



TR-4964: Backup, restauração e clonagem do banco de dados Oracle com SnapCenter Services - AWS

NetApp database solutions

NetApp
August 18, 2025

Índice

TR-4964: Backup, restauração e clonagem do banco de dados Oracle com SnapCenter Services - AWS	1
Propósito	1
Público	1
Ambiente de teste e validação de soluções	1
Arquitetura	2
Componentes de hardware e software	2
Fatores-chave para consideração de implantação	3
Implantação da solução	3
Pré-requisitos para implantação do serviço SnapCenter	3
Preparação para integração ao BlueXP	4
Implantar um conector para serviços SnapCenter	5
Definir uma credencial no BlueXP para acesso aos recursos da AWS	12
Configuração dos serviços do SnapCenter	16
Backup de banco de dados Oracle	24
Restauração e recuperação de banco de dados Oracle	28
Clone de banco de dados Oracle	31
Informações adicionais	36

TR-4964: Backup, restauração e clonagem do banco de dados Oracle com SnapCenter Services - AWS

Esta solução fornece uma visão geral e detalhes para backup, restauração e clonagem de banco de dados Oracle usando o NetApp SnapCenter SaaS usando o console BlueXP na nuvem do Azure.

Allen Cao, Niyaz Mohamed, NetApp

Propósito

O SnapCenter Services é a versão SaaS da ferramenta clássica de interface de usuário de gerenciamento de banco de dados SnapCenter, disponível no console de gerenciamento de nuvem NetApp BlueXP. É parte integrante da oferta de backup em nuvem e proteção de dados da NetApp para bancos de dados como Oracle e HANA executados no armazenamento em nuvem da NetApp. Este serviço baseado em SaaS simplifica a implantação tradicional do servidor autônomo SnapCenter, que geralmente requer um servidor Windows operando em um ambiente de domínio Windows.

Nesta documentação, demonstramos como você pode configurar o SnapCenter Services para fazer backup, restaurar e clonar bancos de dados Oracle implantados no armazenamento Amazon FSx ONTAP e em instâncias de computação EC2. Embora seja muito mais fácil de configurar e usar, o SnapCenter Services oferece funcionalidades essenciais que estão disponíveis na ferramenta de interface do usuário SnapCenter legada.

Esta solução aborda os seguintes casos de uso:

- Backup de banco de dados com snapshots para bancos de dados Oracle hospedados no Amazon FSx ONTAP
- Recuperação de banco de dados Oracle em caso de falha
- Clonagem rápida e eficiente em termos de armazenamento de bancos de dados primários para um ambiente de desenvolvimento/teste ou outros casos de uso

Público

Esta solução é destinada aos seguintes públicos:

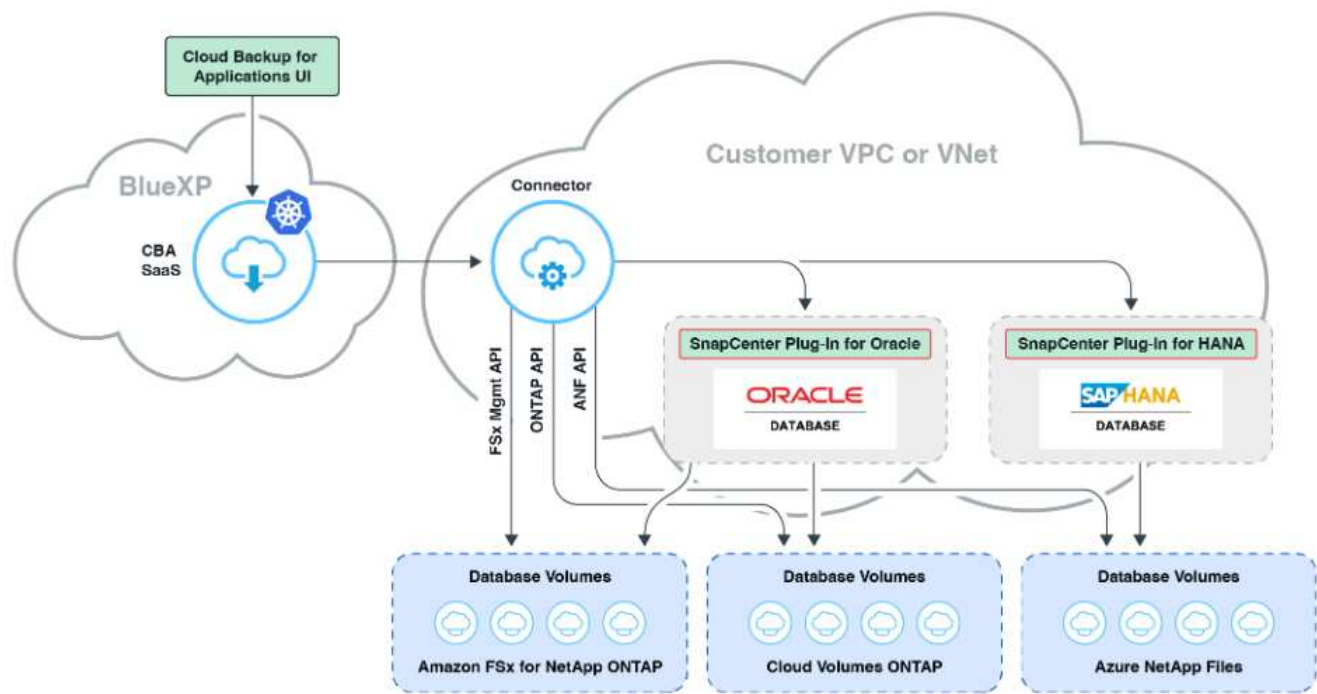
- O DBA que gerencia bancos de dados Oracle em execução no armazenamento Amazon FSx ONTAP
- O arquiteto de soluções interessado em testar backup, restauração e clonagem de banco de dados Oracle na nuvem pública AWS
- O administrador de armazenamento que oferece suporte e gerencia o armazenamento Amazon FSx ONTAP
- O proprietário do aplicativo que possui aplicativos implantados no armazenamento Amazon FSx ONTAP

Ambiente de teste e validação de soluções

O teste e a validação desta solução foram realizados em um ambiente AWS FSx e EC2 que pode não

corresponder ao ambiente de implantação final. Para mais informações, consulte a seção [Fatores-chave para consideração de implantação](#) .

Arquitetura



Esta imagem fornece uma visão detalhada do BlueXP backup and recovery para aplicativos no console do BlueXP , incluindo a interface do usuário, o conector e os recursos que ele gerencia.

Componentes de hardware e software

Hardware

Armazenamento FSx ONTAP	Versão atual oferecida pela AWS	Um cluster FSx HA na mesma VPC e zona de disponibilidade
Instância EC2 para computação	t2.xlarge/4vCPU/16G	Duas instâncias EC2 T2 xlarge EC2, uma como servidor de banco de dados primário e a outra como servidor de banco de dados clone

Software

RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hora2-GP2	Assinatura RedHat implantada para teste
Infraestrutura de grade Oracle	Versão 19.18	Patch RU aplicado p34762026_190000_Linux-x86-64.zip

Banco de Dados Oracle	Versão 19.18	Patch RU aplicado p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Versão 12.2.0.1.36	Último patch p6880880_190000_Linux-x86-64.zip
Serviço SnapCenter	Versão	v2.3.1.2324

Fatores-chave para consideração de implantação

- **Conector a ser implantado na mesma VPC que o banco de dados e o FSx.** Sempre que possível, o conector deve ser implantado na mesma VPC da AWS, o que permite a conectividade com o armazenamento FSx e a instância de computação do EC2.
- **Uma política do AWS IAM criada para o conector SnapCenter.** A política no formato JSON está disponível na documentação detalhada do serviço SnapCenter. Ao iniciar a implantação do conector com o console BlueXP, você também será solicitado a configurar os pré-requisitos com detalhes da permissão necessária no formato JSON. A política deve ser atribuída à conta de usuário da AWS que possui o conector.
- **A chave de acesso da conta AWS e o par de chaves SSH criados na conta AWS.** O par de chaves SSH é atribuído ao usuário ec2 para efetuar login no host do conector e, em seguida, implantar um plug-in de banco de dados no host do servidor de banco de dados EC2. A chave de acesso concede permissão para provisionar o conector necessário com a política do IAM acima.
- **Uma credencial adicionada à configuração do console BlueXP.** Para adicionar o Amazon FSx ONTAP ao ambiente de trabalho do BlueXP, uma credencial que concede permissões ao BlueXP para acessar o Amazon FSx ONTAP é configurada na configuração do console do BlueXP.
- **java-11-openjdk instalado no host da instância do banco de dados EC2.** A instalação do serviço SnapCenter requer o Java versão 11. Ele precisa ser instalado no host do aplicativo antes da tentativa de implantação do plugin.

Implantação da solução

Há uma ampla documentação da NetApp com um escopo mais amplo para ajudar você a proteger os dados do seu aplicativo nativo na nuvem. O objetivo desta documentação é fornecer procedimentos passo a passo que abrangem a implantação do SnapCenter Service com o console BlueXP para proteger seu banco de dados Oracle implantado no Amazon FSx ONTAP e uma instância de computação EC2. Este documento preenche certos detalhes que podem estar faltando em instruções mais gerais.

Para começar, siga estas etapas:

- Leia as instruções gerais "[Proteja os dados dos seus aplicativos nativos da nuvem](#)" e as seções relacionadas ao Oracle e Amazon FSx ONTAP.
- Assista ao vídeo passo a passo a seguir.

Implantação de solução

Pré-requisitos para implantação do serviço SnapCenter

A implantação requer os seguintes pré-requisitos.

1. Um servidor de banco de dados Oracle primário em uma instância EC2 com um banco de dados Oracle totalmente implantado e em execução.
2. Um cluster Amazon FSx ONTAP implantado na AWS que hospeda os volumes de banco de dados acima.
3. Um servidor de banco de dados opcional em uma instância EC2 que pode ser usado para testar a clonagem de um banco de dados Oracle em um host alternativo com a finalidade de dar suporte a uma carga de trabalho de desenvolvimento/teste ou qualquer caso de uso que exija um conjunto de dados completo de um banco de dados Oracle de produção.
4. Se precisar de ajuda para atender aos pré-requisitos acima para implantação do banco de dados Oracle no Amazon FSx ONTAP e na instância de computação EC2, consulte ["Implantação e proteção de banco de dados Oracle no AWS FSx/EC2 com iSCSI/ASM"](#) ou papel branco ["Melhores práticas de implantação do Oracle Database no EC2 e FSx"](#)

Preparação para integração ao BlueXP

1. Use o link ["NetApp BlueXP"](#) para se inscrever no acesso ao console BlueXP .
2. Faça login na sua conta da AWS para criar uma política do IAM com as permissões adequadas e atribuir a política à conta da AWS que será usada para a implantação do conector BlueXP .

The screenshot shows the AWS IAM console interface. On the left is the 'Identity and Access Management (IAM)' sidebar with navigation links like Dashboard, Access management, Policies, and Access reports. The main content area shows the 'Summary' page for a policy named 'snapcenter'. It displays the Policy ARN, description, and tabs for Permissions, Policy usage, Tags, Policy versions, and Access Advisor. The 'Permissions' tab is selected, showing a JSON policy document with the following structure:

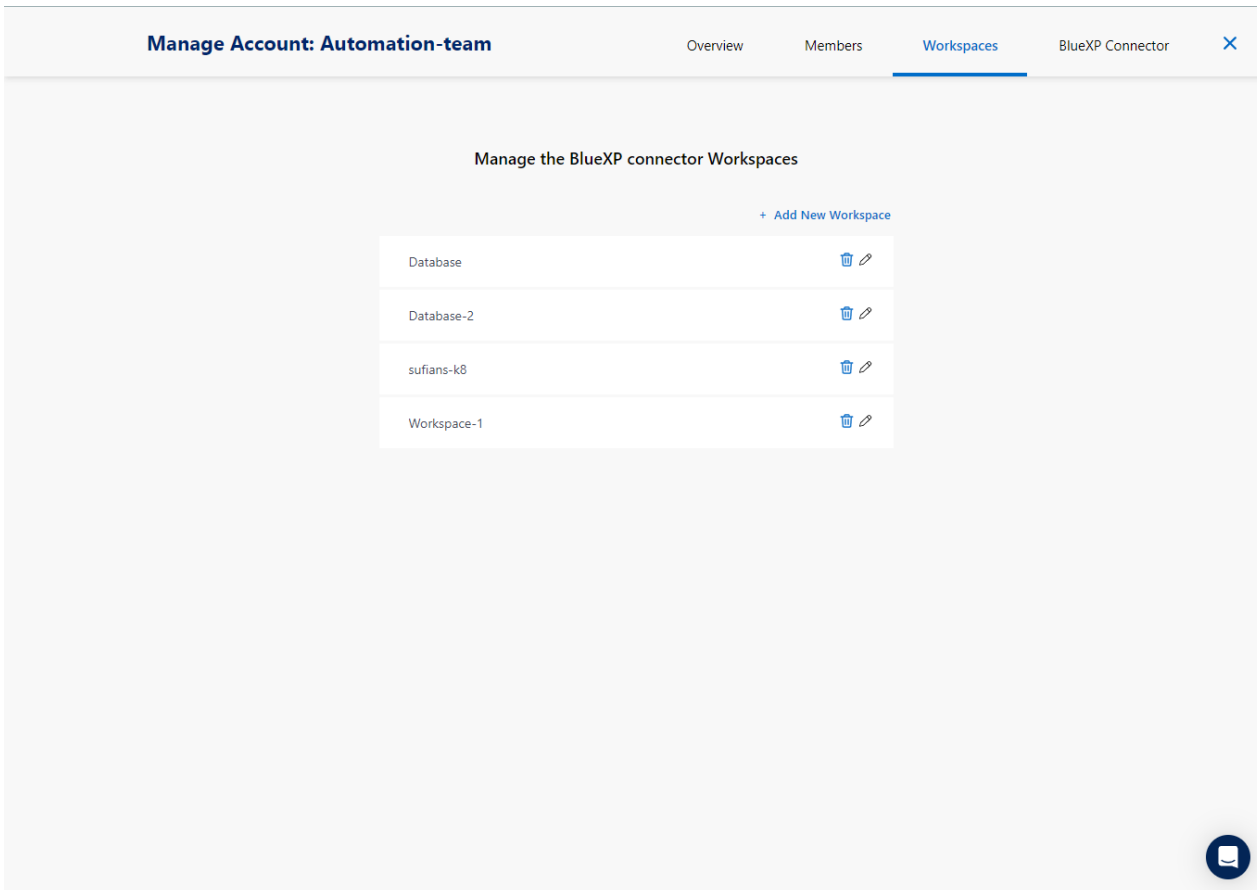
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:CreateRole",
8         "iam:DeleteRole",
9         "iam:PutRolePolicy",
10        "iam:CreateInstanceProfile",
11        "iam:DeleteRolePolicy",
12        "iam:AddRoleToInstanceProfile",
13        "iam:RemoveRoleFromInstanceProfile",
14        "iam:DeleteInstanceProfile",
15        "iam:PassRole",
16        "iam:ListRoles",
17        "ec2:DescribeInstanceStatus",
18        "ec2:RunInstances",
19        "ec2:ModifyInstanceAttribute",
20        "ec2:CreateSecurityGroup",
21        "ec2:DeleteSecurityGroup",
22        "ec2:DescribeSecurityGroups",
23        "ec2:RevokeSecurityGroupEgress",
24        "ec2:AuthorizeSecurityGroupEgress",
25        "ec2:AuthorizeSecurityGroupIngress",
26        "ec2:RevokeSecurityGroupIngress",
27        "ec2:CreateNetworkInterface",
28        "ec2:DescribeNetworkInterfaces"
```

A política deve ser configurada com uma string JSON disponível na documentação da NetApp . A sequência JSON também pode ser recuperada da página quando o provisionamento do conector é iniciado e você é solicitado a fornecer as permissões de pré-requisitos.

3. Você também precisa do AWS VPC, sub-rede, grupo de segurança, uma chave de acesso e segredos da conta de usuário da AWS, uma chave SSH para o usuário ec2 e assim por diante, prontos para o provisionamento do conector.

Implantar um conector para serviços SnapCenter

1. Efetue login no console do BlueXP . Para uma conta compartilhada, é uma prática recomendada criar um espaço de trabalho individual clicando em **Conta > Gerenciar conta > Espaço de trabalho** para adicionar um novo espaço de trabalho.



2. Clique em **Adicionar um conector** para iniciar o fluxo de trabalho de provisionamento do conector.

NetApp Cloud Manager

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

Backup & Restore
Volumes
Restore
Applications
Virtual Machines
Kubernetes
Job Monitoring

Backup & Restore

Fully integrated data protection for ONTAP anywhere

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

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

Add a Connector

Simple & intuitive

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

Hybrid Multicloud

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

Unmatched Efficiency

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

1. Escolha seu provedor de nuvem (neste 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. Ignore as etapas de **Permissão**, **Autenticação** e **Rede** se você já as tiver configurado na sua conta da AWS. Caso contrário, você deve configurá-los antes de prosseguir. A partir daqui, você também pode recuperar as permissões para a política da AWS referenciada na seção anterior "[Preparação](#)"

para integração ao 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. Insira a autenticação da sua conta AWS com **Chave de acesso** e **Chave 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? [v](#)[Previous](#)[Next](#)

2. Nomeie a instância do conector e selecione **Criar função** em **Detalhes**.

[✓ AWS Credentials](#)[2 Details](#)[3 Network](#)[4 Security Group](#)[5 Review](#)

Details

Connector Instance Name

SnapCenterSvs

i

Connector Role

i



Create Role



Select an existing Role

Role Name

Cloud-Manager-Operator-VZzSSP9-SnapCenter



Add Tags to Connector Instance



AWS Managed Encryption

i

Master Key: aws/ebs (default)

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

1. Configure a rede com o **VPC**, **Sub-rede** e **Par de Chaves** SSH adequados para acesso ao conector.

Add BlueXP Connector - AWSMore Information ×

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

Network

Connectivity
VPC
vpc-0b522d5e982a50ceb - 172.30.15.0/25
Subnet
172.30.15.0/25 | priv-subnet-01
Key Pair
sufi_new
Public IP
Use subnet settings (Disable)
Notice: Ensure that the subnet has internet connectivity through a NAT device or proxy server so that the Connector can communicate with AWS services.

Proxy Configuration (Optional)
HTTP Proxy
Example: http://172.16.254.1:8080
Define Credentials for this Proxy
Upload a root certificate

Previous Next

2. Defina o **Grupo de Segurança** para o conector.

 AWS Credentials  Details  Network ** Security Group**  Review

Security Group

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

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

1 Security Group



Security Group Name	Description
☒ default	default VPC security group

[Previous](#)

[Next](#)



3. Revise a página de resumo e clique em **Adicionar** para iniciar a criação do conector. Geralmente, leva cerca de 10 minutos para concluir a implantação. Após a conclusão, a instância do conector aparece no painel do AWS EC2.

Add BlueXP Connector - AWS

More Information

X

✓ AWS Credentials

✓ Details

✓ Network

✓ Security Group

5 Review

Review

[Code for Terraform Automation](#)

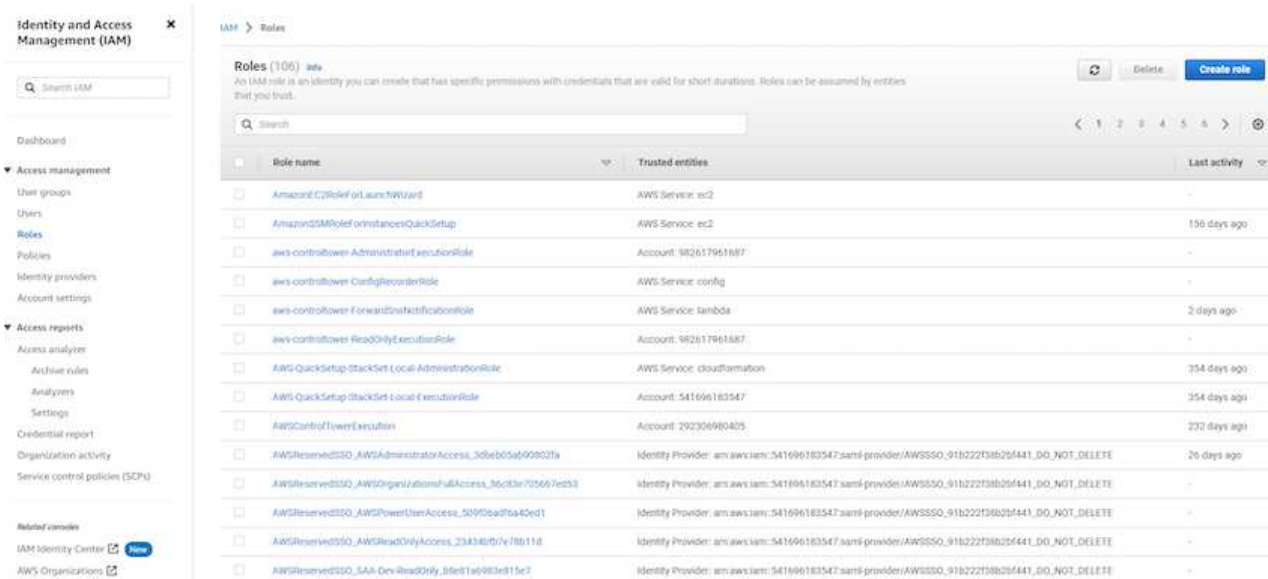
BlueXP Connector Name	aws-snapctr-us-east
AWS Access Key	AKIAH4H43ZT56IWWR3TI
Region	us-east-1
VPC	vpc-0b522d5e982a50ceb - 172.30.15.0/25
Subnet	172.30.15.0/25 priv-subnet-01
Key Pair	sufi_new
Public IP	Use subnet settings (Disable)
Proxy	None
Security Group	default

Previous

Add

Definir uma credencial no BlueXP para acesso aos recursos da AWS

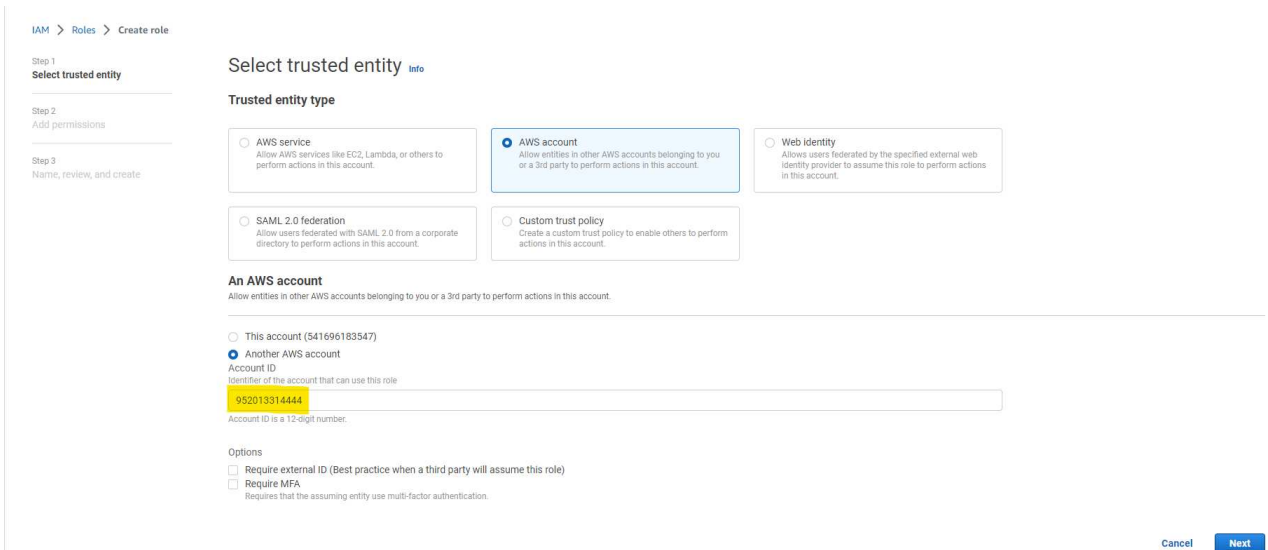
1. Primeiro, no console do AWS EC2, crie uma função no menu **Gerenciamento de Identidade e Acesso (IAM) Funções, Criar função** para iniciar o fluxo de trabalho de criação de função.



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
AmazonEC2RoleforLambda	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_30be605a999021fa	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	26 days ago
AWSReservedSSO_AWSOrganizationalAccess_Mock3e725667e253	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_AWSPowerUserAccess_509f0a0f640ed1	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_AWSReadOnlyAccess_234340fb7c7fb11d	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_SAA-Dev-ReadOnly_Ib6f1a9983e115c7	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-

2. Na página **Selecionar entidade confiável**, escolha **Conta AWS**, **Outra conta AWS** e cole o ID da conta BlueXP , que pode ser recuperado no console BlueXP .



The screenshot shows the 'Create role' page in the AWS IAM console, Step 1: Select trusted entity. The 'Trusted entity type' section shows 'AWS account' selected. The 'An AWS account' section shows 'Another AWS account' selected, with the account ID '992013314444' entered in the text field.

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. Filtre as políticas de permissão por fsx e adicione **Políticas de permissões** à função.

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. Na página **Detalhes da função**, nomeie a função, adicione uma descrição e clique em **Criar função**.

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. De volta ao console BlueXP, clique no ícone de configuração no canto superior direito do console para abrir a página **Credenciais da conta**, clique em **Adicionar credenciais** para iniciar o fluxo de trabalho de configuração de credenciais.

NetApp BlueXP

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

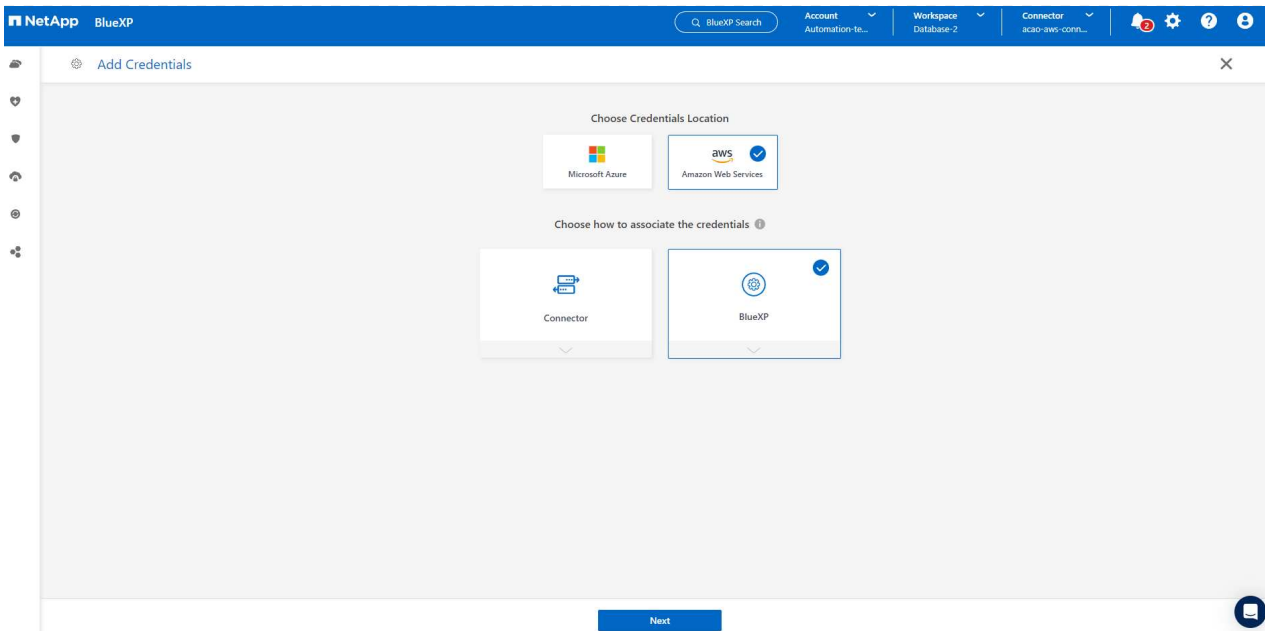
Credentials Account credentials User credentials

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

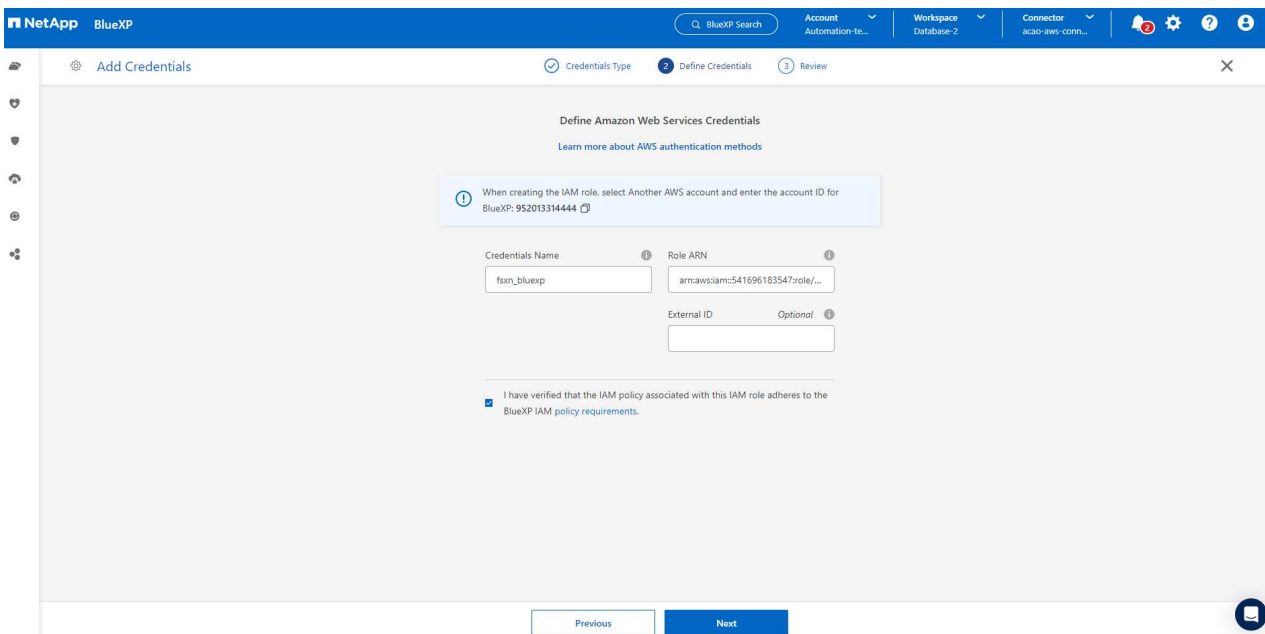
5 Credentials Add credentials

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

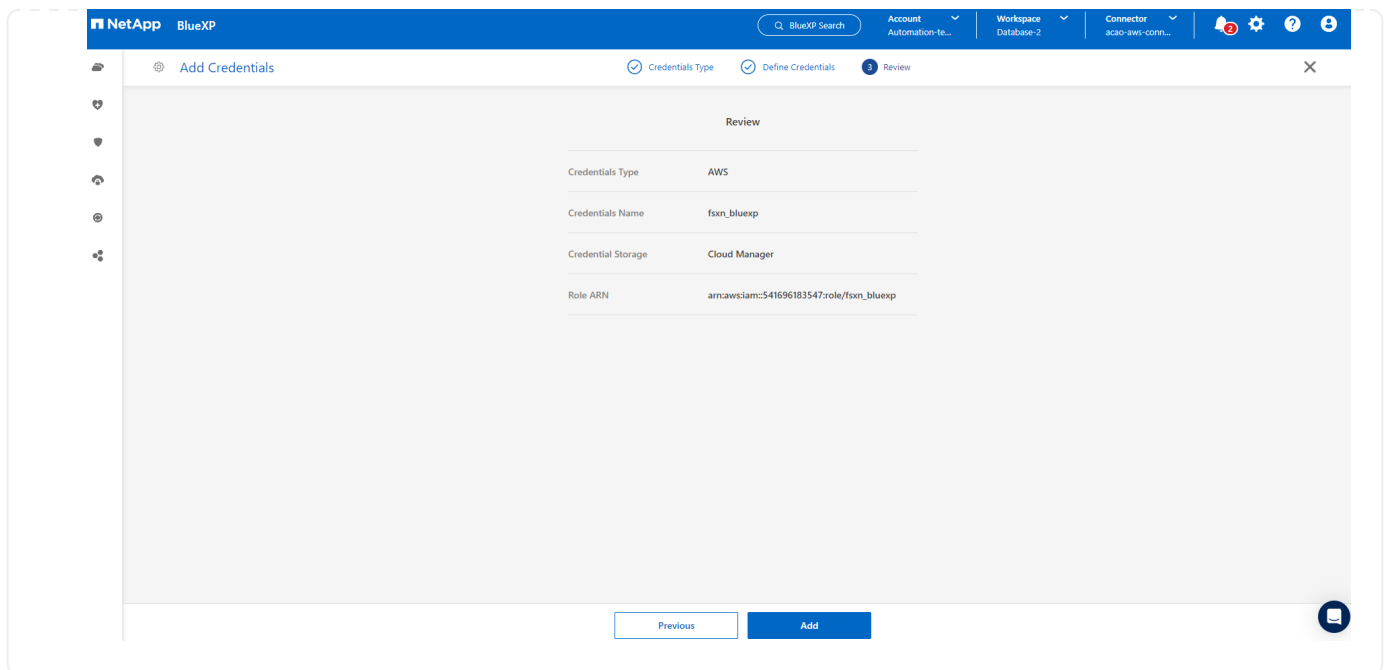
6. Escolha o local da credencial como - **Amazon Web Services - BlueXP**.



- Defina as credenciais da AWS com o **Role ARN** adequado, que pode ser recuperado da função do AWS IAM criada na etapa 1 acima. BlueXP **ID da conta**, que é usado para criar a função do AWS IAM na etapa um.



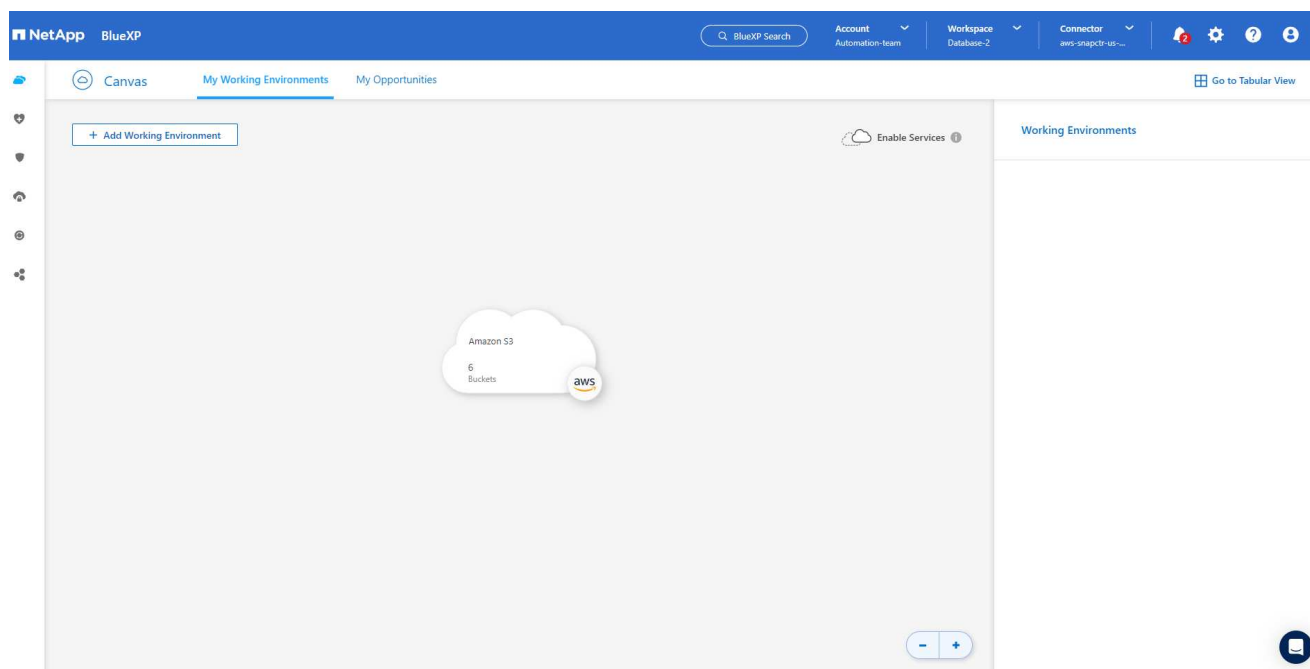
- Revisar e Adicionar



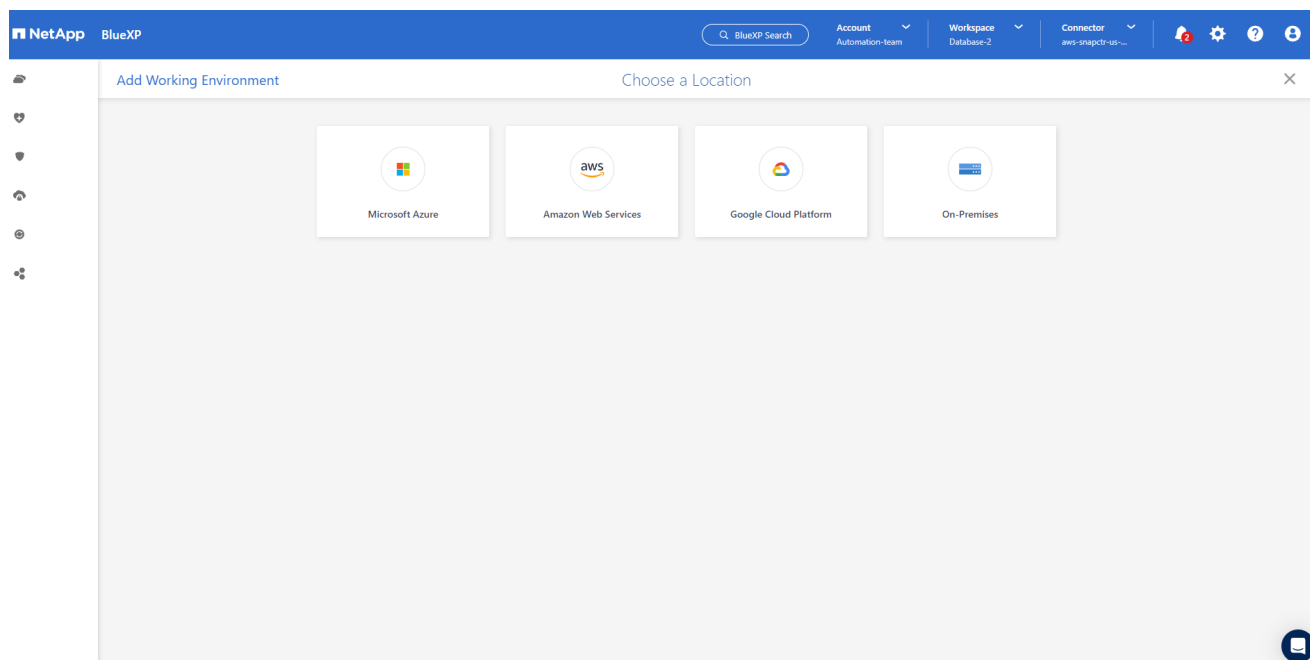
Configuração dos serviços do SnapCenter

Com o conector implantado e a credencial adicionada, os serviços do SnapCenter agora podem ser configurados com o seguinte procedimento:

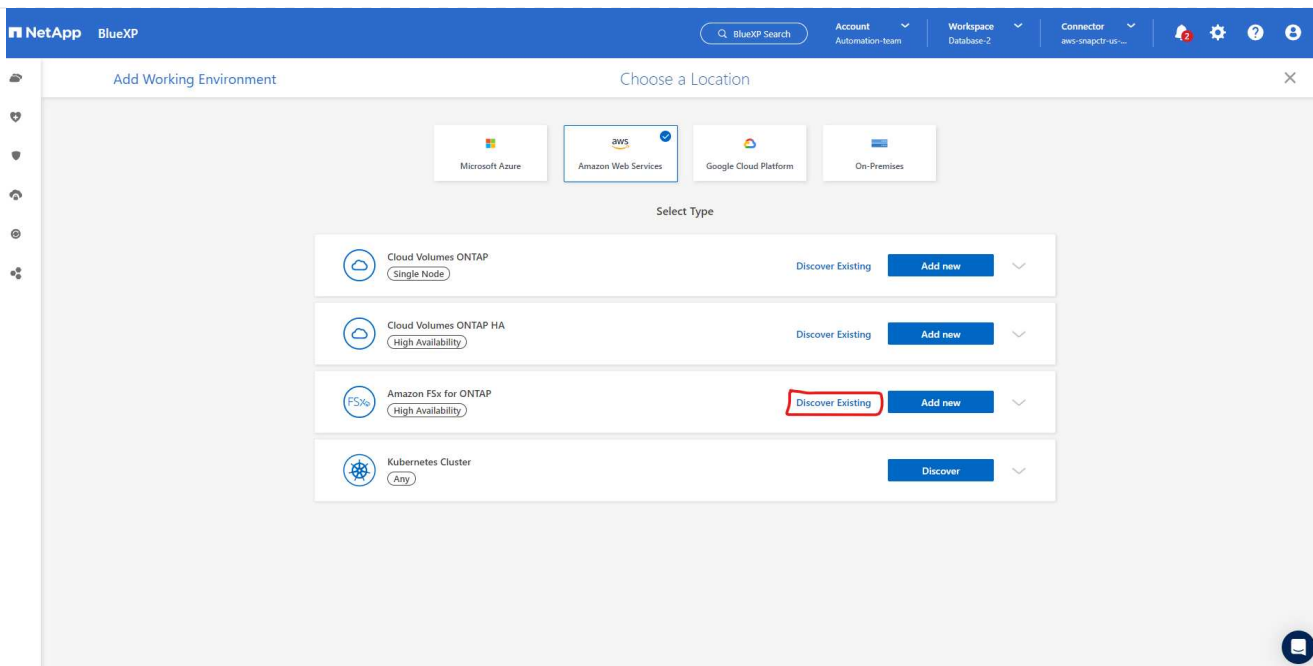
1. Em **Meu ambiente de trabalho**, clique em **Adicionar ambiente de trabalho** para descobrir o FSx implantado na AWS.



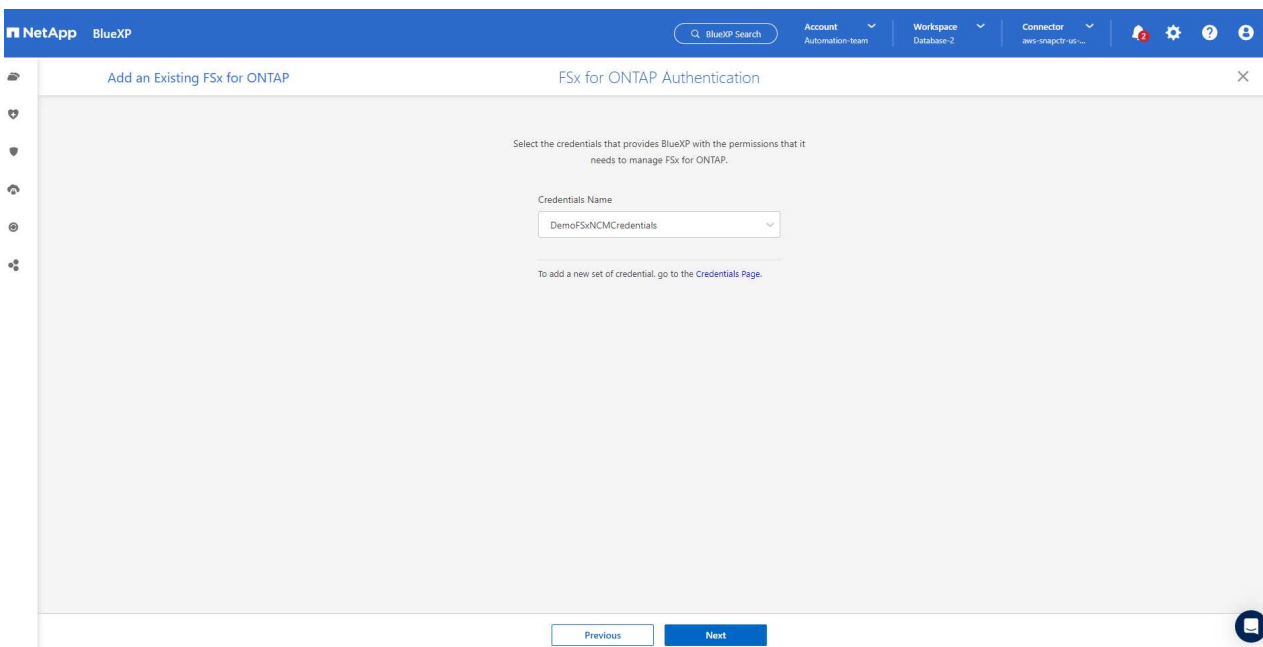
1. Escolha **Amazon Web Services** como local.



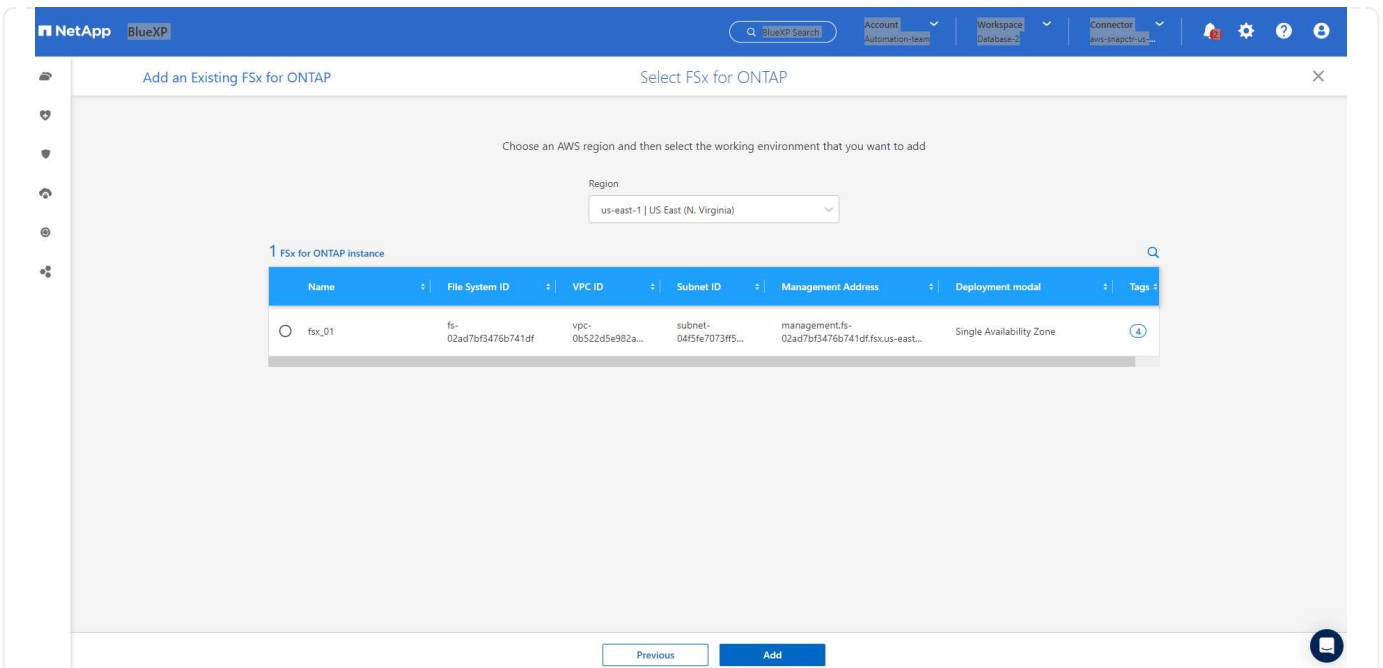
1. Clique em **Descobrir existente** ao lado de * Amazon FSx ONTAP*.



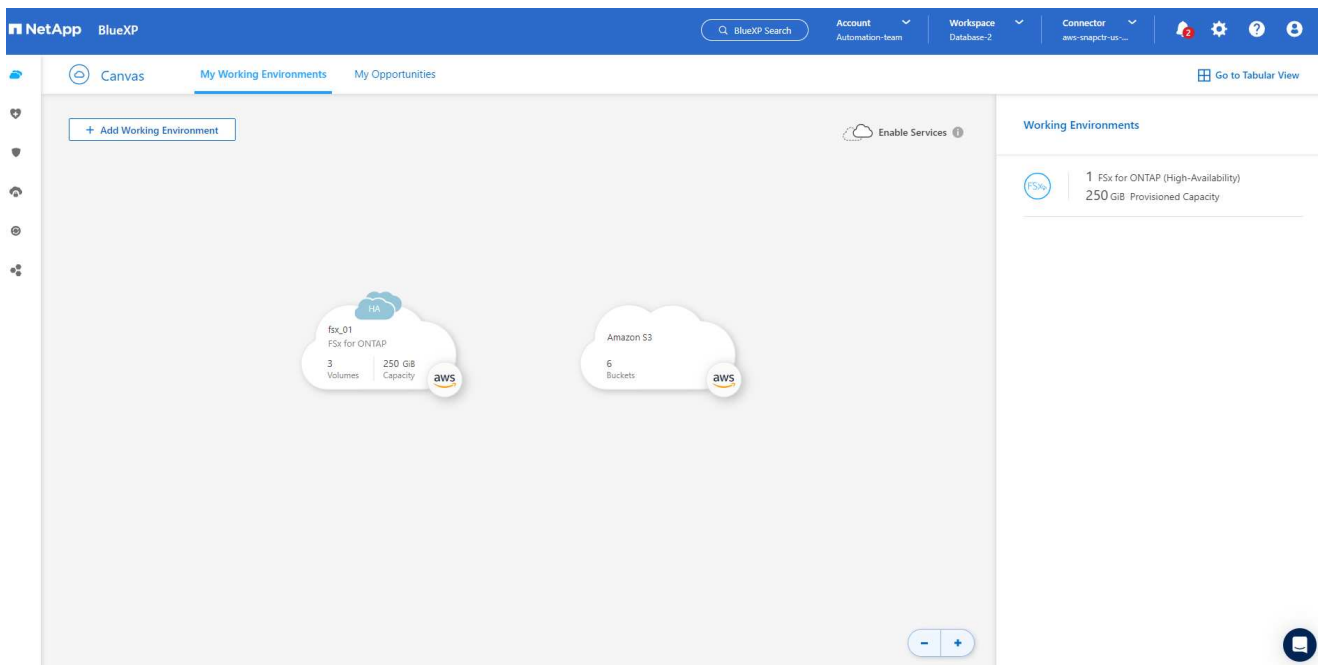
1. Selecione o **Nome das credenciais** que você criou na seção anterior para conceder ao BlueXP as permissões necessárias para gerenciar o FSx ONTAP. Se você não adicionou credenciais, você pode adicioná-las no menu **Configurações** no canto superior direito do console BlueXP .



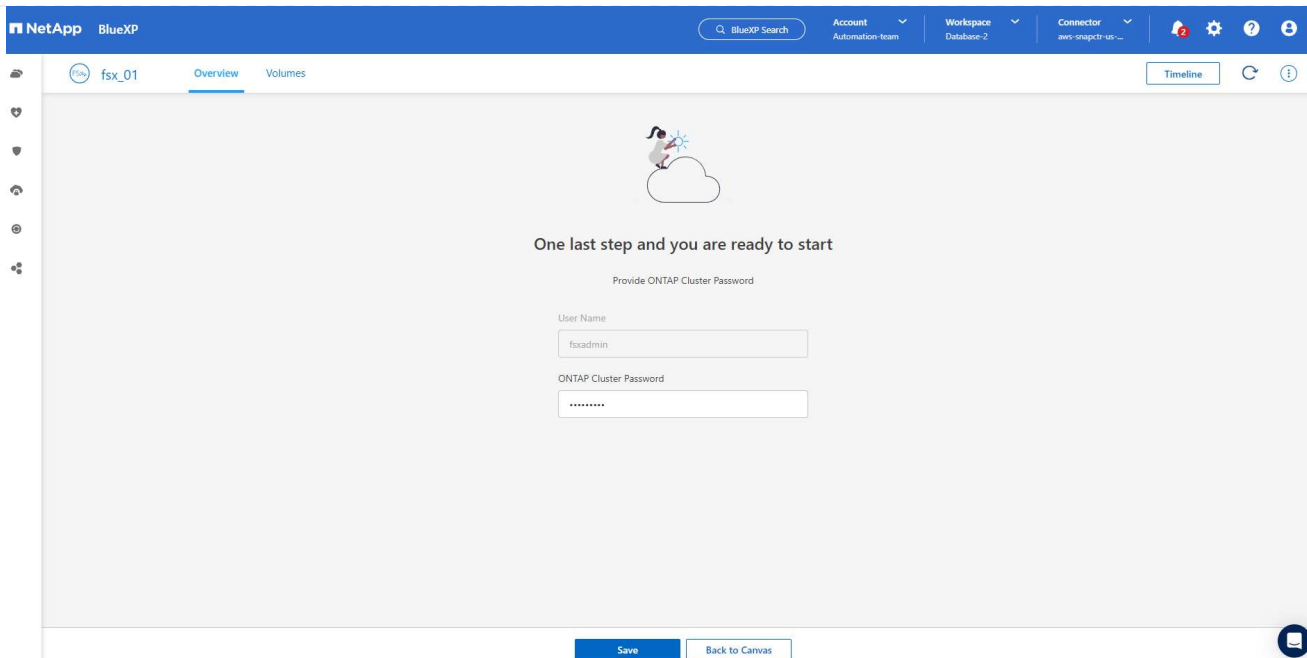
2. Escolha a região da AWS onde o Amazon FSx ONTAP está implantado, selecione o cluster FSx que hospeda o banco de dados Oracle e clique em Adicionar.



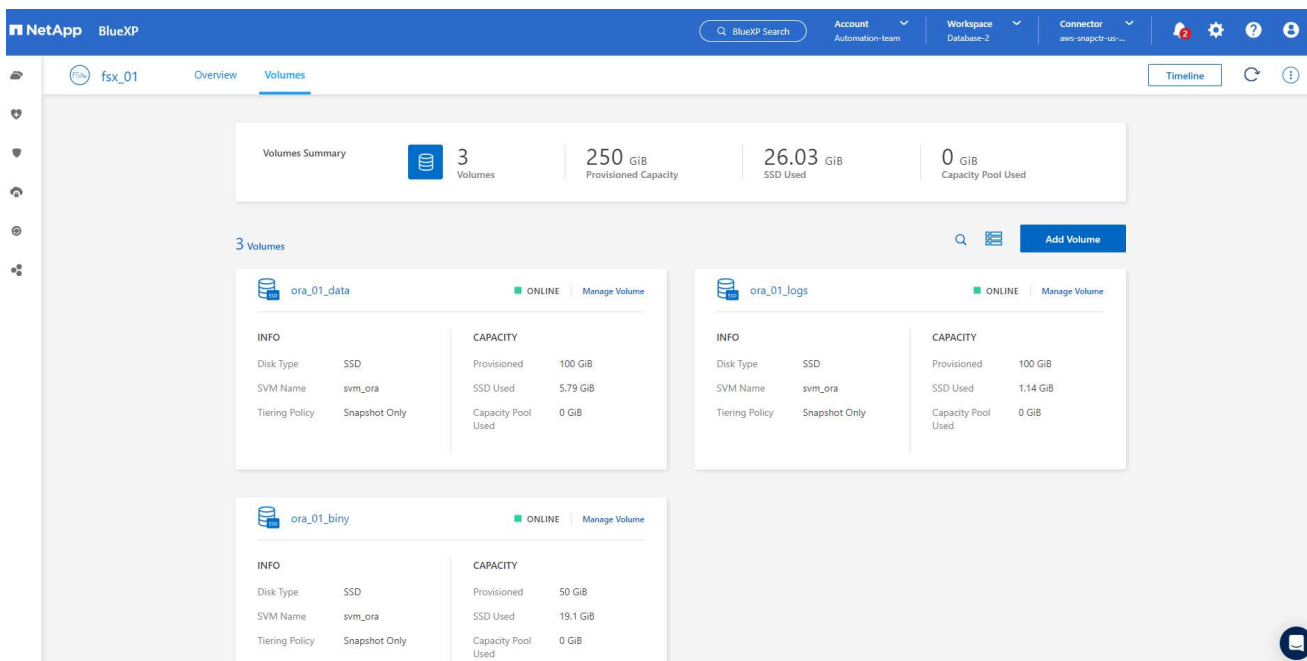
1. A instância descoberta do Amazon FSx ONTAP agora aparece no ambiente de trabalho.



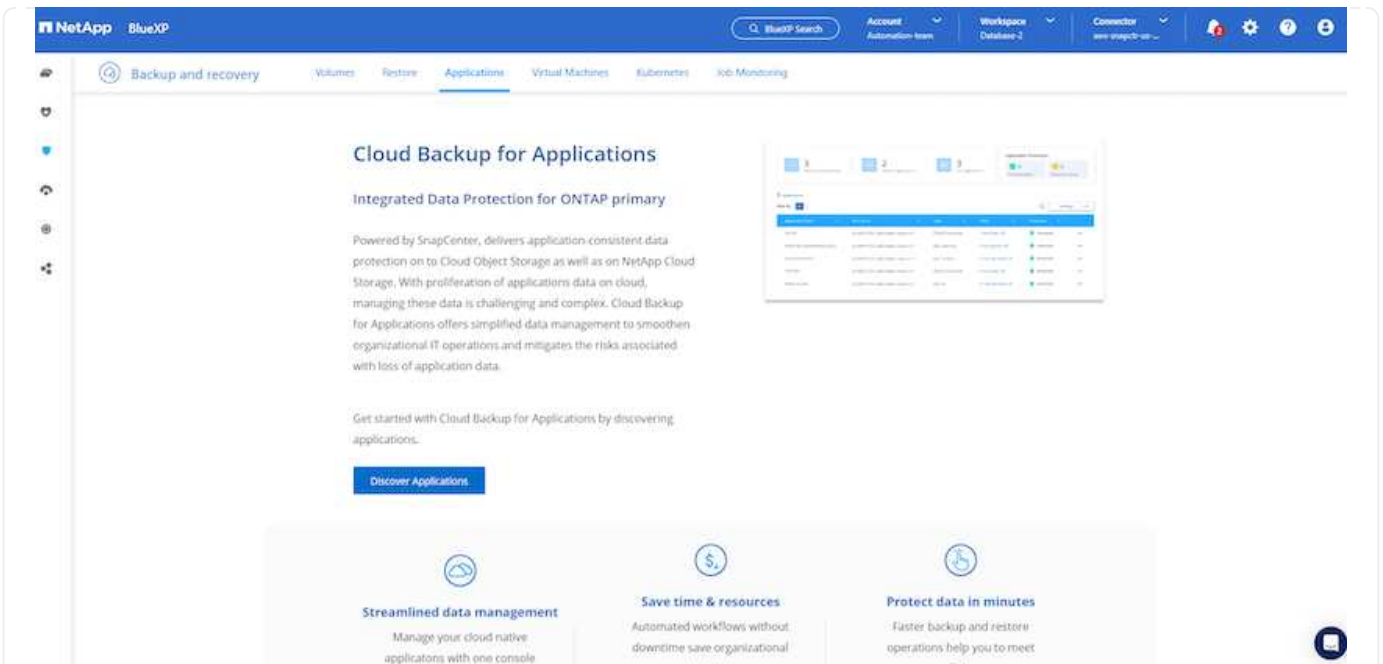
1. Você pode efetuar login no cluster FSx com suas credenciais de conta fsxadmin.



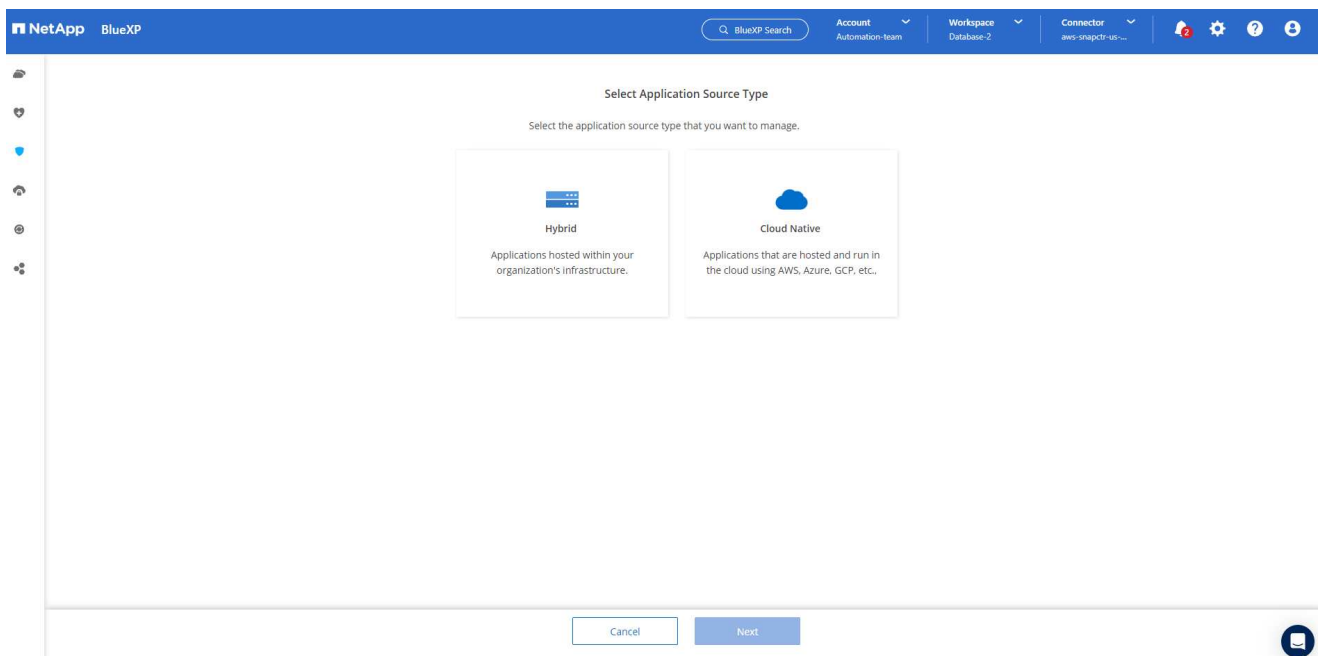
1. Depois de efetuar login no Amazon FSx ONTAP, revise as informações de armazenamento do seu banco de dados (como volumes de banco de dados).



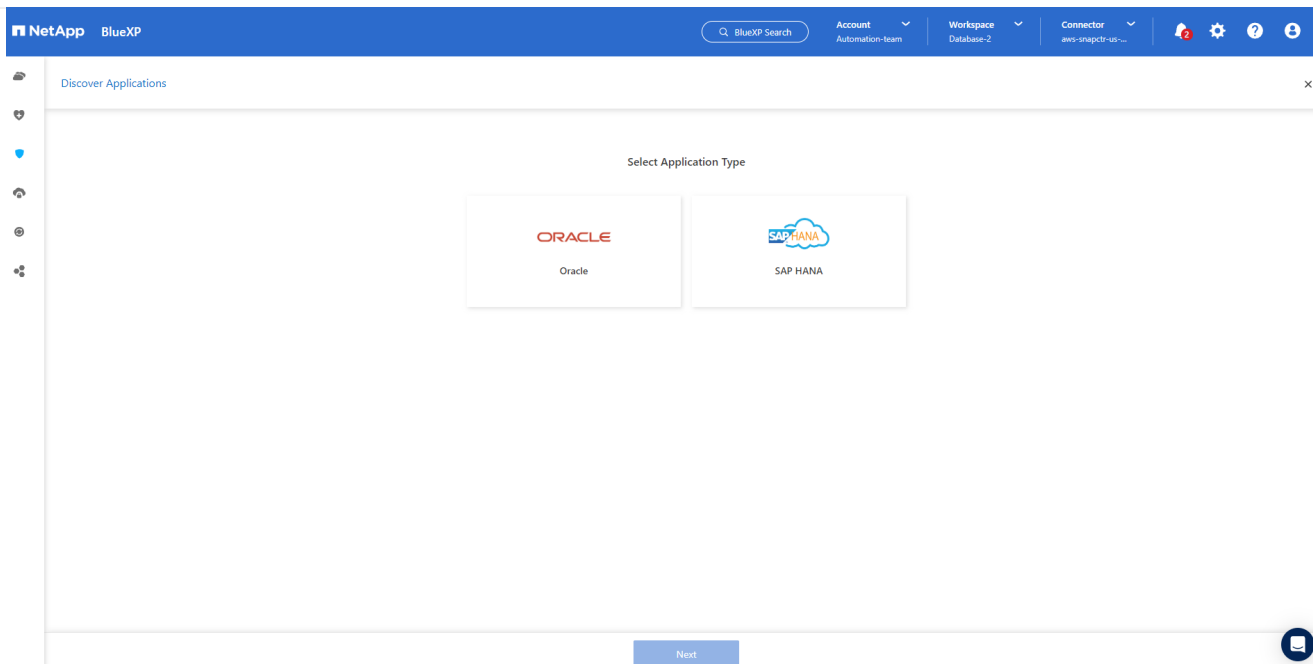
1. Na barra lateral esquerda do console, passe o mouse sobre o ícone de proteção e clique em **Proteção > Aplicativos** para abrir a página de inicialização de aplicativos. Clique em **Descobrir aplicativos**.



1. Selecione **Cloud Native** como o tipo de origem do aplicativo.

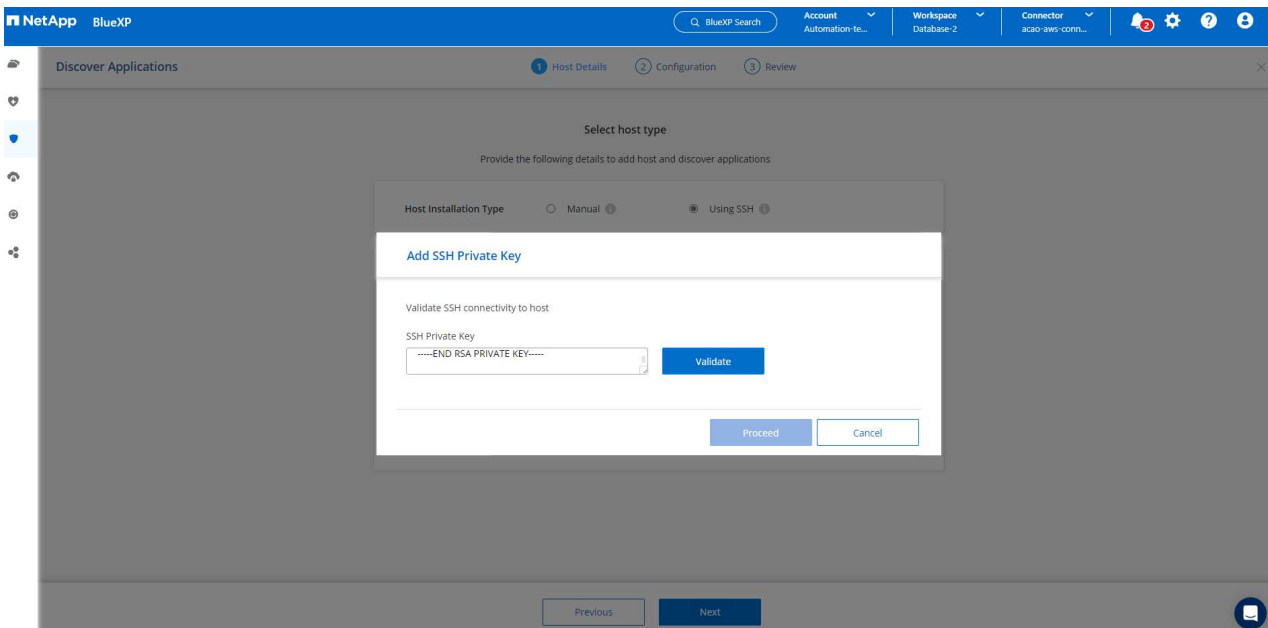


1. Escolha **Oracle** para o tipo de aplicativo.

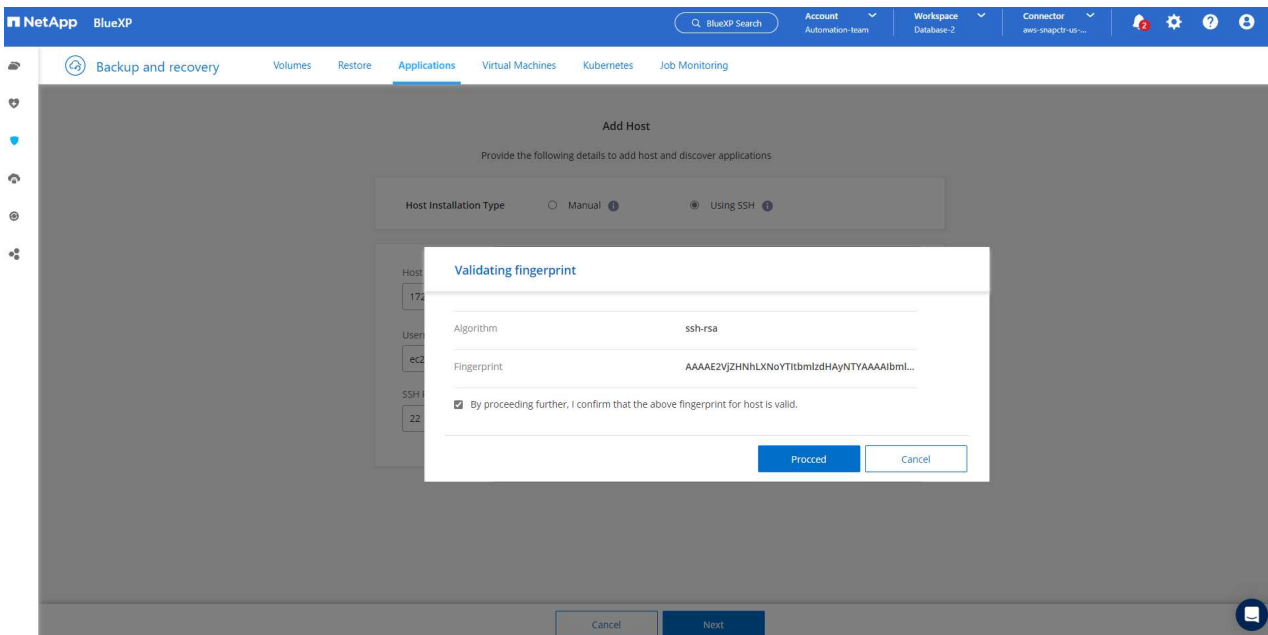


1. Preencha os detalhes do host do aplicativo AWS EC2 Oracle. Escolha **Usando SSH** como **Tipo de instalação de host** para instalação de plugin em uma etapa e descoberta de banco de dados. Em seguida, clique em **Adicionar chave privada SSH**.

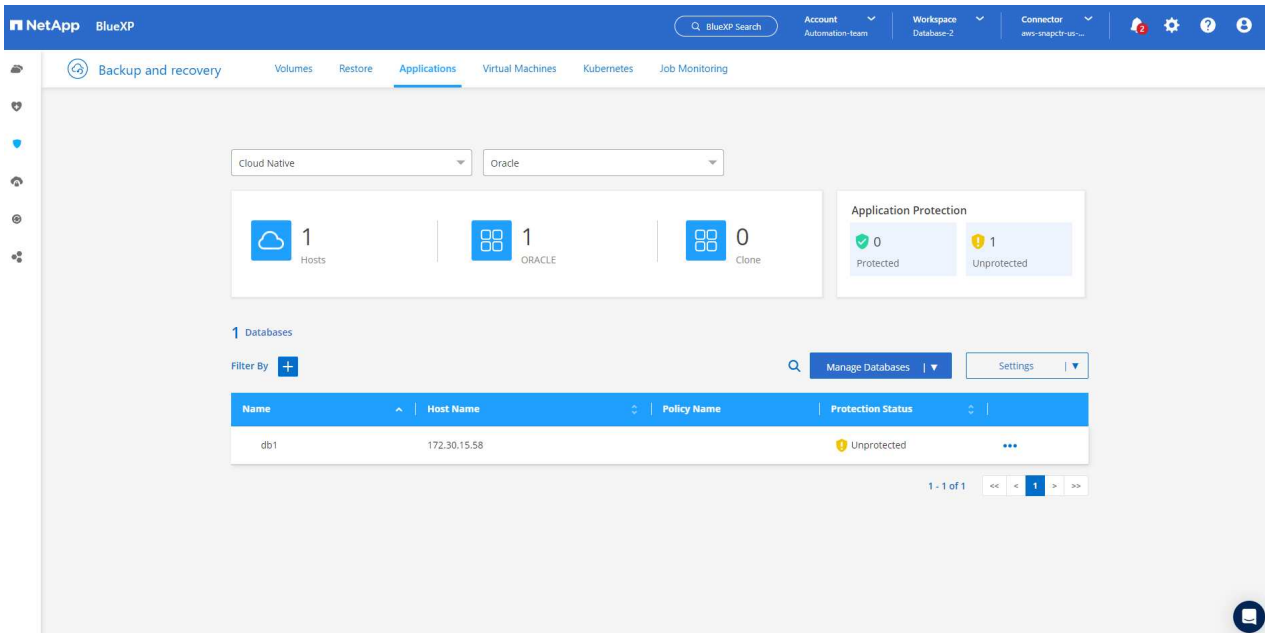
2. Cole sua chave SSH ec2-user para o host EC2 do banco de dados e clique em **Validar** para prosseguir.



3. Você será solicitado a **Validar impressão digital** para prosseguir.



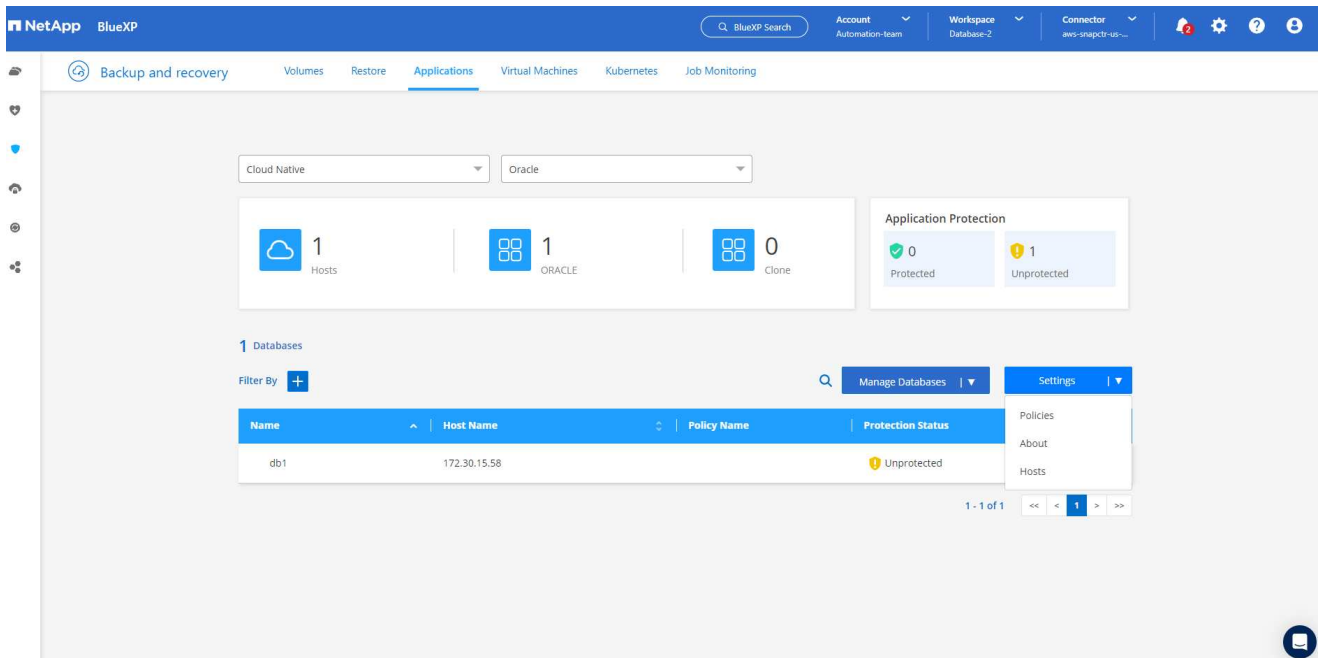
4. Clique em **Avançar** para instalar um plugin de banco de dados Oracle e descobrir os bancos de dados Oracle no host EC2. Os bancos de dados descobertos são adicionados em **Aplicativos**. O banco de dados **Status de Proteção** aparece como **Desprotegido** quando descoberto inicialmente.



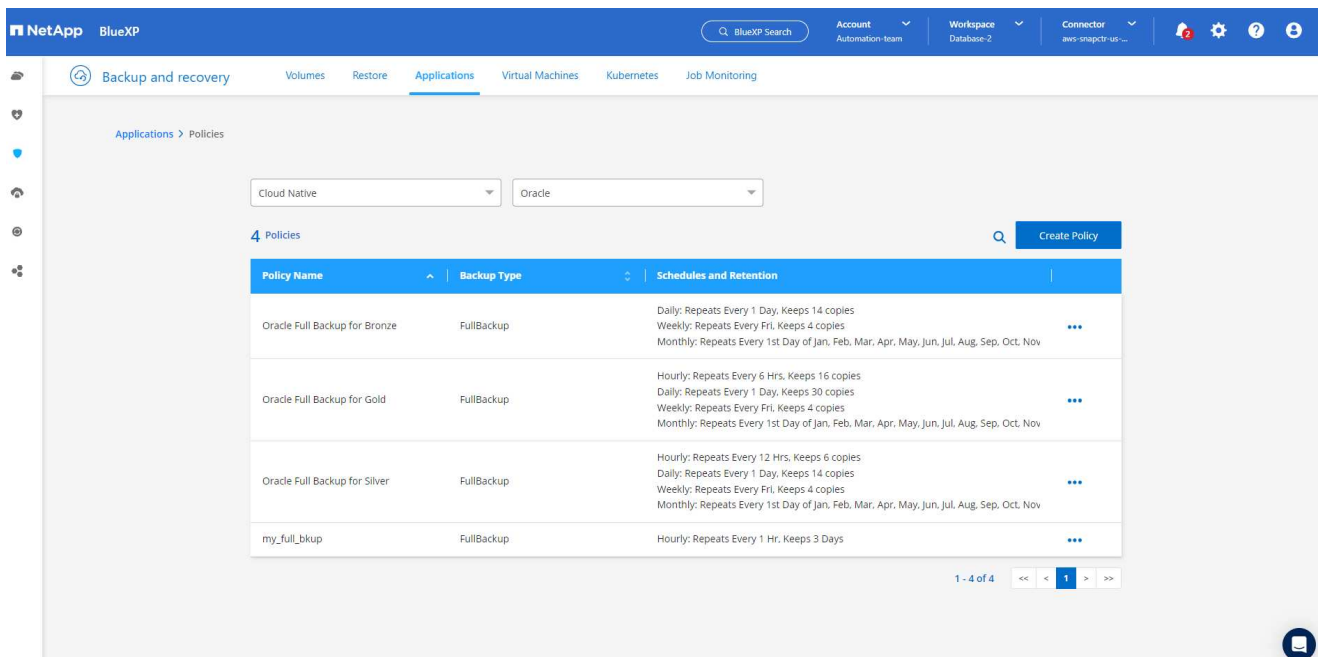
Isso conclui a configuração inicial dos serviços do SnapCenter para Oracle. As próximas três seções deste documento descrevem as operações de backup, restauração e clonagem do banco de dados Oracle.

Backup de banco de dados Oracle

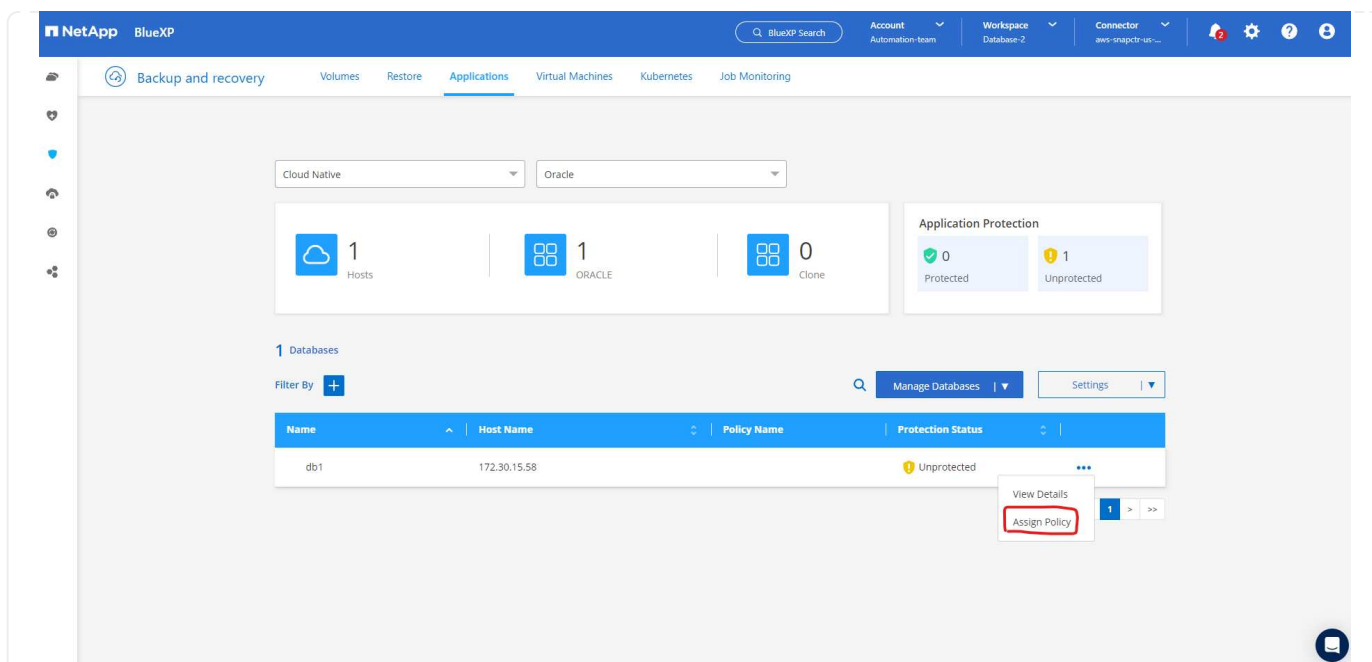
1. Clique nos três pontos ao lado do **Status de proteção** do banco de dados e, em seguida, clique em **Políticas** para visualizar as políticas de proteção de banco de dados pré-carregadas padrão que podem ser aplicadas para proteger seus bancos de dados Oracle.



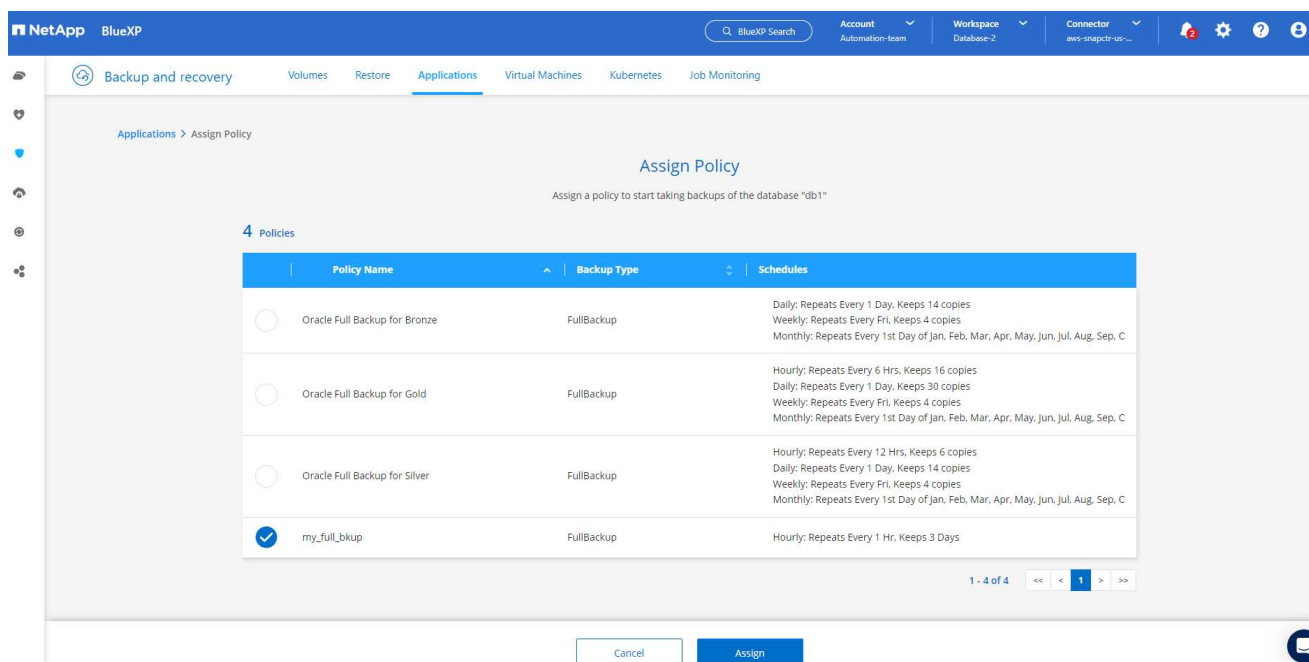
1. Você também pode criar sua própria política com uma frequência de backup personalizada e uma janela de retenção de dados de backup.



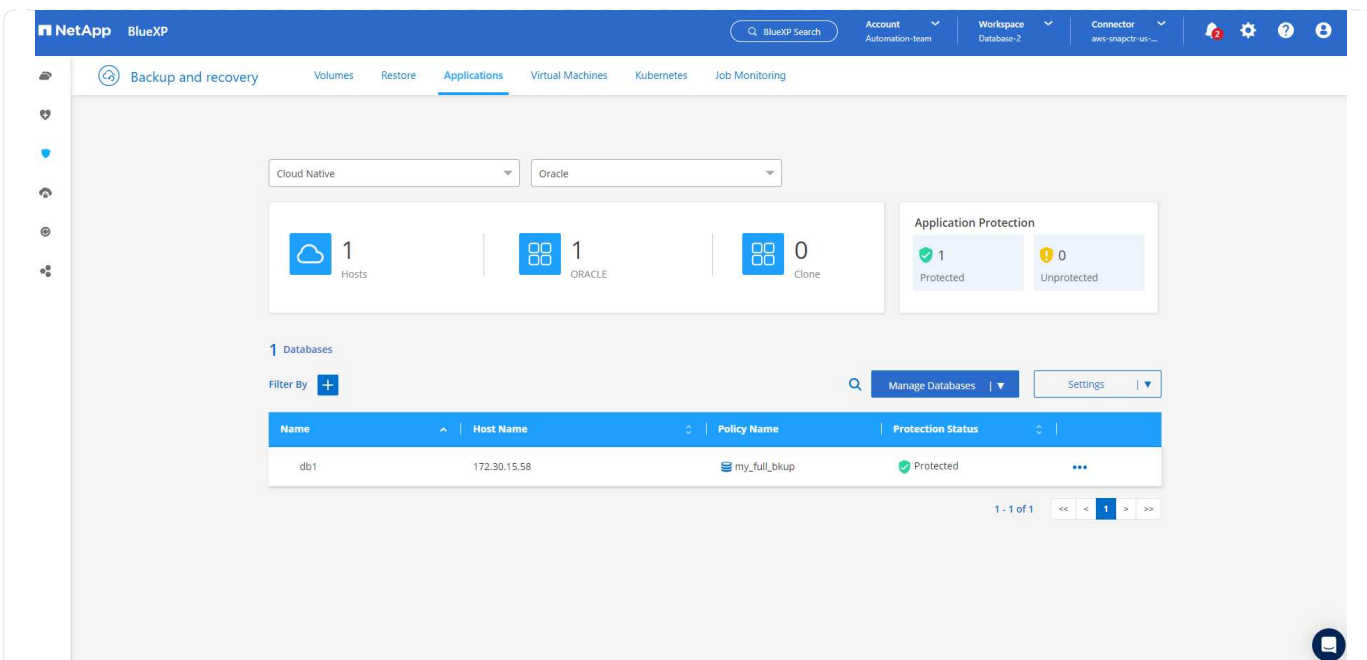
1. Quando estiver satisfeito com a configuração da política, você poderá atribuir a política de sua escolha para proteger o banco de dados.



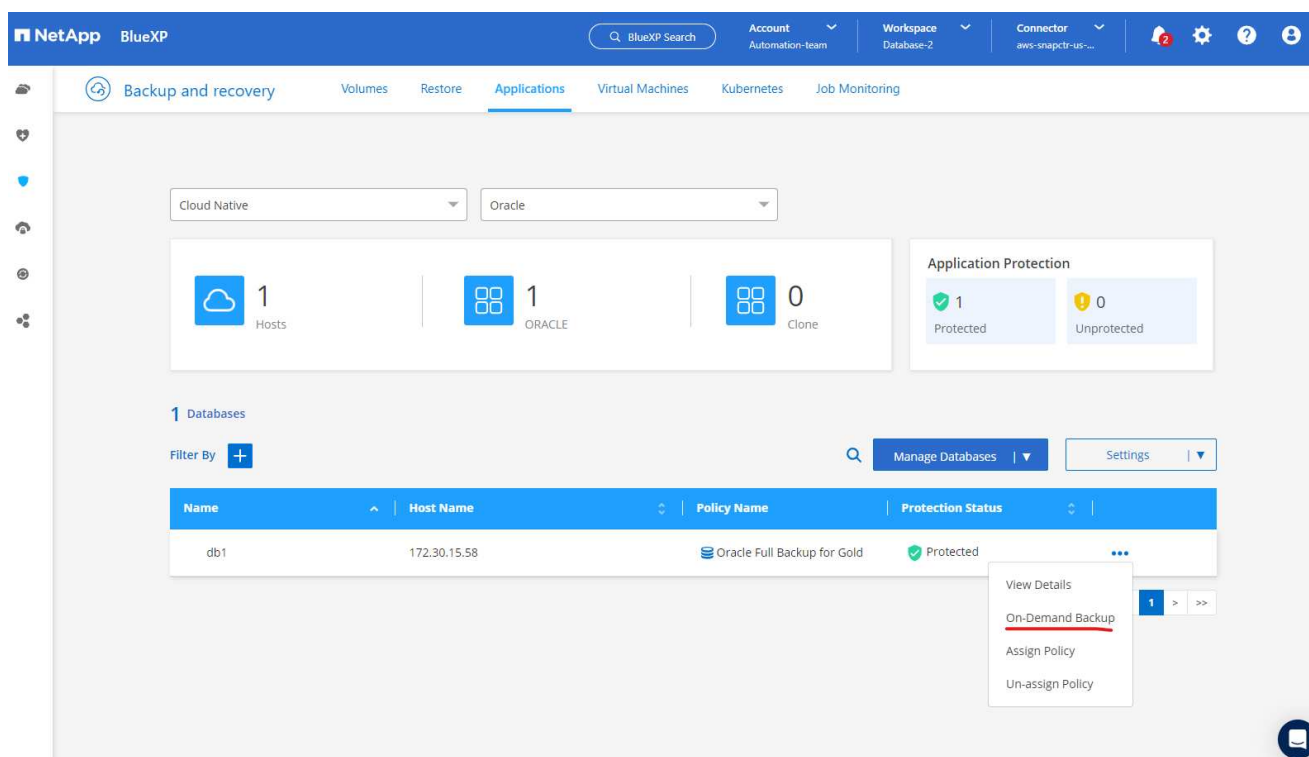
1. Escolha a política a ser atribuída ao banco de dados.



1. Após a aplicação da política, o status de proteção do banco de dados muda para **Protegido** com uma marca de seleção verde.



1. O backup do banco de dados é executado em um cronograma predefinido. Você também pode executar um backup único sob demanda, conforme mostrado abaixo.



1. Os detalhes dos backups do banco de dados podem ser visualizados clicando em **Exibir detalhes** na lista do menu. Isso inclui o nome do backup, o tipo de backup, o SCN e a data do backup. Um conjunto de backup abrange um instantâneo do volume de dados e do volume de log. Um instantâneo de volume de log ocorre logo após um instantâneo de volume de banco de dados. Você pode aplicar um filtro se estiver procurando um backup específico em uma lista longa.

NetApp

BlueXP

BlueXP Search

Account Automation-team

Workspace Database-2

Connector aws-snapctr-us...

2

⚙️

?

👤

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Applications > Database Details

Database Details

db1
Database Name

172.30.15.58
Host Name

-
Clones

Protected Protection

FSx
Host Storage

-
Parent Database

Oracle Full Backup for Gold Policy Names

Unreachable
Database Version

Database Type

bKed8yv2T19BJ0V5QyqvA...
Agent Id

8 Backups

Filter By

+

Search

Select Timeframe ▾

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

1. Para uma restauração de banco de dados, escolha o backup correto, pelo SCN ou pelo horário do backup. Clique nos três pontos do backup de dados do banco de dados e, em seguida, clique em **Restaurar** para iniciar a restauração e recuperação do banco de dados.

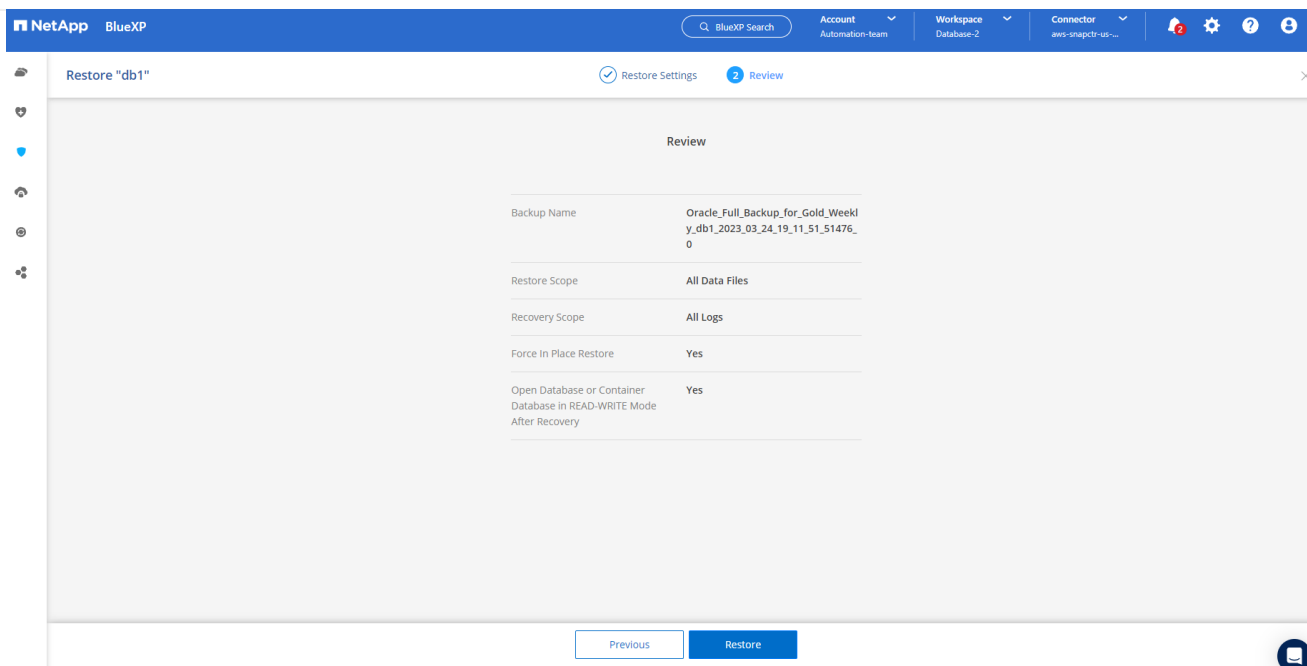
The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' tab is selected, leading to 'Database Details' for a database named 'db1'. Below the details, there are 6 backups listed. The backup 'Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_15_37_04_98851_1' is selected, and the 'Restore' button is highlighted in the context menu.

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

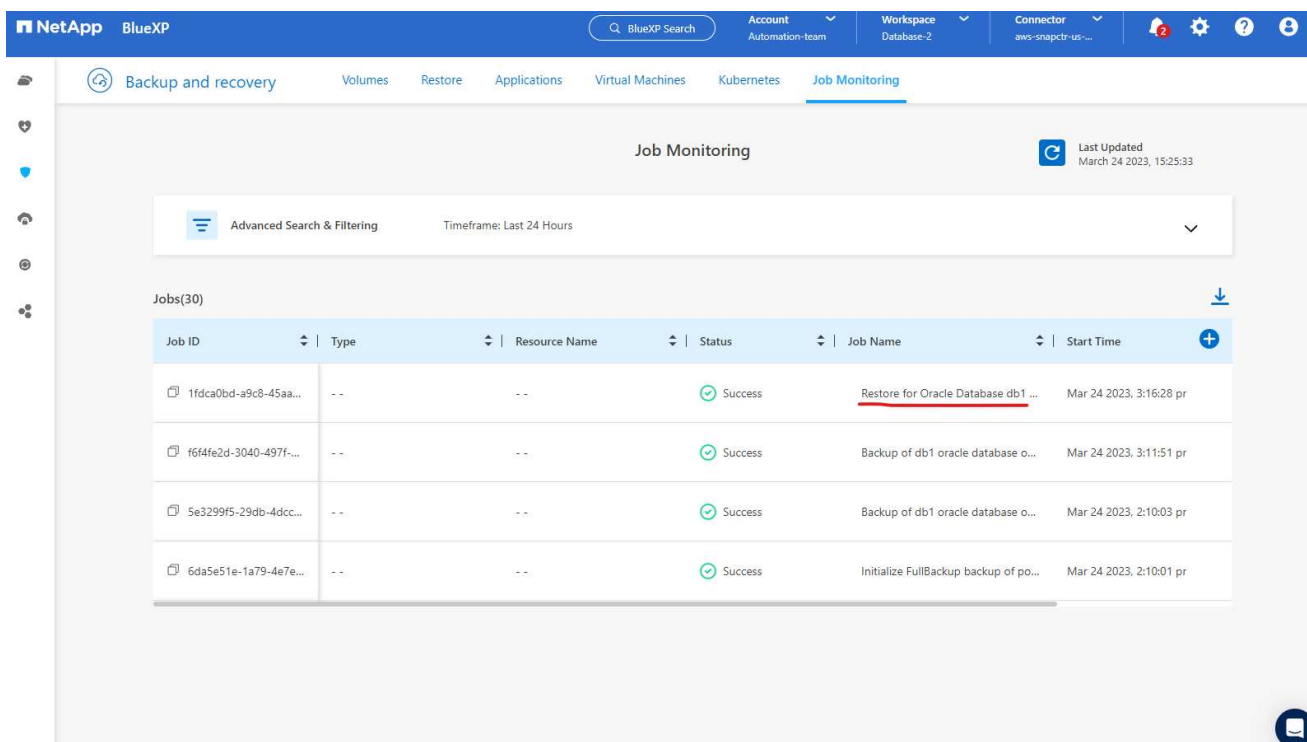
1. Escolha sua configuração de restauração. Se tiver certeza de que nada mudou na estrutura física do banco de dados após o backup (como a adição de um arquivo de dados ou de um grupo de discos), você pode usar a opção **Forçar restauração no local**, que geralmente é mais rápida. Caso contrário, não marque esta caixa.

The screenshot shows the 'Restore Settings' dialog box in the NetApp BlueXP interface. 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.

1. Revise e inicie a restauração e recuperação do banco de dados.



1. Na aba **Monitoramento de Tarefas**, você pode visualizar o status da tarefa de restauração, bem como quaisquer detalhes enquanto ela estiver em execução.



NetApp BlueXP

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

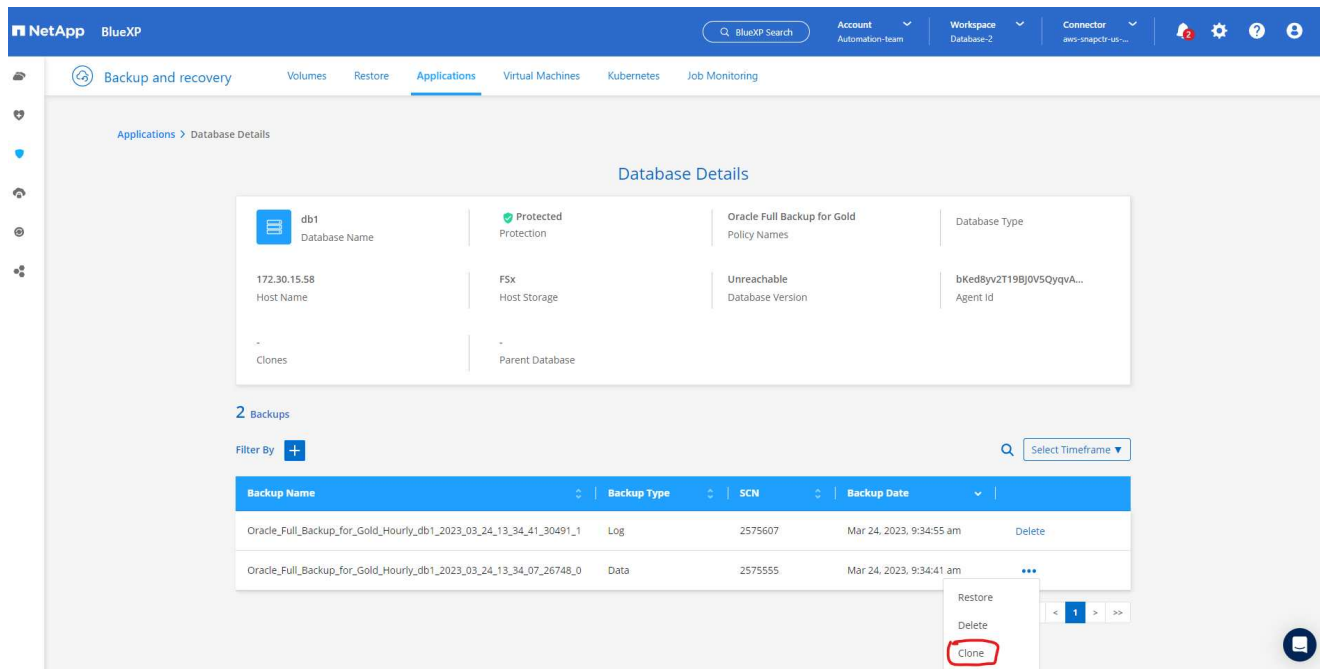
Sub-Jobs(6)

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

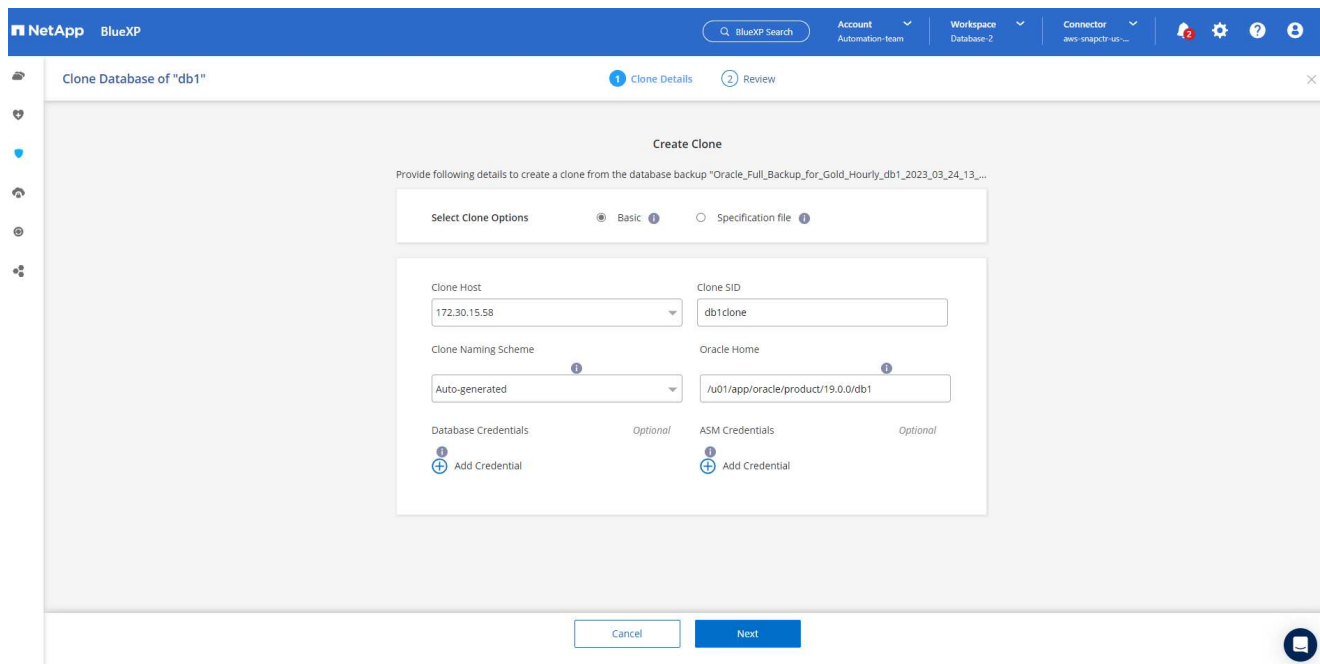
Clone de banco de dados Oracle

Para clonar um banco de dados, inicie o fluxo de trabalho de clonagem na mesma página de detalhes de backup do banco de dados.

1. Selecione a cópia de backup do banco de dados correta, clique nos três pontos para visualizar o menu e escolha a opção **Clonar**.



1. Selecione a opção **Básico** se não precisar alterar nenhum parâmetro do banco de dados clonado.



1. Como alternativa, selecione **Arquivo de especificação**, que lhe dá a opção de baixar o arquivo init atual, fazer alterações e, em seguida, enviá-lo de volta para o trabalho.

NetApp BlueXP

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
 ☒ Specification file

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. Revise e inicie o trabalho.

NetApp BlueXP

BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...

Clone Database of "db1"

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. Monitore o status do trabalho de clonagem na aba **Monitoramento de Trabalho**.

33

NetAppBlueXP

BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapc1r-108-...

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. Valide o banco de dados clonado no host da instância do EC2.

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

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

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

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

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

```
SQL> select name, open_mode from v$databases;
```

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

```
SQL>
```

Informações adicionais

Para saber mais sobre as informações descritas neste documento, revise os seguintes documentos e/ou sites:

- Configurar e administrar o 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)

- Documentação 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=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.