



TR-4964: Copia de seguridad, restauración y clonación de bases de datos Oracle con los servicios de SnapCenter - AWS

NetApp database solutions

NetApp
August 18, 2025

Tabla de contenidos

TR-4964: Copia de seguridad, restauración y clonación de bases de datos Oracle con los servicios de SnapCenter - AWS 1

Objetivo 1

Audiencia 1

Entorno de prueba y validación de soluciones 2

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 4

Preparación para la incorporación a BlueXP 4

Implementar un conector para los servicios de SnapCenter 5

Definir una credencial en BlueXP para acceder a los recursos de AWS 12

Configuración de los servicios de SnapCenter 16

Copia de seguridad de la base de datos de Oracle 24

Restauración y recuperación de bases de datos de Oracle 28

Clon de base de datos de Oracle 31

Información adicional 36

TR-4964: Copia de seguridad, restauración y clonación de bases de datos Oracle con los servicios de SnapCenter - AWS

Esta solución proporciona 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 en la nube de Azure.

Allen Cao, Niyaz Mohamed, NetApp

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 el almacenamiento en la nube de NetApp . 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 el almacenamiento de Amazon FSx ONTAP y en instancias de cómputo de EC2. Si bien es mucho más fácil de configurar y usar, los Servicios de SnapCenter ofrecen funcionalidades clave que están disponibles en la herramienta de interfaz de usuario tradicional de SnapCenter .

Esta solución aborda los siguientes casos de uso:

- Copia de seguridad de base de datos con instantáneas para bases de datos Oracle alojadas en Amazon FSx ONTAP
- Recuperación de la base de datos Oracle en caso de fallo
- Clonación rápida y eficiente en términos de almacenamiento de bases de datos primarias para un entorno de desarrollo/prueba u otros casos de uso

Audiencia

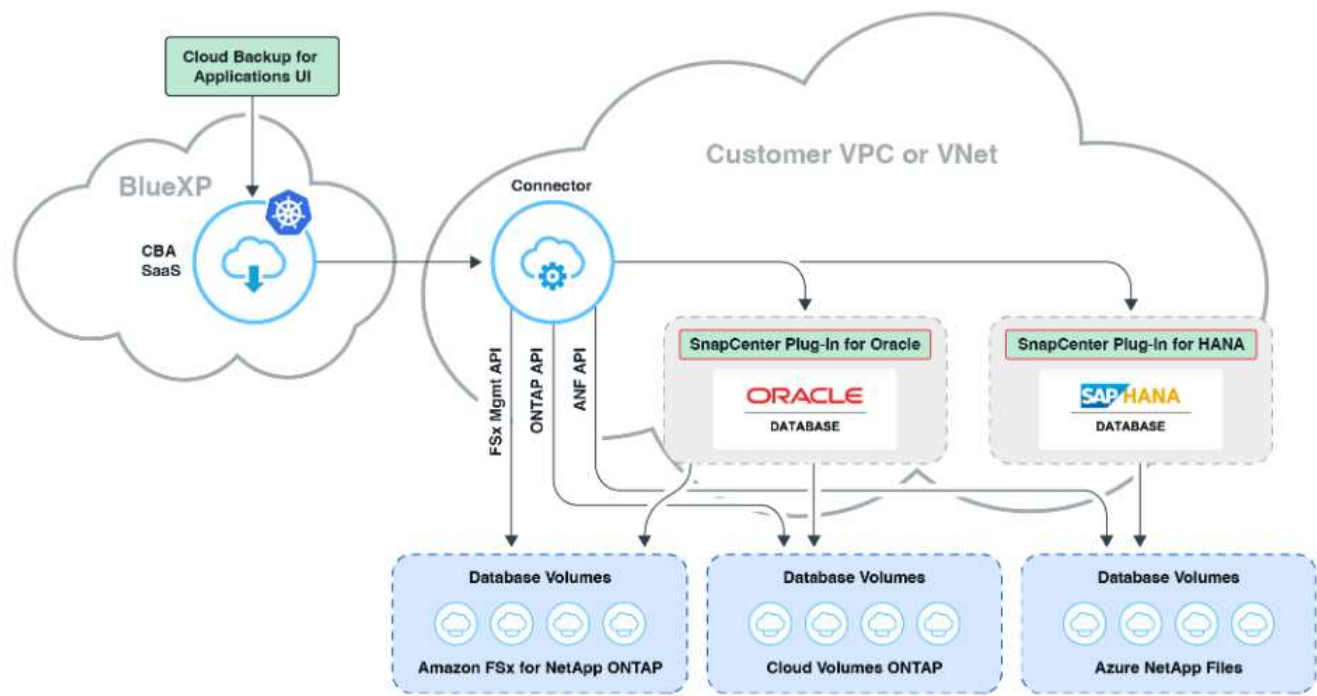
Esta solución está destinada a los siguientes públicos:

- El DBA que administra las bases de datos Oracle que se ejecutan en el almacenamiento Amazon FSx ONTAP
- 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 la nube pública de AWS
- El administrador de almacenamiento que respalda y administra el almacenamiento de Amazon FSx ONTAP
- El propietario de la aplicación que posee las aplicaciones que se implementan en el almacenamiento de Amazon FSx ONTAP

Entorno de prueba y validación de soluciones

La prueba y validación de esta solución se realizó en un entorno AWS FSx y EC2 que podría no coincidir con el entorno de implementación final. Para más información, consulte la sección [Factores clave a considerar en la implementación](#) .

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 FSx ONTAP	Versión actual ofrecida por AWS	Un clúster FSx HA en la misma VPC y zona de disponibilidad
Instancia EC2 para computación	t2.xlarge/4vCPU/16G	Dos instancias EC2 T2 xlarge, una como servidor de base de datos principal y la otra como servidor de base de datos clonado

Software

Red Hat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Se implementó una suscripción a RedHat para realizar pruebas
---------------	--	--

Infraestructura de red de Oracle	Versión 19.18	Parche RU aplicado p34762026_190000_Linux-x86-64.zip
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	v2.3.1.2324

Factores clave a considerar en la implementación

- **El conector se implementará en la misma VPC que la base de datos y FSx.** Cuando sea posible, el conector debe implementarse en la misma VPC de AWS, lo que permite la conectividad con el almacenamiento FSx y la instancia de cómputo EC2.
- **Una política de AWS IAM creada para el conector de SnapCenter .** La política en formato JSON está disponible en la documentación detallada del servicio SnapCenter . Cuando inicia la implementación del conector con la consola BlueXP , también se le solicita que configure los requisitos previos con detalles del permiso requerido en formato JSON. La política debe asignarse a la cuenta de usuario de AWS que posee el conector.
- **La clave de acceso de la cuenta de AWS y el par de claves SSH creados en la cuenta de AWS.** El par de claves SSH se asigna al usuario ec2 para iniciar sesión en el host del conector y luego implementar un complemento de base de datos en el host del servidor de base de datos EC2. La clave de acceso otorga permiso para aprovisionar el conector requerido con la política IAM anterior.
- **Se agregó una credencial a la configuración de la consola BlueXP .** Para agregar Amazon FSx ONTAP al entorno de trabajo de BlueXP , se configura una credencial que otorga a BlueXP permisos para acceder a Amazon FSx ONTAP en la configuración de la consola de BlueXP .
- **java-11-openjdk instalado en el host de la instancia de base de datos EC2.** 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 Amazon FSx ONTAP y una instancia de cómputo EC2. Este documento completa algunos detalles que podrían faltar en instrucciones más generales.

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 Amazon FSx ONTAP.
- Ve a el siguiente video tutorial.

[Implementación de la solución](#)

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 EC2 con una base de datos Oracle completamente implementada y en funcionamiento.
2. Un clúster de Amazon FSx ONTAP implementado en AWS que aloja los volúmenes de base de datos anteriores.
3. Un servidor de base de datos opcional en una instancia EC2 que se puede utilizar para probar la clonación de una base de datos 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 Oracle de producción.
4. Si necesita ayuda para cumplir con los requisitos previos anteriores para la implementación de la base de datos de Oracle en la instancia de cómputo de Amazon FSx ONTAP y EC2, consulte ["Implementación y protección de bases de datos de Oracle en AWS FSx/EC2 con iSCSI/ASM"](#) o libro blanco ["Mejores prácticas para la implementación de bases de datos Oracle en EC2 y FSx"](#)

Preparación para la incorporación a BlueXP

1. Utilice el enlace "[NetApp BlueXP](#)" para registrarse y obtener acceso a la consola BlueXP .
2. Inicie sesión en su cuenta de AWS para crear una política de IAM con los permisos adecuados y asignar la política a la cuenta de AWS que se utilizará para la implementación del conector BlueXP .

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with sections like 'Dashboard', 'Access management', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings', 'Access reports', 'Access analyzer', 'Archive rules', 'Analyzers', 'Settings', 'Credential report', 'Organization activity', and 'Service control policies (SCPs)'. The main content area is titled 'Policies > snapcenter' and 'Summary'. It displays 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' and a 'JSON' view. The JSON view displays the following policy document:

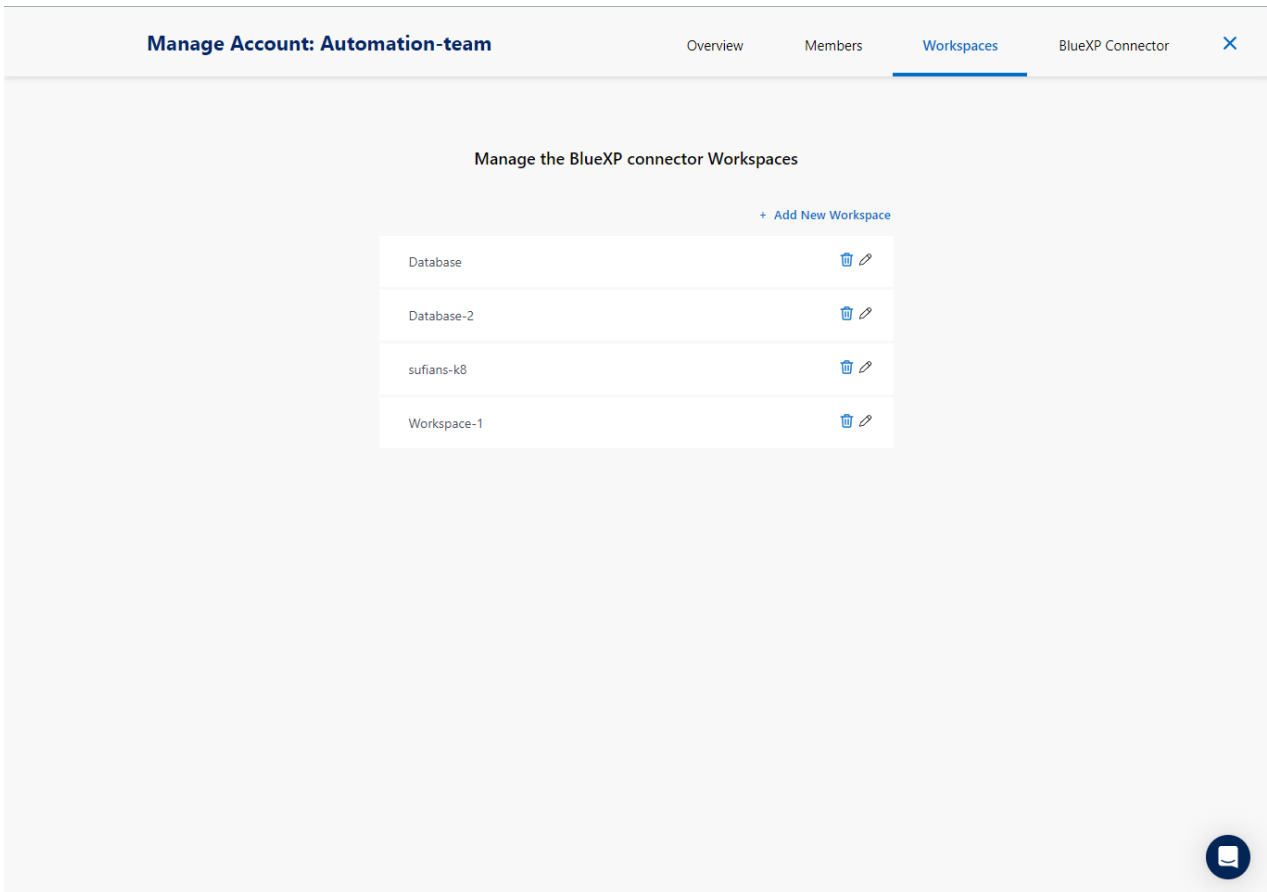
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces"
      ]
    }
  ]
}
```

La política debe configurarse con una cadena JSON que está disponible en la documentación de NetApp . La cadena JSON también se puede recuperar de la página cuando se inicia el aprovisionamiento del conector y se le solicita la asignación de permisos de requisitos previos.

3. También necesita la VPC de AWS, la subred, el grupo de seguridad, una clave de acceso y secretos de cuenta de usuario de AWS, una clave SSH para el usuario ec2, etc., listos para el aprovisionamiento del conector.

Implementar un conector para los servicios de SnapCenter

1. Inicie sesión en la consola BlueXP . Para una cuenta compartida, se recomienda crear un espacio de trabajo individual haciendo clic en **Cuenta > Administrar cuenta > Espacio de trabajo** para agregar un nuevo espacio de trabajo.



2. Haga clic en **Agregar un conector** para iniciar el flujo de trabajo de aprovisionamiento del conector.

NetApp Cloud Manager

Account: Automation-team | Workspace: new-workspace | Connector: N/A

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 and storage efficiencies to reduce time and cost

1. Elija su proveedor de nube (en este caso, **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. Omite los pasos de **Permiso**, **Autenticación** y **Redes** si ya los tienes configurados en tu cuenta de AWS. De lo contrario, deberá configurarlos antes de continuar. Desde aquí, también puede recuperar los permisos para la política de AWS a la que se hace referencia en la sección anterior "[Preparación](#)"

para la incorporación a BlueXP . "

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. Ingrese la autenticación de su cuenta de AWS con **Clave de acceso** y **Clave secreta**.

- 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

AKIA6JRXA6ZVGVF5HMO3

AWS Secret Key

.....

Want to launch an instance without AWS Credentials? ☐[Previous](#)[Next](#)

2. Nombre la instancia del conector y seleccione **Crear rol** en **Detalles**.

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

Details

Connector Instance Name

SnapCenterSvs

[+ Add Tags to Connector Instance](#)

Connector Role

☒ Create Role ☐ Select an existing Role

Role Name

Cloud-Manager-Operator-VZzSSP9-SnapCenter

☐ AWS Managed Encryption

Master Key: aws/ebs (default)

[Change Key](#)[Previous](#)[Next](#)

1. Configure la red con la **VPC**, la **Subred** y el **Par de claves SSH** adecuados para el acceso al conector.

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)

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 AWS services.

Previous

Next

2. Establezca el **Grupo de seguridad** para el conector.

Add BlueXP Connector - AWS

More Information

✓ AWS Credentials

✓ 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

1 Security Group

Security Group Name	Description
☒ default	default VPC security group

Previous

Next

3. 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 aparece en el panel de AWS EC2.

Add BlueXP Connector - AWS

More Information

✓ AWS Credentials

✓ Details

✓ Network

✓ Security Group

5 Review

Review

[Code for Terraform Automation](#)

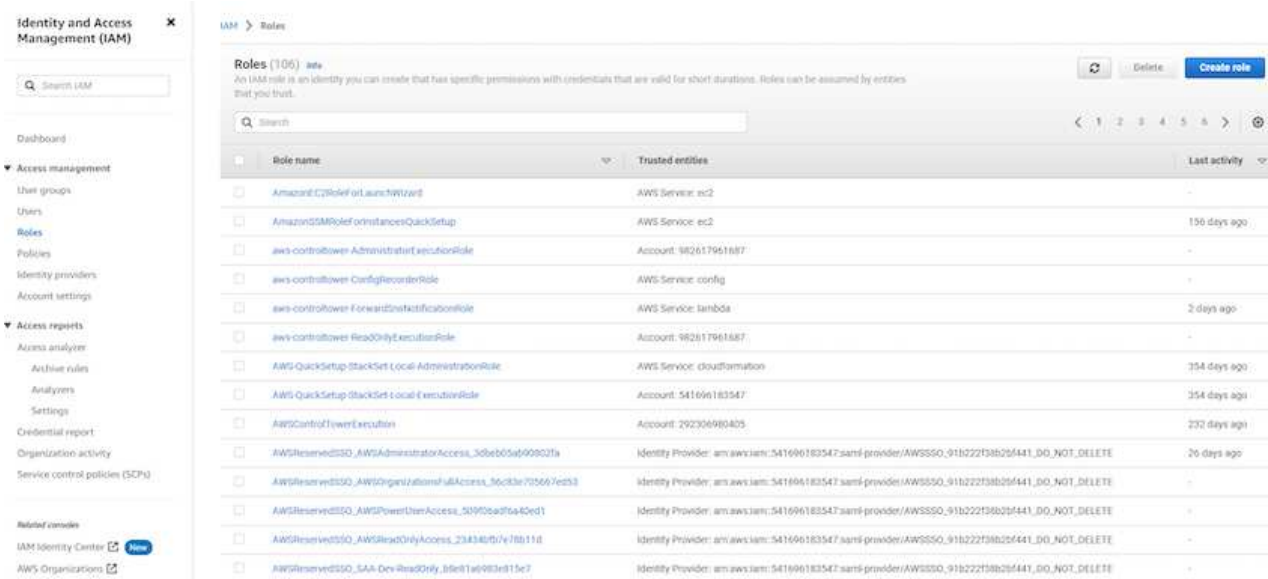
BlueXP Connector Name	aws-snapctr-us-east
AWS Access Key	AKIAH4H43ZT56IWWR3TI
Region	us-east-1
VPC	vpc-0b522d5e982a50ceb - 172.30.15.0/25
Subnet	172.30.15.0/25 priv-subnet-01
Key Pair	sufi_new
Public IP	Use subnet settings (Disable)
Proxy	None
Security Group	default

Previous

Add

Definir una credencial en BlueXP para acceder a los recursos de AWS

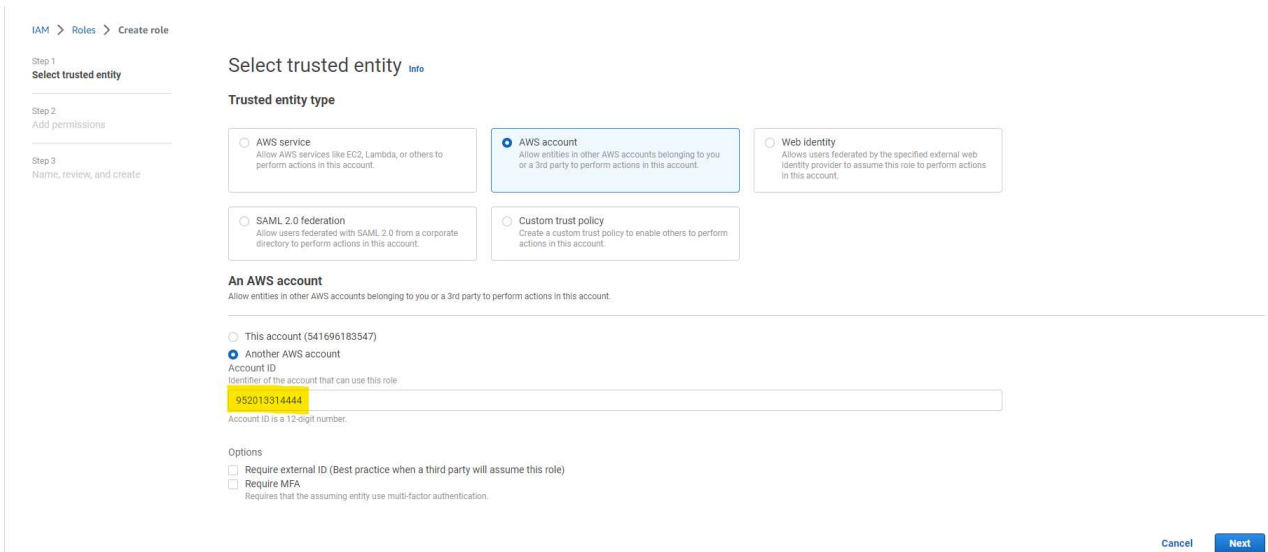
1. Primero, desde la consola de AWS EC2, cree un rol en el menú **Administración de identidad y acceso (IAM) Roles, Crear rol** para iniciar el flujo de trabajo de creación de roles.



The screenshot shows the AWS IAM console. On the left, the 'Identity and Access Management (IAM)' menu is open, and 'Roles' is selected. The main area displays a list of roles. The 'Create role' button is in the top right corner.

Role name	Trusted entities	Last activity
AmazonEC2RoleforAWSUser	AWS Service: ec2	-
AmazonSSMRoleforInstancesQuickSetup	AWS Service: ec2	156 days ago
aws-controltower-AdministratorExecutionRole	Account: 982617961887	-
aws-controltower-ConfigRecorderRole	AWS Service: config	-
aws-controltower-ForwardNotificationRole	AWS Service: lambda	2 days ago
aws-controltower-ReadOnlyExecutionRole	Account: 982617961887	-
AWS-QuickSetup-StackSet-Local-AdministrationRole	AWS Service: cloudformation	154 days ago
AWS-QuickSetup-StackSet-Local-ExecutionRole	Account: 541696183547	154 days ago
AWSControlTowerExecution	Account: 292306980405	232 days ago
AWSReservedSSO_AWSAdministratorAccess_3d8eb05a699802fa	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	26 days ago
AWSReservedSSO_AWSOrganizationalAccess_Mock3e725667e253	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_AWSPowerUserAccess_509f0ad7644ed1	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_AWSReadOnlyAccess_23434b7b71bb11d	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_SAA-Dev-ReadOnly_Ibfe81a9983ed11e7	Identity Provider: am:aws:sam:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-

2. En la página **Seleccionar entidad confiable**, elija **Cuenta de AWS, Otra cuenta de AWS** y pegue el ID de la cuenta de BlueXP , que se puede recuperar desde la consola de BlueXP .



The screenshot shows the 'Create role' page in the AWS IAM console, specifically the 'Select trusted entity' step. The 'AWS account' option is selected. The 'Account ID' field is highlighted with a yellow box, showing the value '992013314444'.

Select trusted entity

Trusted entity type

- ☐ AWS service
- ☒ AWS account
- ☐ Web Identity
- ☐ SAML 2.0 federation
- ☐ Custom trust policy

An AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ This account (541696183547)

☒ Another AWS account

Account ID

Identifier of the account that can use this role

992013314444

Account ID is a 12-digit number.

Options

- ☐ Require external ID (Best practice when a third party will assume this role)
- ☐ Require MFA

Requires that the assuming entity use multi-factor authentication.

Cancel **Next**

3. Filtra las políticas de permisos por fsx y agrega **Políticas de permisos** al rol.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

Permissions policies (Selected 1/889) Info
Choose one or more policies to attach to your new role.

Q Filter policies by property or policy name and press enter. 4 matches

'fsx' X Clear filters

	Policy name	Type	Description
☐	AmazonFSxReadOnlyAccess	AWS ma...	Provides read only access to Amazon FSx.
☒	AmazonFSxFullAccess	AWS ma...	Provides full access to Amazon FSx and access to related AWS services.
☐	AmazonFSxConsoleReadOnlyAccess	AWS ma...	Provides read only access to Amazon FSx and access to related AWS services via the AWS Management Console.
☐	AmazonFSxConsoleFullAccess	AWS ma...	Provides full access to Amazon FSx and access to related AWS services via the AWS Management Console.

► **Set permissions boundary - optional** Info
Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Cancel Previous **Next**

4. En la página **Detalles del rol**, nombre el rol, agregue una descripción y luego haga clic en **Crear rol**.

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
fsxn_bluexp
Maximum 64 characters. Use alphanumeric and "+", "@", "-" characters.

Description
Add a short explanation for this role.
Grant permission for BlueXP access to FSxN in AWS.
Maximum 1000 characters. Use alphanumeric and "+", "@", "-" characters.

Step 1: Select trusted entities Edit

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "952013314444"
9       },
10      "Condition": {}
11    }
12  ]
13 }

```

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

NetApp BlueXP

Q BlueXP Search Account Automation-te... Workspace Database-2 Connector acio-aws-conn...

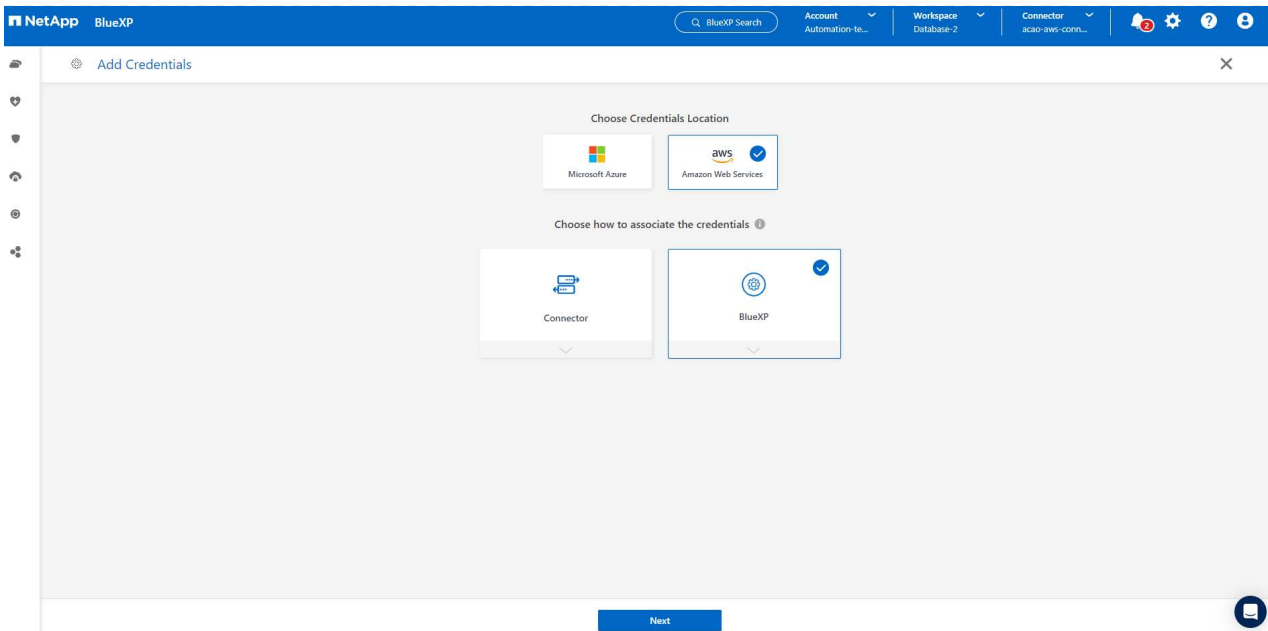
Credentials Account credentials User credentials

BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.

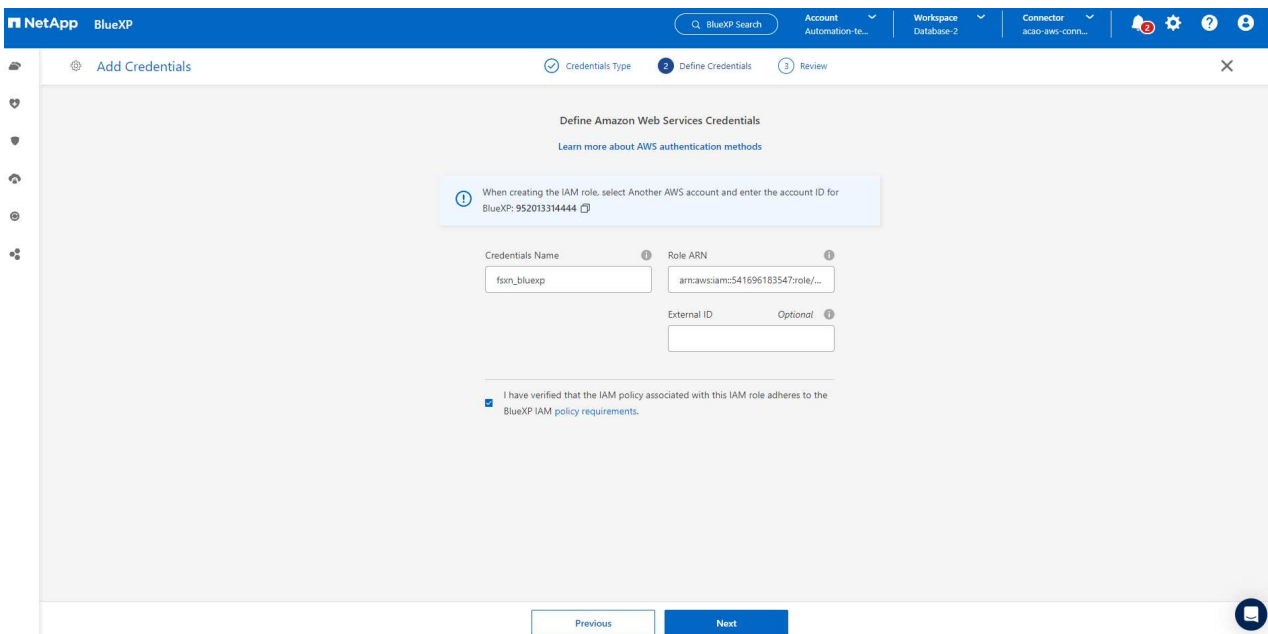
5 Credentials Add credentials

shantanucreds	
Type: Assume Role BlueXP	
210811600188 AWS Account ID	nikarhik_kafka_nfs_role_FSxN Assume Role

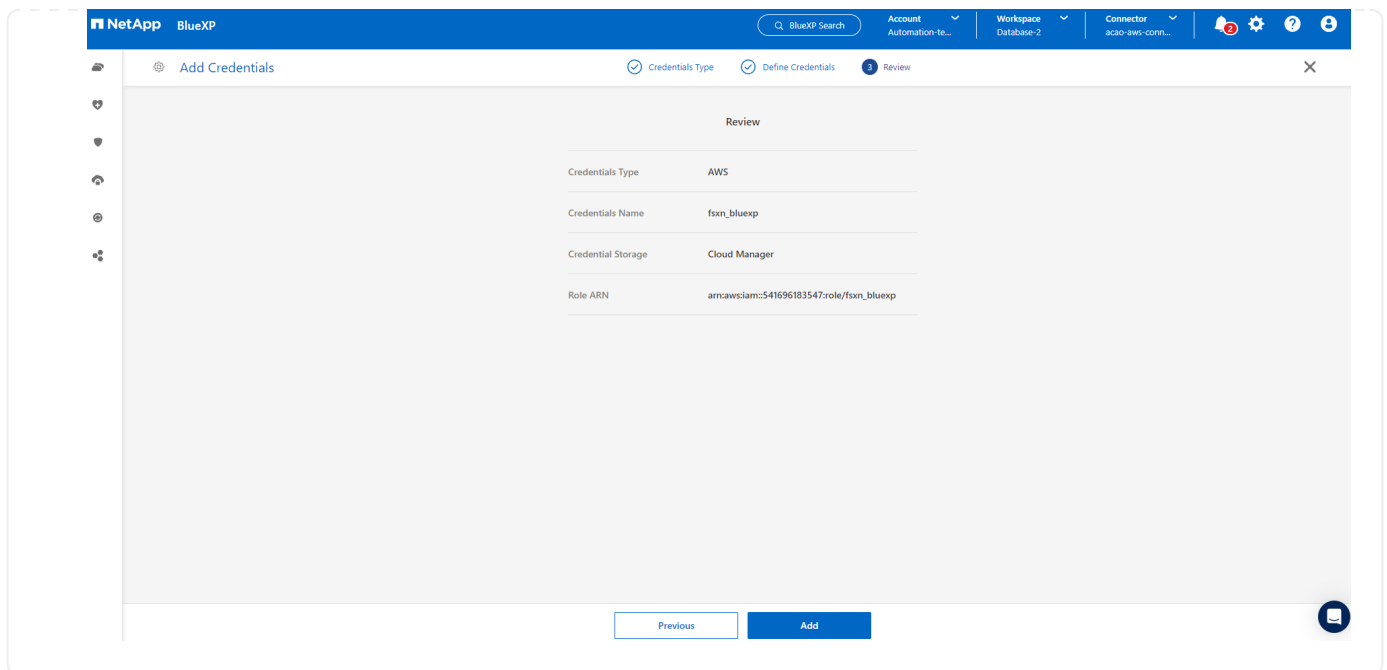
6. Elija la ubicación de las credenciales como - **Amazon Web Services - BlueXP**.



- Defina las credenciales de AWS con el **Role ARN** adecuado, que se puede recuperar del rol de AWS IAM creado en el paso uno anterior. **ID de cuenta** de BlueXP , que se utiliza para crear la función de AWS IAM en el paso uno.



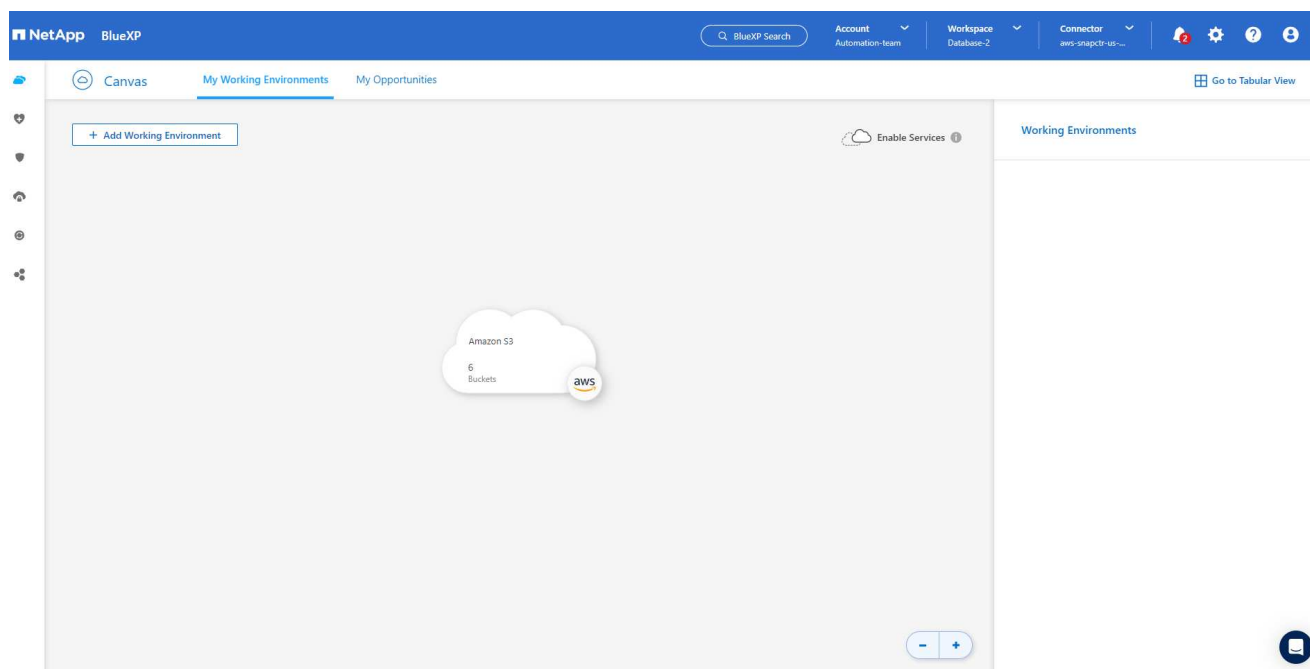
- Revisar y **Agregar**



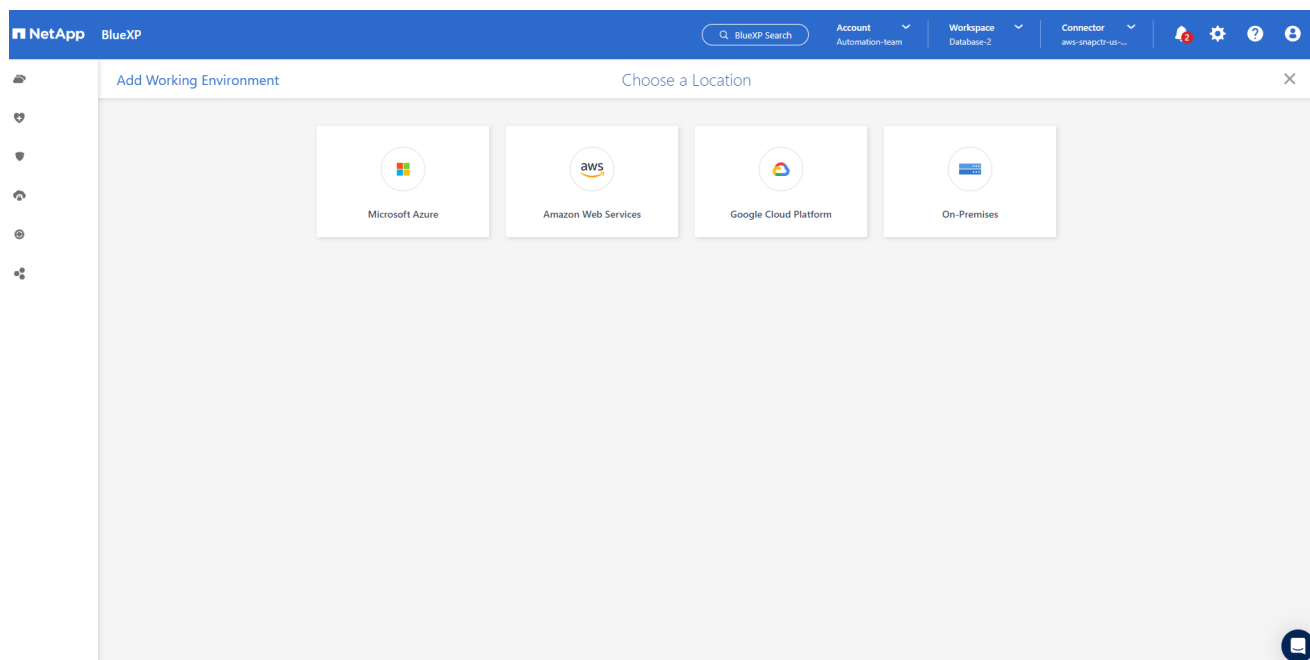
Configuración de los servicios de SnapCenter

Con el conector implementado y la credencial agregada, los servicios de SnapCenter ahora se pueden configurar con el siguiente procedimiento:

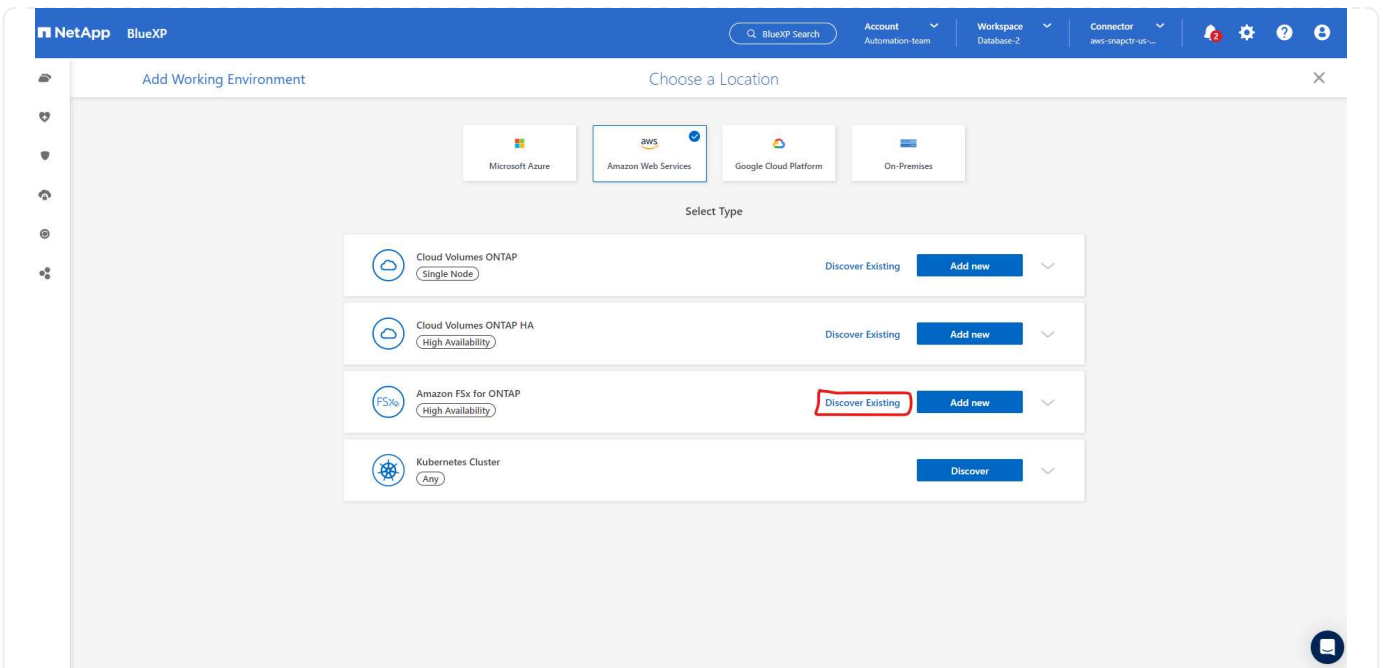
1. Desde **Mi entorno de trabajo**, haga clic en **Agregar entorno de trabajo** para descubrir FSx implementado en AWS.



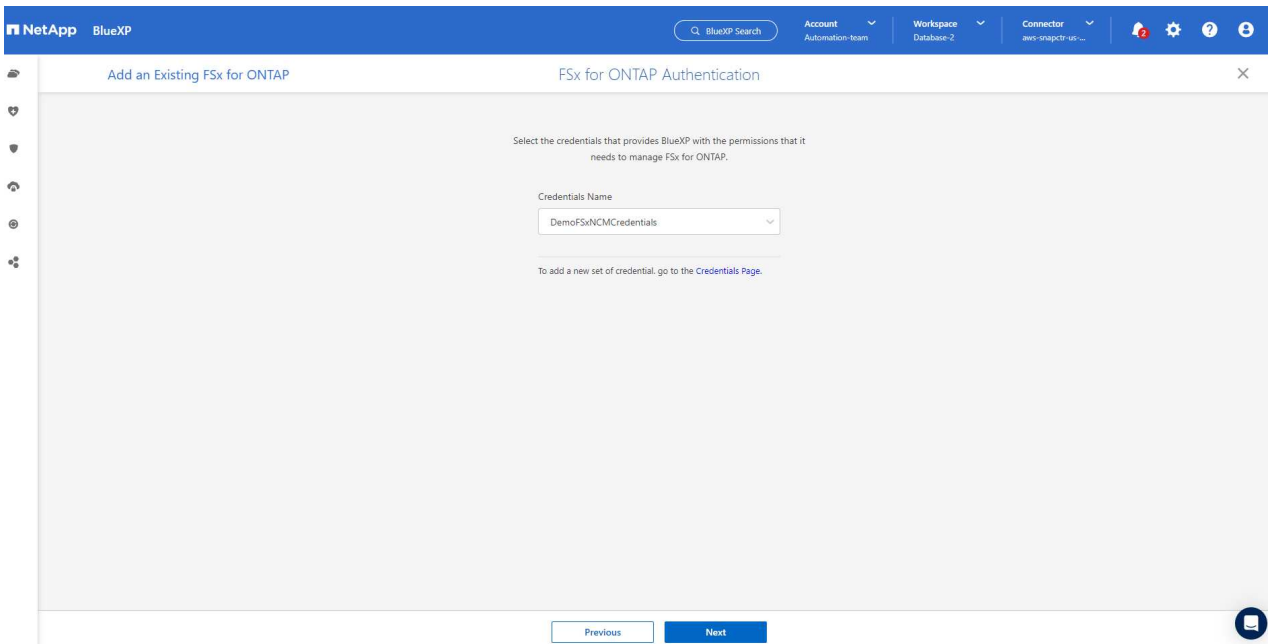
1. Elija **Amazon Web Services** como ubicación.



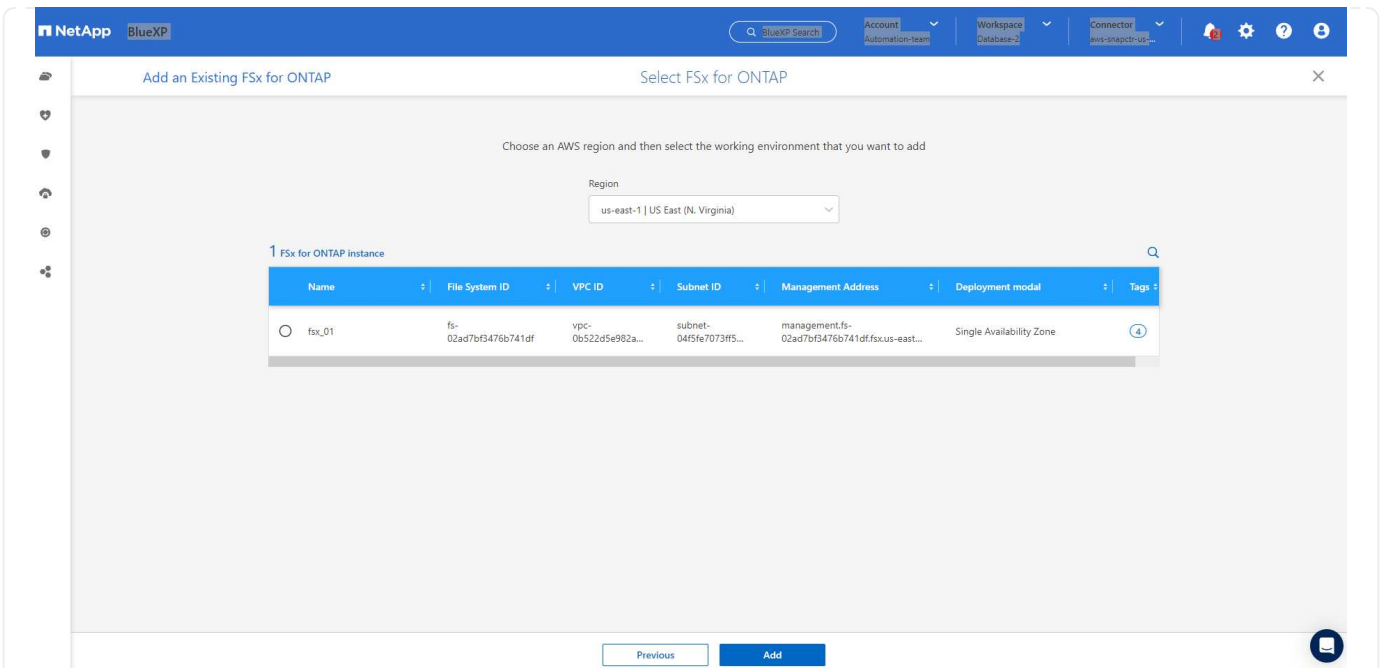
1. Haga clic en **Descubrir existente** junto a * Amazon FSx ONTAP*.



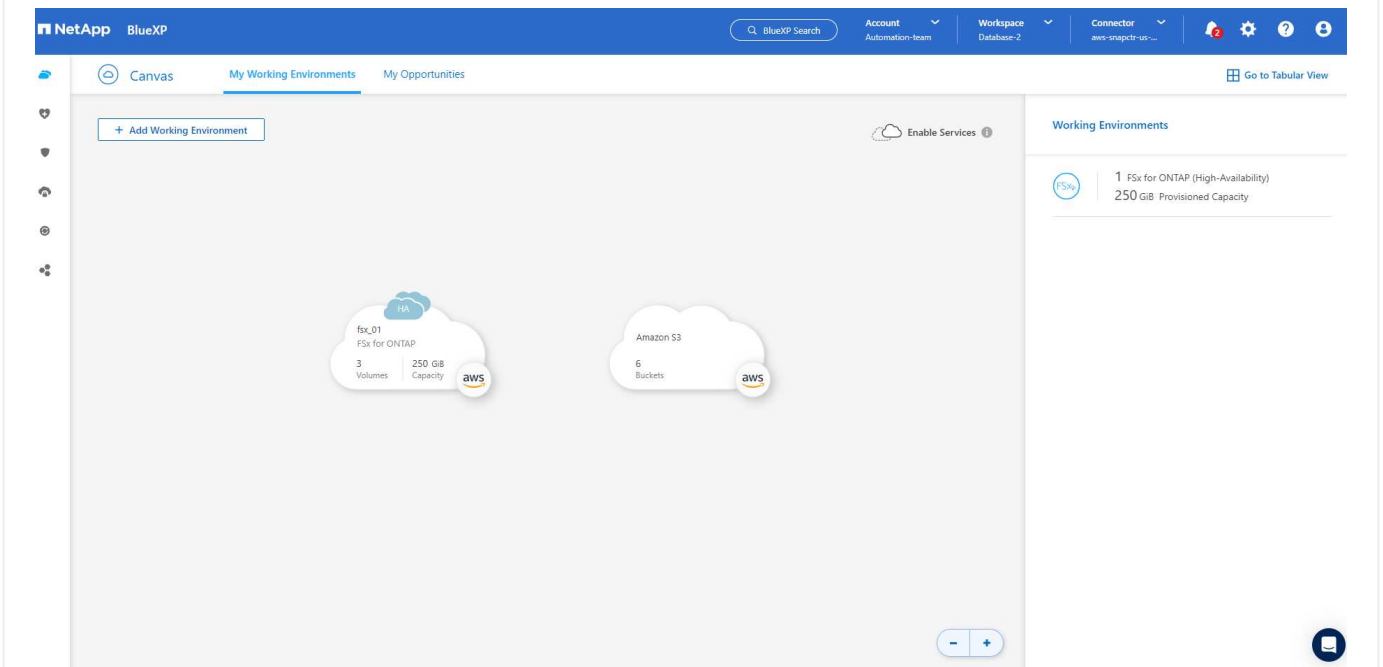
1. Seleccione el **Nombre de credenciales** que ha creado en la sección anterior para otorgarle a BlueXP los permisos que necesita para administrar FSx ONTAP. Si no ha agregado credenciales, puede agregarlas desde el menú **Configuración** en la esquina superior derecha de la consola BlueXP .



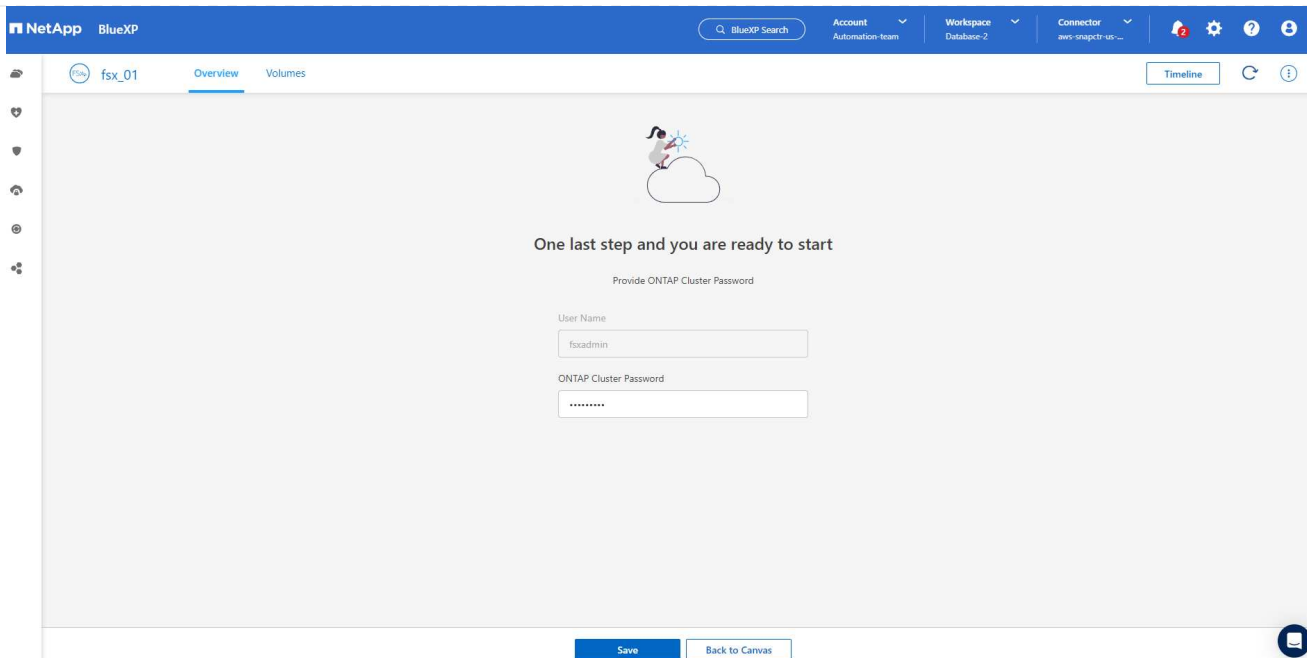
2. Elija la región de AWS donde está implementado Amazon FSx ONTAP , seleccione el clúster FSx que aloja la base de datos de Oracle y haga clic en Agregar.



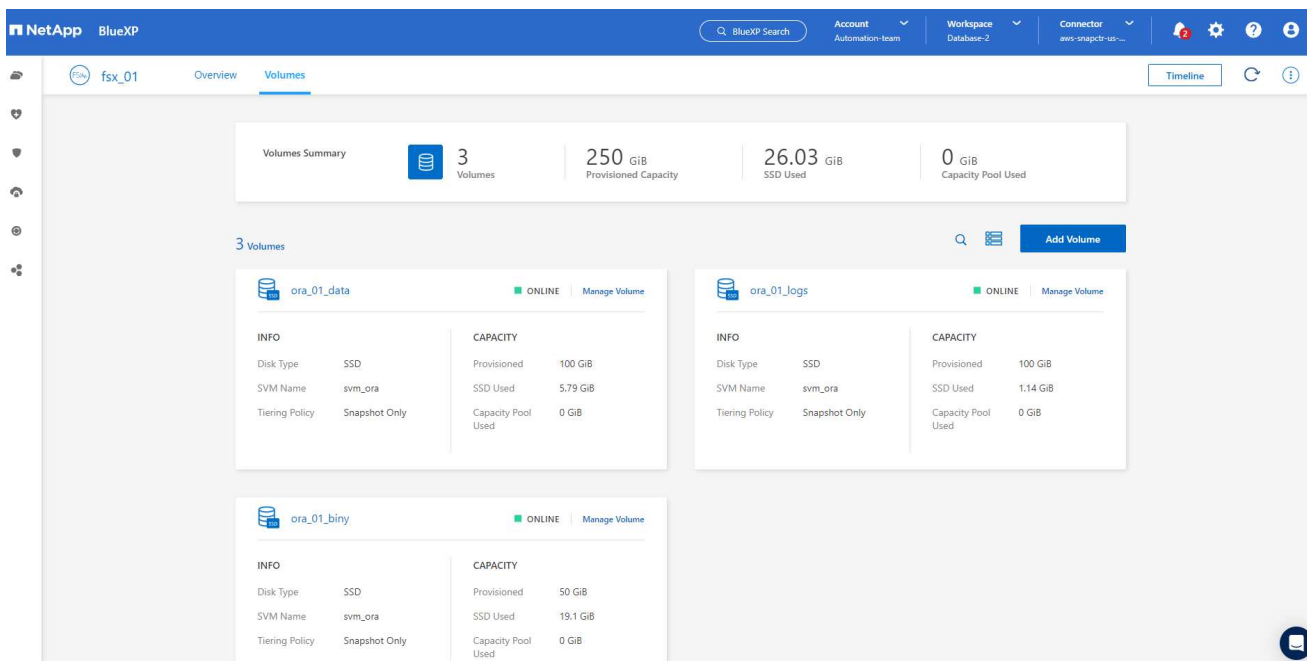
1. La instancia de Amazon FSx ONTAP descubierta ahora aparece en el entorno de trabajo.



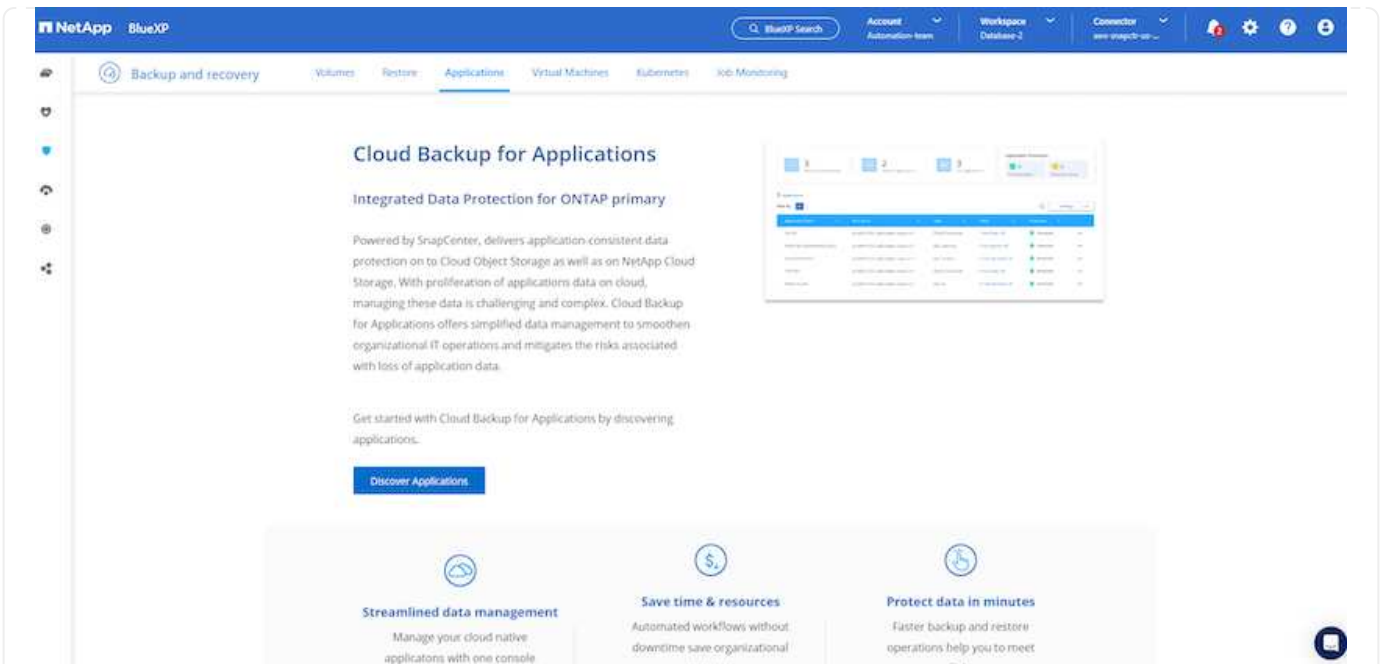
1. Puede iniciar sesión en el clúster FSx con las credenciales de su cuenta fsxadmin.



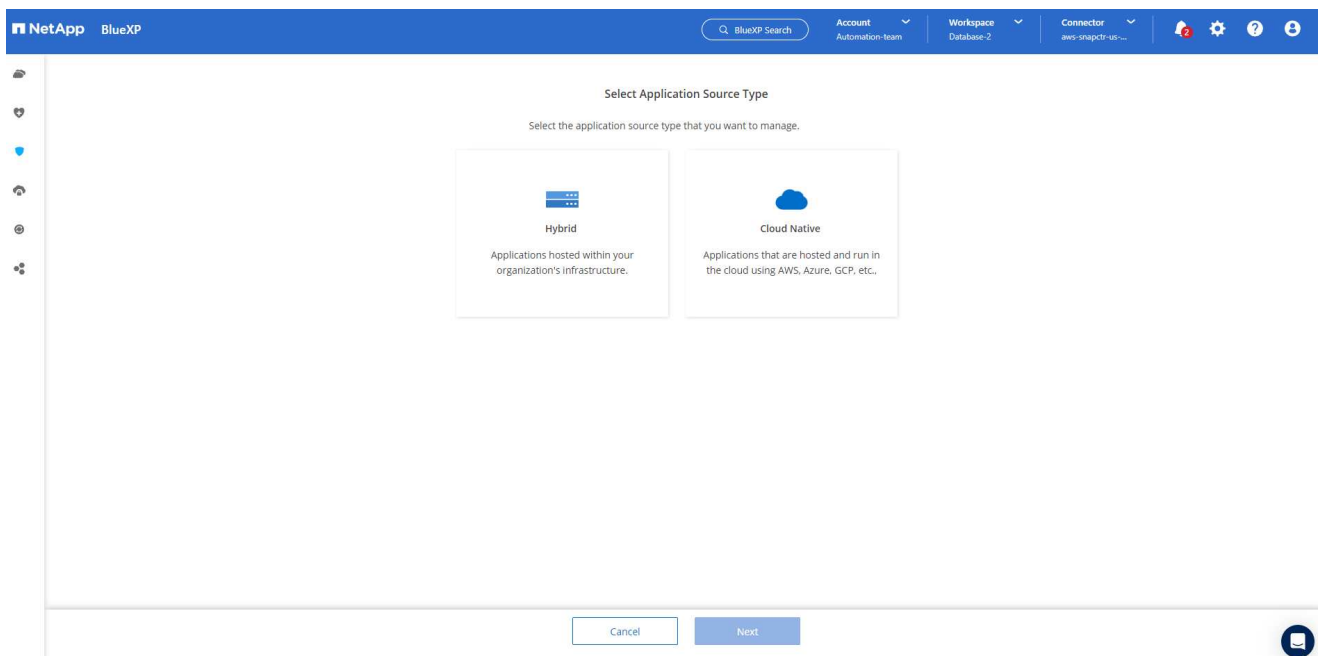
1. Después de iniciar sesión en Amazon FSx ONTAP, revise la información de almacenamiento de su base de datos (como los volúmenes de la base de datos).



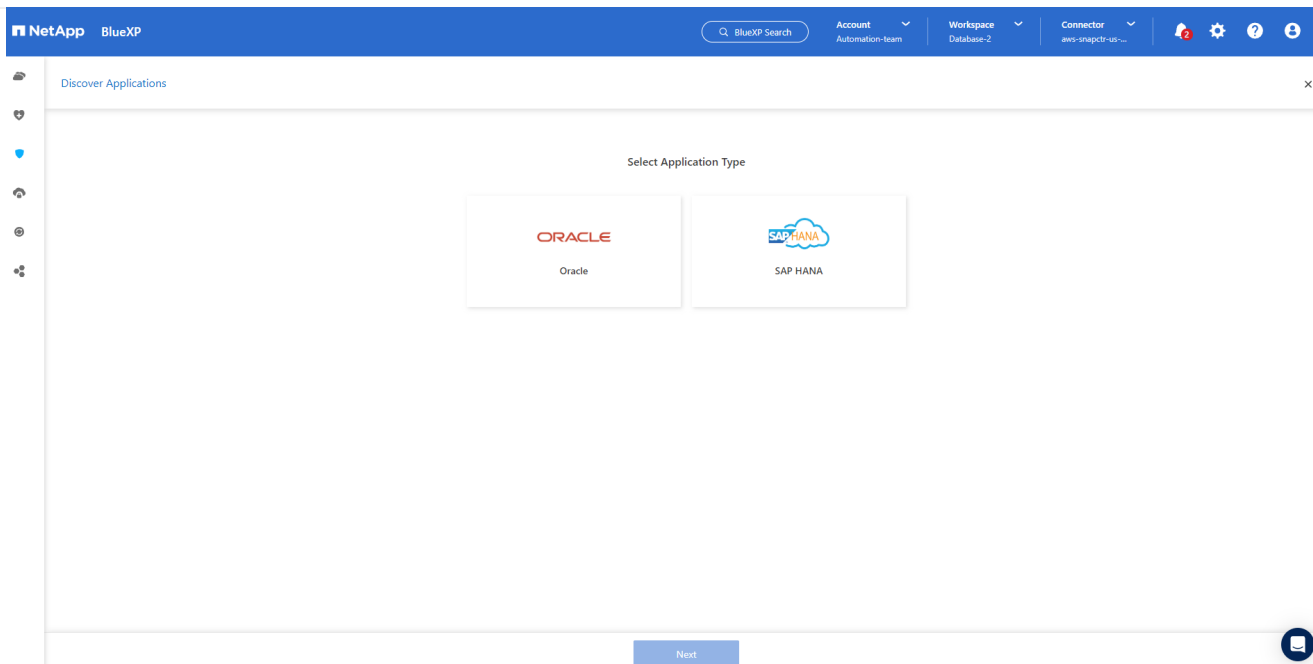
1. Desde la barra lateral izquierda de la consola, pase el mouse sobre el ícono de protección y luego haga clic en **Protección > Aplicaciones** para abrir la página de inicio de Aplicaciones. Haga clic en **Descubrir aplicaciones**.



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

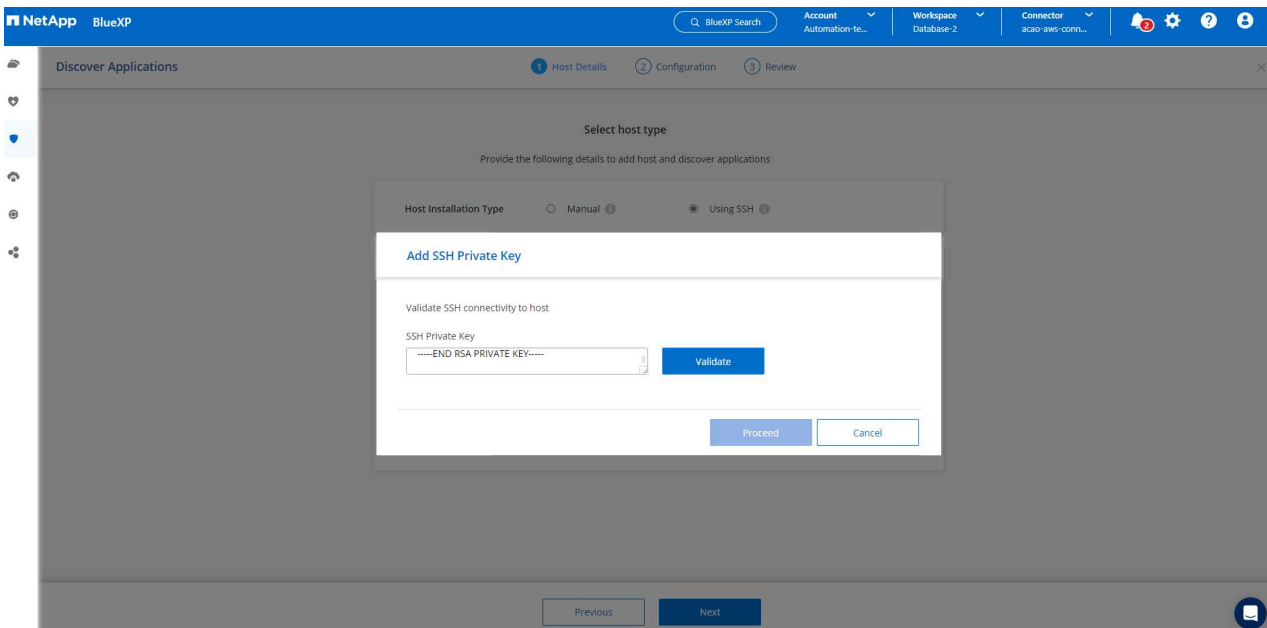


1. Elija **Oracle** como tipo de aplicación.

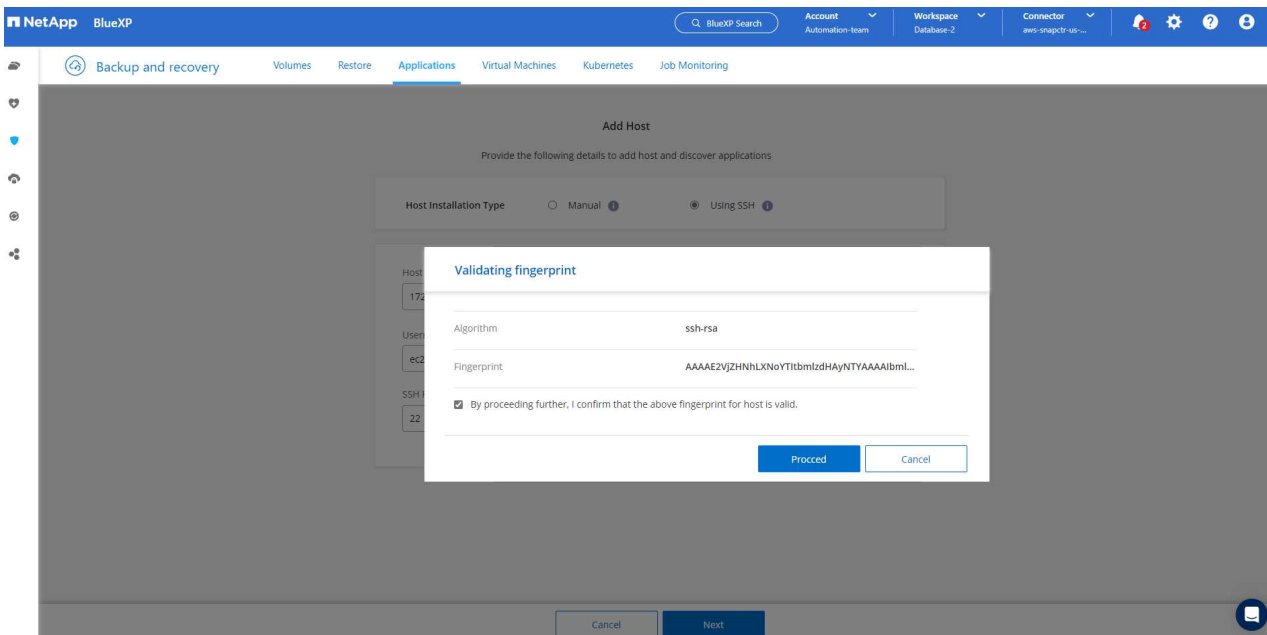


1. Complete los detalles del host de la aplicación Oracle de AWS EC2. Elija **Usar SSH** como **Tipo de instalación de host** para la instalación del complemento y el descubrimiento de la base de datos en un solo paso. Luego, haga clic en **Agregar clave privada SSH**.

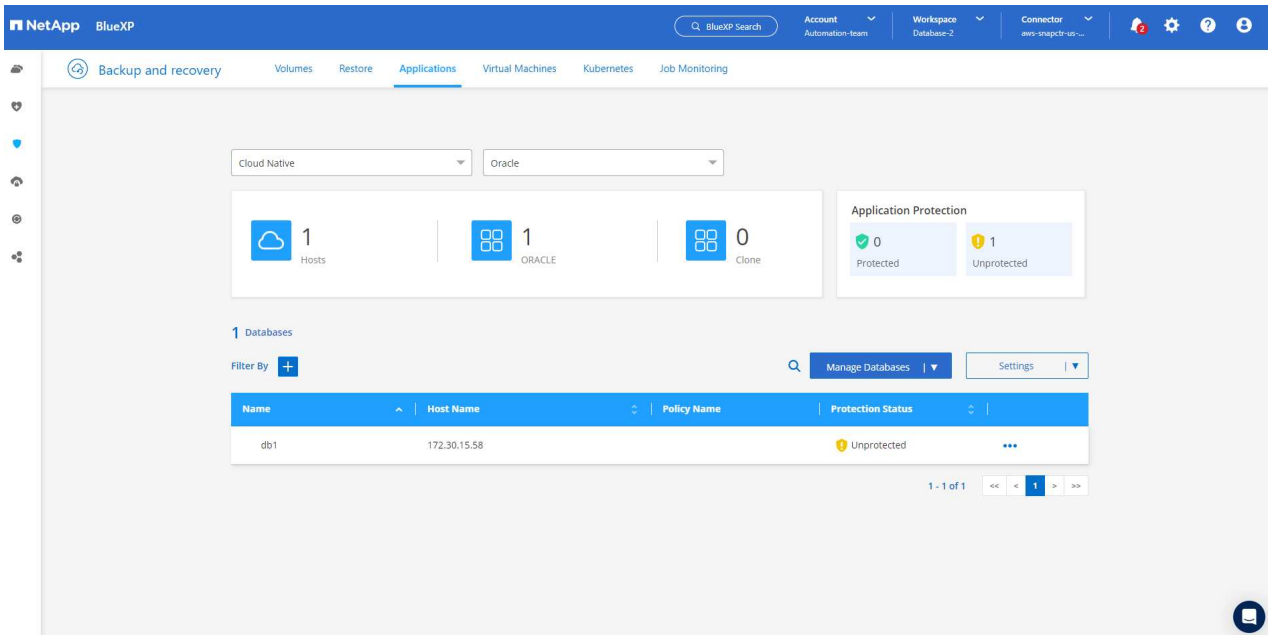
2. Pegue su clave SSH ec2-user para el host de la base de datos EC2 y haga clic en **Validar** para continuar.



3. Se le solicitará **Validando huella digital** para continuar.



4. Haga clic en **Siguiente** para instalar un complemento de base de datos de Oracle y descubrir las bases de datos de Oracle en el host EC2. Las bases de datos descubiertas se agregan a **Aplicaciones**. El **Estado de protección** de la base de datos se muestra como **Desprotegido** cuando se descubre inicialmente.



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

1. Haga clic en los tres puntos junto a **Estado de protección** de la base de datos y, a continuación, haga clic en **Políticas** para ver las políticas de protección de base de datos precargadas predeterminadas que se pueden aplicar para proteger sus bases de datos Oracle.

The screenshot shows the NetApp BlueXP interface. At the top, there's a navigation bar with 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), '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' box indicates '0 Protected' and '1 Unprotected'. A table titled '1 Databases' lists the following:

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

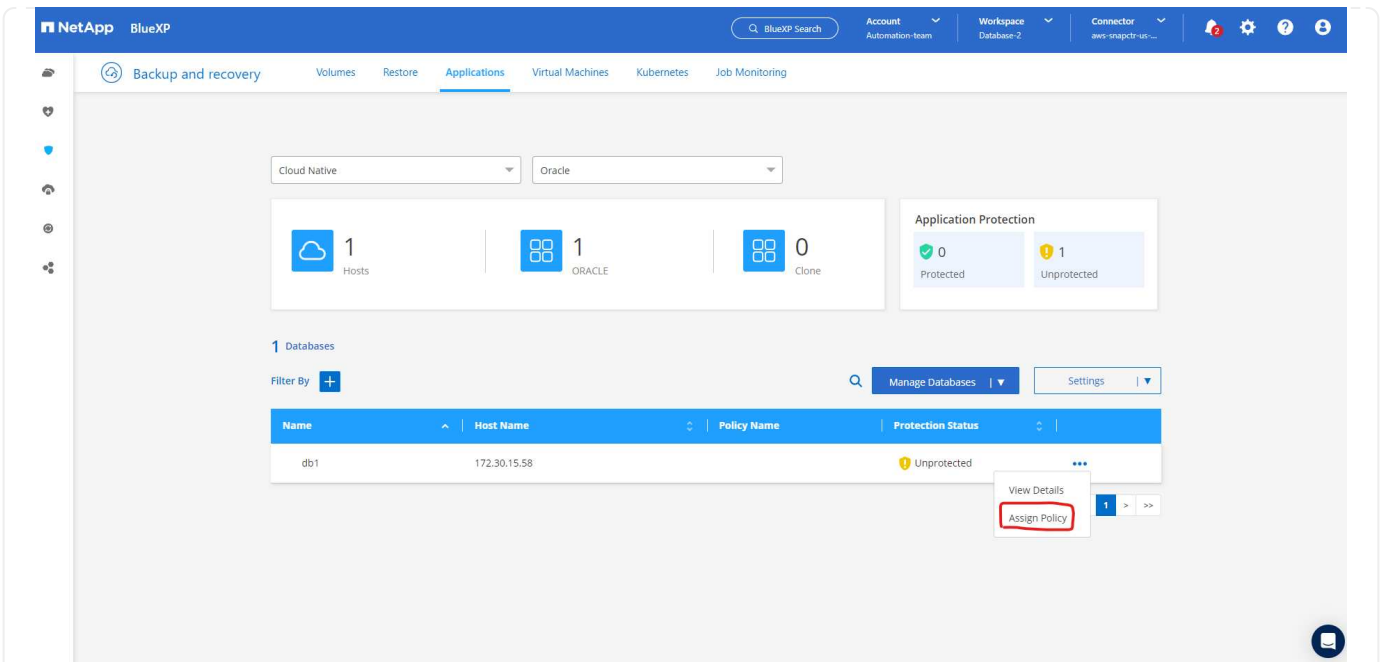
At the bottom right, there's a 'Settings' dropdown menu with options: Policies, About, and Hosts.

1. También puede crear su propia política con una frecuencia de copia de seguridad personalizada y una ventana de retención de datos de copia de seguridad.

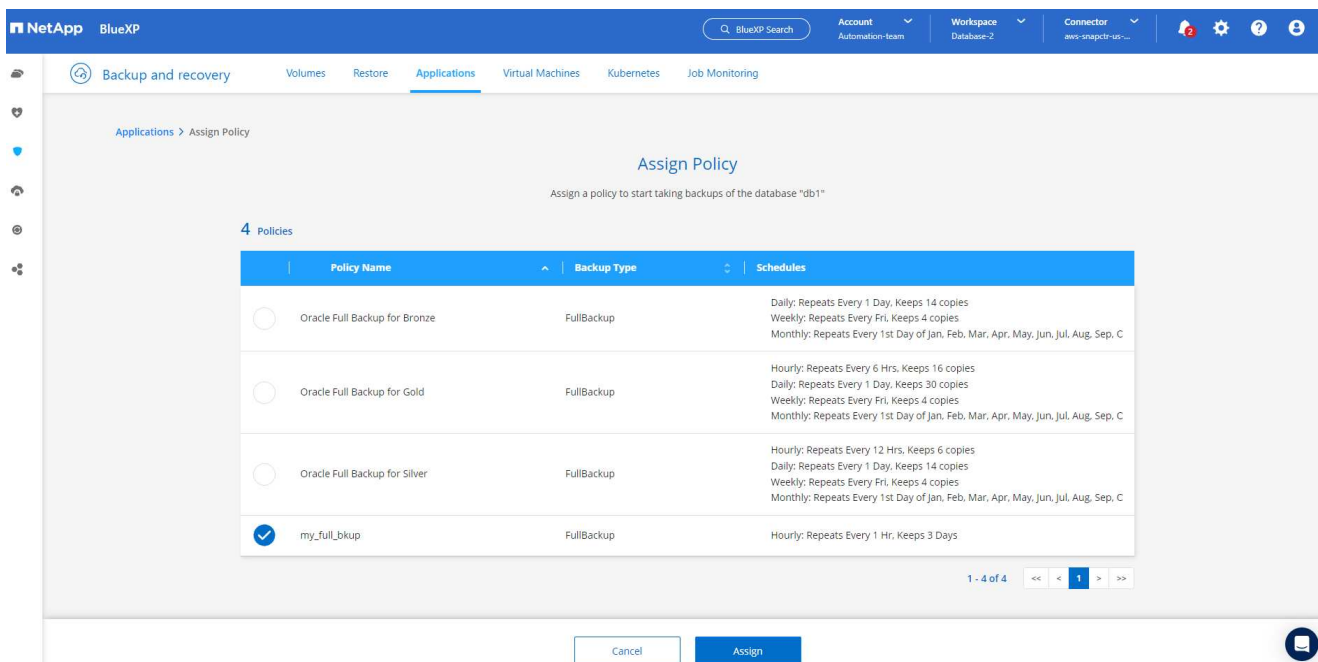
The screenshot shows the 'Applications > Policies' page in NetApp BlueXP. It features filters for 'Cloud Native' and 'Oracle'. A 'Create Policy' button is visible. A table lists the following policies:

Policy Name	Backup Type	Schedules and Retention
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, Oct, Nov
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, Oct, Nov
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, Oct, Nov
my_full_bkup	FullBackup	Hourly: Repeats Every 1 Hr, Keeps 3 Days

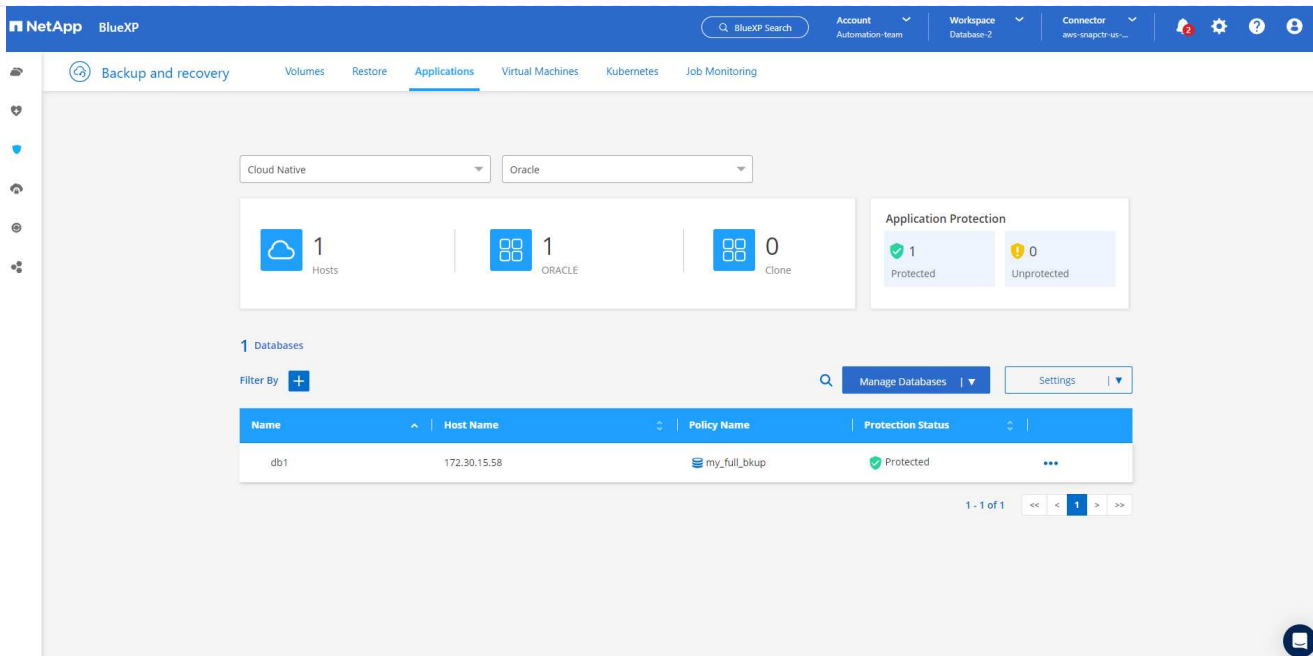
1. Cuando esté satisfecho con la configuración de la política, puede asignar la política que prefiera para proteger la base de datos.



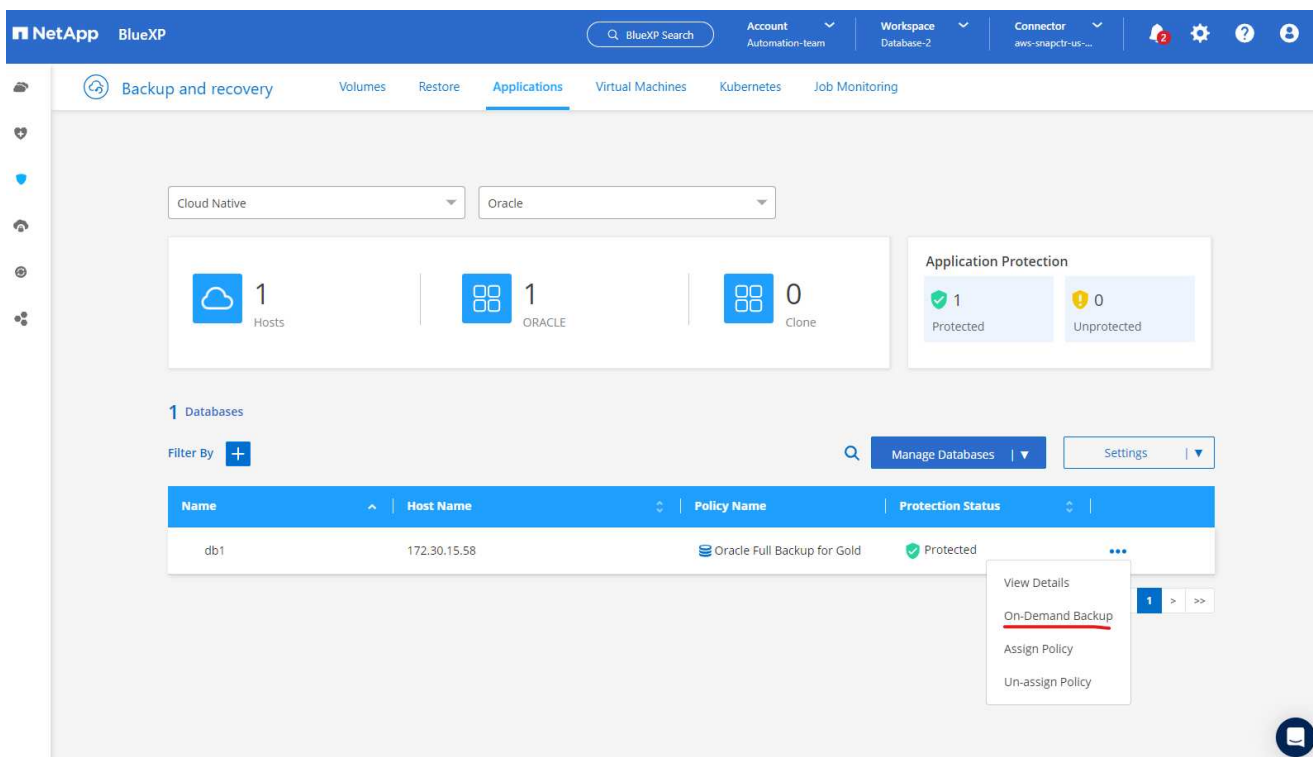
1. Seleccione la política que desea asignar a la base de datos.



1. Después de aplicar la política, el estado de protección de la base de datos cambia a **Protegido** con una marca de verificación verde.



1. La copia de seguridad de la base de datos se ejecuta según una programación predefinida. También puede ejecutar una copia de seguridad única a pedido como se muestra a continuación.



1. Los detalles de las copias de seguridad de la base de datos se pueden ver haciendo clic en **Ver detalles** en la lista del menú. Esto incluye el nombre de la copia de seguridad, el tipo de copia de seguridad, el SCN y la fecha de la copia de seguridad. Un conjunto de respaldo cubre una instantánea tanto del volumen de datos como del volumen de registro. Una instantánea del volumen de registro se realiza inmediatamente después de una instantánea del volumen de base de datos. Puede aplicar un filtro si está buscando una copia de seguridad particular en una lista larga.

NetAppBlueXP

Q BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapctr-us...

2

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

Restauración y recuperación de bases de datos de Oracle

1. Para restaurar una base de datos, elija la copia de seguridad correcta, ya sea por SCN o por hora de la copia de seguridad. Haga clic en los tres puntos de la copia de seguridad de los datos de la base de datos y, a continuación, haga clic en **Restaurar** para iniciar la restauración y recuperación de la base de datos.

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 'Applications' tab is selected, showing 'Database Details' for a database named 'db1'. Below this, there is a table of backups. The table has columns for 'Backup Name', 'Backup Type', 'SCN', 'Backup Date', and 'Actions'. The 'Actions' column for the backup 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_37_04_98851_1' is highlighted, showing a 'Restore' button.

Backup Name	Backup Type	SCN	Backup Date	Actions
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 Delete Clone
Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_36_33_27205_0	Data	2580524	Mar 24, 2023, 11:37:0	

1. Seleccione su configuración de restauración. Si está seguro de que nada ha cambiado en la estructura física de la base de datos después de la copia de seguridad (como la adición de un archivo de datos o un grupo de discos), puede utilizar la opción **Forzar restauración en el lugar**, que generalmente es más rápida. De lo contrario, no marque esta casilla.

The screenshot shows the NetApp BlueXP interface with the 'Restore "db1"' window open. The 'Restore Settings' tab is selected. The 'Restore Scope' section has 'All Data Files' selected. The 'Force in place restore' checkbox is checked. The 'Recovery Scope' section has 'All Logs' selected. The 'Archive Log Files Locations' field is set to '/mnt/log_location001'. The 'Open the database or the container database in READ-WRITE mode after recovery' checkbox is checked. The 'Previous' and 'Next' buttons are at the bottom.

Restore Scope

- ☒ All Data Files
Data Files Restore
- ☐ Control Files
Control Files Restore
- ☒ Force in place restore
In place restore will skip the foreign files(files which are not part of the database) validation check. The Oracle database and the ASM disk group will be restored to the point when the backup was created.
- ☐ Database state will be changed if needed for restore and recovery.

Recovery Scope

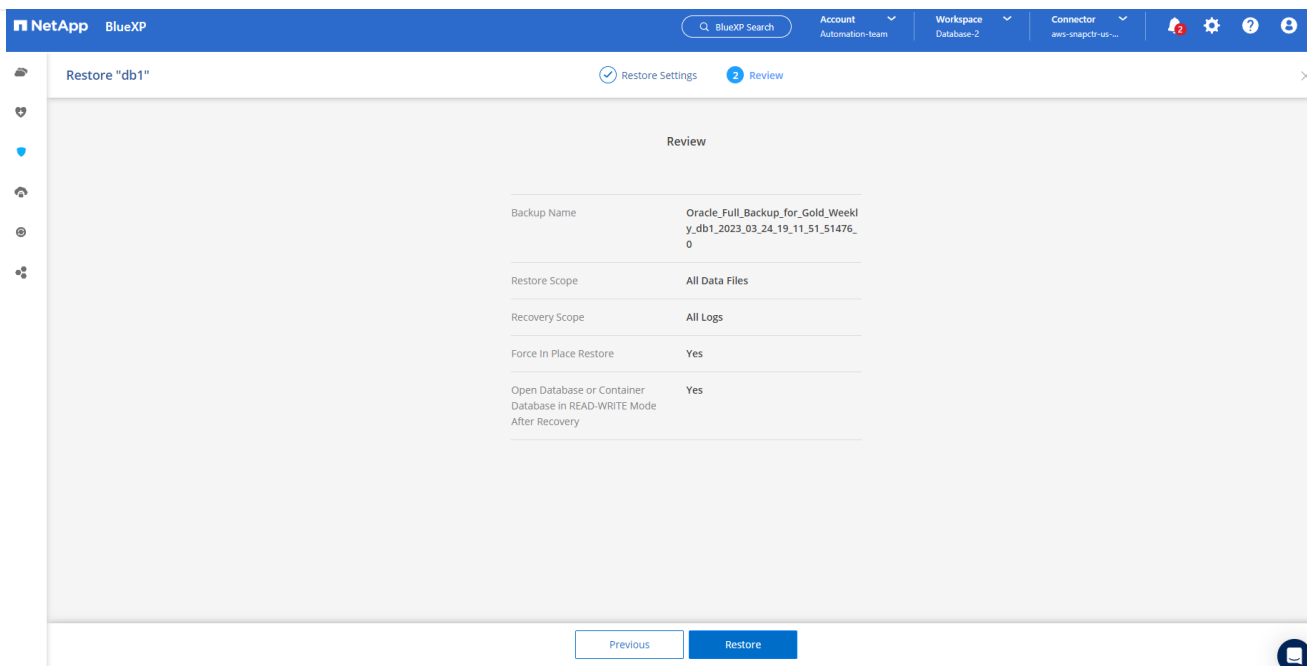
- ☒ All Logs
- ☐ Until System Change Number
- ☐ Date and Time
- ☐ No Recovery

Archive Log Files Locations: /mnt/log_location001

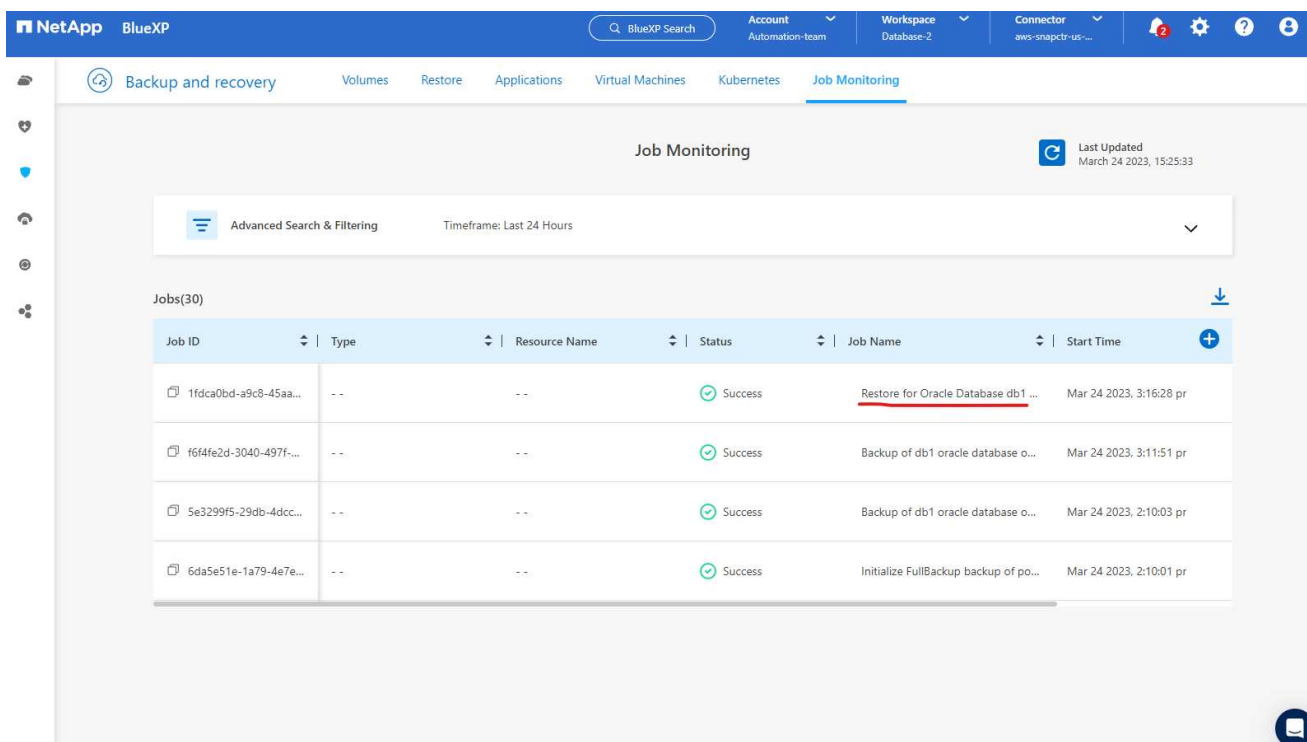
☒ Open the database or the container database in READ-WRITE mode after recovery.

Previous Next

1. Revisar e iniciar la restauración y recuperación de la base de datos.



1. Desde la pestaña **Monitoreo de trabajos**, puede ver el estado del trabajo de restauración, así como cualquier detalle mientras se ejecuta.



NetAppBlueXP

Q BlueXP Search

AccountAutomation team

WorkspaceDatabase-2

Connectoraws-snapctr-us-...

2

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

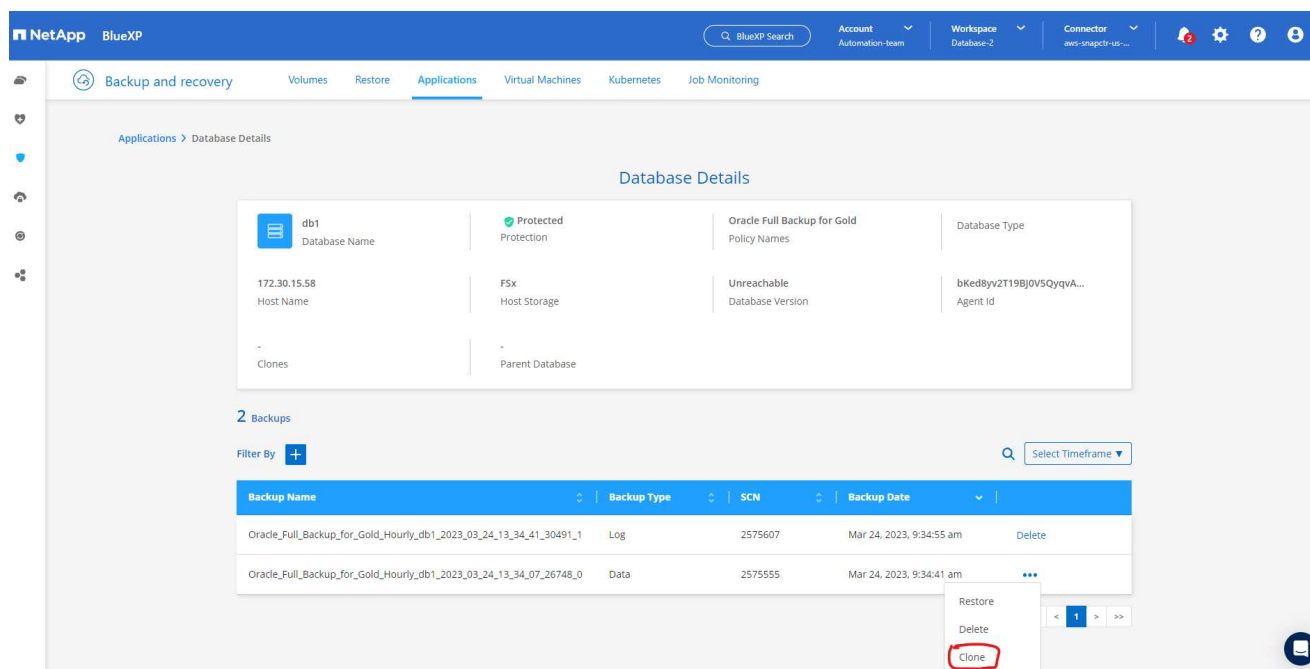
Sub-Jobs(6)

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	fb7b1171-9f6f-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

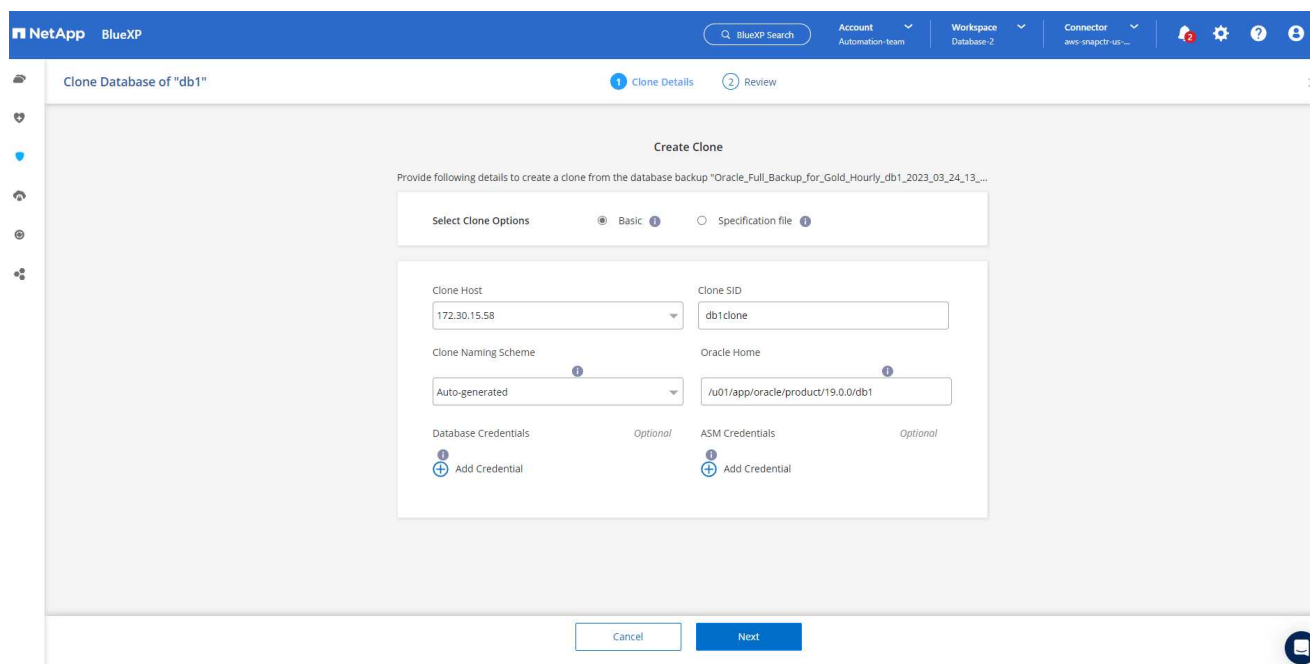
Clon de base de datos de Oracle

Para clonar una base de datos, inicie el flujo de trabajo de clonación desde la misma página de detalles de copia de seguridad de la base de datos.

1. Seleccione la copia de seguridad de la base de datos correcta, haga clic en los tres puntos para ver el menú y elija la opción **Clonar**.



1. Seleccione la opción **Básico** si no necesita cambiar ningún parámetro de la base de datos clonada.



1. Como alternativa, seleccione **Archivo de especificación**, que le brinda la opción de descargar el archivo de inicio actual, realizar cambios y luego volver a cargarlo en el trabajo.

NetApp BlueXP

Q BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...



Clone Database of "db1"

1 Clone Details

2 Review

Create Clone

Provide following details to create a clone from the database backup "Oracle_Full_Backup_for_Gold_Weekly_db1_2023_03_24_19..."

Select Clone Options

☐ Basic ¹

☒ Specification file ¹

¹ Generate specification file to modify input parameters and use for clone.

Download File

Specification File

db1_3_24_2023_10_14_spec.json

Browse

Clone Host

172.30.15.58

Clone SID

db1clone

Database Credentials

Optional

Add Credential

ASM Credentials

Optional

Add Credential

Cancel

Next



1. Revisar y lanzar el trabajo.

NetApp BlueXP

Q BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...



Clone Database of "db1"

1 Clone Details

2 Review

Review

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

Previous

Clone



1. Supervise el estado del trabajo de clonación desde la pestaña **Supervisión del trabajo**.

NetAppBlueXP

BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapc1r18-...

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Job Monitoring > Job Id: cd30abaf-fbe2-4052-a6db-4bf965a8d29b

Job Details

Job Id: cd30abaf-fbe2-4052-a6db-4bf965a8d29b

Expand All

Sub-Jobs(2)

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	51f152c1-853a-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. Validar la base de datos clonada en el host de la instancia EC2.

34

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

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)

- 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=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

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.