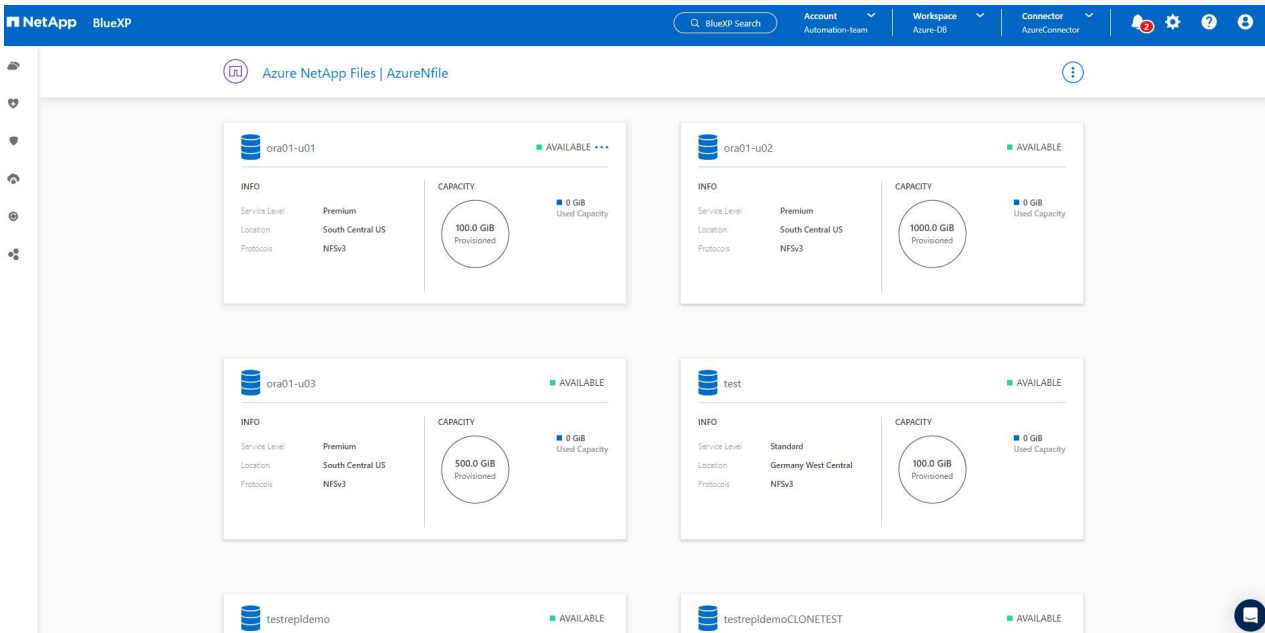
3. Nombre **Entorno de trabajo** y elija **Nombre de credencial** creado en la sección anterior y haga clic en **Continuar**.



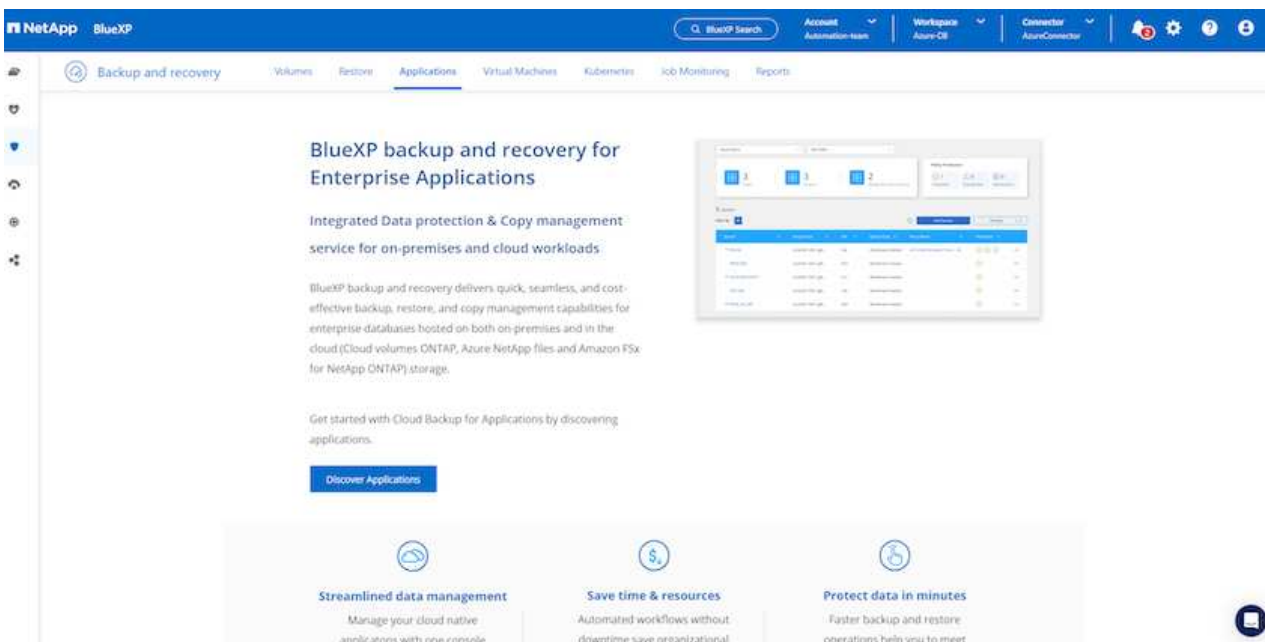
- La consola BlueXP regresa a **Mis entornos de trabajo** y descubrió que Azure NetApp Files de Azure ahora aparece en **Canvas**.



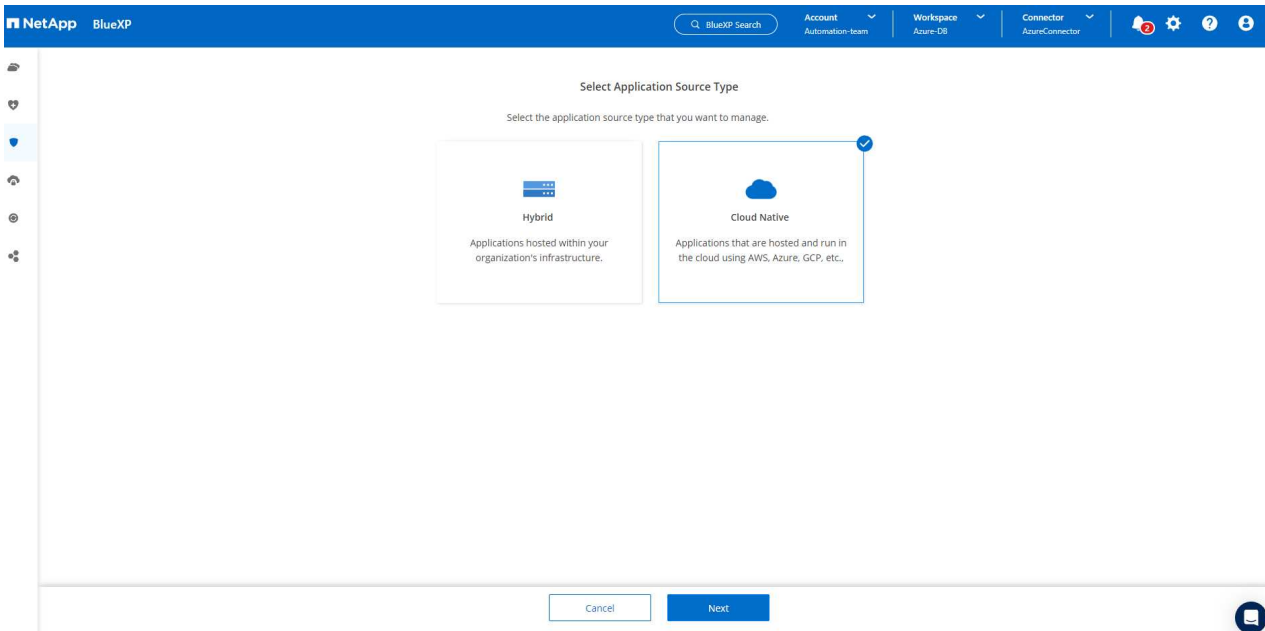
- Haga clic en el ícono * Azure NetApp Files* y luego en **Ingresar al entorno de trabajo** para ver los volúmenes de base de datos de Oracle implementados en el almacenamiento de Azure NetApp Files.



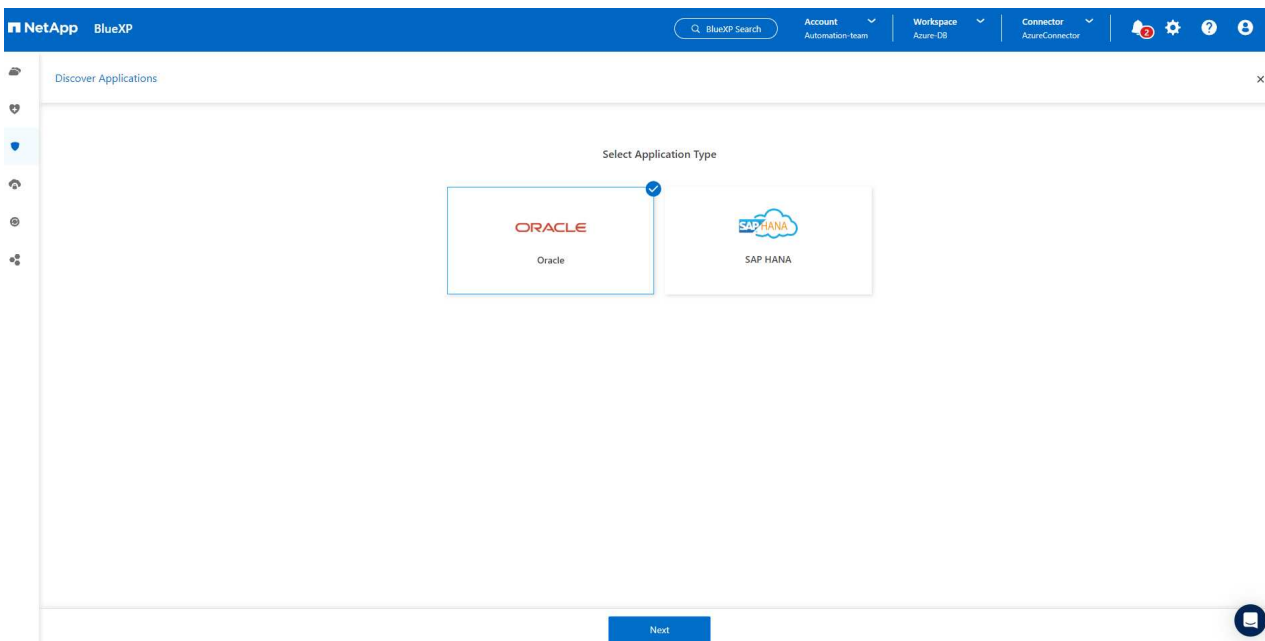
- Desde la barra lateral izquierda de la consola, pase el mouse sobre el ícono de protección y luego haga clic en **Protección > Aplicaciones** para abrir la página de inicio de Aplicaciones. Haga clic en **Descubrir aplicaciones**.



- Seleccione **Cloud Native** como el tipo de fuente de la aplicación.



8. Elija **Oracle** como tipo de aplicación, haga clic en **Siguiente** para abrir la página de detalles del host.



9. Seleccione **Usar SSH** y proporcione los detalles de Oracle Azure VM, como **dirección IP**, **Conector** y **Nombre de usuario** de administración de Azure VM, como azureuser. Haga clic en **Agregar clave privada SSH** para pegar el par de claves SSH que utilizó para implementar la máquina virtual Oracle Azure. También se le pedirá que confirme la huella digital.

NetApp BlueXP

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: 172.30.137.142

Connector: AzureConnector

Username: azureuser

SSH Port: 22

Plug-in Port: 8145

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: ssh-rsa

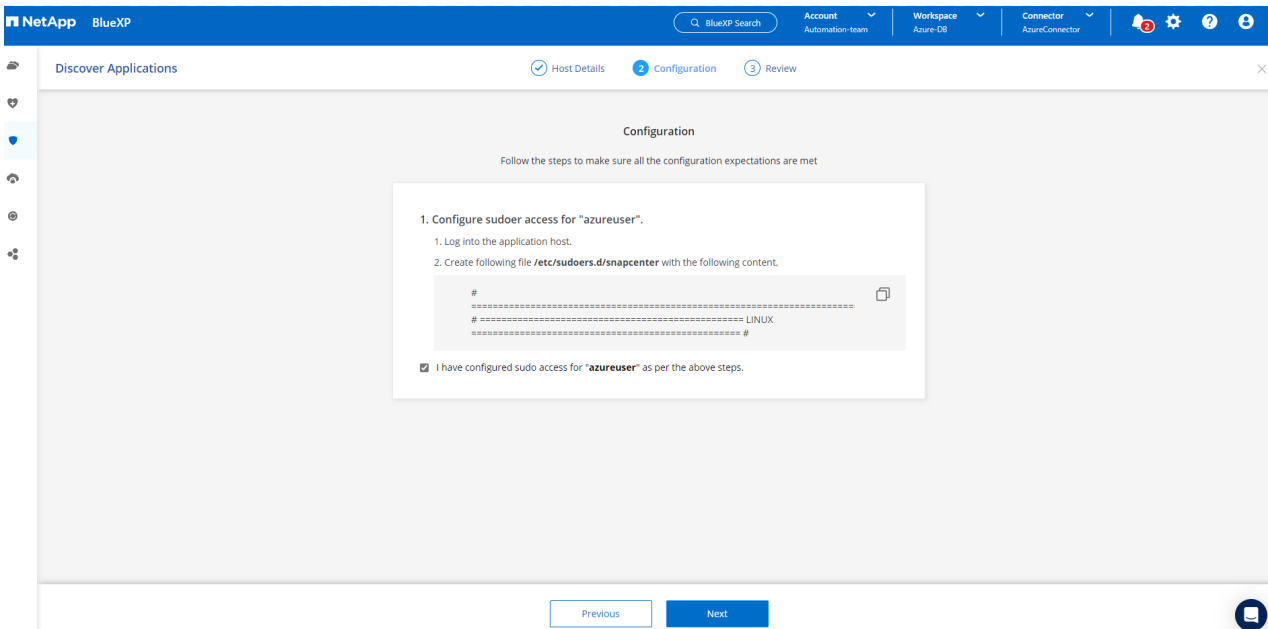
Fingerprint: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAAB...

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

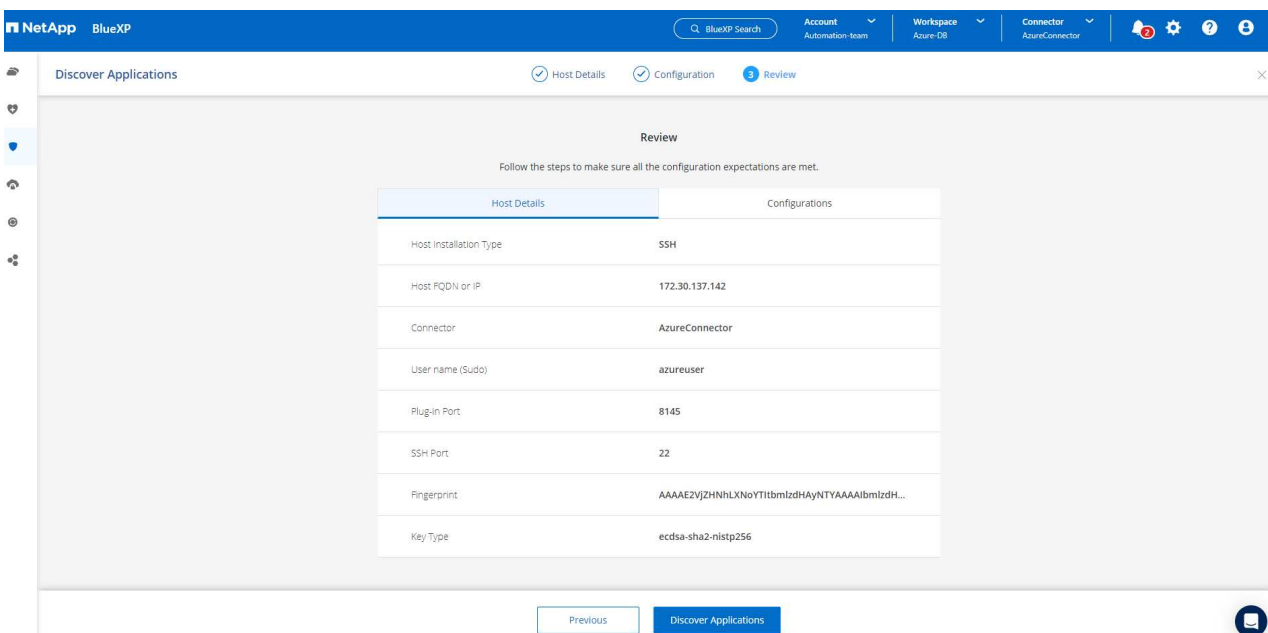
Proceed Cancel

Previous Next

10. Pase a la siguiente página de **Configuración** para configurar el acceso a sudoer en Oracle Azure VM.



11. Revise y haga clic en **Descubrir aplicaciones** para instalar un complemento en la VM Oracle Azure y descubrir la base de datos Oracle en la VM en un solo paso.



12. Las bases de datos de Oracle detectadas en la máquina virtual de Azure se agregan a **Aplicaciones**, y la página **Aplicaciones** enumera la cantidad de hosts y bases de datos de Oracle dentro del entorno. El estado de protección de la base de datos se muestra inicialmente como **Desprotegido**.

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

<<

<

1

>

>>

Esto completa la configuración inicial de los servicios de SnapCenter para Oracle. Las siguientes tres secciones de este documento describen las operaciones de copia de seguridad, restauración y clonación de bases de datos de Oracle.

Copia de seguridad de la base de datos de Oracle

22

1. Nuestra base de datos Oracle de prueba en Azure VM está configurada con tres volúmenes con un almacenamiento total agregado de aproximadamente 1,6 TiB. Esto proporciona contexto sobre el momento oportuno para realizar la copia de seguridad, la restauración y la clonación de una instantánea de una base de datos de este tamaño.

```
[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. Para proteger la base de datos, haga clic en los tres puntos junto a **Estado de protección** de la base de datos y, a continuación, haga clic en **Asignar política** para ver las políticas de protección de base de datos predeterminadas precargadas o definidas por el usuario que se pueden aplicar a sus bases de datos Oracle. En **Configuración - Políticas**, tiene la opción de crear su propia política con una frecuencia de copia de seguridad personalizada y una ventana de retención de datos de copia de seguridad.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. Below the navigation bar, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows '4 Hosts', '3 ORACLE', and '0 Clone'. An 'Application Protection' summary shows '0 Protected' and '3 Unprotected'. Below this, a table lists databases with their protection status. A context menu is open over the 'db1' row, showing 'View Details' and 'Assign Policy' (highlighted with a red box).

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

2. Cuando esté satisfecho con la configuración de la política, puede **Asignar** la política que elija para proteger la base de datos.

The screenshot shows the 'Assign Policy' dialog in the NetApp BlueXP interface. The title is 'Assign Policy' and the subtitle is 'Assign a policy to start taking backups of the database "NTAP"'. Below the title, there are 4 policies listed in a table. The 'my_full_bkup' policy is selected with a blue checkmark. At the bottom, there are 'Cancel' and 'Assign' buttons.

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

3. Después de aplicar la política, el estado de protección de la base de datos cambia a **Protegido** con una marca de verificación verde. BlueXP ejecuta la copia de seguridad de la instantánea según la programación definida. Además, la copia de seguridad **ON-Demand** está disponible en el menú desplegable de tres puntos como se muestra a continuación.

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 context menu is open for the 'db1' entry, highlighting the 'On-Demand Backup' option.

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

4. Desde la pestaña **Monitoreo de trabajos**, se pueden ver los detalles del trabajo de respaldo. Los resultados de nuestras pruebas mostraron que tomó aproximadamente 4 minutos realizar una copia de seguridad de una base de datos Oracle de aproximadamente 1,6 TiB.

The screenshot shows the NetApp BlueXP 'Job Monitoring' page. It displays a specific backup job for the NTAP oracle database. A summary bar shows the job type, start time, end time, and success status. Below, a table lists the sub-jobs of the backup, with the duration of the main backup job 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. Desde el menú desplegable de tres puntos **Ver detalles**, puede ver los conjuntos de copias de seguridad creados a partir de la copia de seguridad instantánea.

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

4 Hosts

3 ORACLE

0 Clone

Application Protection

2 Protected

1 Unprotected

3 Databases

Filter By

Manage Databases

Settings

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. Los detalles de la copia de seguridad de la base de datos incluyen el **Nombre de la copia de seguridad**, el **Tipo de copia de seguridad**, el **SCN**, el **Catálogo RMAN** y el **Tiempo de copia de seguridad**. Un conjunto de copias de seguridad contiene instantáneas consistentes con la aplicación para el volumen de datos y el volumen de registro respectivamente. Una instantánea del volumen de registro se realiza inmediatamente después de una instantánea del volumen de datos de la base de datos. Puede aplicar un filtro si está buscando una copia de seguridad específica en la lista de copias de seguridad.

NetApp BlueXP

BlueXP Search

Account Automation-te...

Workspace Azure-DB

Connector AzureConnector

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

zEHlu7vkdydBnujcxllbkELKVXToyNlclents Connector Id

- Clones

- Parent Database

Disabled RMAN Catalog

- RMAN catalog repository

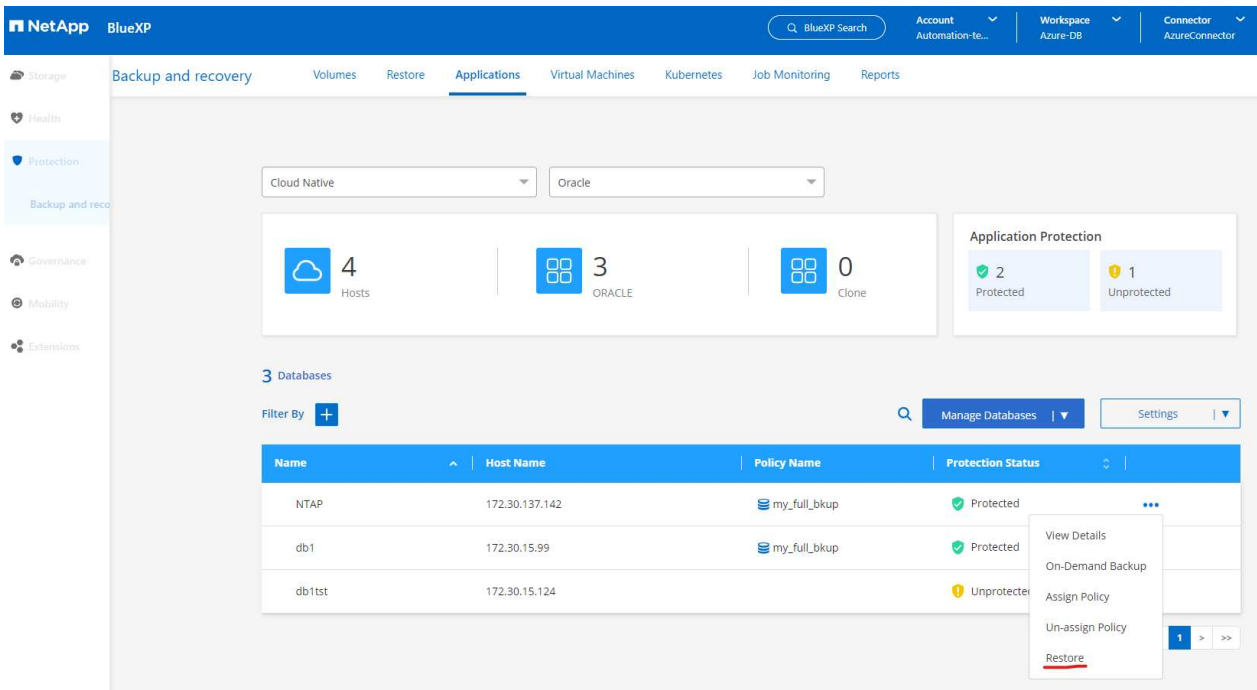
14 Backups

Filter By

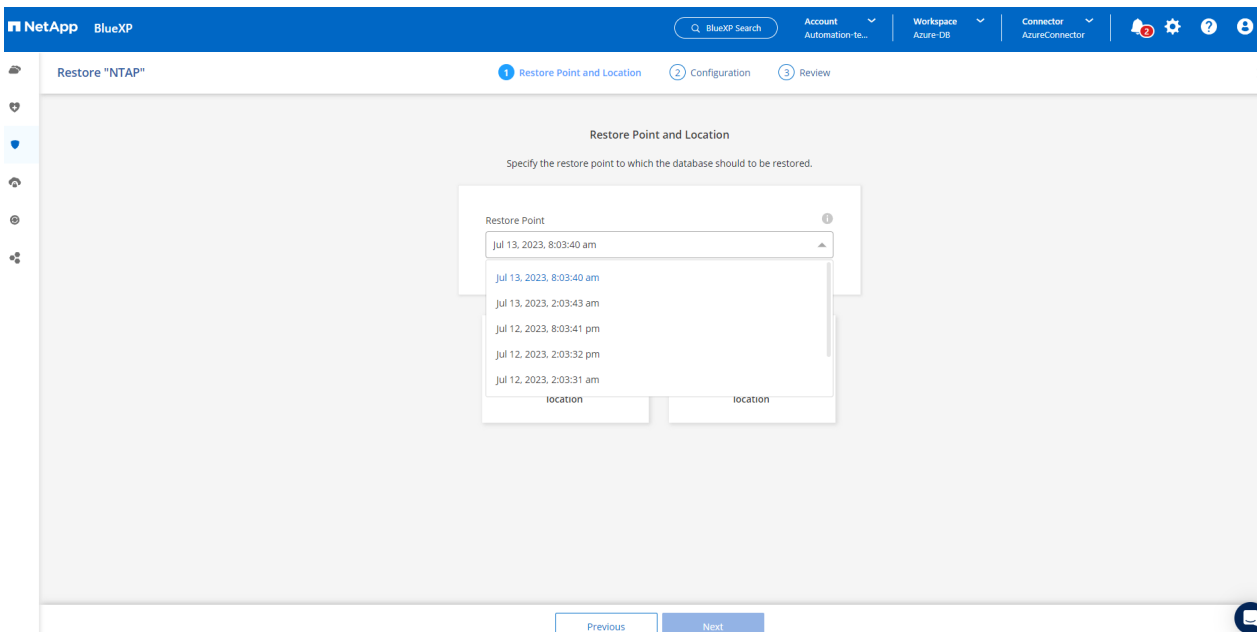
Select Timeframe

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

1. Para restaurar una base de datos, haga clic en el menú desplegable de tres puntos correspondiente a la base de datos particular que se restaurará en **Aplicaciones**, luego haga clic en **Restaurar** para iniciar el flujo de trabajo de restauración y recuperación de la base de datos.



2. Elija su **Punto de restauración** por marca de tiempo. Cada marca de tiempo en la lista representa un conjunto de copias de seguridad de base de datos disponible.



3. Elija su **Ubicación de restauración** a la **ubicación original** para una restauración y recuperación en el lugar de una base de datos Oracle.

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. Define tu **Alcance de restauración** y **Alcance de recuperación**. Todos los registros significan una recuperación completa actualizada, incluidos los registros actuales.

NetApp BlueXP

Restore "NTAP"

1 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

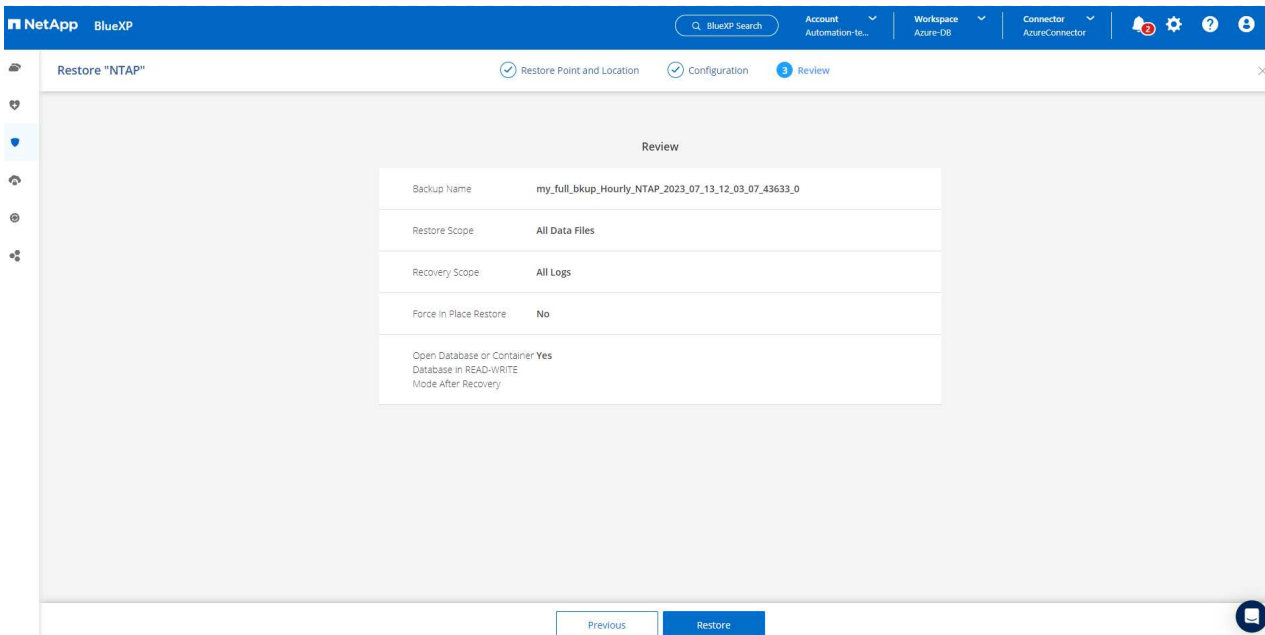
External Archive log locations

/mnt/log_location001

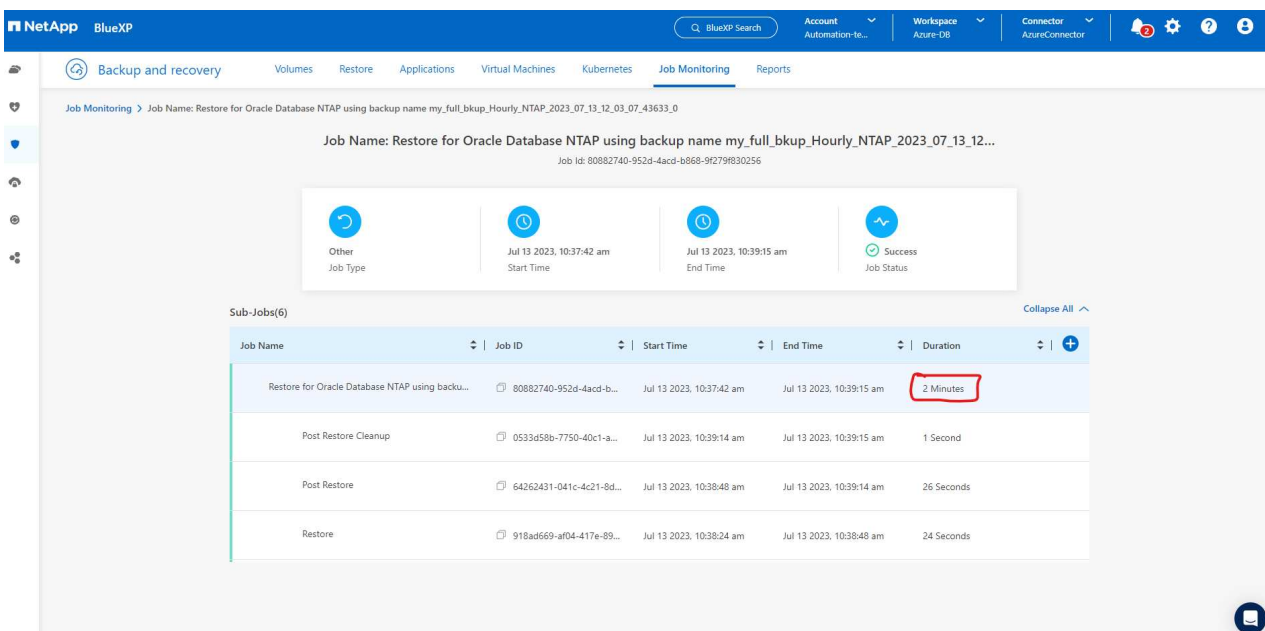
Open the database or the container database in READ-WRITE mode after recovery.

Previous Next

5. Revise y **Restaurar** para iniciar la restauración y recuperación de la base de datos.



6. Desde la pestaña **Monitoreo de trabajos**, observamos que tomó 2 minutos ejecutar una restauración y recuperación completa de la base de datos hasta la fecha.



Clon de base de datos de Oracle

Los procedimientos de clonación de base de datos son similares a los de restauración, pero en una máquina virtual de Azure alternativa con una pila de software Oracle idéntica preinstalada y configurada.



Asegúrese de que su almacenamiento de archivos de Azure NetApp tenga capacidad suficiente para una base de datos clonada del mismo tamaño que la base de datos principal que se va a clonar. La máquina virtual de Azure alternativa se ha agregado a **Aplicaciones**.

1. Haga clic en el menú desplegable de tres puntos correspondiente a la base de datos particular que se va a clonar en **Aplicaciones**, luego haga clic en **Restaurar** para iniciar el flujo de trabajo de clonación.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and dropdown menus 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 'Backup and recovery' and includes tabs for 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. Below the tabs, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows '4 Hosts', '3 ORACLE', and '0 Clone'. An 'Application Protection' section indicates '2 Protected' and '1 Unprotected' items. A table titled '3 Databases' lists the following data:

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

A context menu is open for the 'db1tst' row, showing options: 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore' (which is underlined and highlighted).

2. Seleccione el **Punto de restauración** y marque la opción **Restaurar a ubicación alternativa**.

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. En la siguiente página de **Configuración**, configure el **Host** alternativo, el **SID** de la nueva base de datos y **Oracle Home** tal como se configuraron en la VM de Azure alternativa.

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

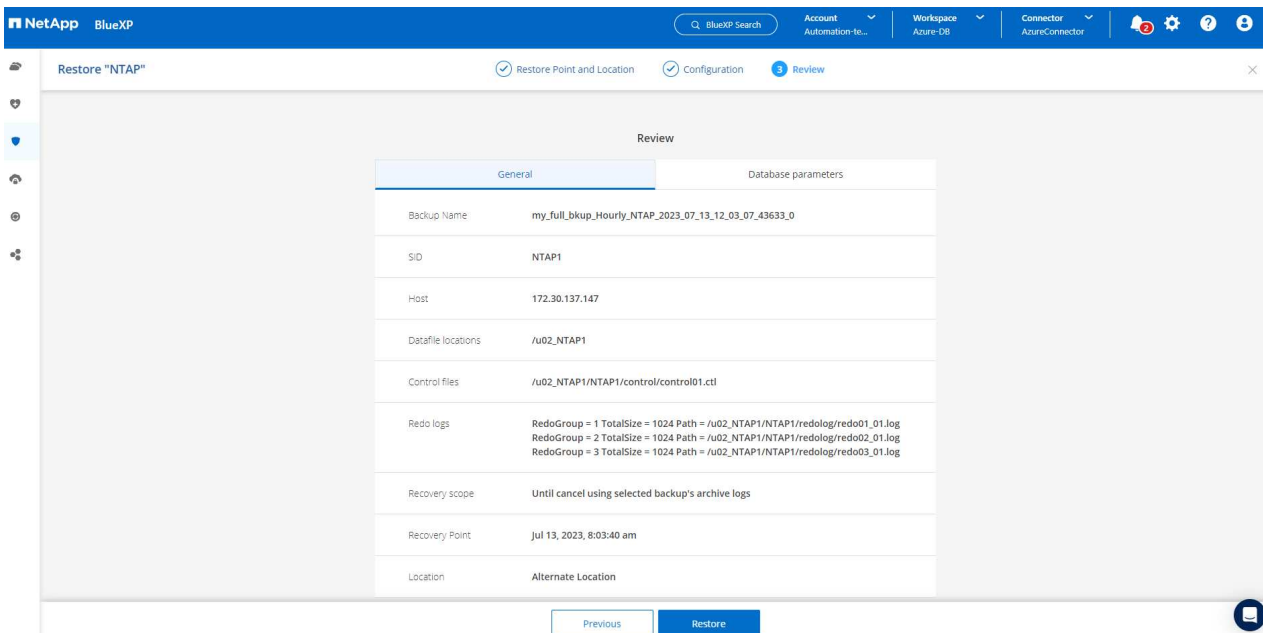
Oracle Home: /u01/app/oracle/product/19.0.0/clone Database Credentials: Optional

Maximum storage throughput (MiB/s): Optional

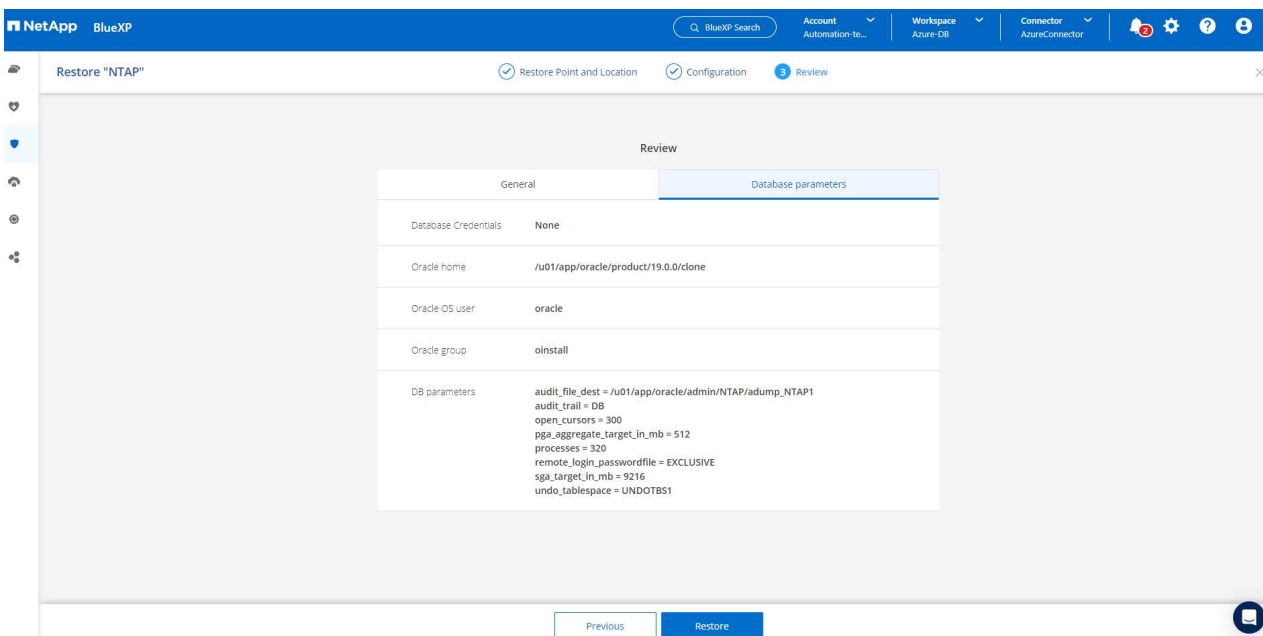
Enter throughput (1-4500)

Previous Next

4. La página de revisión **General** muestra los detalles de la base de datos clonada, como SID, host alternativo, ubicaciones de archivos de datos, alcance de recuperación, etc.



5. La página de revisión **Parámetros de la base de datos** muestra los detalles de la configuración de la base de datos clonada, así como también algunas configuraciones de parámetros de la base de datos.



6. Supervise el estado del trabajo de clonación desde la pestaña **Supervisión del trabajo**. Observamos que tomó 8 minutos clonar una base de datos Oracle de 1,6 TiB.

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. Valide la base de datos clonada en la página **Aplicaciones** de BlueXP que mostró que la base de datos clonada se registró inmediatamente con BlueXP.

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		Unprotected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

1 - 4 of 4

8. Valide la base de datos clonada en la máquina virtual Oracle Azure que mostró que la base de datos clonada se estaba ejecutando como se esperaba.

```

[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$databases;

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

```

Esto completa la demostración de una copia de seguridad, restauración y clonación de una base de datos de Oracle en Azure con la consola NetApp BlueXP usando el servicio SnapCenter .

Información adicional

Para obtener más información sobre la información que se describe en este documento, revise los siguientes documentos y/o sitios web:

- Configurar y administrar BlueXP

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

- Documentación de 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)

- Introducción a Azure

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

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.