



TR-4964: Backup, ripristino e clonazione di Oracle Database con SnapCenter Services - AWS

NetApp database solutions

NetApp
August 18, 2025

Sommario

- TR-4964: Backup, ripristino e clonazione di Oracle Database con SnapCenter Services - AWS 1
 - Scopo 1
 - Pubblico 1
 - Ambiente di test e convalida della soluzione 1
 - Architettura 2
 - Componenti hardware e software 2
 - Fattori chiave per la considerazione dell'implementazione 3
 - Distribuzione della soluzione 3
 - Prerequisiti per la distribuzione del servizio SnapCenter 3
 - Preparazione all'onboarding su BlueXP 4
 - Distribuisci un connettore per i servizi SnapCenter 5
 - Definisci una credenziale in BlueXP per l'accesso alle risorse AWS 12
 - Configurazione dei servizi SnapCenter 16
 - Backup del database Oracle 24
 - Ripristino e recupero del database Oracle 28
 - Clone del database Oracle 31
 - Informazioni aggiuntive 36

TR-4964: Backup, ripristino e clonazione di Oracle Database con SnapCenter Services - AWS

Questa soluzione fornisce una panoramica e dettagli per il backup, il ripristino e la clonazione del database Oracle utilizzando NetApp SnapCenter SaaS tramite la console BlueXP nel cloud di Azure.

Allen Cao, Niyaz Mohamed, NetApp

Scopo

SnapCenter Services è la versione SaaS del classico strumento di interfaccia utente per la gestione del database SnapCenter, disponibile tramite la console di gestione cloud NetApp BlueXP. È parte integrante dell'offerta di backup cloud e protezione dei dati NetApp per database quali Oracle e HANA in esecuzione sullo storage cloud NetApp. Questo servizio basato su SaaS semplifica la distribuzione tradizionale del server autonomo SnapCenter, che in genere richiede un server Windows che opera in un ambiente di dominio Windows.

In questa documentazione, illustriamo come configurare SnapCenter Services per eseguire il backup, il ripristino e la clonazione di database Oracle distribuiti su istanze di archiviazione Amazon FSx ONTAP e di elaborazione EC2. Sebbene siano molto più semplici da configurare e utilizzare, i servizi SnapCenter offrono funzionalità chiave già disponibili nello strumento legacy SnapCenter UI.

Questa soluzione affronta i seguenti casi d'uso:

- Backup del database con snapshot per database Oracle ospitati in Amazon FSx ONTAP
- Ripristino del database Oracle in caso di guasto
- Clonazione rapida ed efficiente in termini di archiviazione di database primari per un ambiente di sviluppo/test o altri casi d'uso

Pubblico

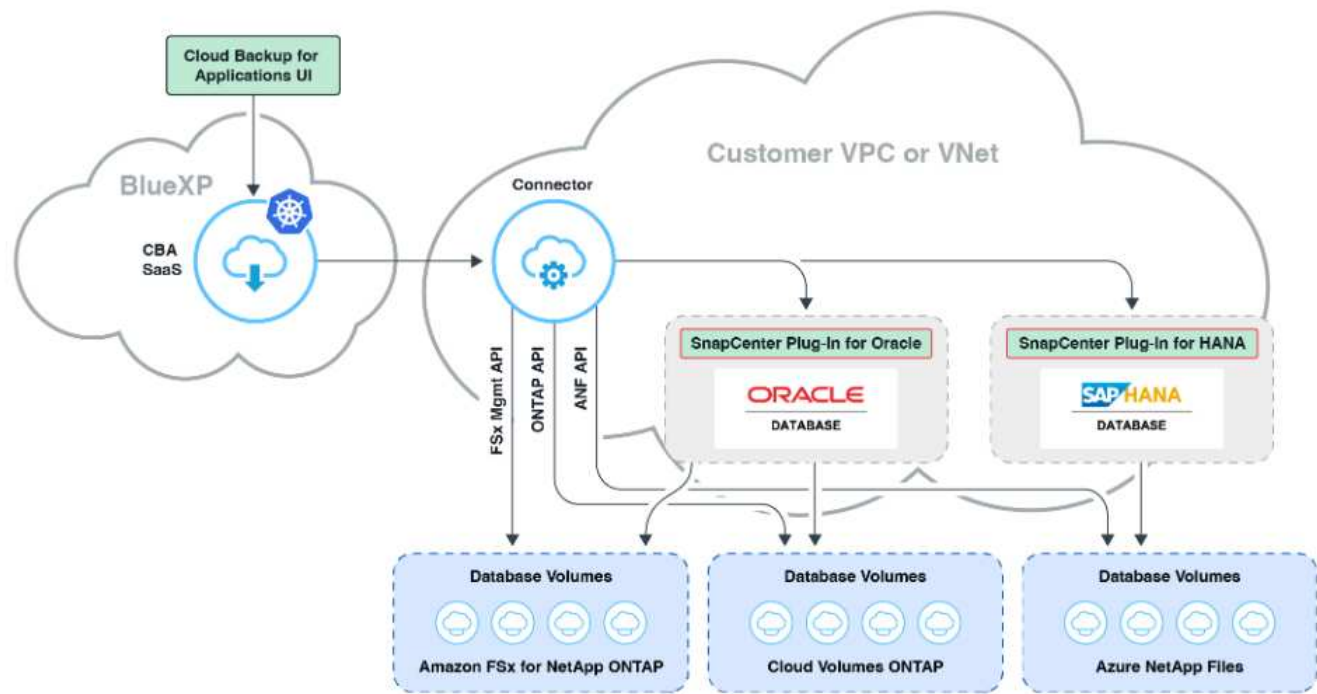
Questa soluzione è destinata ai seguenti pubblici:

- Il DBA che gestisce i database Oracle in esecuzione sullo storage Amazon FSx ONTAP
- L'architetto di soluzioni interessato a testare il backup, il ripristino e la clonazione del database Oracle nel cloud pubblico AWS
- L'amministratore di storage che supporta e gestisce lo storage Amazon FSx ONTAP
- Il proprietario dell'applicazione che possiede le applicazioni distribuite nello storage Amazon FSx ONTAP

Ambiente di test e convalida della soluzione

I test e la convalida di questa soluzione sono stati eseguiti in un ambiente AWS FSx ed EC2 che potrebbe non corrispondere all'ambiente di distribuzione finale. Per ulteriori informazioni, consultare la sezione [Fattori chiave per la considerazione dell'implementazione](#).

Architettura



Questa immagine fornisce un quadro dettagliato del BlueXP backup and recovery per le applicazioni all'interno della console BlueXP , tra cui l'interfaccia utente, il connettore e le risorse che gestisce.

Componenti hardware e software

Hardware

Archiviazione FSx ONTAP	Versione attuale offerta da AWS	Un cluster FSx HA nella stessa VPC e zona di disponibilità
Istanza EC2 per il calcolo	t2.xlarge/4vCPU/16G	Due istanze EC2 T2 xlarge EC2, una come server DB primario e l'altra come server DB clone

Software

RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Abbonamento RedHat distribuito per i test
Infrastruttura Oracle Grid	Versione 19.18	Patch RU applicata p34762026_190000_Linux-x86-64.zip
Database Oracle	Versione 19.18	Patch RU applicata p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Versione 12.2.0.1.36	Ultima patch p6880880_190000_Linux-x86-64.zip

Servizio SnapCenter	Versione	v2.3.1.2324
---------------------	----------	-------------

Fattori chiave per la considerazione dell'implementazione

- **Connettore da distribuire nella stessa VPC del database e di FSx.** Se possibile, il connettore dovrebbe essere distribuito nella stessa AWS VPC, che consente la connettività allo storage FSx e all'istanza di elaborazione EC2.
- **Una policy AWS IAM creata per il connettore SnapCenter .** La policy in formato JSON è disponibile nella documentazione dettagliata del servizio SnapCenter . Quando si avvia la distribuzione del connettore con la console BlueXP , viene anche richiesto di impostare i prerequisiti con i dettagli delle autorizzazioni richieste in formato JSON. La policy deve essere assegnata all'account utente AWS proprietario del connettore.
- **La chiave di accesso all'account AWS e la coppia di chiavi SSH create nell'account AWS.** La coppia di chiavi SSH viene assegnata all'utente ec2 per accedere all'host del connettore e quindi distribuire un plug-in del database all'host del server DB EC2. La chiave di accesso concede l'autorizzazione per il provisioning del connettore richiesto con la policy IAM sopra indicata.
- **Una credenziale aggiunta alle impostazioni della console BlueXP .** Per aggiungere Amazon FSx ONTAP all'ambiente di lavoro BlueXP , è necessario configurare una credenziale che conceda a BlueXP le autorizzazioni per accedere ad Amazon FSx ONTAP nelle impostazioni della console BlueXP .
- **java-11-openjdk installato sull'host dell'istanza del database EC2.** Per installare il servizio SnapCenter è richiesta la versione 11 di Java. Deve essere installato sull'host dell'applicazione prima di tentare la distribuzione del plugin.

Distribuzione della soluzione

È disponibile un'ampia documentazione NetApp con una portata più ampia per aiutarti a proteggere i dati delle tue applicazioni cloud native. L'obiettivo di questa documentazione è fornire procedure dettagliate che riguardano la distribuzione del servizio SnapCenter con la console BlueXP per proteggere il database Oracle distribuito su Amazon FSx ONTAP e un'istanza di elaborazione EC2. Questo documento fornisce alcuni dettagli che potrebbero mancare nelle istruzioni più generali.

Per iniziare, completa i seguenti passaggi:

- Leggi le istruzioni generali "[Proteggi i dati delle tue applicazioni cloud native](#)" e le sezioni relative a Oracle e Amazon FSx ONTAP.
- Guarda il seguente video tutorial.

[Distribuzione della soluzione](#)

Prerequisiti per la distribuzione del servizio SnapCenter

Per la distribuzione sono richiesti i seguenti prerequisiti.

1. Un server di database Oracle primario su un'istanza EC2 con un database Oracle completamente distribuito e in esecuzione.
2. Un cluster Amazon FSx ONTAP distribuito in AWS che ospita i volumi del database sopra indicati.
3. Un server di database opzionale su un'istanza EC2 che può essere utilizzato per testare la clonazione di un database Oracle su un host alternativo allo scopo di supportare un carico di lavoro di sviluppo/test o qualsiasi caso d'uso che richieda un set di dati completo di un database Oracle di produzione.
4. Se hai bisogno di aiuto per soddisfare i prerequisiti sopra indicati per la distribuzione del database Oracle su Amazon FSx ONTAP e sull'istanza di elaborazione EC2, consulta ["Distribuzione e protezione del database Oracle in AWS FSx/EC2 con iSCSI/ASM"](#) o carta bianca ["Procedure consigliate per la distribuzione di Oracle Database su EC2 e FSx"](#)

Preparazione all'onboarding su BlueXP

1. Utilizzare il collegamento **"NetApp BlueXP"** per registrarsi per accedere alla console BlueXP .
2. Accedi al tuo account AWS per creare una policy IAM con le autorizzazioni appropriate e assegnarla all'account AWS che verrà utilizzato per la distribuzione del connettore 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 displays the 'Summary' page for a policy named 'snapcenter'. Key details include the Policy ARN 'arn:aws:iam::541696183547:policy/snapcenter' and the description 'Policy to grant snapcenter service permission to create connector in AWS.' Below this, the 'Permissions' tab is active, showing a JSON policy document. The JSON defines a single statement with an 'Effect' of 'Allow' and a list of actions including IAM operations (CreateRole, DeleteRole, PutRolePolicy, etc.) and EC2 operations (DescribeInstanceStatus, RunInstances, etc.).

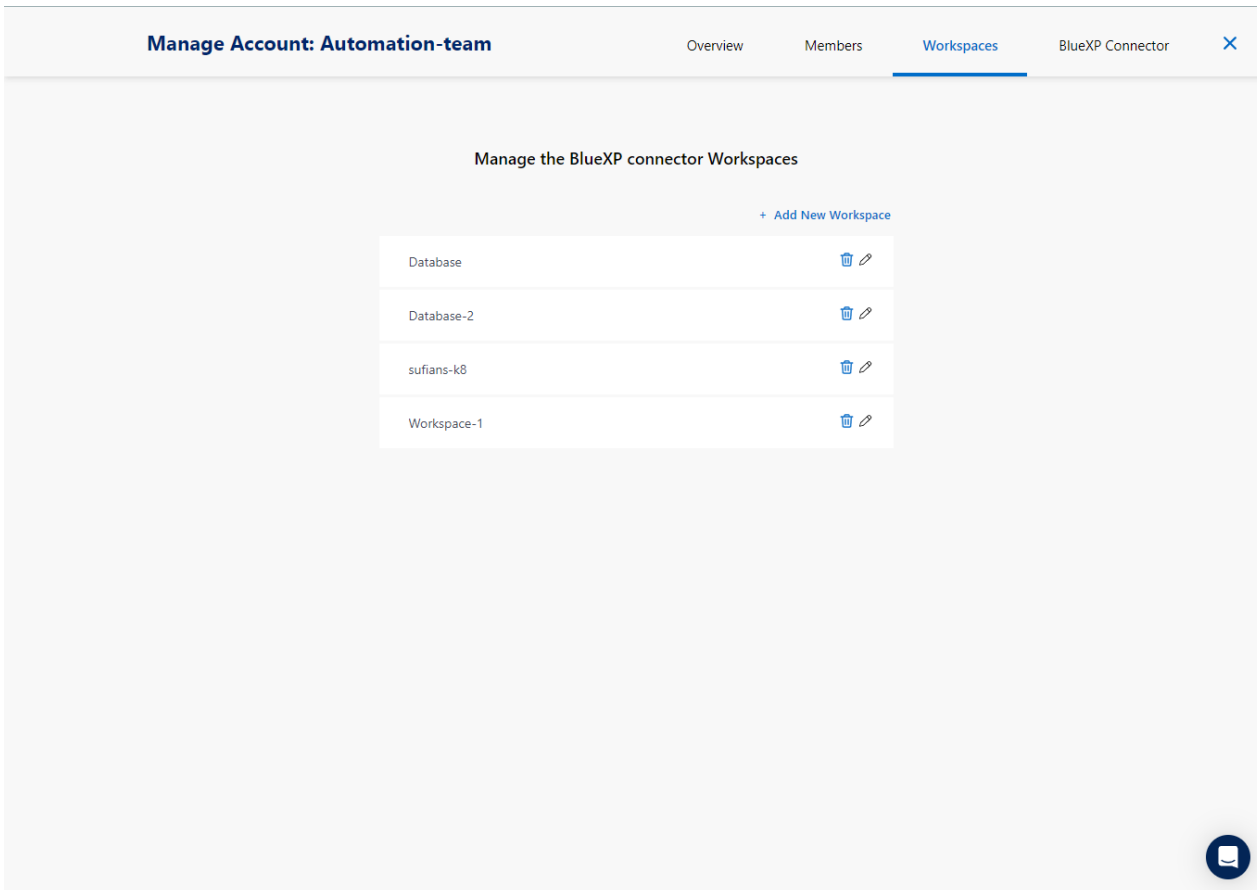
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:CreateRole",
8         "iam:DeleteRole",
9         "iam:PutRolePolicy",
10        "iam:CreateInstanceProfile",
11        "iam:DeleteRolePolicy",
12        "iam:AddRoleToInstanceProfile",
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"
```

La policy deve essere configurata con una stringa JSON disponibile nella documentazione NetApp . La stringa JSON può anche essere recuperata dalla pagina quando viene avviato il provisioning del connettore e viene richiesto di assegnare le autorizzazioni dei prerequisiti.

3. Sono inoltre necessari AWS VPC, subnet, gruppo di sicurezza, una chiave di accesso e segreti dell'account utente AWS, una chiave SSH per ec2-user e così via, pronti per il provisioning del connettore.

Distribuisci un connettore per i servizi SnapCenter

1. Accedi alla console BlueXP . Per un account condiviso, è consigliabile creare un'area di lavoro individuale facendo clic su **Account > Gestisci account > Area di lavoro** per aggiungere una nuova area di lavoro.



2. Fare clic su **Aggiungi un connettore** per avviare il flusso di lavoro di provisioning del connettore.

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

- Scegli il tuo fornitore cloud (in questo 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

- Salta i passaggi **Autorizzazione**, **Autenticazione** e **Rete** se li hai già configurati nel tuo account AWS. In caso contrario, è necessario configurarli prima di procedere. Da qui, è anche possibile recuperare le autorizzazioni per la policy AWS a cui si fa riferimento nella sezione precedente

7

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. Inserisci l'autenticazione del tuo account AWS con **Chiave di accesso** e **Chiave segreta**.

Add Connector - AWS

[More Information](#)

- 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. Assegna un nome all'istanza del connettore e seleziona **Crea ruolo** in **Dettagli**.

Add Connector - AWS

[More Information](#)

- ✓ 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. Configurare la rete con la **VPC**, la **Subnet** e la **coppia di chiavi SSH** appropriate per l'accesso al connettore.

Add BlueXP Connector - AWS

More Information

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

Network

Connectivity

VPC

vpc-0b522d5e982a50ceb - 172.30.15.0/25

Subnet

172.30.15.0/25 | priv-subnet-01

Key Pair

sufi_new

Public IP

Use subnet settings (Disable)

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

Proxy Configuration (Optional)

HTTP Proxy

Example: http://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

Previous

Next

2. Impostare il **Gruppo di sicurezza** per il connettore.

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. Rivedi la pagina di riepilogo e fai clic su **Aggiungi** per avviare la creazione del connettore. In genere, per completare l'implementazione occorrono circa 10 minuti. Una volta completata, l'istanza del connettore viene visualizzata nella dashboard di 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

Definisci una credenziale in BlueXP per l'accesso alle risorse AWS

1. Per prima cosa, dalla console AWS EC2, crea un ruolo nel menu **Identity and Access Management (IAM) Ruoli**, **Crea ruolo** per avviare il flusso di lavoro di creazione del ruolo.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
- Authtue rules
- Analysers
- Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

- IAM Identity Center
- AWS Organizations

Roles (106)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search

Role name	Trusted entities	Last activity
☐ AmazonEC2RoleforLambda	AWS Service: ec2	-
☐ AmazonSSMRoleforInstancesQuickSetup	AWS Service: ec2	156 days ago
☐ aws-controltower-AdministratortExecutionRole	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_Mock3e725667e2b3	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
☐ AWSReservedSSO_AWSPowerUserAccess_509f0a0f6a40ed1	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
☐ AWSReservedSSO_AWSReadOnlyAccess_234340f57c7fb11d	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
☐ AWSReservedSSO_SAA-Dev-ReadOnly_Ib6f1a9983e115e7	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-

2. Nella pagina **Seleziona entità attendibile**, seleziona **Account AWS**, **Altro account AWS** e incolla l'ID dell'account BlueXP , che può essere recuperato dalla console BlueXP .

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity

Trusted entity type

- ☐ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☒ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

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

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 i criteri di autorizzazione per fsx e aggiungi **Criteri di autorizzazione** al ruolo.

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. Nella pagina **Dettagli ruolo**, assegna un nome al ruolo, aggiungi una descrizione, quindi fai clic su **Crea ruolo**.

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. Tornando alla console BlueXP, fare clic sull'icona delle impostazioni nell'angolo in alto a destra della console per aprire la pagina **Credenziali account**, fare clic su **Aggiungi credenziali** per avviare il flusso di lavoro di configurazione delle credenziali.

NetApp BlueXP

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

Credentials Account credentials User credentials

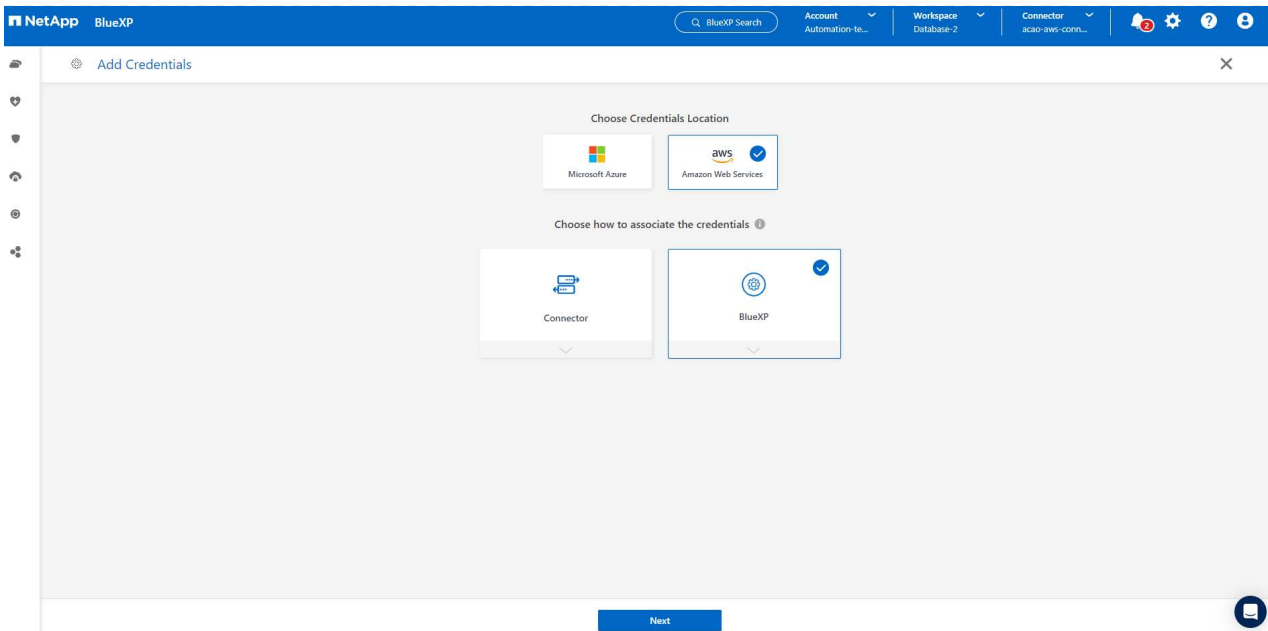
BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.

5 Credentials Add credentials

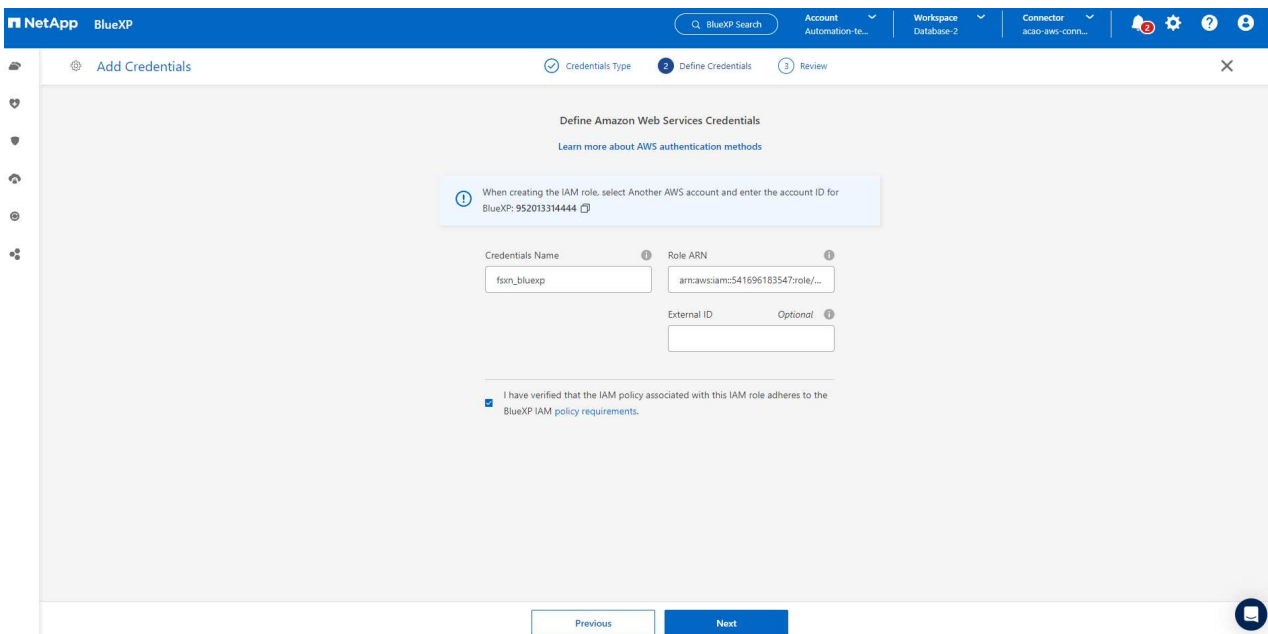
aws shantanucreds
Type: Assume Role | BlueXP

210811600188 AWS Account ID nkanthik_kafka_nfs_role_FSxN Assume Role

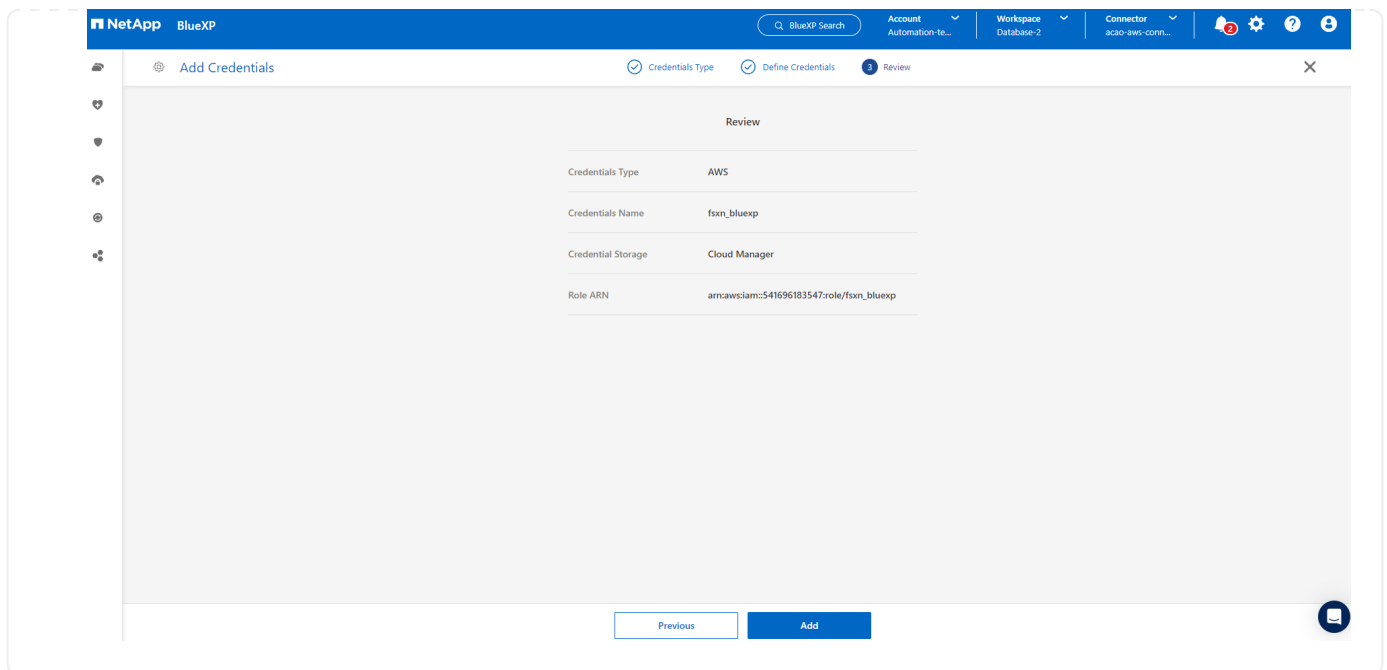
6. Scegli la posizione delle credenziali come - **Amazon Web Services - BlueXP**.



- Definisci le credenziali AWS con il **Role ARN** appropriato, che può essere recuperato dal ruolo AWS IAM creato nel passaggio 1 precedente. **ID account** BlueXP , utilizzato per creare il ruolo AWS IAM nel primo passaggio.



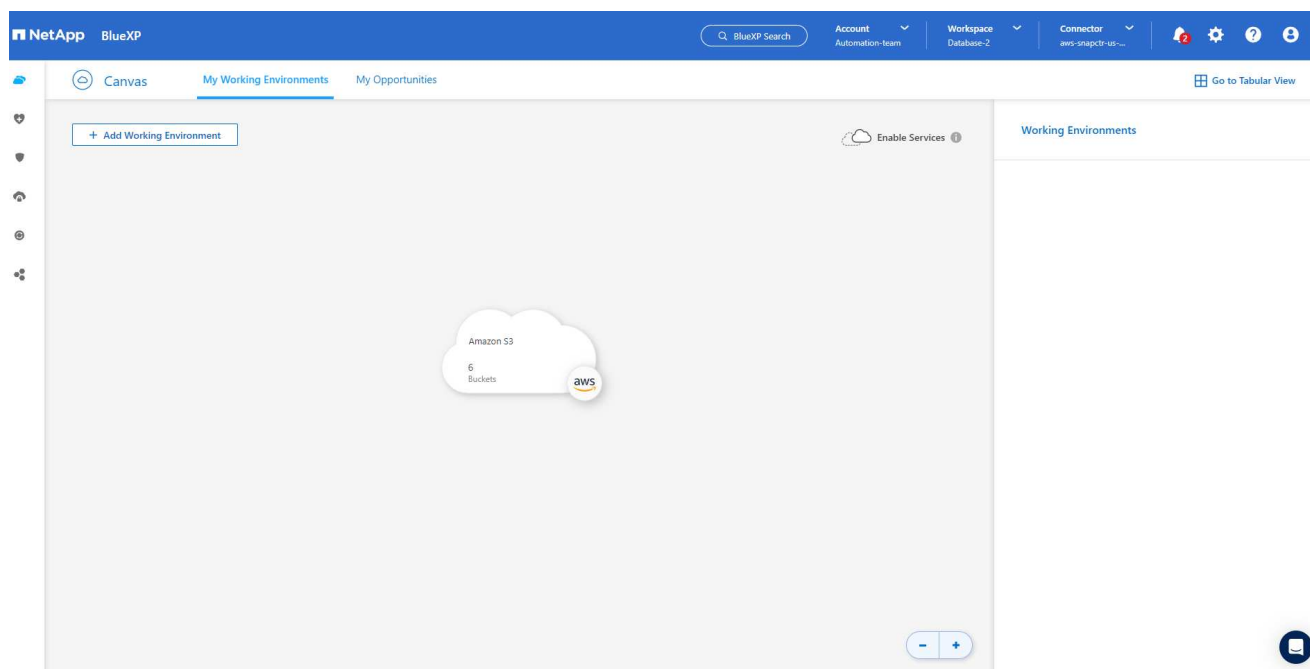
- Rivedi e Aggiungi



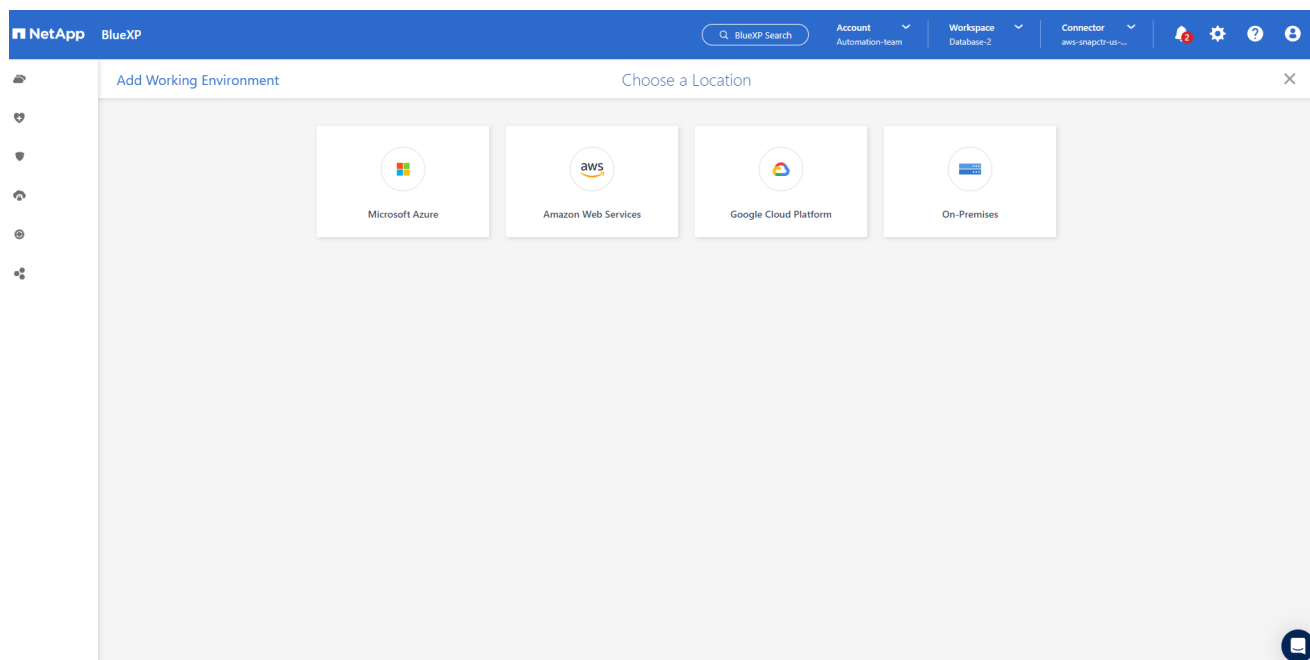
Configurazione dei servizi SnapCenter

Una volta distribuito il connettore e aggiunte le credenziali, è ora possibile configurare i servizi SnapCenter con la seguente procedura:

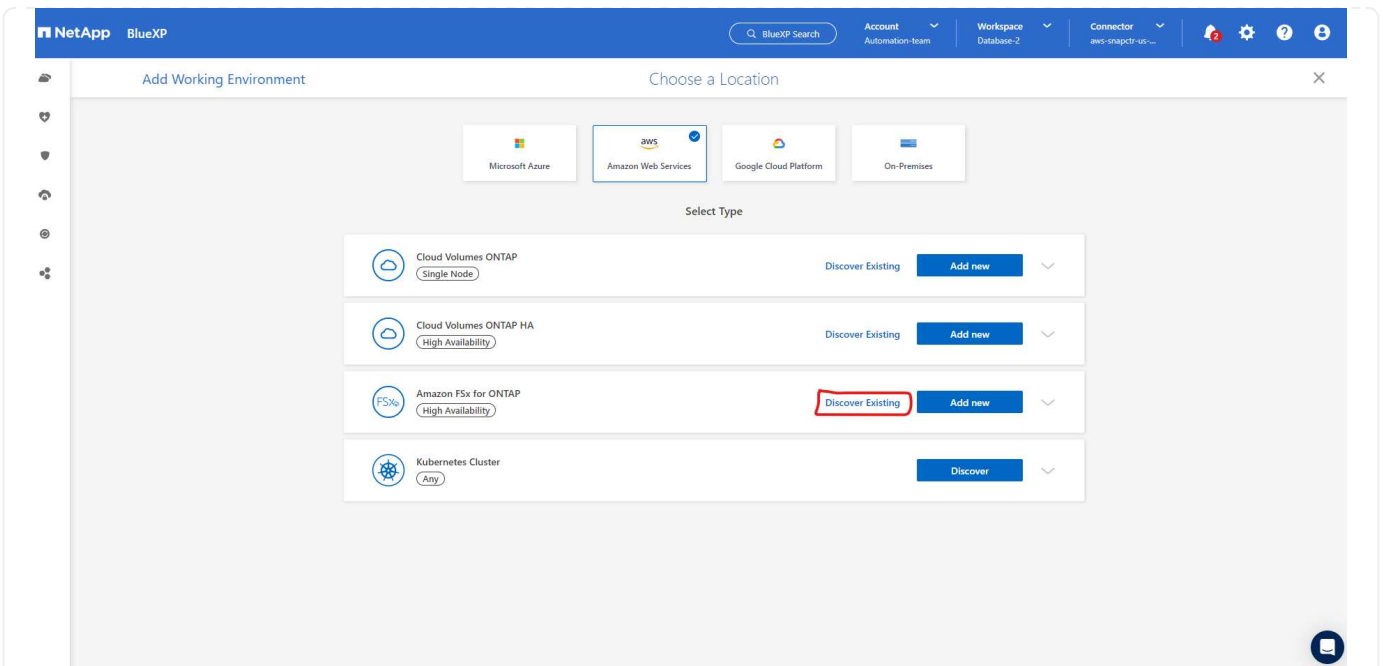
1. Da **Il mio ambiente di lavoro** fare clic su **Aggiungi ambiente di lavoro** per scoprire FSx distribuito in AWS.



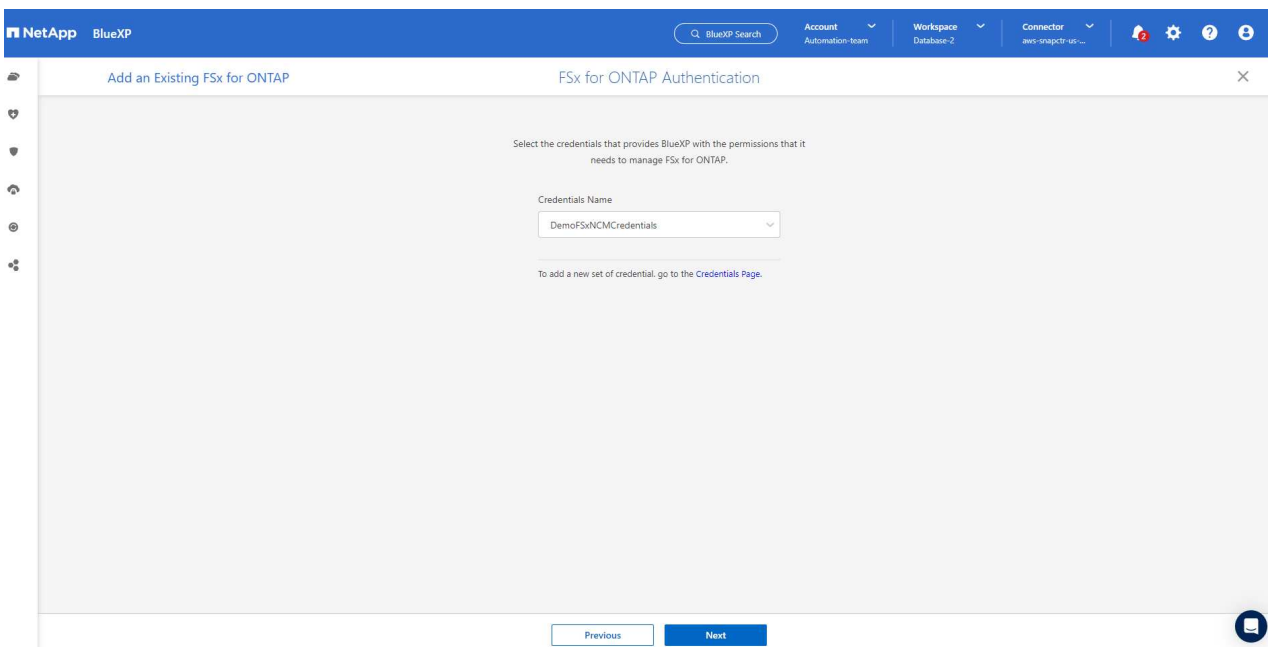
1. Seleziona **Amazon Web Services** come posizione.



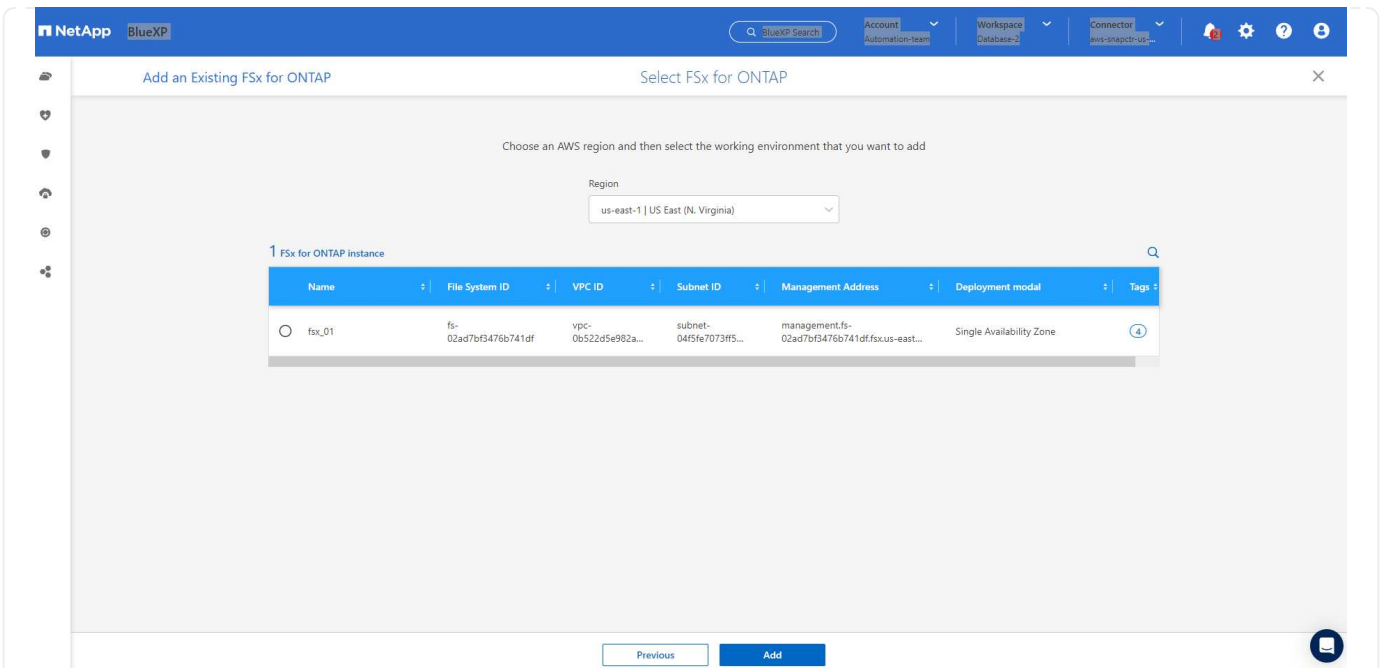
1. Fare clic su **Scopri esistente** accanto a *** Amazon FSx ONTAP***.



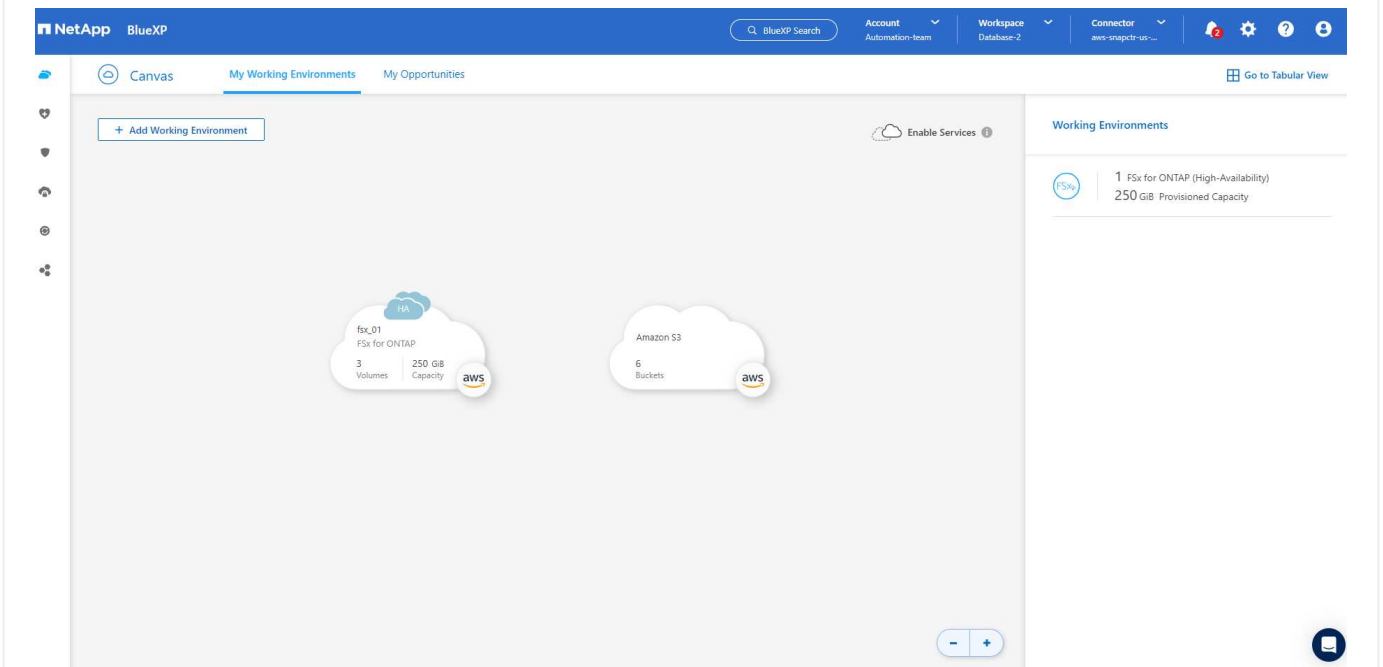
1. Selezionare il **Nome credenziali** creato nella sezione precedente per concedere a BlueXP le autorizzazioni necessarie per gestire FSx ONTAP. Se non hai aggiunto le credenziali, puoi aggiungerle dal menu **Impostazioni** nell'angolo in alto a destra della console BlueXP .



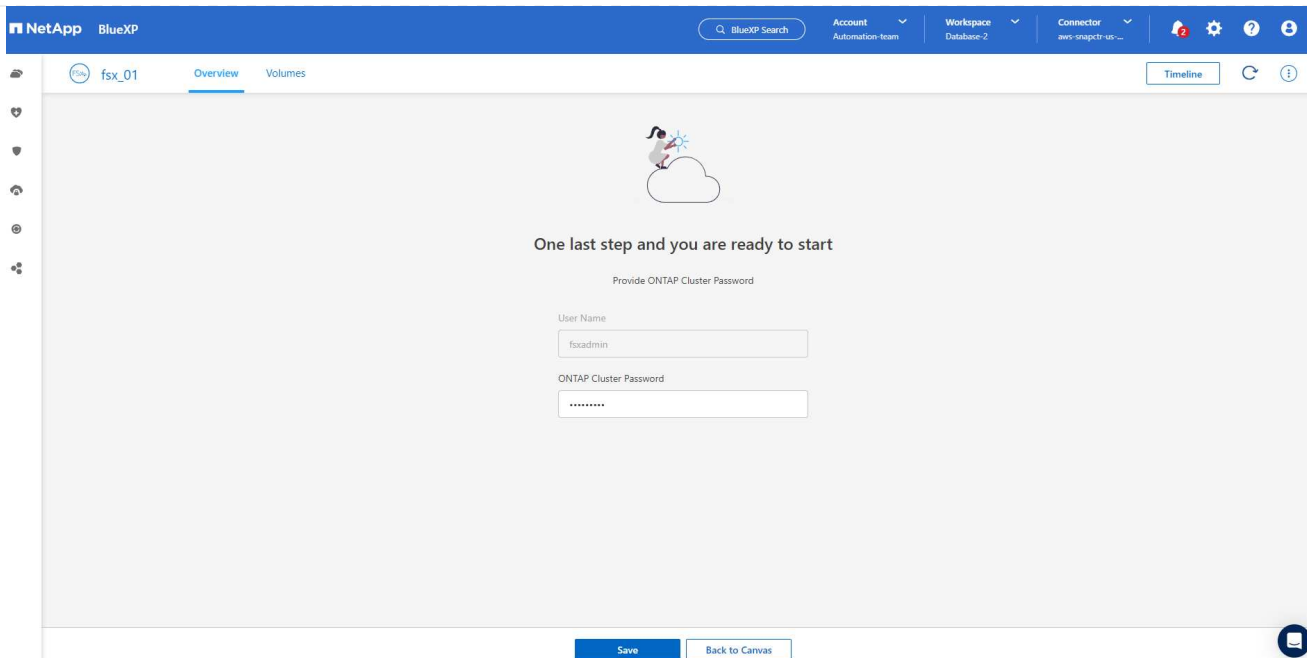
2. Scegli la regione AWS in cui è distribuito Amazon FSx ONTAP , seleziona il cluster FSx che ospita il database Oracle e fai clic su Aggiungi.



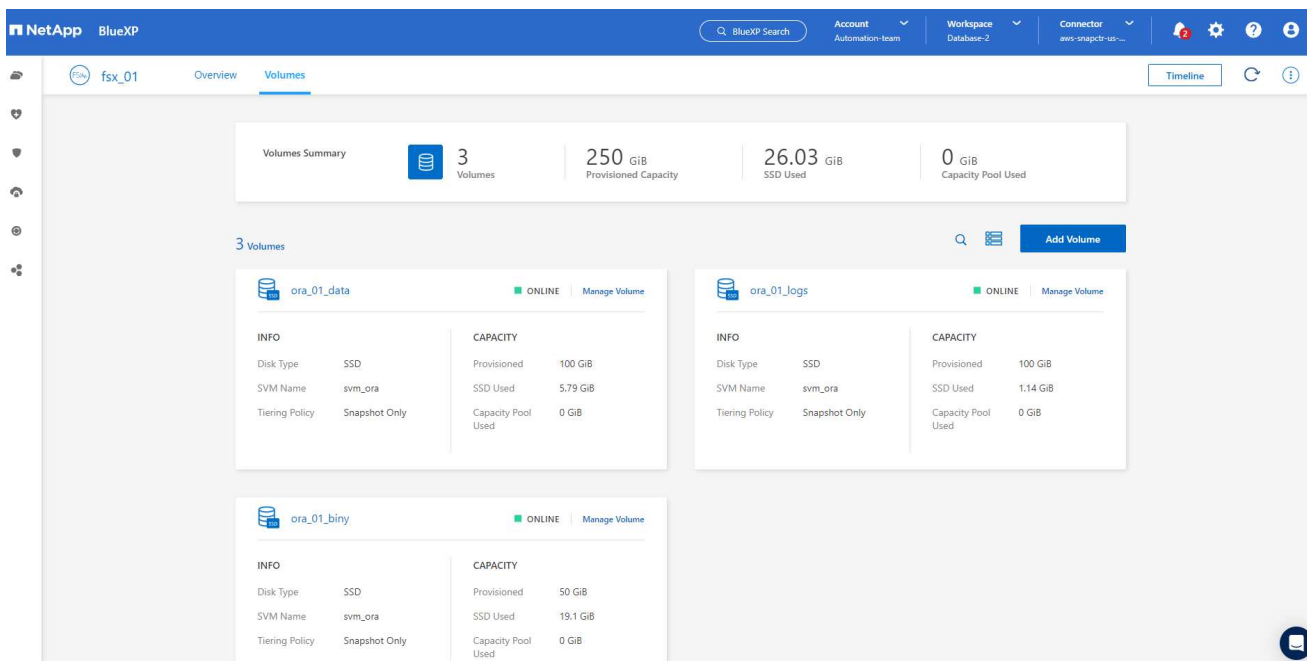
1. L'istanza Amazon FSx ONTAP rilevata ora viene visualizzata nell'ambiente di lavoro.



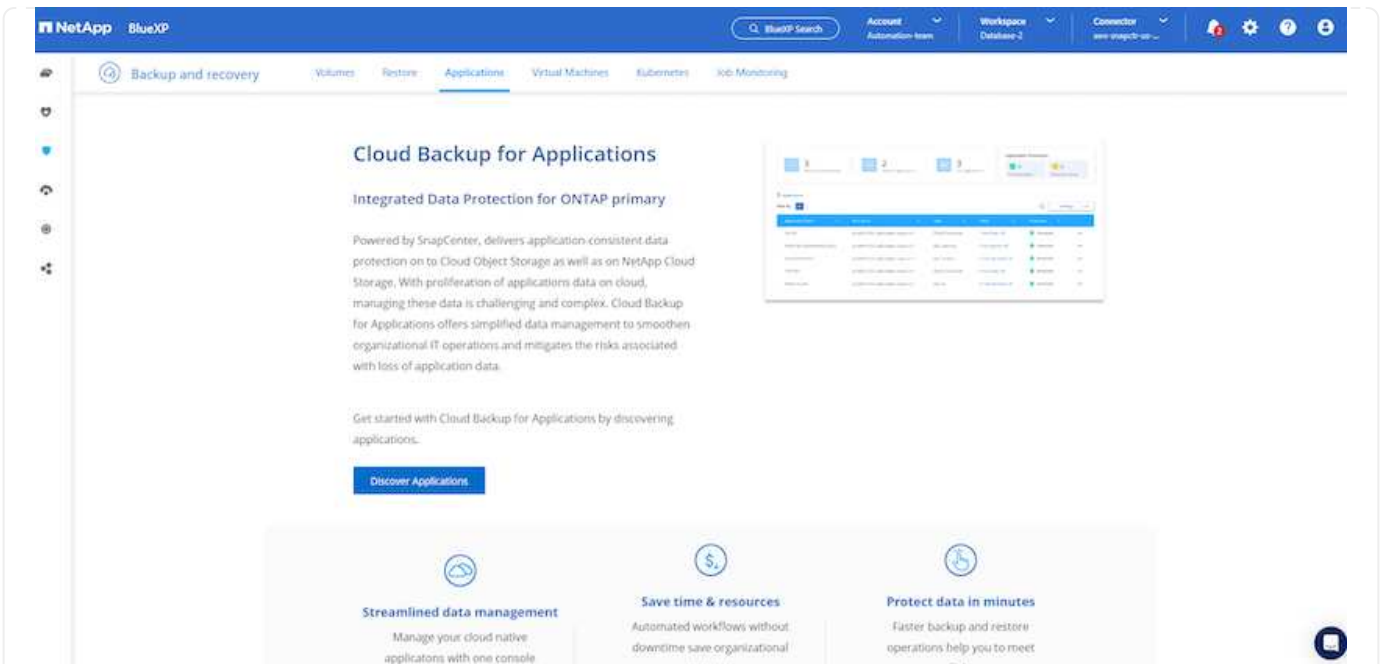
1. Puoi accedere al cluster FSx con le credenziali del tuo account fsxadmin.



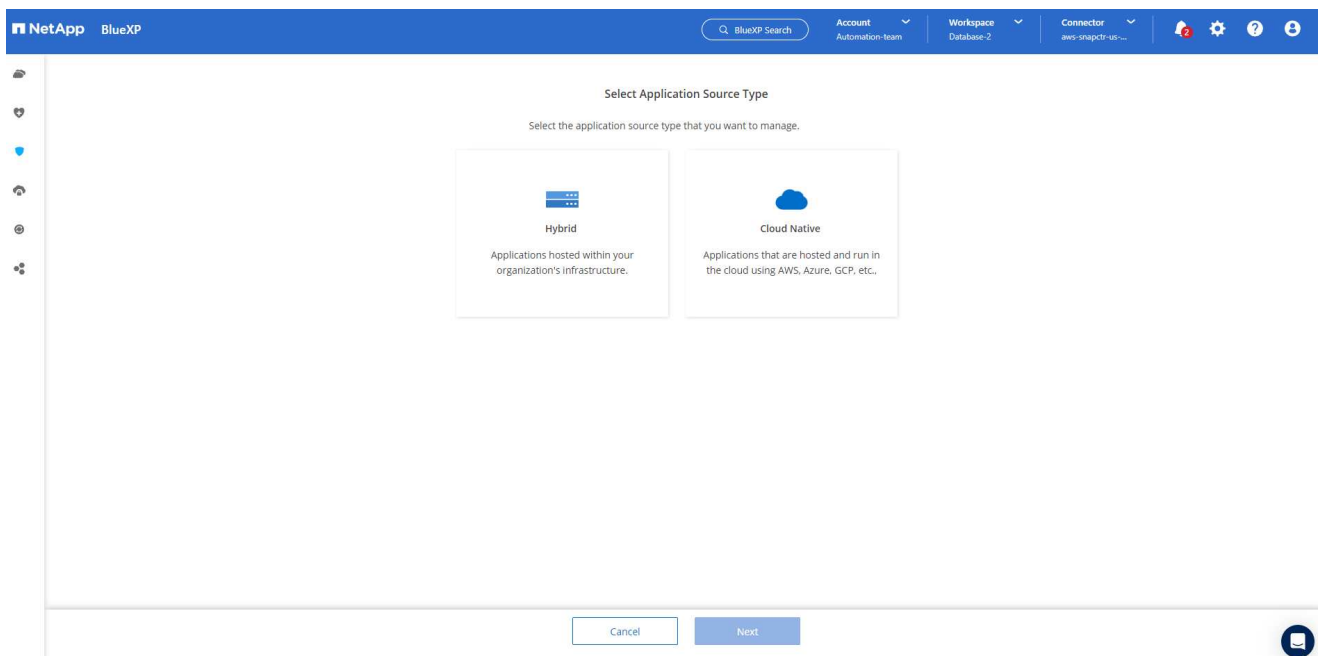
1. Dopo aver effettuato l'accesso ad Amazon FSx ONTAP, rivedi le informazioni di archiviazione del database (ad esempio i volumi del database).



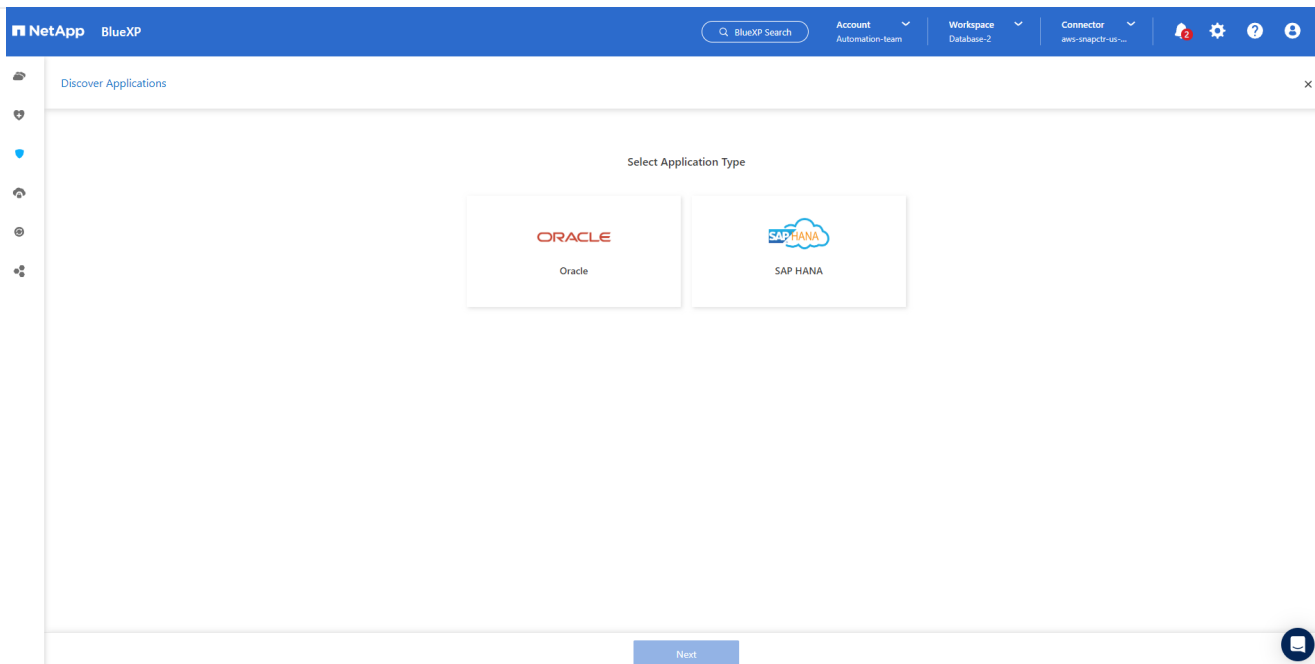
1. Dalla barra laterale sinistra della console, passa il mouse sull'icona di protezione, quindi fai clic su **Protezione > Applicazioni** per aprire la pagina di avvio delle Applicazioni. Fare clic su **Scopri applicazioni**.



1. Selezionare **Cloud Native** come tipo di origine dell'applicazione.

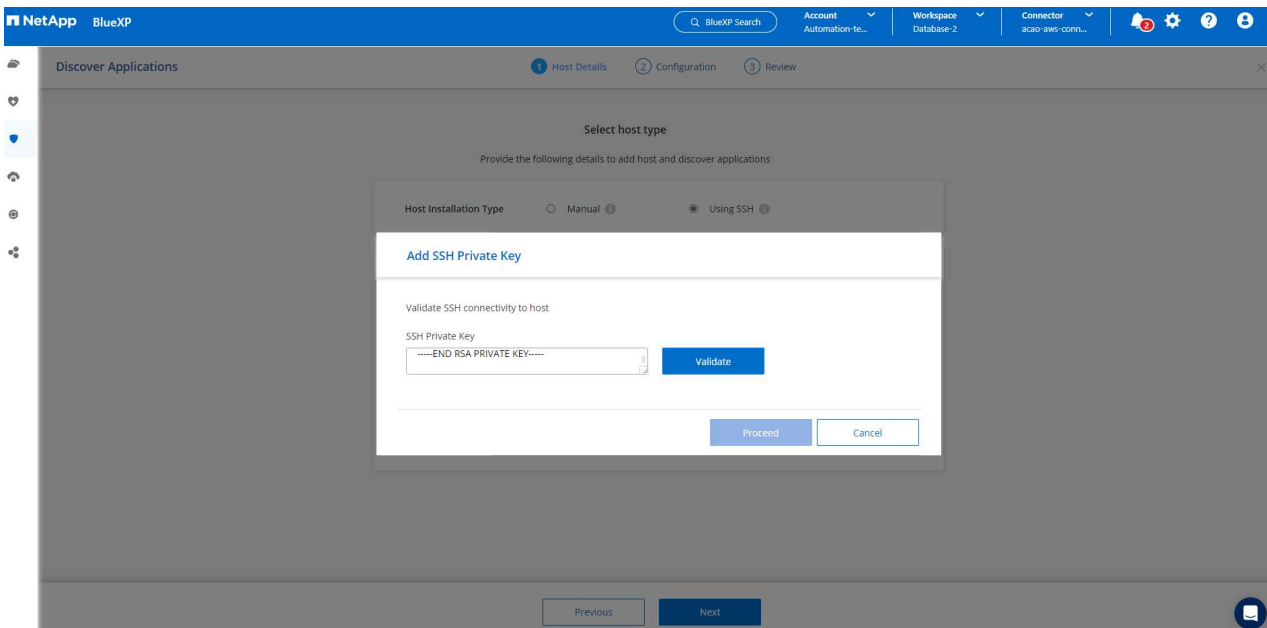


1. Selezionare **Oracle** come tipo di applicazione.

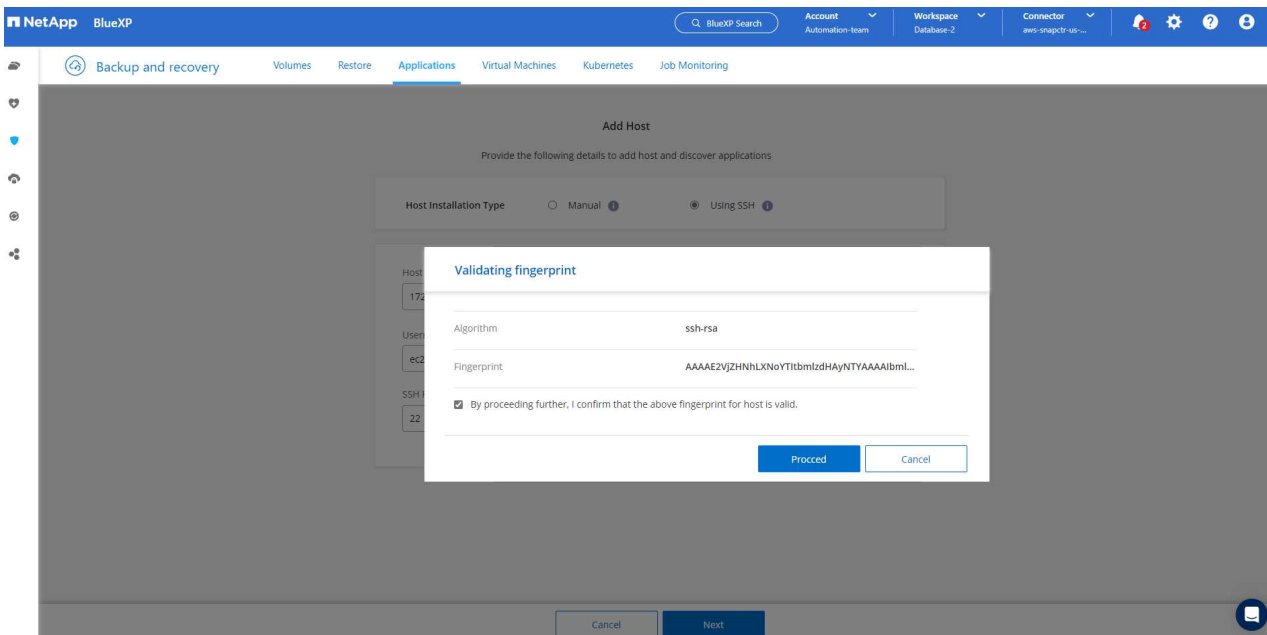


1. Inserisci i dettagli dell'host dell'applicazione Oracle AWS EC2. Seleziona **Utilizzo di SSH** come **Tipo di installazione host** per l'installazione del plugin e la scoperta del database in un unico passaggio. Quindi, fare clic su **Aggiungi chiave privata SSH**.

2. Incolla la tua chiave SSH ec2-user per l'host del database EC2 e fai clic su **Convalida** per procedere.



3. Per procedere, ti verrà richiesto di **Convalidare l'impronta digitale**.



4. Fare clic su **Avanti** per installare un plugin del database Oracle e scoprire i database Oracle sull'host EC2. I database scoperti vengono aggiunti ad **Applicazioni**. Quando viene inizialmente scoperto, lo **Stato di protezione** del database viene visualizzato come **Non protetto**.

The screenshot shows the NetApp BlueXP console interface. At the top, there's a navigation bar with 'NetApp BlueXP' and a search bar. Below it, a secondary navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The main content area is titled 'Cloud Native' and 'Oracle'. It features three summary cards: '1 Hosts' (Cloud Native), '1 ORACLE' (ORACLE), and '0 Clone' (Clone). To the right, an 'Application Protection' summary shows '0 Protected' and '1 Unprotected'. Below this, a section titled '1 Databases' includes a 'Filter By' button and a search bar. A table lists the databases with columns: Name, Host Name, Policy Name, and Protection Status. The table contains one entry: 'db1' with Host Name '172.30.15.58' and Protection Status 'Unprotected'. At the bottom right of the table, it says '1 - 1 of 1' with navigation arrows.

Questa operazione completa la configurazione iniziale dei servizi SnapCenter per Oracle. Le tre sezioni successive di questo documento descrivono le operazioni di backup, ripristino e clonazione del database Oracle.

Backup del database Oracle

1. Fare clic sui tre punti accanto allo **Stato di protezione** del database, quindi fare clic su **Criteri** per visualizzare i criteri di protezione del database precaricati predefiniti che possono essere applicati per proteggere i database Oracle.

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

1. È anche possibile creare una policy personalizzata con una frequenza di backup e una finestra di conservazione dei dati di backup.

The screenshot shows the 'Applications > Policies' page in the NetApp BlueXP interface. It displays a list of predefined policies for Oracle databases. The table has columns: Policy Name, Backup Type, and Schedules and Retention. The policies listed are: 'Oracle Full Backup for Bronze', 'Oracle Full Backup for Gold', 'Oracle Full Backup for Silver', and 'my_full_bkup'. Each policy has a 'FullBackup' type and specific schedules and retention rules. A 'Create Policy' button is visible in the top right corner.

1. Una volta soddisfatti della configurazione della policy, è possibile assegnare la policy desiderata per proteggere il database.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The main content area displays a summary of application protection for 'Cloud Native' and 'Oracle' environments. Below this, a table lists databases, with 'db1' highlighted as 'Unprotected'. A context menu for 'db1' shows options for 'View Details' and 'Assign Policy' (highlighted with a red box).

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

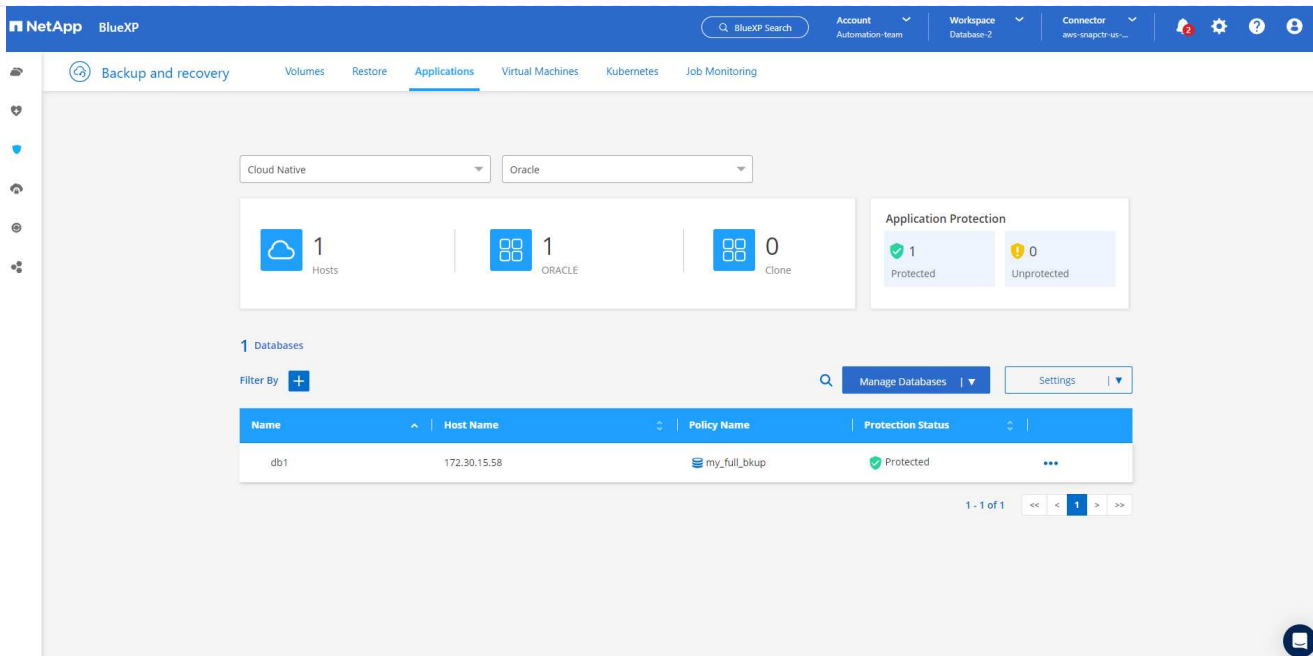
1. Selezionare la policy da assegnare al database.

The screenshot shows the 'Assign Policy' dialog in the NetApp BlueXP interface. The dialog title is 'Assign Policy' with a subtitle 'Assign a policy to start taking backups of the database "db1"'. It displays a list of 4 policies. The policy 'my_full_bkup' is selected with a blue checkmark.

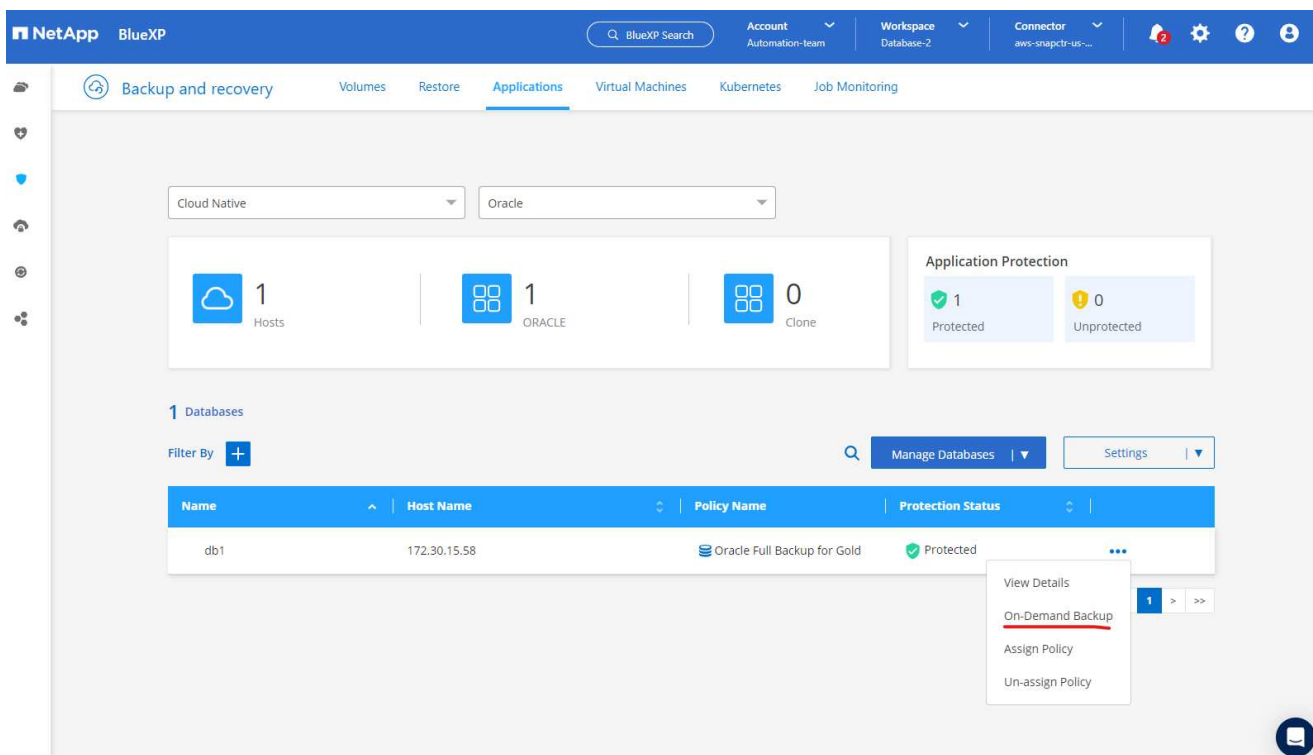
Policy Name	Backup Type	Schedules
Oracle Full Backup for Bronze	FullBackup	Daily: Repeats Every 1 Day, Keeps 14 copies Weekly: Repeats Every Fri, Keeps 4 copies Monthly: Repeats Every 1st Day of Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, C
Oracle Full Backup for Gold	FullBackup	Hourly: Repeats Every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

At the bottom of the dialog are 'Cancel' and 'Assign' buttons.

1. Dopo l'applicazione del criterio, lo stato di protezione del database cambia in **Protetto** con un segno di spunta verde.



1. Il backup del database viene eseguito secondo una pianificazione predefinita. È anche possibile eseguire un backup una tantum su richiesta, come mostrato di seguito.



1. I dettagli dei backup del database possono essere visualizzati facendo clic su **Visualizza dettagli** dall'elenco del menu. Ciò include il nome del backup, il tipo di backup, SCN e la data del backup. Un set di backup comprende uno snapshot sia per il volume dei dati che per il volume del registro. Uno snapshot del volume di registro viene eseguito subito dopo uno snapshot del volume del database. È possibile applicare un filtro se si cerca un backup specifico in un lungo elenco.

NetAppBlueXP

Q BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapctr-us...



Backup and recovery

VolumesRestoreApplicationsVirtual MachinesKubernetesJob Monitoring

Applications > Database Details

Database Details

db1
Database Name

Protected
Protection

Oracle Full Backup for Gold
Policy Names

Database Type

172.30.15.58
Host Name

FSx
Host Storage

Unreachable
Database Version

bKed8yv2T19Bj0V5QyqvA...
Agent Id

-
Clones

-
Parent Database

8 Backups

Filter By 

 Select Timeframe ▼

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

Ripristino e recupero del database Oracle

1. Per il ripristino di un database, scegliere il backup corretto, in base all'SCN o all'ora del backup. Fare clic sui tre puntini dal backup dei dati del database, quindi fare clic su **Ripristina** per avviare il ripristino e il recupero del database.

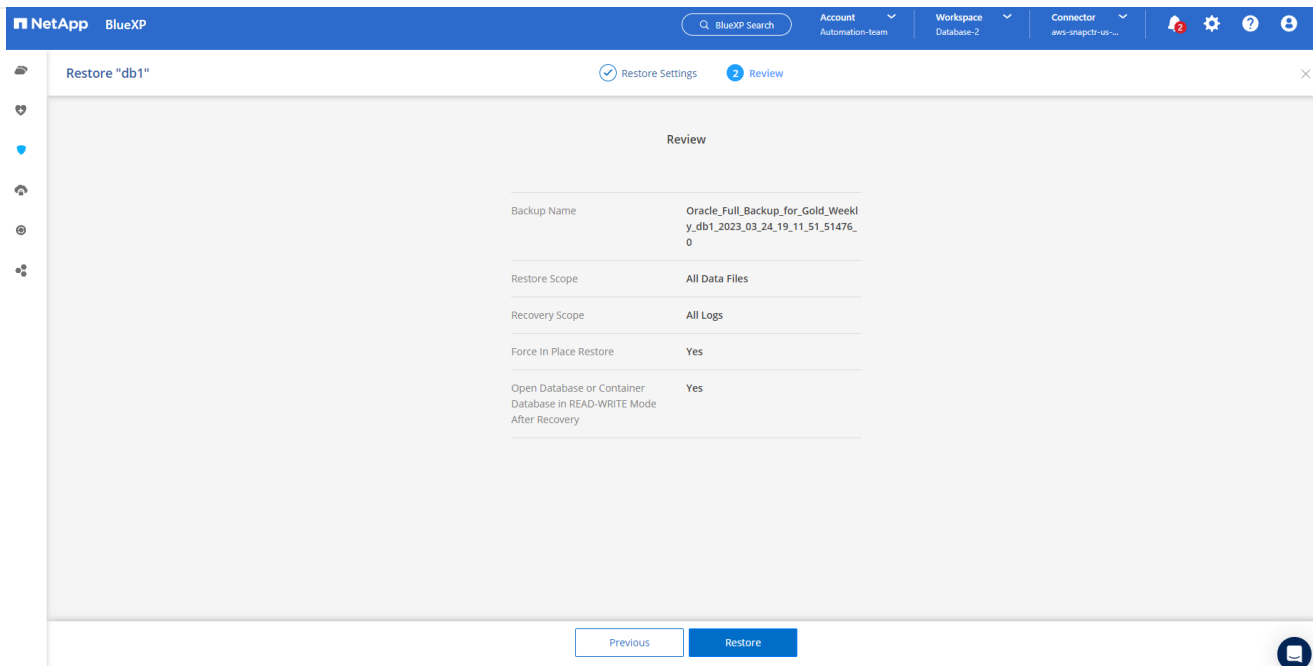
The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' tab is selected, leading to 'Database Details' for a database named 'db1'. Below the 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

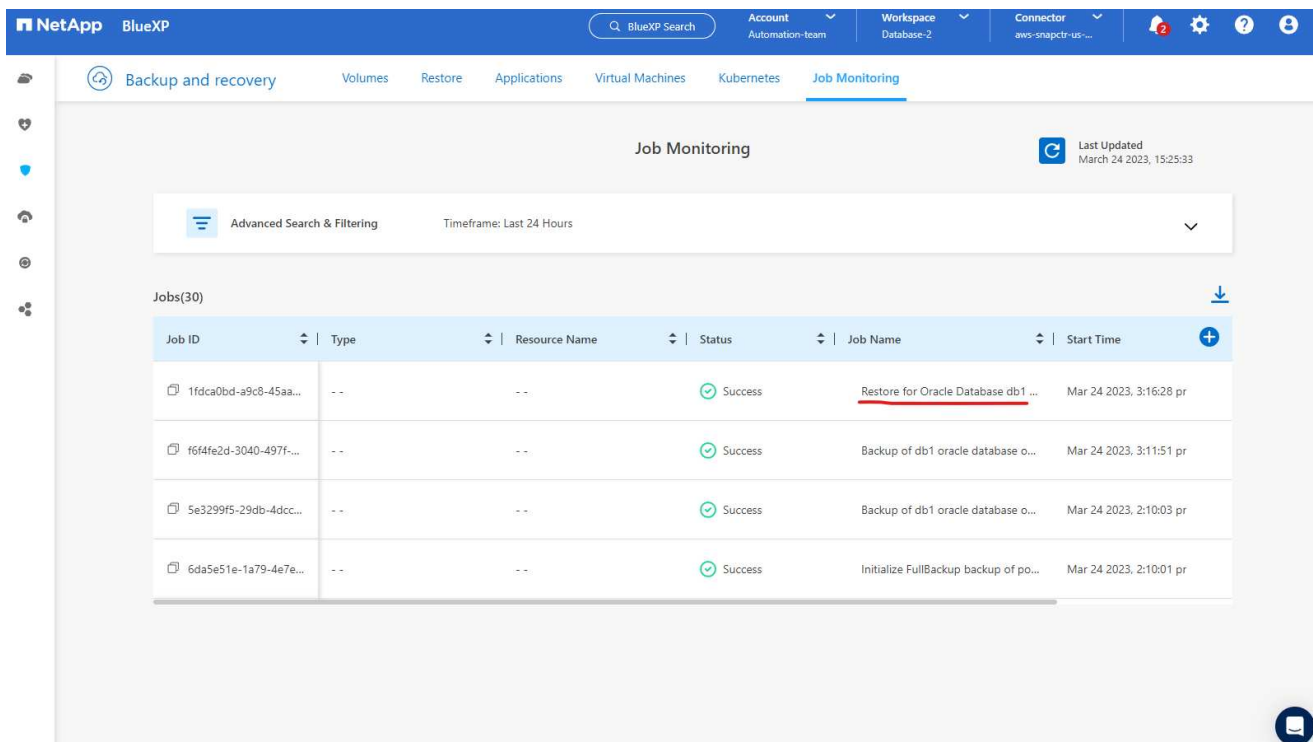
1. Scegli le impostazioni di ripristino. Se si è certi che non è cambiato nulla nella struttura fisica del database dopo il backup (ad esempio l'aggiunta di un file di dati o di un gruppo di dischi), è possibile utilizzare l'opzione **Forza ripristino sul posto**, che in genere è più rapida. In caso contrario, non selezionare questa casella.

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 'Next' button is highlighted.

1. Esaminare e avviare il ripristino e il recupero del database.



1. Dalla scheda **Monitoraggio processi** è possibile visualizzare lo stato del processo di ripristino e tutti i dettagli durante l'esecuzione.



NetAppBlueXP

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

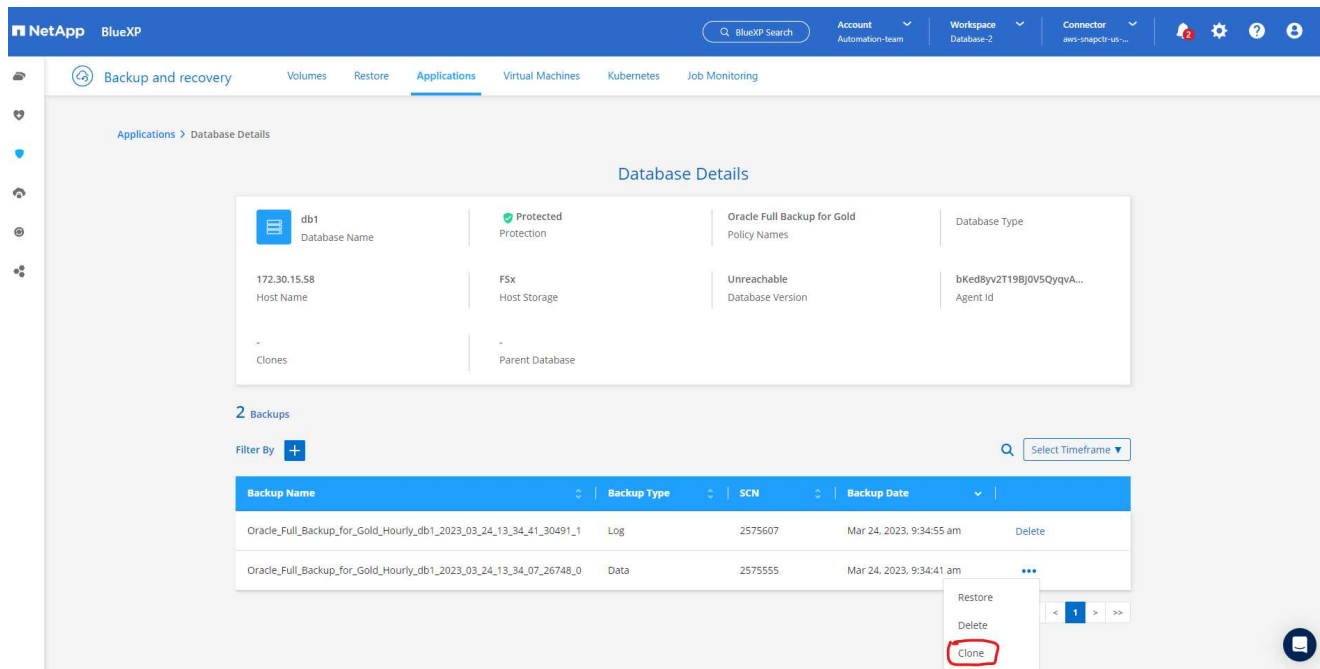
Sub-Jobs(6)

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

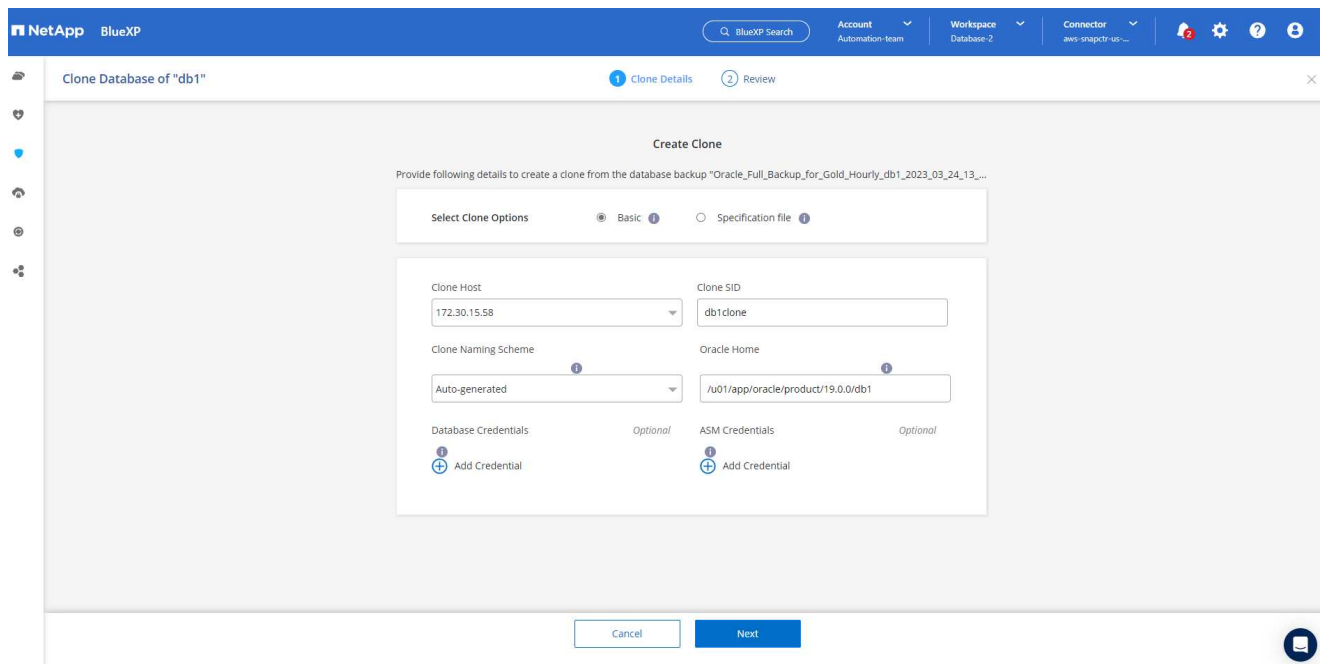
Clone del database Oracle

Per clonare un database, avviare il flusso di lavoro di clonazione dalla stessa pagina dei dettagli del backup del database.

1. Seleziona la copia di backup del database corretta, clicca sui tre punti per visualizzare il menu e scegli l'opzione **Clona**.



1. Selezionare l'opzione **Base** se non è necessario modificare alcun parametro del database clonato.



1. In alternativa, seleziona **File di specifiche**, che ti dà la possibilità di scaricare il file init corrente, apportare modifiche e quindi caricarlo nuovamente nel lavoro.

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. Rivedi e avvia il lavoro.

NetApp BlueXP

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/redolog/redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redolog/redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redolog/redo03_01.log
Recovery scope	Until cancel using selected backup's archive logs

Previous

Clone

1. Monitorare lo stato del processo di clonazione dalla scheda **Monitoraggio processo**.

33

NetAppBlueXP

BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapc1r-18-...

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. Convalidare il database clonato sull'host dell'istanza 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/oracle/product/19.0.0/db1,STABLE
ora.db1clone.db
      1        ONLINE  ONLINE      ip-172-30-15-58          Open,HOME=/u01/app/oracle/product/19.0.0/db1,STABLE
ora.diskmon
      1        OFFLINE OFFLINE                        STABLE
ora.driver.afd
      1        ONLINE  ONLINE      ip-172-30-15-58          STABLE
ora.evmd
      1        ONLINE  ONLINE      ip-172-30-15-58          STABLE
-----
[oracle@ip-172-30-15-58 ~]$
```

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

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

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

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

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

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

```
SQL>
```

Informazioni aggiuntive

Per saperne di più sulle informazioni descritte nel presente documento, consultare i seguenti documenti e/o siti web:

- Configurare e amministrare 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)

- Documentazione 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

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.