TR-4977: Backup, restauração e clonagem do Oracle Database com SnapCenter Services - Azure

NetApp database solutions

NetApp
August 18, 2025

Índice

TR-4977: Backup, restauração e clonagem do Oracle Database com SnapCenter Services - Azure

Allen Cao, Niyaz Mohamed, NetApp

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 .

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 em execução no Azure NetApp Files. 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 em volumes do Azure NetApp Files e instâncias de computação do Azure. É muito fácil configurar a proteção de dados para o banco de dados Oracle implantado no Azure NetApp Files com a interface de usuário BlueXP baseada na Web.

Esta solução aborda os seguintes casos de uso:

- Backup de banco de dados com snapshots para bancos de dados Oracle hospedados no Azure NetApp Files e VMs do Azure
- Recuperação de banco de dados Oracle em caso de falha
- Clonagem rápida de bancos de dados primários para desenvolvimento, ambientes de teste ou outros casos de uso

Público

Esta solução é destinada aos seguintes públicos:

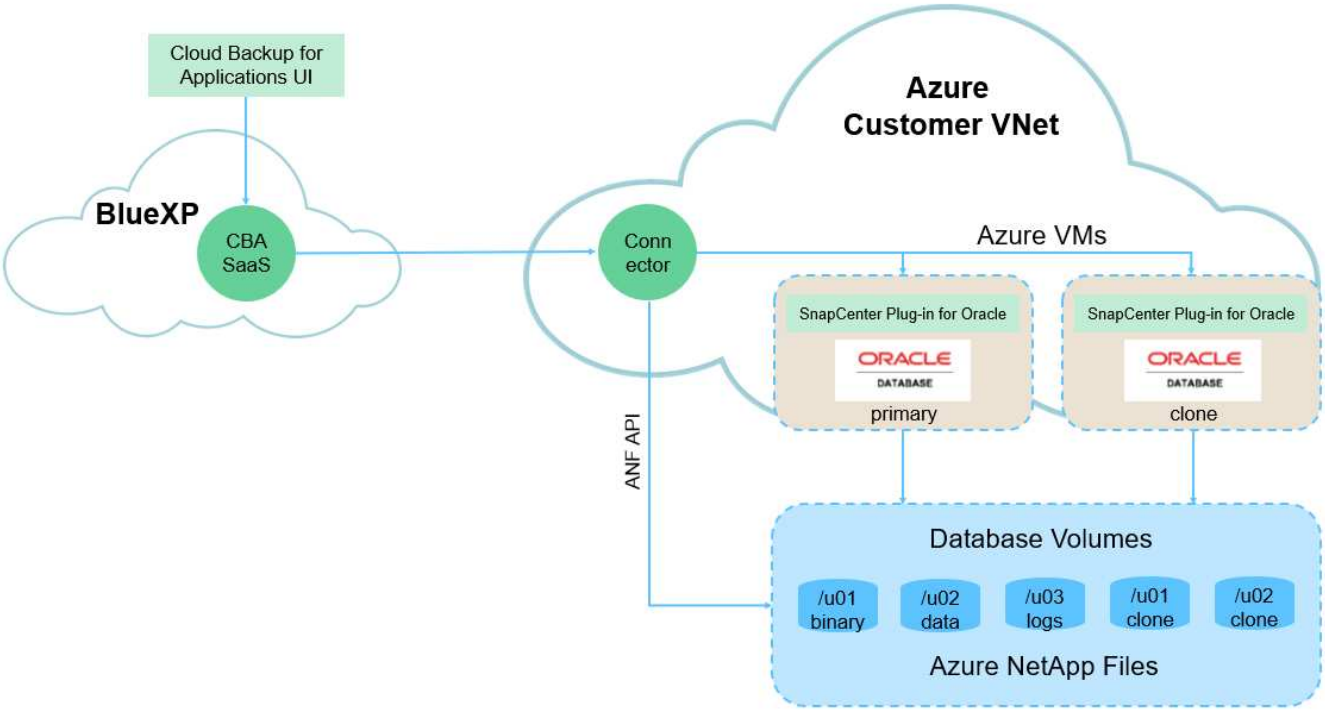
- O DBA que gerencia bancos de dados Oracle em execução no armazenamento do Azure NetApp Files
- O arquiteto de soluções interessado em testar backup, restauração e clonagem de banco de dados Oracle no Azure
- O administrador de armazenamento que oferece suporte e gerencia o armazenamento do Azure NetApp Files
- O proprietário do aplicativo que possui aplicativos implantados no armazenamento do Azure NetApp Files e nas VMs do Azure

Ambiente de teste e validação de soluções

O teste e a validação desta solução foram realizados em um ambiente de laboratório 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 de Azure NetApp Files	Nível de serviço premium	Tipo QoS automático e 4 TB de capacidade de armazenamento em teste
Instância do Azure para computação	B4ms padrão (4 vcpus, 16 GiB de memória)	Duas instâncias implantadas, uma como servidor de banco de dados primário e a outra como servidor de banco de dados clone

Software

RedHat Linux	Red Hat Enterprise Linux 8.7 (LVM) - x64 Gen2	Assinatura RedHat implantada para teste
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 v2.5.0-2822	Versão do agente v2.5.0-2822

Fatores-chave para consideração de implantação

- **Conector a ser implantado na mesma rede virtual/sub-rede que os bancos de dados e o Azure NetApp Files.** Sempre que possível, o conector deve ser implantado nas mesmas redes virtuais e grupos de recursos do Azure, o que permite a conectividade com o armazenamento do Azure NetApp Files e as instâncias de computação do Azure.
- **Uma conta de usuário do Azure ou princípio de serviço do Active Directory criado no portal do Azure para o conector SnapCenter .** A implantação de um conector BlueXP requer permissões específicas para criar e configurar uma máquina virtual e outros recursos de computação, para configurar a rede e para obter acesso à assinatura do Azure. Ele também requer permissões para criar posteriormente funções e permissões para o Conector operar. Crie uma função personalizada no Azure com permissões e atribua à conta de usuário ou ao princípio de serviço. Revise o link a seguir para obter detalhes:"Configurar permissões do Azure" .
- **Um par de chaves SSH criado no grupo de recursos do Azure.** O par de chaves SSH é atribuído ao usuário da VM do Azure para efetuar login no host do conector e também no host da VM do banco de dados para implantar e executar um plug-in. A interface de usuário do console do BlueXP usa a chave SSH para implantar o plug-in de serviço SnapCenter no host do banco de dados para instalação do plug-in em uma etapa e descoberta do banco de dados do host do aplicativo.
- **Uma credencial adicionada à configuração do console BlueXP .** Para adicionar o armazenamento do Azure NetApp Files ao ambiente de trabalho do BlueXP , uma credencial que concede permissões para acessar o Azure NetApp Files do console do BlueXP precisa ser configurada na configuração do console do BlueXP .
- **java-11-openjdk instalado no host da instância do banco de dados da VM do Azure.** 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 em um armazenamento do Azure NetApp Files e uma instância de computação do Azure.

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 ao Azure NetApp Files.
- Assista ao seguinte vídeo passo a passo

  Vídeo de implantação do Oracle e ANF

Pré-requisitos para implantação do serviço SnapCenter

A implantação requer os seguintes pré-requisitos.

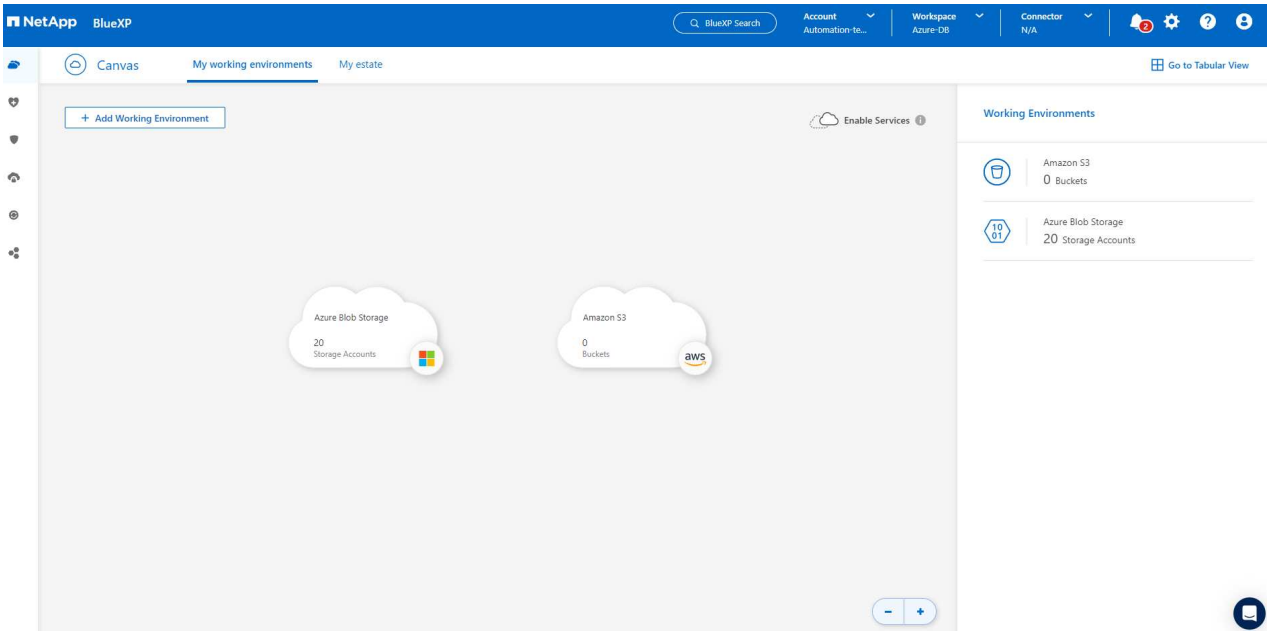
1. Um servidor de banco de dados Oracle primário em uma instância de VM do Azure com um banco de dados Oracle totalmente implantado e em execução.
2. Um pool de capacidade de serviço de armazenamento do Azure NetApp Files implantado no Azure que tem capacidade para atender às necessidades de armazenamento de banco de dados listadas na seção de componentes de hardware.
3. Um servidor de banco de dados secundário em uma instância de VM do Azure 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. Para obter informações adicionais sobre a implantação do banco de dados Oracle no Azure NetApp Files e na instância de computação do Azure, consulte"Implantação e proteção do banco de dados Oracle no Azure NetApp Files" .

Preparação para integração ao BlueXP

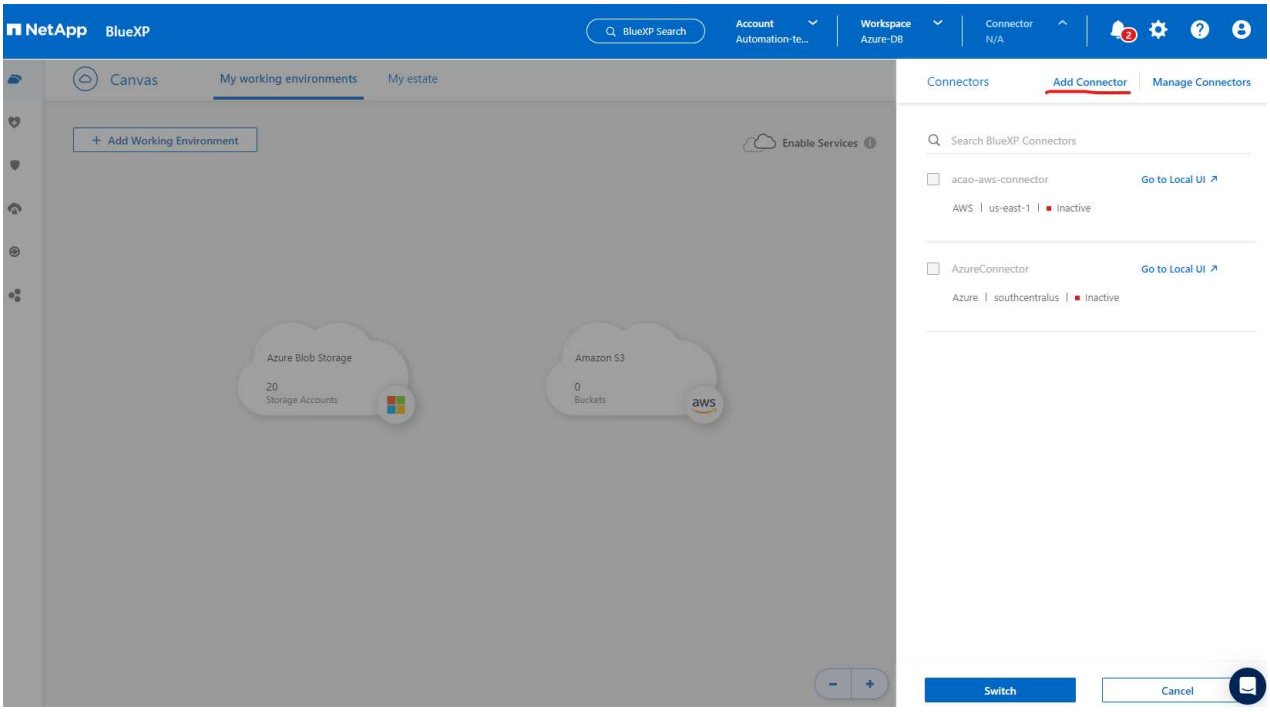
1. Use o link"NetApp BlueXP" para se inscrever no acesso ao console BlueXP .
2. Crie uma conta de usuário do Azure ou um princípio de serviço do Active Directory e conceda permissões com função no portal do Azure para implantação do conector do Azure.
3. Para configurar o BlueXP para gerenciar recursos do Azure, adicione uma credencial do BlueXP com detalhes de uma entidade de serviço do Active Directory que o BlueXP pode usar para autenticar com o Azure Active Directory (ID do cliente do aplicativo), um segredo do cliente para o aplicativo da entidade de serviço (Segredo do cliente) e a ID do Active Directory para sua organização (ID do locatário).
4. Você também precisa da rede virtual do Azure, do grupo de recursos, do grupo de segurança, de uma chave SSH para acesso à VM, etc., prontos para o provisionamento do conector e a instalação do plug-in do banco de dados.

Implantar um conector para serviços SnapCenter

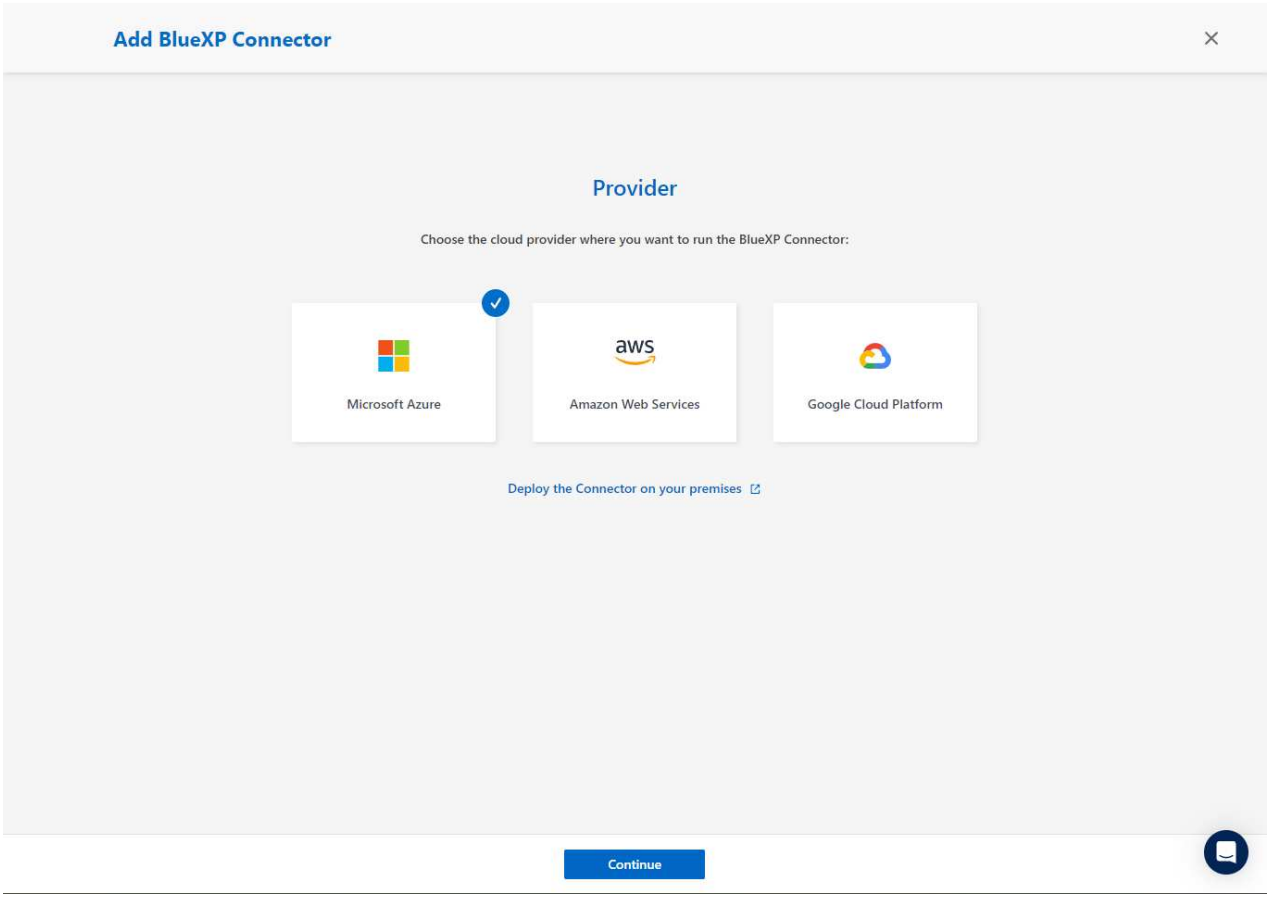
1. Efetue login no console do BlueXP .



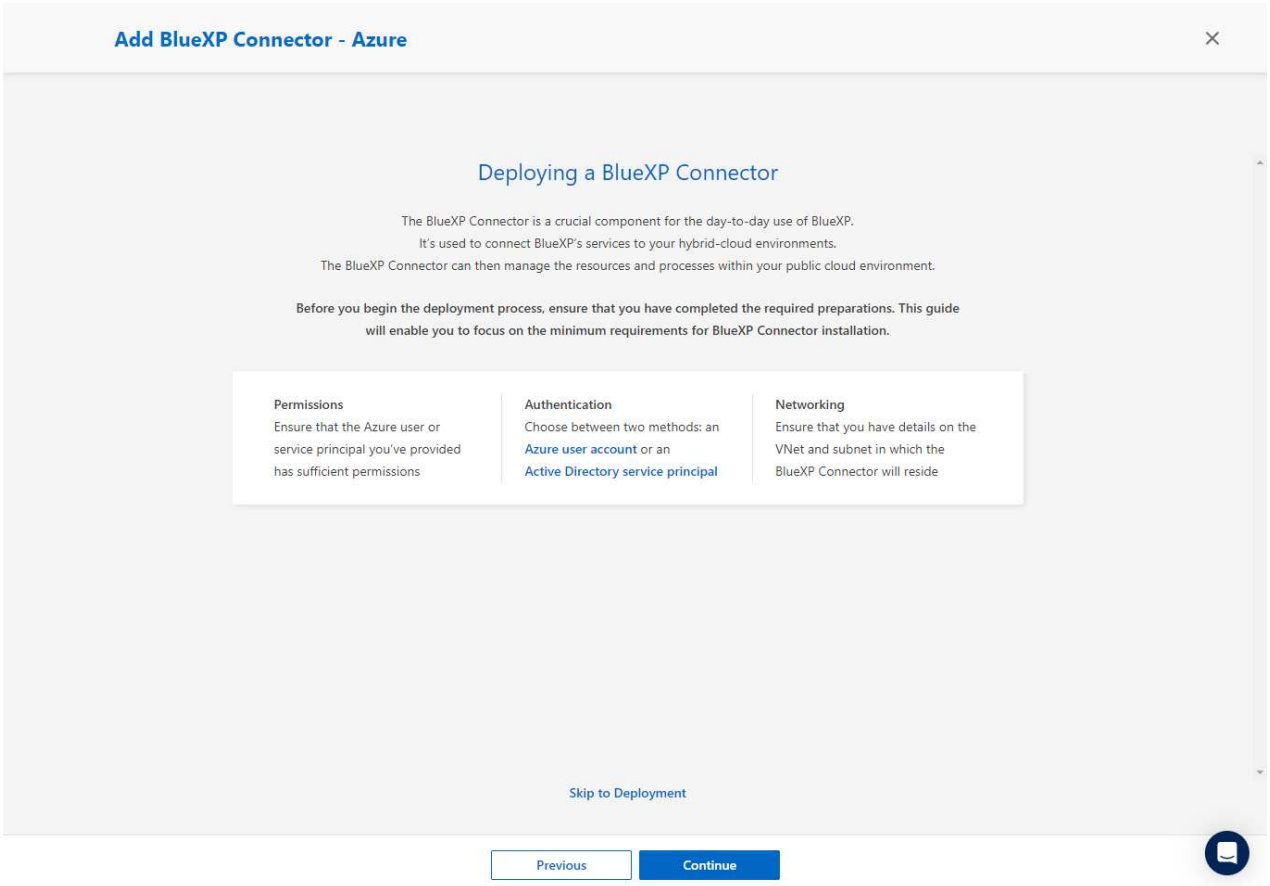
2. Clique na seta suspensa **Conector** e em **Adicionar Conector** para iniciar o fluxo de trabalho de provisionamento do conector.



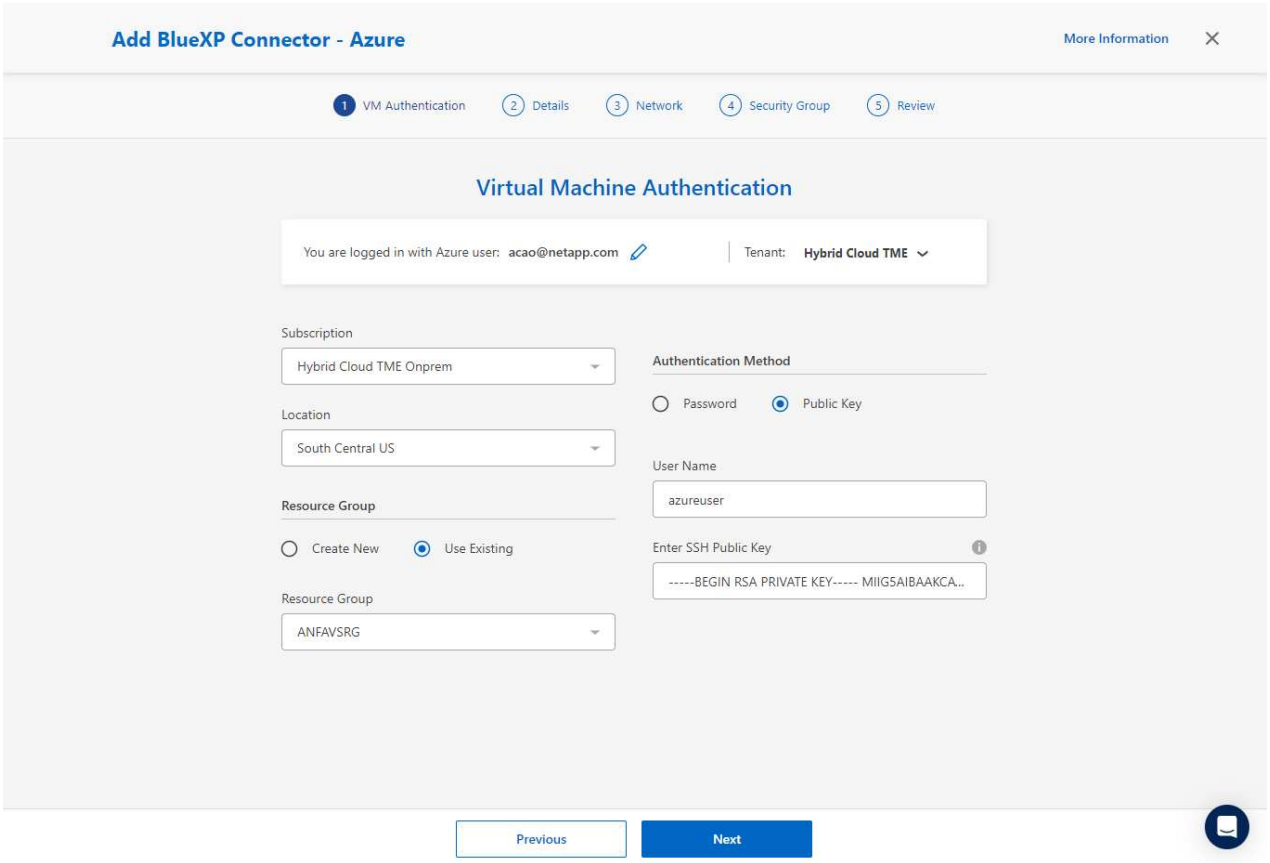
3. Escolha seu provedor de nuvem (neste caso, **Microsoft Azure**).



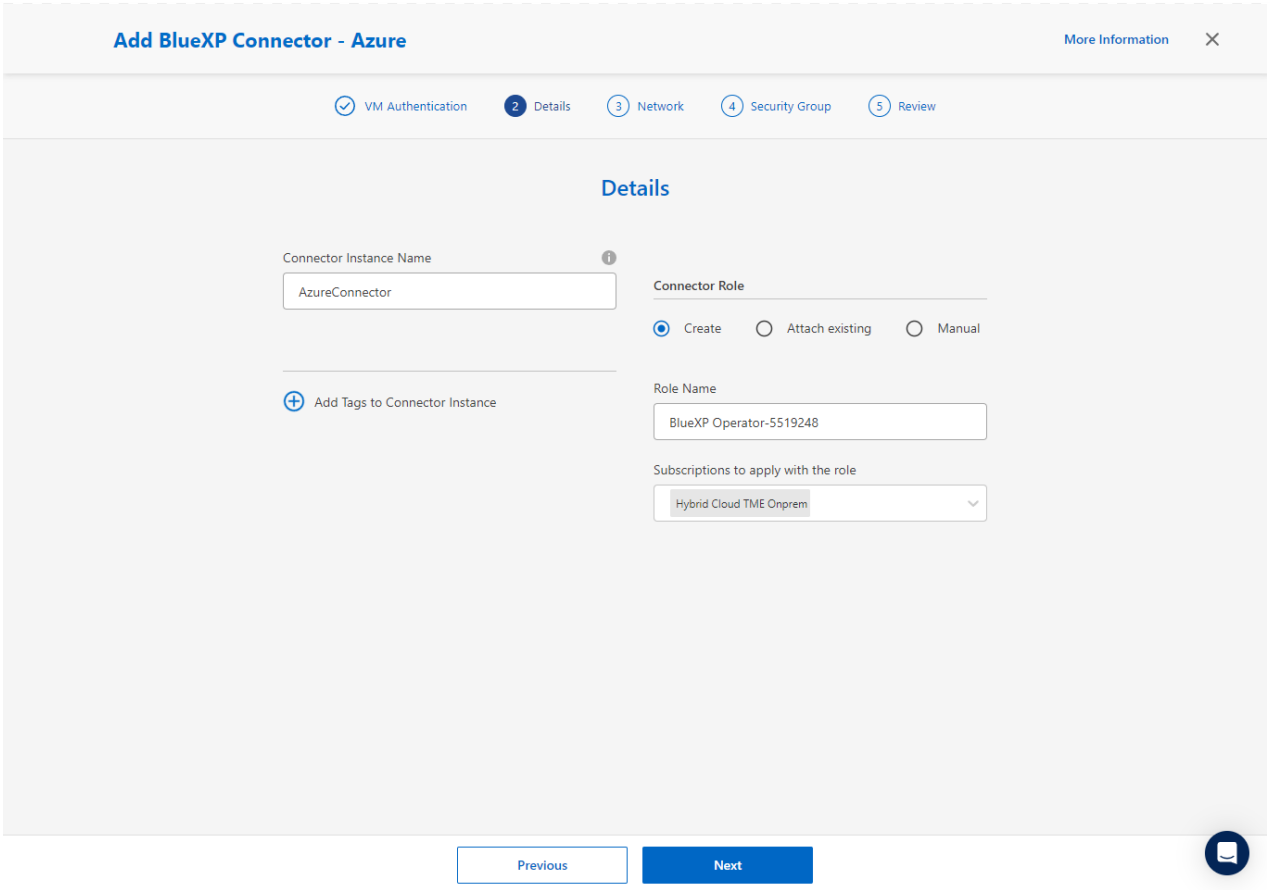
4. Ignore as etapas de **Permissão**, **Autenticação** e **Rede** se você já as tiver configurado na sua conta do Azure. Caso contrário, você deve configurá-los antes de prosseguir. A partir daqui, você também pode recuperar as permissões para a política do Azure referenciada na seção anterior "Preparação para integração ao BlueXP ."



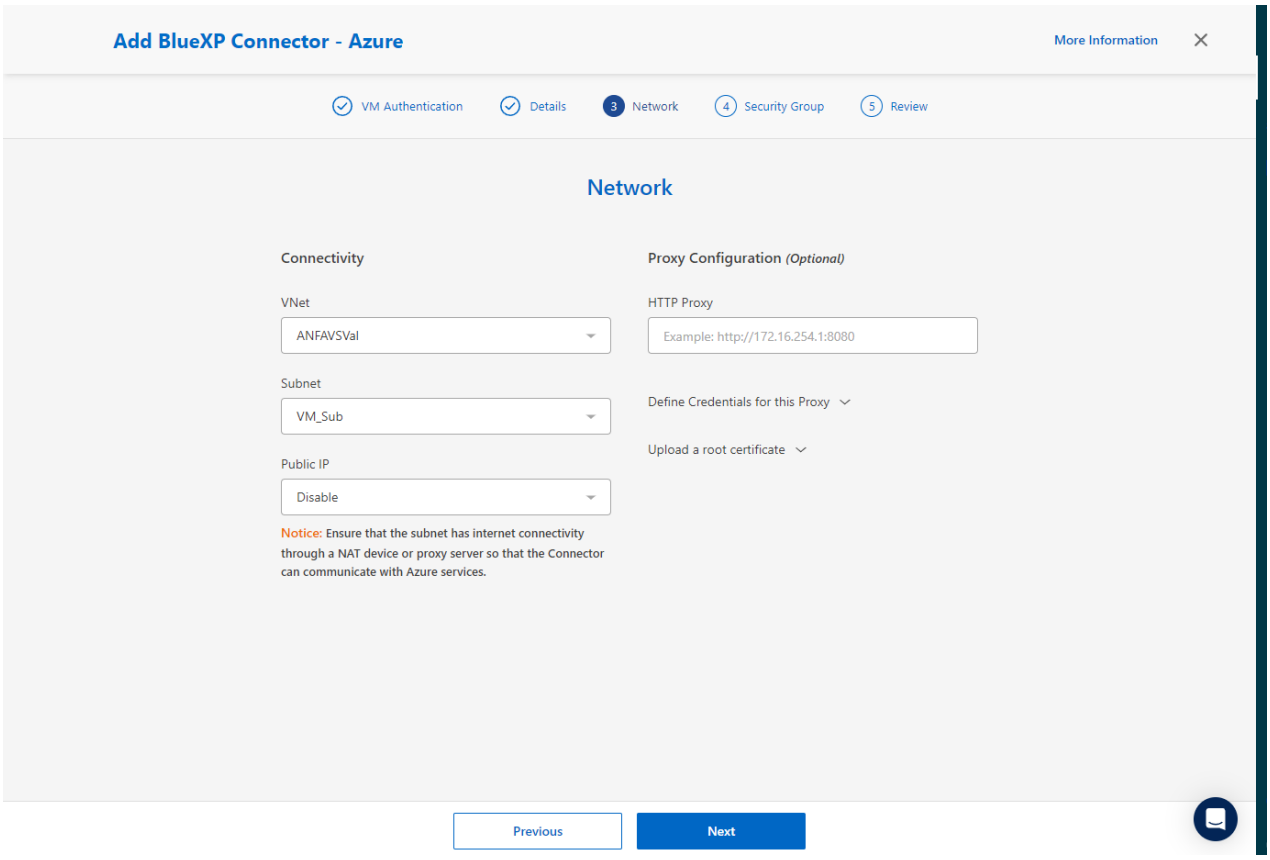
5. Clique em **Ir para implantação** para configurar seu conector **Autenticação de máquina virtual**. Adicione o par de chaves SSH que você criou no grupo de recursos do Azure durante a integração ao BlueXP em preparação para autenticação do sistema operacional do conector.



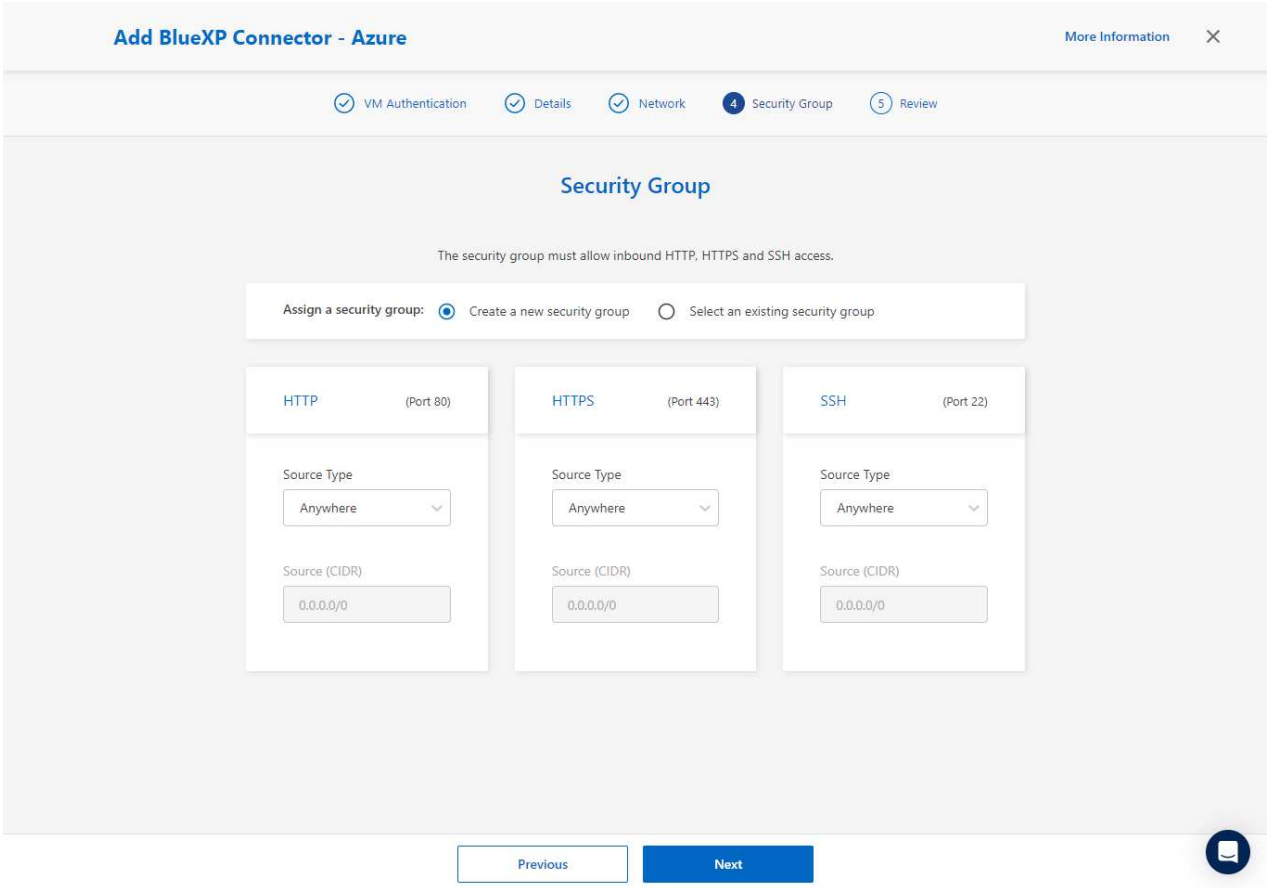
6. Forneça um nome para a instância do conector, selecione **Criar** e aceite o **Nome da Função** padrão em **Detalhes** e escolha a assinatura para a conta do Azure.



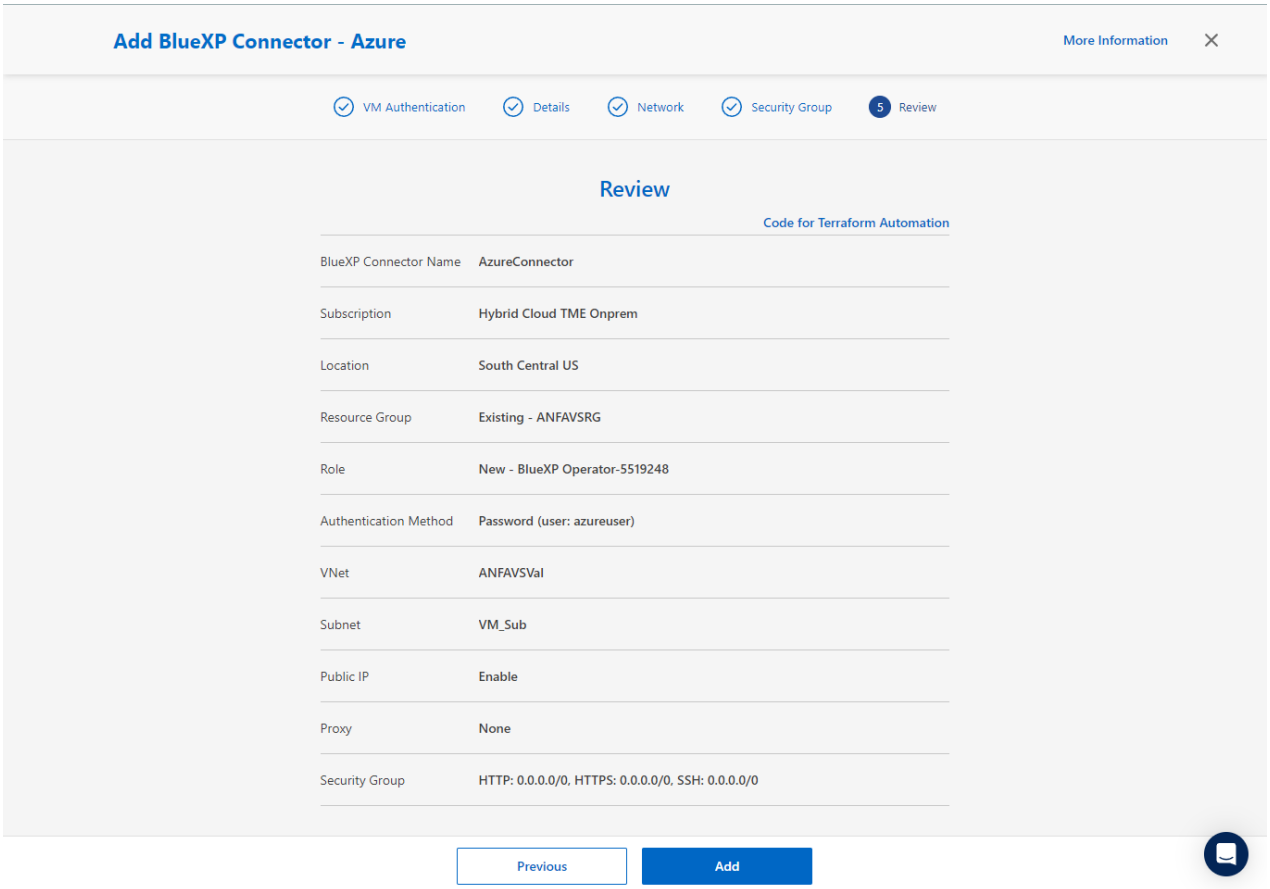
7. Configure a rede com a **VNet**, **Sub-rede** adequada e desabilite o **IP público**, mas certifique-se de que o conector tenha acesso à Internet no seu ambiente do Azure.



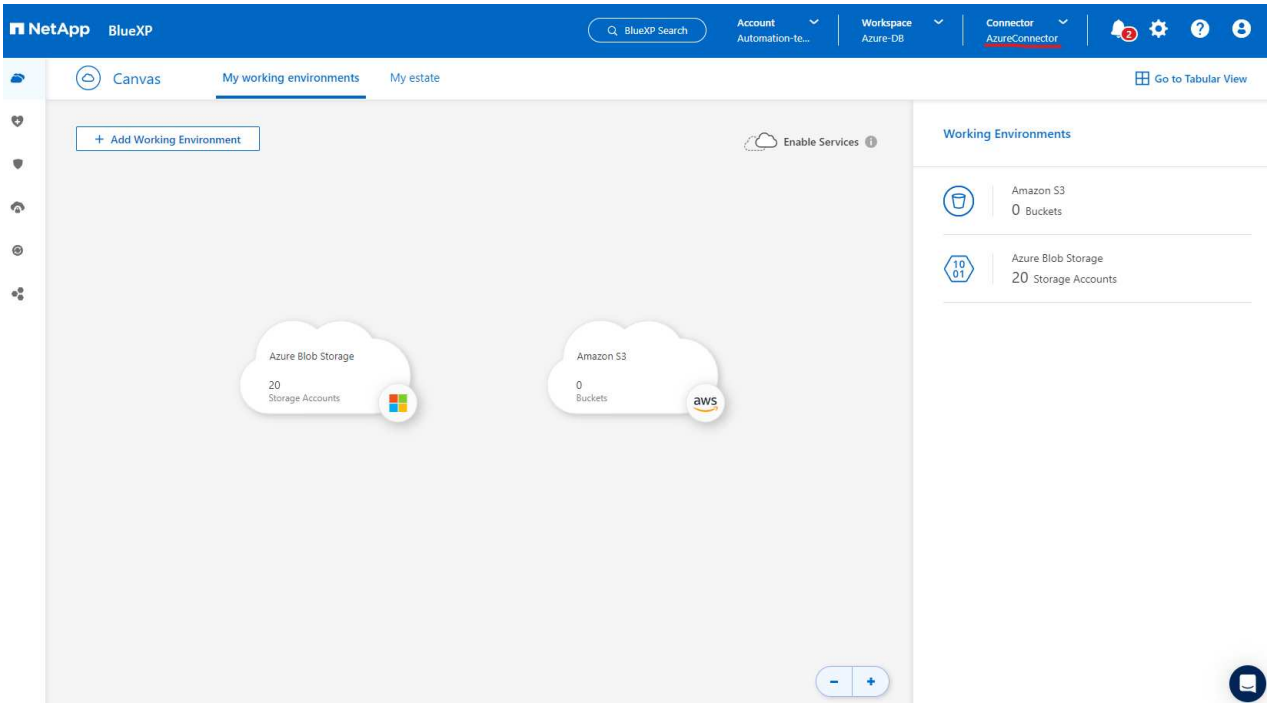
8. Configure o **Grupo de Segurança** para o conector que permite acesso HTTP, HTTPS e SSH.



9. 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 VM da instância do conector aparece no portal do Azure.

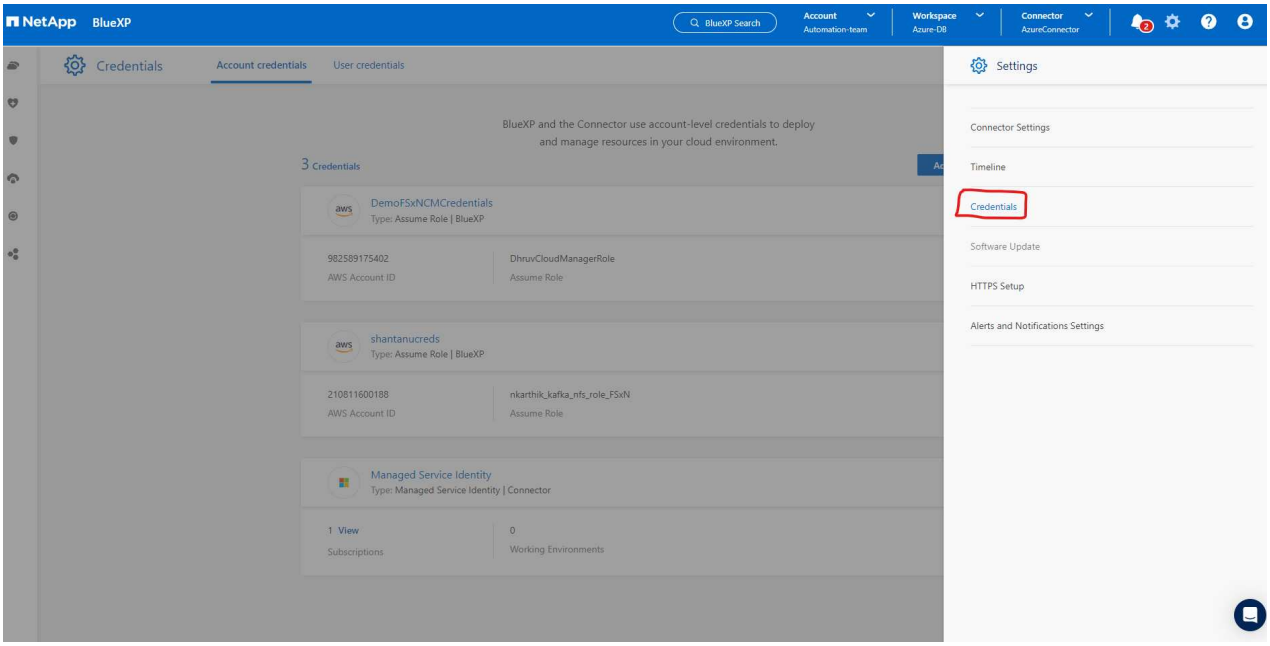


10. Após o conector ser implantado, o conector recém-criado aparece no menu suspenso **Conector**.

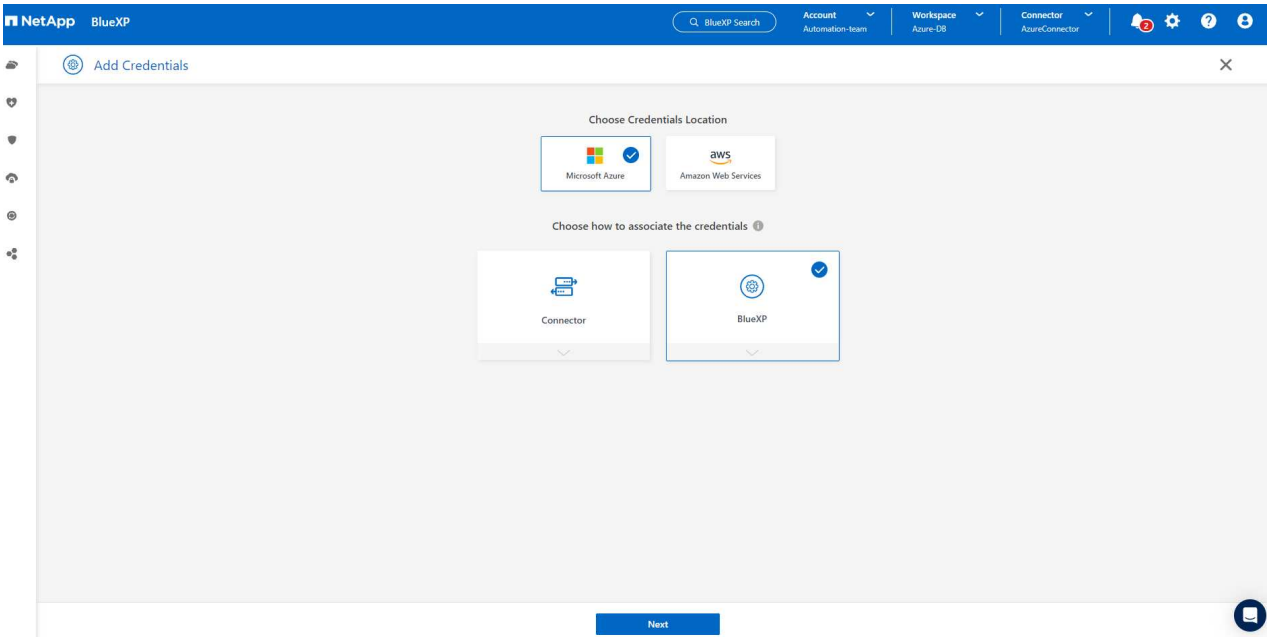


Definir uma credencial no BlueXP para acesso aos recursos do Azure

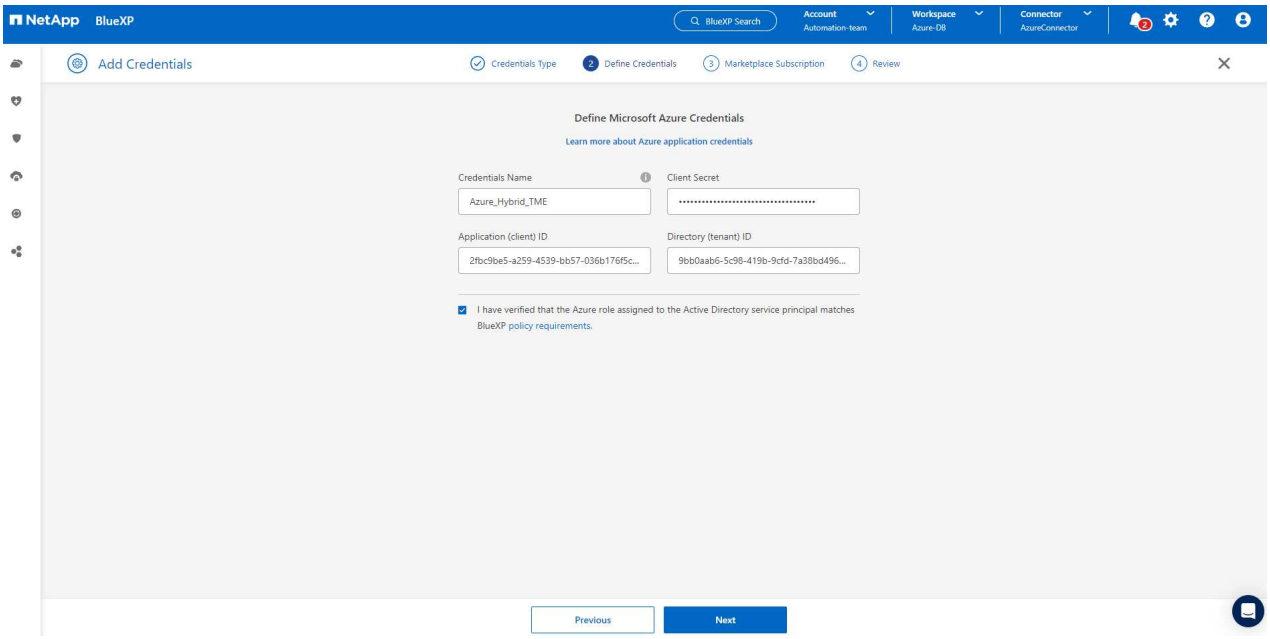
1. Clique no ícone de configuração no canto superior direito do console BlueXP para abrir a página **Credenciais da conta** e clique em **Adicionar credenciais** para iniciar o fluxo de trabalho de configuração de credenciais.



2. Escolha o local da credencial como - **Microsoft Azure - BlueXP**.

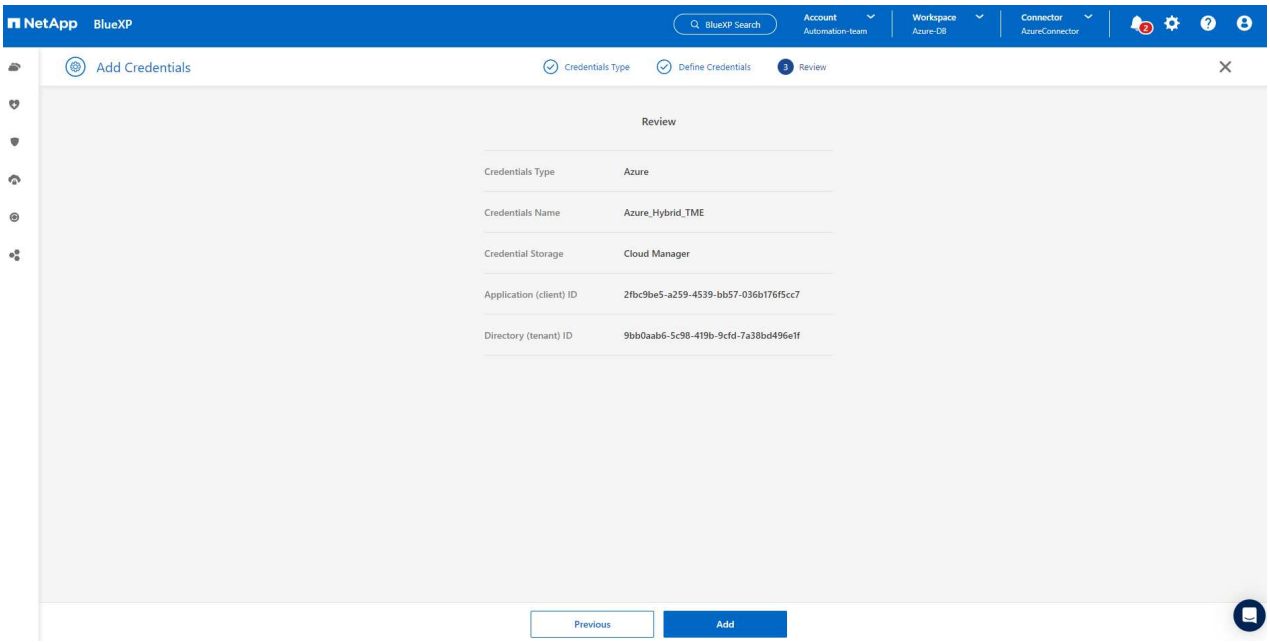


3. Defina as credenciais do Azure com o **Segredo do Cliente**, **ID do Cliente** e **ID do Locatário** adequados, que devem ter sido coletados durante o processo de integração anterior do BlueXP .

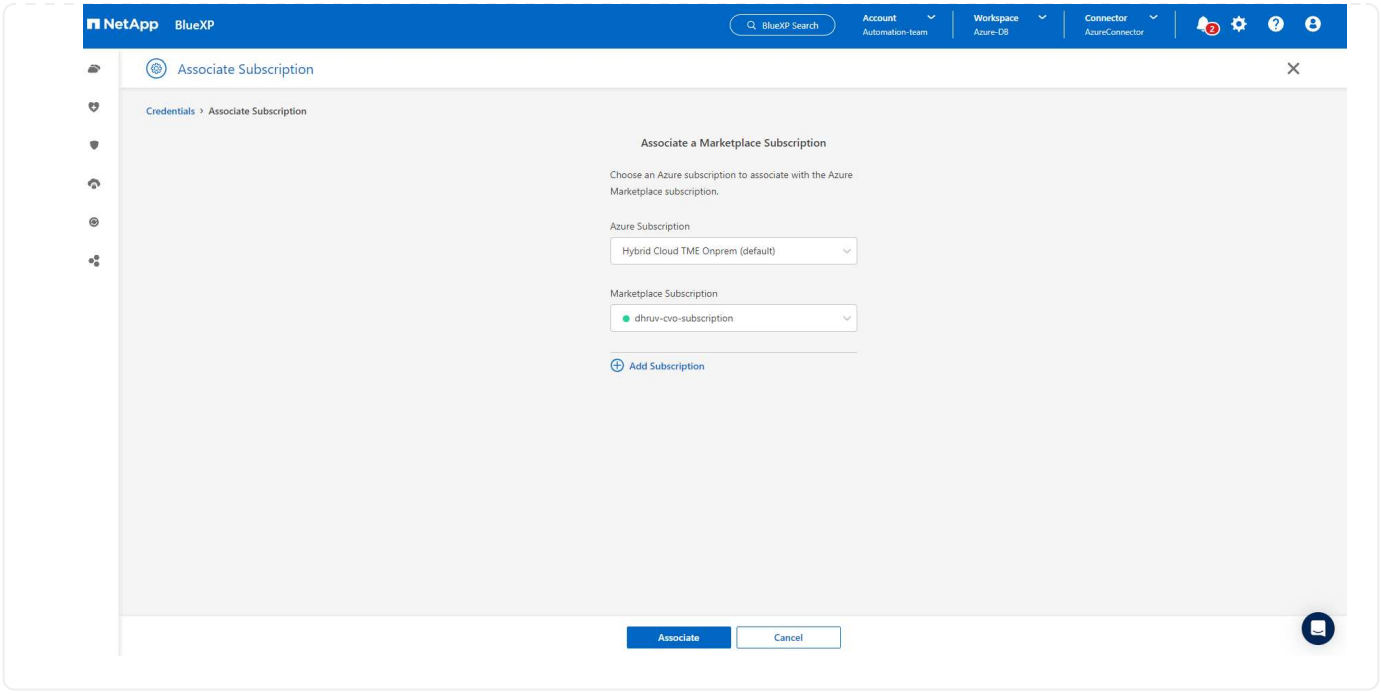


4. Revisar e **Adicionar**

.



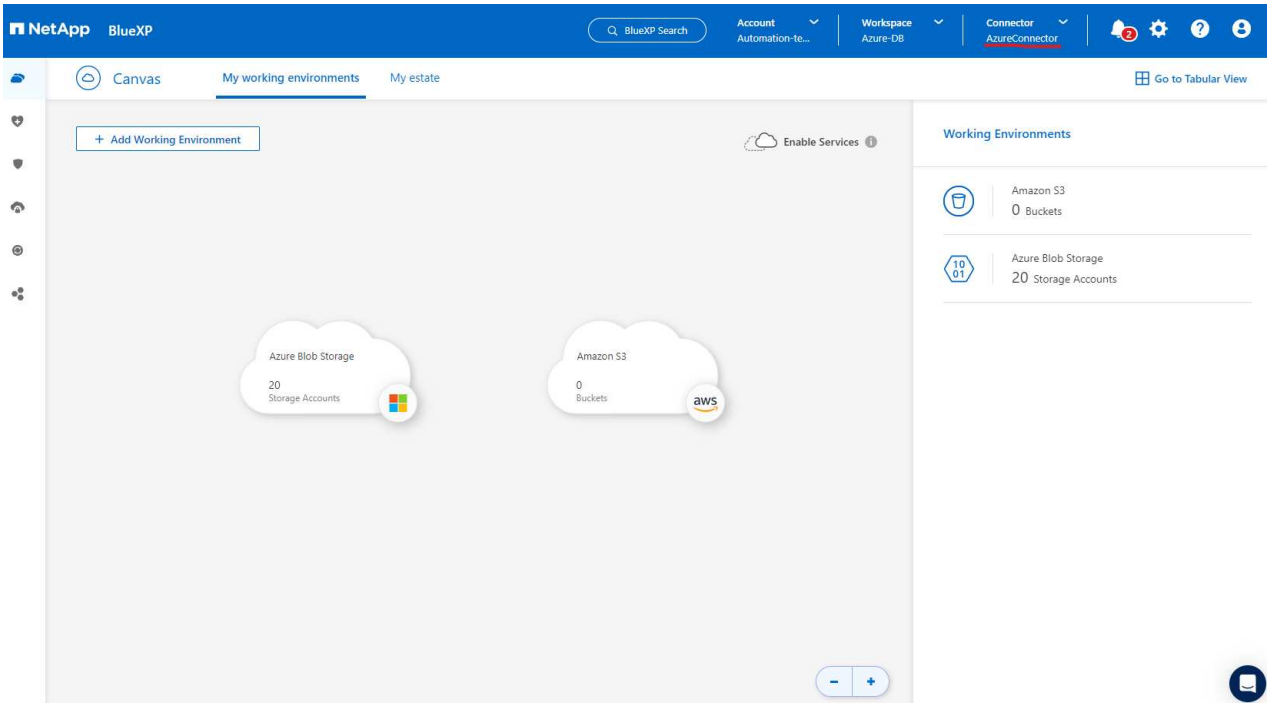
5. Também pode ser necessário associar uma **Assinatura do Marketplace** à credencial.



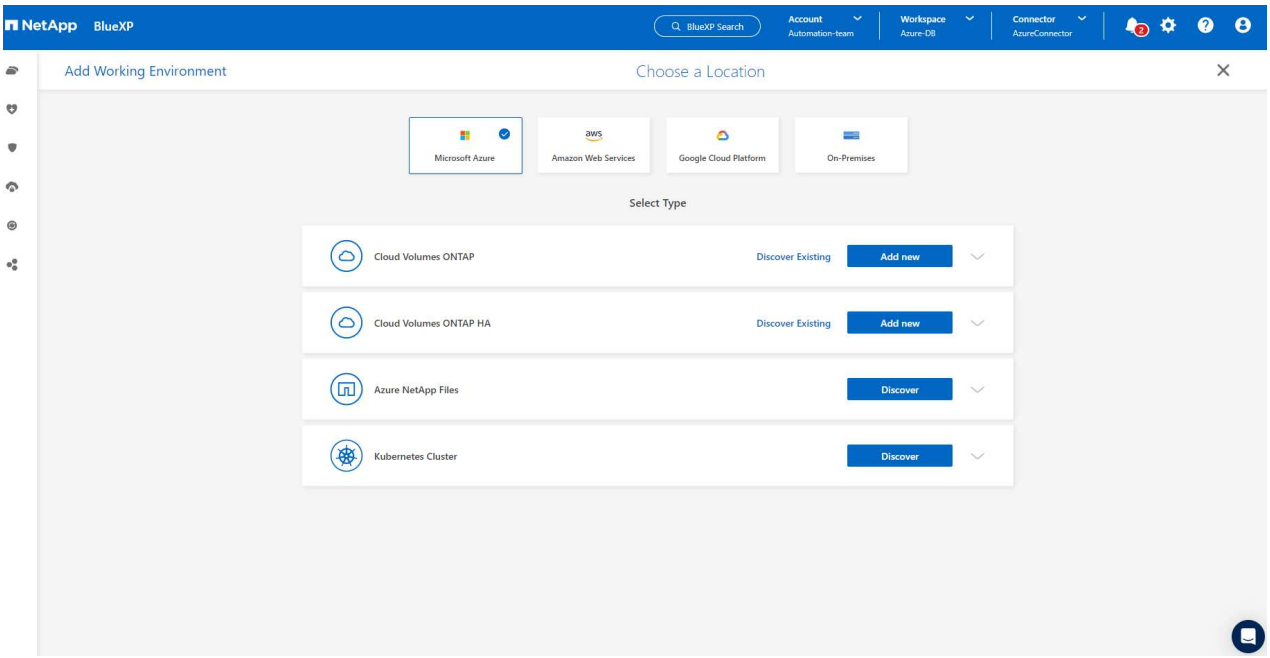
Configuração dos serviços do SnapCenter

Com a credencial do Azure configurada, os serviços do SnapCenter agora podem ser configurados com os seguintes procedimentos:

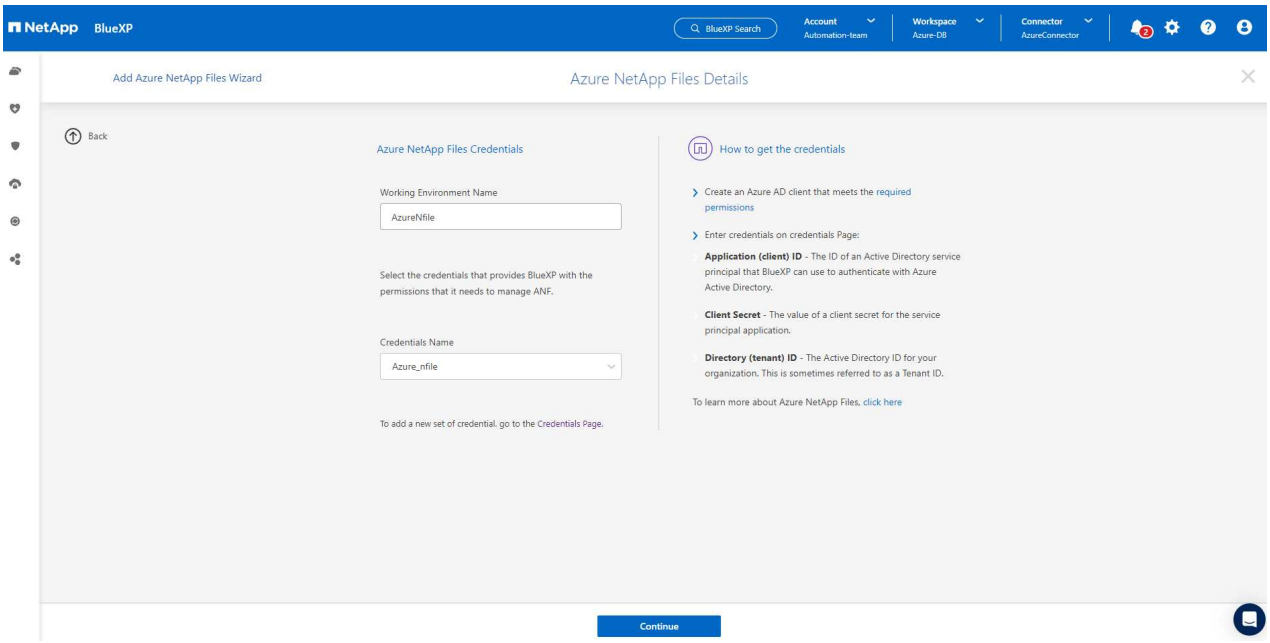
1. De volta à página do Canvas, em **Meu ambiente de trabalho** clique em **Adicionar ambiente de trabalho** para descobrir o Azure NetApp Files implantado no Azure.



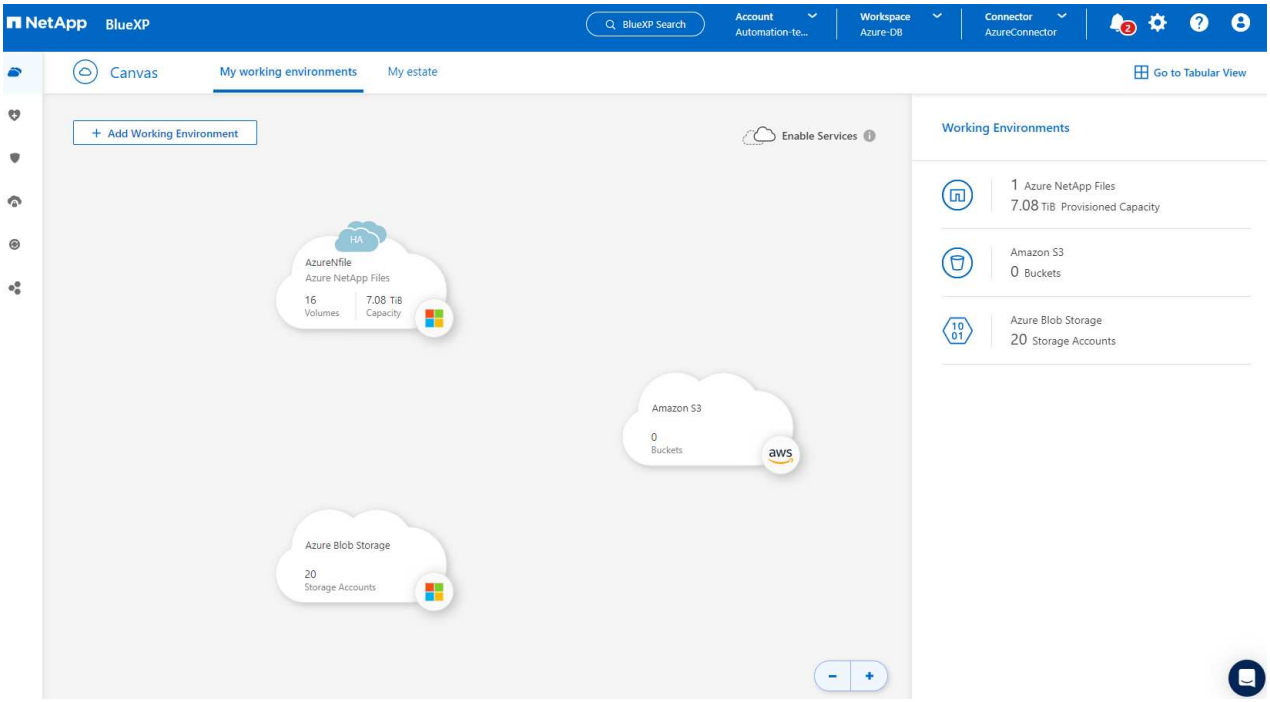
2. Escolha **Microsoft Azure** como local e clique em **Descobrir**.



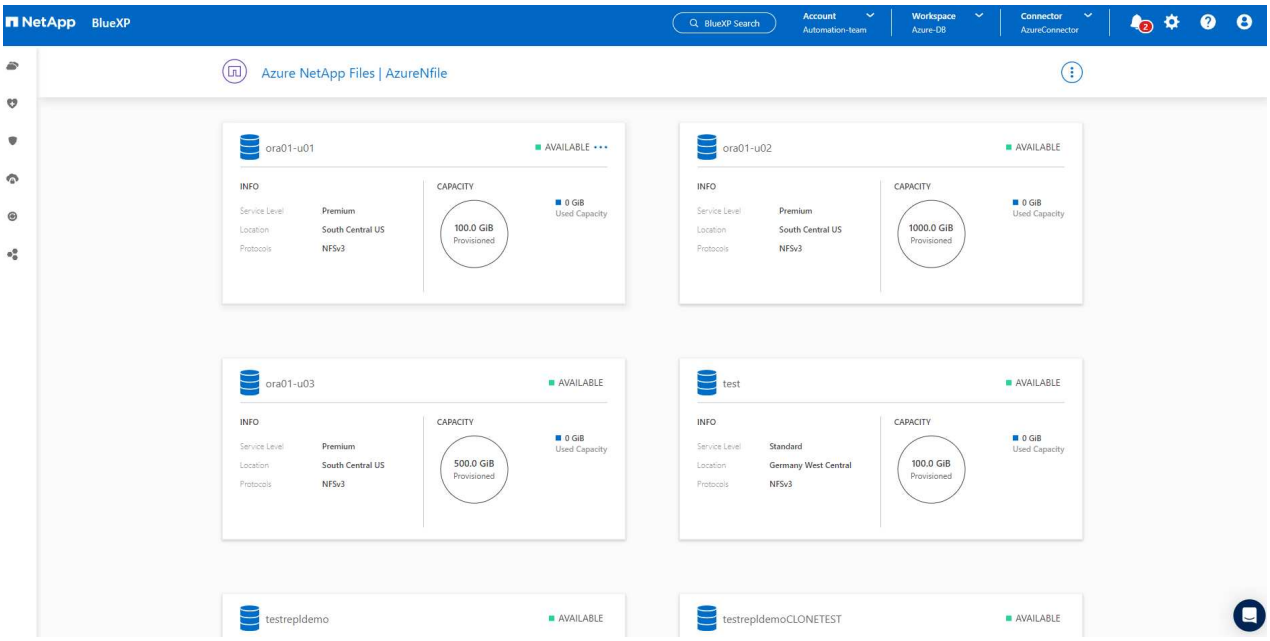
3. Nomeie **Ambiente de trabalho** e escolha **Nome da credencial** criado na seção anterior e clique em **Continuar**.



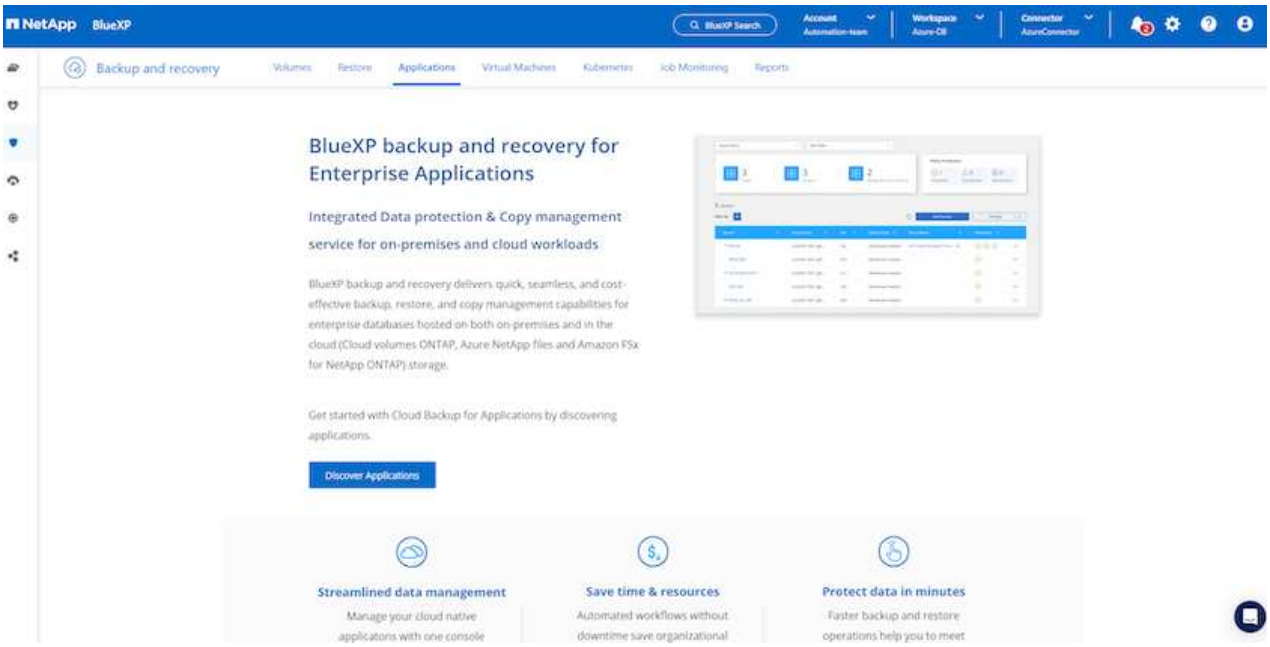
4. O console BlueXP retorna para **Meus ambientes de trabalho** e o Azure NetApp Files descoberto do Azure agora aparece no **Canvas**.



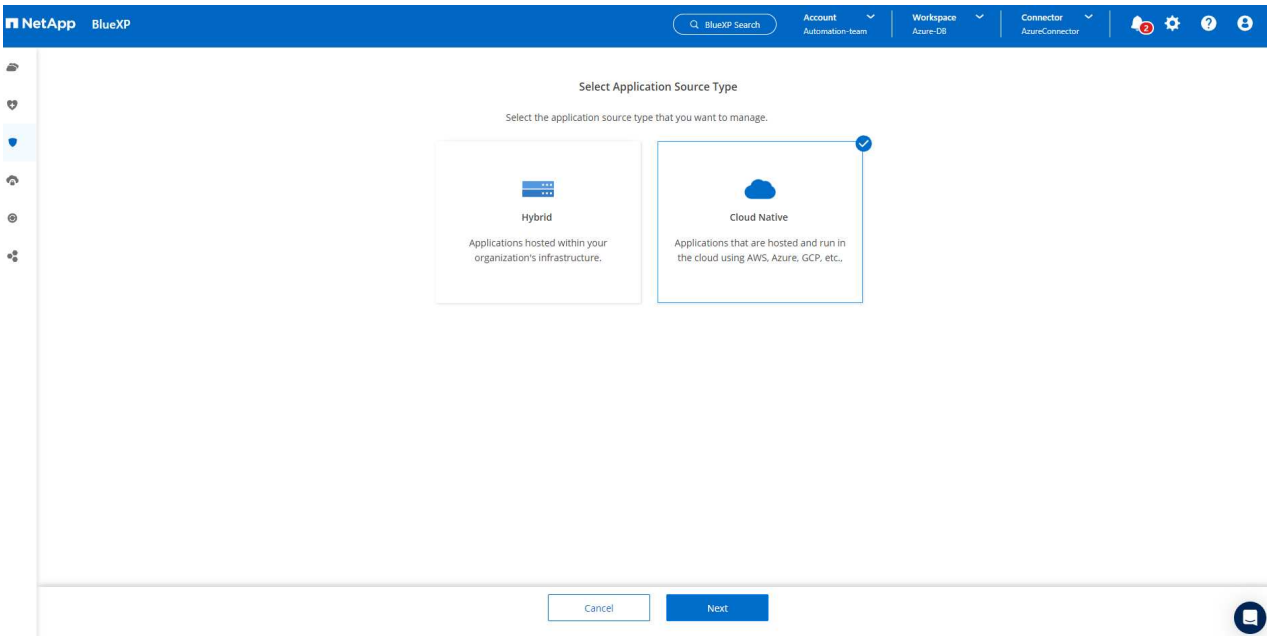
5. Clique no ícone * Azure NetApp Files* e depois em **Entrar em ambiente de trabalho** para visualizar os volumes do banco de dados Oracle implantados no armazenamento do Azure NetApp Files .



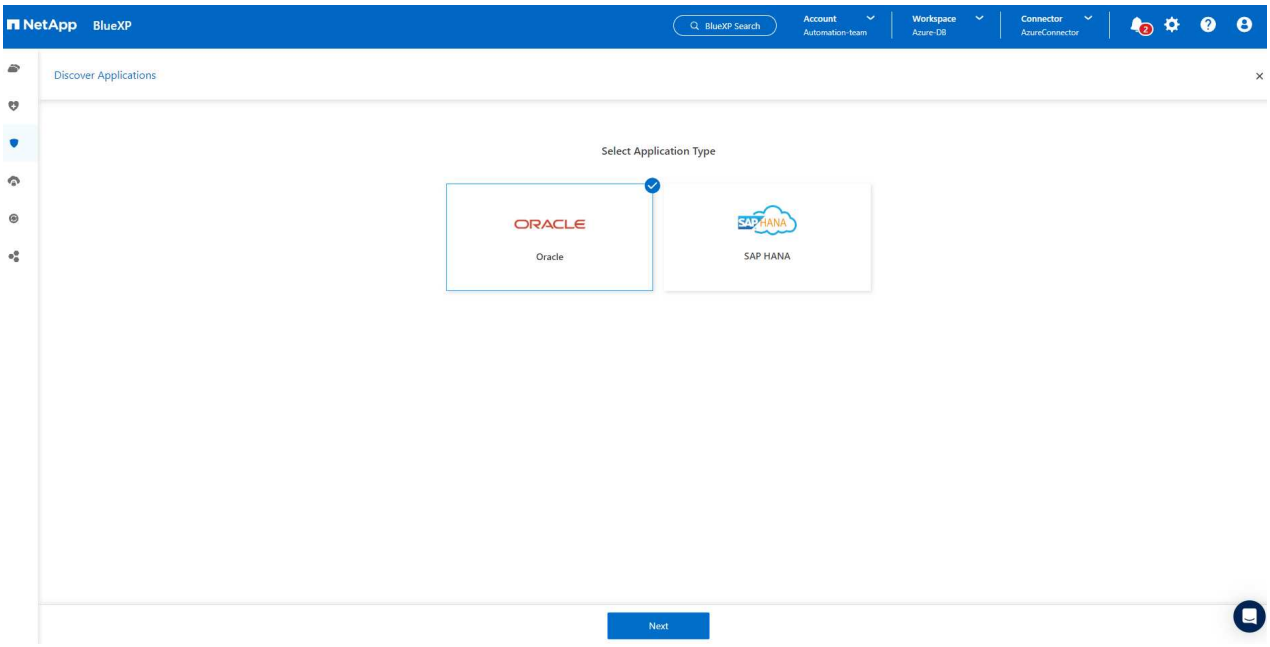
6. Na barra lateral esquerda do console, passe o mouse sobre o ícone de proteção e clique em **Proteção** > **Aplicativos** para abrir a página de inicialização de aplicativos. Clique em **Descobrir aplicativos**.



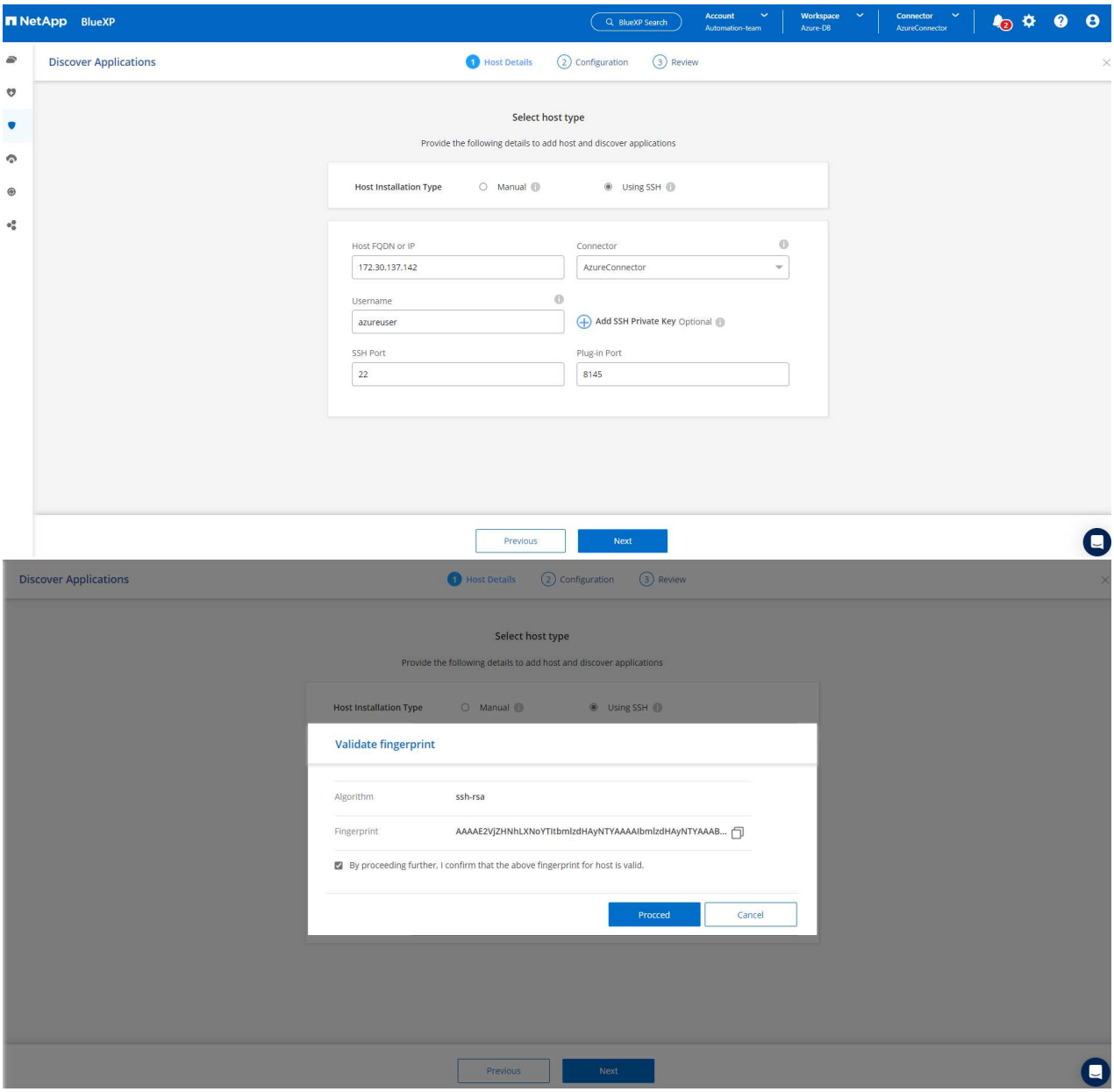
7. Selecione **Cloud Native** como o tipo de origem do aplicativo.



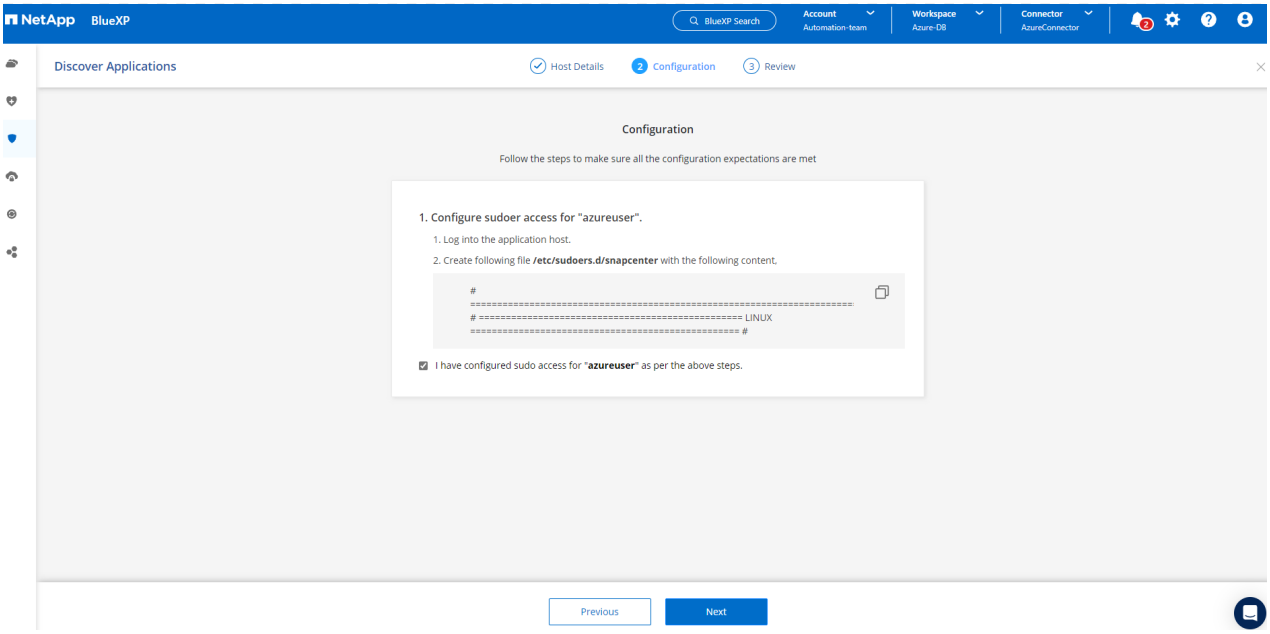
8. Escolha **Oracle** para o tipo de aplicativo e clique em **Avançar** para abrir a página de detalhes do host.



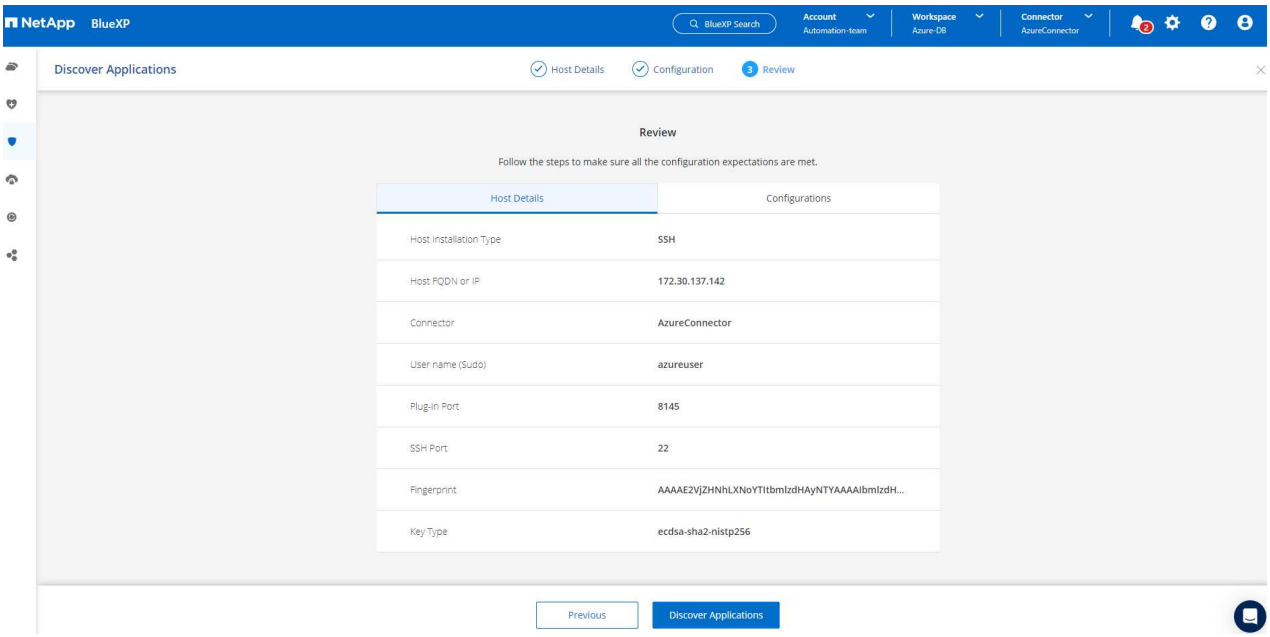
9. Selecione **Usando SSH** e forneça os detalhes da VM Oracle Azure, como **endereço IP**, **conector**, **nome de usuário** de gerenciamento da VM Azure, como azureuser. Clique em **Adicionar chave privada SSH** para colar o par de chaves SSH que você usou para implantar a VM do Oracle Azure. Você também será solicitado a confirmar a impressão digital.



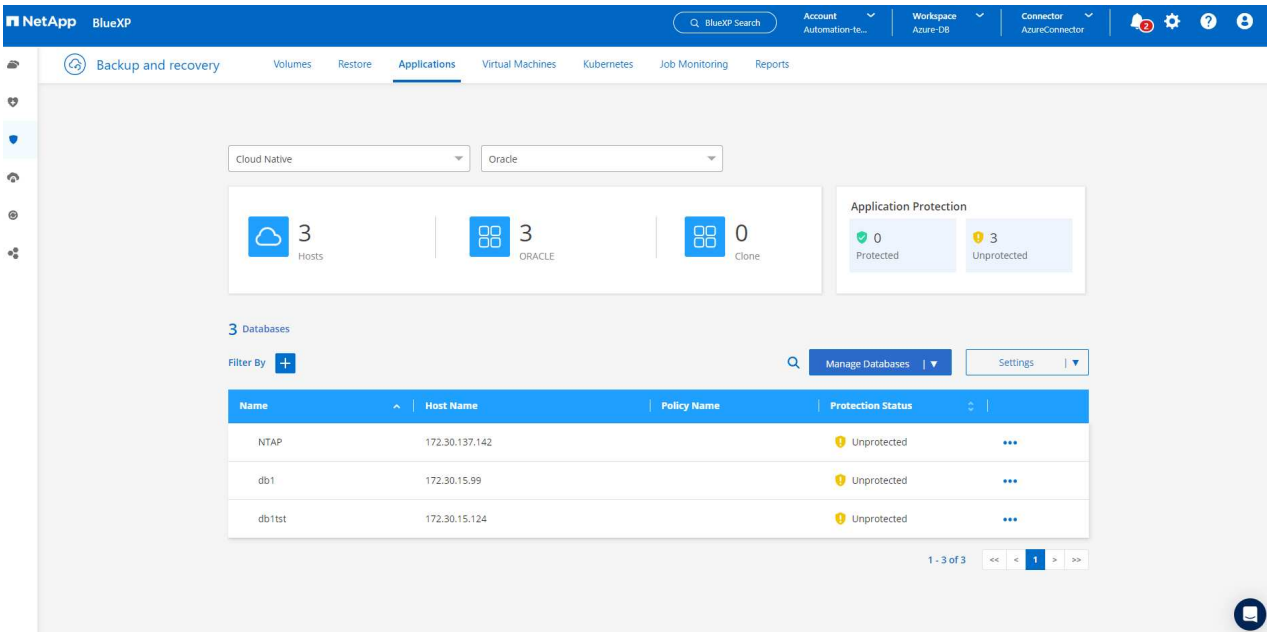
10. Vá para a próxima página **Configuração** para configurar o acesso sudoer na VM do Oracle Azure.



11. Revise e clique em **Descobrir aplicativos** para instalar um plug-in na VM do Oracle Azure e descobrir o banco de dados Oracle na VM em uma única etapa.



12. Os bancos de dados Oracle descobertos na VM do Azure são adicionados a **Aplicativos**, e a página **Aplicativos** lista o número de hosts e bancos de dados Oracle no ambiente. O banco de dados **Status de Proteção** inicialmente é exibido como **Desprotegido**.



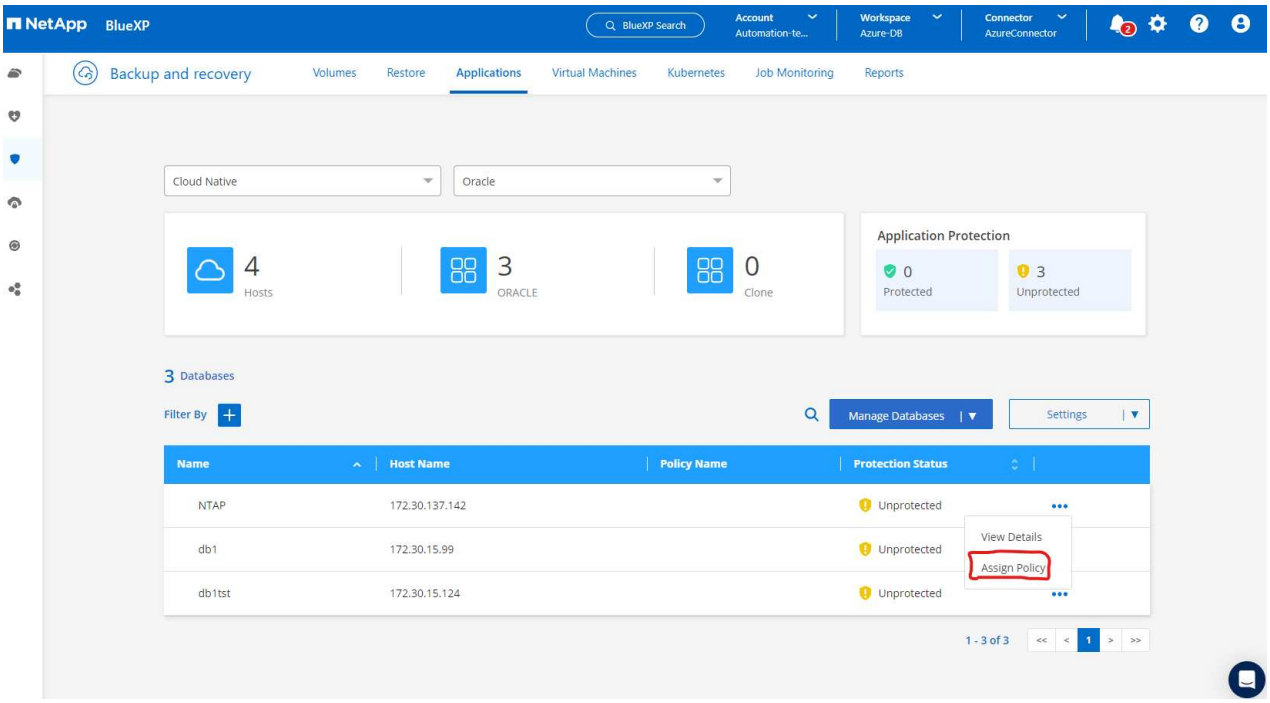
Isso conclui a configuração inicial dos serviços do SnapCenter para Oracle. As próximas três seções deste documento descrevem as operações de backup, restauração e clonagem do banco de dados Oracle.

Backup de banco de dados Oracle

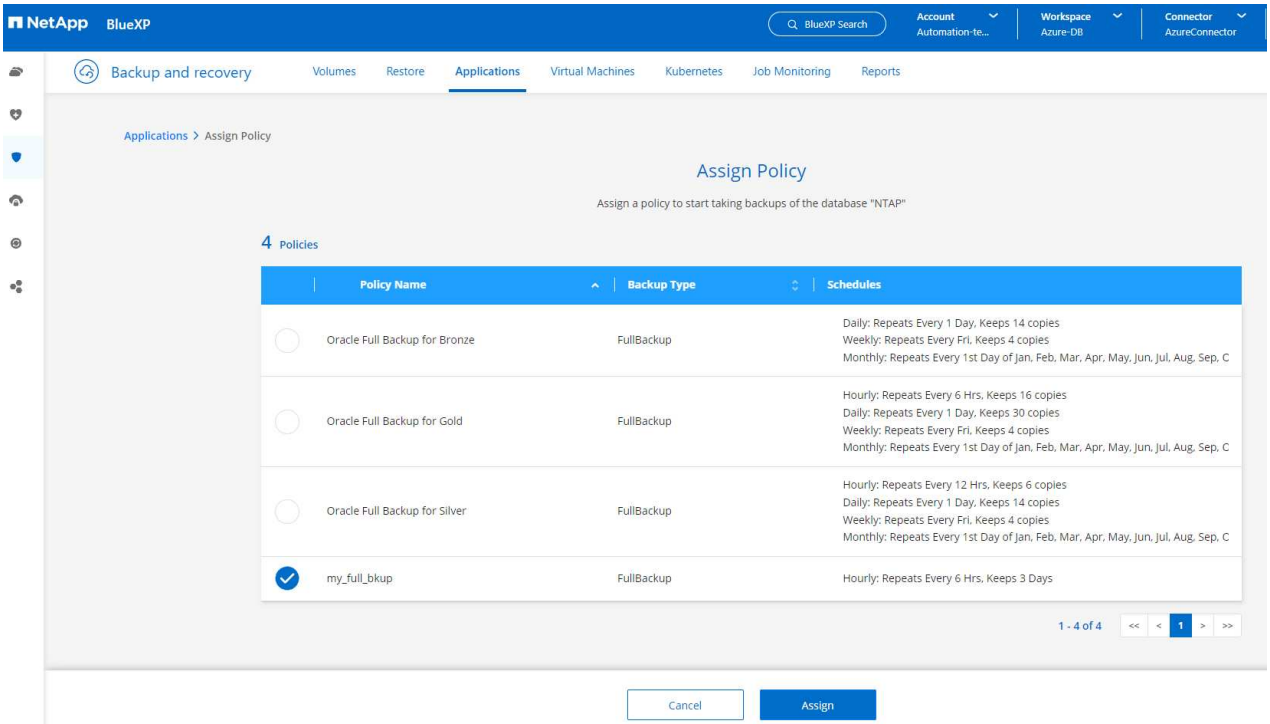
1. Nosso banco de dados Oracle de teste na VM do Azure está configurado com três volumes com um armazenamento total agregado de cerca de 1,6 TiB. Isso fornece contexto sobre o momento certo para o backup instantâneo, restauração e clonagem de um banco de dados desse tamanho.

```
[oracle@acao-ora01 ~]$ df -h
Filesystem                 Size  Used Avail Use% Mounted on
devtmpfs                   7.9G     0  7.9G   0% /dev
tmpfs                      7.9G     0  7.9G   0% /dev/shm
tmpfs                      7.9G   17M  7.9G   1% /run
tmpfs                      7.9G     0  7.9G   0% /sys/fs/cgroup
/dev/mapper/rootvg-rootlv   40G   23G   15G  62% /
/dev/mapper/rootvg-usrlv   9.8G  1.6G  7.7G  18% /usr
/dev/sda2                  496M  115M  381M  24% /boot
/dev/mapper/rootvg-varlv   7.9G  787M  6.7G  11% /var
/dev/mapper/rootvg-homelv  976M  323M  586M  36% /home
/dev/mapper/rootvg-optlv   2.0G  9.6M  1.8G   1% /opt
/dev/mapper/rootvg-tmplv   2.0G   22M  1.8G   2% /tmp
/dev/sda1                  500M  6.8M  493M   2% /boot/efi
172.30.136.68:/ora01-u01   100G   23G   78G  23% /u01
172.30.136.68:/ora01-u03   500G  117G  384G  24% /u03
172.30.136.68:/ora01-u02  1000G  804G  197G  81% /u02
tmpfs                      1.6G     0  1.6G   0% /run/user/1000
[oracle@acao-ora01 ~]$
```

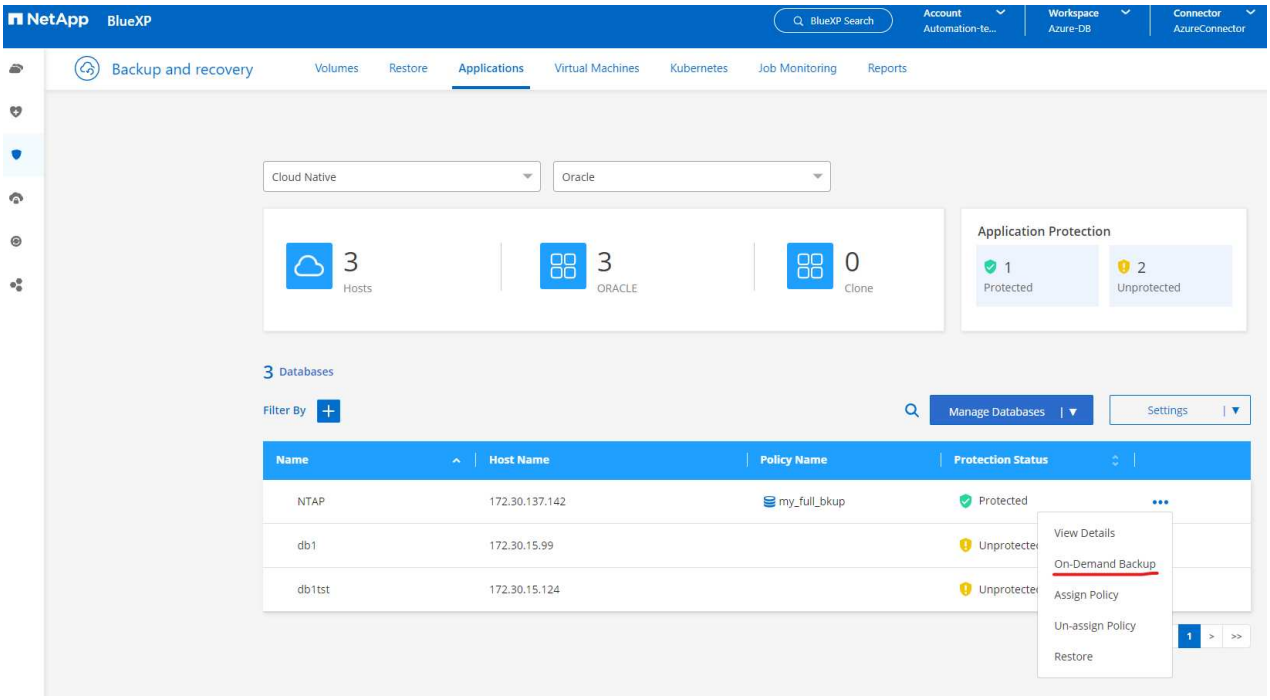
1. Para proteger o banco de dados, clique nos três pontos ao lado do **Status de proteção** do banco de dados e, em seguida, clique em **Atribuir política** para visualizar as políticas de proteção de banco de dados padrão pré-carregadas ou definidas pelo usuário que podem ser aplicadas aos seus bancos de dados Oracle. Em **Configurações** - **Políticas**, você tem a opção de criar sua própria política com uma frequência de backup personalizada e uma janela de retenção de dados de backup.



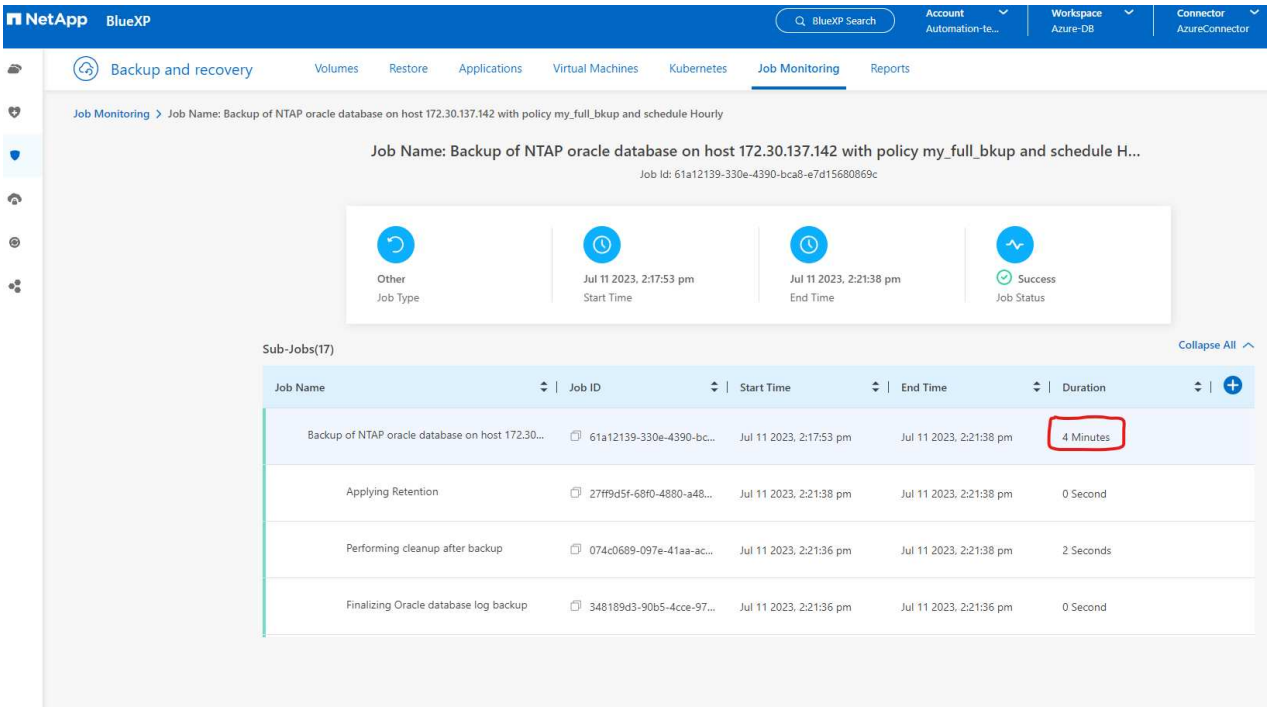
2. Quando estiver satisfeito com a configuração da política, você poderá **Atribuir** a política de sua escolha para proteger o banco de dados.



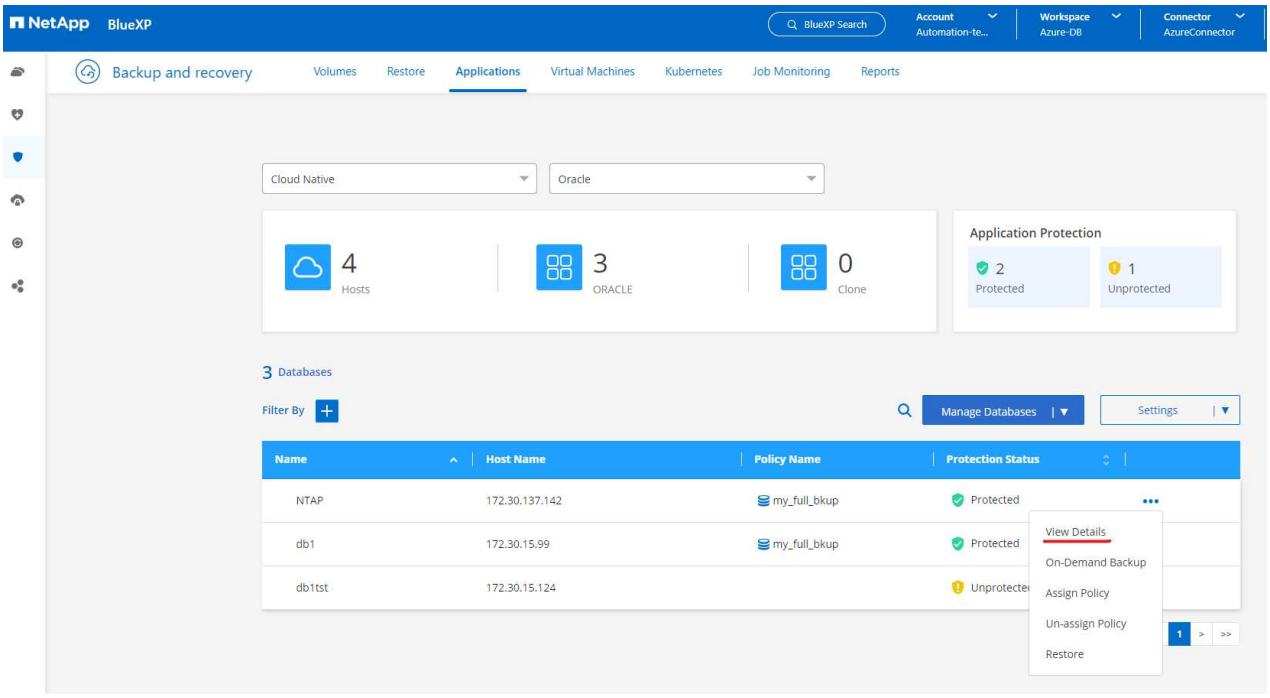
3. Após a aplicação da política, o status de proteção do banco de dados muda para **Protegido** com uma marca de seleção verde. O BlueXP executa o backup instantâneo de acordo com o agendamento definido. Além disso, o **Backup ON-Demand** está disponível no menu suspenso de três pontos, conforme mostrado abaixo.



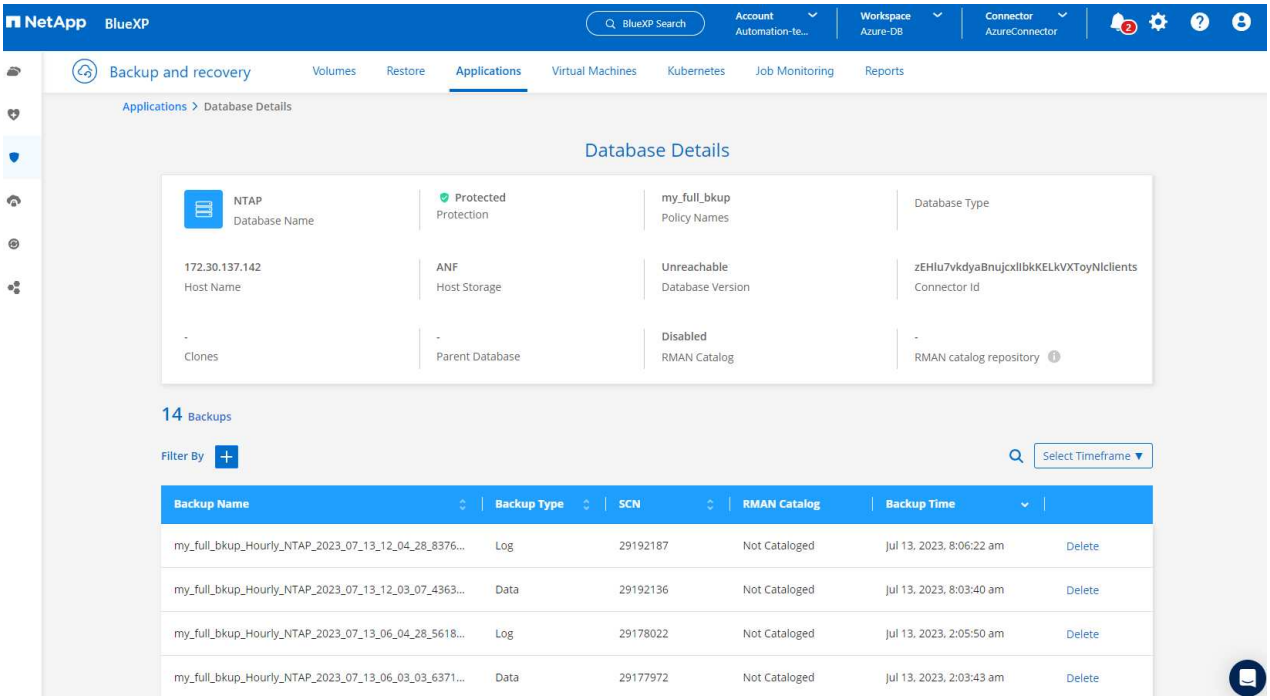
4. Na aba **Monitoramento de Tarefas**, os detalhes da tarefa de backup podem ser visualizados. Nossos resultados de teste mostraram que levou cerca de 4 minutos para fazer backup de um banco de dados Oracle de aproximadamente 1,6 TiB.



5. No menu suspenso de três pontos **Exibir detalhes**, você pode visualizar os conjuntos de backup criados a partir do backup instantâneo.

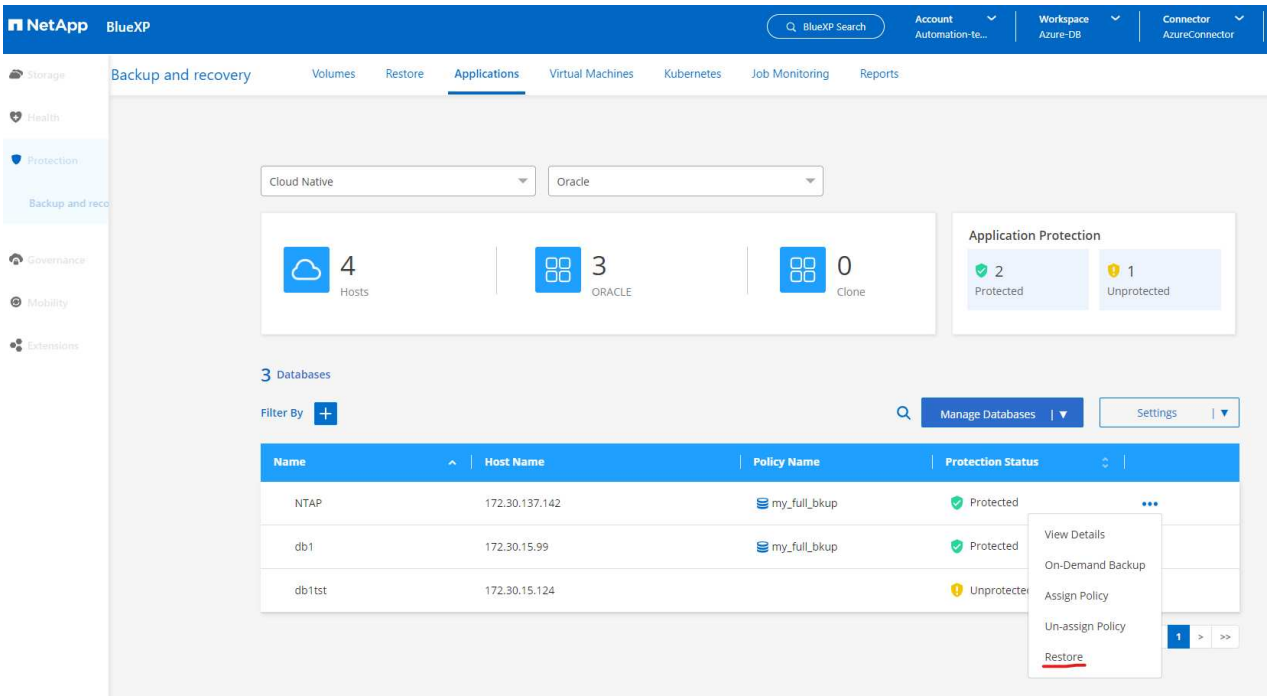


6. Os detalhes do backup do banco de dados incluem **Nome do backup**, **Tipo de backup**, **SCN**, **Catálogo RMAN** e **Hora do backup**. Um conjunto de backup contém instantâneos consistentes com o aplicativo para volume de dados e volume de log, respectivamente. Um instantâneo do volume de log ocorre logo após um instantâneo do volume de dados do banco de dados. Você pode aplicar um filtro se estiver procurando um backup específico na lista de backups.

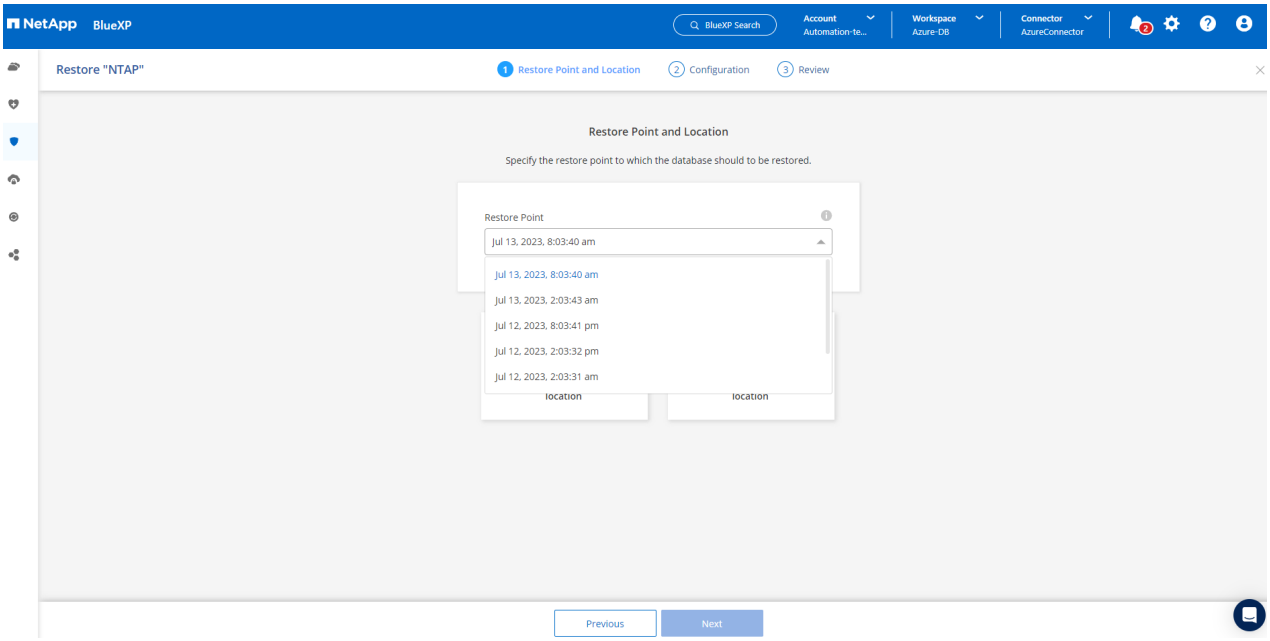


Restauração e recuperação de banco de dados Oracle

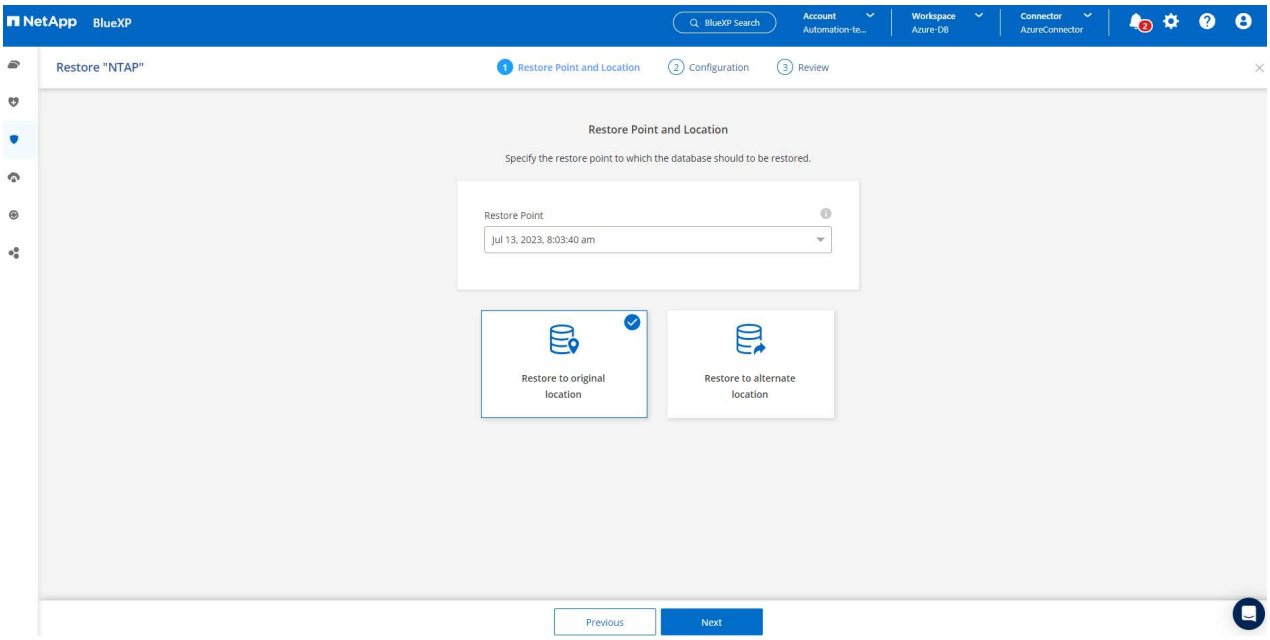
1. Para restaurar um banco de dados, clique no menu suspenso de três pontos do banco de dados específico a ser restaurado em **Aplicativos** e, em seguida, clique em **Restaurar** para iniciar o fluxo de trabalho de restauração e recuperação do banco de dados.



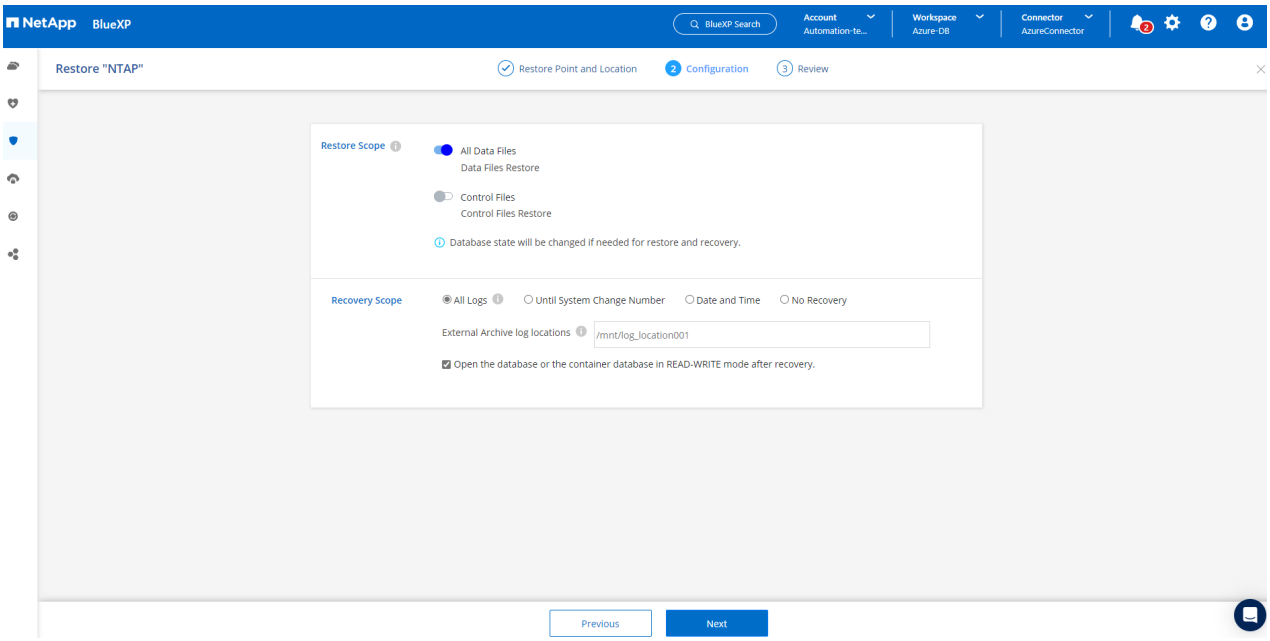
2. Escolha seu **Ponto de Restauração** por carimbo de data/hora. Cada registro de data e hora na lista representa um conjunto de backup de banco de dados disponível.



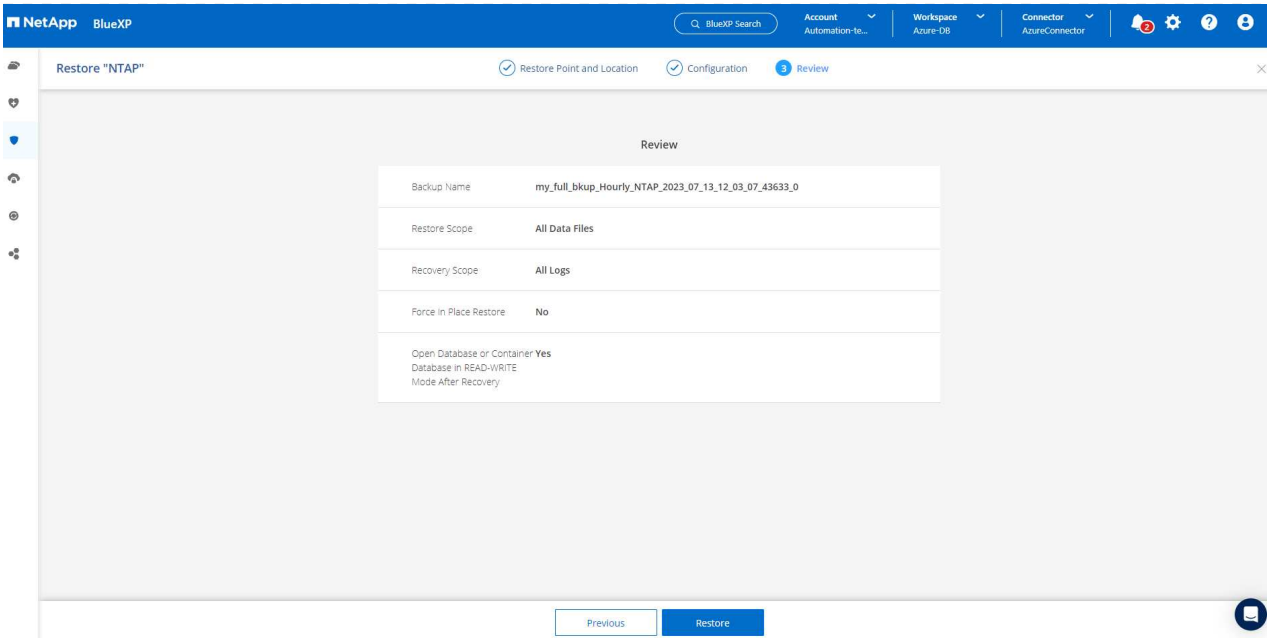
3. Selecione seu **Local de Restauração** para o **local original** para uma restauração e recuperação de banco de dados Oracle no local.



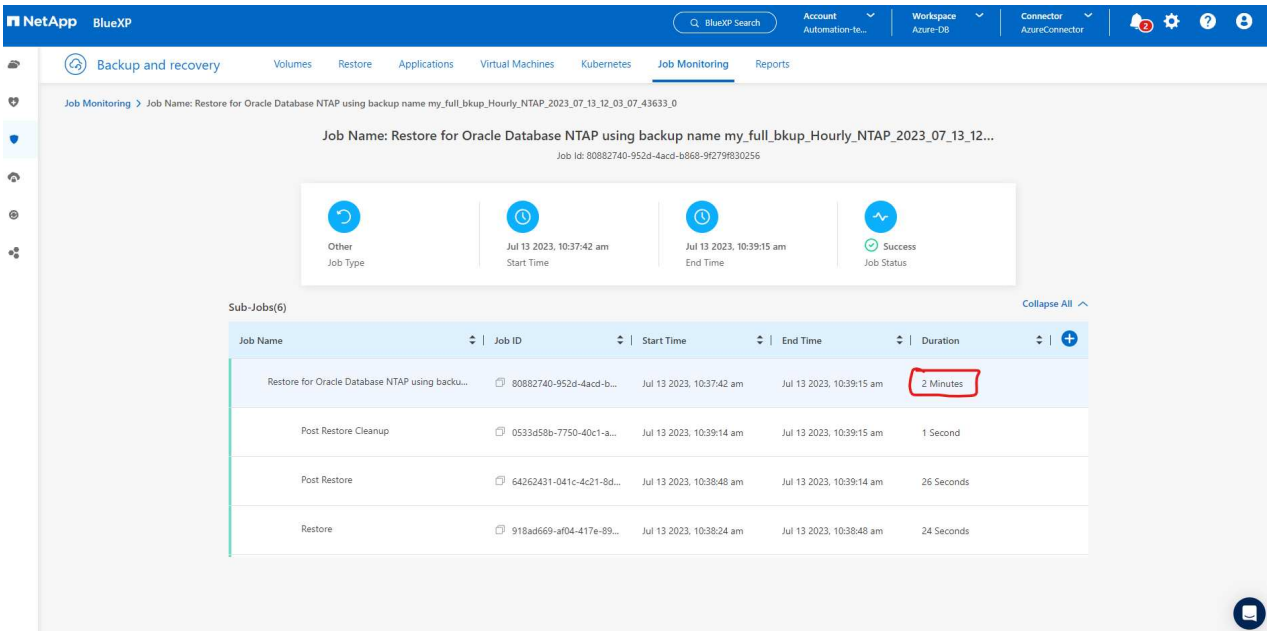
4. Defina seu **Escopo de Restauração** e **Escopo de Recuperação**. Todos os logs significam uma recuperação completa e atualizada, incluindo logs atuais.



5. Revise e **Restaure** para iniciar a restauração e recuperação do banco de dados.



6. Na aba **Monitoramento de Tarefas**, observamos que demorava 2 minutos para executar uma restauração completa do banco de dados e uma recuperação atualizada.

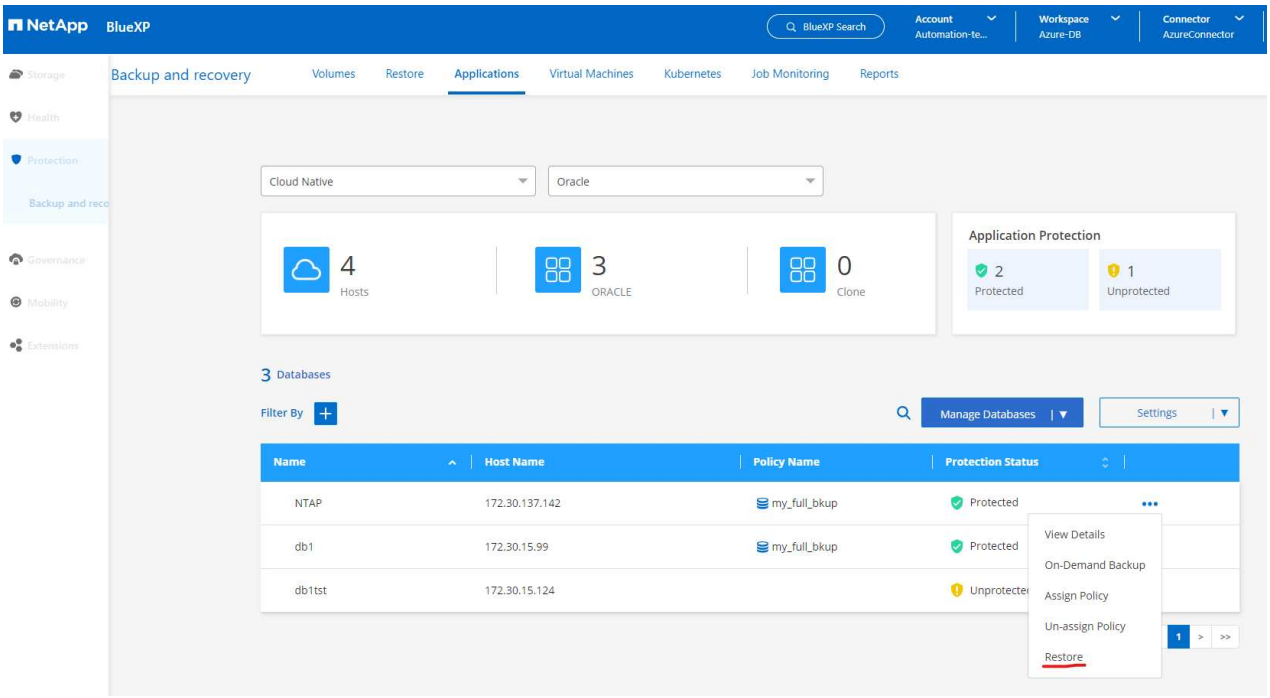


Clone de banco de dados Oracle

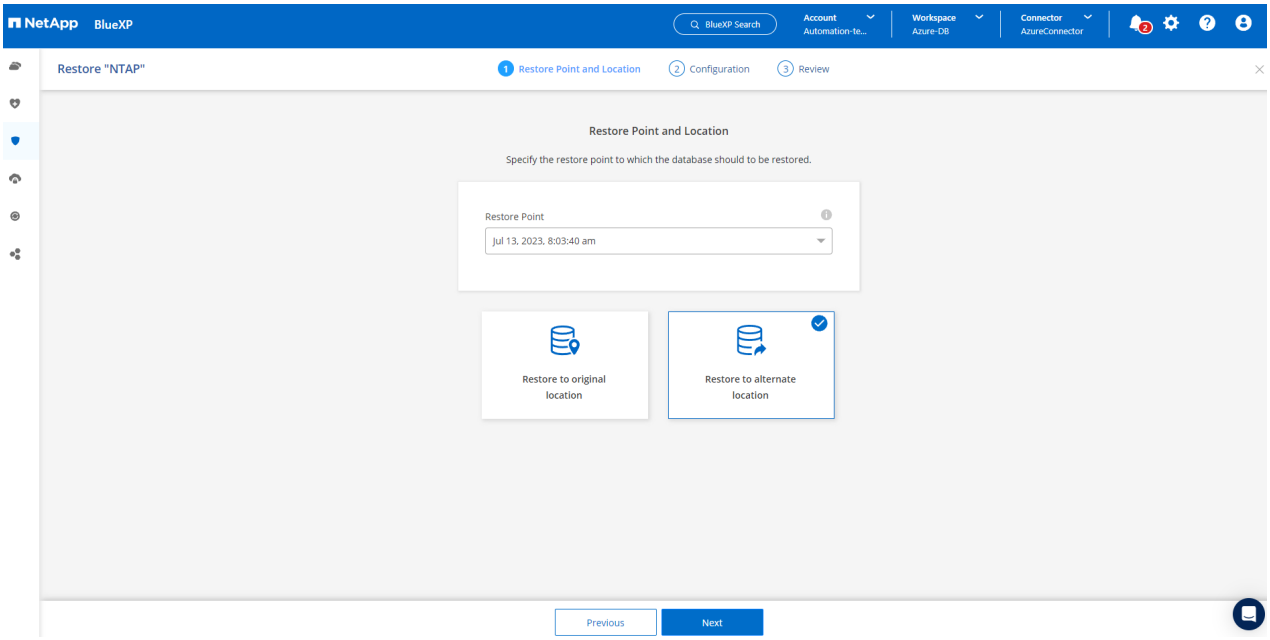
Os procedimentos de clonagem de banco de dados são semelhantes à restauração, mas para uma VM alternativa do Azure com pilha de software Oracle idêntica pré-instalada e configurada.

Certifique-se de que o armazenamento do Azure NetApp File tenha capacidade suficiente para um banco de dados clonado do mesmo tamanho que o banco de dados principal a ser clonado. A VM alternativa do Azure foi adicionada a **Aplicativos**.

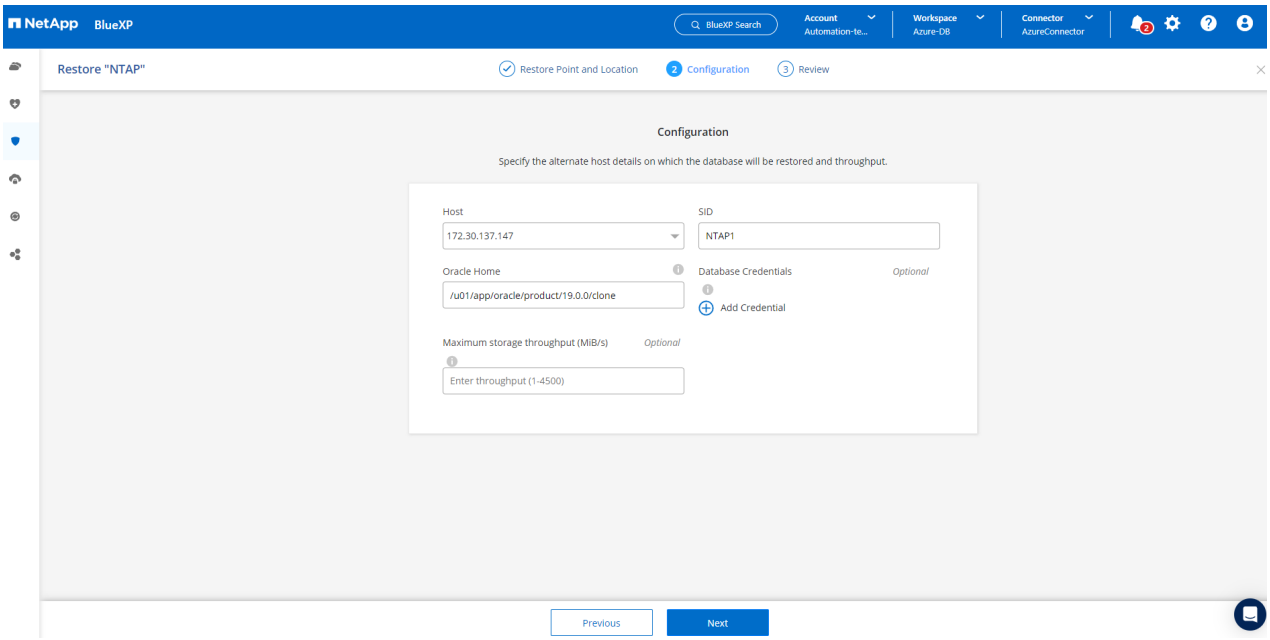
1. Clique no menu suspenso de três pontos do banco de dados específico a ser clonado em **Aplicativos** e, em seguida, clique em **Restaurar** para iniciar o fluxo de trabalho de clonagem.



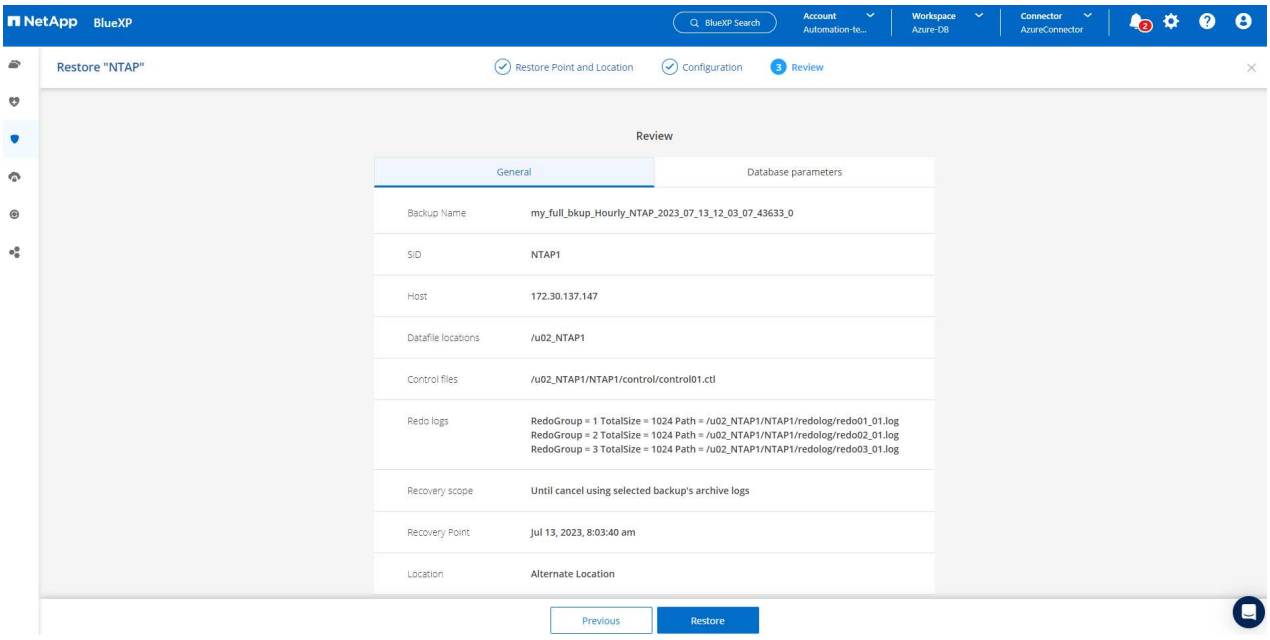
2. Selecione o **Ponto de restauração** e marque a opção **Restaurar em local alternativo**.



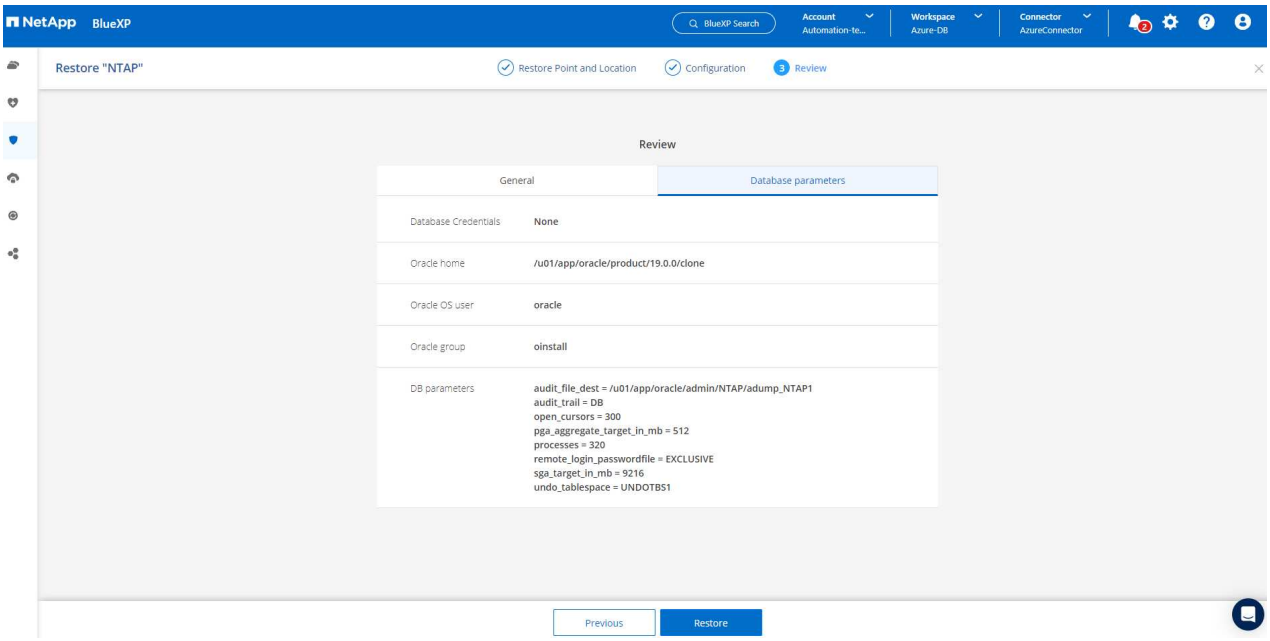
3. Na próxima página **Configuração**, defina o **Host** alternativo, o novo **SID** do banco de dados e o **Oracle Home** conforme configurado na VM alternativa do Azure.



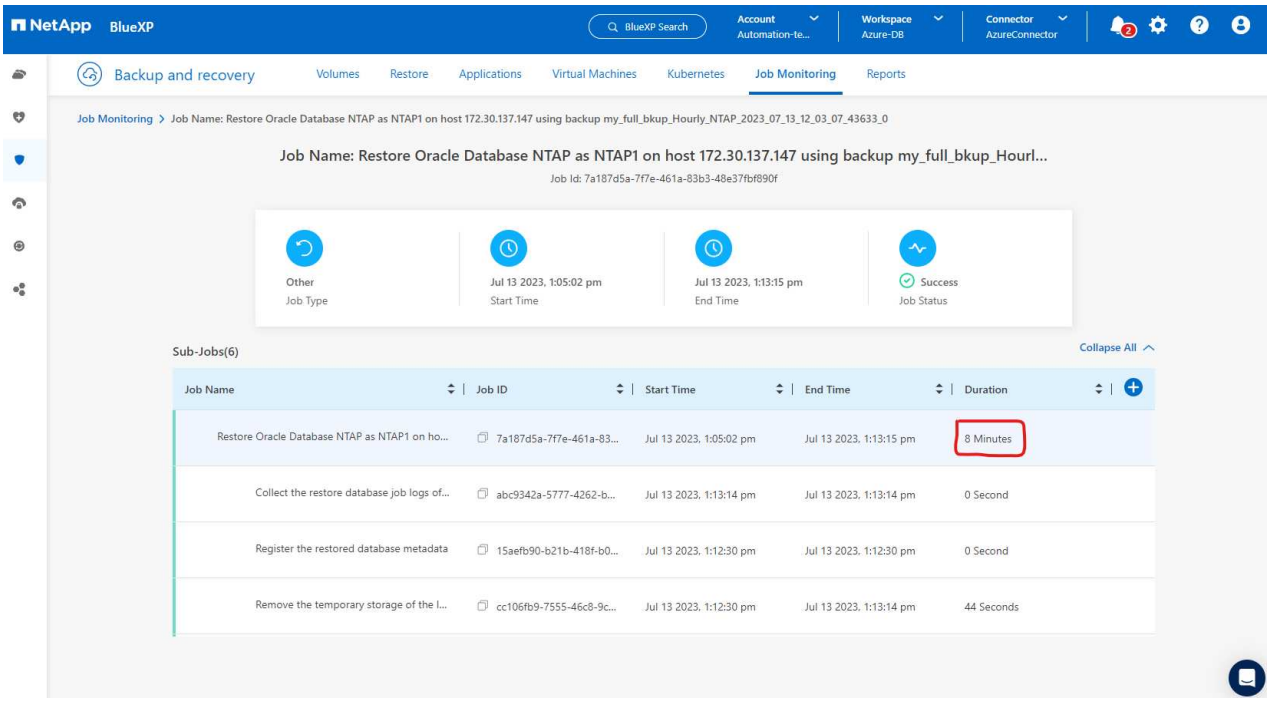
4. A página **Geral** de revisão mostra os detalhes do banco de dados clonado, como SID, host alternativo, locais de arquivos de dados, escopo de recuperação etc.



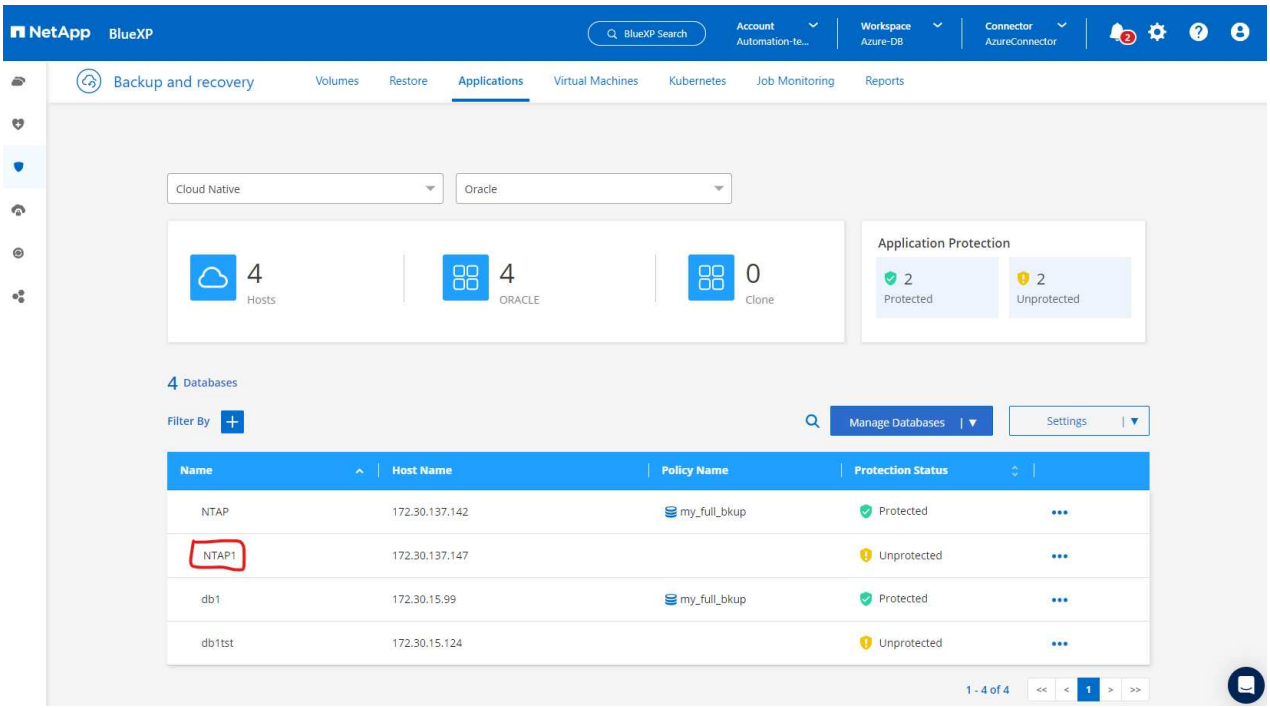
5. A página Revisar **Parâmetros do banco de dados** mostra os detalhes da configuração do banco de dados clonado, bem como algumas configurações de parâmetros do banco de dados.



6. Monitore o status do trabalho de clonagem na guia **Monitoramento de Trabalho**. Observamos que levou 8 minutos para clonar um banco de dados Oracle de 1,6 TiB.



7. Valide o banco de dados clonado na página **Aplicativos** do BlueXP que mostrou que o banco de dados clonado foi imediatamente registrado no BlueXP.



8. Valide o banco de dados clonado na VM do Oracle Azure que mostrou que o banco de dados clonado estava sendo executado conforme o esperado.

```
[oracle@acao-ora02 admin]$ cat /etc/oratab
#



# This file is used by ORACLE utilities.  It is created by root.sh
# and updated by either Database Configuration Assistant while creating
# a database or ASM Configuration Assistant while creating ASM instance.

# A colon, ':', is used as the field terminator.  A new line terminates
# the entry.  Lines beginning with a pound sign, '#', are comments.
#
# Entries are of the form:
#   $ORACLE_SID:$ORACLE_HOME:<N|Y>:
#
# The first and second fields are the system identifier and home
# directory of the database respectively.  The third field indicates
# to the dbstart utility that the database should , "Y", or should not,
# "N", be brought up at system boot time.
#
# Multiple entries with the same $ORACLE_SID are not allowed.
#
#
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
NTAP1:/u01/app/oracle/product/19.0.0/clone:N
[oracle@acao-ora02 admin]$ export ORACLE_SID=NTAP1
[oracle@acao-ora02 admin]$ export ORACLE_HOME=/u01/app/oracle/product/19.0.0/clone
[oracle@acao-ora02 admin]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@acao-ora02 admin]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Jul 13 17:16:31 2023
Version 19.18.0.0.0

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


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

SQL> select name, open_mode, log_mode from v$database;

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

Isso conclui a demonstração de um backup, restauração e clonagem de banco de dados Oracle no Azure com o console NetApp BlueXP usando o SnapCenter Service.

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"

- Documentação de BlueXP backup and recovery

  "https://docs.netapp.com/us-en/cloud-manager-backup-restore/index.html"

- Azure NetApp Files

"https://azure.microsoft.com/en-us/products/netapp"

- Comece a usar o Azure

  "https://azure.microsoft.com/en-us/get-started/"

Informações sobre direitos autorais

Informações sobre marcas comerciais