



TR-4977: Backup, ripristino e clonazione di Oracle Database con SnapCenter Services - Azure

NetApp database solutions

NetApp
August 18, 2025

Sommario

- TR-4977: Backup, ripristino e clonazione di Oracle Database con SnapCenter Services - Azure 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 4
 - Definisci una credenziale in BlueXP per l'accesso alle risorse di Azure 12
 - Configurazione dei servizi SnapCenter 15
 - Backup del database Oracle 22
 - Ripristino e recupero del database Oracle 26
 - Clone del database Oracle 29
 - Informazioni aggiuntive 34

TR-4977: Backup, ripristino e clonazione di Oracle Database con SnapCenter Services - Azure

Allen Cao, Niyaz Mohamed, NetApp

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 .

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 su Azure NetApp Files. 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 volumi Azure NetApp Files e istanze di calcolo di Azure. È molto semplice configurare la protezione dei dati per il database Oracle distribuito su Azure NetApp Files con l'interfaccia utente BlueXP basata sul Web.

Questa soluzione affronta i seguenti casi d'uso:

- Backup del database con snapshot per database Oracle ospitati in Azure NetApp Files e macchine virtuali di Azure
- Ripristino del database Oracle in caso di guasto
- Clonazione rapida di database primari per ambienti di sviluppo, test o altri casi d'uso

Pubblico

Questa soluzione è destinata ai seguenti pubblici:

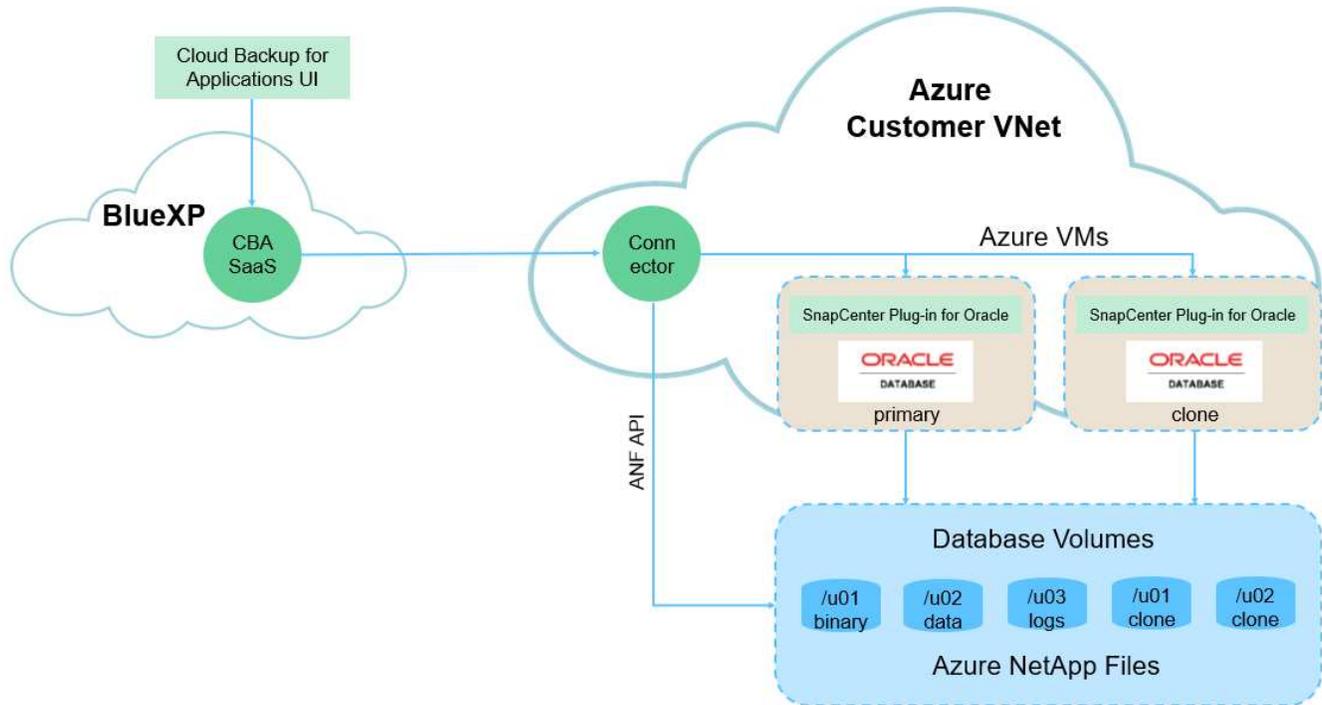
- L'amministratore di database che gestisce i database Oracle in esecuzione sullo storage Azure NetApp Files
- L'architetto di soluzioni interessato a testare il backup, il ripristino e la clonazione del database Oracle in Azure
- L'amministratore di archiviazione che supporta e gestisce l'archiviazione Azure NetApp Files
- Il proprietario dell'applicazione che possiede le applicazioni distribuite nell'archiviazione Azure NetApp Files e nelle VM di Azure

Ambiente di test e convalida della soluzione

I test e la convalida di questa soluzione sono stati eseguiti in un ambiente di laboratorio 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 Azure NetApp Files	Livello di servizio Premium	Tipo di QoS automatico e 4 TB di capacità di archiviazione in fase di test
Istanza di Azure per il calcolo	Standard B4ms (4 vCPU, 16 GiB di memoria)	Due istanze distribuite, una come server DB primario e l'altra come server DB clone

Software

RedHat Linux	Red Hat Enterprise Linux 8.7 (LVM) - x64 Gen2	Abbonamento RedHat distribuito per i test
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 v2.5.0-2822	Versione agente v2.5.0-2822

Fattori chiave per la considerazione dell'implementazione

- **Connettore da distribuire nella stessa rete virtuale/subnet dei database e Azure NetApp Files.** Se possibile, il connettore dovrebbe essere distribuito nelle stesse reti virtuali e gruppi di risorse di Azure, il che consente la connettività all'archiviazione Azure NetApp Files e alle istanze di calcolo di Azure.
- **Un account utente di Azure o un principio di servizio Active Directory creato nel portale di Azure per il connettore SnapCenter .** Per distribuire un connettore BlueXP sono necessarie autorizzazioni specifiche per creare e configurare una macchina virtuale e altre risorse di elaborazione, per configurare la rete e per ottenere l'accesso alla sottoscrizione di Azure. Richiede inoltre autorizzazioni per creare in seguito ruoli e autorizzazioni affinché il connettore possa funzionare. Crea un ruolo personalizzato in Azure con autorizzazioni e assegnalo all'account utente o al principio del servizio. Per maggiori dettagli consultare il seguente xref:./oracle/"[Configurare le autorizzazioni di Azure](#)" .
- **Una coppia di chiavi SSH creata nel gruppo di risorse di Azure.** La coppia di chiavi SSH viene assegnata all'utente della VM di Azure per l'accesso all'host del connettore e anche all'host della VM del database per la distribuzione e l'esecuzione di un plug-in. L'interfaccia utente della console di BlueXP utilizza la chiave SSH per distribuire il plug-in del servizio SnapCenter sull'host del database, per l'installazione del plug-in in un unico passaggio e l'individuazione del database dell'host dell'applicazione.
- **Una credenziale aggiunta alle impostazioni della console BlueXP .** Per aggiungere l'archiviazione Azure NetApp Files all'ambiente di lavoro BlueXP , è necessario configurare una credenziale che conceda le autorizzazioni per accedere ad Azure NetApp Files dalla console BlueXP nelle impostazioni della console BlueXP .
- **java-11-openjdk installato sull'host dell'istanza del database della macchina virtuale di Azure.** 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 un archivio Azure NetApp Files e un'istanza di elaborazione di Azure.

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 Azure NetApp Files.
- Guarda il seguente video tutorial

[Video dell'implementazione di Oracle e ANF](#)

Prerequisiti per la distribuzione del servizio SnapCenter

Per la distribuzione sono richiesti i seguenti prerequisiti.

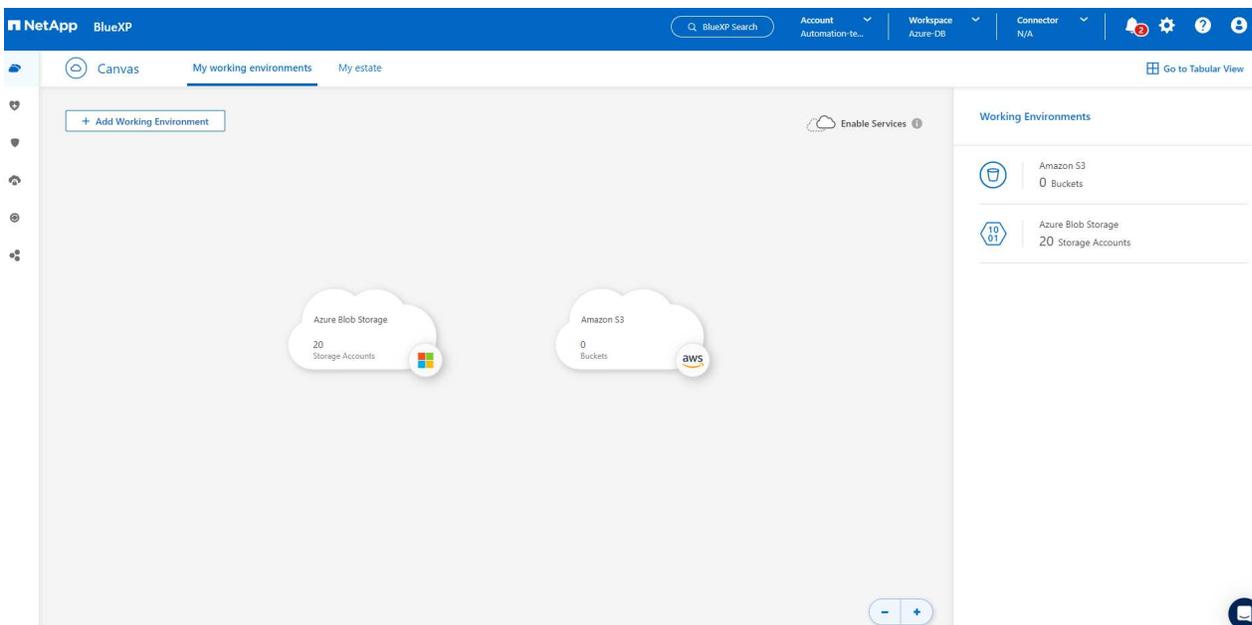
1. Un server di database Oracle primario su un'istanza di macchina virtuale di Azure con un database Oracle completamente distribuito e in esecuzione.
2. Un pool di capacità del servizio di archiviazione Azure NetApp Files distribuito in Azure con capacità sufficiente a soddisfare le esigenze di archiviazione del database elencate nella sezione dei componenti hardware.
3. Un server di database secondario su un'istanza di macchina virtuale di Azure 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 del database Oracle di produzione.
4. Per ulteriori informazioni sulla distribuzione del database Oracle su Azure NetApp Files e sull'istanza di calcolo di Azure, vedere "[Distribuzione e protezione del database Oracle su Azure NetApp Files](#)".

Preparazione all'onboarding su BlueXP

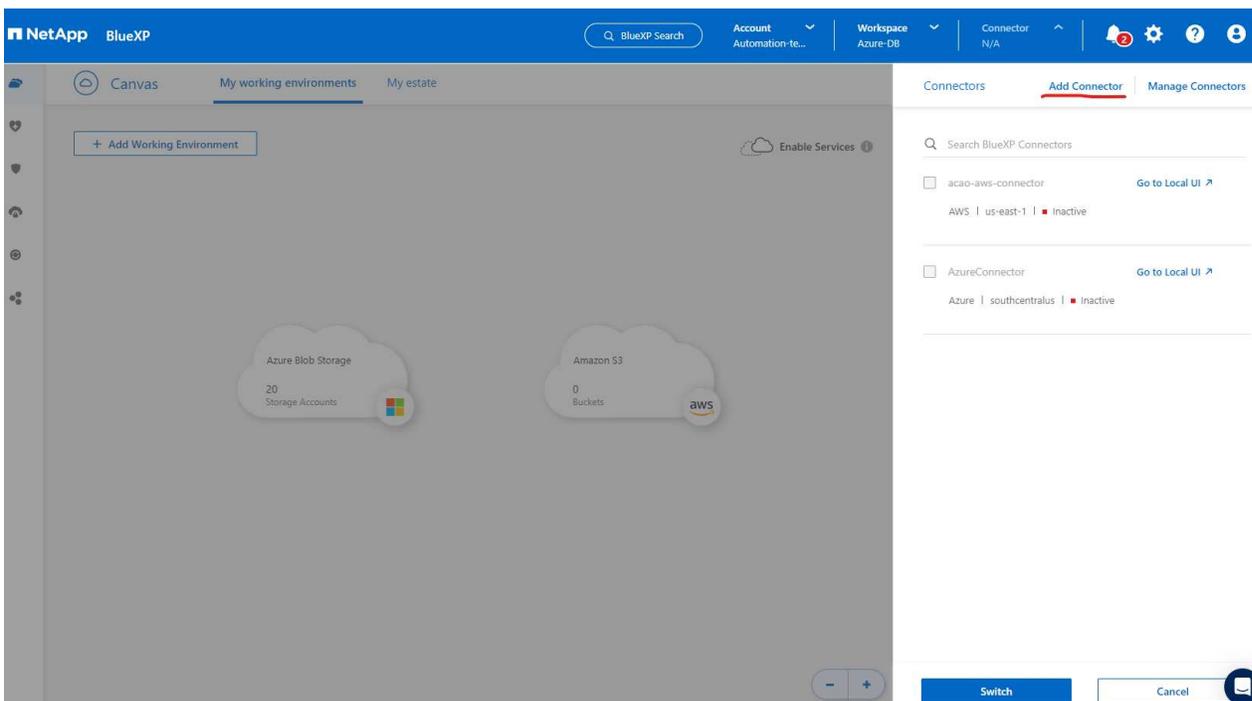
1. Utilizzare il collegamento "[NetApp BlueXP](#)" per registrarsi per accedere alla console BlueXP.
2. Creare un account utente di Azure o un principio di servizio Active Directory e concedere autorizzazioni con ruolo nel portale di Azure per la distribuzione del connettore di Azure.
3. Per configurare BlueXP per la gestione delle risorse di Azure, aggiungere una credenziale BlueXP con i dettagli di un'entità servizio di Active Directory che BlueXP può utilizzare per l'autenticazione con Azure Active Directory (ID client app), un segreto client per l'applicazione dell'entità servizio (segreto client) e l'ID Active Directory per l'organizzazione (ID tenant).
4. Sono inoltre necessari la rete virtuale di Azure, il gruppo di risorse, il gruppo di sicurezza, una chiave SSH per l'accesso alla macchina virtuale, ecc. pronti per il provisioning del connettore e l'installazione del plug-in del database.

Distribuisce un connettore per i servizi SnapCenter

1. Accedi alla console BlueXP .



2. Fare clic sulla freccia a discesa **Connettore** e su **Aggiungi connettore** per avviare il flusso di lavoro di provisioning del connettore.



3. Scegli il tuo provider cloud (in questo caso, **Microsoft Azure**).

Provider

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



[Deploy the Connector on your premises](#)

Continue



4. Ignora i passaggi **Autorizzazione**, **Autenticazione** e **Rete** se sono già configurati nel tuo account Azure. In caso contrario, è necessario configurarli prima di procedere. Da qui, è anche possibile recuperare le autorizzazioni per il criterio di Azure a cui si fa riferimento nella sezione precedente "[Preparazione all'onboarding su BlueXP](#) ."

Deploying a BlueXP Connector

The BlueXP Connector is a crucial component for the day-to-day use of BlueXP.

It's used to connect BlueXP's services to your hybrid-cloud environments.

The BlueXP 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 BlueXP Connector installation.

Permissions

Ensure that the Azure user or service principal you've provided has sufficient permissions

Authentication

Choose between two methods: an [Azure user account](#) or an [Active Directory service principal](#)

Networking

Ensure that you have details on the VNet and subnet in which the BlueXP Connector will reside

[Skip to Deployment](#)

[Previous](#)

[Continue](#)



5. Fare clic su **Vai alla distribuzione** per configurare il connettore **Autenticazione macchina virtuale**. Aggiungere la coppia di chiavi SSH creata nel gruppo di risorse di Azure durante l'onboarding alla preparazione di BlueXP per l'autenticazione del sistema operativo del connettore.

1 VM Authentication 2 Details 3 Network 4 Security Group 5 Review

Virtual Machine Authentication

You are logged in with Azure user: [acao@netapp.com](#) | Tenant: **Hybrid Cloud TME**

Subscription

Hybrid Cloud TME Onprem

Location

South Central US

Resource Group

Create New Use Existing

Resource Group

ANFAVSRG

Authentication Method

Password Public Key

User Name

azureuser

Enter SSH Public Key

-----BEGIN RSA PRIVATE KEY----- MIIGSAIBAAKCA...

Previous

Next



6. Specificare un nome per l'istanza del connettore, selezionare **Crea** e accettare il **Nome ruolo** predefinito in **Dettagli**, quindi scegliere la sottoscrizione per l'account Azure.

 VM Authentication  Details  Network  Security Group  Review

Details

Connector Instance Name 

AzureConnector

Connector Role

Create Attach existing Manual

Role Name

BlueXP Operator-5519248

Subscriptions to apply with the role

Hybrid Cloud TME Onprem

 Add Tags to Connector Instance

Previous

Next



7. Configurare la rete con la **VNet**, la **Subnet** appropriate e disabilitare l'**IP pubblico**, ma assicurarsi che il connettore abbia accesso a Internet nel proprio ambiente Azure.

 VM Authentication  Details  Network  Security Group  Review

Network

Connectivity

VNet

ANFAVSVal

Subnet

VM_Sub

Public IP

Disable

Proxy Configuration (Optional)

HTTP Proxy

Example: http://172.16.254.1:8080

Define Credentials for this Proxy 

Upload a root certificate 

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

Previous

Next



8. Configurare il **Gruppo di sicurezza** per il connettore che consente l'accesso HTTP, HTTPS e SSH.

The screenshot shows the 'Add BlueXP Connector - Azure' wizard in the 'Security Group' step. The breadcrumb trail includes 'VM Authentication', 'Details', 'Network', 'Security Group' (highlighted with a blue circle and the number 4), and 'Review' (highlighted with a blue circle and the number 5). The main heading is 'Security Group'. Below it, a note states: 'The security group must allow inbound HTTP, HTTPS and SSH access.' There are two radio buttons for 'Assign a security group': 'Create a new security group' (selected) and 'Select an existing security group'. Below this are three configuration cards for 'HTTP (Port 80)', 'HTTPS (Port 443)', and 'SSH (Port 22)'. Each card has a 'Source Type' dropdown menu set to 'Anywhere' and a 'Source (CIDR)' text input field containing '0.0.0.0/0'. At the bottom, there are 'Previous' and 'Next' buttons, with 'Next' being highlighted in blue. A help icon is visible in the bottom right corner.

9. 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, la VM dell'istanza del connettore viene visualizzata nel portale di Azure.

✓ VM Authentication ✓ Details ✓ Network ✓ Security Group **5** Review

Review

[Code for Terraform Automation](#)

BlueXP Connector Name	AzureConnector
Subscription	Hybrid Cloud TME Onprem
Location	South Central US
Resource Group	Existing - ANFAVSRG
Role	New - BlueXP Operator-5519248
Authentication Method	Password (user: azureuser)
VNet	ANFAVSV1
Subnet	VM_Sub
Public IP	Enable
Proxy	None
Security Group	HTTP: 0.0.0.0/0, HTTPS: 0.0.0.0/0, SSH: 0.0.0.0/0

Previous

Add

10. Dopo aver distribuito il connettore, il connettore appena creato viene visualizzato nel menu a discesa **Connettore**.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes the NetApp logo, 'BlueXP', a search bar, and dropdown menus for 'Account Automation-te...', 'Workspace Azure-DB', and 'Connettore AzureConnector'. The 'Connettore' dropdown is open, showing 'AzureConnector' selected. Below the navigation bar, there are tabs for 'Canvas', 'My working environments', and 'My estate'. The main area displays a canvas with two cloud icons: 'Azure Blob Storage' (20 Storage Accounts) and 'Amazon S3' (0 Buckets). A right-hand sidebar titled 'Working Environments' shows a summary of these resources. At the bottom right, there are zoom controls and a help icon.

NetApp BlueXP

Account Automation-te... Workspace Azure-DB **Connettore AzureConnector**

Canvas My working environments My estate

+ Add Working Environment Enable Services

Azure Blob Storage
20 Storage Accounts

Amazon S3
0 Buckets

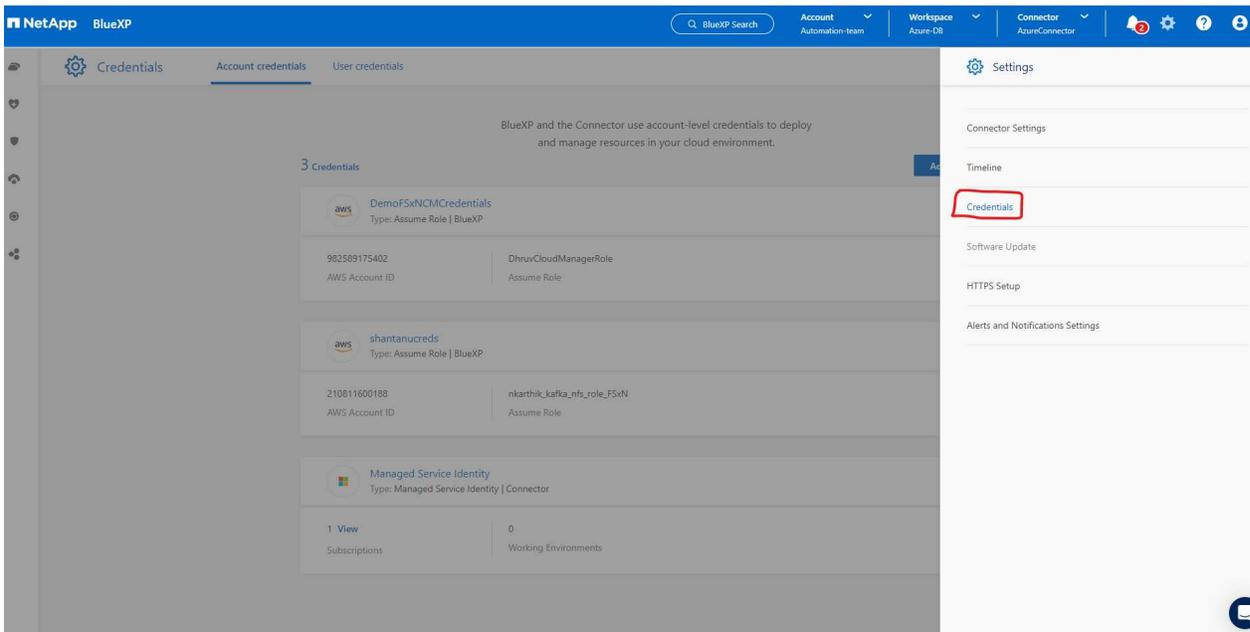
Working Environments

Amazon S3
0 Buckets

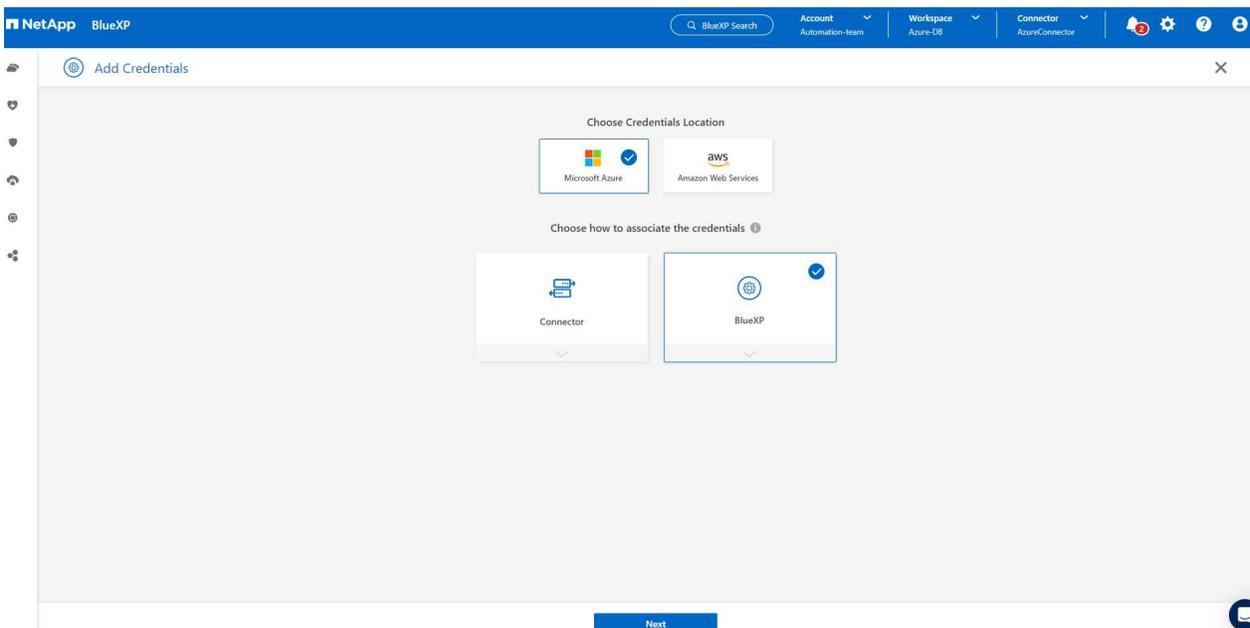
Azure Blob Storage
20 Storage Accounts

Definisci una credenziale in BlueXP per l'accesso alle risorse di Azure

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



2. Selezionare la posizione delle credenziali come - **Microsoft Azure - BlueXP**.



3. Definire le credenziali di Azure con **Segreto client**, **ID client** e **ID tenant** corretti, che avrebbero dovuto essere raccolti durante il precedente processo di onboarding BlueXP .

NetApp BlueXP

BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector

Add Credentials Credentials Type Define Credentials Marketplace Subscription Review

Define Microsoft Azure Credentials

Learn more about Azure application credentials

Credentials Name: Azure_Hybrid_TME Client Secret:

Application (client) ID: 2fbc9be5-a259-4539-bb57-036b176f5cc7 Directory (tenant) ID: 9bb0aab6-5c98-419b-9cfd-7a38bd496e1f

I have verified that the Azure role assigned to the Active Directory service principal matches BlueXP policy requirements.

Previous Next

4. Rivedi e Aggiungi

NetApp BlueXP

BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector

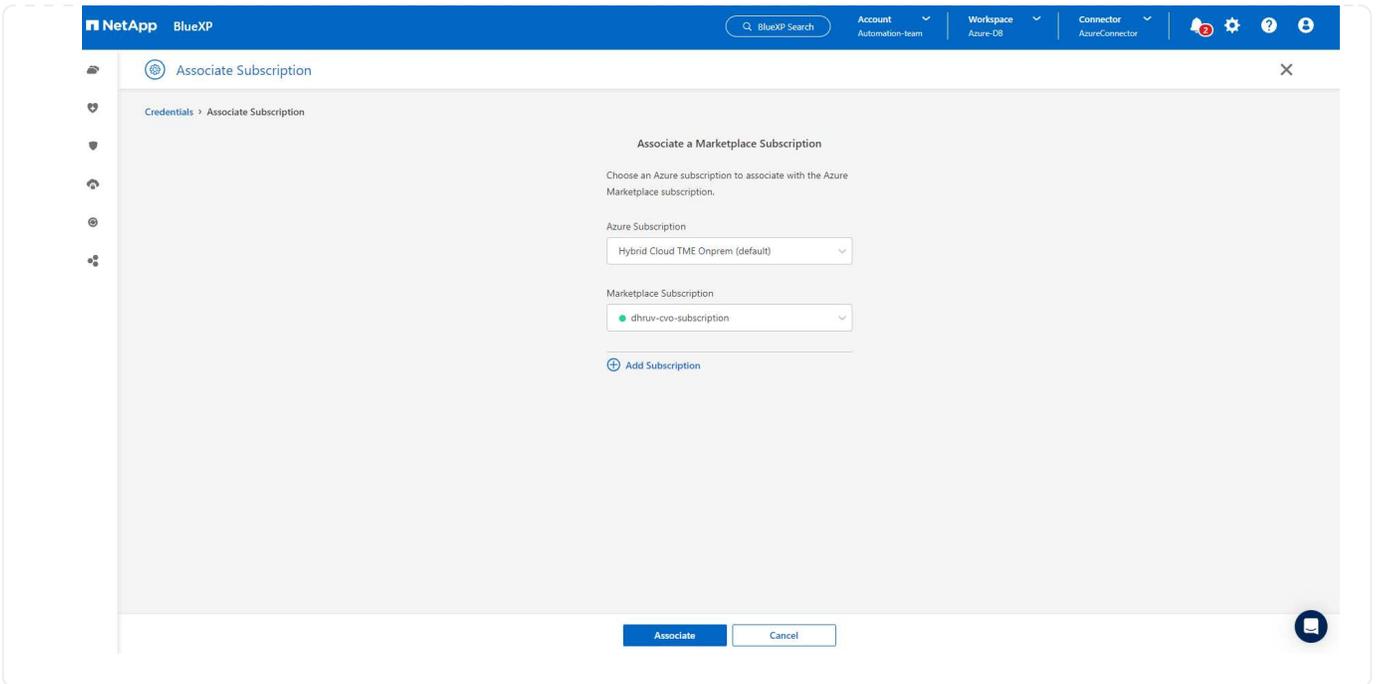
Add Credentials Credentials Type Define Credentials Review

Review

Credentials Type	Azure
Credentials Name	Azure_Hybrid_TME
Credential Storage	Cloud Manager
Application (client) ID	2fbc9be5-a259-4539-bb57-036b176f5cc7
Directory (tenant) ID	9bb0aab6-5c98-419b-9cfd-7a38bd496e1f

Previous Add

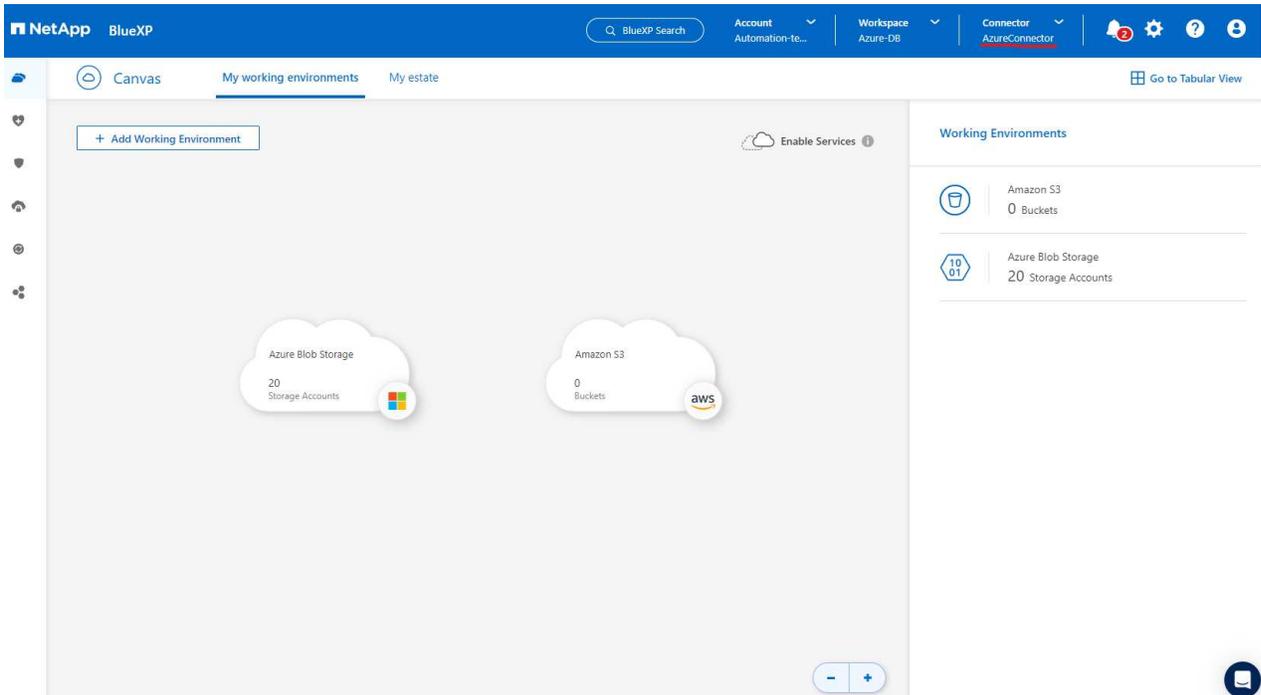
5. Potrebbe anche essere necessario associare un **abbonamento Marketplace** alle credenziali.



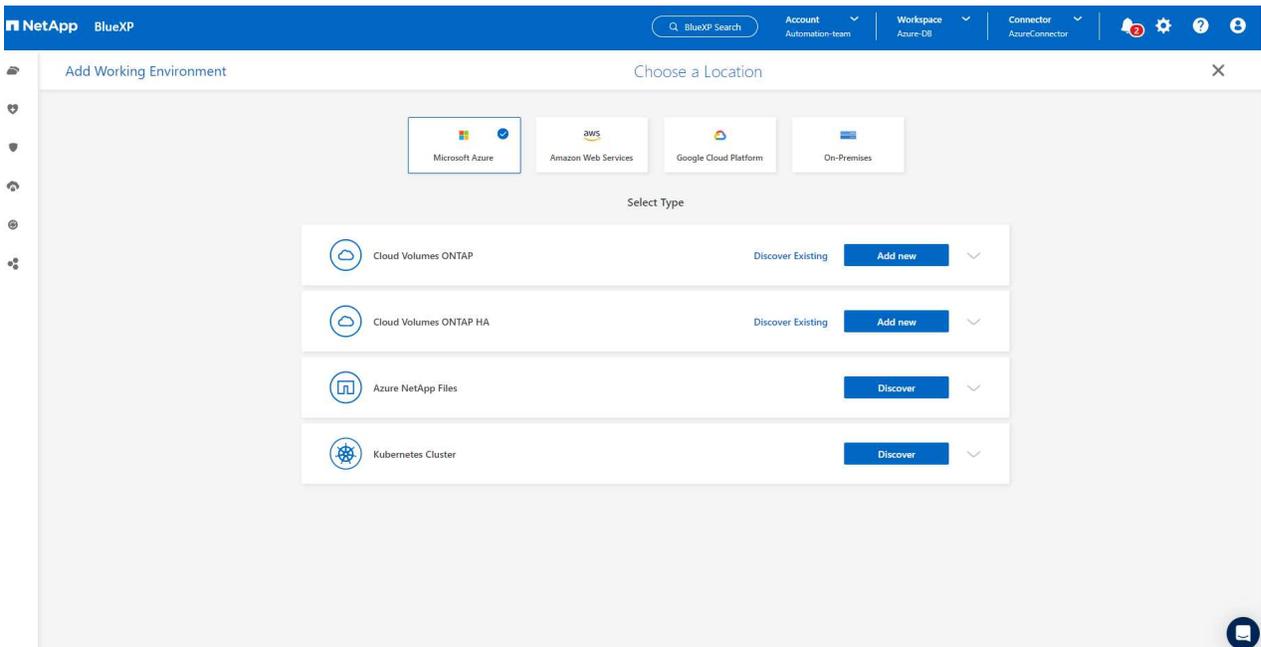
Configurazione dei servizi SnapCenter

Una volta configurate le credenziali di Azure, è ora possibile impostare i servizi SnapCenter con le seguenti procedure:

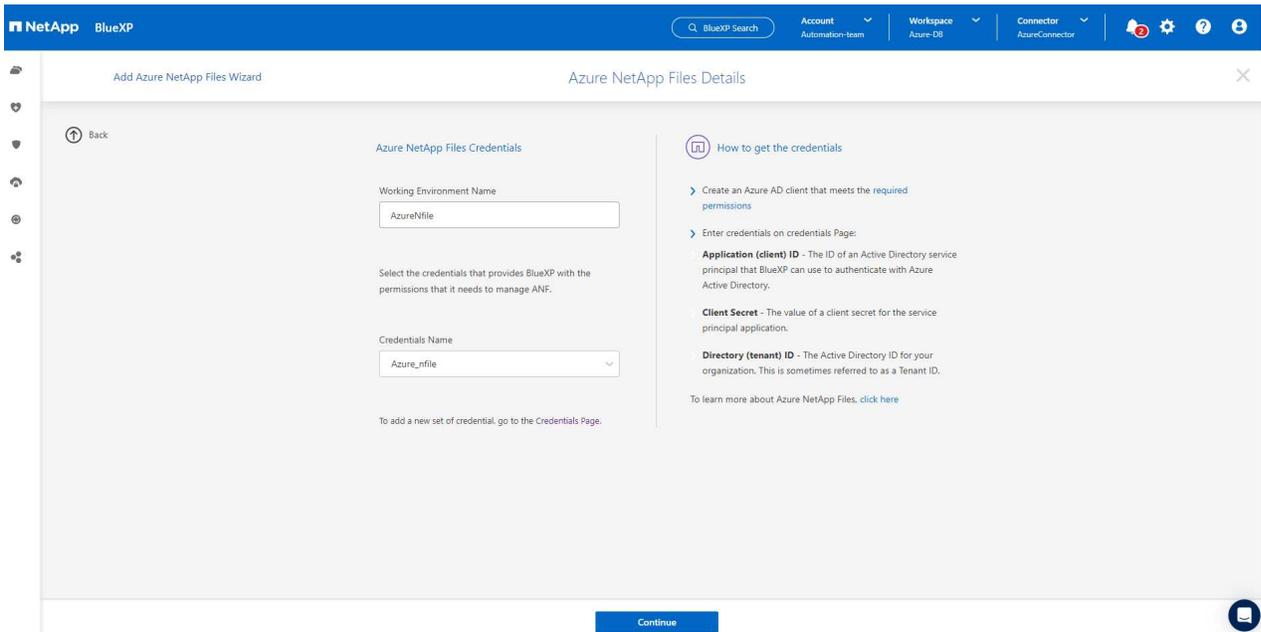
1. Tornando alla pagina Canvas, da **Il mio ambiente di lavoro** fare clic su **Aggiungi ambiente di lavoro** per scoprire Azure NetApp Files distribuito in Azure.



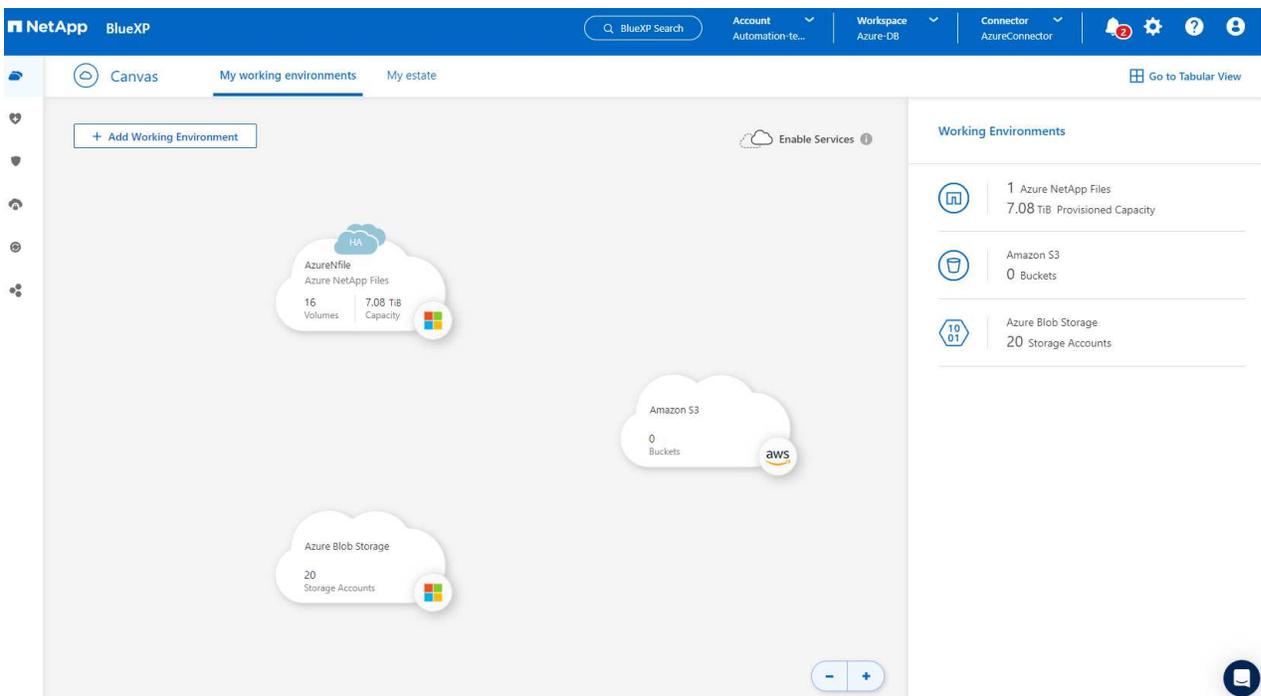
2. Seleziona **Microsoft Azure** come posizione e clicca su **Scopri**.



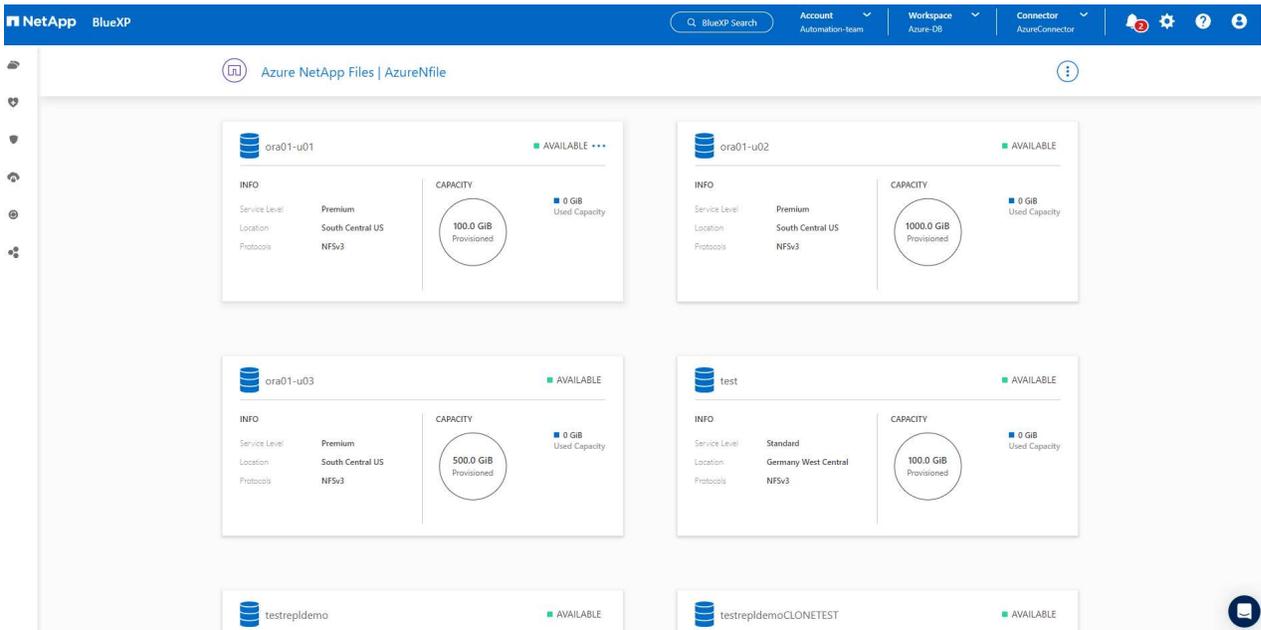
3. Assegna un nome **Ambiente di lavoro** e scegli **Nome credenziale** creato nella sezione precedente, quindi fai clic su **Continua**.



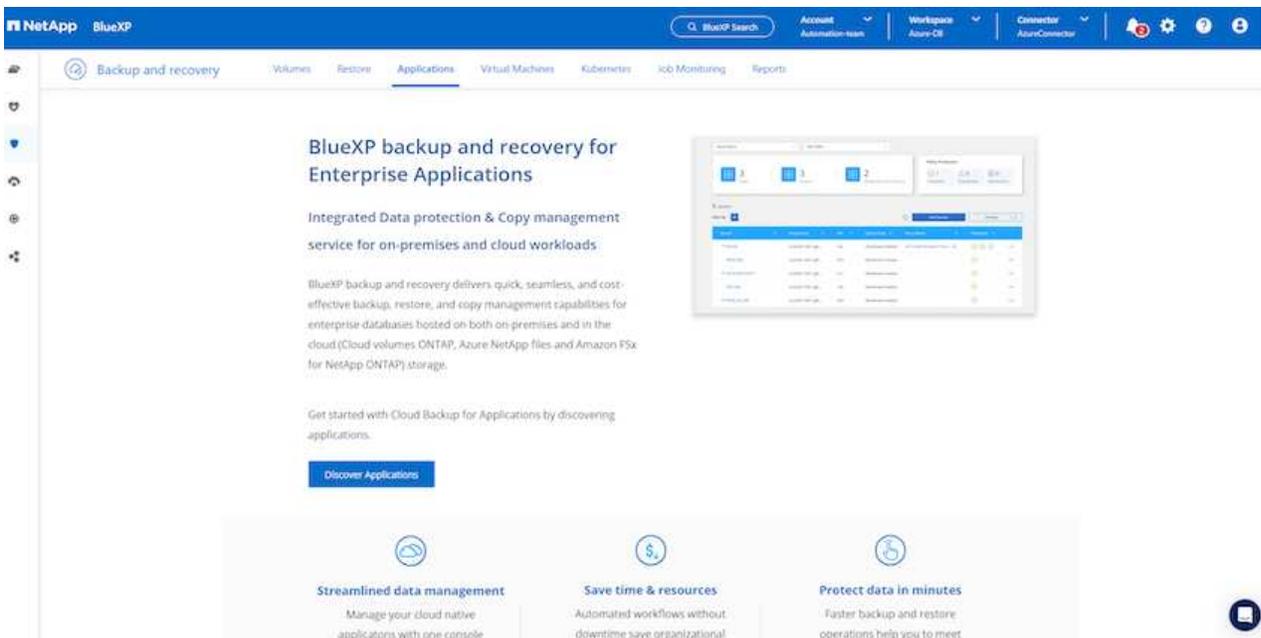
4. La console BlueXP torna a **I miei ambienti di lavoro** e ha scoperto che Azure NetApp Files di Azure ora appare su **Canvas**.



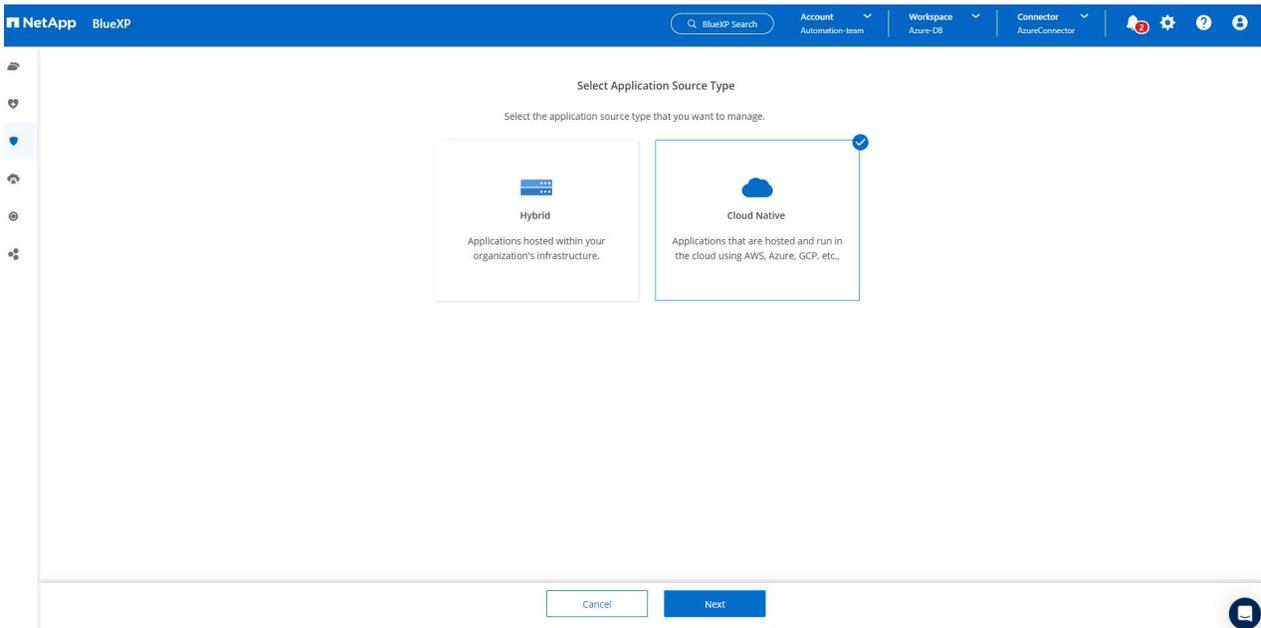
5. Fare clic sull'icona * Azure NetApp Files*, quindi su **Entra nell'ambiente di lavoro** per visualizzare i volumi del database Oracle distribuiti nell'archiviazione di Azure NetApp Files .



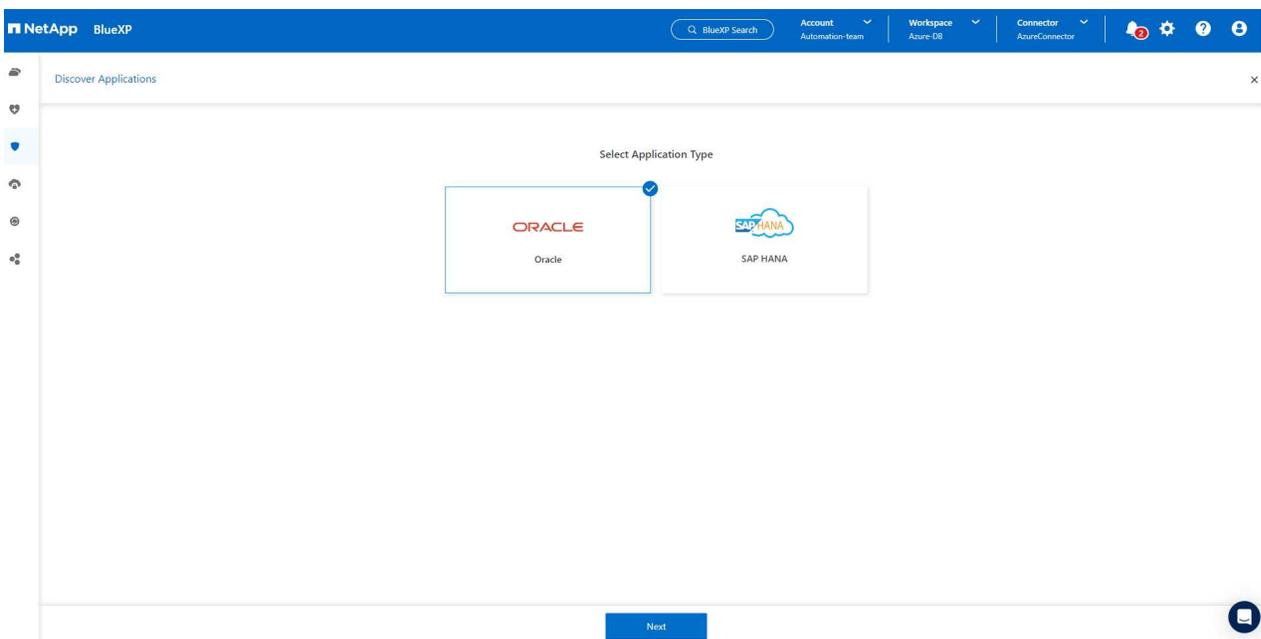
6. Dalla barra laterale sinistra della console, passa il mouse sull'icona di protezione, quindi fai clic su **Protezione** > **Applicazioni** per aprire la pagina di avvio delle Applicazioni. Fare clic su **Scopri applicazioni**.



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



8. Selezionare **Oracle** come tipo di applicazione, fare clic su **Avanti** per aprire la pagina dei dettagli dell'host.



9. Selezionare **Utilizzo di SSH** e fornire i dettagli della macchina virtuale Oracle Azure, ad esempio **Indirizzo IP**, **Connettore**, **Nome utente** di gestione della macchina virtuale Azure, ad esempio azureuser. Fare clic su **Aggiungi chiave privata SSH** per incollare la coppia di chiavi SSH utilizzata per distribuire la macchina virtuale Oracle Azure. Ti verrà anche chiesto di confermare l'impronta digitale.

The screenshot shows the 'Discover Applications' window in NetApp BlueXP. The 'Host Details' step is active. The 'Host Installation Type' is set to 'Using SSH'. The 'Host FQDN or IP' is '172.30.137.142', the 'Connector' is 'AzureConnector', the 'Username' is 'azureuser', the 'SSH Port' is '22', and the 'Plug-in Port' is '8145'. There is an 'Add SSH Private Key Optional' button. At the bottom, there are 'Previous' and 'Next' buttons.

The screenshot shows the 'Discover Applications' window in NetApp BlueXP, now at the 'Validate fingerprint' step. The 'Host Installation Type' remains 'Using SSH'. The 'Algorithm' is 'ssh-rsa' and the 'Fingerprint' is 'AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAABmlzdHAyNTYAAAB...'. A checkbox is checked with the text 'By proceeding further, I confirm that the above fingerprint for host is valid.' At the bottom, there are 'Previous' and 'Next' buttons.

10. Passare alla pagina successiva di **Configurazione** per impostare l'accesso sudoer sulla macchina virtuale Oracle Azure.

NetApp BlueXP

Backup and recovery | Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring | Reports

Cloud Native | Oracle

3 Hosts | 3 ORACLE | 0 Clone

Application Protection

0 Protected | 3 Unprotected

3 Databases

Filter By + | Manage Databases | Settings

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1st	172.30.15.124		Unprotected

1 - 3 of 3

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. Il nostro database Oracle di prova in Azure VM è configurato con tre volumi con uno spazio di archiviazione totale aggregato di circa 1,6 TiB. Ciò fornisce un contesto sui tempi per il backup, il ripristino e la clonazione degli snapshot di un database di queste dimensioni.

```
[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. Per proteggere il database, fare clic sui tre punti accanto allo **Stato di protezione** del database, quindi fare clic su **Assegna criterio** per visualizzare i criteri di protezione del database predefiniti, predefiniti o definiti dall'utente, che possono essere applicati ai database Oracle. In **Impostazioni - Criteri**, puoi creare il tuo criterio personalizzato con una frequenza di backup e una finestra di conservazione dei dati di backup personalizzate.

The screenshot shows the NetApp BlueXP interface. At the top, there's a navigation bar with 'Backup and recovery' selected. Below it, there are filters for 'Cloud Native' and 'Oracle'. A summary card shows '4 Hosts', '3 ORACLE', and '0 Clone'. An 'Application Protection' card shows '0 Protected' and '3 Unprotected'. A table lists three databases: 'NTAP', 'db1', and 'db1tst', all with 'Unprotected' status. A dropdown menu for 'NTAP' is open, with 'Assign Policy' highlighted.

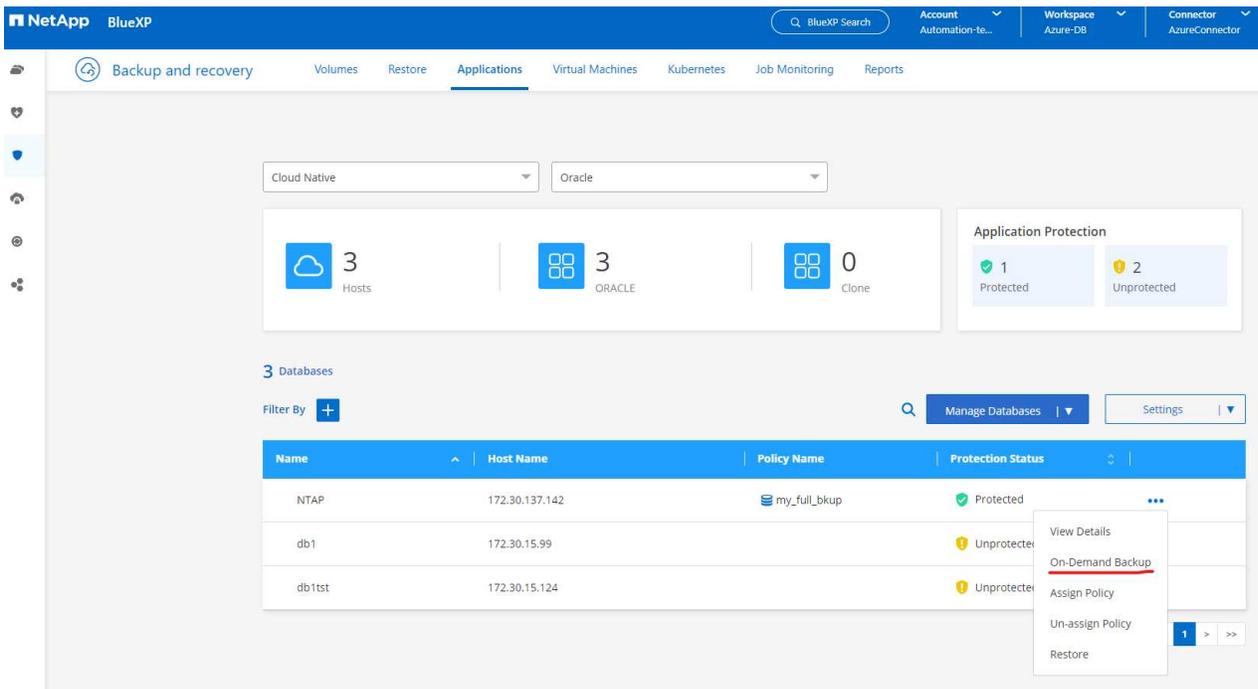
Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142		Unprotected
db1	172.30.15.99		Unprotected
db1tst	172.30.15.124		Unprotected

2. Una volta che sei soddisfatto della configurazione della policy, puoi **assegnare** la policy che preferisci per proteggere il database.

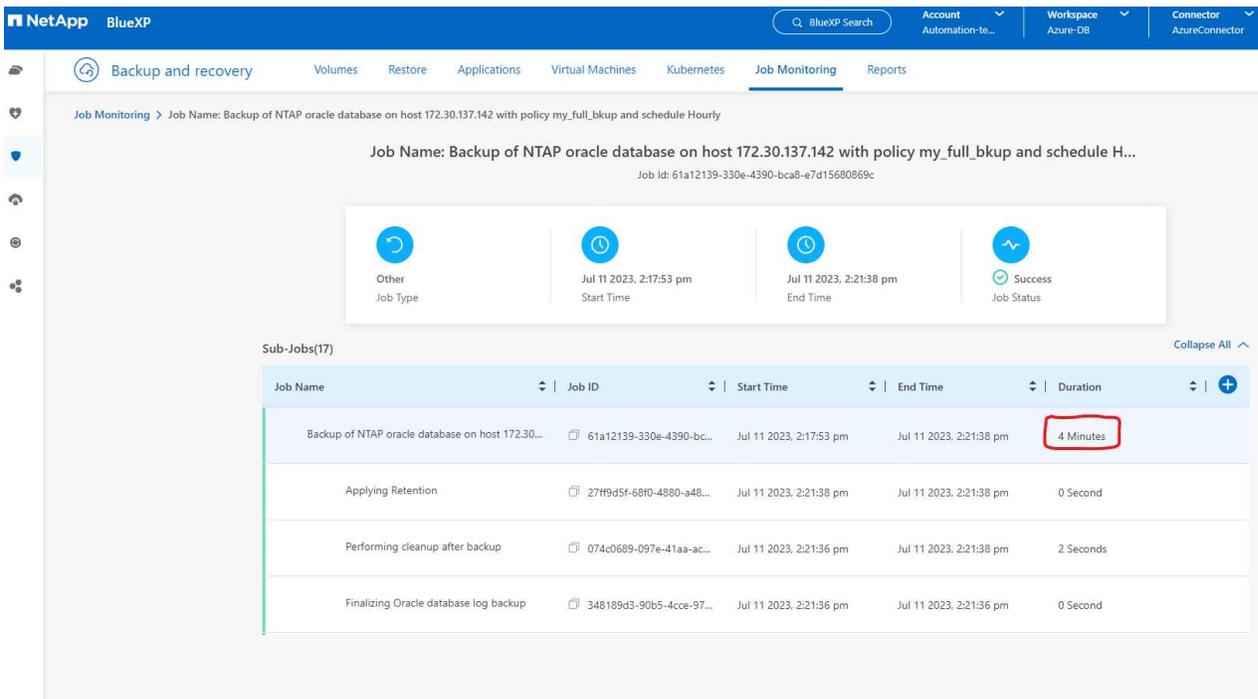
The screenshot shows the 'Assign Policy' dialog in the NetApp BlueXP interface. It prompts the user to 'Assign a policy to start taking backups of the database "NTAP"'. There are four policies listed in a table. The 'my_full_bkup' policy is selected with a checkmark.

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 6 Hrs, Keeps 3 Days

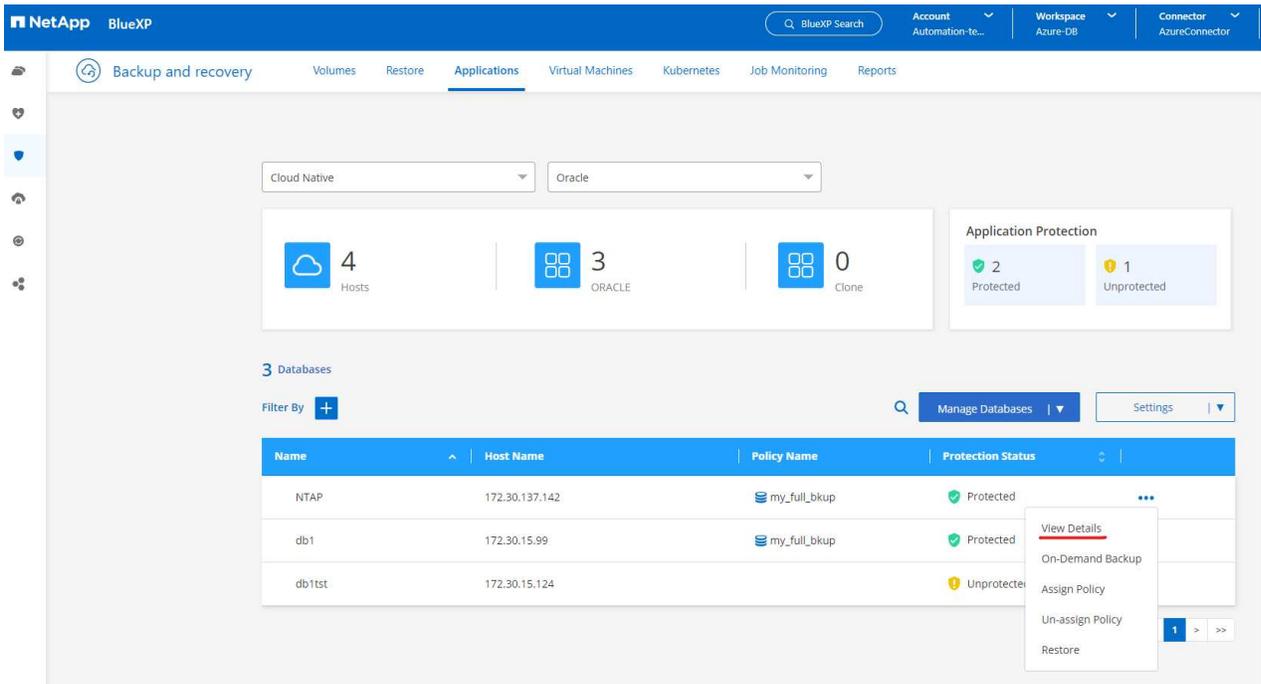
3. Dopo l'applicazione del criterio, lo stato di protezione del database cambia in **Protetto** con un segno di spunta verde. BlueXP esegue il backup degli snapshot in base alla pianificazione definita. Inoltre, **Backup su richiesta** è disponibile dal menu a discesa a tre punti, come mostrato di seguito.



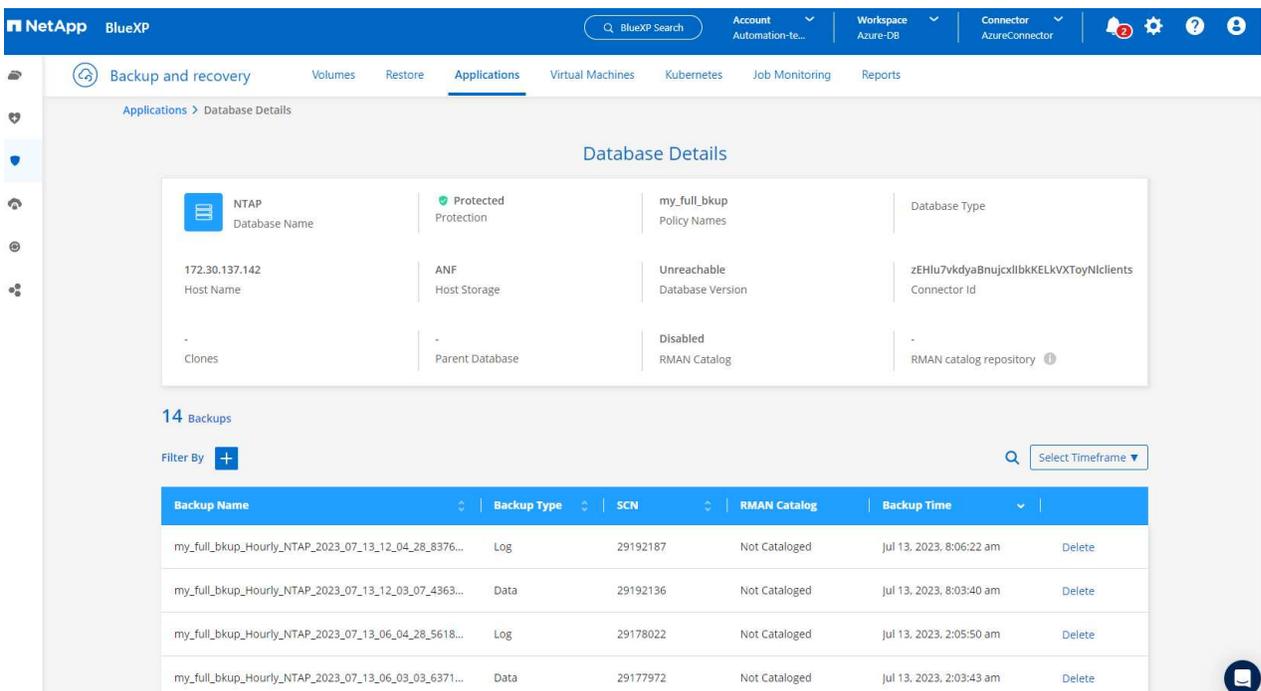
4. Dalla scheda **Monitoraggio lavori** è possibile visualizzare i dettagli del lavoro di backup. I risultati dei nostri test hanno mostrato che ci sono voluti circa 4 minuti per eseguire il backup di un database Oracle di circa 1,6 TiB.



5. Dal menu a discesa a tre punti **Visualizza dettagli**, è possibile visualizzare i set di backup creati dal backup snapshot.



6. I dettagli del backup del database includono **Nome del backup**, **Tipo di backup**, **SCN**, **Catalogo RMAN** e **Ora del backup**. Un set di backup contiene snapshot coerenti con l'applicazione, rispettivamente per il volume dei dati e per il volume del registro. Uno snapshot del volume di log viene eseguito subito dopo uno snapshot del volume di dati del database. È possibile applicare un filtro se si sta cercando un backup specifico nell'elenco dei backup.



Ripristino e recupero del database Oracle

1. Per ripristinare un database, fare clic sul menu a discesa con tre punti per il database specifico da ripristinare in **Applicazioni**, quindi fare clic su **Ripristina** per avviare il flusso di lavoro di ripristino e recupero del database.

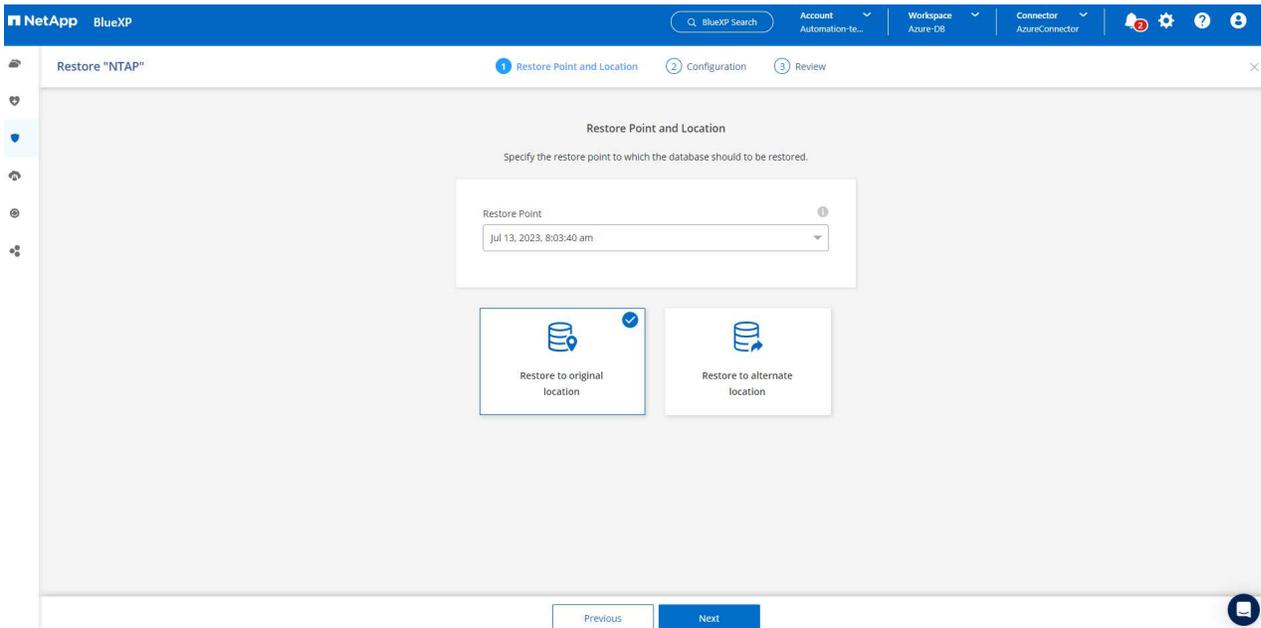
The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and dropdown menus for 'Account', 'Workspace', and 'Connector'. The main navigation bar has tabs for 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. The 'Applications' tab is active, showing a summary of resources: 4 Cloud Native Hosts, 3 ORACLE, and 0 Clones. An 'Application Protection' summary shows 2 Protected and 1 Unprotected. Below this is a table of 3 Databases. The table has columns for Name, Host Name, Policy Name, and Protection Status. The 'db1tst' database is highlighted, and a context menu is open over it, showing options: View Details, On-Demand Backup, Assign Policy, Un-assign Policy, and Restore (which is underlined).

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

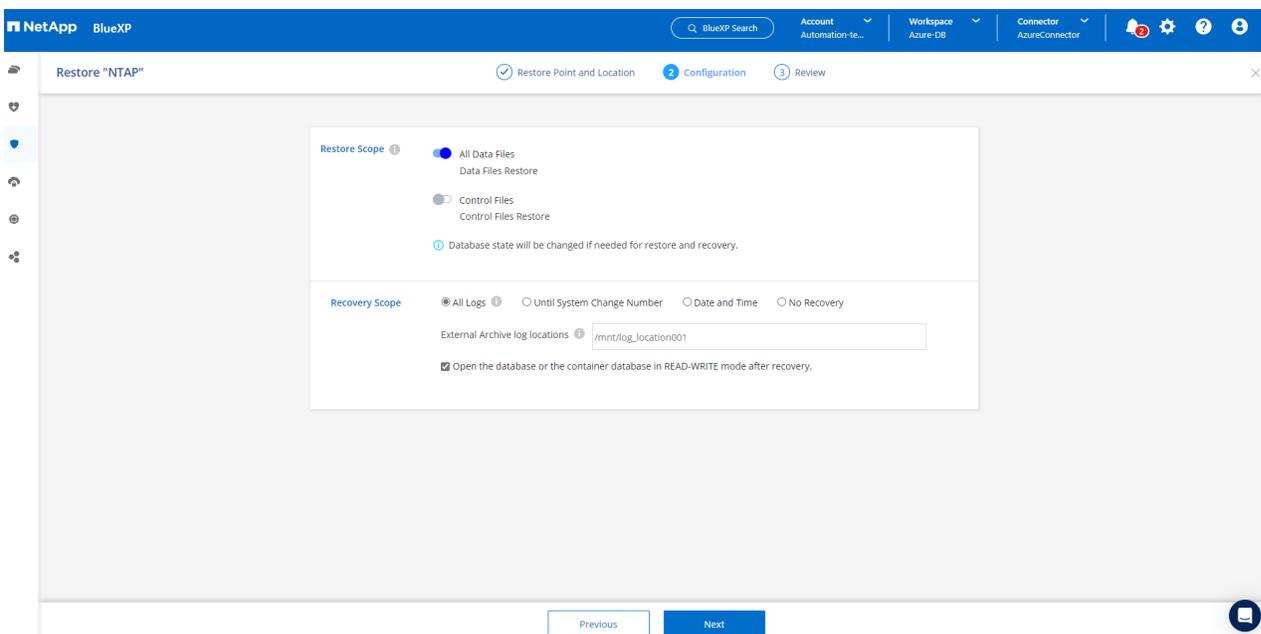
2. Scegli il tuo **Punto di ripristino** in base alla marca temporale. Ogni timestamp nell'elenco rappresenta un set di backup del database disponibile.

The screenshot shows the 'Restore "NTAP"' workflow in the NetApp BlueXP interface. The current step is 'Restore Point and Location', with sub-steps 'Restore Point and Location', 'Configuration', and 'Review'. The main content area displays the instruction: 'Specify the restore point to which the database should be restored.' A dropdown menu for 'Restore Point' is open, showing a list of timestamps: Jul 13, 2023, 8:03:40 am; Jul 13, 2023, 8:03:40 am; Jul 13, 2023, 2:03:43 am; Jul 12, 2023, 8:03:41 pm; Jul 12, 2023, 2:03:32 pm; Jul 12, 2023, 2:03:31 am. Below the list are two 'location' input fields. At the bottom, there are 'Previous' and 'Next' buttons.

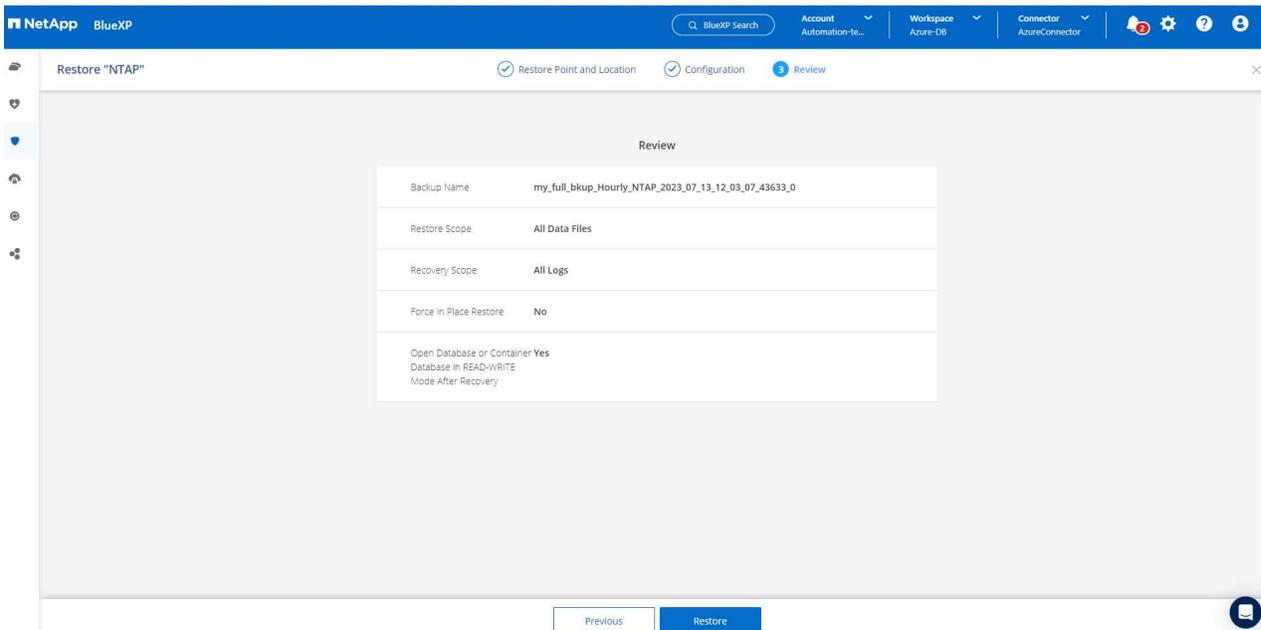
3. Seleziona la **Posizione di ripristino** nella **posizione originale** per un ripristino e recupero in loco del database Oracle.



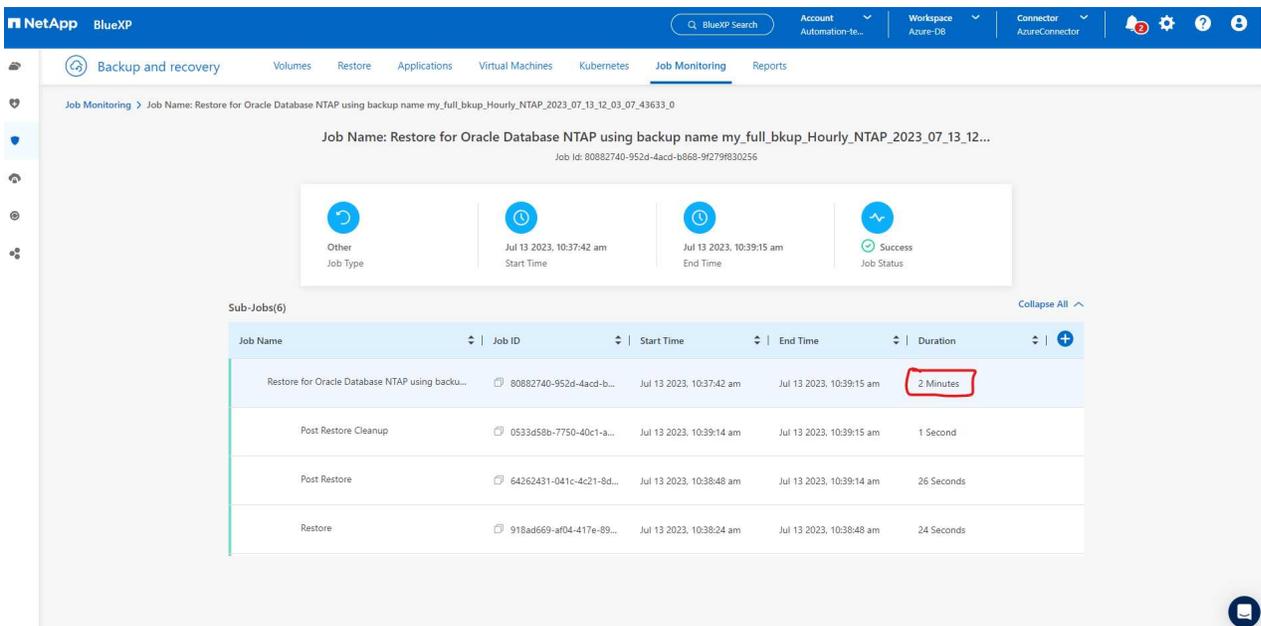
4. Definisci l'**Ambito di ripristino** e l'**Ambito di ripristino**. Tutti i registri indicano un ripristino completo aggiornato, inclusi i registri correnti.



5. Rivedi e **Ripristina** per avviare il ripristino e il recupero del database.



6. Dalla scheda **Monitoraggio processi**, abbiamo osservato che ci sono voluti 2 minuti per eseguire un ripristino completo del database e un ripristino aggiornato.



Clone del database Oracle

Le procedure di clonazione del database sono simili al ripristino, ma su una macchina virtuale di Azure alternativa con stack software Oracle identico preinstallato e configurato.



Assicurati che l'archiviazione file di Azure NetApp abbia una capacità sufficiente per un database clonato delle stesse dimensioni del database primario da clonare. La VM di Azure alternativa è stata aggiunta ad **Applicazioni**.

1. Fare clic sul menu a discesa con tre punti per il database specifico da clonare in **Applicazioni**, quindi fare clic su **Ripristina** per avviare il flusso di lavoro di clonazione.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', a search bar, and dropdown menus for 'Account', 'Workspace', and 'Connector'. The main navigation tabs are 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. The 'Applications' tab is active, showing a summary of 'Cloud Native' (4 Hosts) and 'Oracle' (3 ORACLE, 0 Clone) resources. An 'Application Protection' summary shows 2 Protected and 1 Unprotected. Below this is a table of databases:

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

A context menu is open for the 'db1tst' database, with the 'Restore' option highlighted. Other menu items include 'View Details', 'On-Demand Backup', 'Assign Policy', and 'Un-assign Policy'.

2. Selezionare il **Punto di ripristino** e selezionare la casella **Ripristina in posizione alternativa**.

The screenshot shows the 'Restore "NTAP"' configuration page in NetApp BlueXP. The page has three steps: 'Restore Point and Location', 'Configuration', and 'Review'. The current step is 'Restore Point and Location', which prompts the user to 'Specify the restore point to which the database should be restored.' A dropdown menu shows the selected restore point: 'Jul 13, 2023, 8:03:40 am'. Below this are two options: 'Restore to original location' and 'Restore to alternate location'. The 'Restore to alternate location' option is selected, indicated by a blue checkmark. At the bottom, there are 'Previous' and 'Next' buttons.

3. Nella pagina **Configurazione** successiva, imposta **Host** alternativo, **SID** del nuovo database e **Oracle Home** come configurato nella VM di Azure alternativa.

The screenshot shows the 'Configuration' step in the NetApp BlueXP interface. The page title is 'Restore "NTAP"'. The breadcrumb navigation shows 'Restore Point and Location' (checked), 'Configuration' (active), and 'Review'. The main content area is titled 'Configuration' and contains the instruction: 'Specify the alternate host details on which the database will be restored and throughput.' Below this, there are several input fields: 'Host' (172.30.137.147), 'SID' (NTAP1), 'Oracle Home' (/u01/app/oracle/product/19.0.0/clone), 'Database Credentials' (Optional) with an 'Add Credential' button, and 'Maximum storage throughput (MiB/s)' (Optional) with a field 'Enter throughput (1-4500)'. At the bottom, there are 'Previous' and 'Next' buttons.

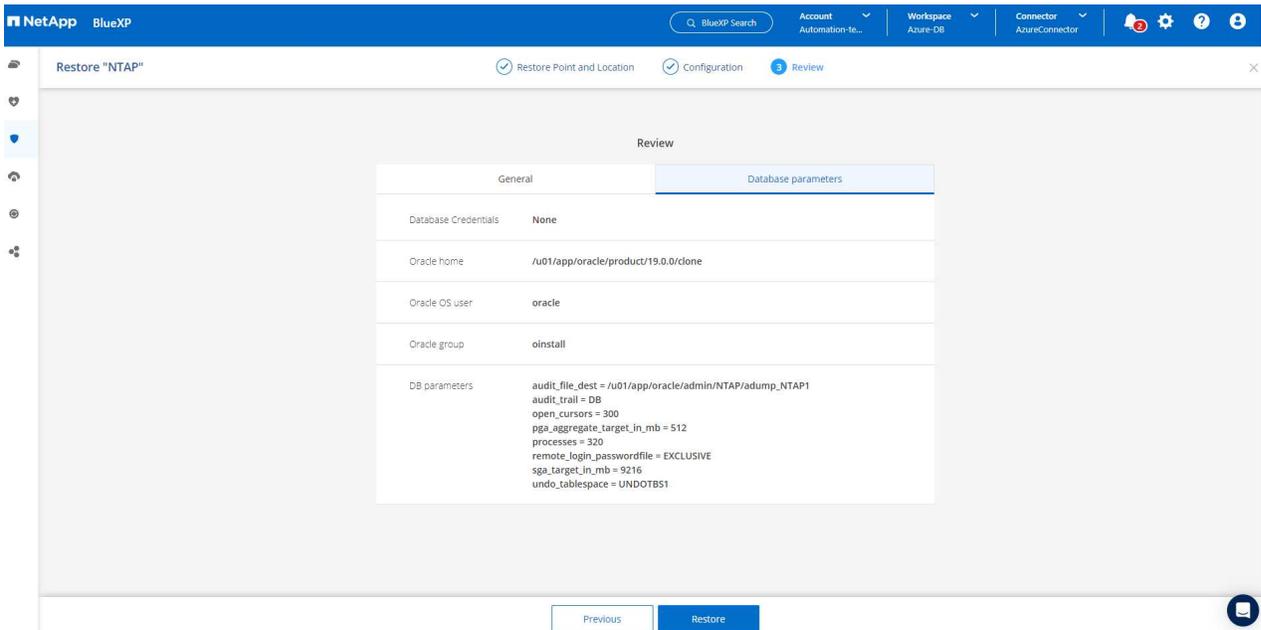
4. La pagina di revisione **Generale** mostra i dettagli del database clonato, come SID, host alternativo, posizioni dei file di dati, ambito di ripristino, ecc.

The screenshot shows the 'Review' step in the NetApp BlueXP interface. The page title is 'Restore "NTAP"'. The breadcrumb navigation shows 'Restore Point and Location' (checked), 'Configuration' (checked), and 'Review' (active). The main content area is titled 'Review' and contains a table with two tabs: 'General' (selected) and 'Database parameters'. The table lists the following details:

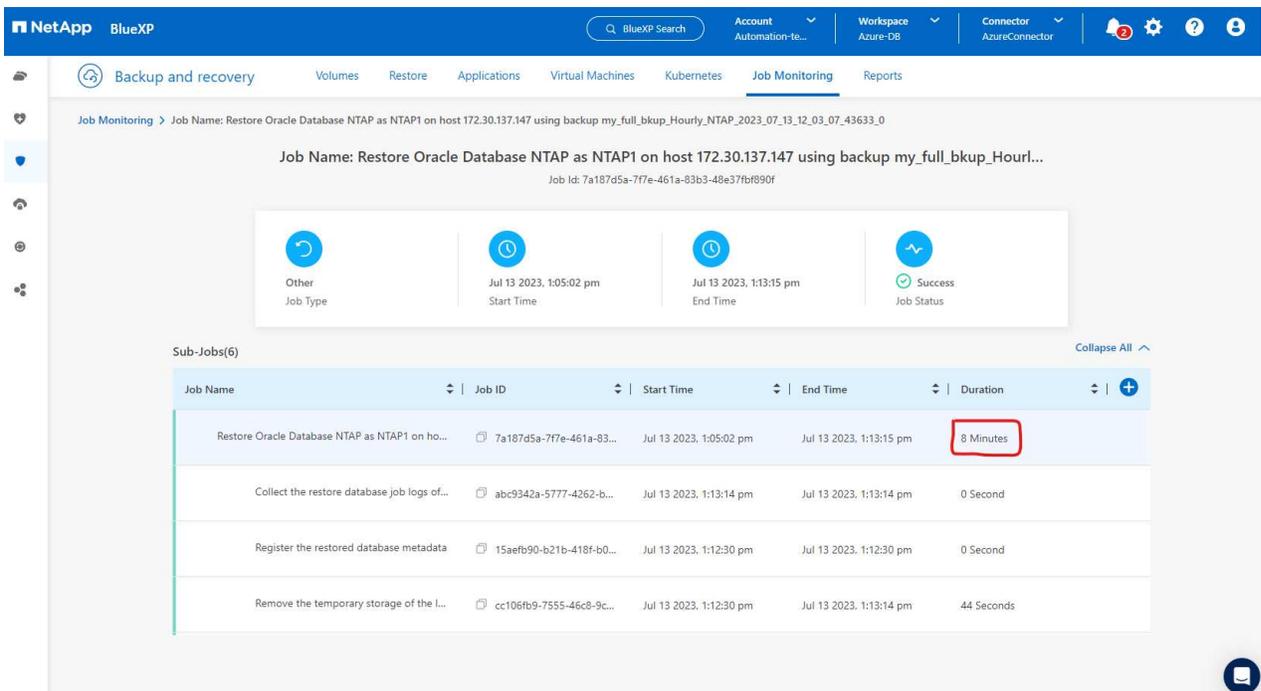
General	Database parameters
Backup Name	my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_43633_0
SID	NTAP1
Host	172.30.137.147
Datafile locations	/u02_NTAP1
Control files	/u02_NTAP1/NTAP1/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo03_01.log
Recovery scope	Until cancel using selected backup's archive logs
Recovery Point	Jul 13, 2023, 8:03:40 am
Location	Alternate Location

At the bottom, there are 'Previous' and 'Restore' buttons.

5. La pagina di revisione **Parametri del database** mostra i dettagli della configurazione del database clonato, nonché alcune impostazioni dei parametri del database.



6. Monitorando lo stato del processo di clonazione dalla scheda **Monitoraggio processo**, abbiamo osservato che ci sono voluti 8 minuti per clonare un database Oracle da 1,6 TiB.



7. Convalida il database clonato nella pagina **Applicazioni** BlueXP che mostra che il database clonato è stato immediatamente registrato con BlueXP.

NetApp BlueXP

Account Automation-te... Workspace Azure-DB Connector AzureConnector

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring Reports

Cloud Native Oracle

4 Hosts 4 ORACLE 0 Clone

Application Protection 2 Protected 2 Unprotected

4 Databases

Filter By + Manage Databases Settings

Name	Host Name	Policy Name	Protection Status
NTAP	172.30.137.142	my_full_bkup	Protected
NTAP1	172.30.137.147		Unprotected
db1	172.30.15.99	my_full_bkup	Protected
db1tst	172.30.15.124		Unprotected

1 - 4 of 4

8. Convalidare il database clonato sulla macchina virtuale Oracle Azure che ha mostrato che il database clonato era in esecuzione come previsto.

```

[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 $ORACLE_SID are not allowed.
#
#
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
NTAPI:/u01/app/oracle/product/19.0.0/clone:N
[oracle@acao-ora02 admin]$ export ORACLE_SID=NTAPI
[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$databases;

NAME          OPEN_MODE          LOG_MODE
-----
NTAPI         READ WRITE         NOARCHIVELOG

```

Questo completa la dimostrazione di un backup, ripristino e clonazione del database Oracle in Azure con la console NetApp BlueXP utilizzando il servizio SnapCenter .

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)

- Azure NetApp Files

["https://azure.microsoft.com/en-us/products/netapp"](https://azure.microsoft.com/en-us/products/netapp)

- Inizia con Azure

["https://azure.microsoft.com/en-us/get-started/"](https://azure.microsoft.com/en-us/get-started/)

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.