



# **SnapCenter per database**

## **NetApp Solutions**

NetApp  
April 26, 2024

This PDF was generated from [https://docs.netapp.com/it-it/netapp-solutions/databases/automation\\_ora\\_clone\\_lifecycle.html](https://docs.netapp.com/it-it/netapp-solutions/databases/automation_ora_clone_lifecycle.html) on April 26, 2024. Always check docs.netapp.com for the latest.

# Sommario

- SnapCenter per database ..... 1
  - Automazione del ciclo di vita dei cloni Oracle di SnapCenter ..... 1
  - TR-4988: Backup, recovery e cloning di database Oracle su ANF con SnapCenter ..... 5
  - TR-4977: Backup, ripristino e cloning del database Oracle con servizi SnapCenter - Azure ..... 46
  - TR-4964: Backup, ripristino e cloning del database Oracle con servizi SnapCenter - AWS ..... 80
  - Soluzioni di database per il cloud ibrido con SnapCenter ..... 114

# SnapCenter per database

## Automazione del ciclo di vita dei cloni Oracle di SnapCenter

Allen Cao, Niyaz Mohamed, NetApp

### Scopo

I clienti apprezzano la funzionalità FlexClone dello storage NetApp ONTAP per i database che offre significativi risparmi sui costi di storage. Questo toolkit basato su Ansible automatizza setup, cloning e aggiornamento dei database Oracle clonati in base alle tempistiche, utilizzando le utilità della riga di comando di NetApp SnapCenter per una gestione ottimizzata del ciclo di vita. Il toolkit è applicabile ai database Oracle implementati sullo storage ONTAP on-premise o nel cloud pubblico e gestiti dal tool dell'interfaccia utente di NetApp SnapCenter.

Questa soluzione risolve i seguenti casi di utilizzo:

- Setup del file di configurazione delle specifiche dei cloni del database Oracle.
- Creare e aggiornare il database Oracle clone in base alla pianificazione definita dall'utente.

### Pubblico

Questa soluzione è destinata alle seguenti persone:

- Un DBA che gestisce i database Oracle con SnapCenter.
- Un amministratore dello storage che gestisce lo storage ONTAP con SnapCenter.
- Proprietario di un'applicazione che ha accesso all'interfaccia utente di SnapCenter.

### Licenza

Accedendo, scaricando, installando o utilizzando il contenuto di questo repository GitHub, l'utente accetta i termini della licenza riportata in ["File di licenza"](#).



Ci sono alcune restrizioni riguardo alla produzione e/o alla condivisione di qualsiasi opera derivata con il contenuto di questo repository GitHub. Prima di utilizzare il contenuto, leggere i termini della licenza. Se non si accettano tutti i termini, non accedere, scaricare o utilizzare il contenuto di questo repository.

### Implementazione della soluzione

#### Prerequisiti per l'implementazione

L'implementazione richiede i seguenti prerequisiti.

**Ansible controller:**

Ansible v.2.10 and higher

ONTAP collection 21.19.1

Python 3

**Python libraries:**

netapp-lib

xmltodict

jmespath

**SnapCenter server:**

version 5.0

backup policy configured

Source database protected with a backup policy

**Oracle servers:**

Source server managed by SnapCenter

Target server managed by SnapCenter

Target server with identical Oracle software stack as source server installed and configured

## Scaricare il toolkit

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-  
bb/na_oracle_clone_lifecycle.git
```

## Configurazione dei file host di destinazione Ansible



Il toolkit include un file hosts che definisce le destinazioni per cui viene eseguito un playbook Ansible. In genere, si tratta degli host clone di Oracle di destinazione. Di seguito è riportato un file di esempio. Una voce dell'host include l'indirizzo IP dell'host di destinazione e la chiave ssh per l'accesso di un utente amministratore all'host per eseguire il comando clone o refresh.

#Host cloni Oracle

```
[clone_1]
ora_04.cie.netapp.com ansible_host=10.61.180.29
ansible_ssh_private_key_file=ora_04.pem
```

```
[clone_2]
[clone_3]
```

## Configurazione variabili globali

I playbook Ansible prendono input variabili da diversi file variabili. Di seguito è riportato un esempio di file variabile globale vars.yml.

```
# ONTAP specific config variables
# SnapCtr specific config variables
```

```
snapctr_usr: xxxxxxxx
snapctr_pwd: 'xxxxxxx'
```

```
backup_policy: 'Oracle Full offline Backup'
# Linux specific config variables
# Oracle specific config variables
```

## Configurazione variabili host

Le variabili host sono definite nella directory `host_vars` denominata `{{ host_name }}`.yml. Di seguito è riportato un esempio di file di variabile host Oracle di destinazione `ora_04.cie.netapp.com.yml` che mostra la configurazione tipica.

```
# User configurable Oracle clone db host specific parameters
```

```
# Source database to clone from
source_db_sid: NTAP1
source_db_host: ora_03.cie.netapp.com
```

```
# Clone database
clone_db_sid: NTAP1DEV
```

```
snapctr_obj_id: '{{ source_db_host }}\{{ source_db_sid }}
```

### Configurazione aggiuntiva del server Oracle di destinazione dei cloni

Il server Oracle di destinazione della clonazione deve avere lo stesso stack software Oracle del server Oracle di origine installato e sottoposto a patch. L'utente Oracle `.bash_profile` ha `$ORACLE_BASE` e `$ORACLE_HOME` configurato. Inoltre, la variabile `$ORACLE_HOME` deve corrispondere all'impostazione del server Oracle di origine. Di seguito viene riportato un esempio.

```
# .bash_profile
```

```
# Get the aliases and functions
if [ -f ~/.bashrc ]; then
    . ~/.bashrc
fi
```

```
# User specific environment and startup programs
export ORACLE_BASE=/u01/app/oracle
export ORACLE_HOME=/u01/app/oracle/product/19.0.0/NTAP1
```

### Esecuzione Playbook

Sono disponibili un totale di tre playbook per eseguire il ciclo di vita dei cloni del database Oracle con le utility della CLI di SnapCenter.

1. Installare i prerequisiti del controller Ansible - una sola volta.

```
ansible-playbook -i hosts ansible_requirements.yml
```

2. File di configurazione clone - una sola volta.

```
ansible-playbook -i hosts clone_1_setup.yml -u admin -e  
@vars/vars.yml
```

3. Crea e aggiorna regolarmente il database dei cloni da crontab con uno script shell per chiamare un playbook di refresh.

```
0 */4 * * * /home/admin/na_oracle_clone_lifecycle/clone_1_refresh.sh
```

Per un database clone aggiuntivo, creare un clone\_n\_setup.yml e clone\_n\_refresh.yml separati e clone\_n\_refresh.sh. Configurare di conseguenza gli host di destinazione Ansible e il file hostname.yml nella directory host\_vars.

## Dove trovare ulteriori informazioni

Per ulteriori informazioni sull'automazione delle soluzioni NetApp, consulta il seguente sito Web ["Automazione delle soluzioni NetApp"](#)

# TR-4988: Backup, recovery e cloning di database Oracle su ANF con SnapCenter

Allen Cao, Niyaz Mohamed, NetApp

## Scopo

Il software NetApp SnapCenter è una piattaforma aziendale di facile utilizzo per coordinare e gestire in modo sicuro la protezione dei dati tra applicazioni, database e file system. Semplifica backup, ripristino e Lifecycle management dei cloni scaricando questi task ai proprietari delle applicazioni senza sacrificare la capacità di sovrintendere e regolamentare l'attività nei sistemi storage. Sfruttando la gestione dei dati basata su storage, consente di aumentare performance e disponibilità, nonché di ridurre i tempi richiesti per test e sviluppo.

In TR-4987, ["Implementazione semplificata e automatizzata di Oracle su Azure NetApp Files con NFS"](#), Dimostriamo la distribuzione automatizzata di Oracle su Azure NetApp Files (ANF) nel cloud Azure. In questa documentazione, presenteremo la protezione e la gestione dei database Oracle su ANF nel cloud Azure con un tool dell'interfaccia utente SnapCenter molto intuitivo.

Questa soluzione risolve i seguenti casi di utilizzo:

- Backup e recovery di database Oracle implementati in ANF nel cloud Azure con SnapCenter.
- Gestisci snapshot del database e copie clonate per accelerare lo sviluppo applicativo e migliorare la gestione del ciclo di vita dei dati.

## Pubblico

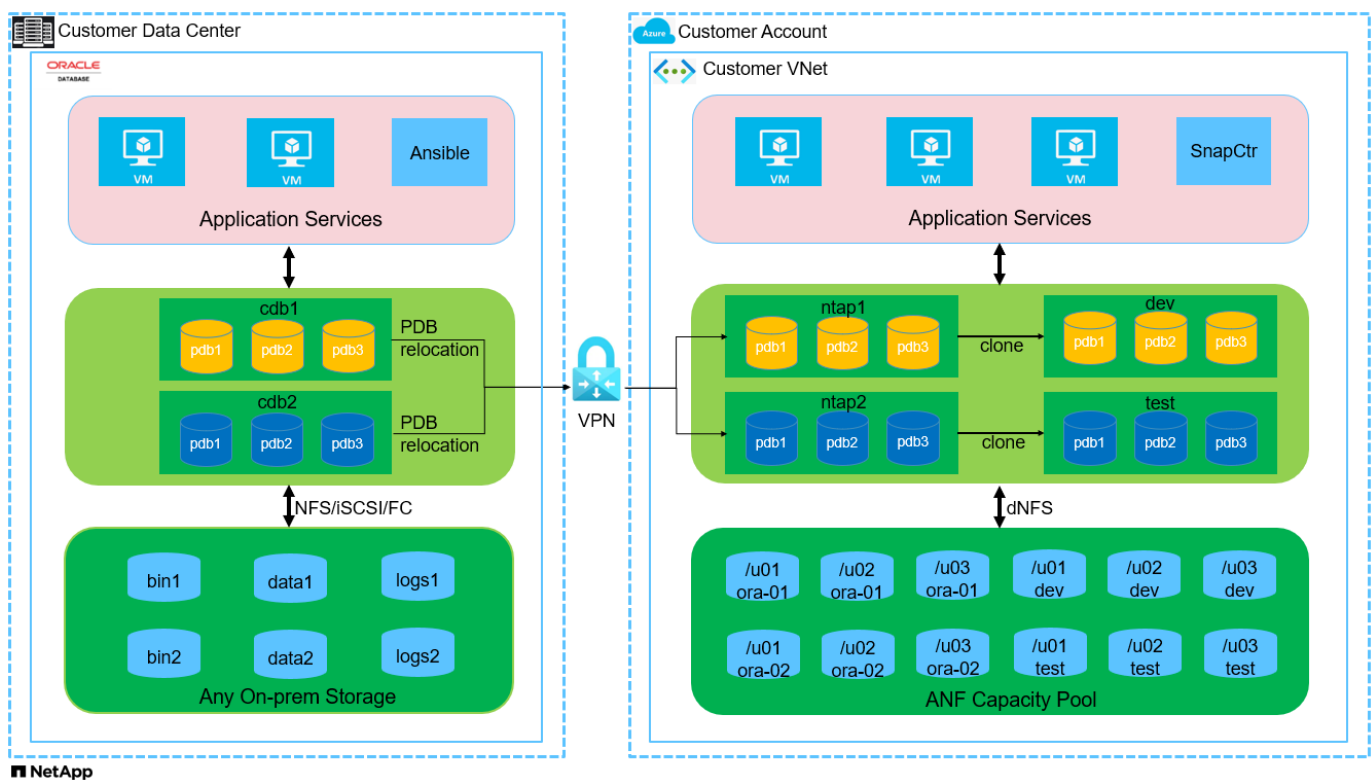
Questa soluzione è destinata alle seguenti persone:

- Un DBA che vorrebbe implementare i database Oracle su Azure NetApp Files.
- Un Solution Architect per database che vorrebbe testare i carichi di lavoro Oracle su Azure NetApp Files.
- Un amministratore dello storage che desidera implementare e gestire i database Oracle su Azure NetApp Files.
- Un proprietario di applicazioni che desidera creare un database Oracle su Azure NetApp Files.

## Ambiente di test e convalida della soluzione

Il test e la convalida di questa soluzione sono stati eseguiti in un laboratorio che potrebbe non corrispondere all'ambiente di distribuzione finale. Vedere la sezione [\[Key Factors for Deployment Consideration\]](#) per ulteriori informazioni.

## Architettura



## Componenti hardware e software

Hardware		
Azure NetApp Files	Attuale offerta in Azure di Microsoft	Pool di capacità con livello di servizio Premium

Azure VM per server DB	Standard_B4ms - 4 vCPU, 16GiB	Due istanze di macchine virtuali Linux
Azure VM per SnapCenter	Standard_B4ms - 4 vCPU, 16GiB	Una istanza di macchina virtuale Windows
<b>Software</b>		
RedHat Linux	RHEL Linux 8,6 (LVM) - x64 Gen2	Implementazione dell'abbonamento a RedHat per il test
Server Windows	2022 DataCenter; AE HotPatch - x64 Gen2	Server SnapCenter di hosting
Database Oracle	Versione 19.18	Patch p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Versione 12.2.0.1.36	Patch p6880880_190000_Linux-x86-64.zip
Server SnapCenter	Versione 5,0	Distribuzione di gruppi di lavoro
Aprire JDK	Versione java-11-openjdk	Requisito del plugin SnapCenter per macchine virtuali DB
NFS	Versione 3.0	Oracle DNFS abilitato
Ansible	nucleo 2.16.2	Python 3.6.8

### Configurazione del database Oracle nell'ambiente di laboratorio

Server	Database	Archiviazione DB
ora-01	NTAP1 (NTAP1_PDB1,NTAP1_PDB2,NTAP1_PDB3)	/U01, /U02, /U03 montaggi NFS su pool di capacità ANF
ora-02	NTAP2 (NTAP2_PDB1,NTAP2_PDB2,NTAP2_PDB3)	/U01, /U02, /U03 montaggi NFS su pool di capacità ANF

### Fattori chiave per l'implementazione

- **Distribuzione SnapCenter.** SnapCenter può essere distribuito in un dominio Windows o in un ambiente workgroup. Per la distribuzione basata sul dominio, l'account utente del dominio deve essere un account amministratore del dominio o l'utente del dominio appartiene al gruppo dell'amministratore locale sul server host SnapCenter.
- **Risoluzione del nome.** il server SnapCenter deve risolvere il nome all'indirizzo IP per ogni host del server del database di destinazione gestito. Ciascun host del server di database di destinazione deve risolvere il nome del server SnapCenter all'indirizzo IP. Se un server DNS non è disponibile, aggiungere la denominazione ai file host locali per la risoluzione.
- **Configurazione del gruppo di risorse.** il gruppo di risorse in SnapCenter è un raggruppamento logico di risorse simili che possono essere sottoposte a backup insieme. In questo modo, semplifica e riduce il numero di processi di backup in un ambiente di database di grandi dimensioni.
- **Backup completo del database e del log di archivio.** il backup completo del database include snapshot di gruppo coerenti dei volumi di dati e di registro. Una snapshot frequente e completa del database implica

un maggiore consumo dello storage, ma migliora l'RTO. Un'alternativa è rappresentata da snapshot di database completi meno frequenti e backup dei registri di archivio più frequenti, che consumano meno storage e migliorano l'RPO ma possono estendere l'RTO. Durante la configurazione dello schema di backup, tieni in considerazione gli obiettivi di RTO e RPO. Esiste anche un limite (1023) del numero di backup snapshot su un volume.

- **Delega dei privilegi.** sfruttare il controllo dell'accesso basato sui ruoli integrato nell'interfaccia utente di SnapCenter per delegare i privilegi ai team di applicazioni e database, se lo si desidera.

## Implementazione della soluzione

Le seguenti sezioni forniscono procedure passo per passo per implementazione di SnapCenter, configurazione e backup, recovery e cloning dei database Oracle in Azure NetApp Files nel cloud Azure.

### Prerequisiti per l'implementazione

L'implementazione richiede database Oracle esistenti in esecuzione su ANF in Azure. In caso contrario, attenersi alla procedura riportata di seguito per creare due database Oracle da convalidare con la soluzione. Per informazioni dettagliate sull'implementazione del database Oracle in ANF nel cloud Azure con automazione, fare riferimento al documento TR-4987: ["Implementazione semplificata e automatizzata di Oracle su Azure NetApp Files con NFS"](#)

1. È stato configurato un account Azure e all'interno dell'account Azure sono stati creati i segmenti di rete e VNET necessari.
2. Dal portale cloud Azure, implementa le macchine virtuali Azure Linux come server Oracle DB. Creare un pool di capacità Azure NetApp Files e volumi di database per il database Oracle. Abilitare l'autenticazione a chiave privata/pubblica SSH VM per azureuser nei server DB. Per ulteriori informazioni sulla configurazione dell'ambiente, fare riferimento al diagramma dell'architettura riportato nella sezione precedente. A cui si fa anche riferimento ["Procedure di implementazione Oracle dettagliate su Azure VM e Azure NetApp Files"](#) per informazioni dettagliate.



Per le macchine virtuali Azure distribuite con ridondanza del disco locale, assicurarsi di aver allocato almeno 128G GB nel disco principale della macchina virtuale in modo da avere spazio sufficiente per preparare i file di installazione di Oracle e aggiungere il file di swap del sistema operativo. Espandere di conseguenza la partizione del sistema operativo /tmplv e /rootlv. Assicurarsi che la denominazione del volume del database sia conforme alle convenzioni VMname-U01, VMname-U02 e VMname-U03.

```
sudo lvresize -r -L +20G /dev/mapper/rootvg-rootlv
```

```
sudo lvresize -r -L +10G /dev/mapper/rootvg-tmplv
```

3. Dal portale cloud Azure, eseguire il provisioning di un server Windows per eseguire lo strumento UI di NetApp SnapCenter con la versione più recente. Fare riferimento al seguente link per i dettagli: ["Installare il server SnapCenter"](#).
4. Esegui il provisioning di una VM Linux come nodo di controller Ansible con l'ultima versione di Ansible e Git installata. Fare riferimento al seguente link per i dettagli: ["Introduzione all'automazione delle soluzioni NetApp"](#) nella sezione -  
Setup the Ansible Control Node for CLI deployments on RHEL / CentOS oppure  
Setup the Ansible Control Node for CLI deployments on Ubuntu / Debian.



Il nodo del controller Ansible può individuare on-premise o nel cloud Azure, nella misura in cui può raggiungere le VM di Azure DB tramite la porta ssh.

5. Clona una copia del toolkit di automazione dell'implementazione Oracle di NetApp per NFS. Seguire le istruzioni riportate in ["TR-4887"](#) per eseguire i playbook.

```
git clone https://bitbucket.ngage.netapp.com/scm/ns-bb/na_oracle_deploy_nfs.git
```

6. Fase successiva ai file di installazione di Oracle 19c nella directory Azure DB VM /tmp/archive con autorizzazione 777.

```
installer_archives:  
- "LINUX.X64_193000_db_home.zip"  
- "p34765931_190000_Linux-x86-64.zip"  
- "p6880880_190000_Linux-x86-64.zip"
```

7. Guarda il seguente video:

[Backup, ripristino e cloning di database Oracle su ANF con SnapCenter](#)

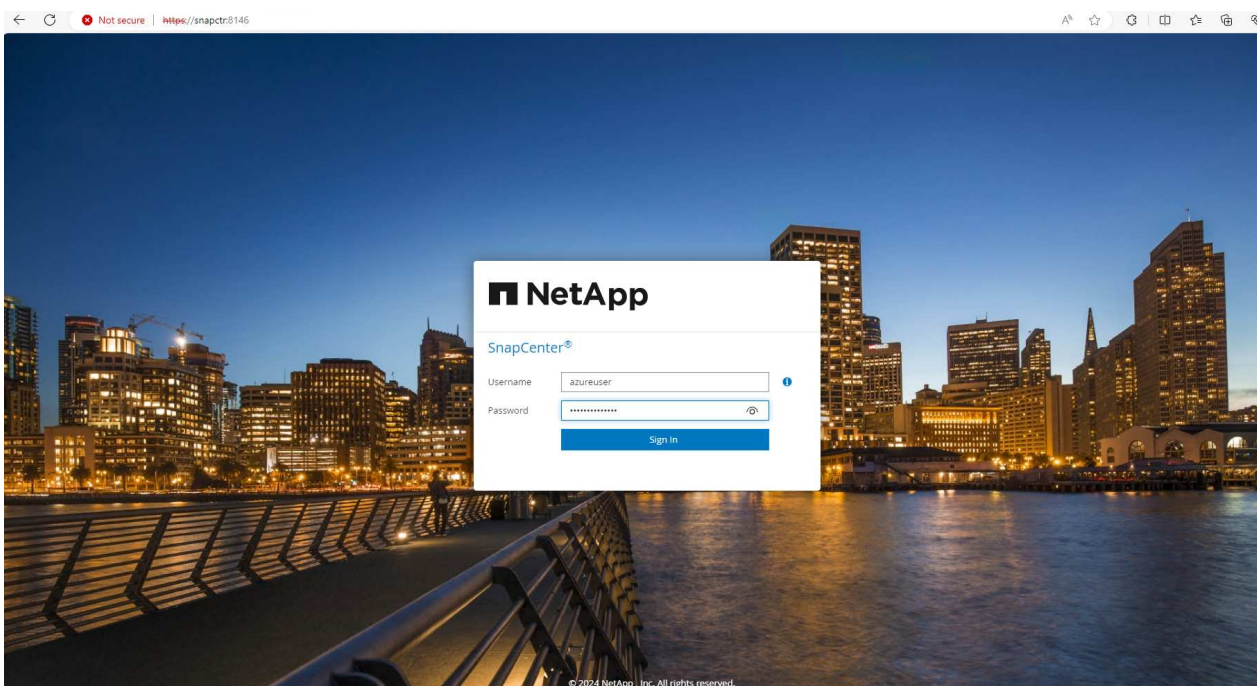
8. Esaminare Get Started menu online.

## Installazione e configurazione di SnapCenter

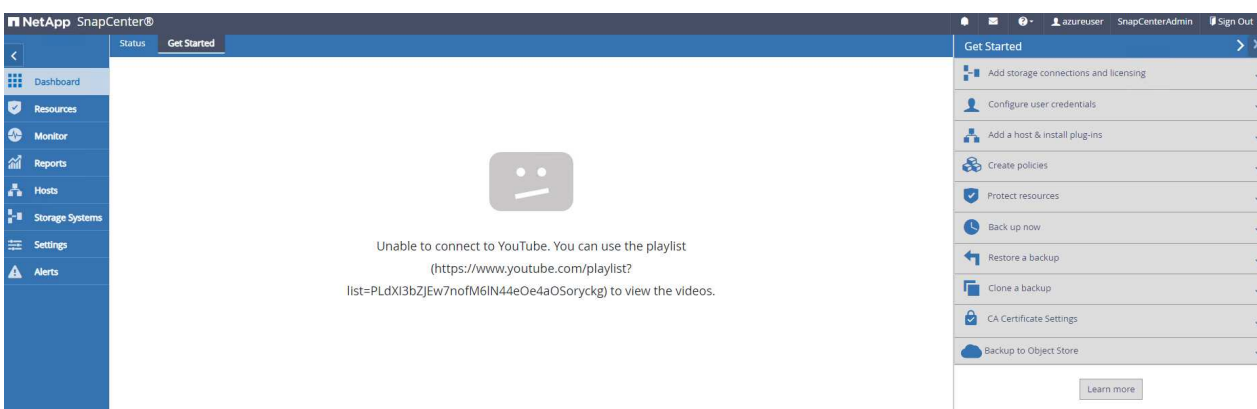


Si consiglia di accedere online "[Documentazione del software SnapCenter](#)" Prima di procedere all'installazione e alla configurazione di SnapCenter: . Di seguito viene fornito un riepilogo ad alto livello dei passaggi per l'installazione e la configurazione del software SnapCenter per Oracle su Azure ANF.

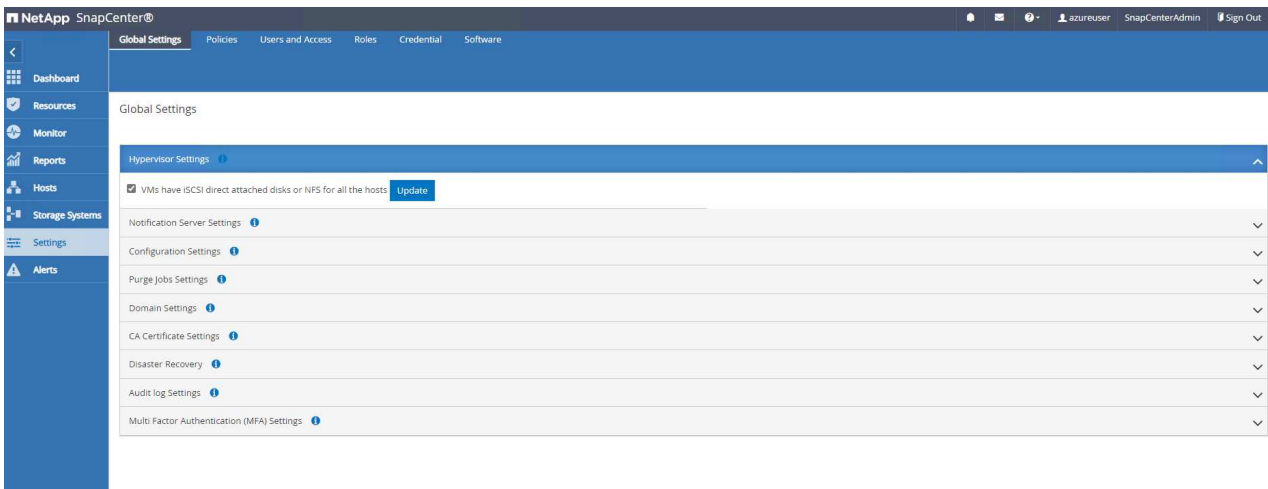
1. Dal server SnapCenter Windows, scaricare e installare l'ultima versione di java JDK dal sito Web "[Scarica Java per le applicazioni desktop](#)".
2. Dal server Windows SnapCenter, scaricare e installare la versione più recente (attualmente 5,0) del file eseguibile di installazione SnapCenter dal sito di supporto NetApp: "[NetApp | Assistenza](#)".
3. Dopo l'installazione del server SnapCenter, avviare il browser per accedere a SnapCenter con le credenziali dell'utente amministratore locale o dell'utente di dominio Windows tramite la porta 8146.



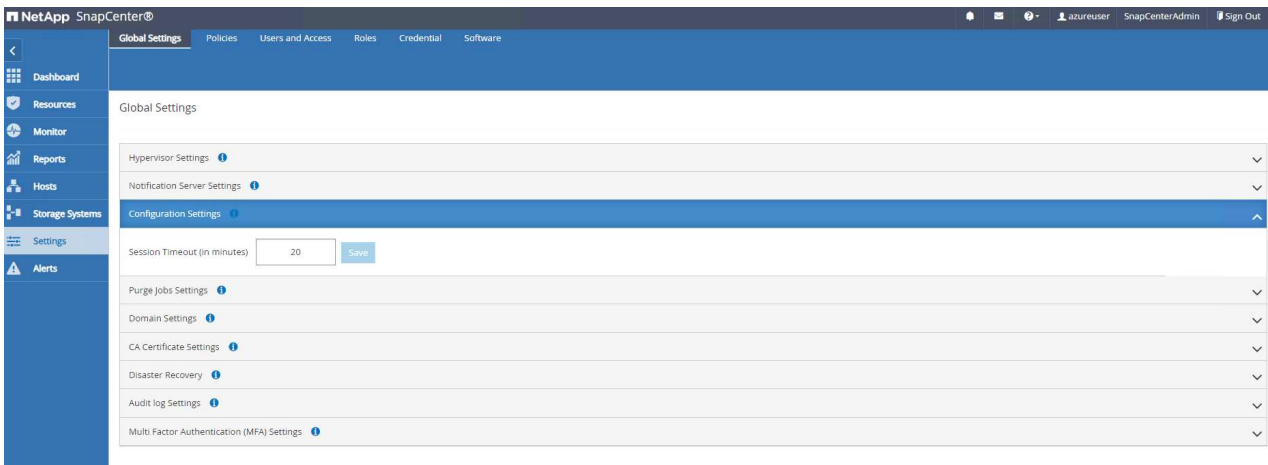
4. Revisione Get Started menu online.



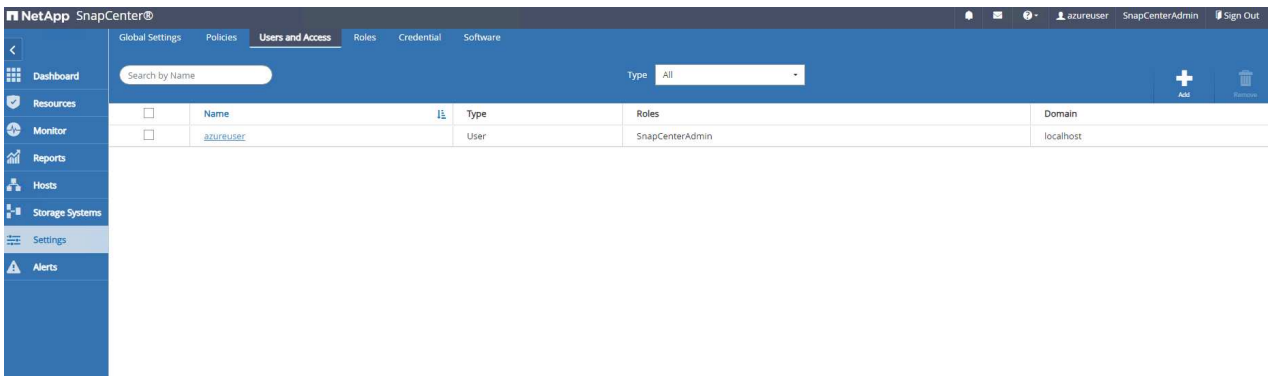
5. Poll Settings-Global Settings, controllo Hypervisor Settings E fare clic su Aggiorna.



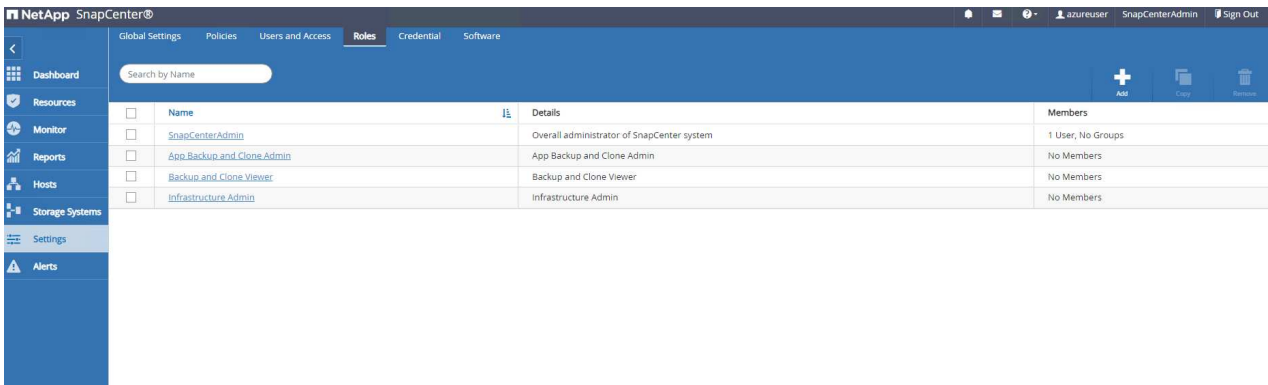
6. Se necessario, regolare Session Timeout Per l'interfaccia utente di SnapCenter all'intervallo desiderato.



7. Se necessario, aggiungere altri utenti a SnapCenter.



8. Il Roles Elenca i ruoli incorporati che possono essere assegnati a diversi utenti SnapCenter. I ruoli personalizzati possono anche essere creati dall'utente amministratore con i privilegi desiderati.



NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

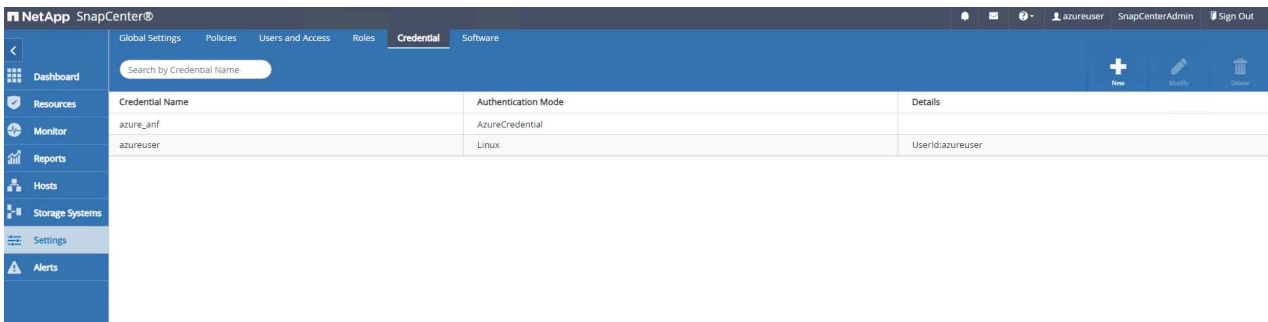
Search by Name

Name	Details	Members
<a href="#">SnapCenterAdmin</a>	Overall administrator of SnapCenter system	1 User, No Groups
<a href="#">App Backup and Clone Admin</a>	App Backup and Clone Admin	No Members
<a href="#">Backup and Clone Viewer</a>	Backup and Clone Viewer	No Members
<a href="#">Infrastructure Admin</a>	Infrastructure Admin	No Members

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

+ Add Copy Remove

9. Da Settings-Credential, Creare le credenziali per gli obiettivi di gestione SnapCenter. In questo caso di utilizzo dimostrativo, sono utenti linux per l'accesso ad Azure VM e credenziali ANF per l'accesso al pool di capacità.



NetApp SnapCenter®

Global Settings Policies Users and Access Roles Credential Software

Search by Credential Name

Credential Name	Authentication Mode	Details
azure_anf	AzureCredential	
azureuser	Linux	Userid:azureuser

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

+ New Modify Remove

Credential

✕

Credential Name

azureuser

Authentication Mode

Linux

▼

Authentication Type

☐ Password Based

☒ SSH Key Based

i

Username

azureuser

i

SSH Private Key

XRlRk1QCaE0Hg==  
-----END RSA PRIVATE KEY-----

i

☒ Use sudo privileges

i

Cancel

OK

Credential

Credential Name

azure\_anf

Authentication Mode

Azure Credential

Azure Details

Tenant ID

Enter Tenant Id

Client ID

Enter Client Id

Client Secret Key

Enter client secret key

Cancel

OK

- Da Storage Systems scheda, aggiungi Azure NetApp Files con la credenziale creata in precedenza.

NetApp SnapCenter®

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

ONTAP Storage

Azure NetApp Files

Search by NetApp Account

NetApp Account

Resource Group

Credential

ANFAVSAcct

ANFAVSRG

azure\_anf

Add Azure NetApp Account

Credential

azure\_anf

Subscription

Hybrid Cloud TME Onprem

NetApp Account

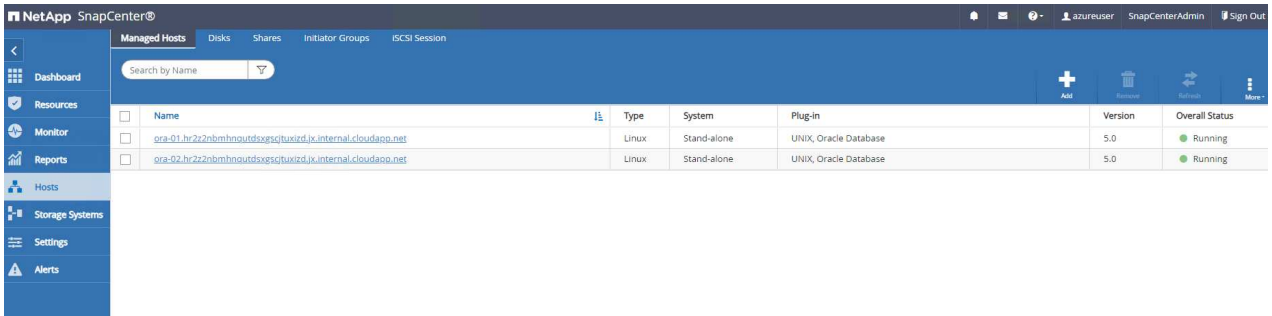
ANFAVSAcct (ResourceGroup: ANFAVSRG)

Submit

Cancel

15

11. Da Hosts Tab, Aggiungi Azure DB VM, che installa il plug-in SnapCenter per Oracle su Linux.



Name	Type	System	Plug-in	Version	Overall Status
ora-01.hr2z2nbmhnoutdxxsgtuoazd.ix.internal.cloudapp.net	Linux	Stand-alone	UNIX, Oracle Database	5.0	Running
ora-02.hr2z2nbmhnoutdxxsgtuoazd.ix.internal.cloudapp.net	Linux	Stand-alone	UNIX, Oracle Database	5.0	Running

### Add Host

Host Type:

Host Name:

Credentials:   

### Select Plug-ins to Install SnapCenter Plug-ins Package 5.0 for Linux

- ☒ Oracle Database
- ☐ SAP HANA
- ☐ Unix File Systems

 [More Options](#): Port, Install Path, Custom Plug-Ins...

More Options

Port

8145

Installation Path

/opt/NetApp/snapcenter

☒

Skip optional preinstall checks

☒

Add all hosts in the oracle RAC

Custom Plug-ins

Choose a File

Browse

Upload

No plug-ins found.

Save

Cancel

12. Una volta installato il plug-in host sulla VM del server DB, i database sull'host vengono rilevati automaticamente e visibili in Resources scheda. Torna a. Settings-Polices, Creare criteri di backup per il backup online completo del database Oracle e il backup solo dei registri di archivio. Consultare questo documento "[Creare policy di backup per i database Oracle](#)" per le procedure dettagliate.

NetApp SnapCenter®

Global Settings

Policies

Users and Access

Roles

Credential

Software

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

Oracle Database

Search by Name

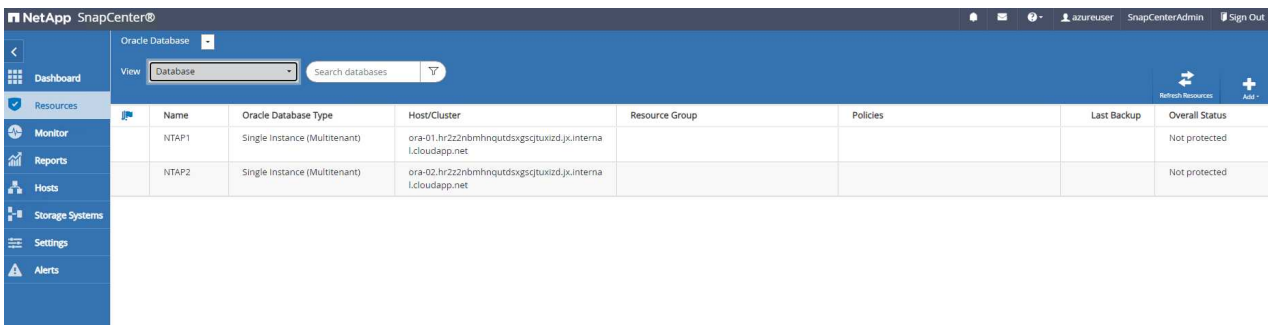
+

Name	Backup Type	Schedule Type	Replication	Verification
Oracle archivelogs backup	LOG, ONLINE	Hourly		
Oracle full online backup	FULL, ONLINE	Hourly		

## Backup del database

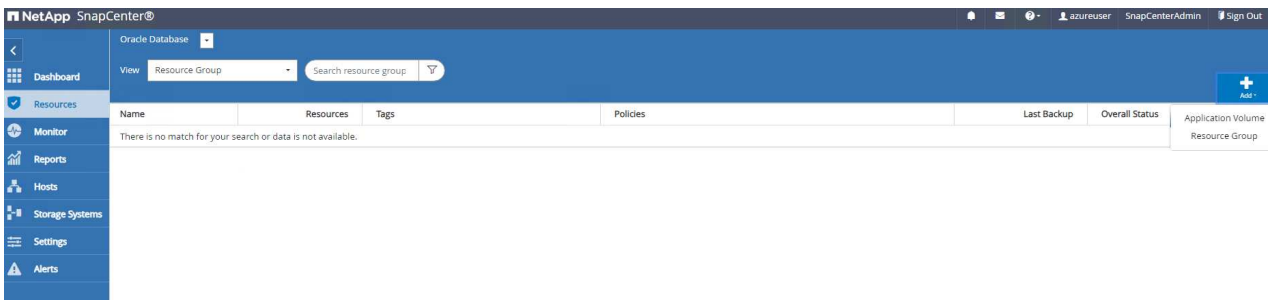
Il backup di uno snapshot NetApp crea un'immagine point-in-time dei volumi di database che è possibile utilizzare per il ripristino in caso di errore di sistema o perdita di dati. I backup di Snapshot richiedono pochissimo tempo, generalmente meno di un minuto. L'immagine di backup consuma uno spazio di storage minimo e subisce un overhead delle performance trascurabile poiché registra solo le modifiche ai file dall'ultima copia snapshot effettuata. Nella sezione seguente viene illustrata l'implementazione di snapshot per il backup del database Oracle in SnapCenter.

1. Navigazione verso **Resources** Che elenca i database rilevati dopo l'installazione del plugin SnapCenter sulla VM del database. Inizialmente, il **Overall Status** del database viene visualizzato come **Not protected**.



Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
INTAP1	Single Instance (Multitenant)	ora-01.hr2z2nbnhngutdsxsgtuzidj.xu.interna.lcloudapp.net				Not protected
INTAP2	Single Instance (Multitenant)	ora-02.hr2z2nbnhngutdsxsgtuzidj.xu.interna.lcloudapp.net				Not protected

2. Fare clic su **View** a discesa per passare a **Resource Group**. Fare clic su **Add** Accedere a destra per aggiungere un gruppo di risorse.



Name	Resources	Tags	Policies	Last Backup	Overall Status	Application Volume
There is no match for your search or data is not available.						

3. Assegnare un nome al gruppo di risorse, ai tag e a qualsiasi denominazione personalizzata.



New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name

Tags

☒ Use custom name format for Snapshot copy

Backup settings

Exclude archive log destinations from backup

Previous Next

4. Aggiungere risorse al Resource Group. Il raggruppamento di risorse simili può semplificare la gestione dei database in un ambiente di grandi dimensioni.

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host

Available Resources

Selected Resources

NTAP1 (ora-01.hr2z2nbmhnqutdsxsgqtuxizd.jk.internal.cloudapp.net)  
NTAP2 (ora-02.hr2z2nbmhnqutdsxsgqtuxizd.jk.internal.cloudapp.net)

»  
«

Previous Next

5. Selezionare il criterio di backup e impostare una pianificazione facendo clic sul segno "+" in Configure Schedules.



Select one or more policies and configure schedules

Oracle full online backup + ⓘ

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
Oracle full online backup	None	+

Total 1

Previous Next

## Add schedules for policy Oracle full online backup

### Hourly

Start date

02/06/2024 05:55 pm



☐ Expires on

03/06/2024 05:51 pm



Repeat every

2



hours

0

mins



The schedules are triggered in the SnapCenter Server time zone.

Cancel

OK

6. Se la verifica del backup non è configurata nel criterio, lasciare la pagina di verifica così com'è.

New Resource Group

1

2

3

4

5

6

Name

Resources

Policies

Verification

Notification

Summary

Configure verification schedules

Policy

🔍

Schedule Type

Applied Schedules

Configure Schedules

There is no match for your search or data is not available.

Total 0

Previous

Next

7. Per inviare un report di backup e una notifica tramite e-mail, è necessario un server di posta SMTP nell'ambiente. Oppure lasciarla nera se un server di posta non è configurato.

New Resource Group

1

2

3

4

5

6

Name

Resources

Policies

Verification

Notification

Summary

Provide email settings ⓘ

Select the service accounts or people to notify regarding protection issues.

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

Previous

Next

8. Riepilogo del nuovo gruppo di risorse.

New Resource Group

1

2

3

4

5

6

Name

Resources

Policies

Verification

Notification

Summary

Resource group name

full\_online\_bkup

Tags

oradata

Policy

Oracle full online backup: Hourly

Plug-in

SnapCenter Plug-in for Oracle Database

Verification enabled for policy

None

Send email

No

Previous

Finish

9. Ripetere le procedure descritte sopra per creare un backup solo del registro di archivio del database con i criteri di backup corrispondenti.

NetApp SnapCenter®

Oracle Database

View Resource Group

Search resource group

Name	Resources	Tags	Policies	Last Backup	Overall Status
full_online_bkup	2	oradata	Oracle full online backup	02/06/2024 6:00:44 PM	Completed
archivelog_bkup	2	oralog	Oracle archivelogs backup	02/06/2024 5:59:25 PM	Completed

10. Fare clic su un gruppo di risorse per visualizzare le risorse incluse. Oltre al processo di backup pianificato, è possibile attivare un backup singolo facendo clic su Backup Now.

NetApp SnapCenter®

Oracle Database

full\_online\_bkup Details

Search resource groups

search

Modify Resource Group

Backup Now

Maintenance

Delete

Name	Resource Name	Type	Host
full_online_bkup	NTAP1	Oracle Database	ora-01.hr22n2bmhnqutdsxgscjuxizd.jx.internal.cloudapp.net
archivelog_bkup	NTAP2	Oracle Database	ora-02.hr22n2bmhnqutdsxgscjuxizd.jx.internal.cloudapp.net

Backup

×

Create a backup for the selected resource group

Resource Group

full\_online\_bkup

Policy

Oracle full online backup

▼

i

☐ Verify after backup

Cancel

Backup

11. Fare clic sul lavoro in esecuzione per aprire una finestra di monitoraggio che consente all'operatore di tenere traccia dell'avanzamento del lavoro in tempo reale.

## Job Details



Backup of Resource Group 'full\_online\_bkup' with policy 'Oracle full online backup'

✓ ▾ Backup of Resource Group 'full\_online\_bkup' with policy 'Oracle full online backup'

✓ ▶ ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net

✓ ▶ ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net

📘 Task Name: Backup of Resource Group 'full\_online\_bkup' with policy 'Oracle full online backup' Start Time: 02/06/2024 6:00:05 PM End Time: 02/06/2024 6:00:44 PM

View Logs

Cancel Job

Close

- Una volta completato un processo di backup, viene visualizzato un set di backup snapshot nella topologia del database. Un set di backup completo del database include uno snapshot dei volumi dei dati del database e uno snapshot dei volumi del log del database. Un backup di solo registro contiene solo uno snapshot dei volumi di registro del database.

NetApp SnapCenter

azureuser SnapCenterAdmin Sign Out

Oracle Database

Search resource groups

full\_online\_bkup Details

search

NTAP1 Topology

Manage Copies

3 Backups0 ClonesLocal copies

Summary Card

3 Backups1 Data Backup2 Log Backups0 Clones0 Snapshots Locked

Primary Backup(s)

search

Backup Name	Snapshot Lock Expiration	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora-01_02-06-2024_18_00_06_0582_1		1	Log	02/06/2024 6:00:41 PM	Not Applicable	False	Not Cataloged	3374950
ora-01_02-06-2024_18_00_06_0582_0		1	Data	02/06/2024 6:00:26 PM	Unverified	False	Not Cataloged	3374903
ora-01_02-06-2024_17_59_01_1158_1		1	Log	02/06/2024 5:59:18 PM	Not Applicable	False	Not Cataloged	3374762

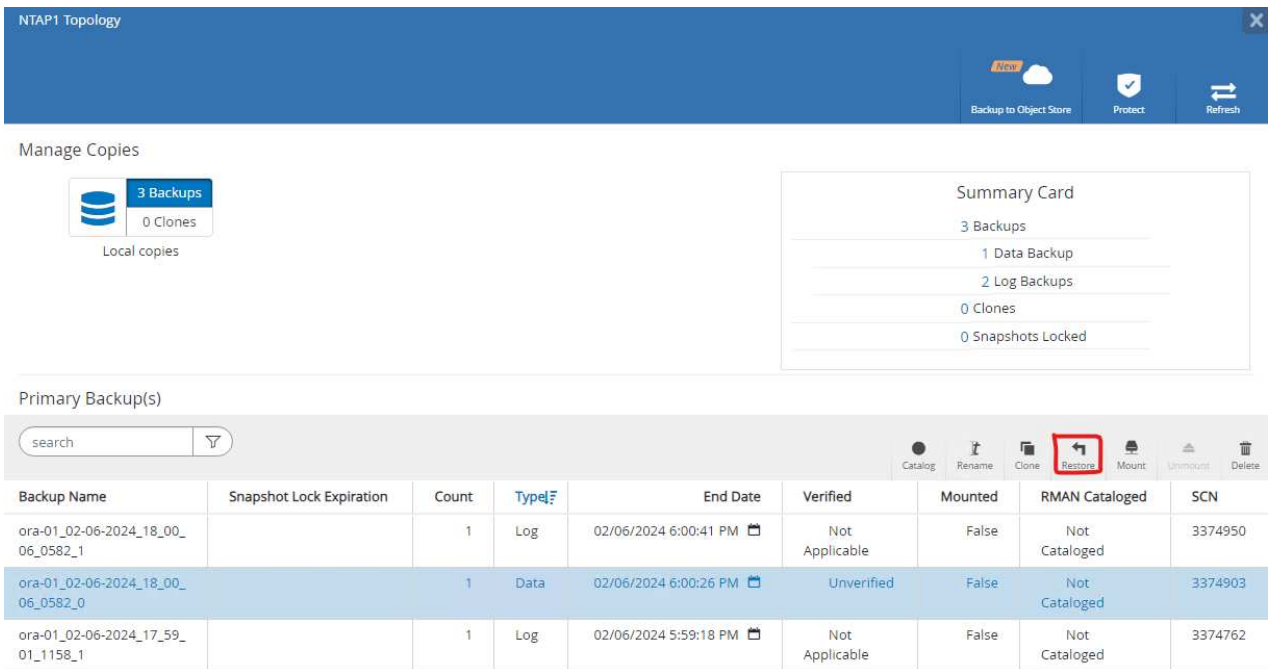
Total 2

Total 3

Recovery del database

Ripristino di database tramite SnapCenter consente di ripristinare una copia Snapshot point-in-time dell'immagine del volume di database. Il database viene quindi inoltrato a un punto desiderato da SCN/timestamp o da un punto come consentito dai log di archivio disponibili nel set di backup. Nella sezione seguente viene illustrato il flusso di lavoro di ripristino del database con l'interfaccia utente di SnapCenter.

1. Da **Resources** aprire il database **Primary Backup(s)** pagina. Scegliere lo snapshot del volume di dati del database, quindi fare clic su **Restore** per avviare il flusso di lavoro di ripristino del database. Se si desidera eseguire il ripristino da Oracle SCN o timestamp, annotare il numero SCN o l'indicatore data e ora nei set di backup.



NTAP1 Topology

Manage Copies

3 Backups  
0 Clones  
Local copies

Summary Card

3 Backups

1 Data Backup

2 Log Backups

0 Clones

0 Snapshots Locked

Primary Backup(s)

search

Catalog Rename Clone **Restore** Mount Unmount Delete

Backup Name	Snapshot Lock Expiration	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora-01_02-06-2024_18_00_06_0582_1		1	Log	02/06/2024 6:00:41 PM	Not Applicable	False	Not Cataloged	3374950
ora-01_02-06-2024_18_00_06_0582_0		1	Data	02/06/2024 6:00:26 PM	Unverified	False	Not Cataloged	3374903
ora-01_02-06-2024_17_59_01_1158_1		1	Log	02/06/2024 5:59:18 PM	Not Applicable	False	Not Cataloged	3374762

2. Selezionare **Restore Scope**. Per un database di container, SnapCenter è flessibile per eseguire un ripristino a livello di tablespace, database inseribili o database completo di container (tutti i file di dati).



Restore NTAP1

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Restore Scope ⓘ

☒ All Datafiles

☐ Pluggable databases (PDBs)

☐ Pluggable database (PDB) tablespaces

☐ Control files

Database State

☒ Change database state if needed for restore and recovery

Restore Mode ⓘ

☐ Force in place restore

If this check box is not selected and if any of the in place restore criteria is not met, restore will be performed using the connect and copy method. The connect and copy restore method might take time based on the files being restored.

Previous

Next

3. **Selezionare Recovery Scope.** All logs significa applicare tutti i log di archivio disponibili nel set di backup. Sono disponibili anche il ripristino point-in-time da parte di SCN o timestamp.

Restore NTAP1

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Choose Recovery Scope

☒ All Logs

☐ Until SCN (System Change Number)

☐ Date and Time

☐ No recovery

Specify external archive log files locations

Previous

Next

4. Il **PreOps** consente l'esecuzione di script sul database prima dell'operazione di ripristino/ripristino.

Restore NTAP1

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Specify optional scripts to run before performing a restore job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Previous

Next

5. Il `PostOps` consente l'esecuzione di script sul database dopo l'operazione di ripristino/ripristino.

Restore NTAP1

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Specify optional scripts to run after performing a restore job

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Arguments

☒ Open the database or container database in READ-WRITE mode after recovery

Previous

Next

6. Notifica via e-mail, se lo si desidera.

Restore NTAP1

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

⚠ If you want to send notifications for Restore jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Next

## 7. Ripristinare il riepilogo del processo

Restore NTAP1

1 Restore Scope

2 Recovery Scope

3 PreOps

4 PostOps

5 Notification

6 Summary

Summary

Backup name	ora-01_02-06-2024_18_00_06_0582_0
Backup date	02/06/2024 6:00:26 PM
Restore scope	All DataFiles
Recovery scope	All Logs
Options	Change database state if necessary , Open the database or container database in READ-WRITE mode after recovery
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

Previous

Finish

8. Fare clic su processo in esecuzione per aprirlo Job Details finestra. Lo stato del lavoro può essere aperto e visualizzato anche da Monitor scheda.

## Job Details



Restore 'ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net\NTAP1'

✓ ▼ Restore 'ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net\NTAP1'

✓ ▼ ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net

- ✓ ▶ Prescripts
- ✓ ▶ Mount log backups
- ✓ ▶ Pre Restore
- ✓ ▶ Restore
- ✓ ▶ Post Restore
- ✓ ▶ Unmount log backups
- ✓ ▶ Postscripts
- ✓ ▶ Post Restore Cleanup
- ✓ ▶ Data Collection

❗ Task Name: ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net Start Time: 02/06/2024 4:04:55 PM End Time: 02/06/2024 4:08:42 PM

View Logs

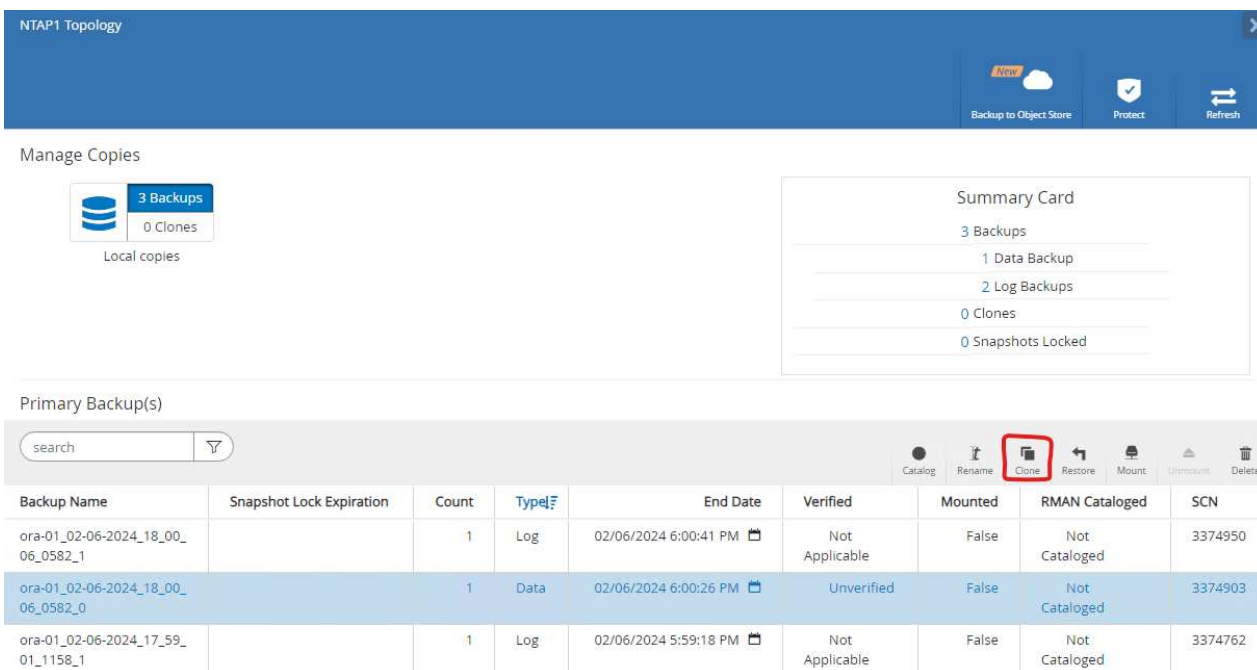
Cancel Job

Close

## Clone del database

Clone del database tramite SnapCenter viene ottenuto creando un nuovo volume da una snapshot di un volume. Il sistema utilizza le informazioni dello snapshot per clonare un nuovo volume utilizzando i dati sul volume quando è stata acquisita la snapshot. Cosa più importante, è rapida ed efficiente rispetto ad altri metodi per creare una copia clonata del database di produzione per supportare lo sviluppo o i test. Pertanto, migliora drasticamente la gestione del ciclo di vita delle applicazioni del database. Nella sezione seguente viene illustrato il flusso di lavoro del clone del database con interfaccia utente di SnapCenter.

1. Da **Resources** aprire il database **Primary Backup(s)** pagina. Scegliere lo snapshot del volume di dati del database, quindi fare clic su **clone** per avviare il flusso di lavoro dei cloni del database.



NTAP1 Topology

Manage Copies

3 Backups  
0 Clones  
Local copies

Summary Card

3 Backups

1 Data Backup

2 Log Backups

0 Clones

0 Snapshots Locked

Primary Backup(s)

search

Clone

Backup Name	Snapshot Lock Expiration	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
ora-01_02-06-2024_18_00_06_0582_1		1	Log	02/06/2024 6:00:41 PM	Not Applicable	False	Not Cataloged	3374950
ora-01_02-06-2024_18_00_06_0582_0		1	Data	02/06/2024 6:00:26 PM	Unverified	False	Not Cataloged	3374903
ora-01_02-06-2024_17_59_01_1158_1		1	Log	02/06/2024 5:59:18 PM	Not Applicable	False	Not Cataloged	3374762

2. Assegnare un nome al SID del database clone. In alternativa, per un database di container, il cloning può essere eseguito anche a livello di PDB.



Clone from NTAP1

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Capacity Pool Max. Throughput (MiB/s)

Complete Database Clone

Clone SID

Exclude PDBs

PDB Clone

ntap1dev

Type to find PDBs

Previous

Next

3. Selezionare il server DB in cui si desidera collocare la copia del database clonata. Mantenere le posizioni predefinite dei file a meno che non si desideri assegnare loro un nome diverso.

Clone from NTAP1

1 Name
2 Locations
3 Credentials
4 PreOps
5 PostOps
6 Notification
7 Summary

Select the host to create a clone

Clone host
ora-02.hr2z2nbmhnqudtsxgscjtuxizd.jx.inter

Datafile locations ⓘ

/u02\_ntap1dev
Reset

Control files ⓘ

/u02\_ntap1dev/ntap1dev/control/control01.ctl
X
+

/u02\_ntap1dev/ntap1dev/control/control02.ctl
X
Reset

Redo logs ⓘ

Group		Size	Unit	Number of files		
RedoGroup 1	X	200	MB	1	+	+ Reset
RedoGroup 2	X	200	MB	1	+	
RedoGroup 3	X	200	MB	1	+	

Previous
Next

- Lo stack software Oracle identico a quello del database di origine deve essere installato e configurato sull'host DB clone. Mantenere la credenziale predefinita ma modificarla Oracle Home Settings Per la corrispondenza con le impostazioni sull'host DB clone.

Clone from NTAP1

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user

None

+

i

Database port

1521

Oracle Home Settings

i

Oracle Home

/u01/app/oracle/product/19.0.0/NTAP2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

5. Il `PreOps` consente l'esecuzione degli script prima dell'operazione di clonazione. I parametri del database possono essere regolati per soddisfare le esigenze di un DB clone rispetto a un database di produzione, come una destinazione SGA ridotta.

Clone from NTAP1

×

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

processes	320	×	<div>+</div> <div>Reset</div>
remote_login_passwordfile	EXCLUSIVE	×	
sga_target	3G	×	
undo_tablespace	UNDOTBS1	×	

Previous

Next

- Il `PostOps` consente l'esecuzione di script sul database dopo l'operazione di clonazione. Il ripristino del database clone può essere basato su SCN, timestamp o fino a quando non viene annullato (rollforward del database all'ultimo log archiviato nel set di backup).

## Clone from NTAP1



1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

☒ Recover Database

☒ Until Cancel






☐ Date and Time



Date-time format: MM/DD/YYYY hh:mm:ss

☐ Until SCN (System Change Number)



Specify external archive log locations   

☒ Create new DBID 

☒ Create tempfile for temporary tablespace 

 Enter SQL queries to apply when clone is created

 Enter scripts to run after clone operation 

Previous

Next

7. Notifica via e-mail, se lo si desidera.

1 Name

Provide email settings ⓘ

2 Locations

Email preference

Never ▾

3 Credentials

From

From email

4 PreOps

To

Email to

5 PostOps

Subject

Notification

6 Notification

☐ Attach job report

7 Summary



If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

Previous

Next

## 8. Clona riepilogo processi.

Clone from NTAP1

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Summary

Clone from backup	ora-01_02-06-2024_18_00_06_0582_0
Clone SID	ntap1dev
Capacity Pool Max. Throughput (MiB/s)	none
Clone server	ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net
Exclude PDBs	none
Oracle home	/u01/app/oracle/product/19.0.0/NTAP2
Oracle OS user	oracle
Oracle OS group	oinstall
Datafile mountpaths	/u02_ntap1dev
Control files	/u02_ntap1dev/ntap1dev/control/control01.ctl /u02_ntap1dev/ntap1dev/control/control02.ctl
Redo groups	RedoGroup =1 TotalSize =200 Path =/u02_ntap1dev/ntap1dev/redolog/redo01_01.log RedoGroup =2 TotalSize =200 Path =/u02_ntap1dev/ntap1dev/redolog/redo02_01.log RedoGroup =3 TotalSize =200 Path =/u02_ntap1dev/ntap1dev/redolog/redo03_01.log
Recovery scope	Until Cancel
Prescript full path	none
Prescript arguments	
Postscript full path	none
Postscript arguments	
Send email	No

Previous

Finish

9. Fare clic su processo in esecuzione per aprirlo Job Details finestra. Lo stato del lavoro può essere aperto e visualizzato anche da Monitor scheda.

Job Details

×

Clone from backup 'ora-01\_02-06-2024\_18\_00\_06\_0582\_0'

▼

Clone from backup 'ora-01\_02-06-2024\_18\_00\_06\_0582\_0'

▼

ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net

▶ Prescripts

▶ Query Host Information

▶ Prepare for Cloning

▶ Cloning Resources

▶ FileSystem Clone

▶ Application Clone

▶ Postscripts

▶ Register Clone

▶ Unmount Clone

▶ Data Collection

Task Name: ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net Start Time: 02/06/2024 6:21:59 PM End Time: 02/06/2024 6:28:10 PM

View Logs

Cancel Job

Close

10. Il database clonato si registra immediatamente con SnapCenter.

NetApp SnapCenter®								
Oracle Database								
View Database Search databases								
	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status	
	NTAP1	Single Instance (Multitenant)	ora-01.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net	archivelog_bkup full_online_bkup	Oracle archivelogs backup Oracle full online backup	02/06/2024 7:29:18 PM	Backup succeeded	
	ntap1dev	Single Instance (Multitenant)	ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net				Not protected	
	NTAP2	Single Instance (Multitenant)	ora-02.hr2z2nbmhnqutdsxgscjtuxizd.jx.internal.cloudapp.net	archivelog_bkup full_online_bkup	Oracle archivelogs backup Oracle full online backup	02/06/2024 7:29:19 PM	Backup succeeded	

11. Convalidare il database clone sull'host del server DB. Per un database di sviluppo clonato, la modalità di archiviazione dei database deve essere disattivata.



```

[azureuser@ora-02 ~]$ sudo su
[root@ora-02 azureuser]# su - oracle
Last login: Tue Feb  6 16:26:28 UTC 2024 on pts/0

[oracle@ora-02 ~]$ uname -a
Linux ora-02 4.18.0-372.9.1.el8.x86_64 #1 SMP Fri Apr 15 22:12:19
EDT 2022 x86_64 x86_64 x86_64 GNU/Linux
[oracle@ora-02 ~]$ df -h

```

Filesystem	Size	Used	Avail
Use% Mounted on			
devtmpfs	7.7G	0	7.7G
0% /dev			
tmpfs	7.8G	0	7.8G
0% /dev/shm			
tmpfs	7.8G	49M	7.7G
1% /run			
tmpfs	7.8G	0	7.8G
0% /sys/fs/cgroup			
/dev/mapper/rootvg-rootlv	22G	17G	5.6G
75% /			
/dev/mapper/rootvg-usrlv	10G	2.0G	8.1G
20% /usr			
/dev/mapper/rootvg-homelv	1014M	40M	975M
4% /home			
/dev/sda1	496M	106M	390M
22% /boot			
/dev/mapper/rootvg-varlv	8.0G	958M	7.1G
12% /var			
/dev/sda15	495M	5.9M	489M
2% /boot/efi			
/dev/mapper/rootvg-tmplv	12G	8.4G	3.7G
70% /tmp			
tmpfs	1.6G	0	1.6G
0% /run/user/54321			
172.30.136.68:/ora-02-u03	250G	2.1G	248G
1% /u03			
172.30.136.68:/ora-02-u01	100G	10G	91G
10% /u01			
172.30.136.68:/ora-02-u02	250G	7.5G	243G
3% /u02			
tmpfs	1.6G	0	1.6G
0% /run/user/1000			
tmpfs	1.6G	0	1.6G
0% /run/user/0			
172.30.136.68:/ora-01-u02-Clone-020624161543077	250G	8.2G	242G

```
4% /u02_ntapldev
```

```
[oracle@ora-02 ~]$ 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.
```

```
#
```

```
#
```

```
NTAP2:/u01/app/oracle/product/19.0.0/NTAP2:Y
```

```
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT  
REMOVE THIS LINE)
```

```
ntapldev:/u01/app/oracle/product/19.0.0/NTAP2:N
```

```
[oracle@ora-02 ~]$ export ORACLE_SID=ntapldev
```

```
[oracle@ora-02 ~]$ sqlplus / as sysdba
```

```
SQL*Plus: Release 19.0.0.0.0 - Production on Tue Feb 6 16:29:02 2024  
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
NTAP1DEV	READ WRITE	ARCHIVELOG

```
SQL> shutdown immediate;
```

Database closed.

Database dismounted.

ORACLE instance shut down.

```
SQL> startup mount;
```

ORACLE instance started.

Total System Global Area 3221223168 bytes

Fixed Size 9168640 bytes

Variable Size 654311424 bytes

Database Buffers 2550136832 bytes

Redo Buffers 7606272 bytes

Database mounted.

```
SQL> alter database noarchivelog;
```

Database altered.

```
SQL> alter database open;
```

Database altered.

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

NAME	OPEN_MODE	LOG_MODE
NTAP1DEV	READ WRITE	NOARCHIVELOG

```
SQL> show pdbs
```

CON_ID	CON_NAME	OPEN MODE	RESTRICTED
2	PDB\$SEED	READ ONLY	NO
3	NTAP1_PDB1	MOUNTED	
4	NTAP1_PDB2	MOUNTED	
5	NTAP1_PDB3	MOUNTED	

```
SQL> alter pluggable database all open;
```

## Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Azure NetApp Files

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

- Documentazione del software SnapCenter

["https://docs.netapp.com/us-en/snapcenter/index.html"](https://docs.netapp.com/us-en/snapcenter/index.html)

- TR-4987: Implementazione di Oracle semplificata e automatizzata su Azure NetApp Files con NFS

["https://docs.netapp.com/us-en/netapp-solutions/databases/automation\\_ora\\_anf\\_nfs.html"](https://docs.netapp.com/us-en/netapp-solutions/databases/automation_ora_anf_nfs.html)

## TR-4977: Backup, ripristino e cloning del database Oracle con servizi SnapCenter - Azure

Allen Cao, Niyaz Mohamed, NetApp

### Scopo

I servizi SnapCenter sono la versione SaaS del classico tool di interfaccia utente per la gestione dei database SnapCenter disponibile tramite la console di gestione del cloud NetApp BlueXP. È parte integrante dell'offerta di data Protection e backup per cloud di NetApp per database come Oracle e HANA eseguito su Azure NetApp Files. Questo servizio basato su SaaS semplifica l'implementazione di un server standalone SnapCenter tradizionale, che in genere richiede un server Windows che opera in un ambiente di dominio Windows.

In questa documentazione, dimostreremo come configurare i servizi SnapCenter per il backup, il ripristino e la clonazione di database Oracle implementati su Azure NetApp Files Volumes e istanze di calcolo Azure. È molto semplice configurare la data Protection per i database Oracle implementati su Azure NetApp Files con l'interfaccia utente BlueXP basata su web.

Questa soluzione risolve i seguenti casi di utilizzo:

- Backup del database con Snapshot per i database Oracle ospitati su macchine virtuali Azure NetApp Files e Azure
- Ripristino del database Oracle in caso di guasto
- Clonazione rapida di database primari per sviluppo, ambienti di test o altri casi di utilizzo

### Pubblico

Questa soluzione è destinata ai seguenti destinatari:

- I DBA che gestiscono i database Oracle in esecuzione su storage Azure NetApp Files
- Il Solution architect che è interessato a testare il backup, il ripristino e il clone del database Oracle in Azure
- L'amministratore dello storage che supporta e gestisce lo storage Azure NetApp Files
- Il proprietario dell'applicazione, che è proprietario delle applicazioni implementate sullo storage Azure NetApp Files e sulle macchine virtuali di Azure

## Ambiente di test e convalida della soluzione

Il 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, vedere la sezione [\[Key Factors for Deployment Consideration\]](#).

### Architettura

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

### Componenti hardware e software

#### Hardware

Storage Azure NetApp Files	Livello di servizio Premium	Tipo di qualità del servizio automatica e 4TB TB di capacità dello storage per il test
Istanza di Azure per il calcolo	B4ms standard (4 vcpus, 16 GB di memoria GiB)	Due istanze implementate, una come server DB primario e l'altra come server DB clone

#### Software

RedHat Linux	Red Hat Enterprise Linux 8,7 (LVM) - x64 Gen2	Implementazione dell'abbonamento a RedHat per il 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 l'implementazione

- **Connettore da implementare nella stessa rete/subnet virtuale dei database e di Azure NetApp Files.** se possibile, il connettore deve essere distribuito nelle stesse reti virtuali e gruppi di risorse di Azure, consentendo la connettività allo storage Azure NetApp Files e alle istanze di elaborazione di Azure.
- **Un account utente Azure o un principio del servizio Active Directory creato nel portale Azure per SnapCenter Connector.** l'implementazione di un connettore BlueXP richiede autorizzazioni specifiche per creare e configurare una macchina virtuale e altre risorse di calcolo, per configurare il networking e ottenere l'accesso all'abbonamento ad Azure. Richiede inoltre autorizzazioni per creare successivamente ruoli e autorizzazioni per il funzionamento del connettore. Creare un ruolo personalizzato in Azure con autorizzazioni e assegnarlo all'account utente o al principio del servizio. Fai clic sul link seguente per ulteriori informazioni: ["Impostare le autorizzazioni Azure"](#).
- **Una coppia di chiavi ssh creata nel gruppo di risorse Azure.** la coppia di chiavi ssh è assegnata all'utente VM di Azure per accedere all'host del connettore e anche all'host VM del database per distribuire ed eseguire un plug-in. L'interfaccia utente della console BlueXP utilizza la chiave ssh per implementare il plug-in di servizio SnapCenter nell'host del database, per l'installazione di un plug-in in un solo passaggio e il rilevamento del database dell'host dell'applicazione.

- **Una credenziale aggiunta all'impostazione della console BlueXP.** per aggiungere storage Azure NetApp Files all'ambiente di lavoro BlueXP, è necessario configurare una credenziale che concede autorizzazioni per accedere a Azure NetApp Files dalla console BlueXP nell'impostazione della console BlueXP.
- **java-11-openjdk installato sull'host di istanza del database di Azure VM.** l'installazione del servizio SnapCenter richiede java versione 11. Deve essere installato sull'host dell'applicazione prima di tentare la distribuzione del plugin.

## Implementazione della soluzione

È disponibile un'ampia documentazione NetApp con un ambito più ampio per aiutarti a proteggere i dati delle applicazioni native del cloud. L'obiettivo di questa documentazione è fornire procedure dettagliate per l'implementazione del servizio SnapCenter con console BlueXP per proteggere il database Oracle implementato su storage Azure NetApp Files e un'istanza di calcolo Azure.

Per iniziare, attenersi alla seguente procedura:

- Leggere le istruzioni generali ["Proteggi i dati delle tue applicazioni native nel cloud"](#) E le sezioni relative a Oracle e Azure NetApp Files.
- Guardare la seguente procedura dettagliata sul video

[Video sulla distribuzione di Oracle e ANF](#)

## Prerequisiti per l'implementazione del servizio SnapCenter

L'implementazione richiede i seguenti prerequisiti.

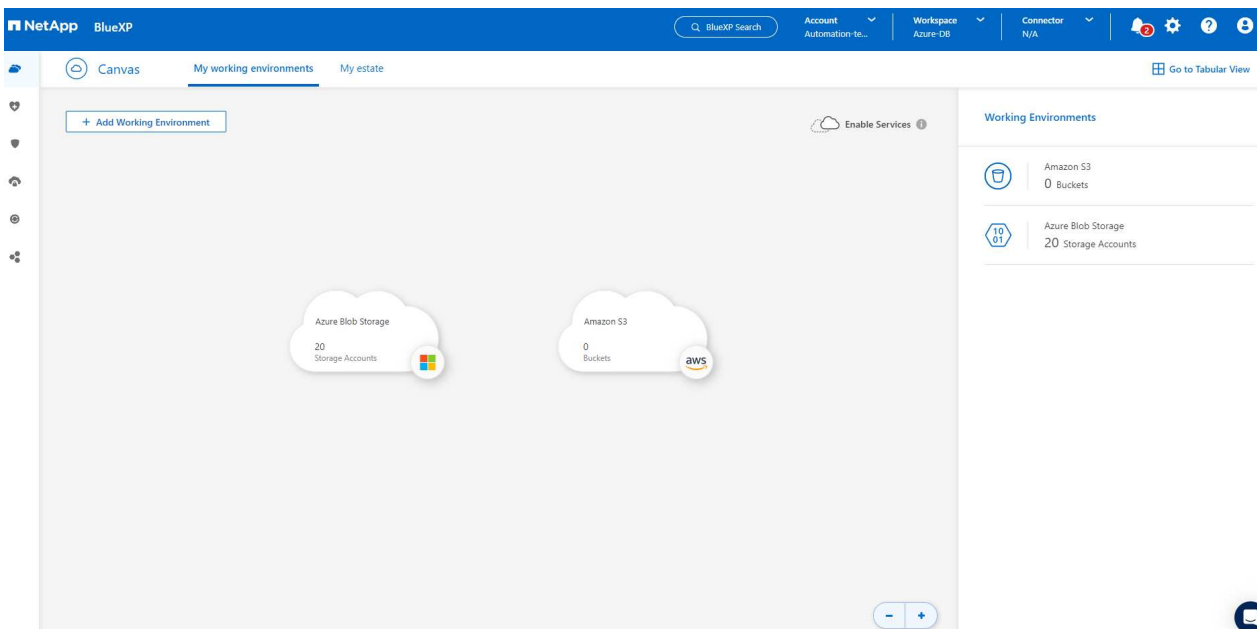
1. Un server di database Oracle primario su un'istanza di Azure VM con un database Oracle completamente implementato e in esecuzione.
2. Un pool di capacità dei servizi di storage Azure NetApp Files implementato in Azure che ha capacità per soddisfare le esigenze di storage per il database elencate nella sezione dei componenti hardware.
3. Un server di database secondario su un'istanza di macchina virtuale Azure che può essere utilizzato per testare il cloning di un database Oracle su un host alternativo al fine di supportare un carico di lavoro di sviluppo/test o casi d'utilizzo che richiedono un set di dati completo di database Oracle in produzione.
4. Per ulteriori informazioni sull'implementazione dei database Oracle su un'istanza di calcolo Azure NetApp Files e Azure, vedere ["Implementazione e protezione di database Oracle su Azure NetApp Files"](#).

## Preparazione al BlueXP

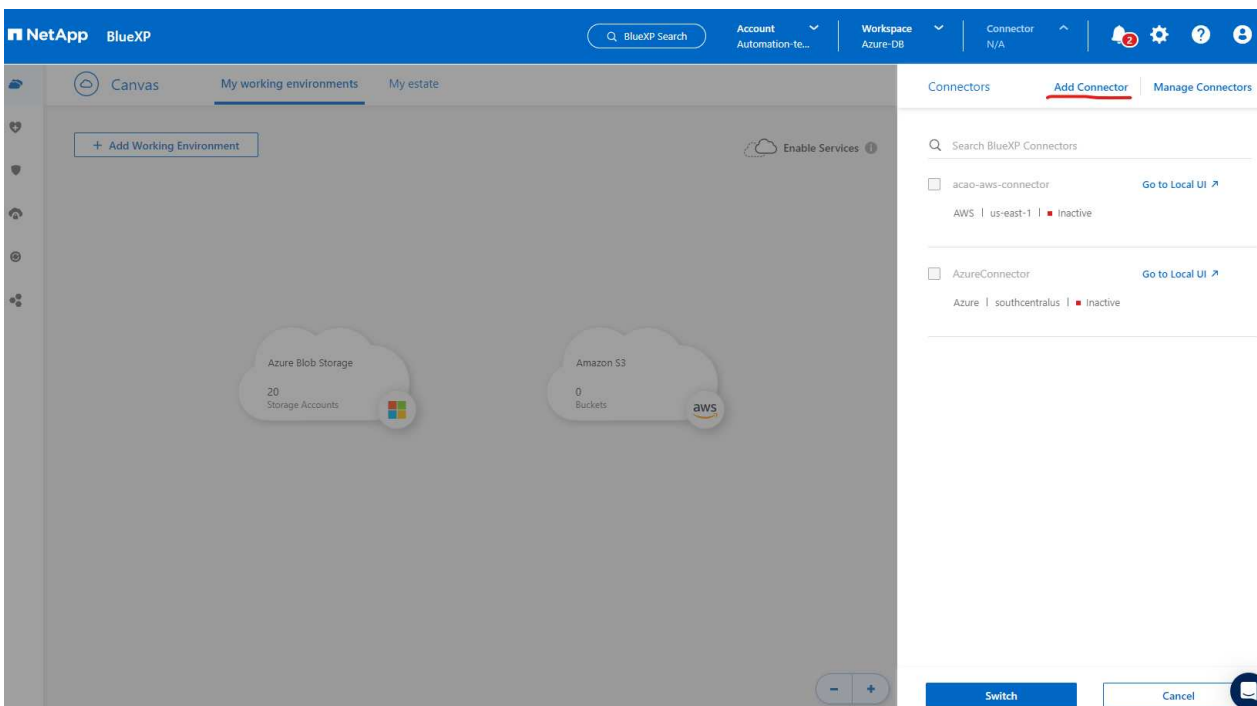
1. Utilizzare il link "[NetApp BlueXP](#)" Per iscriversi all'accesso alla console BlueXP.
2. Creare un account utente Azure o un principio di servizio Active Directory e concedere autorizzazioni con ruolo nel portale Azure per la distribuzione di Azure Connector.
3. Per configurare BlueXP per gestire le risorse Azure, aggiungere una credenziale BlueXP con i dettagli di un'identità di servizio Active Directory che BlueXP può utilizzare per autenticarsi con Azure Active Directory (ID client app), un segreto client per l'applicazione principale del servizio (Segreto client), e l'ID Active Directory dell'organizzazione (ID tenant).
4. Sono inoltre necessari la rete virtuale Azure, il gruppo di risorse, il gruppo di sicurezza, una chiave SSH per l'accesso alla VM, ecc. pronti per il provisioning dei connettori e l'installazione dei plug-in del database.

## **Implementare un connettore per i servizi SnapCenter**

1. Accedi alla console BlueXP.



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



3. Scegli il tuo cloud provider (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. Saltare i passaggi **Permission**, **Authentication** e **Networking** se sono già stati configurati nell'account Azure. In caso contrario, è necessario configurarli prima di procedere. Da qui, è anche possibile recuperare le autorizzazioni per la policy di Azure a cui si fa riferimento nella sezione precedente "[Preparazione al 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 **Salta a distribuzione** per configurare il connettore **autenticazione macchina virtuale**. Aggiungi la coppia di chiavi SSH che hai creato nel gruppo di risorse Azure durante l'onboarding alla preparazione BlueXP per l'autenticazione del sistema operativo del connettore.

Add BlueXP Connector - Azure

More Information

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

53

Add BlueXP Connector - Azure

More Information

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 **VNET**, **Subnet** e disattivare **Public IP**, ma assicurarsi che il connettore disponga dell'accesso a Internet nell'ambiente Azure.

Add BlueXP Connector - Azure

More Information

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 at the top indicates the following steps: VM Authentication, Details, Network, Security Group (current), and Review. A 'More Information' link and a close icon are also present. The main heading is 'Security Group'. Below it, a note states: 'The security group must allow inbound HTTP, HTTPS and SSH access.' A section titled 'Assign a security group:' contains two radio buttons: 'Create a new security group' (selected) and 'Select an existing security group'. Below this, there are three columns for configuring inbound rules for HTTP, HTTPS, and SSH. Each column 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, and a help icon in the bottom right corner.

**Add BlueXP Connector - Azure** More Information ×

✓ VM Authentication ✓ 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

HTTP (Port 80)	HTTPS (Port 443)	SSH (Port 22)
Source Type: <input type="text" value="Anywhere"/>	Source Type: <input type="text" value="Anywhere"/>	Source Type: <input type="text" value="Anywhere"/>
Source (CIDR): <input type="text" value="0.0.0.0/0"/>	Source (CIDR): <input type="text" value="0.0.0.0/0"/>	Source (CIDR): <input type="text" value="0.0.0.0/0"/>

Previous Next ?

9. Esaminare la pagina di riepilogo e fare clic su **Aggiungi** per avviare la creazione del connettore. In genere occorrono circa 10 minuti per completare l'implementazione. Una volta completata l'operazione, la VM di istanza del connettore viene visualizzata nel portale di Azure.

Add BlueXP Connector - Azure

More Information

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	ANFAVSub
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 l'attivazione del connettore, il connettore appena creato viene visualizzato nell'elenco a discesa **connettore**.

NetApp BlueXP

BlueXP Search

Account Automation-to...

Workspace Azure-DB

Connector AzureConnector

2

Settings

Help

User

Canvas

My working environments

My estate

+ Add Working Environment

Enable Services

Azure Blob Storage  
20 Storage Accounts

Amazon S3  
0 Buckets

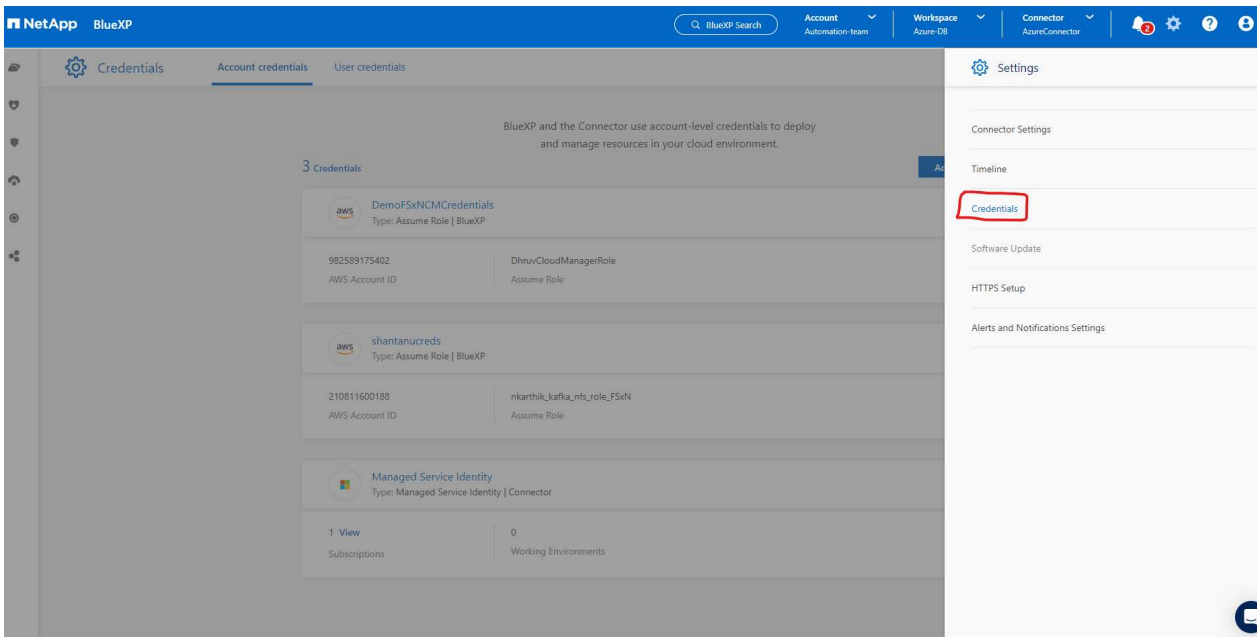
Working Environments

Amazon S3  
0 Buckets

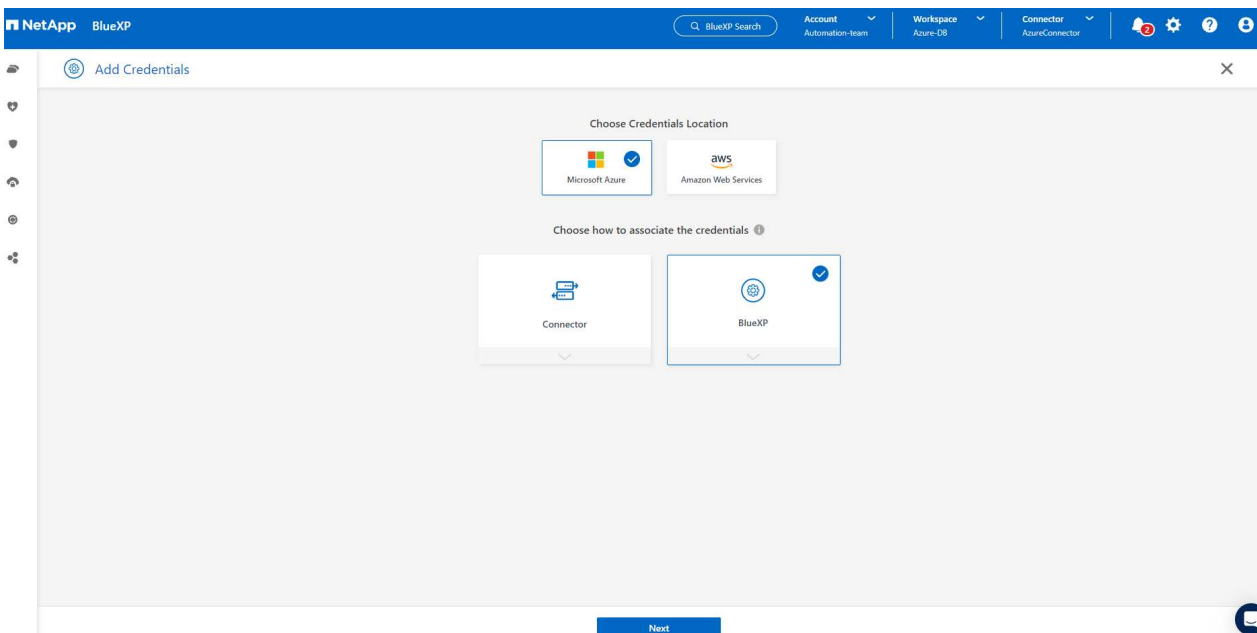
Azure Blob Storage  
20 Storage Accounts

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

1. Fare clic sull'icona delle impostazioni nell'angolo superiore destro della console BlueXP per aprire la pagina **credenziali account**, fare clic su **Aggiungi credenziali** per avviare il flusso di lavoro di configurazione delle credenziali.



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



3. Definisci le credenziali di Azure con **Client Secret**, **Client ID** e **Tenant ID** appropriati, che dovrebbero essere state raccolte durante il precedente processo di onboarding di BlueXP.



**NetApp BlueXP** Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector 2 ? !

**Add Credentials** 1 Credentials Type 2 Define Credentials 3 Marketplace Subscription 4 Review X

**Define Microsoft Azure Credentials**  
Learn more about Azure application credentials

Credentials Name ? Client Secret

Azure\_Hybrid\_TME

Application (client) ID Directory (tenant) ID

2fbc9be5-a259-4539-bb57-036b176f5cc7 9bb0aab6-5c98-419b-9cfd-7a38bd496...

☒ 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** Q BlueXP Search Account Automation-team Workspace Azure-DB Connector AzureConnector 2 ? !

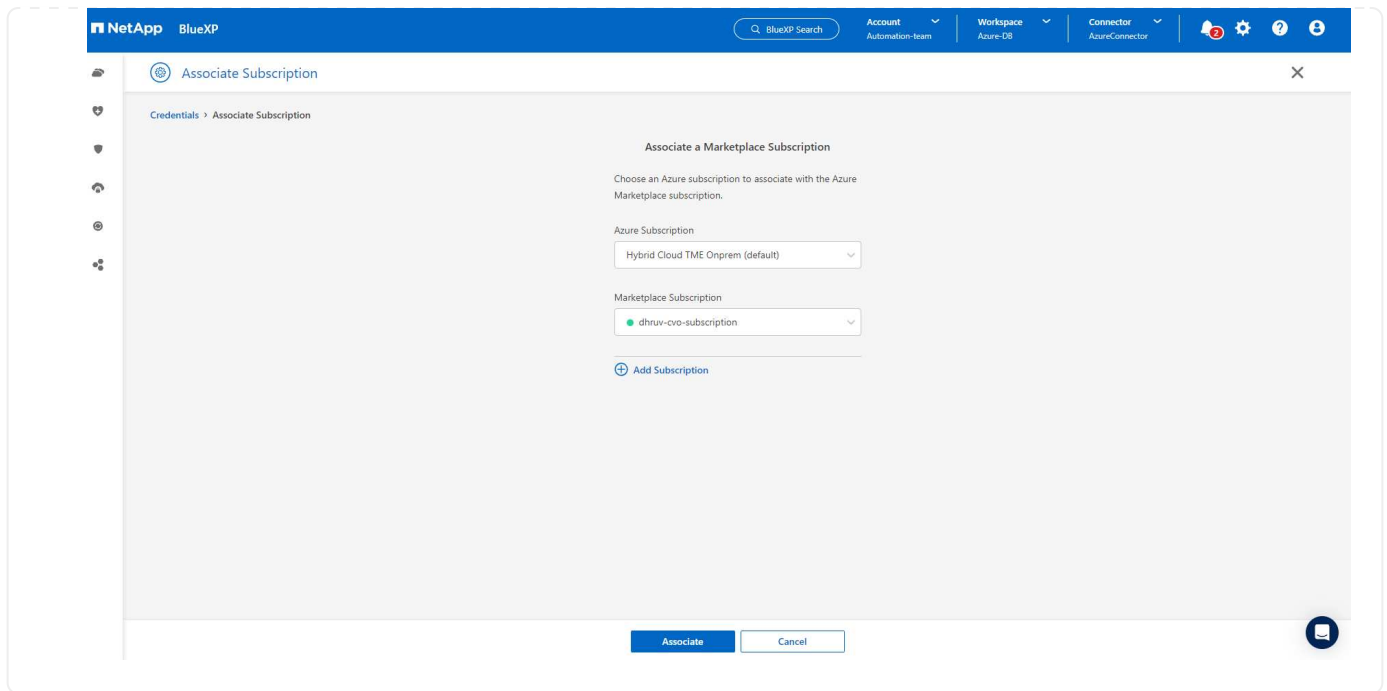
**Add Credentials** 1 Credentials Type 2 Define Credentials 3 Review X

**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 !

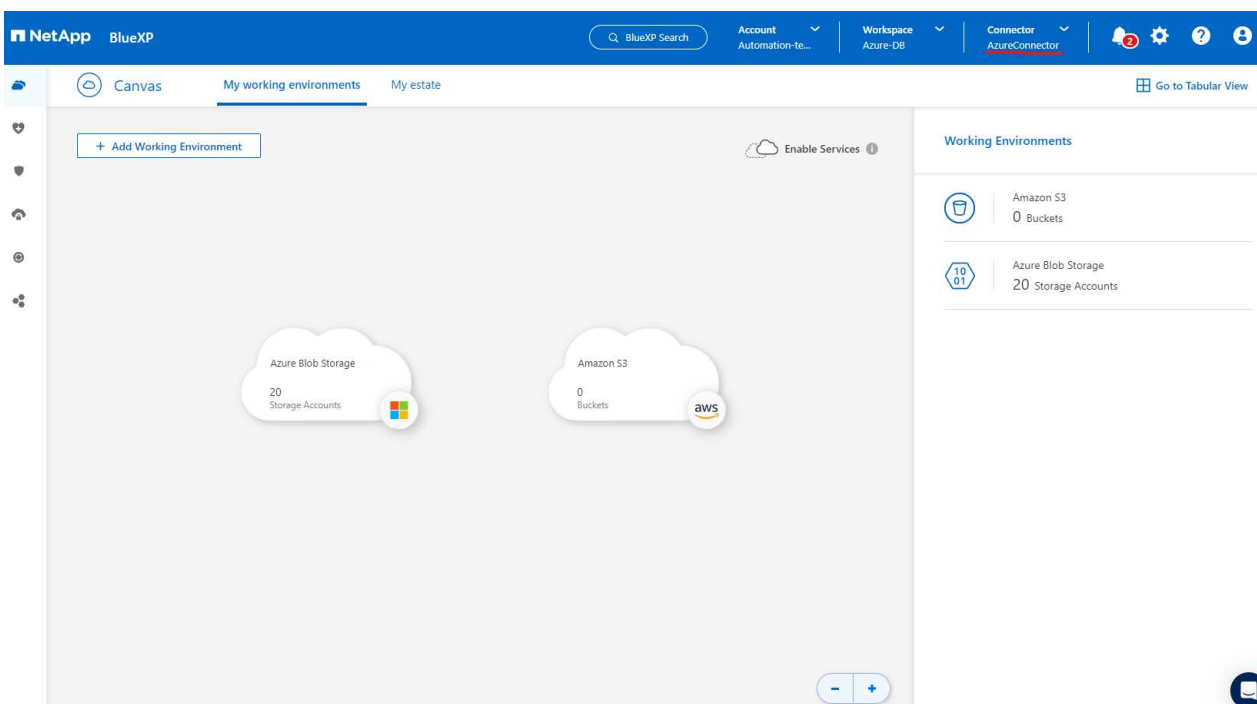
5. Potrebbe inoltre essere necessario associare un abbonamento **Marketplace** alla credenziale.



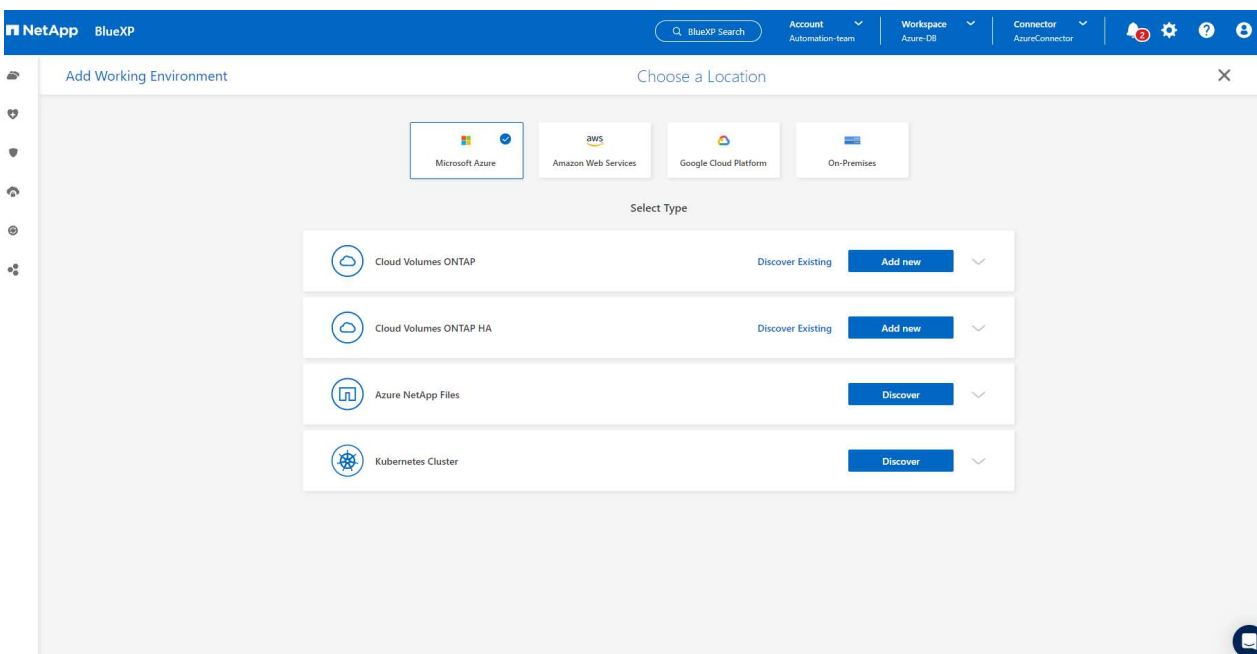
## Configurazione dei servizi SnapCenter

Con la credenziale Azure configurata, i servizi SnapCenter possono ora essere configurati con le seguenti procedure:

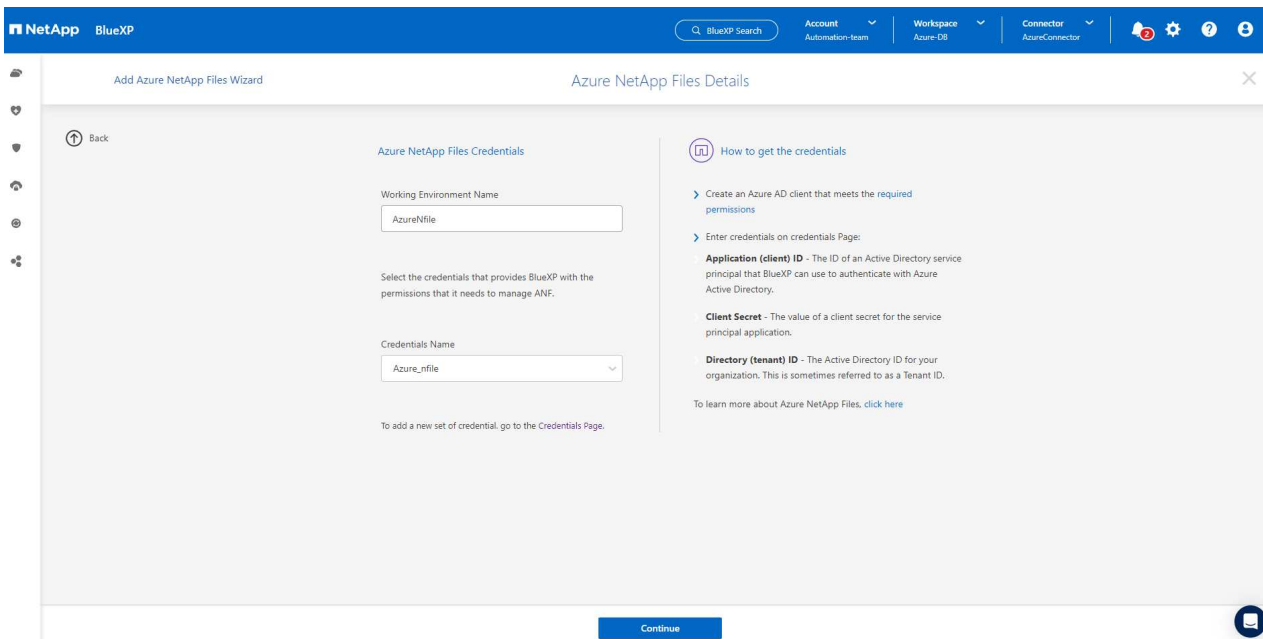
1. Torna alla pagina Canvas, da **ambiente di lavoro** fare clic su **Aggiungi ambiente di lavoro** per scoprire Azure NetApp Files distribuito in Azure.



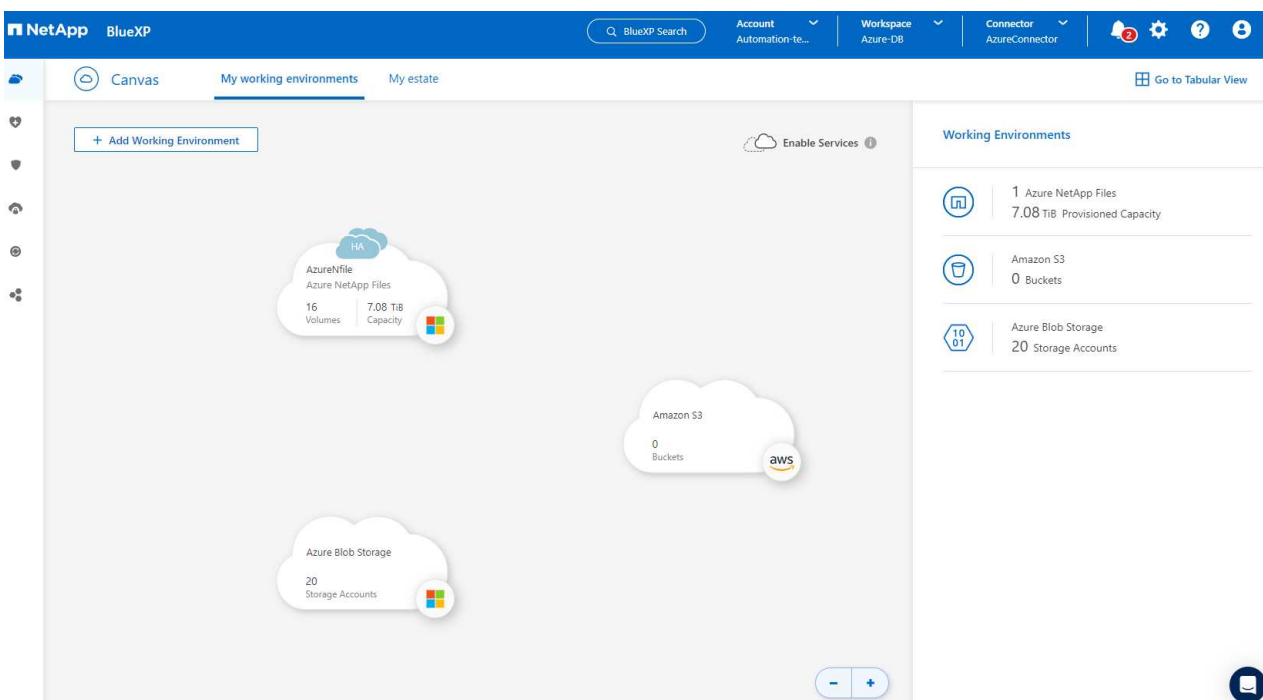
2. Scegliere **Microsoft Azure** come percorso e fare clic su **Scopri**.



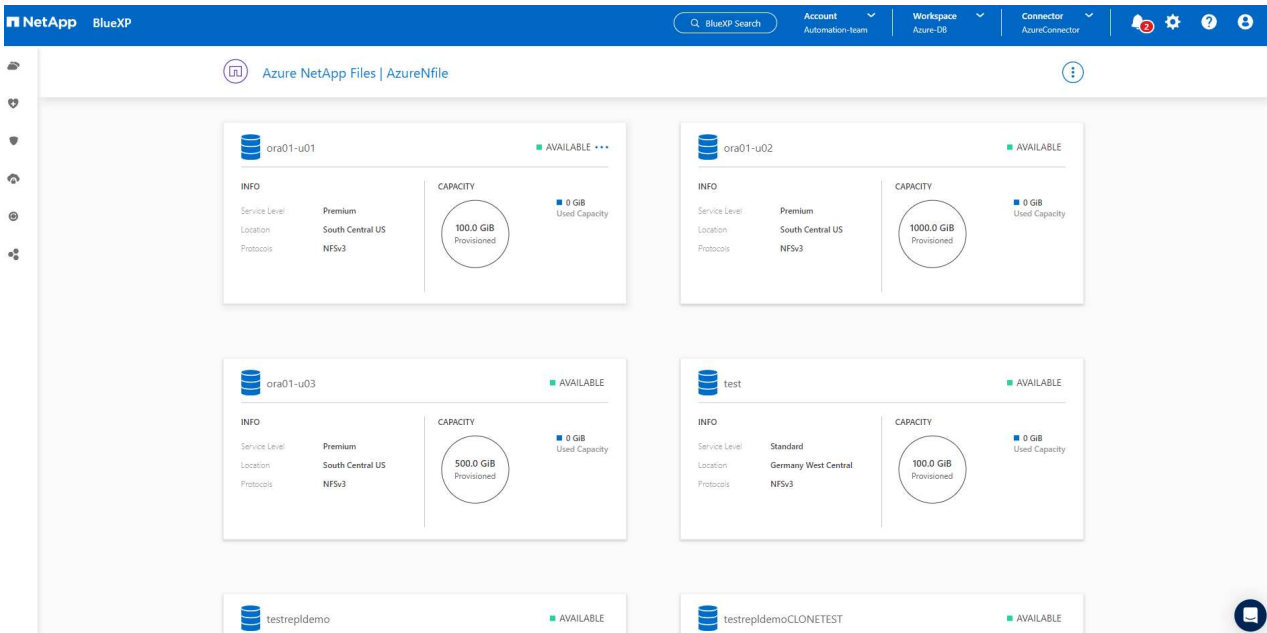
3. Nome **ambiente di lavoro** e scegliere **Nome credenziale** creato nella sezione precedente, quindi fare clic su **continua**.



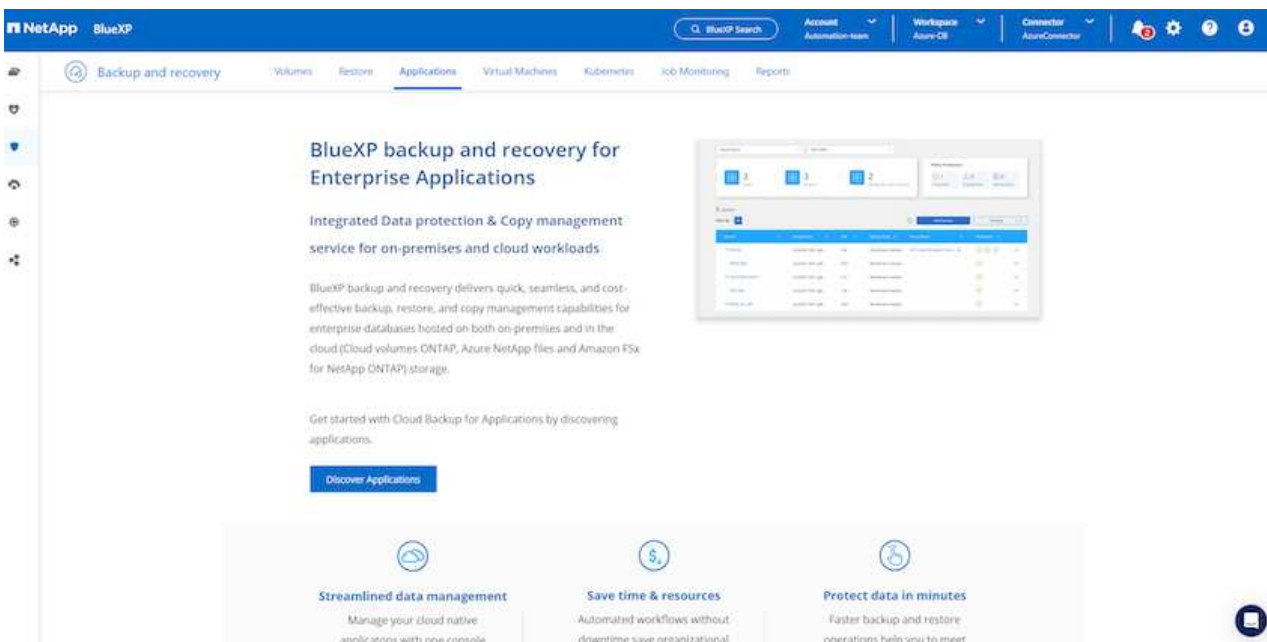
4. La console BlueXP torna a **i miei ambienti di lavoro** e Azure NetApp Files rilevato da Azure ora appare su **Canvas**.



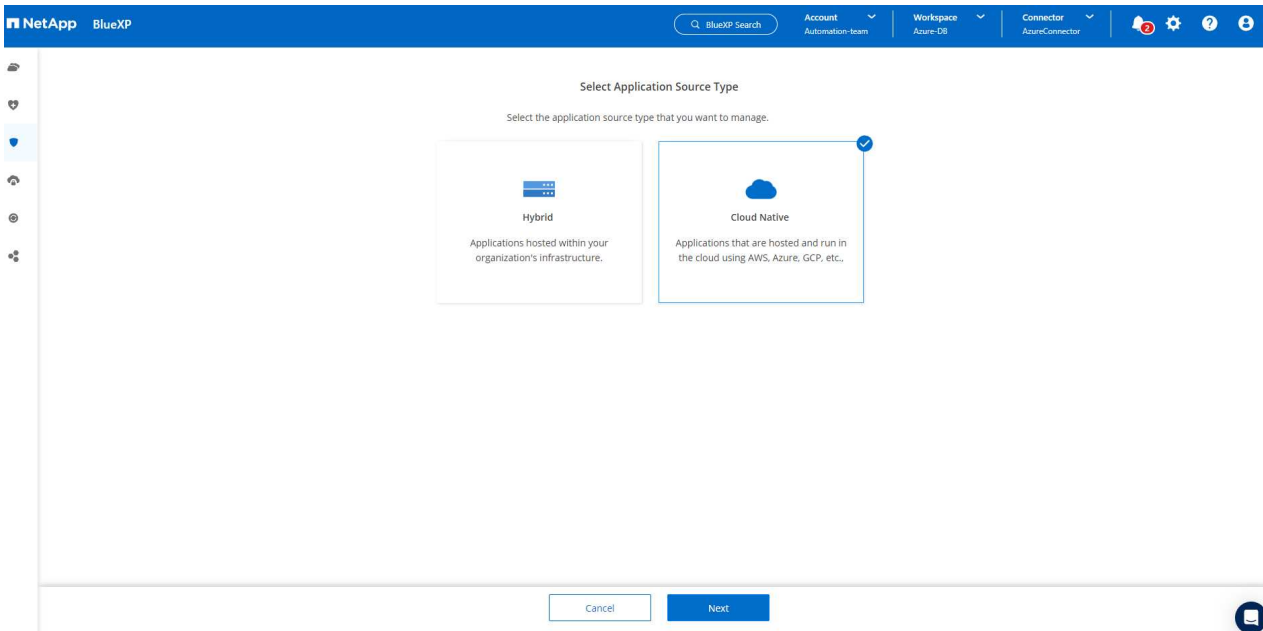
5. Fare clic sull'icona **Azure NetApp Files**, quindi **Inserisci ambiente di lavoro** per visualizzare i volumi di database Oracle distribuiti nello storage Azure NetApp Files.



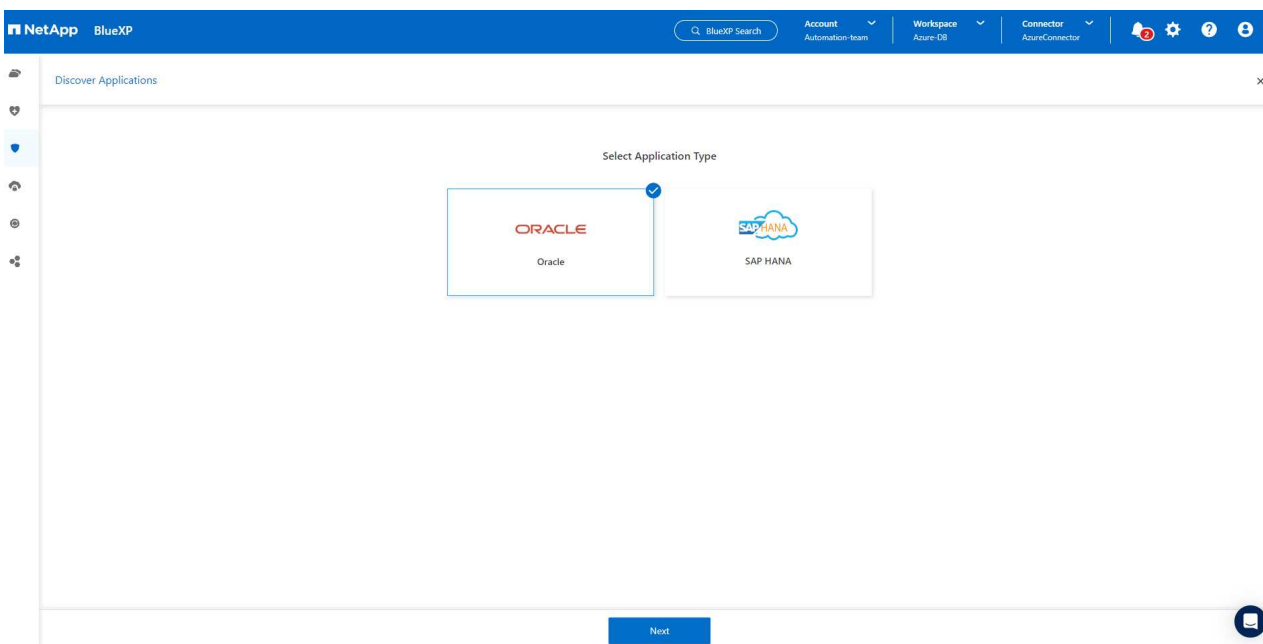
6. Dalla barra laterale sinistra della console, passare il mouse sull'icona di protezione, quindi fare clic su **protezione > applicazioni** per aprire la pagina di avvio delle applicazioni. Fare clic su **Scopri applicazioni**.



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



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



9. Selezionare **usando SSH** e fornire i dettagli di Oracle Azure VM come **indirizzo IP**, **connettore**, gestione di Azure VM **Nome utente** come azureuser. Fare clic su **Aggiungi chiave privata SSH** per incollare la coppia di chiavi SSH utilizzata per implementare la VM Oracle Azure. Verrà inoltre richiesto di confermare l'impronta digitale.

NetApp BlueXP

Discover Applications

1 Host Details 2 Configuration 3 Review

Select host type

Provide the following details to add host and discover applications

Host Installation Type ☐ Manual ☒ Using SSH

Host FQDN or IP 172.30.137.142 Connector AzureConnector

Username azureuser Add SSH Private Key Optional

SSH Port 22 Plug-in Port 8145

Previous Next

Discover Applications

1 Host Details 2 Configuration 3 Review

Select host type

Provide the following details to add host and discover applications

Host Installation Type ☐ Manual ☒ Using SSH

Validate fingerprint

Algorithm ssh-rsa

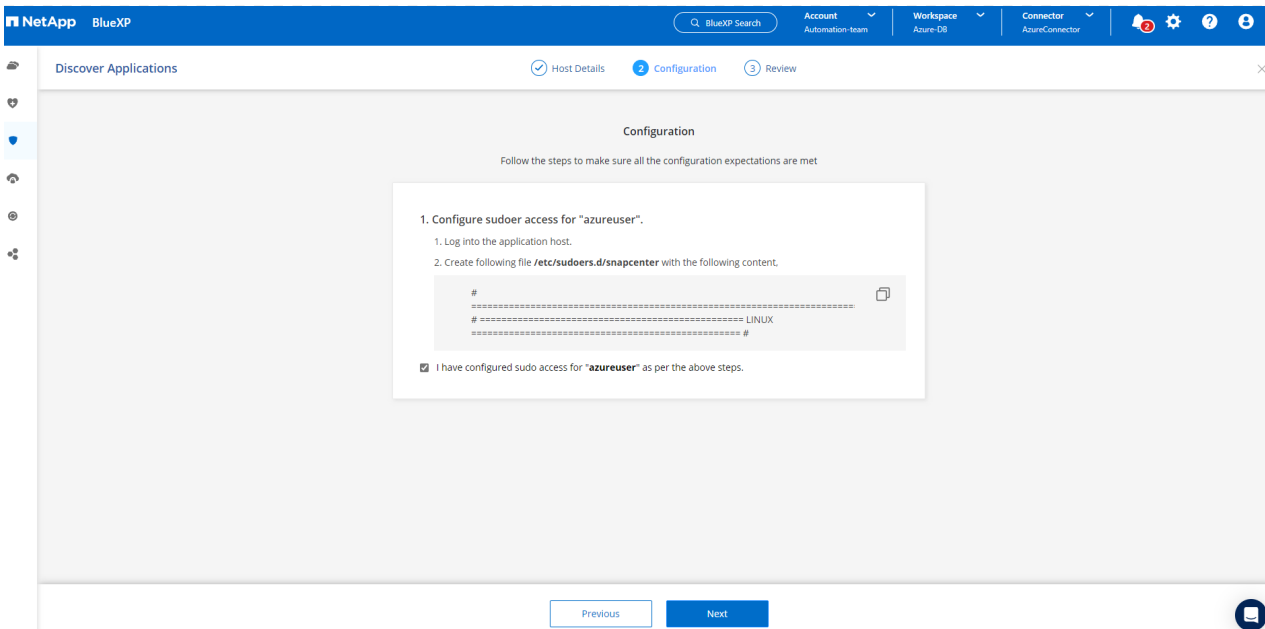
Fingerprint AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIbmlzdHAyNTYAAAB...

☒ By proceeding further, I confirm that the above fingerprint for host is valid.

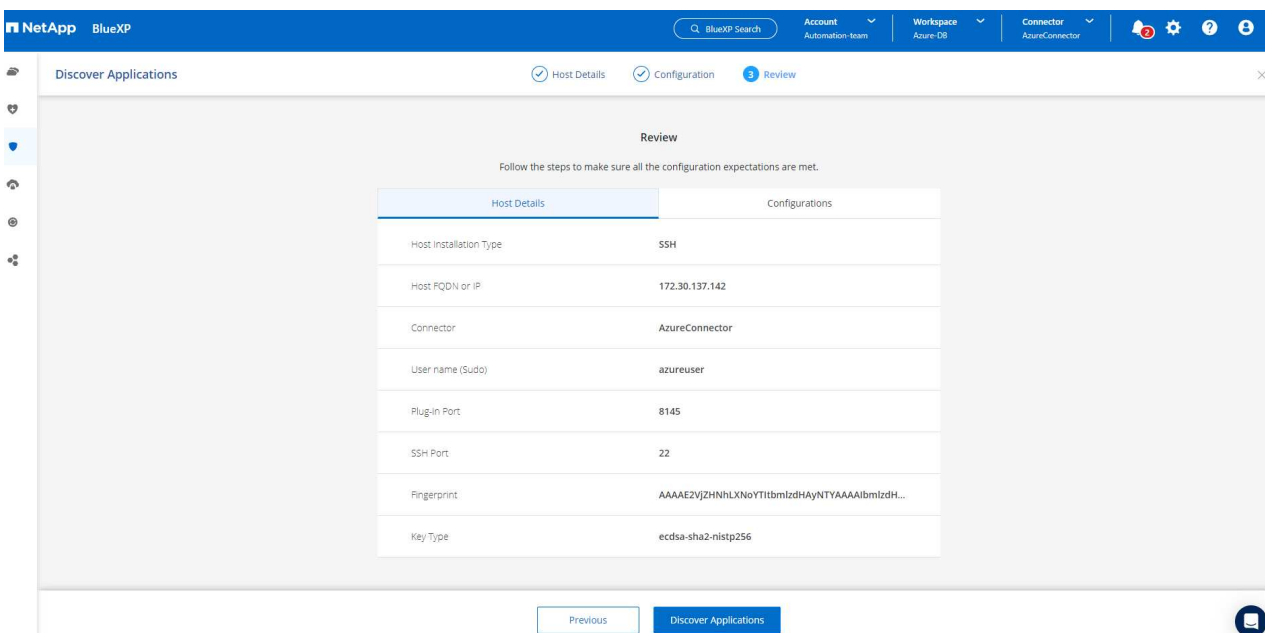
Proceed Cancel

Previous Next

10. Passare alla pagina successiva **Configurazione** per impostare l'accesso sudocer su Oracle Azure VM.



11. Rivedere e fare clic su **Scopri applicazioni** per installare un plug-in su Oracle Azure VM e scoprire il database Oracle sulla VM in un'unica fase.



12. I database Oracle rilevati su Azure VM vengono aggiunti a **applicazioni**, mentre la pagina **applicazioni** elenca il numero di host e di database Oracle all'interno dell'ambiente. Il database **Stato di protezione** viene inizialmente visualizzato come **non protetto**.



NetAppBlueXP

Q BlueXP SearchAccount Automation-te...Workspace Azure-DBConnector AzureConnector

Backup and recoveryVolumesRestoreApplicationsVirtual MachinesKubernetesJob MonitoringReports

Cloud NativeOracle

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<<<1>>>

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

### Backup del database Oracle

1. Il nostro database Oracle di test in Azure VM è configurato con tre volumi con uno storage totale aggregato di circa 1,6 TiB. Questo fornisce un contesto in cui vengono descritte le tempistiche per il backup, il ripristino e il clone 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 al database **Stato protezione**, quindi fare clic su **Assegna criterio** per visualizzare i criteri di protezione predefiniti predefiniti o definiti dall'utente che possono essere applicati ai database Oracle. In **Impostazioni - Criteri**, è possibile creare criteri personalizzati con una frequenza di backup personalizzata e una finestra di conservazione dei dati di backup.

The screenshot shows the NetApp BlueXP interface. At the top, there's a navigation bar with 'Backup and recovery', 'Volumes', 'Restore', 'Applications' (selected), 'Virtual Machines', 'Kubernetes', 'Job Monitoring', and 'Reports'. Below this, there are filters for 'Cloud Native' and 'Oracle'. A summary section shows '4 Hosts', '3 ORACLE', and '0 Clone'. An 'Application Protection' box indicates '0 Protected' and '3 Unprotected' databases. Below this, a table lists databases with their protection status. A dropdown menu for the 'NTAP' database shows the 'Assign Policy' option 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

- Quando si è soddisfatti della configurazione dei criteri, è possibile **assegnare** il criterio scelto per proteggere il database.

The screenshot shows the 'Assign Policy' dialog in the NetApp BlueXP interface. The title is 'Assign Policy' with a subtitle 'Assign a policy to start taking backups of the database "NTAP"'. Below this, there's a table with 4 policies. The 'my\_full\_bkup' policy is selected with a checkmark. At the bottom, there are 'Cancel' and 'Assign' buttons.

Policy Name	Backup Type	Schedules
<input type="radio"/> 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
<input type="radio"/> 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
<input type="radio"/> 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
<input checked="" type="radio"/> my_full_bkup	FullBackup	Hourly: Repeats Every 6 Hrs, Keeps 3 Days

- Una volta applicato il criterio, lo stato di protezione del database è cambiato in **Protected** con un segno di spunta verde. BlueXP esegue il backup snapshot in base al programma definito. Inoltre, **Backup SU richiesta** è disponibile dal menu a discesa a tre punti, come mostrato di seguito.

The screenshot shows the NetApp BlueXP interface with the 'Applications' tab selected. At the top, there are filters for 'Cloud Native' and 'Oracle'. Below these, there are three summary cards: '3 Hosts', '3 ORACLE', and '0 Clone'. To the right, an 'Application Protection' summary shows '1 Protected' and '2 Unprotected' databases. The main section is titled '3 Databases' and includes a 'Filter By' button and a search bar. A table lists the databases:

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

A context menu is open for the 'NTAP' database, showing options: 'View Details', 'On-Demand Backup' (highlighted), 'Assign Policy', 'Un-assign Policy', and 'Restore'.

4. Dalla scheda **Job Monitoring** è possibile visualizzare i dettagli del processo di backup. I risultati del test hanno dimostrato che il backup di un database Oracle ha richiesto circa 4 minuti e circa 1,6 TiB.

The screenshot shows the NetApp BlueXP 'Job Monitoring' page. The breadcrumb trail is 'Job Monitoring > Job Name: Backup of NTAP oracle database on host 172.30.137.142 with policy my\_full\_bkup and schedule Hourly'. The job name is displayed as 'Job Name: Backup of NTAP oracle database on host 172.30.137.142 with policy my\_full\_bkup and schedule H...' with a job ID '61a12139-330e-4390-bca8-e7d15680869c'. Below this, a summary bar shows: 'Other Job Type', 'Jul 11 2023, 2:17:53 pm Start Time', 'Jul 11 2023, 2:21:38 pm End Time', and 'Success Job Status'. The 'Sub-Jobs(17)' section is expanded, showing a table of sub-jobs:

Job Name	Job ID	Start Time	End Time	Duration
Backup of NTAP oracle database on host 172.30...	61a12139-330e-4390-bc...	Jul 11 2023, 2:17:53 pm	Jul 11 2023, 2:21:38 pm	4 Minutes
Applying Retention	27ff9d5f-68f0-4880-a48...	Jul 11 2023, 2:21:38 pm	Jul 11 2023, 2:21:38 pm	0 Second
Performing cleanup after backup	074c0689-097e-41aa-ac...	Jul 11 2023, 2:21:36 pm	Jul 11 2023, 2:21:38 pm	2 Seconds
Finalizing Oracle database log backup	348189d3-90b5-4cce-97...	Jul 11 2023, 2:21:36 pm	Jul 11 2023, 2:21:36 pm	0 Second

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

NetApp BlueXP

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

Cloud Native Oracle

4 Hosts 3 ORACLE 0 Clone

Application Protection 2 Protected 1 Unprotected

3 Databases

Filter By +

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

Manage Databases Settings

View Details On-Demand Backup Assign Policy Un-assign Policy Restore

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

NetApp BlueXP

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

Applications > Database Details

Database Details

NTAP Database Name	Protected Protection	my_full_bkup Policy Names	Database Type
172.30.137.142 Host Name	ANF Host Storage	Unreachable Database Version	zEHlu7vkdya8nujcxllbkKELKvXTToyNcllents Connector Id
- Clones	- Parent Database	Disabled RMAN Catalog	- RMAN catalog repository

14 Backups

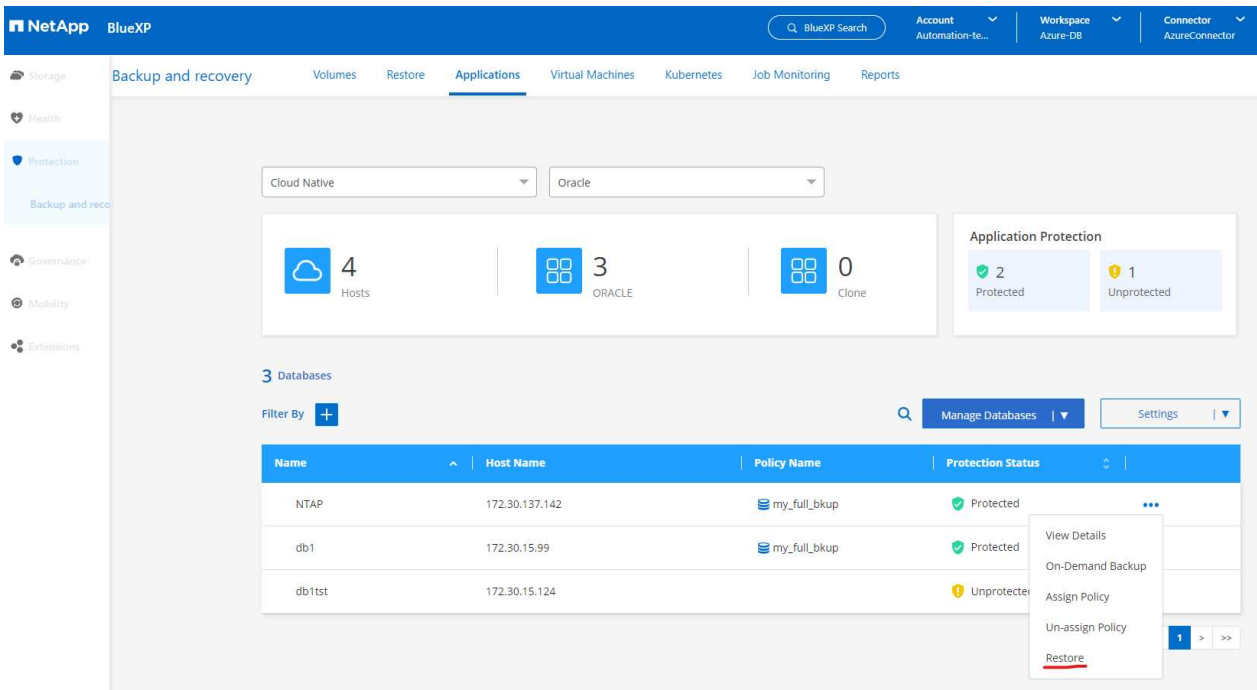
Filter By +

Select Timeframe

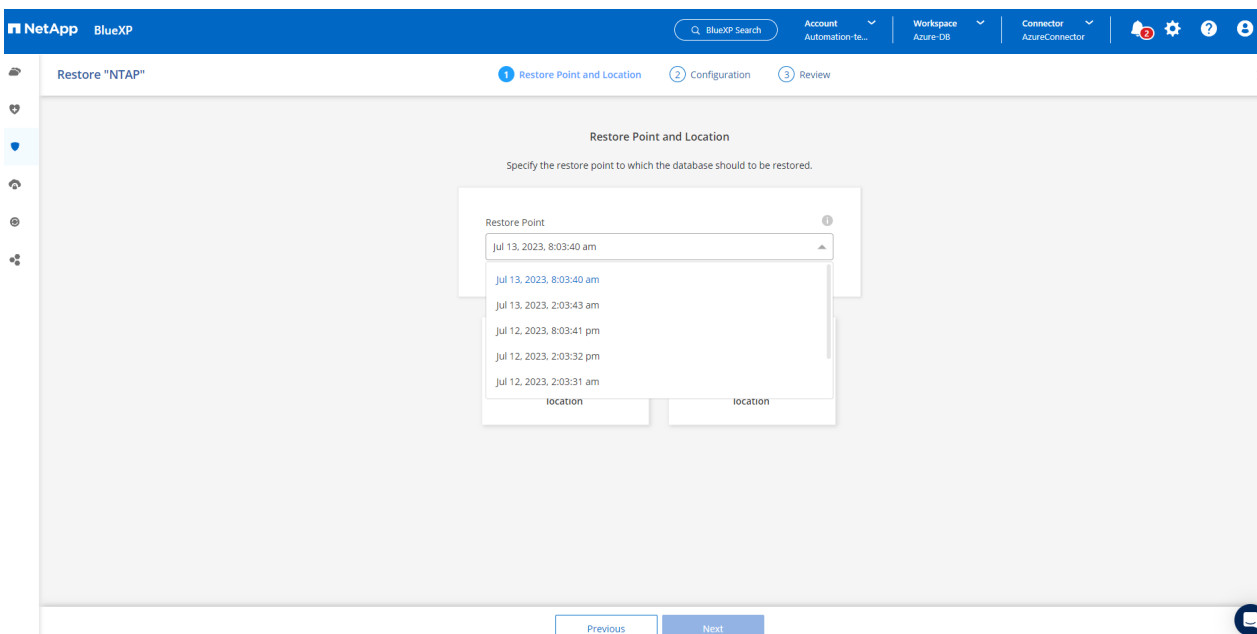
Backup Name	Backup Type	SCN	RMAN Catalog	Backup Time	
my_full_bkup_Hourly_NTAP_2023_07_13_12_04_28_8376...	Log	29192187	Not Cataloged	Jul 13, 2023, 8:06:22 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_4363...	Data	29192136	Not Cataloged	Jul 13, 2023, 8:03:40 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_04_28_5618...	Log	29178022	Not Cataloged	Jul 13, 2023, 2:05:50 am	Delete
my_full_bkup_Hourly_NTAP_2023_07_13_06_03_03_6371...	Data	29177972	Not Cataloged	Jul 13, 2023, 2:03:43 am	Delete

## Ripristino e ripristino del database Oracle

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



2. Scegliere il **punto di ripristino** in base all'indicazione dell'ora. Ogni indicatore orario nell'elenco rappresenta un set di backup del database disponibile.



3. Scegliere **Restore Location** to **Original Location** (posizione di ripristino\* in **posizione originale**) per il ripristino e il ripristino di un database Oracle.

NetApp BlueXP

Restore "NTAP"

1 Restore Point and Location 2 Configuration 3 Review

Restore Point and Location

Specify the restore point to which the database should be restored.

Restore Point  
Jul 13, 2023, 8:03:40 am

Restore to original location

Restore to alternate location

Previous Next

4. Definire **ambito di ripristino** e **ambito di ripristino**. Tutti i registri indicano un ripristino completo aggiornato, inclusi i registri correnti.

NetApp BlueXP

Restore "NTAP"

Restore Point and Location 2 Configuration 3 Review

Restore Scope

☒ All Data Files  
Data Files Restore

☐ Control Files  
Control Files Restore

Database state will be changed if needed for restore and recovery.

Recovery Scope

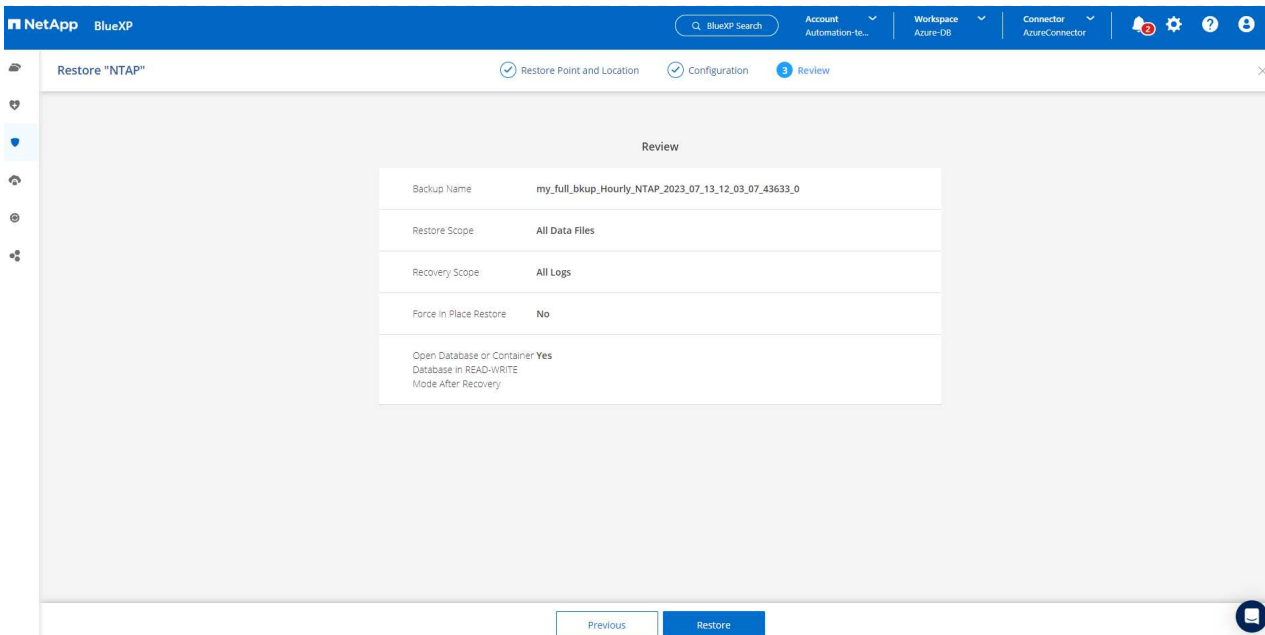
☒ All Logs ☐ Until System Change Number ☐ Date and Time ☐ No Recovery

External Archive log locations

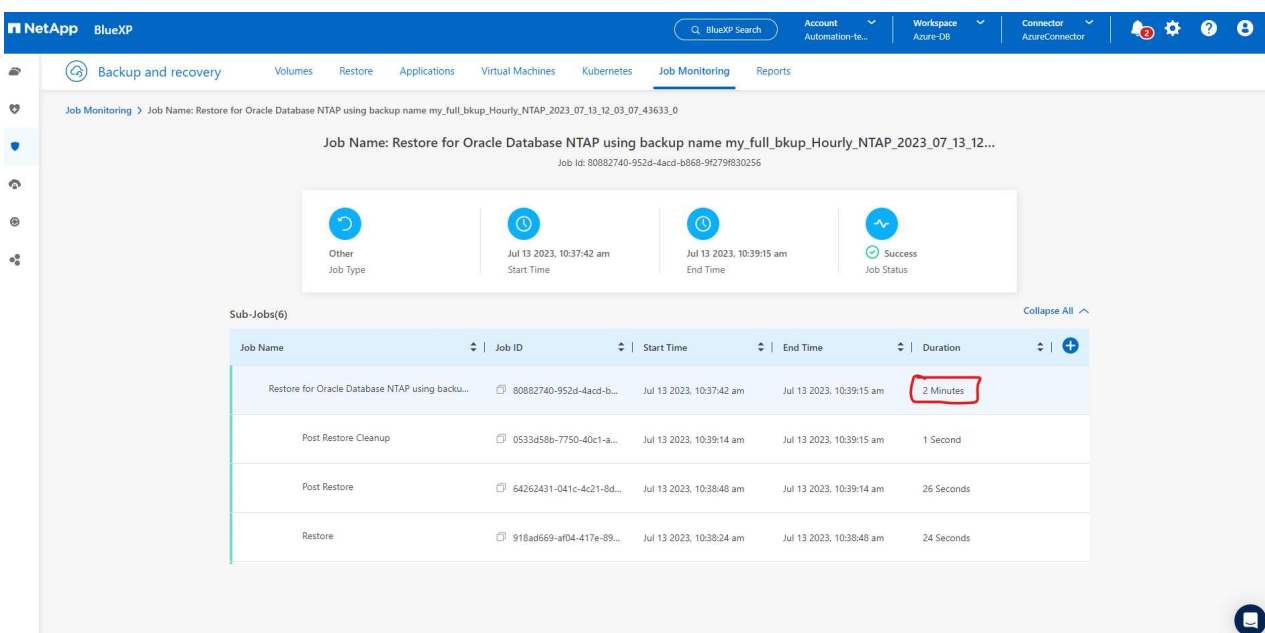
☒ Open the database or the container database in READ-WRITE mode after recovery.

Previous Next

5. Rivedere e **Restore** per avviare il ripristino e il ripristino del database.



6. Dalla scheda **Job Monitoring**, abbiamo osservato che sono stati necessari 2 minuti per eseguire un ripristino completo del database e un ripristino aggiornato.



## Clone del database Oracle



Le procedure di clone del database sono simili al ripristino, ma a una VM Azure alternativa con stack software Oracle identico preinstallato e configurato.



Verificare che il sistema di storage file Azure NetApp disponga di capacità sufficiente per consentire a un database clonato di avere le stesse dimensioni del database primario da clonare. La VM alternativa di Azure è stata aggiunta alle **applicazioni**.

1. Fare clic sul menu a discesa a 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 left sidebar lists various categories like Storage, Health, Protection, Governance, Mobility, and Extensions. The main content area is titled 'Applications' and shows a summary of resources: 4 Cloud Native Hosts, 3 ORACLE, and 0 Clones. Below this, there's a section for '3 Databases' with a table listing them. A context menu is open for the 'db1tst' database, showing options like 'View Details', 'On-Demand Backup', 'Assign Policy', 'Un-assign Policy', and 'Restore' (which is highlighted).

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. Selezionare **Restore Point** e selezionare **Restore to Alternate Location**.

The screenshot shows the 'Restore "NTAP"' configuration page in NetApp BlueXP. The page has three steps: '1 Restore Point and Location', '2 Configuration', and '3 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 for 'Restore Point' shows 'Jul 13, 2023, 8:03:40 am'. Below this, there 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 successiva **Configurazione**, impostare alternativo **host**, nuovo database **SID** e **Oracle Home** come configurato in alternativa ad Azure VM.

The screenshot shows the 'Configuration' step in the 'Restore "NTAP"' workflow. The interface includes a top navigation bar with 'NetApp BlueXP', a search bar, and various account and workspace settings. The main content area is titled 'Configuration' and contains a form with the following fields:

- Host:** A dropdown menu showing '172.30.137.147'.
- SID:** A text input field containing 'NTAP1'.
- Oracle Home:** A text input field containing '/u01/app/oracle/product/19.0.0/clone'.
- Database Credentials:** A section labeled 'Optional' with an 'Add Credential' button.
- Maximum storage throughput (MiB/s):** A section labeled 'Optional' with a text input field containing 'Enter throughput (1-4500)'.

At the bottom of the form, there are 'Previous' and 'Next' buttons.

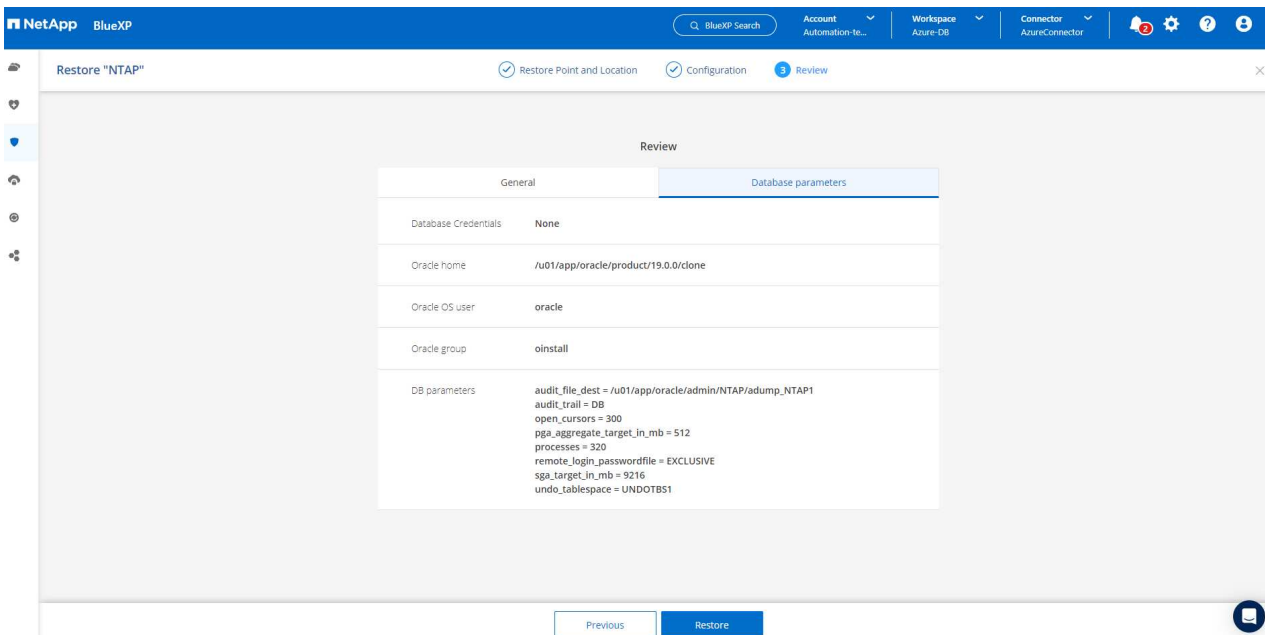
4. La pagina Review **General** (Revisione **Generale**) mostra i dettagli del database clonato, come SID, host alternativo, posizioni dei file di dati, ambito di ripristino e così via

The screenshot shows the 'Review' step in the 'Restore "NTAP"' workflow. The interface includes the same top navigation bar as the previous page. The main content area is titled 'Review' and contains a table with two tabs: 'General' and 'Database parameters'. The 'General' tab is selected, showing the following details:

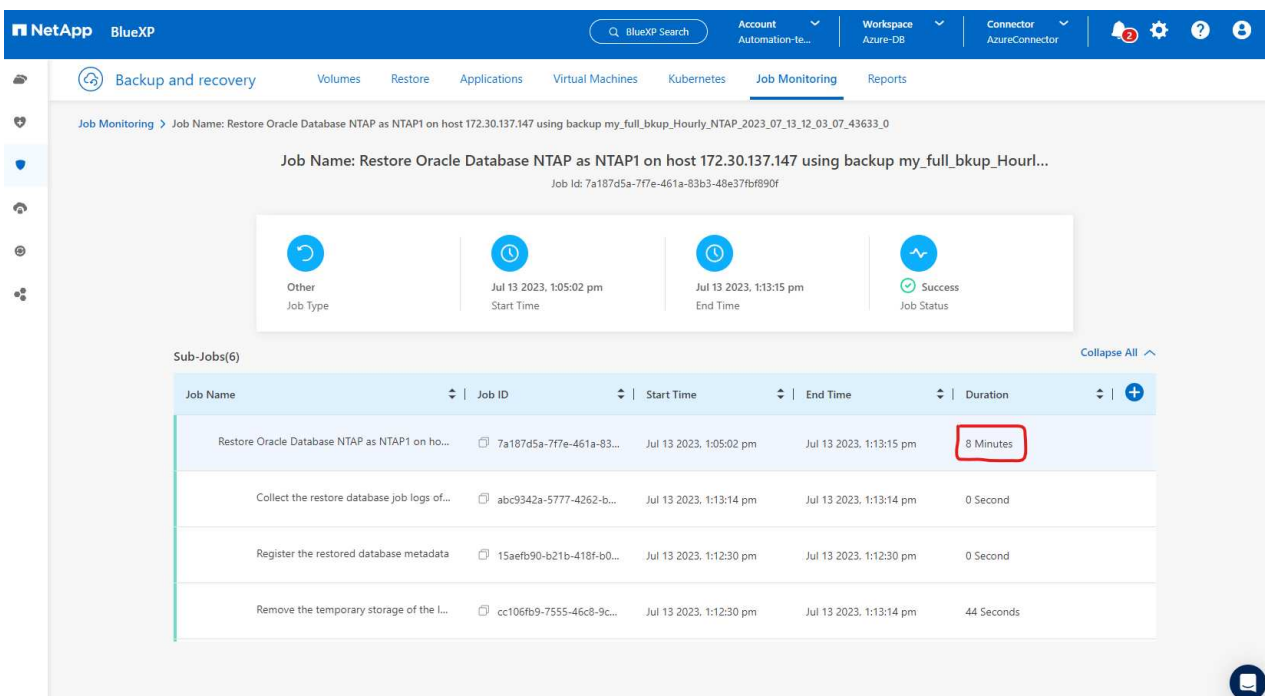
General	
Backup Name	my_full_bkup_Hourly_NTAP_2023_07_13_12_03_07_43633_0
SID	NTAP1
Host	172.30.137.147
Datafile locations	/u02_NTAP1
Control files	/u02_NTAP1/NTAP1/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = /u02_NTAP1/NTAP1/redolog/redo01_01.log RedoGroup = 2 TotalSize = 1024 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 of the table, there are 'Previous' and 'Restore' buttons.

5. Nella pagina Review **Database parameters** sono riportati i dettagli della configurazione clonata del database e alcune impostazioni dei parametri del database.



6. Monitorare lo stato del lavoro di clonazione dalla scheda **Job Monitoring**, abbiamo osservato che sono stati necessari 8 minuti per clonare un database Oracle 1,6 TiB.



7. Convalidare il database clonato nella pagina BlueXP **Applications** che indicava che il database clonato è stato registrato immediatamente con BlueXP.

NetApp
BlueXP

BlueXP Search
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 su Oracle Azure VM che indicava l'esecuzione del database clonato 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 $ORACLE_SID are not allowed.
#
#
# SnapCenter Plug-in for Oracle Database generated entry (DO NOT REMOVE THIS LINE)
NTAP1:/u01/app/oracle/product/19.0.0/clone:N
[oracle@acao-ora02 admin]$ 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

```

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

## Ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo 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 di backup e ripristino BlueXP

["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 subito con Azure

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

## TR-4964: Backup, ripristino e cloning del database Oracle con servizi SnapCenter - AWS

Allen Cao, Niyaz Mohamed, NetApp

### Scopo

I servizi SnapCenter sono la versione SaaS del classico tool di interfaccia utente per la gestione dei database SnapCenter disponibile tramite la console di gestione del cloud NetApp BlueXP. È parte integrante dell'offerta NetApp di cloud-backup e protezione dei dati per database come Oracle e HANA in esecuzione su cloud storage NetApp. Questo servizio basato su SaaS semplifica l'implementazione di un server standalone SnapCenter tradizionale, che in genere richiede un server Windows che opera in un ambiente di dominio Windows.

In questa documentazione, illustreremo come configurare i servizi SnapCenter per il backup, il ripristino e la clonazione dei database Oracle distribuiti su Amazon FSX per lo storage ONTAP e le istanze di calcolo EC2. Sebbene sia molto più semplice da configurare e utilizzare, i servizi SnapCenter offrono funzionalità chiave disponibili nel tool precedente dell'interfaccia utente di SnapCenter.

Questa soluzione risolve i seguenti casi di utilizzo:

- Backup del database con snapshot per i database Oracle ospitati in Amazon FSX per ONTAP
- Ripristino del database Oracle in caso di guasto
- Clonazione rapida ed efficiente in termini di storage dei database primari per un ambiente di sviluppo/test o altri casi di utilizzo

### Pubblico

Questa soluzione è destinata ai seguenti destinatari:

- Il DBA che gestisce i database Oracle in esecuzione su Amazon FSX per lo storage ONTAP
- Il Solution architect che è interessato a testare il backup, il ripristino e la clonazione del database Oracle nel cloud AWS pubblico
- L'amministratore dello storage che supporta e gestisce Amazon FSX per lo storage ONTAP
- Il proprietario dell'applicazione che possiede applicazioni distribuite su Amazon FSX per lo storage ONTAP

### Ambiente di test e convalida della soluzione

Il test e la convalida di questa soluzione sono stati eseguiti in un ambiente AWS FSX e EC2 che potrebbe non corrispondere all'ambiente di implementazione finale. Per ulteriori informazioni, vedere la sezione [\[Key Factors for Deployment Consideration\]](#).

## Architettura

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

### Componenti hardware e software

#### Hardware

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

#### Software

RedHat Linux	RHEL-8.6.0_HVM-20220503-x86_64-2-Hourly2-GP2	Implementazione dell'abbonamento a RedHat per il test
Oracle Grid Infrastructure	Versione 19.18	Patch RU applicata p34762026_190000_Linux-x86-64.zip
Database Oracle	Versione 19.18	Patch RU applicata p34765931_190000_Linux-x86-64.zip
Oracle OPatch	Versione 12.2.0.1.36	Ultima patch p6880880_190000_Linux-x86-64.zip
Servizio SnapCenter	Versione	v2.3.1.2324

### Fattori chiave per l'implementazione

- **Il connettore deve essere implementato nello stesso VPC del database e FSX.** quando possibile, il connettore deve essere implementato nello stesso AWS VPC, che consente la connettività allo storage FSX e all'istanza di calcolo EC2.
- **Una policy IAM AWS creata per SnapCenter Connector.** la policy in formato JSON è disponibile nella documentazione dettagliata del servizio SnapCenter. Quando si avvia l'implementazione di Connector con la console BlueXP, viene anche richiesto di impostare i prerequisiti con i dettagli dell'autorizzazione richiesta in formato JSON. Il criterio deve essere assegnato all'account utente AWS proprietario del connettore.
- **La chiave di accesso dell'account AWS e la coppia di chiavi SSH create nell'account AWS.** la coppia di chiavi SSH viene assegnata all'utente ec2 per l'accesso all'host del connettore e l'implementazione di un plug-in del database nell'host del server DB EC2. La chiave di accesso concede l'autorizzazione per il provisioning del connettore richiesto con il criterio IAM di cui sopra.
- **Una credenziale aggiunta all'impostazione della console BlueXP.** per aggiungere Amazon FSX per ONTAP all'ambiente di lavoro BlueXP, una credenziale che concede i permessi BlueXP per accedere ad Amazon FSX per ONTAP viene impostata nell'impostazione della console BlueXP.

- **java-11-openjdk installato sull'host di istanza del database EC2.** l'installazione del servizio SnapCenter richiede la versione 11 di java. Deve essere installato sull'host dell'applicazione prima di tentare la distribuzione del plugin.

## Implementazione della soluzione

È disponibile un'ampia documentazione NetApp con un ambito più ampio per aiutarti a proteggere i dati delle applicazioni native del cloud. L'obiettivo di questa documentazione è fornire procedure passo-passo che coprano l'implementazione del servizio SnapCenter con la console BlueXP per proteggere il database Oracle distribuito su Amazon FSX per ONTAP e un'istanza di calcolo EC2. Questo documento contiene alcuni dettagli che potrebbero non essere presenti nelle istruzioni più generali.

Per iniziare, attenersi alla seguente procedura:

- Leggere le istruzioni generali ["Proteggi i dati delle tue applicazioni native nel cloud"](#) E le sezioni relative a Oracle e Amazon FSX per ONTAP.
- Guarda il video seguente.

### Implementazione della soluzione

#### Prerequisiti per l'implementazione del servizio SnapCenter

L'implementazione richiede i seguenti prerequisiti.

1. Un server database Oracle primario su un'istanza EC2 con un database Oracle completamente implementato e in esecuzione.
2. Un cluster Amazon FSX per ONTAP implementato in AWS che ospita i volumi di database qui sopra.
3. Un server di database opzionale su un'istanza EC2, utilizzabile per il test del cloning di un database Oracle su un host alternativo al fine di supportare un carico di lavoro di sviluppo/test o qualsiasi caso d'utilizzo che richiede un set di dati completo di un database Oracle di produzione.
4. Se hai bisogno di aiuto per soddisfare i prerequisiti sopra indicati per l'implementazione del database Oracle su Amazon FSX per ONTAP e istanze di calcolo EC2, consulta ["Implementazione e protezione di database Oracle in AWS FSX/EC2 con iSCSI/ASM"](#) o white paper ["Oracle Database Deployment su EC2 e FSX Best Practice"](#)

#### Preparazione al BlueXP



1. Utilizzare il link "[NetApp BlueXP](#)" Per iscriversi all'accesso alla console BlueXP.
2. Effettua l'accesso al tuo account AWS per creare una policy IAM con autorizzazioni appropriate e assegnare la policy all'account AWS che verrà utilizzato per l'implementazione di BlueXP Connector.

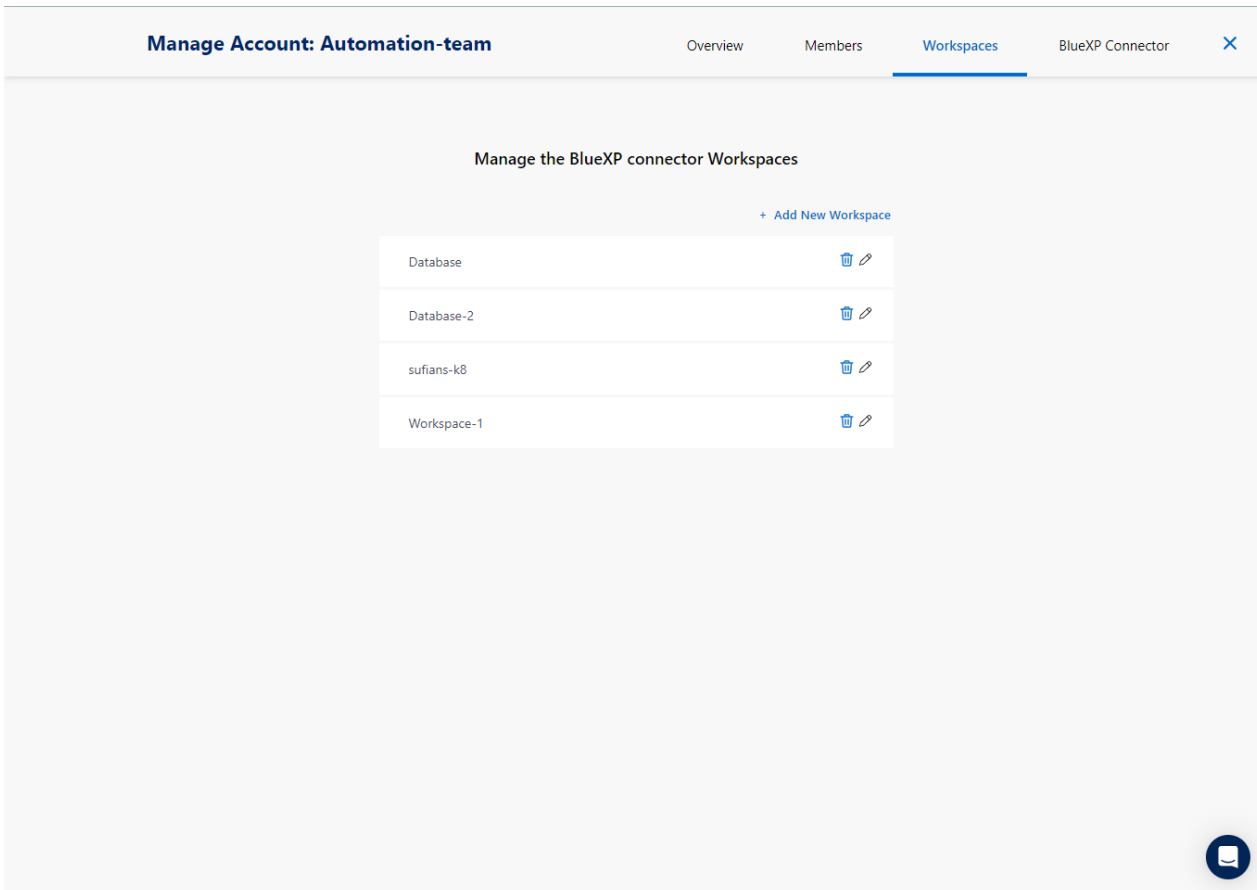
The screenshot shows the AWS IAM console interface. On the left is the navigation menu with sections like 'Identity and Access Management (IAM)', 'Access management', 'Policies', and 'Access reports'. The main content area is titled 'Policies > snapcenter' and shows the 'Summary' tab. It displays the 'Policy ARN' as 'arn:aws:iam::541696183547:policy/snapcenter' and the 'Description' as 'Policy to grant snapcenter service permission to create connector in AWS.' Below this 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's permissions, including actions like 'iam:CreateRole', 'iam:DeleteRole', 'iam:PutRolePolicy', 'iam:CreateInstanceProfile', 'iam:DeleteRolePolicy', 'iam:AddRoleToInstanceProfile', 'iam:RemoveRoleFromInstanceProfile', 'iam:DeleteInstanceProfile', 'iam:PassRole', 'iam:ListRoles', 'ec2:DescribeInstanceStatus', 'ec2:RunInstances', 'ec2:ModifyInstanceAttribute', 'ec2:CreateSecurityGroup', 'ec2:DeleteSecurityGroup', 'ec2:DescribeSecurityGroups', 'ec2:RevokeSecurityGroupEgress', 'ec2:AuthorizeSecurityGroupEgress', 'ec2:AuthorizeSecurityGroupIngress', 'ec2:RevokeSecurityGroupIngress', 'ec2:CreateNetworkInterface', and 'ec2:DescribeNetworkInterfaces'.

Il criterio deve essere configurato con una stringa JSON disponibile nella documentazione di NetApp. La stringa JSON può essere recuperata anche dalla pagina quando viene avviato il provisioning del connettore e viene richiesto l'assegnazione delle autorizzazioni prerequisites.

3. Ti servono anche VPC AWS, subnet, gruppo di sicurezza, una chiave di accesso e segreti per un account utente AWS, una chiave SSH per EC2 utenti e così via, pronti per il provisioning dei connettori.

## Implementare un connettore per i servizi SnapCenter

1. Accedi alla console BlueXP. Per un account condiviso, è consigliabile creare un singolo spazio di lavoro facendo clic su **account** > **Manage account** > **Workspace** per aggiungere un nuovo spazio di lavoro.



2. Fare clic su **Add a Connector** (Aggiungi un connettore) per avviare il flusso di lavoro di provisioning del connettore.

**NetApp Cloud Manager**

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

**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. Scegli il tuo cloud provider (in questo caso, **Amazon Web Services**).

**Add Connector**

**Provider**

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

- Microsoft Azure
- Amazon Web Services
- Google Cloud Platform

**Continue**

1. Ignorare i passaggi **Permission**, **Authentication** e **Networking** se sono già stati configurati nell'account AWS. In caso contrario, è necessario configurarli prima di procedere. Da qui, è possibile recuperare anche le autorizzazioni per il criterio AWS a cui si fa riferimento nella sezione precedente

## Add Connector - AWS



### Deploying a Connector

The Connector is a crucial component for the day-to-day use of Cloud Manager.  
It's used to connect Cloud Manager's services to your hybrid-cloud environments.  
The Connector can then manage the resources and processes within your public cloud environment.

Before you begin the deployment process, ensure that you have completed the required preparations. This guide will enable you to focus on the minimum requirements for Connector installation.

#### Permissions

Set up an IAM role with the required permissions

#### Authentication

Choose between two AWS authentication methods: AWS keys or assuming an IAM role

#### Networking

Obtain details about the VPC and subnet in which the Connector will reside

[Skip to Deployment](#)

[Previous](#)

[Continue](#)



1. Inserisci l'autenticazione del tuo account AWS con **Access Key** e **Secret Key**.

- 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. Assegnare un nome all'istanza del connettore e selezionare **Crea ruolo** in **Dettagli**.

- ✓ AWS Credentials 2 Details 3 Network 4 Security Group 5 Review

## Details

Connector Instance Name

SnapCenterSvs

[+](#) Add Tags to Connector Instance

Connector Role

☒ Create Role ☐ Select an existing Role

Role Name

Cloud-Manager-Operator-VZzSSP9-SnapCenter

☐ AWS Managed Encryption

Master Key: aws/ebs (default)

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

1. Configurare la rete con **VPC**, **Subnet** e SSH **Coppia di chiavi** per l'accesso al connettore.

Add BlueXP Connector - AWS

More Information X

✓ 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)

**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 AWS services.

Previous

Next

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

Add BlueXP Connector - AWS

More Information

✓ AWS Credentials

✓ Details

✓ Network

4 Security Group

5 Review

### Security Group

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

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

1 Security Group

Security Group Name	Description
<input checked="" type="radio"/> default	default VPC security group

Previous

Next

3. Esaminare la pagina di riepilogo e fare clic su **Aggiungi** per avviare la creazione del connettore. In genere occorrono circa 10 minuti per completare l'implementazione. Una volta completata l'operazione, l'istanza del connettore viene visualizzata nella dashboard di AWS EC2.

Add BlueXP Connector - AWS

More Information

✓ AWS Credentials

✓ Details

✓ Network

✓ Security Group

5 Review

Review

[Code for Terraform Automation](#)

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

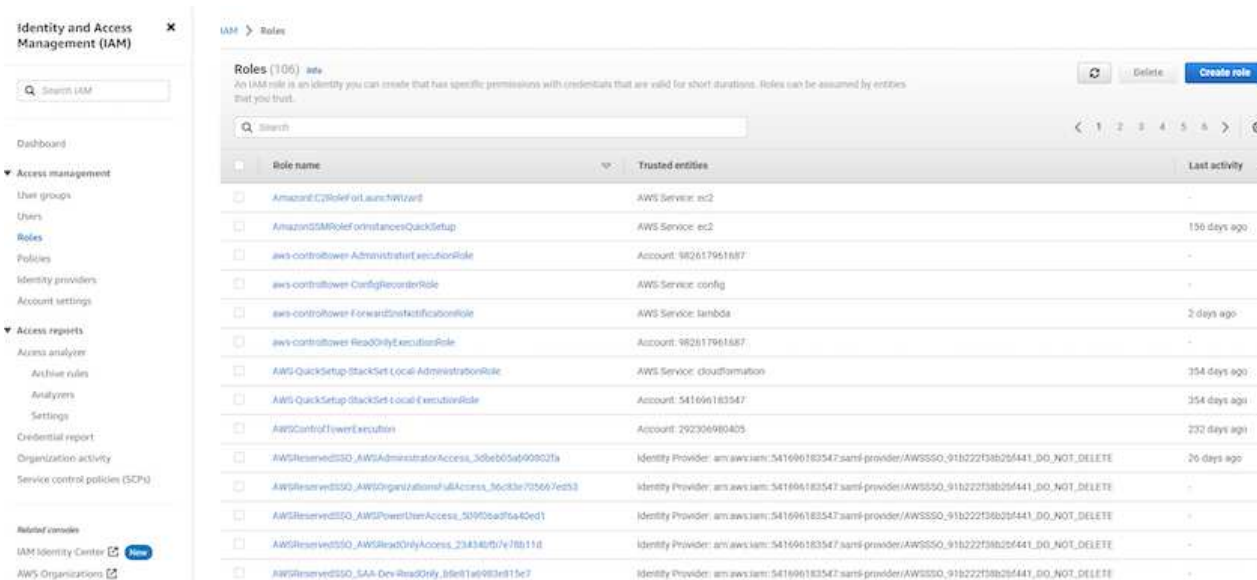
Previous

Add

**Definisci una credenziale nell'accesso alle risorse BlueXP per AWS**



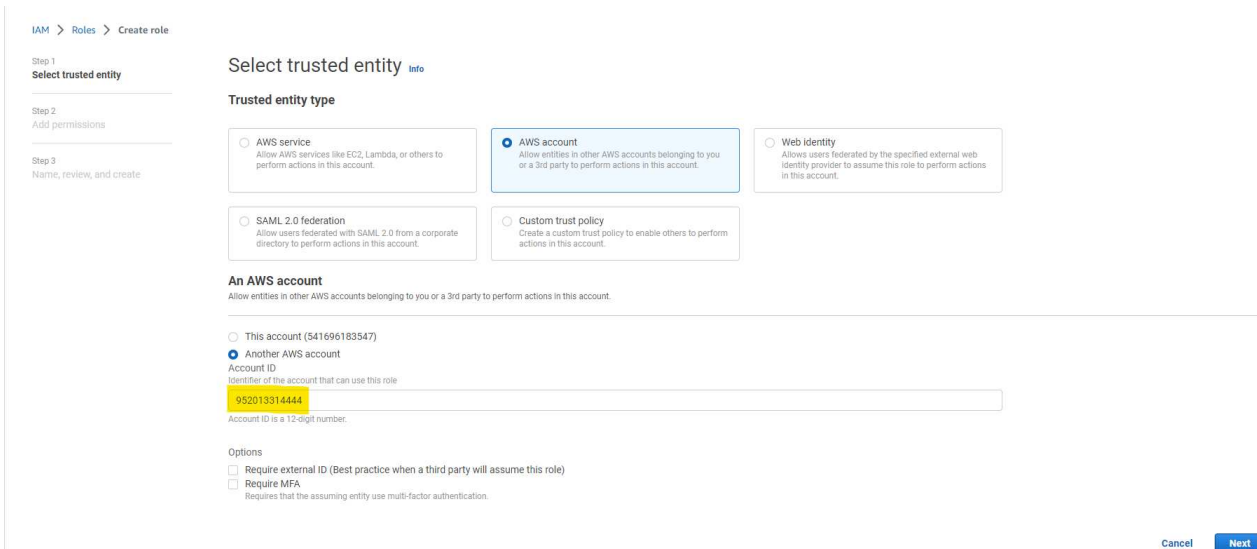
1. Innanzitutto, dalla console AWS EC2, creare un ruolo nel menu **Identity and Access Management (IAM) Roles, Create role** per avviare il flusso di lavoro di creazione dei ruoli.



The screenshot shows the AWS IAM console. The left sidebar has a navigation menu with 'Roles' selected. The main content area shows a list of roles. The 'Create role' button is in the top right corner.

Role name	Trusted entities	Last activity
AmazonEC2RoleforLambda	AWS Service: ec2	-
AmazonSSMRoleforInstancesQuickSetup	AWS Service: ec2	156 days ago
aws-controltower-AdministratorExecutionRole	Account: 982617961887	-
aws-controltower-ConfigRecorderRole	AWS Service: config	-
aws-controltower-ForwardNotificationRole	AWS Service: lambda	2 days ago
aws-controltower-ReadOnlyExecutionRole	Account: 982617961887	-
AWS-QuickSetup-StackSet-Local-AdministrationRole	AWS Service: cloudformation	154 days ago
AWS-QuickSetup-StackSet-Local-ExecutionRole	Account: 541696183547	154 days ago
AWSControlTowerExecution	Account: 292306980405	232 days ago
AWSReservedSSO_AWSAdministratorAccess_3d8eb05a699802fa	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	26 days ago
AWSReservedSSO_AWSOrganizationalAccess_Mock3e725667e253	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_AWSPowerUserAccess_509f0ba0f640ed1	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_AWSReadOnlyAccess_234340b7c71bb11d	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-
AWSReservedSSO_SAA-Dev-ReadOnly_I8e81e983ed11e7	Identity Provider: am.aws.saml:541696183547:saml-provider:AWSSSO_91b222f38b25f441_ID_NOT_DELETE	-

2. Nella pagina **Seleziona entità attendibile**, scegli **account AWS**, un altro account AWS e incolla nell'ID account BlueXP, che può essere recuperato dalla console BlueXP.



The screenshot shows the 'Create role' wizard in the AWS IAM console. Step 1 is 'Select trusted entity'. The 'AWS account' option is selected. The 'Account ID' field is highlighted with a yellow box, showing the value '992013314444'.

**Select trusted entity**

**Trusted entity type**

- ☐ AWS service
- ☒ AWS account
- ☐ Web Identity
- ☐ SAML 2.0 federation
- ☐ Custom trust policy

**An AWS account**

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ This account (541696183547)

☒ Another AWS account

Account ID

Identifier of the account that can use this role

992013314444

Account ID is a 12-digit number.

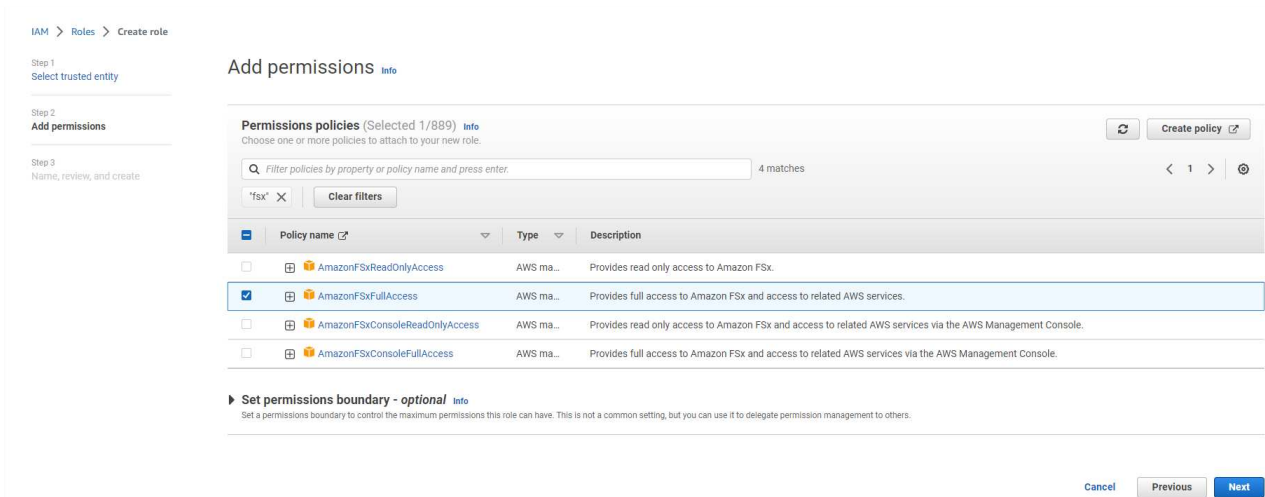
**Options**

- ☐ Require external ID (Best practice when a third party will assume this role)
- ☐ Require MFA

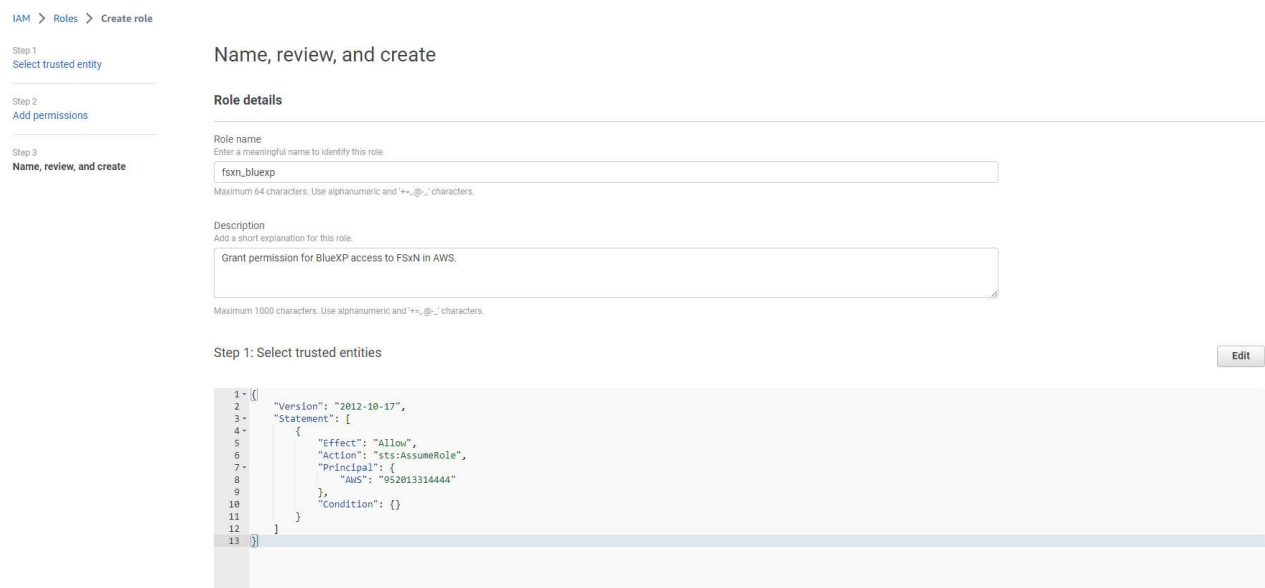
Requires that the assuming entity use multi-factor authentication.

**Cancel** **Next**

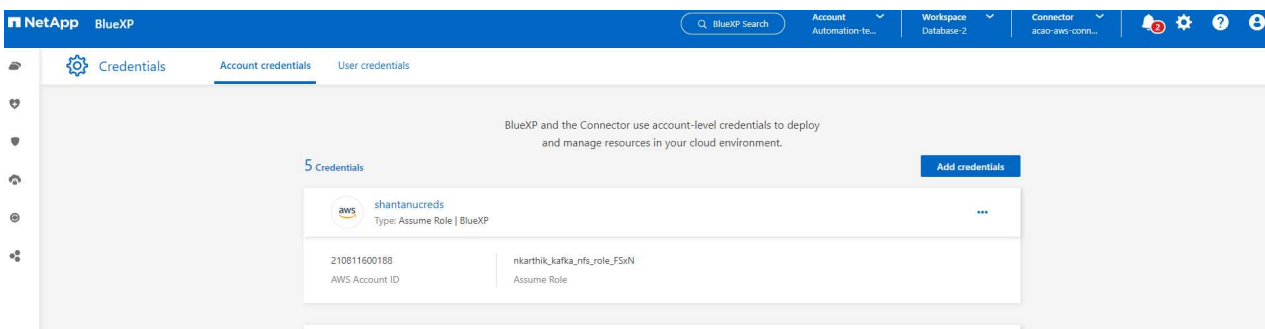
3. Filtrare i criteri di autorizzazione in base a fsx e aggiungere **Criteri di autorizzazione** al ruolo.



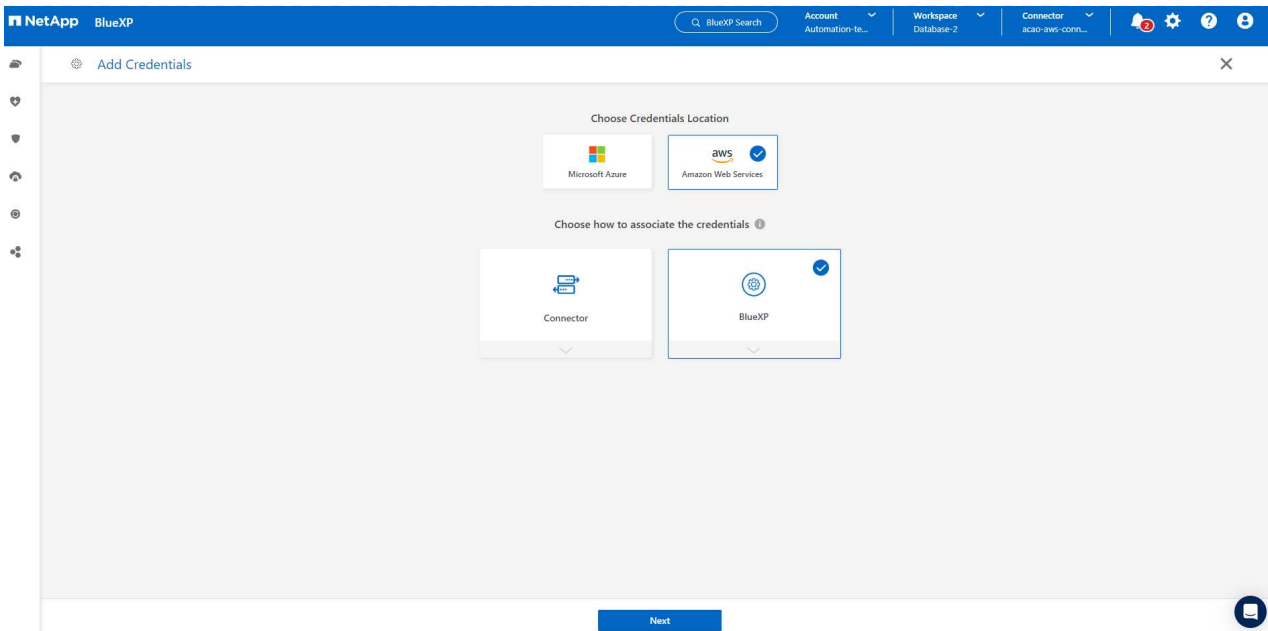
4. Nella pagina **dettagli ruolo**, assegnare un nome al ruolo, aggiungere una descrizione, quindi fare clic su **Crea ruolo**.



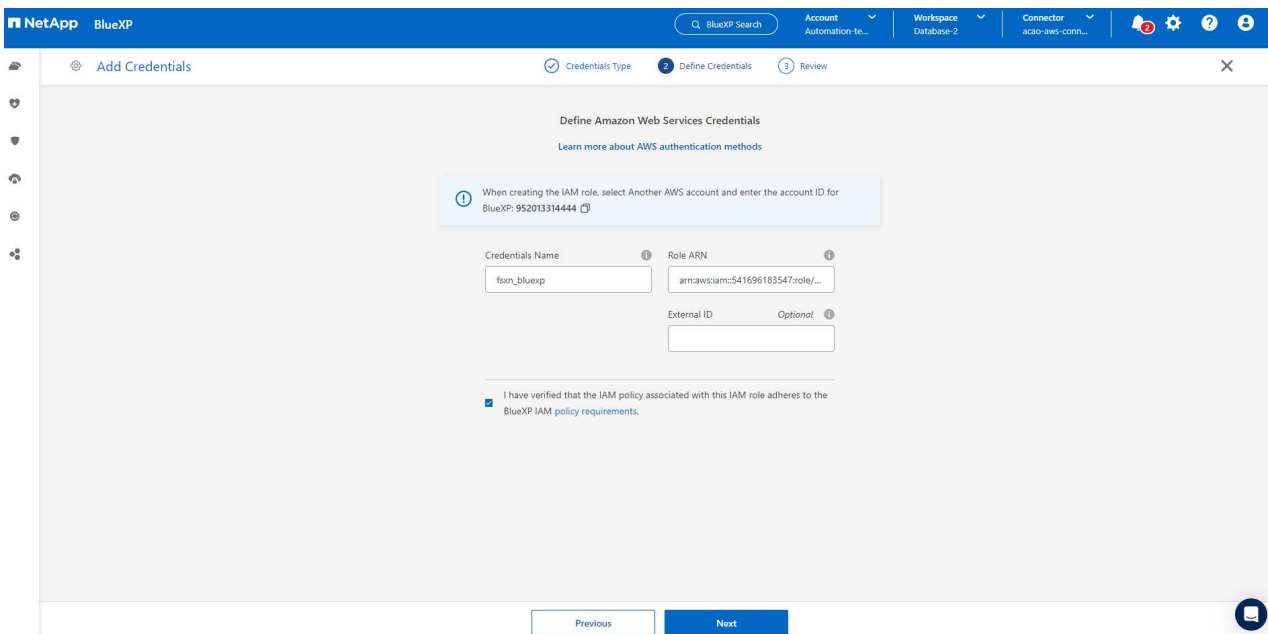
5. Tornando alla console BlueXP, fare clic sull'icona delle impostazioni nell'angolo superiore destro della console per aprire la pagina **credenziali account**, fare clic su **Aggiungi credenziali** per avviare il flusso di lavoro di configurazione delle credenziali.



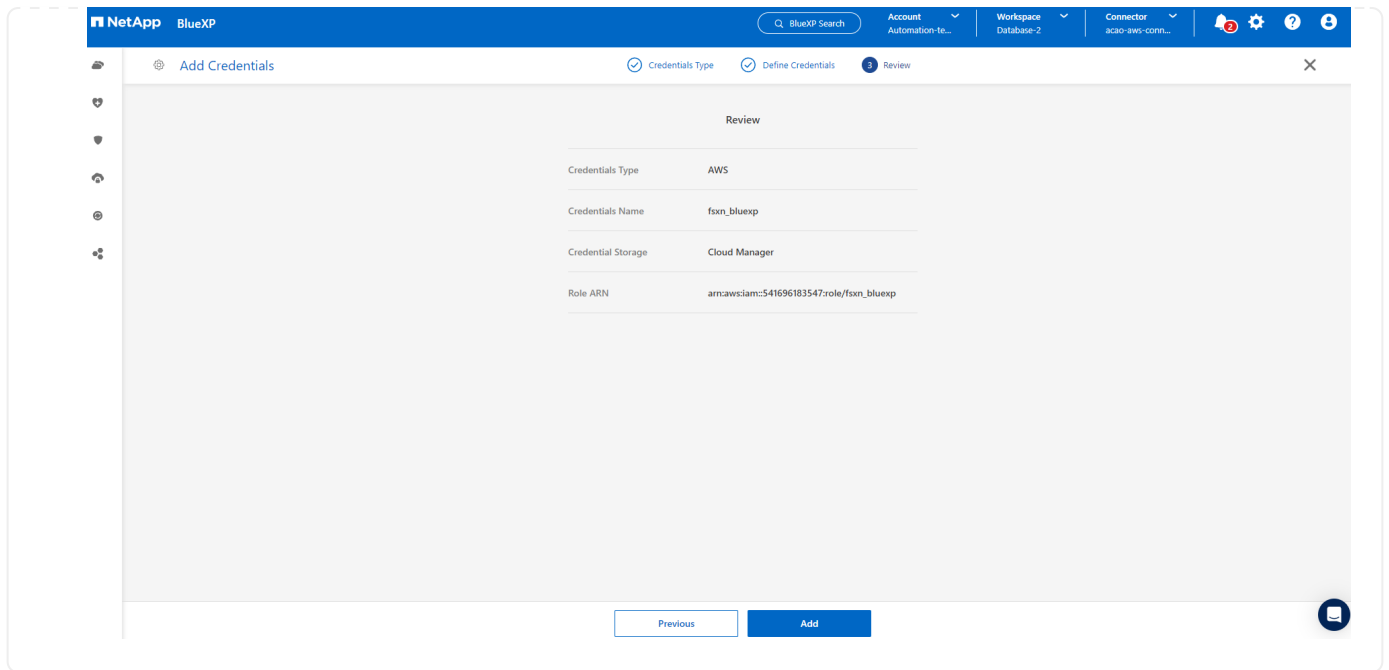
6. Scegli la posizione delle credenziali come - **Amazon Web Services - BlueXP**.



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



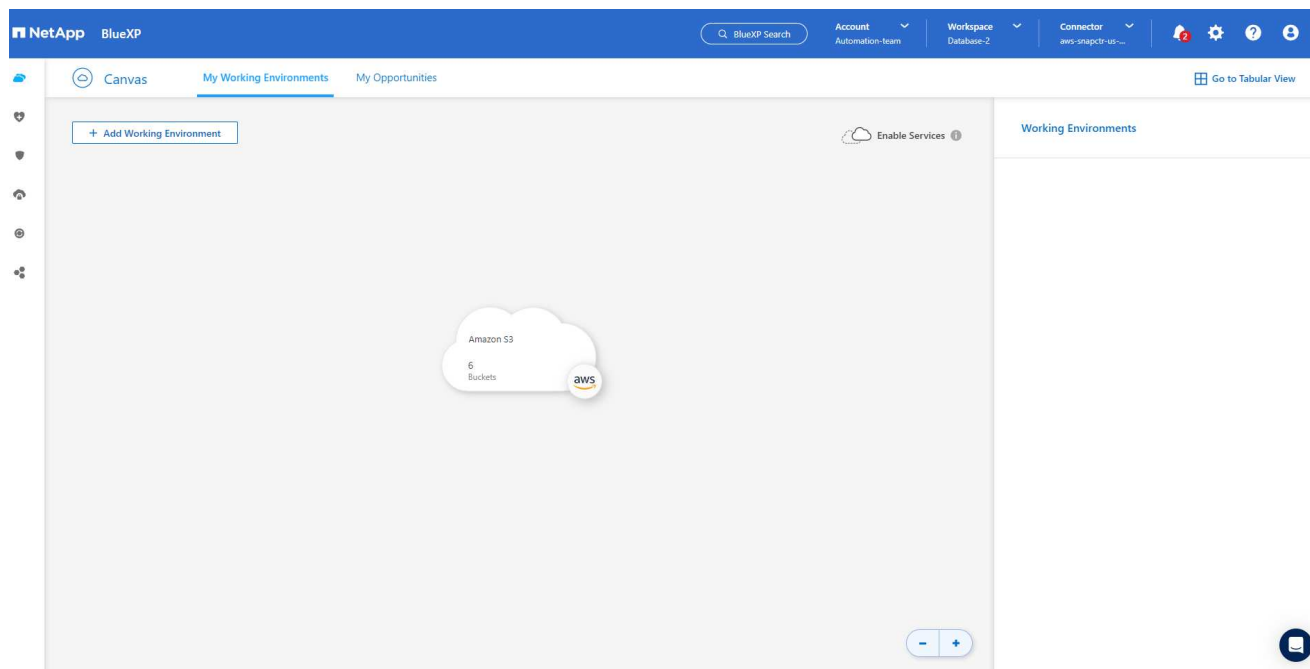
8. Rivedi e **Aggiungi**.



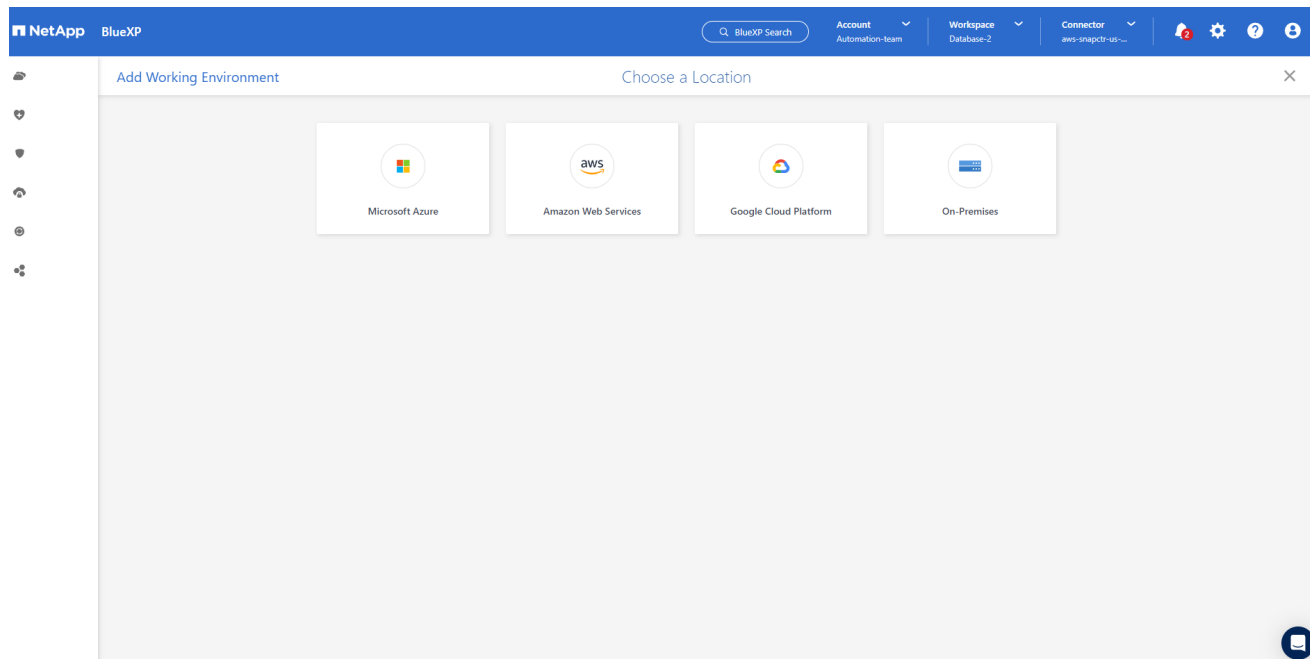
## Configurazione dei servizi SnapCenter

Con il connettore distribuito e la credenziale aggiunta, i servizi SnapCenter possono ora essere configurati con la seguente procedura:

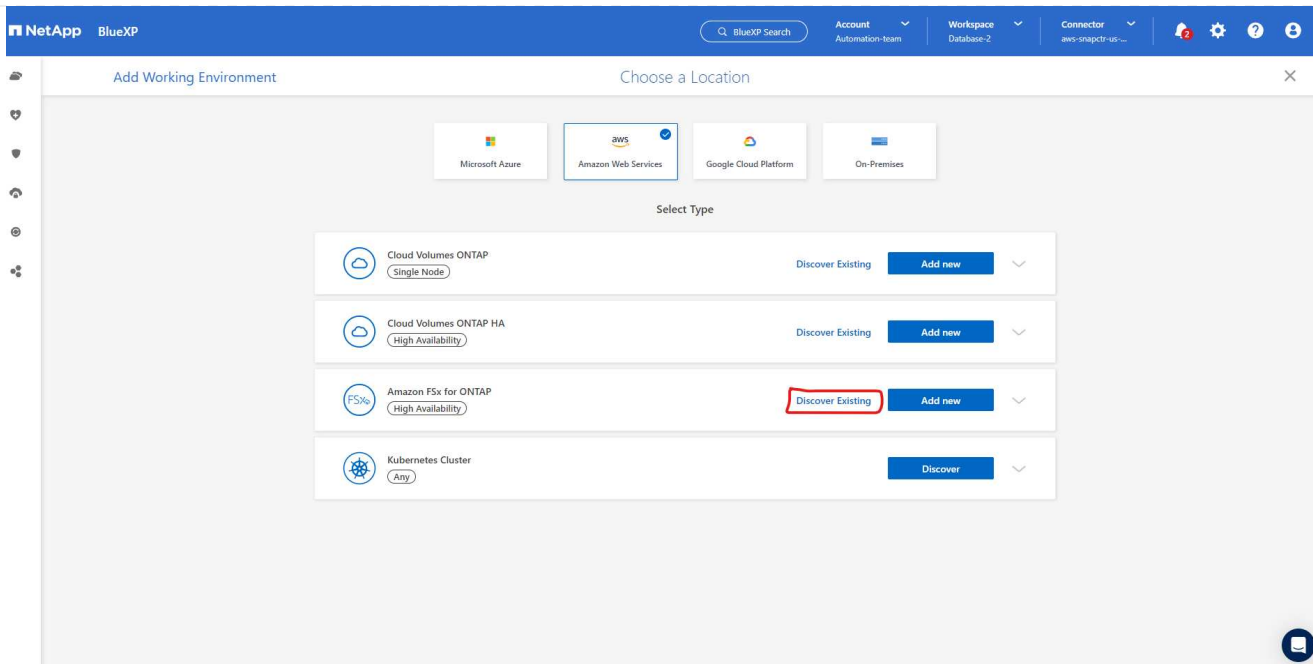
1. Da **My Working Environment** fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) per scoprire FSX implementato in AWS.



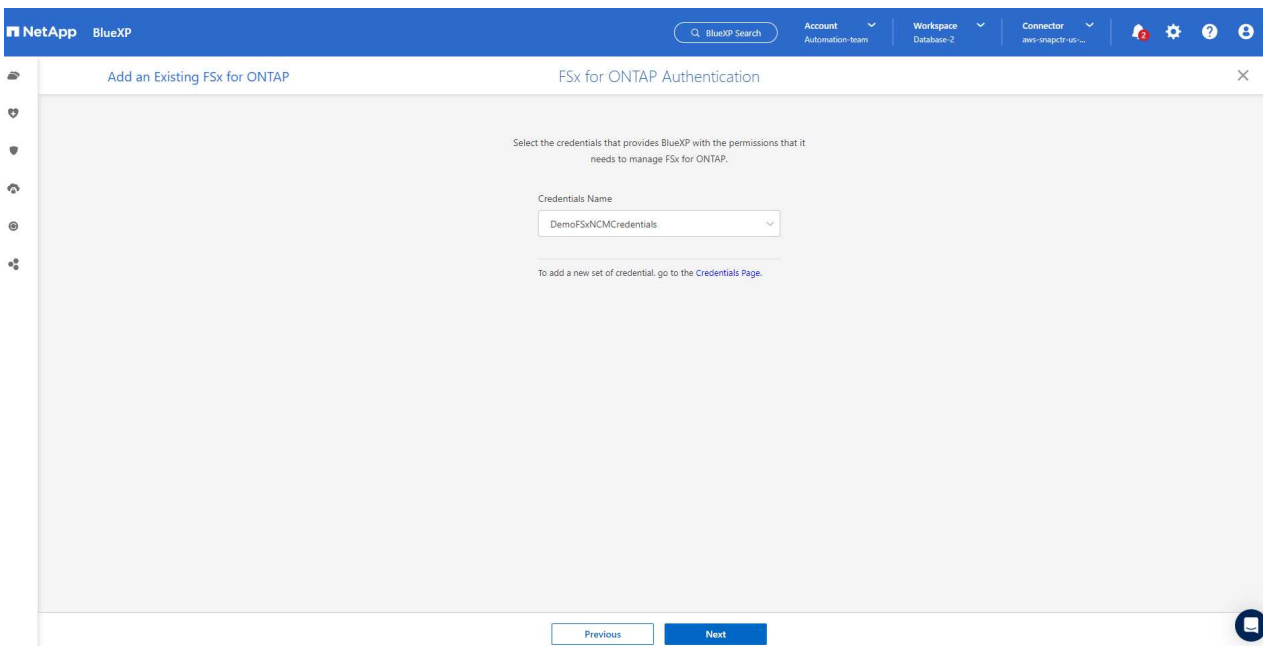
1. Scegliere **Amazon Web Services** come posizione.



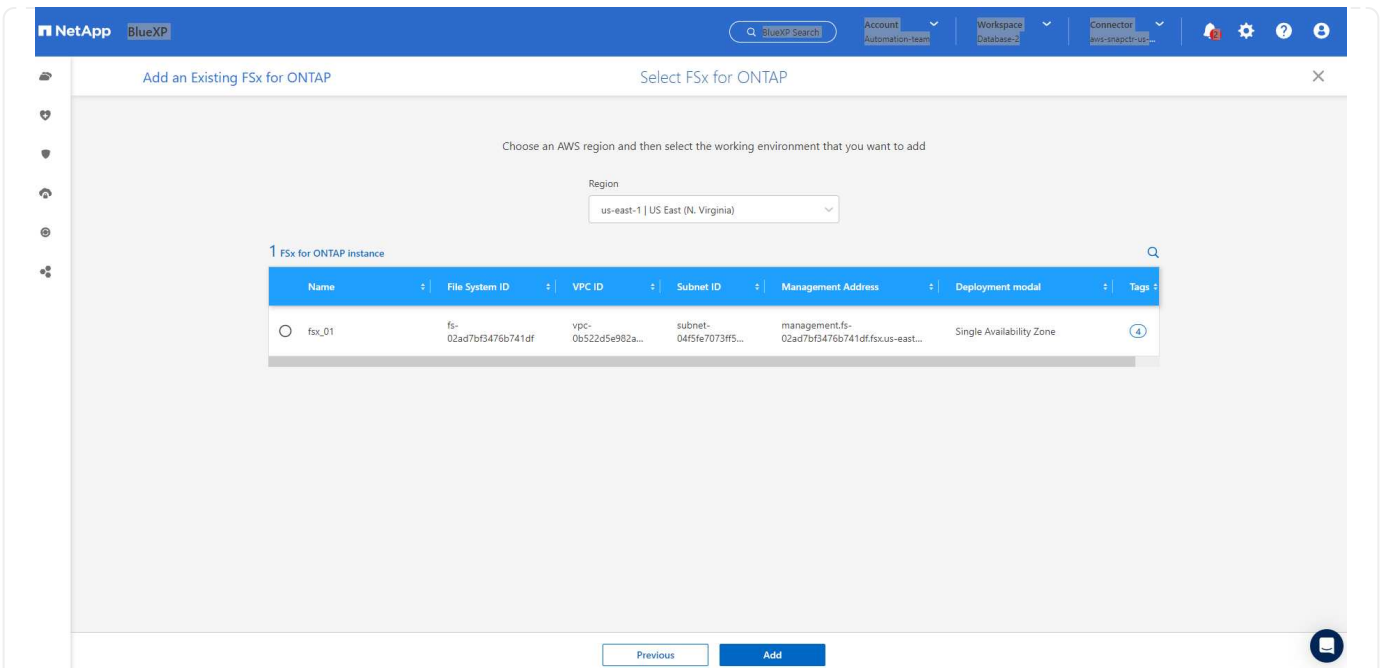
1. Fai clic su **Scopri esistente** accanto a **Amazon FSX per ONTAP**.



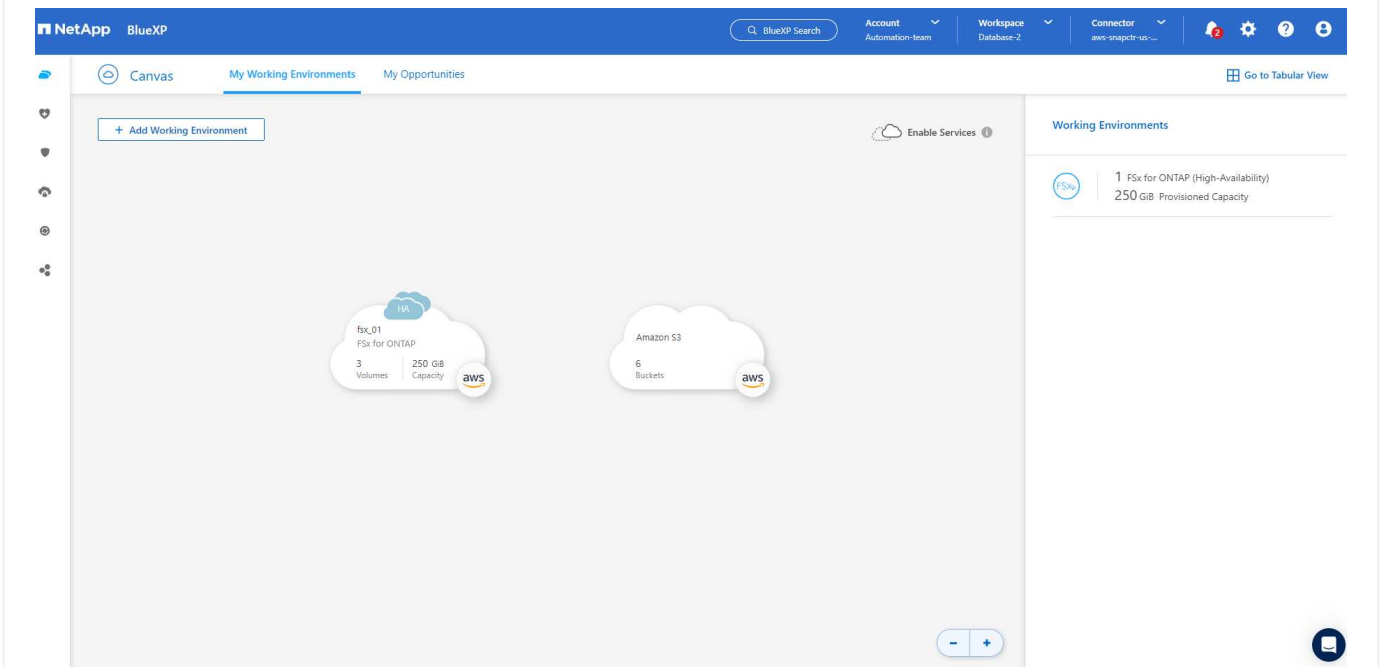
1. Seleziona il **Nome credenziali** creato nella sezione precedente per assegnare ad BlueXP le autorizzazioni necessarie per gestire FSX per ONTAP. Se non sono state aggiunte credenziali, è possibile aggiungerle dal menu **Settings** (Impostazioni) nell'angolo superiore destro della console BlueXP.



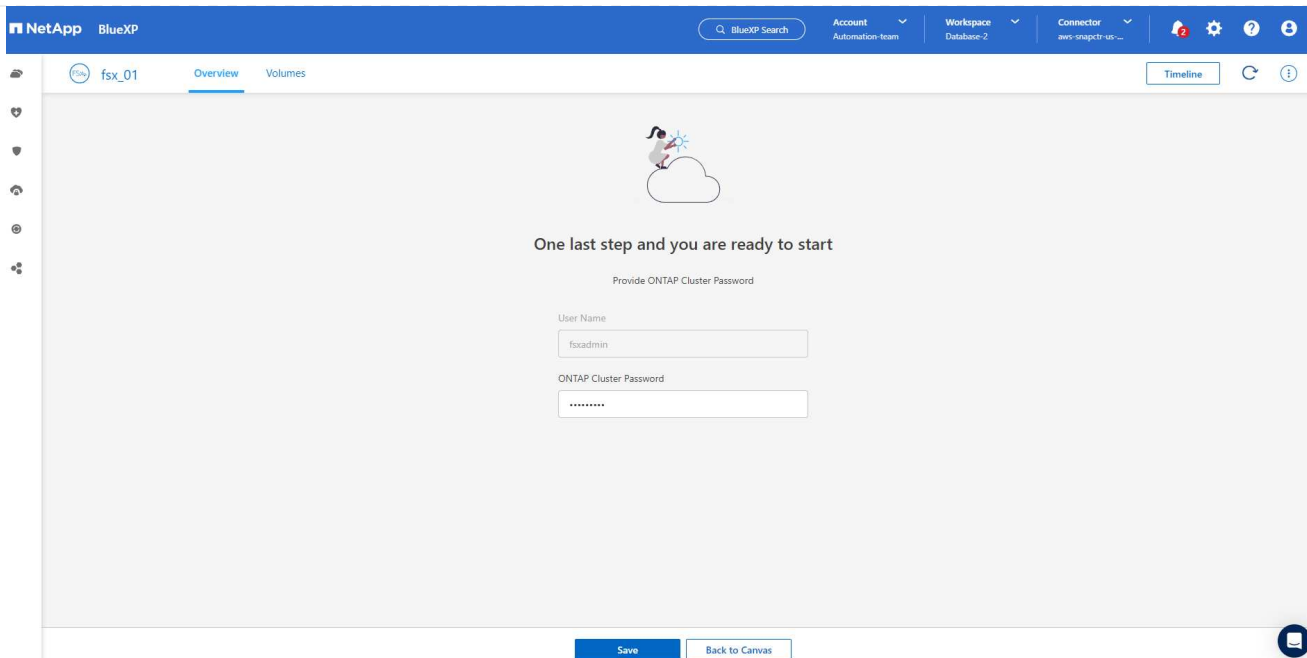
2. Scegliere la regione AWS in cui viene implementato Amazon FSX per ONTAP, selezionare il cluster FSX che ospita il database Oracle e fare clic su Aggiungi.



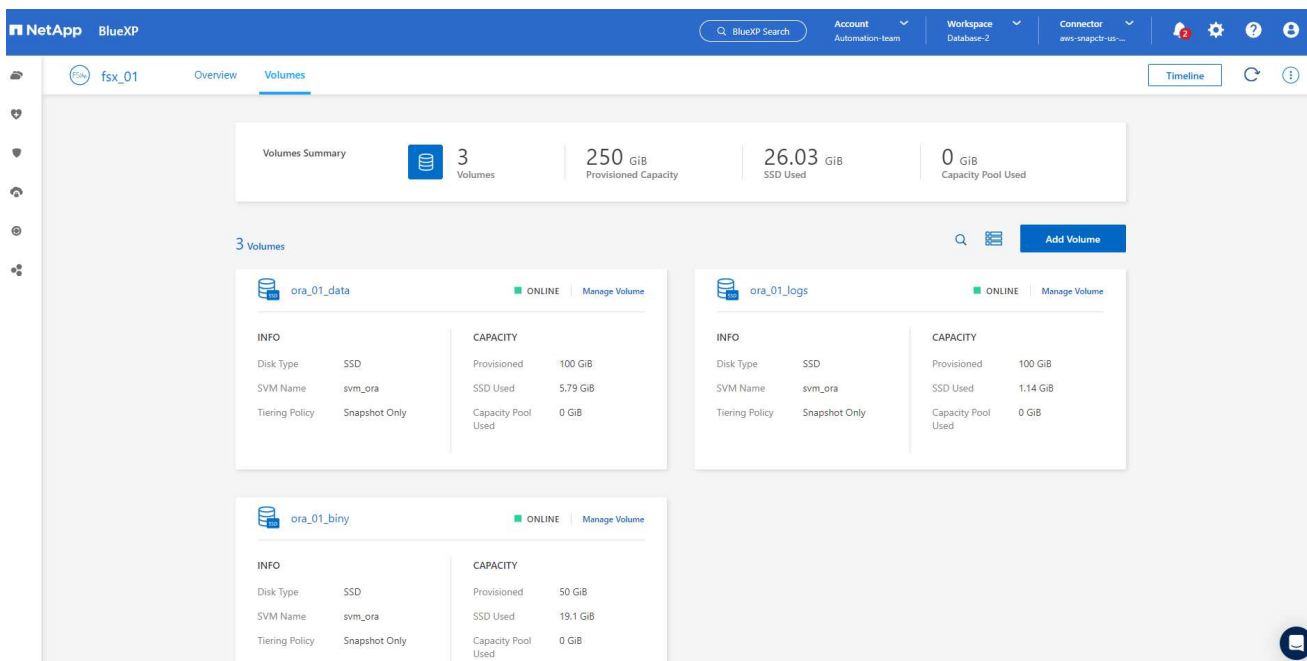
1. L'istanza scoperta di Amazon FSX per ONTAP viene ora visualizzata nell'ambiente di lavoro.



1. È possibile accedere al cluster FSX con le credenziali dell'account fsxadmin.

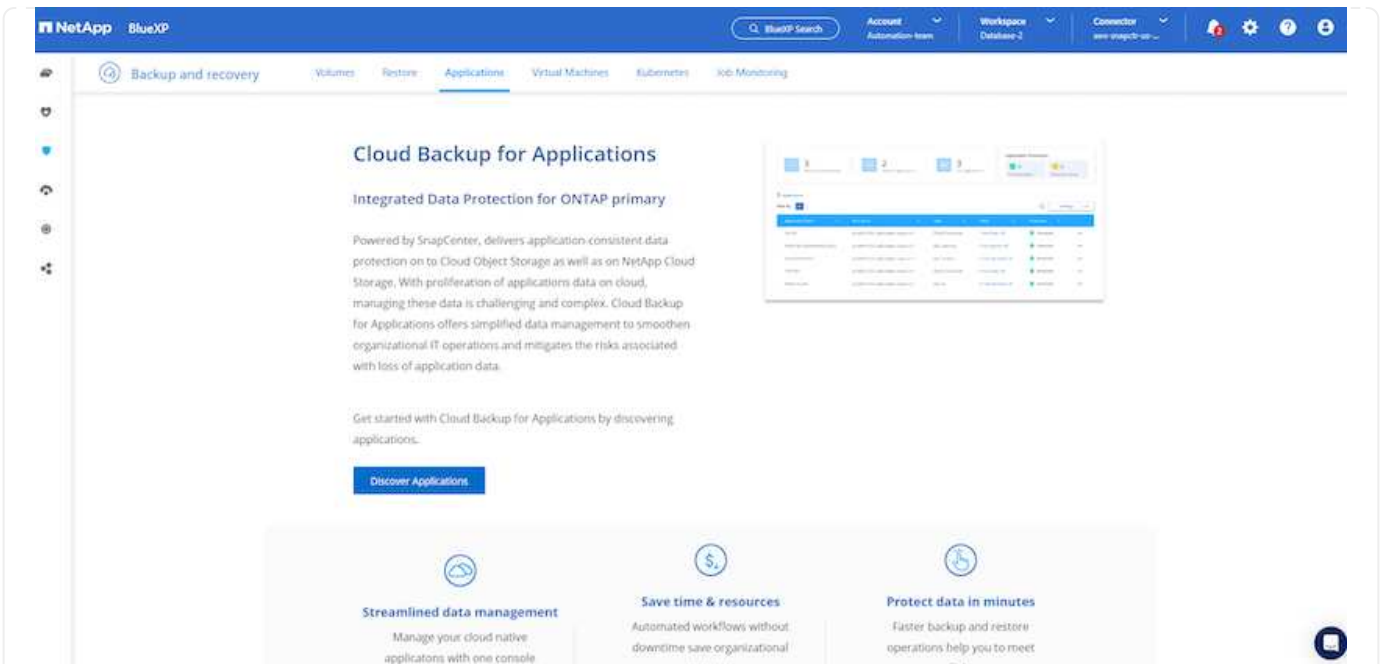


1. Dopo aver effettuato l'accesso ad Amazon FSX per ONTAP, esaminare le informazioni di storage del database (ad esempio i volumi del database).

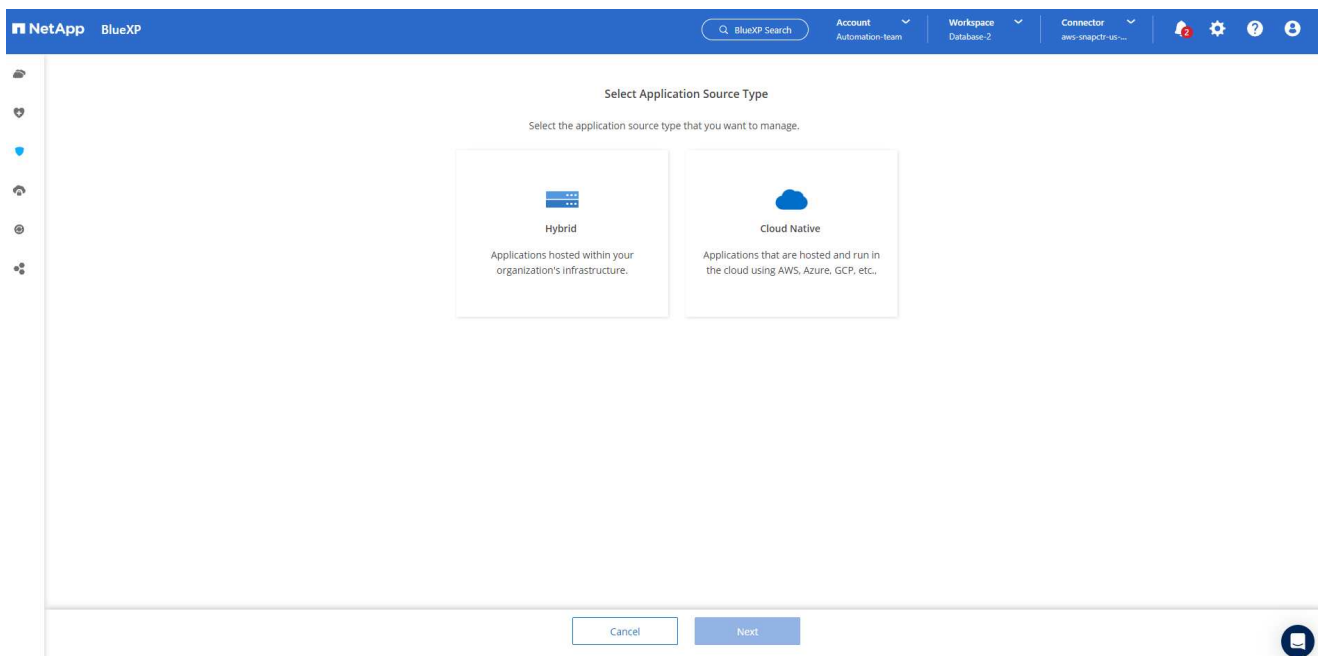


1. Dalla barra laterale sinistra della console, passare il mouse sull'icona di protezione, quindi fare clic su **protezione > applicazioni** per aprire la pagina di avvio delle applicazioni. Fare clic su **Scopri applicazioni**.

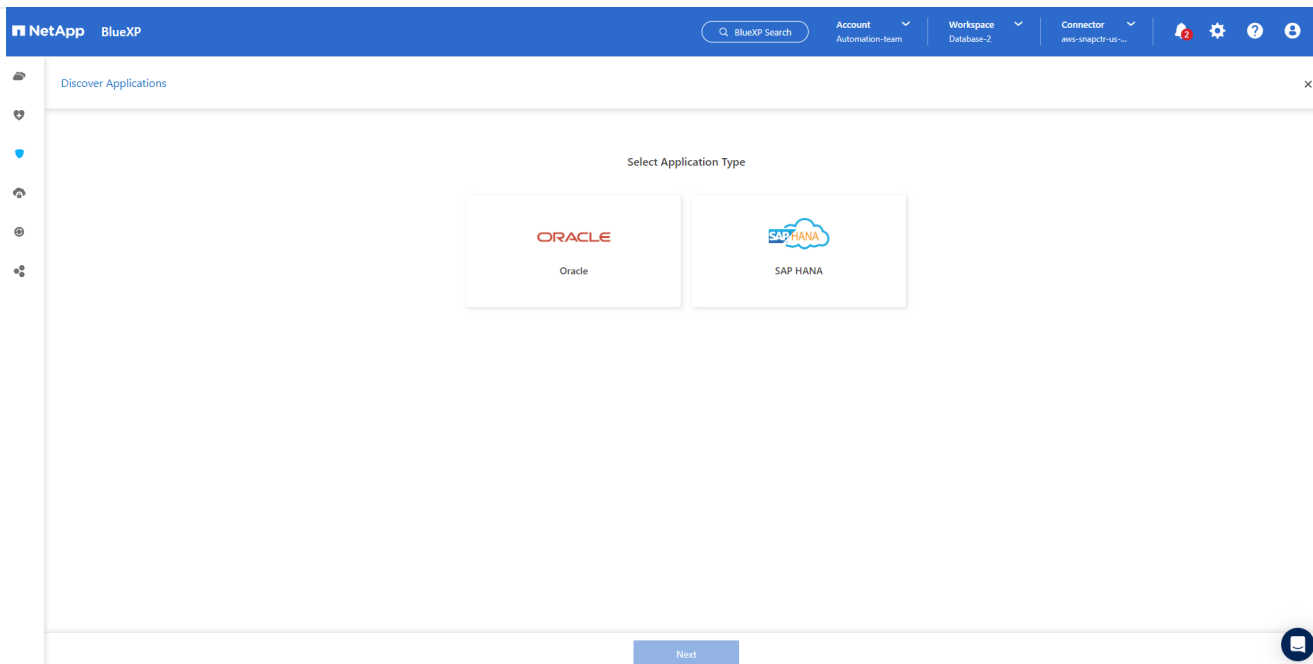




1. Selezionare **Cloud Native** come tipo di origine dell'applicazione.

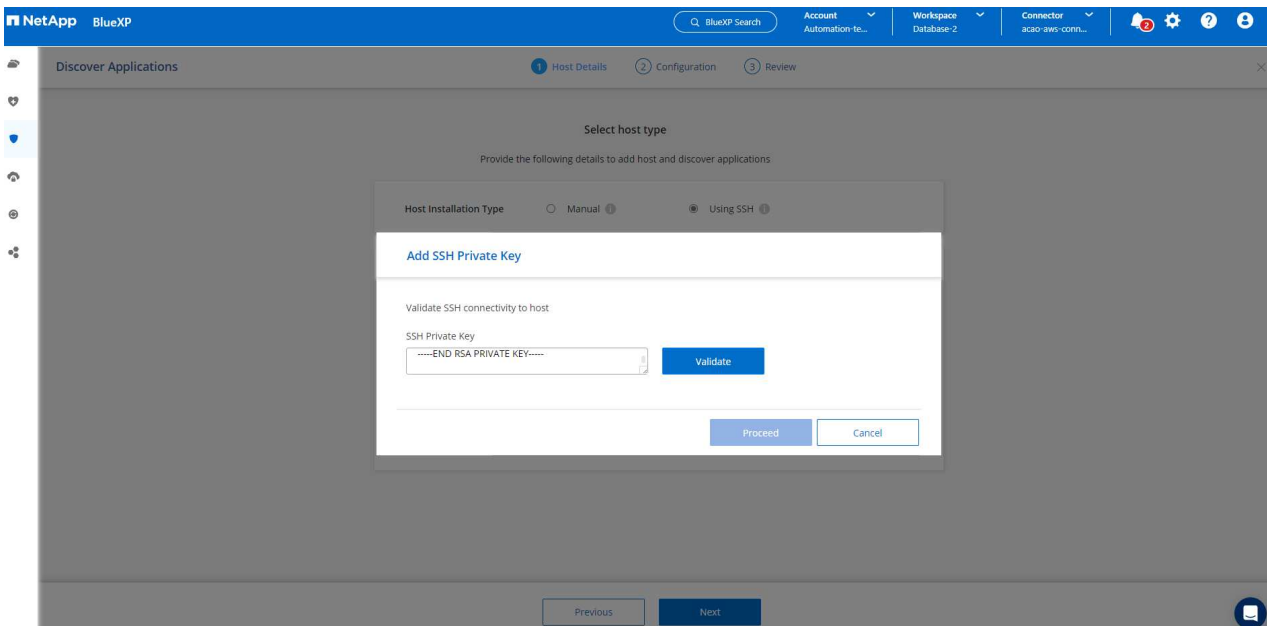


1. Scegliere **Oracle** come tipo di applicazione.

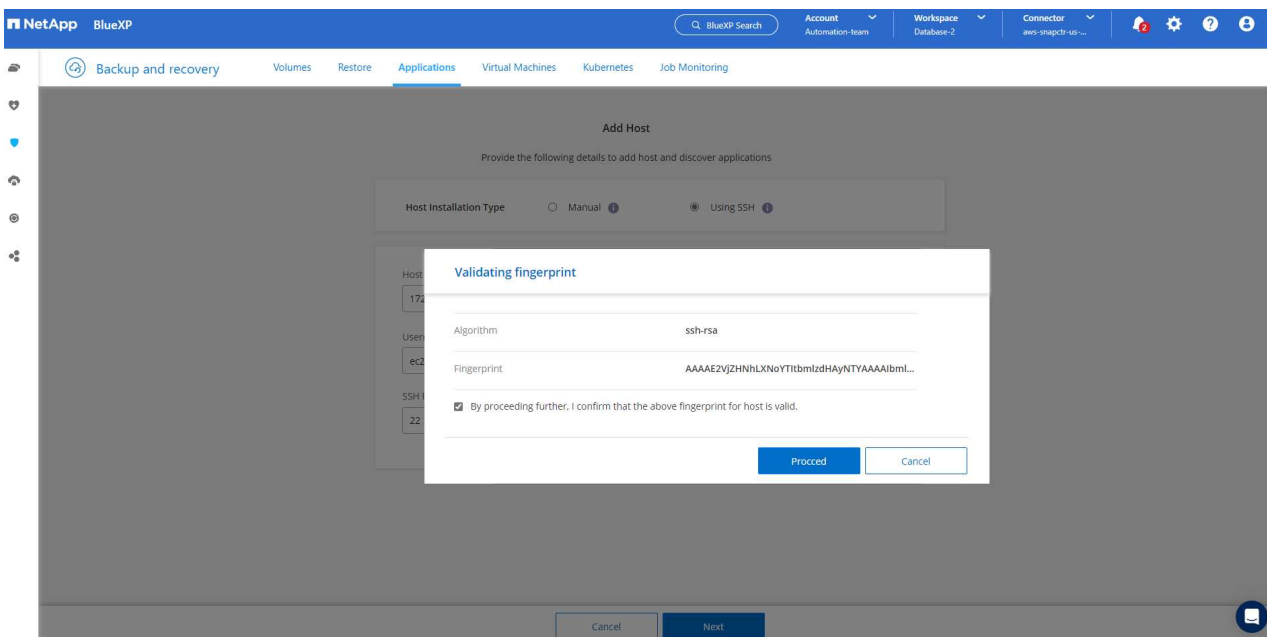


1. Inserisci i dettagli dell'host dell'applicazione AWS EC2 Oracle. Scegliere **utilizzo di SSH** come **tipo di installazione host** per l'installazione di un plug-in e il rilevamento del database. Quindi, fare clic su **Aggiungi chiave privata SSH**.

2. Incollare la chiave SSH per EC2 utenti per l'host database EC2 e fare clic su **convalida** per continuare.



3. Verrà richiesto di **convalidare l'impronta digitale** per continuare.



4. Fare clic su **Next** (Avanti) per installare un plug-in del database Oracle e scoprire i database Oracle sull'host EC2. I database rilevati vengono aggiunti ad **applicazioni**. Il database **Stato protezione** viene visualizzato come **non protetto** quando viene rilevato inizialmente.

NetApp BlueXP

Backup and recovery Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

Cloud Native Oracle

1 Hosts 1 ORACLE 0 Clone

Application Protection

0 Protected 1 Unprotected

1 Databases

Filter By +

Manage Databases Settings

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

1 - 1 of 1

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

## Backup del database Oracle

1. Fare clic sui tre punti accanto al database **Protection Status** (Stato protezione), quindi fare clic su **Policies** (Criteri) per visualizzare i criteri di protezione predefiniti del database che è possibile applicare per proteggere i database Oracle.

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

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

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

1. Quando si è soddisfatti della configurazione dei criteri, è possibile assegnare i criteri scelti per proteggere il database.

NetApp BlueXP

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

Cloud Native | Oracle

1 Hosts | 1 ORACLE | 0 Clone

Application Protection: 0 Protected, 1 Unprotected

1 Databases

Filter By +

Name	Host Name	Policy Name	Protection Status
db1	172.30.15.58		Unprotected

View Details | **Assign Policy**

1. Scegliere il criterio da assegnare al database.

NetApp BlueXP

Applications > Assign Policy

Assign Policy

Assign a policy to start taking backups of the database "db1"

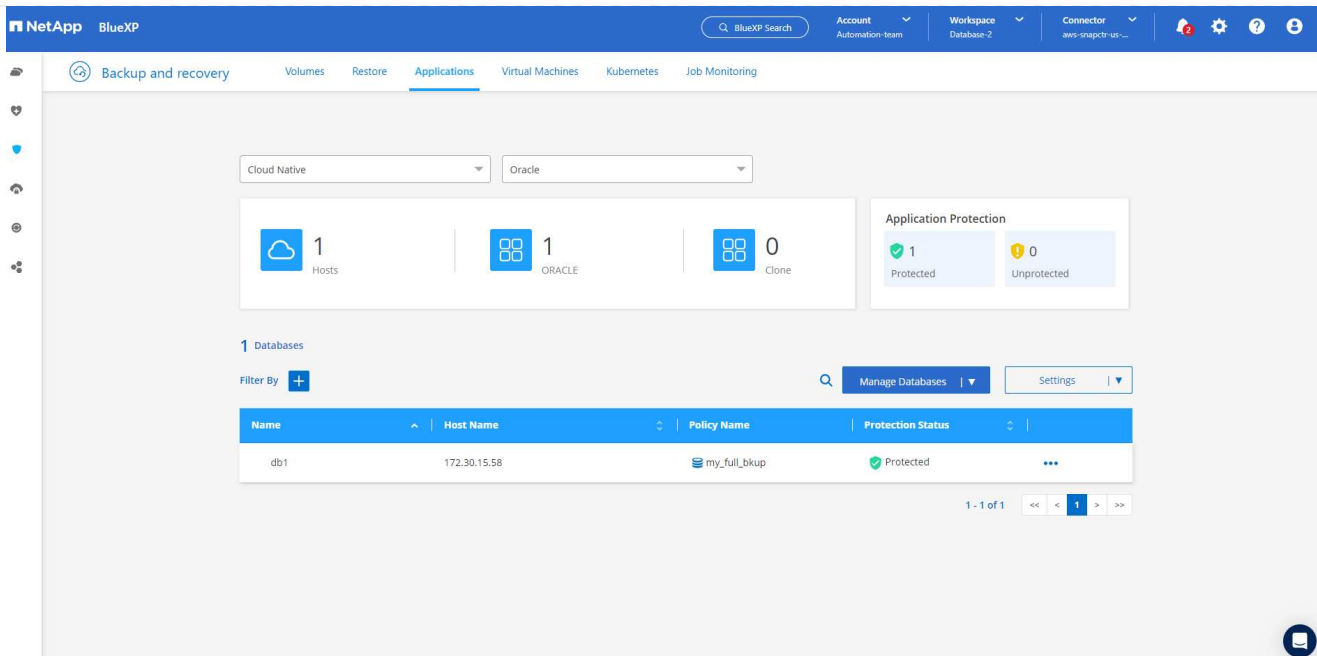
4 Policies

Policy Name	Backup Type	Schedules
<input type="radio"/> 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
<input type="radio"/> 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
<input type="radio"/> 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
<input checked="" type="radio"/> my_full_bkup	FullBackup	Hourly: Repeats Every 1 Hr, Keeps 3 Days

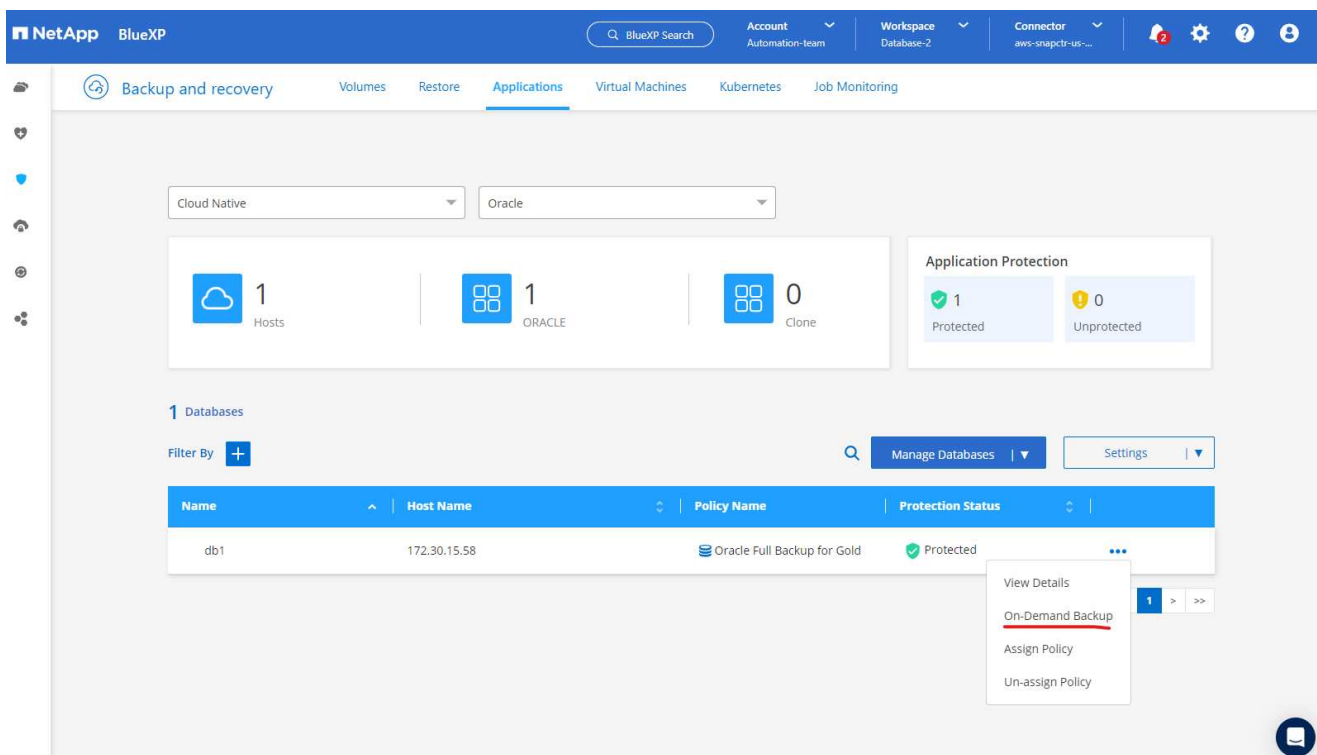
1 - 4 of 4

Cancel Assign

1. Una volta applicato il criterio, lo stato di protezione del database è cambiato in **Protected** con un segno di spunta verde.



1. Il backup del database viene eseguito in base a una pianificazione predefinita. È inoltre possibile eseguire un backup on-demand one-off, come illustrato di seguito.



1. I dettagli dei backup del database possono essere visualizzati facendo clic su **View Details** (Visualizza dettagli) dall'elenco dei menu. Tra cui nome, tipo di backup, SCN e data di backup. Un set di backup copre un'istantanea sia per il volume di dati che per il volume di log. Lo snapshot di un volume di log viene eseguito subito dopo lo snapshot di un volume di database. È possibile applicare un filtro se si cerca un backup particolare in un elenco lungo.

NetAppBlueXP

Q BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapctr-us...

2

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Applications &gt; Database Details

Database Details

db1  
Database Name

Protected  
Protection

Oracle Full Backup for Gold  
Policy Names

Database Type

172.30.15.58  
Host Name

FSx  
Host Storage

Unreachable  
Database Version

bKed8yv2T19Bj0V5QyqvA...  
Agent Id

-  
Clones

-  
Parent Database

8 Backups

Filter By

Select Timeframe

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

Ripristino e ripristino del database Oracle



1. Per un ripristino del database, scegliere il backup corretto, in base al tempo di backup o SCN. Fare clic sui tre punti del backup dei dati del database, quindi fare clic su **Restore** (Ripristina) per avviare il ripristino e il ripristino del database.

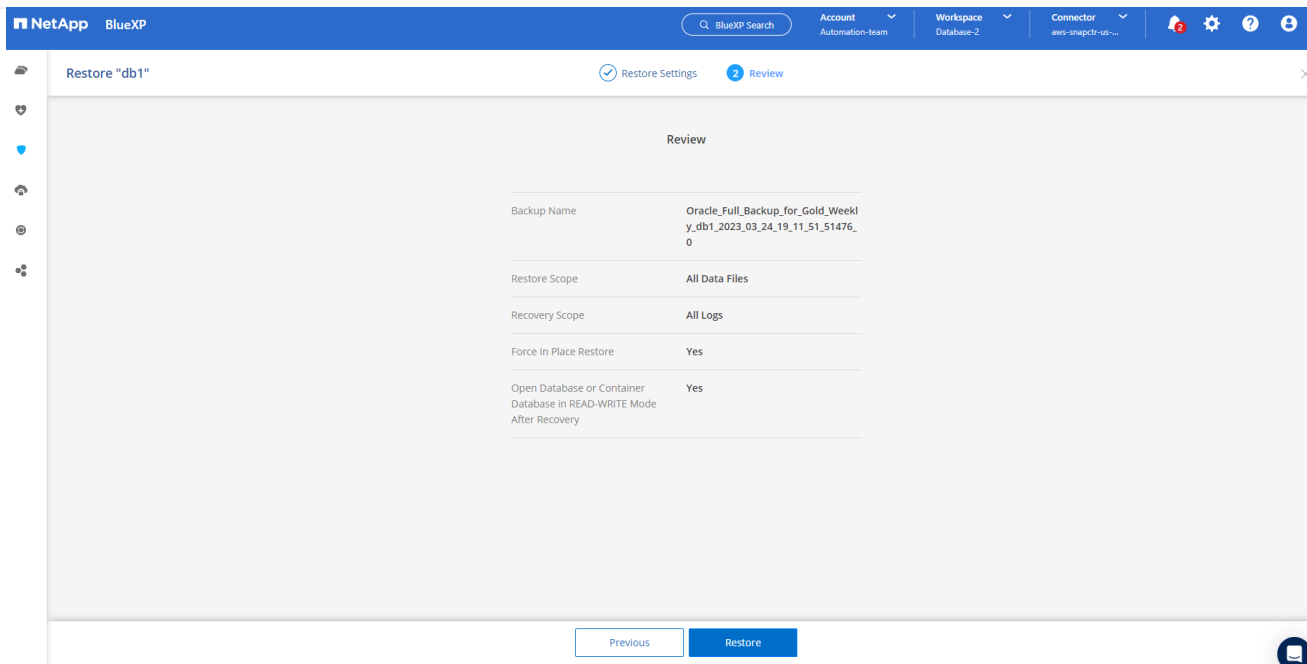
The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'Backup and recovery', 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. The 'Applications' tab is selected, leading to 'Database Details' for a database named 'db1'. Below the details, there are 6 backups listed. The backup 'Oracle\_Full\_Backup\_for\_Gold\_Hourly\_db1\_2023\_03\_24\_15\_37\_04\_98851\_1' is selected, and the 'Restore' button is highlighted in the context menu.

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

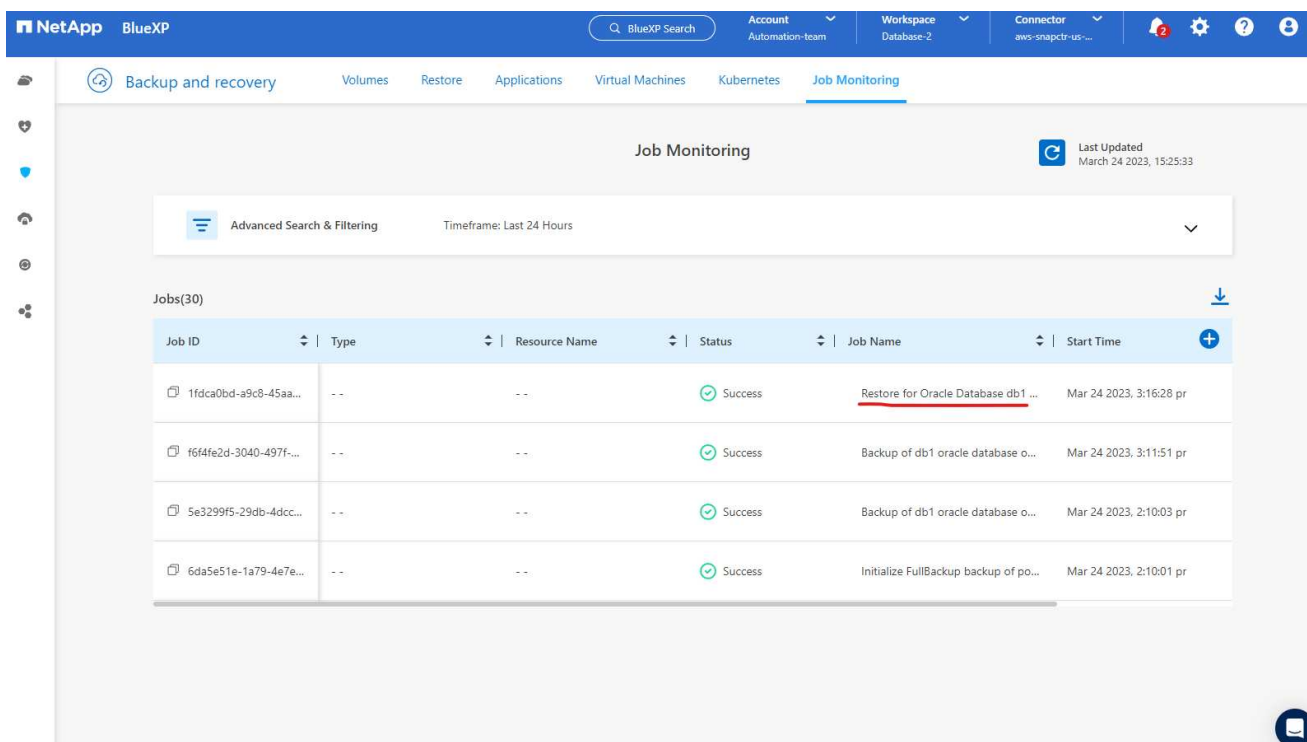
1. Scegliere l'impostazione di ripristino. Se dopo il backup non è cambiato nulla nella struttura fisica del database (ad esempio l'aggiunta di un file di dati o di un gruppo di dischi), è possibile utilizzare l'opzione **Force in Place restore** (Ripristino forzato in posizione), che in genere è più veloce. In caso contrario, non selezionare questa casella.

The screenshot shows the 'Restore "db1"' dialog box in the NetApp BlueXP interface. The 'Restore Settings' tab is selected. Under 'Restore Scope', the 'All Data Files' option is selected, and 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.

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



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



NetApp BlueXP

BlueXP Search

AccountAutomation team

WorkspaceDatabase-2

Connectoraws-snapctr-us-...

2

?

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Job Monitoring > Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4

Job Details

Job Id: 1fdca0bd-a9c8-45aa-9d7a-05a07cb291f4

Expand All

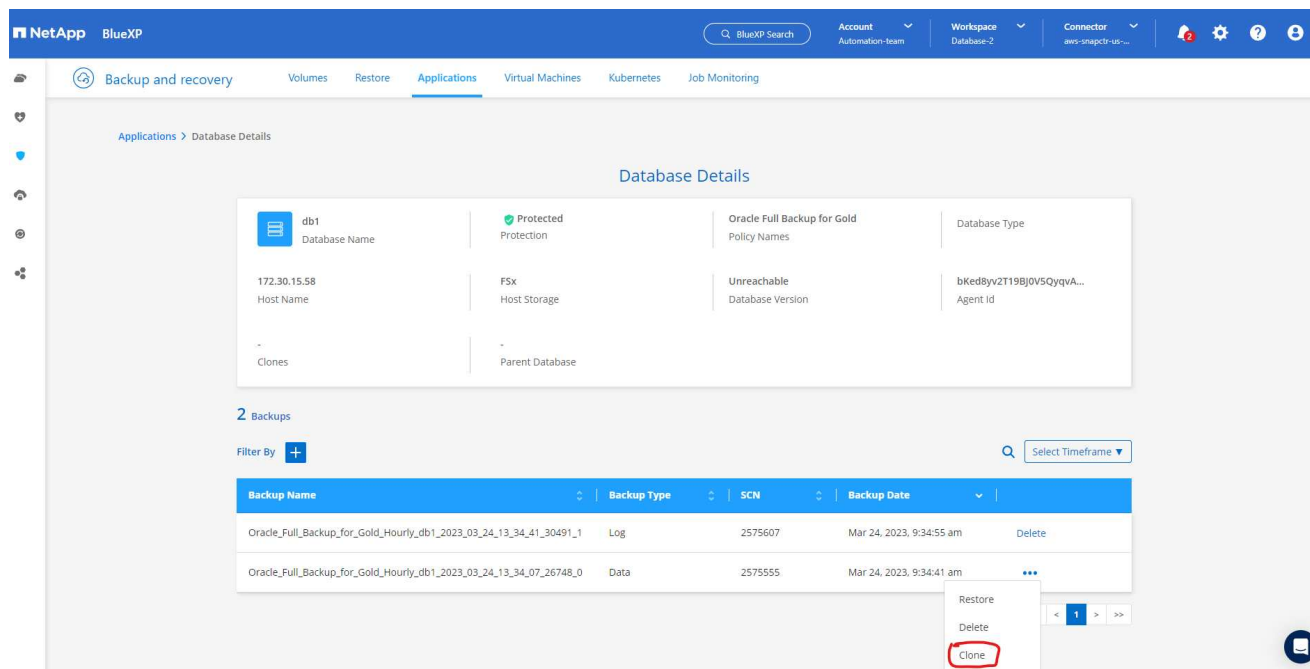
Sub-Jobs(6)

Job Name	Job ID	Start Time	End Time	Duration
Restore for Oracle Database db1 using backup ...	1fdca0bd-a9c8-45aa-9d...	Mar 24 2023, 3:16:28 pm	Mar 24 2023, 3:23:33 pm	7 Minutes
Post Restore Cleanup	2096a8e4-889d-4b2a-9...	Mar 24 2023, 3:23:18 pm	Mar 24 2023, 3:23:32 pm	14 Seconds
Post Restore	fb7b1171-9f6f-4228-9e...	Mar 24 2023, 3:20:06 pm	Mar 24 2023, 3:23:19 pm	3 Minutes
Restore	0f4580d0-6598-458b-a7...	Mar 24 2023, 3:17:49 pm	Mar 24 2023, 3:20:07 pm	2 Minutes

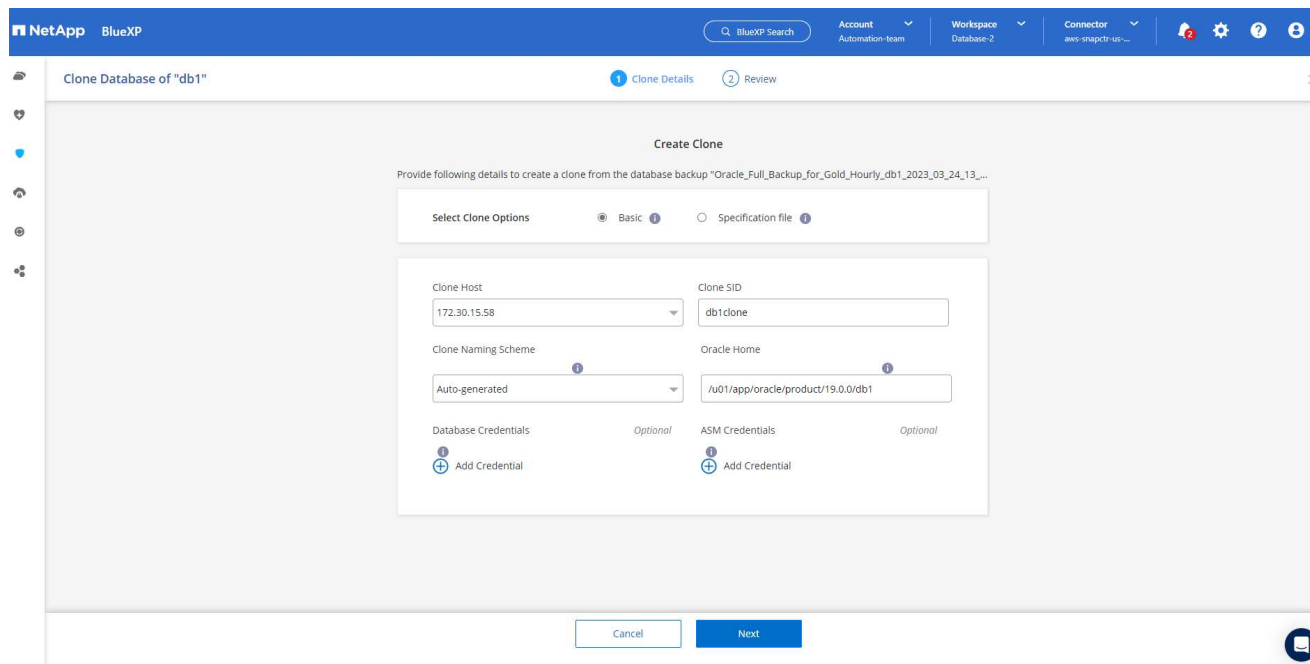
Clone del database Oracle

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

1. Selezionare la copia di backup del database corretta, fare clic sui tre punti per visualizzare il menu e scegliere l'opzione **Clone**.



1. Selezionare l'opzione **Basic** se non è necessario modificare i parametri del database clonati.



1. In alternativa, selezionare **Specification file**, che consente di scaricare il file init corrente, apportare modifiche e quindi caricarlo nuovamente nel lavoro.

NetApp BlueXP

BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...

Clone Database of "db1"

1 Clone Details

2 Review

Create Clone

Provide following details to create a clone from the database backup "Oracle\_Full\_Backup\_for\_Gold\_Weekly\_db1\_2023\_03\_24\_19..."

Select Clone Options

☐ Basic
 ☒ Specification file

Generate specification file to modify input parameters and use for clone.

Download File

Specification File

db1\_3\_24\_2023\_10\_14\_spec.json

Browse

Clone Host

172.30.15.58

Clone SID

db1clone

Database Credentials

Optional

Add Credential

ASM Credentials

Optional

Add Credential

Cancel

Next

1. Esaminare e avviare il lavoro.

NetApp BlueXP

BlueXP Search

Account Automation team

Workspace Database-2

Connector aws-snapctr-us...

Clone Database of "db1"

1 Clone Details

2 Review

Review

General	Database parameters
Backup Name	Oracle_Full_Backup_for_Gold_Hourly_db1_2023_03_24_13_34_07_26748_0
Clone SID	db1clone
Clone Host	172.30.15.58
Datafile locations	DATA_db1clone
Control files	+DATA_db1clone/db1clone/control/control01.ctl
Redo logs	RedoGroup = 1 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redolog/redo01_01.log RedoGroup = 2 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redolog/redo02_01.log RedoGroup = 3 TotalSize = 1024 Path = +DATA_db1clone/db1clone/redolog/redo03_01.log
Recovery scope	Until cancel using selected backup's archive logs

Previous

Clone

1. Controllare lo stato del lavoro di clonazione dalla scheda **Job Monitoring**.

111

NetAppBlueXP

BlueXP Search

AccountAutomation-team

WorkspaceDatabase-2

Connectoraws-snapc1r-108-...

Backup and recovery

Volumes

Restore

Applications

Virtual Machines

Kubernetes

Job Monitoring

Job Monitoring > Job Id: cd30abaf-fbe2-4052-a6db-4bf965a8d29b

Job Details

Job Id: cd30abaf-fbe2-4052-a6db-4bf965a8d29b

Expand All

Sub-Jobs(2)

Job Name	Job ID	Start Time	End Time	Duration
Cloning Oracle Database db1 as db1clone on h...	cd30abaf-fbe2-4052-a6...	Mar 24 2023, 1:30:36 pm		--
Running pre scripts	51f152c1-853a-4ec6-a4f...	Mar 24 2023, 1:30:41 pm	Mar 24 2023, 1:30:41 pm	0 Second
Validating clone request	f93a6c44-2eb2-4c5e-9f...	Mar 24 2023, 1:30:35 pm	Mar 24 2023, 1:30:42 pm	7 Seconds

1. Convalidare il database clonato sull'host dell'istanza EC2.

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

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

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

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

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

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

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

```
SQL>
```

## Ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo 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 di backup e ripristino BlueXP

["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 per NetApp 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-8225-4784bcd9843&sc\\_channel=ps&s\\_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef\\_id=Cj0KCQiA54KfBhCKARIsAjzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw\\_wcB:G:s&s\\_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2](https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bcd9843&sc_channel=ps&s_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAjzSrdqwQrghn6l71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwid=AL!4422!3!467723097970!e!!g!!aws%20ec2)

## Soluzioni di database per il cloud ibrido con SnapCenter

### TR-4908: Panoramica delle soluzioni di database per il cloud ibrido con SnapCenter

Alan Cao, Felix Meligan, NetApp

Questa soluzione fornisce ai clienti e al campo NetApp istruzioni e istruzioni per la configurazione, il funzionamento e la migrazione dei database in un ambiente di cloud ibrido utilizzando lo strumento basato sull'interfaccia grafica di NetApp SnapCenter e il servizio di storage CVO di NetApp nei cloud pubblici per i seguenti casi di utilizzo:

- Operazioni di sviluppo/test del database nel cloud ibrido
- Disaster recovery del database nel cloud ibrido

Oggi, molti database aziendali risiedono ancora in data center aziendali privati per motivi di performance, sicurezza e/o altro. Questa soluzione di database per il cloud ibrido consente alle aziende di gestire i propri database primari on-site utilizzando un cloud pubblico per le operazioni di sviluppo/test dei database e per il disaster recovery per ridurre i costi operativi e di licenza.

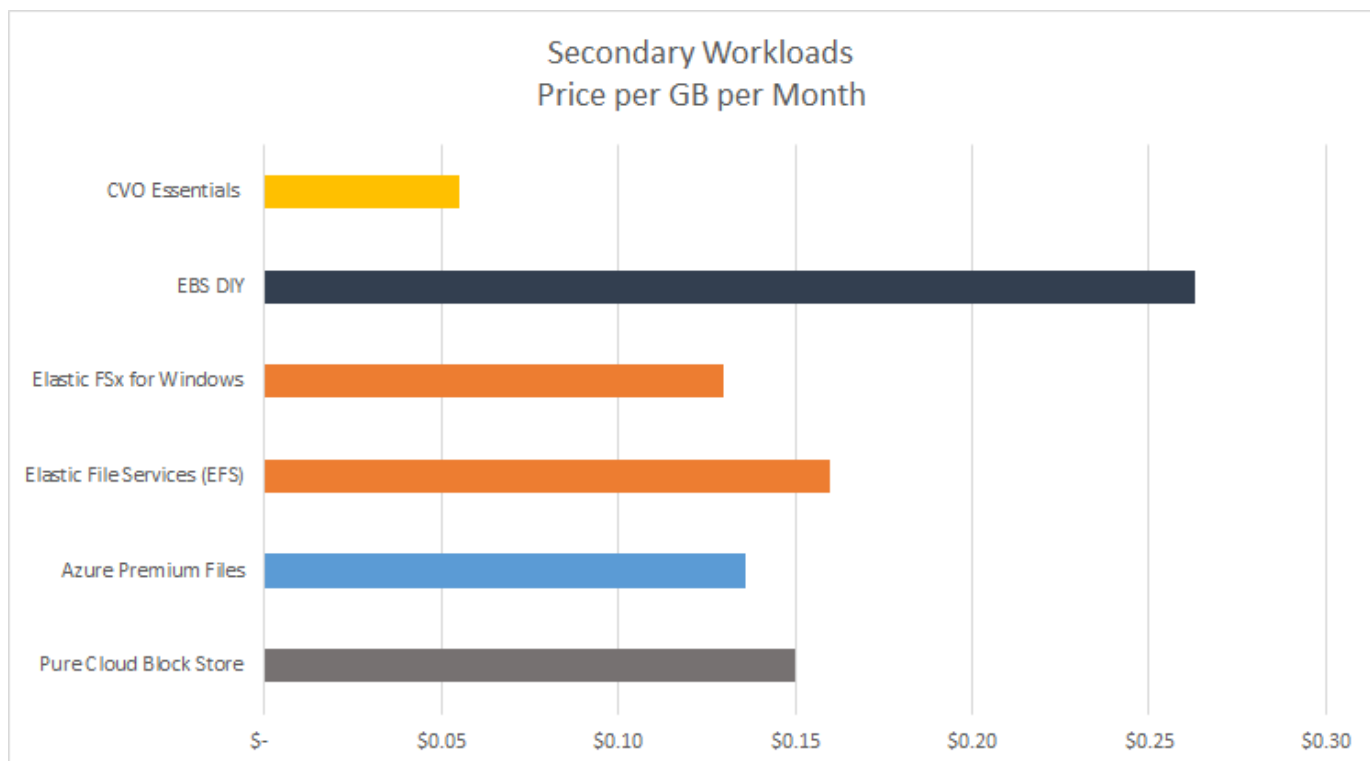
Molti database aziendali, come Oracle, SQL Server, SAP HANA e così via, costi operativi e di licenza elevati. Molti clienti pagano una quota di licenza a tantum e i costi di supporto annuali in base al numero di core di calcolo nel proprio ambiente di database, indipendentemente dal fatto che i core siano utilizzati per lo sviluppo, il test, la produzione o il disaster recovery. Molti di questi ambienti potrebbero non essere completamente utilizzati durante l'intero ciclo di vita dell'applicazione.

Le soluzioni offrono ai clienti l'opzione di ridurre potenzialmente il numero di core licenziabili spostando nel cloud gli ambienti di database dedicati allo sviluppo, al test o al disaster recovery. Utilizzando la scalabilità del cloud pubblico, la ridondanza, l'alta disponibilità e un modello di fatturazione basato sui consumi, il risparmio



sui costi per le licenze e le operazioni può essere sostanziale, senza sacrificare l'usabilità o la disponibilità delle applicazioni.

Oltre ai potenziali risparmi sui costi di licenza dei database, il modello di licenza CVO basato sulla capacità di NetApp consente ai clienti di risparmiare sui costi di storage per GB, offrendo al contempo un elevato livello di gestibilità dei database che non è disponibile dai servizi di storage della concorrenza. Il grafico seguente mostra un confronto dei costi di storage dei più diffusi servizi di storage disponibili nel cloud pubblico.



Questa soluzione dimostra che, utilizzando lo strumento software basato su interfaccia grafica e la tecnologia SnapCenter SnapMirror, è possibile configurare, implementare e gestire in modo semplice le operazioni di database del cloud ibrido.

I seguenti video mostrano SnapCenter in azione:

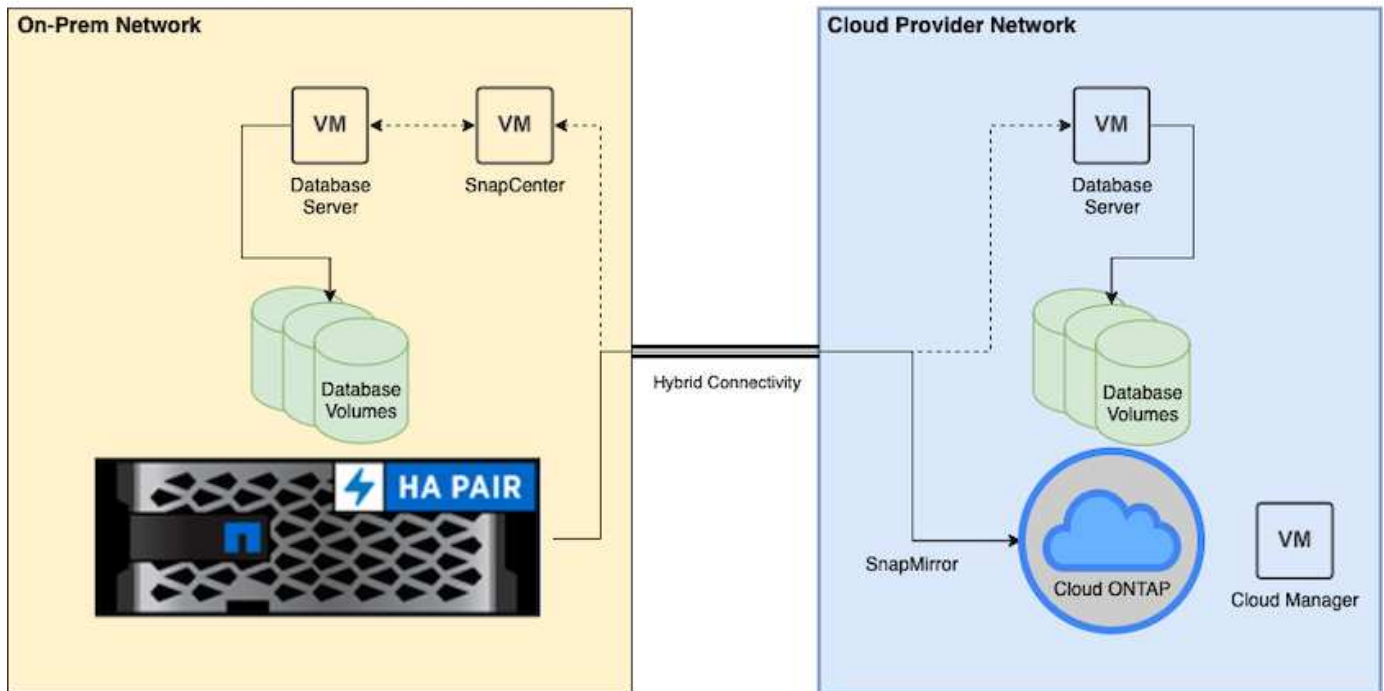
- ["Backup di un database Oracle su un cloud ibrido utilizzando SnapCenter"](#)
- ["SnapCenter - Clona SVILUPPO/TEST su cloud AWS per un database Oracle"](#)

In particolare, sebbene le illustrazioni di questo documento mostrino CVO come istanza di storage di destinazione nel cloud pubblico, la soluzione è anche pienamente validata per la nuova release del motore di storage FSX ONTAP per AWS.

Per testare la soluzione e i casi di utilizzo, è possibile richiedere un NetApp Lab-on-Demand SL10680 al seguente xref: [./databases/ TL\\_AWS\\_004 HCoD: AWS - NW,SnapCenter\(OnPrem\)](#).

## Architettura della soluzione

Il seguente diagramma dell'architettura illustra un'implementazione tipica del funzionamento del database aziendale in un cloud ibrido per le operazioni di sviluppo/test e disaster recovery.



Nelle normali operazioni di business, i volumi di database sincronizzati nel cloud possono essere clonati e montati su istanze di database di sviluppo/test per lo sviluppo o il test delle applicazioni. In caso di guasto, i volumi di database sincronizzati nel cloud possono essere attivati per il disaster recovery.

## Requisiti SnapCenter

Questa soluzione è progettata in un ambiente di cloud ibrido per supportare i database di produzione on-premise che possono esplodere in tutti i cloud pubblici più diffusi per le operazioni di sviluppo/test e disaster recovery.

Questa soluzione supporta tutti i database attualmente supportati da SnapCenter, anche se qui vengono dimostrati solo i database Oracle e SQL Server. Questa soluzione è validata con carichi di lavoro di database virtualizzati, sebbene siano supportati anche i carichi di lavoro bare-metal.

Supponiamo che i server di database in produzione siano ospitati on-premise con volumi DB presentati agli host DB da un cluster di storage ONTAP. Il software SnapCenter viene installato on-premise per il backup del database e la replica dei dati nel cloud. Un controller Ansible è consigliato ma non richiesto per l'automazione dell'implementazione del database o per la sincronizzazione della configurazione del kernel e del database del sistema operativo con un'istanza di DR di standby o istanze di sviluppo/test nel cloud pubblico.

## Requisiti

Ambiente	Requisiti
On-premise	Qualsiasi database e versione supportati da SnapCenter
	SnapCenter v4.4 o superiore
	Ansible v2.09 o superiore
	Cluster ONTAP 9.x
	LIF intercluster configurati
	Connettività da on-premise a un VPC cloud (VPN, interconnessione e così via)
	Porte di rete aperte - ssh 22 - tcp 8145, 8146, 10000, 11104, 11105
Cloud - AWS	"Connettore Cloud Manager"
	"Cloud Volumes ONTAP"
	Corrispondenza delle istanze DB OS EC2 con quelle on-premise
Cloud - Azure	"Connettore Cloud Manager"
	"Cloud Volumes ONTAP"
	Abbinamento delle macchine virtuali DB OS Azure alle macchine virtuali on-premise
Cloud - GCP	"Connettore Cloud Manager"
	"Cloud Volumes ONTAP"
	Corrispondenza delle istanze di DB OS Google Compute Engine con quelle on-premise

## Configurazione dei prerequisiti

Alcuni prerequisiti devono essere configurati sia on-premise che nel cloud prima dell'esecuzione dei carichi di lavoro del database del cloud ibrido. La sezione seguente fornisce un riepilogo generale di questo processo e i seguenti collegamenti forniscono ulteriori informazioni sulla configurazione di sistema necessaria.

### On-premise

- Installazione e configurazione di SnapCenter
- Configurazione dello storage del server di database on-premise
- Requisiti di licenza
- Networking e sicurezza
- Automazione

### Cloud pubblico

- Accesso a NetApp Cloud Central
- Accesso alla rete da un browser Web a diversi endpoint
- Percorso di rete per un connettore

- Permessi del cloud provider
- Networking per singoli servizi

Considerazioni importanti:

1. Dove implementare Cloud Manager Connector?
2. Dimensionamento e architettura di Cloud Volume ONTAP
3. Nodo singolo o alta disponibilità?

I seguenti link forniscono ulteriori dettagli:

["On-premise"](#)

["Cloud pubblico"](#)

### Prerequisiti on-premise

Le seguenti attività devono essere completate on-premise per preparare l'ambiente di carico di lavoro del database del cloud ibrido SnapCenter.

#### Installazione e configurazione di SnapCenter

Il tool NetApp SnapCenter è un'applicazione basata su Windows che in genere viene eseguita in un ambiente di dominio Windows, anche se è possibile implementare un gruppo di lavoro. Si basa su un'architettura a più livelli che include un server di gestione centralizzato (il server SnapCenter) e un plug-in SnapCenter sugli host del server di database per i carichi di lavoro del database. Ecco alcune considerazioni chiave per l'implementazione del cloud ibrido.

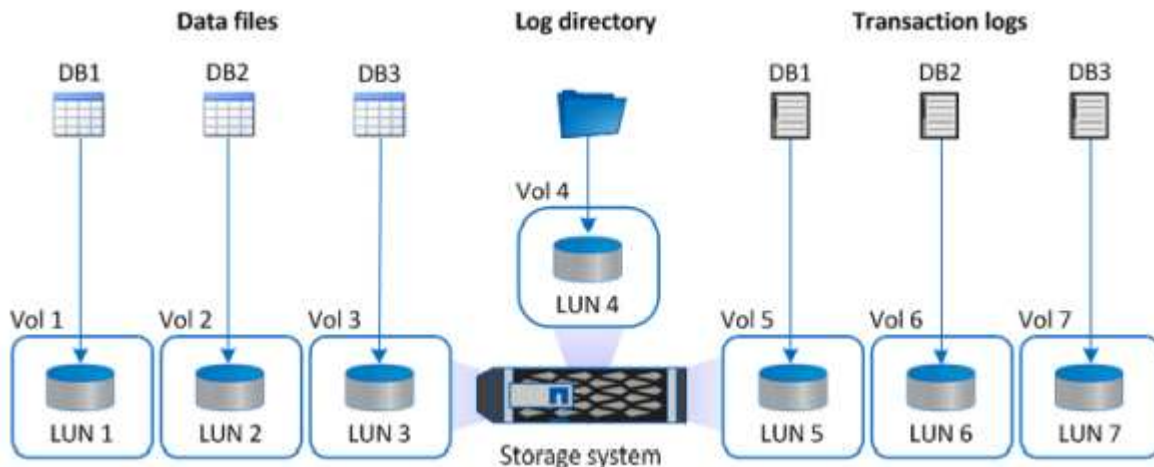
- **Implementazione ha o istanza singola.** l'implementazione ha fornisce ridondanza in caso di guasto di un singolo server di istanza SnapCenter.
- **Risoluzione del nome.** il DNS deve essere configurato sul server SnapCenter per risolvere tutti gli host di database e sulla SVM di storage per la ricerca in avanti e indietro. Il DNS deve essere configurato anche sui server di database per risolvere il server SnapCenter e la SVM di storage per la ricerca in avanti e in retromarcia.
- **Configurazione RBAC (role-based access control).** per i carichi di lavoro di database misti, è possibile utilizzare RBAC per separare la responsabilità di gestione per diverse piattaforme di database, ad esempio un amministratore per database Oracle o un amministratore per SQL Server. Le autorizzazioni necessarie devono essere concesse all'utente amministratore del database.
- **Attivare una strategia di backup basata su policy.** per garantire la coerenza e l'affidabilità del backup.
- **Aprire le porte di rete necessarie sul firewall.** per consentire al server SnapCenter on-premise di comunicare con gli agenti installati nell'host del DB cloud.
- **Le porte devono essere aperte per consentire il traffico SnapMirror tra cloud pubblico e on-premise.** il server SnapCenter si affida a SnapMirror di ONTAP per replicare i backup Snapshot in loco sulle SVM di storage CVO nel cloud.

Dopo un'attenta pianificazione e valutazione della preinstallazione, fare clic su questa opzione ["Workflow di installazione di SnapCenter"](#) Per informazioni dettagliate sull'installazione e la configurazione di SnapCenter.

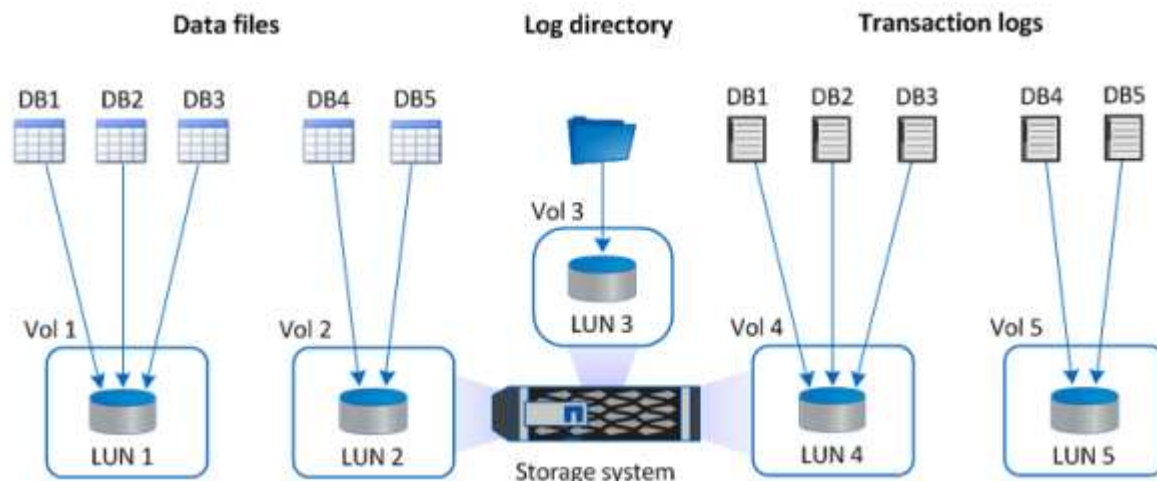
## Configurazione dello storage del server di database on-premise

Le performance dello storage giocano un ruolo importante nelle performance generali di database e applicazioni. Un layout dello storage ben progettato non solo può migliorare le performance del database, ma anche semplificare la gestione del backup e ripristino del database. Durante la definizione del layout dello storage, è necessario prendere in considerazione diversi fattori, tra cui la dimensione del database, il tasso di variazione dei dati previsti per il database e la frequenza con cui vengono eseguiti i backup.

Il collegamento diretto delle LUN di storage alla macchina virtuale guest tramite NFS o iSCSI per carichi di lavoro di database virtualizzati offre generalmente performance migliori rispetto allo storage allocato tramite VMDK. NetApp consiglia il layout dello storage per un database SQL Server di grandi dimensioni su LUN, illustrato nella figura seguente.



La figura seguente mostra il layout di storage consigliato da NetApp per database SQL Server di piccole o medie dimensioni su LUN.



La directory Log è dedicata a SnapCenter per eseguire il rollup del log delle transazioni per il ripristino del database. Per un database di grandi dimensioni, è possibile allocare più LUN a un volume per migliorare le performance.

Per i carichi di lavoro dei database Oracle, SnapCenter supporta ambienti di database supportati dallo storage ONTAP montato sull'host come dispositivi fisici o virtuali. È possibile ospitare l'intero database su uno o più dispositivi di storage in base alla criticità dell'ambiente. In genere, i clienti isolano i file di dati sullo storage dedicato da tutti gli altri file, ad esempio file di controllo, file di ripristino e file di log di archiviazione. In questo

modo, gli amministratori possono eseguire rapidamente il ripristino (ONTAP single-file SnapRestore) o clonare un database critico di grandi dimensioni (scala di petabyte) utilizzando la tecnologia Snapshot in pochi secondi o minuti.



Per i carichi di lavoro mission-critical sensibili alla latenza, è necessario implementare un volume di storage dedicato a diversi tipi di file Oracle per ottenere la migliore latenza possibile. Per un database di grandi dimensioni, è necessario allocare più LUN (NetApp consiglia fino a otto) per volume ai file di dati.



Per i database Oracle più piccoli, SnapCenter supporta layout di storage condivisi in cui è possibile ospitare più database o parte di un database sullo stesso volume di storage o LUN. Come esempio di questo layout, è possibile ospitare file di dati per tutti i database su un gruppo di dischi +DATA ASM o un gruppo di volumi. Il resto dei file (redo, log di archiviazione e file di controllo) può essere ospitato su un altro gruppo di dischi o un gruppo di volumi dedicato (LVM). Di seguito viene illustrato uno scenario di implementazione di questo tipo.



Per facilitare il trasferimento dei database Oracle, il file binario Oracle deve essere installato su un LUN separato incluso nella normale policy di backup. In questo modo, in caso di trasferimento del database su un nuovo host server, lo stack Oracle può essere avviato per il ripristino senza potenziali problemi dovuti a un binario Oracle non sincronizzato.

#### Requisiti di licenza

SnapCenter è un software concesso in licenza da NetApp. Generalmente è incluso in una licenza ONTAP on-premise. Tuttavia, per l'implementazione del cloud ibrido, è necessaria anche una licenza cloud per SnapCenter per aggiungere CVO a SnapCenter come destinazione di replica dei dati di destinazione. Per ulteriori informazioni, consultare i seguenti collegamenti per la licenza basata sulla capacità standard di SnapCenter:

["Licenze standard SnapCenter basate sulla capacità"](#)

## Networking e sicurezza

In un'operazione di database ibrido che richiede un database di produzione on-premise che sia burstable nel cloud per lo sviluppo/test e il disaster recovery, il networking e la sicurezza sono fattori importanti da prendere in considerazione durante la configurazione dell'ambiente e la connessione al cloud pubblico da un data center on-premise.

I cloud pubblici in genere utilizzano un cloud privato virtuale (VPC) per isolare diversi utenti all'interno di una piattaforma di cloud pubblico. All'interno di un singolo VPC, la sicurezza viene controllata mediante misure come i gruppi di sicurezza configurabili in base alle esigenze dell'utente per il blocco di un VPC.

La connettività dal data center on-premise al VPC può essere protetta attraverso un tunnel VPN. Sul gateway VPN, la sicurezza può essere potenziata utilizzando le regole NAT e firewall che bloccano i tentativi di stabilire connessioni di rete dagli host su Internet agli host all'interno del data center aziendale.

Per considerazioni relative a networking e sicurezza, consulta le regole CVO in entrata e in uscita per il tuo cloud pubblico preferito:

- ["Regole del gruppo di sicurezza per CVO - AWS"](#)
- ["Regole del gruppo di sicurezza per CVO - Azure"](#)
- ["Regole firewall per CVO - GCP"](#)

### Utilizzo di Ansible Automation per sincronizzare istanze di DB tra on-premise e cloud - opzionale

Per semplificare la gestione di un ambiente di database di cloud ibrido, NetApp consiglia, ma non richiede, di implementare un controller Ansible per automatizzare alcune attività di gestione, ad esempio mantenendo le istanze di calcolo on-premise e nel cloud sincronizzate. Questo è particolarmente importante perché un'istanza di calcolo fuori sincronizzazione nel cloud potrebbe rendere il database recuperato nel cloud soggetto a errori a causa di pacchetti del kernel mancanti e di altri problemi.

La funzionalità di automazione di un controller Ansible può anche essere utilizzata per aumentare il SnapCenter per determinate attività, come la rottura dell'istanza di SnapMirror per attivare la copia dei dati DR per la produzione.

Seguire queste istruzioni per configurare il nodo di controllo Ansible per le macchine RedHat o CentOS: ["RedHat/CentOS Ansible Controller Setup"](#). Seguire queste istruzioni per configurare il nodo di controllo Ansible per le macchine Ubuntu o Debian: ["Installazione di Ubuntu/Debian Ansible Controller"](#).

## Prerequisiti per il cloud pubblico

Prima di installare Cloud Manager Connector e Cloud Volumes ONTAP e configurare SnapMirror, è necessario eseguire alcune operazioni di preparazione per il nostro ambiente cloud. In questa pagina vengono descritte le operazioni da eseguire e le considerazioni da tenere in considerazione durante l'implementazione di Cloud Volumes ONTAP.

### Elenco di controllo dei prerequisiti per l'implementazione di Cloud Manager e Cloud Volumes ONTAP

- Accesso a NetApp Cloud Central
- Accesso alla rete da un browser Web a diversi endpoint
- Percorso di rete per un connettore
- Permessi del cloud provider



- Networking per singoli servizi

Per ulteriori informazioni su ciò di cui hai bisogno per iniziare, visita il nostro ["documentazione cloud"](#).

## Considerazioni

### 1. Che cos'è un connettore Cloud Manager?

Nella maggior parte dei casi, un amministratore dell'account Cloud Central deve implementare un connettore nel cloud o nella rete on-premise. Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente di cloud pubblico.

Per ulteriori informazioni sui connettori, visita il nostro ["documentazione cloud"](#).

### 2. Dimensionamento e architettura Cloud Volumes ONTAP

Durante l'implementazione di Cloud Volumes ONTAP, è possibile scegliere un pacchetto predefinito o la creazione di una propria configurazione. Sebbene molti di questi valori possano essere modificati in seguito senza interruzioni, è necessario prendere alcune decisioni chiave prima dell'implementazione in base ai carichi di lavoro da implementare nel cloud.

Ogni cloud provider dispone di diverse opzioni per l'implementazione e quasi tutti i workload hanno proprietà esclusive. NetApp dispone di un ["Tool di dimensionamento CVO"](#) questo può aiutare a dimensionare correttamente le implementazioni in base a capacità e performance, ma è stato costruito attorno ad alcuni concetti di base che vale la pena considerare:

- Capacità richiesta
- Funzionalità di rete della macchina virtuale cloud
- Caratteristiche delle performance dello storage cloud

La chiave è pianificare una configurazione che non solo soddisfi gli attuali requisiti di capacità e performance, ma che guardi anche alla crescita futura. Questo è generalmente noto come spazio di crescita della capacità e spazio di crescita delle performance.

Per ulteriori informazioni, leggere la documentazione relativa alla pianificazione corretta per ["AWS"](#), ["Azure"](#), e ["GCP"](#).

### 3. Nodo singolo o alta disponibilità?

In tutti i cloud, è possibile implementare CVO in un singolo nodo o in una coppia ad alta disponibilità in cluster con due nodi. A seconda del caso di utilizzo, è possibile implementare un singolo nodo per risparmiare sui costi o una coppia ha per fornire ulteriore disponibilità e ridondanza.

Per un caso di utilizzo di DR o per lo storage temporaneo in fase di spinning per lo sviluppo e il test, i nodi singoli sono comuni poiché l'impatto di un'interruzione improvvisa dell'infrastruttura o di un'interruzione dell'infrastruttura è inferiore. Tuttavia, per qualsiasi caso di utilizzo in produzione, quando i dati si trovano in una sola posizione o quando il dataset deve avere maggiore ridondanza e disponibilità, si consiglia un'alta disponibilità.

Per ulteriori informazioni sull'architettura della versione ad alta disponibilità di ogni cloud, consulta la documentazione per ["AWS"](#), ["Azure"](#) e ["GCP"](#).



## Panoramica introduttiva

Questa sezione fornisce un riepilogo delle attività che devono essere completate per soddisfare i requisiti dei prerequisiti, come descritto nella sezione precedente. La sezione seguente fornisce un elenco di task di alto livello per le operazioni on-premise e di cloud pubblico. È possibile accedere ai processi e alle procedure dettagliate facendo clic sui relativi collegamenti.

### On-premise

- Configurare l'utente amministratore del database in SnapCenter
- Prerequisiti per l'installazione del plug-in SnapCenter
- Installazione del plug-in host SnapCenter
- Rilevamento delle risorse DB
- Configurare il peering del cluster di storage e la replica del volume DB
- Aggiunta di SVM per lo storage del database CVO a SnapCenter
- Impostare il criterio di backup del database in SnapCenter
- Implementare policy di backup per proteggere il database
- Validare il backup

### Cloud pubblico AWS

- Controllo prima del volo
- Passaggi per implementare Cloud Manager e Cloud Volumes ONTAP in AWS
- Implementare l'istanza di calcolo EC2 per il carico di lavoro del database

Per ulteriori informazioni, fare clic sui seguenti collegamenti:

["On-premise"](#), ["Cloud pubblico - AWS"](#)

### Introduzione on-premise

Il tool NetApp SnapCenter utilizza RBAC (role based access control) per gestire l'accesso alle risorse utente e le autorizzazioni concesse, mentre l'installazione di SnapCenter crea ruoli prepopolati. Puoi anche creare ruoli personalizzati in base alle tue esigenze o alle tue applicazioni.

#### On-premise

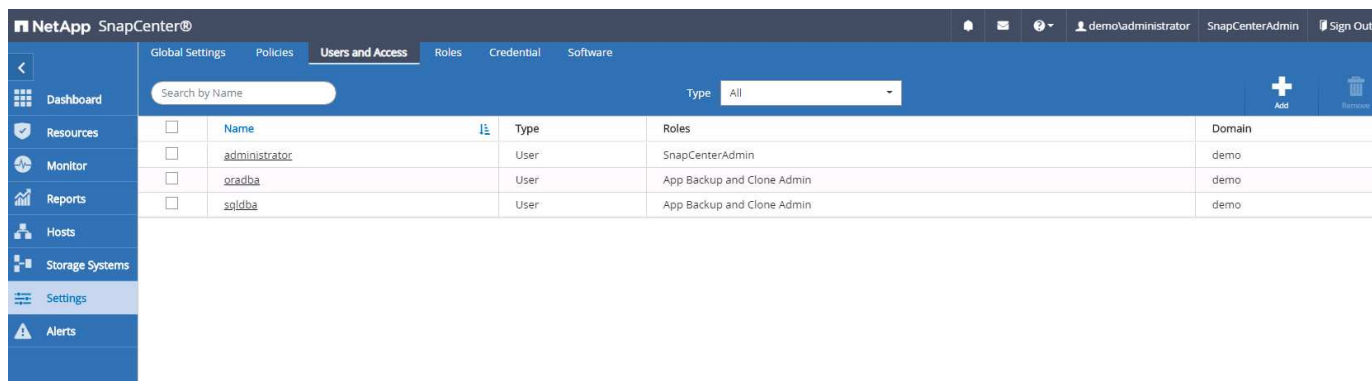
##### 1. Configurare l'utente amministratore del database in SnapCenter

È opportuno disporre di un ID utente admin dedicato per ciascuna piattaforma di database supportata da SnapCenter per il backup, il ripristino e/o il disaster recovery del database. È inoltre possibile utilizzare un unico ID per gestire tutti i database. Nei nostri test case e dimostrazioni, abbiamo creato un utente amministratore dedicato per Oracle e SQL Server, rispettivamente.

Alcune risorse SnapCenter possono essere fornite solo con il ruolo SnapCenterAdmin. Le risorse possono quindi essere assegnate ad altri ID utente per l'accesso.

In un ambiente SnapCenter on-premise preinstallato e configurato, le seguenti attività potrebbero essere già state completate. In caso contrario, i seguenti passaggi creano un utente amministratore del database:

1. Aggiungere l'utente amministratore a Windows Active Directory.
2. Accedere a SnapCenter utilizzando un ID concesso con il ruolo SnapCenterAdmin.
3. Accedere alla scheda Access (accesso) in Settings and Users (Impostazioni e utenti) e fare clic su Add (Aggiungi) per aggiungere un nuovo utente. Il nuovo ID utente è collegato all'utente amministratore creato in Active Directory di Windows nel passaggio 1. . Assegnare all'utente il ruolo appropriato in base alle necessità. Assegnare le risorse all'utente amministratore in base alle esigenze.



## 2. Prerequisiti per l'installazione del plug-in SnapCenter

SnapCenter esegue il backup, il ripristino, la clonazione e altre funzioni utilizzando un agente plug-in in esecuzione sugli host DB. Si connette all'host del database e al database tramite credenziali configurate nella scheda Impostazioni e credenziali per l'installazione del plug-in e altre funzioni di gestione. Esistono requisiti specifici per i privilegi in base al tipo di host di destinazione, ad esempio Linux o Windows, nonché al tipo di database.

Le credenziali DEGLI host DB devono essere configurate prima dell'installazione del plug-in SnapCenter. In genere, si desidera utilizzare account utente amministratore sull'host DB come credenziali di connessione host per l'installazione del plug-in. È inoltre possibile concedere lo stesso ID utente per l'accesso al database utilizzando l'autenticazione basata sul sistema operativo. D'altra parte, è possibile utilizzare l'autenticazione del database con diversi ID utente del database per l'accesso alla gestione del database. Se si decide di utilizzare l'autenticazione basata sul sistema operativo, l'ID utente amministratore del sistema operativo deve avere accesso al DB. Per l'installazione di SQL Server basata su dominio di Windows, è possibile utilizzare un account amministratore di dominio per gestire tutti gli SQL Server all'interno del dominio.

Host Windows per SQL Server:

1. Se si utilizzano credenziali Windows per l'autenticazione, è necessario impostare le credenziali prima di installare i plug-in.
2. Se si utilizza un'istanza di SQL Server per l'autenticazione, è necessario aggiungere le credenziali dopo l'installazione dei plug-in.
3. Se è stata attivata l'autenticazione SQL durante la configurazione delle credenziali, l'istanza o il database rilevato viene visualizzato con un'icona a forma di lucchetto rosso. Se viene visualizzata l'icona a forma di lucchetto, è necessario specificare le credenziali dell'istanza o del database per aggiungere correttamente l'istanza o il database a un gruppo di risorse.
4. È necessario assegnare la credenziale a un utente RBAC senza accesso sysadmin quando vengono soddisfatte le seguenti condizioni:

- La credenziale viene assegnata a un'istanza SQL.
- L'istanza o l'host SQL viene assegnato a un utente RBAC.
- L'utente amministratore DB RBAC deve disporre sia del gruppo di risorse che dei privilegi di backup.

Host UNIX per Oracle:

1. È necessario attivare la connessione SSH basata su password per l'utente root o non root modificando sshd.conf e riavviando il servizio sshd. L'autenticazione SSH basata su password sull'istanza di AWS è disattivata per impostazione predefinita.
2. Configurare i privilegi sudo per l'utente non root per l'installazione e l'avvio del processo di plug-in. Dopo aver installato il plug-in, i processi vengono eseguiti come utente root effettivo.
3. Creare le credenziali con la modalità di autenticazione Linux per l'utente di installazione.
4. È necessario installare Java 1.8.x (64 bit) sull'host Linux.
5. L'installazione del plug-in del database Oracle installa anche il plug-in SnapCenter per Unix.

### 3. Installazione del plug-in host SnapCenter

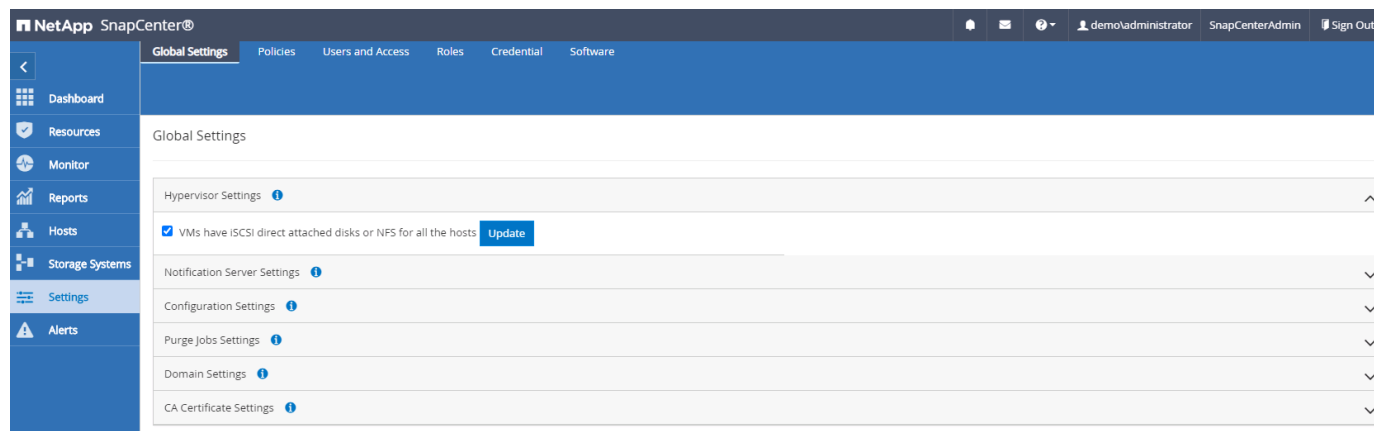


Prima di tentare di installare i plug-in SnapCenter sulle istanze del server DB cloud, assicurarsi che tutte le fasi di configurazione siano state completate come indicato nella relativa sezione cloud per l'implementazione dell'istanza di calcolo.

La seguente procedura illustra come aggiungere un host di database a SnapCenter mentre è installato un plug-in SnapCenter sull'host. La procedura si applica all'aggiunta di host on-premise e host cloud. La seguente dimostrazione aggiunge un host Windows o Linux residente in AWS.

### Configurare le impostazioni globali di SnapCenter

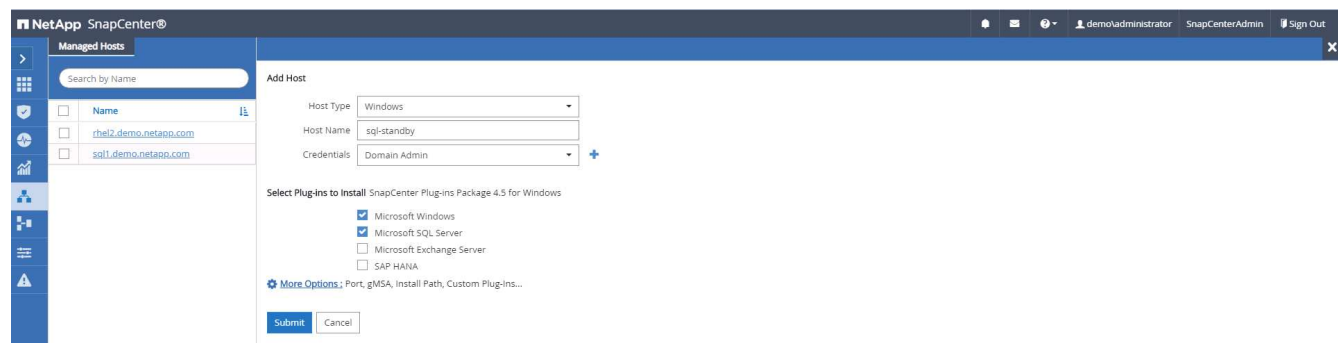
Accedere a Impostazioni > Impostazioni globali. Selezionare "VM con iSCSI direct attached disks o NFS per tutti gli host" in Impostazioni hypervisor e fare clic su Aggiorna.



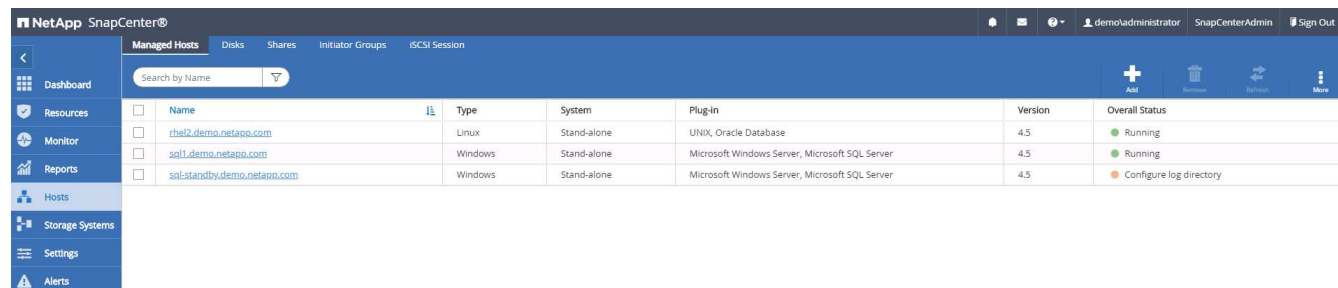
### Aggiungere l'host Windows e l'installazione del plug-in sull'host

1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda host dal menu a sinistra, quindi fare clic su Add (Aggiungi) per aprire il flusso di lavoro Add host (Aggiungi host).
3. Scegliere Windows come tipo di host; il nome host può essere un nome host o un indirizzo IP. Il nome host deve essere risolto con l'indirizzo IP host corretto dall'host SnapCenter. Scegliere le credenziali host create

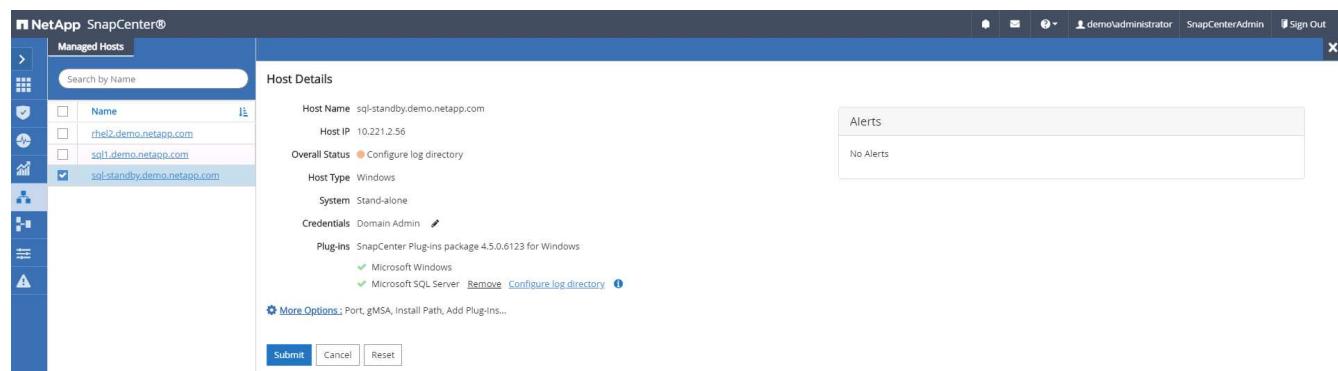
al punto 2. Scegliere Microsoft Windows e Microsoft SQL Server come pacchetti di plug-in da installare.



4. Una volta installato il plug-in su un host Windows, il relativo stato generale viene visualizzato come "Configure log directory" (Configura directory log).



5. Fare clic su host Name (Nome host) per aprire la configurazione della directory di log di SQL Server.



6. Fare clic su "Configure log directory" (Configura directory log) per aprire "Configure Plug-in for SQL Server" (Configura plug-in per SQL Server).

Configure Plug-in for SQL Server

Configure the log backup directory for sql-standby.demo.netapp.com

Configure host log directory

Host log directory

7. Fare clic su Browse (Sfoglia) per scoprire lo storage NetApp in modo da poter impostare una directory di log; SnapCenter utilizza questa directory di log per eseguire il rolloup dei file di log delle transazioni di SQL Server. Quindi fare clic su Save (Salva).


Configure Plug-in for SQL Server


Configure the log backup directory for sql-standby.demo.netapp.com


Configure host log directory

Host log directory

Choose directory on NetApp Storage

 sql-standby.demo.netapp.com

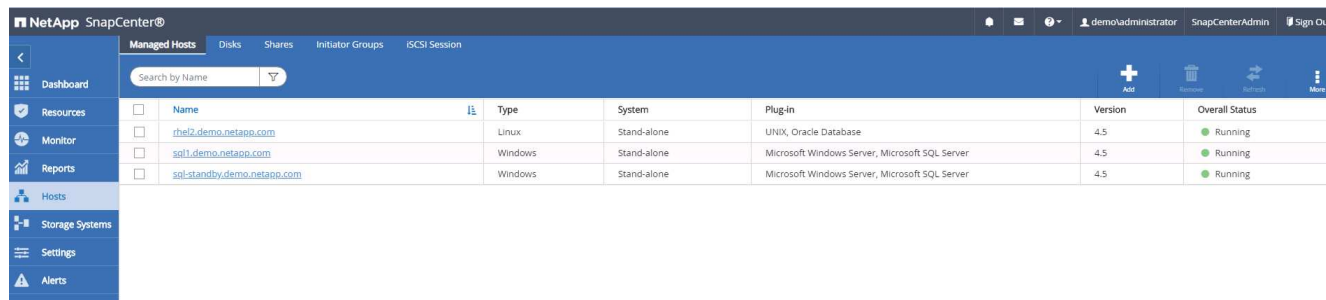
 G:\

 System Volume Information



Affinché lo storage NetApp fornito a un host DB venga rilevato, lo storage (on-premise o CVO) deve essere aggiunto a SnapCenter, come illustrato nella fase 6 per CVO come esempio.

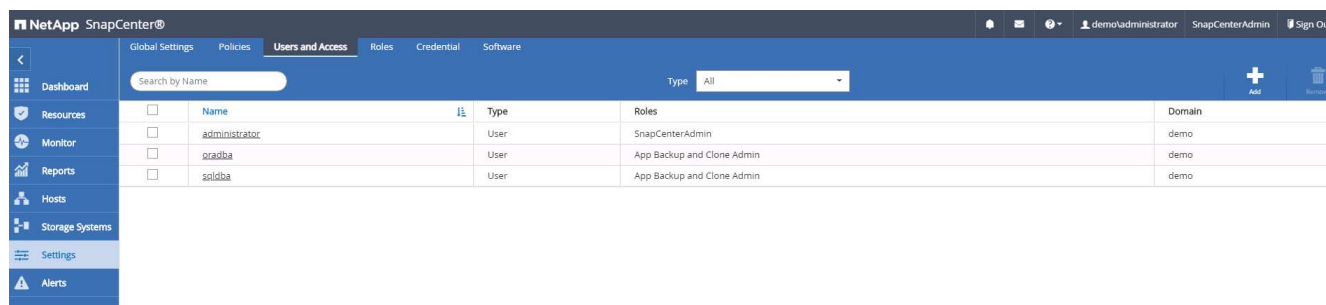
8. Una volta configurata la directory di log, lo stato generale del plug-in host di Windows viene modificato in in esecuzione.



The screenshot shows the NetApp SnapCenter interface with the 'Managed Hosts' tab selected. The table lists three hosts: 'rhel2.demo.netapp.com' (Linux, Stand-alone, UNIX, Oracle Database, Version 4.5, Running), 'sql1.demo.netapp.com' (Windows, Stand-alone, Microsoft Windows Server, Microsoft SQL Server, Version 4.5, Running), and 'sql-standby.demo.netapp.com' (Windows, Stand-alone, Microsoft Windows Server, Microsoft SQL Server, Version 4.5, Running).

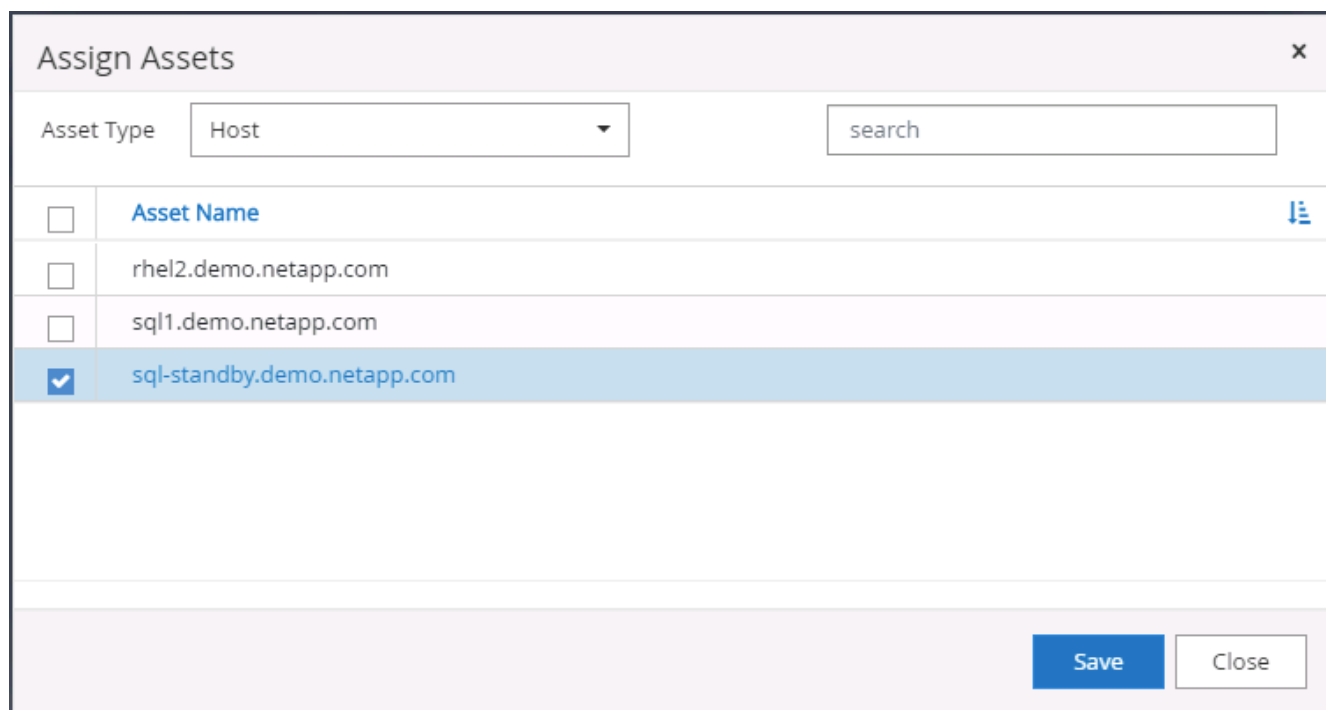
Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running

9. Per assegnare l'host all'ID utente per la gestione del database, accedere alla scheda Access (accesso) in Settings and Users (Impostazioni e utenti), fare clic sull'ID utente per la gestione del database (nel caso in cui sia necessario assegnare l'host all'host) e fare clic su Save (Salva) per completare l'assegnazione delle risorse host.



The screenshot shows the NetApp SnapCenter interface with the 'Users and Access' tab selected. The table lists three users: 'administrator' (User, SnapCenterAdmin, demo), 'oraoba' (User, App Backup and Clone Admin, demo), and 'sqloba' (User, App Backup and Clone Admin, demo).

Name	Type	Roles	Domain
administrator	User	SnapCenterAdmin	demo
oraoba	User	App Backup and Clone Admin	demo
sqloba	User	App Backup and Clone Admin	demo



The screenshot shows the 'Assign Assets' dialog box. The 'Asset Type' is set to 'Host'. The search bar is empty. The table lists three assets: 'rhel2.demo.netapp.com', 'sql1.demo.netapp.com', and 'sql-standby.demo.netapp.com'. The 'sql-standby.demo.netapp.com' asset is selected with a checkmark.

Asset Name
rhel2.demo.netapp.com
sql1.demo.netapp.com
sql-standby.demo.netapp.com

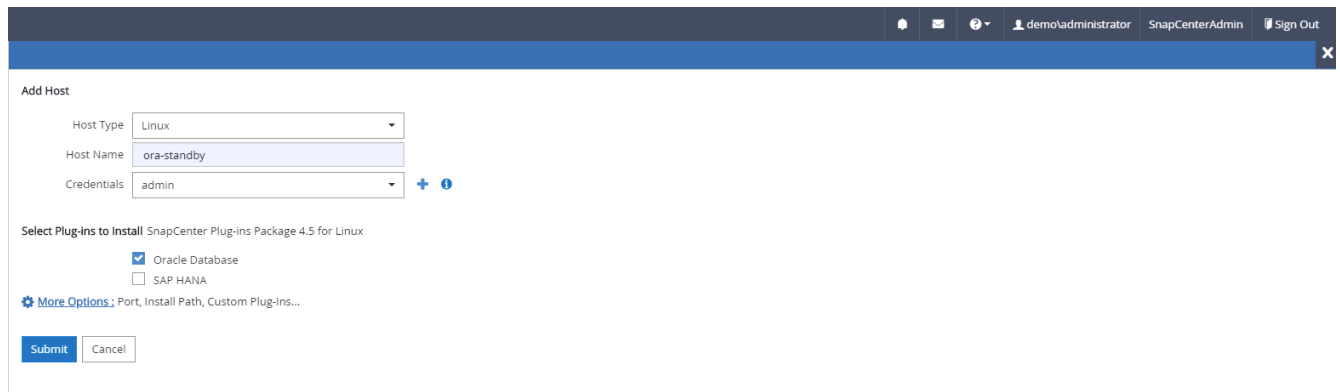
Save Close

## Aggiungere l'host Unix e l'installazione del plug-in sull'host

1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda host dal menu a sinistra, quindi fare clic su Add (Aggiungi) per aprire il flusso di

lavoro Add host (Aggiungi host).

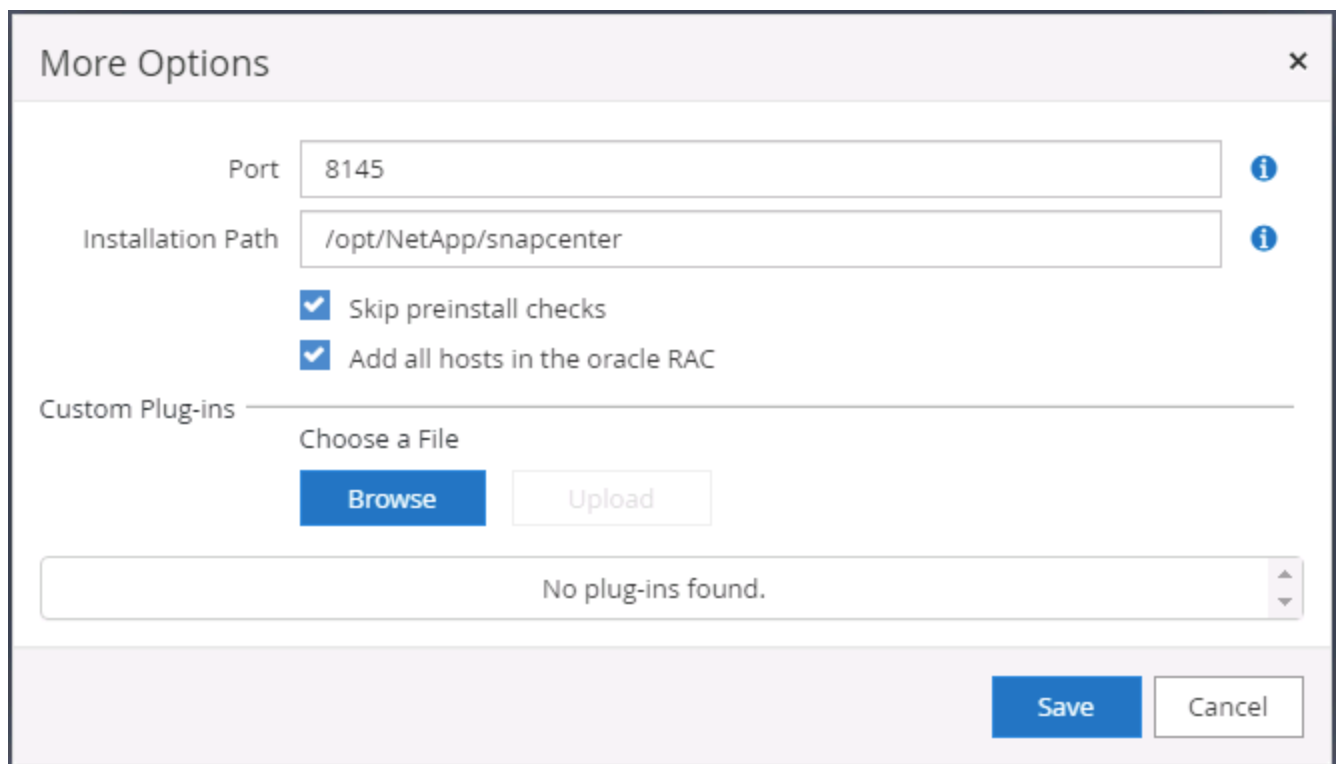
3. Scegliere Linux come tipo di host. Il nome host può essere il nome host o un indirizzo IP. Tuttavia, il nome host deve essere risolto per correggere l'indirizzo IP host dall'host SnapCenter. Scegliere le credenziali host create nel passaggio 2. Le credenziali host richiedono privilegi sudo. Selezionare Oracle Database come plug-in da installare, che installa sia i plug-in host Oracle che Linux.



The screenshot shows the 'Add Host' form in the SnapCenter Admin interface. The form is titled 'Add Host' and has a blue header bar with user information: 'demo\administrator', 'SnapCenterAdmin', and 'Sign Out'. The form contains the following fields and options:

- Host Type:** A dropdown menu with 'Linux' selected.
- Host Name:** A text input field with 'ora-standby' entered.
- Credentials:** A dropdown menu with 'admin' selected.
- Select Plug-ins to Install:** A section titled 'SnapCenter Plug-ins Package 4.5 for Linux' with two checkboxes: 'Oracle Database' (checked) and 'SAP HANA' (unchecked).
- More Options:** A link labeled 'More Options: Port, Install Path, Custom Plug-ins...'.
- Buttons:** 'Submit' and 'Cancel' buttons at the bottom.

4. Fare clic su altre opzioni e selezionare "Ignora controlli di preinstallazione". Viene richiesto di confermare l'omissione del controllo di preinstallazione. Fare clic su Sì, quindi su Salva.



The screenshot shows the 'More Options' dialog box in the SnapCenter Admin interface. The dialog has a title bar 'More Options' and a close button (X). The form contains the following fields and options:

- Port:** A text input field with '8145' entered.
- Installation Path:** A text input field with '/opt/NetApp/snapcenter' entered.
- Checkboxes:** 'Skip preinstall checks' (checked) and 'Add all hosts in the oracle RAC' (checked).
- Custom Plug-ins:** A section with a 'Choose a File' label and two buttons: 'Browse' and 'Upload'.
- Message:** A text area displaying 'No plug-ins found.'
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

5. Fare clic su Submit (Invia) per avviare l'installazione del plug-in. Viene richiesto di confermare l'impronta digitale come mostrato di seguito.

Confirm Fingerprint

Authenticity of the host cannot be determined

Host name	Fingerprint	Valid
ora-standby.demo.netapp.com	ssh-rsa 3072 5C:02:EF:6B:63:54:59:10:84:DF:4D:6B:AB:FB:61:67	

Confirm and Submit

Close

6. SnapCenter esegue la convalida e la registrazione dell'host, quindi il plug-in viene installato sull'host Linux. Lo stato cambia da Installing Plugin (Installazione del plug-in) a running (in esecuzione)

NetApp SnapCenter®							
<div>Managed Hosts</div> <div>Search by Name</div>							
	Name	Type	System	Plug-in	Version	Overall Status	
<input type="checkbox"/>	ora-standby.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
<input type="checkbox"/>	rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running	
<input type="checkbox"/>	sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	
<input type="checkbox"/>	sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running	

7. Assegnare l'host appena aggiunto all'ID utente corretto per la gestione del database (nel nostro caso, oradba).

NetApp SnapCenter®

Users and Access

Users/Groups Details

Search by Name

Name
administrator
<b>oradba</b>
sqlidba

User Name

Domain

Roles

Assign Assets

Asset Name	Type	Asset Type
10.0.0.1	DataOntapCluster	Storage Connection
192.168.0.101	DataOntapCluster	Storage Connection
admin		Credentials
Linux Admin		Credentials
Oracle Archive Log Backup		Policy
Oracle Full Online Backup		Policy
rhel2.demo.netapp.com		host

Submit

Cancel



Assign Assets

Asset Type
Host
search

<input type="checkbox"/>	Asset Name
<input checked="" type="checkbox"/>	ora-standby.demo.netapp.com
<input type="checkbox"/>	rhel2.demo.netapp.com
<input type="checkbox"/>	sql1.demo.netapp.com
<input type="checkbox"/>	sql-standby.demo.netapp.com

Save
Close

#### 4. Rilevamento delle risorse del database

Una volta completata l'installazione del plug-in, è possibile rilevare immediatamente le risorse del database sull'host. Fare clic sulla scheda Resources (risorse) nel menu a sinistra. A seconda del tipo di piattaforma di database, sono disponibili diverse visualizzazioni, ad esempio il database, il gruppo di risorse e così via. Se le risorse dell'host non vengono rilevate e visualizzate, potrebbe essere necessario fare clic sulla scheda Refresh Resources (Aggiorna risorse).

NetApp SnapCenter®

Oracle Database

View Database Search databases

Refresh Resources New Resource Group

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhel2.demo.netapp.com				Not protected

Dashboard
Resources
Monitor
Reports
Hosts
Storage Systems
Settings
Alerts

Quando il database viene rilevato inizialmente, lo stato generale viene visualizzato come "Not Protected" (non protetto). La schermata precedente mostra un database Oracle non ancora protetto da una policy di backup.

Quando viene impostata una configurazione o un criterio di backup ed è stato eseguito un backup, lo Stato generale del database mostra lo stato del backup come "Backup riuscito" e l'indicazione dell'ora dell'ultimo backup. La seguente schermata mostra lo stato del backup di un database utente SQL Server.

Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/14/2021 2:35:07 PM	Backup succeeded	User database

Se le credenziali di accesso al database non sono impostate correttamente, un pulsante di blocco rosso indica che il database non è accessibile. Ad esempio, se le credenziali Windows non dispongono dell'accesso sysadmin a un'istanza di database, è necessario riconfigurare le credenziali del database per sbloccare il blocco rosso.

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby.demo.netapp.com			Running	Standalone ()
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)

Name	Host	Resource Groups	Policies	State	Type
sql-standby	sql-standby	None	None	Not available for backup. DB is not on NetApp storage, auto-close is enabled or in recovery mode.	

Una volta configurate le credenziali appropriate a livello di Windows o di database, il blocco rosso scompare e le informazioni sul tipo di SQL Server vengono raccolte e riviste.

Name	Host	Resource Groups	Policies	State	Type
sql1	sql1.demo.netapp.com			Running	Standalone (15.0.2000)
sql-standby	sql-standby.demo.netapp.com			Running	Standalone (15.0.2000)

## 5. Configurare il peering del cluster di storage e la replica dei volumi DB

Per proteggere i dati del database on-premise utilizzando un cloud pubblico come destinazione di destinazione, i volumi di database del cluster ONTAP on-premise vengono replicati nel CVO del cloud utilizzando la tecnologia NetApp SnapMirror. I volumi di destinazione replicati possono quindi essere clonati per LO SVILUPPO/OPS o il disaster recovery. I seguenti passaggi di alto livello consentono di configurare il peering dei cluster e la replica dei volumi DB.

1. Configurare le LIF di intercluster per il peering dei cluster sia sul cluster on-premise che sull'istanza del cluster CVO. Questo passaggio può essere eseguito con Gestione sistema ONTAP. Un'implementazione CVO predefinita prevede la configurazione automatica di LIF tra cluster.

Cluster on-premise:

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type
onPrem-01_ic	✓		Default	192.168.0.113	onPrem-01	e0b		Intercluster
onPrem-01_mgmt1	✓		Default	192.168.0.111	onPrem-01	e0c		Cluster/Node Mgmt
cluster_mgmt	✓		Default	192.168.0.101	onPrem-01	e0a		Cluster/Node Mgmt

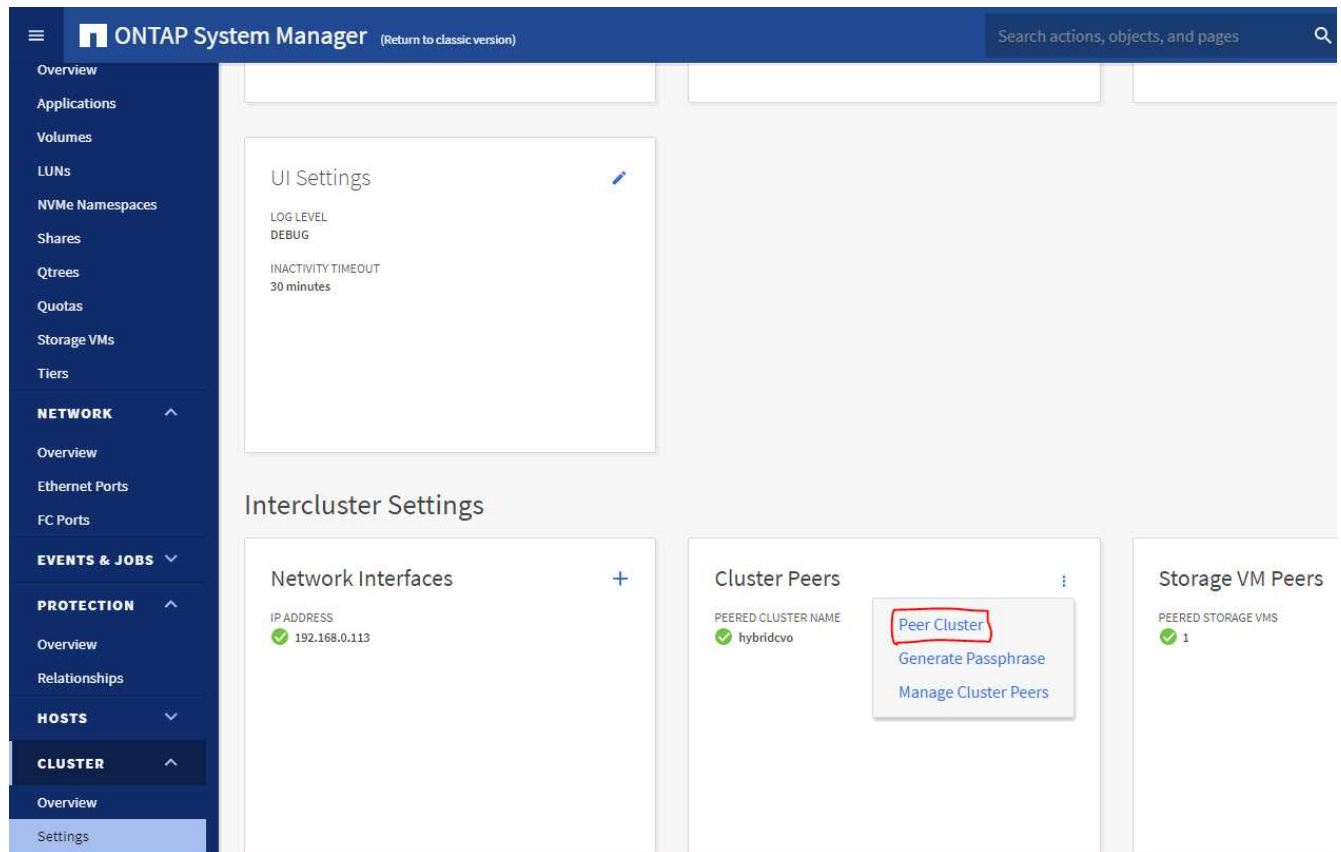
Cluster CVO di destinazione:

Name	Status	Storage VM	IPspace	Address	Current Node	Current Port	Protocols	Type	Throughput (I)
hybridcvo-02_mgmt1	✓		Default	10.221.2.104	hybridcvo-02	e0a		Cluster/Node Mgmt	0
inter_1	✓		Default	10.221.1.180	hybridcvo-01	e0a		Intercluster,Cluster/Node Mgmt	0.02
inter_2	✓		Default	10.221.2.250	hybridcvo-02	e0a		Intercluster,Cluster/Node Mgmt	0.03
iscsi_1	✓	svm_hybridcvo	Default	10.221.1.5	hybridcvo-01	e0a	ISCSI	Data	0
iscsi_2	✓	svm_hybridcvo	Default	10.221.2.168	hybridcvo-02	e0a	ISCSI	Data	0

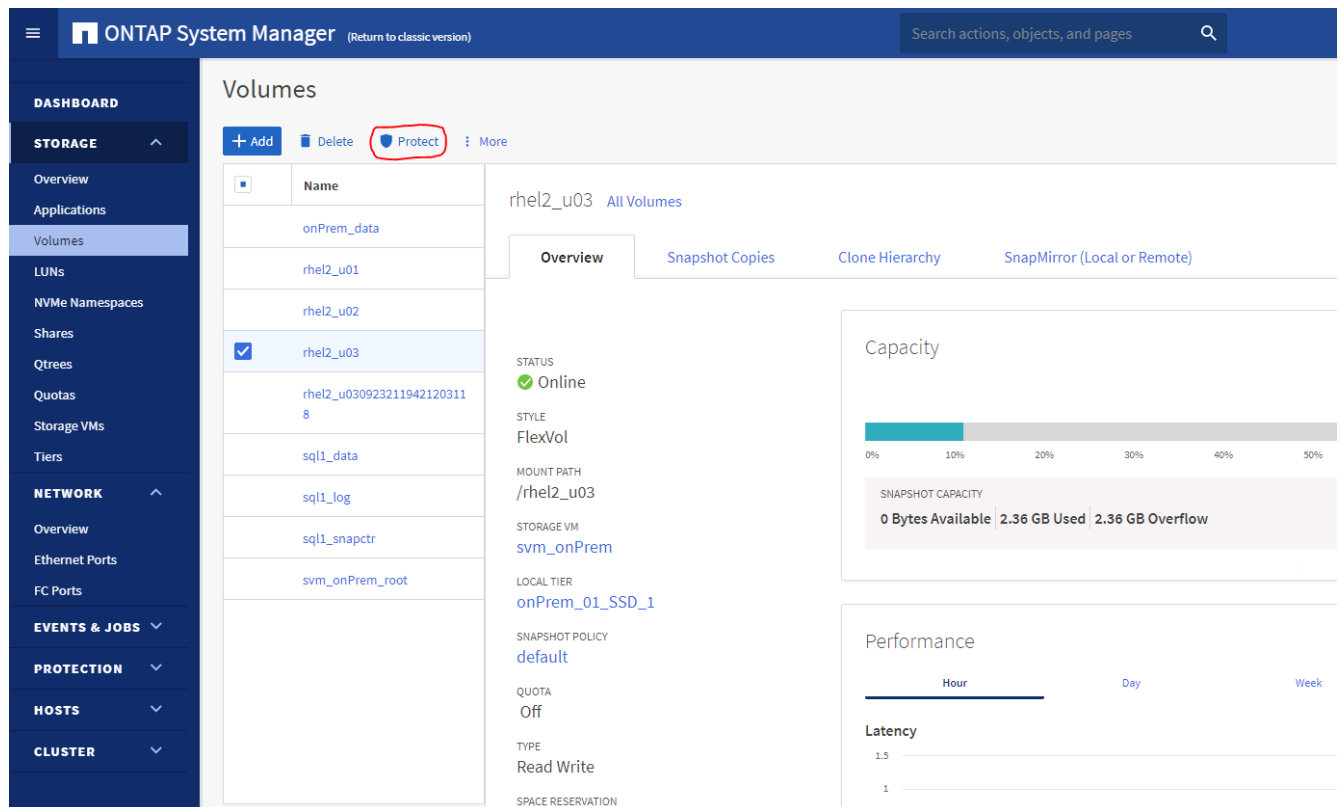
2. Con le LIF intercluster configurate, è possibile configurare il peering dei cluster e la replica dei volumi utilizzando la funzione di trascinamento della selezione in NetApp Cloud Manager. Vedere ["Getting started - AWS Public Cloud"](#) per ulteriori informazioni.

In alternativa, è possibile eseguire il peering del cluster e la replica del volume DB utilizzando Gestione di sistema di ONTAP come indicato di seguito:

3. Accedere a Gestore di sistema di ONTAP. Accedere a Cluster > Settings (Cluster > Impostazioni) e fare clic su Peer Cluster (Cluster peer) per impostare il peering del cluster con l'istanza CVO nel cloud.



- Accedere alla scheda Volumes (volumi). Selezionare il volume di database da replicare e fare clic su Proteggi.



- Impostare il criterio di protezione su asincrono. Selezionare la SVM del cluster e dello storage di

destinazione.

ONTAP System Manager

(Return to classic version)

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Protect Volumes

PROTECTION POLICY

Asynchronous

Source

CLUSTER

onPrem

STORAGE VM

svm\_onPrem

SELECTED VOLUMES

rhel2\_u03

Destination

CLUSTER

hybridcvo

STORAGE VM

svm\_hybridcvo

Destination Settings

2 matching labels

VOLUME NAME

PREFIX

vol\_

<SourceVolumeName>

SUFFIX

\_dest

Override default storage service name

Configuration Details

Initialize relationship

Enable FabricPool

Save

Cancel

6. Verificare che il volume sia sincronizzato tra l'origine e la destinazione e che la relazione di replica sia corretta.

Volumes

+ Add

Delete

Protect

More

rhel2\_u03

All Volumes

Edit

More

onPrem\_data

rhel2\_u01

rhel2\_u02

rhel2\_u03

rhel2\_u0309232119421203118

Overview

Snapshot Copies

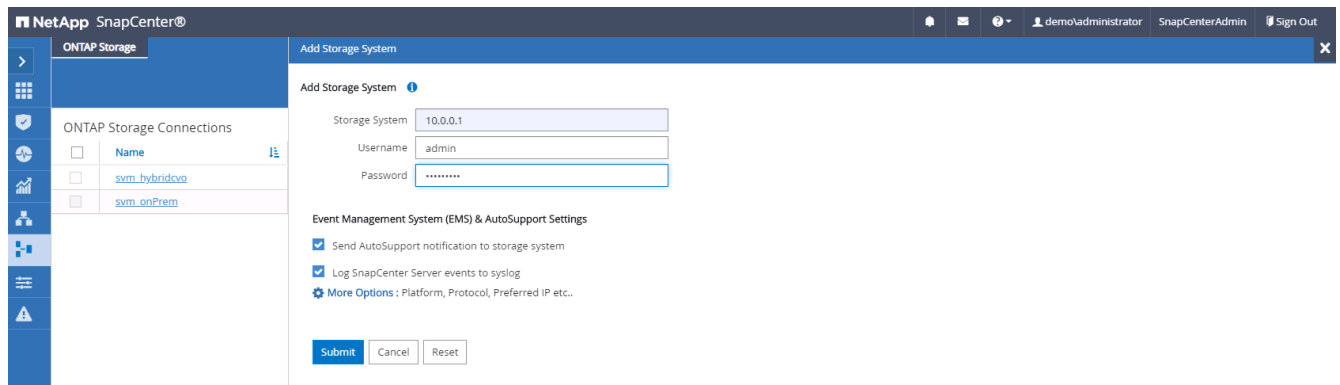
Clone Hierarchy

SnapMirror (Local or Remote)

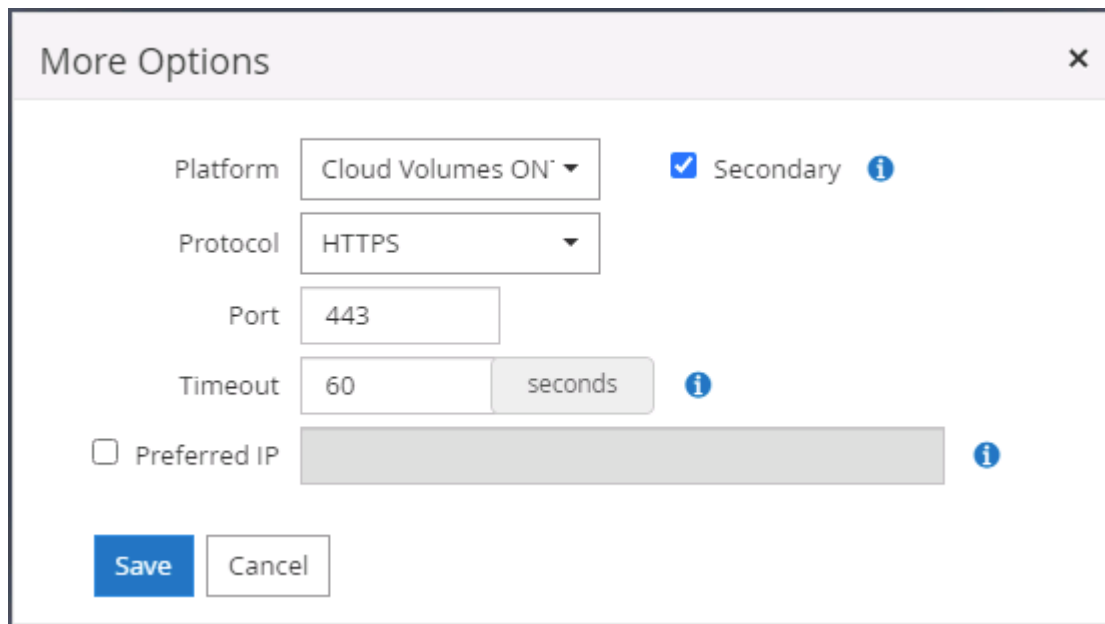
Source	Destination	Protection Policy	Relationship Health	Relationship Status	Lag
svm_onPremorhel2_u03	svm_hybridcvoorhel2_u03_dr	MirrorAllSnapshots	Healthy	Mirrored	12 seconds

6. Aggiunta di SVM per lo storage di database CVO a SnapCenter

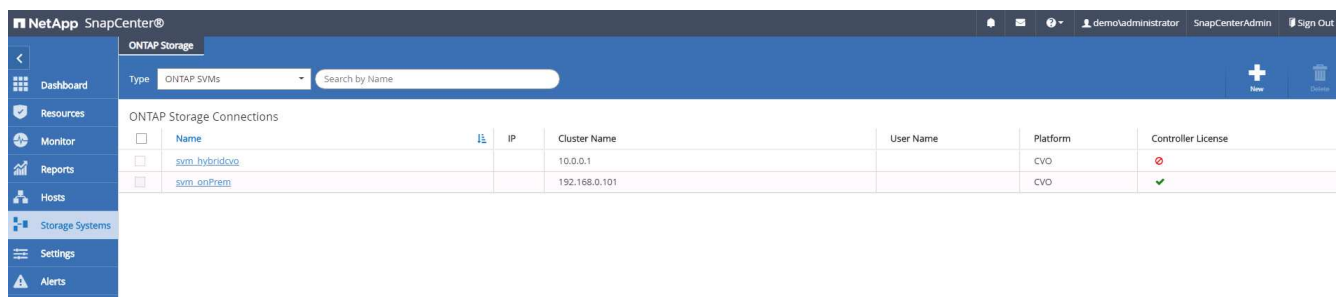
1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda sistema di storage dal menu, quindi fare clic su nuovo per aggiungere una SVM di storage CVO che ospita volumi di database di destinazione replicati in SnapCenter. Inserire l'IP di gestione del cluster nel campo Storage System (sistema di storage) e immettere il nome utente e la password appropriati.



3. Fare clic su More Options (altre opzioni) per aprire ulteriori opzioni di configurazione dello storage. Nel campo piattaforma, selezionare Cloud Volumes ONTAP, selezionare secondario, quindi fare clic su Salva.



4. Assegnare i sistemi storage agli ID utente di gestione del database SnapCenter, come illustrato nella [3. Installazione del plug-in host SnapCenter](#).

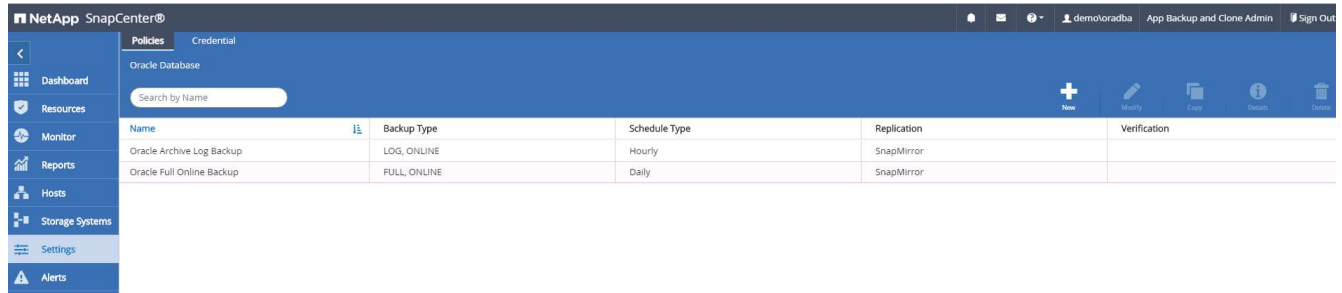


## 7. Configurare i criteri di backup del database in SnapCenter

Le seguenti procedure illustrano come creare un database completo o un criterio di backup del file di log. Il criterio può quindi essere implementato per proteggere le risorse dei database. L'RPO (Recovery Point Objective) o RTO (Recovery Time Objective) determina la frequenza dei backup del database e/o del log.

## Creare una policy di backup completa del database per Oracle

1. Accedere a SnapCenter come ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.



2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.

The screenshot shows a 'Modify Oracle Database Backup Policy' dialog box. It has a sidebar with seven steps: 1 Name, 2 Backup Type, 3 Retention, 4 Replication, 5 Script, 6 Verification, and 7 Summary. The 'Name' step is currently selected. The main area is titled 'Provide a policy name' and contains two input fields: 'Policy name' with the value 'Oracle Full Online Backup' and 'Details' with the value 'Backup all data and log files'. At the bottom right, there are 'Previous' and 'Next' buttons.

3. Selezionare il tipo di backup e la frequenza di pianificazione.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☒ Datafiles, control files, and archive logs

☐ Datafiles and control files

☐ Archive logs

☐ Offline backup 

i

☒ Mount

☐ Shutdown

☐ Save state of PDBs 

i

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☐ Hourly

☒ Daily

Previous

Next

4. Impostare la conservazione del backup. Definisce il numero di copie di backup complete del database da conservare.

138



Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Daily retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Previous

Next

5. Selezionare le opzioni di replica secondaria per inviare i backup delle snapshot primarie locali da replicare in una posizione secondaria nel cloud.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

6. Specificare qualsiasi script opzionale da eseguire prima e dopo l'esecuzione di un backup.

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Eseguire la verifica del backup, se necessario.

141

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

☐ Daily

Verification script commands

Script timeout

60secs

Prescript full path

/var/opt/snapcenter/spl/scripts/Enter Prescript path

Prescript arguments

Choose optional arguments...

Postscript full path

/var/opt/snapcenter/spl/scripts/Enter Postscript path

Postscript arguments

Choose optional arguments...

Previous

Next

8. Riepilogo.

142

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	Oracle Full Online Backup
Details	Backup all data and log files
Backup type	Online backup
Schedule type	Daily
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	None
Daily data backup retention	Delete Snapshot copies older than : 14 days
Daily archive log backup retention	Delete Snapshot copies older than : 14 days
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3

Previous

Finish

## Creare una policy di backup del log del database per Oracle

1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.
2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

Oracle Archive Log Backup

Backup Oracle archive logs

Previous

Next

3. Selezionare il tipo di backup e la frequenza di pianificazione.

144

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☐ Datafiles, control files, and archive logs

☐ Datafiles and control files

☒ Archive logs

☐ Offline backup 

i

☒ Mount

☐ Shutdown

☐ Save state of PDBs 

i

Choose schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☒ Hourly

☐ Daily

Previous

Next

4. Impostare il periodo di conservazione del registro.

145

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Hourly retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14 days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

7 days

Previous

Next

5. Abilitare la replica in una posizione secondaria nel cloud pubblico.

146



New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Hourly

Error retry count

3

Previous

Next

6. Specificare eventuali script opzionali da eseguire prima e dopo il backup del registro.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before and after performing a backup job

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Specificare eventuali script di verifica del backup.

148

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

Verification script commands

Script timeout

60secs

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Choose optional arguments...

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Choose optional arguments...

Previous

Next

8. Riepilogo.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

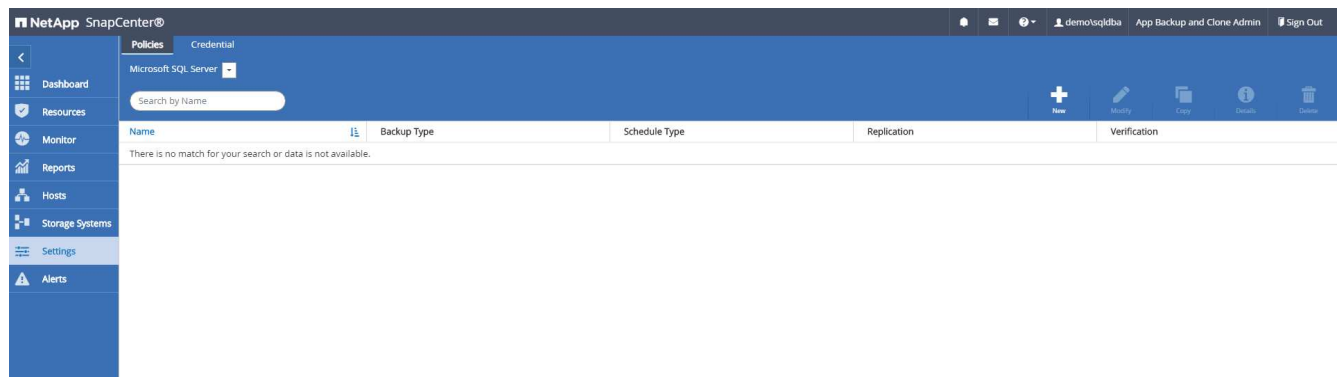
Policy name	Oracle Archive Log Backup
Details	Backup Oracle archive logs
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive log backup retention	Delete Snapshot copies older than : 7 days
Daily data backup retention	None
Daily archive log backup retention	None
Weekly data backup retention	None
Weekly archive log backup retention	None
Monthly data backup retention	None
Monthly archive log backup retention	None
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3

Previous

Finish

## Creare una policy di backup completa del database per SQL

1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.



2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

SQL Server Full Backup

Details

Backup all data and log files

Previous

Next

3. Definire l'opzione di backup e la frequenza di pianificazione. Per SQL Server configurato con un gruppo di disponibilità, è possibile impostare una replica di backup preferita.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☒ Full backup and log backup

☐ Full backup

☐ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☐ Hourly

☒ Daily

☐ Weekly

☐ Monthly

Previous

Next

4. Impostare il periodo di conservazione del backup.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Retention settings for up-to-the-minute restore operation ⓘ

☒ Keep log backups applicable to last

7

full backups

☐ Keep log backups applicable to last

14

days

Full backup retention settings ⓘ

Daily

☒ Total Snapshot copies to keep

7

☐ Keep Snapshot copies for

14

days

Previous

Next

5. Abilitare la replica delle copie di backup in una posizione secondaria nel cloud.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

6. Specificare eventuali script opzionali da eseguire prima o dopo un processo di backup.



New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Choose optional arguments...

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

7. Specificare le opzioni per eseguire la verifica del backup.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.

☐ Daily

Database consistency checks options

☒ Limit the integrity structure to physical structure of the database (PHYSICAL\_ONLY)

☒ Suppress all information message (NO\_INFOMSGS)

☐ Display all reported error messages per object (ALL\_ERRORMSGSGS)

☐ Do not check non-clustered indexes (NOINDEX)

☐ Limit the checks and obtain the locks instead of using an internal database Snapshot copy (TABLOCK)

Log backup

☐ Verify log backup.

Verification script settings

Script timeout  secs

Previous

Next

8. Riepilogo.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

Policy name	SQL Server Full Backup
Details	Backup all data and log files
Backup type	Full backup and log backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Daily
UTM retention	Total backup copies to retain : 7
Daily Full backup retention	Total backup copies to retain : 7
Replication	SnapMirror enabled , Secondary policy label: Daily , Error retry count: 3
Backup prescript settings	undefined Prescript arguments:
Backup postscript settings	undefined Postscript arguments:
Verification for backup schedule type	none
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous

Finish

## Creare un criterio di backup del log del database per SQL.

1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni > Criteri, quindi su nuovo per avviare un nuovo flusso di lavoro per la creazione di policy.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

SQL Server Log Backup

Backup SQL server log

Previous

Next

2. Definire l'opzione di backup del registro e la frequenza di pianificazione. Per SQL Server configurato con un gruppo di disponibilità, è possibile impostare una replica di backup preferita.

158

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☐ Full backup and log backup

☐ Full backup

☒ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

Select how often you want the schedules to occur in the policy. The specific times are set at backup job creation enabling you to stagger your start times.

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

☐ Monthly

Previous

Next

3. Il criterio di backup dei dati di SQL Server definisce la conservazione del backup del registro; accettare i valori predefiniti qui.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Log backup retention settings

Up-to-the-minute (UTM) retention settings retains log backups created as part of full backup and full and log backup operations. UTM retention settings also decides for how many full backups the log backups are to be retained. For example, if UTM retention settings is configured to retain log backups of the last 5 full backups, then the log backups of the last 5 full backups are retained and the rest are deleted.

Previous

Next

4. Abilitare la replica del backup dei log su secondario nel cloud.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Hourly

Error retry count

3

Previous

Next

5. Specificare eventuali script opzionali da eseguire prima o dopo un processo di backup.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

Choose optional arguments...

Choose optional arguments...

60secs

Previous

Next

6. Riepilogo.



New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Summary

Policy name	SQL Server Log Backup
Details	Backup SQL server log
Backup type	Log transaction backup
Availability group settings	Backup only on preferred backup replica
Schedule Type	Hourly
Replication	SnapMirror enabled , Secondary policy label: Hourly , Error retry count: 3
Backup prescript settings	undefined Prescript arguments:
Backup postscript settings	undefined Postscript arguments:
Verification for backup schedule type	none
Verification prescript settings	undefined Prescript arguments:
Verification postscript settings	undefined Postscript arguments:

Previous

Finish

## 8. Implementare policy di backup per proteggere il database

SnapCenter utilizza un gruppo di risorse per eseguire il backup di un database in un gruppo logico di risorse di database, ad esempio più database ospitati su un server, un database che condivide gli stessi volumi di storage, più database che supportano un'applicazione di business e così via. La protezione di un singolo database crea un proprio gruppo di risorse. Le seguenti procedure mostrano come implementare una policy di backup creata nella sezione 7 per proteggere i database Oracle e SQL Server.

## Creare un gruppo di risorse per il backup completo di Oracle

1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.

NetApp SnapCenter

Dashboard

Resources

Monitor

Reports

Hosts

Storage Systems

Settings

Alerts

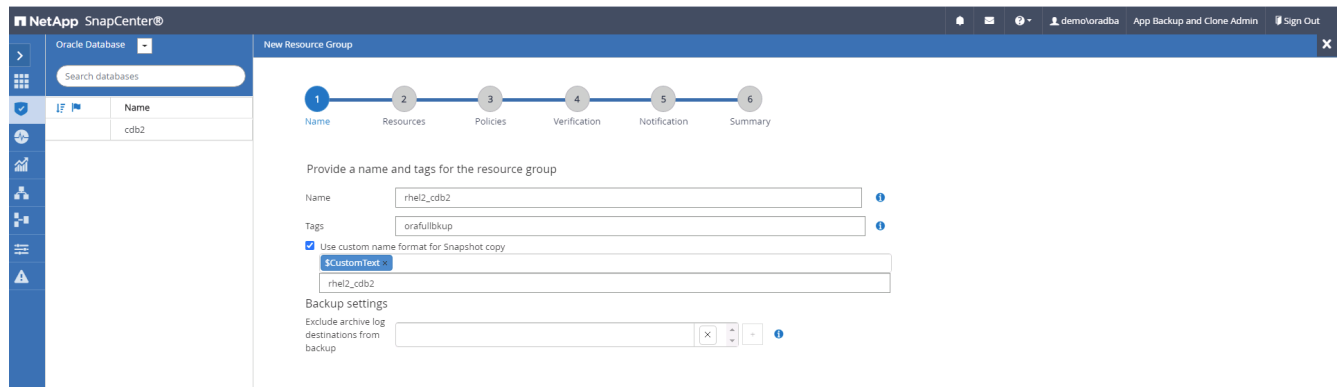
Oracle Database

View Database Search databases

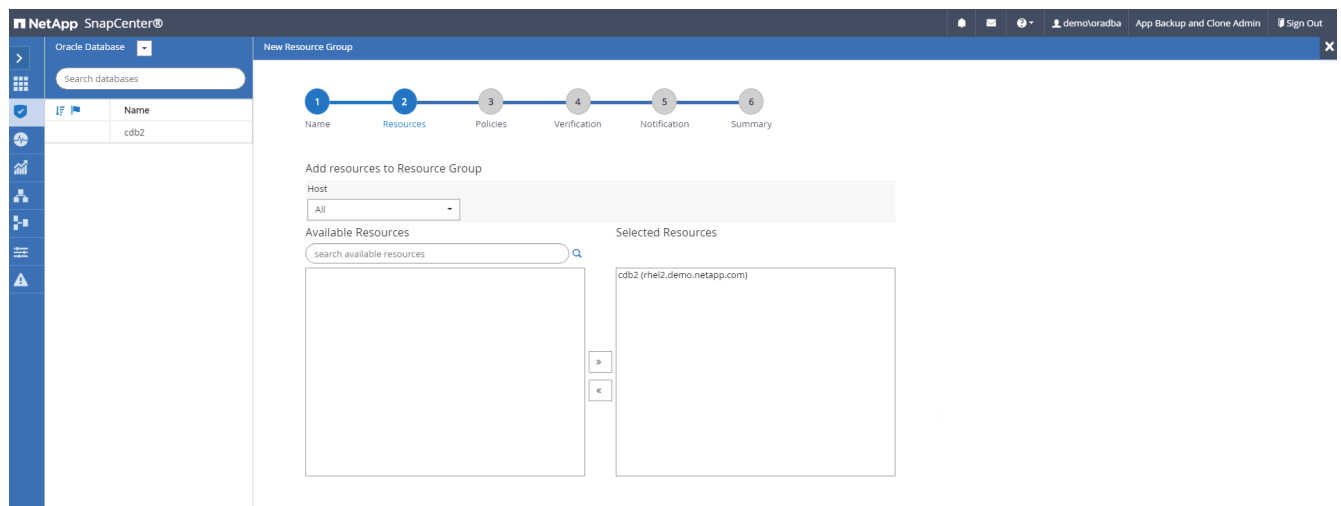
Refresh Resources New Resource Group

Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
cdb2	Single Instance (Multitenant)	rhe12.demo.netapp.com				Not protected

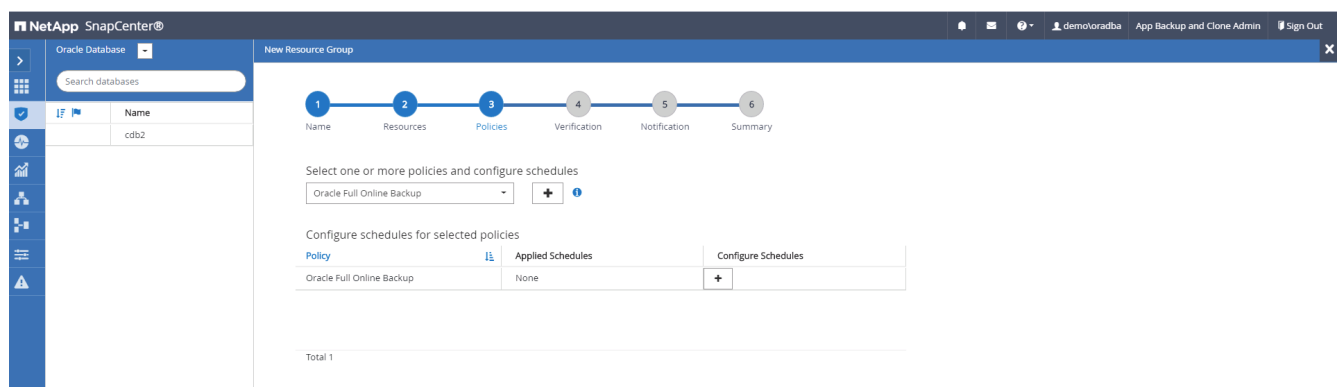
2. Fornire un nome e tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archiviazione ridondante, se configurata.



3. Aggiungere risorse di database al gruppo di risorse.



4. Selezionare una policy di backup completa creata nella sezione 7 dall'elenco a discesa.



5. Fare clic sul segno (+) per configurare la pianificazione di backup desiderata.



## 8. Riepilogo.

Resource group name	Tags	Policy	Plug-in	Verification enabled for policy	Send email
rhei2_cdb2	orafulbkup	Oracle Full Online Backup: Daily	SnapCenter Plug-in for Oracle Database	None	No

## Creare un gruppo di risorse per il backup dei log di Oracle

1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhei2_cdb2	1	orafulbkup	Oracle Full Online Backup		

2. Fornire un nome e tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archiviazione ridondante, se configurata.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2\_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide a name and tags for the resource group

Name

Tags

☒ Use custom name format for Snapshot copy

Backup settings

Exclude archive log destinations from backup ☐

3. Aggiungere risorse di database al gruppo di risorse.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2\_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Add resources to Resource Group

Host

Available Resources

search available resources

Selected Resources

cdb2 (rhel2.demo.netapp.com)

Previous Next

4. Selezionare un criterio di backup del registro creato nella sezione 7 dall'elenco a discesa.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2\_cdb2

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

Oracle Archive Log Backup

Oracle Full Online Backup

Oracle Archive Log Backup

Policy

Applied Schedules

None

Configure Schedules

Previous Next

5. Fare clic sul segno (+) per configurare la pianificazione di backup desiderata.

Add schedules for policy Oracle Archive Log Backup

Hourly

Start date

09/10/2021 3:00 PM

☒ Expires on

12/31/2021 3:00 PM

Repeat every

1

hours

0

mins

*i* The schedules are triggered in the SnapCenter Server time zone.

Cancel

OK

6. Se la verifica del backup è configurata, viene visualizzata qui.

NetApp SnapCenter®

demolatordba
App Backup and Clone Admin
Sign Out

Oracle Database

Search resource groups

Name

rhel2\_cdb2

Total 1

New Resource Group

1 Name

2 Resources

3 Policies

4 Verification

5 Notification

6 Summary

Configure verification schedules

Policy

Schedule Type

Applied Schedules

Configure Schedules

There is no match for your search or data is not available.

Total 0

Previous

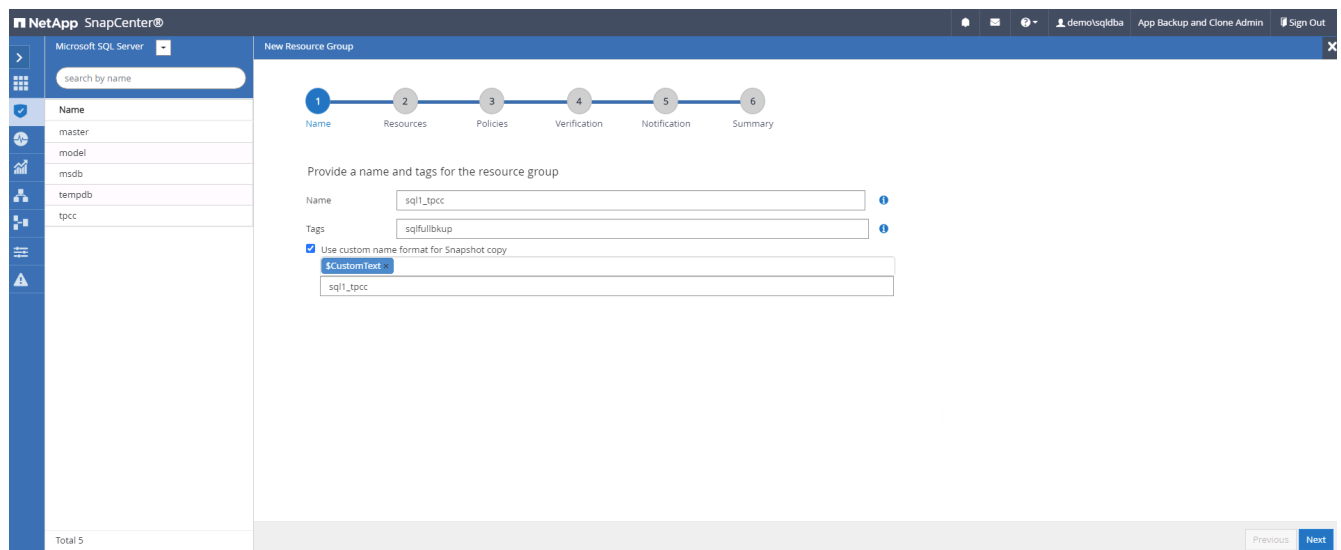
Next

7. Configurare un server SMTP per la notifica via email, se lo si desidera.

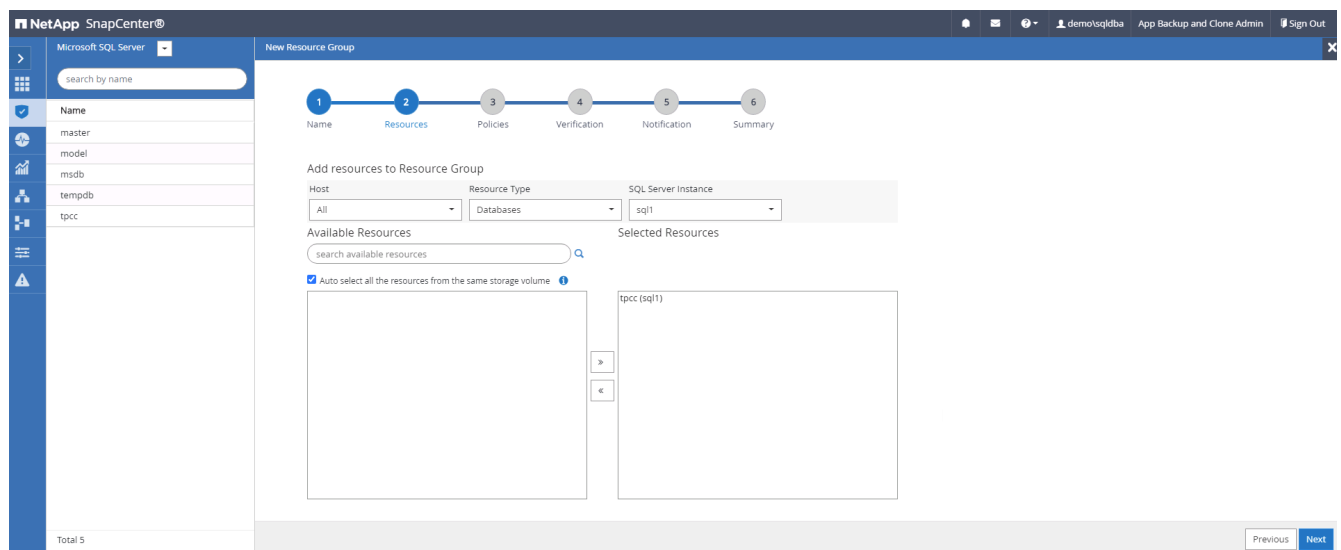
## 8. Riepilogo.

## Creare un gruppo di risorse per il backup completo di SQL Server

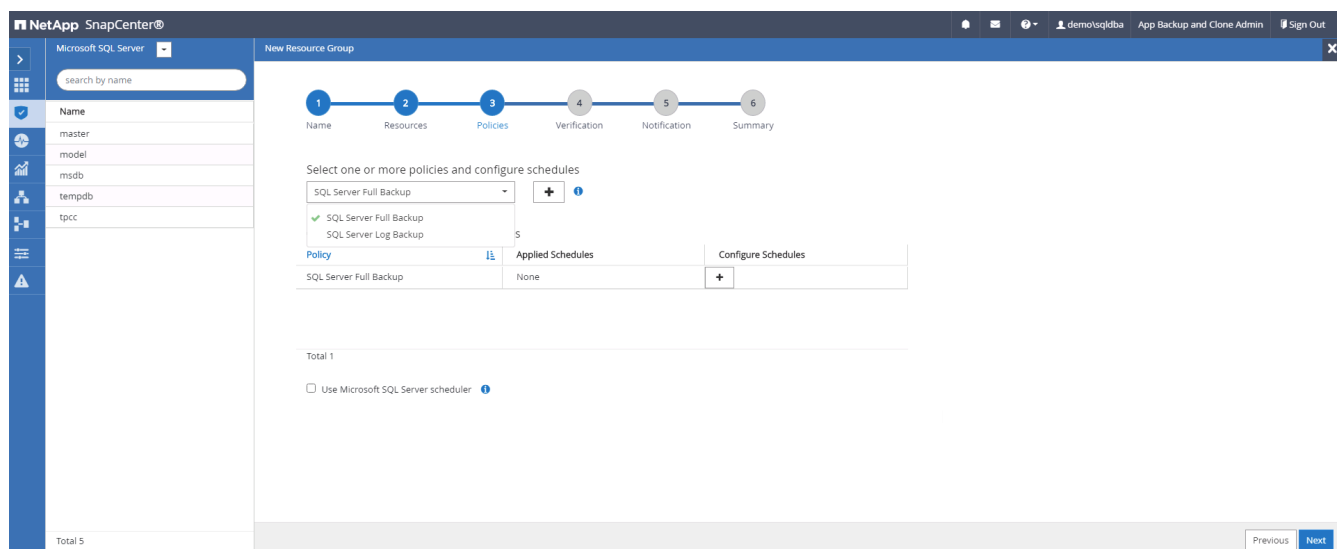
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire un nome e tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot.



2. Selezionare le risorse di database di cui eseguire il backup.



3. Selezionare una policy di backup SQL completa creata nella sezione 7.





4. Aggiungi tempi esatti per i backup e la frequenza.

Add schedules for policy SQL Server Full Backup

Daily

Start date 09/10/2021 6:20 PM

☒ Expires on 12/31/2021 6:20 PM

Repeat every 1 days

*i* The schedules are triggered in the SnapCenter Server time zone.

Cancel OK

5. Scegliere il server di verifica per il backup su secondario se deve essere eseguita la verifica del backup. Fare clic su Load Locator (carica localizzatore) per popolare la posizione dello storage secondario.

NetApp SnapCenter®

Microsoft SQL Server

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select the verification servers

Verification server Select one or more servers

Load secondary locators to verify backups on secondary Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPremsql1_data	svm_hybridcvosql1_data_dr
svm_onPremsql1_log	svm_hybridcvosql1_log_dr

Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

There is no match for your search or data is not available.

Total 5

Previous Next

6. Configurare il server SMTP per la notifica via email, se lo si desidera.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

master

model

msdb

tempdb

tpcc

Total 5

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

## 7. Riepilogo.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

There is no match for your search or data is not available.

Resources are not found. Click Refresh Resources to discover databases in the database view or create new resource group on the discovered databases from the resource view.

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: sql1\_tpcc

Tags: sqlfullbkup

Policy: SQL Server Full Backup: Daily

Plug-in: SnapCenter Plug-in for Microsoft SQL Server

Verification Server: None

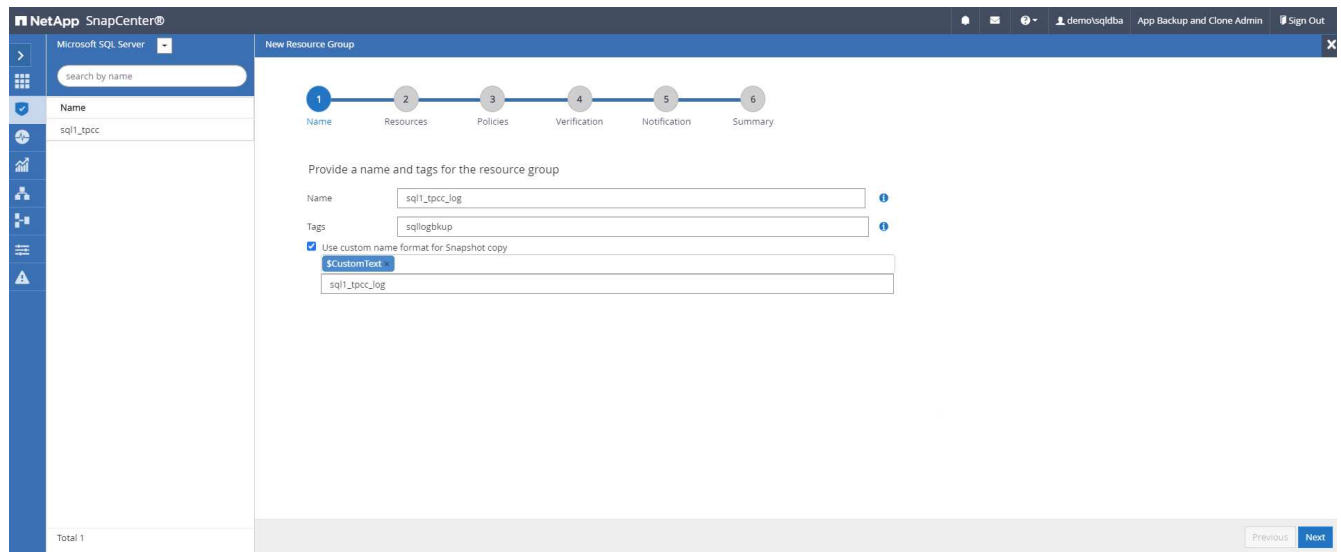
Verification enabled for policy: None

Send email: No

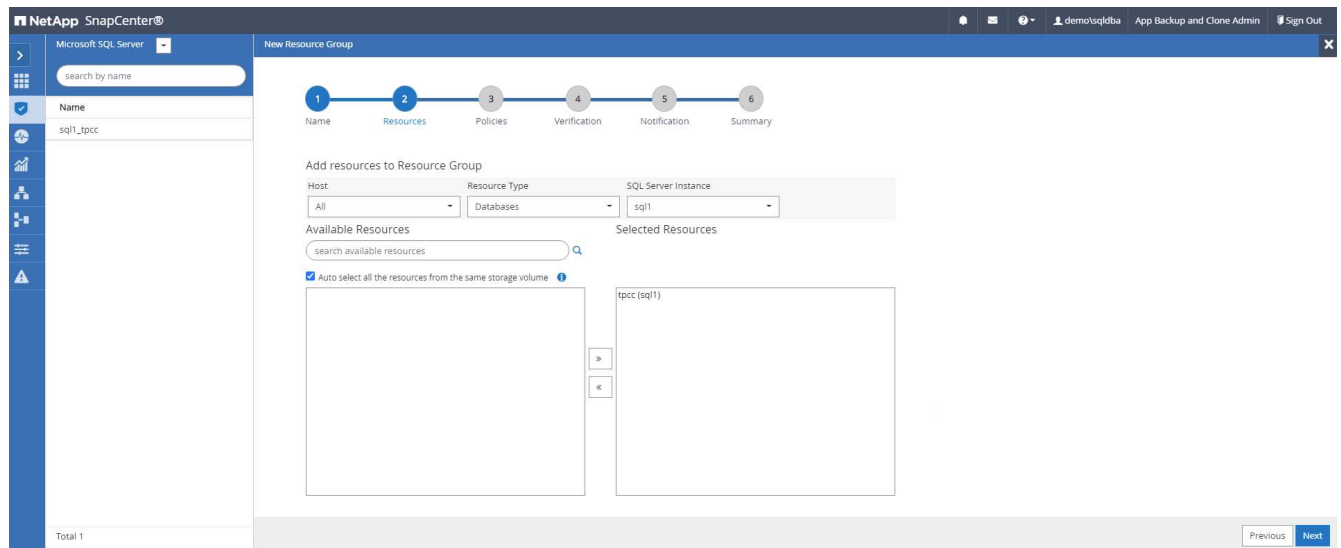
Previous Finish

## Creare un gruppo di risorse per il backup del log di SQL Server

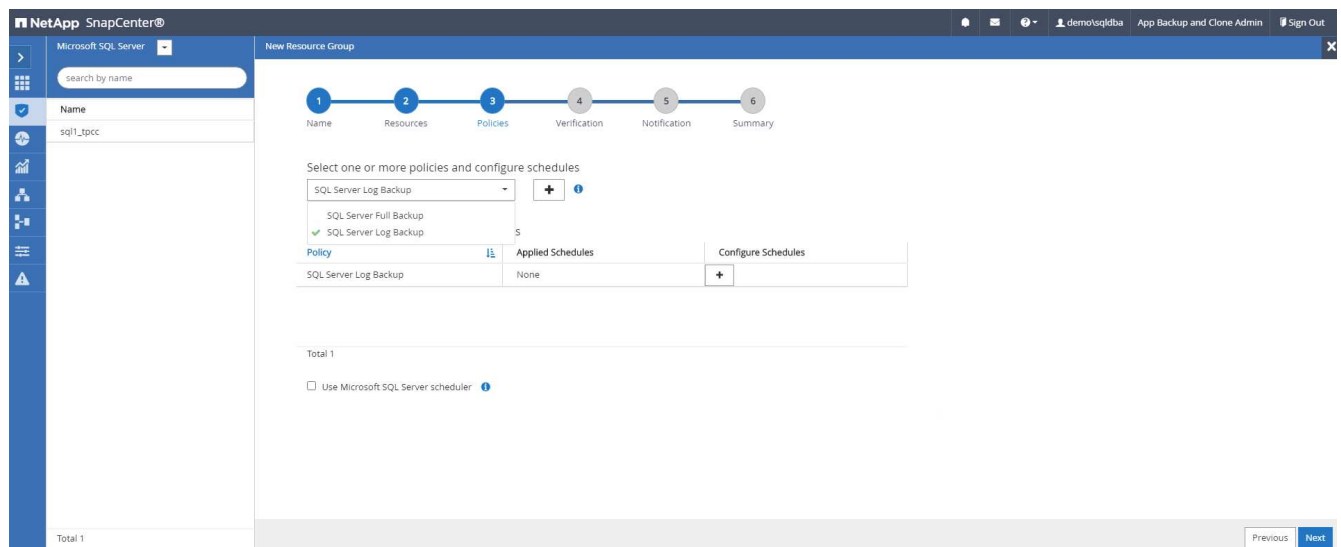
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire il nome e i tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot.



2. Selezionare le risorse di database di cui eseguire il backup.



3. Selezionare un criterio di backup del registro SQL creato nella sezione 7.



4. Aggiungere la tempistica esatta per il backup e la frequenza.

The screenshot shows the NetApp SnapCenter interface for configuring a new resource group. The 'Policies' step is active, showing a list of policies. The 'SQL Server Log Backup' policy is selected, and its schedule is configured as 'Hourly: Repeat every 1 hours'.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1\_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select one or more policies and configure schedules

SQL Server Log Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
SQL Server Log Backup	Hourly: Repeat every 1 hours	<a href="#">Configure Schedules</a>

Total 1

☐ Use Microsoft SQL Server scheduler

Previous Next

5. Scegliere il server di verifica per il backup su secondario se deve essere eseguita la verifica del backup. Fare clic su Load Locator per popolare la posizione dello storage secondario.

The screenshot shows the NetApp SnapCenter interface for configuring a new resource group. The 'Verification' step is active, showing the 'Verification server' dropdown set to 'Select one or more servers'. The 'Load secondary locators to verify backups on secondary' button is clicked. The 'Secondary storage location' is set to 'SnapVault or SnapMirror'. The 'Source Volume' and 'Destination Volume' are configured.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1\_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Select the verification servers

Verification server: Select one or more servers

Load secondary locators to verify backups on secondary

Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridvolsql1_data_dr
svm_onPrem:sql1_log	svm_hybridvolsql1_log_dr

Configure verification schedules

Policy	Schedule Type	Applied Schedules	Configure Schedules
There is no match for your search or data is not available.			

Previous Next

6. Configurare il server SMTP per la notifica via email, se lo si desidera.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1\_tpcc

Total 1

New Resource Group

If you want to send notifications for scheduled or on demand jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Provide email settings

Select the service accounts or people to notify regarding protection issues.

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

## 7. Riepilogo.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1\_tpcc

Total 1

New Resource Group

1 Name 2 Resources 3 Policies 4 Verification 5 Notification 6 Summary

Resource group name: sql1\_tpcc\_log

Tags: sqllogbkup

Policy: SQL Server Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Microsoft SQL Server

Verification Server: None

Verification enabled for policy: None

Send email: No

Previous Finish

## 9. Convalidare il backup

Una volta creati i gruppi di risorse di backup del database per proteggere le risorse del database, i processi di backup vengono eseguiti in base alla pianificazione predefinita. Controllare lo stato di esecuzione del lavoro nella scheda Monitor.

NetApp SnapCenter®

Jobs Schedules Events Logs

search by name

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

Jobs - Filter

ID	Status	Name	Start date	End date	Owner
532	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 8:35:01 PM	09/14/2021 8:37:10 PM	demo/sqldba
528	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 7:35:01 PM	09/14/2021 7:37:09 PM	demo/sqldba
524	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 6:35:01 PM	09/14/2021 6:37:08 PM	demo/sqldba
521	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/14/2021 6:25:01 PM	09/14/2021 6:27:14 PM	demo/sqldba
517	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 5:35:01 PM	09/14/2021 5:37:09 PM	demo/sqldba
513	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 4:35:01 PM	09/14/2021 4:37:08 PM	demo/sqldba
509	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 3:35:01 PM	09/14/2021 3:37:10 PM	demo/sqldba
503	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/14/2021 2:35:01 PM	09/14/2021 2:37:09 PM	demo/sqldba

Accedere alla scheda Resources (risorse), fare clic sul nome del database per visualizzare i dettagli del

backup del database e alternare tra Local Copies (copie locali) e Mirror Copies (copie mirror) per verificare che i backup Snapshot siano replicati in una posizione secondaria nel cloud pubblico.

The screenshot shows the NetApp SnapCenter web interface. On the left, there's a sidebar with navigation icons. The main area is titled 'Oracle Database' and 'cdb2 Topology'. It displays a 'Manage Copies' section with a diagram showing 'Local copies' (197 Backups, 0 Clones) and 'Mirror copies' (197 Backups, 3 Clones). A 'Summary Card' on the right shows: 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. Below this is a table of 'Primary Backup(s)' with columns: Backup Name, Count, Type, End Date, Verified, Mounted, RMAN Cataloged, and SCN. The table lists five backup entries with their respective details.

Backup Name	Count	Type	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_09-23-2021_14.35.03.3242_1	1	Log	09/23/2021 2:35:45 PM	Not Applicable	False	Not Cataloged	6872761
rhel2_cdb2_09-23-2021_14.35.03.3242_0	1	Data	09/23/2021 2:35:30 PM	Unverified	False	Not Cataloged	6872715
rhel2_cdb2_09-22-2021_14.35.02.0014_1	1	Log	09/22/2021 2:35:24 PM	Not Applicable	False	Not Cataloged	6737479
rhel2_cdb2_09-22-2021_14.35.02.0014_0	1	Data	09/22/2021 2:35:14 PM	Unverified	False	Not Cataloged	6737395
rhel2_cdb2_09-21-2021_14.35.02.1884_1	1	Log	09/21/2021 2:35:35 PM	Not Applicable	False	Not Cataloged	6598735

A questo punto, le copie di backup del database nel cloud sono pronte per essere clonate per eseguire processi di sviluppo/test o per il disaster recovery in caso di guasto primario.

## Introduzione al cloud pubblico AWS

Questa sezione descrive il processo di implementazione di Cloud Manager e Cloud Volumes ONTAP in AWS.

### Cloud pubblico AWS



Per semplificare la procedura, abbiamo creato questo documento sulla base di un'implementazione in AWS. Tuttavia, il processo è molto simile per Azure e GCP.

### 1. Controllo prima del volo

Prima dell'implementazione, assicurarsi che l'infrastruttura sia in uso per consentire l'implementazione nella fase successiva. Ciò include quanto segue:

- Account AWS
- VPC nella tua regione di scelta
- Subnet con accesso a Internet pubblico
- Autorizzazioni per aggiungere ruoli IAM all'account AWS
- Chiave segreta e chiave di accesso per l'utente AWS

### 2. Fasi per implementare Cloud Manager e Cloud Volumes ONTAP in AWS



Esistono molti metodi per implementare Cloud Manager e Cloud Volumes ONTAP; questo metodo è il più semplice ma richiede la maggior parte delle autorizzazioni. Se questo metodo non è appropriato per l'ambiente AWS in uso, consultare ["Documentazione cloud di NetApp"](#).

### Implementare Cloud Manager Connector

1. Selezionare ["NetApp Cloud Central"](#) ed effettuare l'accesso o l'iscrizione.



[Continue to Cloud Manager](#)

## Log In to NetApp Cloud Central

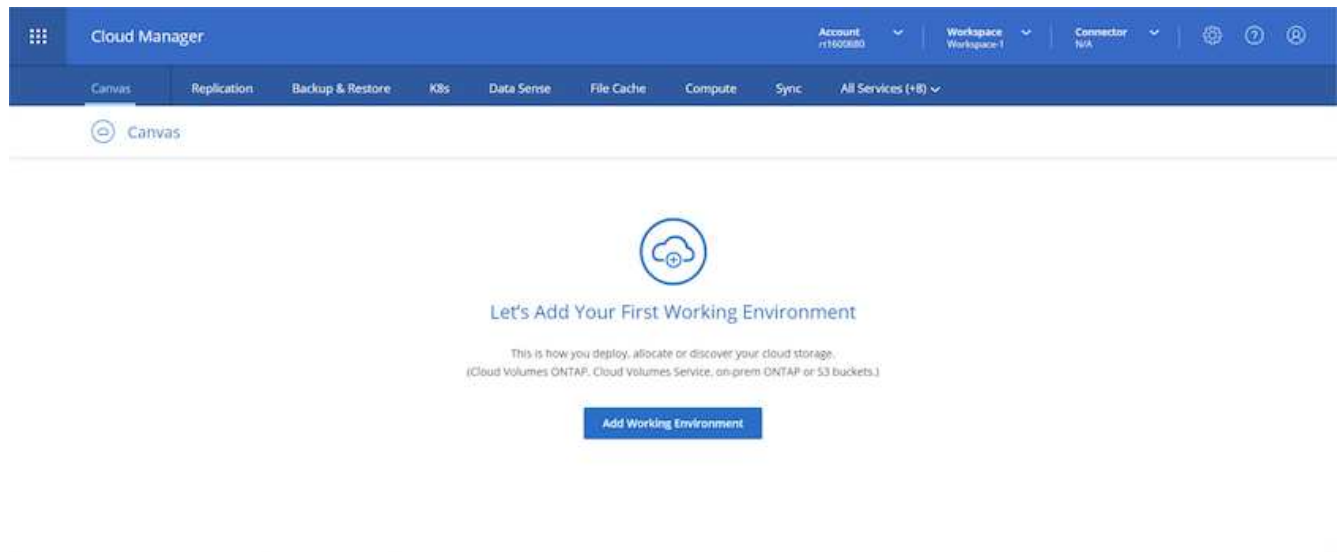
---

Don't have an account yet? [Sign Up](#)

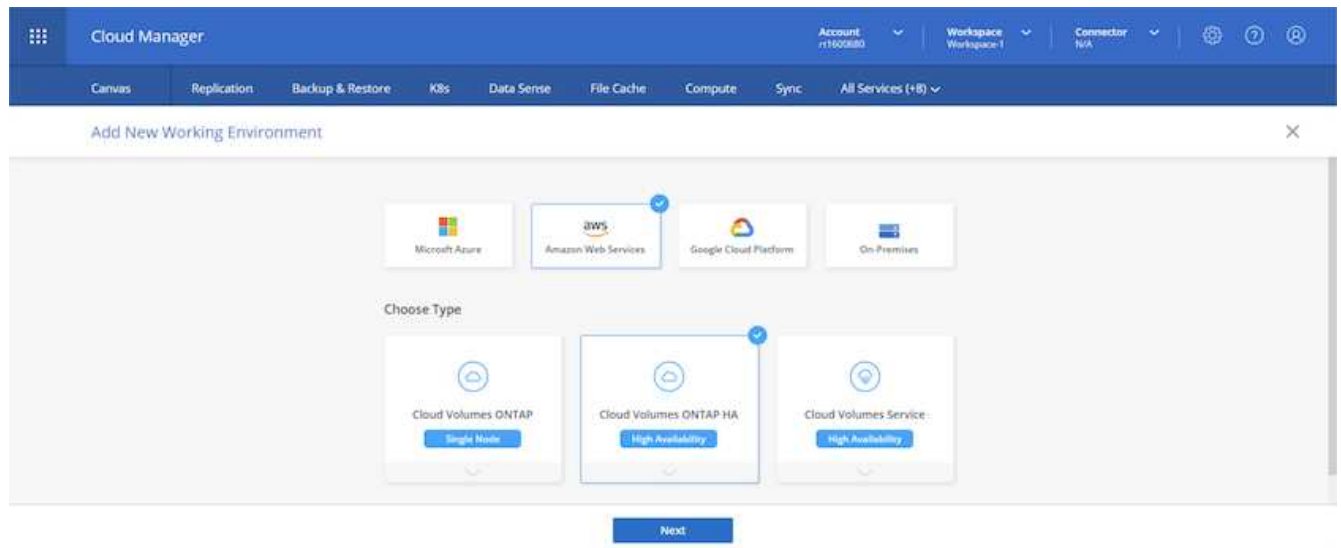
**LOGIN**

[Forgot your password?](#)

2. Dopo aver effettuato l'accesso, si dovrebbe essere portati a Canvas.

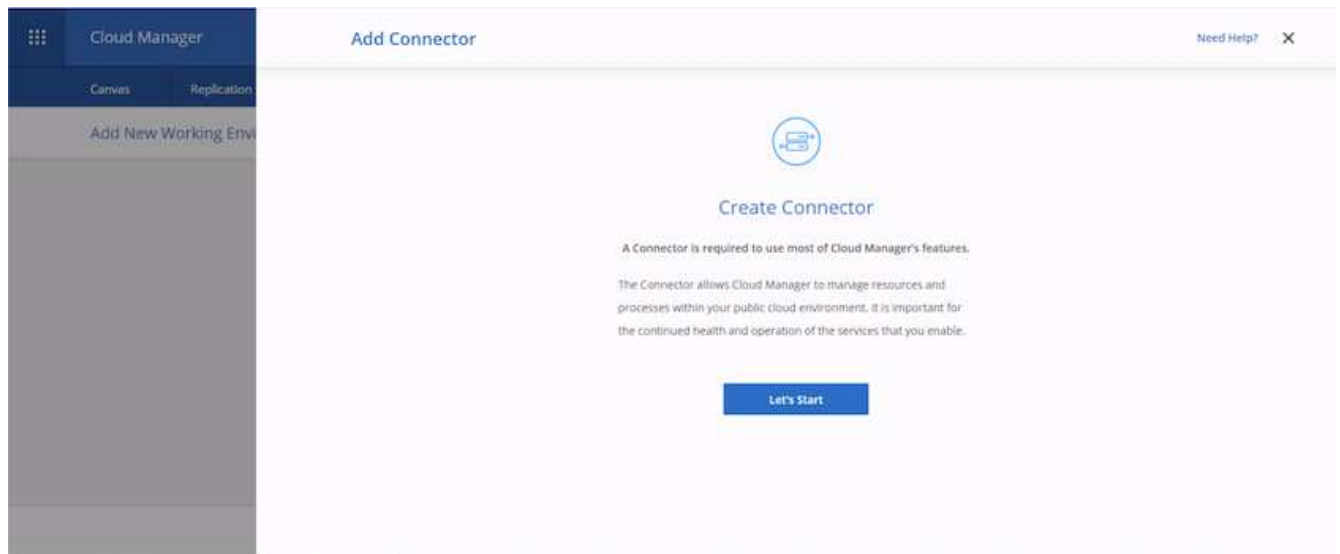


3. Fai clic su "Aggiungi ambiente di lavoro" e scegli Cloud Volumes ONTAP in AWS. In questo caso, è anche possibile scegliere se implementare un sistema a nodo singolo o una coppia ad alta disponibilità. Ho scelto di implementare una coppia ad alta disponibilità.

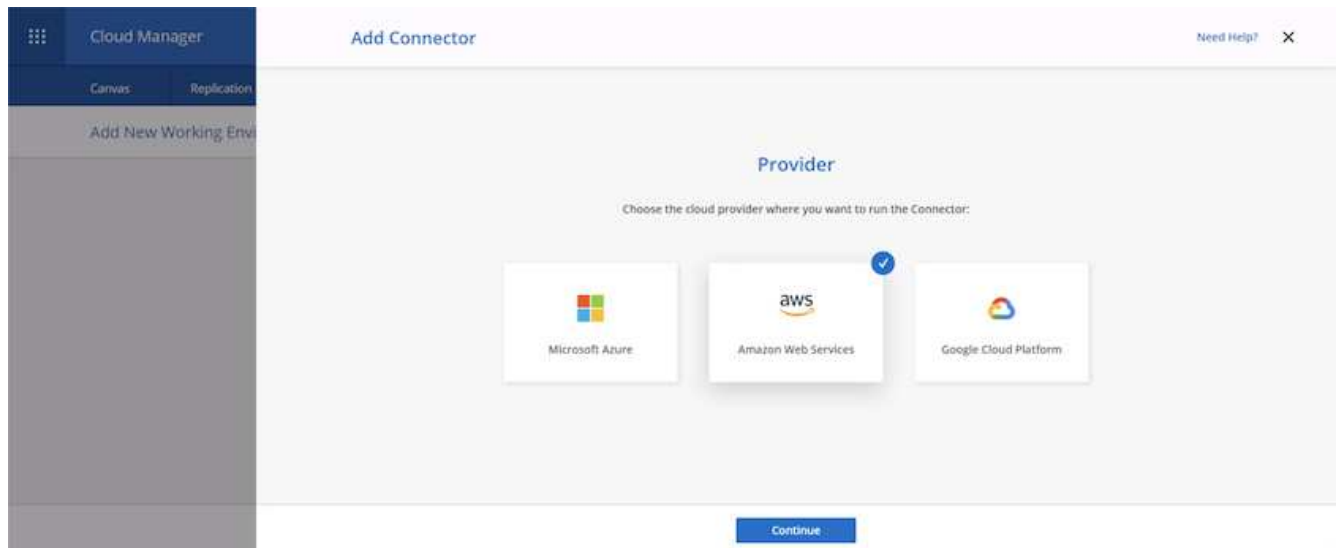


4. Se non è stato creato alcun connettore, viene visualizzata una finestra a comparsa che richiede di creare un connettore.





5. Fare clic su Avvia, quindi scegliere AWS.



6. Inserire la chiave segreta e la chiave di accesso. Assicurarsi che l'utente disponga delle autorizzazioni corrette descritte in ["Pagina delle policy di NetApp"](#).

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

### AWS Credentials

AWS Access Key

AWS Access Key is required

AWS Secret Key

Region

us-east-1 | US East (N. Virginia)

Want to launch an instance without AWS Credentials?

Previous Next

7. Assegnare un nome al connettore e utilizzare un ruolo predefinito come descritto in "[Pagina delle policy di NetApp](#)" Oppure chiedi a Cloud Manager di creare il tuo ruolo.

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

### Details

Connector Instance Name

awscloudmanager

Connector Role

Create Role Select an existing Role

Role Name

Cloud-Manager-Operator-IBHt24j

Add Tags to Connector Instance

Previous Next

8. Fornire le informazioni di rete necessarie per implementare il connettore. Verificare che l'accesso a Internet in uscita sia attivato:
- Fornire al connettore un indirizzo IP pubblico
  - Fornire al connettore un proxy da utilizzare
  - Fornire al connettore un percorso verso Internet pubblico attraverso un gateway Internet

**Cloud Manager** | Add Connector | Need Help? X

Get Ready | AWS Credentials | Details | **4 Network** | Security Group | Review

**Connectivity**

VPC: vpc-083fcd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN-us-east-1a\_r11600...

Key Pair: r11600680

Public IP: Enable

**Proxy Configuration (Optional)**

HTTP Proxy: Example: https://172.16.254.1:8080

Define Credentials for this Proxy

Upload a root certificate

Previous Next

9. Fornire la comunicazione con il connettore tramite SSH, HTTP e HTTPS fornendo un gruppo di protezione o creando un nuovo gruppo di protezione. È stato attivato l'accesso al connettore solo dall'indirizzo IP.

**Cloud Manager** | Add Connector | Need Help? X

Get Ready | AWS Credentials | Details | Network | **5 Security Group** | Review

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

HTTP (Port 80)	HTTPS (Port 443)	SSH (Port 22)
Source Type: My IP	Source Type: My IP	Source Type: My IP
Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32	Source (CIDR): 216.240.31.145/32

Previous Next

10. Esaminare le informazioni nella pagina di riepilogo e fare clic su Add (Aggiungi) per implementare il connettore.

Cloud Manager

Canvas Replication

Add New Working Environment

### Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group **Review**

Code for Terraform Automation

Connector Name	awscloudmanager
Region	us-east-1
VPC	vpc-083fcbd79f75dfb6e - 10.221.0.0/16
Subnet	10.221.4.0/24   publicSN-us-east-1a-rt1600680
Key Pair	rt1600680
Public IP	Enable
Proxy	None
Security Group	HTTP: 216.240.31.145/32, HTTPS: 216.240.31.145/32, SSH: 216.240.31.145/32

Previous Add

11. Il connettore viene ora implementato utilizzando uno stack di formazione cloud. Puoi monitorarne i progressi da Cloud Manager o tramite AWS.

Cloud Manager

Canvas Replication

Add New Working Environment

### Deploying a Connector

Show Details

- Keep this wizard open until the deployment process is complete. It usually takes about 7 minutes.
- No other Cloud Manager features are available during deployment.
- When the process is complete, you can continue the operation that you started.

12. Una volta completata l'implementazione, viene visualizzata una pagina di successo.

Cloud Manager

Canvas Replication

Add New Working Environment

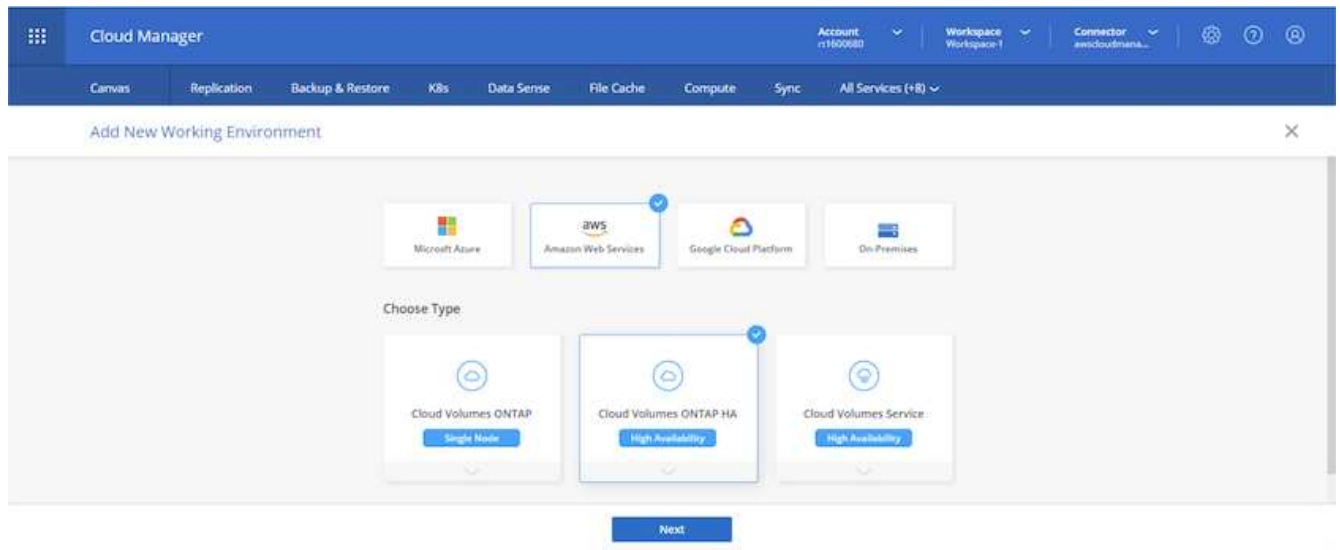
### Connector Successfully Created

The Connector was created successfully.

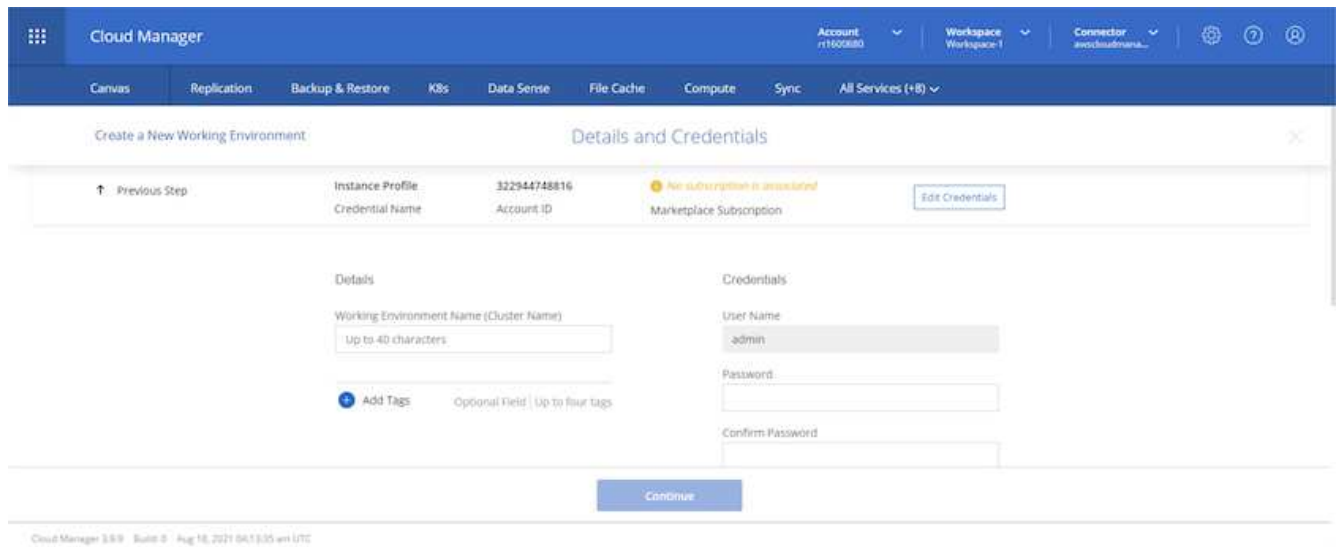
Continue

## Implementare Cloud Volumes ONTAP

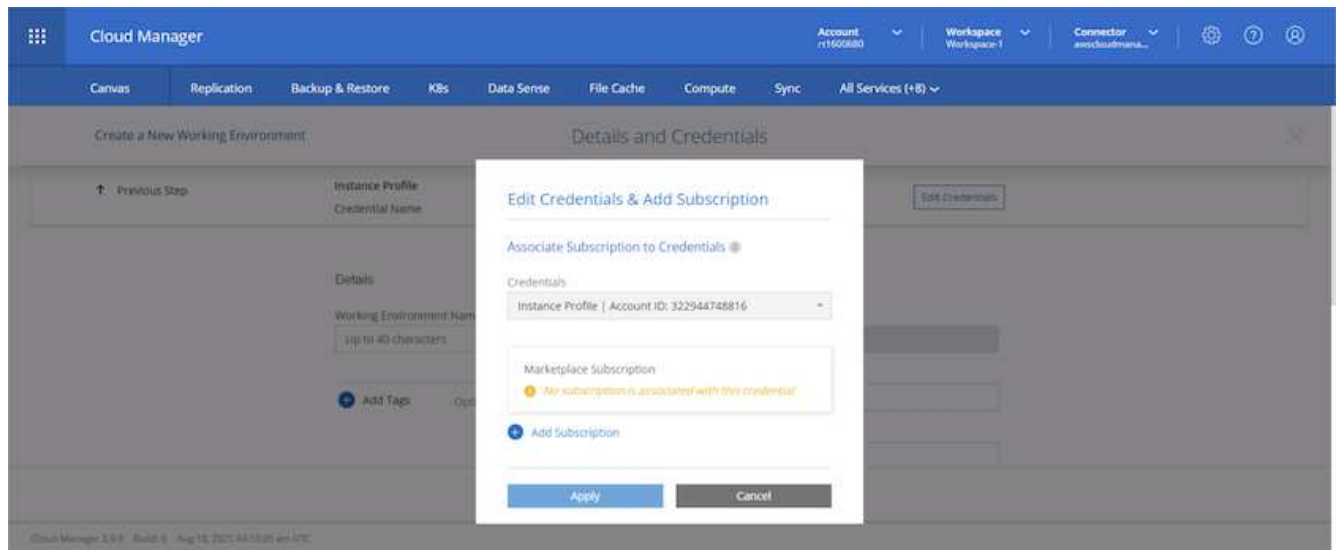
1. Selezionare AWS e il tipo di implementazione in base ai requisiti.



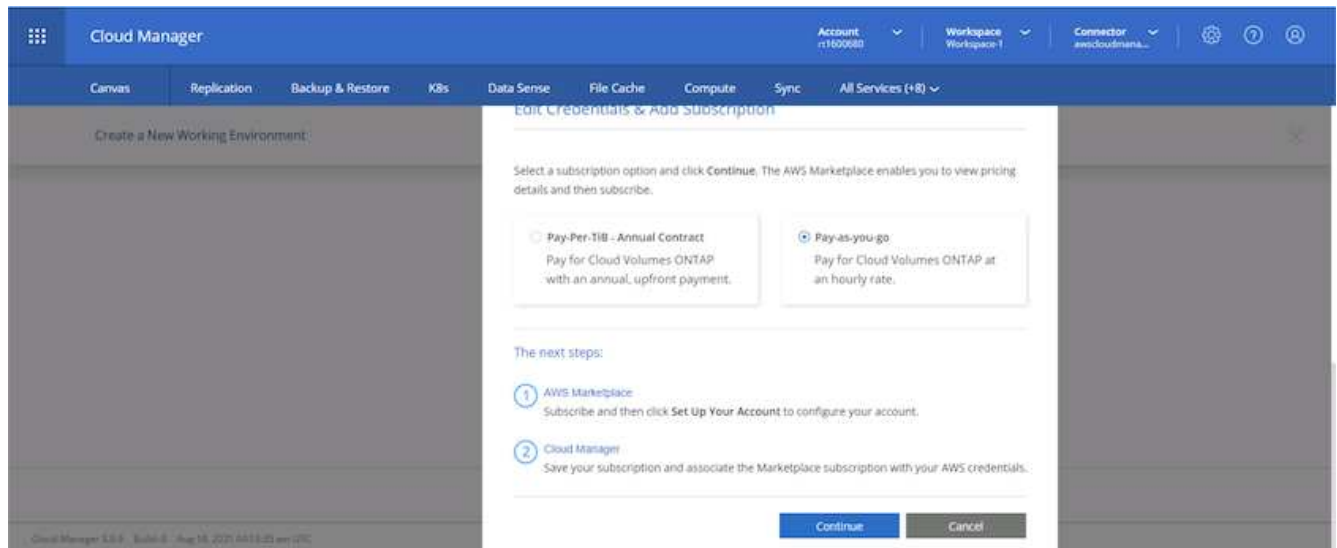
2. Se non è stato assegnato alcun abbonamento e si desidera effettuare l'acquisto con PAYGO, scegliere Modifica credenziali.



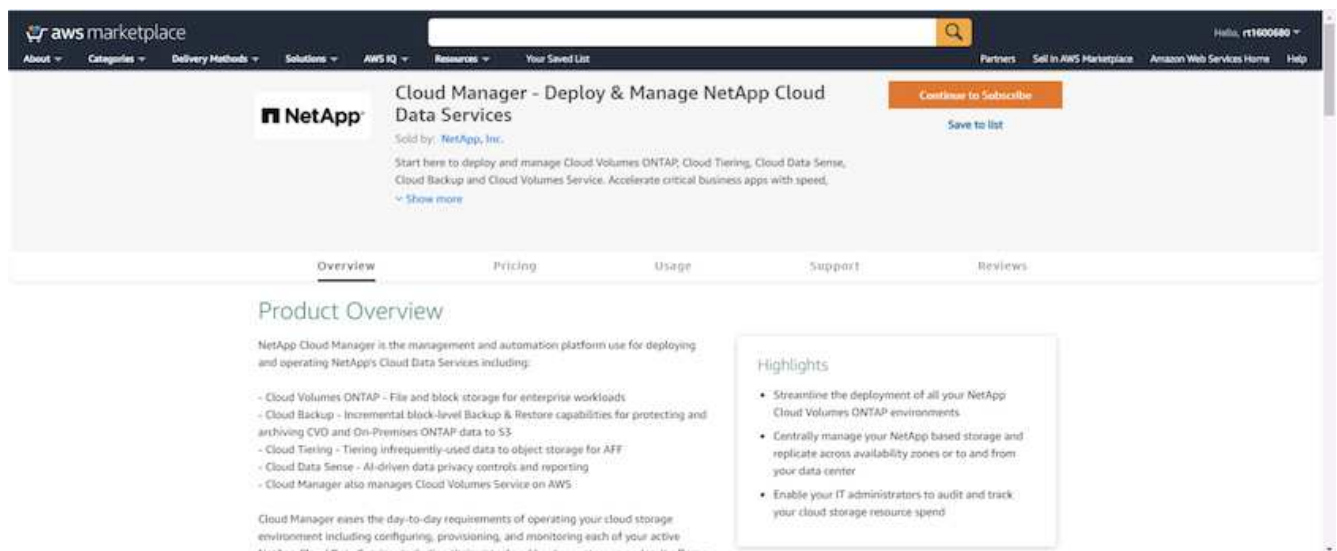
3. Scegliere Aggiungi abbonamento.



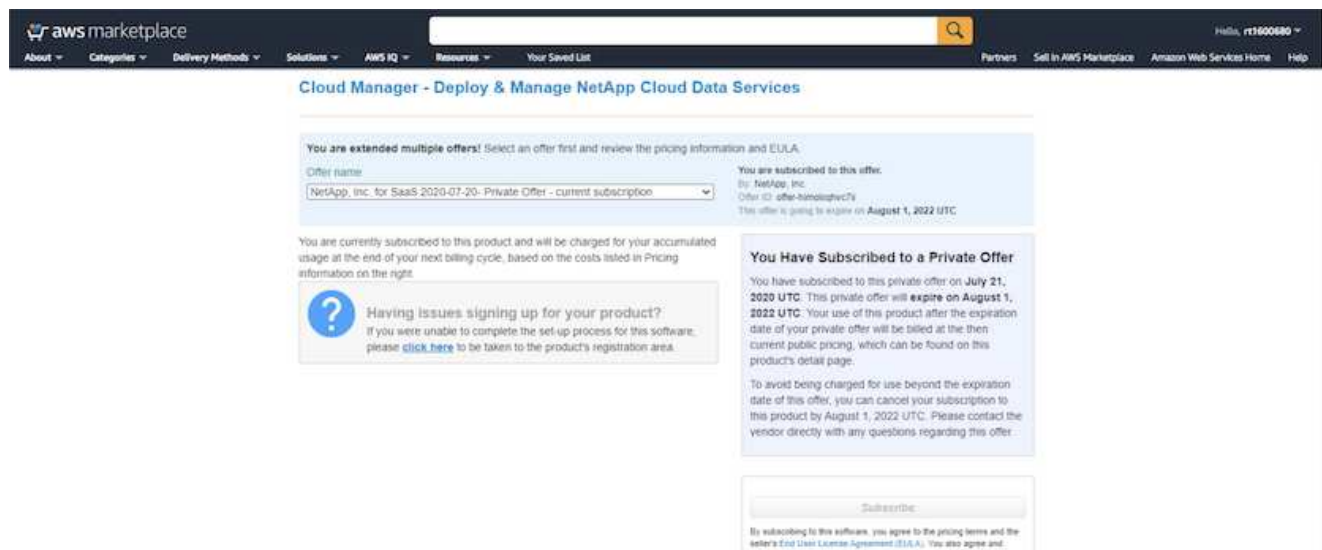
4. Scegliere il tipo di contratto a cui si desidera sottoscrivere. Ho scelto il pay-as-you-go.



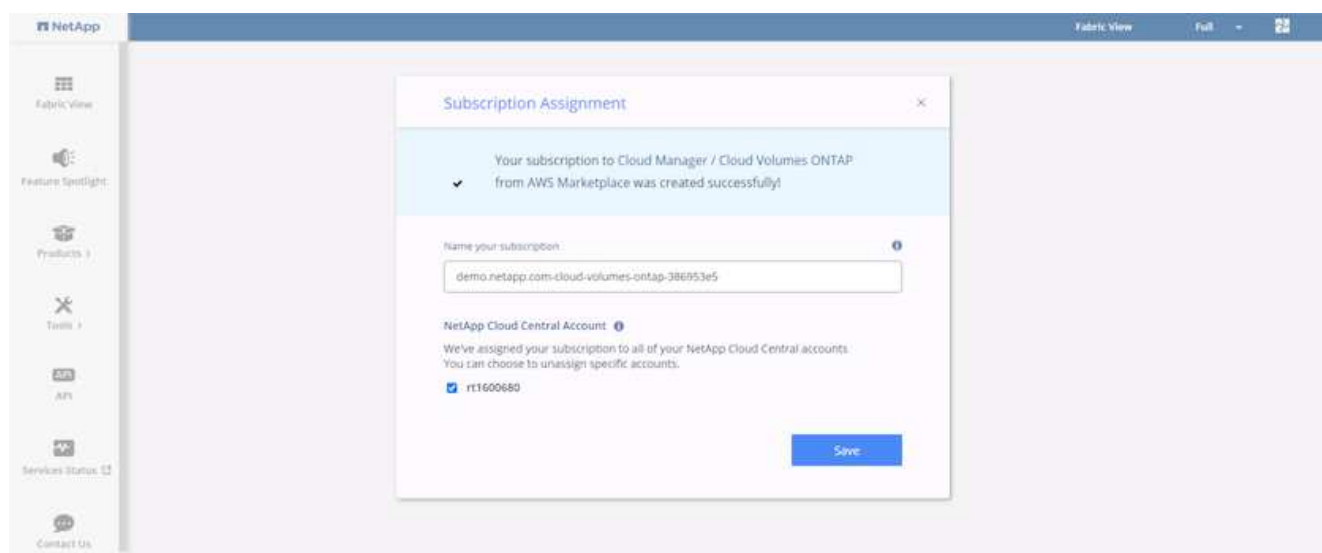
5. Si viene reindirizzati ad AWS; scegliere continua per iscriversi.



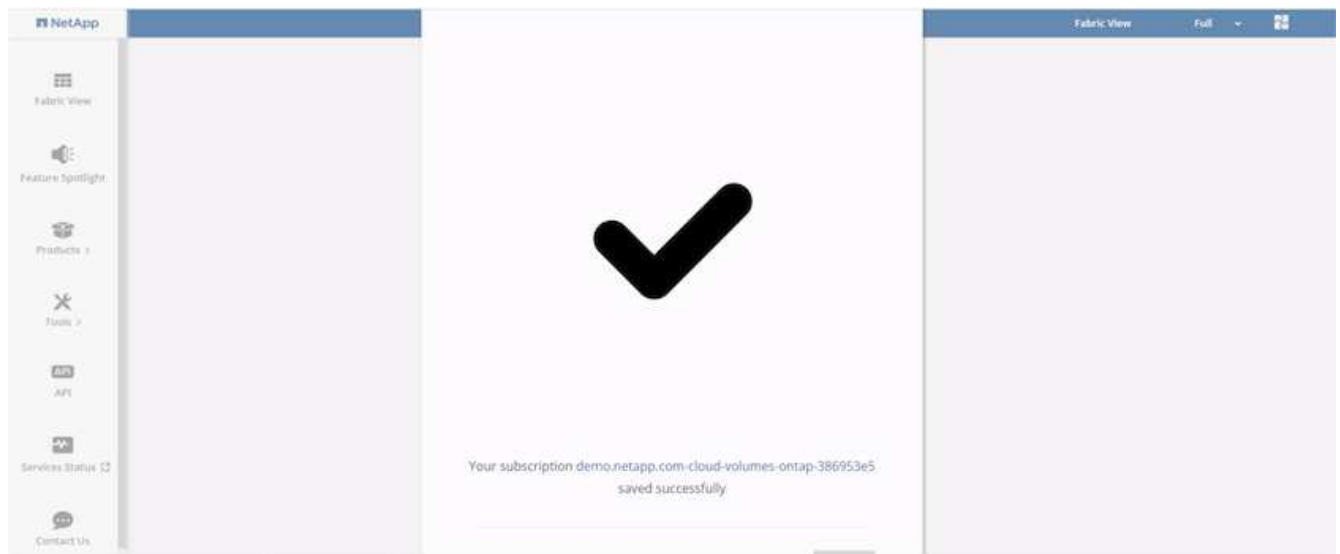
6. Iscriviti e verrai reindirizzato a NetApp Cloud Central. Se sei già iscritto e non ricevi il reindirizzamento, scegli il link "Clicca qui".



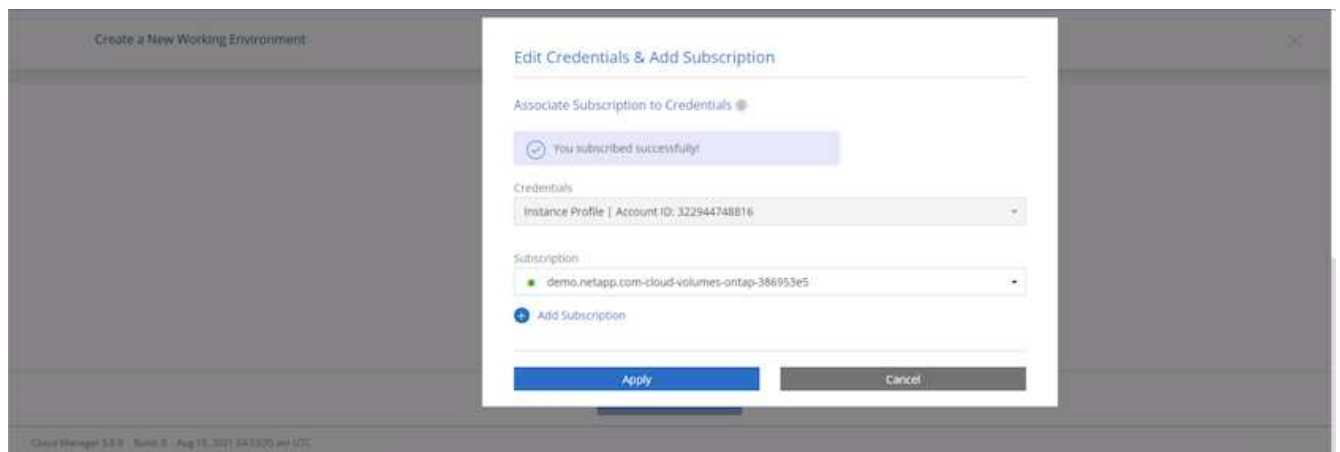
7. Verrai reindirizzato a Cloud Central dove devi assegnare un nome all'abbonamento e assegnarlo al tuo account Cloud Central.



8. Una volta completata la stampa, viene visualizzata una pagina con un segno di spunta. Tornare alla scheda Cloud Manager.



9. L'abbonamento viene ora visualizzato in Cloud Central. Fare clic su Apply (Applica) per continuare.



10. Inserire i dettagli dell'ambiente di lavoro, ad esempio:

- a. Nome del cluster
- b. Password del cluster
- c. Tag AWS (opzionale)



The screenshot shows the 'Details and Credentials' step in the Cloud Manager interface. The top navigation bar includes 'Cloud Manager', 'Account: r1600880', 'Workspace: Workspace 1', and 'Connector: awscloudmana...'. The main navigation tabs are 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The 'Create a New Working Environment' window is open, showing a 'Previous Step' button and a table with the following details:

Instance Profile	322944748816	demo.netapp.com-cloud-vol...
Credential Name	Account ID	Marketplace Subscription

Below the table, there are two sections: 'Details' and 'Credentials'. The 'Details' section has a 'Working Environment Name (Cluster Name)' field with the value 'hybridawsco' and an 'Add Tags' button. The 'Credentials' section has 'User Name' (admin), 'Password' (masked), and 'Confirm Password' (masked) fields. A 'Continue' button is at the bottom right.

Cloud Manager 3.9.9 Built 0 Aug 18, 2021 06:13:35 am UTC

- Scegliere i servizi aggiuntivi che si desidera implementare. Per ulteriori informazioni su questi servizi, visitare il ["Homepage di NetApp Cloud"](#).

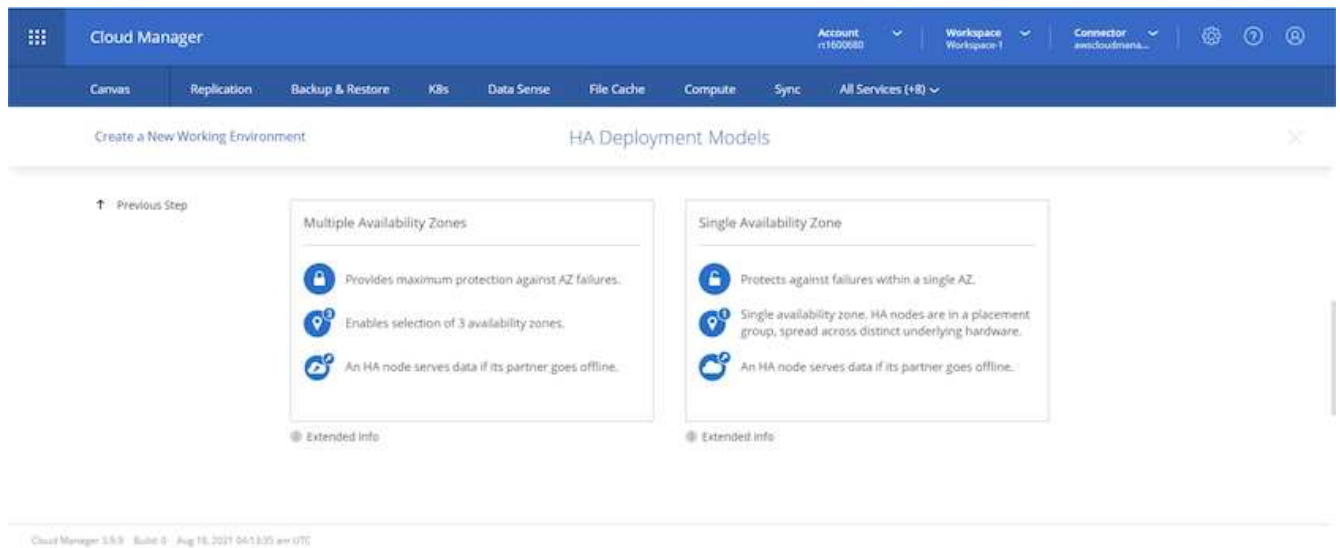
The screenshot shows the 'Services' step in the Cloud Manager interface. The top navigation bar is the same as the previous screenshot. The 'Create a New Working Environment' window is open, showing a 'Previous Step' button and a list of services with toggle switches and dropdown menus:

- Data Sense & Compliance
- Backup to Cloud
- Monitoring

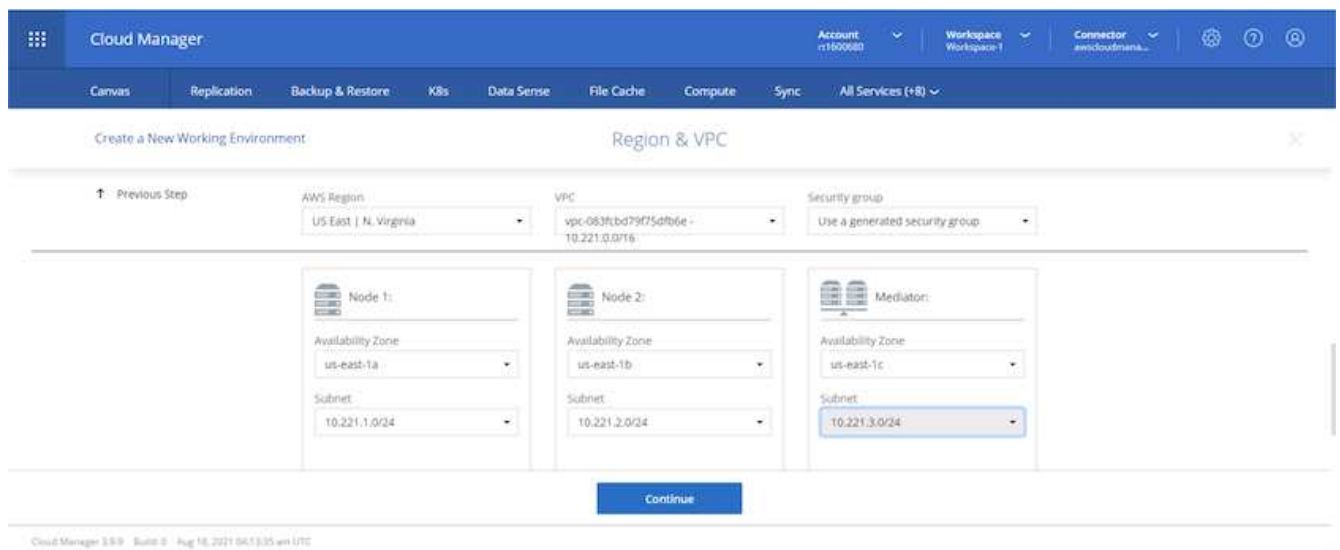
A 'Continue' button is at the bottom right.

Cloud Manager 3.9.9 Built 0 Aug 18, 2021 06:13:35 am UTC

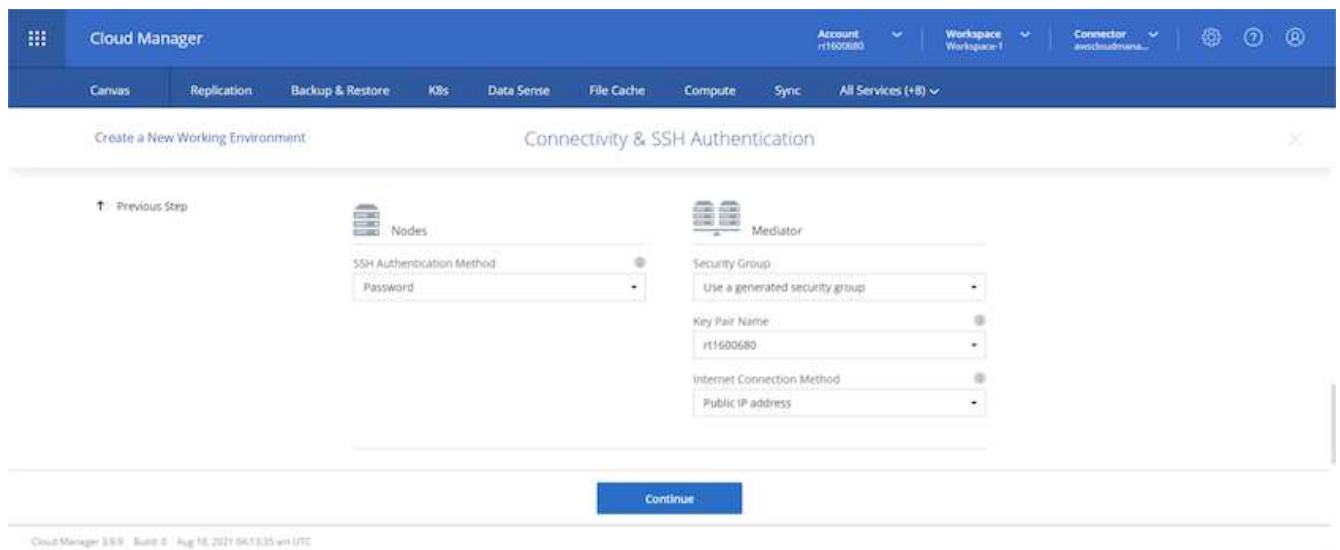
- Scegliere se eseguire l'implementazione in più zone di disponibilità (si recuperano tre subnet, ciascuna in un AZ diverso) o in una singola zona di disponibilità. Ho scelto più AZS.



13. Scegliere la regione, il VPC e il gruppo di sicurezza in cui implementare il cluster. In questa sezione, vengono assegnate anche le zone di disponibilità per nodo (e mediatore) e le subnet occupate.



14. Scegliere i metodi di connessione per i nodi e il mediatore.





Il mediatore richiede la comunicazione con le API AWS. Non è richiesto un indirizzo IP pubblico, purché le API siano raggiungibili dopo l'implementazione dell'istanza EC2 del mediatore.

1. Gli indirizzi IP mobili vengono utilizzati per consentire l'accesso ai vari indirizzi IP utilizzati da Cloud Volumes ONTAP, inclusi gli IP di gestione del cluster e di erogazione dei dati. Devono essere indirizzi non ancora instradabili all'interno della rete e aggiunti alle tabelle di routing nell'ambiente AWS. Questi sono necessari per abilitare indirizzi IP coerenti per una coppia ha durante il failover. Ulteriori informazioni sugli indirizzi IP mobili sono disponibili nella ["Documentazione sul cloud di NetApp"](#).

Cloud Manager

Account: r1618349 | Workspace: Workspace-1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) ▾

Create a New Working Environment

### Floating IPs

↑ Previous Step

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access. These floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an AWS transit gateway.

You must specify IP addresses that are outside of the CIDR blocks for all VPCs in the selected AWS region.

Floating IP address for cluster management  
10.222.0.200

Floating IP address 1 for NFS and CIFS data  
10.222.0.201

Floating IP address 2 for NFS and CIFS data  
10.222.0.202

Floating IP address for SVM management (Optional)  
Enter Floating IP Address

Continue

2. Selezionare le tabelle di routing a cui aggiungere gli indirizzi IP mobili. Queste tabelle di routing vengono utilizzate dai client per comunicare con Cloud Volumes ONTAP.

Cloud Manager

Account: r1600680 | Workspace: Workspace-1 | Connector: awscloudmana...

Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) ▾

Create a New Working Environment

### Route Tables

↑ Previous Step

Select the route tables that should include routes to the Floating IP addresses. This enables client access to the Cloud Volumes ONTAP HA pair. If you leave a route table unselected, clients that are associated with the route table cannot access the HA pair.

Additional information ⓘ

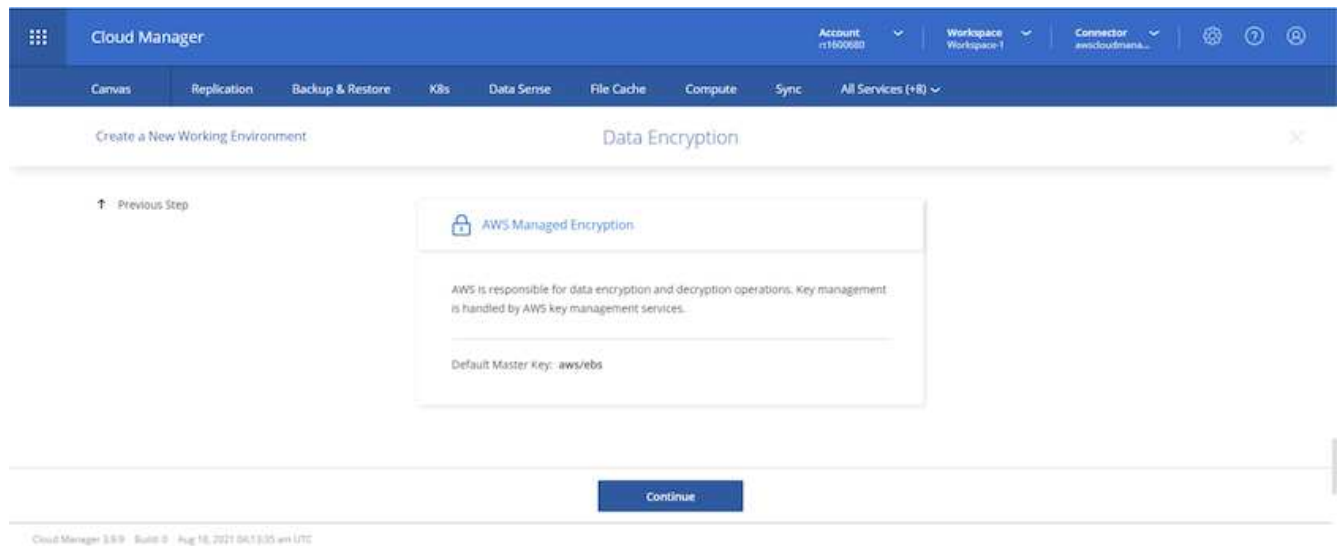
<input checked="" type="checkbox"/>	Name	Main	ID	Associate with Subnet	Tags
<input checked="" type="checkbox"/>	private_rt_r1600680	No	rtb-08b4cb88f5c826a5	3 Subnets	1 Tags
<input checked="" type="checkbox"/>	public_rt_r1600680	Yes	rtb-0e46720d0da10c593	1 Subnets	1 Tags

2 Route Tables | The main route table is the default for the VPC

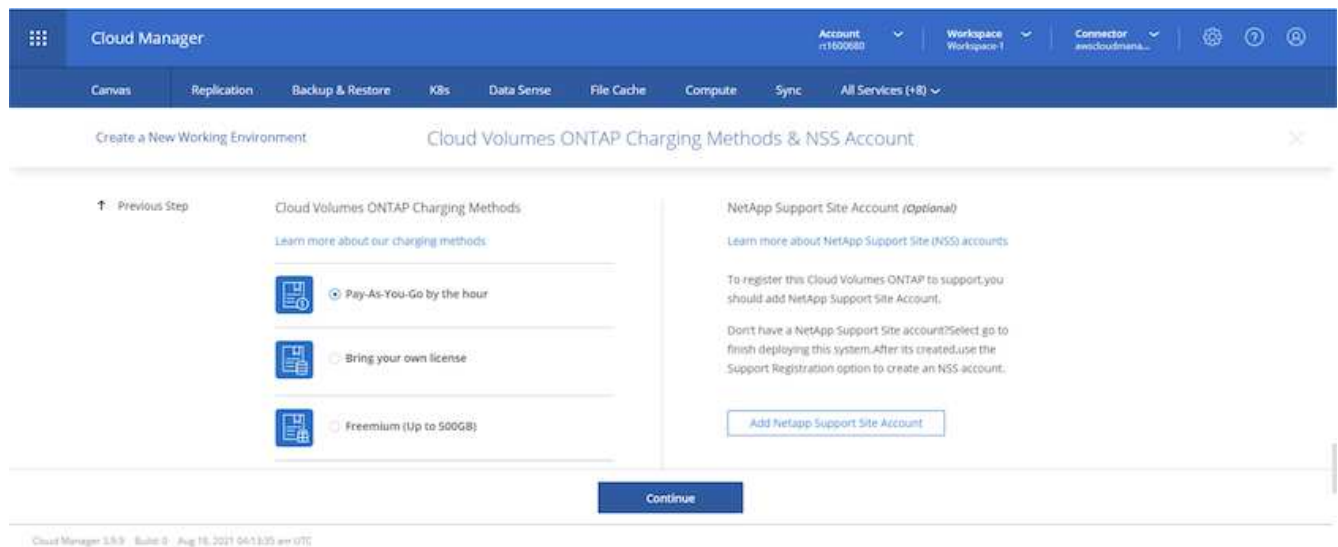
Continue

Cloud Manager 5.8.9 | Build 0 | Aug 18, 2021 06:13:35 am UTC

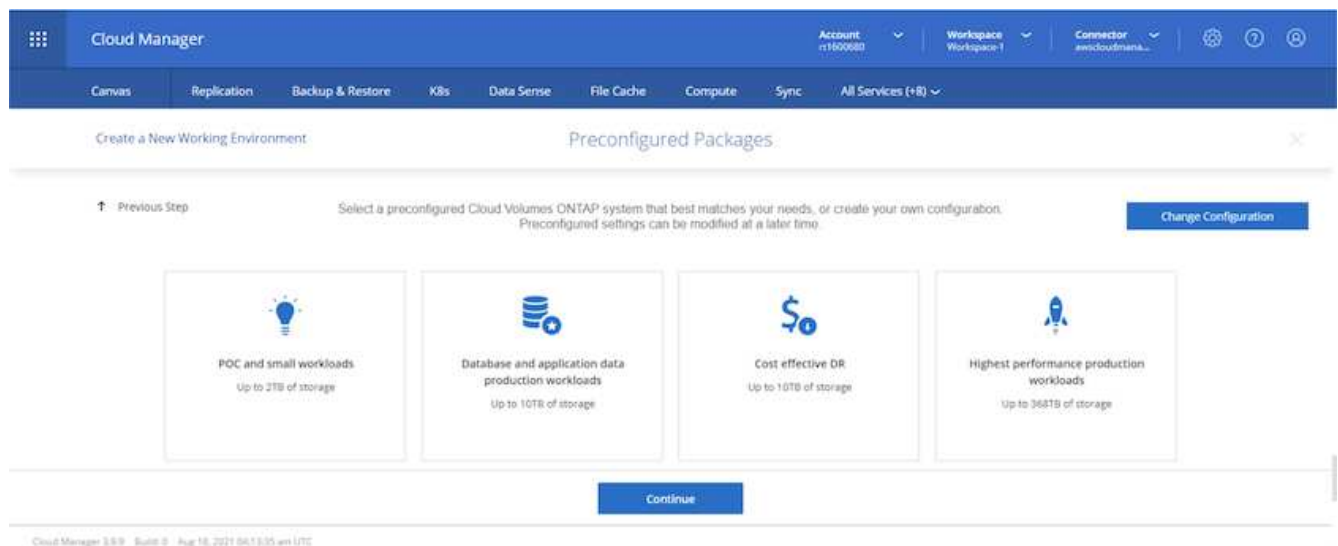
3. Scegliere se attivare la crittografia gestita AWS o AWS KMS per crittografare i dischi root, boot e dati ONTAP.



4. Scegli il tuo modello di licenza. Se non sai quale scegliere, contatta il tuo rappresentante NetApp.



5. Selezionare la configurazione più adatta al caso d'utilizzo. Ciò è correlato alle considerazioni sul dimensionamento trattate nella pagina dei prerequisiti.



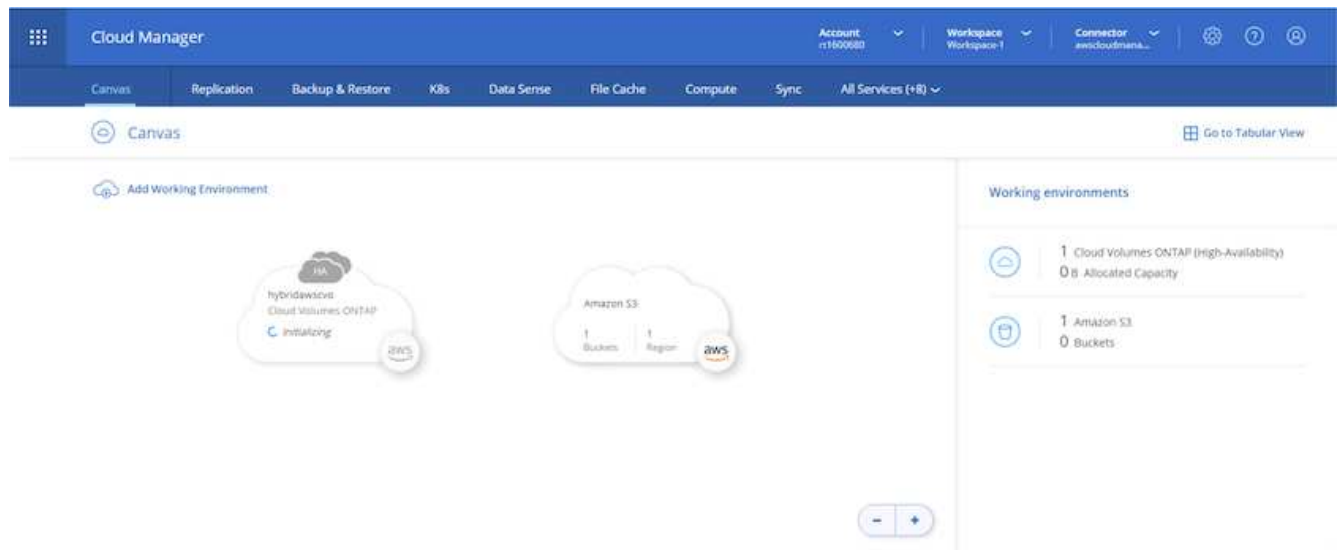
6. Se si desidera, creare un volume. Questo non è necessario, perché le fasi successive utilizzano SnapMirror, che crea i volumi per noi.

The screenshot shows the 'Create Volume' step in the Cloud Manager console. The interface includes a top navigation bar with 'Cloud Manager' and various service tabs like 'Canvas', 'Replication', 'Backup & Restore', etc. The main content area is titled 'Create a New Working Environment' and 'Create Volume'. It features a 'Details & Protection' section with fields for 'Volume Name', 'Size (GB)', 'Snapshot Policy', and 'Default Policy'. A 'Protocol' section on the right allows selection between 'NFS', 'CIFS', and 'iSCSI', with 'NFS' being the selected option. Below these are 'Access Control' and 'Custom export policy' settings. At the bottom, there are 'Continue' and 'Skip' buttons. A footer indicates 'Cloud Manager 3.8.9 Build 0 Aug 18, 2021 04:13:35 am UTC'.

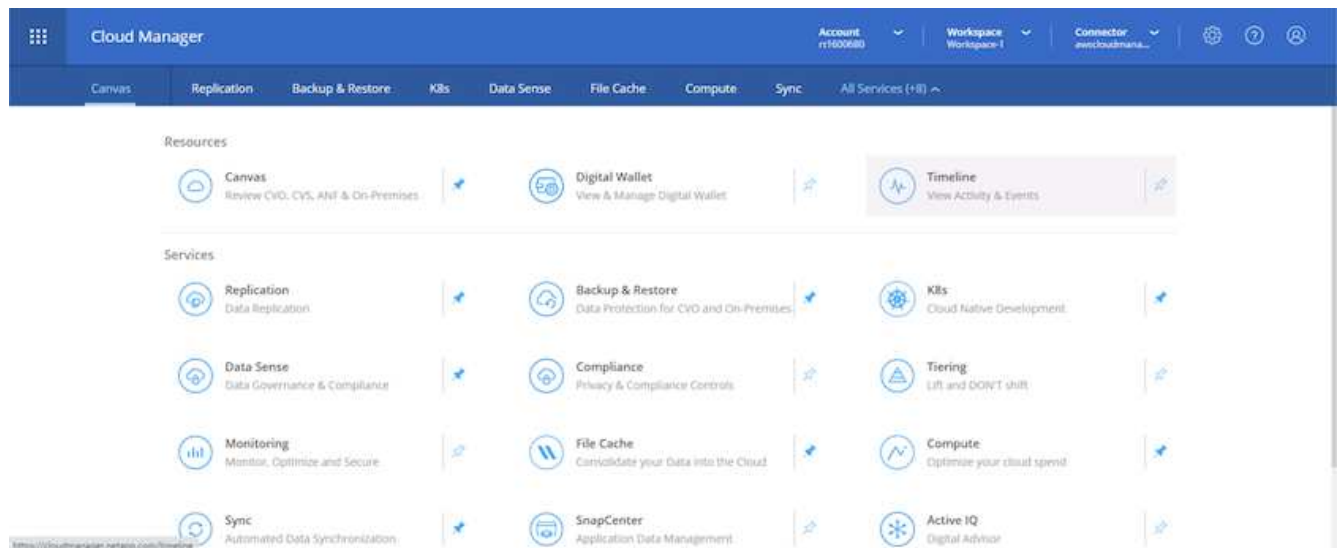
7. Esaminare le selezioni effettuate e spuntare le caselle per verificare che Cloud Manager implementa le risorse nel proprio ambiente AWS. Quando si è pronti, fare clic su Go (Vai).

The screenshot shows the 'Review & Approve' step in the Cloud Manager console. The interface includes a top navigation bar with 'Cloud Manager' and various service tabs. The main content area is titled 'Create a New Working Environment' and 'Review & Approve'. It features a 'hybridawscvo' section with tabs for 'AWS', 'us-east-1', and 'HA'. Below this are two checkboxes for terms and conditions, both of which are checked. A 'Show API request' link is also present. The 'Overview' tab is selected, showing a table with details about the storage system, license type, capacity limit, HA deployment model, encryption, and customer master key. At the bottom, there is a 'Go' button. A footer indicates 'Cloud Manager 3.8.9 Build 0 Aug 18, 2021 04:13:35 am UTC'.

8. Cloud Volumes ONTAP avvia ora il processo di implementazione. Cloud Manager utilizza le API AWS e gli stack di formazione del cloud per implementare Cloud Volumes ONTAP. Quindi, configura il sistema in base alle tue specifiche, offrendo un sistema pronto all'uso che può essere utilizzato immediatamente. I tempi di questo processo variano a seconda delle selezioni effettuate.



9. È possibile monitorare l'avanzamento passando alla Timeline.



10. La cronologia funge da audit di tutte le azioni eseguite in Cloud Manager. È possibile visualizzare tutte le chiamate API effettuate da Cloud Manager durante la configurazione di AWS e del cluster ONTAP. Questo può essere utilizzato in modo efficace anche per risolvere qualsiasi problema che si deve affrontare.

**Cloud Manager** Account: r1600680 Workspace: Workspace-1 Connector: awscloudmana...

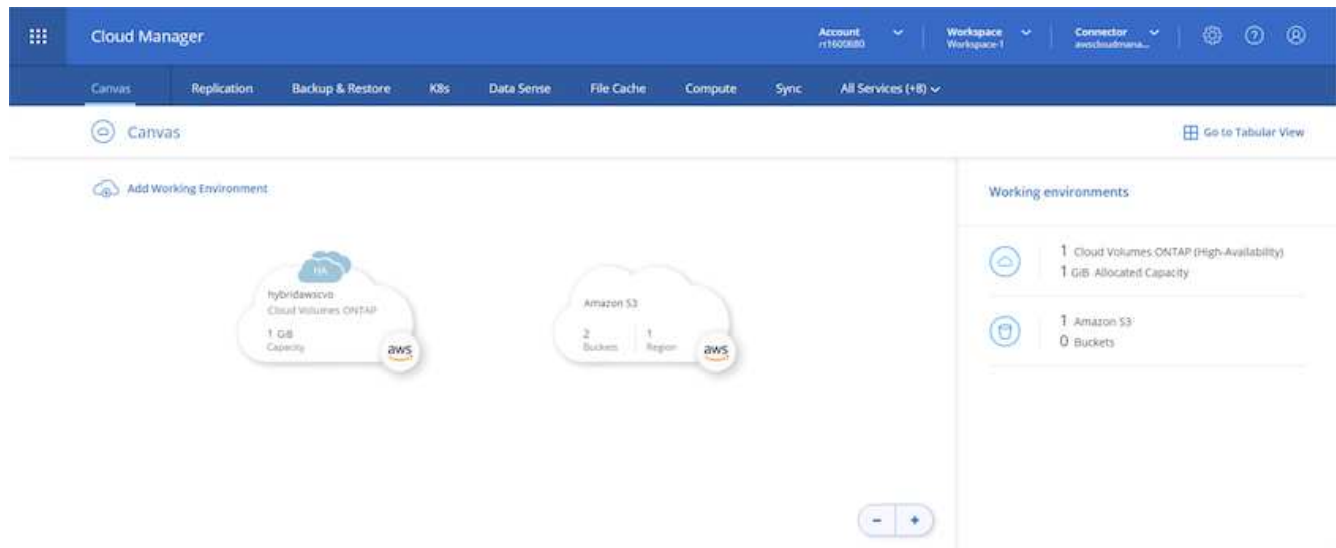
Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) v

Timeline

Filters: Time (1) Service Action Agent (1) Resource User Status Reset

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudman...	hybridawsco	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawsco	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 18 2021, 10:00:01 pm	Describe Operation Status					Success

11. Una volta completata l'implementazione, il cluster CVO viene visualizzato sul Canvas, che corrisponde alla capacità corrente. Il cluster ONTAP nello stato attuale è completamente configurato per consentire un'esperienza reale e immediata.

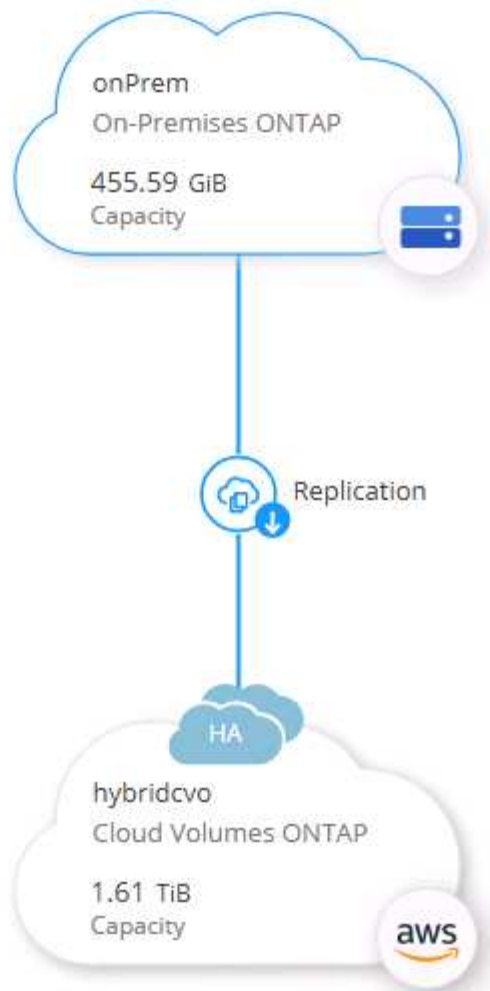


## Configurare SnapMirror da on-premise a cloud

Ora che hai implementato un sistema ONTAP di origine e un sistema ONTAP di destinazione, puoi replicare volumi contenenti dati di database nel cloud.

Per una guida sulle versioni compatibili di ONTAP per SnapMirror, consultare ["Matrice di compatibilità di SnapMirror"](#).

1. Fare clic sul sistema ONTAP di origine (on-premise) e trascinarlo nella destinazione, selezionare Replication > Enable (Replica > attiva) oppure selezionare Replication > Menu > Replicate (Replica > Menu > Replica).



Selezionare Enable (attiva).

#### SERVICES



Replication

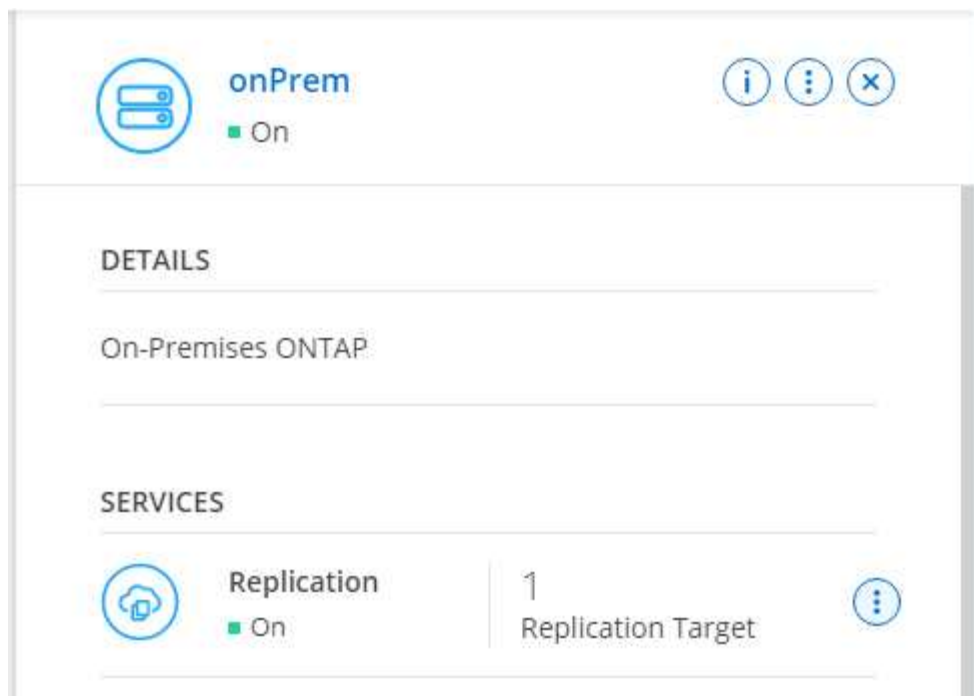
■ Off

Enable

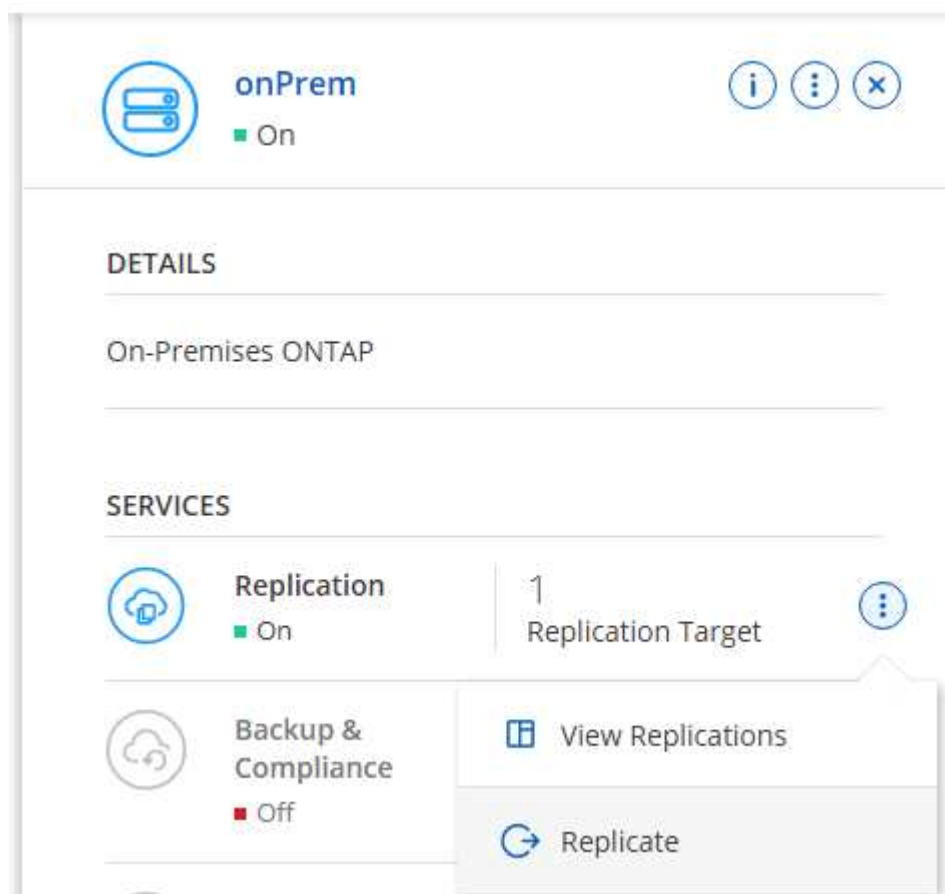


O Opzioni.

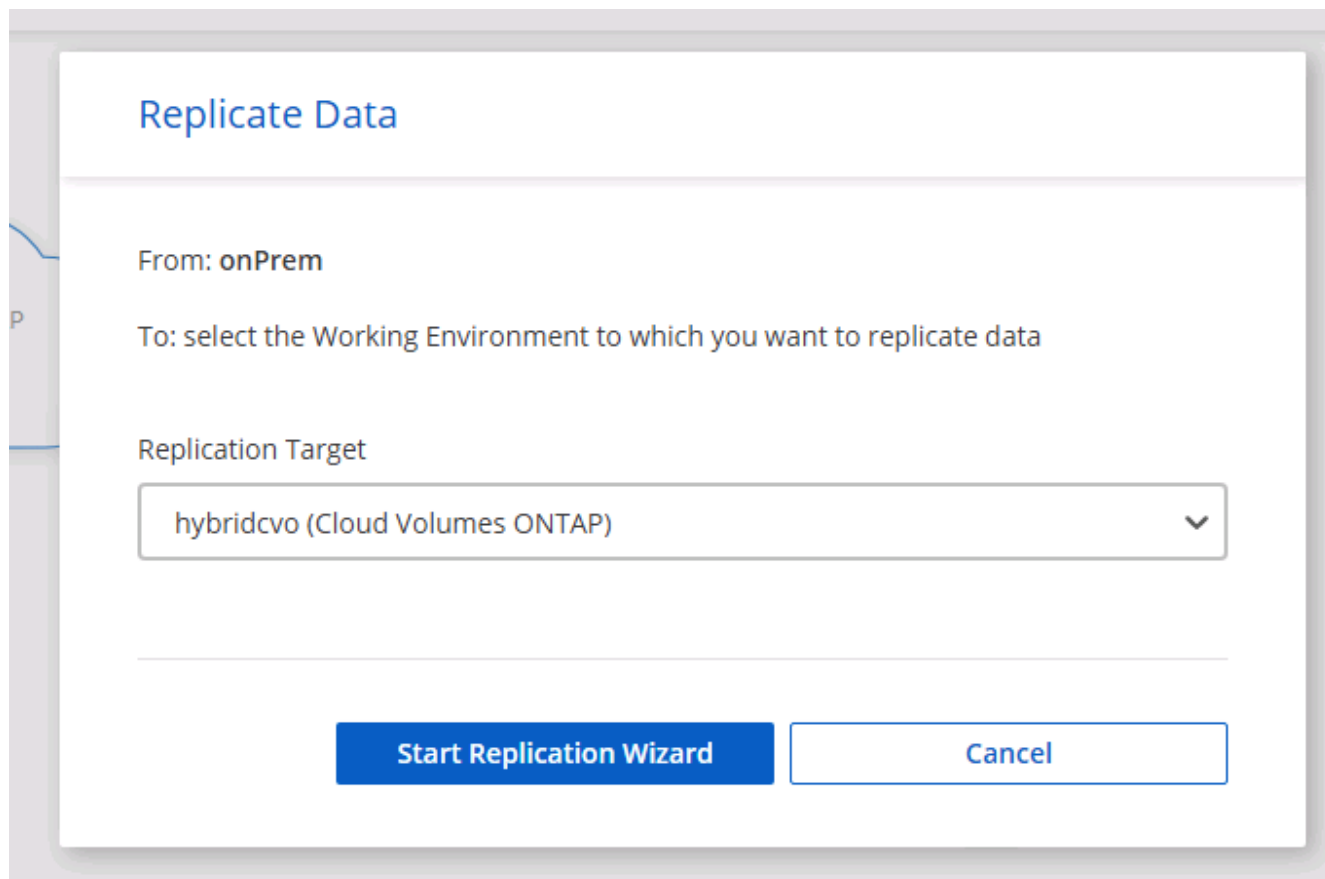




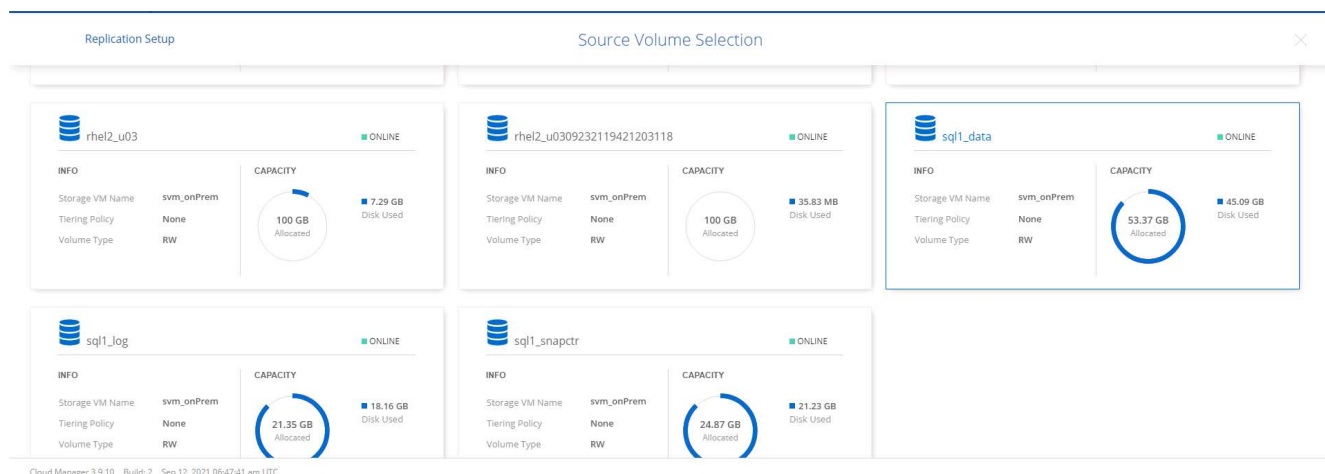
Replicare.



2. Se non è stato trascinato, scegliere il cluster di destinazione in cui replicare.



3. Scegliere il volume che si desidera replicare. Abbiamo replicato i dati e tutti i volumi di log.




4. Scegliere il tipo di disco di destinazione e il criterio di tiering. Per il disaster recovery, consigliamo un SSD come tipo di disco e per mantenere il tiering dei dati. Il tiering dei dati tiering i dati mirrorati in storage a oggetti a basso costo e consente di risparmiare denaro sui dischi locali. Quando si rompe la relazione o si clonano i volumi, i dati utilizzano lo storage locale veloce.


Replication Setup Destination Disk Type and Tiering ×


---


[↑ Previous Step](#)

Destination Disk Type

  
General Purpose SSD

  
General Purpose SSD - Dynamic Performance

  
Throughput Optimized HDD

 S3 Tiering [What are storage tiers?](#)

☒ Enabled ☐ Disabled

Note: If you enable S3 tiering, thin provisioning must be enabled on volumes created in this aggregate.

Continue

---

Cloud Manager 3.9.10 Build: 2 Sep 12, 2021 06:47:41 am UTC

5. Selezionare il nome del volume di destinazione scelto `[source_volume_name]_dr`.

---

## Destination Volume Name

---

Destination Volume Name

`sql1_data_dr`

Destination Aggregate

Automatically select the best aggregate ▼

6. Selezionare la velocità di trasferimento massima per la replica. Ciò consente di risparmiare larghezza di banda se si dispone di una connessione a bassa larghezza di banda al cloud, ad esempio una VPN.

## Max Transfer Rate

You should limit the transfer rate. An unlimited rate might negatively impact the performance of other applications and it might impact your Internet performance.


- ☒ Limited to:  MB/s
- ☐ Unlimited (recommended for DR only machines)

7. Definire il criterio di replica. Abbiamo scelto un Mirror, che prende i dataset più recenti e li replica nel volume di destinazione. Puoi anche scegliere una policy diversa in base ai tuoi requisiti.

## Replication Policy


Default Policies

Additional Policies

 Mirror

Typically used for disaster recovery

More info

 Mirror and Backup (1 month retention)

Configures disaster recovery and long-term retention of backups on the same destination volume

More info

8. Scegliere la pianificazione per l'attivazione della replica. NetApp consiglia di impostare una pianificazione "giornaliera" di per il volume di dati e una pianificazione "oraria" per i volumi di log, sebbene sia possibile modificarla in base ai requisiti.

Replication Setup Schedule

---

↑ Previous Step Select a replication schedule

One-time copy

No schedule

10min

Every hour  
Minutes: 0th, 10th, 20th, 3...

12-hourly

Every day  
Hours: 12 AM and 12 PM  
Minutes: 15th minute

5min

Every hour  
Minutes: 0th, 5th, 10th, 15t...

6-hourly

Every day  
Hours: 12 AM, 6 AM, 12 PM...  
Minutes: 15th minute

8hour

Every day  
Hours: 2 AM, 10 AM and 6 ...  
Minutes: 15th minute

daily

Every day  
Hours: 12 AM  
Minutes: 10th minute

hourly

Every hour  
Minutes: 5th minute

monthly

Every month  
Days: 2nd  
Hours: 12 AM  
Minutes: 20th minute

pg-15-minutely

Every hour

pg-6-hourly

Every day

pg-daily

Every day

pg-daily-set2

Every day

9. Esaminare le informazioni immesse, fare clic su Go (Vai) per attivare il peer del cluster e il peer SVM (se si tratta della prima replica tra i due cluster), quindi implementare e inizializzare la relazione SnapMirror.

Replication Setup Review & Approve

---

↑ Previous Step Review your selection and start the replication process

Source

onPrem

sql1\_data

Destination

hybridcvo

sql1\_data\_copy

☒ I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements.  
[More information >](#)

Source Volume Allocated Size:	53.37 GB	Destination Thin Provisioning:	Yes
Source Volume Used Size:	45.09 GB	Destination Aggregate:	aggr1 (Automatically s...
Source Thin Provisioning:	Yes	Destination Storage VM:	svm_hybridcvo
Destination Volume Allocated Size:	53.37 GB	Max Transfer Rate:	100 MB/s
Destination Volume Disk Type:	General Purpose SSD (...)	SnapMirror Policy:	Mirror
Capacity Tiering:	S3	Replication Schedule:	daily

[Go](#)

10. Continuare questa procedura per i volumi di dati e i volumi di log.
11. Per controllare tutte le relazioni, accedere alla scheda Replication (Replica) in Cloud Manager. Qui puoi gestire le tue relazioni e verificare il loro stato.

Replication

7 Volume Relationships

153.32 GiB Replicated Capacity

0 Currently Transferring

7 Healthy

0 Failed

7 Volume Relationships 🔍 ↻

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	
	rhel2_u01 onPrem	rhel2_u01_dr hybridcvo	43 minutes 43 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:50 AI 19.73 MiB	...
	rhel2_u02 onPrem	rhel2_u02_dr hybridcvo	1 hour 37 minutes 59 seconds	idle	snapmirrored	Sep 30, 2021, 2:37:08 PM 239.78 MiB	...
	rhel2_u03 onPrem	rhel2_u03_dr hybridcvo	16 hours 1 minute 9 seconds	idle	snapmirrored	Sep 30, 2021, 4:07:14 PM 225.37 KiB	...
	sql1_data onPrem	sql1_data_dr hybridcvo	1 hour 6 minutes 50 seconds	idle	snapmirrored	Sep 30, 2021, 12:12:28 AI 24.56 KiB	...

12. Una volta replicati tutti i volumi, si è in uno stato stabile e si è pronti per passare ai flussi di lavoro di disaster recovery e di sviluppo/test.

### 3. Implementare l'istanza di calcolo EC2 per il carico di lavoro del database

AWS ha preconfigurato istanze di calcolo EC2 per diversi carichi di lavoro. La scelta del tipo di istanza determina il numero di core della CPU, la capacità della memoria, il tipo e la capacità di storage e le performance di rete. Per i casi di utilizzo, ad eccezione della partizione del sistema operativo, lo storage principale per eseguire il carico di lavoro del database viene allocato da CVO o dal motore di storage FSX ONTAP. Pertanto, i fattori principali da considerare sono la scelta dei core della CPU, la memoria e il livello di performance di rete. I tipi di istanze tipiche di AWS EC2 sono disponibili qui: ["Tipo di istanza EC2"](#).

#### Dimensionamento dell'istanza di calcolo

1. Selezionare il tipo di istanza corretto in base al carico di lavoro richiesto. I fattori da considerare includono il numero di transazioni di business da supportare, il numero di utenti simultanei, il dimensionamento dei set di dati e così via.
2. L'implementazione dell'istanza EC2 può essere avviata tramite il dashboard EC2. Le procedure di implementazione esulano dall'ambito di questa soluzione. Vedere ["Amazon EC2"](#) per ulteriori informazioni.

#### Configurazione dell'istanza di Linux per il carico di lavoro Oracle

Questa sezione contiene ulteriori passaggi di configurazione dopo la distribuzione di un'istanza EC2 Linux.

1. Aggiungere un'istanza di standby Oracle al server DNS per la risoluzione dei nomi all'interno del dominio di gestione SnapCenter.
2. Aggiungere un ID utente di gestione Linux come credenziali del sistema operativo SnapCenter con autorizzazioni sudo senza password. Attivare l'ID con l'autenticazione della password SSH sull'istanza EC2. (Per impostazione predefinita, l'autenticazione della password SSH e il sudo senza password sono disattivati sulle istanze EC2).
3. Configurare l'installazione di Oracle in modo che corrisponda all'installazione Oracle on-premise, ad esempio patch del sistema operativo, versioni e patch di Oracle e così via.
4. I ruoli di automazione Ansible DB di NetApp possono essere sfruttati per configurare le istanze EC2 per i casi di utilizzo di sviluppo/test di database e disaster recovery. Il codice di automazione può essere scaricato dal sito GitHub pubblico di NetApp: ["Implementazione automatizzata di Oracle 19c"](#). L'obiettivo è quello di installare e configurare uno stack software di database su un'istanza EC2 in modo che corrisponda alle configurazioni del sistema operativo e del database on-premise.

#### Configurazione dell'istanza di Windows per il carico di lavoro di SQL Server

In questa sezione sono elencati ulteriori passaggi di configurazione dopo la distribuzione iniziale di un'istanza di EC2 Windows.

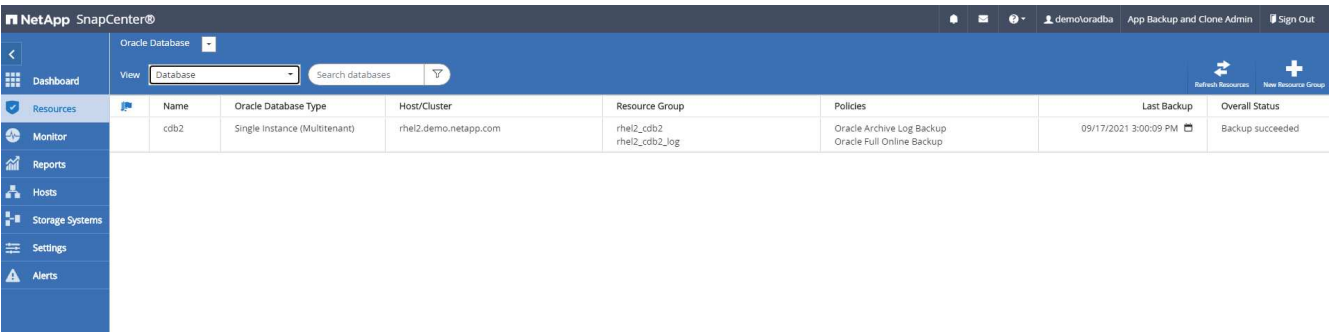
1. Recuperare la password dell'amministratore di Windows per accedere a un'istanza tramite RDP.
2. Disattivare il firewall Windows, unire l'host al dominio Windows SnapCenter e aggiungere l'istanza al server DNS per la risoluzione dei nomi.
3. Eseguire il provisioning di un volume di log di SnapCenter per memorizzare i file di log di SQL Server.
4. Configurare iSCSI sull'host Windows per montare il volume e formattare il disco.
5. Ancora una volta, molte delle attività precedenti possono essere automatizzate con la soluzione di automazione NetApp per SQL Server. Consulta il sito GitHub pubblico di automazione di NetApp per i ruoli e le soluzioni pubblicati di recente: ["Automazione NetApp"](#).

## Workflow per sviluppo/test bursting nel cloud

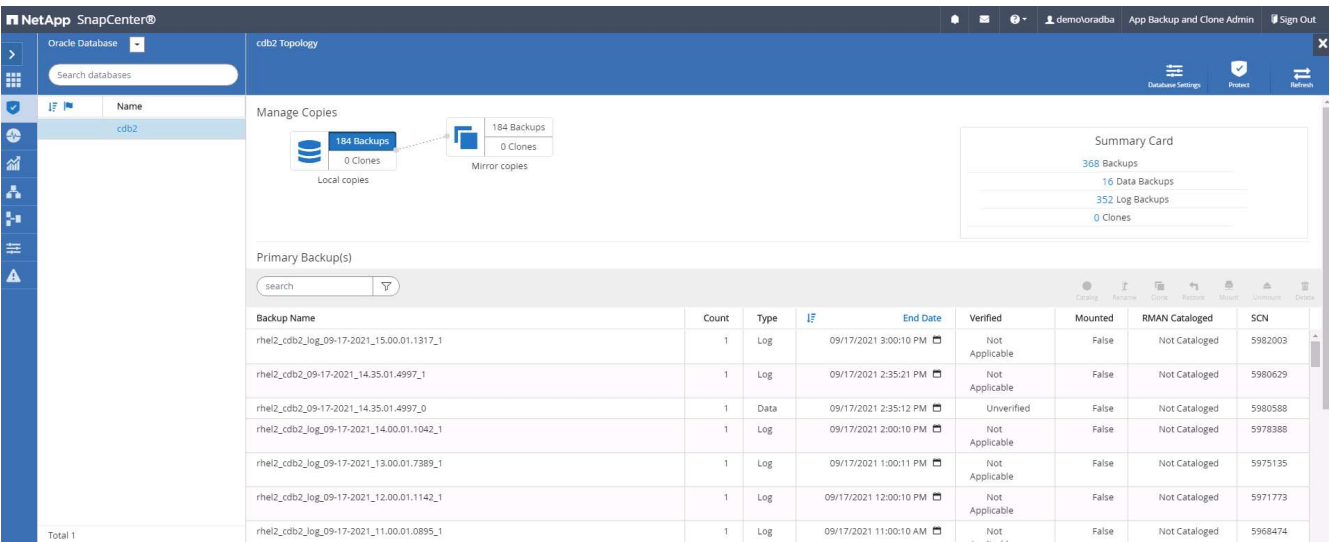
L'agilità del cloud pubblico, il time-to-value e i risparmi sui costi sono tutte proposte di valore significative per le aziende che adottano il cloud pubblico per lo sviluppo e il test delle applicazioni di database. Non esiste uno strumento migliore di SnapCenter per trasformare questo in realtà. SnapCenter non solo può proteggere il database di produzione on-premise, ma può anche clonare rapidamente una copia per lo sviluppo di applicazioni o il test del codice nel cloud pubblico, consumando pochissimo storage aggiuntivo. Di seguito sono riportati i dettagli dei processi passo-passo per l'utilizzo di questo strumento.

### Clonare un database Oracle per lo sviluppo/test da un backup di snapshot replicato

1. Accedere a SnapCenter con un ID utente per la gestione del database per Oracle. Accedere alla scheda risorse, che mostra i database Oracle protetti da SnapCenter.



2. Fare clic sul nome del database on-premise desiderato per la topologia di backup e la vista dettagliata. Se è attivata una posizione replicata secondaria, vengono visualizzati i backup mirror collegati.



3. Per passare alla vista dei backup mirrorati, fare clic su Backup mirrorati. Vengono quindi visualizzati i backup dei mirror secondari.

NetApp SnapCenter®

Oracle Database cdb2 Topology

Search databases

Manage Copies

Local copies: 184 Backups, 0 Clones

Mirror copies: 184 Backups, 0 Clones

Summary Card

- 368 Backups
- 16 Data Backups
- 352 Log Backups
- 0 Clones

Secondary Mirror Backup(s)

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_log_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388
rhel2_cdb2_log_09-17-2021_13.00.01.7389_1	1	Log		09/17/2021 1:00:11 PM	Not Applicable	False	Not Cataloged	5975135
rhel2_cdb2_log_09-17-2021_12.00.01.1142_1	1	Log		09/17/2021 12:00:10 PM	Not Applicable	False	Not Cataloged	5971773
rhel2_cdb2_log_09-17-2021_11.00.01.0895_1	1	Log		09/17/2021 11:00:10 AM	Not Applicable	False	Not Cataloged	5968474

Total 1

- Scegliere una copia di backup del database secondario mirrorata da clonare e determinare un punto di ripristino in base all'ora e al numero di modifica del sistema o in base alla SCN. In genere, il punto di ripristino deve essere sottoposto a un periodo di tempo inferiore rispetto al tempo di backup completo del database o alla data SCN da clonare. Dopo aver deciso un punto di ripristino, il backup del file di registro richiesto deve essere montato per il ripristino. Il backup del file di log deve essere montato sul server DB di destinazione in cui deve essere ospitato il database clone.

Mount backups

Choose the host to mount the backup: ora-standby.demo.netapp.com

Mount path : /var/opt/snapcenter/sco/backup\_mount/rhel2\_cdb2\_09-17-2021\_14.35.01.4997\_1/cdb2

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:rhel2_u03	svm_hybridcvo:rhel2_u03_dr

Mount Cancel



NetApp SnapCenter®

Oracle Database

Search databases

cdb2 Topology

Manage Copies

184 Backups  
0 Clones  
Local copies

184 Backups  
1 Clone  
Mirror copies

Summary Card

368 Backups  
16 Data Backups  
352 Log Backups  
1 Clone

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_log_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388



Se la funzione di eliminazione dei log è attivata e il punto di ripristino viene esteso oltre l'ultima eliminazione dei log, potrebbe essere necessario montare più backup dei log di archiviazione.

- Evidenziare la copia di backup completa del database da clonare, quindi fare clic sul pulsante clone per avviare il flusso di lavoro del clone del database.

cdb2 Topology

search

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	True	Not Cataloged	5980629
rhel2_cdb2_log_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588
rhel2_cdb2_log_09-17-2021_14.00.01.1042_1	1	Log		09/17/2021 2:00:10 PM	Not Applicable	False	Not Cataloged	5978388

- Scegliere un SID DB clone appropriato per un database container completo o un clone CDB.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

☒ Complete Database Clone

Clone SID

cdb2test

Exclude PDBs

Type to find PDBs

☐ PDB Clone

Secondary storage location : Snap Vault / Snap Mirror

Data

Source Volume

svm\_onPrem:rhel2\_u02

Destination Volume

svm\_hybridcvo:rhel2\_u02\_dr

Logs

Source Volume

svm\_onPrem:rhel2\_u03

Destination Volume

svm\_hybridcvo:rhel2\_u03\_dr

Previous

Next

- Selezionare l'host clone di destinazione nel cloud e le directory del file di dati, del file di controllo e del log di ripristino vengono create dal flusso di lavoro del clone.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

Select the host to create a clone

Clone host
ora-standby.demo.netapp.com

Datafile locations ⓘ

/u02\_cdb2test
Reset

Control files ⓘ

/u02\_cdb2test/cdb2test/control/control01.ctl
/u02\_cdb2test/cdb2test/control/control02.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
<div> <div> RedoGroup 1 </div> <div> </div> </div>	200	MB	1
/u02_cdb2test/cdb2test/redolog/redolog3.log			
<div> <div> RedoGroup 2 </div> <div> </div> </div>	200	MB	1

Previous
Next

8. Il nome della credenziale Nessuno viene utilizzato per l'autenticazione basata sul sistema operativo, rendendo la porta del database irrilevante. Compilare i campi Oracle Home, Oracle OS User e Oracle OS Group appropriati, come configurati nel server DB clone di destinazione.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user

None

+

i

Database port

1521

Oracle Home Settings

i

Oracle Home

/u01/app/oracle/product/19800/cdb2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

9. Specificare gli script da eseguire prima dell'operazione di clonazione. Cosa ancora più importante, il parametro dell'istanza del database può essere modificato o definito qui.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

5

6

7

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

processes	320	×
remote_login_passwordfile	EXCLUSIVE	×
sga_target	4311744512	×
undo_tablespace	UNDOTBS1	×

+

Reset

Previous

Next

10. Specificare il punto di ripristino in base alla data e all'ora o alla SCN. Fino a quando Annulla ripristina il database fino ai log di archiviazione disponibili. Specificare la posizione del log di archiviazione esterno dall'host di destinazione in cui è montato il volume del log di archiviazione. Se il proprietario del server di destinazione Oracle è diverso dal server di produzione on-premise, verificare che la directory del log di archiviazione sia leggibile dal proprietario del server di destinazione Oracle.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

☒ Recover Database

☐ Until Cancel

☐ Date and Time

☒ Until SCN (System Change Number)
 

5980629

Date-time format: MM/DD/YYYY hh:mm:ss

Specify external archive log locations

/var/opt/snapcenter/sco/backup\_mount/rhel2\_cdb2\_09-17-2021\_14.35.01.4997\_1/cdb2/1/orareco/CDB2/archivelog/

☒ Create new DBID

☒ Create tempfile for temporary tablespace

☐ Enter SQL queries to apply when clone is created

☐ Enter scripts to run after clone operation

Previous

Next

```

oracle@ora-standby/tmp
[oracle@ora-standby tmp]$ ls /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_09-17-2021_14.35.01.4997_1/cdb2/1/orareco/CDB2/archivelog/
2021_08_26 2021_08_28 2021_08_30 2021_09_01 2021_09_03 2021_09_05 2021_09_07 2021_09_09 2021_09_11 2021_09_13 2021_09_15 2021_09_17
2021_08_27 2021_08_29 2021_08_31 2021_09_02 2021_09_04 2021_09_06 2021_09_08 2021_09_10 2021_09_12 2021_09_14 2021_09_16
[oracle@ora-standby tmp]$
  
```

11. Configurare il server SMTP per la notifica via email, se lo si desidera.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

⚠

If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

12. Riepilogo dei cloni.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

Summary

Clone from backup

rhel2\_cdb2\_09-17-2021\_14.35.01.4997\_0

Clone SID

cdb2test

Clone server

ora-standby.demo.netapp.com

Exclude PDBs

none

Oracle home

/u01/app/oracle/product/19800/cdb2

Oracle OS user

oracle

Oracle OS group

oinstall

Datafile mountpaths

/u02\_cdb2test

Control files

/u02\_cdb2test/cdb2test/control/control01.ctl

/u02\_cdb2test/cdb2test/control/control02.ctl

Redo groups

RedoGroup =1 TotalSize =200 Path =/u02\_cdb2test/cdb2test/redolog/redo03.log

RedoGroup =2 TotalSize =200 Path =/u02\_cdb2test/cdb2test/redolog/redo02.log

RedoGroup =3 TotalSize =200 Path =/u02\_cdb2test/cdb2test/redolog/redo01.log

Recovery scope

Until SCN 5980629

Prescript full path

none

Prescript arguments

Postscript full path

none

Postscript arguments

Previous

Finish

13. Dopo il cloning, è necessario eseguire la convalida per assicurarsi che il database clonato sia operativo. Alcune attività aggiuntive, come l'avvio del listener o la disattivazione della modalità di archiviazione del registro DB, possono essere eseguite sul database di sviluppo/test.

```

oracle@ora-standby/tmp
[oracle@ora-standby tmp]$ export ORACLE_SID=cdb2test
[oracle@ora-standby tmp]$ export ORACLE_HOME=/u01/app/oracle/product/19800/cdb2
[oracle@ora-standby tmp]$ export PATH=$PATH:$ORACLE_HOME/bin
[oracle@ora-standby tmp]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 17:49:29 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> select name, log_mode from v$database;

NAME          LOG MODE
-----
CDB2TEST      ARCHIVELOG

SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME
-----
HOST_NAME
-----
cdb2test
ora-standby.demo.netapp.com

SQL> show pdbs

  CON_ID CON_NAME              OPEN MODE RESTRICTED
  -
2 PDB$SEED                  READ ONLY NO
3 CDB2_PDB1                  READ WRITE NO
4 CDB2_PDB2                  READ WRITE NO
5 CDB2_PDB3                  READ WRITE NO

SQL>

```



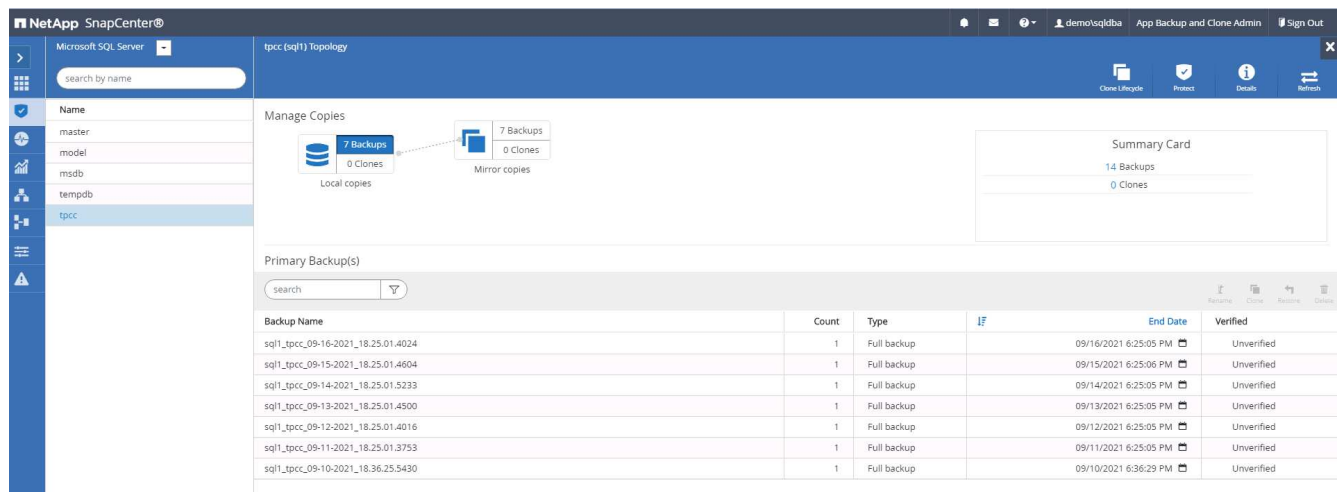
## Clonare un database SQL per lo sviluppo/test da un backup Snapshot replicato

1. Accedere a SnapCenter con un ID utente per la gestione del database per SQL Server. Accedere alla scheda risorse, che mostra i database degli utenti SQL Server protetti da SnapCenter e un'istanza SQL di standby di destinazione nel cloud pubblico.



Name	Instance	Host	Last Backup	Overall Status	Type
master	sql1	sql1.demo.netapp.com		Not available for backup	System database
model	sql1	sql1.demo.netapp.com		Not available for backup	System database
msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database
tpcc	sql1	sql1.demo.netapp.com	09/16/2021 7:35:05 PM	Backup succeeded	User database
master	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
model	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
msdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database
tempdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database

2. Fare clic sul nome del database utente SQL Server on-premise desiderato per la topologia dei backup e la vista dettagliata. Se è attivata una posizione replicata secondaria, vengono visualizzati i backup mirror collegati.



tpcc (sql1) Topology

Manage Copies

Local copies: 7 Backups, 0 Clones. Mirror copies: 7 Backups, 0 Clones.

Summary Card

14 Backups, 0 Clones

Primary Backup(s)

Backup Name	Count	Type	IF	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup		09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup		09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup		09/10/2021 6:36:29 PM	Unverified

3. Passare alla vista dei backup mirrorati facendo clic su Backup mirrorati. Vengono quindi visualizzati i backup mirror secondari. Poiché SnapCenter esegue il backup del log delle transazioni di SQL Server su un'unità dedicata per il ripristino, vengono visualizzati solo i backup completi del database.

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

search by name

Clone Library | Protect | Details | Refresh

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 0 Clones

Summary Card

14 Backups

0 Clones

Secondary Mirror Backup(s)

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified
sql1_tpcc_09-12-2021_18.25.01.4016	1	Full backup		09/12/2021 6:25:05 PM	Unverified
sql1_tpcc_09-11-2021_18.25.01.3753	1	Full backup		09/11/2021 6:25:05 PM	Unverified
sql1_tpcc_09-10-2021_18.36.25.5430	1	Full backup		09/10/2021 6:36:29 PM	Unverified

4. Scegliere una copia di backup, quindi fare clic sul pulsante Clone (Copia) per avviare il flusso di lavoro Clone from Backup (Copia da backup).

NetApp SnapCenter®

Microsoft SQL Server

tpcc (sql1) Topology

search by name

Clone Library | Protect | Details | Refresh

Manage Copies

Local copies: 7 Backups, 0 Clones

Mirror copies: 7 Backups, 1 Clone

Summary Card

14 Backups

1 Clone

Secondary Mirror Backup(s)

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup		09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup		09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup		09/17/2021 6:25:05 PM	Unverified
sql1_tpcc_09-16-2021_18.25.01.4024	1	Full backup		09/16/2021 6:25:05 PM	Unverified
sql1_tpcc_09-15-2021_18.25.01.4604	1	Full backup		09/15/2021 6:25:06 PM	Unverified
sql1_tpcc_09-14-2021_18.25.01.5233	1	Full backup		09/14/2021 6:25:05 PM	Unverified
sql1_tpcc_09-13-2021_18.25.01.4500	1	Full backup		09/13/2021 6:25:05 PM	Unverified

Clone from backup

1 Clone Options
2 Logs
3 Script
4 Notification
5 Summary

### Clone settings

Clone server
Choose

Clone instance
Nothing selected

Clone name
tpcc

### Choose mount option

☒ Auto assign mount point
☐ Auto assign volume mount point under path
full file path

### Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous
Next

- Selezionare un server cloud come server clone di destinazione, nome istanza clone e nome database clone. Scegliere un punto di montaggio ad assegnazione automatica o un percorso del punto di montaggio definito dall'utente.

Clone from backup

1 Clone Options
2 Logs
3 Script
4 Notification
5 Summary

Clone settings

Clone server
sql-standby.demo.netapp.com

Clone instance
sql-standby

Clone name
tpcc\_clone

Choose mount option

☒ Auto assign mount point
☐ Auto assign volume mount point under path
full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous
Next

6. Determinare un punto di ripristino in base all'ora di backup del registro o a una data e un'ora specifiche.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

☐ All log backups

☒ By log backups until

9/17/2021 6:25:10 PM

☐ By specific date until

09/17/2021 6:25:05 PM

☐ None

Previous

Next

7. Specificare gli script opzionali da eseguire prima e dopo l'operazione di cloning.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments

Choose optional arguments...

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

8. Configurare un server SMTP se si desidera inviare una notifica via email.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

9. Riepilogo dei cloni.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Summary

Clone server	sql-standby.demo.netapp.com
Clone instance	sql-standby
Clone name	tpcc_dev
Mount option	Auto assign volume mount point under custom path
Prescript full path	None
Prescript arguments	
Postscript full path	None
Postscript arguments	
Send email	No

Previous

Finish

- Monitorare lo stato del processo e verificare che il database utente desiderato sia stato collegato a un'istanza SQL di destinazione nel server clone cloud.

NetApp SnapCenter®						
Jobs - Filter						
	ID	Status	Name	Start date	End date	Owner
	766	✓	Clone from backup 'sql1_tpcc-09-16-2021_18.25.01.4024'	09/16/2021 8:05:25 PM	09/16/2021 8:06:17 PM	demo:sqlqdba
	763	✓	Discover resources for all hosts	09/16/2021 7:56:49 PM	09/16/2021 7:56:54 PM	demo:sqlqdba
	761	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 7:35:00 PM	09/16/2021 7:37:08 PM	demo:sqlqdba
	760	⚠	Discover resources for all hosts	09/16/2021 7:19:05 PM	09/16/2021 7:19:09 PM	demo:sqlqdba
	759	⚠	Discover resources for all hosts	09/16/2021 7:18:43 PM	09/16/2021 7:18:48 PM	demo:sqlqdba
	756	⚠	Discover resources for all hosts	09/16/2021 6:59:51 PM	09/16/2021 6:59:56 PM	demo:sqlqdba
	753	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 6:35:00 PM	09/16/2021 6:37:07 PM	demo:sqlqdba
	750	✓	Backup of Resource Group 'sql1_tpcc' with policy 'SQL Server Full Backup'	09/16/2021 6:25:01 PM	09/16/2021 6:27:14 PM	demo:sqlqdba
	749	✓	Discover resources for host 'sql-standby.demo.netapp.com'	09/16/2021 6:19:00 PM	09/16/2021 6:19:05 PM	DemoAdministrator
	745	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/16/2021 5:35:00 PM	09/16/2021 5:37:08 PM	demo:sqlqdba

## Configurazione post-clone

- Un database di produzione Oracle on-premise viene in genere eseguito in modalità di archiviazione dei log. Questa modalità non è necessaria per un database di sviluppo o test. Per disattivare la modalità di archiviazione dei log, accedere a Oracle DB come sysdba, eseguire un comando di modifica della modalità di log e avviare il database per l'accesso.
- Configurare un listener Oracle o registrare il database appena clonato con un listener esistente per l'accesso dell'utente.
- Per SQL Server, modificare la modalità di log da Full a Easy in modo che il file di log di sviluppo/test di SQL Server possa essere facilmente ridotto quando si riempie il volume di log.



## Aggiornare il database dei cloni

1. Eliminare i database clonati e ripulire l'ambiente del server DB cloud. Seguire quindi le procedure precedenti per clonare un nuovo database con nuovi dati. La clonazione di un nuovo database richiede solo pochi minuti.
2. Chiudere il database dei cloni, eseguire un comando di refresh dei cloni utilizzando la CLI. Per ulteriori informazioni, consultare la seguente documentazione SnapCenter: ["Aggiornare un clone"](#).

## Dove cercare aiuto?

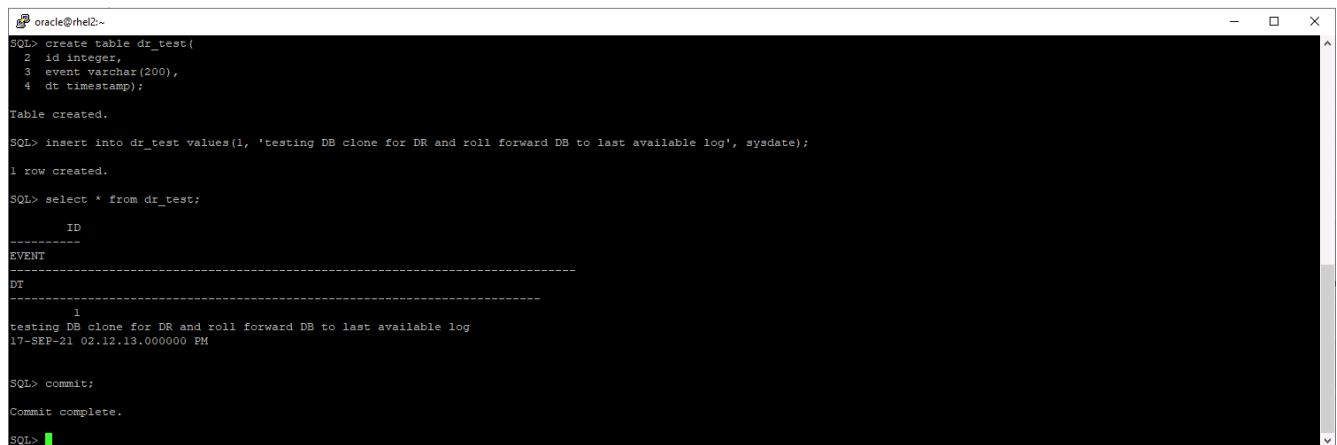
Se hai bisogno di aiuto per questa soluzione e per i casi d'utilizzo, partecipa a. ["La community di NetApp Solution Automation supporta il canale slack"](#) e cerca il canale di automazione della soluzione per inviare domande o domande.

## Workflow di disaster recovery

Le aziende hanno adottato il cloud pubblico come risorsa e destinazione praticabili per il disaster recovery. SnapCenter rende questo processo il più possibile perfetto. Questo flusso di lavoro di disaster recovery è molto simile al flusso di lavoro dei cloni, ma il ripristino del database viene eseguito attraverso l'ultimo log disponibile replicato nel cloud per ripristinare tutte le transazioni di business possibili. Tuttavia, sono disponibili ulteriori fasi di pre-configurazione e post-configurazione specifiche per il disaster recovery.

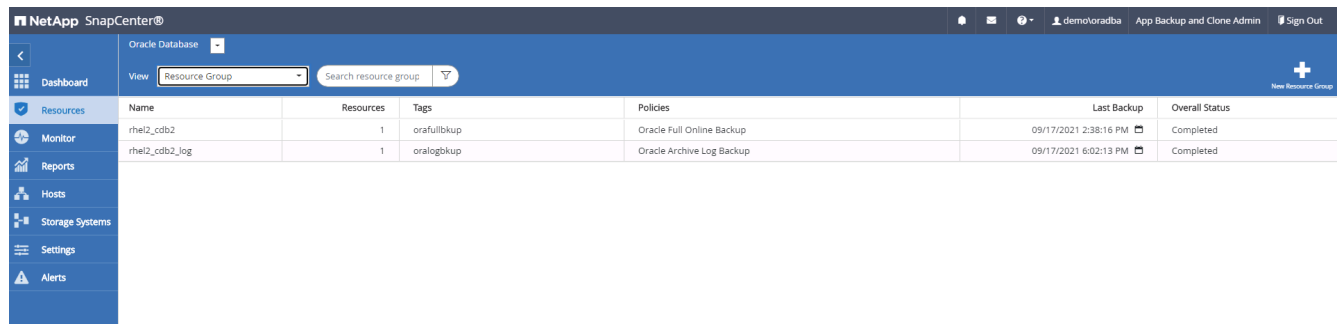
## Clonare un database di produzione Oracle on-premise nel cloud per il DR

1. Per verificare che il ripristino del clone venga eseguito attraverso l'ultimo log disponibile, abbiamo creato una piccola tabella di test e inserito una riga. I dati del test vengono ripristinati dopo un ripristino completo dell'ultimo registro disponibile.



```
oracle@rhel2~$
SQL> create table dr_test(
  2 id integer,
  3 event varchar(200),
  4 dt timestamp);
Table created.
SQL> insert into dr_test values(1, 'testing DB clone for DR and roll forward DB to last available log', sysdate);
1 row created.
SQL> select * from dr_test;
      ID
-----
EVENT
-----
DT
-----
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM
SQL> commit;
Commit complete.
SQL>
```

2. Accedere a SnapCenter come ID utente per la gestione del database per Oracle. Accedere alla scheda risorse, che mostra i database Oracle protetti da SnapCenter.



NetApp SnapCenter® Oracle Database

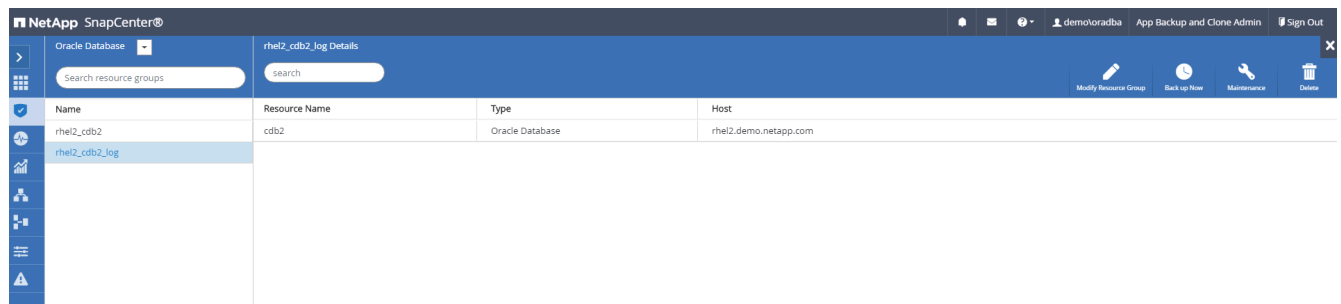
View: Resource Group Search resource group

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhel2_cdb2	1	orafullbkup	Oracle Full Online Backup	09/17/2021 2:38:16 PM	Completed
rhel2_cdb2_log	1	oralogbkup	Oracle Archive Log Backup	09/17/2021 6:02:13 PM	Completed

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

demo/oradba App Backup and Clone Admin Sign Out

- Selezionare il gruppo di risorse del registro Oracle e fare clic su Backup Now (Esegui backup ora) per eseguire manualmente un backup del registro Oracle per scaricare l'ultima transazione verso la destinazione nel cloud. In un vero scenario di DR, l'ultima transazione ripristinabile dipende dalla frequenza di replica del volume del log del database nel cloud, che a sua volta dipende dalla policy RTO o RPO dell'azienda.



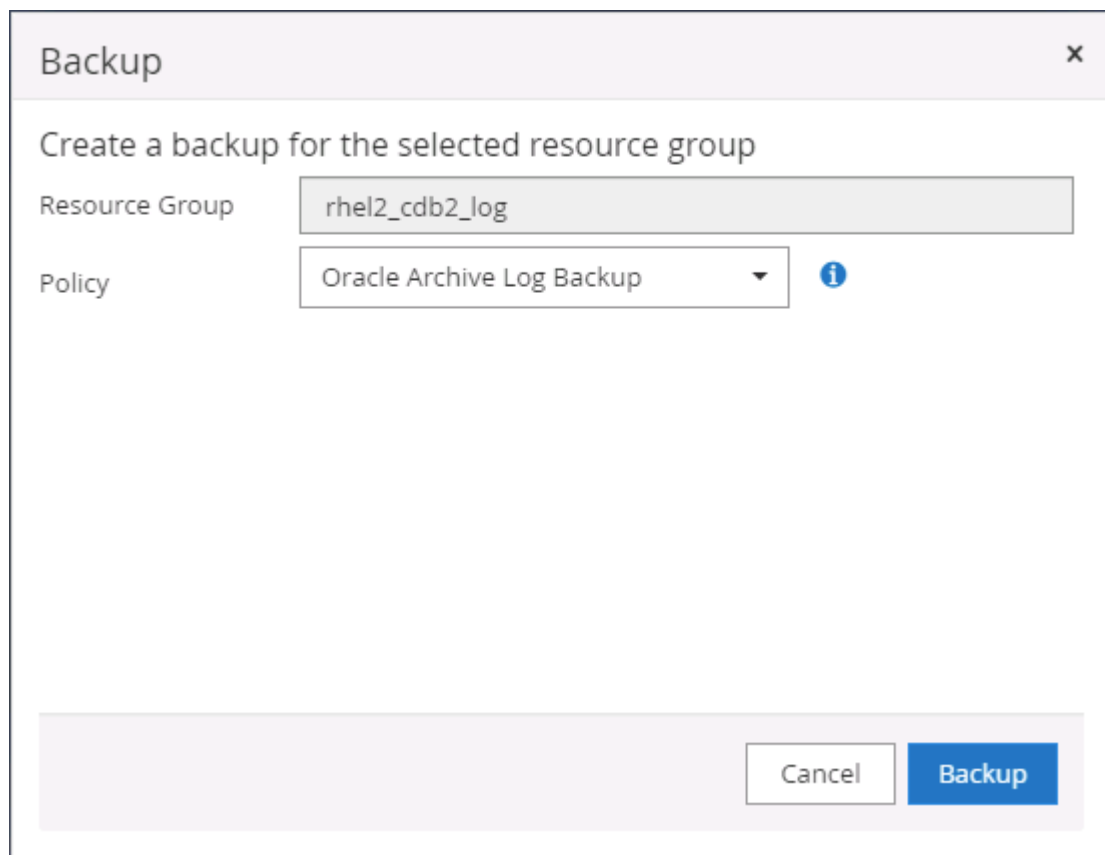
NetApp SnapCenter® Oracle Database

Search resource groups

Search

Name	Resource Name	Type	Host
rhel2_cdb2	cdb2	Oracle Database	rhel2.demo.netapp.com
rhel2_cdb2_log			

Modify Resource Group Backup Now Maintenance Delete



**Backup** [X]

Create a backup for the selected resource group

Resource Group: rhel2\_cdb2\_log

Policy: Oracle Archive Log Backup [i]

Cancel Backup



SnapMirror asincrono perde i dati che non l'hanno fatto alla destinazione cloud nell'intervallo di backup del registro del database in uno scenario di disaster recovery. Per ridurre al minimo la perdita di dati, è possibile pianificare backup dei log più frequenti. Tuttavia, esiste un limite alla frequenza di backup dei log tecnicamente raggiungibile.

4. Selezionare l'ultimo backup del registro in Secondary Mirror Backup(s) (Backup mirror secondario) e montare il backup del registro.

The screenshot shows the NetApp SnapCenter interface for Oracle Database. The left sidebar contains navigation icons. The main area displays the 'cdb2 Topology' with a 'Manage Copies' section showing 'Local copies' (185 Backups, 0 Clones) and 'Mirror copies' (185 Backups, 2 Clones). A 'Summary Card' on the right shows: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this is the 'Secondary Mirror Backup(s)' section with a search bar and a table of backups.

Backup Name	Count	Type	LF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log		09/17/2021 6:20:13 PM	Not Applicable	False	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log		09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log		09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842

The 'Mount backups' dialog box is shown. It includes a dropdown for 'Choose the host to mount the backup' with the value 'ora-standby.demo.netapp.com'. The 'Mount path' is '/var/opt/snapcenter/sco/backup\_mount/rhel2\_cdb2\_log\_09-17-2021\_18.20.04.1177\_1/cdb2'. Below this, the 'Secondary storage location' is set to 'Snap Vault / Snap Mirror'. There are two sections: 'Source Volume' with the value 'svm\_onPrem:rhel2\_u03' and 'Destination Volume' with a dropdown showing 'svm\_hybridcvo:rhel2\_u03\_dr'. At the bottom right are 'Mount' and 'Cancel' buttons.

5. Selezionare l'ultimo backup completo del database e fare clic su Clone (Clona) per avviare il flusso di lavoro dei cloni.

The screenshot shows the NetApp SnapCenter Oracle Database console. The left sidebar contains navigation icons. The main area displays the 'cdb2 Topology' with a diagram showing 'Local copies' (185 Backups, 0 Clones) and 'Mirror copies' (185 Backups, 2 Clones). A 'Summary Card' on the right shows: 370 Backups, 16 Data Backups, 354 Log Backups, and 2 Clones. Below this is a table of 'Secondary Mirror Backup(s)'.

Backup Name	Count	Type	IF	End Date	Verified	Mounted	RMAN Cataloged	SCN
rhel2_cdb2_log_09-17-2021_18.20.04.1177_1	1	Log		09/17/2021 6:20:13 PM	Not Applicable	True	Not Cataloged	5994710
rhel2_cdb2_log_09-17-2021_18.00.01.2424_1	1	Log		09/17/2021 6:00:09 PM	Not Applicable	False	Not Cataloged	5992079
rhel2_cdb2_log_09-17-2021_17.00.01.1566_1	1	Log		09/17/2021 5:00:20 PM	Not Applicable	False	Not Cataloged	5988842
rhel2_cdb2_log_09-17-2021_16.00.01.2156_1	1	Log		09/17/2021 4:00:10 PM	Not Applicable	False	Not Cataloged	5985272
rhel2_cdb2_log_09-17-2021_15.00.01.1317_1	1	Log		09/17/2021 3:00:10 PM	Not Applicable	False	Not Cataloged	5982003
rhel2_cdb2_log_09-17-2021_14.35.01.4997_1	1	Log		09/17/2021 2:35:21 PM	Not Applicable	False	Not Cataloged	5980629
rhel2_cdb2_09-17-2021_14.35.01.4997_0	1	Data		09/17/2021 2:35:12 PM	Unverified	False	Not Cataloged	5980588

Total 3

6. Selezionare un ID DB clone univoco sull'host.

The 'Clone from cdb2' dialog box is shown with the following configuration:

- 1 Name**: ☒ Complete Database Clone
  - Clone SID:
  - Exclude PDBs:
- ☐ PDB Clone
- Secondary storage location : Snap Vault / Snap Mirror
- Data**
  - Source Volume: svm\_onPrem:rhel2\_u02
  - Destination Volume:
- Logs**
  - Source Volume: svm\_onPrem:rhel2\_u03
  - Destination Volume:

Navigation buttons: Previous, Next

7. Eseguire il provisioning di un volume di log e montarlo sul server DR di destinazione per l'area di ripristino flash Oracle e i registri online.

ONTAP System Manager

Search actions, objects, and pages

**Volumes**

+ Add More

Name	Storage VM	Status	Capacity
ora_standby_u01	svm_hybridcvo	Online	12.3 GB used / 17.7 GB available / 31.6 GB
rhel2_u01_dr	svm_hybridcvo	Online	
rhel2_u02_dr	svm_hybridcvo	Online	
rhel2_u02_dr0917211608119360	svm_hybridcvo	Online	
rhel2_u02_dr0917211703534863	svm_hybridcvo	Online	
rhel2_u03_dr	svm_hybridcvo	Online	
rhel2_u03_dr0917211824574775	svm_hybridcvo	Online	

**Add Volume**

NAME

ora\_standby\_u03

CAPACITY

20 GB

More Options Cancel Save

```
ec2-user@ora-standby/tmp$ sudo mkdir /u03_cdb2dr
[ec2-user@ora-standby tmp]$ chown oracle:oinstall /u03_cdb2dr
chown: changing ownership of '/u03_cdb2dr': Operation not permitted
[ec2-user@ora-standby tmp]$ sudo chown oracle:oinstall /u03_cdb2dr
[ec2-user@ora-standby tmp]$ sudo mount -t nfs 10.221.1.6:/ora_standby_u03 /u03_cdb2dr
[ec2-user@ora-standby tmp]$ df -h
Filesystem                Size      Used Avail Use% Mounted on
devtmpfs                  7.6G         0   7.6G   0% /dev
tmpfs                     7.6G         0   7.6G   0% /dev/shm
tmpfs                     7.6G      17M   7.6G   1% /run
tmpfs                     7.6G         0   7.6G   0% /sys/fs/cgroup
/dev/nvme0nlp2            10G       9.0G   1.1G  90% /
10.221.1.6:/ora_standby_u01 31G       13G    18G  42% /u01
tmpfs                     1.6G         0   1.6G   0% /run/user/1000
10.221.1.6:/Sc28182452-3fa8-448c-9e4a-c5a9e465f353 100G       3.1G   97G   4% /u02_cdb2dev
tmpfs                     1.6G         0   1.6G   0% /run/user/54321
10.221.1.6:/Sc39c05df8-4b00-4b3a-853c-9d6d338e5df7 100G       3.7G   97G   4% /u02_cdb2test
10.221.1.6:/Sccf886a5c-3273-479e-ad97-472b2a8dccee 100G       3.8G   97G   4% /var/opt/snapcenter/sco/backup_mount/rhel2_cdb2_log_09-17-2021_18.20.04.1177_1/cdb2/1
10.221.1.6:/ora_standby_u03 21G       320K   20G   1% /u03_cdb2dr
[ec2-user@ora-standby tmp]$
```



La procedura di clonazione Oracle non crea un volume di log, che deve essere fornito sul server DR prima della clonazione.

- Selezionare l'host clone di destinazione e la posizione in cui inserire i file di dati, i file di controllo e i log di ripristino.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

PreOps

5

PostOps

6

Notification

7

Summary

Select the host to create a clone

Clone host
ora-standby.demo.netapp.com

Datafile locations ⓘ

/u02\_cdb2dr
Reset

Control files ⓘ

/u02\_cdb2dr/cdb2dr/control/control01.ctl
/u03\_cdb2dr/cdb2dr/control/control02.ctl
Reset

Redo logs ⓘ

Group	Size	Unit	Number of files
<div> RedoGroup 1 </div>	200	MB	1
/u03_cdb2dr/cdb2dr/redolog/redo03.log			
<div> RedoGroup 2 </div>	200	MB	1

Reset

Previous
Next

9. Selezionare le credenziali per il clone. Inserire i dettagli della configurazione Oracle home sul server di destinazione.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Database Credentials for the clone

Credential name for sys user

None

+

i

Database port

1521

Oracle Home Settings

i

Oracle Home

/u01/app/oracle/product/19800/cdb2

Oracle OS User

oracle

Oracle OS Group

oinstall

Previous

Next

10. Specificare gli script da eseguire prima della clonazione. Se necessario, è possibile regolare i parametri del database.

Clone from cdb2

1

Name

2

Locations

3

Credentials

4

5

6

7

Specify scripts to run before clone operation ⓘ

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Arguments

Script timeout

60

secs

Database Parameter settings

Previous

Next

- Selezionare l'opzione di ripristino fino a quando non viene eseguita l'opzione Cancel (Annulla), in modo che il ripristino venga eseguito attraverso tutti i log di archivio disponibili per recuperare l'ultima transazione replicata nella posizione del cloud secondario.



### Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

☒ Recover Database

☒ Until Cancel

☐ Date and Time

☐ Until SCN (System Change Number)

Date-time format: MM/DD/YYYY hh:mm:ss

Specify external archive log locations

/var/opt/snapcenter/sco/backup\_mount/rhel2\_cdb2\_log\_09-17-2021\_18.20.04.1177\_1/cdb2/1/orareco/CDB2/archivelog/

Create new DBID

Create tempfile for temporary tablespace

Enter SQL queries to apply when clone is created

Enter scripts to run after clone operation

Previous

Next

12. Configurare il server SMTP per la notifica via email, se necessario.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach job report

⚠

If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

✕

Previous

Next

13. Riepilogo dei cloni DR.

Clone from cdb2

1 Name

2 Locations

3 Credentials

4 PreOps

5 PostOps

6 Notification

7 Summary

Summary

Clone from backup

rhe12\_cdb2\_09-17-2021\_14.35.01.4997\_0

Clone SID

cdb2dr

Clone server

ora-standby.demo.netapp.com

Exclude PDBs

none

Oracle home

/u01/app/oracle/product/19800/cdb2

Oracle OS user

oracle

Oracle OS group

oinstall

Datafile mountpaths

/u02\_cdb2dr

Control files

/u02\_cdb2dr/cdb2dr/control/control01.ctl

/u03\_cdb2dr/cdb2dr/control/control02.ctl

Redo groups

RedoGroup =1 TotalSize =200 Path =/u03\_cdb2dr/cdb2dr/redolog/redo03.log

RedoGroup =2 TotalSize =200 Path =/u03\_cdb2dr/cdb2dr/redolog/redo02.log

RedoGroup =3 TotalSize =200 Path =/u03\_cdb2dr/cdb2dr/redolog/redo01.log

Recovery scope

Until Cancel

Prescript full path

none

Prescript arguments

Postscript full path

none

Postscript arguments

Previous

Finish

14. I DBS clonati vengono registrati con SnapCenter subito dopo il completamento del clone e sono quindi disponibili per la protezione del backup.

NetApp SnapCenter®							
Oracle Database							
View Database Search databases							
	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
	cdb2	Single Instance (Multitenant)	rhe12.demo.netapp.com	rhe12_cdb2 rhe12_cdb2_log	Oracle Archive Log Backup Oracle Full Online Backup	09/17/2021 7:00:10 PM	Backup succeeded
	cdb2dev	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected
	cdb2dr	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected
	cdb2test	Single Instance (Multitenant)	ora-standby.demo.netapp.com				Not protected

## Convalida e configurazione dei cloni post-DR per Oracle

1. Convalida l'ultima transazione di test che è stata scaricata, replicata e ripristinata nella posizione DR nel cloud.

```
oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> set lin 200
SQL> select instance_name, host_name from v$instance;

INSTANCE_NAME      HOST_NAME
-----
cdb2dr             ora-standby.demo.netapp.com

SQL> alter pluggable database cdb2_pdb1 open;

Pluggable database altered.

SQL> alter session set container=cdb2_pdb1;

Session altered.

SQL> select * from pdbadmin.dr_test;

      ID
-----
EVENT
-----
DT
-----
1
testing DB clone for DR and roll forward DB to last available log
17-SEP-21 02.12.13.000000 PM

SQL>
```

2. Configurare l'area di ripristino della flash.

```
oracle@ora-standby:/u01/app/oracle/product/19800/cdb2/dbs
[oracle@ora-standby:db]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Fri Sep 17 22:07:11 2021
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle. All rights reserved.

Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> show parameter db_recovery_file_dest

NAME                                TYPE        VALUE
-----
db_recovery_file_dest               string      /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size          big integer 17208M
SQL> alter system set db_recovery_file_dest='/u03_cdb2dr/cdb2dr' scope=both;


System altered.

SQL> show parameter db_recovery_file_dest

NAME                                TYPE        VALUE
-----
db_recovery_file_dest               string      /u03_cdb2dr/cdb2dr
db_recovery_file_dest_size          big integer 17208M

SQL>
```

- 3. Configurare il listener Oracle per l'accesso degli utenti.
- 4. Separare il volume clonato dal volume di origine replicato.
- 5. Eseguire la replica inversa dal cloud a on-premise e ricostruire il server di database on-premise guasto.



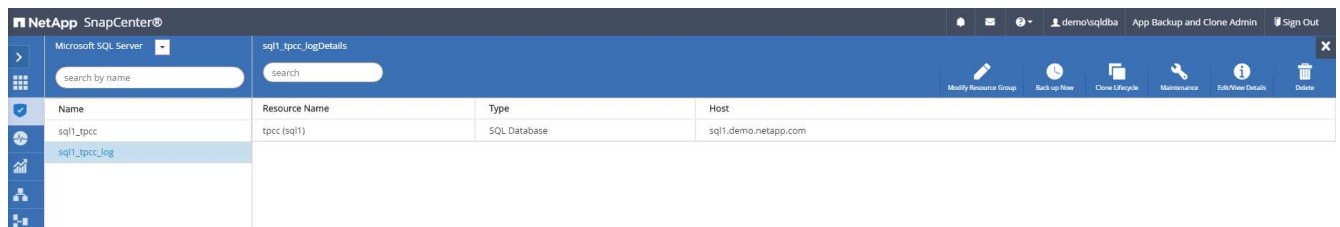
La suddivisione dei cloni può comportare un utilizzo temporaneo dello spazio di storage molto più elevato del normale funzionamento. Tuttavia, dopo la ricostruzione del server DB on-premise, è possibile liberare spazio aggiuntivo.

Clonare un database di produzione SQL on-premise nel cloud per il DR

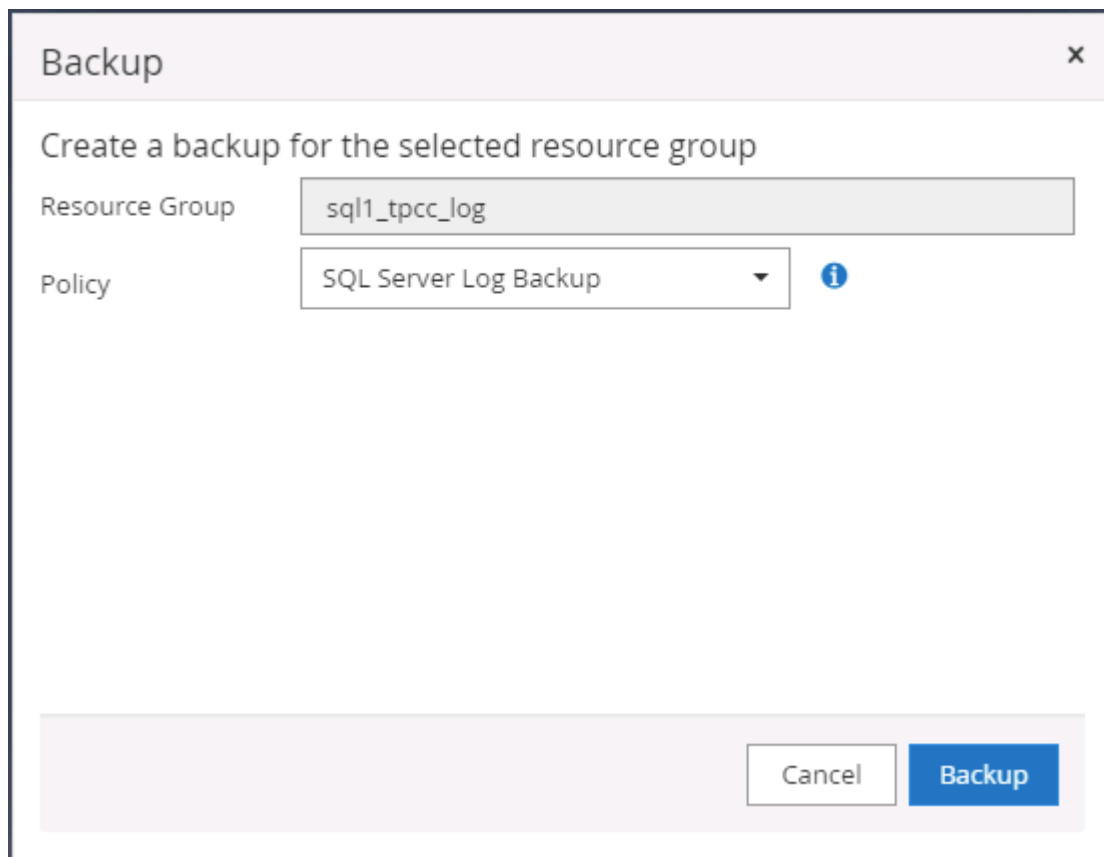
- 1. Allo stesso modo, per verificare che il ripristino del clone SQL sia stato eseguito attraverso l'ultimo log disponibile, abbiamo creato una piccola tabella di test e inserito una riga. I dati del test vengono ripristinati dopo un ripristino completo dell'ultimo registro disponibile.

```
Administrator Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go
-----
SQL1
(1 rows affected)
1> use tpcc
2> go
Changed database context to 'tpcc'.
1> insert into snap_sync values ('test snap mirror DR for SQL', getdate())
2> go
(1 rows affected)
1> select * from snap_sync
2> go
event                                         dt
-----
test snap mirror DR for SQL                 2021-09-20 14:23:04.533
(1 rows affected)
1>
```

2. Accedere a SnapCenter con un ID utente per la gestione del database per SQL Server. Accedere alla scheda Resources (risorse), che mostra il gruppo di risorse di protezione di SQL Server.



3. Eseguire manualmente un backup del log per svuotare l'ultima transazione da replicare sullo storage secondario nel cloud pubblico.



4. Selezionare l'ultimo backup completo di SQL Server per il clone.

NetApp SnapCenter®

Microsoft SQL Server - tpcc (sql1) Topology

search by name

Clone Lifecycle Protect Details Refresh

Manage Copies

7 Backups 0 Clones Local copies

7 Backups 2 Clones Mirror copies

Summary Card

14 Backups

2 Clones

Secondary Mirror Backup(s)

search

Backup Name	Count	Type	if	End Date	Verified
sql1_tpcc_09-19-2021_18.25.01.4134	1	Full backup		09/19/2021 6:25:05 PM	Unverified
sql1_tpcc_09-18-2021_18.25.01.3963	1	Full backup		09/18/2021 6:25:05 PM	Unverified
sql1_tpcc_09-17-2021_18.25.01.4218	1	Full backup		09/17/2021 6:25:05 PM	Unverified

- Impostare l'impostazione del clone, ad esempio Clone Server, Clone Instance, Clone Name e mount. Il percorso di storage secondario in cui viene eseguita la clonazione viene popolato automaticamente.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Clone settings

Clone server sql-standby.demo.netapp.com

Clone instance sql-standby

Clone name tpcc\_dr

Choose mount option

☒ Auto assign mount point

☐ Auto assign volume mount point under path full file path

Secondary storage location : Snap Vault / Snap Mirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvo:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvo:sql1_log_dr

Previous Next

- Selezionare tutti i backup del registro da applicare.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Choose logs

☒ All log backups

☐ By log backups until

9/19/2021 6:25:10 PM

☐ By specific date until

09/19/2021 6:25:05 PM

☐ None

Previous

Next

7. Specificare eventuali script opzionali da eseguire prima o dopo la clonazione.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Specify optional scripts to run before and after performing a clone from backup job

Prescript full path

Prescript arguments

Choose optional arguments...

Postscript full path

Postscript arguments

Choose optional arguments...

Script timeout

60

secs

Previous

Next

8. Specificare un server SMTP se si desidera inviare una notifica via e-mail.



Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Provide email settings ⓘ

Email preference

Never

From

From email

To

Email to

Subject

Notification

☐ Attach Job Report

⚠ If you want to send notifications for Clone jobs, an SMTP server must be configured. Continue to the Summary page to save your information, and then go to Settings>Global Settings>Notification Server Settings to configure the SMTP server.

×

Previous

Next

9. Riepilogo dei cloni DR. I database clonati vengono immediatamente registrati con SnapCenter e sono disponibili per la protezione del backup.

Clone from backup

1 Clone Options

2 Logs

3 Script

4 Notification

5 Summary

Summary

Clone server

sql-standby.demo.netapp.com

Clone instance

sql-standby

Clone name

tpcc\_dr

Mount option

Auto Mount

Prescript full path

None

Prescript arguments

Postscript full path

None

Postscript arguments

Send email

No

Previous

Finish

NetApp SnapCenter®							
Microsoft SQL Server							
View Database search by name							
Resources	Name	Instance	Host	Last Backup	Overall Status	Type	
Monitor	master	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Reports	model	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Hosts	msdb	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Storage Systems	tempdb	sql1	sql1.demo.netapp.com		Not available for backup	System database	
Settings	tpcc	sql1	sql1.demo.netapp.com	09/22/2021 5:35:08 PM	Backup failed, Schedules on hold	User database	
Alerts	master	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	model	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	msdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	tempdb	sql-standby	sql-standby.demo.netapp.com		Not available for backup	System database	
	tpcc_clone	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	
	tpcc_dev	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	
	tpcc_dr	sql-standby	sql-standby.demo.netapp.com		Not protected	User database	

## Convalida e configurazione dei cloni post-DR per SQL

1. Monitorare lo stato del lavoro clone.

NetApp SnapCenter®						
Jobs Schedules Events Logs						
search by name						
Jobs - Filter						
ID	Status	Name	Start date	End date	Owner	
1052	✓	Clone from backup 'sql1_tpcc_09-19-2021_18.25.01.4134'	09/20/2021 2:36:17 PM	09/20/2021 2:37:06 PM	demo/sqlqdba	
1047	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:35:01 PM	09/20/2021 2:37:08 PM	demo/sqlqdba	
1045	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 2:28:17 PM	09/20/2021 2:30:25 PM	demo/sqlqdba	
1044	✓	Clone from backup 'sql1_tpcc_09-17-2021_18.25.01.4218'	09/20/2021 1:39:24 PM	09/20/2021 1:40:09 PM	demo/sqlqdba	
1042	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 1:35:01 PM	09/20/2021 1:37:08 PM	demo/sqlqdba	
1040	✓	Backup of Resource Group 'sql1_tpcc_log' with policy 'SQL Server Log Backup'	09/20/2021 12:35:01 PM	09/20/2021 12:37:08 PM	demo/sqlqdba	

2. Verificare che l'ultima transazione sia stata replicata e ripristinata con tutti i cloni dei file di log e il ripristino.

```
Administrator: Command Prompt - sqlcmd - SQLCMD
C:\Users\administrator.DEMO>sqlcmd
1> select host_name()
2> go

-----
SQL-STANDBY
(1 rows affected)
1> use tpcc_dr
2> go
Changed database context to 'tpcc_dr'.
1> select * from snap_sync
2> go
event dt
-----
test snap mirror DR for SQL 2021-09-20 14:23:04.533
(1 rows affected)
1> select getdate()
2> go

-----
2021-09-20 14:39:19.937
(1 rows affected)
1> _
```

3. Configurare una nuova directory di log di SnapCenter sul server DR per il backup del log di SQL Server.
4. Separare il volume clonato dal volume di origine replicato.
5. Eseguire la replica inversa dal cloud a on-premise e ricostruire il server di database on-premise guasto.

### Dove cercare aiuto?

Se hai bisogno di aiuto per questa soluzione e per i casi d'utilizzo, partecipa al ["La community di NetApp Solution Automation supporta il canale slack"](#) e cerca il canale di automazione della soluzione per inviare domande o domande.

## Informazioni sul copyright

Copyright © 2024 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.