



TR-4964: SnapCenterサービスを使用した Oracle データベースのバックアップ、リストア、クロー ン作成 - **AWS**

NetApp database solutions

NetApp
August 18, 2025

目次

TR-4964: SnapCenterサービスを使用した Oracle データベースのバックアップ、リストア、クローン作成

- AWS	1
目的	1
観客	1
ソリューションのテストおよび検証環境	1
アーキテクチャ	2
ハードウェアおよびソフトウェアコンポーネント	2
導入検討の重要な要素	3
ソリューションの展開	3
SnapCenterサービスの展開の前提条件	3
BlueXPへのオンボーディングの準備	4
SnapCenterサービス用のコネクタを展開する	5
BlueXPでAWSリソースへのアクセスのための認証情報を定義する	12
SnapCenterサービスのセットアップ	16
Oracleデータベースのバックアップ	24
Oracleデータベースの復元と回復	28
Oracle データベースクローン	31
追加情報	36

TR-4964: SnapCenterサービスを使用した Oracle データベースのバックアップ、リストア、クローン作成 - AWS

このソリューションでは、Azure クラウドのBlueXPコンソールを使用して、NetApp SnapCenter SaaS を使用した Oracle データベースのバックアップ、復元、クローン作成の概要と詳細を説明します。

アレン・カオ、ニヤズ・モハメド、NetApp

目的

SnapCenterサービスは、NetApp BlueXPクラウド管理コンソールを通じて利用できる従来のSnapCenterデータベース管理 UI ツールの SaaS バージョンです。これは、NetAppクラウド ストレージ上で実行される Oracle や HANA などのデータベース向けのNetAppクラウド バックアップおよびデータ保護サービスの不可欠な部分です。この SaaS ベースのサービスは、通常 Windows ドメイン環境で動作する Windows サーバーを必要とする従来のSnapCenterスタンドアロン サーバーの展開を簡素化します。

このドキュメントでは、Amazon FSx ONTAPストレージおよび EC2 コンピューティングインスタンスにデプロイされた Oracle データベースをバックアップ、復元、およびクローンするようにSnapCenterサービスを設定する方法を説明します。セットアップと使用がはるかに簡単ですが、SnapCenterサービスは、従来のSnapCenter UI ツールで利用できる主要な機能を提供します。

このソリューションは、次のユースケースに対応します。

- Amazon FSx ONTAPでホストされている Oracle データベースのスナップショットを使用したデータベースバックアップ
- 障害発生時のOracleデータベースのリカバリ
- 開発/テスト環境やその他のユースケース向けのプライマリ データベースの高速かつストレージ効率の高いクローン作成

観客

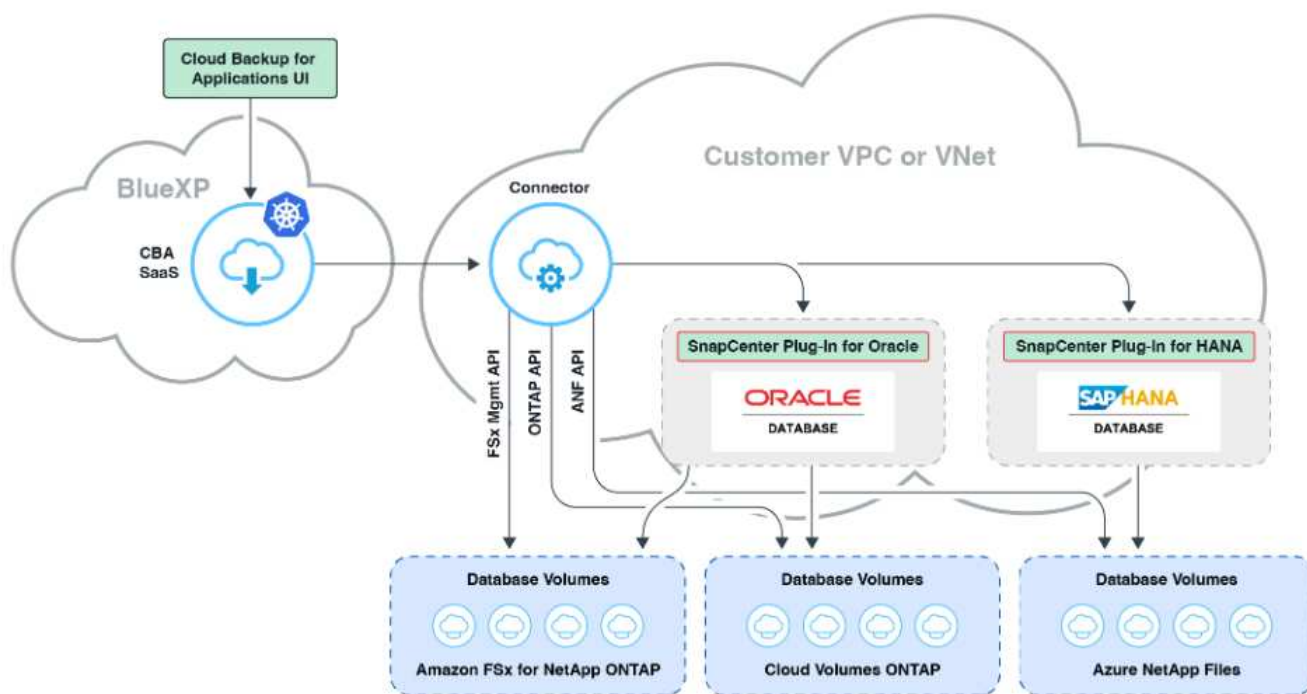
このソリューションは、次の対象者を対象としています。

- Amazon FSx ONTAPストレージ上で実行される Oracle データベースを管理する DBA
- パブリック AWS クラウドで Oracle データベースのバックアップ、リストア、クローンをテストすることに関心のあるソリューション アーキテクト
- Amazon FSx ONTAPストレージをサポートおよび管理するストレージ管理者
- Amazon FSx ONTAPストレージにデプロイされたアプリケーションを所有するアプリケーション所有者

ソリューションのテストおよび検証環境

このソリューションのテストと検証は、最終的な展開環境と一致しない可能性のある AWS FSx および EC2 環境で実行されました。詳細については、セクションをご覧ください。 [\[導入検討の重要な要素\]](#)。

アーキテクチャ



この画像は、UI、コネクタ、管理するリソースなど、BlueXPコンソール内のアプリケーションのBlueXP backup and recoveryの詳細を示しています。

ハードウェアおよびソフトウェアコンポーネント

ハードウェア

FSx ONTAPストレージ	AWSが提供する現在のバージョン	同じ VPC およびアベイラビリティゾーン内の 1 つの FSx HA クラスター
コンピューティング用のEC2インスタンス	t2.xlarge/4vCPU/16G	2 つの EC2 T2 xlarge EC2 インスタンス (1 つはプライマリ DB サーバー、もう 1 つはクローン DB サーバー)

ソフトウェア

レッドハットリナックス	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	テスト用にRedHatサブスクリプションを導入
Oracle グリッド・インフラストラクチャ	バージョン19.18	RUパッチp34762026_190000_Linux-x86-64.zipを適用しました
Oracle Database	バージョン19.18	RUパッチp34765931_190000_Linux-x86-64.zipを適用しました

Oracle OPatch	バージョン 12.2.0.1.36	最新パッチ p6880880_190000_Linux-x86-64.zip
SnapCenterサービス	version	v2.3.1.2324

導入検討の重要な要素

- *コネクタはデータベースおよび FSx と同じ VPC にデプロイされます。*可能であれば、コネクタを同じ AWS VPC にデプロイして、FSx ストレージと EC2 コンピューティングインスタンスへの接続を可能にする必要があります。
- * SnapCenterコネクタ用に作成された AWS IAM ポリシー。* JSON 形式のポリシーは、詳細なSnapCenterサービス ドキュメントで入手できます。 BlueXPコンソールを使用してコネクタのデプロイメントを開始すると、必要な権限の詳細を JSON 形式で入力して前提条件を設定するように求められます。ポリシーは、コネクタを所有する AWS ユーザーアカウントに割り当てる必要があります。
- **AWS** アカウントアクセスキーと **AWS** アカウントで作成された **SSH** キーペア。SSH キー ペアは、コネクタ ホストにログインし、EC2 DB サーバー ホストにデータベース プラグインをデプロイするために ec2-user に割り当てられます。アクセス キーは、上記の IAM ポリシーを使用して必要なコネクタをプロビジョニングするための権限を付与します。
- * BlueXPコンソール設定に資格情報が追加されました。* Amazon FSx ONTAP をBlueXP作業環境に追加するには、BlueXPコンソール設定で、Amazon FSx ONTAPにアクセスするための権限をBlueXP に付与する認証情報を設定します。
- **EC2** データベース インスタンス ホストに **java-11-openjdk** がインストールされています。 SnapCenter サービスのインストールには Java バージョン 11 が必要です。プラグインのデプロイメントを試みる前に、アプリケーション ホストにインストールする必要があります。

ソリューションの展開

クラウドネイティブ アプリケーション データの保護に役立つ、より広範な範囲を網羅したNetAppドキュメントが用意されています。このドキュメントの目的は、Amazon FSx ONTAPおよび EC2 コンピューティングインスタンスにデプロイされた Oracle データベースを保護するために、BlueXPコンソールを使用してSnapCenterサービスのデプロイに関する手順を段階的に提供することです。このドキュメントでは、より一般的な手順では不足している可能性のある特定の詳細について説明します。

開始するには、次の手順を実行します。

- 一般的な指示を読む["クラウドネイティブアプリケーションのデータを保護する"](#)Oracle およびAmazon FSx ONTAPに関連するセクション。
- 次のビデオウォークスルーをご覧ください。

ソリューションの展開

SnapCenterサービスの展開の前提条件

展開には次の前提条件が必要です。

1. Oracle データベースが完全にデプロイされ、実行されている EC2 インスタンス上のプライマリ Oracle データベース サーバー。
2. 上記のデータベースボリュームをホストしている AWS にデプロイされた Amazon FSx ONTAP クラスター。
3. 開発/テストのワークロードをサポートする目的で、または本番環境の Oracle データベースの完全なデータセットを必要とするユースケースをサポートする目的で、Oracle データベースのクローンを代替ホストにテストするために使用できる、EC2 インスタンス上のオプションのデータベース サーバー。
4. Amazon FSx ONTAP および EC2 コンピューティング インスタンスでの Oracle データベースのデプロイメントに関する上記の前提条件を満たすためにサポートが必要な場合は、以下を参照してください。["AWS FSx/EC2 における iSCSI/ASM を使用した Oracle データベースのデプロイメントと保護"](#) またはホワイトペーパー ["EC2 および FSx での Oracle データベースのデプロイメントのベストプラクティス"](#)

BlueXP へのオンボーディングの準備

1. リンクを使用してください"[NetAppBlueXP](#)"BlueXPコンソール アクセスにサインアップします。
2. AWS アカウントにログインして、適切な権限を持つ IAM ポリシーを作成し、BlueXPコネクタのデプロイメントに使用する AWS アカウントにポリシーを割り当てます。

The screenshot shows the AWS IAM console interface. On the left is the 'Identity and Access Management (IAM)' sidebar with various navigation options. The main content area displays the 'Summary' for a policy named 'snapcenter'. The policy's ARN is 'arn:aws:iam::541696183547:policy/snapcenter' and its description is 'Policy to grant snapcenter service permission to create connector in AWS.' Below this, there are tabs for 'Permissions', 'Policy usage', 'Tags', 'Policy versions', and 'Access Advisor'. The 'Permissions' tab is active, showing a 'Policy summary' and a 'JSON' view. The JSON view displays the policy document, which grants 'Allow' permissions for a list of IAM and EC2 actions.

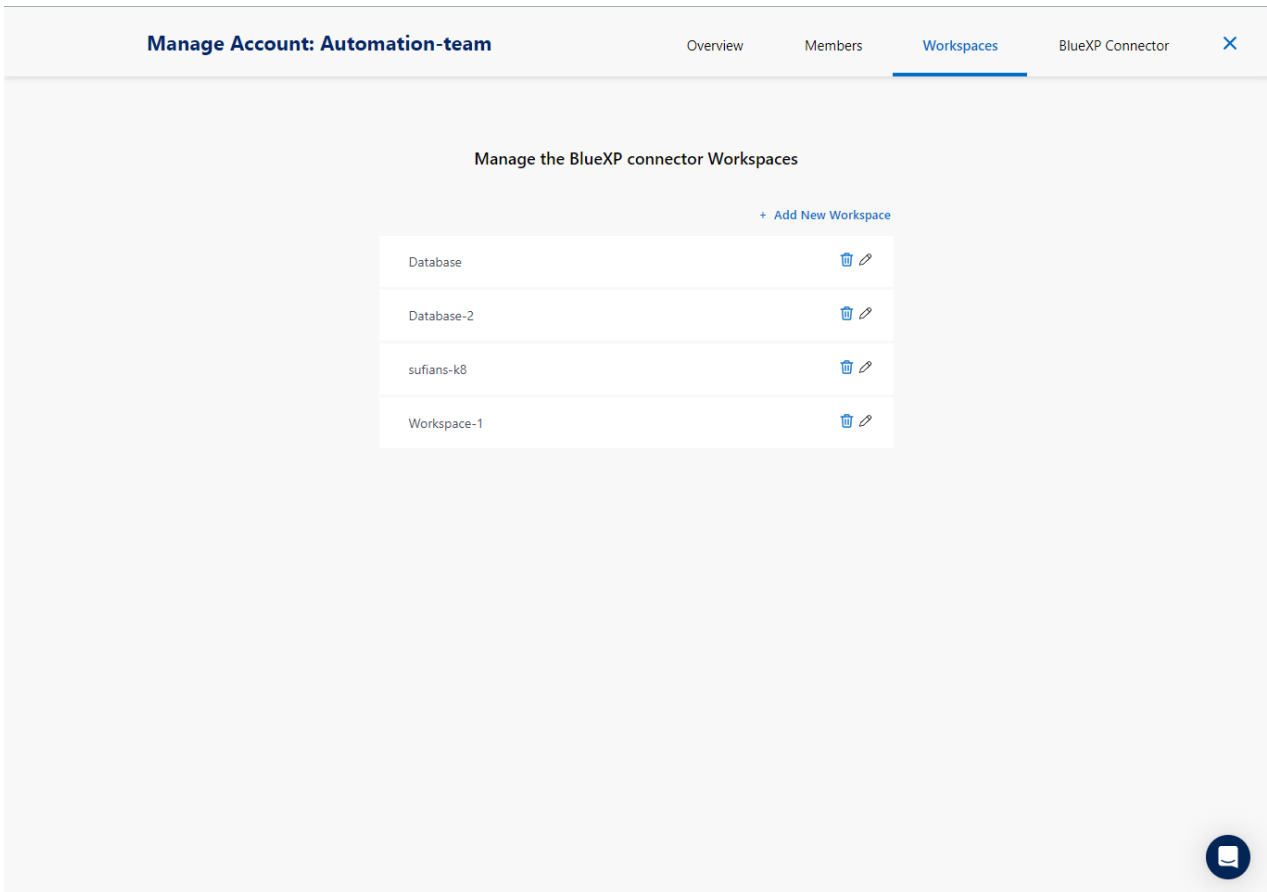
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:CreateRole",
8         "iam:DeleteRole",
9         "iam:PutRolePolicy",
10        "iam:CreateInstanceProfile",
11        "iam:DeleteRolePolicy",
12        "iam:AddRoleToInstanceProfile",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

ポリシーは、NetApp のドキュメントに記載されている JSON 文字列を使用して構成する必要があります。コネクタのプロビジョニングが起動され、前提条件のアクセス許可の割り当てを求めるプロンプトが表示されたときに、JSON 文字列をページから取得することもできます。

3. また、コネクタのプロビジョニングに備えて、AWS VPC、サブネット、セキュリティグループ、AWS ユーザーアカウントのアクセスキーとシークレット、ec2-user の SSH キーなども準備しておく必要があります。

SnapCenterサービス用のコネクタを展開する

1. BlueXPコンソールにログインします。共有アカウントの場合は、[アカウント]>[アカウントの管理]>[ワークスペース] をクリックして新しいワークスペースを追加し、個別のワークスペースを作成するのがベストプラクティスです。



2. コネクタの追加 をクリックして、コネクタのプロビジョニング ワークフローを起動します。

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. クラウド プロバイダー (この場合は **Amazon Web Services**) を選択します。

Add Connector

Provider

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

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

[Continue](#)

1. AWS アカウントで既に 権限、認証、および ネットワーク の手順が設定されている場合は、これらの手順をスキップしてください。そうでない場合は、続行する前にこれらを設定する必要があります。ここから、前のセクションで参照したAWSポリシーの権限を取得することもできます。[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. *アクセスキー*と*シークレットキー*を使用して AWS アカウント認証を入力します。

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

AWS Authentication

Region

us-east-1 | US East (N. Virginia) ▼

Select the Authentication Method: ☐ Assume Role ☒ AWS Keys

AWS Access Key

AKIA6JRXA6ZVGVF5HMO3

AWS Secret Key

.....

Want to launch an instance without AWS Credentials? ▼

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

2. コネクタ インスタンスに名前を付け、[詳細] の下にある [ロールの作成] を選択します。

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

Details

Connector Instance Name ⓘ

SnapCenterSvs

Connector Role ⓘ

☒ Create Role ☐ Select an existing Role

Role Name

Cloud-Manager-Operator-VZzSSP9-SnapCenter

[+](#) Add Tags to Connector Instance☐ AWS Managed Encryption ⓘ

Master Key: aws/ebs (default)

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

1. コネクタ アクセス用の適切な **VPC**、サブネット、および SSH キー ペア を使用してネットワークを構成します。

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. コネクタの*セキュリティ グループ*を設定します。

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

- 概要ページを確認し、「追加」をクリックしてコネクタの作成を開始します。通常、デプロイが完了するまでに約 10 分かかります。完了すると、コネクタインスタンスが AWS EC2 ダッシュボードに表示されます。

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

BlueXPで**AWS**リソースへのアクセスのための認証情報を定義する

1. まず、AWS EC2 コンソールから、**Identity and Access Management (IAM)** メニューの ロール、ロールの作成 でロールを作成し、ロール作成ワークフローを開始します。

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

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

Access reports

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

Related consoles

- IAM Identity Center
- AWS Organizations

IAM > Roles

Roles (106) [aws](#)

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
☐ AmazonEC2RoleforLaunchWizard	AWS Service: ec2	-
☐ AmazonSSMRoleforInstancesQuickSetup	AWS Service: ec2	156 days ago
☐ aws-controltower-AdministratorExecutionRole	Account: 982617961887	-
☐ aws-controltower-ConfigRecorderRole	AWS Service: config	-
☐ aws-controltower-ForwardInstanceNotificationRole	AWS Service: lambda	2 days ago
☐ aws-controltower-ReadOnlyExecutionRole	Account: 982617961887	-
☐ aws-QuickSetup-StackSet-Local-AdministrationRole	AWS Service: cloudformation	154 days ago
☐ AWSQuickSetup-StackSet-Local-ExecutionRole	Account: 541696183547	154 days ago
☐ AWSControlTowerExecution	Account: 292306980405	232 days ago
☐ AWSReservedSSO_AWSAdministratorAccess_3d8eb65a690827fa	Identity Provider: arn:aws:iam:541696183547:saml-provider/AWSSSO_91b222f38b25f441_DO_NOT_DELETE	26 days ago
☐ AWSReservedSSO_AWSOrganizationalAccess_f6c3be705667ed53	Identity Provider: arn:aws:iam:541696183547:saml-provider/AWSSSO_91b222f38b25f441_DO_NOT_DELETE	-
☐ AWSReservedSSO_AWSPowerUserAccess_5a9f0a0f5a40ed1	Identity Provider: arn:aws:iam:541696183547:saml-provider/AWSSSO_91b222f38b25f441_DO_NOT_DELETE	-
☐ AWSReservedSSO_AWSReadOnlyAccess_23a346f51e1bb118	Identity Provider: arn:aws:iam:541696183547:saml-provider/AWSSSO_91b222f38b25f441_DO_NOT_DELETE	-
☐ AWSReservedSSO_SAA-DevReadOnly_Ibfef1a6083e815e7	Identity Provider: arn:aws:iam:541696183547:saml-provider/AWSSSO_91b222f38b25f441_DO_NOT_DELETE	-

2. 信頼できるエンティティの選択*ページで、*AWS アカウント、*別の AWS アカウント*を選択し、BlueXPコンソールから取得できるBlueXPアカウント ID を貼り付けます。

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity [info](#)

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. 権限ポリシーを fsx でフィルタリングし、権限ポリシー をロールに追加します。

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. *ロールの詳細*ページで、ロールに名前を付け、説明を追加して、*ロールの作成*をクリックします。

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

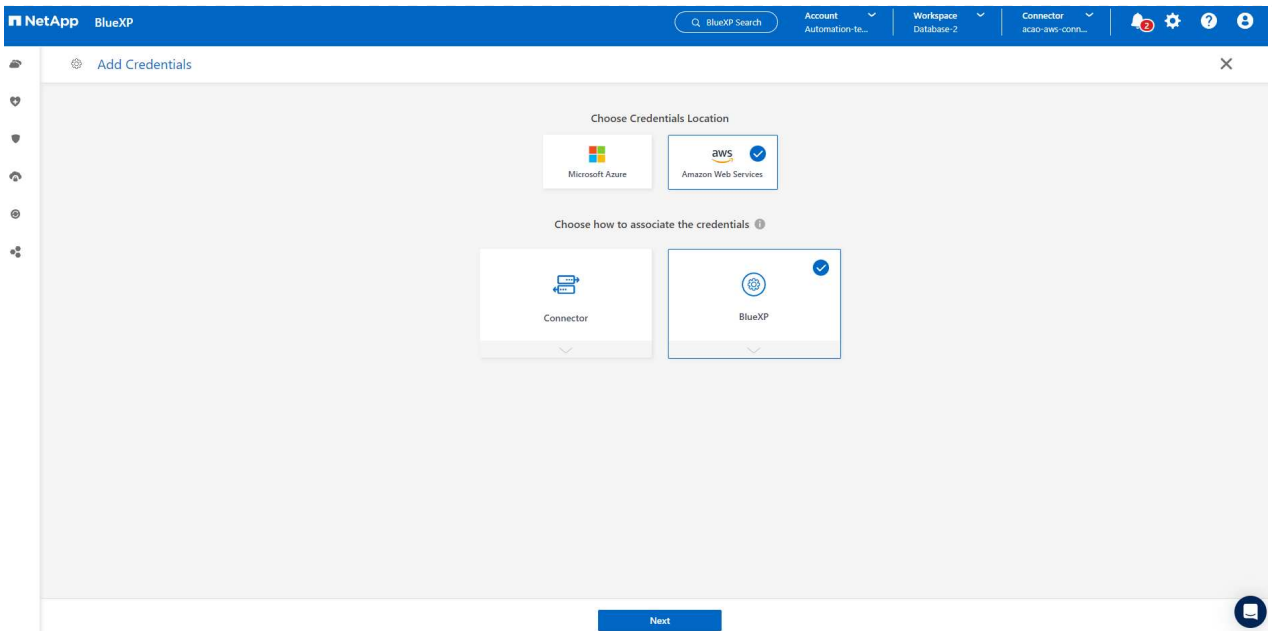
[Edit](#)

```

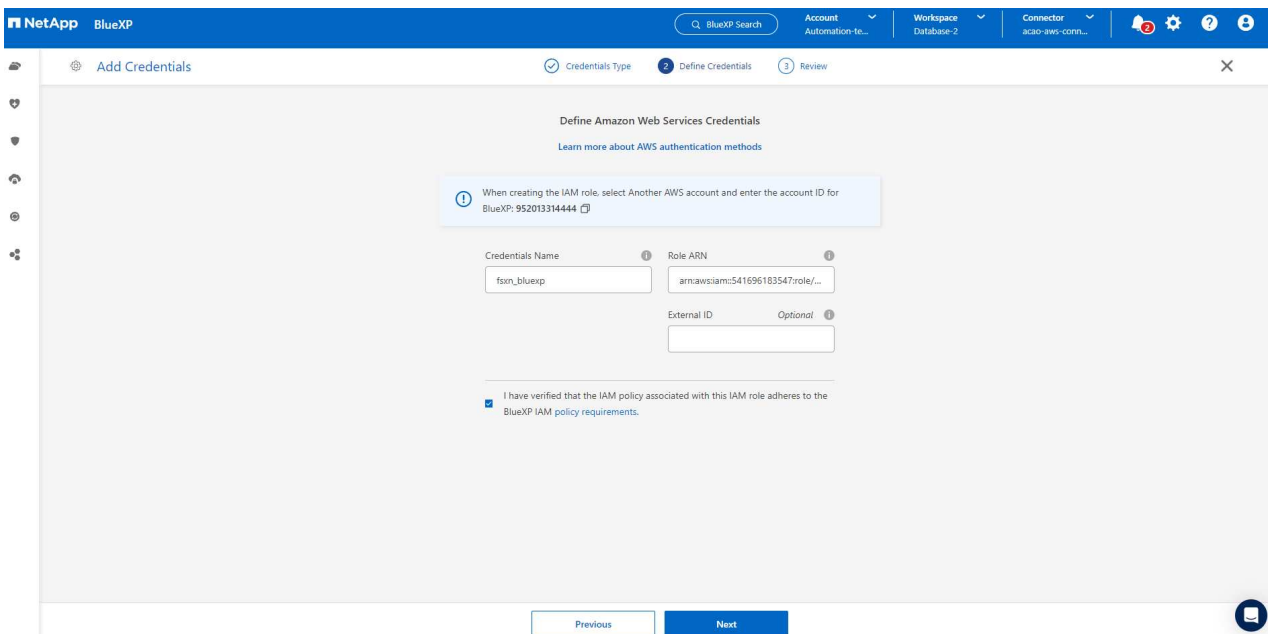
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "sts:AssumeRole",
7       "Principal": {
8         "AWS": "952013314444"
9       },
10      "Condition": {}
11    }
12  ]
13 }
```

5. BlueXPコンソールに戻り、コンソールの右上隅にある設定アイコンをクリックして アカウント資格情報 ページを開き、資格情報の追加 をクリックして資格情報構成ワークフローを開始します。

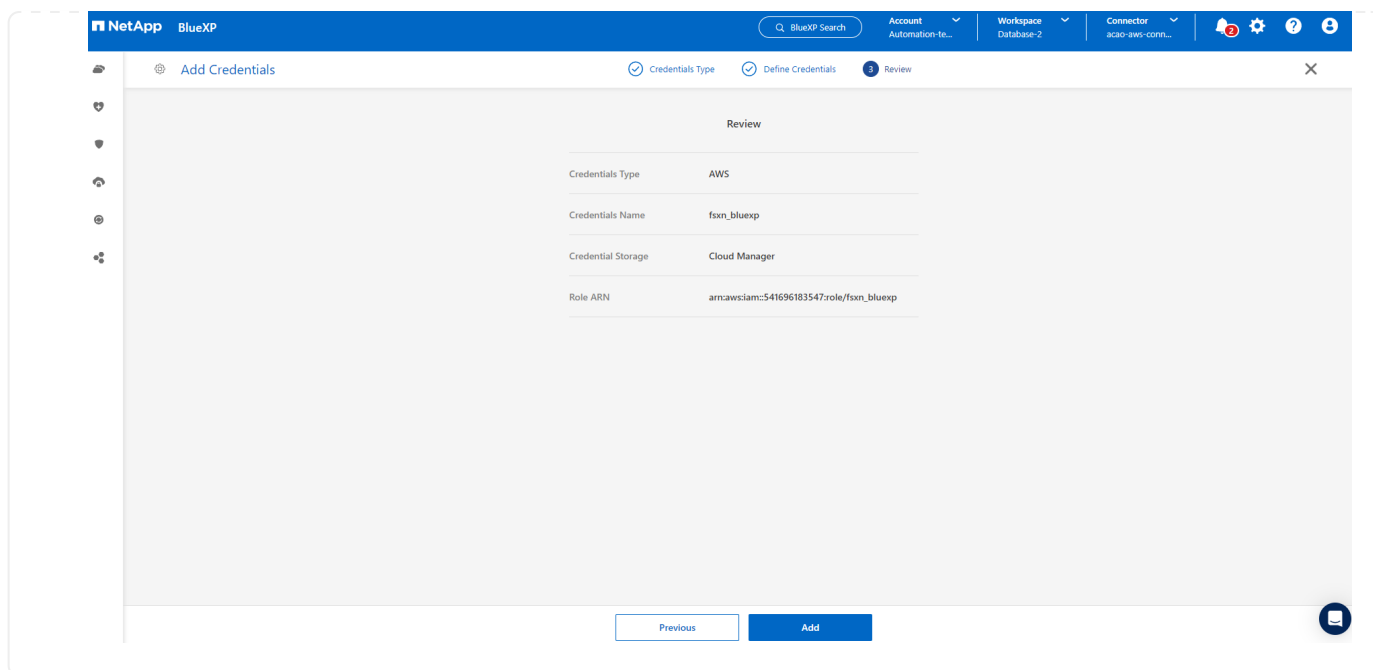
6. 資格情報の場所として **Amazon Web Services - BlueXP** を選択します。



7. 上記の手順 1 で作成した AWS IAM ロールから取得できる適切な ロール **ARN** を使用して AWS 認証情報を定義します。BlueXP アカウント **ID**。ステップ 1 で AWS IAM ロールを作成するために使用されます。



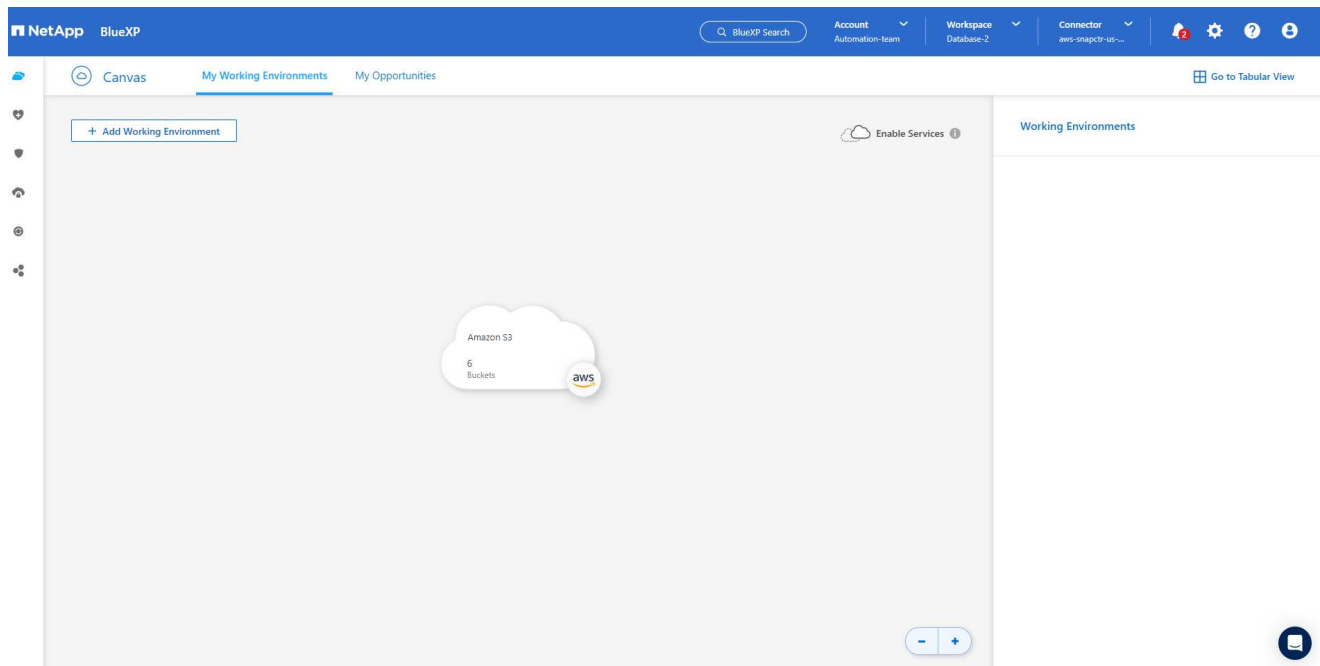
8. 確認して*追加*します。



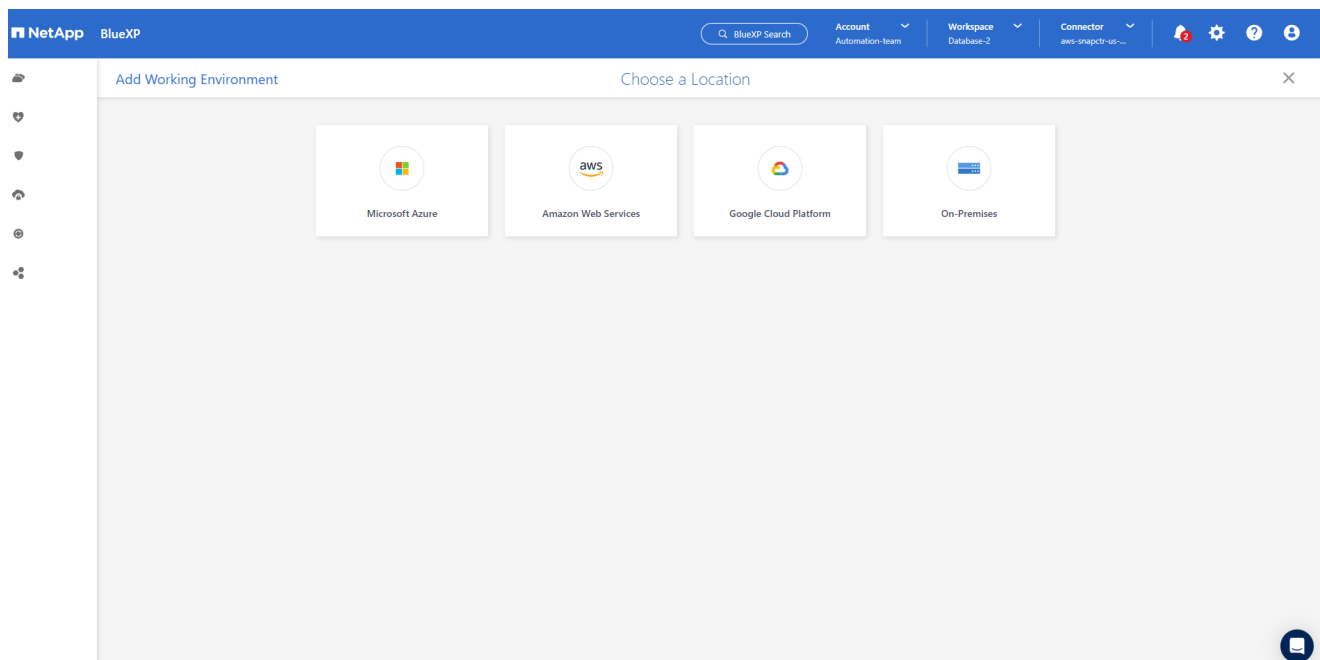
SnapCenterサービスのセットアップ

コネクタがデプロイされ、資格情報が追加されたら、次の手順でSnapCenterサービスを設定できるようになります。

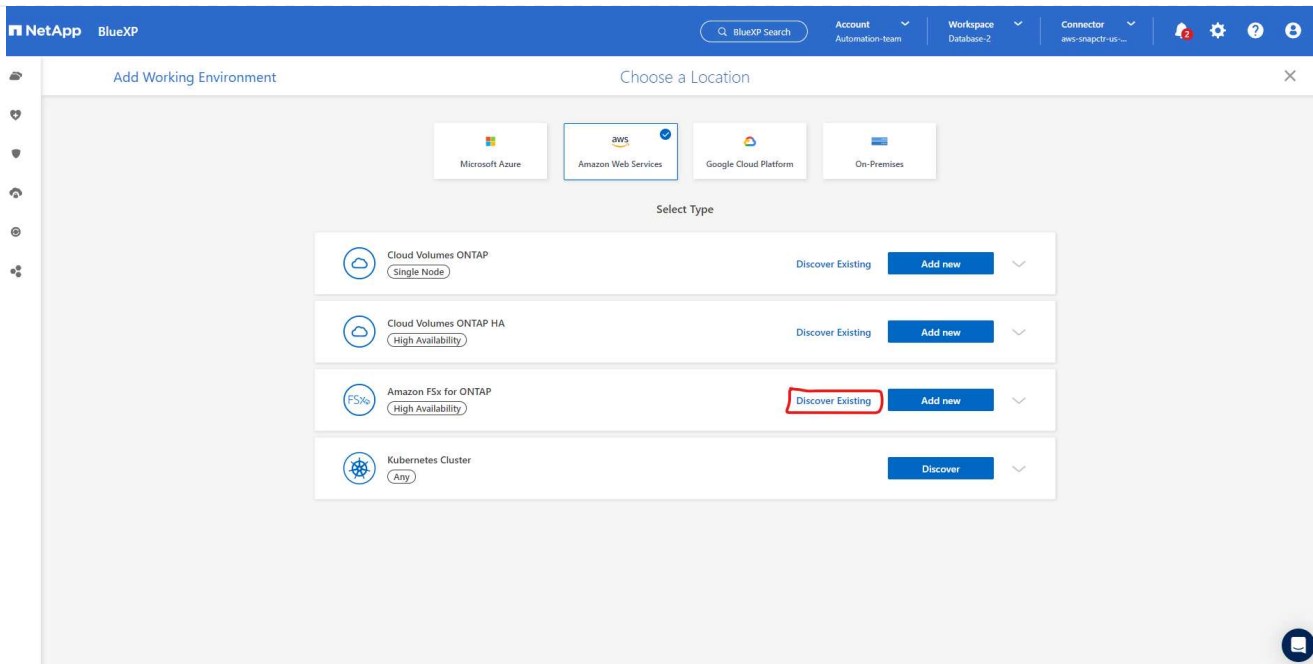
1. **My Working Environment** から **Add working Environment** をクリックして、AWS にデプロイされた FSx を検出します。



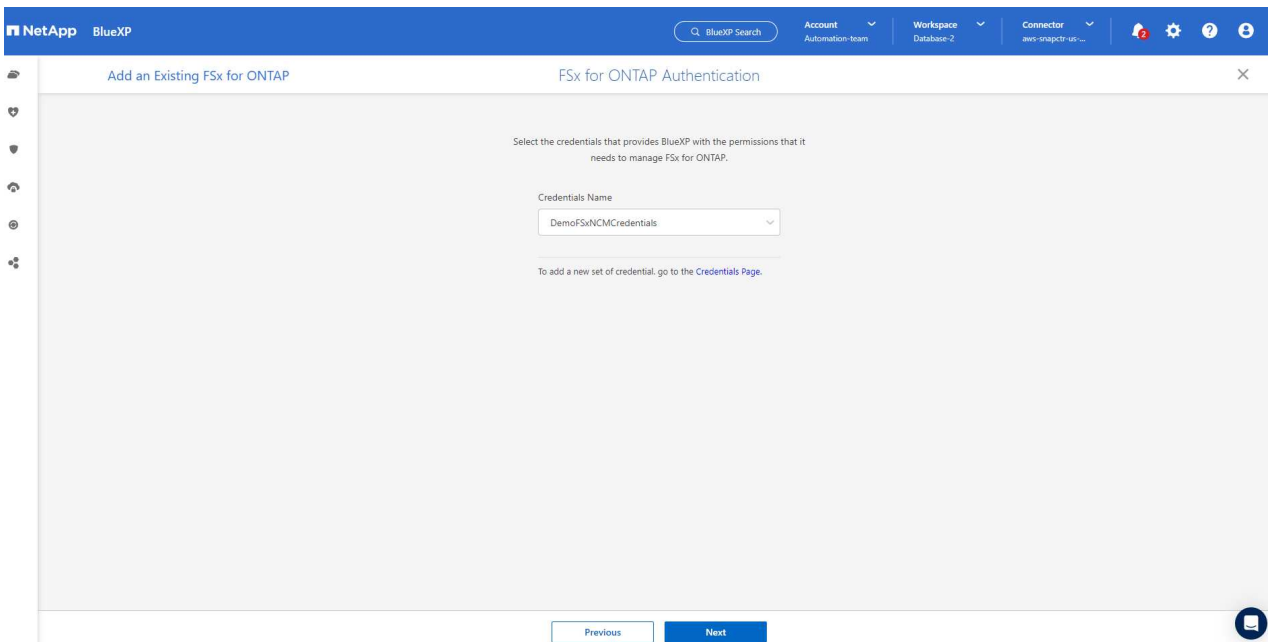
1. 場所として*Amazon Web Services*を選択します。



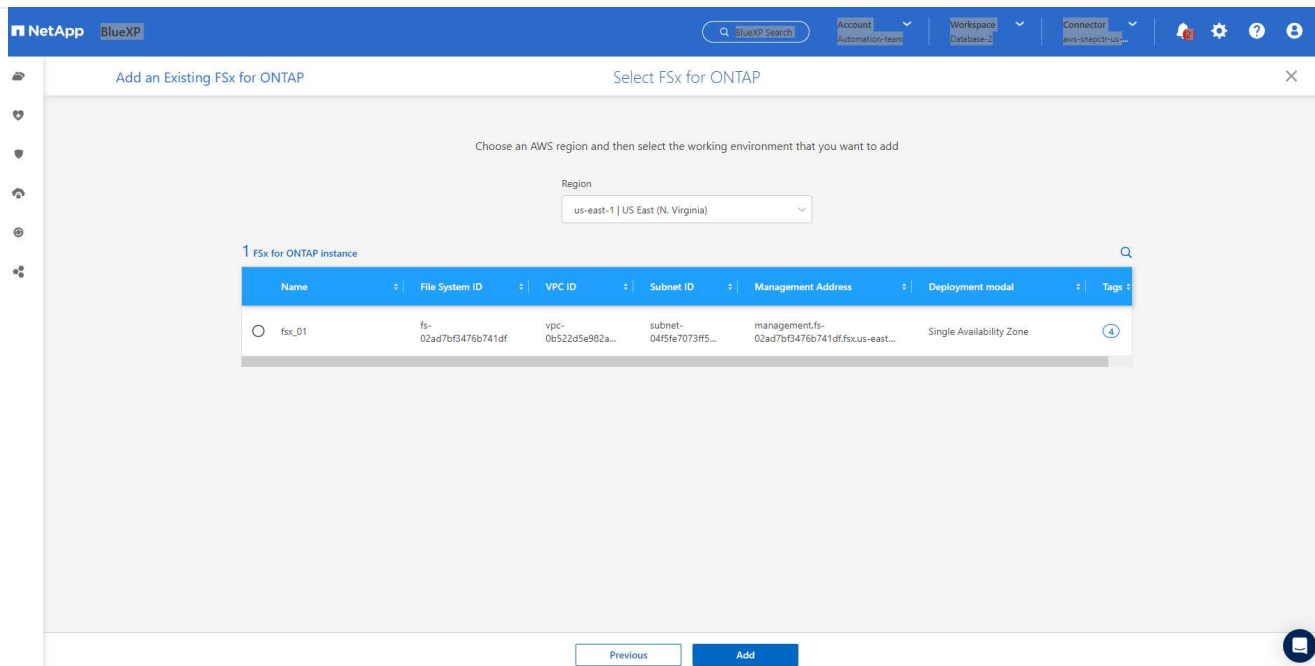
1. * Amazon FSx ONTAP* の横にある 既存の検出 をクリックします。



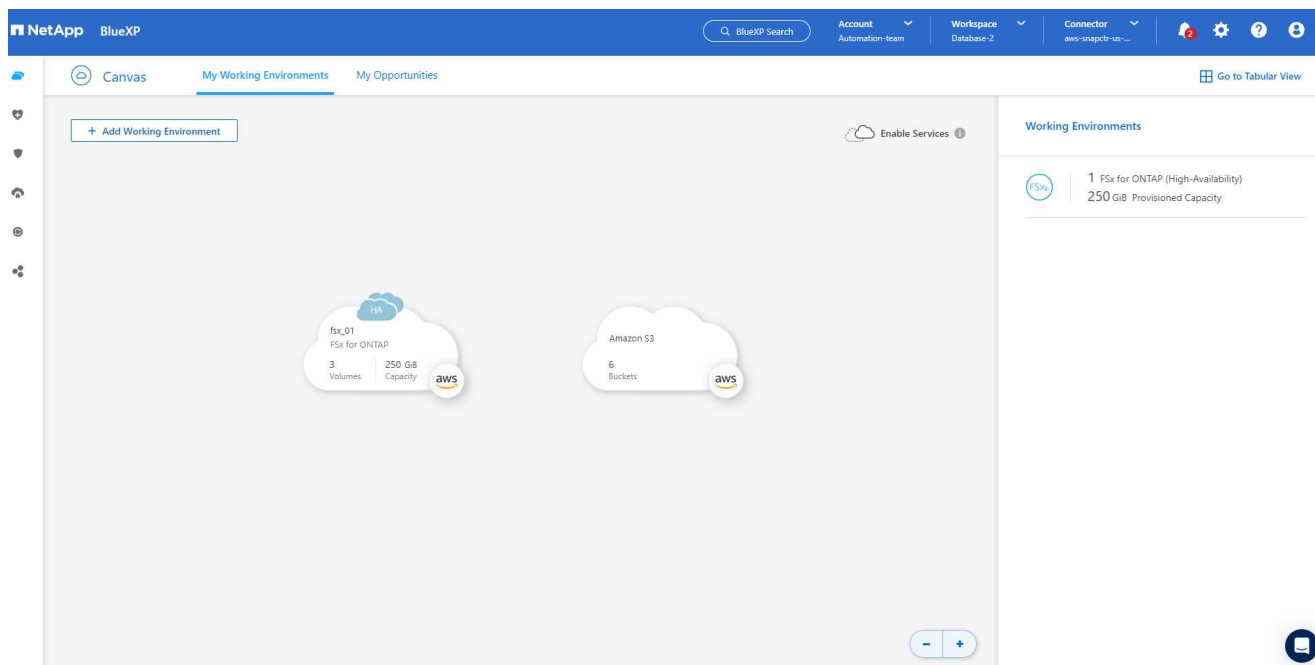
1. 前のセクションで作成した 資格情報名 を選択して、BlueXPに FSx ONTAPを管理するために必要な権限を付与します。資格情報を追加していない場合は、BlueXPコンソールの右上隅にある 設定 メニューから追加できます。



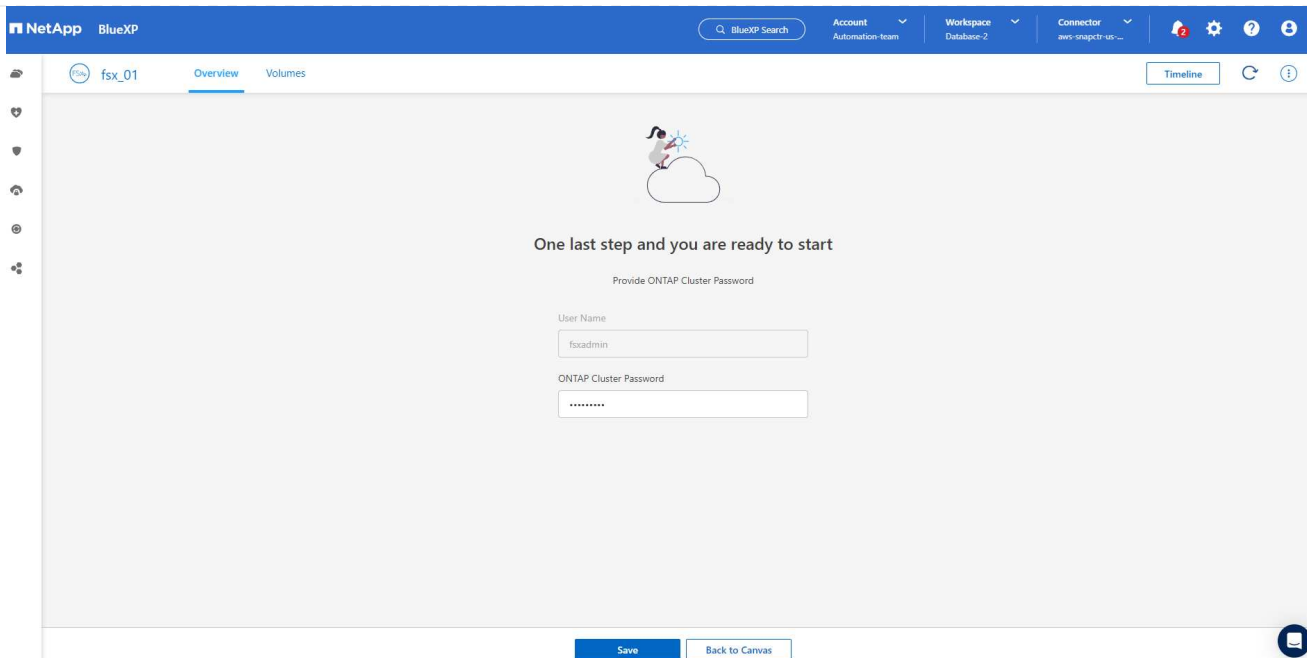
2. Amazon FSx ONTAPがデプロイされている AWS リージョンを選択し、Oracle データベースをホストしている FSx クラスターを選択して、[追加] をクリックします。



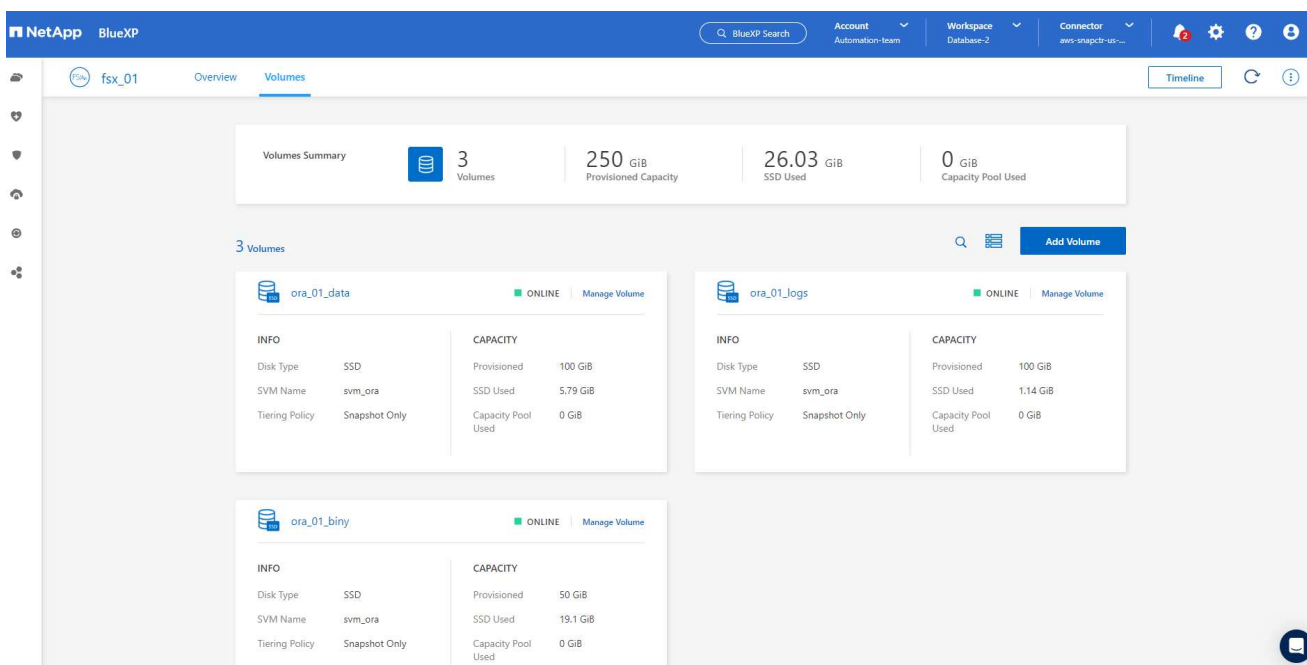
1. 検出されたAmazon FSx ONTAPインスタンスが作業環境に表示されます。



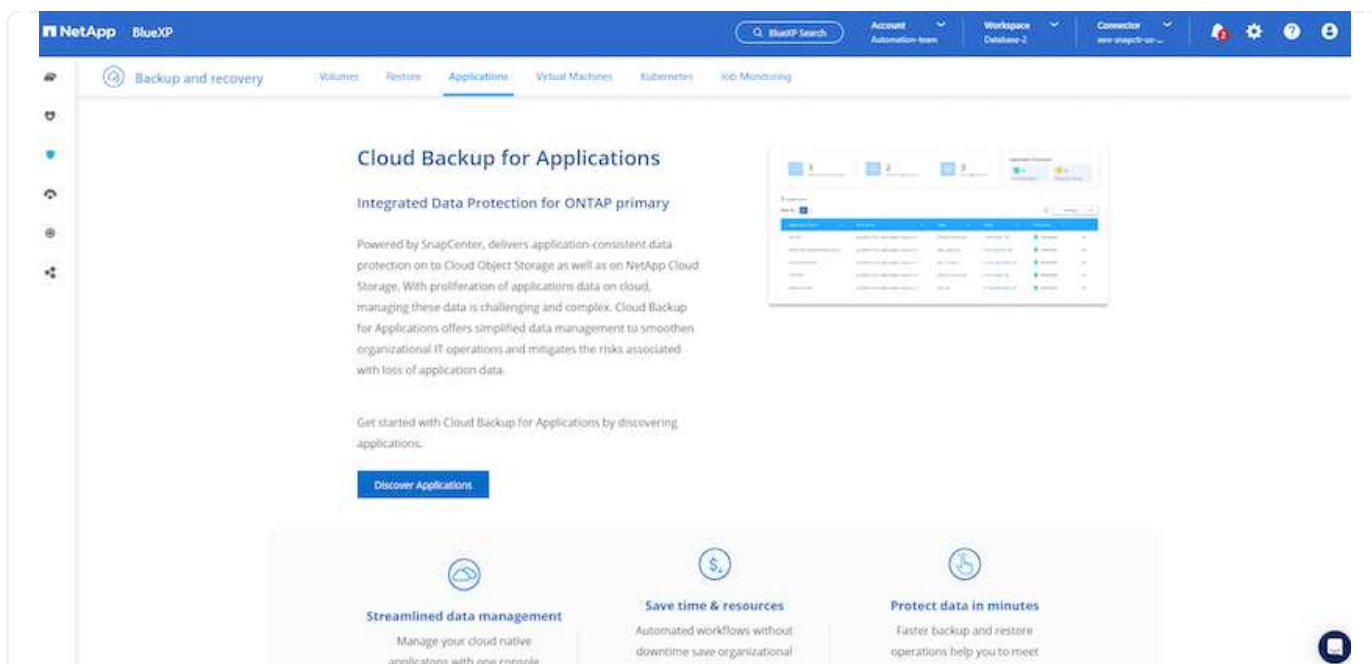
1. fsxadmin アカウントの資格情報を使用して FSx クラスターにログインできます。



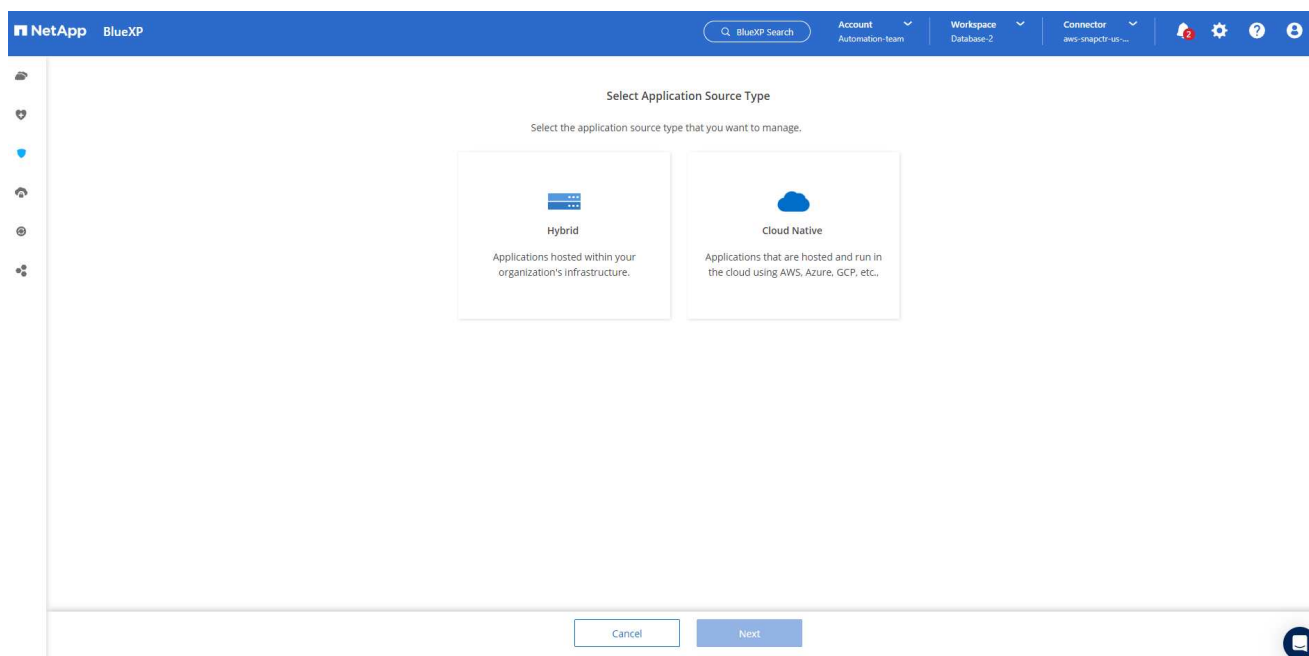
1. Amazon FSx ONTAPにログインしたら、データベースのストレージ情報 (データベースボリュームなど) を確認します。



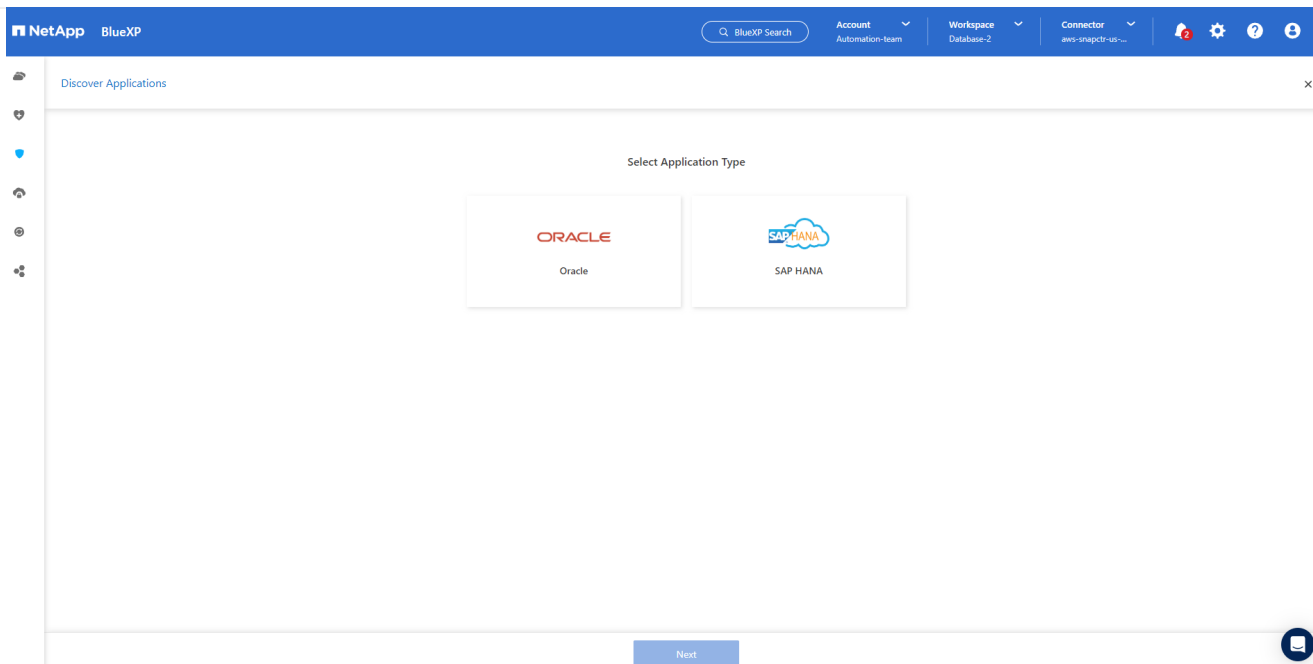
1. コンソールの左側のサイドバーで、保護アイコンの上にマウスを移動し、保護 > アプリケーションをクリックして、アプリケーションの起動ページを開きます。*アプリケーションの検出*をクリックします。



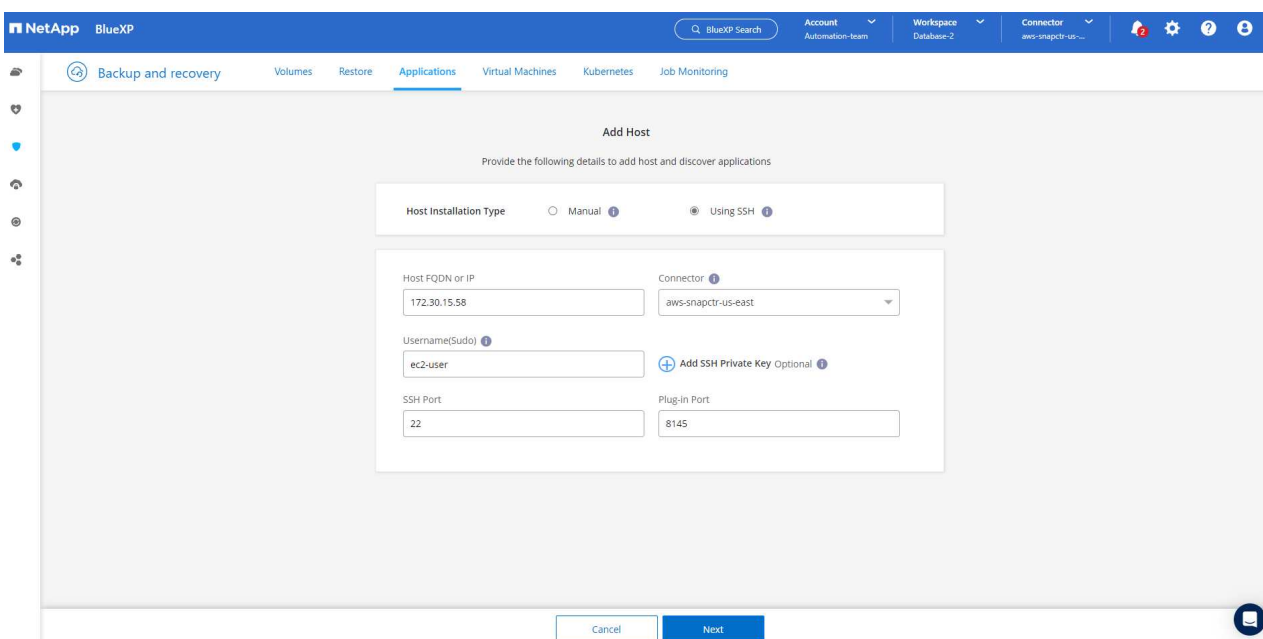
1. アプリケーション ソース タイプとして **Cloud Native** を選択します。



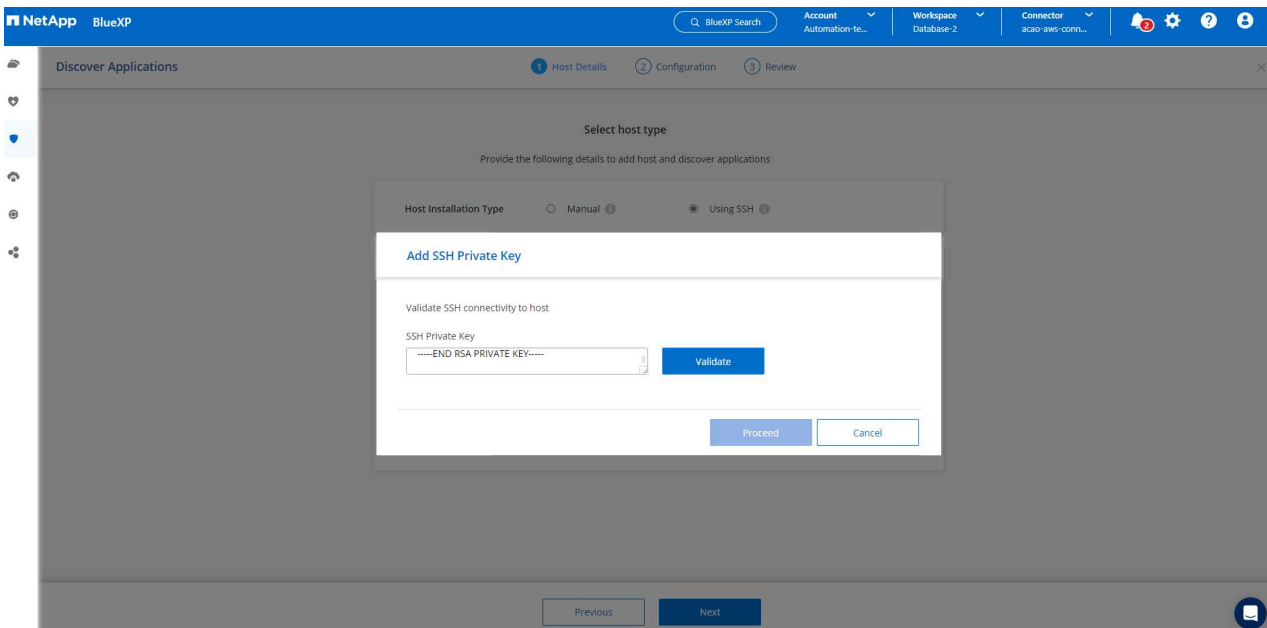
1. アプリケーション タイプとして **Oracle** を選択します。



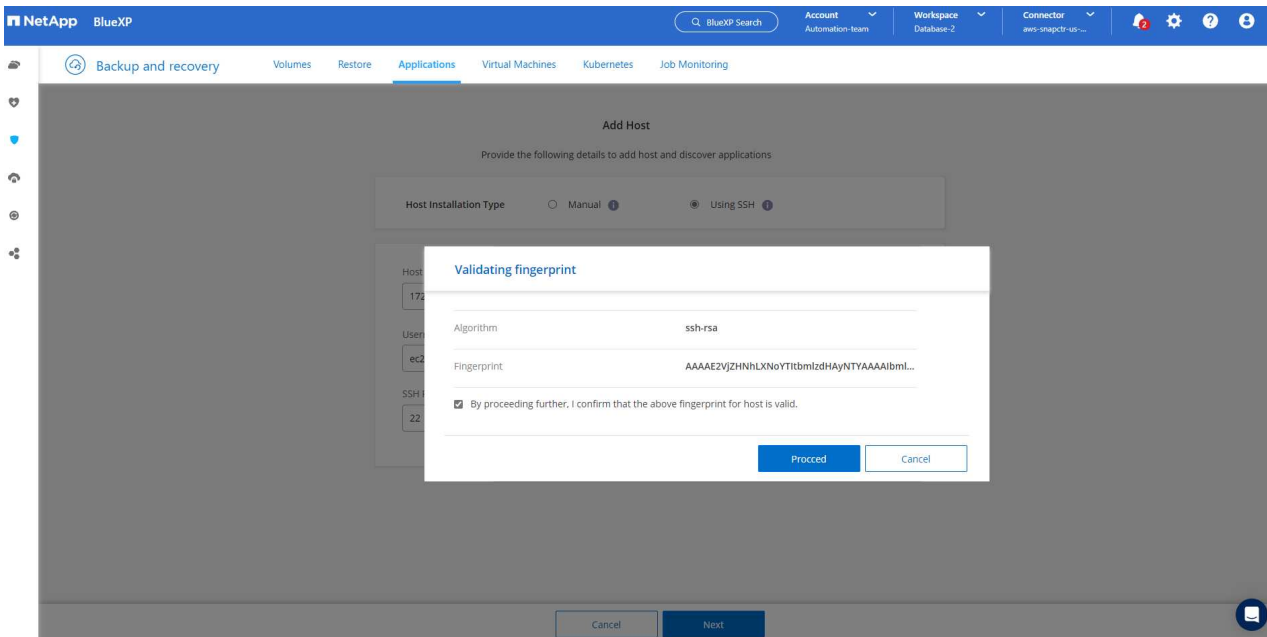
1. AWS EC2 Oracle アプリケーション ホストの詳細を入力します。ワンステップのプラグインのインストールとデータベースの検出を行うには、ホストのインストールタイプ*として*SSH の使用*を選択します。次に、「*SSH 秘密キーの追加」をクリックします。



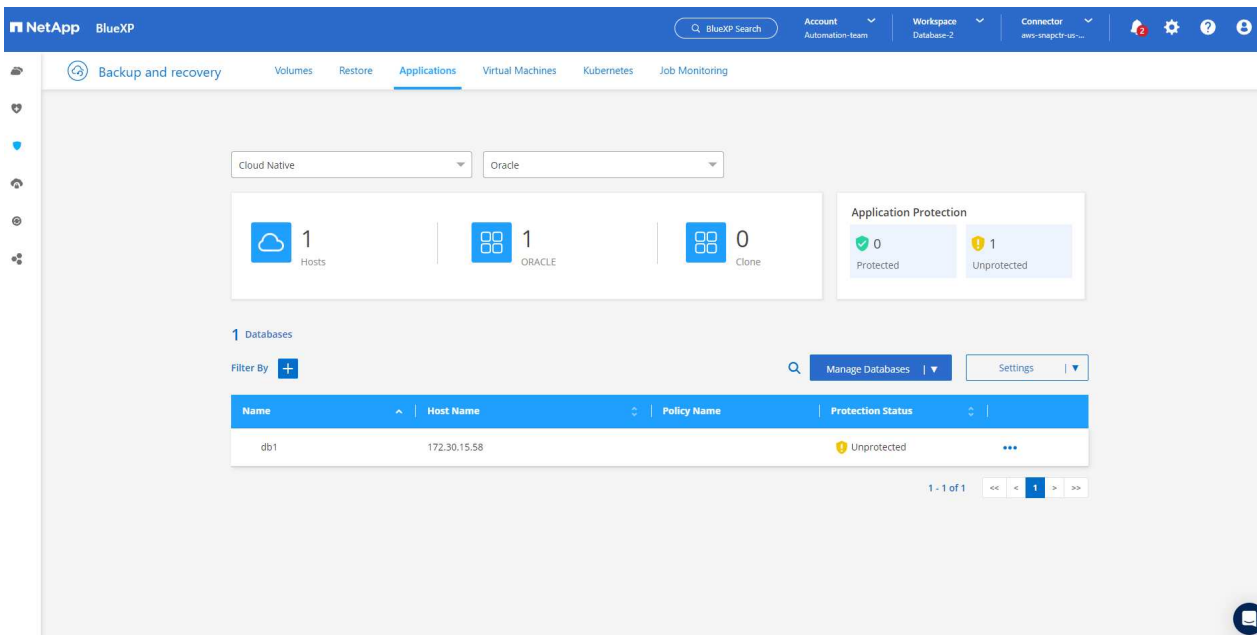
2. データベース EC2 ホストの ec2-user SSH キーを貼り付けて、「検証」をクリックして続行します。



3. 続行するには、「指紋を検証しています」というプロンプトが表示されます。



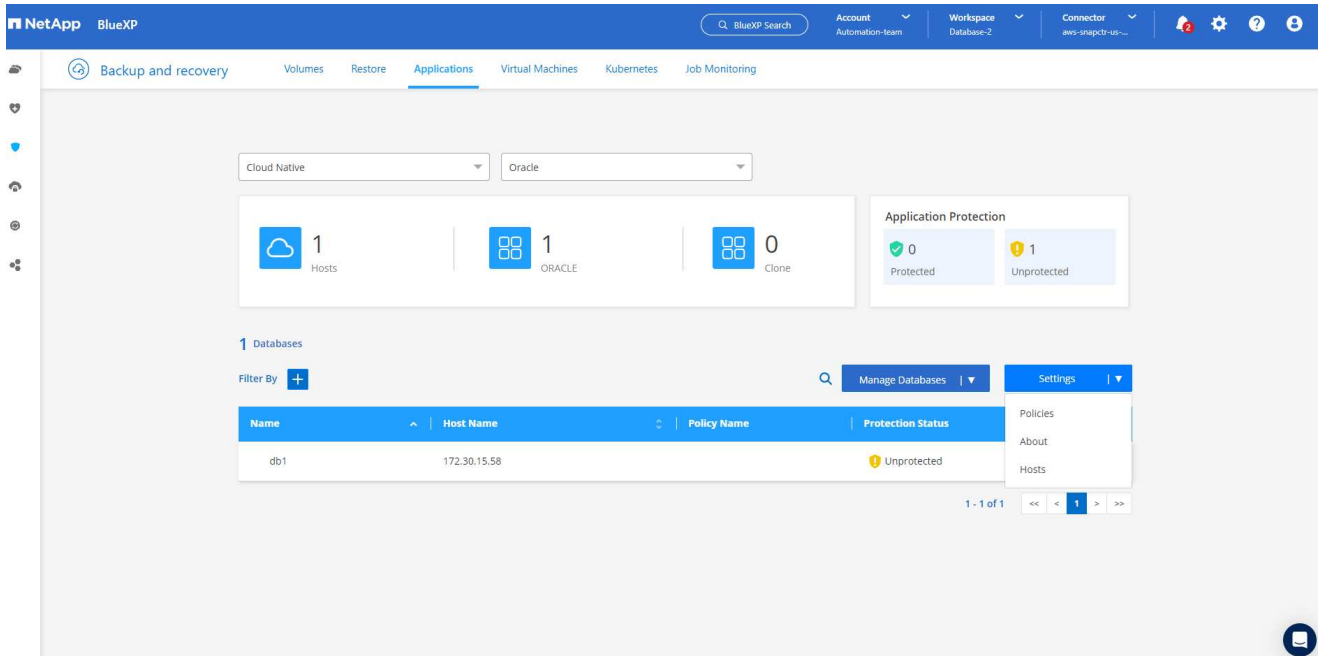
4. 次へ をクリックして、Oracle データベース プラグインをインストールし、EC2 ホスト上の Oracle データベースを検出します。検出されたデータベースは アプリケーション に追加されます。データベースの 保護ステータス は、最初に検出されたときには 保護なし と表示されます。



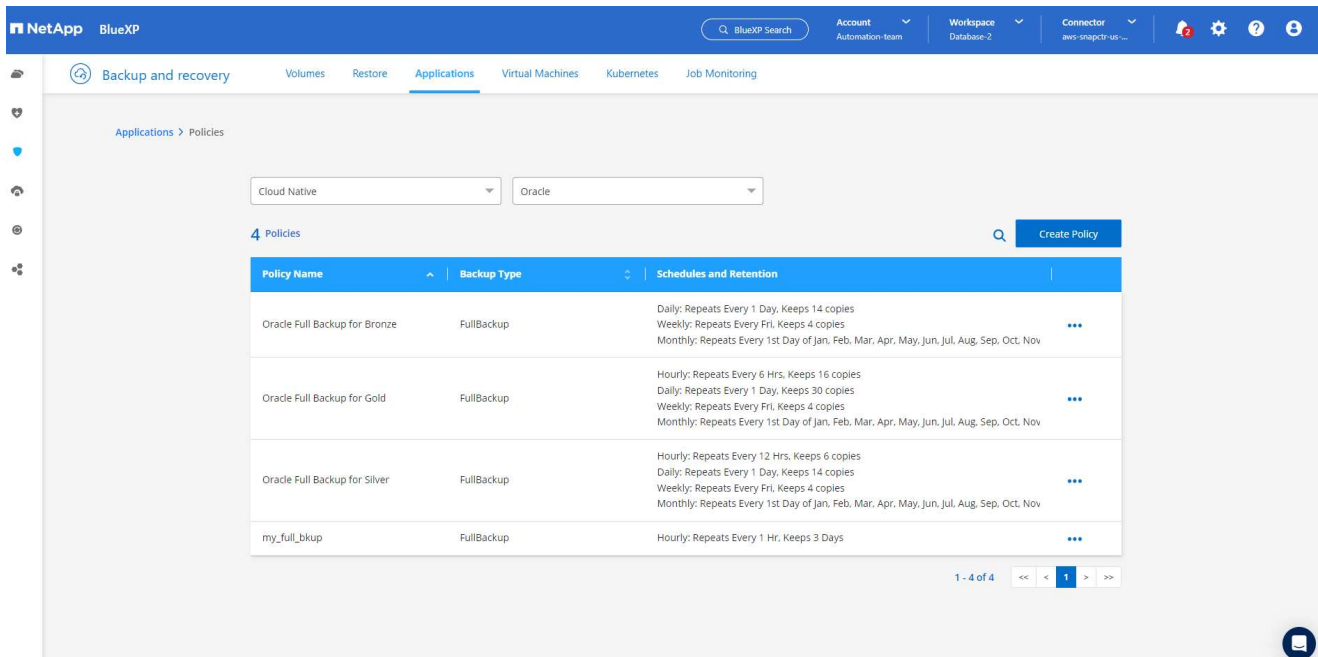
これで、Oracle 用のSnapCenterサービスの初期セットアップが完了します。このドキュメントの次の 3 つのセクションでは、Oracle データベースのバックアップ、復元、およびクローン操作について説明します。

Oracleデータベースのバックアップ

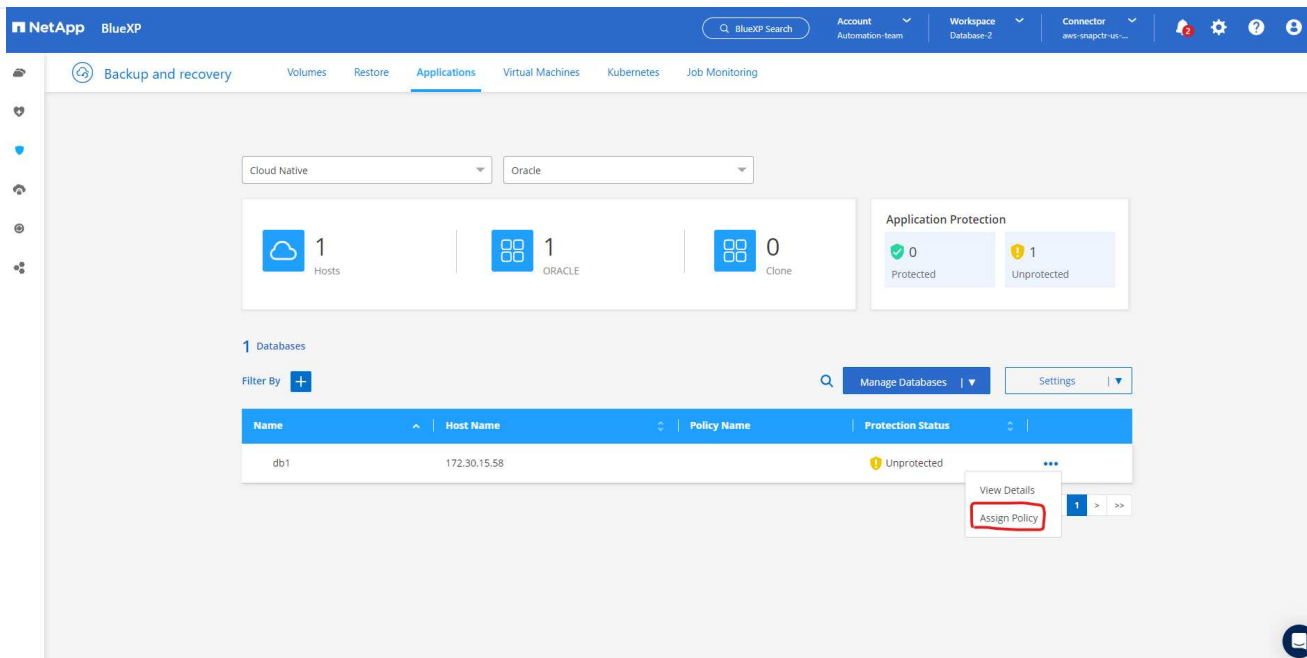
1. データベースの 保護ステータス の横にある 3 つのドットをクリックし、ポリシー をクリックして、Oracle データベースを保護するために適用できる、事前にロードされたデフォルトのデータベース保護ポリシーを表示します。



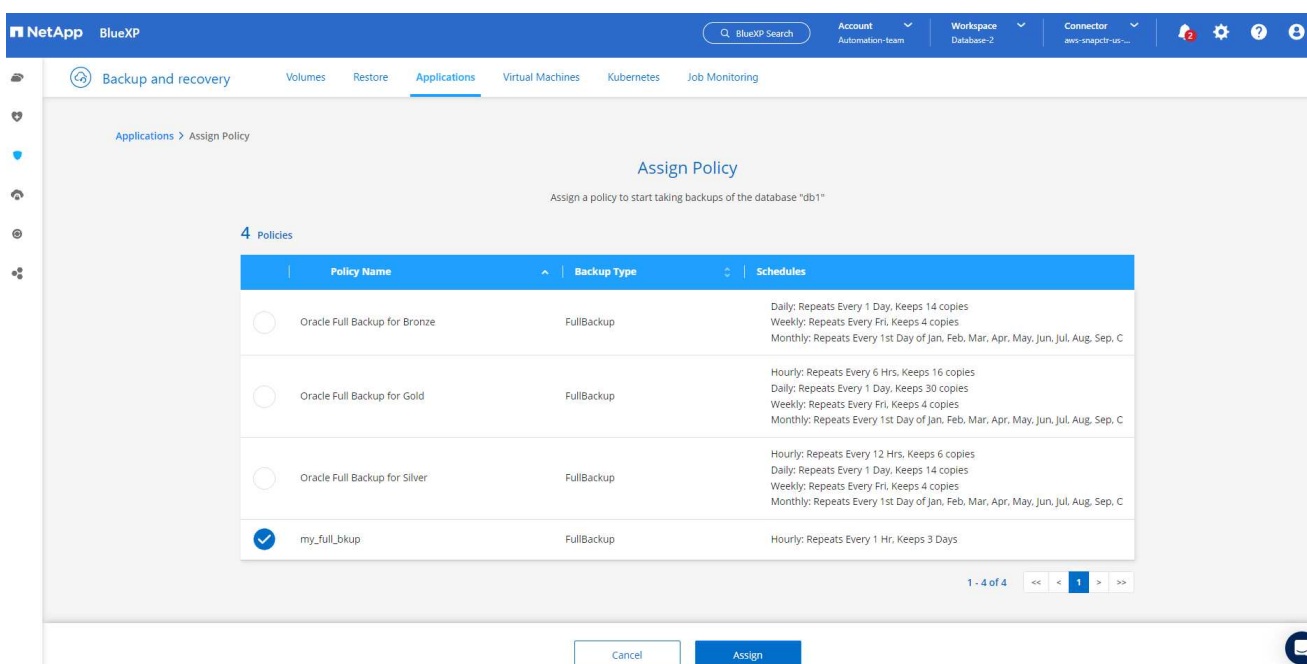
1. カスタマイズされたバックアップ頻度とバックアップ データ保持期間を使用して独自のポリシーを作成することもできます。



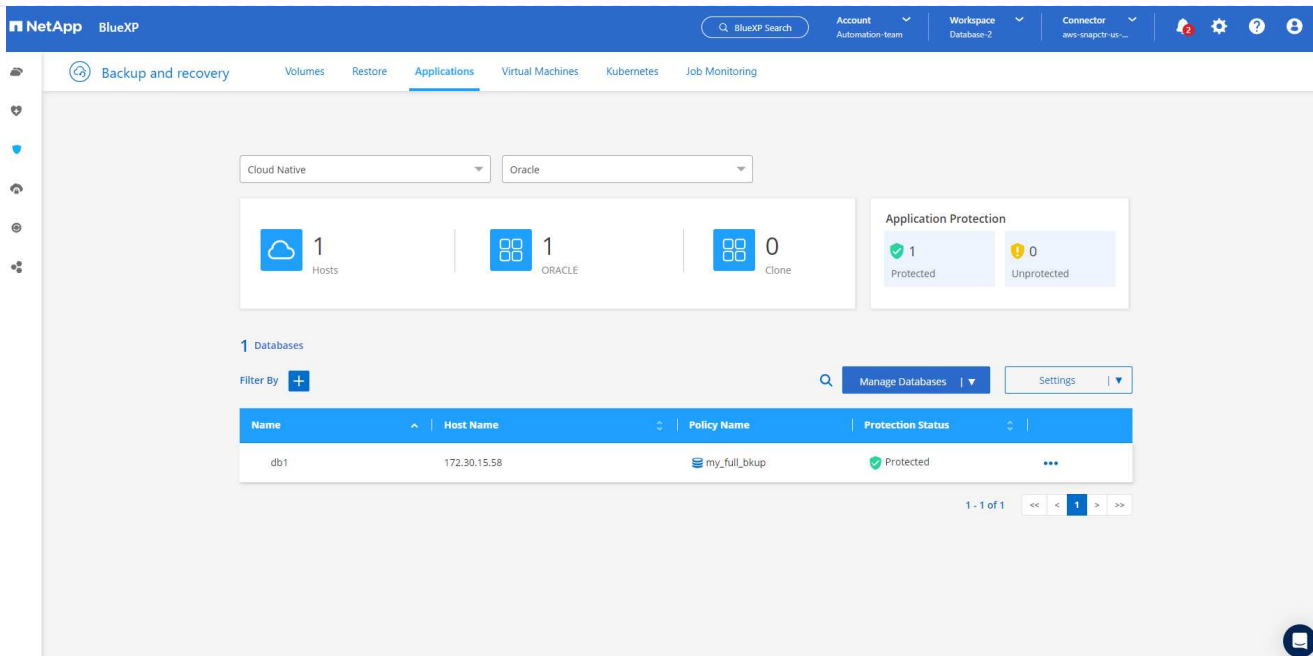
1. ポリシー構成に満足したら、データベースを保護するために選択したポリシーを割り当てることができます。



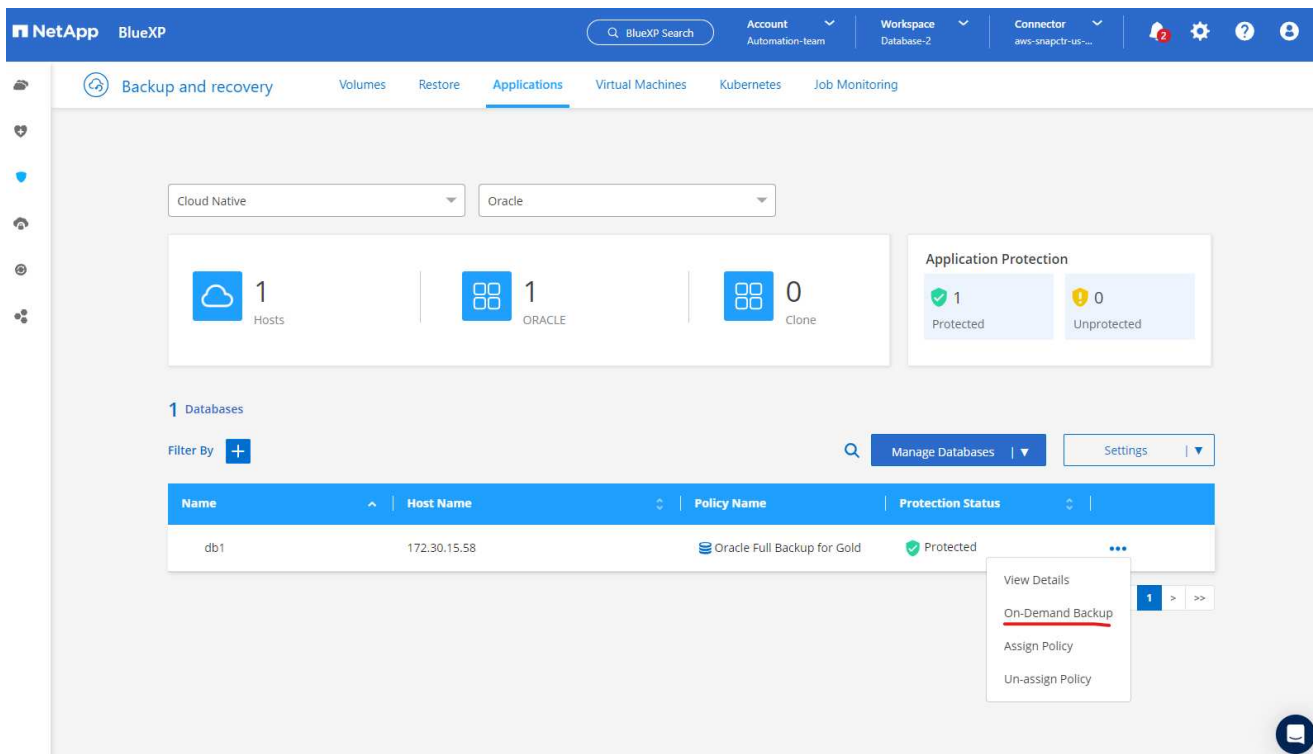
1. データベースに割り当てるポリシーを選択します。



1. ポリシーが適用されると、データベースの保護ステータスが緑色のチェックマーク付きの「保護済み」に変わります。



1. データベースのバックアップは、事前に定義されたスケジュールに従って実行されます。以下に示すように、1 回限りのオンデマンド バックアップを実行することもできます。



1. データベースのバックアップの詳細は、メニュー リストから [詳細の表示] をクリックすると表示できます。これには、バックアップ名、バックアップ タイプ、SCN、バックアップの日付が含まれます。バックアップセットは、データ ボリュームとログ ボリュームの両方のスナップショットをカバーします。ログ ボリューム スナップショットは、データベース ボリューム スナップショットの直後に実行されます。長いリストの中で特定のバックアップを探している場合は、フィルターを適用できます。

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

Applications > Database Details

Database Details

db1 Database Name	Protected Protection	Oracle Full Backup for Gold Policy Names	Database Type
172.30.15.58 Host Name	FSx Host Storage	Unreachable Database Version	bKed8yv2T19Bj0V5QyqvA... Agent Id
- Clones	- Parent Database		

8 Backups

Filter By +

Select Timeframe

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	...

Oracleデータベースの復元と回復

1. データベースを復元する場合は、SCN またはバックアップ時間によって適切なバックアップを選択します。データベース データのバックアップから 3 つのドットをクリックし、[復元] をクリックしてデータベースの復元と回復を開始します。

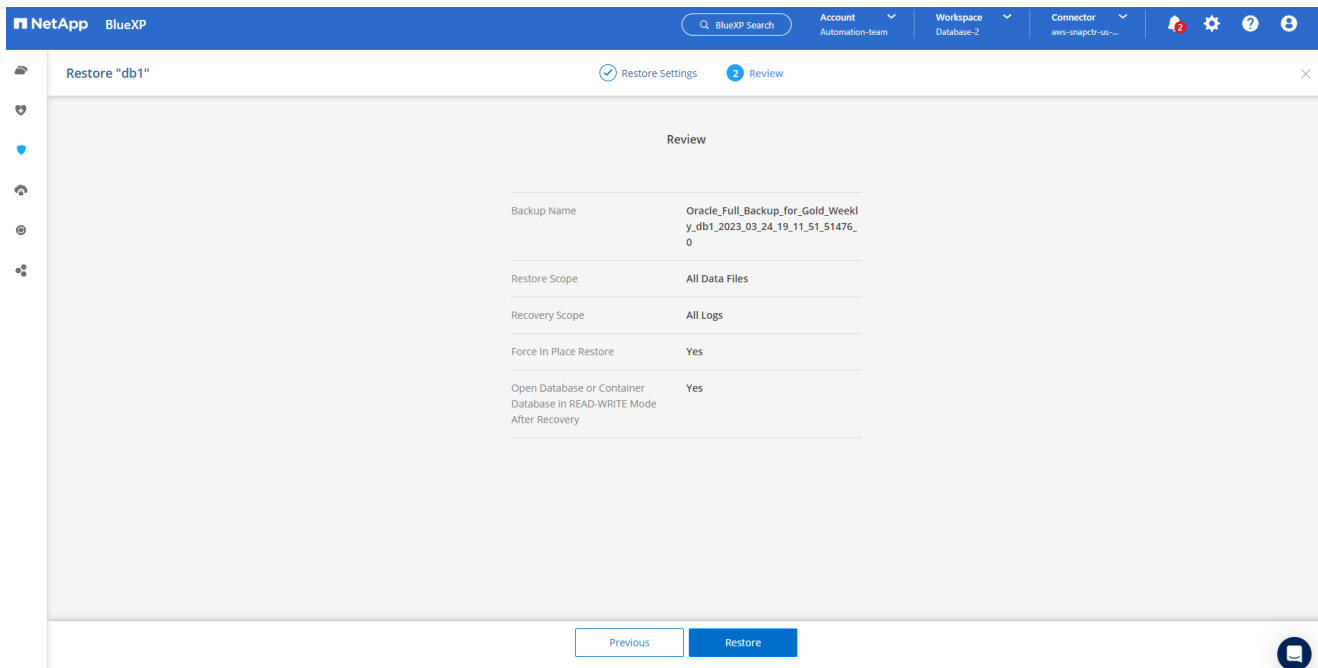
The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' tab is selected, leading to 'Database Details' for a database named 'db1'. The details section shows various attributes like 'Protected Protection', 'FSx Host Storage', and 'Database Type'. Below this, the 'Backups' section is displayed with a table of backup records. The table has columns for 'Backup Name', 'Backup Type', 'SCN', 'Backup Date', and 'Delete'. One backup record is highlighted, and a context menu is open showing the 'Restore' option.

Backup Name	Backup Type	SCN	Backup Date	Delete
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, 11:37:0	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

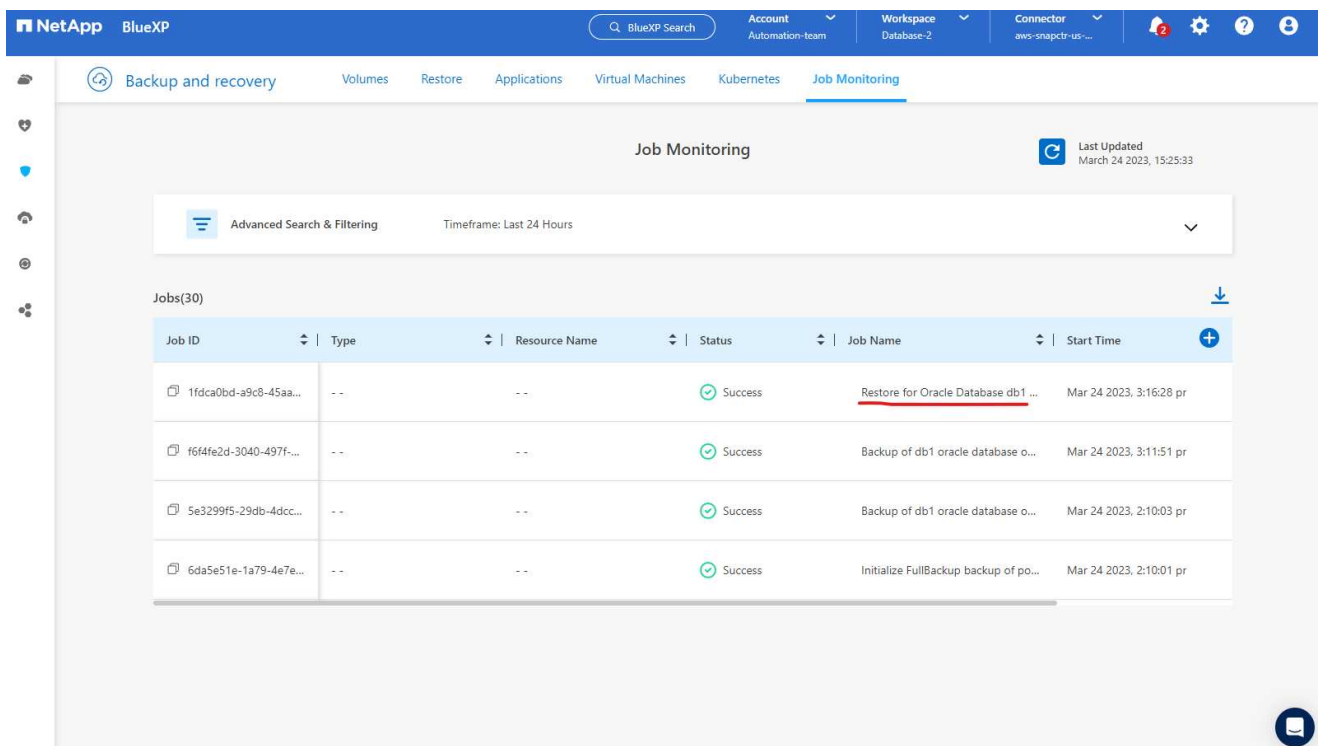
1. 復元設定を選択します。バックアップ後に物理データベース構造に何も変更されていないことが確実な場合は (データ ファイルやディスク グループの追加など)、強制インプレース リストア オプションを使用できます。このオプションは通常、より高速です。それ以外の場合は、このボックスをチェックしないでください。

The screenshot shows the 'Restore Settings' dialog box in the NetApp BlueXP interface. The dialog has two main sections: 'Restore Scope' and 'Recovery Scope'. Under 'Restore Scope', the 'All Data Files' option is selected, and 'Control Files' is also selected. The 'Force in place restore' checkbox is checked. Under 'Recovery Scope', the 'All Logs' option is 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 also checked. The dialog has 'Previous' and 'Next' buttons at the bottom.

1. データベースの復元と回復を確認して開始します。



1. ジョブ監視 タブでは、復元ジョブのステータスと実行中の詳細を表示できます。



NetAppBlueXP

BlueXP Search

AccountAutomation team

WorkspaceDatabase-2

Connectoraws-snapctr-us-...

2

?

3

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

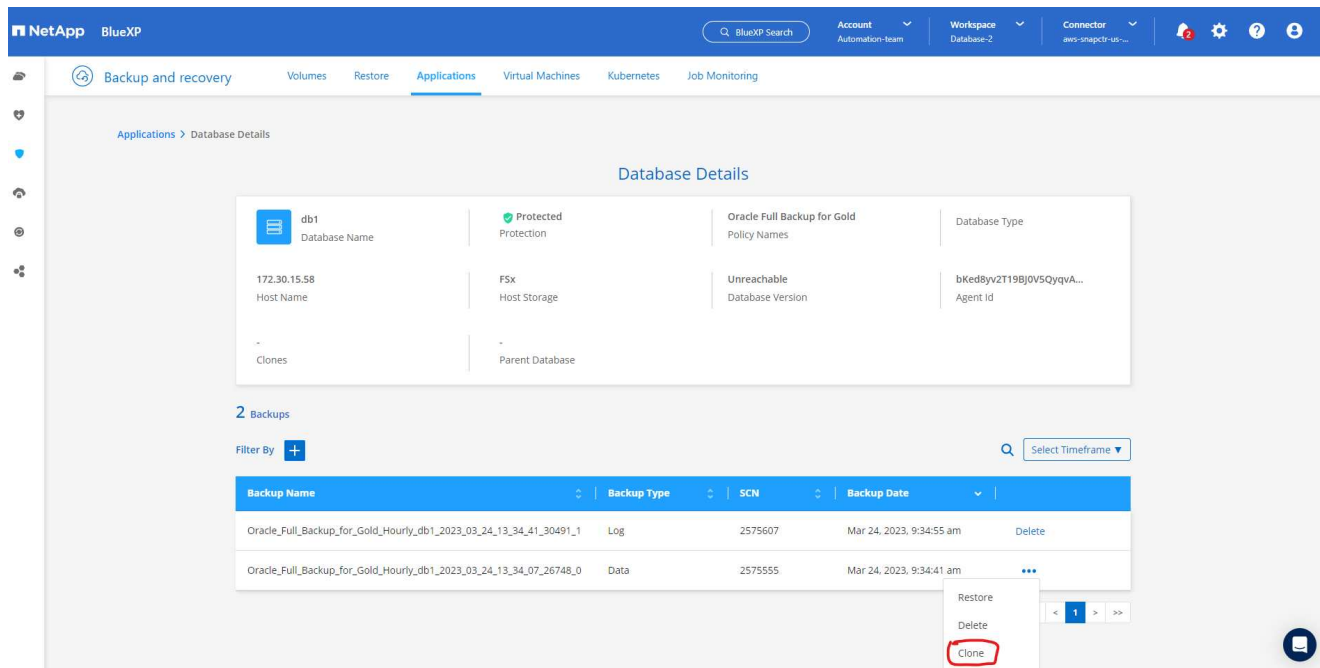
Sub-Jobs(6)

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

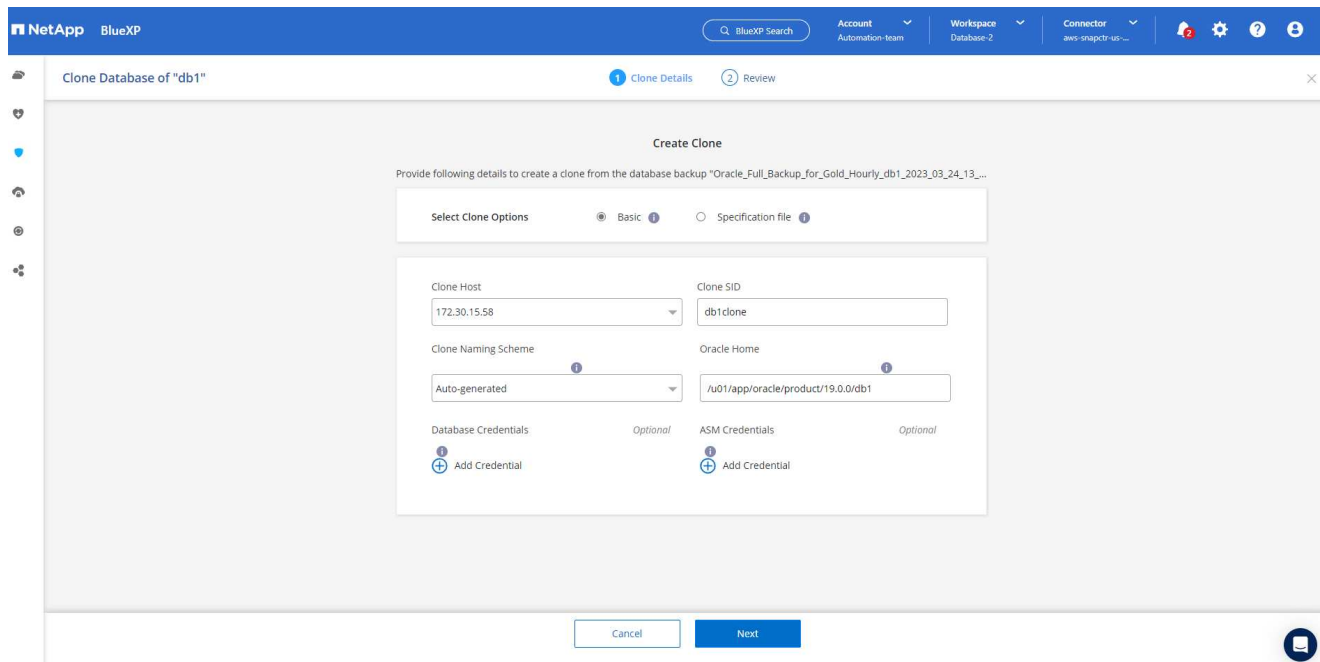
Oracle データベースクローン

データベースのクローンを作成するには、同じデータベース バックアップの詳細ページからクローンワークフローを起動します。

1. 適切なデータベースのバックアップ コピーを選択し、3 つのドットをクリックしてメニューを表示し、[クローン] オプションを選択します。



1. クローンされたデータベースのパラメータを変更する必要がない場合は、基本 オプションを選択します。



1. または、「仕様ファイル」を選択すると、現在の init ファイルをダウンロードし、変更を加えてからジョブに再度アップロードするオプションが提供されます。

NetApp BlueXP

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. ジョブを確認して起動します。

NetApp BlueXP

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. *ジョブ監視*タブからクローン作成ジョブのステータスを監視します。

NetApp BlueXP

BlueXP Search Account Automation-team Workspace Database-2 Connector aws-snapc1r-10-...

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. EC2 インスタンス ホスト上でクローンされたデータベースを検証します。

```
#
# 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>
```

追加情報

このドキュメントに記載されている情報の詳細については、次のドキュメントや Web サイトを参照してください。

- BlueXPのセットアップと管理

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

- BlueXP backup and recovery ドキュメント

["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

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。