SnapCenter per database

NetApp Solutions

NetApp
April 26, 2024

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: 'xxxxxxxx'
```

```
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

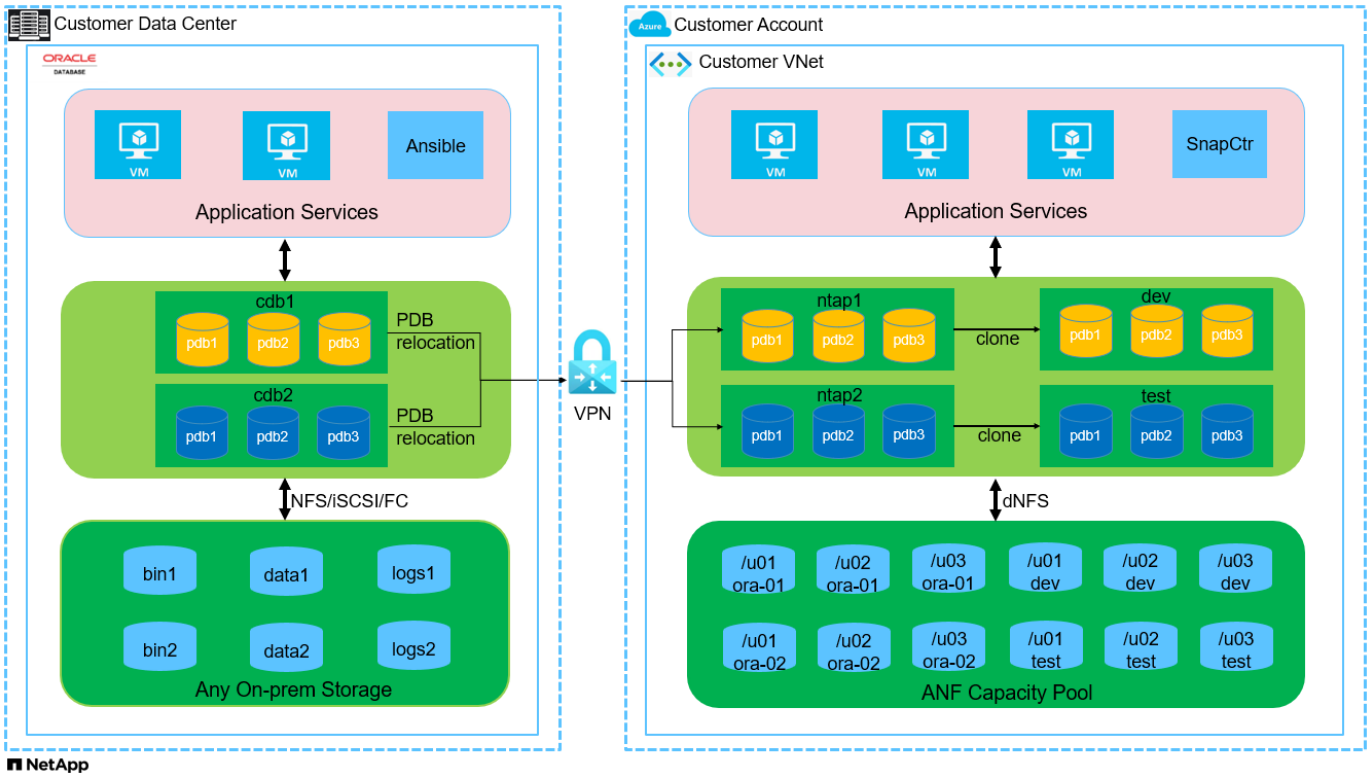
Questa soluzione è destinata alle seguenti persone:

- 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
Software		
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:

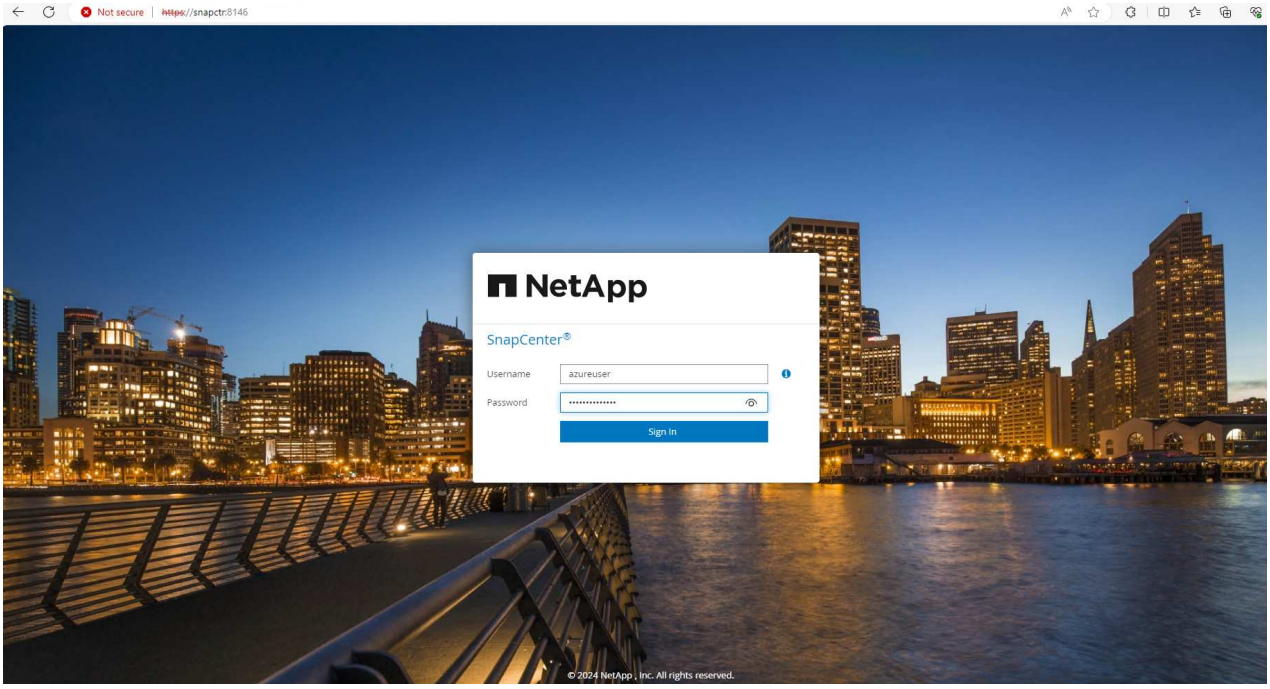
   Backup, ripristino e cloning di database Oracle su ANF con SnapCenter

8. Esaminare `Get Started` menu online.

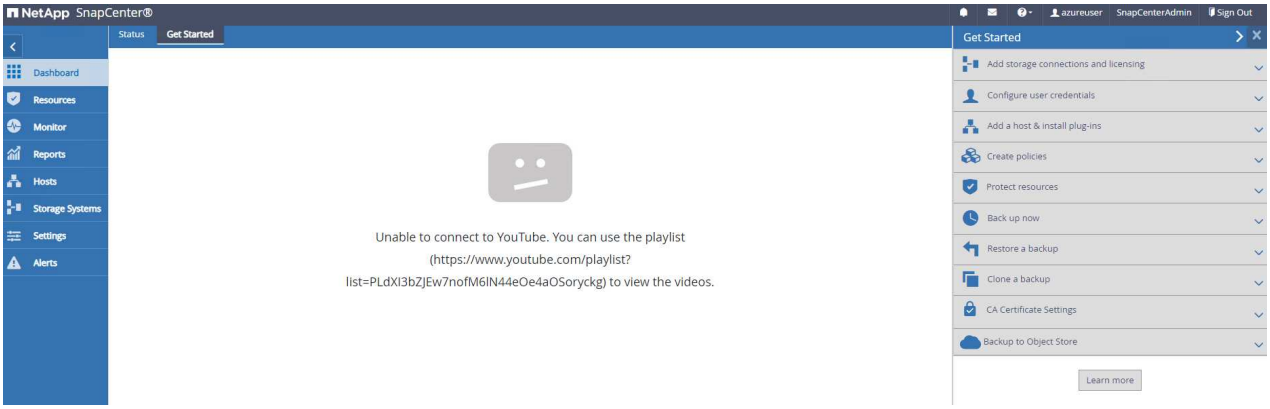
Installazione e configurazione di SnapCenter

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.

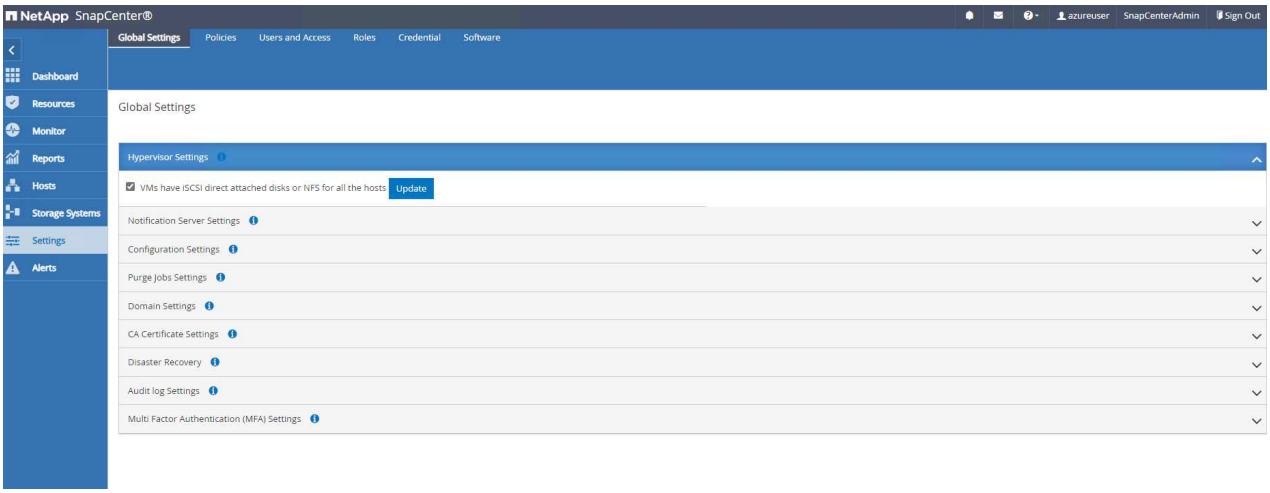
1. Dal server SnapCenter Windows, scaricare e installare l'ultima versione di java JDK dal sito Web "Scarica Java per le applicazioni desktop".
2. Dal server Windows SnapCenter, scaricare e installare la versione più recente (attualmente 5,0) del file eseguibile di installazione SnapCenter dal sito di 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.



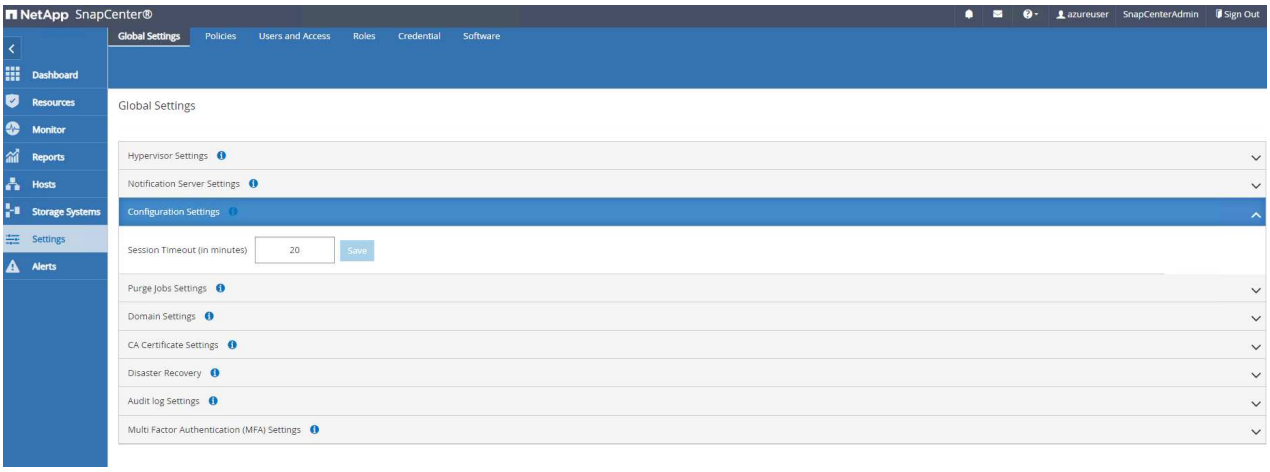
4. Revisione `Get Started` menu online.



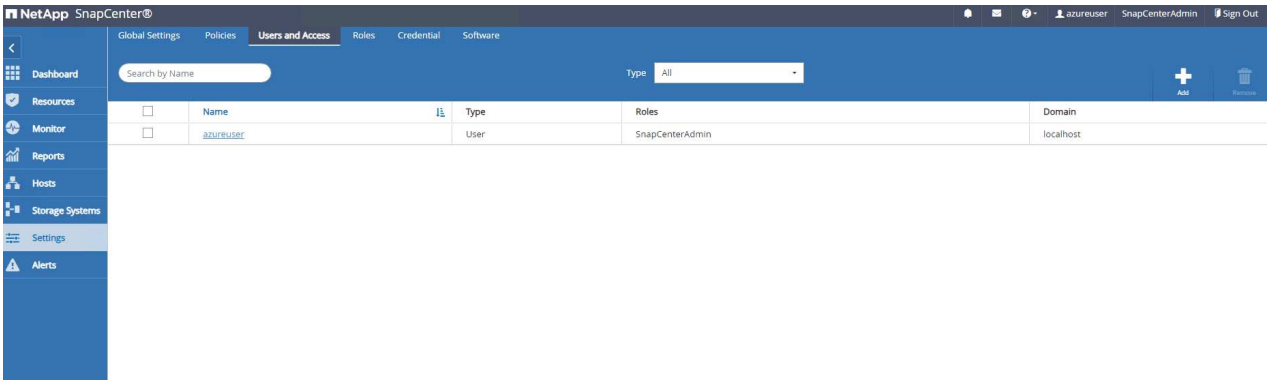
5. Poll `Settings-Global Settings`, controllo `Hypervisor Settings` E fare clic su Aggiorna.



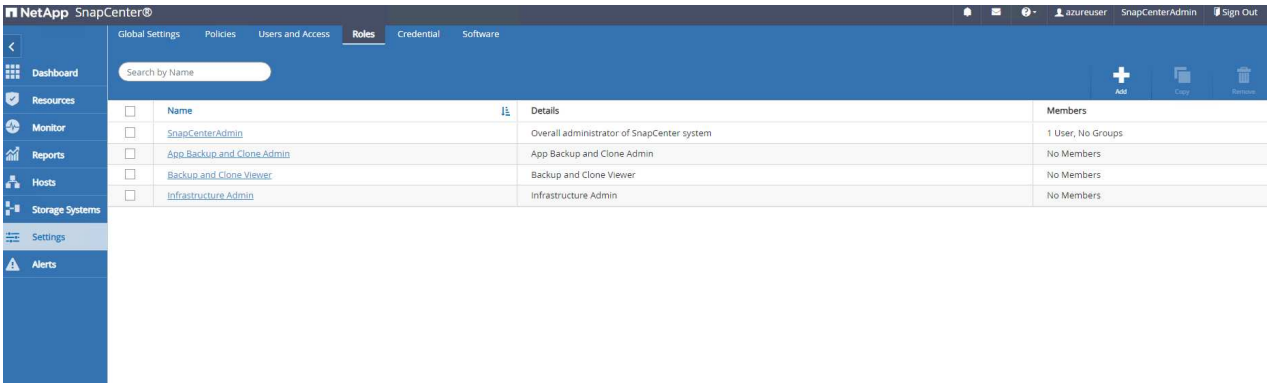
6. Se necessario, regolare `Session Timeout` Per l'interfaccia utente di SnapCenter all'intervallo desiderato.



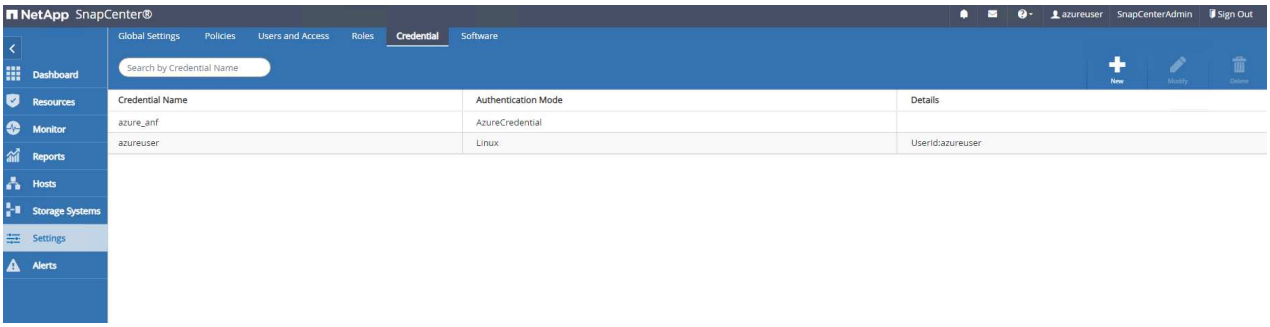
7. Se necessario, aggiungere altri utenti a SnapCenter.

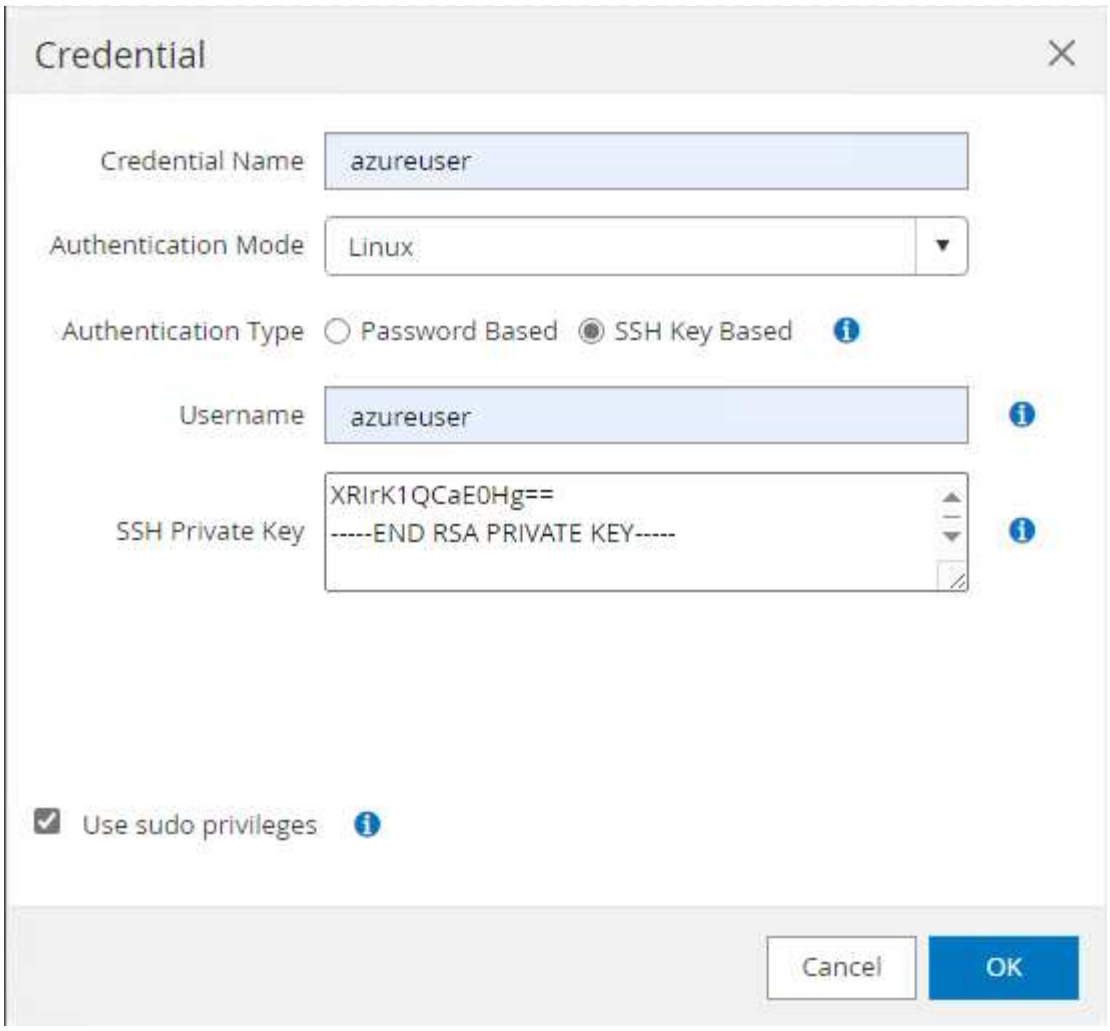


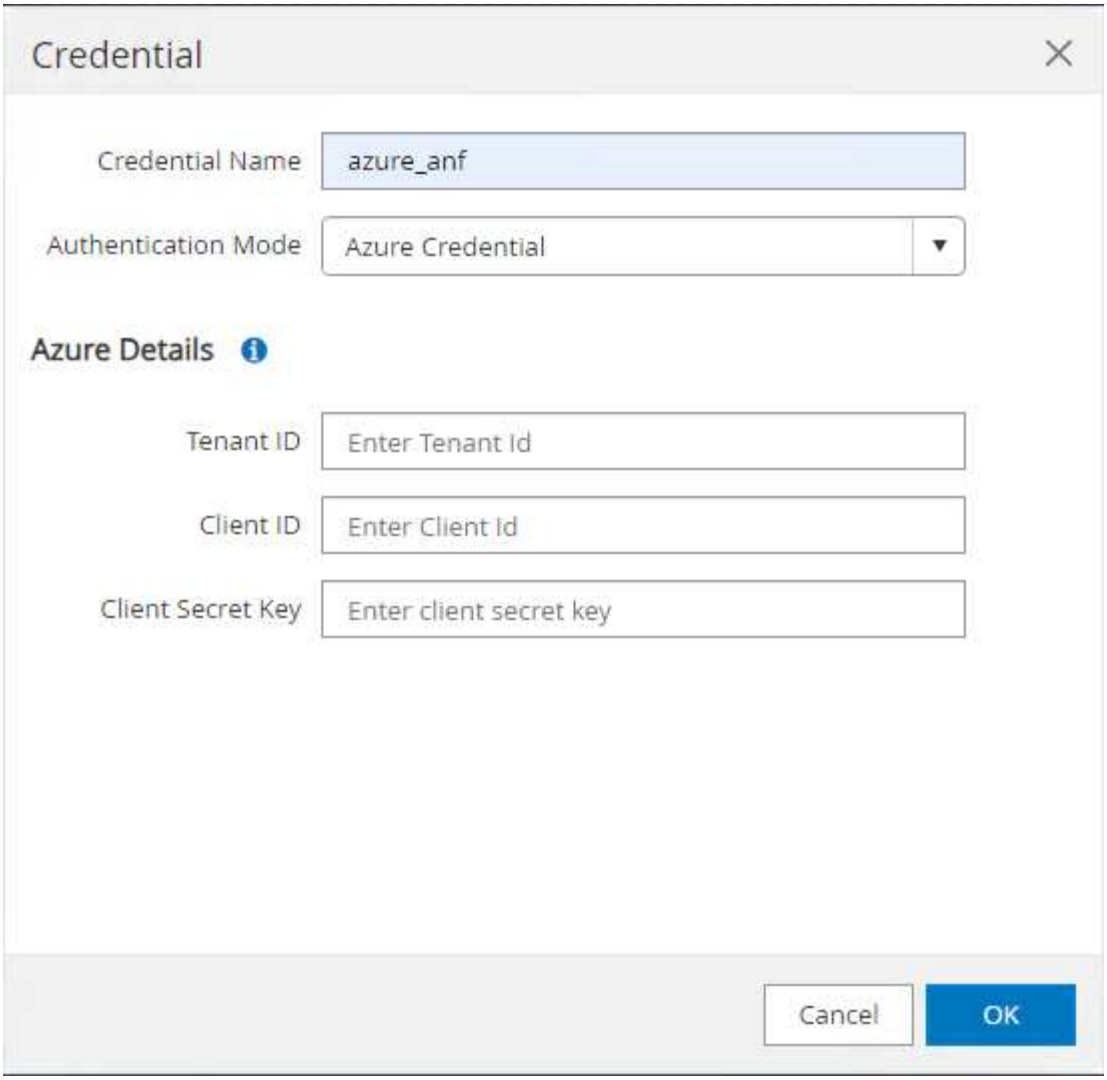
8. Il `Roles` Elenca i ruoli incorporati che possono essere assegnati a diversi utenti SnapCenter. I ruoli personalizzati possono anche essere creati dall'utente amministratore con i privilegi desiderati.



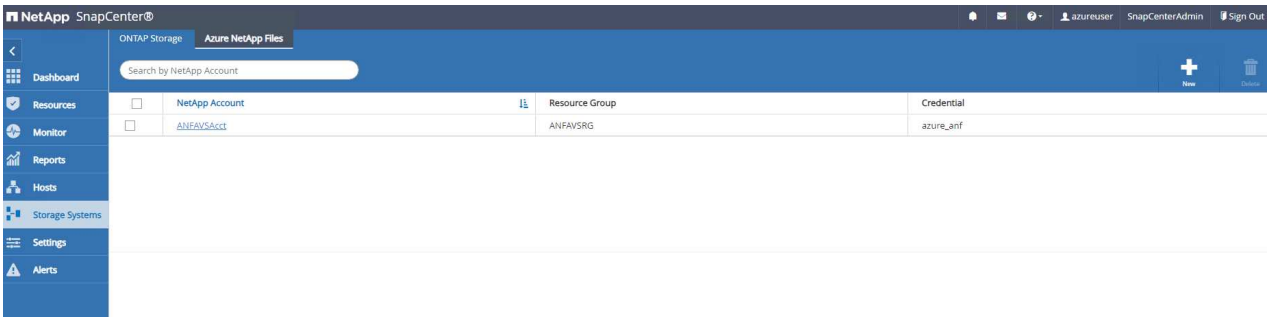
9. Da `Settings-Credential`, Creare le credenziali per gli obiettivi di gestione SnapCenter. In questo caso di utilizzo dimostrativo, sono utenti linux per l'accesso ad Azure VM e credenziali ANF per l'accesso al pool di capacità.



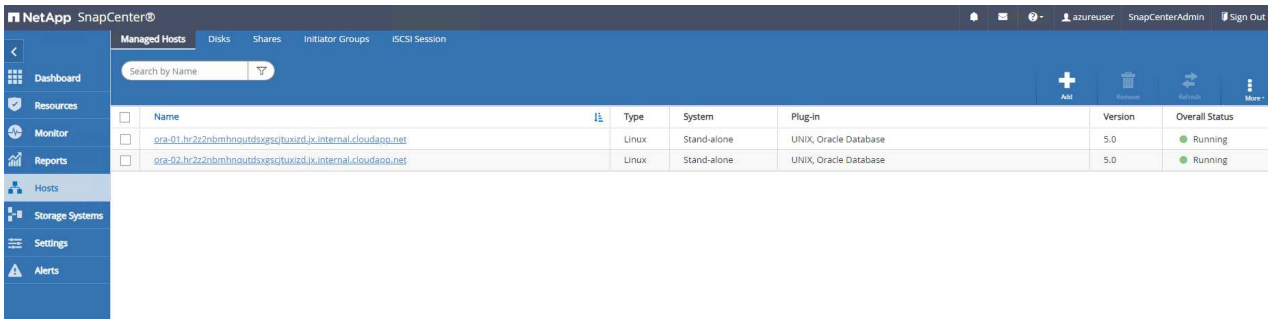

Credential
Credential Name
azureuser
Authentication Mode
Linux
Authentication Type
Password Based
SSH Key Based
Username
azureuser
SSH Private Key
XRIrK1QCaE0Hg==
-----END RSA PRIVATE KEY-----
Use sudo privileges
Cancel
OK

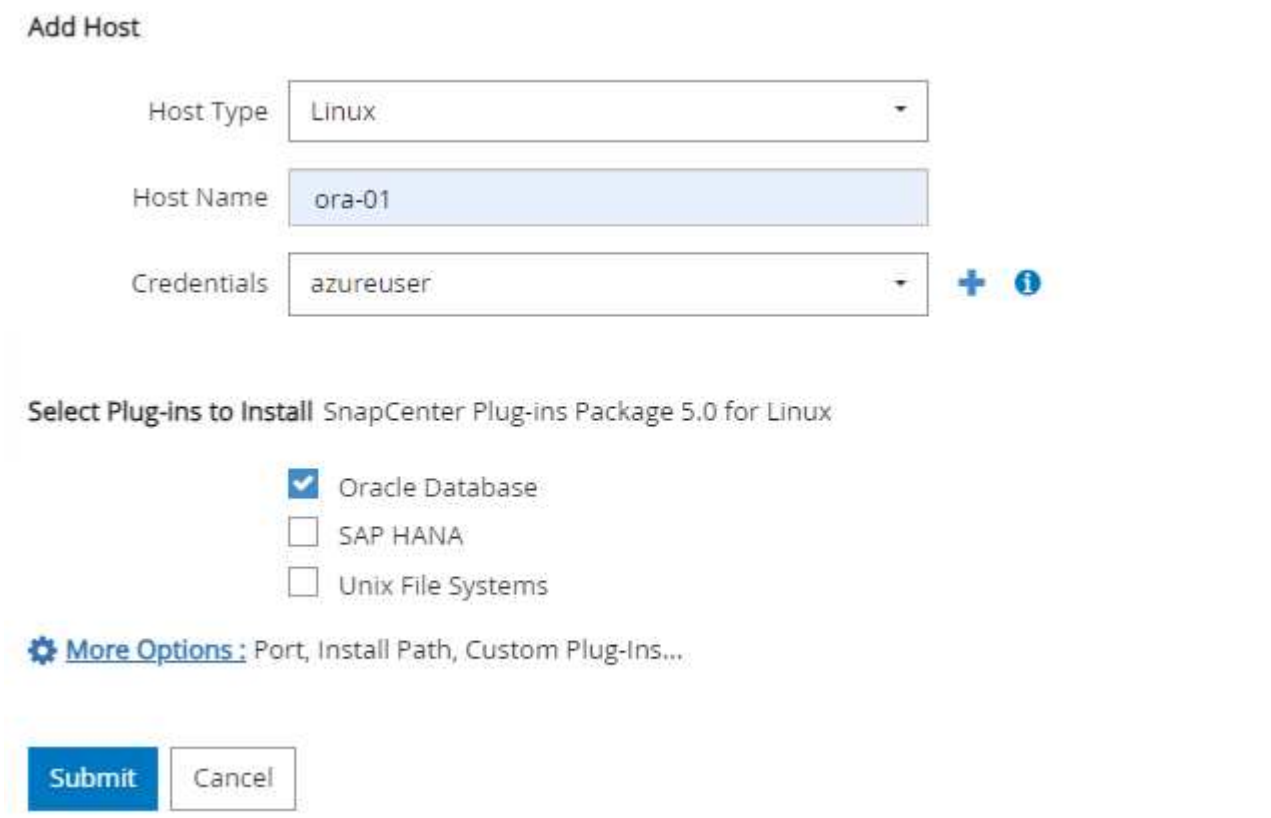


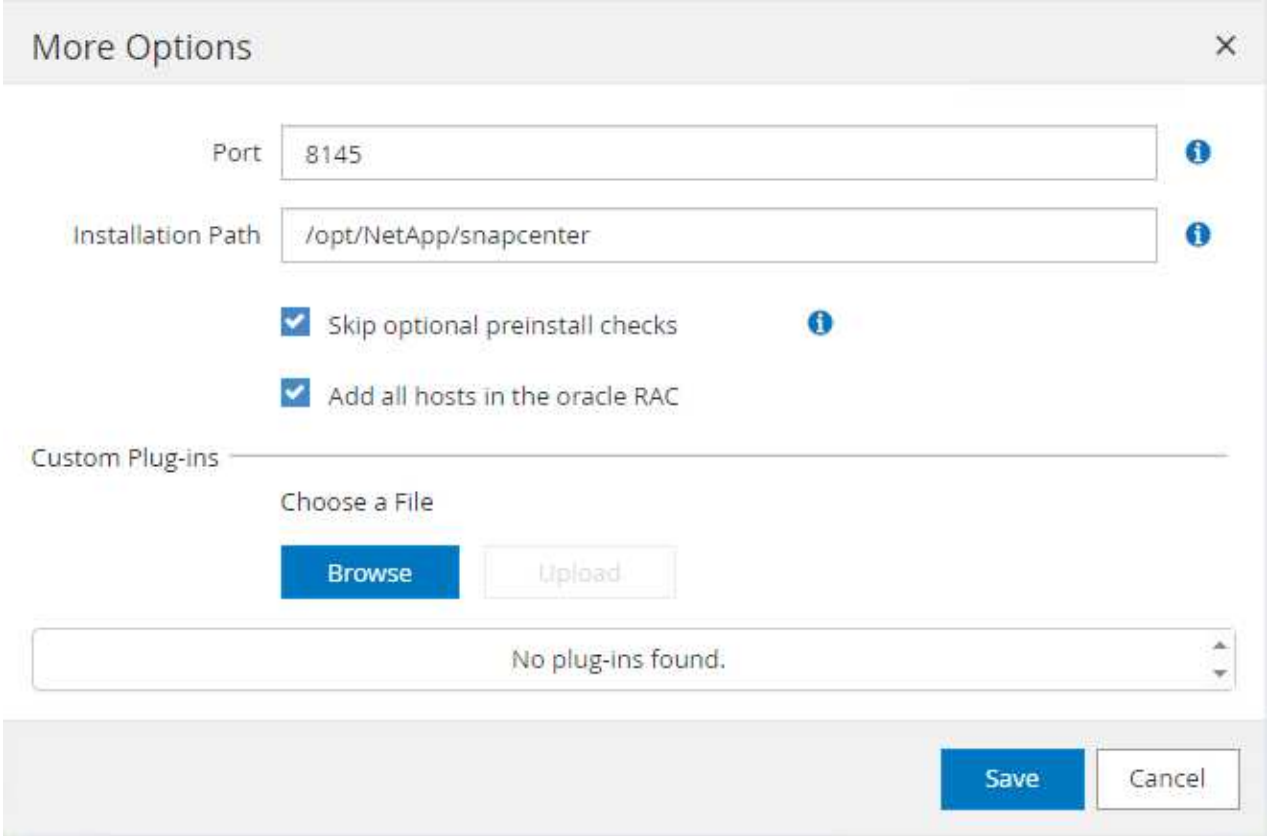
10. Da `Storage Systems` scheda, aggiungi `Azure NetApp Files` con la credenziale creata in precedenza.



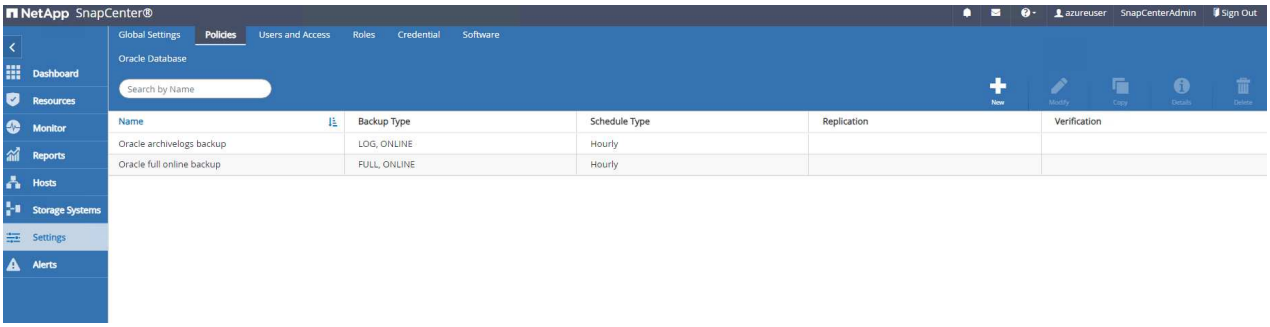
11. Da `Hosts` Tab, Aggiungi Azure DB VM, che installa il plug-in SnapCenter per Oracle su Linux.







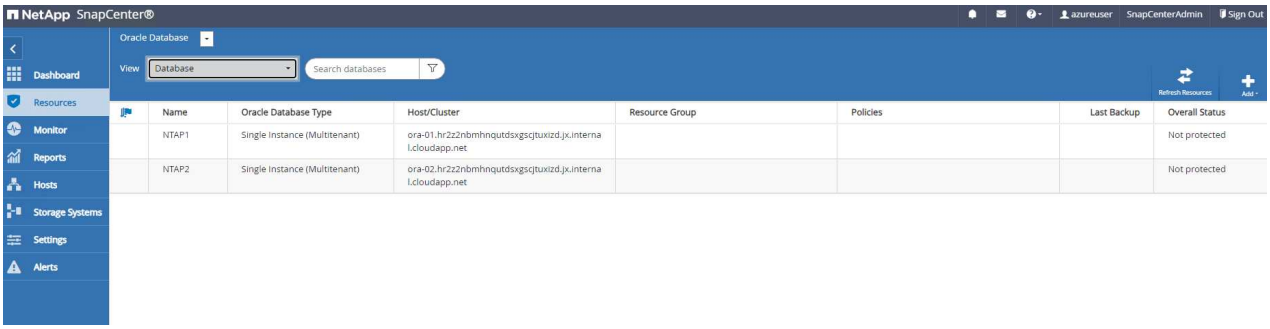
12. Una volta installato il plug-in host sulla VM del server DB, i database sull'host vengono rilevati automaticamente e visibili in `Resources` scheda. Torna a. `Settings-Polices`, Creare criteri di backup per il backup online completo del database Oracle e il backup solo dei registri di archivio. Consultare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



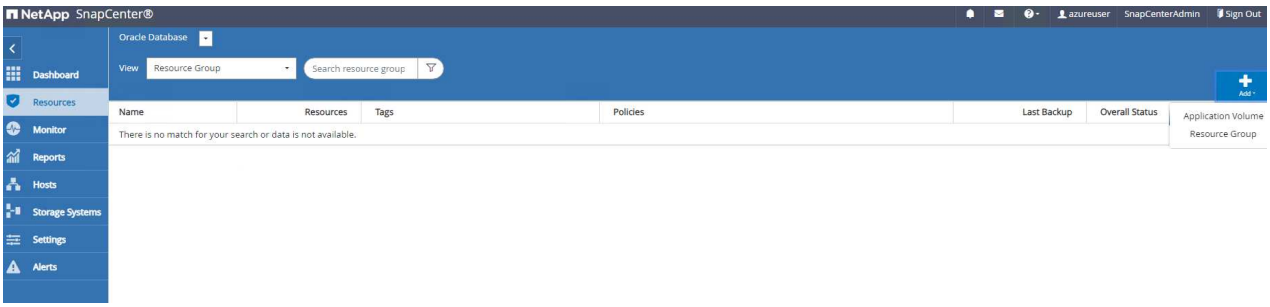
Backup del database

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.

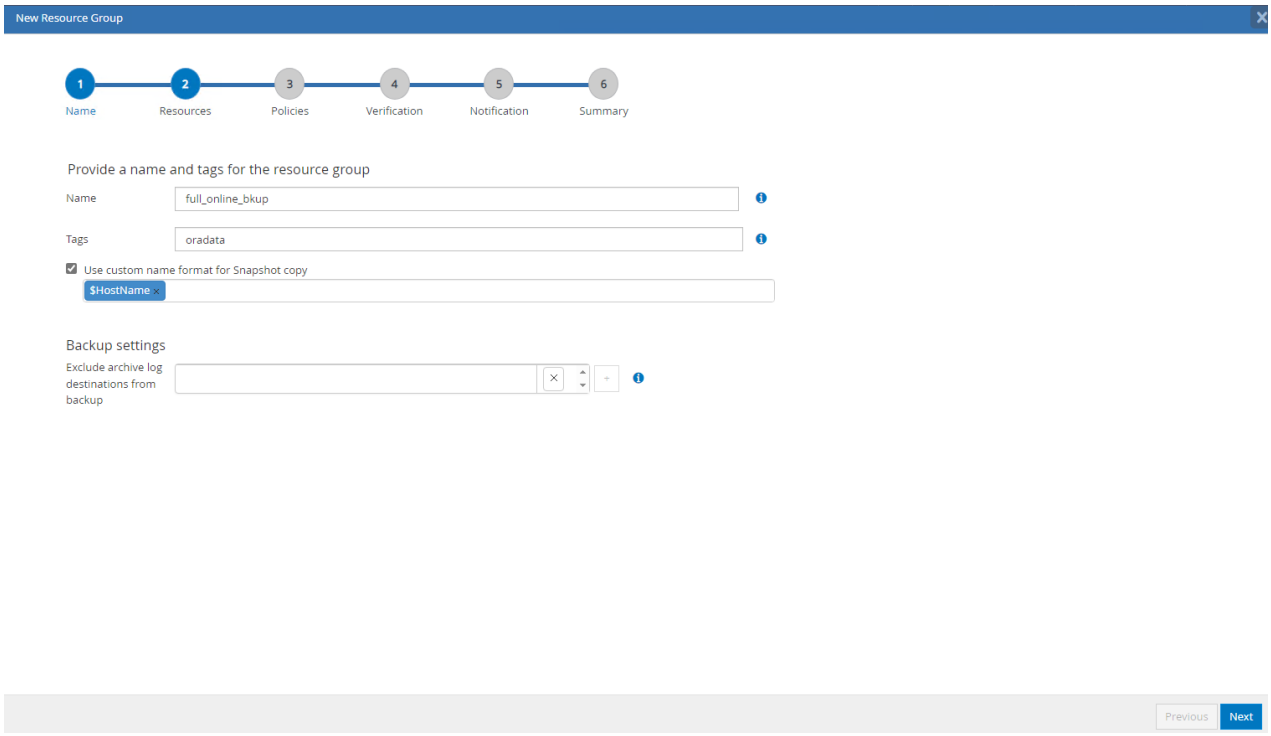
1. Navigazione verso `Resources` Che elenca i database rilevati dopo l'installazione del plugin SnapCenter sulla VM del database. Inizialmente, il `Overall Status` del database viene visualizzato come `Not protected`.



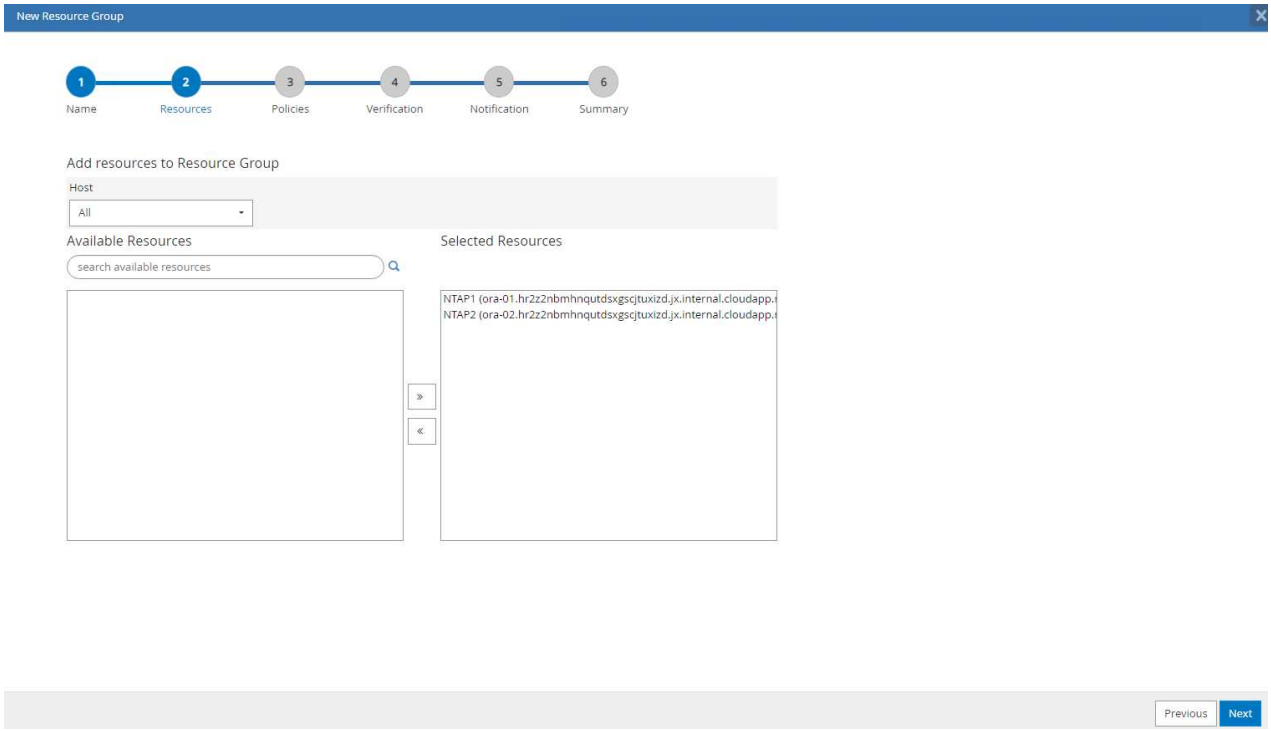
2. Fare clic su `View` a discesa per passare a. `Resource Group`. Fare clic su `Add` Accedere a destra per aggiungere un gruppo di risorse.



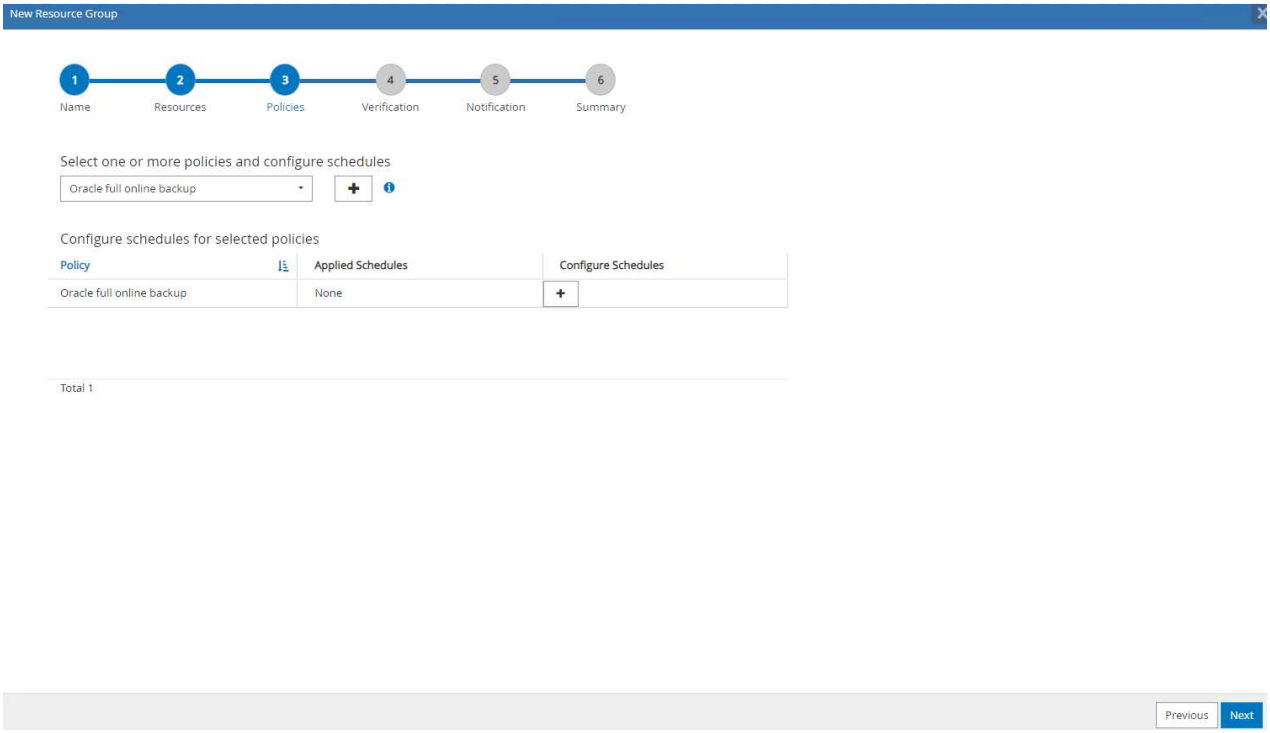
3. Assegnare un nome al gruppo di risorse, ai tag e a qualsiasi denominazione personalizzata.

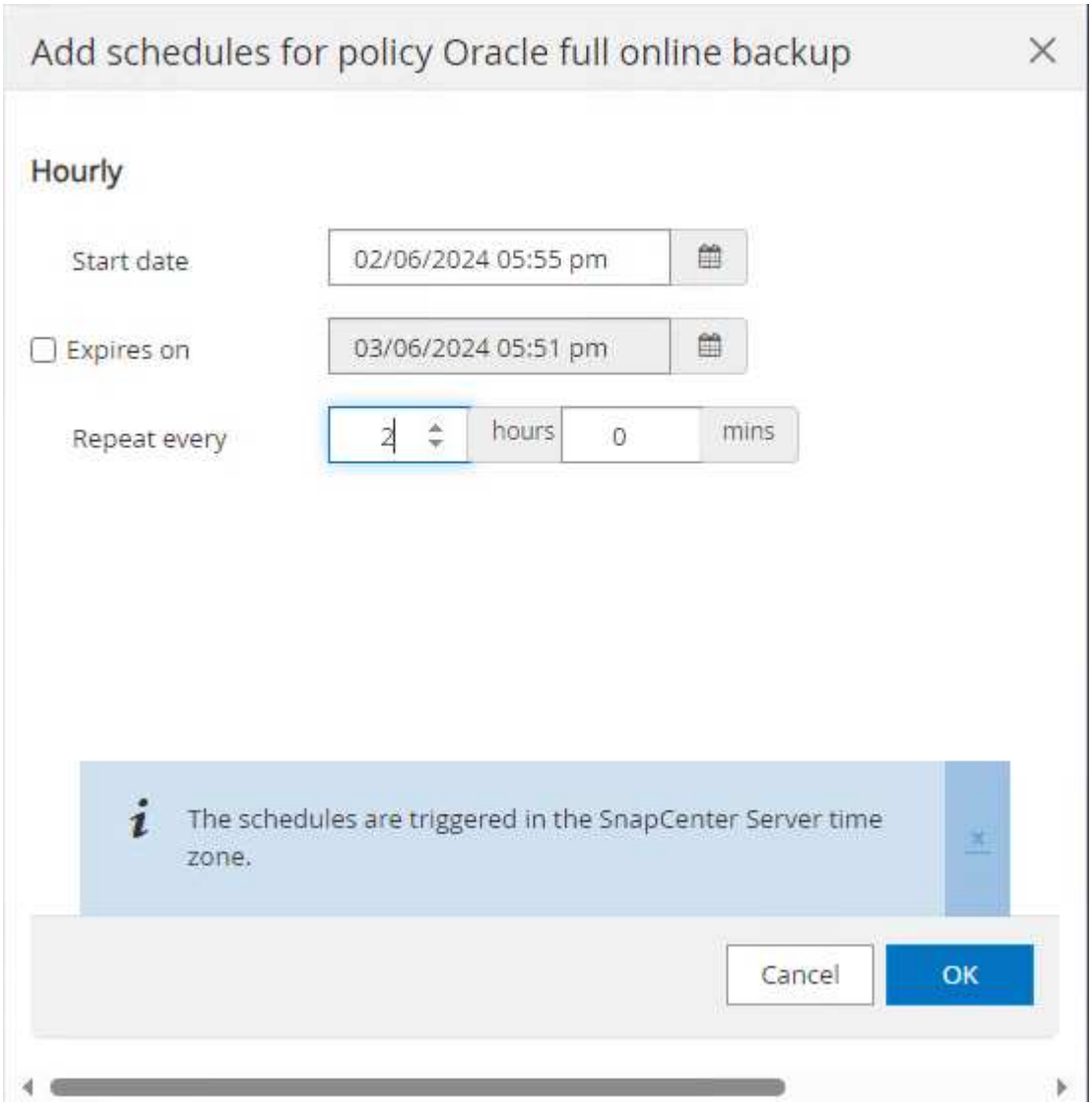


4. Aggiungere risorse al `Resource Group`. Il raggruppamento di risorse simili può semplificare la gestione dei database in un ambiente di grandi dimensioni.

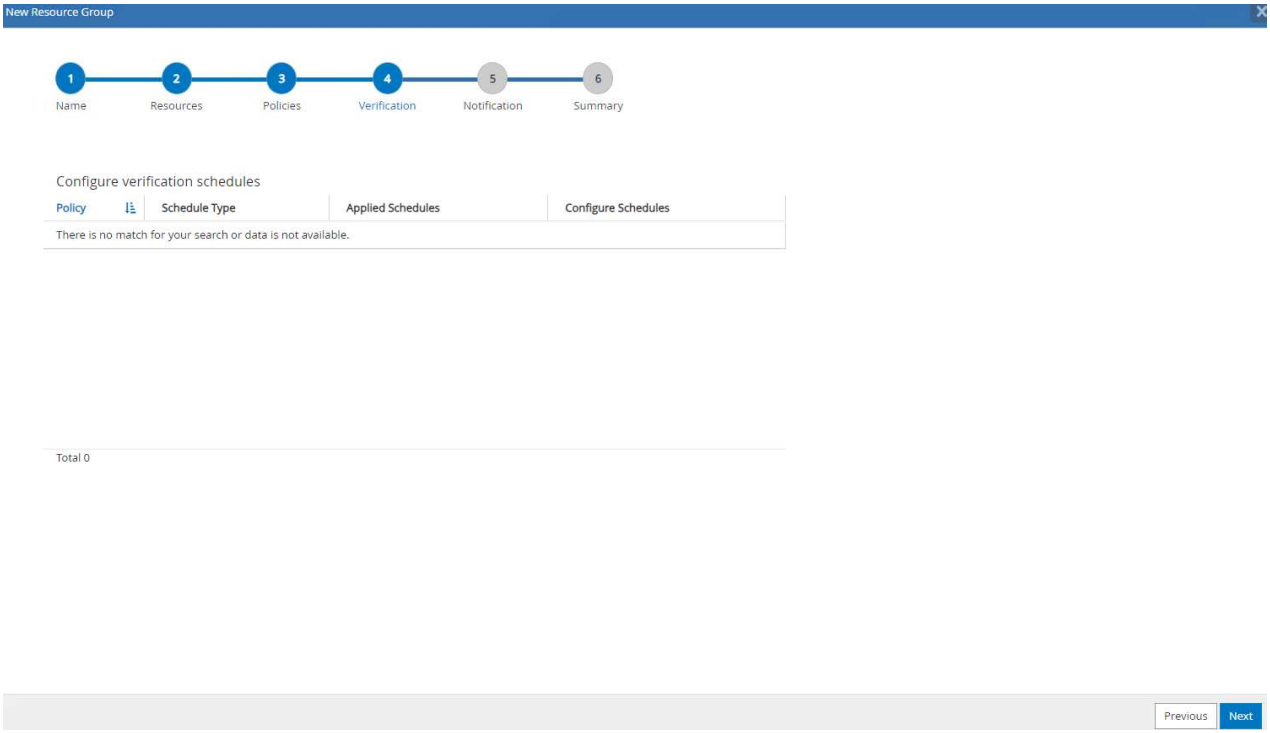


5. Selezionare il criterio di backup e impostare una pianificazione facendo clic sul segno "+" in `Configure Schedules`.

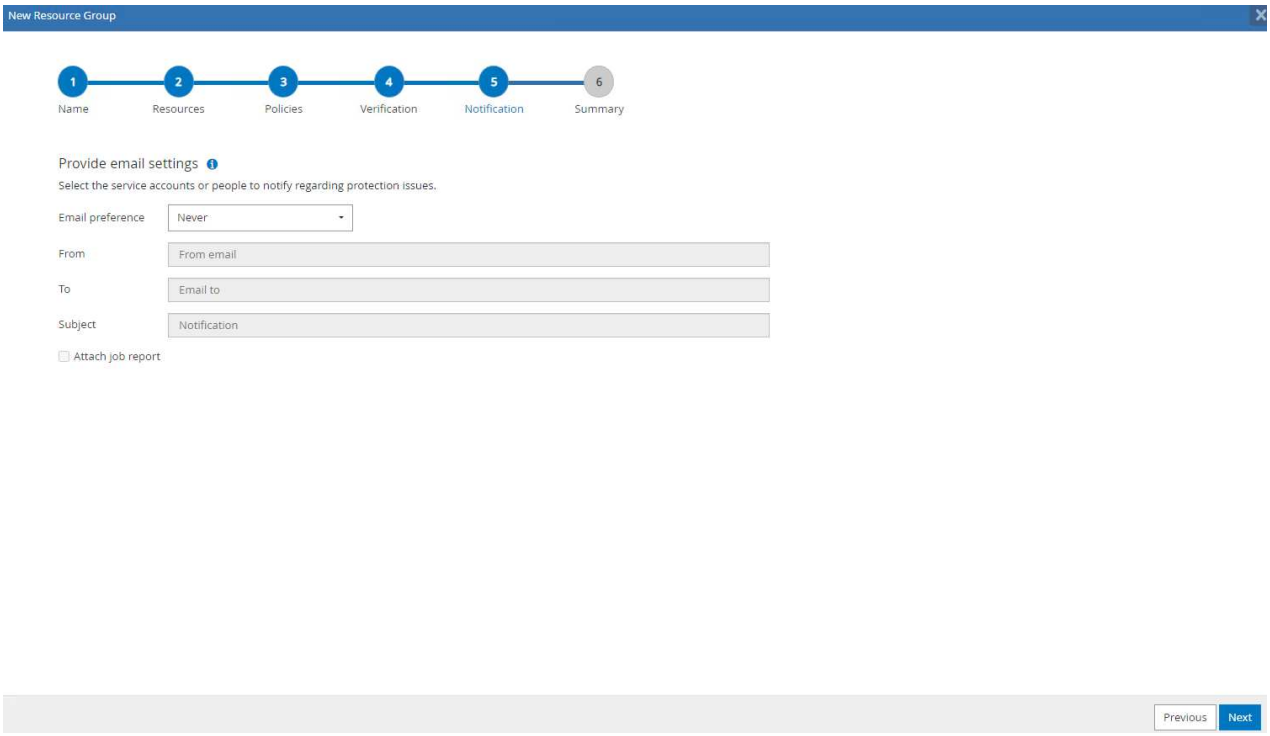

New Resource Group
1 Name
2 Resources
3 Policies
4 Verification
5 Notification
6 Summary
Select one or more policies and configure schedules
Oracle full online backup
Configure schedules for selected policies
Policy
Applied Schedules
Configure Schedules
Oracle full online backup
None
Total 1
Previous
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

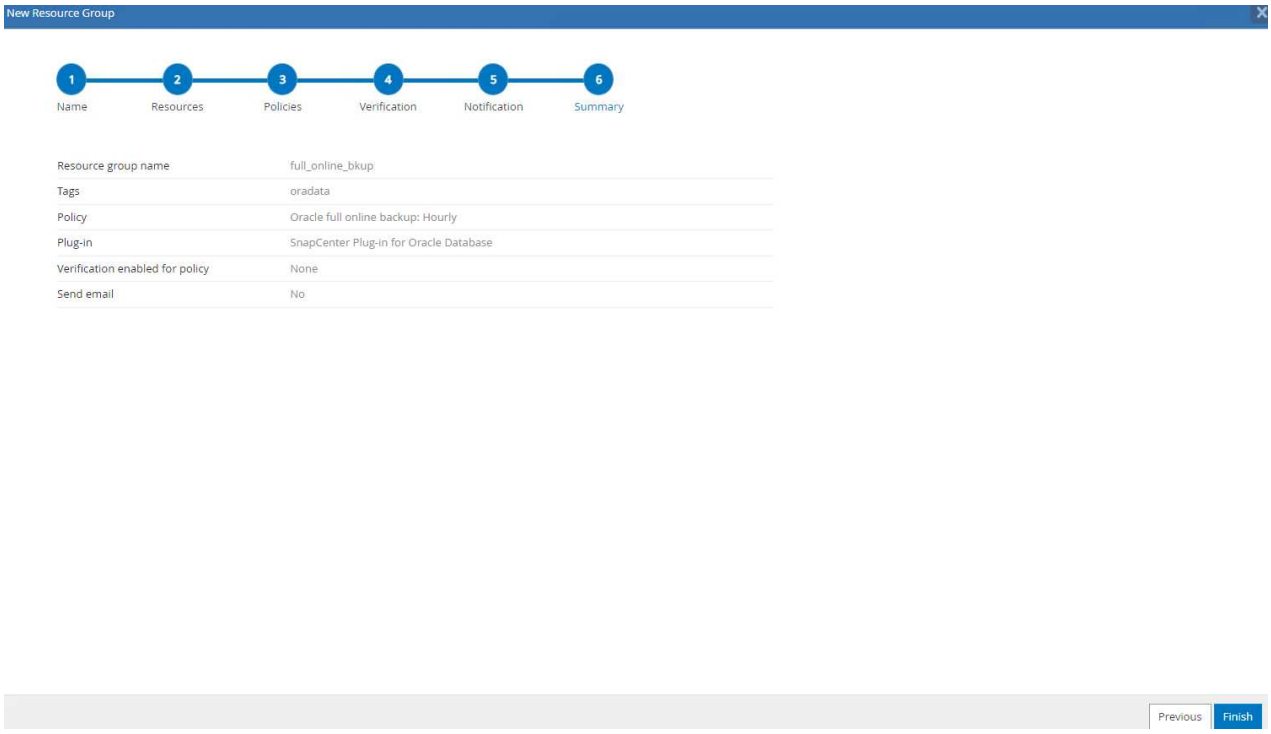
6. Se la verifica del backup non è configurata nel criterio, lasciare la pagina di verifica così com'è.



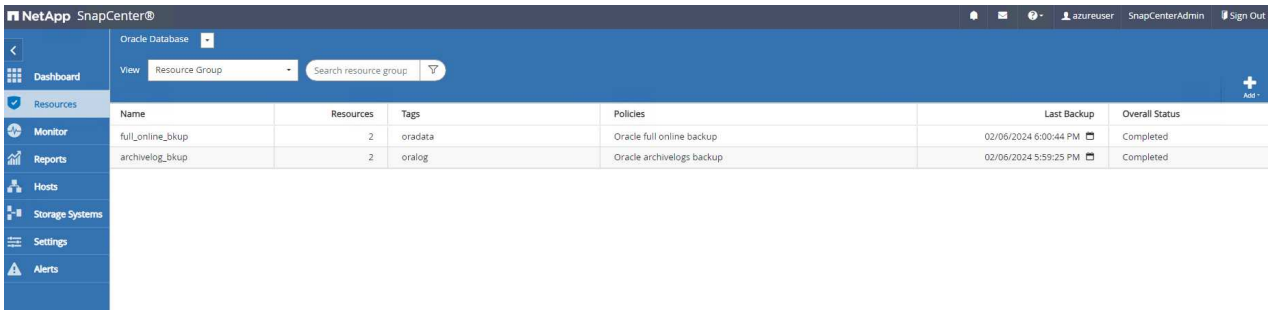
7. Per inviare un report di backup e una notifica tramite e-mail, è necessario un server di posta SMTP nell'ambiente. Oppure lasciarla nera se un server di posta non è configurato.



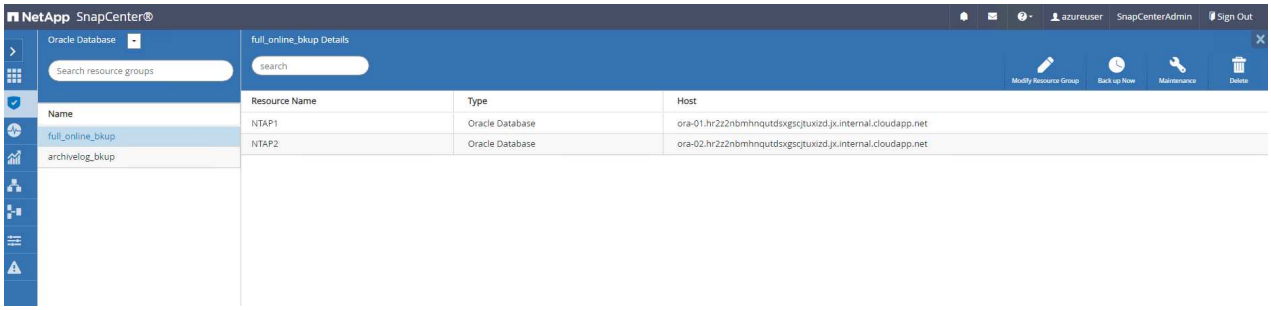
8. Riepilogo del nuovo gruppo di risorse.

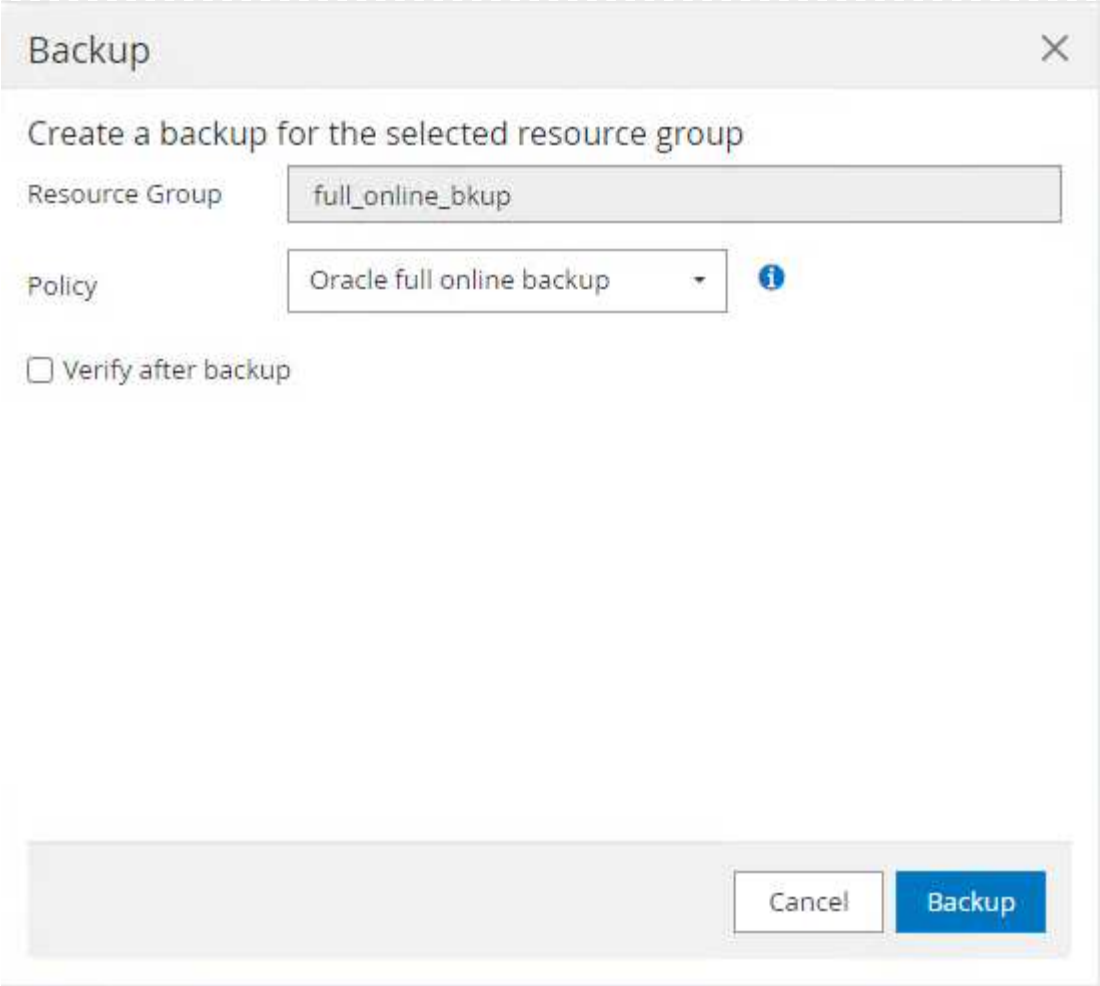


9. Ripetere le procedure descritte sopra per creare un backup solo del registro di archivio del database con i criteri di backup corrispondenti.

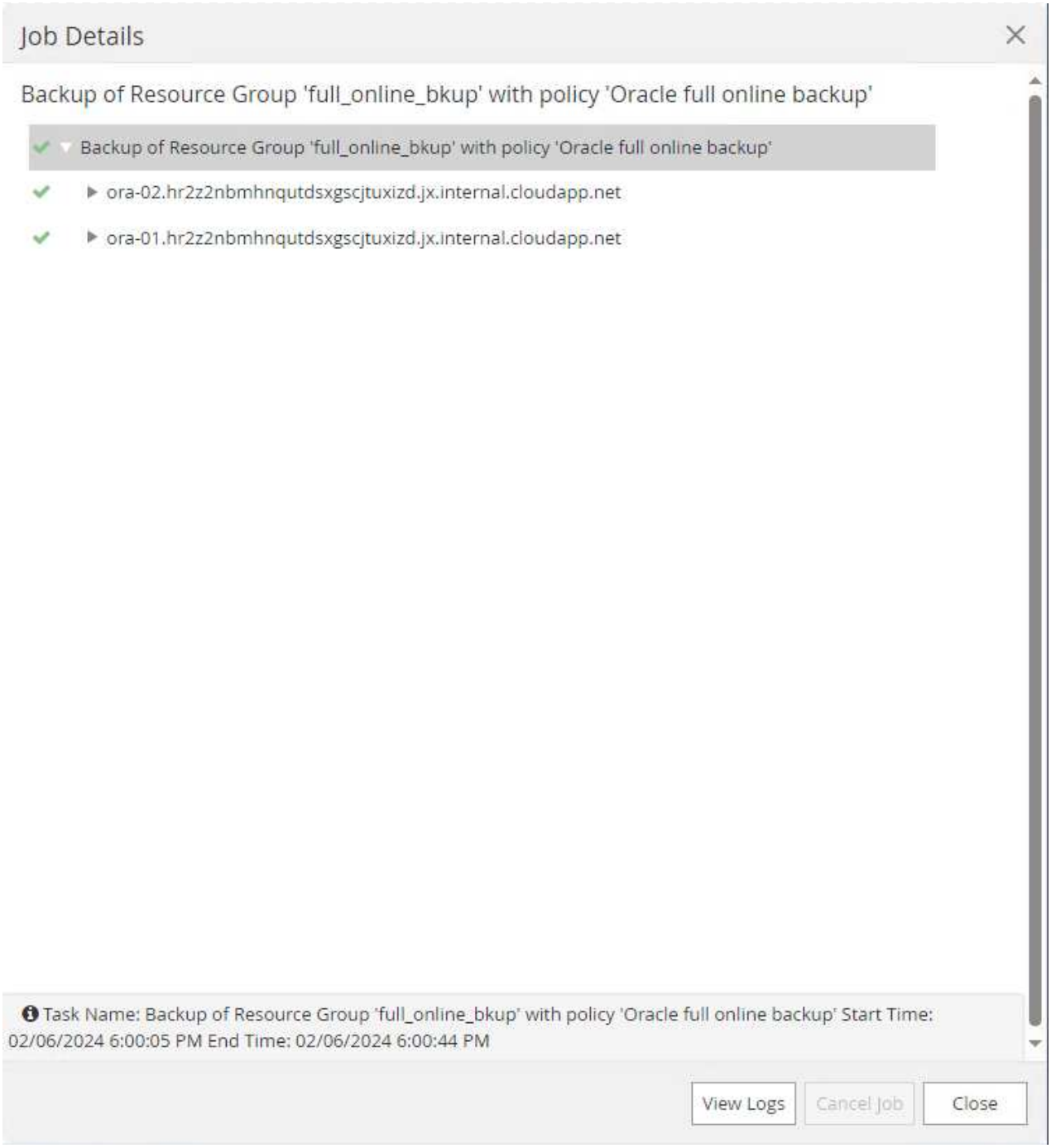


10. Fare clic su un gruppo di risorse per visualizzare le risorse incluse. Oltre al processo di backup pianificato, è possibile attivare un backup singolo facendo clic su `Backup Now`.

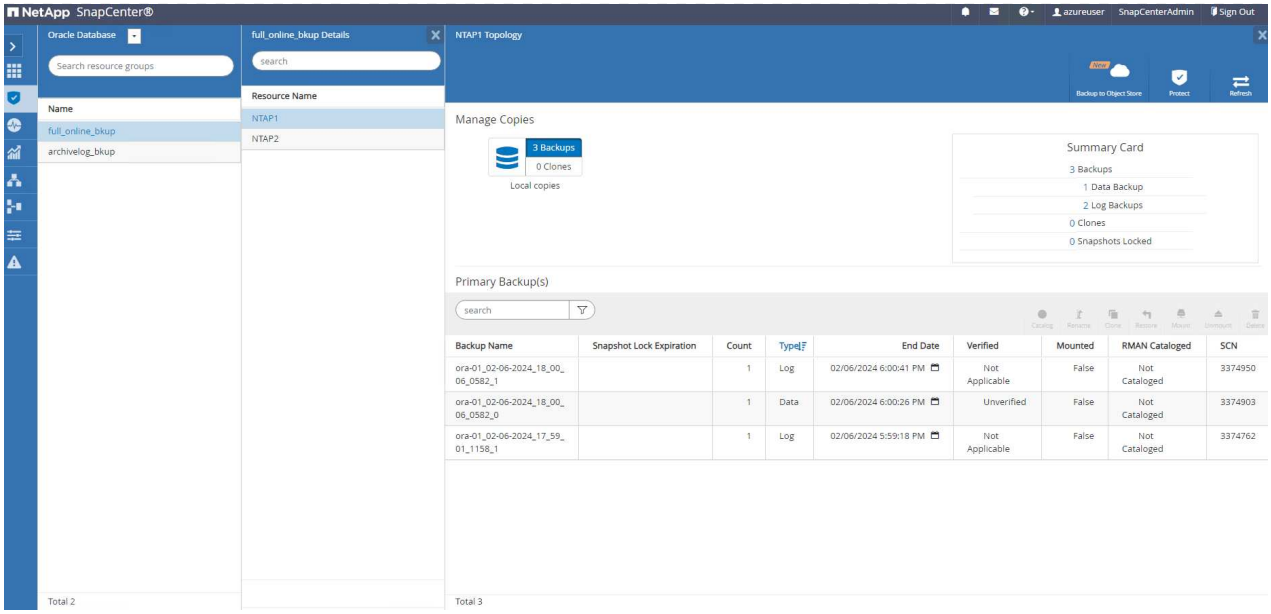




11. Fare clic sul lavoro in esecuzione per aprire una finestra di monitoraggio che consente all'operatore di tenere traccia dell'avanzamento del lavoro in tempo reale.



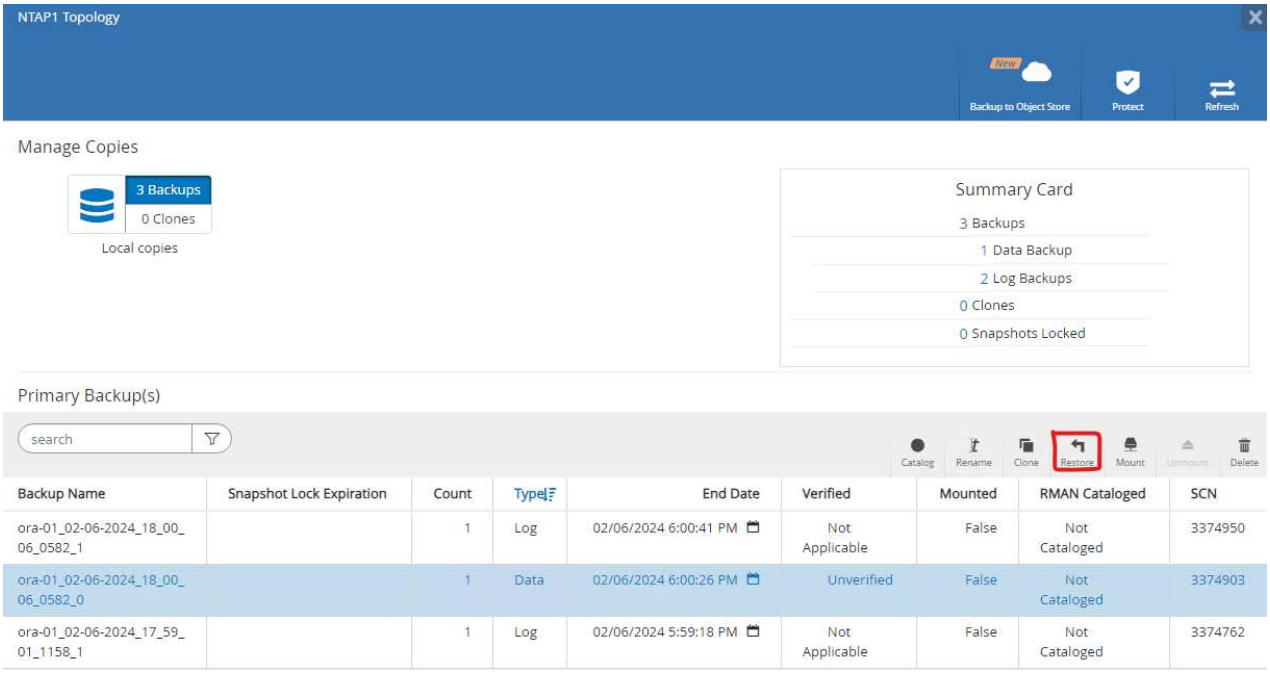
12. Una volta completato un processo di backup, viene visualizzato un set di backup snapshot nella topologia del database. Un set di backup completo del database include uno snapshot dei volumi dei dati del database e uno snapshot dei volumi del log del database. Un backup di solo registro contiene solo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



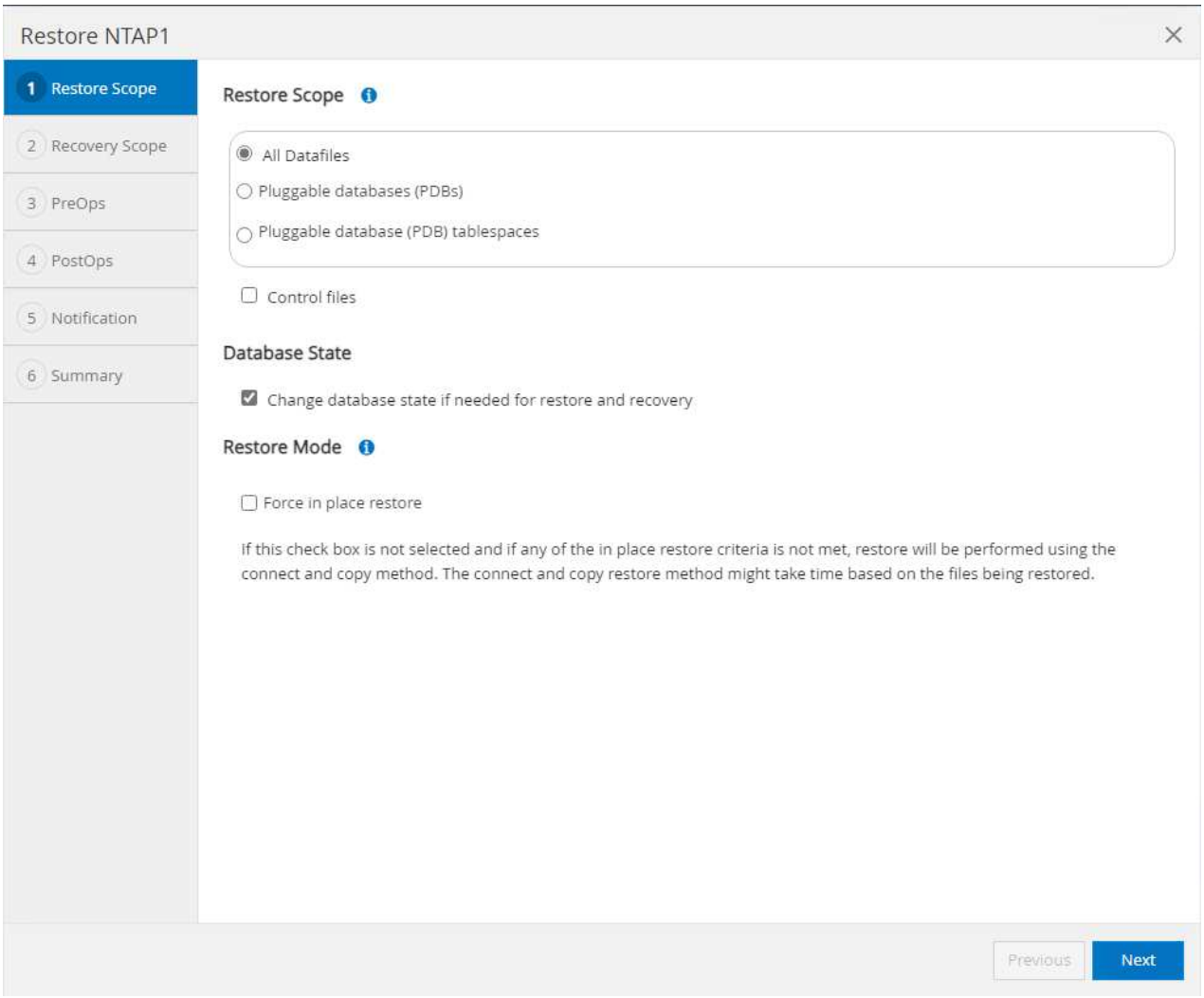
Recovery del database

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.

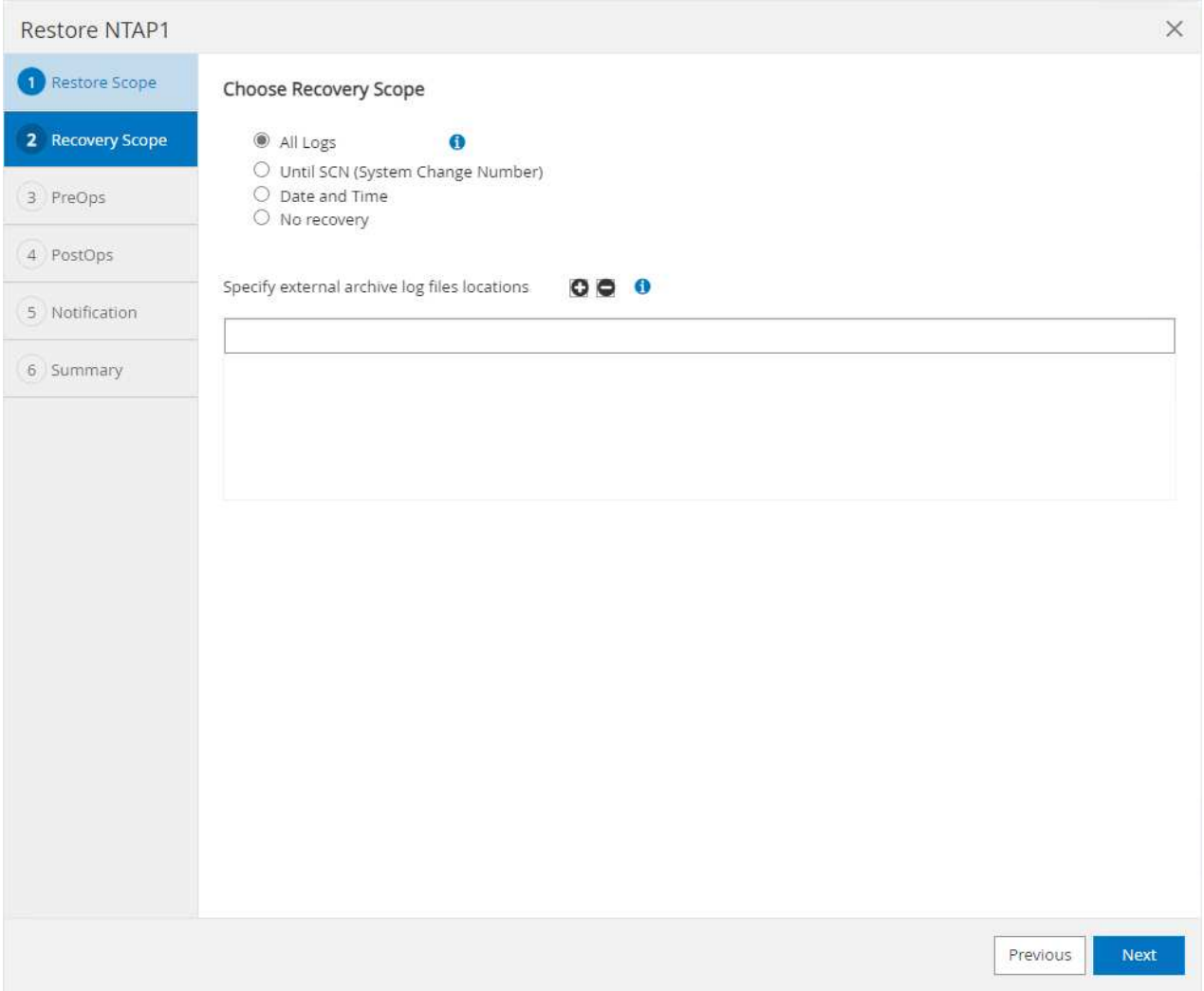
1. Da `Resources` aprire il database `Primary Backup(s)` pagina. Scegliere lo snapshot del volume di dati del database, quindi fare clic su `Restore` per avviare il flusso di lavoro di ripristino del database. Se si desidera eseguire il ripristino da Oracle SCN o timestamp, annotare il numero SCN o l'indicatore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



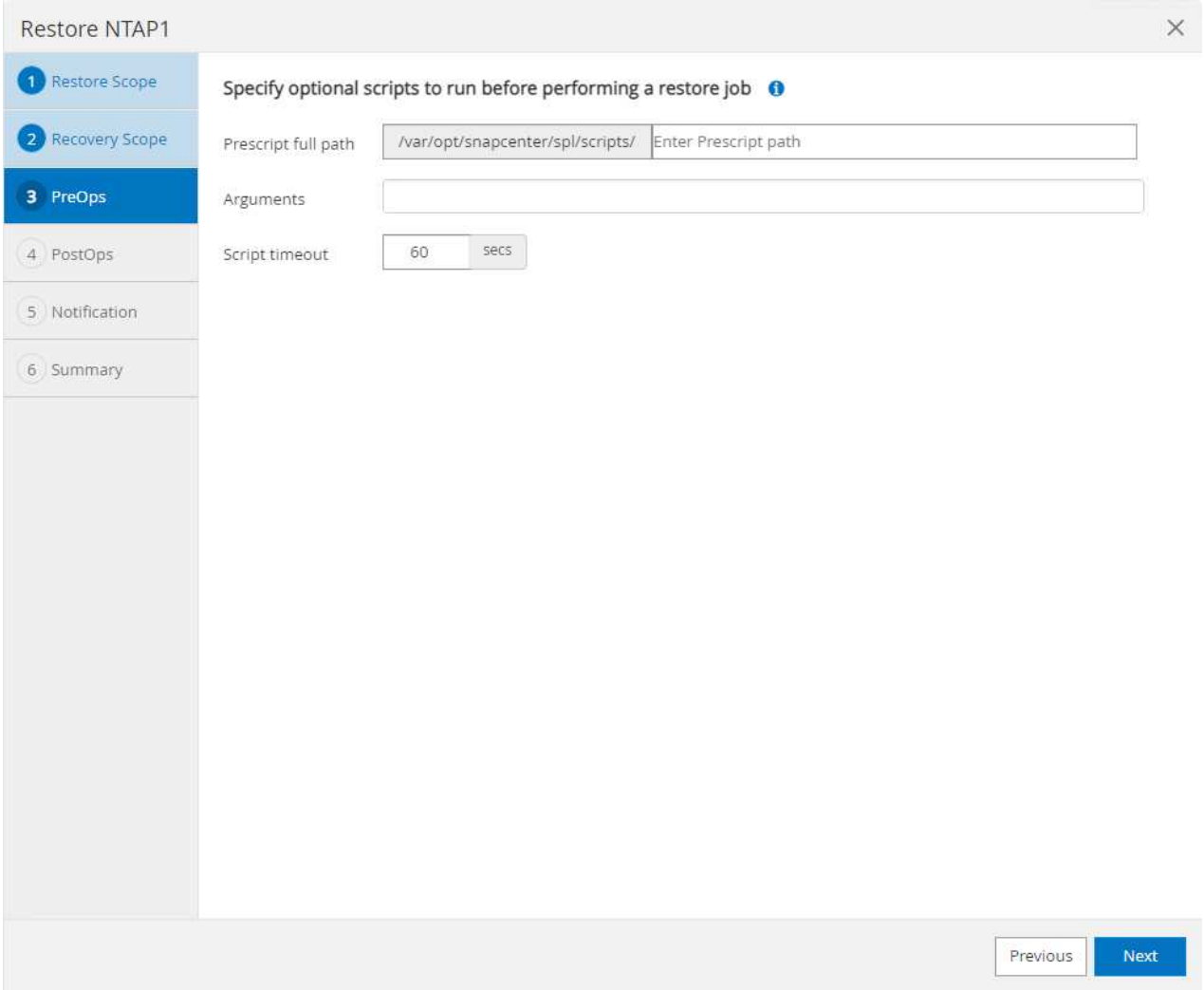
2. Selezionare `Restore Scope`. Per un database di container, SnapCenter è flessibile per eseguire un ripristino a livello di tablespace, database inseribili o database completo di container (tutti i file di dati).



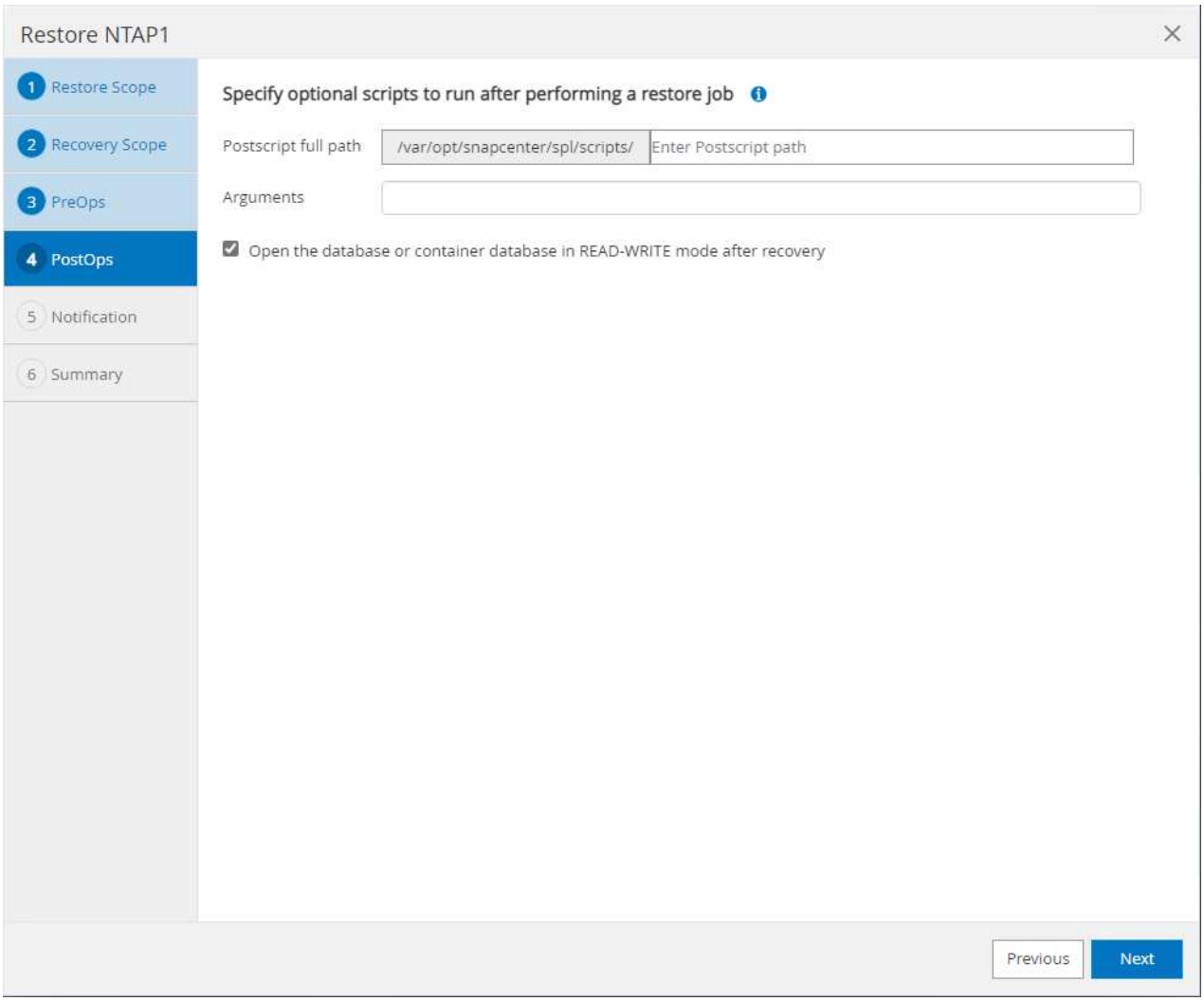
3. Selezionare `Recovery Scope`. `All logs` significa applicare tutti i log di archivio disponibili nel set di backup. Sono disponibili anche il ripristino point-in-time da parte di SCN o timestamp.



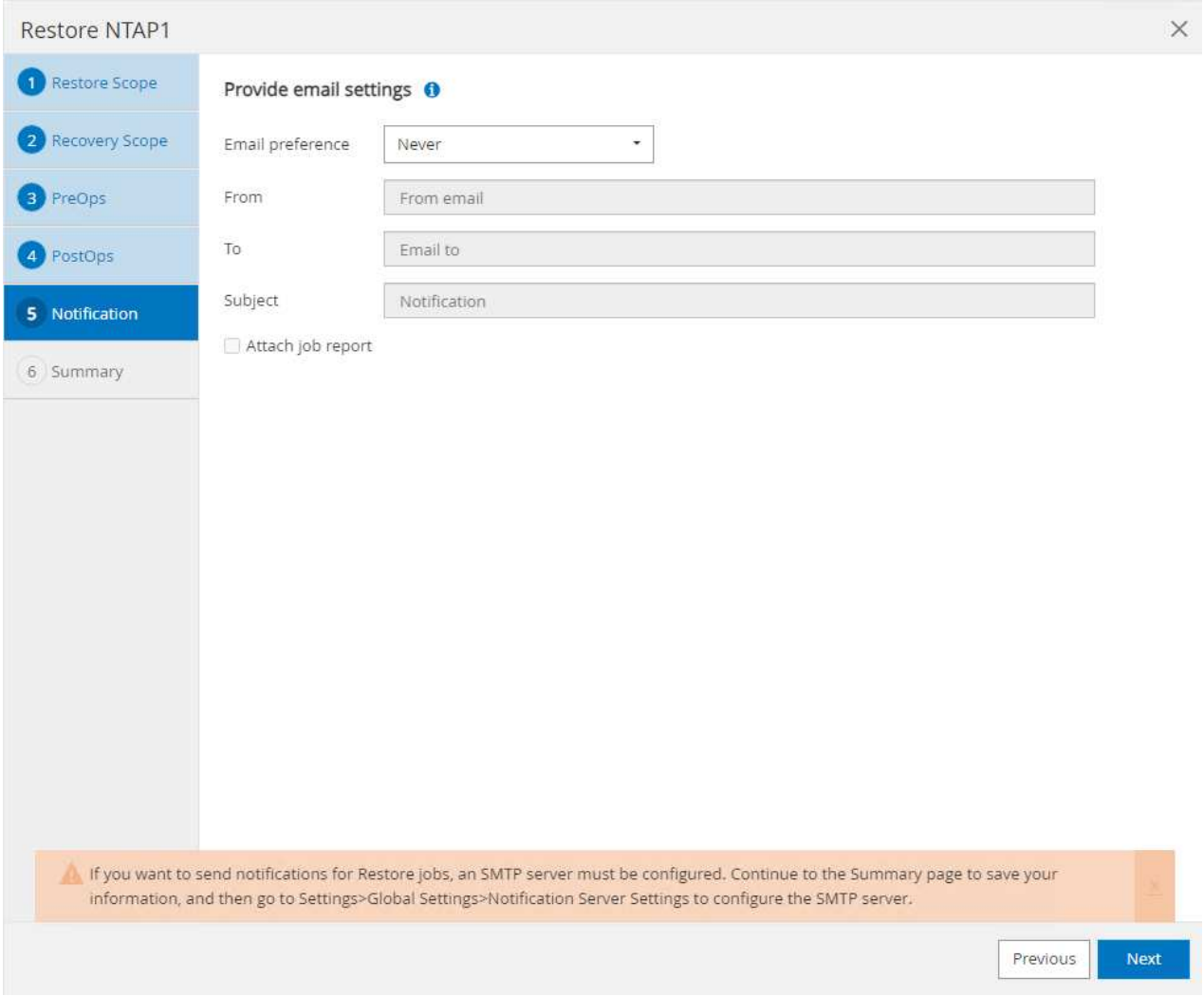
4. Il `PreOps` consente l'esecuzione di script sul database prima dell'operazione di ripristino/ripristino.



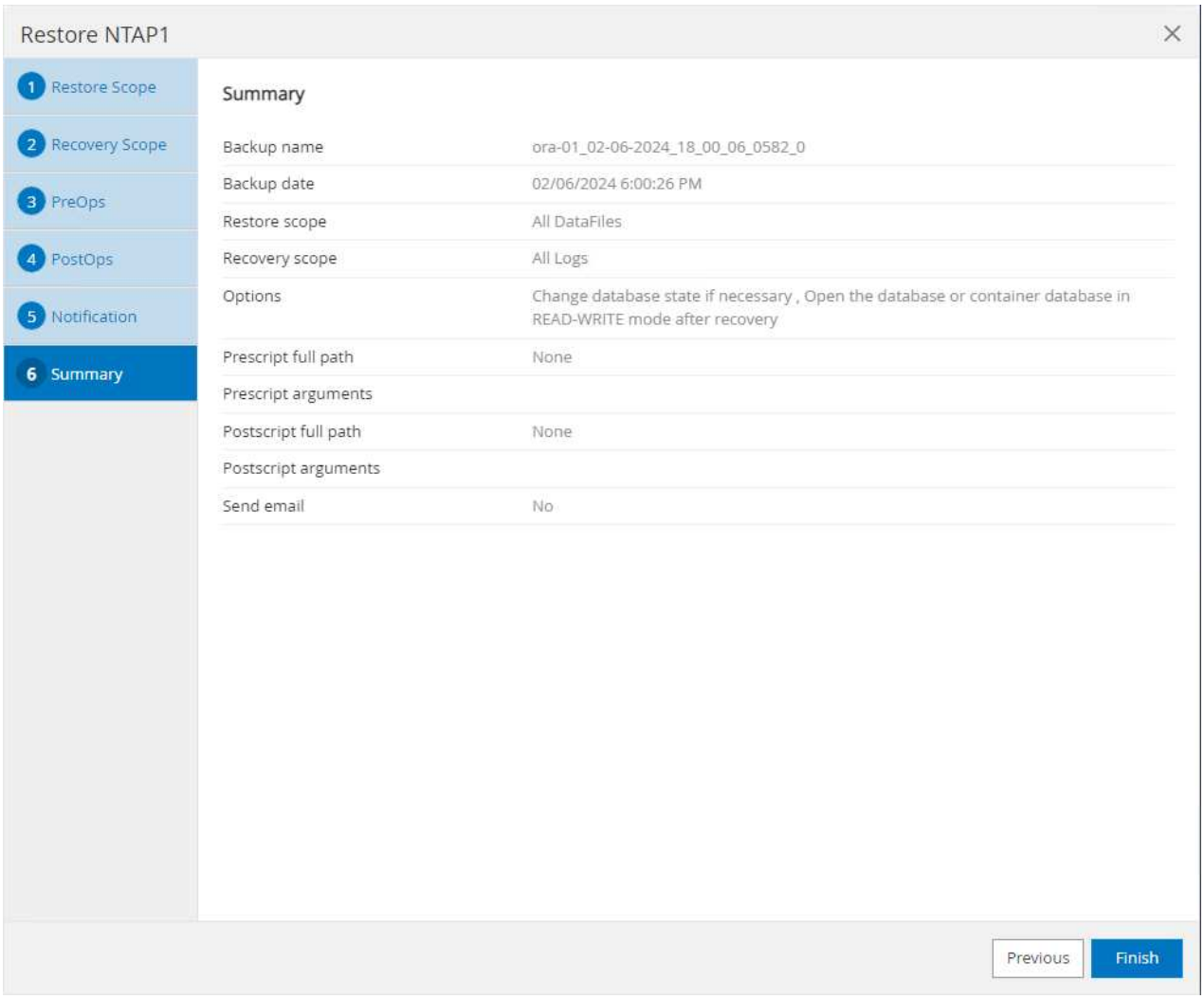
5. Il `PostOps` consente l'esecuzione di script sul database dopo l'operazione di ripristino/ripristino.



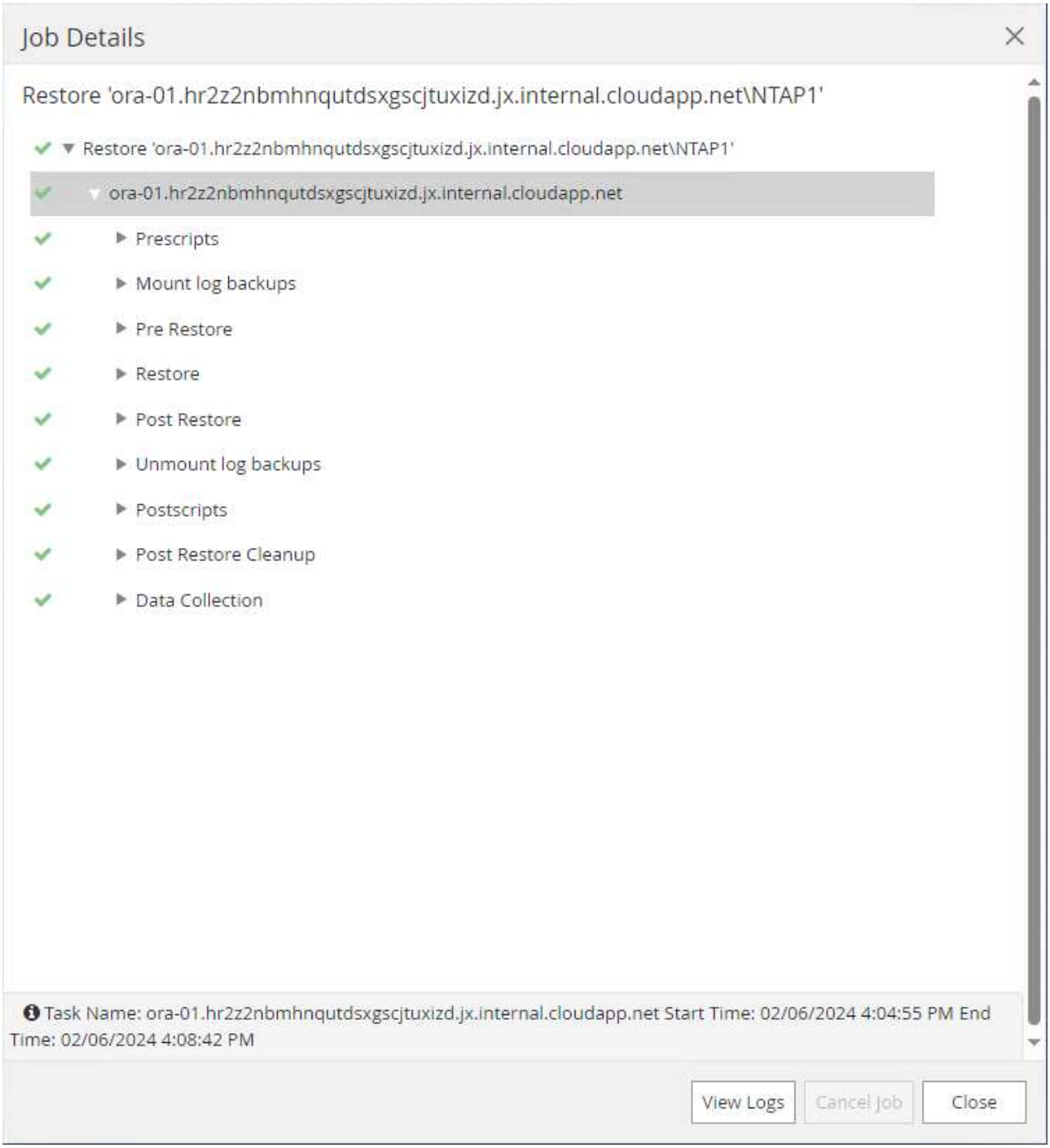
6. Notifica via e-mail, se lo si desidera.



7. Ripristinare il riepilogo del processo



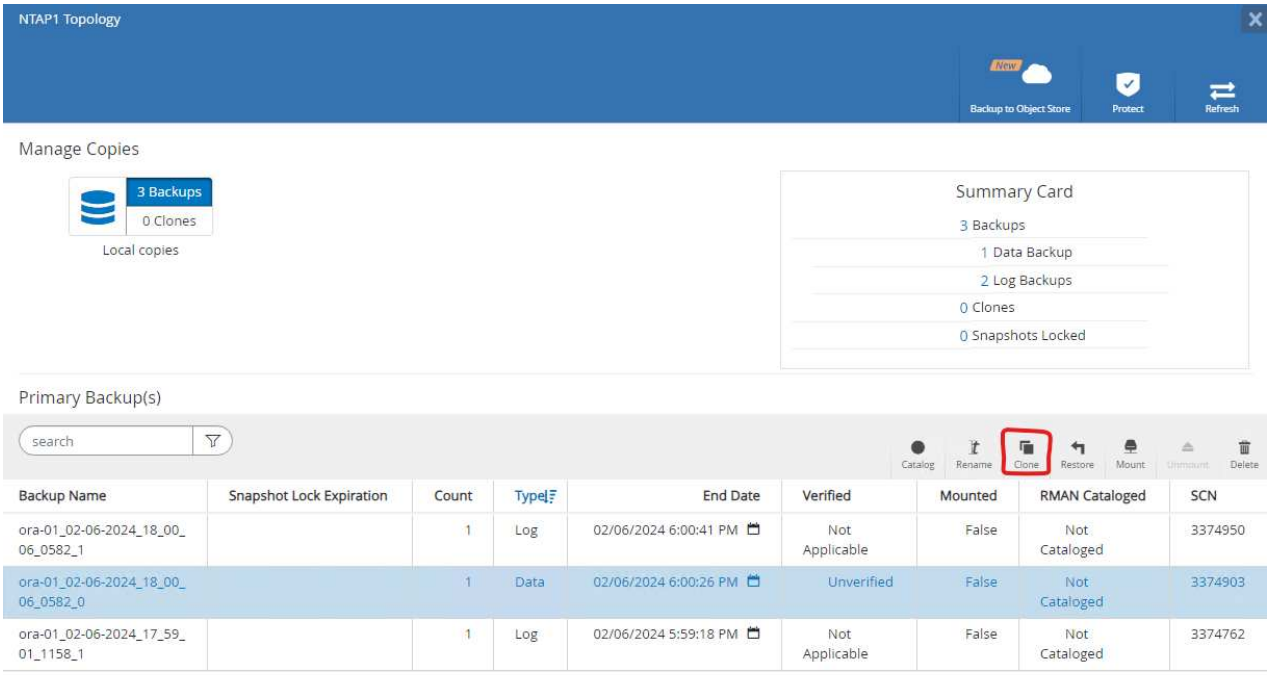
8. Fare clic su processo in esecuzione per aprirlo `Job Details` finestra. Lo stato del lavoro può essere aperto e visualizzato anche da `Monitor` scheda.



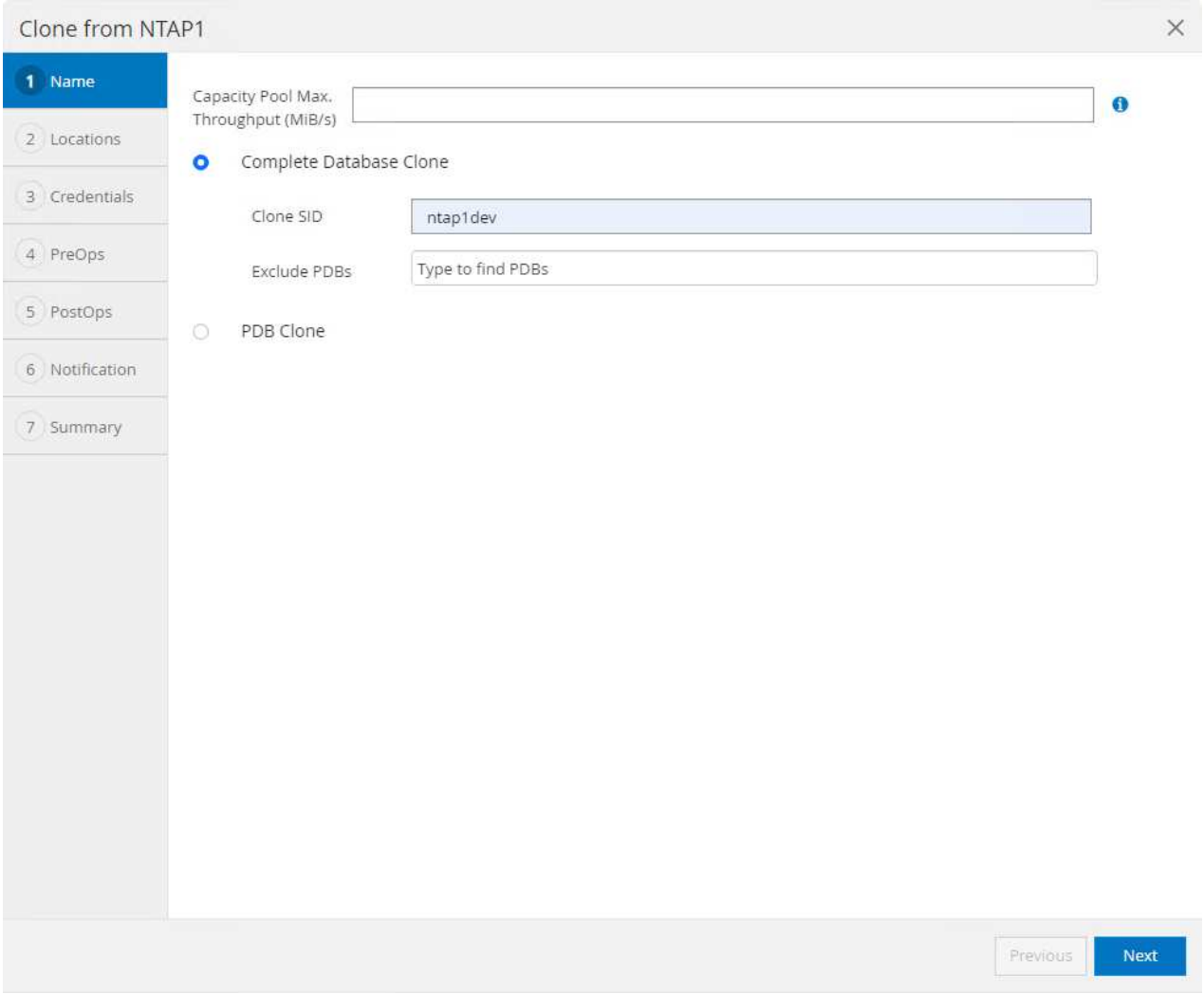
Clone del database

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.

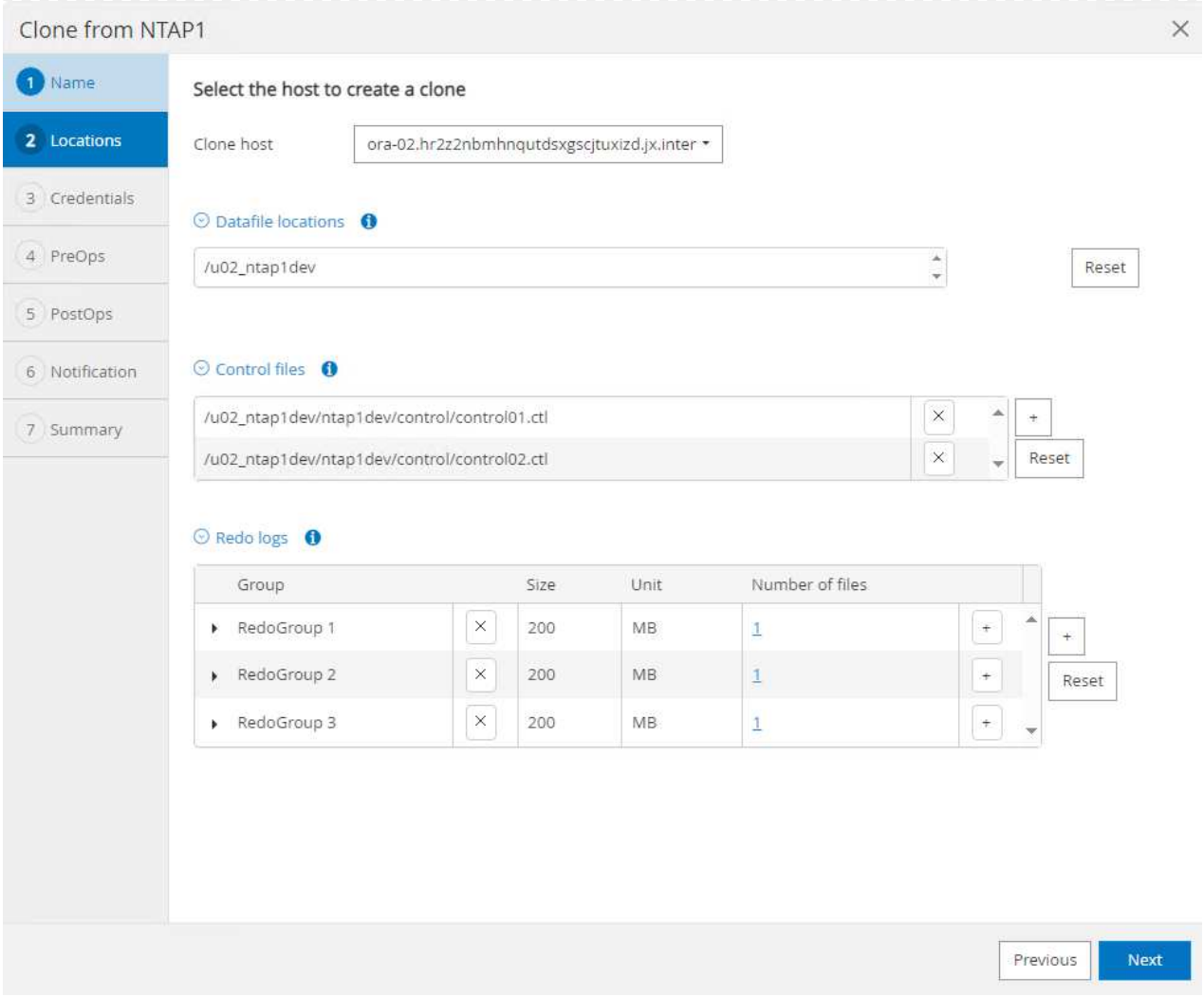
1. Da `Resources` aprire il database `Primary Backup(s)` pagina. Scegliere lo snapshot del volume di dati del database, quindi fare clic su `clone` per avviare il flusso di lavoro dei cloni del database.



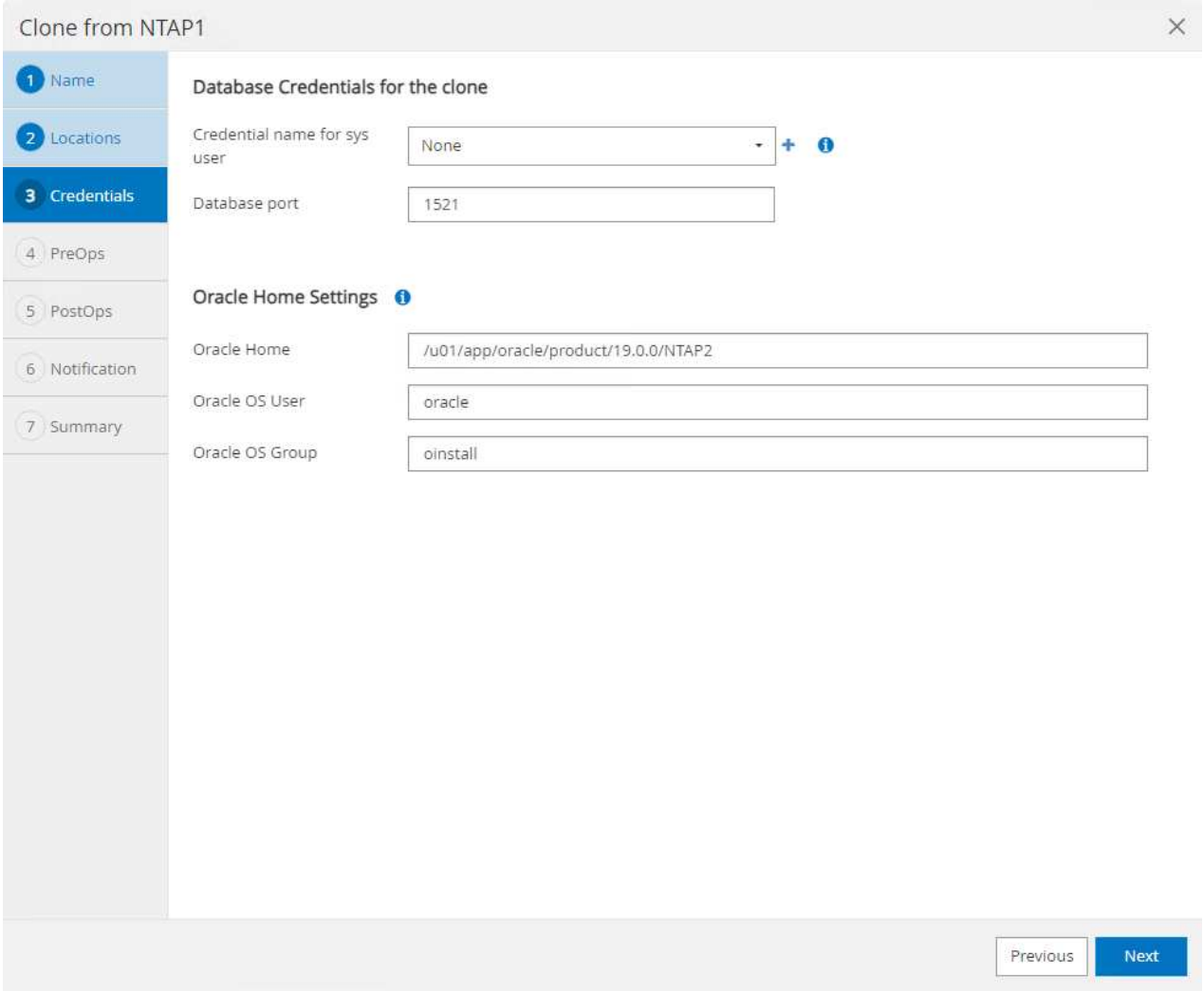
2. Assegnare un nome al SID del database clone. In alternativa, per un database di container, il cloning può essere eseguito anche a livello di PDB.



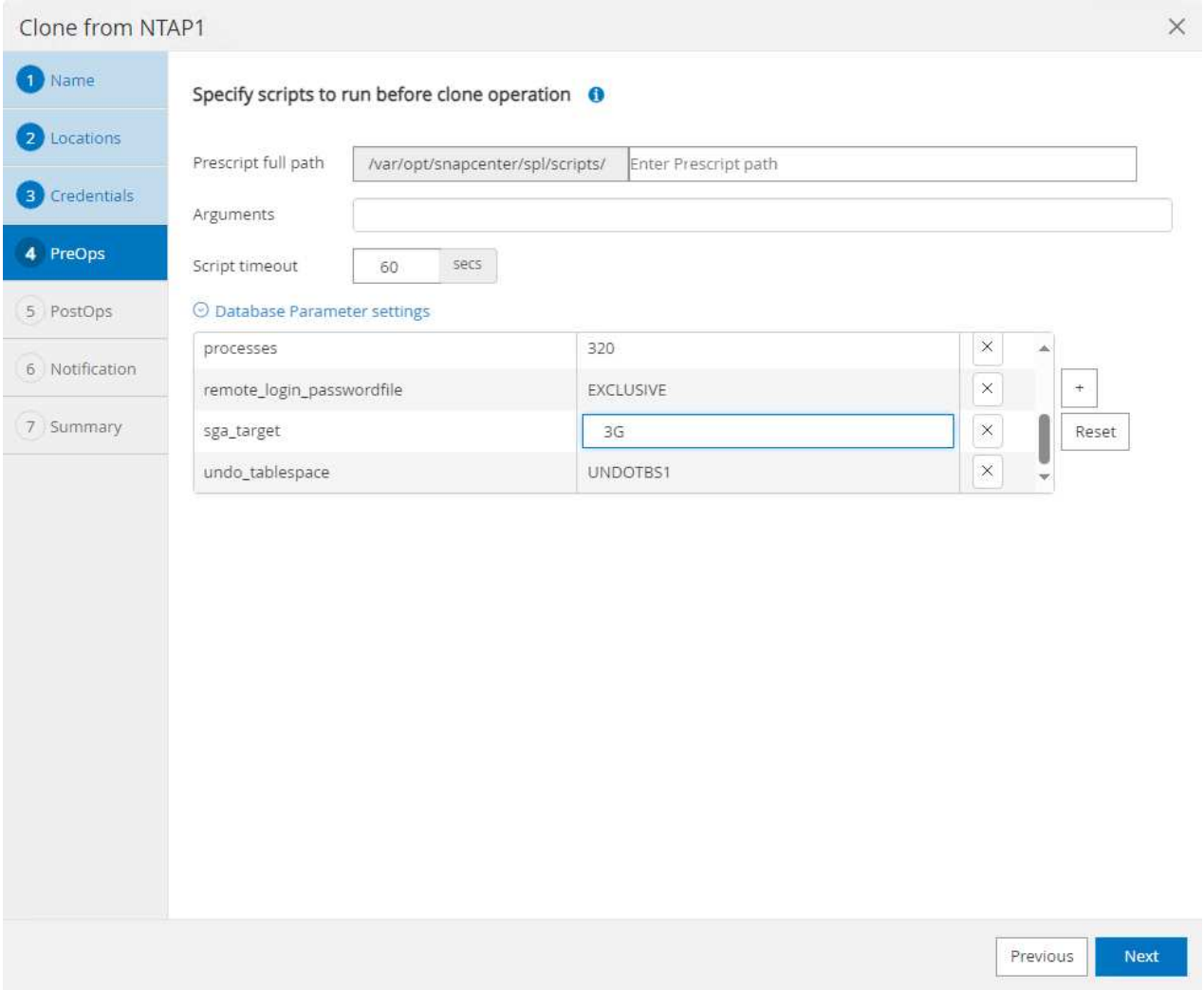
3. Selezionare il server DB in cui si desidera collocare la copia del database clonata. Mantenere le posizioni predefinite dei file a meno che non si desideri assegnare loro un nome diverso.



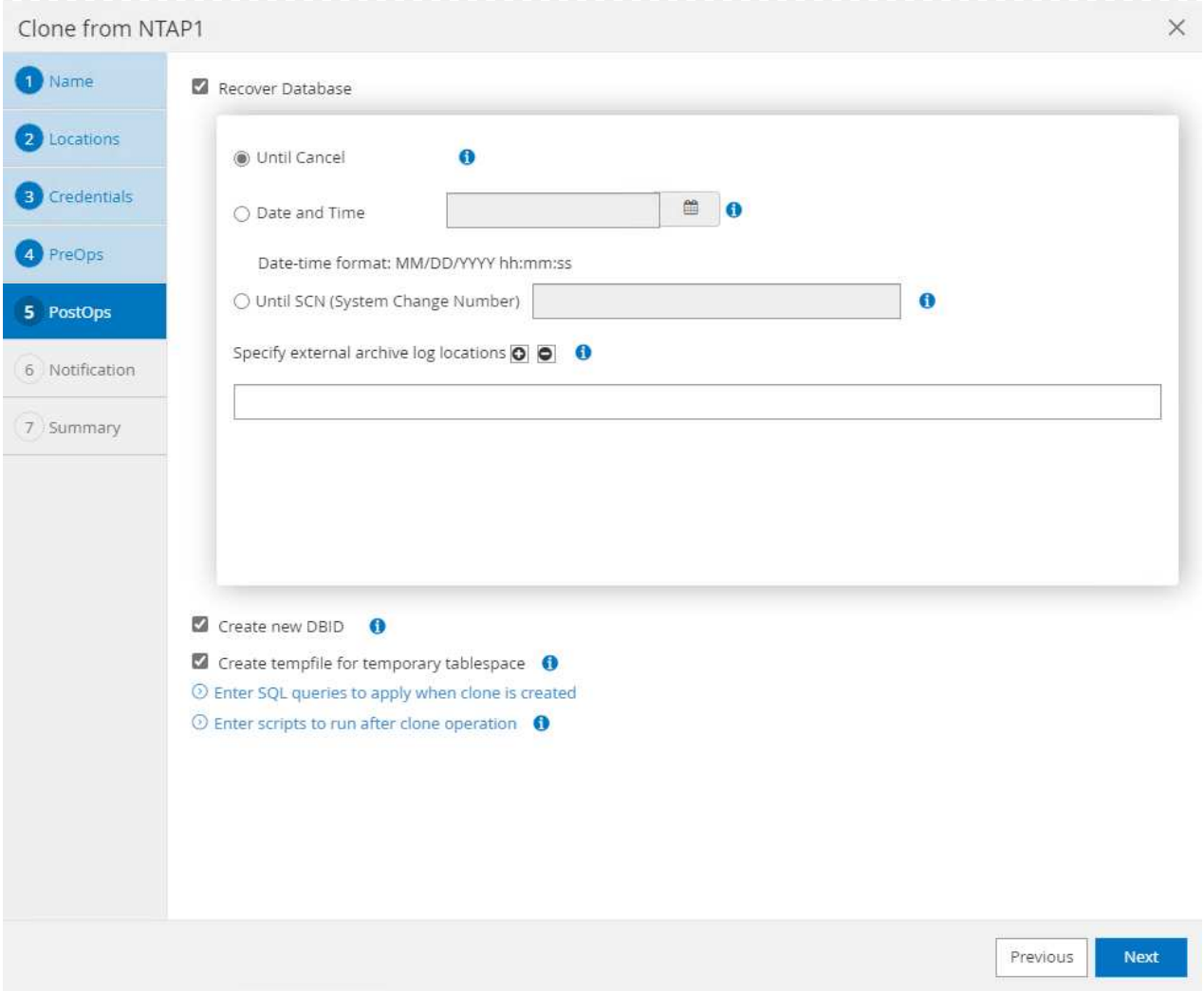
4. Lo stack software Oracle identico a quello del database di origine deve essere installato e configurato sull'host DB clone. Mantenere la credenziale predefinita ma modificarla `Oracle Home Settings` Per la corrispondenza con le impostazioni sull'host DB clone.



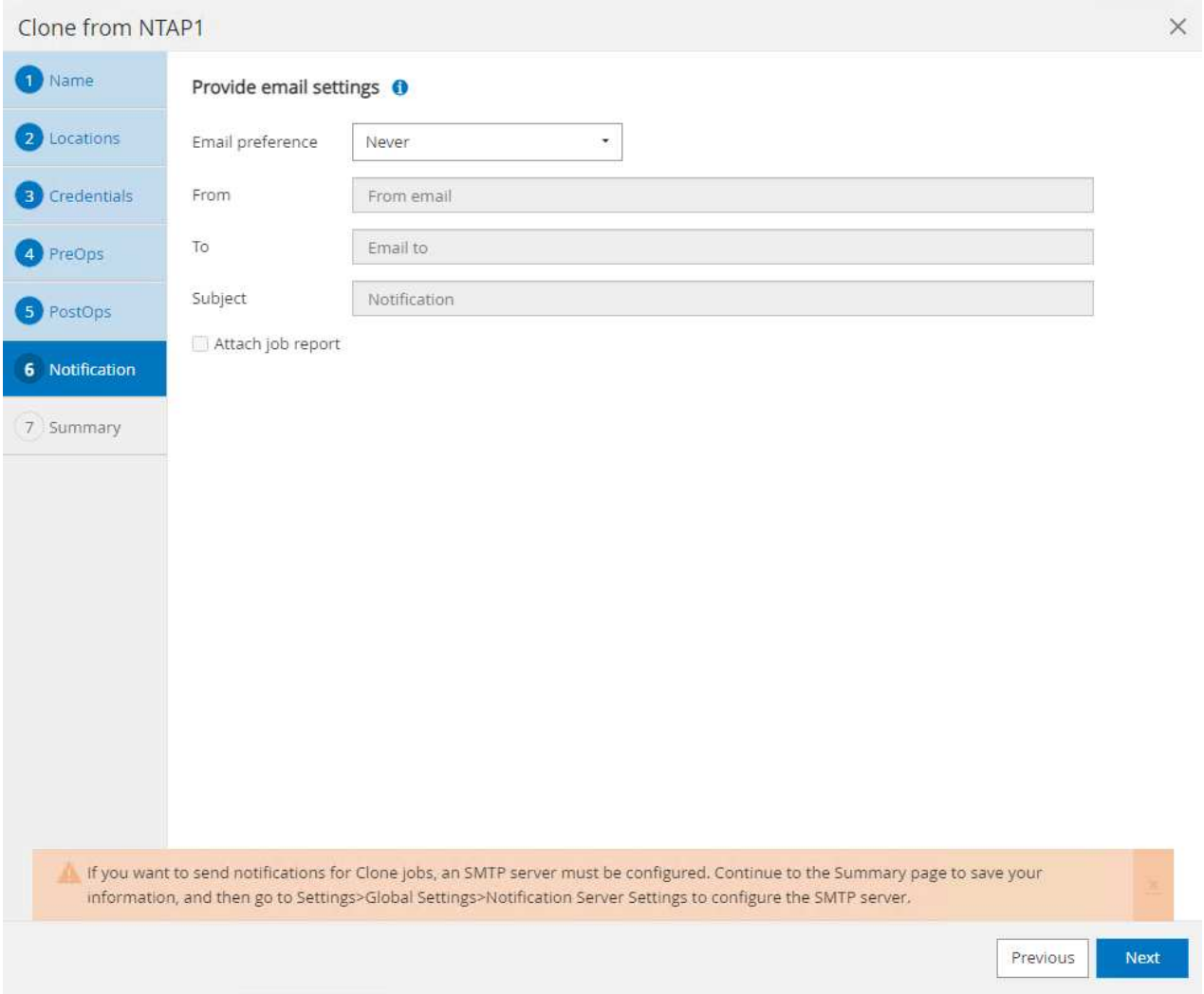
5. Il `PreOps` consente l'esecuzione degli script prima dell'operazione di clonazione. I parametri del database possono essere regolati per soddisfare le esigenze di un DB clone rispetto a un database di produzione, come una destinazione SGA ridotta.



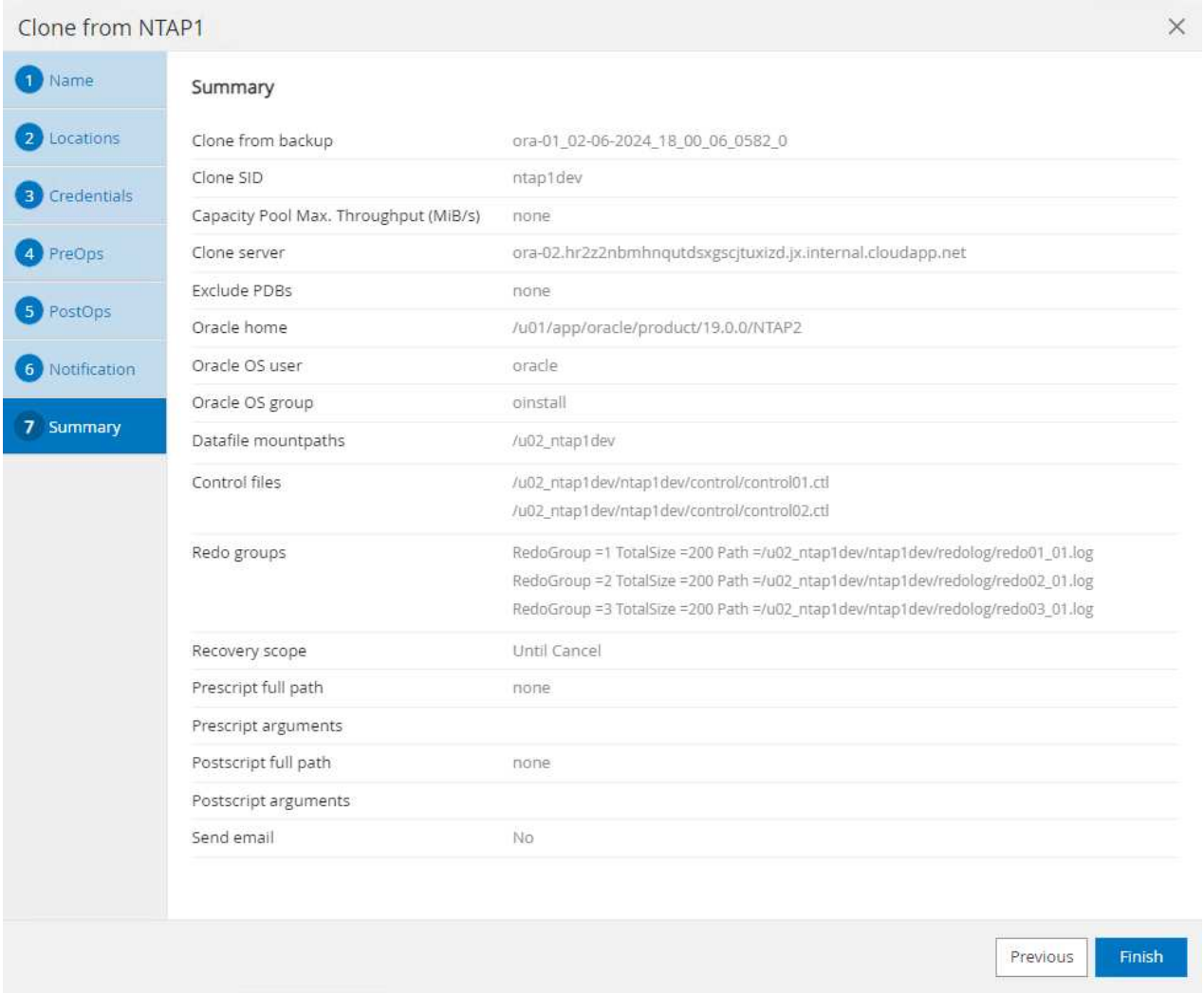
6. Il `PostOps` consente l'esecuzione di script sul database dopo l'operazione di clonazione. Il ripristino del database clone può essere basato su SCN, timestamp o fino a quando non viene annullato (rollforward del database all'ultimo log archiviato nel set di backup).



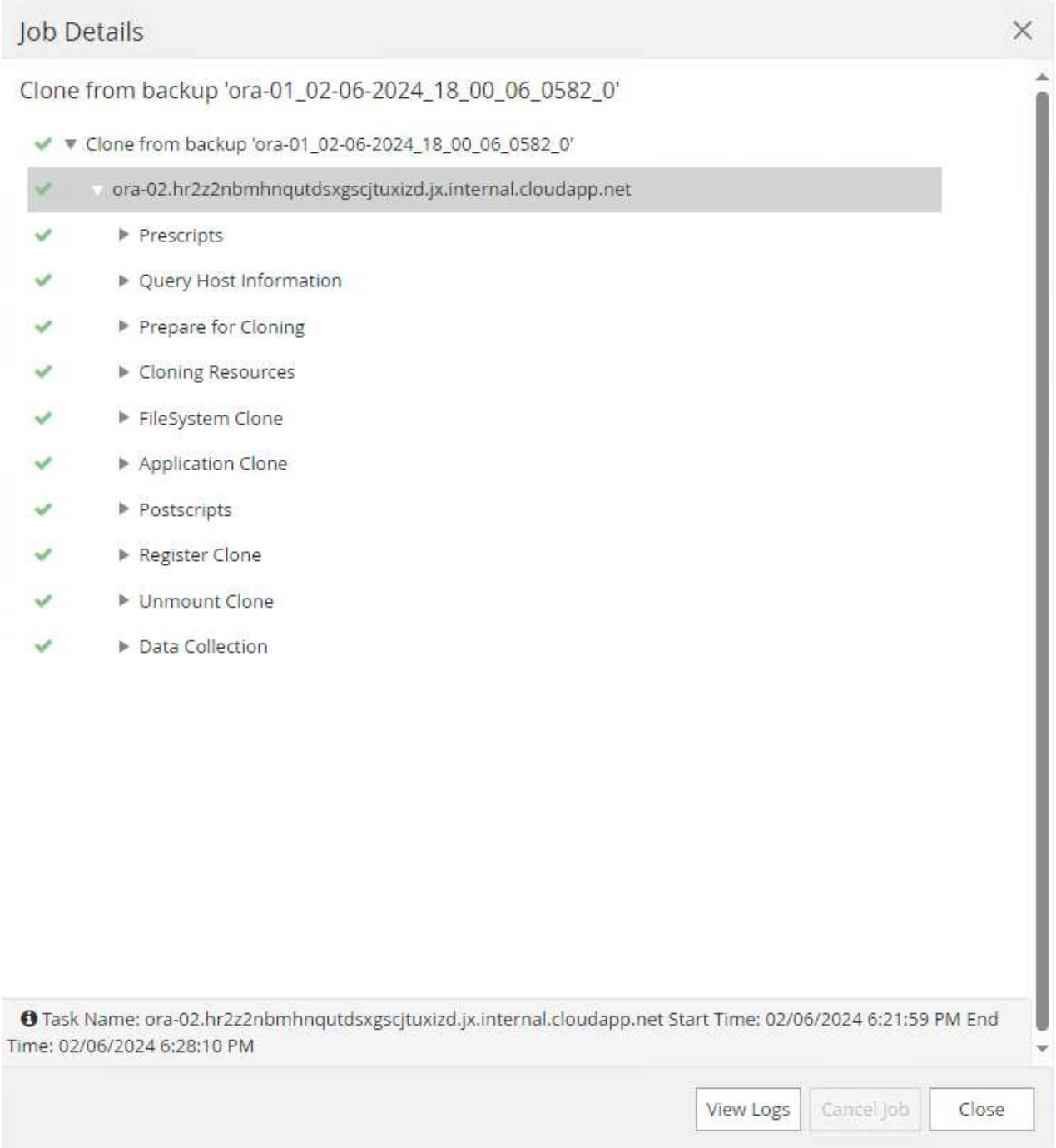
7. Notifica via e-mail, se lo si desidera.



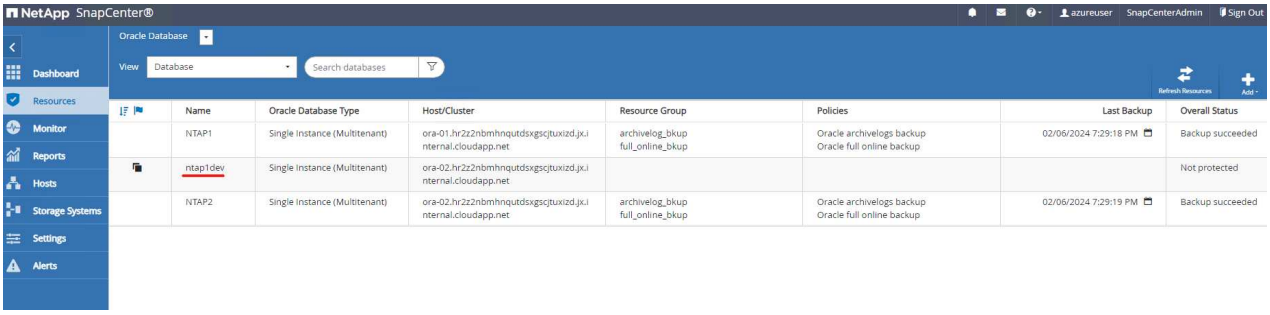
8. Clona riepilogo processi.



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.



10. Il database clonato si registra immediatamente con SnapCenter.



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_ntap1dev

[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)
ntap1dev:/u01/app/oracle/product/19.0.0/NTAP2:N


[oracle@ora-02 ~]$ export ORACLE_SID=ntap1dev
[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"

- Documentazione del software SnapCenter

  "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"

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.

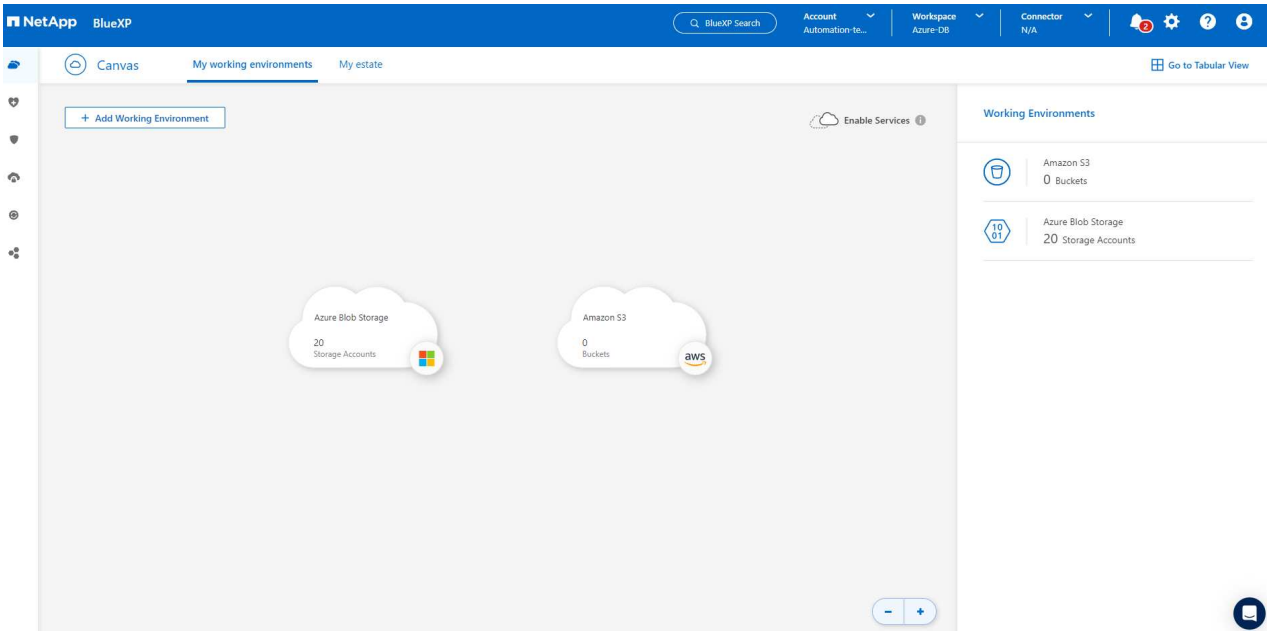
1. Un server di database Oracle primario su un'istanza di Azure VM con un database Oracle completamente implementato e in esecuzione.
2. Un pool di capacità dei servizi di storage Azure NetApp Files implementato in Azure che ha capacità per soddisfare le esigenze di storage per il database elencate nella 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

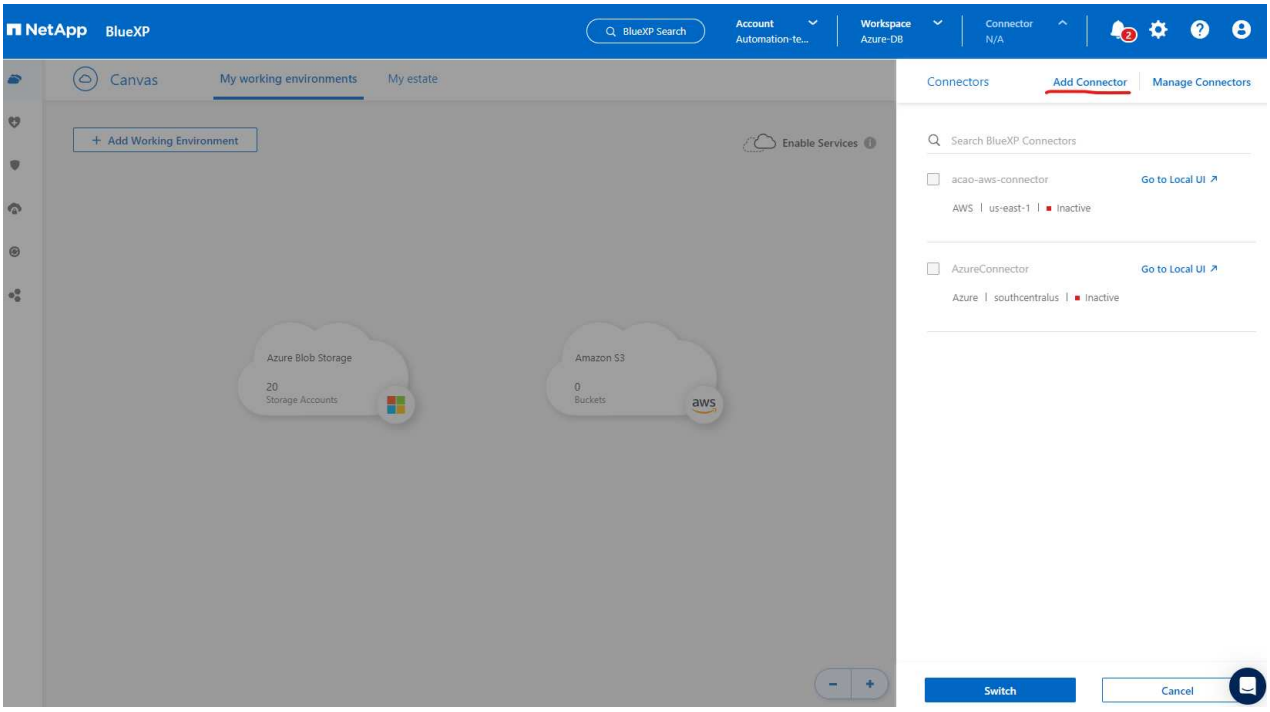
1. Utilizzare il link "NetApp BlueXP" Per iscriversi all'accesso alla console BlueXP.
2. Creare un account utente Azure o un principio di servizio Active Directory e concedere autorizzazioni con ruolo nel portale Azure per la distribuzione di Azure Connector.
3. Per configurare BlueXP per gestire le 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

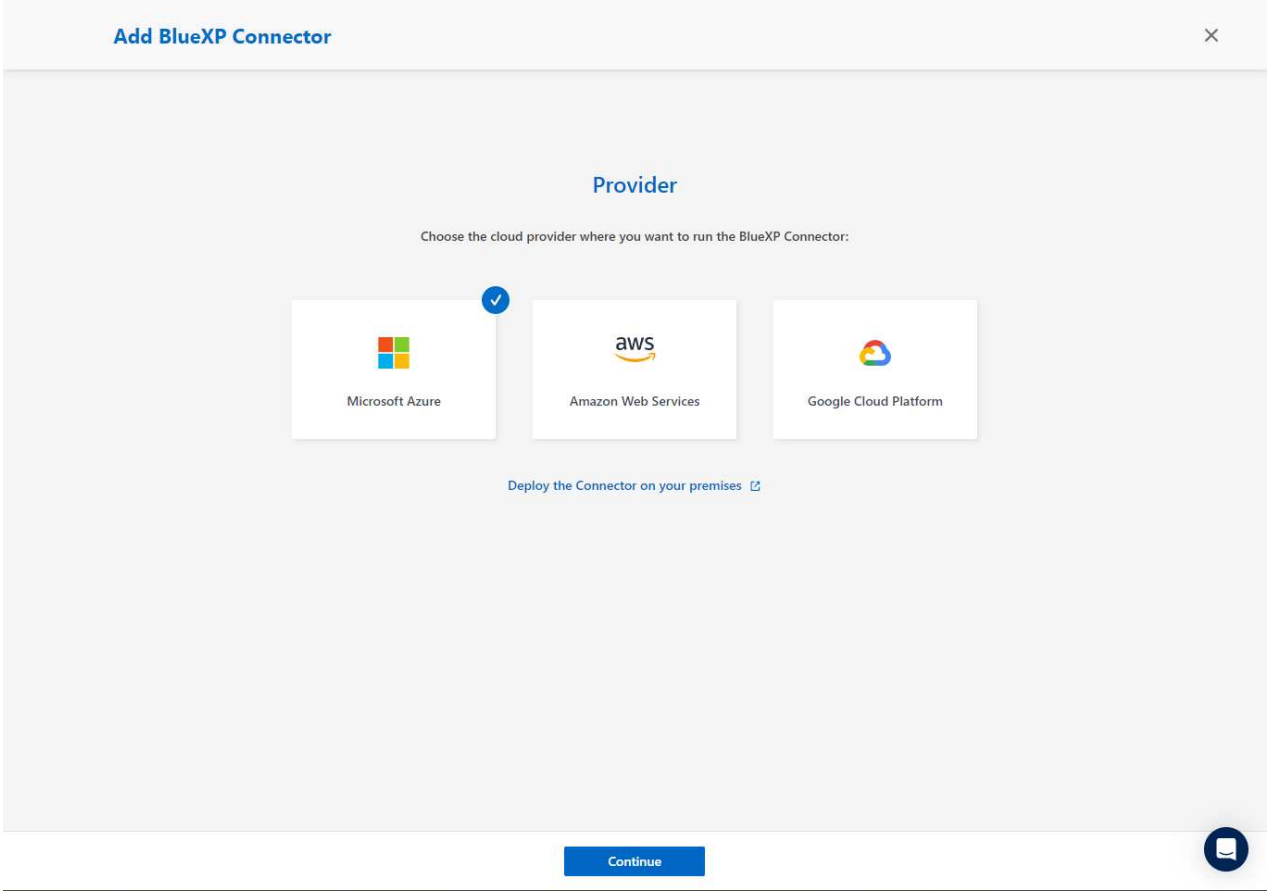
1. Accedi alla console BlueXP.



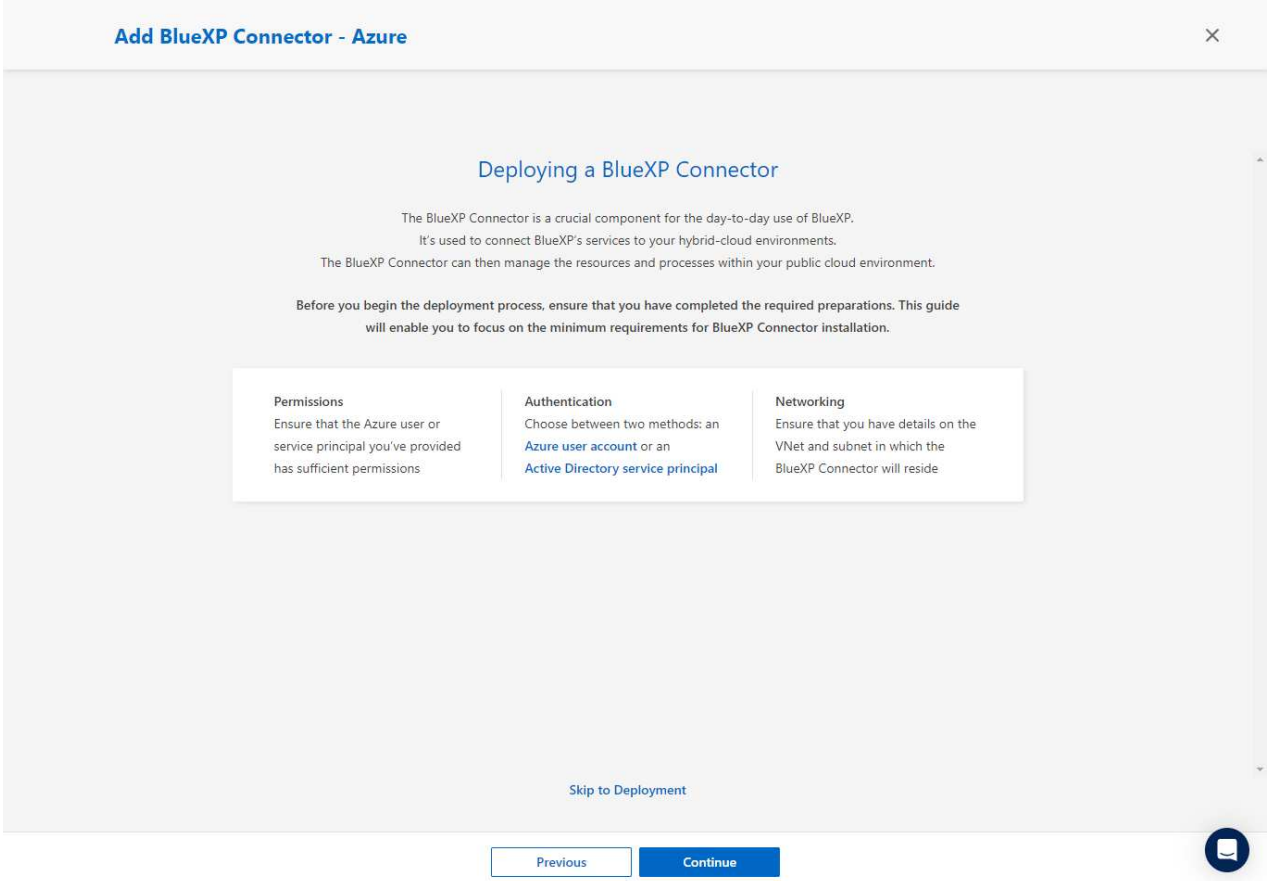
2. Fare clic sulla freccia a discesa **connettore** e **Aggiungi connettore** per avviare il flusso di lavoro di provisioning del connettore.



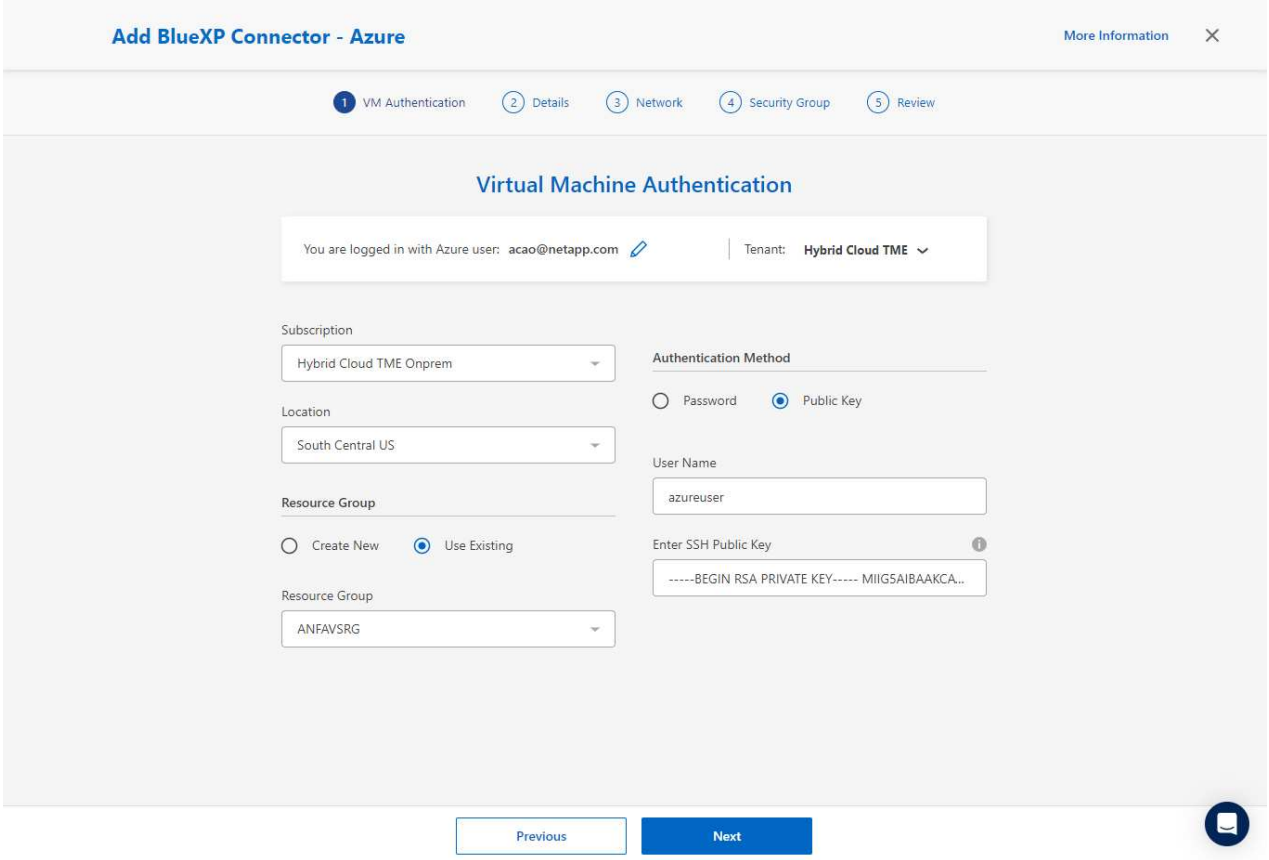
3. Scegli il tuo cloud provider (in questo caso, **Microsoft Azure**).



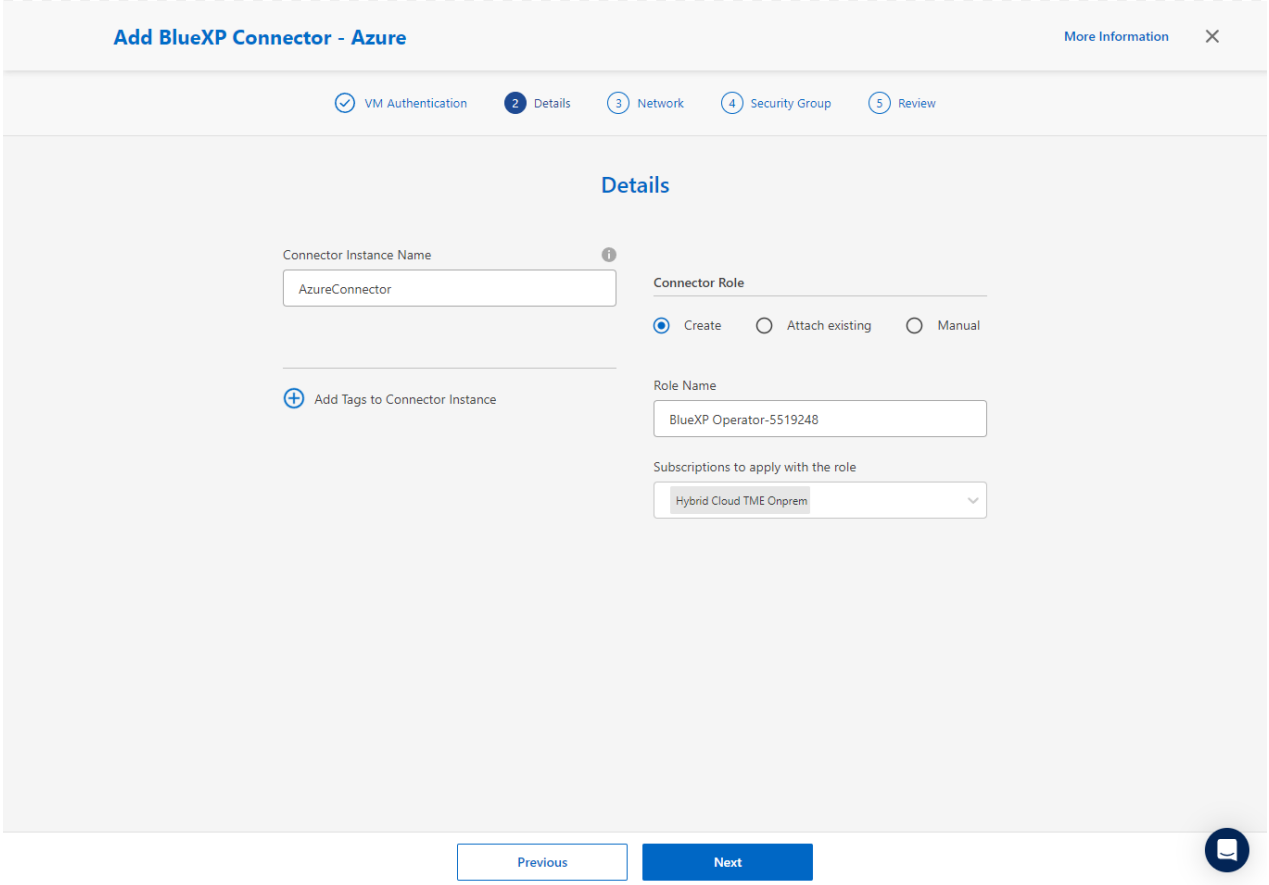
4. Saltare i passaggi **Permission**, **Authentication** e **Networking** se sono già stati configurati nell'account Azure. In caso contrario, è necessario configurarli prima di procedere. Da qui, è anche possibile recuperare le autorizzazioni per la policy di Azure a cui si fa riferimento nella sezione precedente "Preparazione al BlueXP."



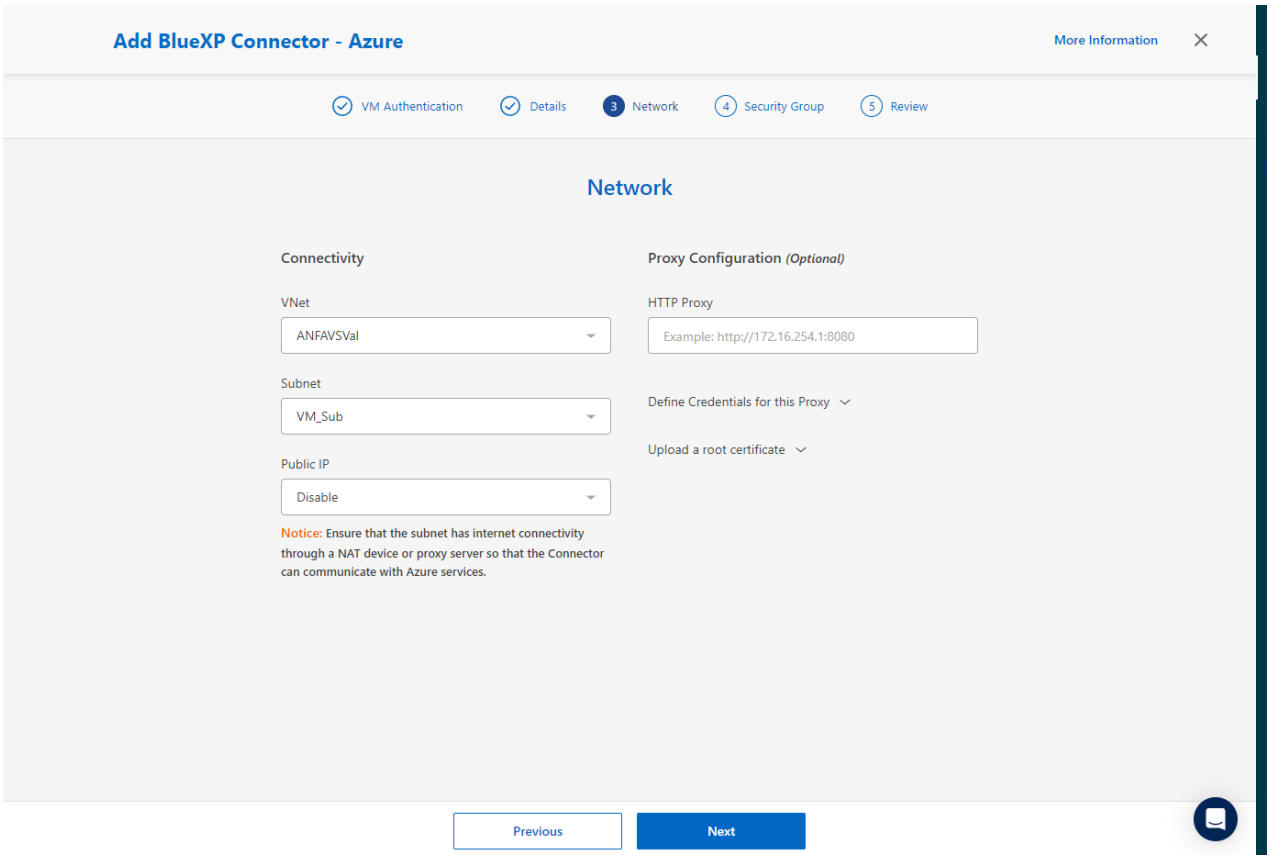
5. Fare clic su **Salta a distribuzione** per configurare il connettore **autenticazione macchina virtuale**. Aggiungi la coppia di chiavi SSH che hai creato nel gruppo di risorse Azure durante l'onboarding alla preparazione BlueXP per l'autenticazione del sistema operativo del connettore.



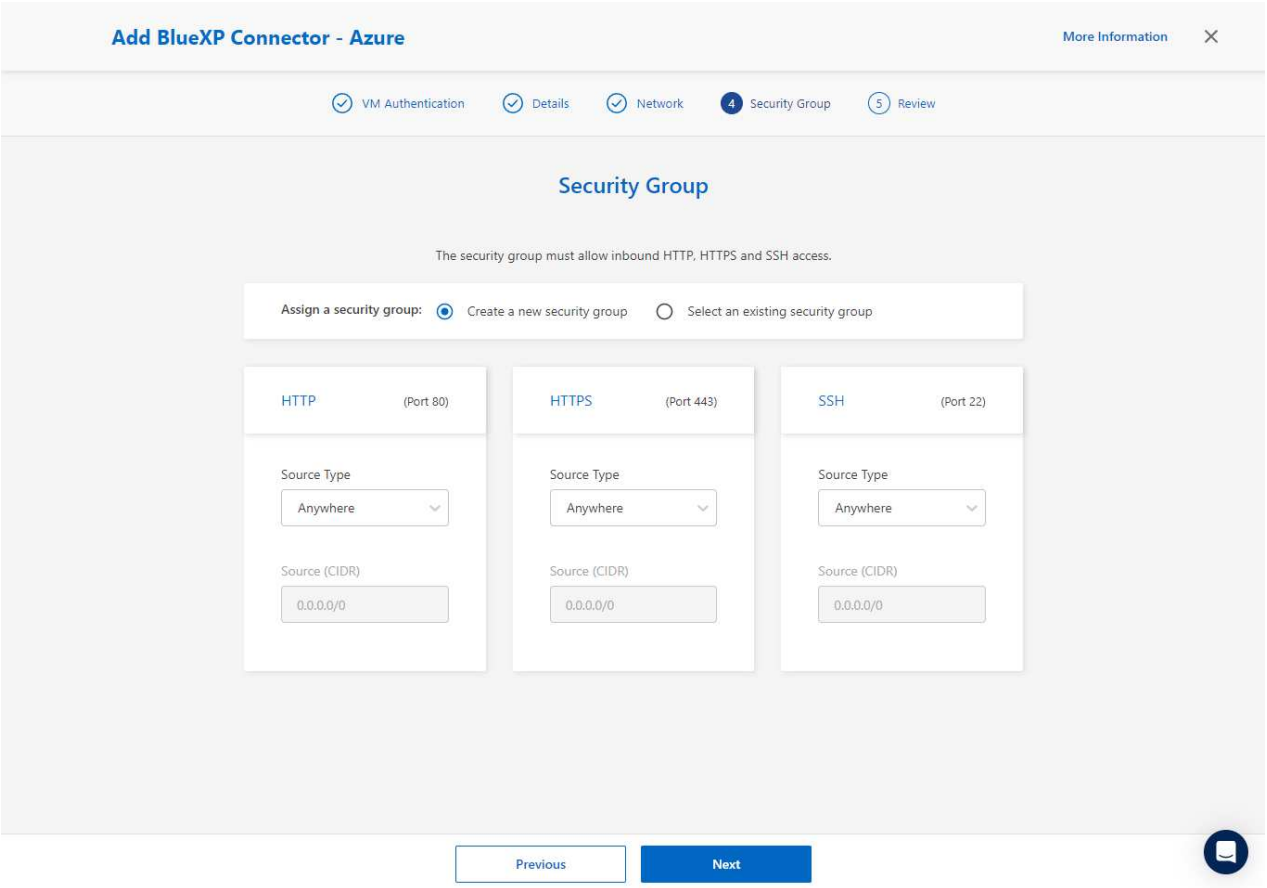
6. Fornire un nome per l'istanza del connettore, selezionare **Crea** e accettare il **Nome ruolo** predefinito in **Dettagli**, quindi scegliere l'abbonamento per l'account Azure.



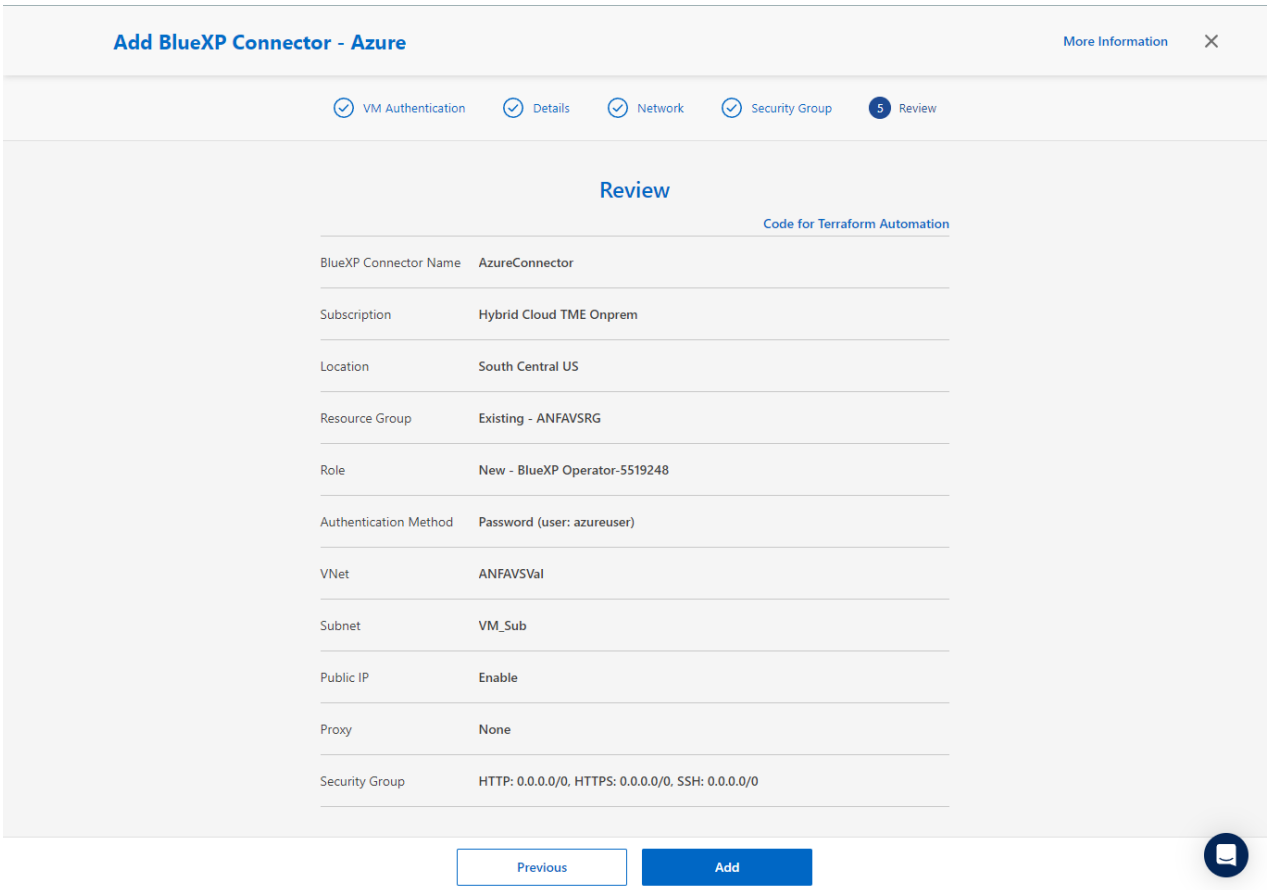
7. Configurare la rete con **VNET**, **Subnet** e disattivare **Public IP**, ma assicurarsi che il connettore disponga dell'accesso a Internet nell'ambiente Azure.



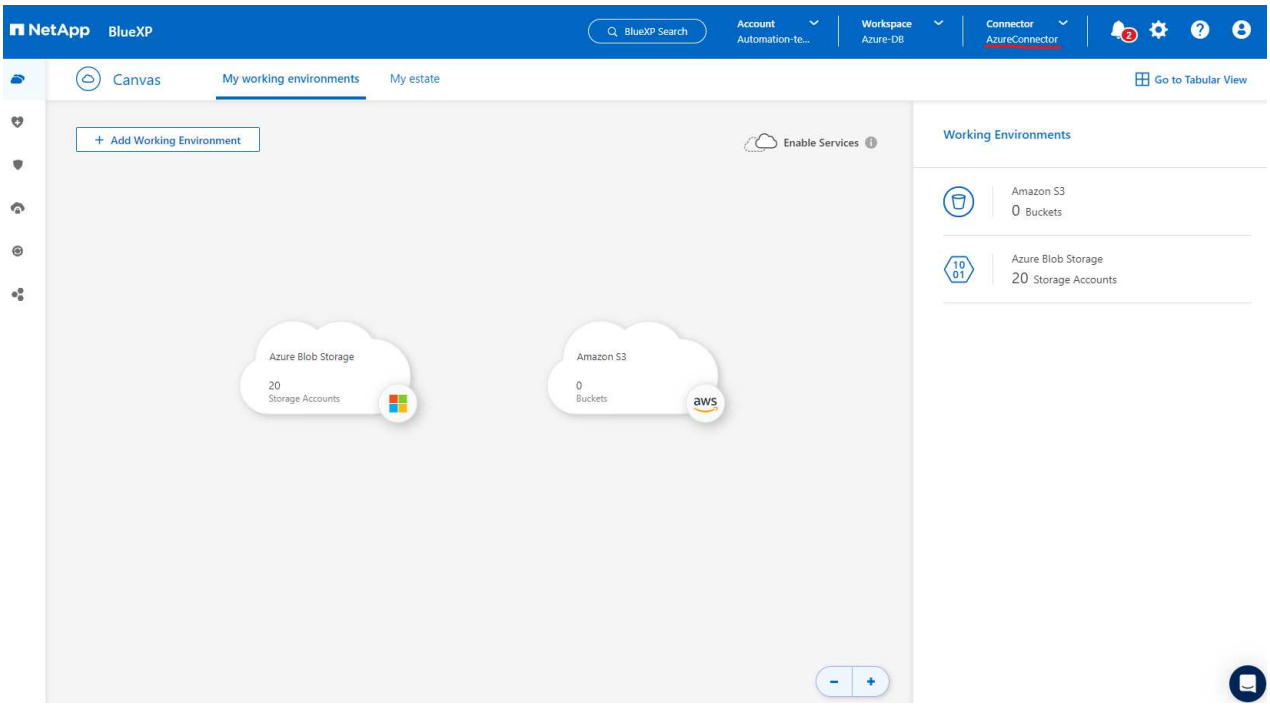
8. Configurare il **Gruppo di sicurezza** per il connettore che consente l'accesso HTTP, HTTPS e SSH.



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.

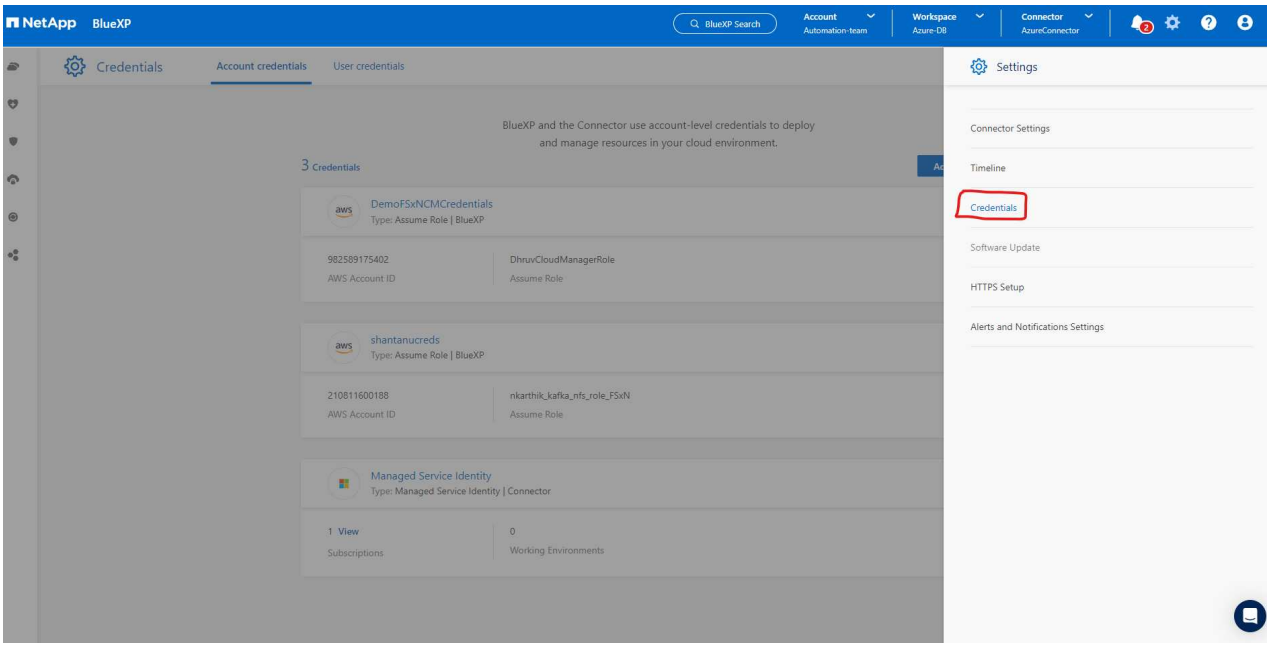


10. Dopo l'attivazione del connettore, il connettore appena creato viene visualizzato nell'elenco a discesa **connettore**.

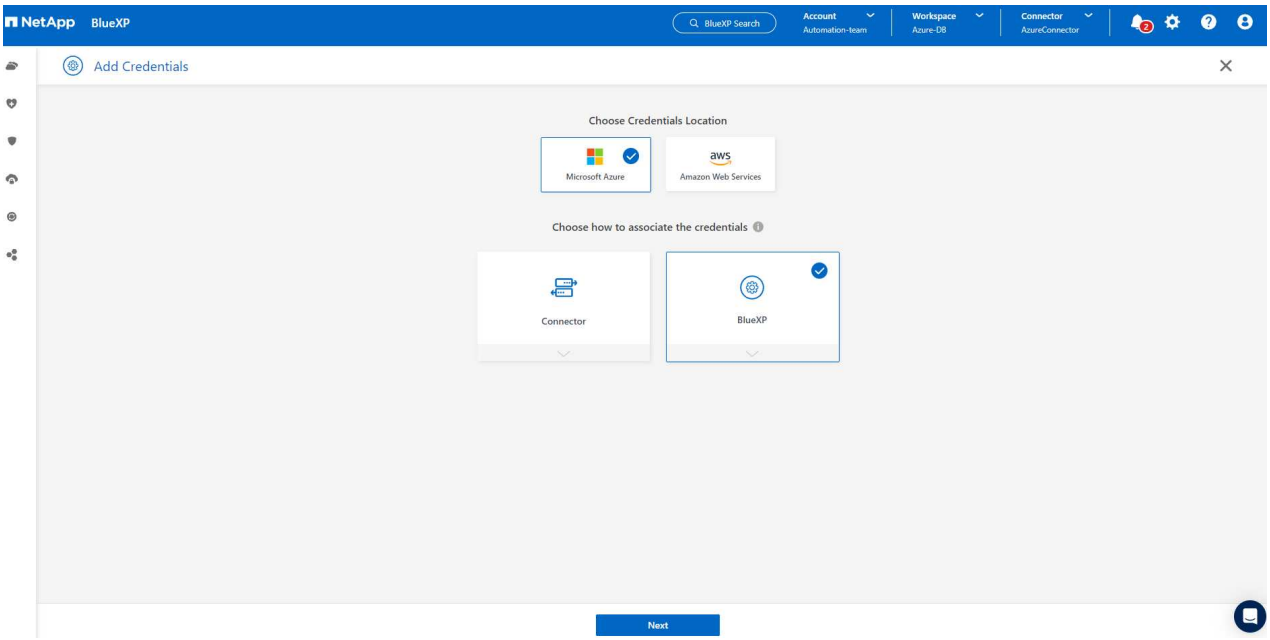


Definisci una credenziale in BlueXP per l’accesso alle risorse di Azure

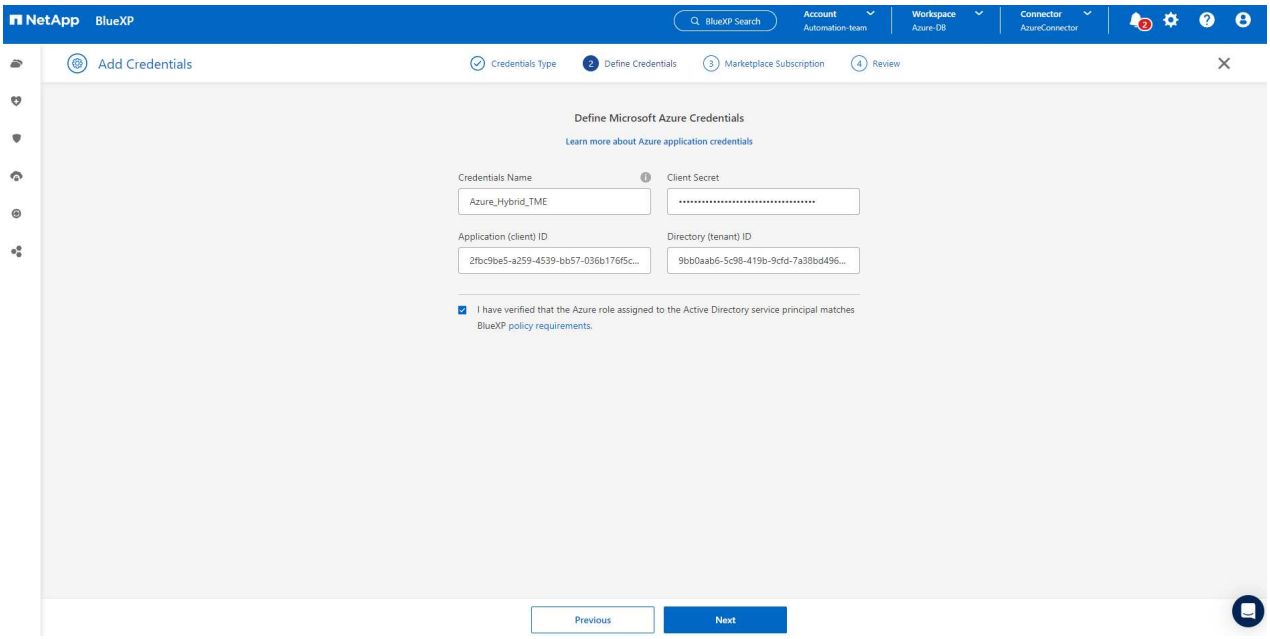
1. Fare clic sull'icona delle impostazioni nell'angolo superiore destro della console BlueXP per aprire la pagina **credenziali account**, fare clic su **Aggiungi credenziali** per avviare il flusso di lavoro di configurazione delle credenziali.



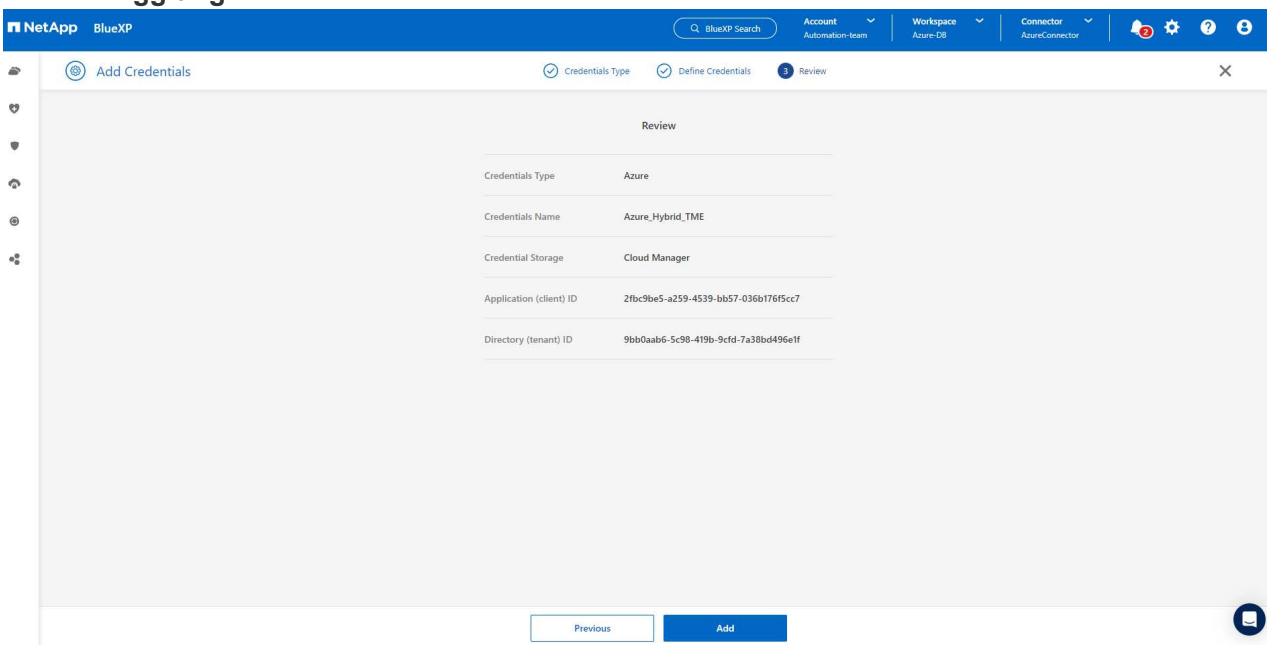
2. Scegliere la posizione delle credenziali come - **Microsoft Azure - BlueXP**.



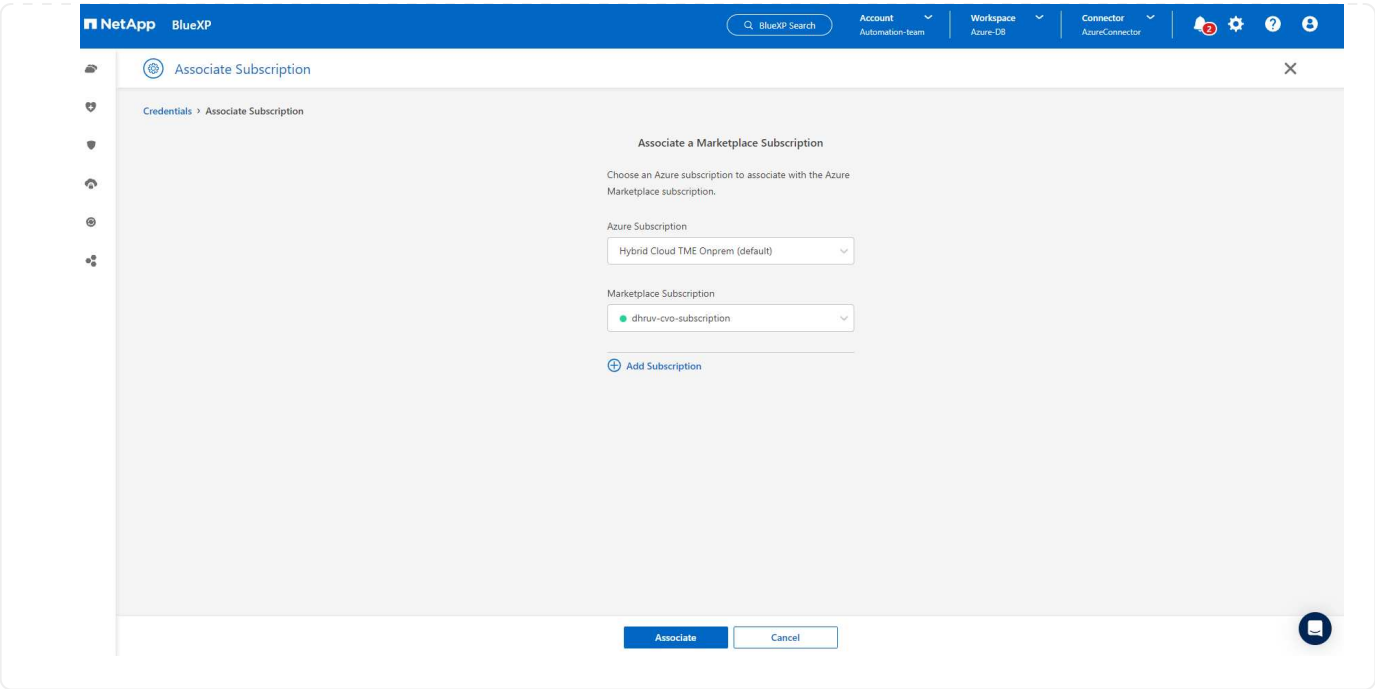
3. Definisci le credenziali di Azure con **Client Secret**, **Client ID** e **Tenant ID** appropriati, che dovrebbero essere state raccolte durante il precedente processo di onboarding di BlueXP.



4. Rivedi e **Aggiungi**.



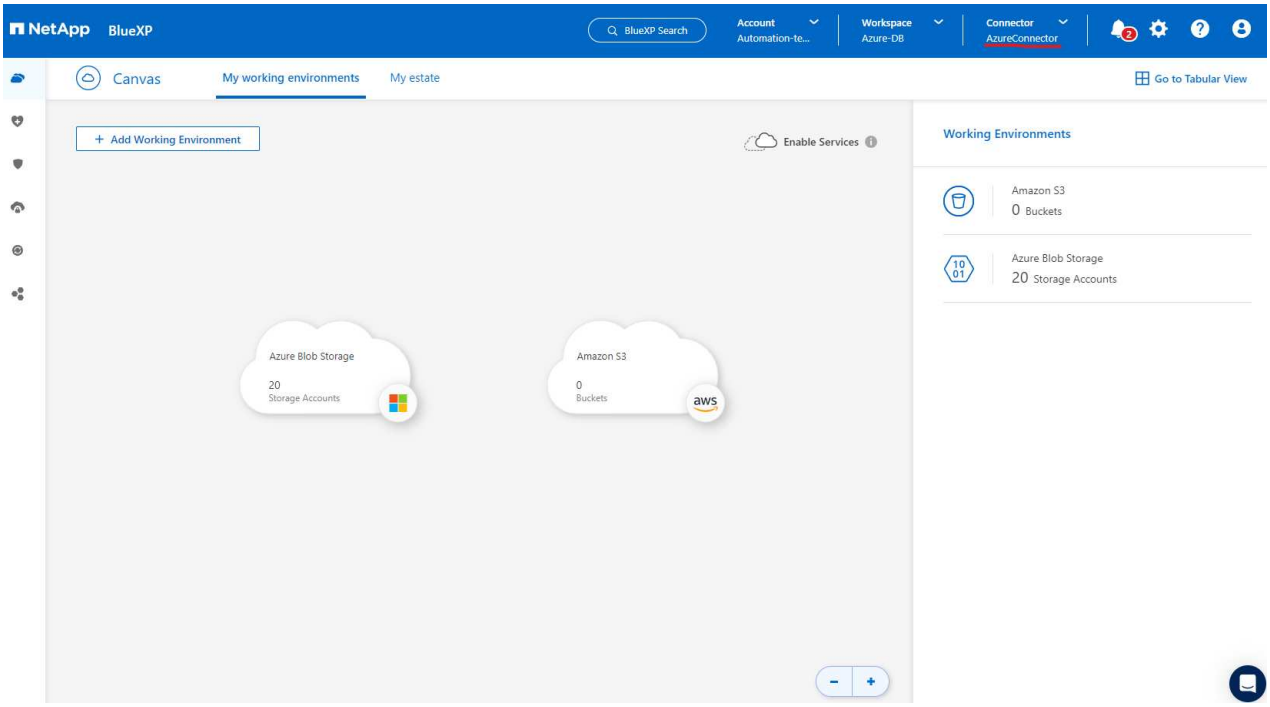
5. Potrebbe inoltre essere necessario associare un abbonamento **Marketplace** alla credenziale.



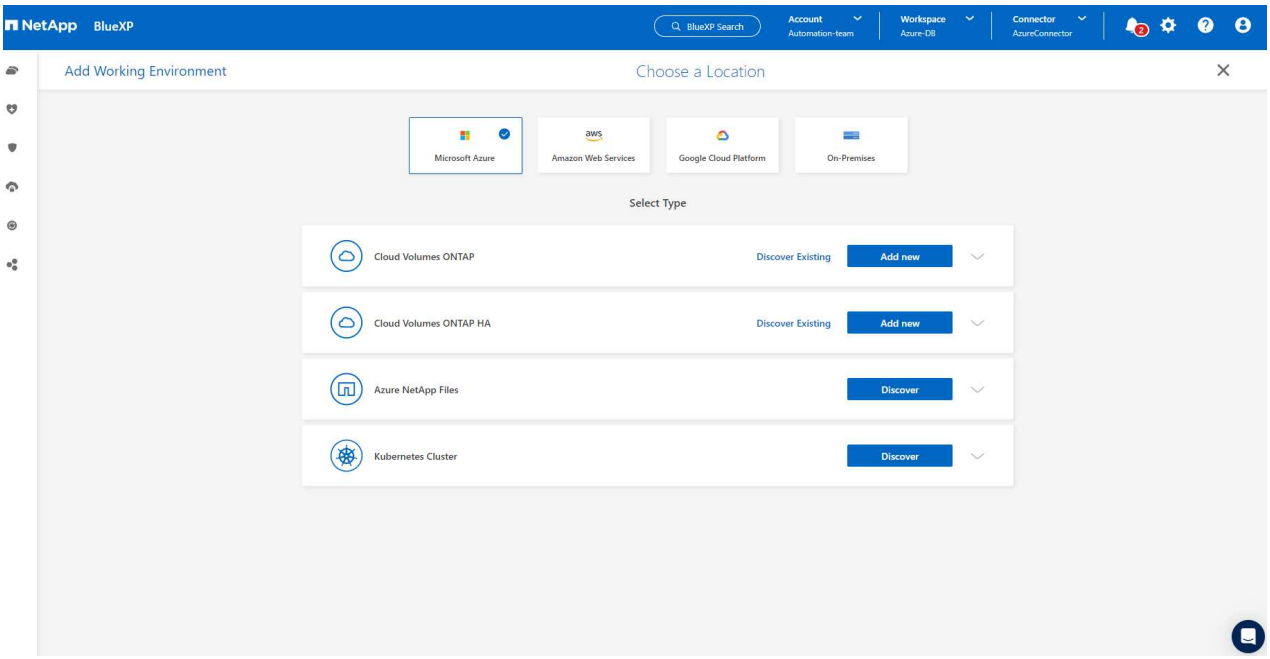
Configurazione dei servizi SnapCenter

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

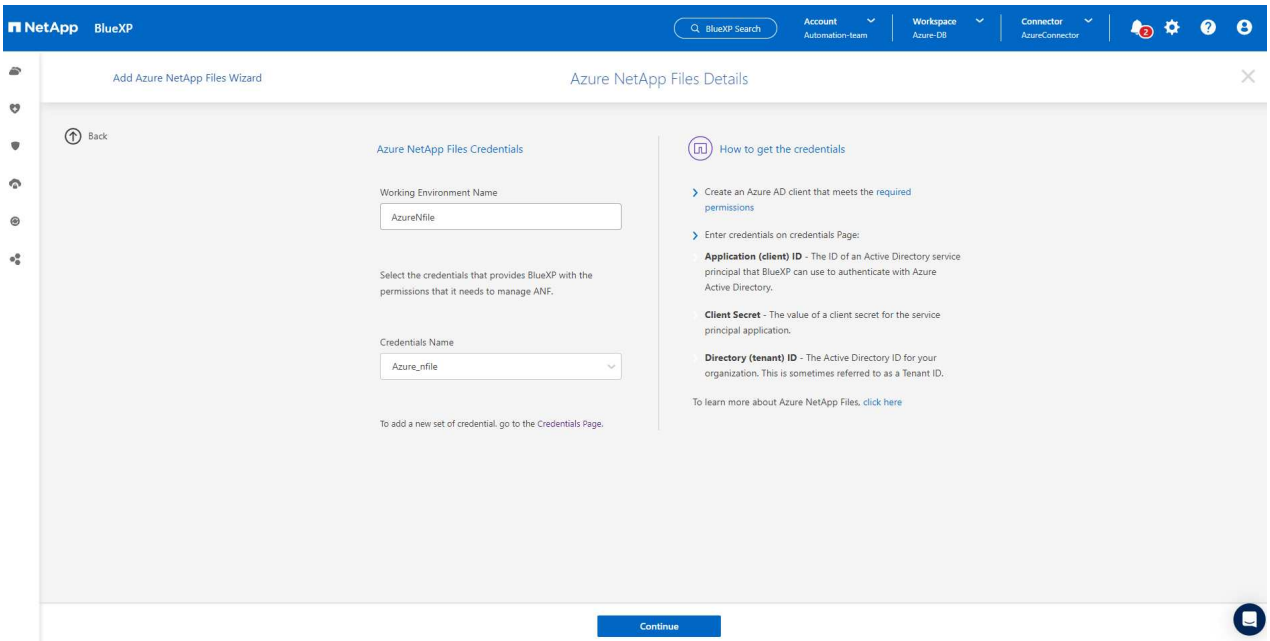
1. Torna alla pagina Canvas, da **ambiente di lavoro** fare clic su **Aggiungi ambiente di lavoro** per scoprire Azure NetApp Files distribuito in Azure.



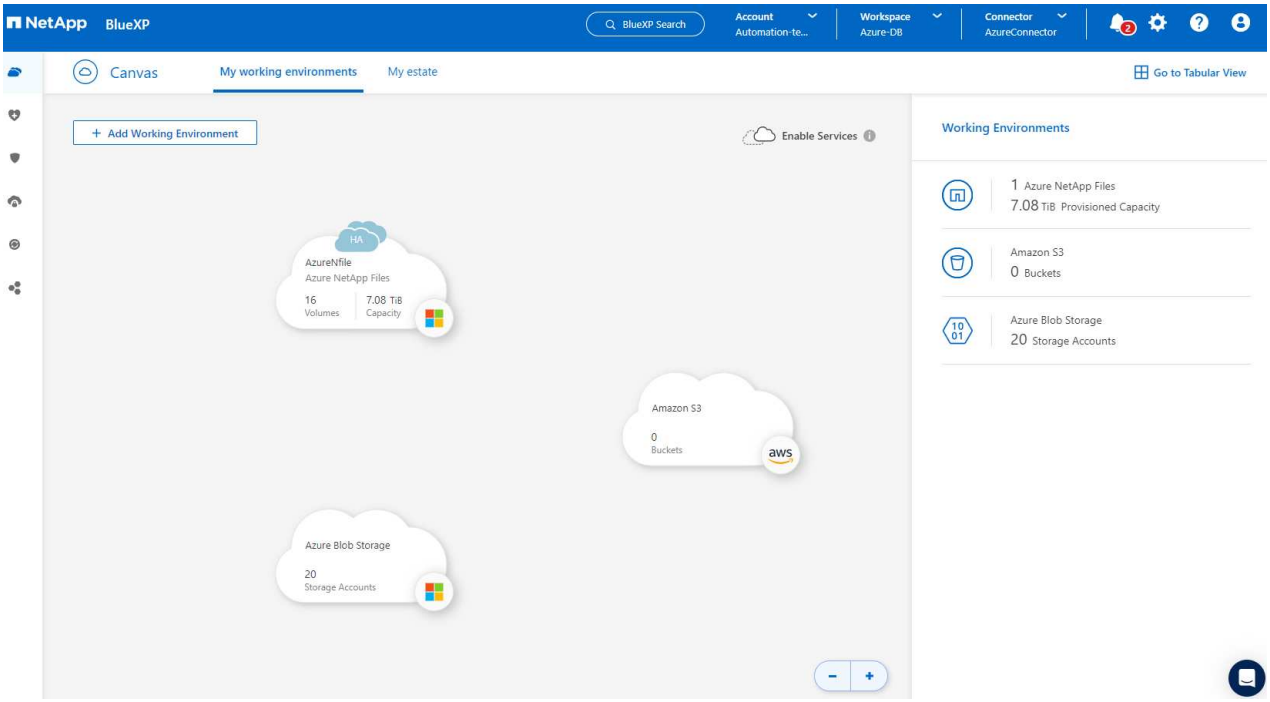
2. Scegliere **Microsoft Azure** come percorso e fare clic su **Scopri**.



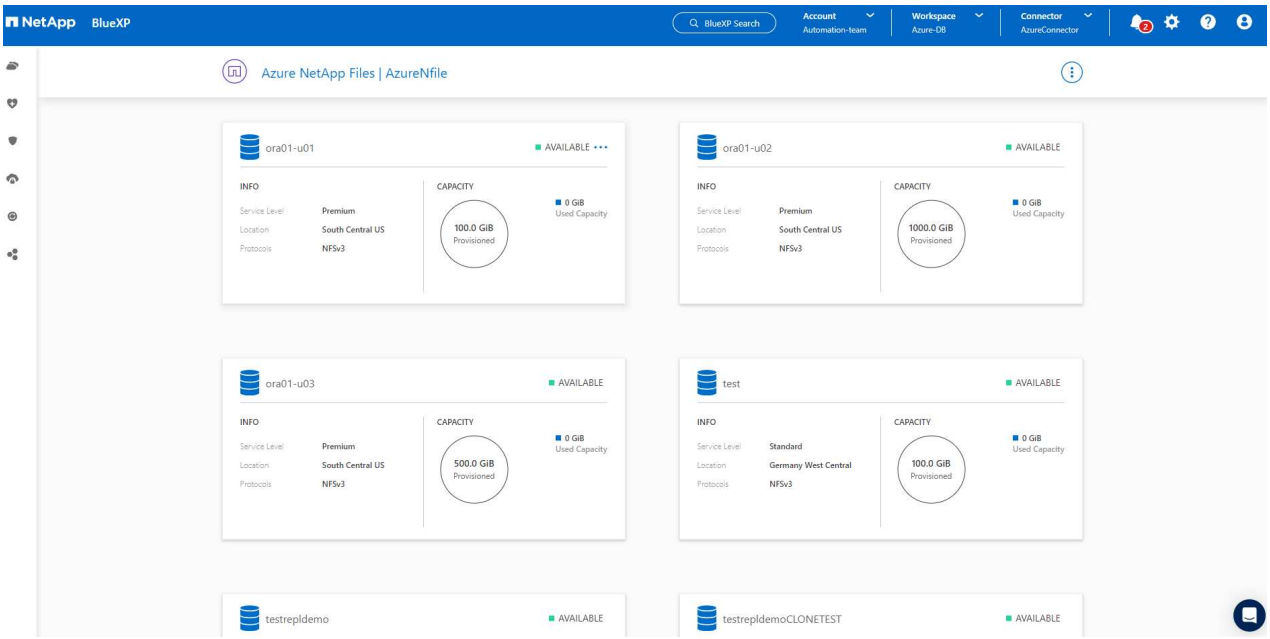
3. Nome **ambiente di lavoro** e scegliere **Nome credenziale** creato nella sezione precedente, quindi fare clic su **continua**.



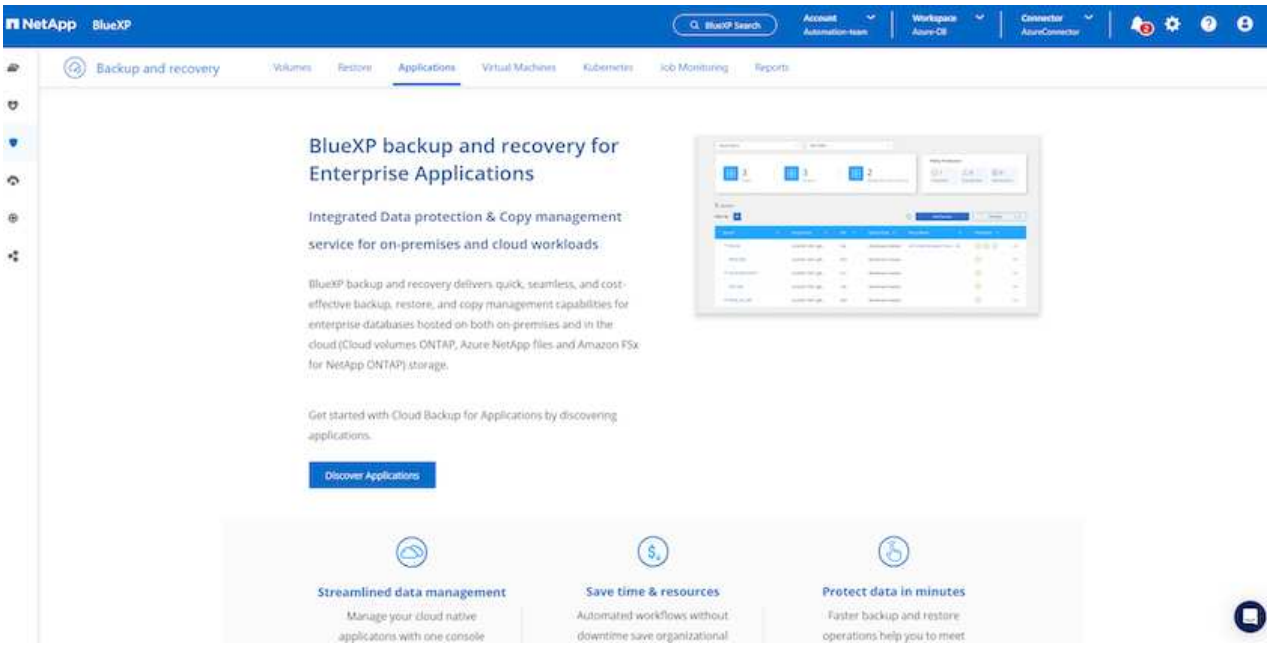
4. La console BlueXP torna a **i miei ambienti di lavoro** e Azure NetApp Files rilevato da Azure ora appare su **Canvas**.



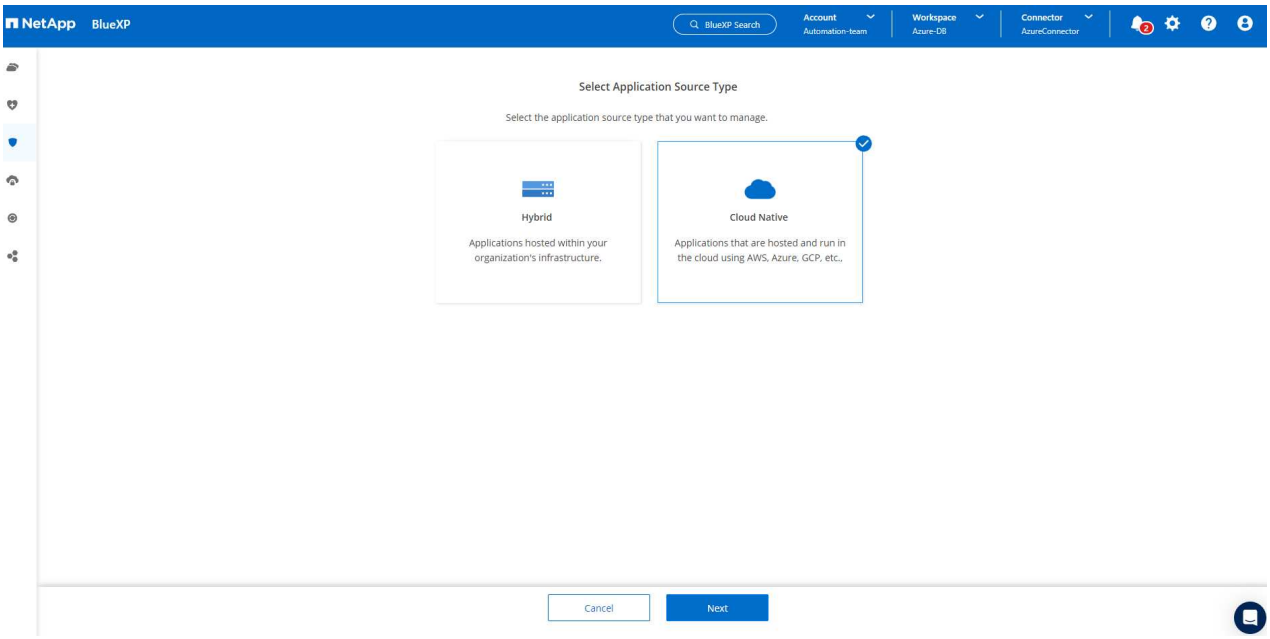
5. Fare clic sull'icona **Azure NetApp Files**, quindi **Inserisci ambiente di lavoro** per visualizzare i volumi di database Oracle distribuiti nello storage Azure NetApp Files.



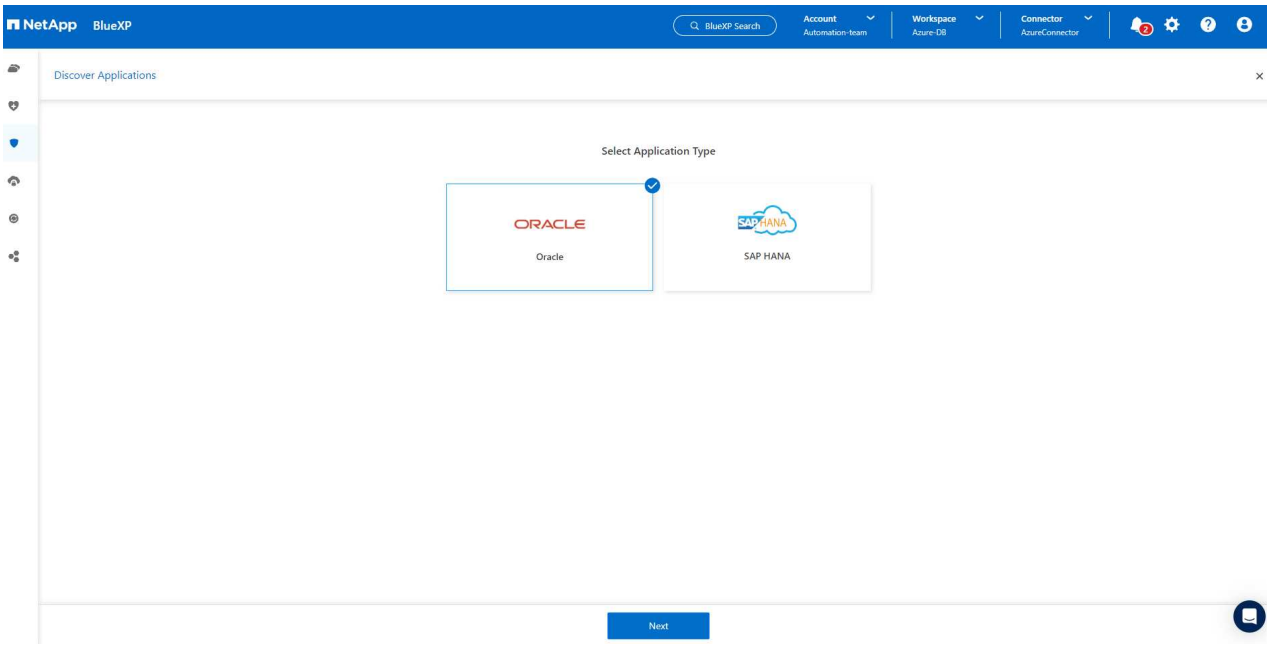
6. Dalla barra laterale sinistra della console, passare il mouse sull'icona di protezione, quindi fare clic su **protezione** > **applicazioni** per aprire la pagina di avvio delle applicazioni. Fare clic su **Scopri applicazioni**.



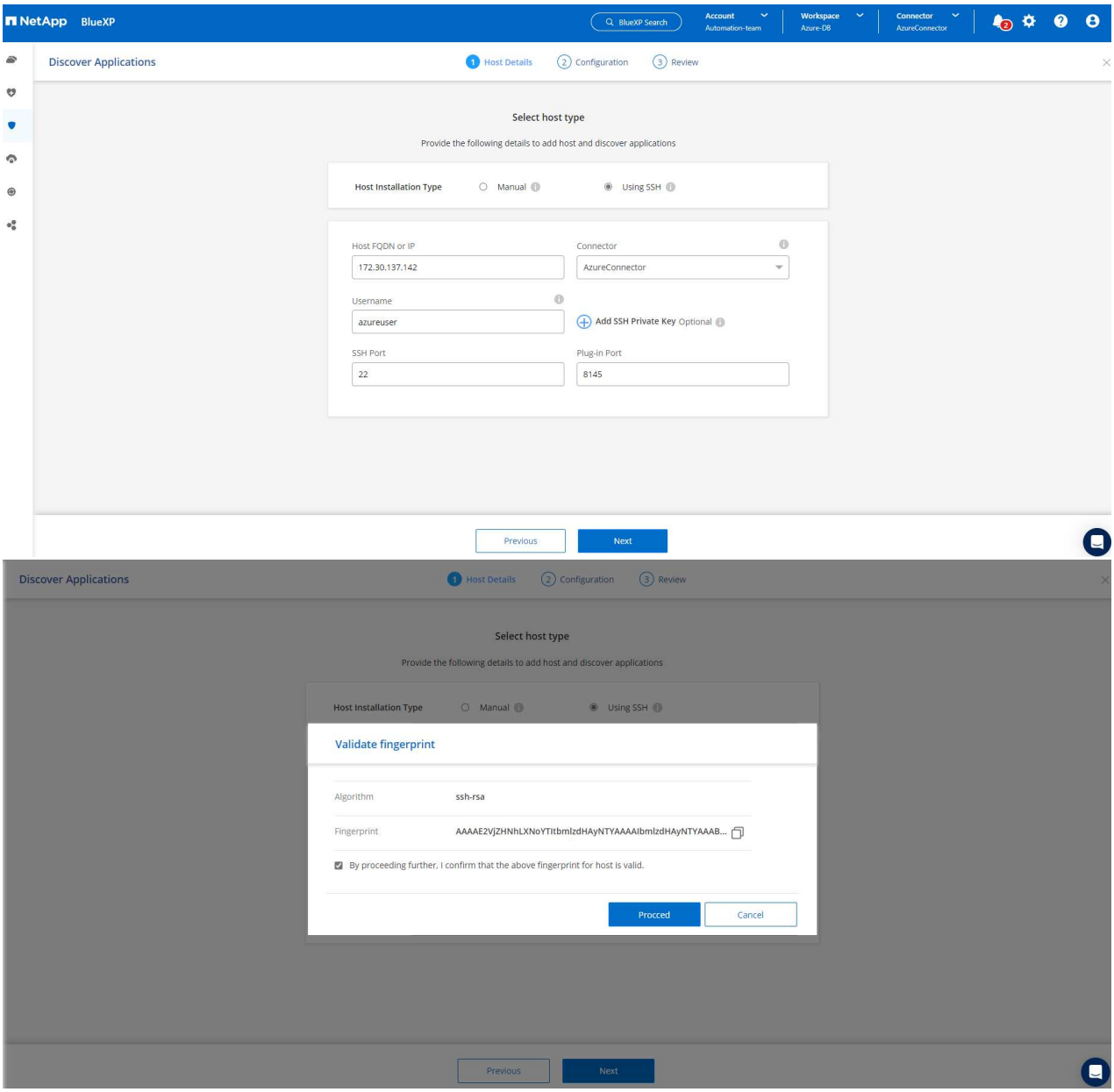
7. Selezionare **Cloud Native** come tipo di origine dell'applicazione.



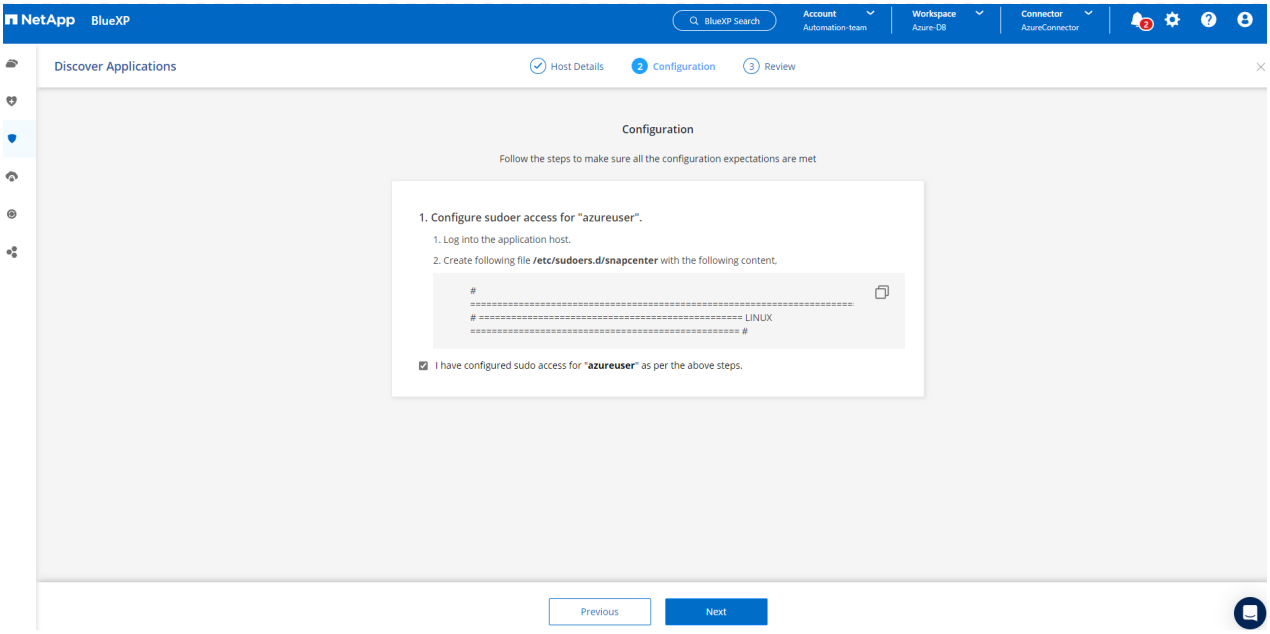
8. Scegliere **Oracle** per il tipo di applicazione, fare clic su **Avanti** per aprire la pagina dei dettagli dell'host.



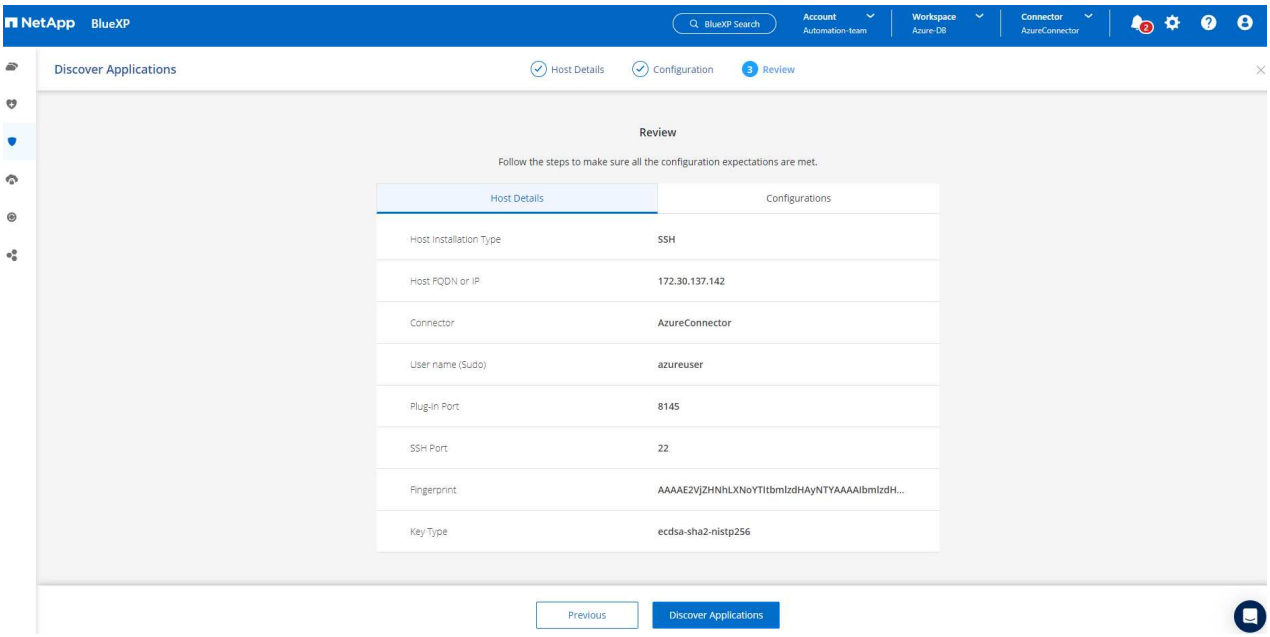
9. Selezionare **usando SSH** e fornire i dettagli di Oracle Azure VM come **indirizzo IP**, **connettore**, gestione di Azure VM **Nome utente** come azureuser. Fare clic su **Aggiungi chiave privata SSH** per incollare la coppia di chiavi SSH utilizzata per implementare la VM Oracle Azure. Verrà inoltre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



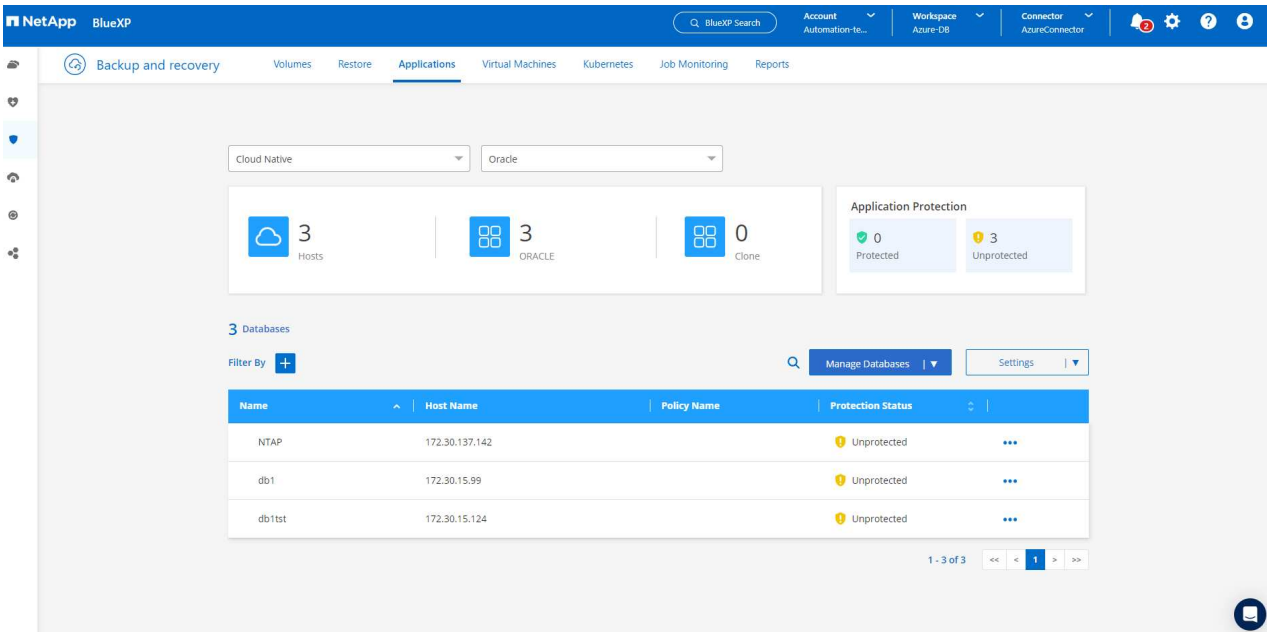
10. Passare alla pagina successiva **Configurazione** per impostare l'accesso sudocer su Oracle Azure VM.



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**.



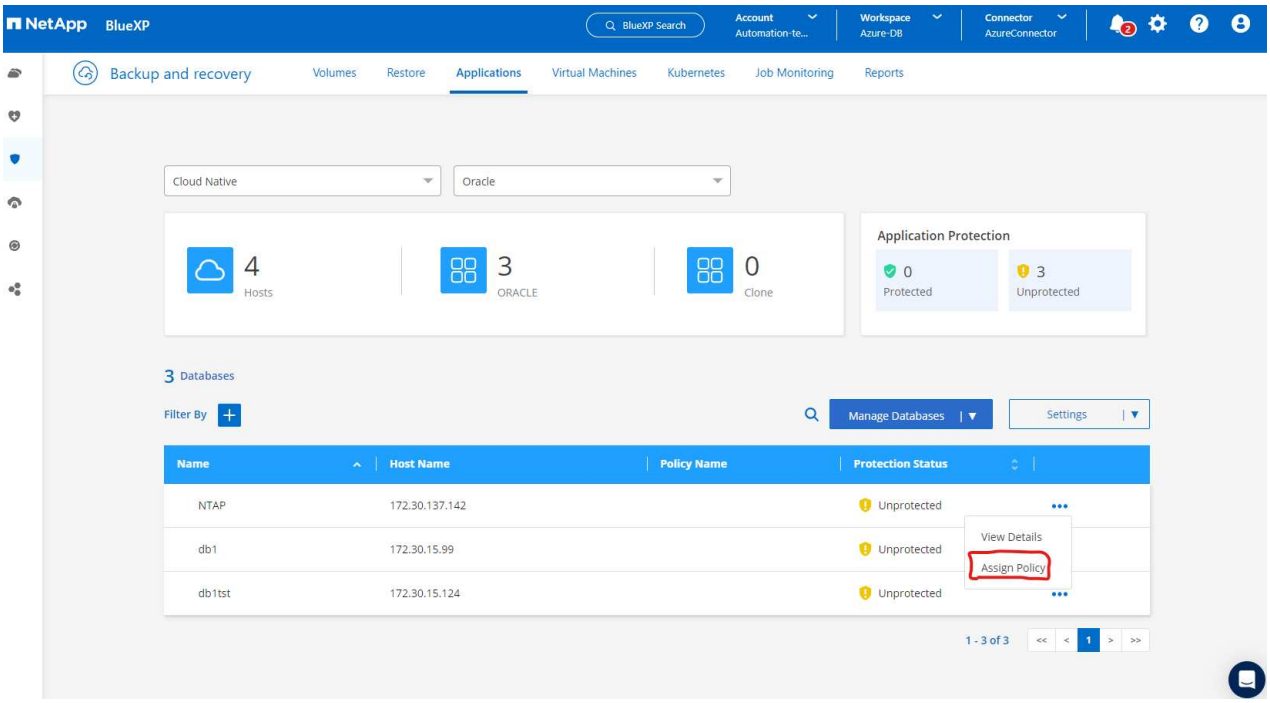
Questa operazione completa la configurazione iniziale dei servizi SnapCenter per Oracle. Nelle tre sezioni successive di questo documento vengono descritte le operazioni di backup, ripristino e clonazione del database Oracle.

Backup del database Oracle

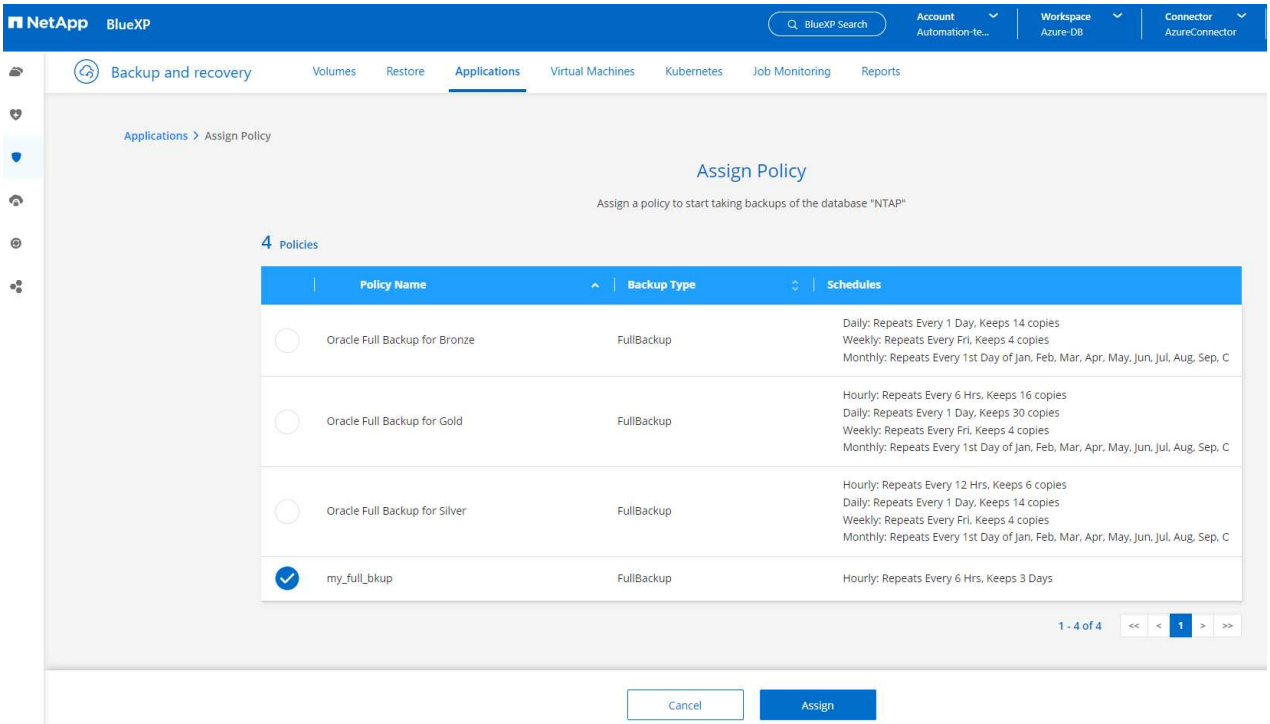
1. Il nostro database Oracle di test in Azure VM è configurato con tre volumi con uno storage totale aggregato di circa 1,6 TiB. Questo fornisce un contesto in cui vengono descritte le tempistiche per il backup, il ripristino e il clone di un database di queste dimensioni.

```
[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 ~]$
```

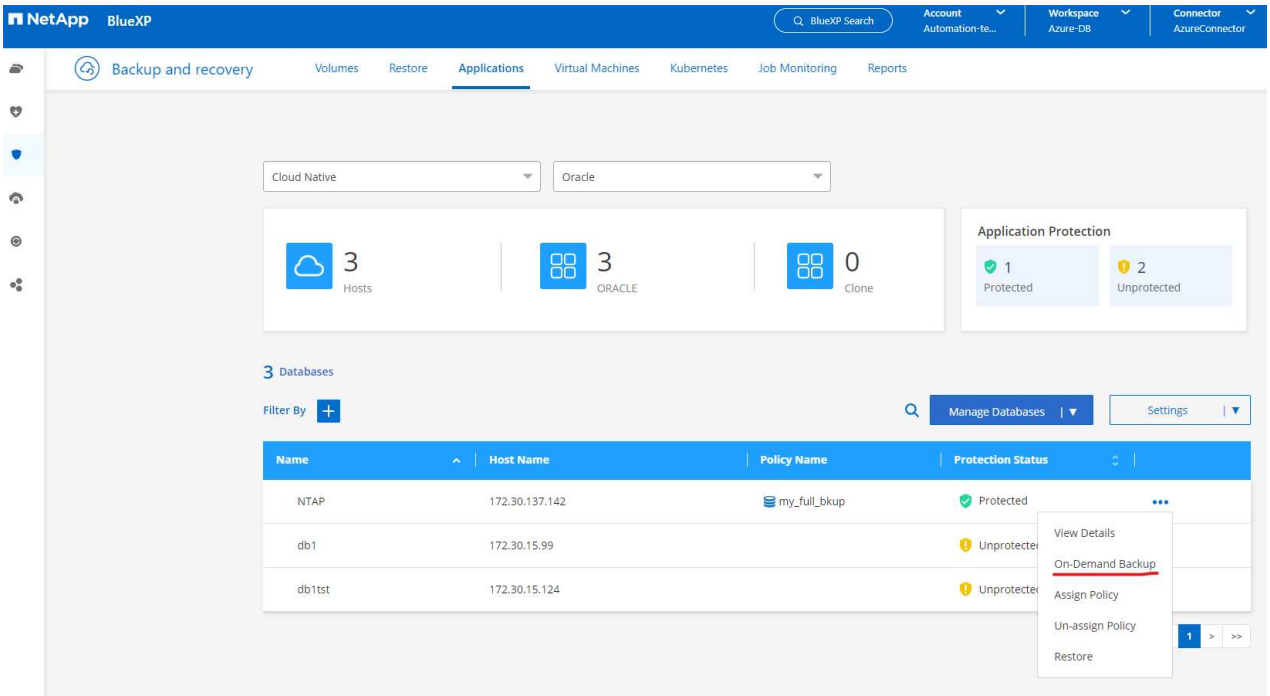
1. Per proteggere il database, fare clic sui tre punti accanto al database **Stato protezione**, quindi fare clic su **Assegna criterio** per visualizzare i criteri di protezione predefiniti precaricati o definiti dall'utente che possono essere applicati ai database Oracle. In **Impostazioni** - **Criteri**, è possibile creare criteri personalizzati con una frequenza di backup personalizzata e una finestra di conservazione dei dati di backup.



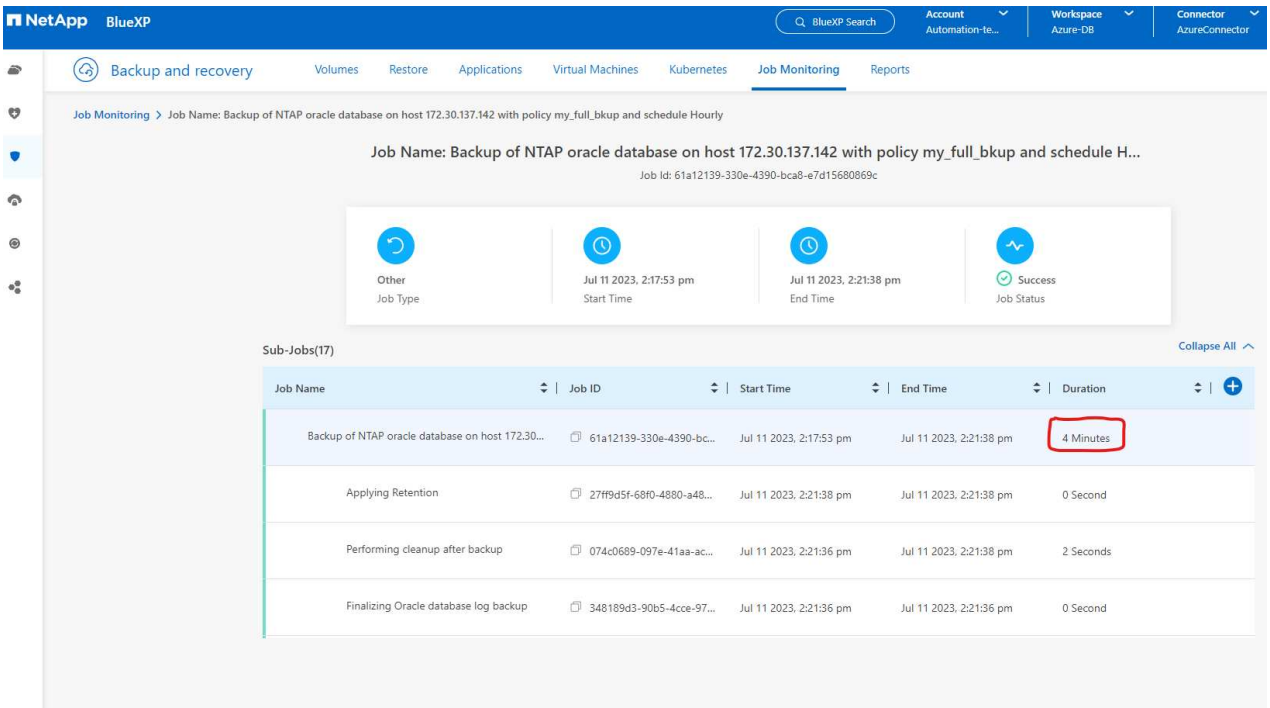
2. Quando si è soddisfatti della configurazione dei criteri, è possibile **assegnare** il criterio scelto per proteggere il database.



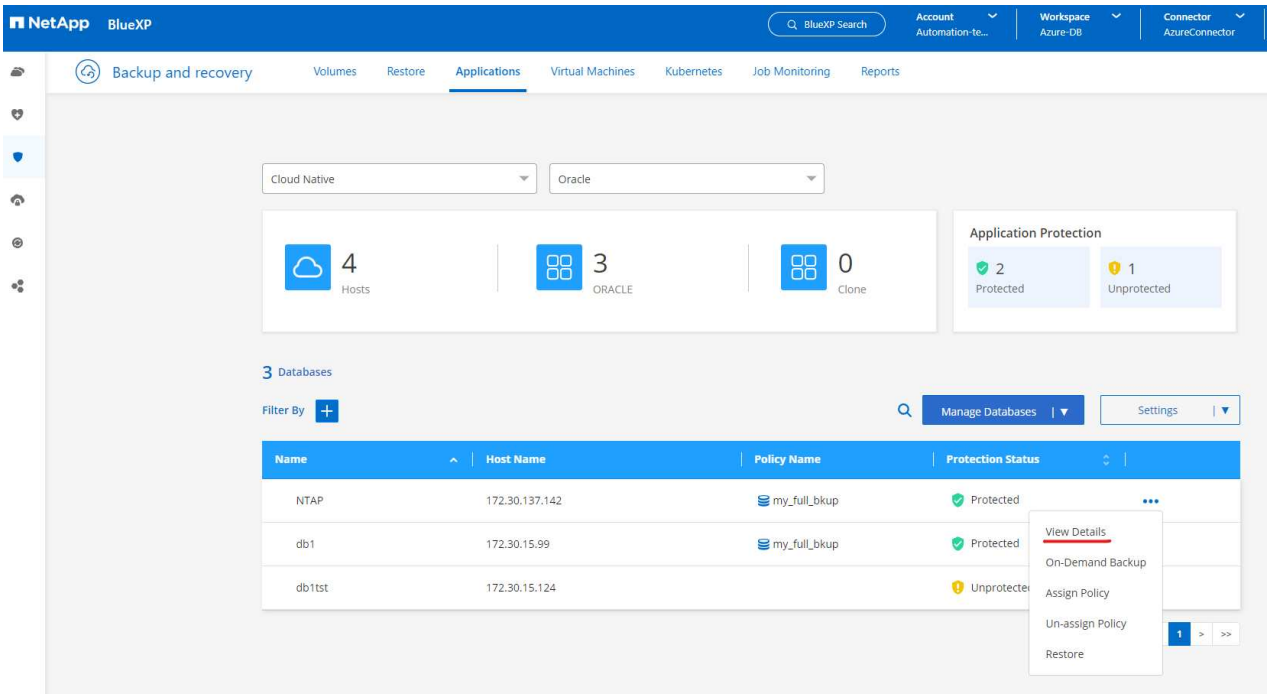
3. Una volta applicato il criterio, lo stato di protezione del database è cambiato in **Protected** con un segno di spunta verde. BlueXP esegue il backup snapshot in base al programma definito. Inoltre, **Backup SU richiesta** è disponibile dal menu a discesa a tre punti, come mostrato di seguito.



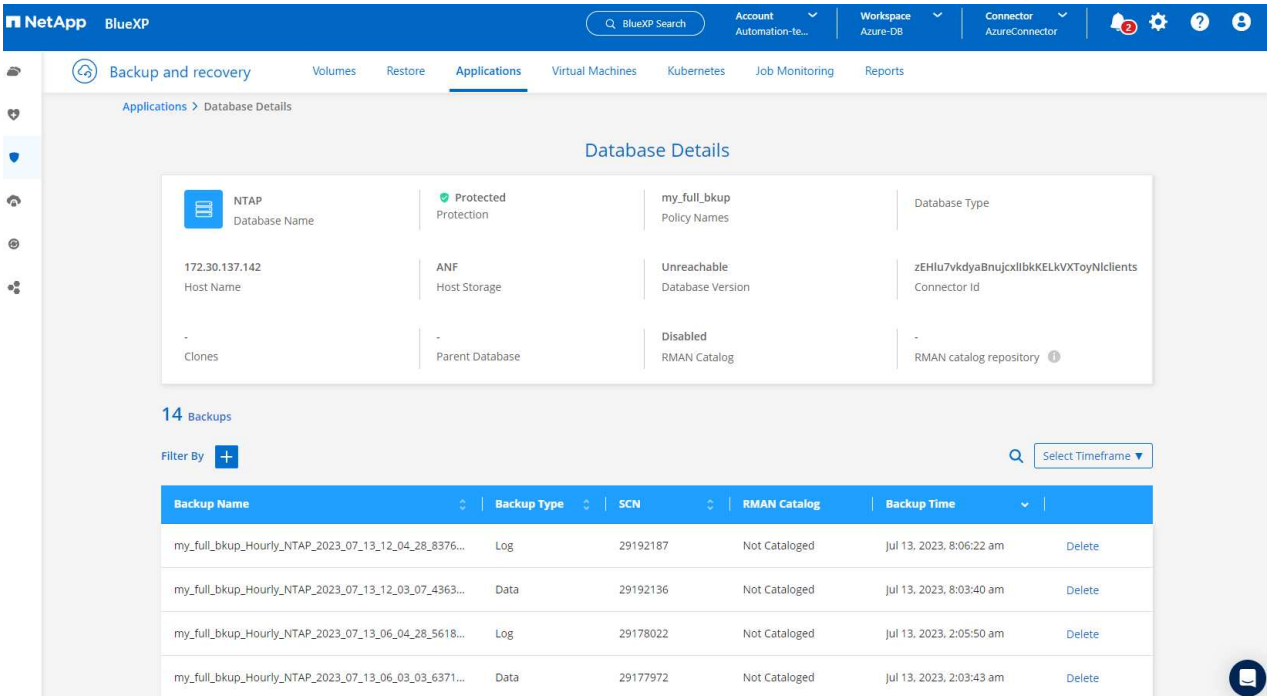
4. Dalla scheda **Job Monitoring** è possibile visualizzare i dettagli del processo di backup. I risultati del test hanno dimostrato che il backup di un database Oracle ha richiesto circa 4 minuti e circa 1,6 TiB.



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

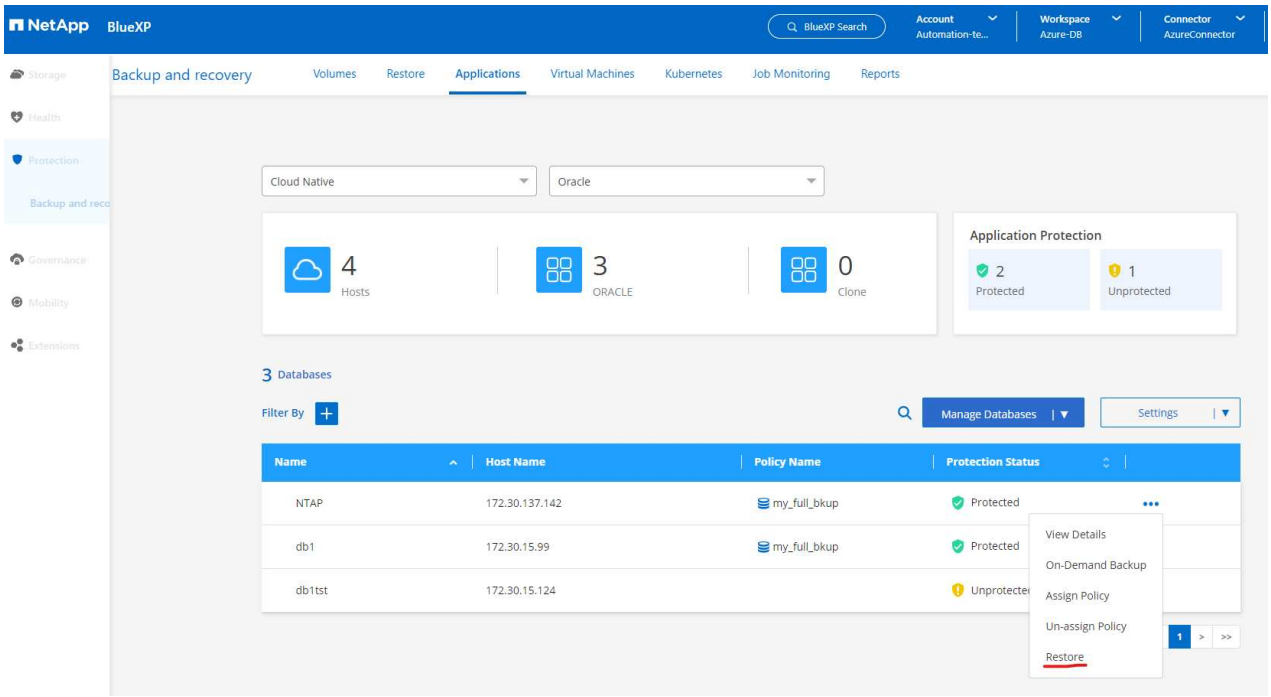


6. I dettagli del backup del database includono **Backup Name**, **Backup Type**, **SCN**, **RMAN Catalog** e **Backup Time**. Un set di backup contiene snapshot coerenti con l'applicazione per il volume di dati e il volume di log, rispettivamente. Uno snapshot del volume di registro viene eseguito subito 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.

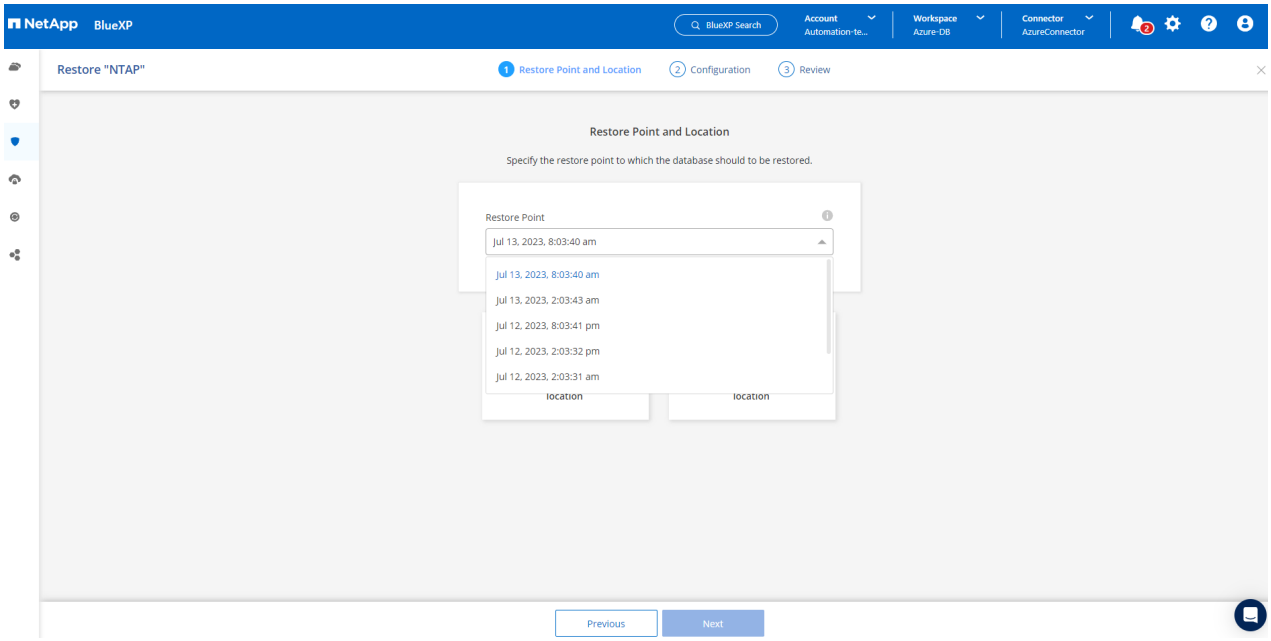


Ripristino e ripristino del database Oracle

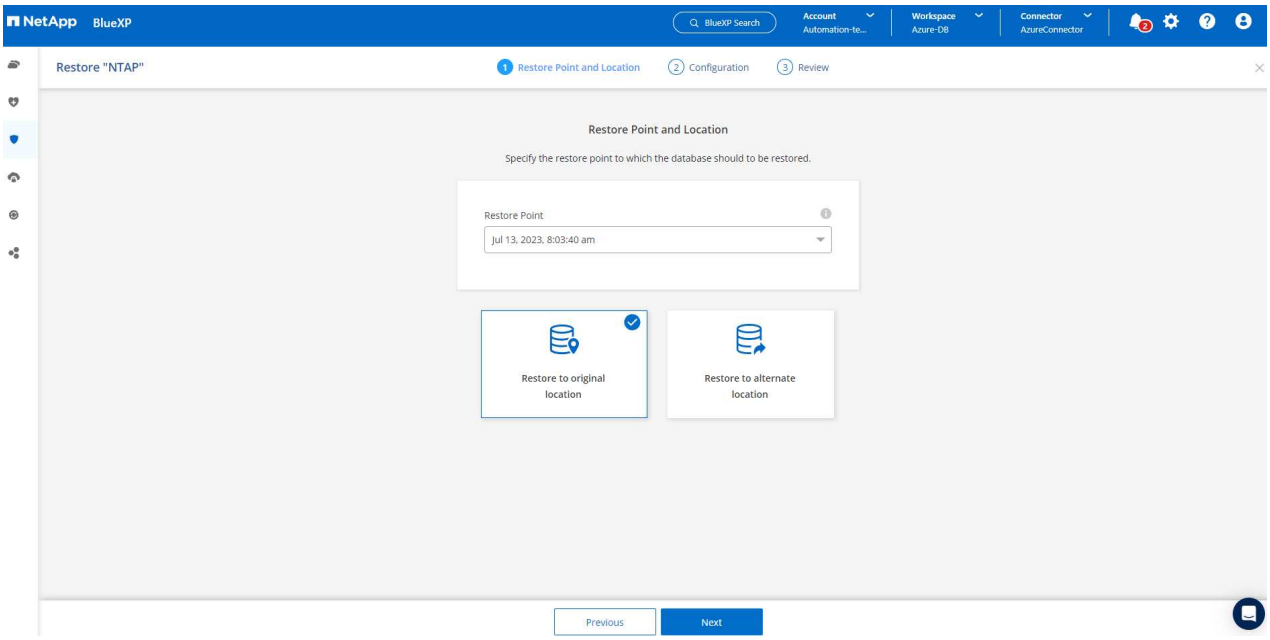
1. Per il ripristino di un database, fare clic sul menu a discesa a tre punti per il database specifico da ripristinare in **applicazioni**, quindi fare clic su **Ripristina** per avviare il flusso di lavoro di ripristino e ripristino del database.



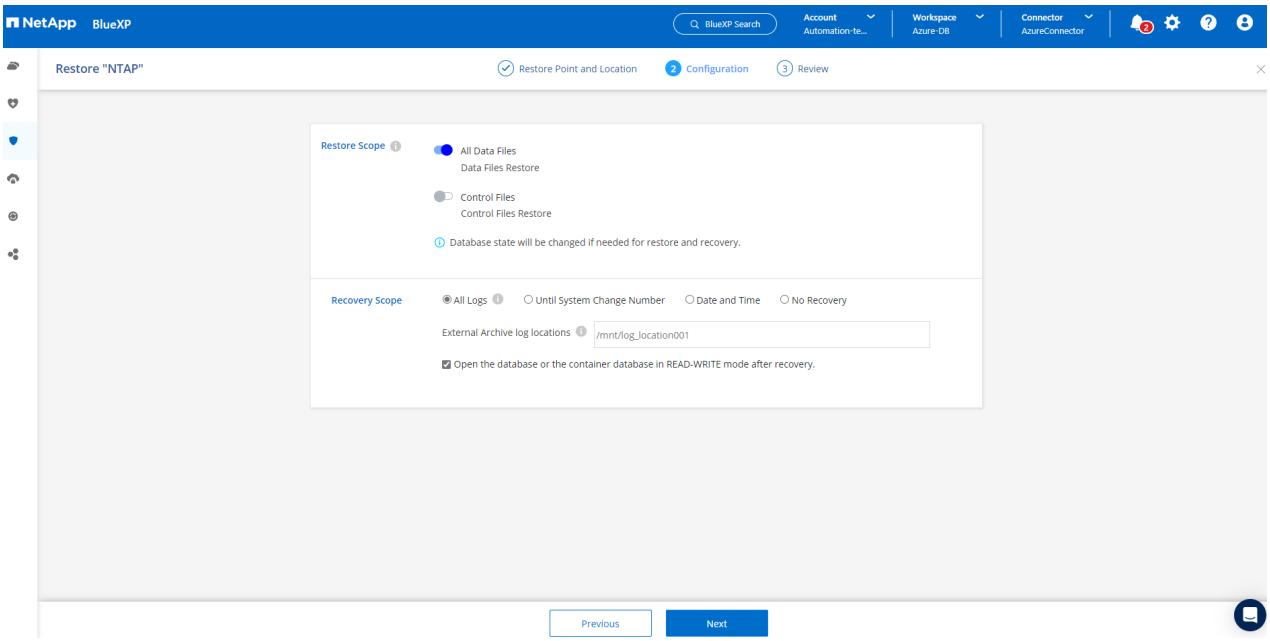
2. Scegliere il **punto di ripristino** in base all'indicazione dell'ora. Ogni indicatore orario nell'elenco rappresenta un set di backup del database disponibile.



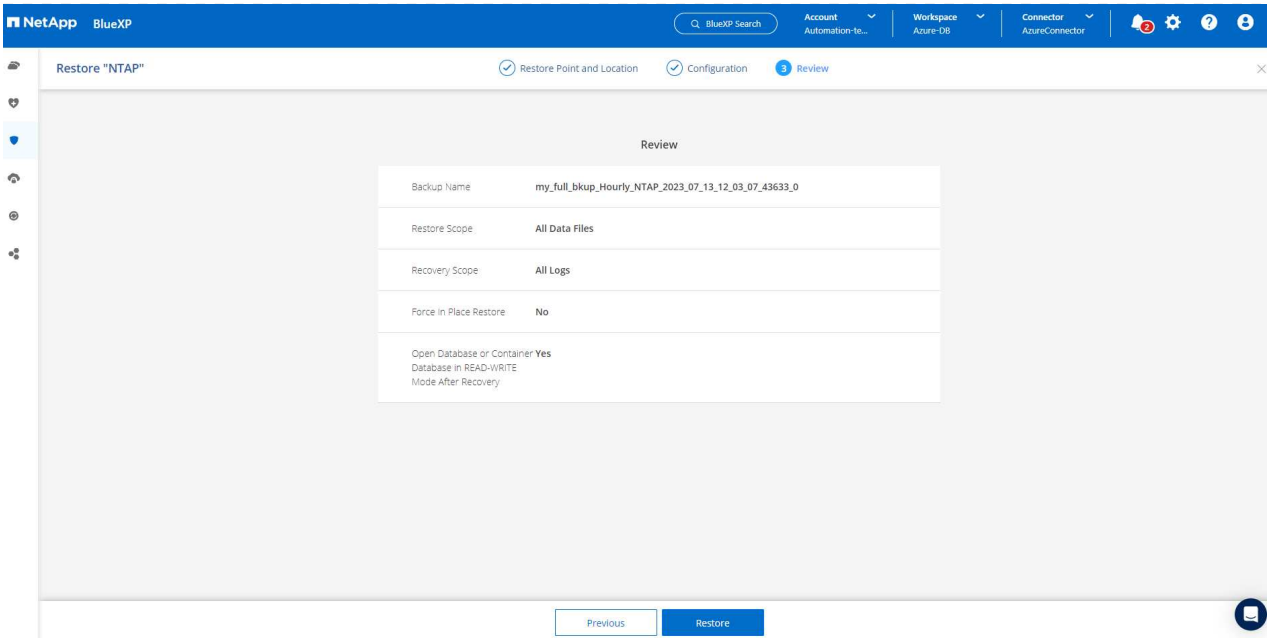
3. Scegliere **Restore Location** to **Original Location** (posizione di ripristino* in **posizione originale**) per il ripristino e il ripristino di un database Oracle.



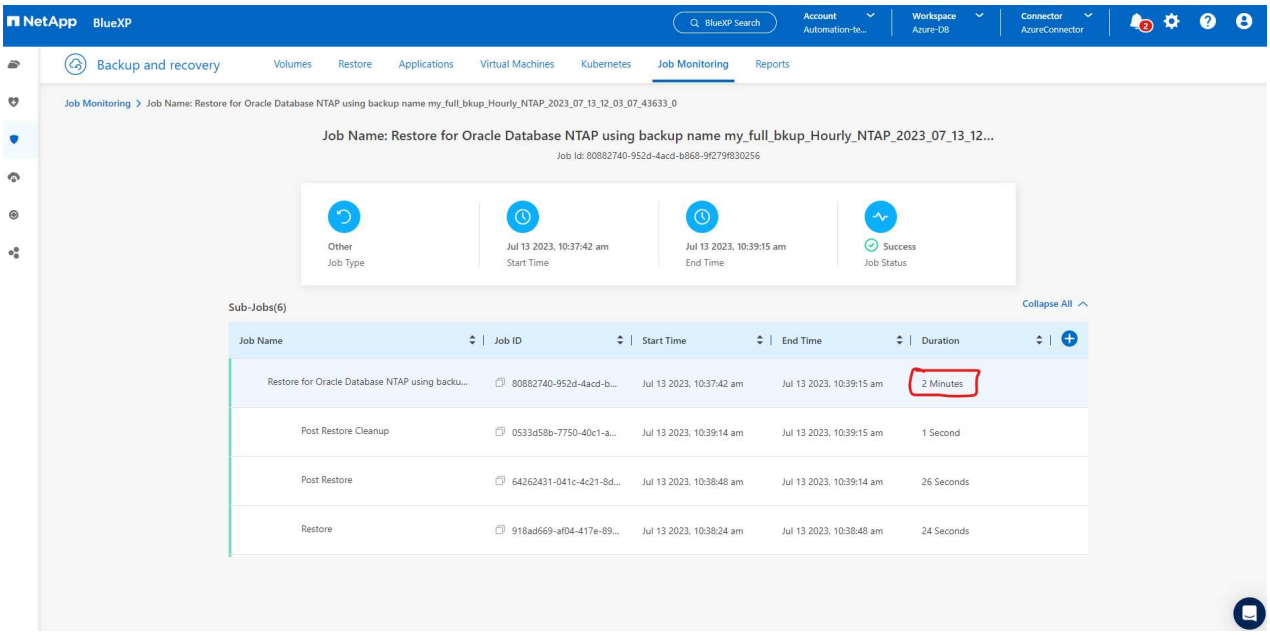
4. Definire **ambito di ripristino** e **ambito di ripristino**. Tutti i registri indicano un ripristino completo aggiornato, inclusi i registri correnti.



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.

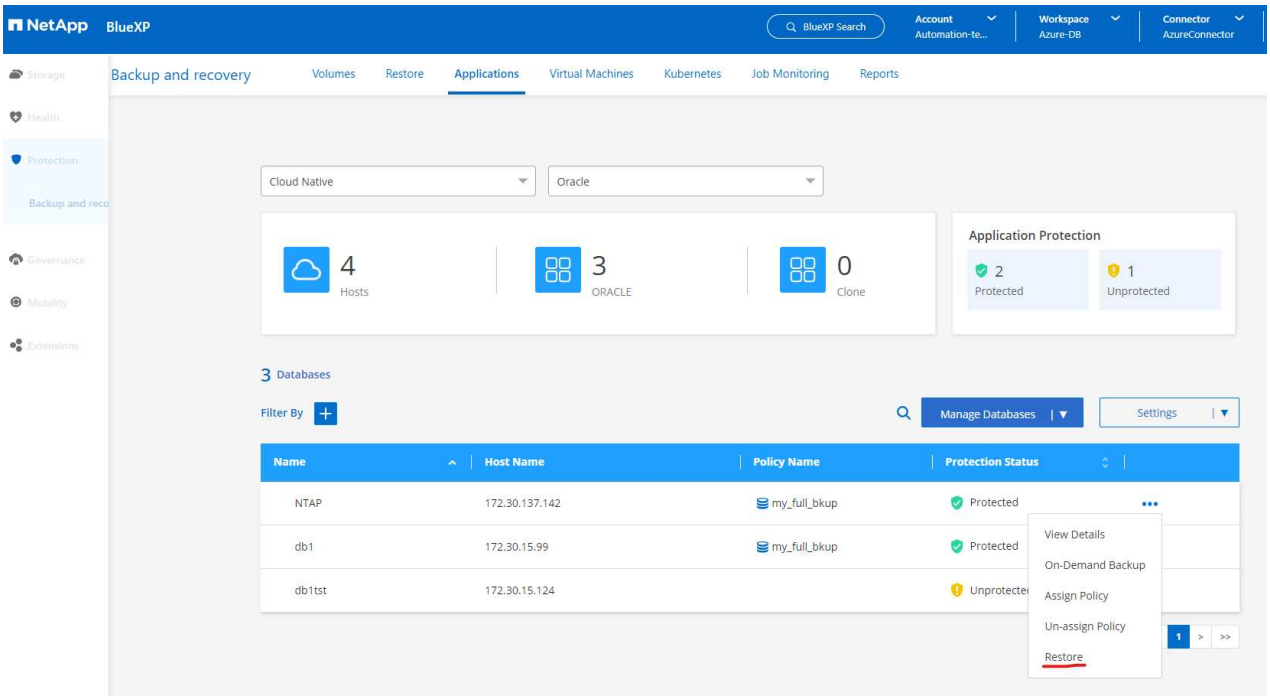


Clone del database Oracle

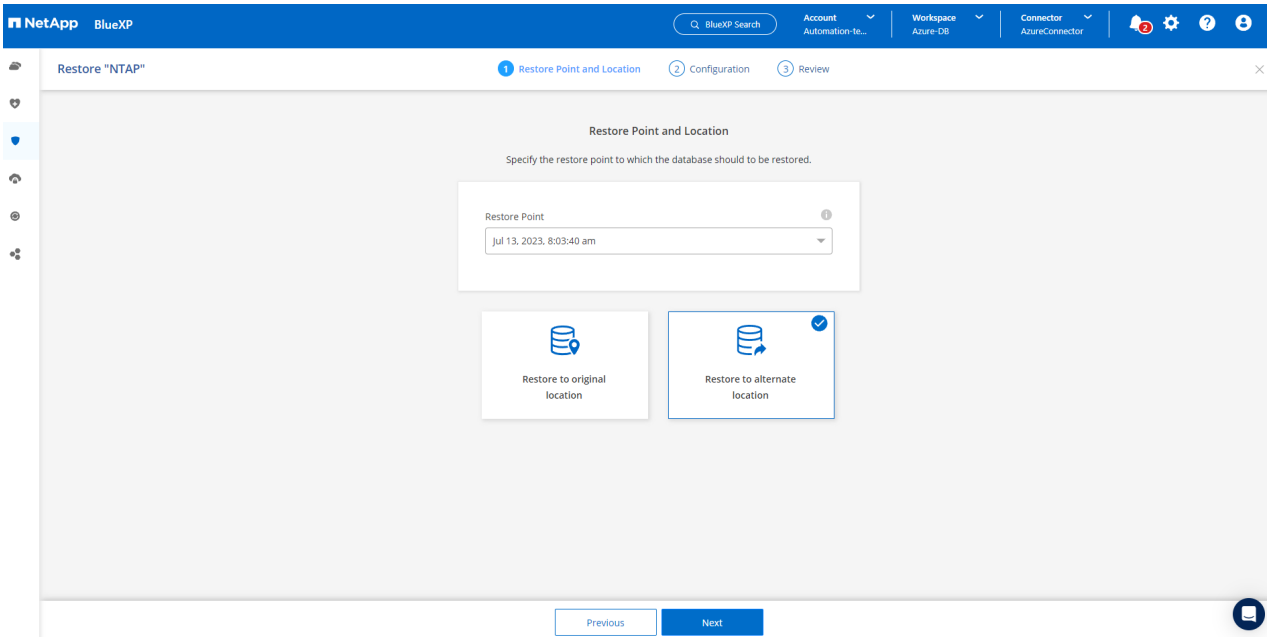
Le procedure di clone del database sono simili al ripristino, ma a una VM Azure alternativa con stack software Oracle identico preinstallato e configurato.

> 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**.

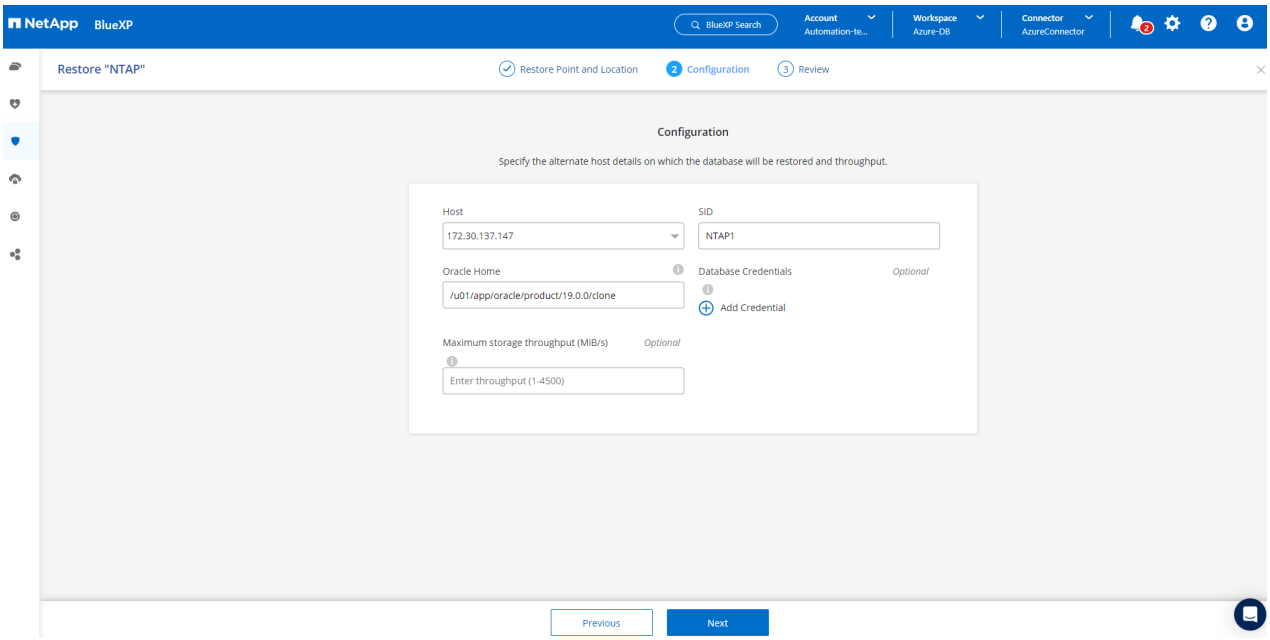
1. Fare clic sul menu a discesa a tre punti per il database specifico da clonare in **applicazioni**, quindi fare clic su **Ripristina** per avviare il flusso di lavoro di clonazione.



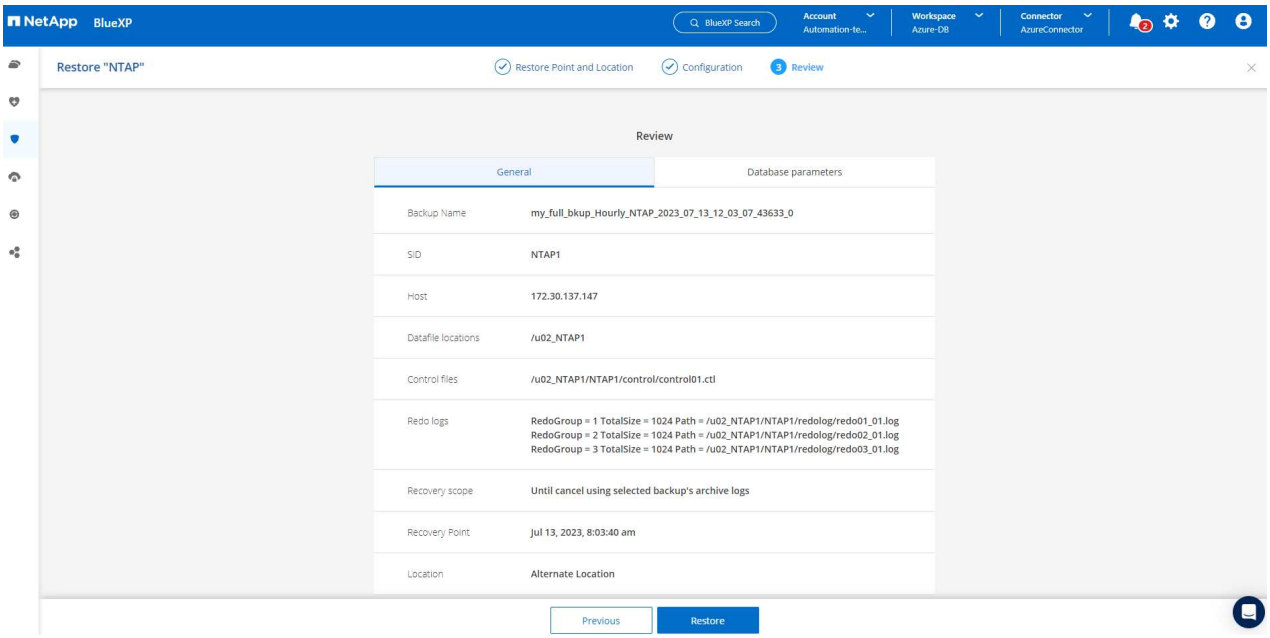
2. Selezionare **Restore Point** e selezionare **Restore to Alternate Location**.



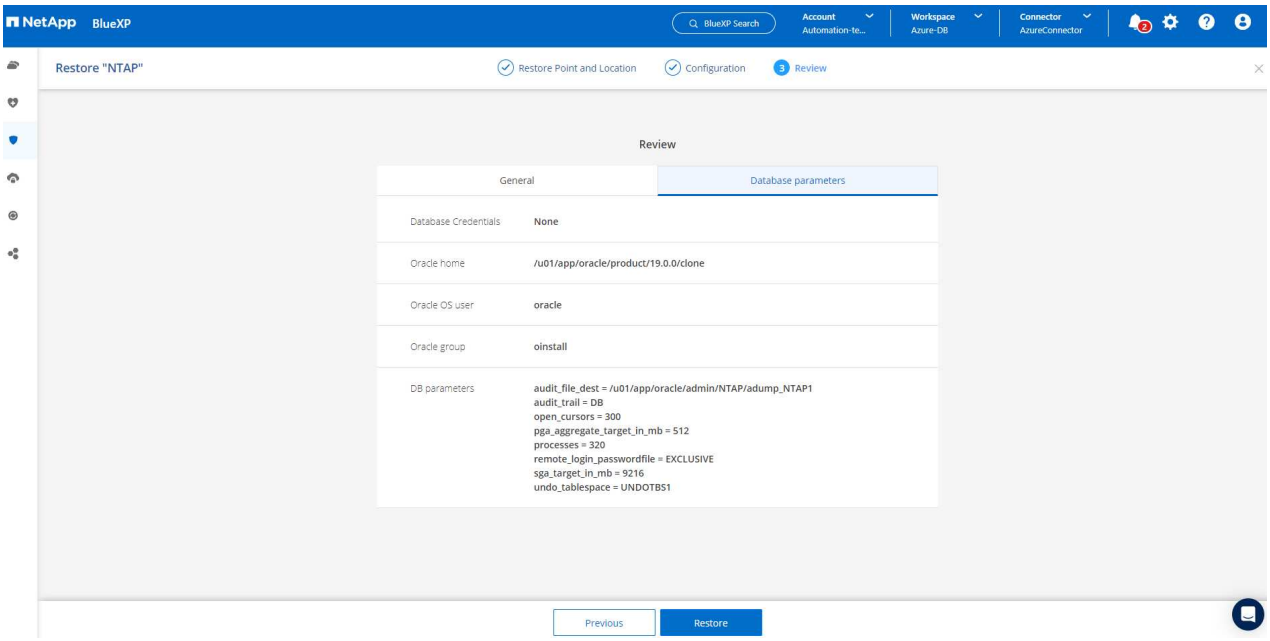
3. Nella pagina successiva **Configurazione**, impostare alternativo **host**, nuovo database **SID** e **Oracle Home** come configurato in alternativa ad Azure VM.



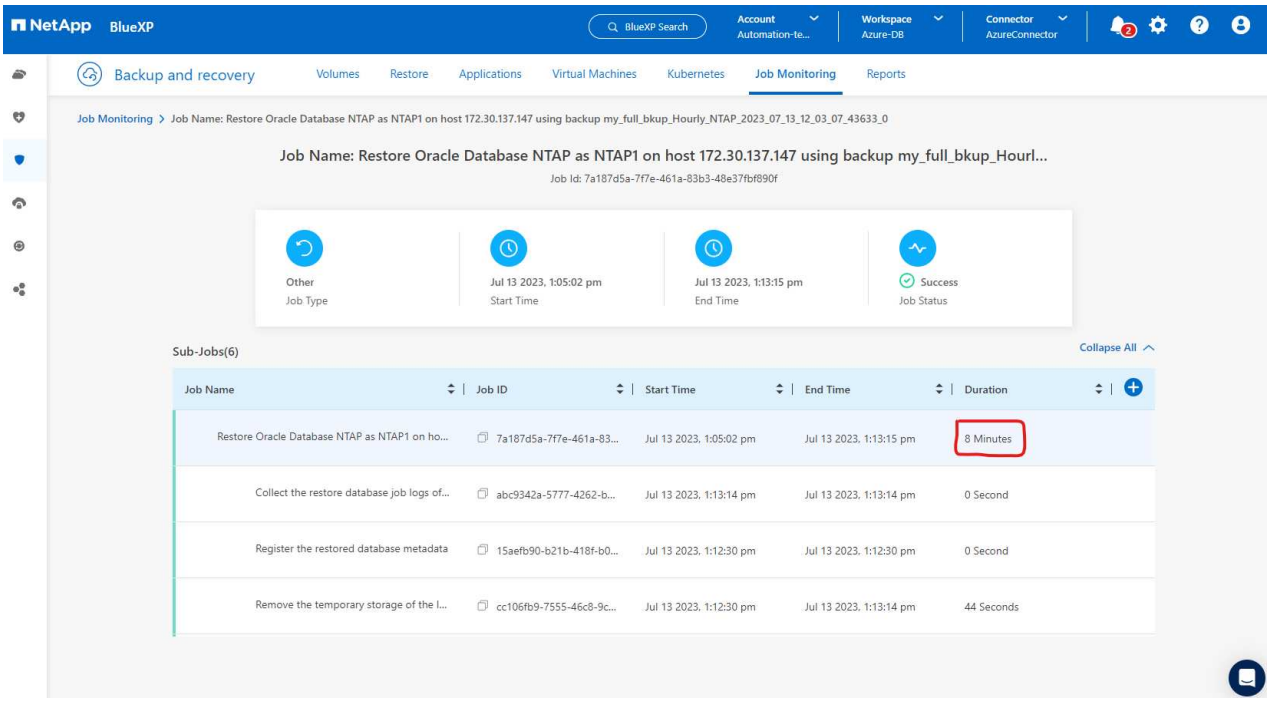
4. La pagina Review **General** (Revisione **Generale**) mostra i dettagli del database clonato, come SID, host alternativo, posizioni dei file di dati, ambito di ripristino e così via



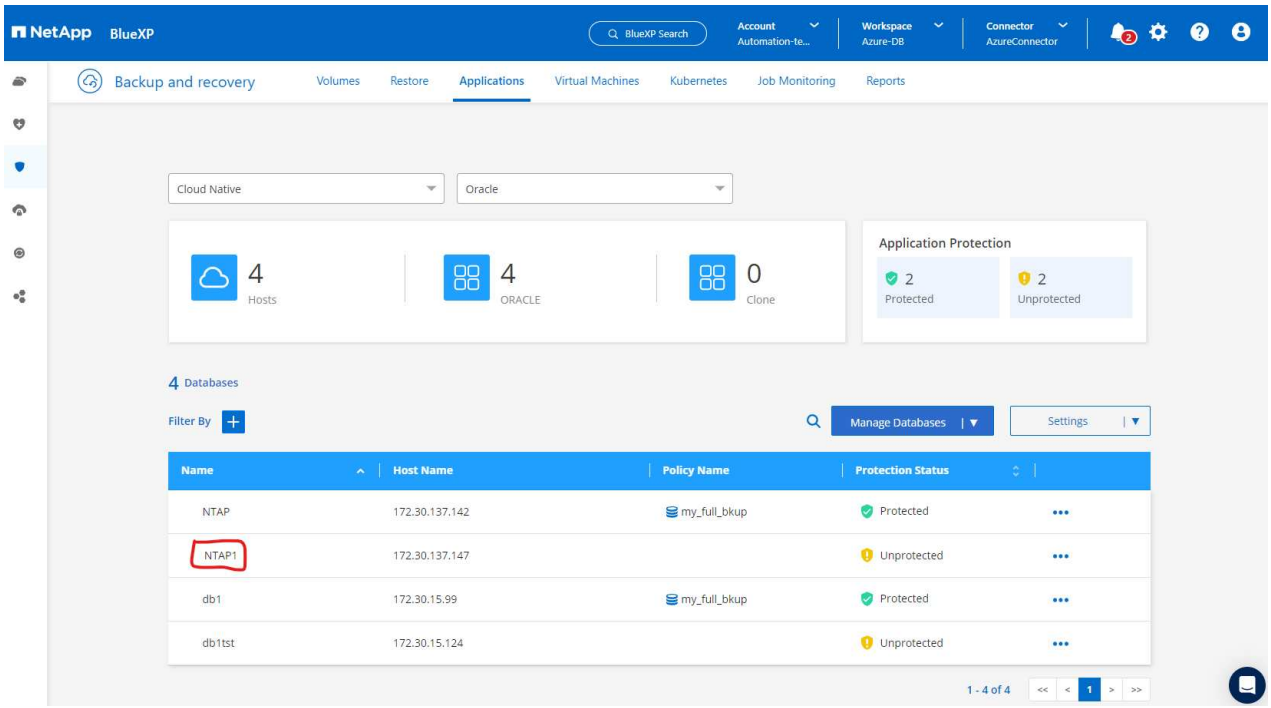
5. Nella pagina Review **Database parameters** sono riportati i dettagli della configurazione clonata del database e alcune impostazioni dei parametri del database.



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.



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"

- Documentazione di backup e ripristino BlueXP

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

- Azure NetApp Files

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

- Inizia subito con Azure

  "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

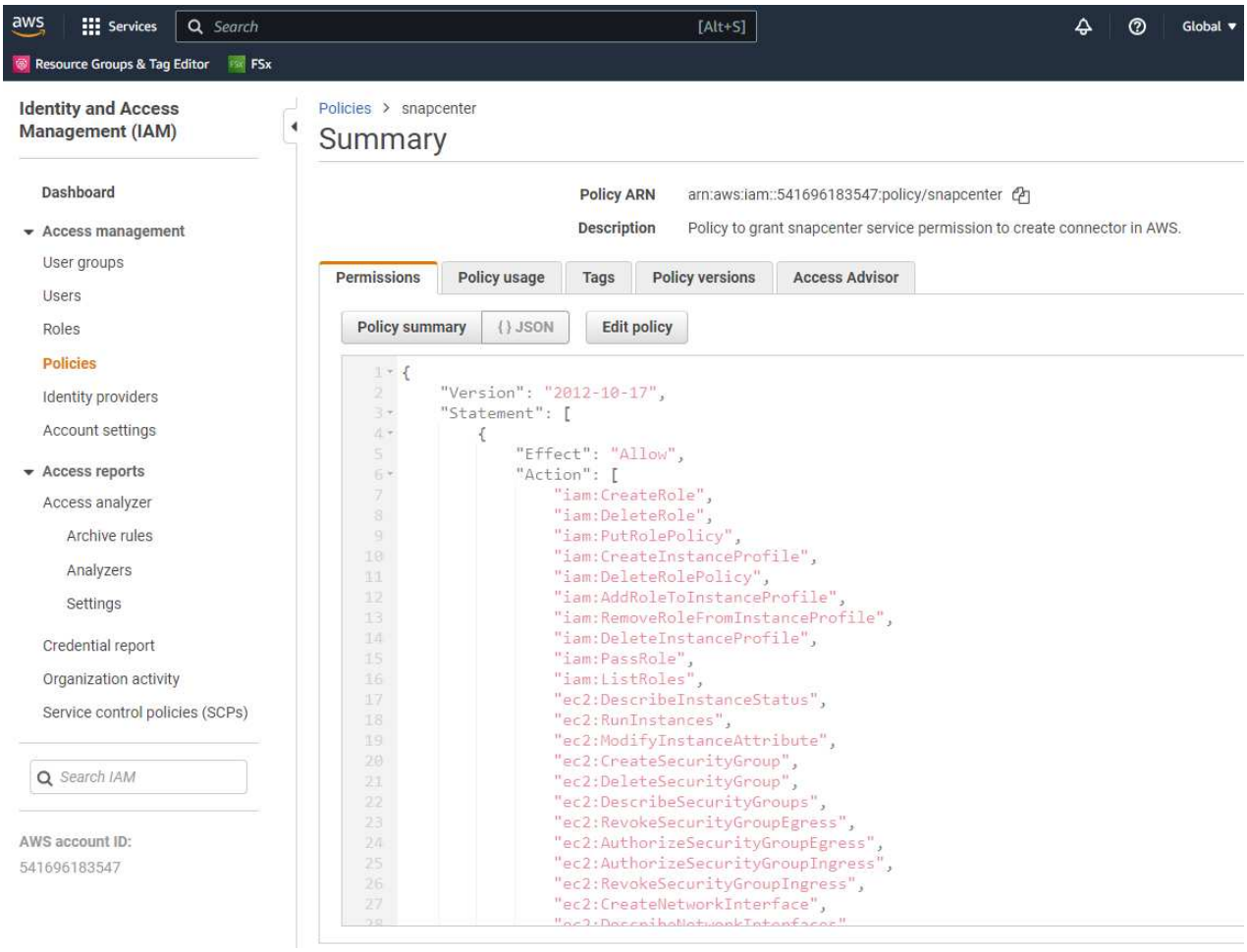
Prerequisiti per l'implementazione del servizio SnapCenter

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.

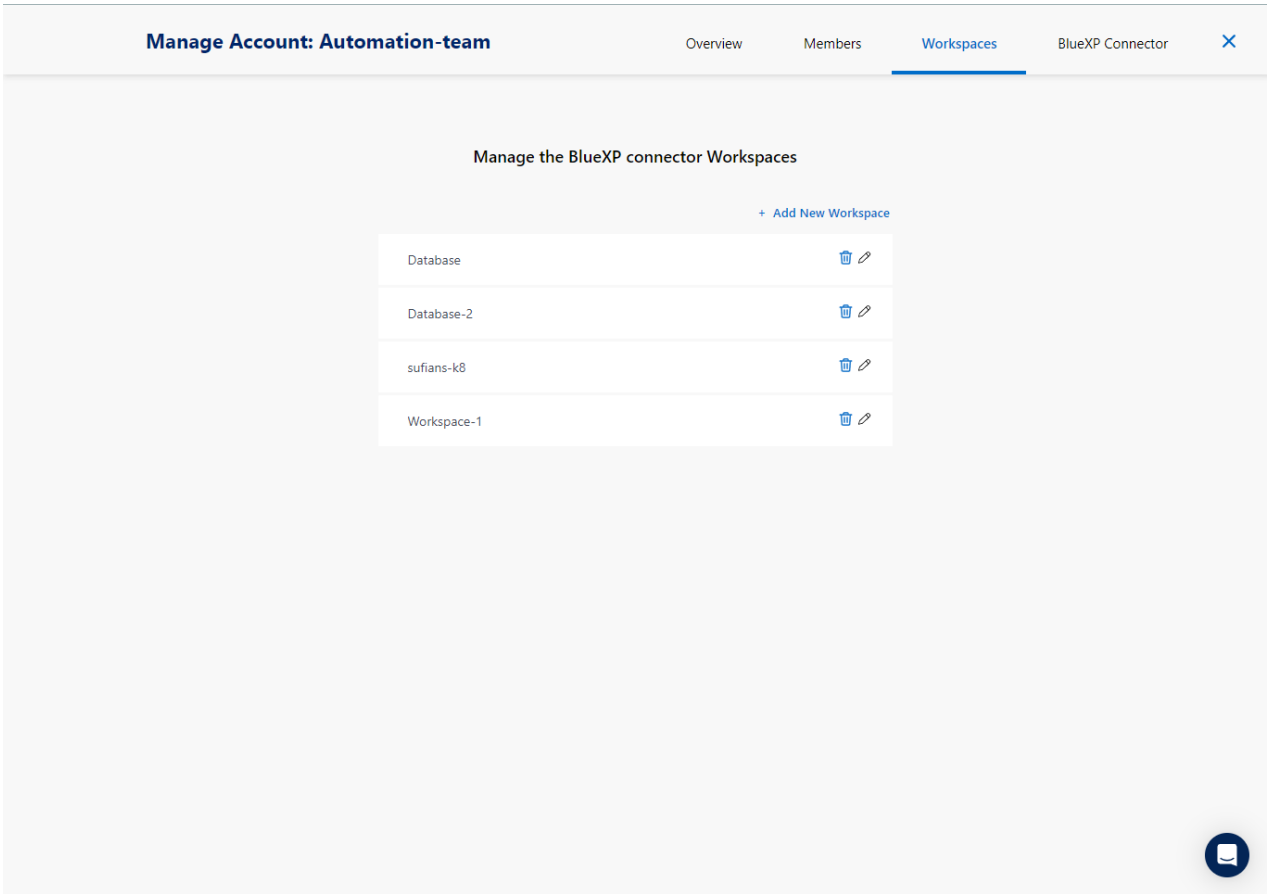


   Il criterio deve essere configurato con una stringa JSON disponibile nella documentazione di NetApp. La stringa JSON può essere recuperata anche dalla pagina quando viene avviato il provisioning del connettore e viene richiesto l'assegnazione delle autorizzazioni prerequisiti.

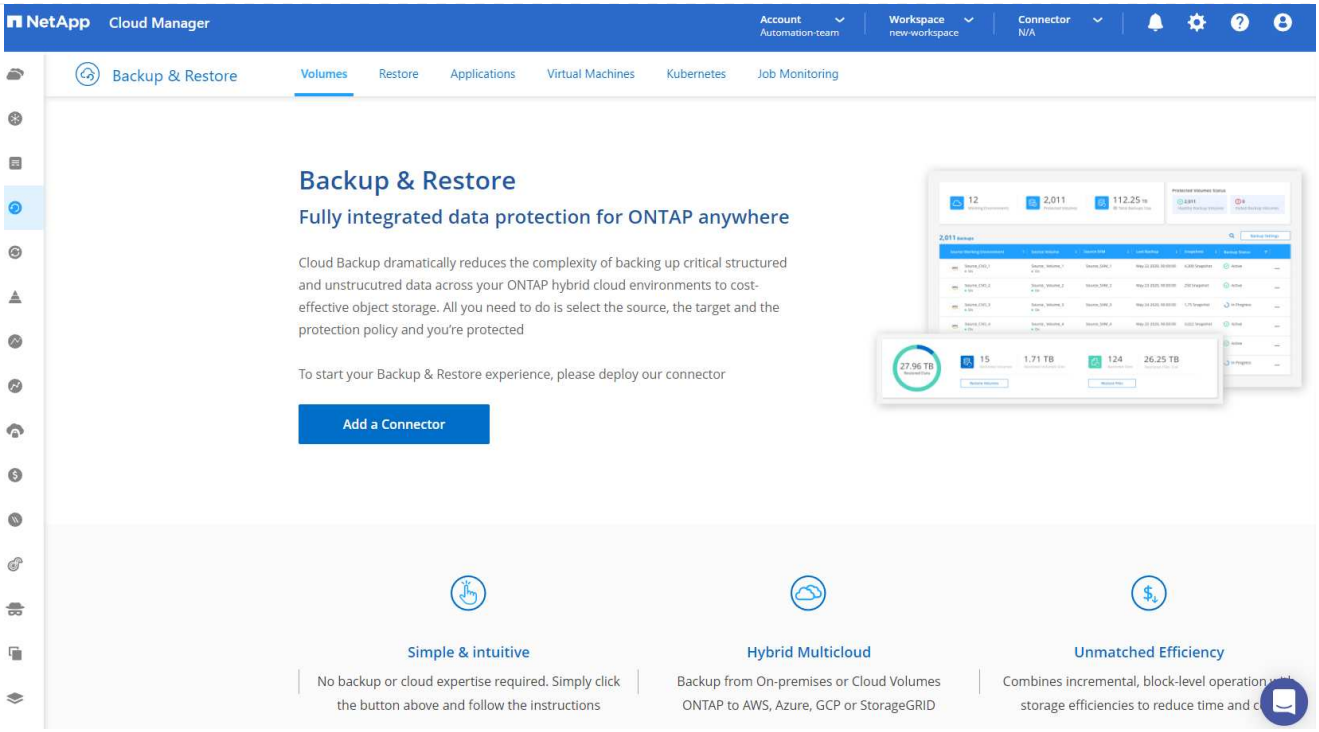
3. Ti servono anche VPC AWS, subnet, gruppo di sicurezza, una chiave di accesso e segreti per un account utente AWS, una chiave SSH per EC2 utenti e così via, pronti per il provisioning dei connettori.

Implementare un connettore per i servizi SnapCenter

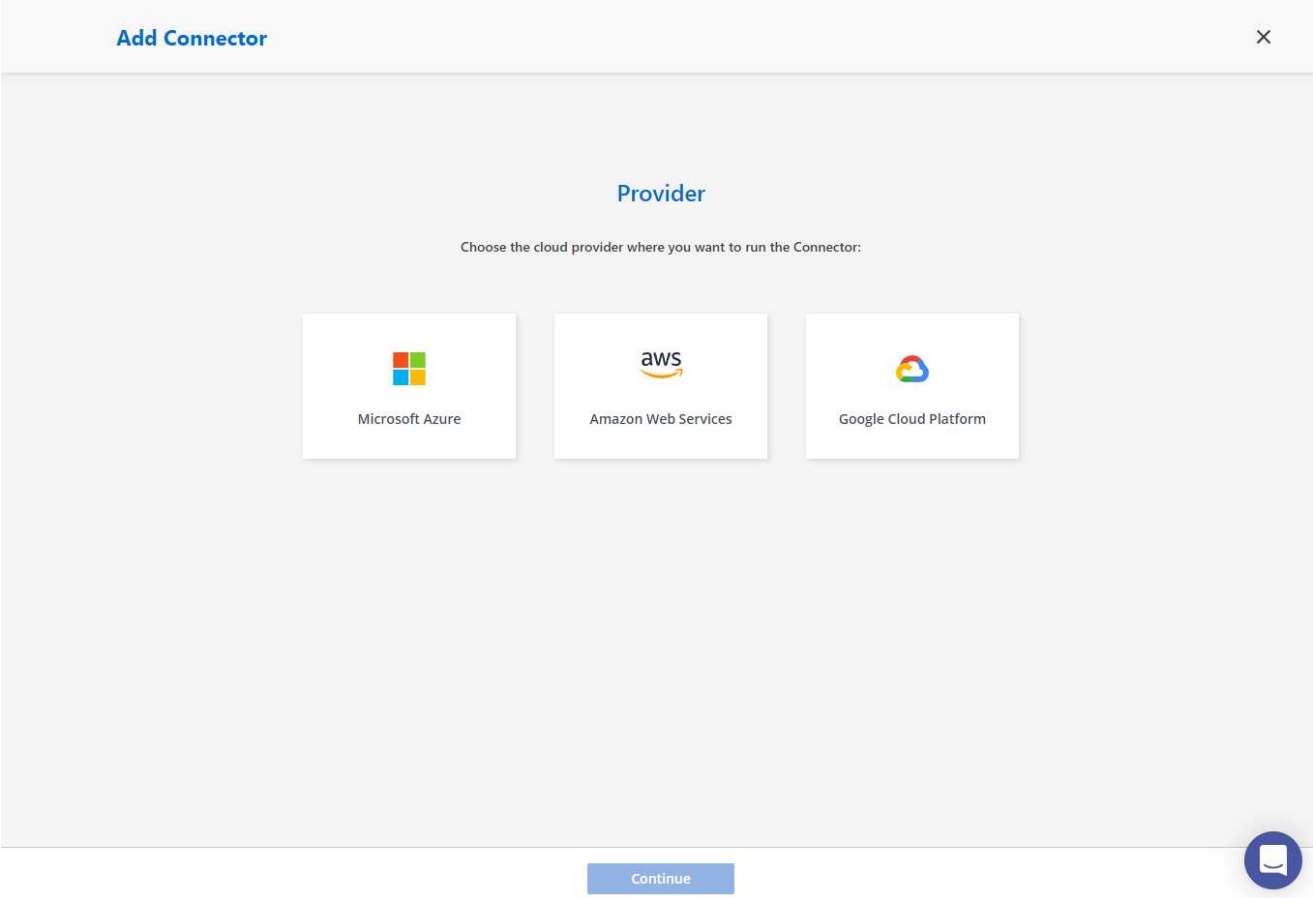
1. Accedi alla console BlueXP. Per un account condiviso, è consigliabile creare un singolo spazio di lavoro facendo clic su **account** > **Manage account** > **Workspace** per aggiungere un nuovo spazio di lavoro.



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

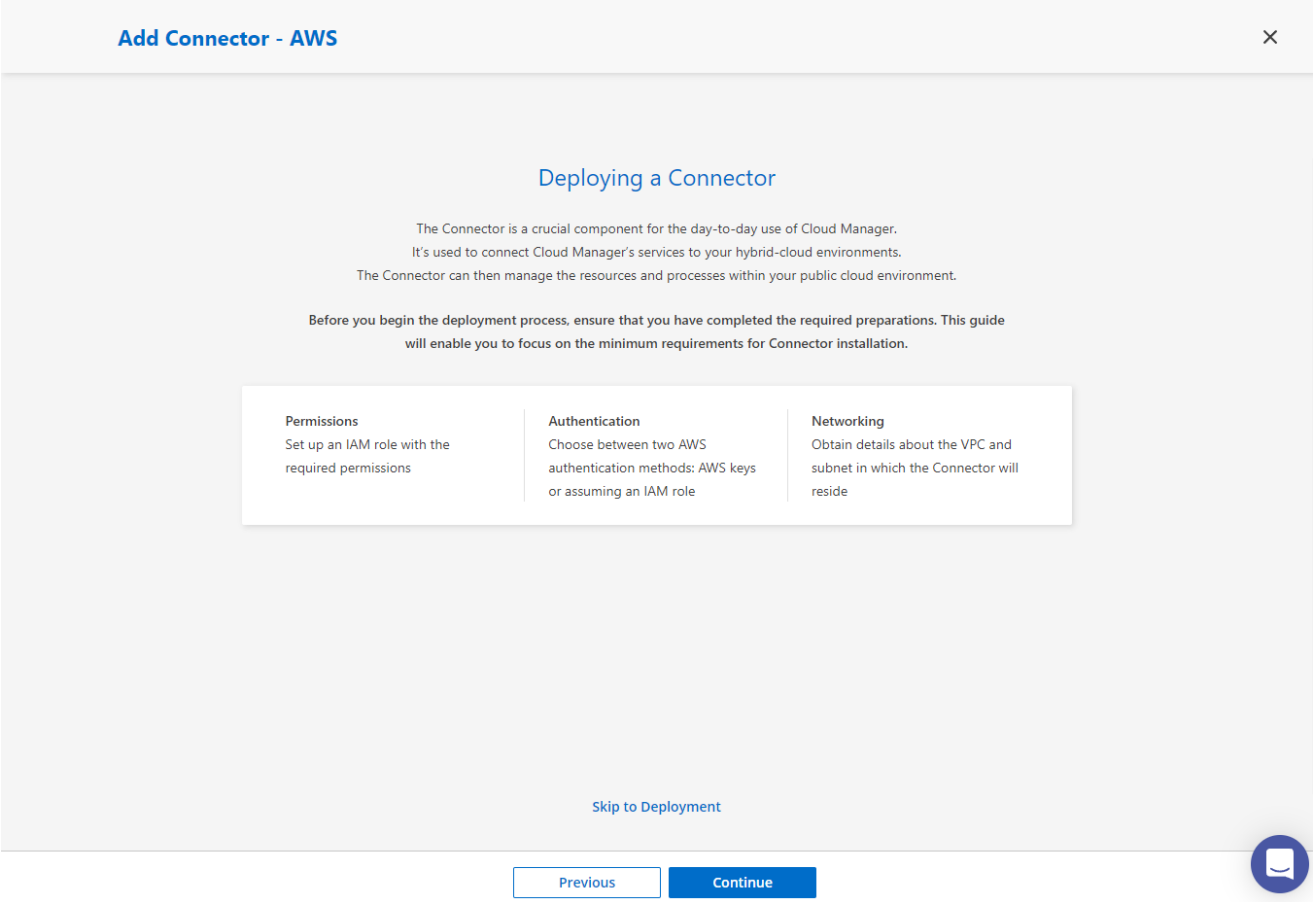


1. Scegli il tuo cloud provider (in questo caso, **Amazon Web Services**).

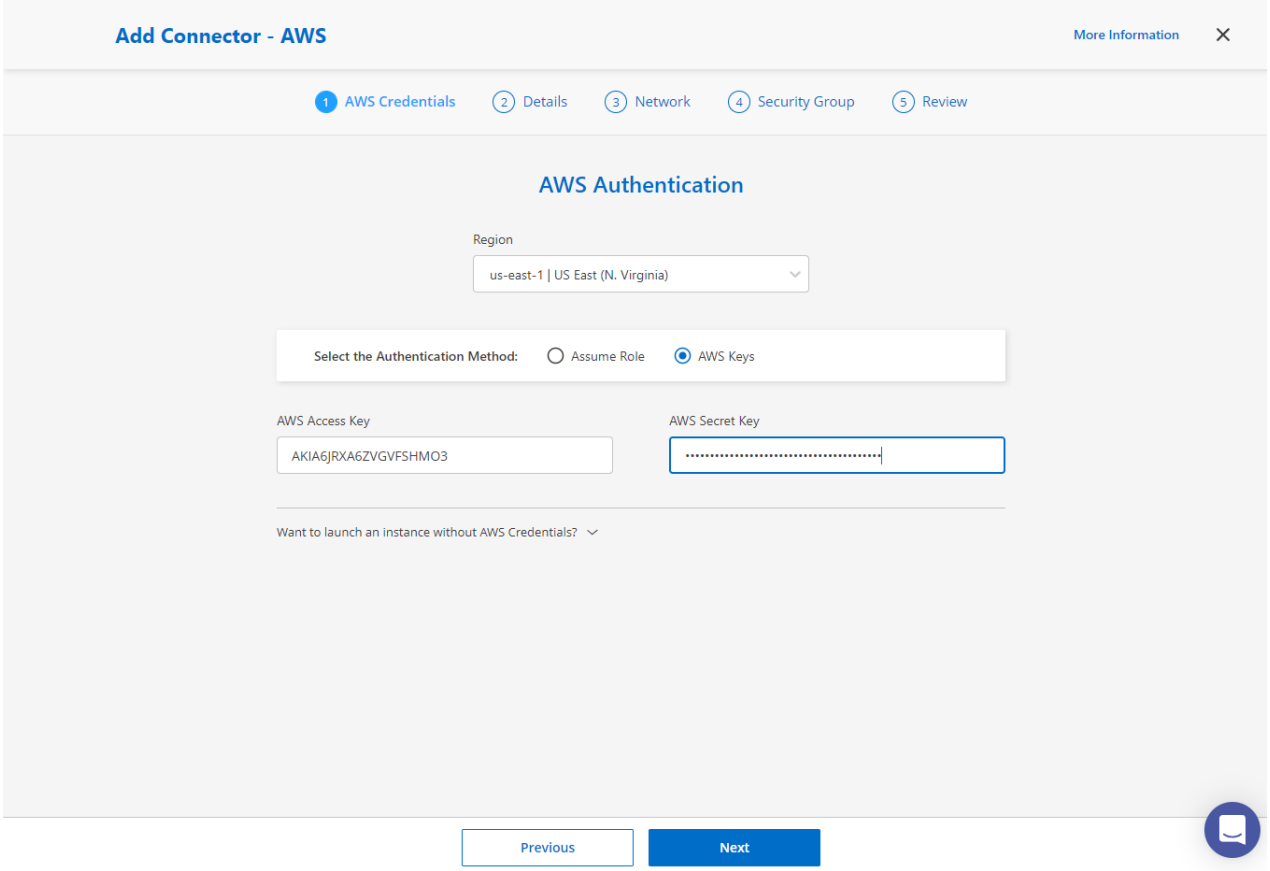


1. Ignorare i passaggi **Permission**, **Authentication** e **Networking** se sono già stati configurati nell'account AWS. In caso contrario, è necessario configurarli prima di procedere. Da qui, è possibile recuperare anche le autorizzazioni per il criterio AWS a cui si fa riferimento nella sezione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

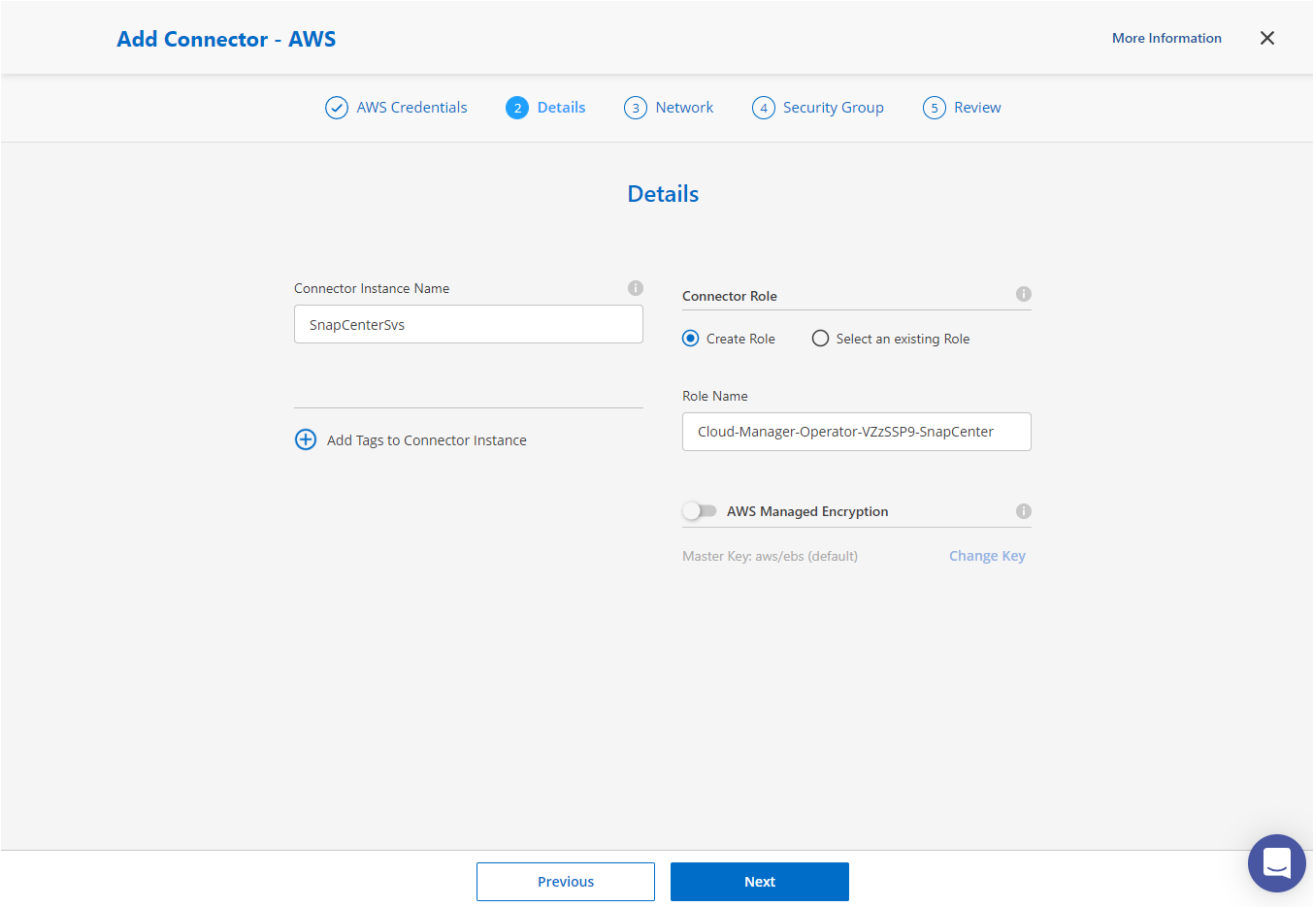
"Preparazione al BlueXP."



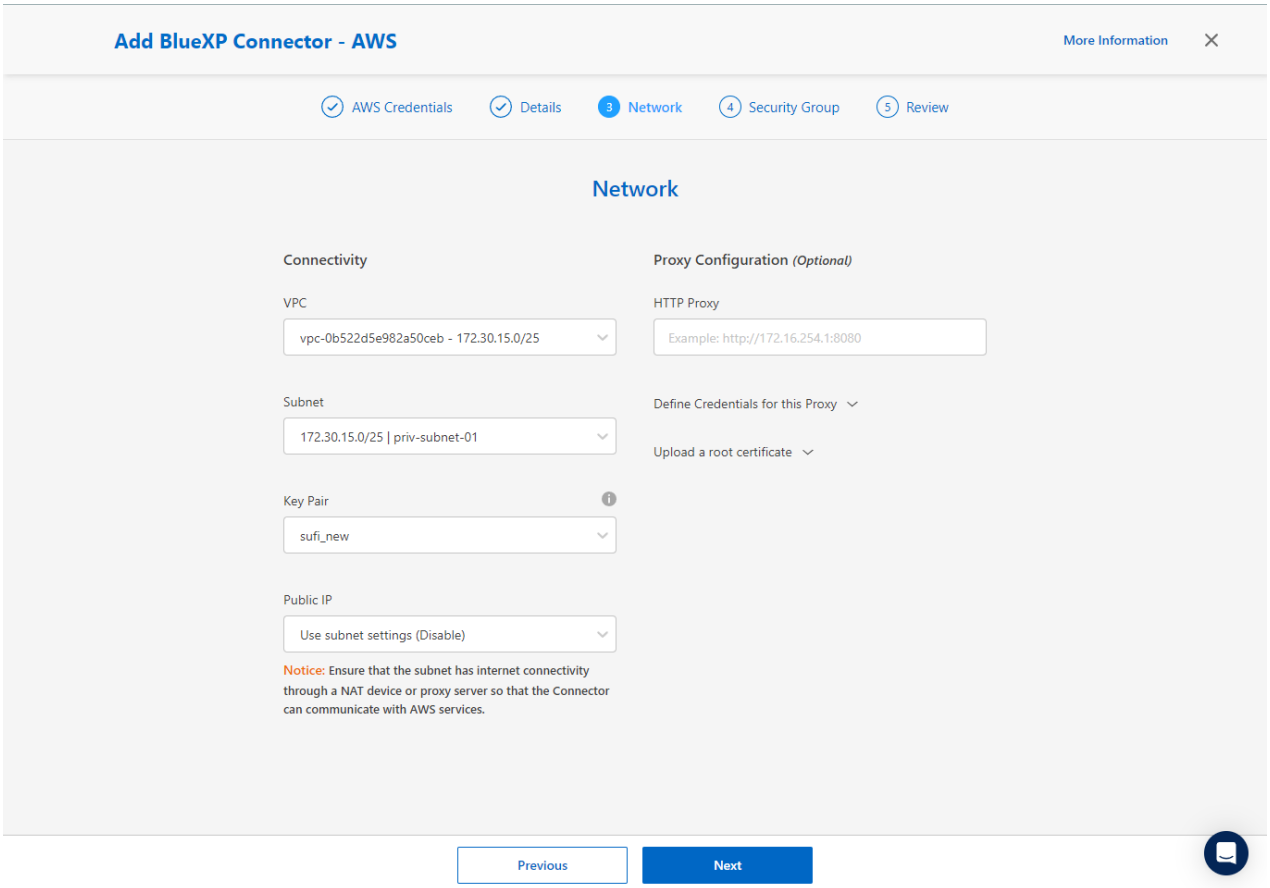
1. Inserisci l'autenticazione del tuo account AWS con **Access Key** e **Secret Key**.



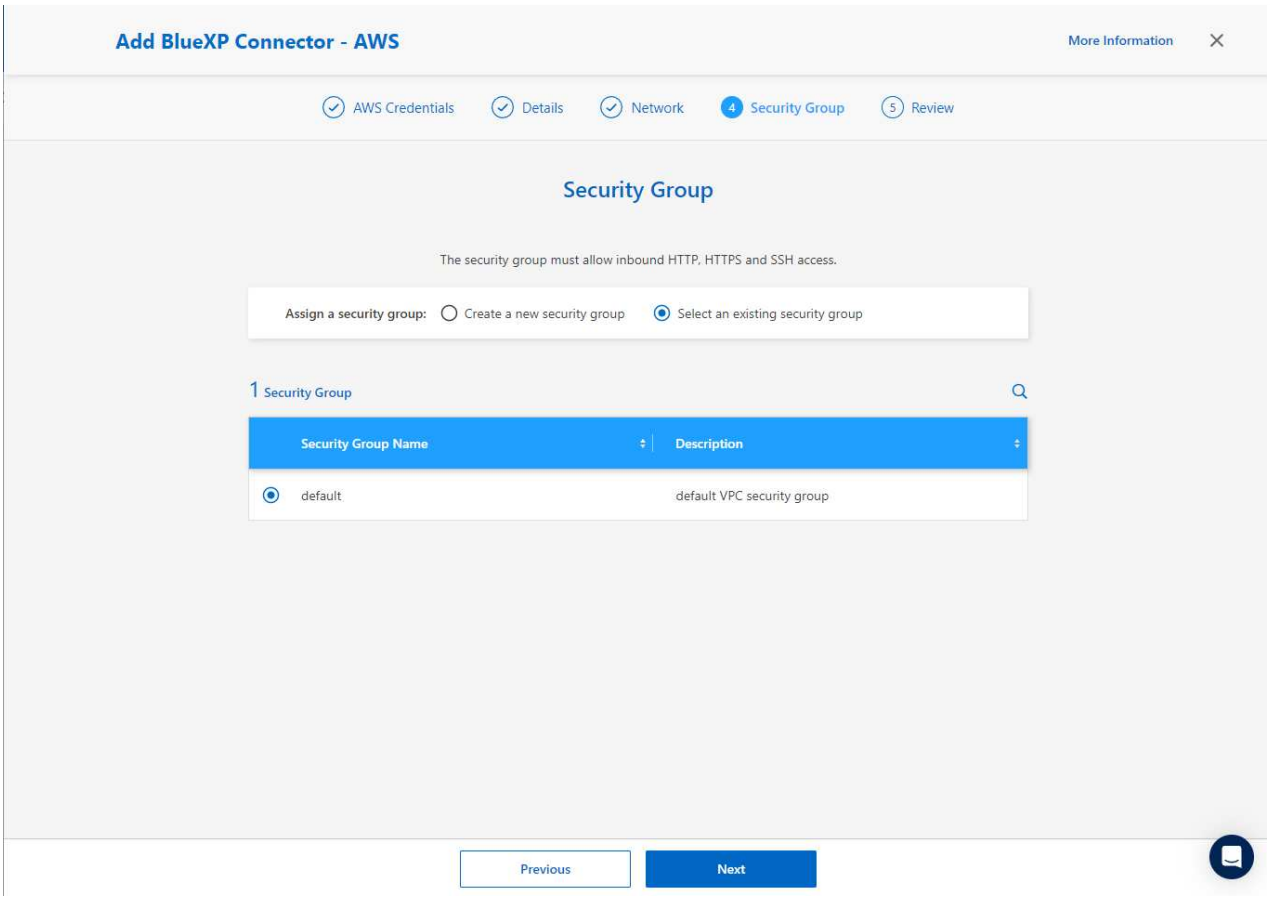
2. Assegnare un nome all'istanza del connettore e selezionare **Crea ruolo** in **Dettagli**.



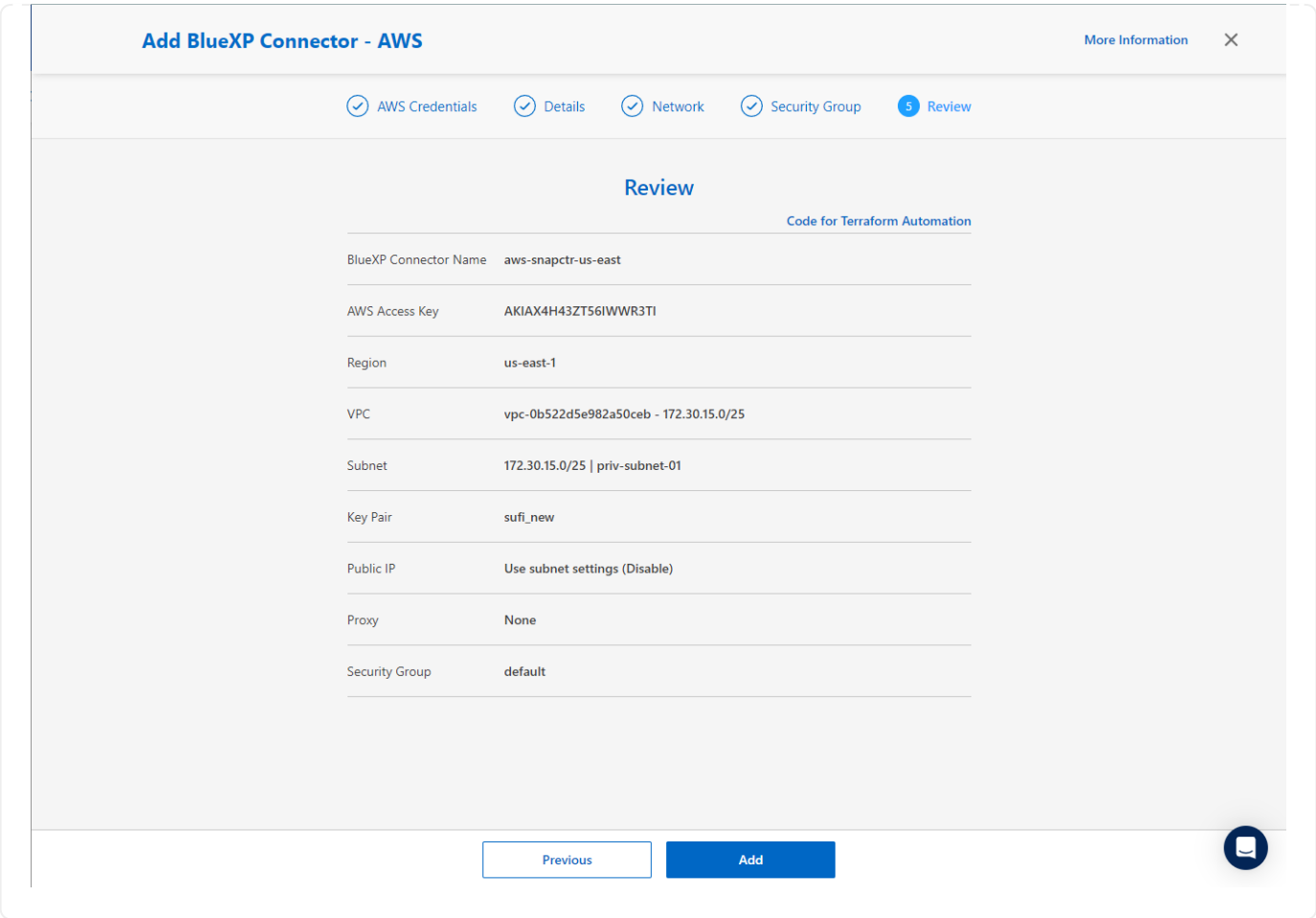
1. Configurare la rete con **VPC**, **Subnet** e SSH **Coppia di chiavi** per l'accesso al connettore.



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

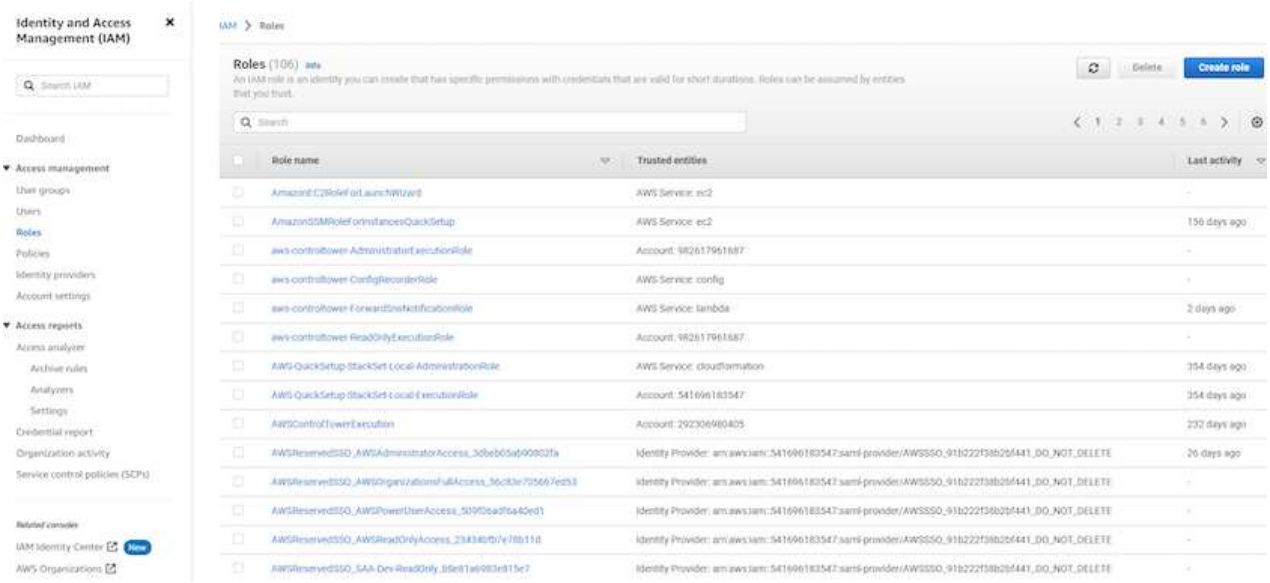


3. Esaminare la pagina di riepilogo e fare clic su **Aggiungi** per avviare la creazione del connettore. In genere occorrono circa 10 minuti per completare l'implementazione. Una volta completata l'operazione, l'istanza del connettore viene visualizzata nella dashboard di AWS EC2.

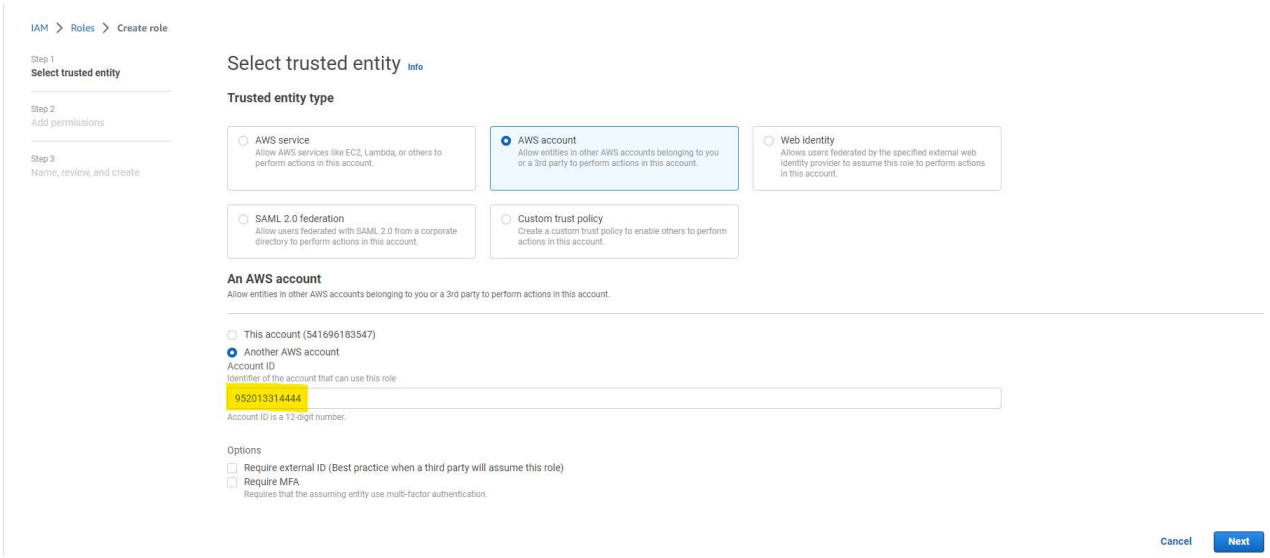


Definisci una credenziale nell’accesso alle risorse BlueXP per AWS

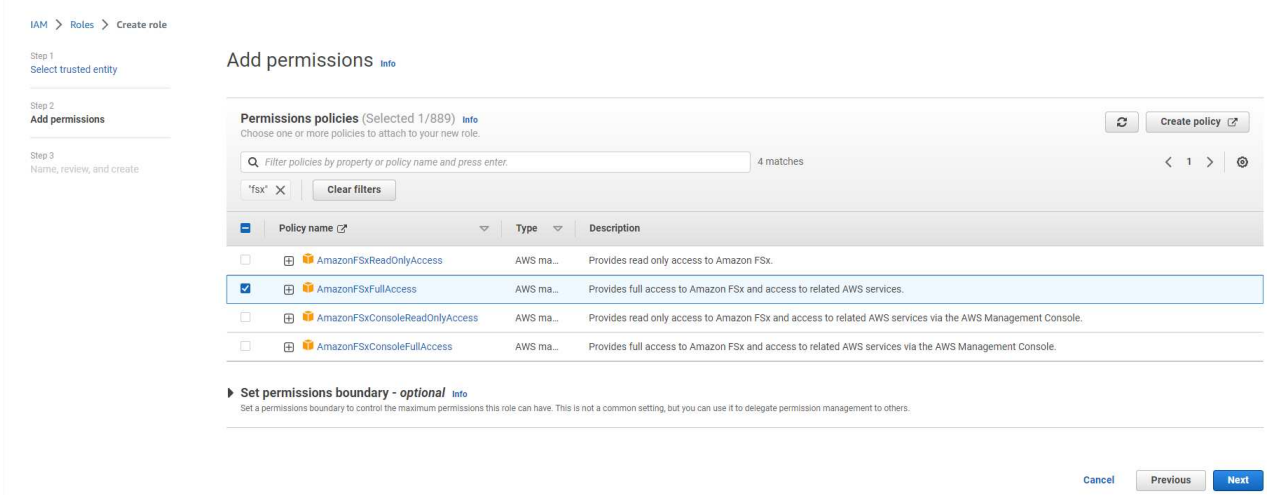
1. Innanzitutto, dalla console AWS EC2, creare un ruolo nel menu **Identity and Access Management (IAM) Roles**, **Create role** per avviare il flusso di lavoro di creazione dei ruoli.



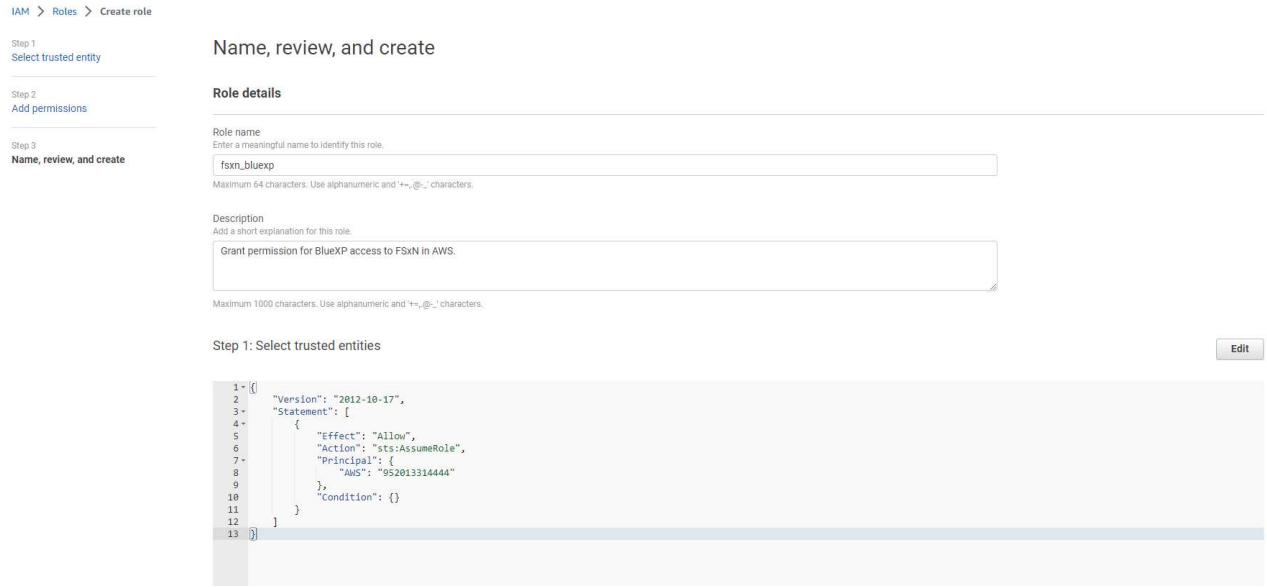
2. Nella pagina **Seleziona entità attendibile**, scegli **account AWS**, **un altro account AWS** e incolla nell'ID account BlueXP, che può essere recuperato dalla console BlueXP.



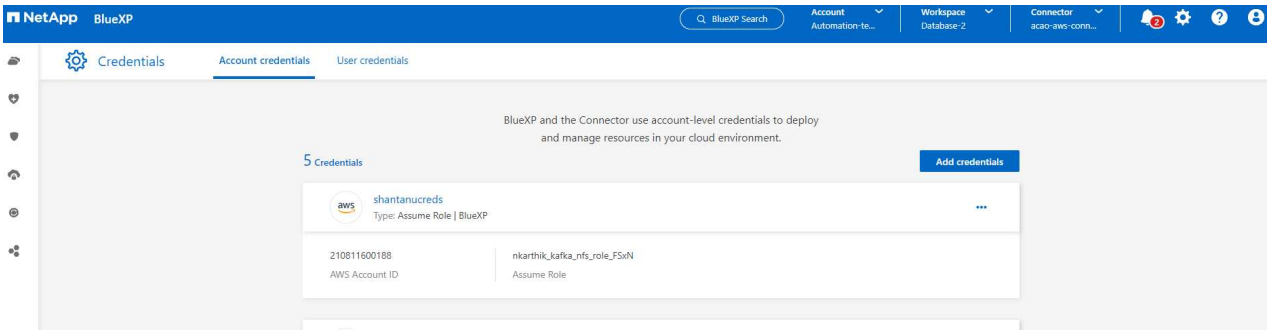
3. Filtrare i criteri di autorizzazione in base a fsx e aggiungere **Criteri di autorizzazione** al ruolo.



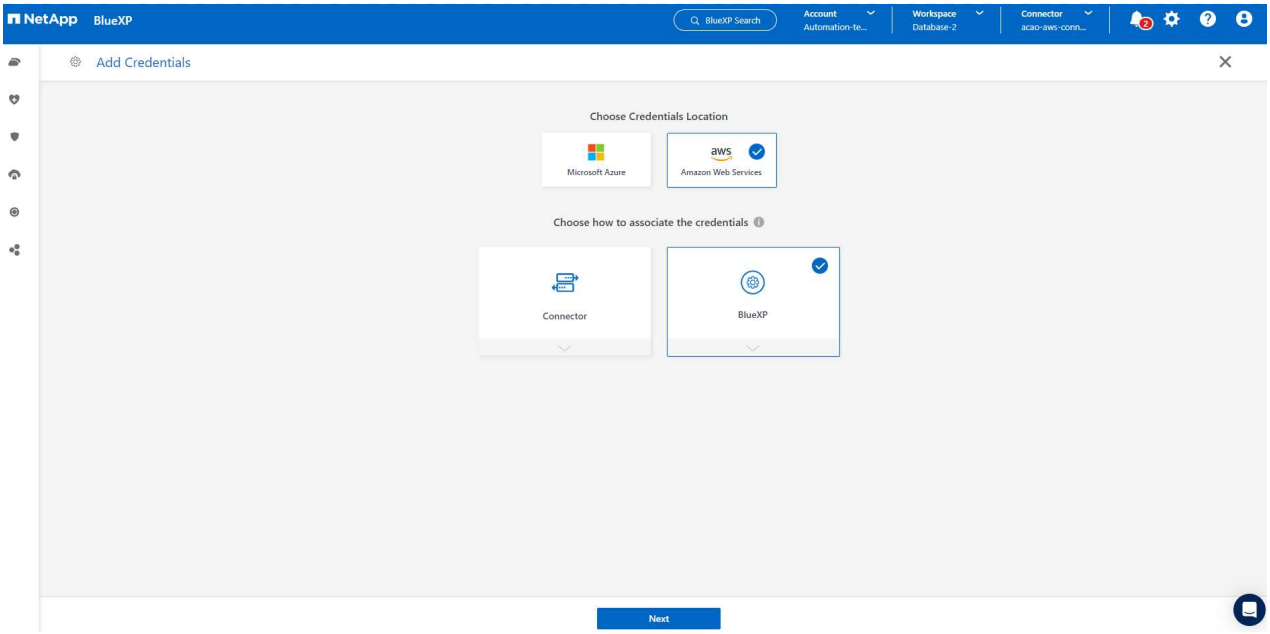
4. Nella pagina **dettagli ruolo**, assegnare un nome al ruolo, aggiungere una descrizione, quindi fare clic su **Crea ruolo**.



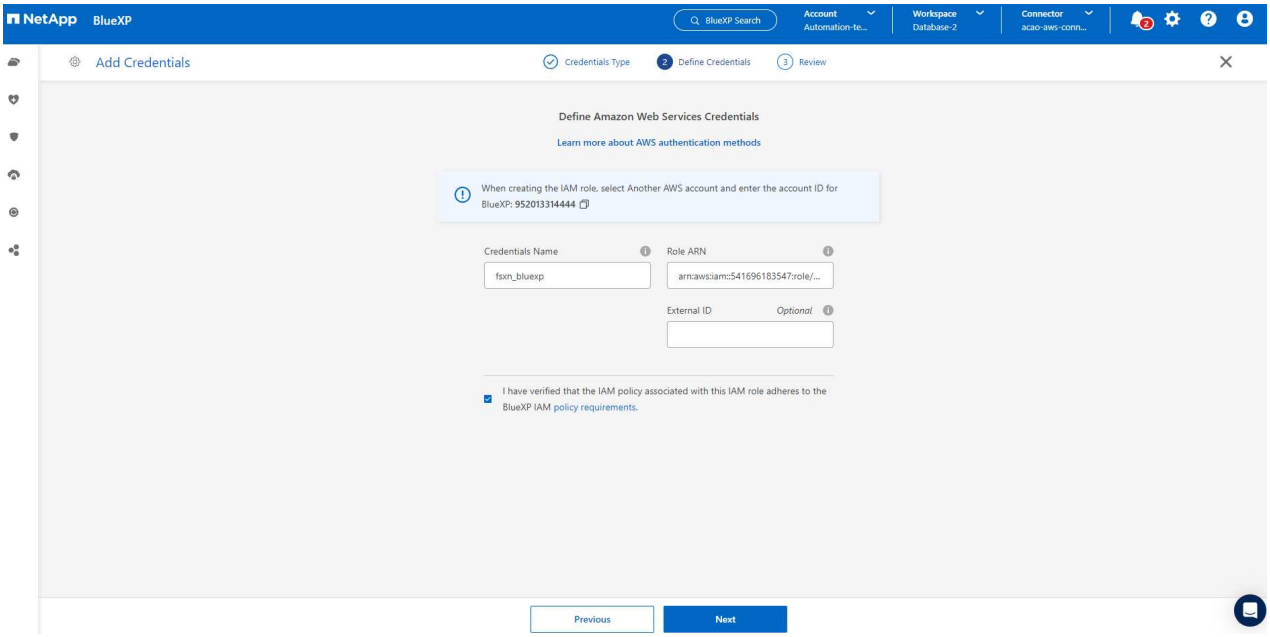
5. Tornando alla console BlueXP, fare clic sull'icona delle impostazioni nell'angolo superiore destro della console per aprire la pagina **credenziali account**, fare clic su **Aggiungi credenziali** per avviare il flusso di lavoro di configurazione delle credenziali.



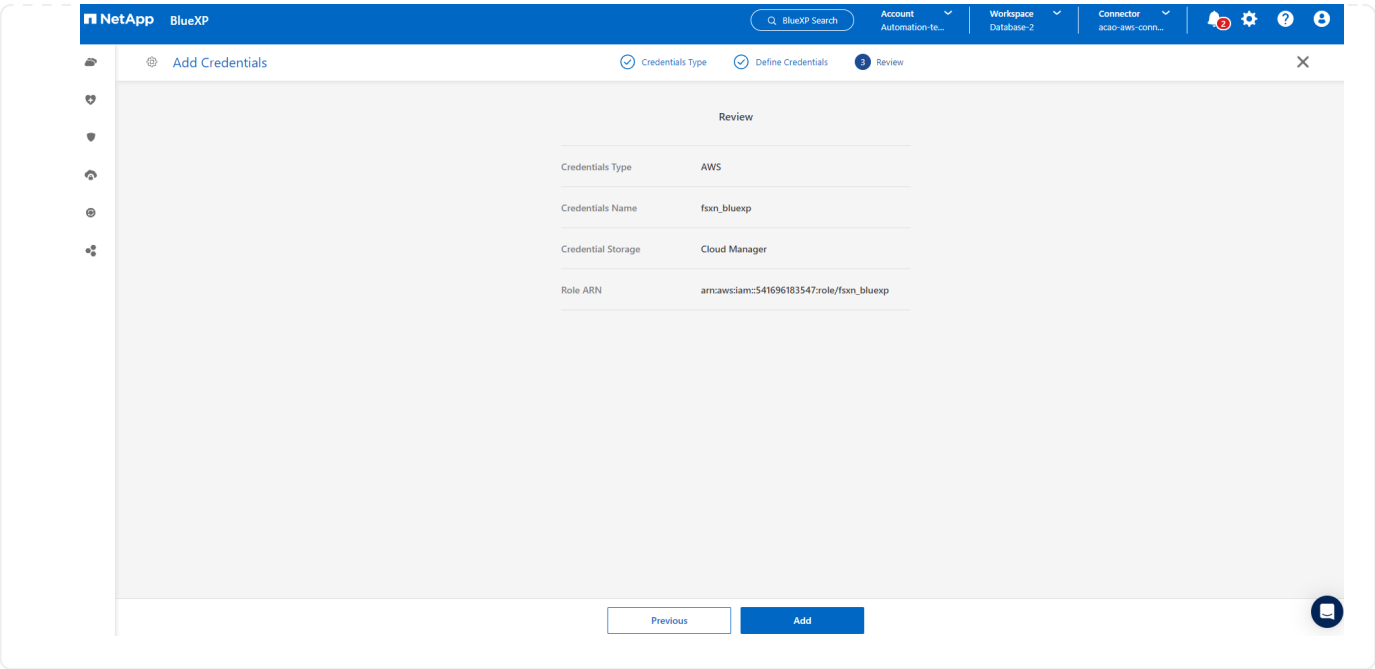
6. Scegli la posizione delle credenziali come - **Amazon Web Services - BlueXP**.



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.



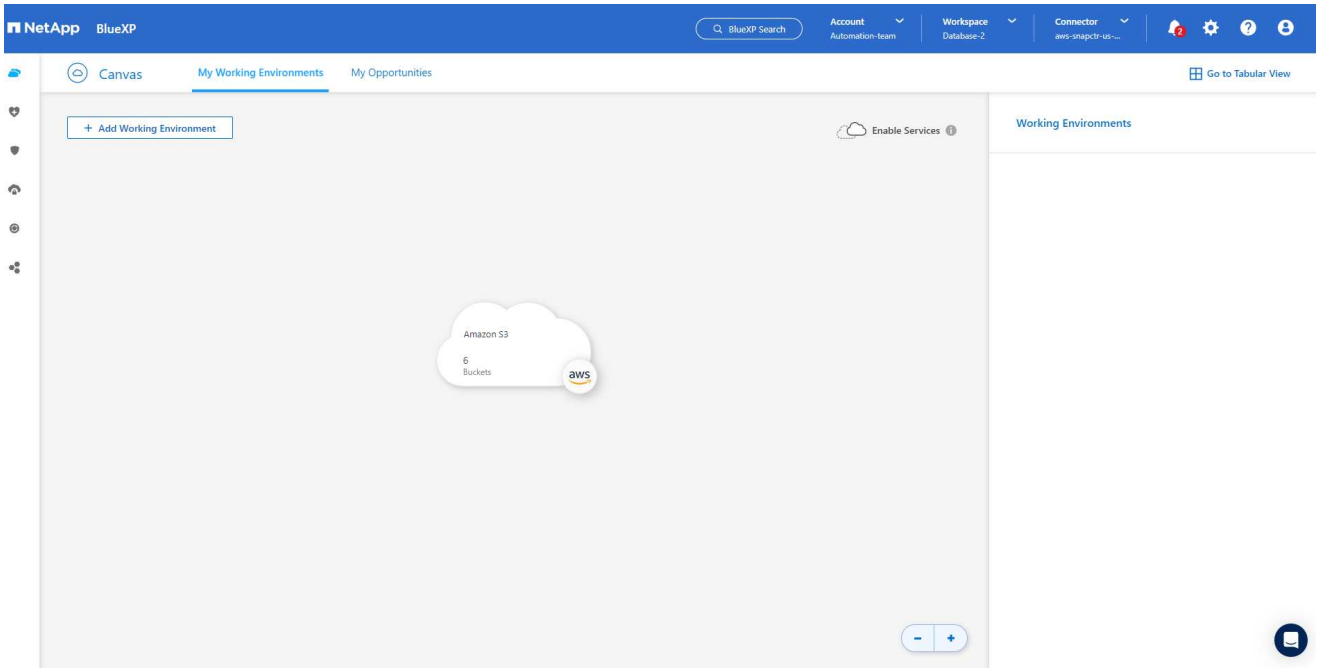
8. Rivedi e **Aggiungi**.



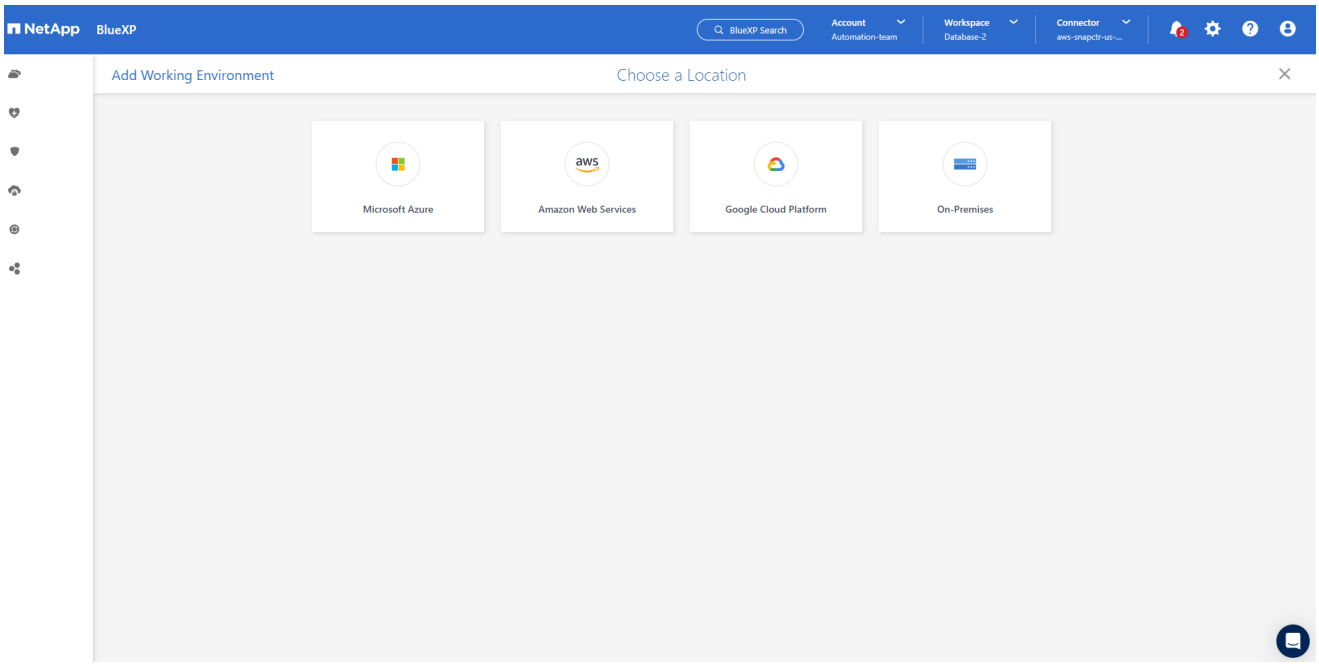
Configurazione dei servizi SnapCenter

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

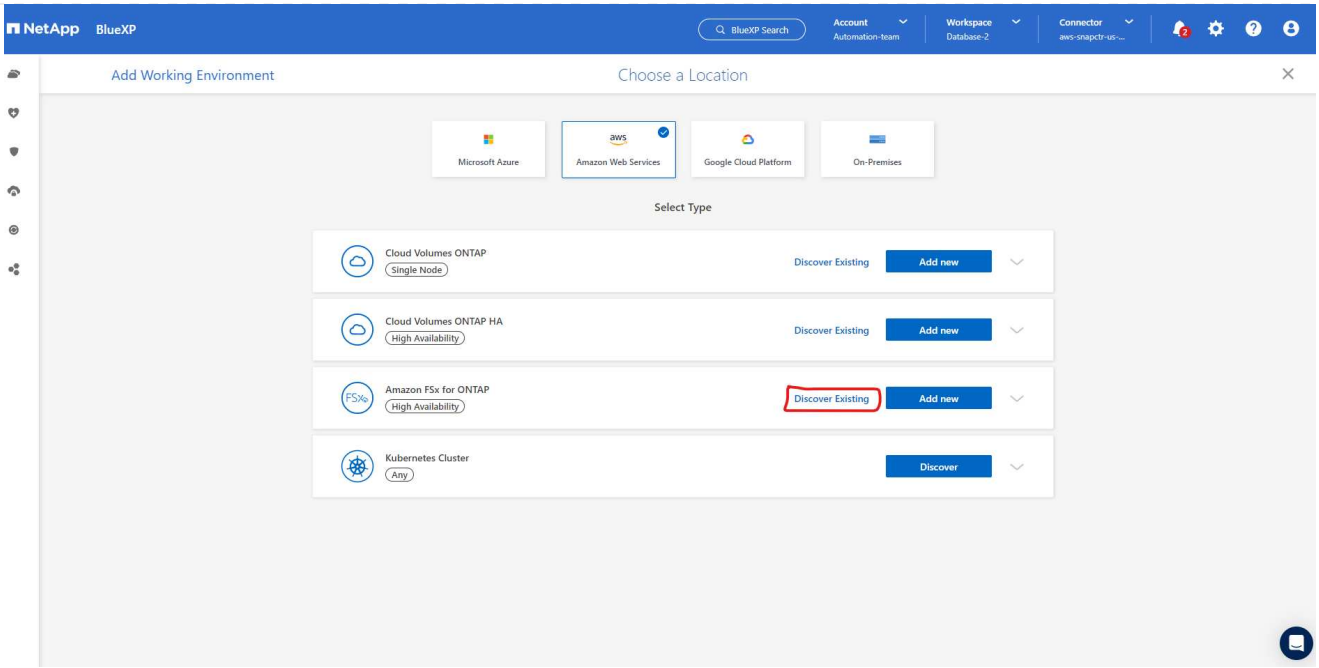
1. Da **My Working Environment** fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) per scoprire FSX implementato in AWS.



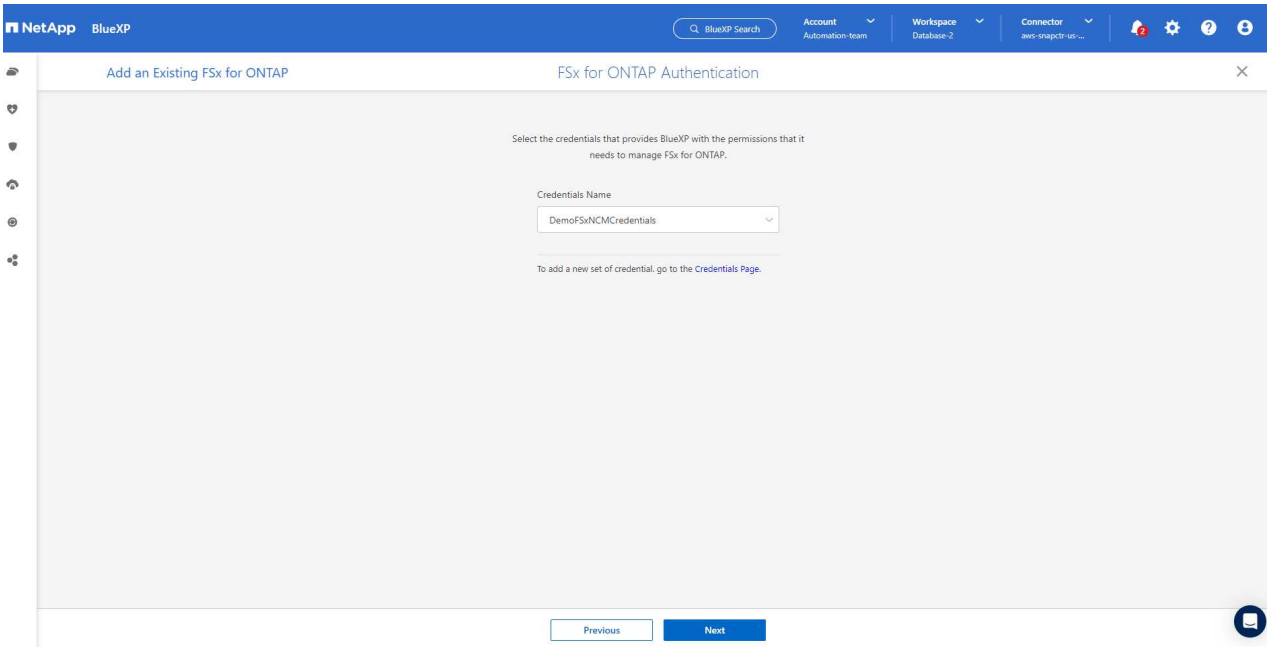
1. Scegliere **Amazon Web Services** come posizione.



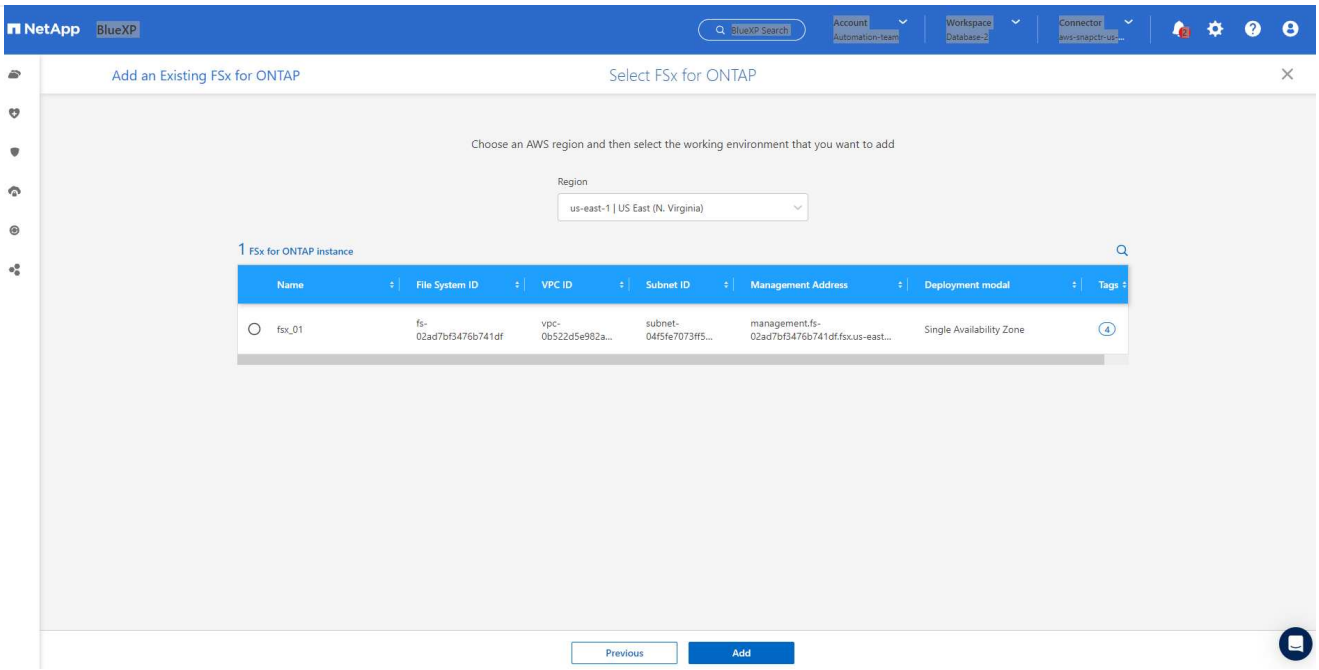
1. Fai clic su **Scopri esistente** accanto a **Amazon FSX per ONTAP**.



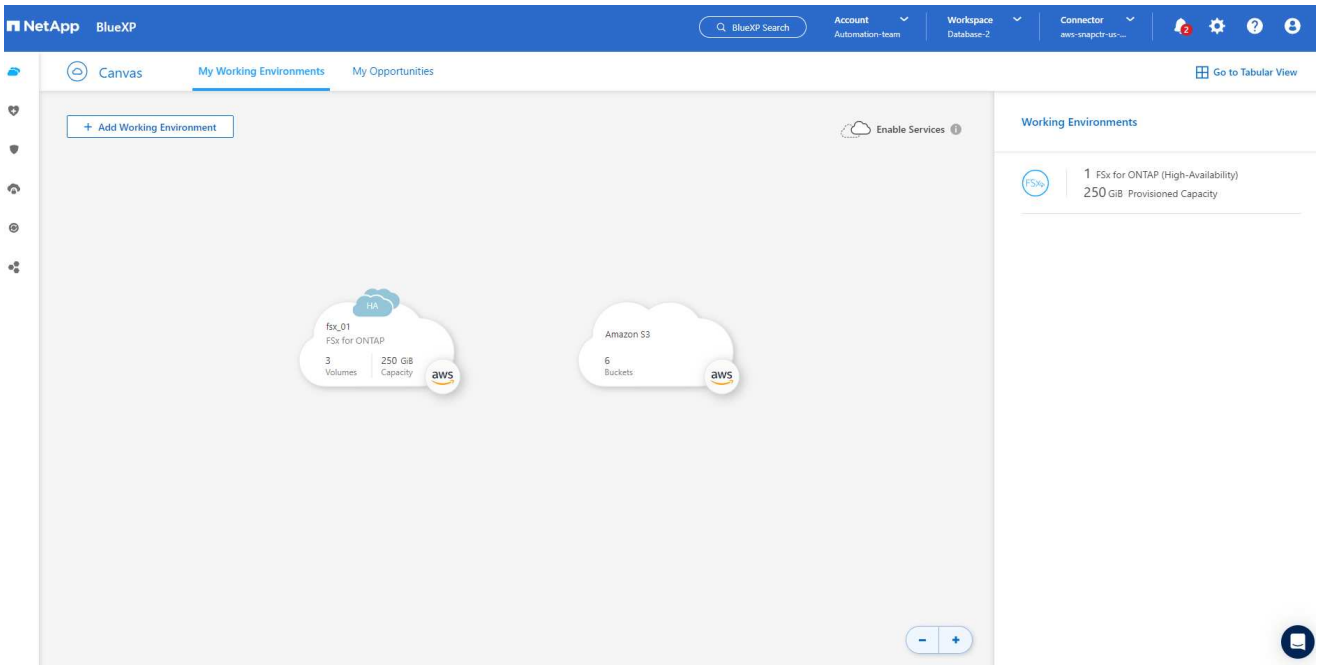
1. Seleziona il **Nome credenziali** creato nella sezione precedente per assegnare ad BlueXP le autorizzazioni necessarie per gestire FSX per ONTAP. Se non sono state aggiunte credenziali, è possibile aggiungerle dal menu **Settings** (Impostazioni) nell'angolo superiore destro della console BlueXP.



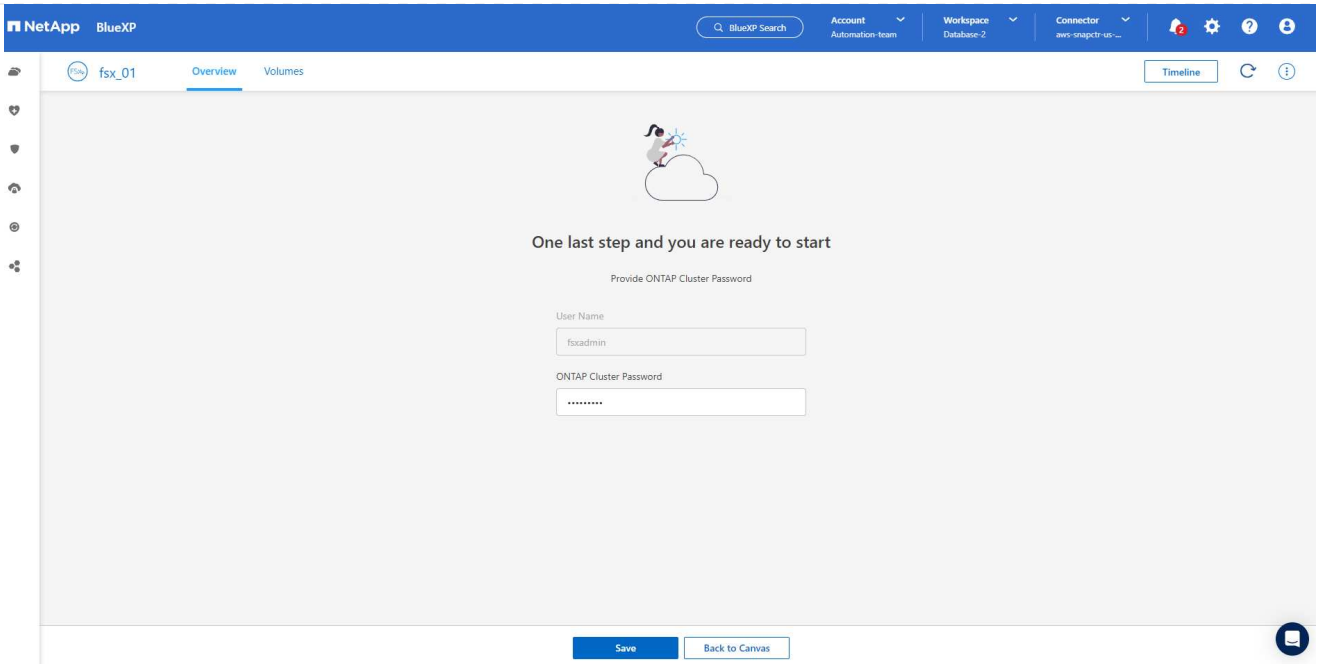
2. Scegliere la regione AWS in cui viene implementato Amazon FSX per ONTAP, selezionare il cluster FSX che ospita il database Oracle e fare clic su Aggiungi.



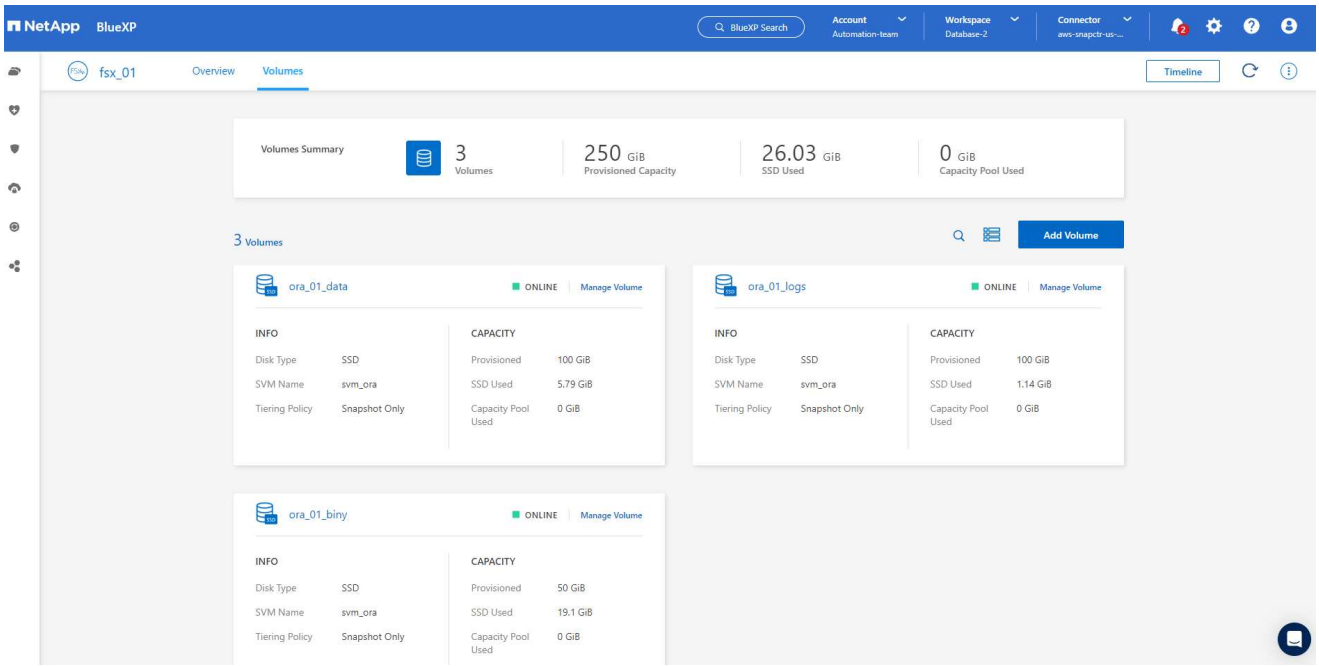
1. L’istanza scoperta di Amazon FSX per ONTAP viene ora visualizzata nell’ambiente di lavoro.



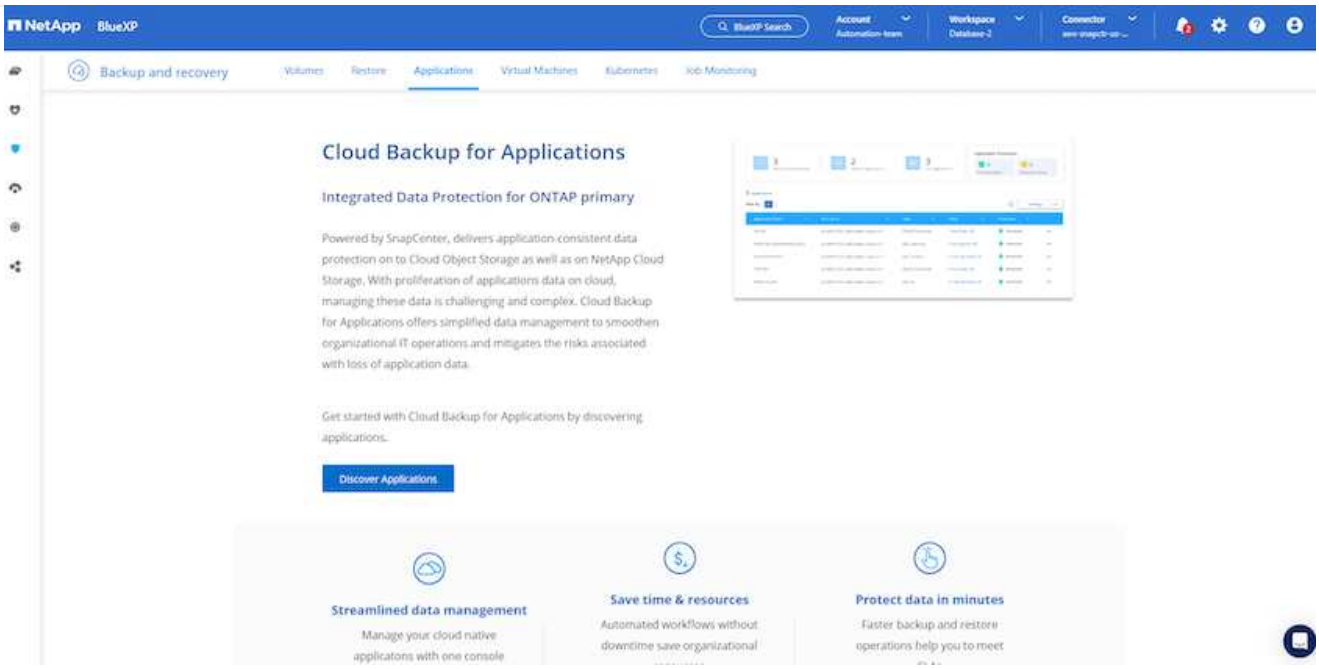
1. È possibile accedere al cluster FSX con le credenziali dell’account fsxadmin.



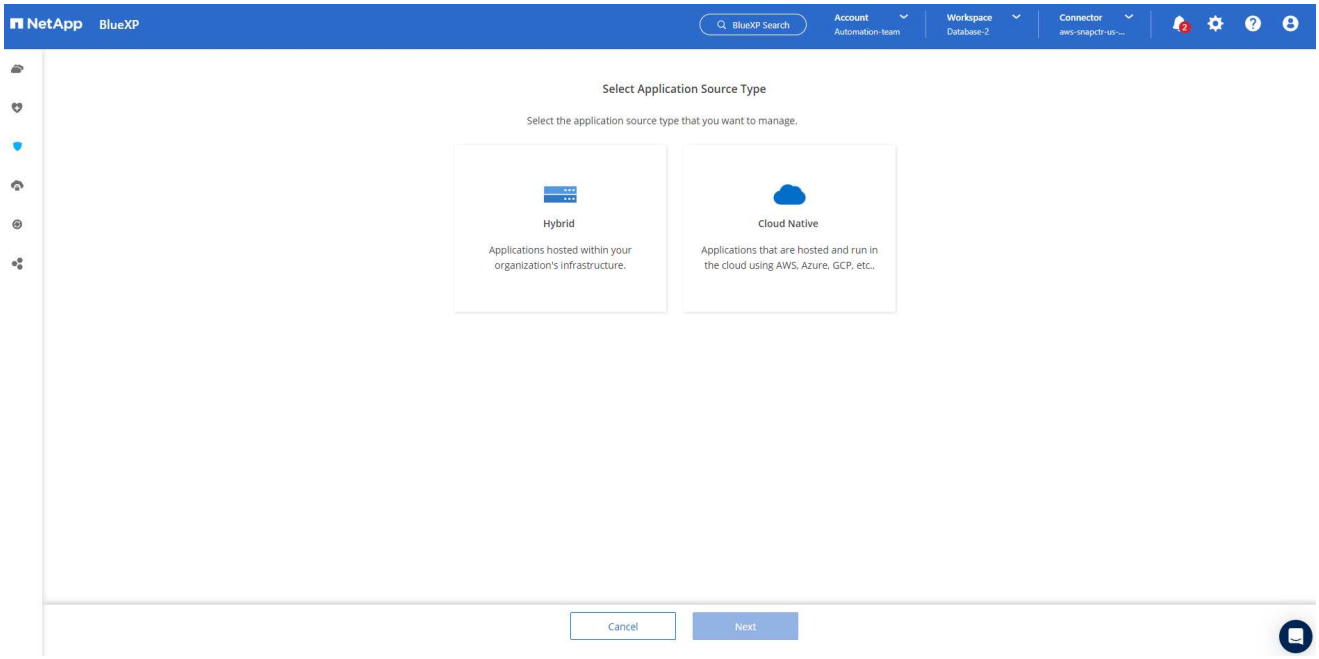
1. Dopo aver effettuato l'accesso ad Amazon FSX per ONTAP, esaminare le informazioni di storage del database (ad esempio i volumi del database).



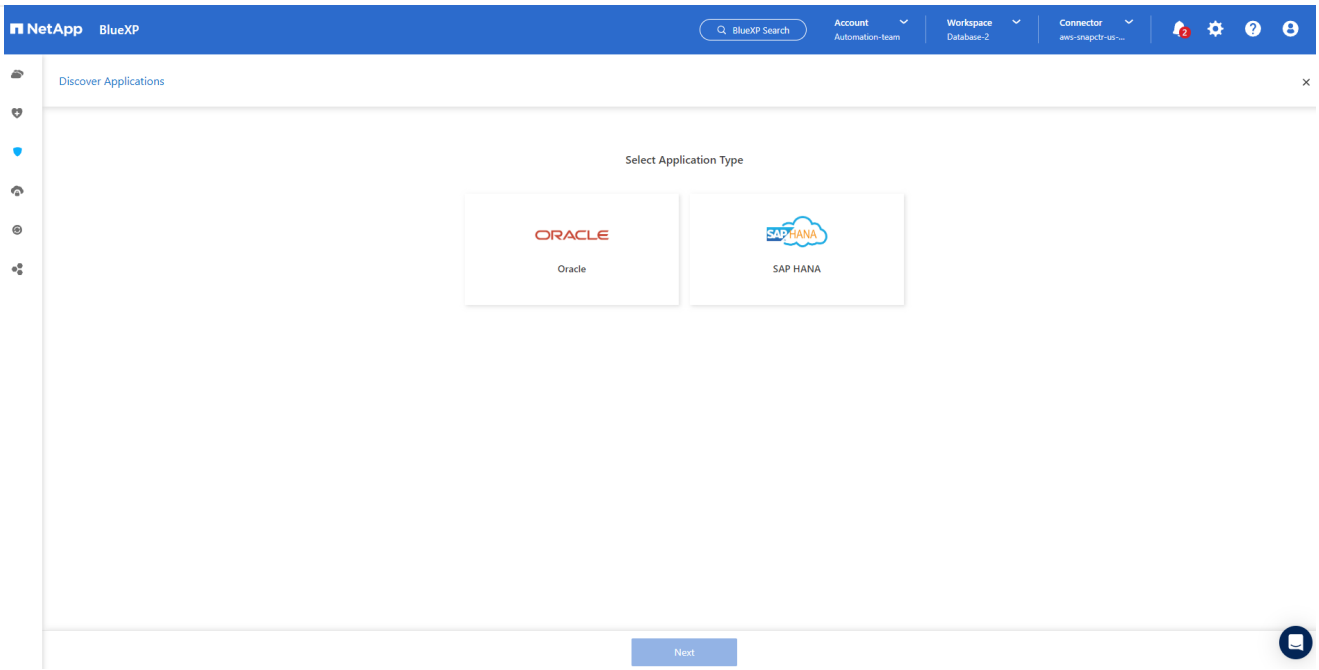
1. Dalla barra laterale sinistra della console, passare il mouse sull'icona di protezione, quindi fare clic su **protezione** > **applicazioni** per aprire la pagina di avvio delle applicazioni. Fare clic su **Scopri applicazioni**.



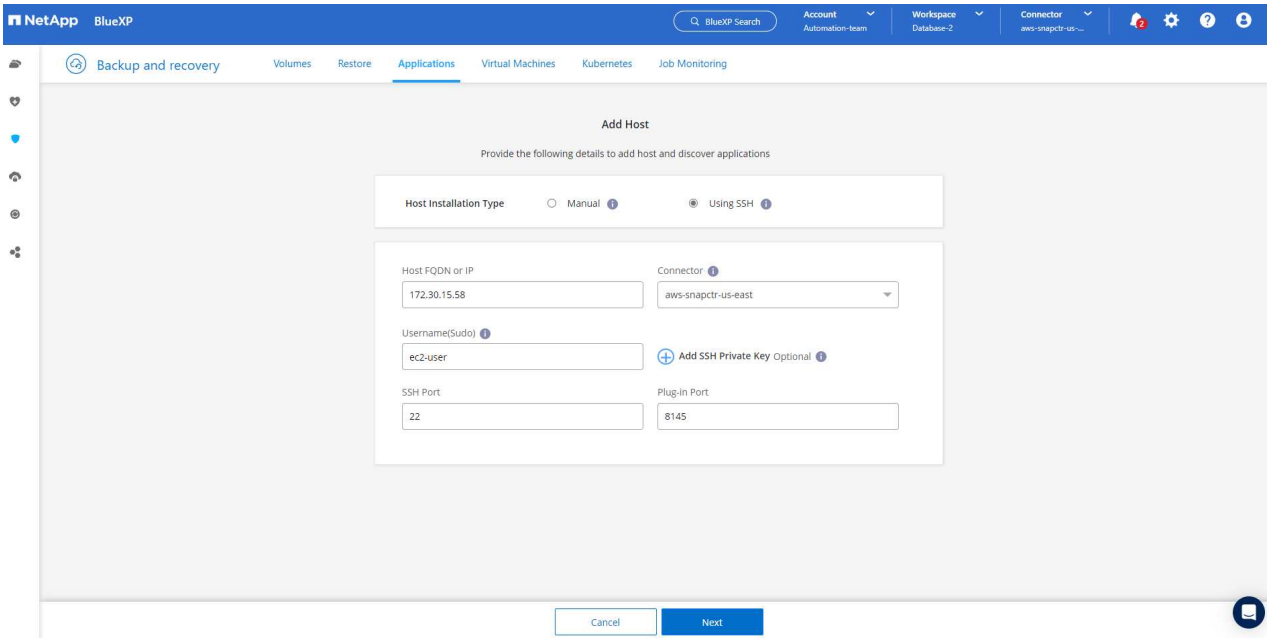
1. Selezionare **Cloud Native** come tipo di origine dell'applicazione.



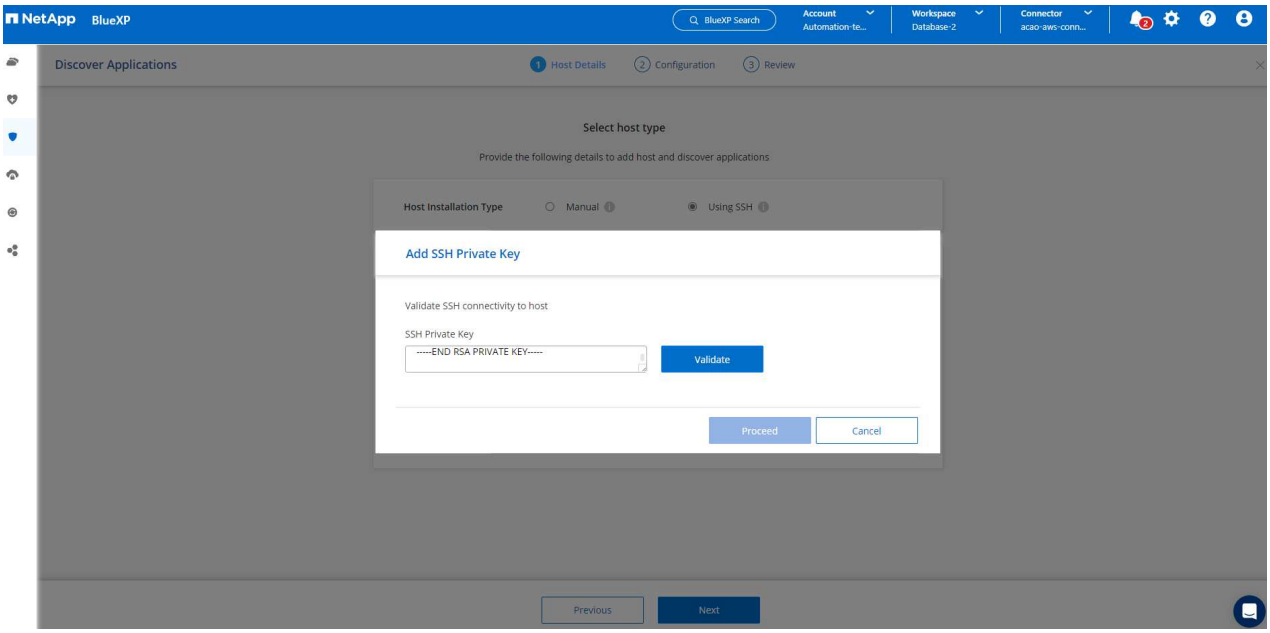
1. Scegliere **Oracle** come tipo di applicazione.



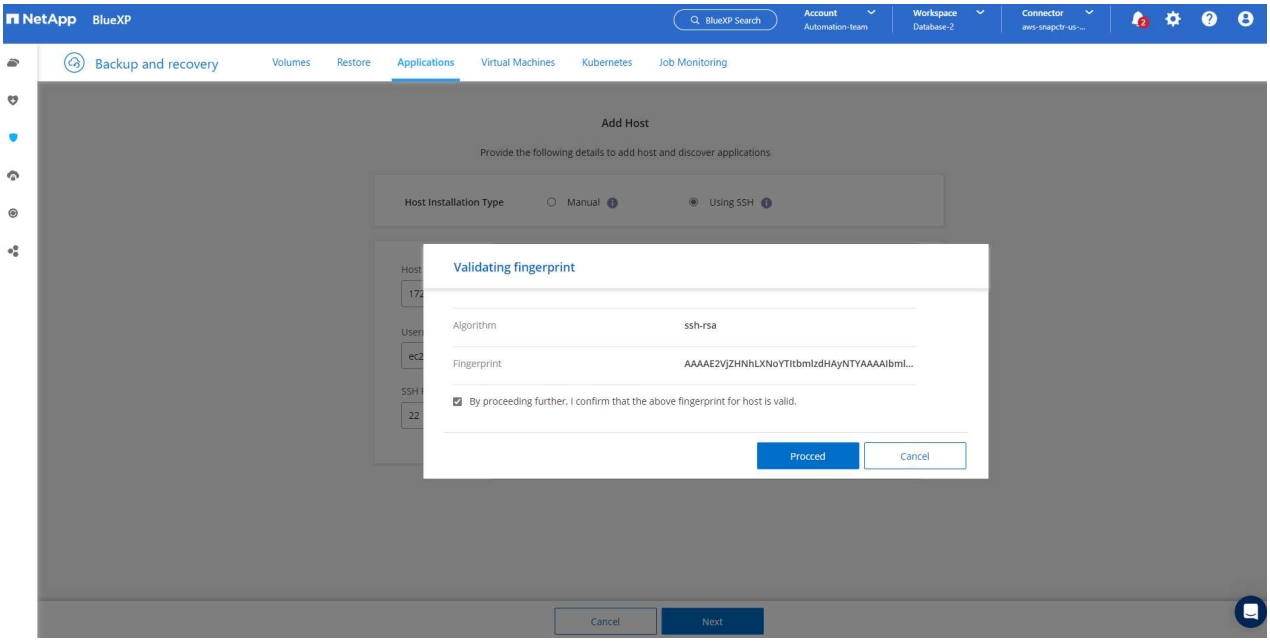
1. Inserisci i dettagli dell'host dell'applicazione AWS EC2 Oracle. Scegliere **utilizzo di SSH** come **tipo di installazione host** per l'installazione di un plug-in e il rilevamento del database. Quindi, fare clic su **Aggiungi chiave privata SSH**.



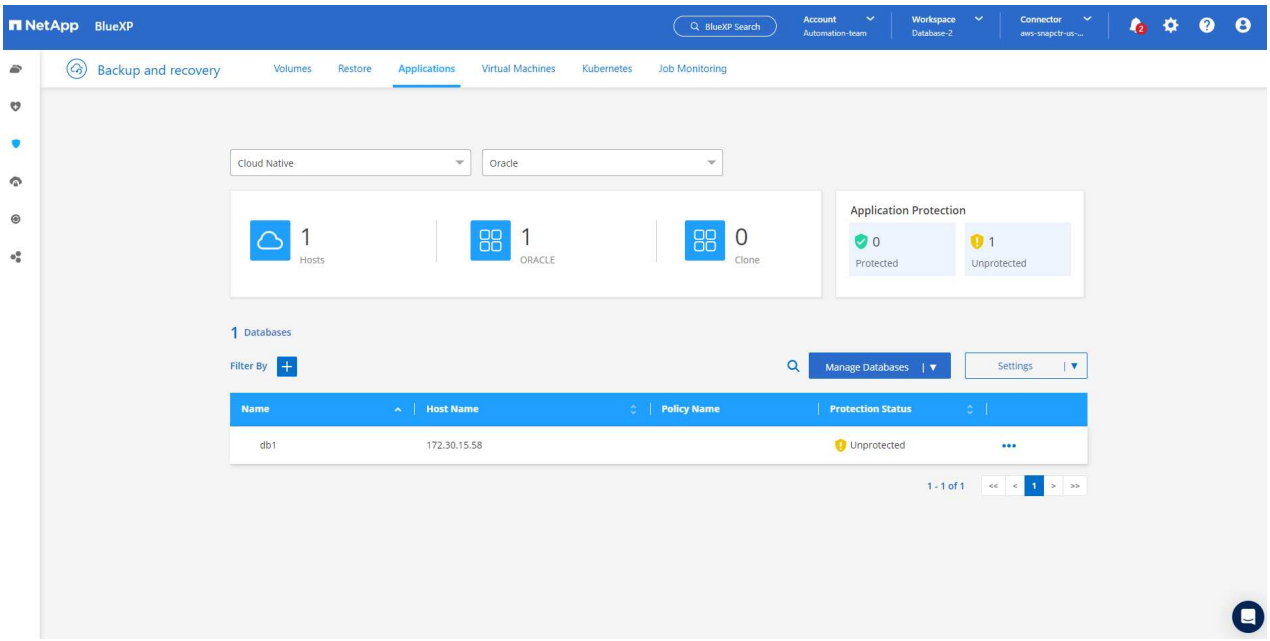
2. Incollare la chiave SSH per EC2 utenti per l'host database EC2 e fare clic su **convalida** per continuare.



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



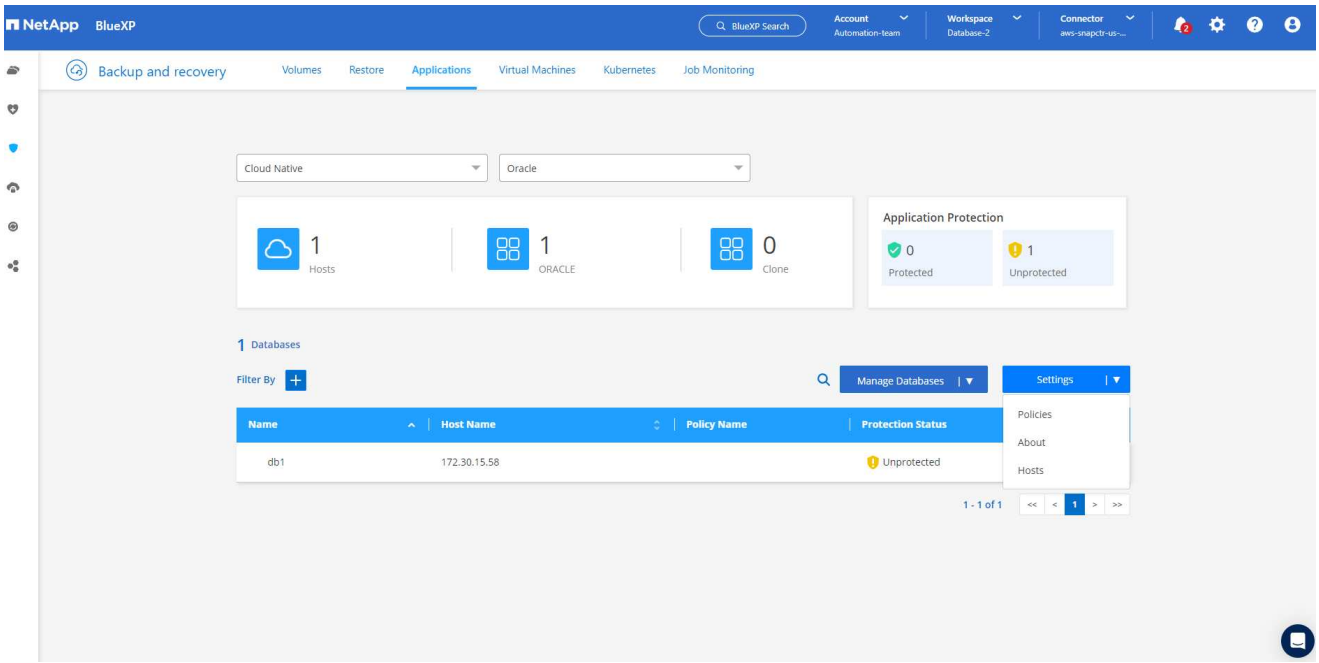
4. Fare clic su **Next** (Avanti) per installare un plug-in del database Oracle e scoprire i database Oracle sull'host EC2. I database rilevati vengono aggiunti ad **applicazioni**. Il database **Stato protezione** viene visualizzato come **non protetto** quando viene rilevato inizialmente.



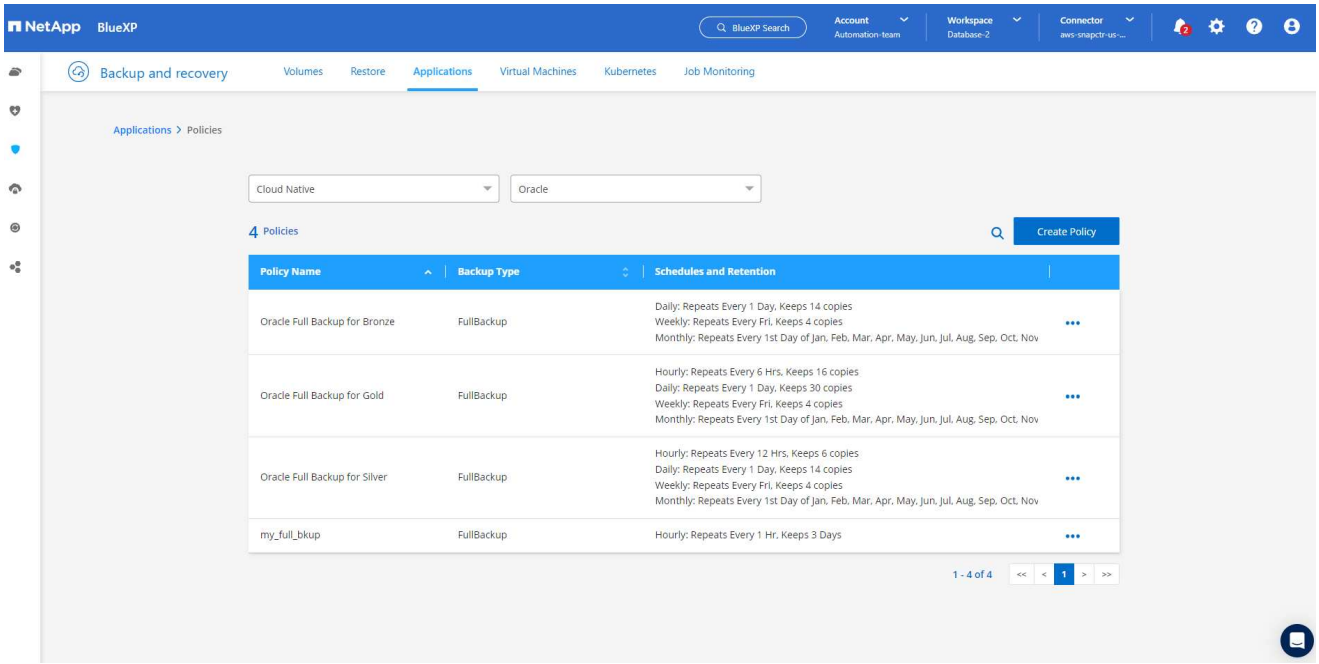
Questa operazione completa la configurazione iniziale dei servizi SnapCenter per Oracle. Nelle tre sezioni successive di questo documento vengono descritte le operazioni di backup, ripristino e clonazione del database Oracle.

Backup del database Oracle

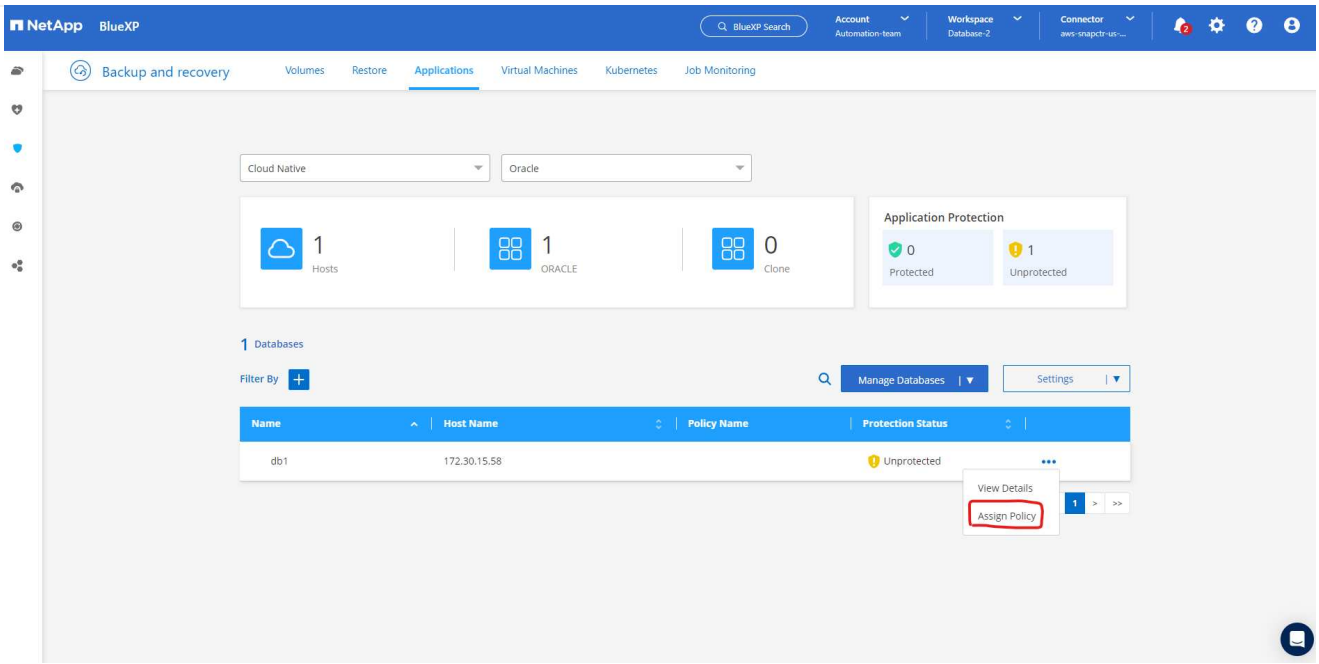
1. Fare clic sui tre punti accanto al database **Protection Status** (Stato protezione), quindi fare clic su **Polices** (Criteri) per visualizzare i criteri di protezione predefiniti del database che è possibile applicare per proteggere i database Oracle.



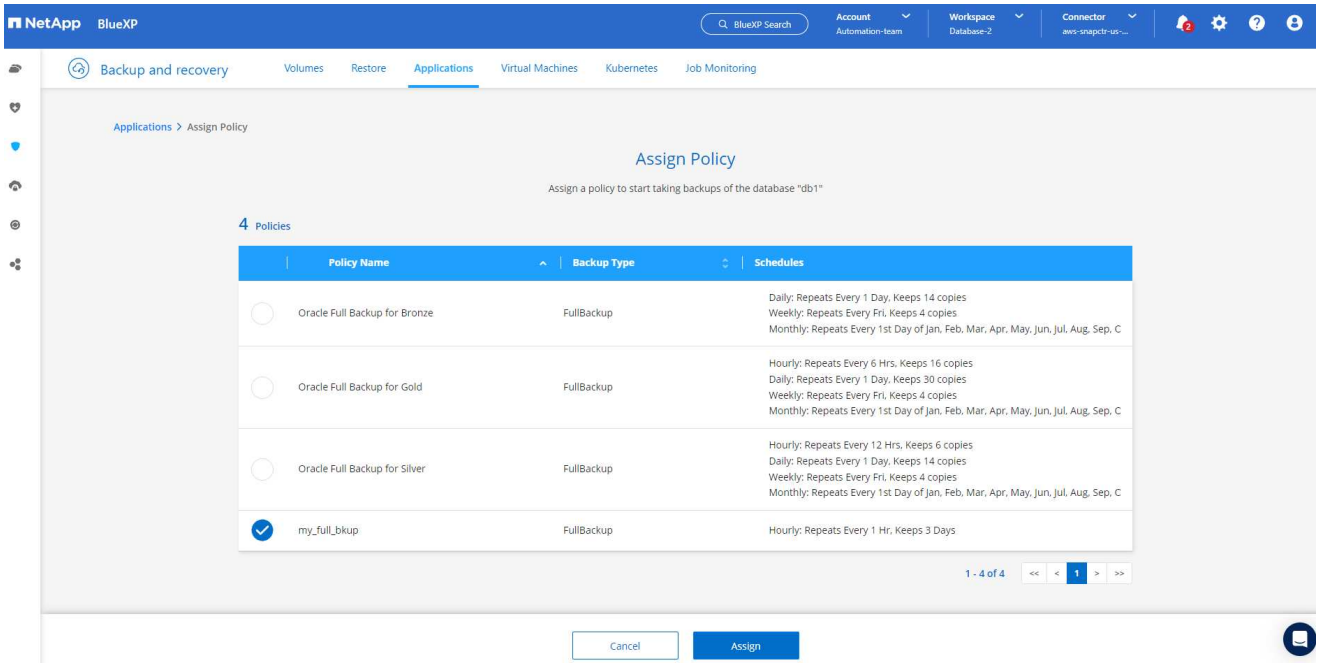
1. È inoltre possibile creare policy personalizzate con una frequenza di backup personalizzata e una finestra di conservazione dei dati di backup.



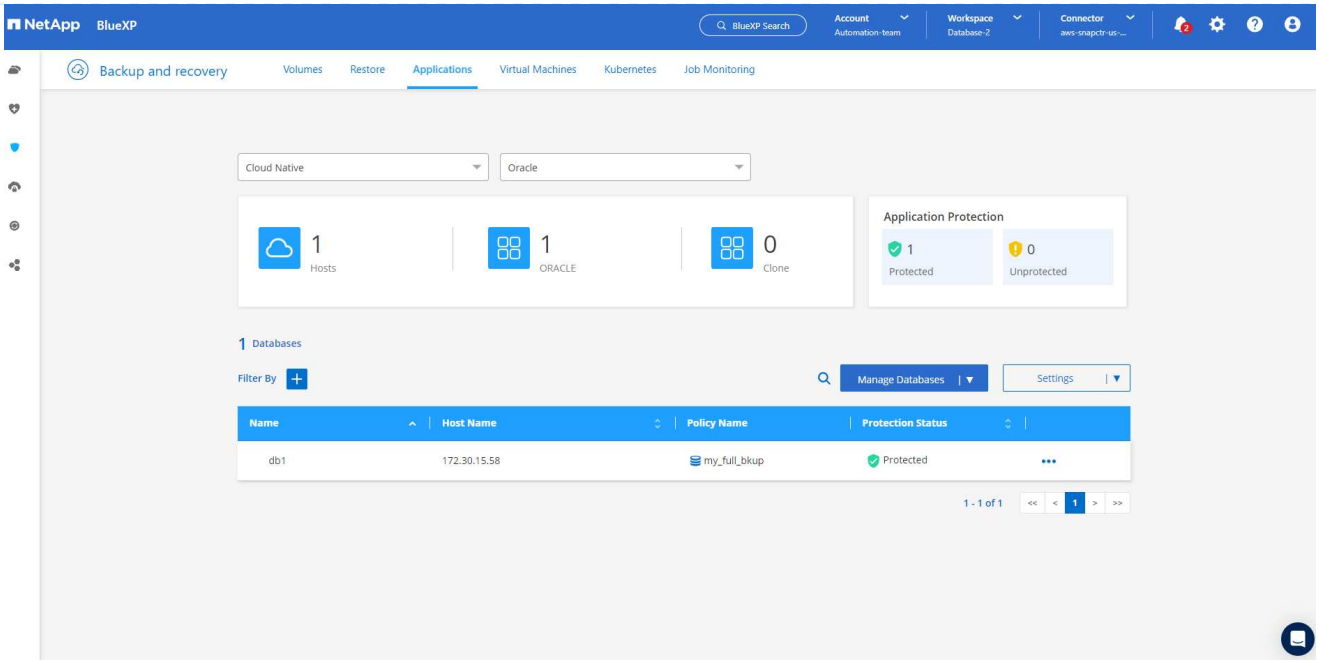
1. Quando si è soddisfatti della configurazione dei criteri, è possibile assegnare i criteri scelti per proteggere il database.



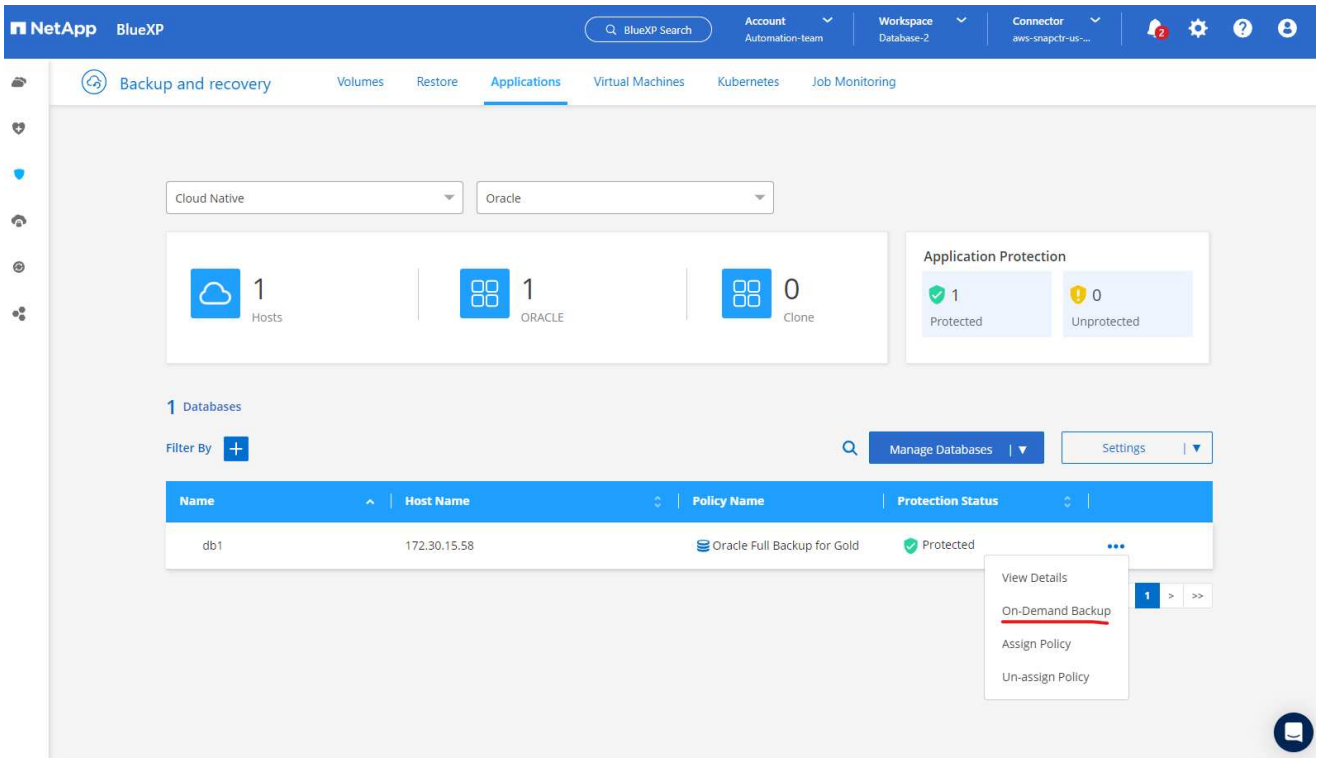
1. Scegliere il criterio da assegnare al database.



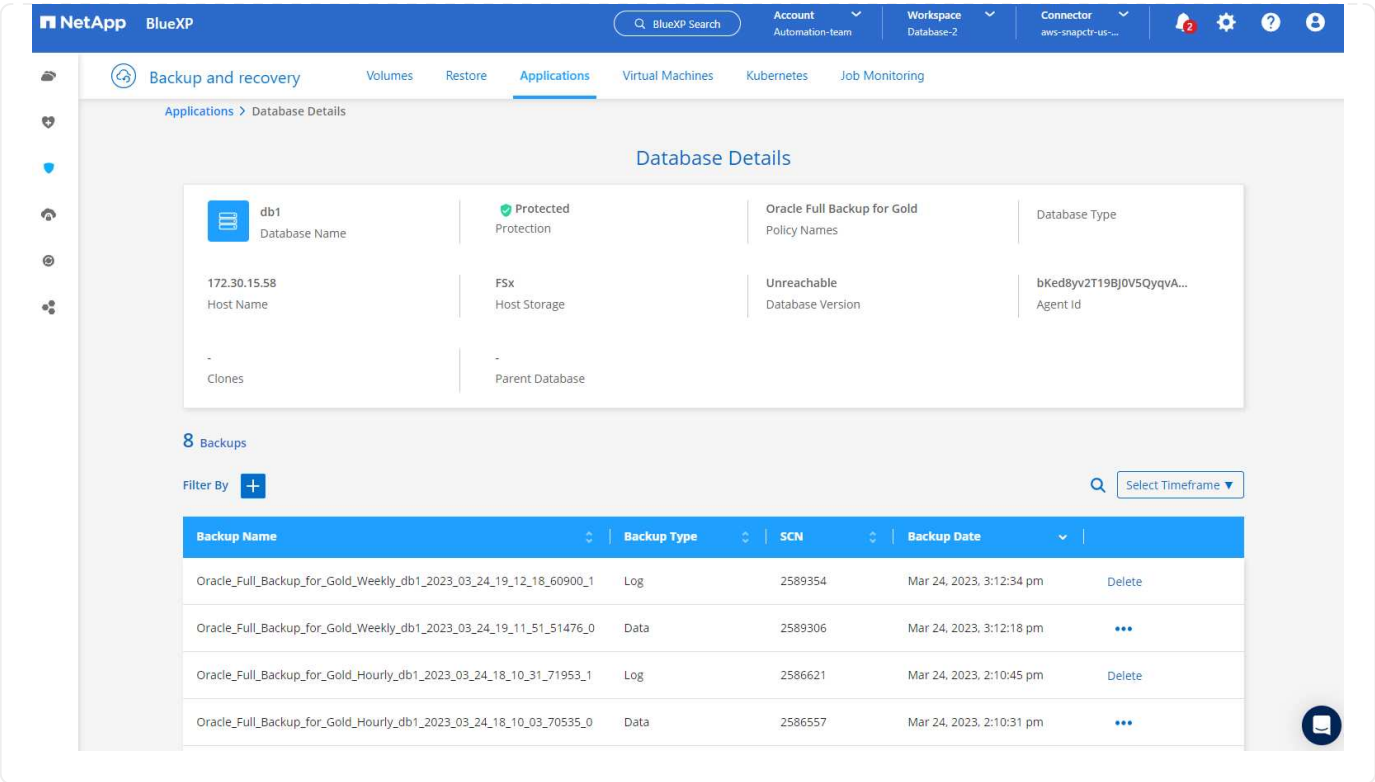
1. Una volta applicato il criterio, lo stato di protezione del database è cambiato in **Protected** con un segno di spunta verde.



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.

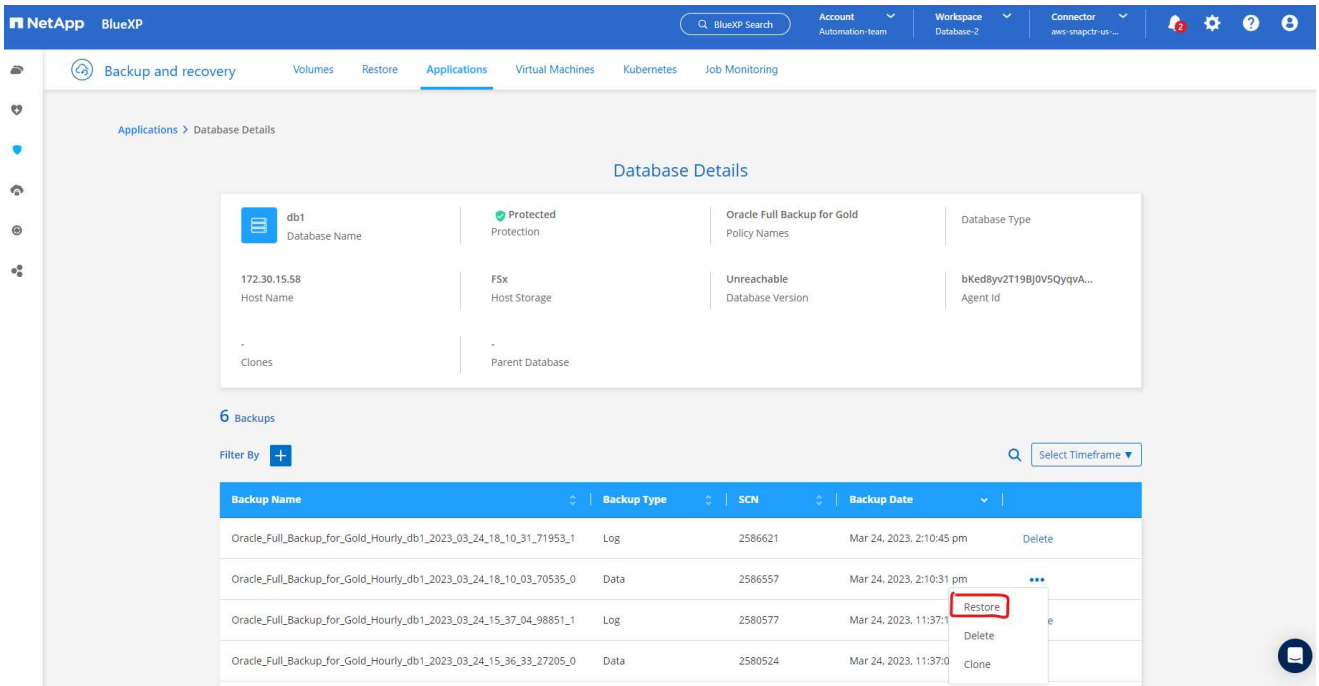


1. I dettagli dei backup del database possono essere visualizzati facendo clic su **View Details** (Visualizza dettagli) dall'elenco dei menu. Tra cui nome, tipo di backup, SCN e data di backup. Un set di backup copre un'istantanea sia per il volume di dati che per il volume di log. Lo snapshot di un 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.

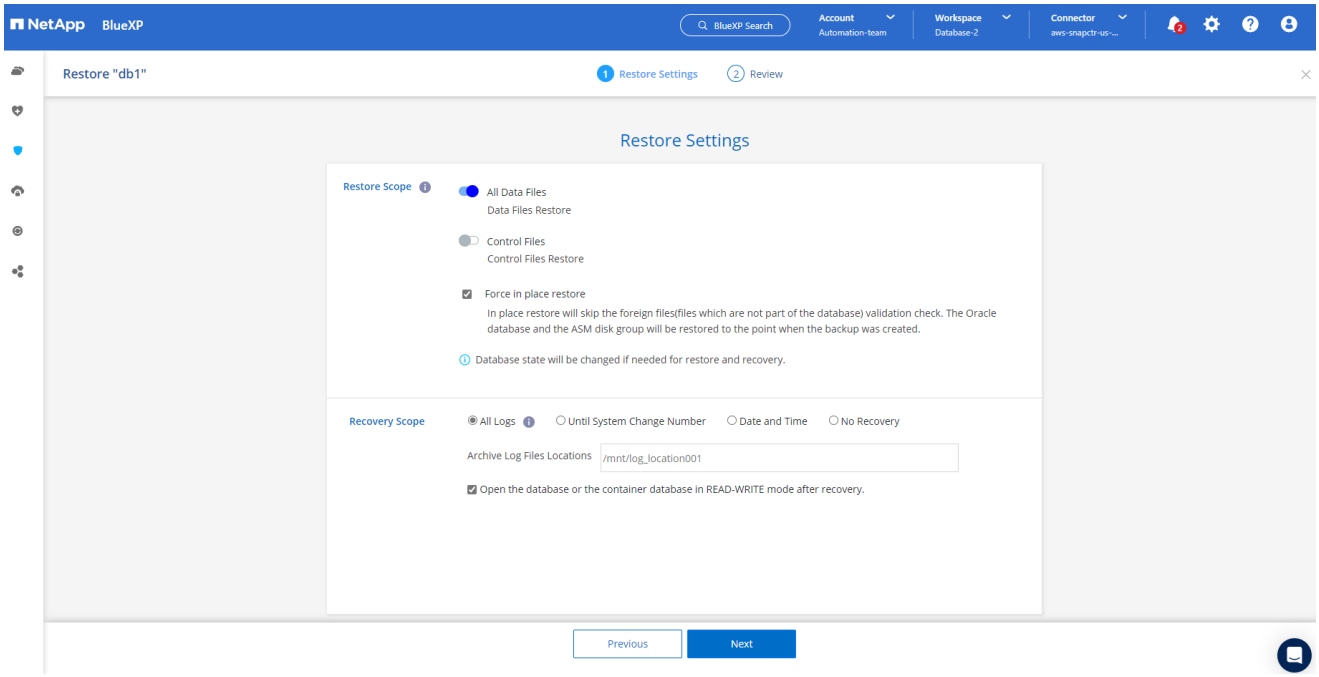


Ripristino e ripristino del database Oracle

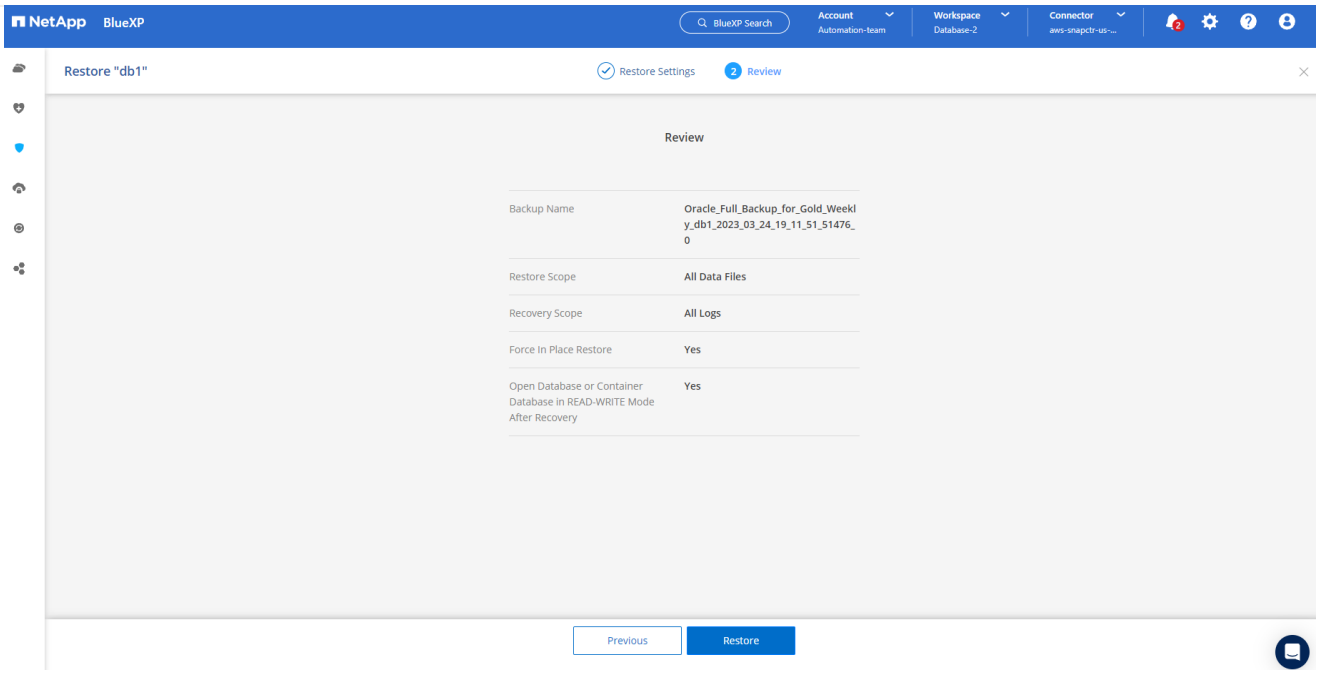
1. Per un ripristino del database, scegliere il backup corretto, in base al tempo di backup o SCN. Fare clic sui tre punti del backup dei dati del database, quindi fare clic su **Restore** (Ripristina) per avviare il ripristino e il ripristino del database.



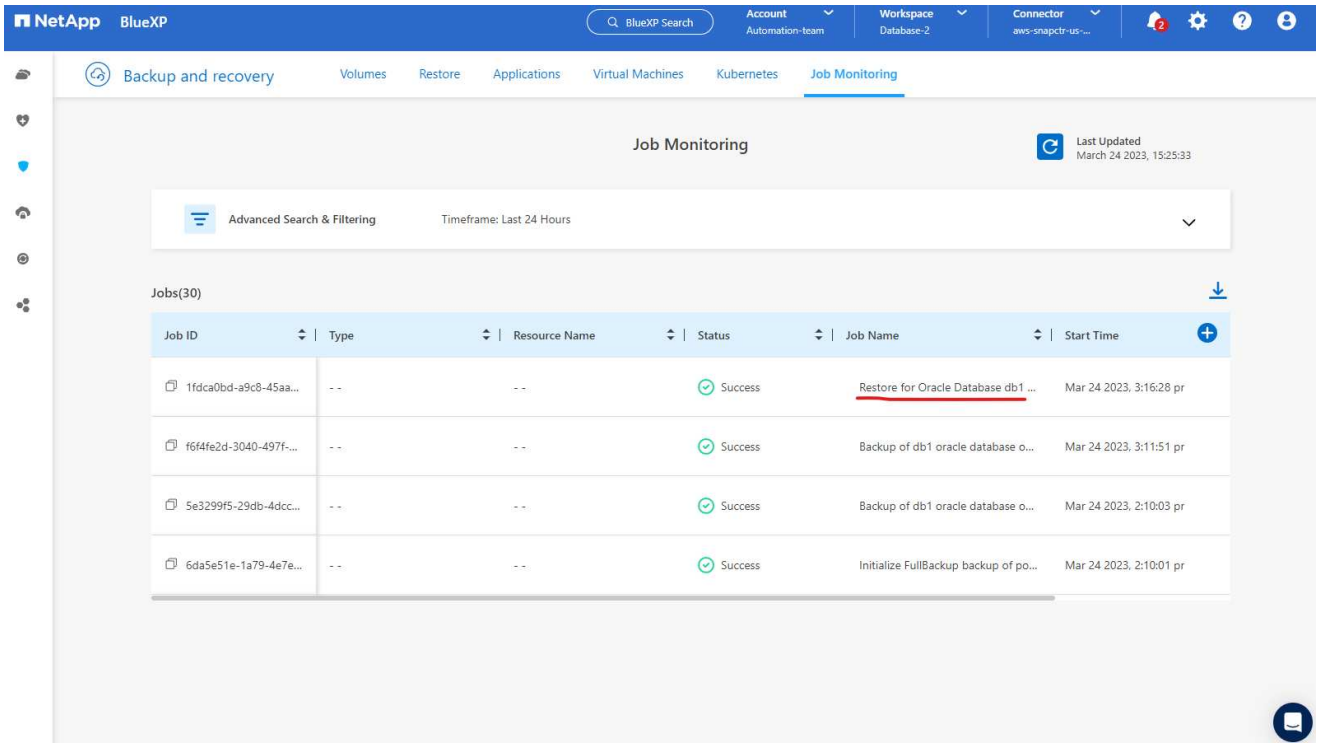
1. Scegliere l'impostazione di ripristino. Se dopo il backup non è cambiato nulla nella struttura fisica del database (ad esempio l'aggiunta di un file di dati o di un gruppo di dischi), è possibile utilizzare l'opzione **Force in Place restore** (Ripristino forzato in posizione), che in genere è più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

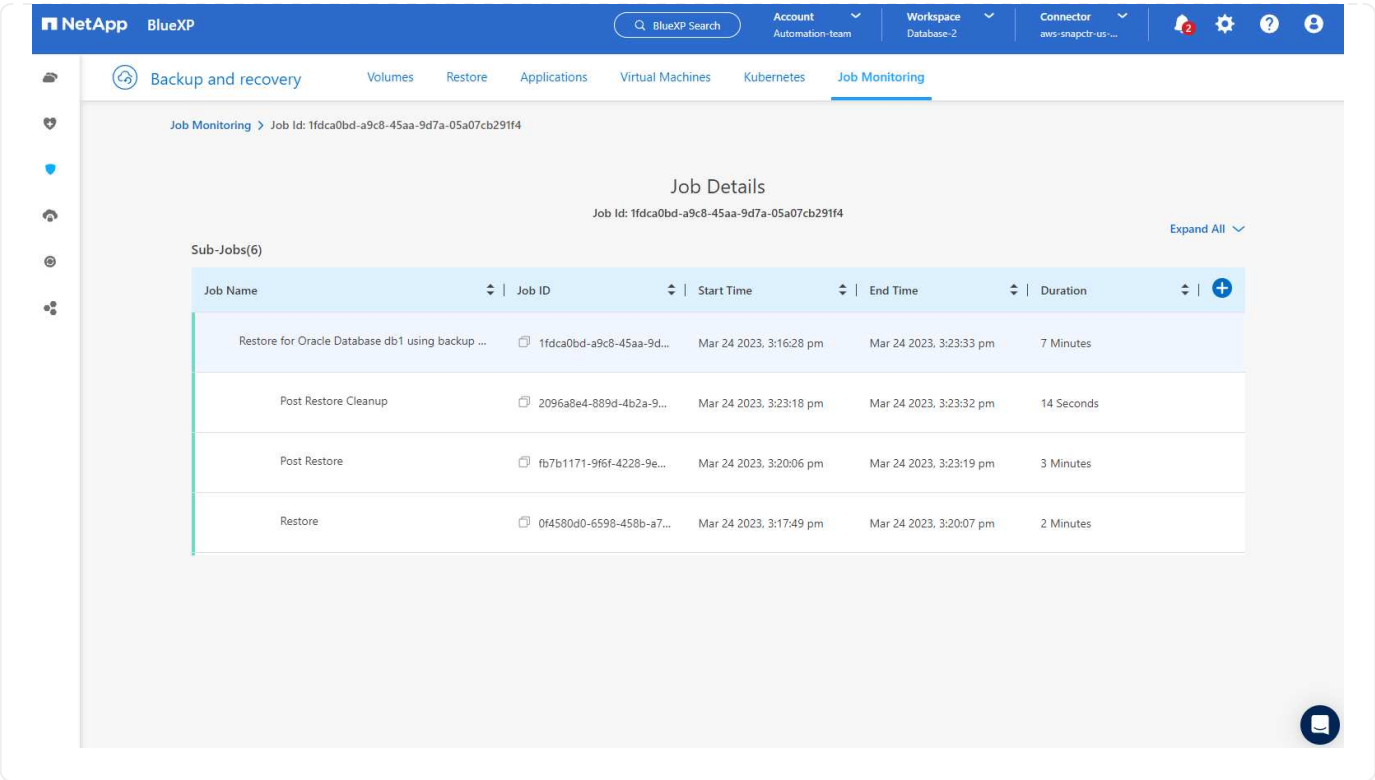


1. Esaminare e avviare il ripristino e il ripristino del database.



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

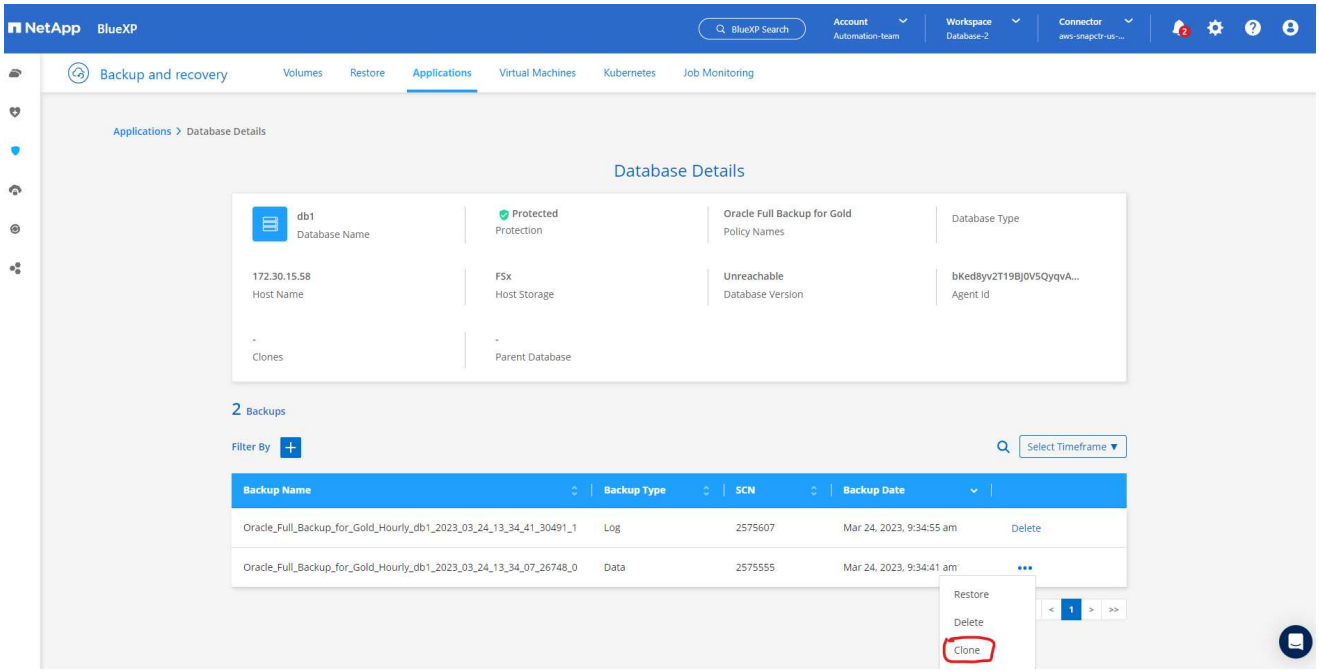




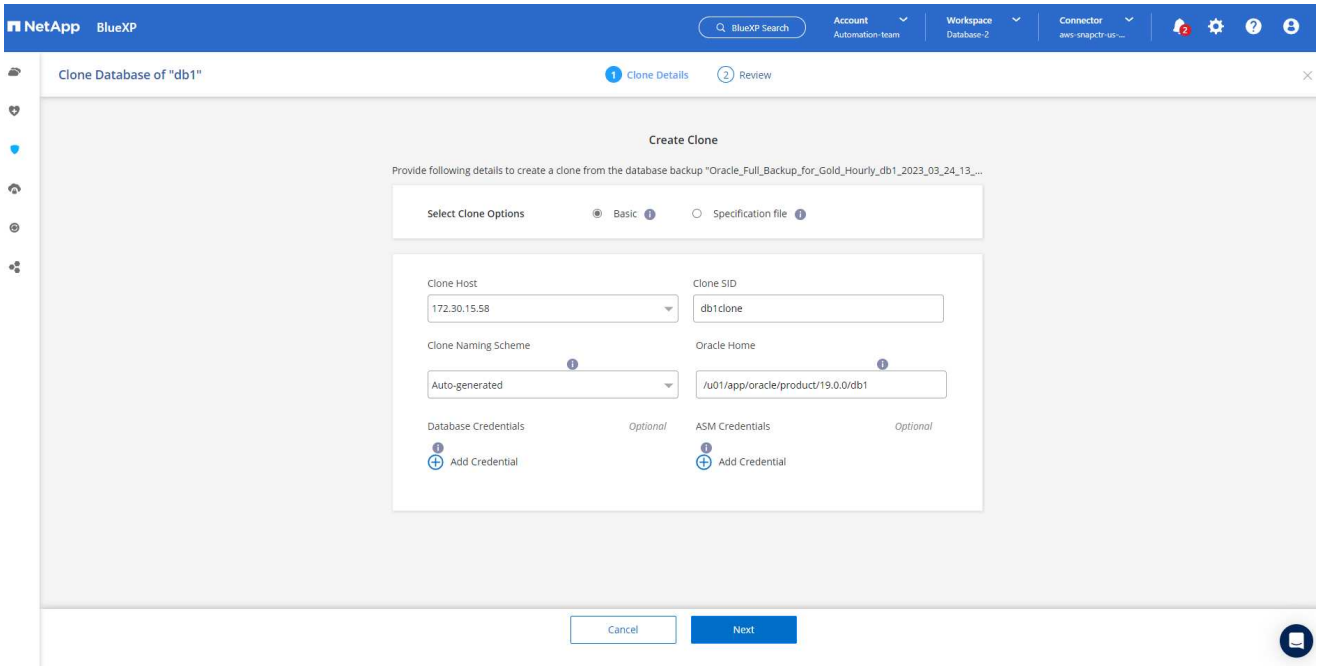
Clone del database Oracle

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

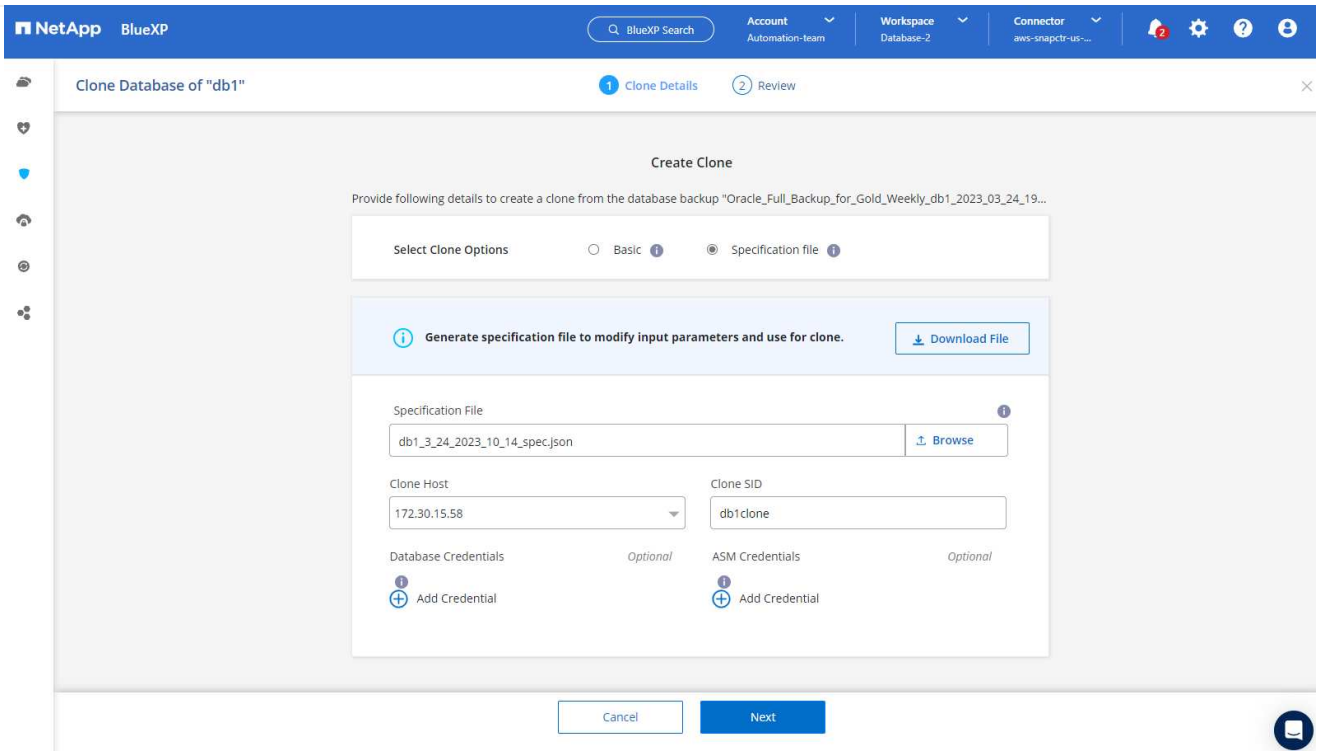
1. Selezionare la copia di backup del database corretta, fare clic sui tre punti per visualizzare il menu e scegliere l'opzione **Clone**.



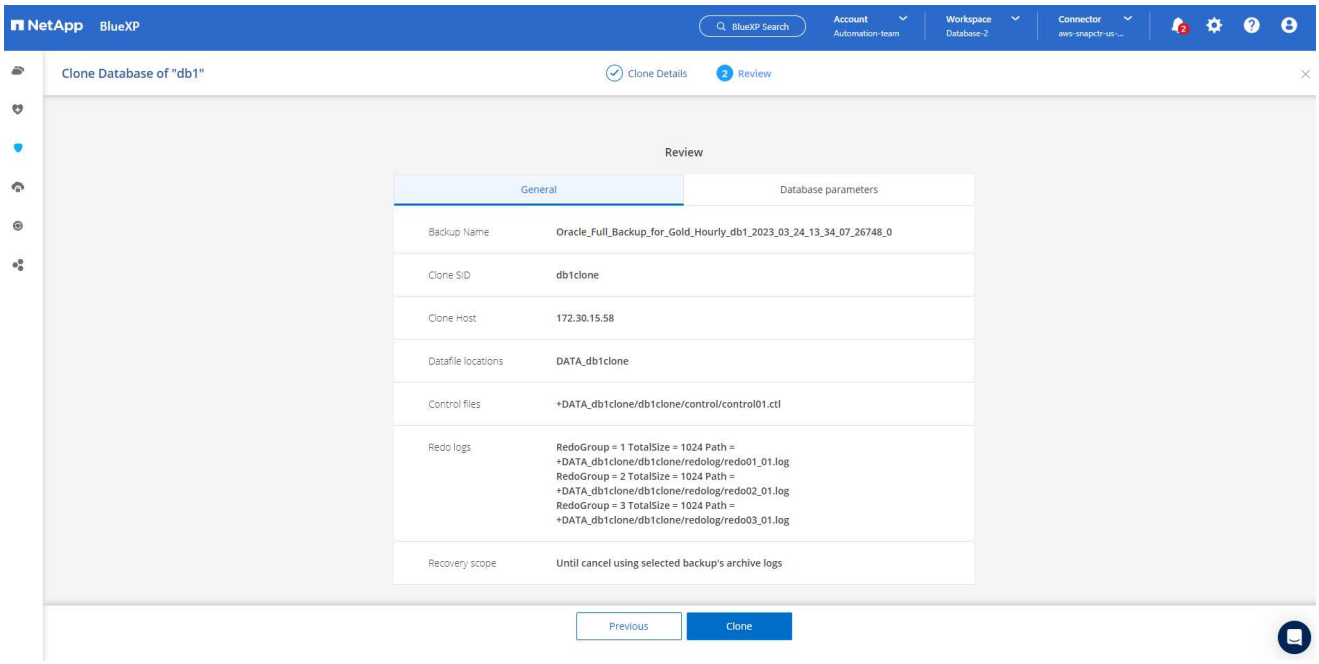
1. Selezionare l'opzione **Basic** se non è necessario modificare i parametri del database clonati.



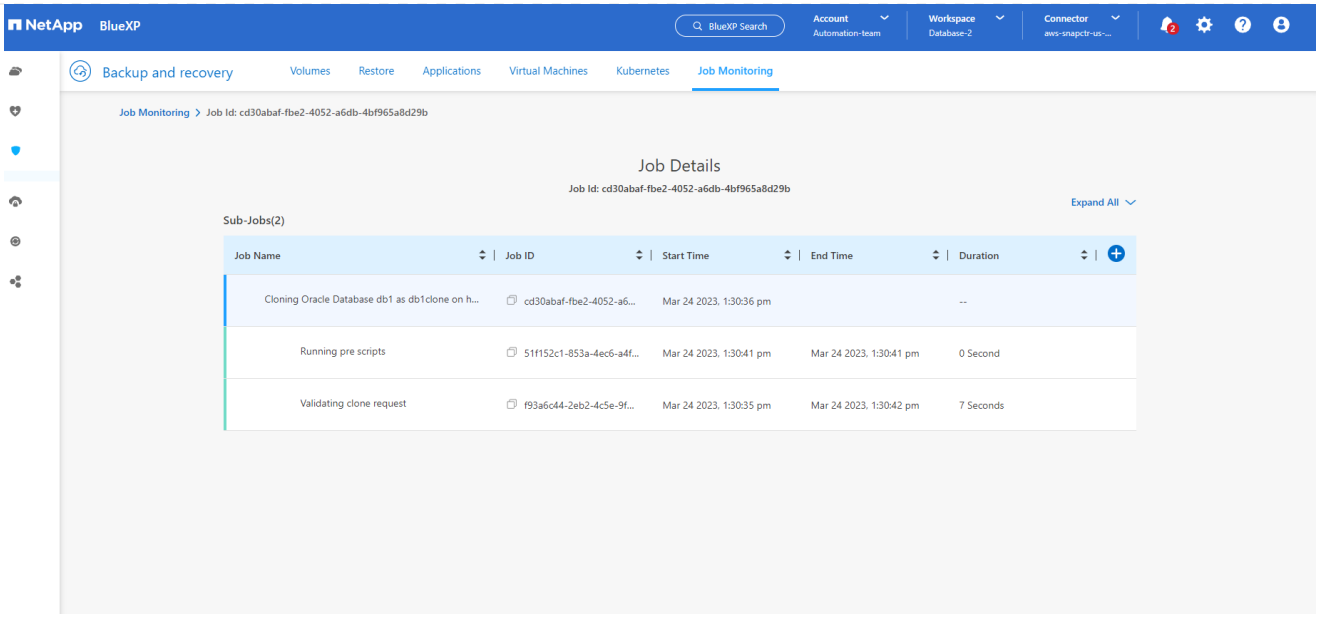
1. In alternativa, selezionare **Specification file**, che consente di scaricare il file init corrente, apportare modifiche e quindi caricarlo nuovamente nel lavoro.



1. Esaminare e avviare il lavoro.



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



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/o
                                                             racle/product/19.0.0
                                                             /db1,STABLE
ora.db1clone.db
      1        ONLINE  ONLINE       ip-172-30-15-58          Open,HOME=/u01/app/o
                                                             racle/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$database;

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"

- Documentazione di backup e ripristino BlueXP

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

- Amazon FSX per NetApp ONTAP

"https://aws.amazon.com/fsx/netapp-ontap/"

- Amazon EC2

https://aws.amazon.com/pm/ec2/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&s_kwcid=AL!4422!3!467723097970!e!!g!!aws%20ec2&ef_id=Cj0KCQiA54KfBhCKARIsAJzSrdqwQrghn6I71jiWzSeaT9Uh1-vY-VfhJixF-xnv5rWwn2S7RqZOTQ0aAh7eEALw_wcB:G:s&s_kwcid=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

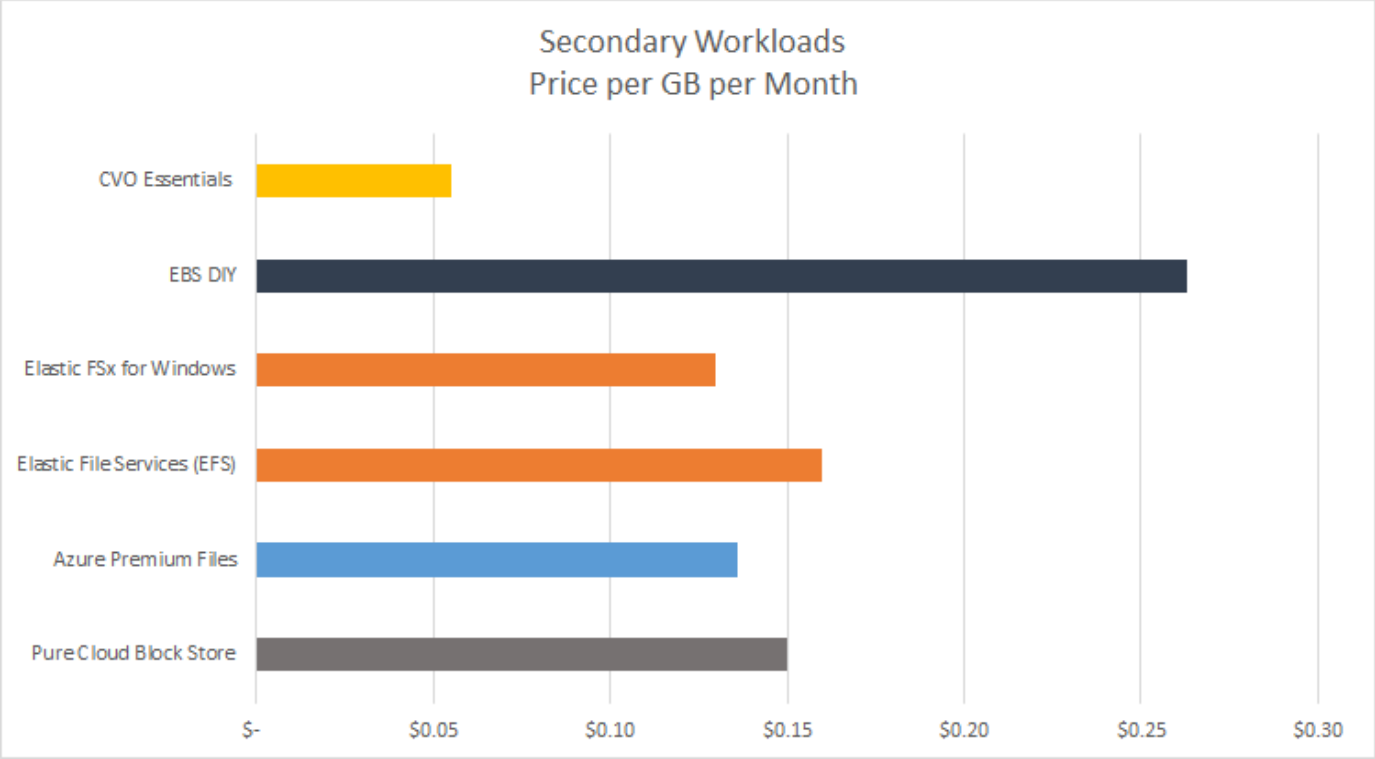
Oggi, molti database aziendali risiedono ancora in data center aziendali privati per motivi di performance, sicurezza e/o altro. Questa soluzione di database per il cloud ibrido consente alle aziende di gestire i propri database primari on-site utilizzando un cloud pubblico per le operazioni di sviluppo/test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

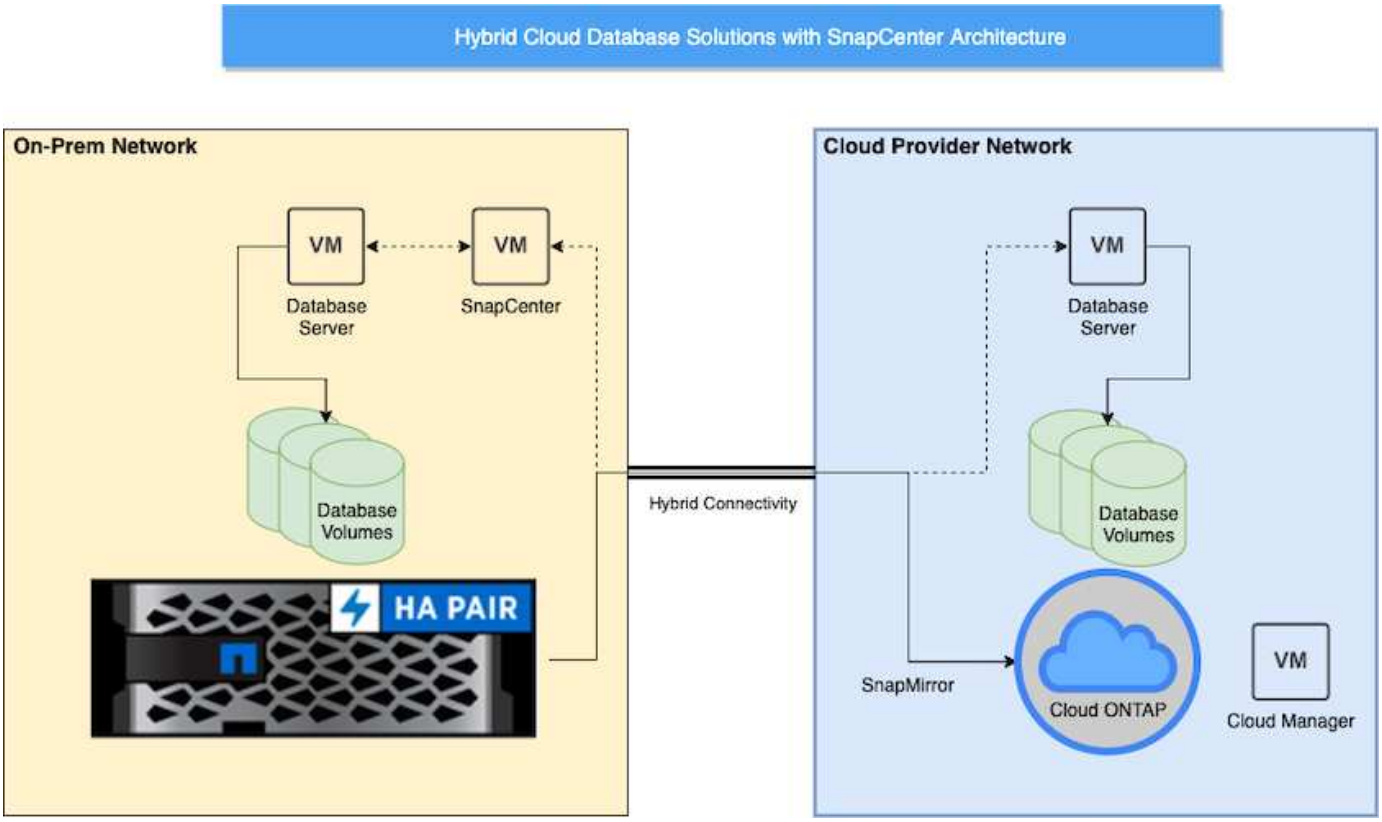
- "Backup di un database Oracle su un cloud ibrido utilizzando SnapCenter"
- "SnapCenter - Clona SVILUPPO/TEST su cloud AWS per un database Oracle"

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.

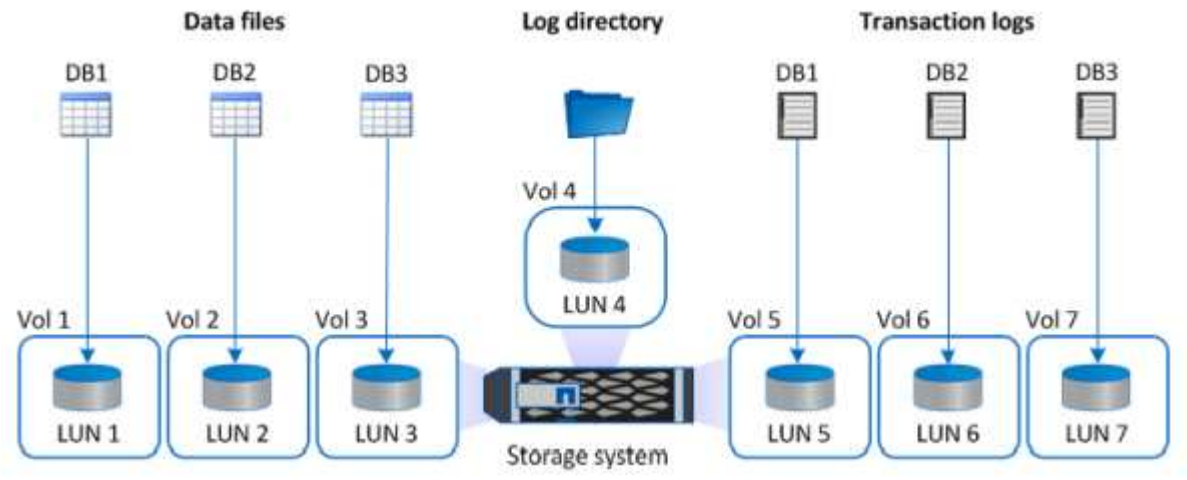
- **Implementazione ha o istanza singola.** l'implementazione ha fornisce ridondanza in caso di guasto di un singolo server di istanza SnapCenter.
- **Risoluzione del nome.** il DNS deve essere configurato sul server SnapCenter per risolvere tutti gli host di database e sulla SVM di storage per la ricerca 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.

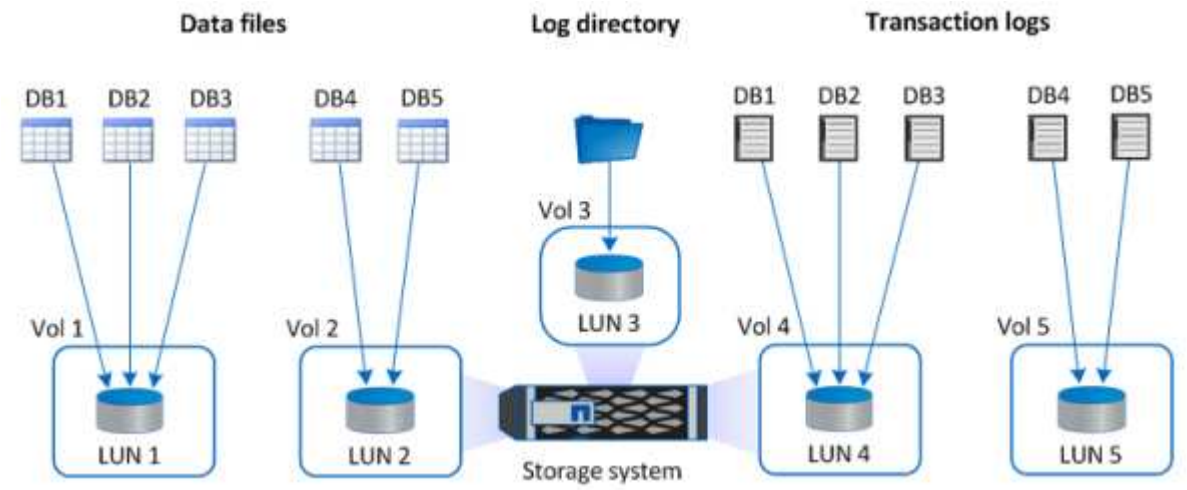
Configurazione dello storage del server di database on-premise

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.



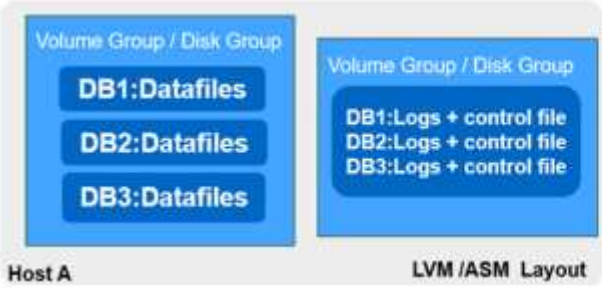
> La directory Log è dedicata a SnapCenter per eseguire il rollup del log delle transazioni per il ripristino del database. Per un database di grandi dimensioni, è possibile allocare più LUN a un volume per migliorare le performance.

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

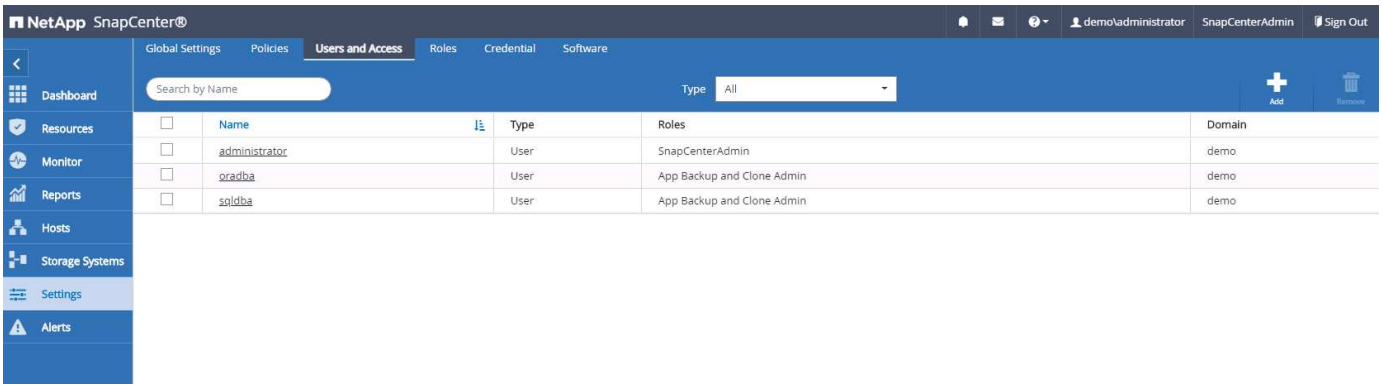
1. Configurare l'utente amministratore del database in SnapCenter

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.

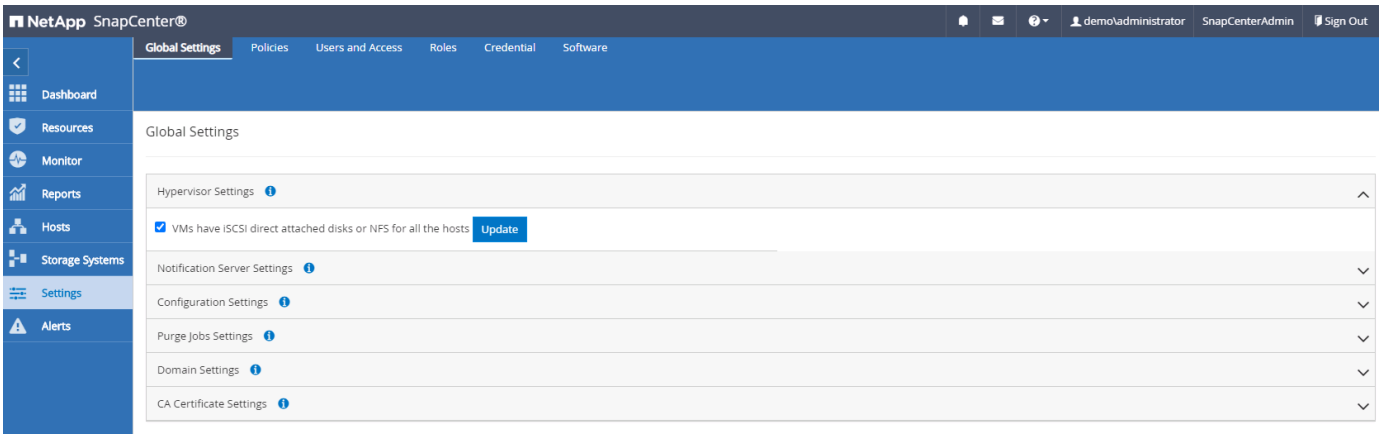
3. Installazione del plug-in host SnapCenter

> 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

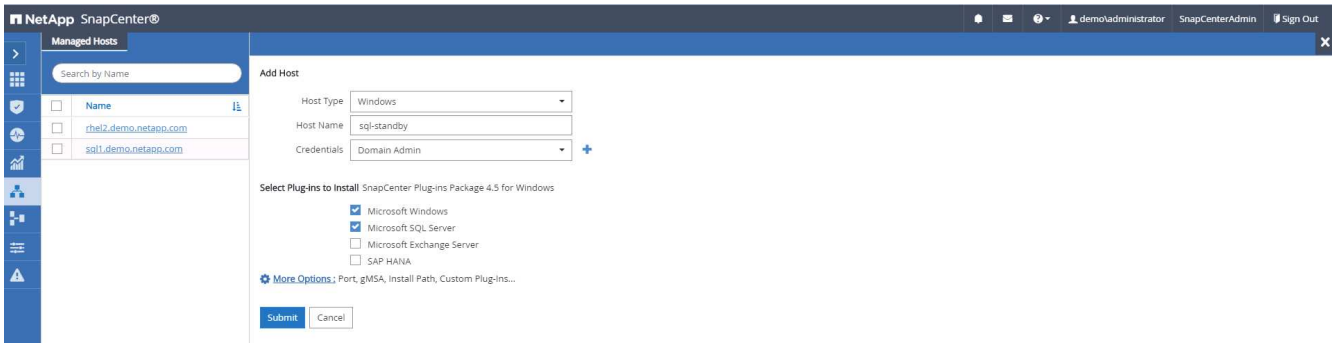
Accedere a Impostazioni > Impostazioni globali. Selezionare "VM con iSCSI direct attached disks o NFS per tutti gli host" in Impostazioni hypervisor e fare clic su Aggiorna.



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

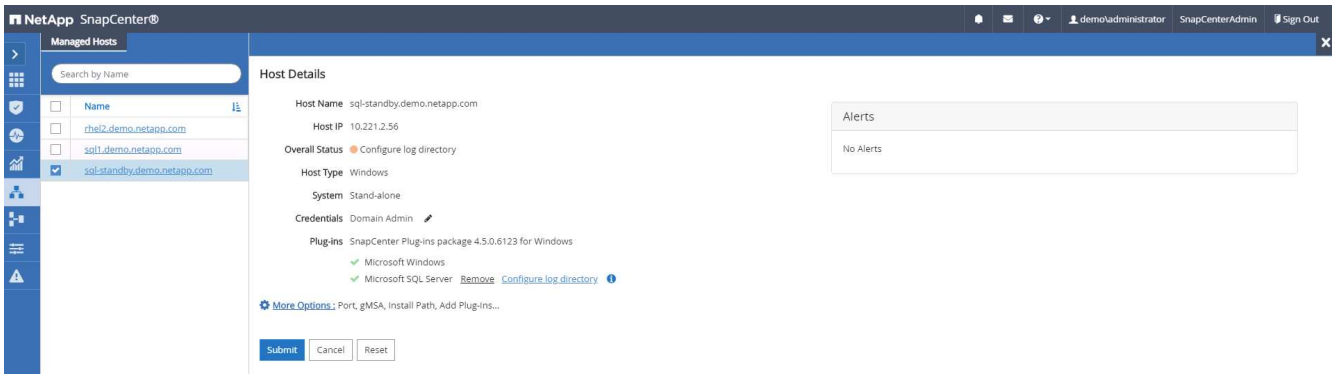
1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda host dal menu a sinistra, quindi fare clic su Add (Aggiungi) per aprire il flusso di lavoro Add host (Aggiungi host).
3. Scegliere Windows come tipo di host; il nome host può essere un nome host o un indirizzo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

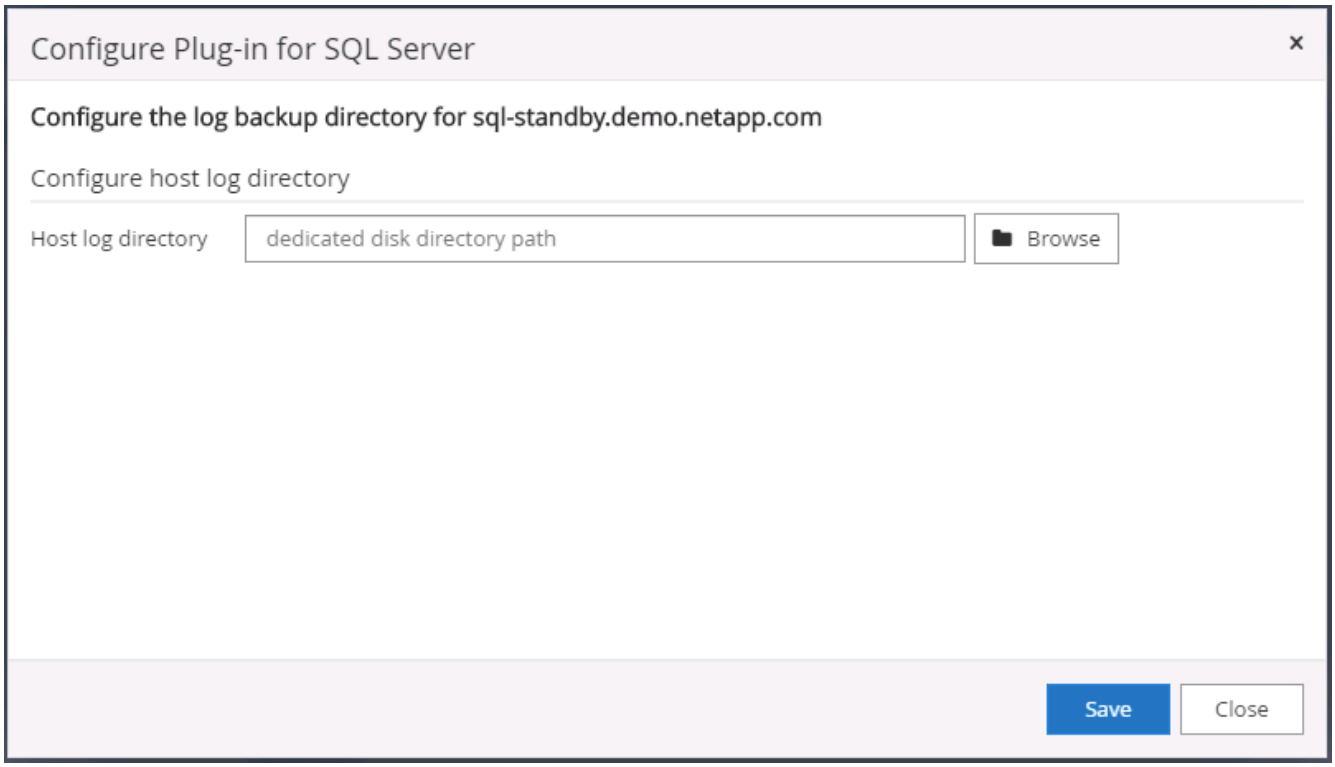


4. Una volta installato il plug-in su un host Windows, il relativo stato generale viene visualizzato come "Configure log directory" (Configura directory log).

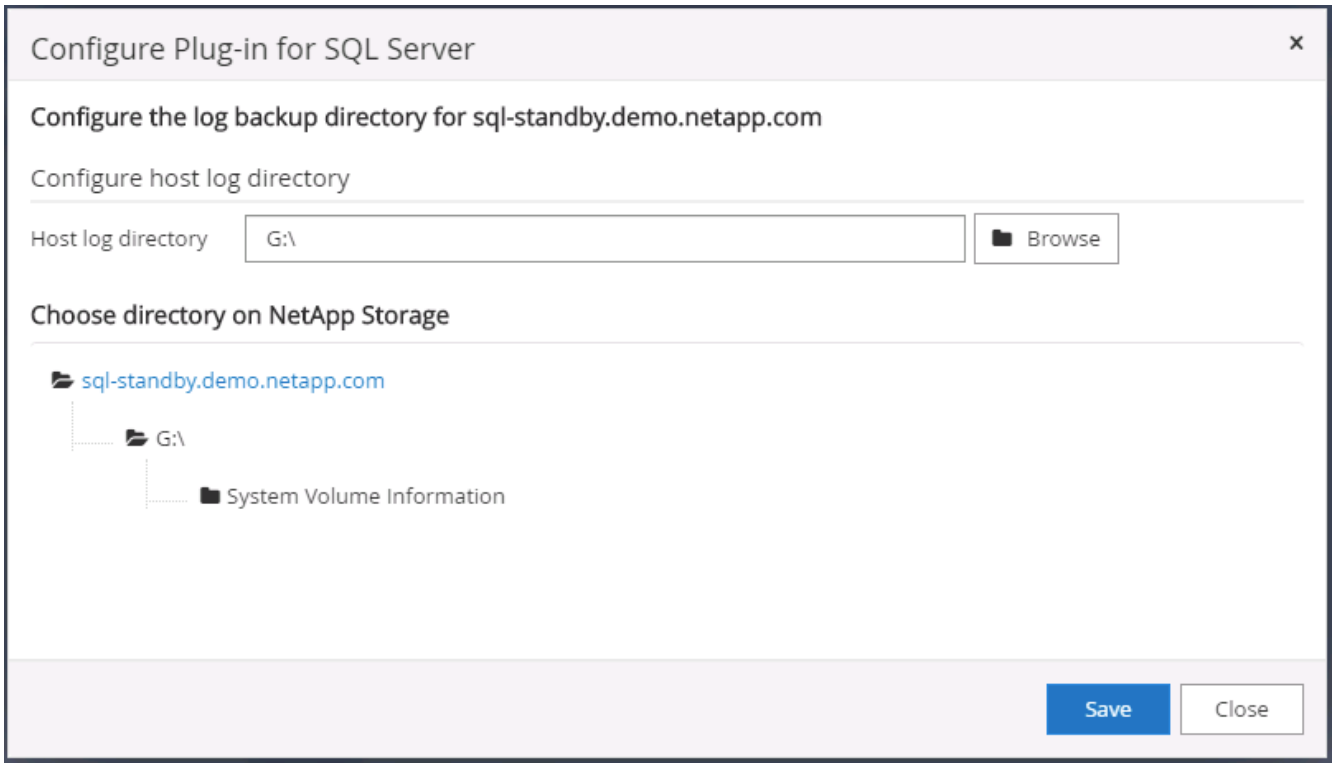
5. Fare clic su host Name (Nome host) per aprire la configurazione della directory di log di SQL Server.



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

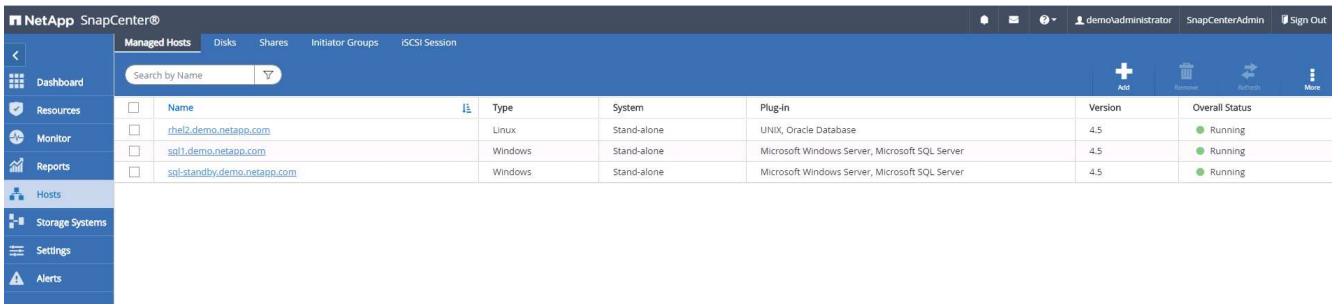


7. Fare clic su Browse (Sfoglia) per scoprire lo storage NetApp in modo da poter impostare una directory di log; SnapCenter utilizza questa directory di log per eseguire il rolloup dei file di log delle transazioni di SQL Server. Quindi fare clic su Save (Salva).

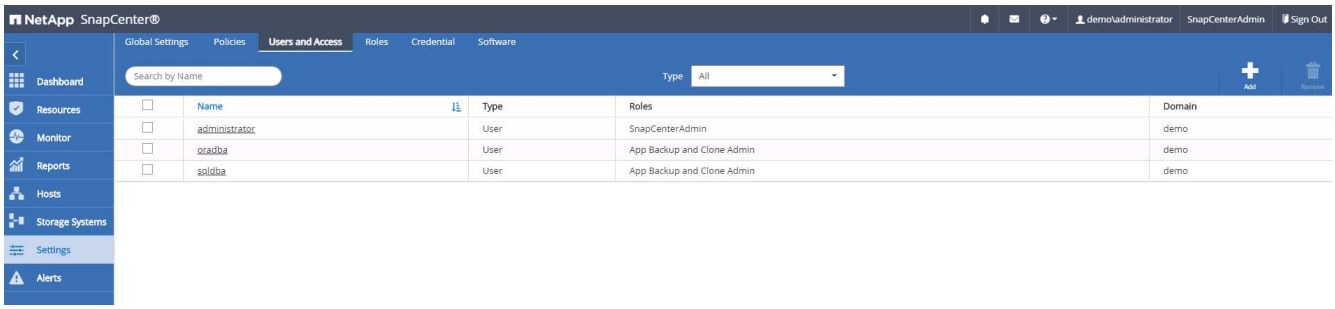


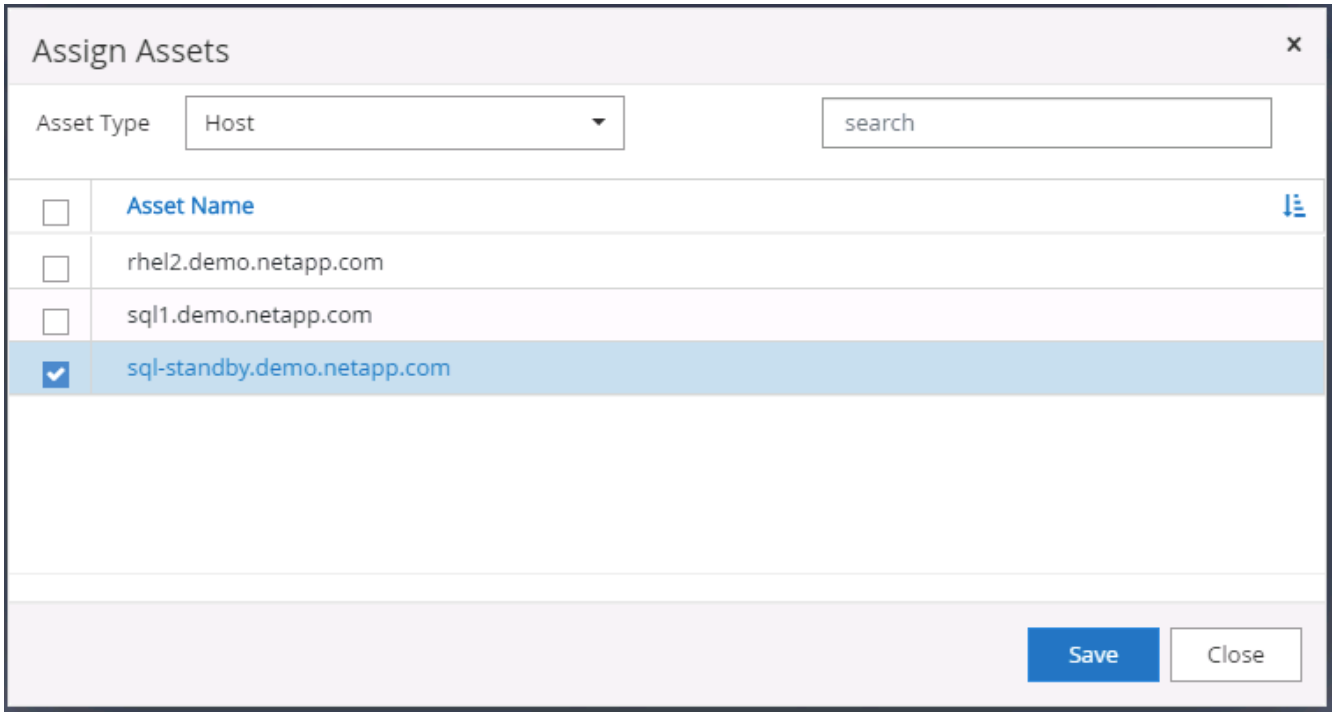
Affinché lo storage NetApp fornito a un host DB venga rilevato, lo storage (on-premise o CVO) deve essere aggiunto a SnapCenter, come illustrato nella fase 6 per CVO come esempio.

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



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.



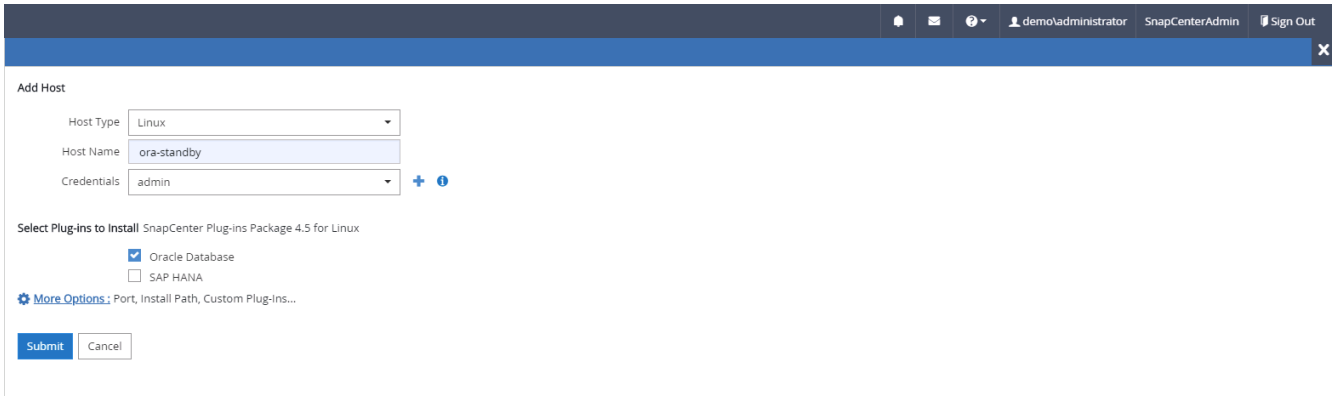


Aggiungere l'host Unix e l'installazione del plug-in sull'host

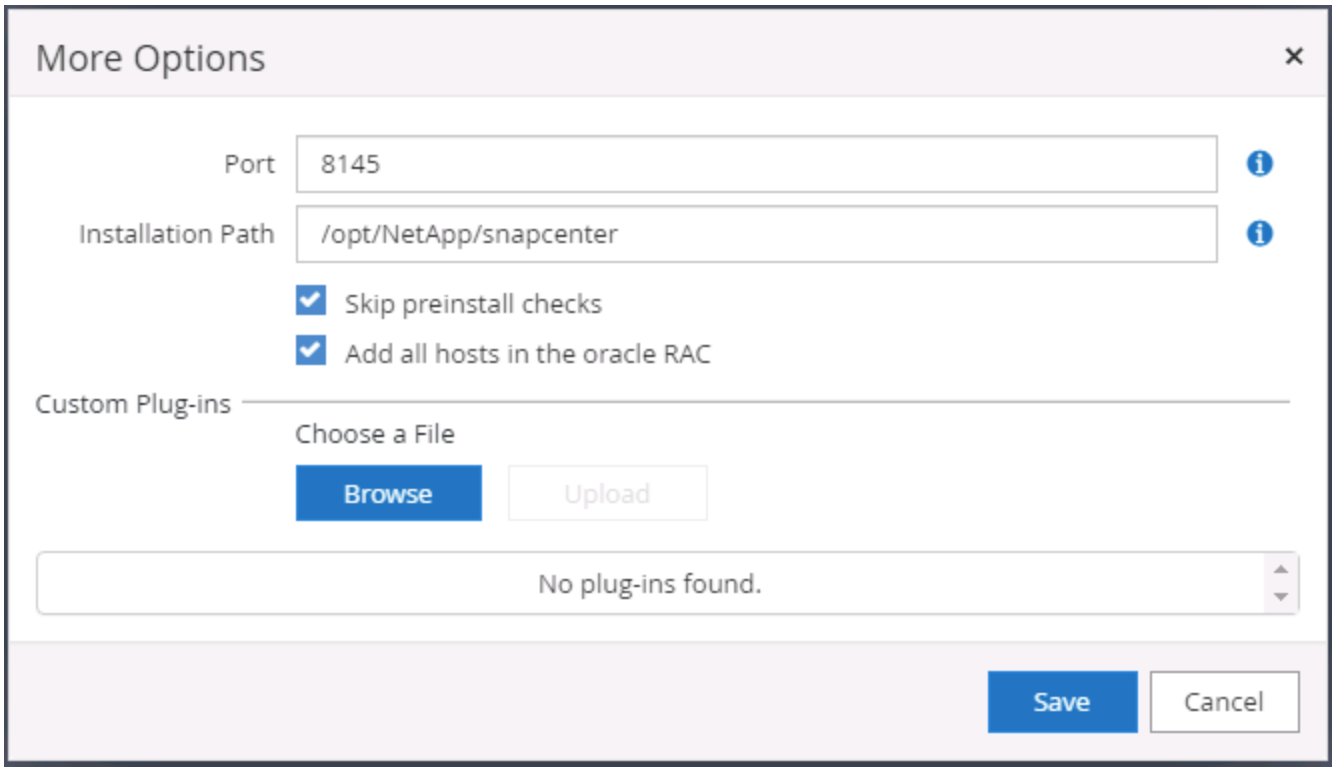
1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda host dal menu a sinistra, quindi fare clic su Add (Aggiungi) per aprire il flusso di

lavoro Add host (Aggiungi host).

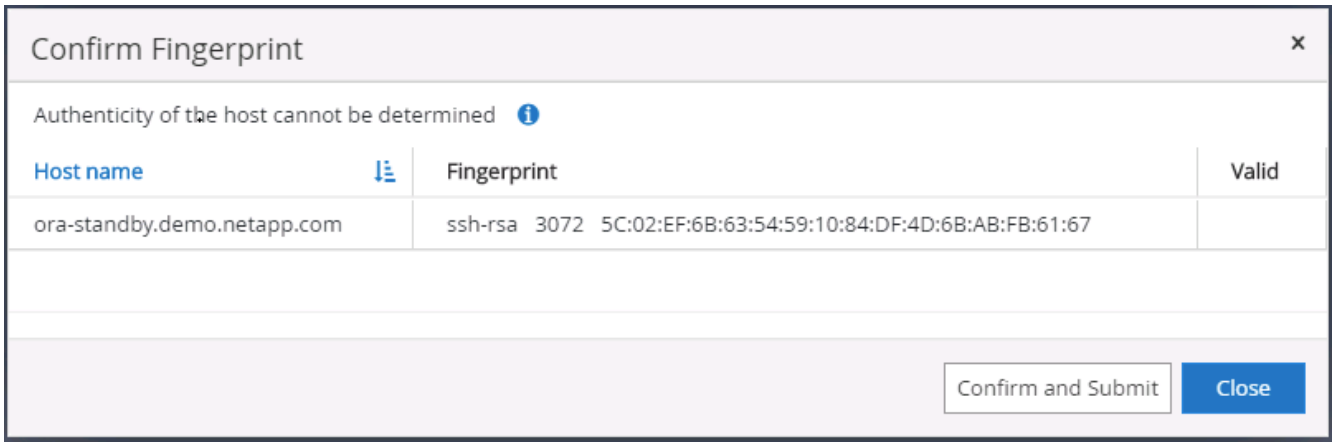
3. Scegliere Linux come tipo di host. Il nome host può essere il nome host o un indirizzo IP. Tuttavia, il nome host deve essere risolto per correggere l'indirizzo IP host dall'host SnapCenter. Scegliere le credenziali host create nel passaggio 2. Le credenziali host richiedono privilegi sudo. Selezionare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



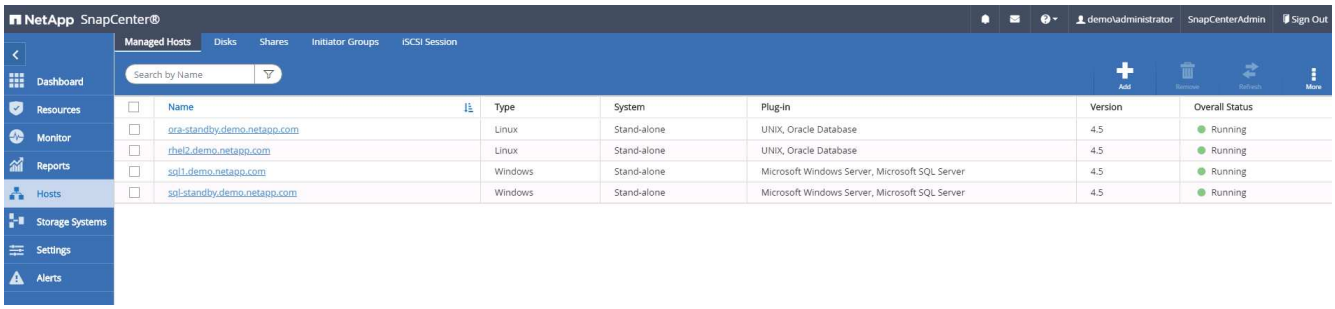
4. Fare clic su altre opzioni e selezionare "Ignora controlli di preinstallazione". Viene richiesto di confermare l'omissione del controllo di preinstallazione. Fare clic su Sì, quindi su Salva.



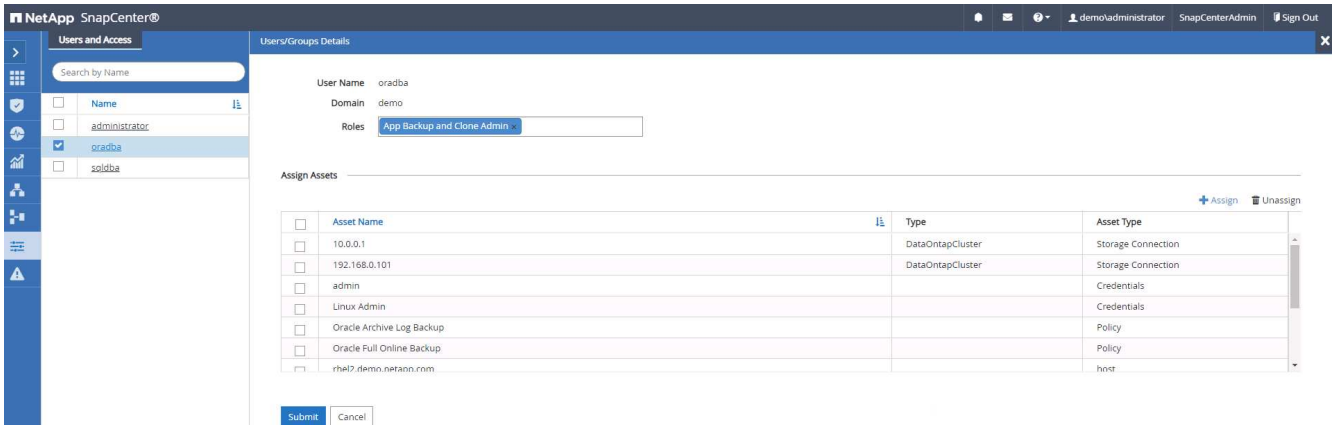
5. Fare clic su Submit (Invia) per avviare l'installazione del plug-in. Viene richiesto di confermare l'impronta digitale come mostrato di seguito.

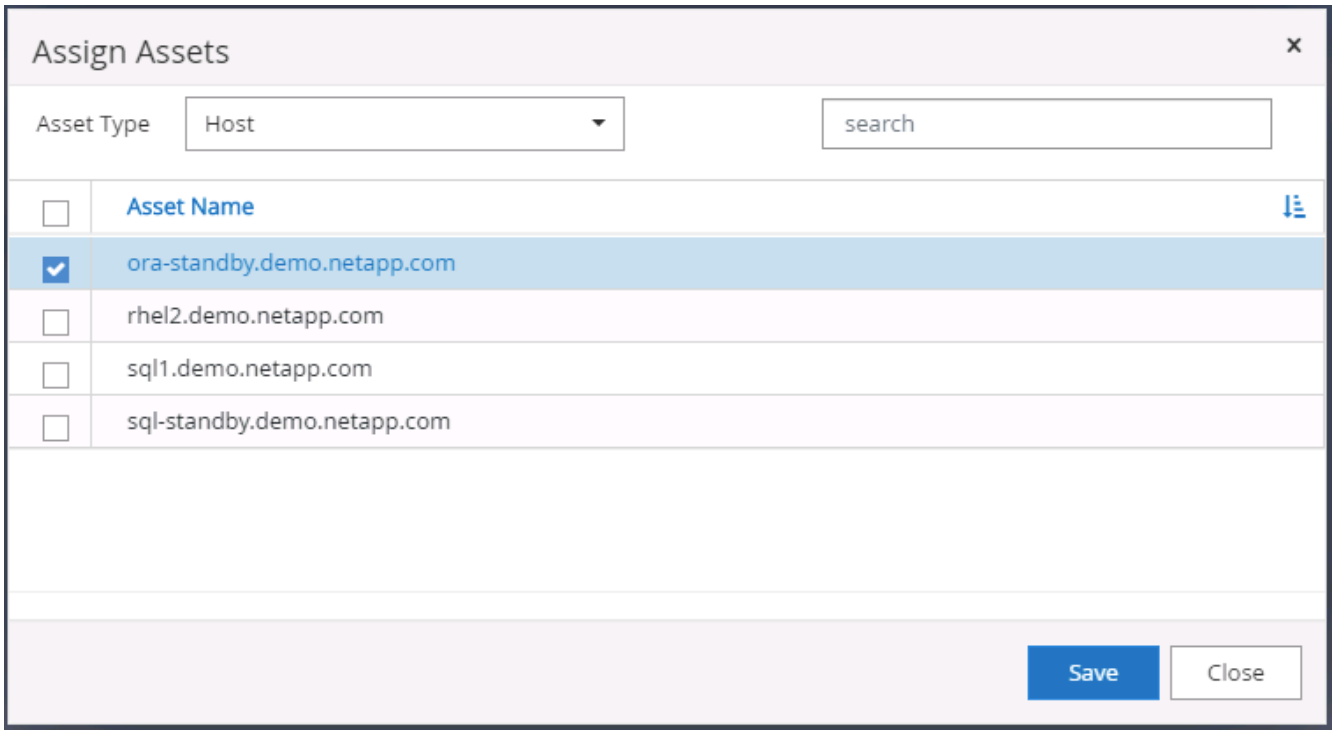


6. SnapCenter esegue la convalida e la registrazione dell'host, quindi il plug-in viene installato sull'host Linux. Lo stato cambia da Installing Plugin (Installazione del plug-in) a running (in esecuzione)



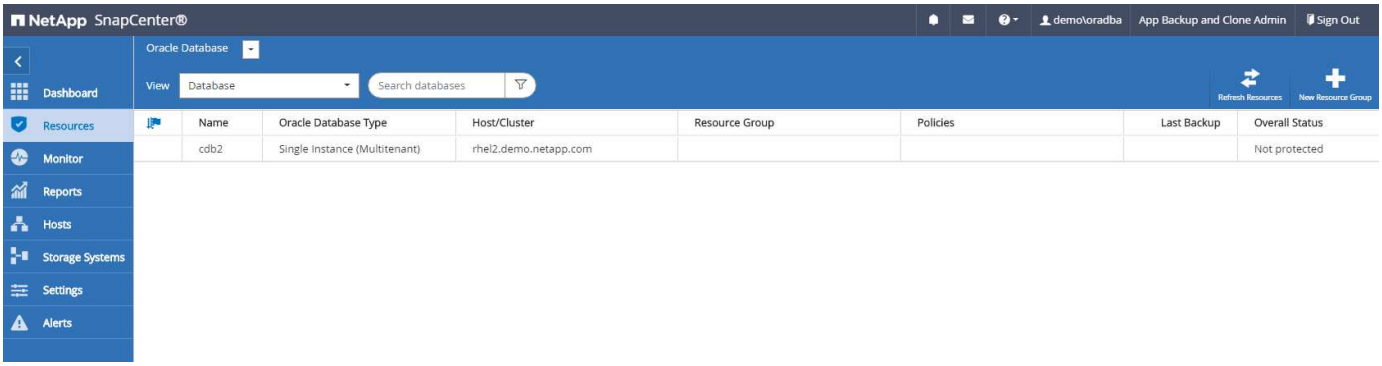
7. Assegnare l'host appena aggiunto all'ID utente corretto per la gestione del database (nel nostro caso, oradba).





4. Rilevamento delle risorse del database

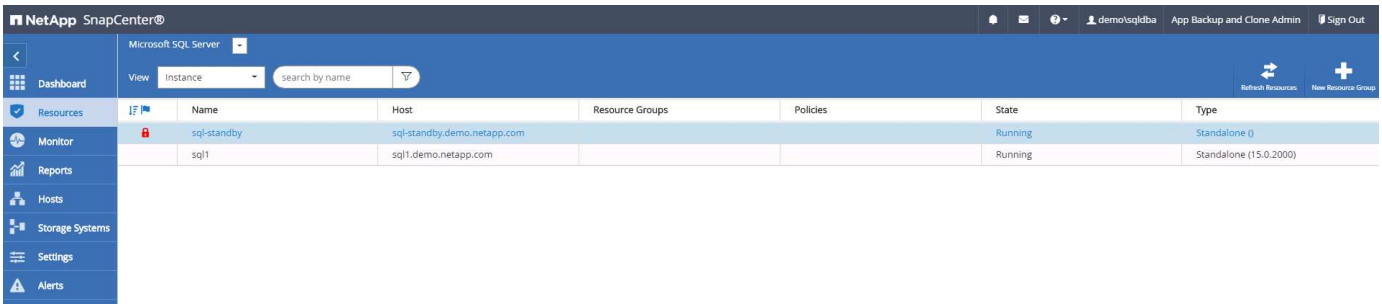
Una volta completata l'installazione del plug-in, è possibile rilevare immediatamente le risorse del database sull'host. Fare clic sulla scheda Resources (risorse) nel menu a sinistra. A seconda del tipo di piattaforma di database, sono disponibili diverse visualizzazioni, ad esempio il database, il 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).

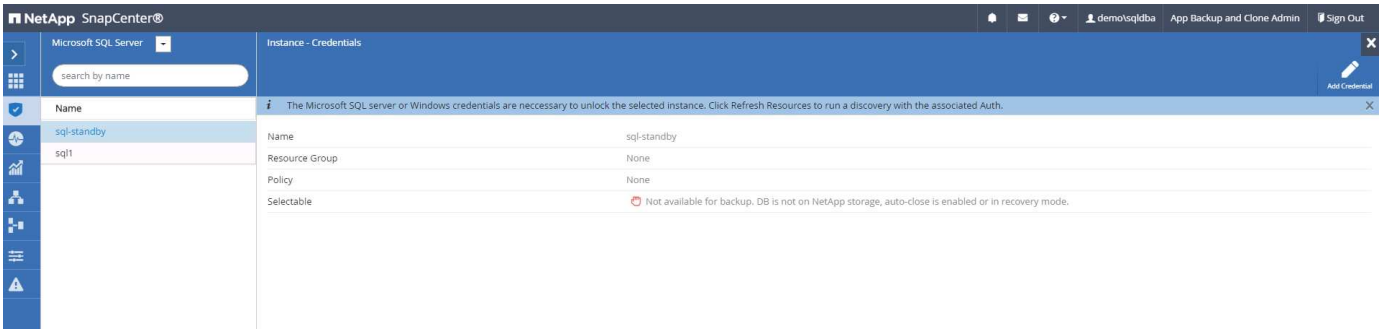


Quando il database viene rilevato inizialmente, lo stato generale viene visualizzato come "Not Protected" (non protetto). La schermata precedente mostra un database Oracle non ancora protetto da una policy di backup.

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.

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.





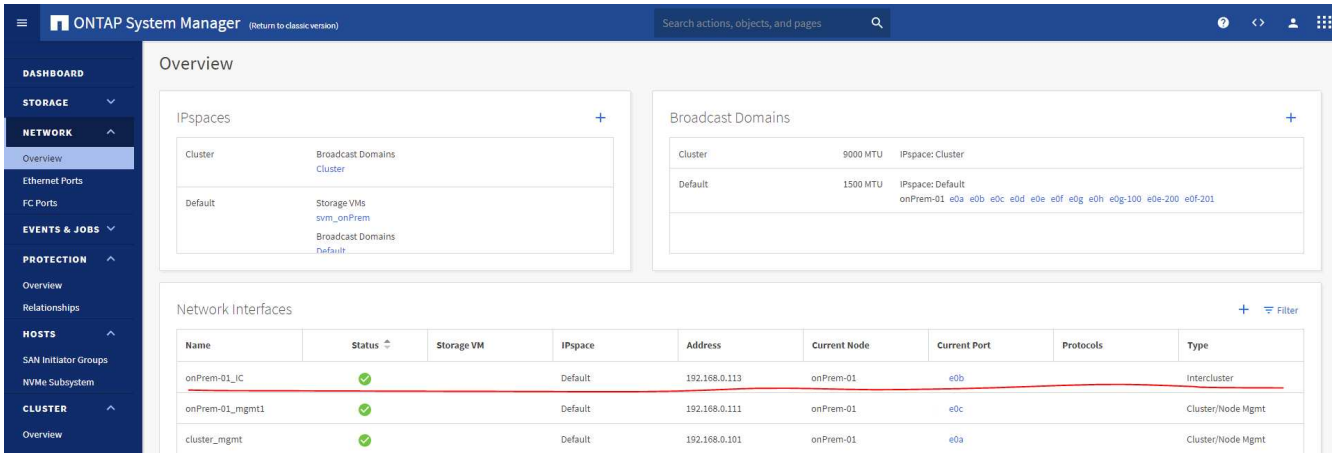
Una volta configurate le credenziali appropriate a livello di Windows o di database, il blocco rosso scompare e le informazioni sul tipo di SQL Server vengono raccolte e riviste.

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

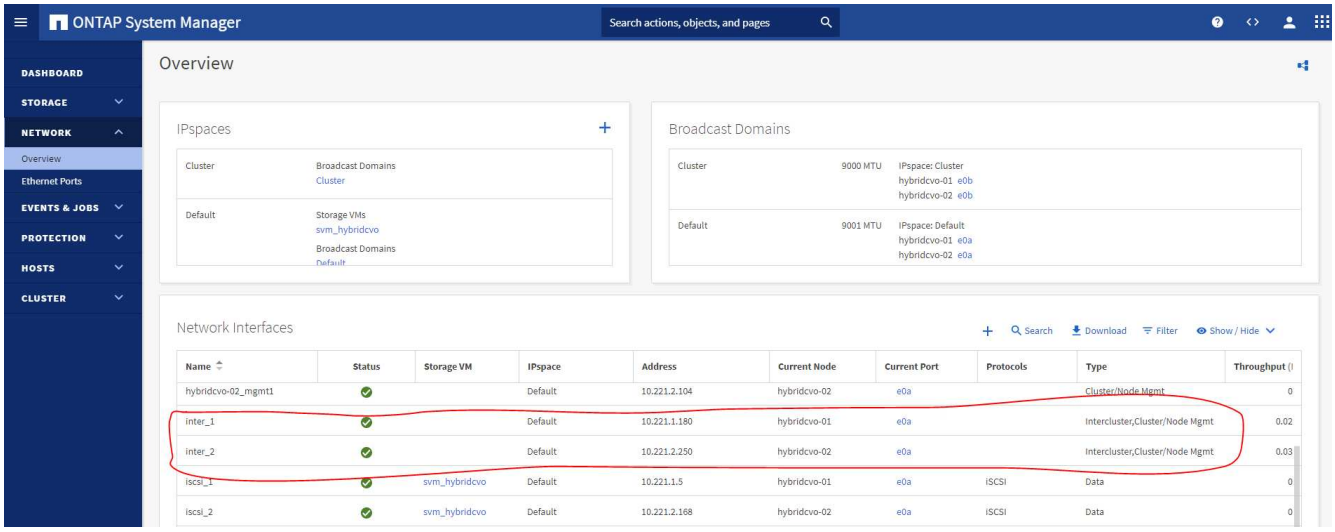
Per proteggere i dati del database on-premise utilizzando un cloud pubblico come destinazione di destinazione, i volumi di database del cluster ONTAP on-premise vengono replicati nel CVO del cloud utilizzando la tecnologia NetApp SnapMirror. I volumi di destinazione replicati possono quindi essere clonati 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:



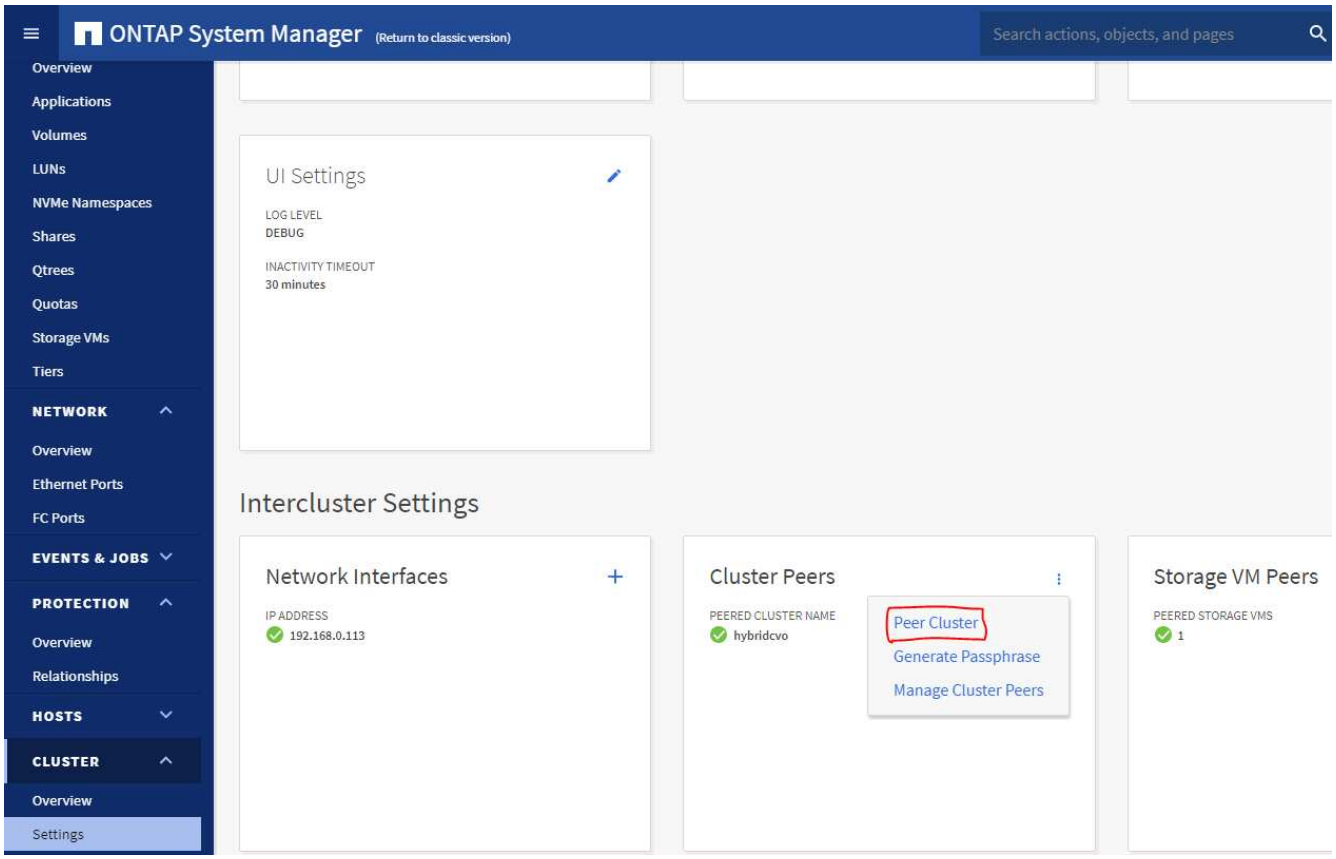
   Cluster CVO di destinazione:



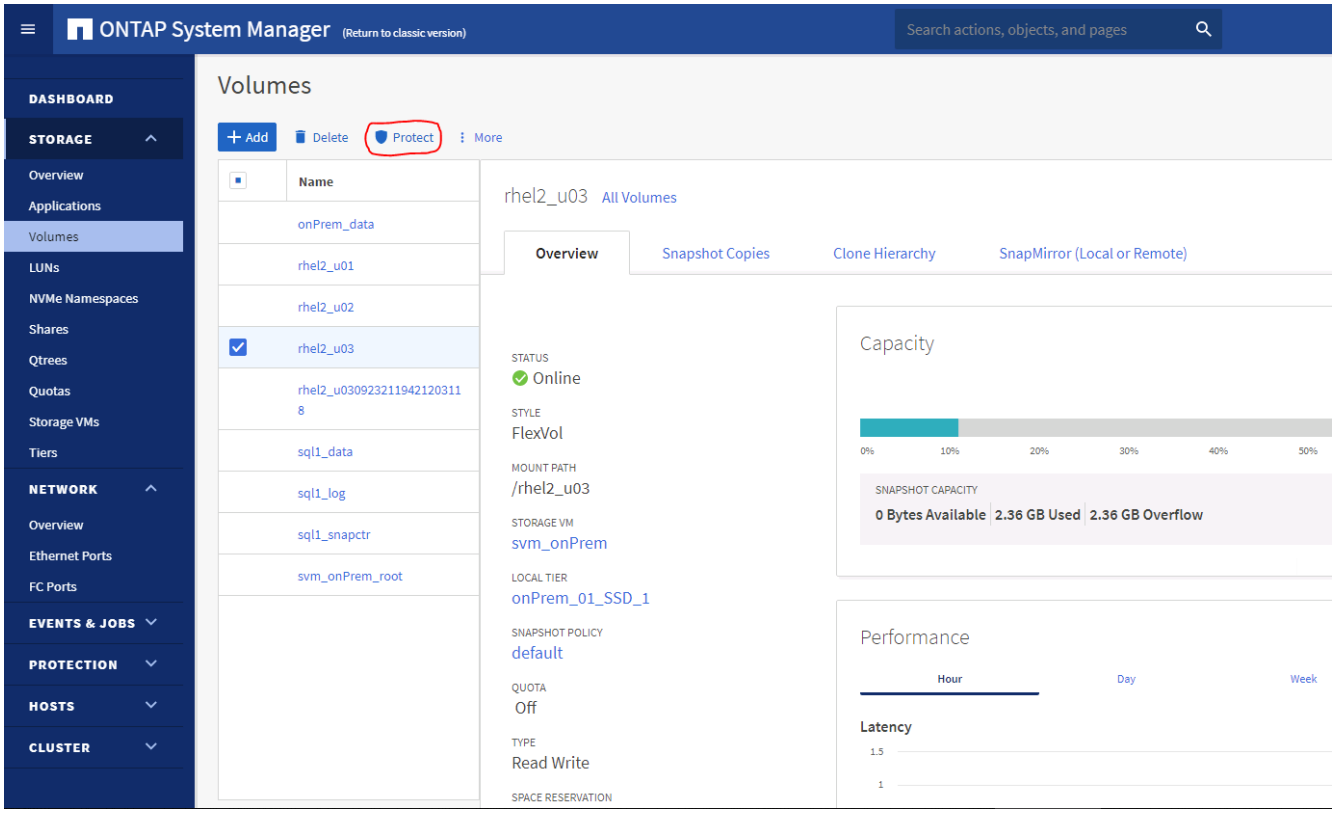
2. Con le LIF intercluster configurate, è possibile configurare il peering dei cluster e la replica dei volumi utilizzando la funzione di trascinamento della selezione in NetApp Cloud Manager. Vedere "Getting started - AWS Public Cloud" per ulteriori informazioni.

   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.

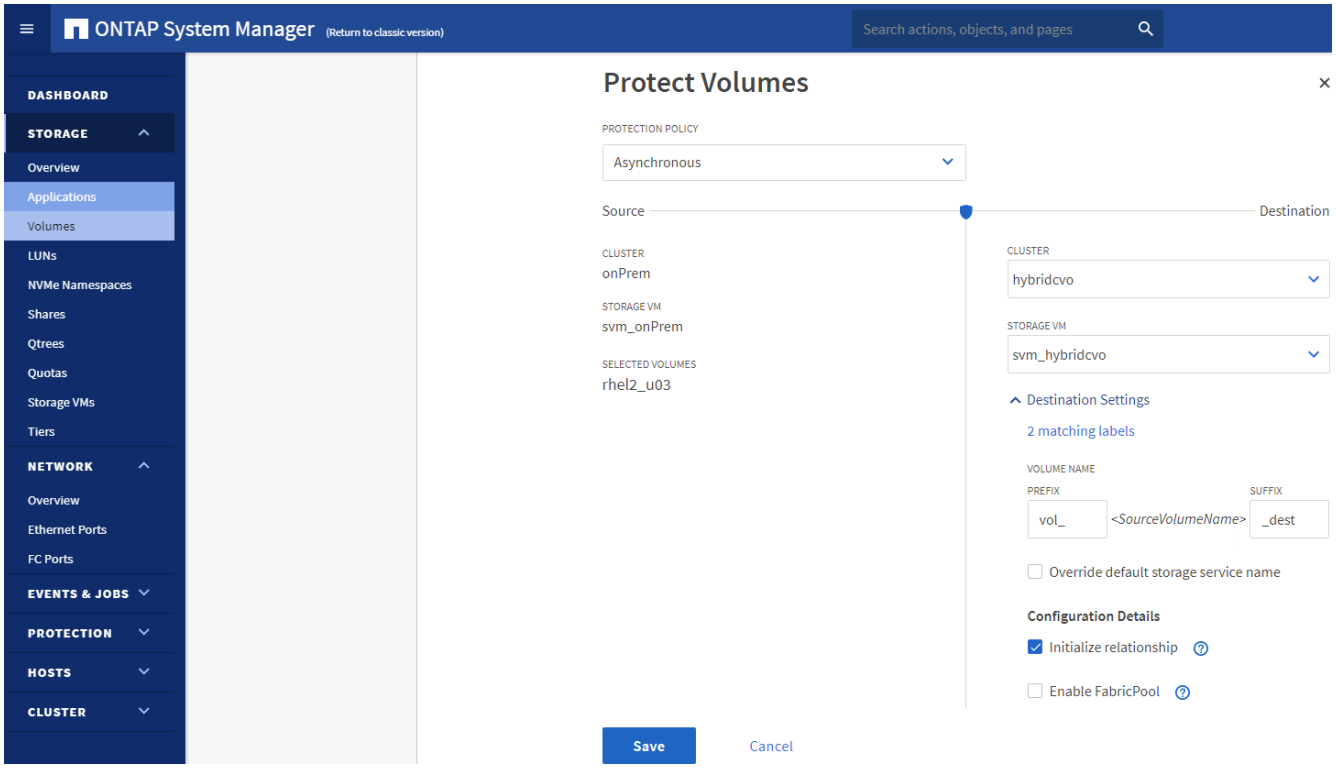


4. Accedere alla scheda Volumes (volumi). Selezionare il volume di database da replicare e fare clic su Proteggi.

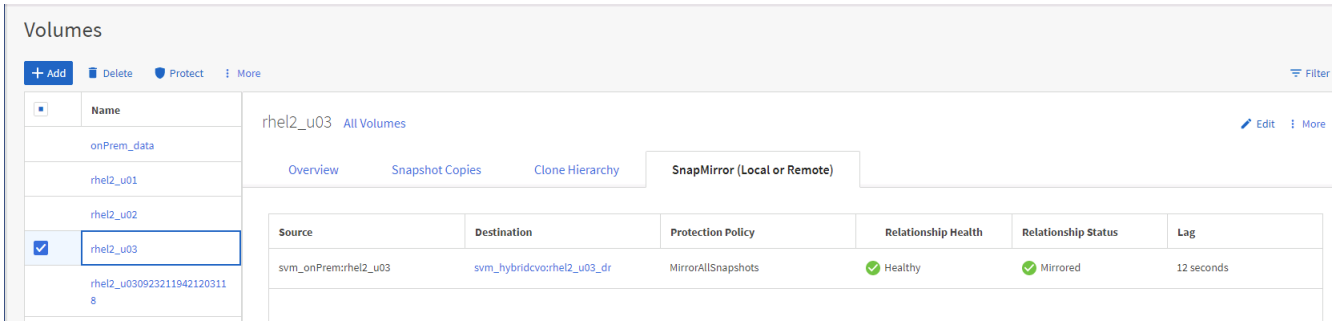


5. Impostare il criterio di protezione su asincrono. Selezionare la SVM del cluster e dello storage di

destinazione.

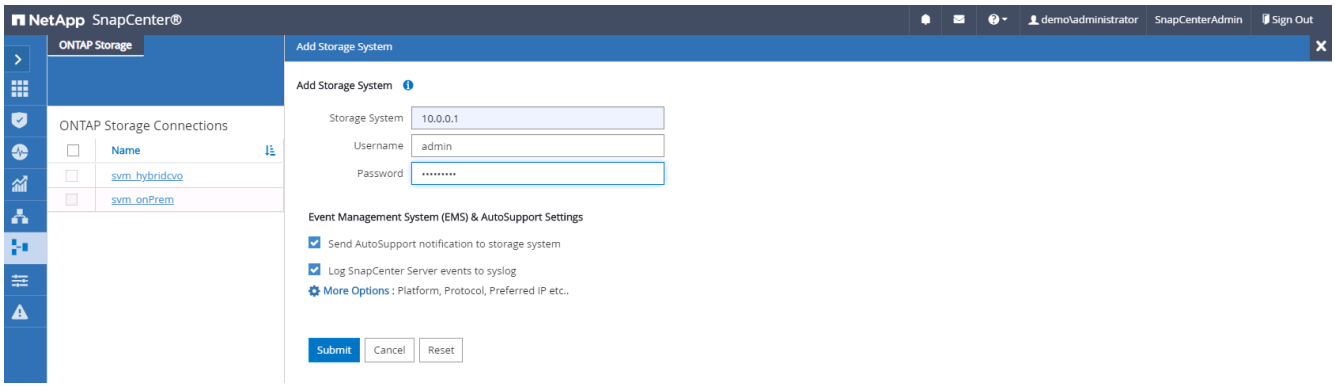


6. Verificare che il volume sia sincronizzato tra l'origine e la destinazione e che la relazione di replica sia corretta.

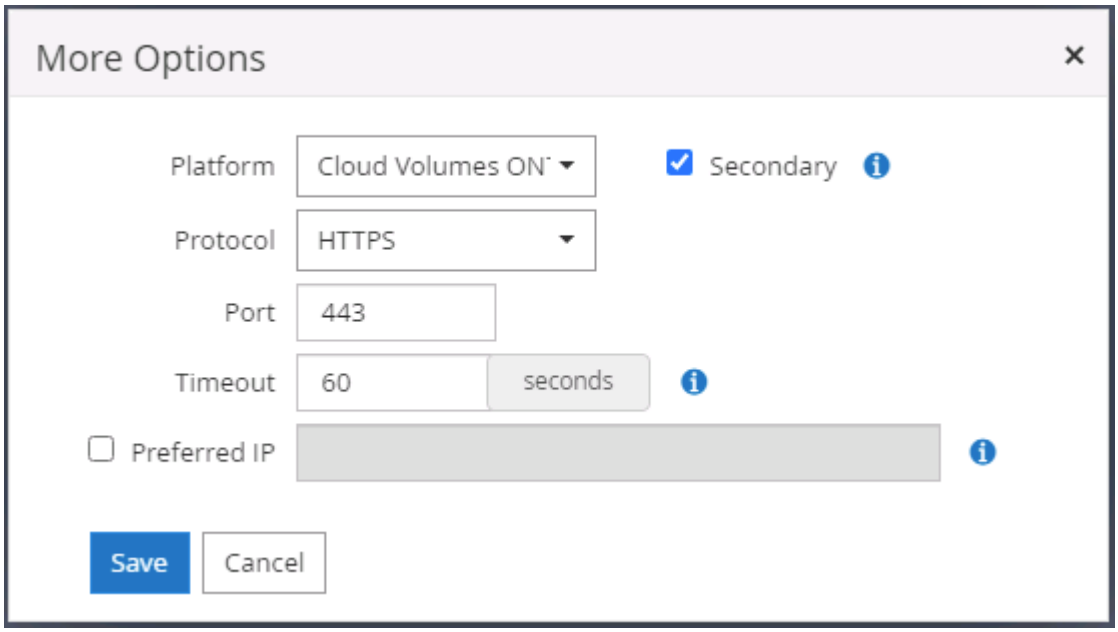


6. Aggiunta di SVM per lo storage di database CVO a SnapCenter

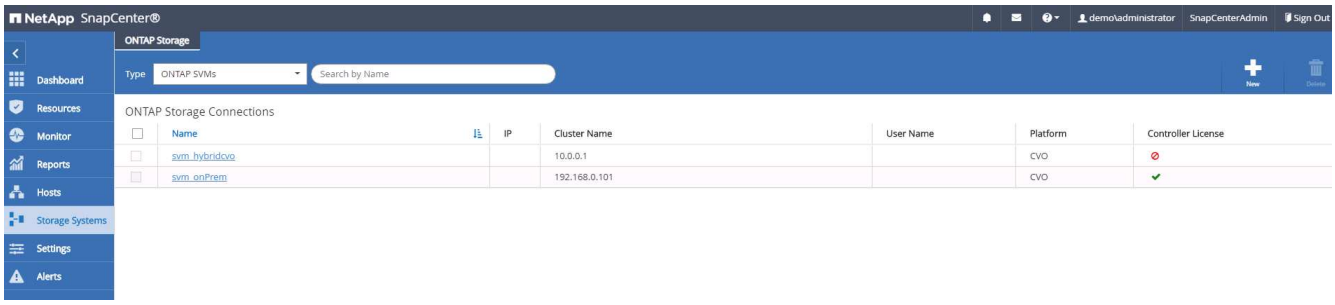
1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda sistema di storage dal menu, quindi fare clic su nuovo per aggiungere una SVM di storage CVO che ospita volumi di database di destinazione replicati in SnapCenter. Inserire l'IP di gestione del cluster 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.

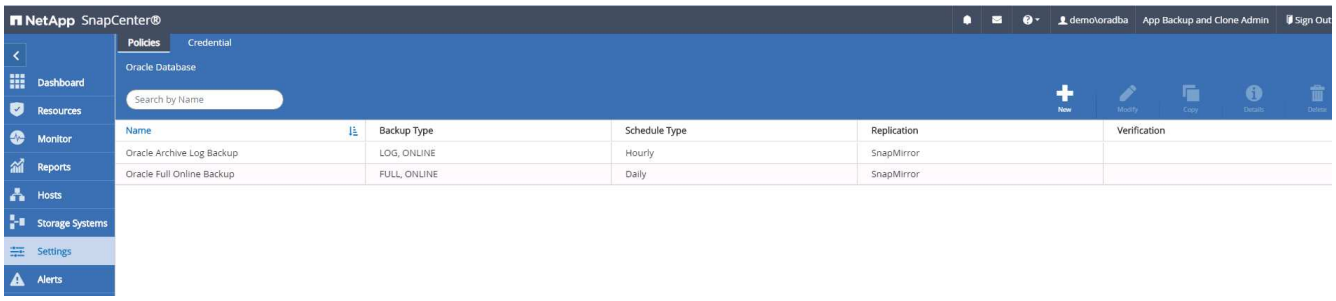


7. Configurare i criteri di backup del database in SnapCenter

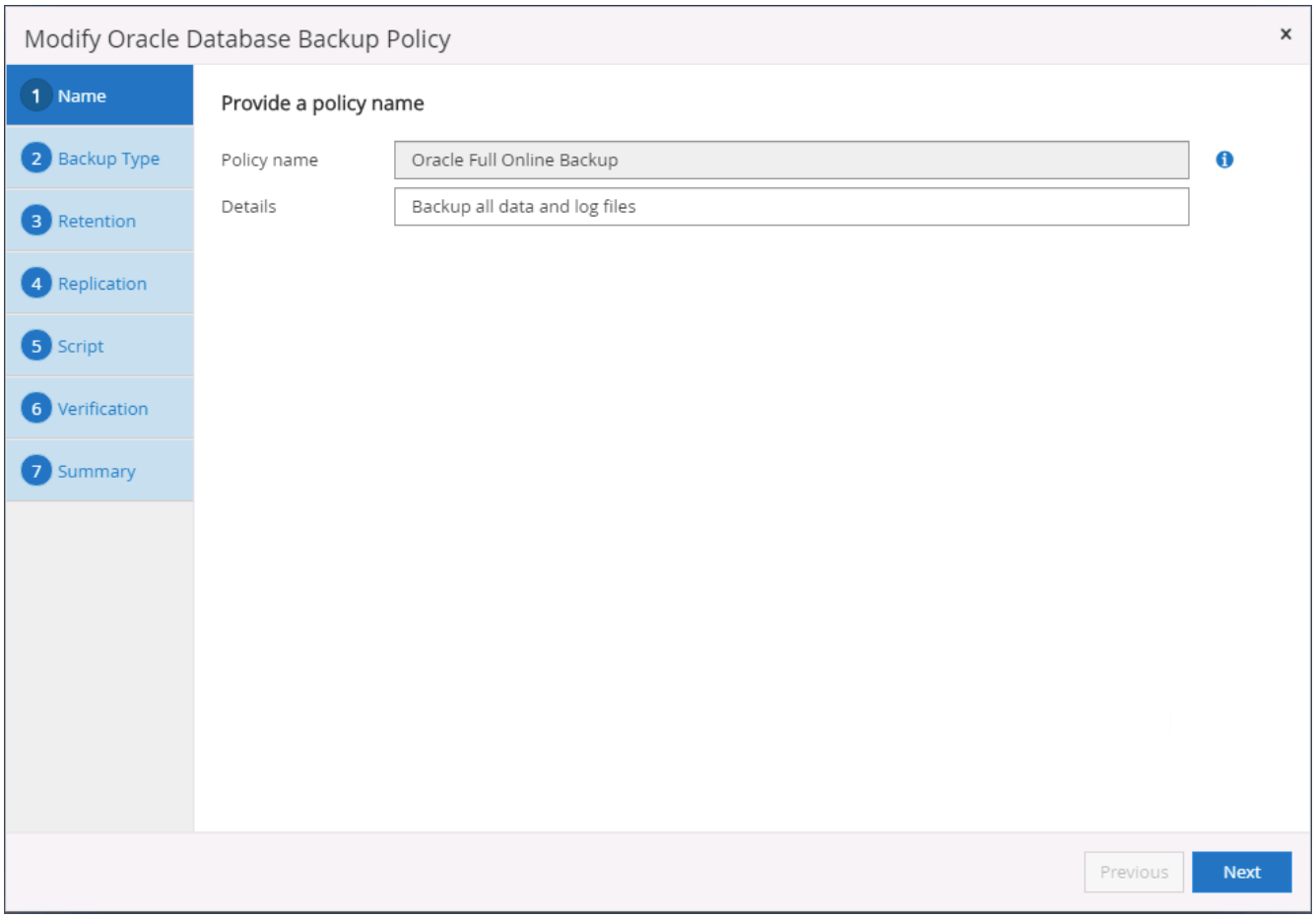
Le seguenti procedure illustrano come creare un database completo o un criterio di backup del file di log. Il criterio può quindi essere implementato per proteggere le risorse dei database. L'RPO (Recovery Point Objective) o RTO (Recovery Time Objective) determina la frequenza dei backup del database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

Creare una policy di backup completa del database per Oracle

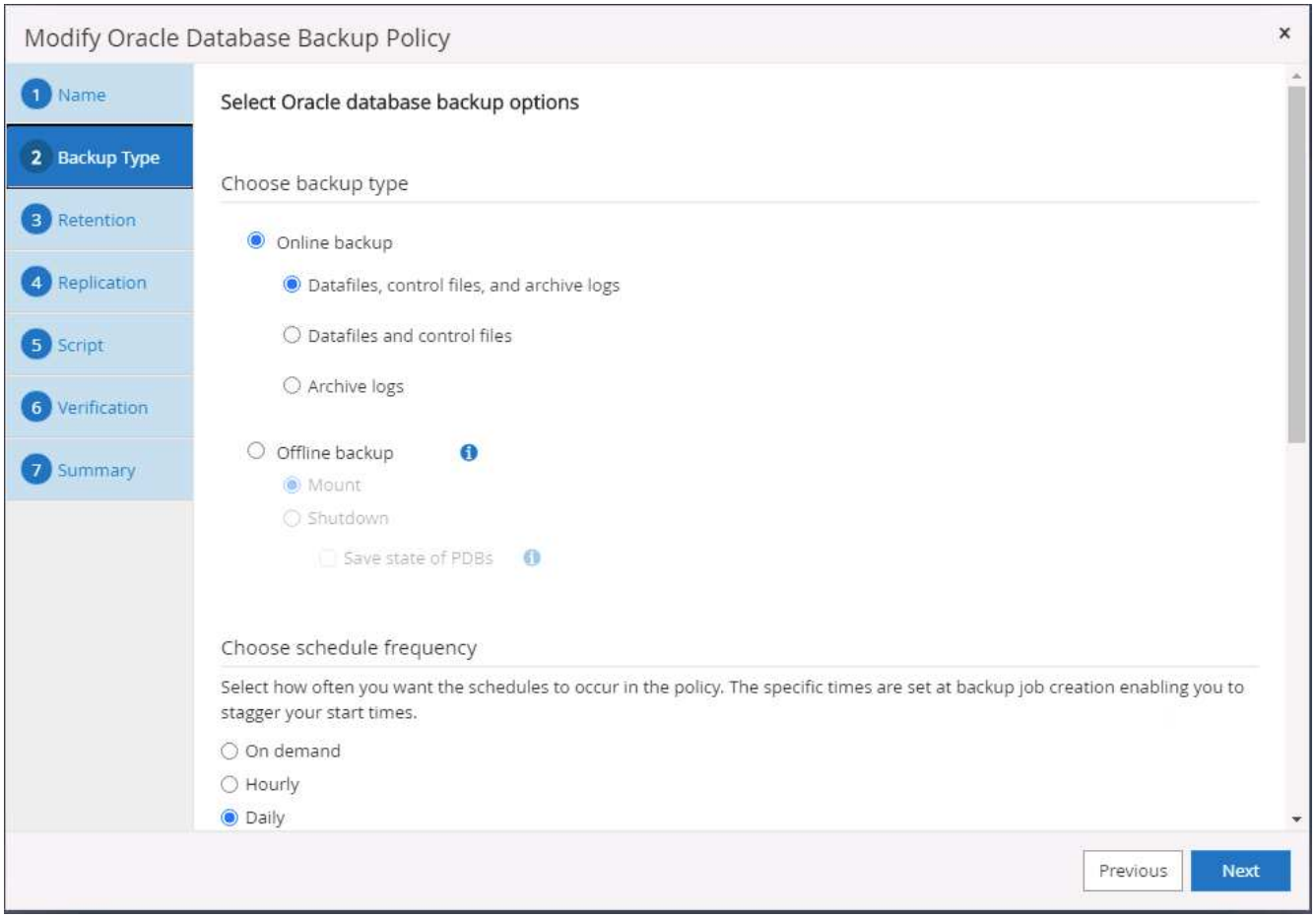
1. Accedere a SnapCenter come ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.



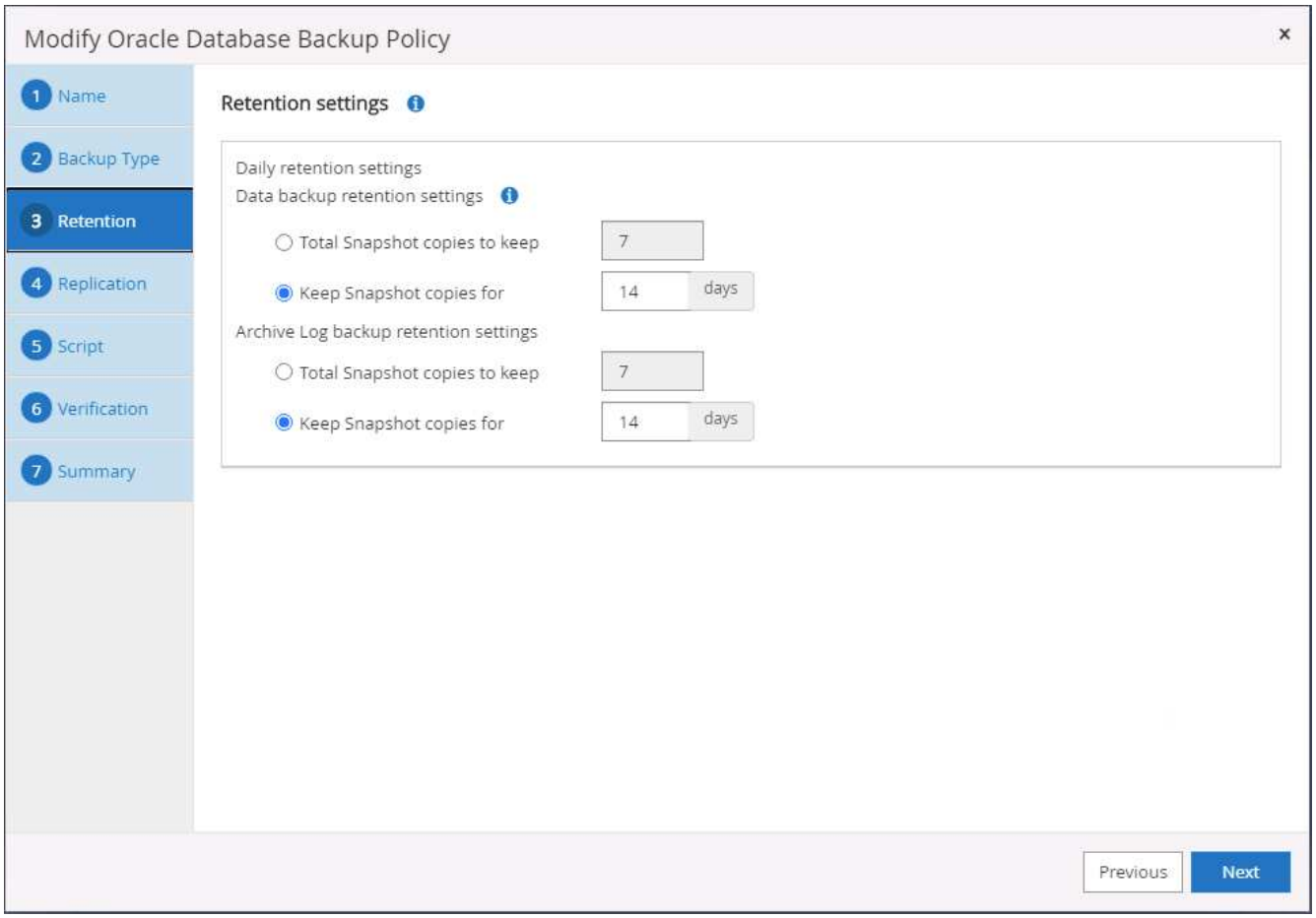
2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.



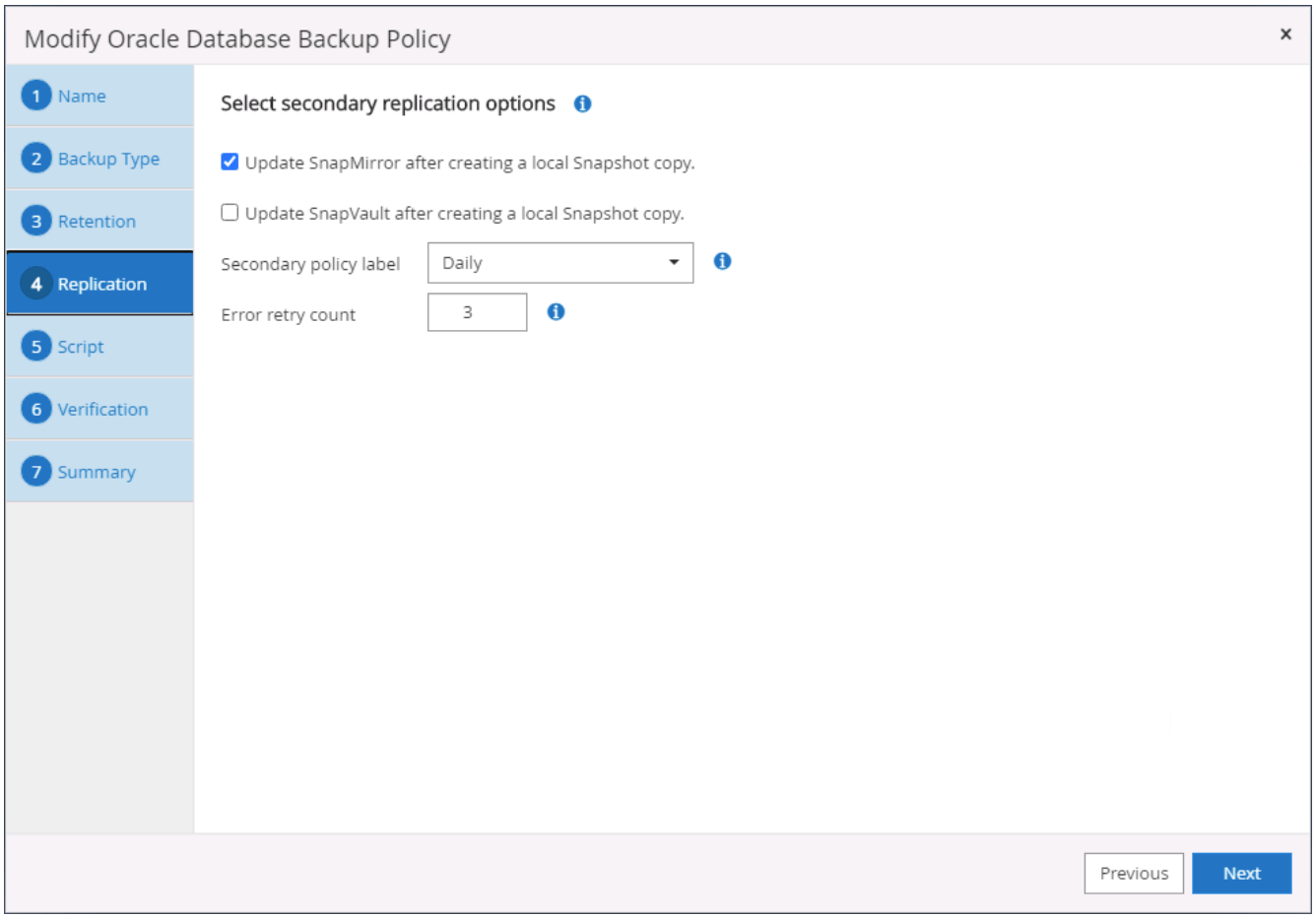
3. Selezionare il tipo di backup e la frequenza di pianificazione.



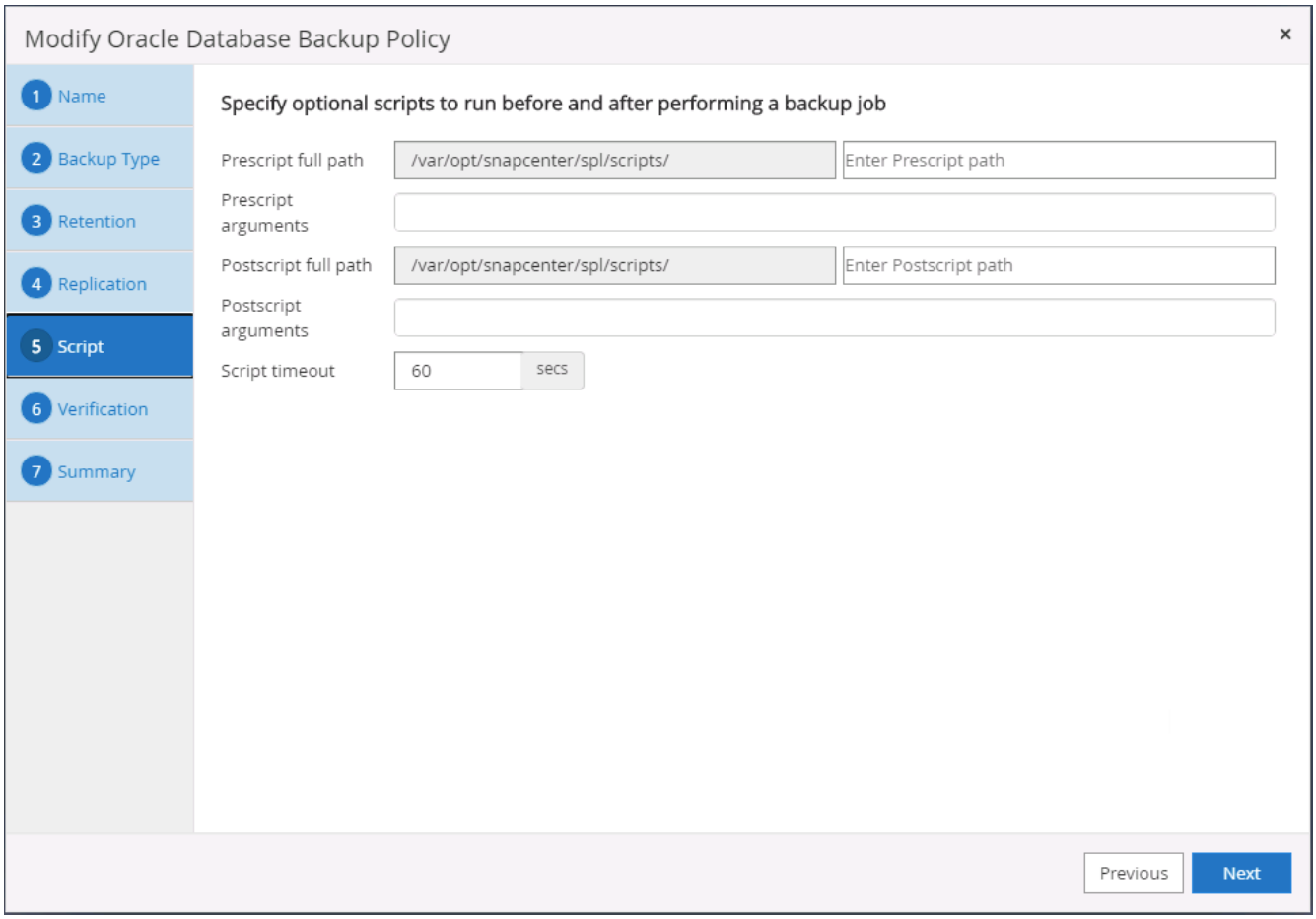
4. Impostare la conservazione del backup. Definisce il numero di copie di backup complete del database da conservare.



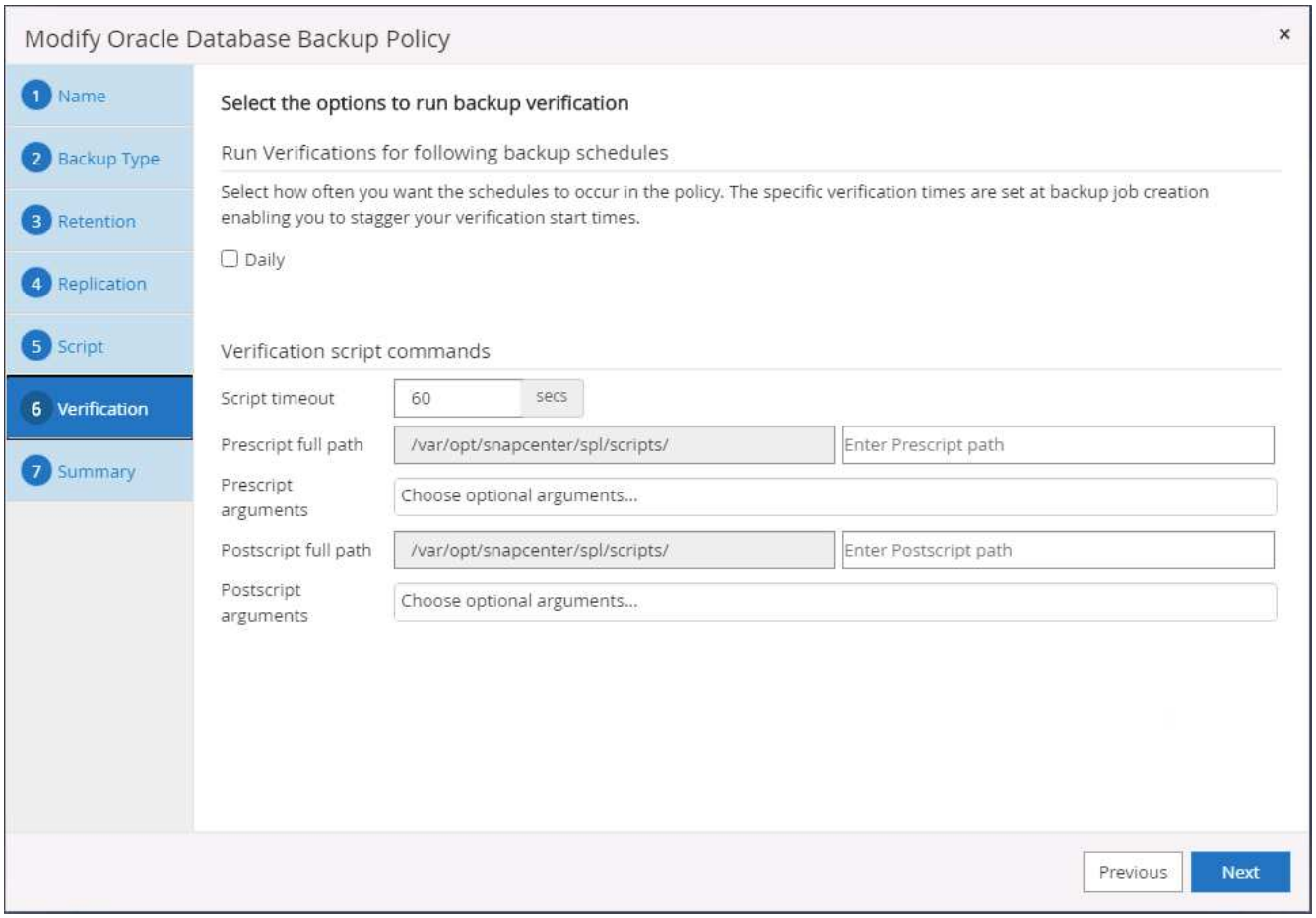
5. Selezionare le opzioni di replica secondaria per inviare i backup delle snapshot primarie locali da replicare in una posizione secondaria nel cloud.



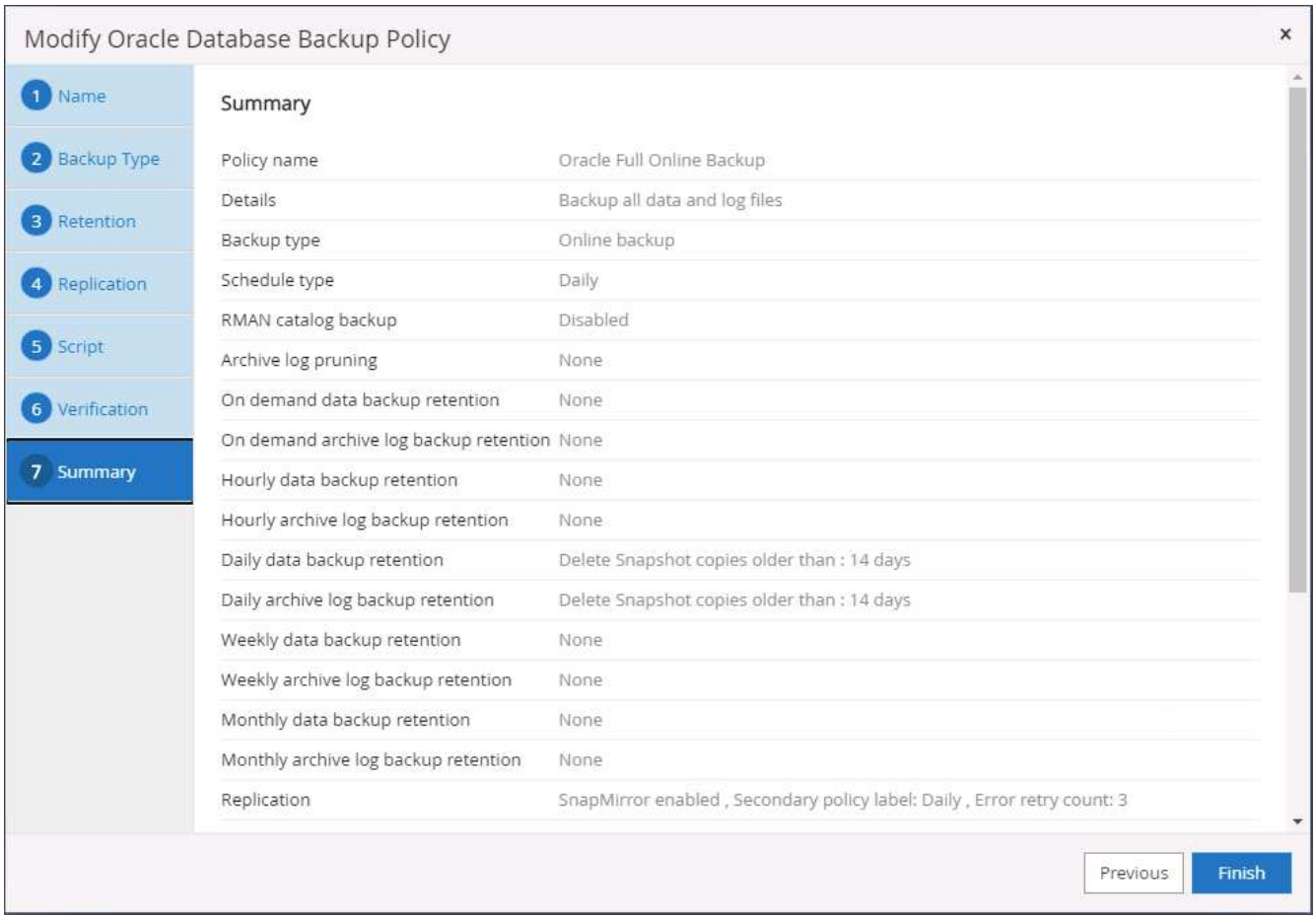
6. Specificare qualsiasi script opzionale da eseguire prima e dopo l'esecuzione di un backup.



7. Eseguire la verifica del backup, se necessario.

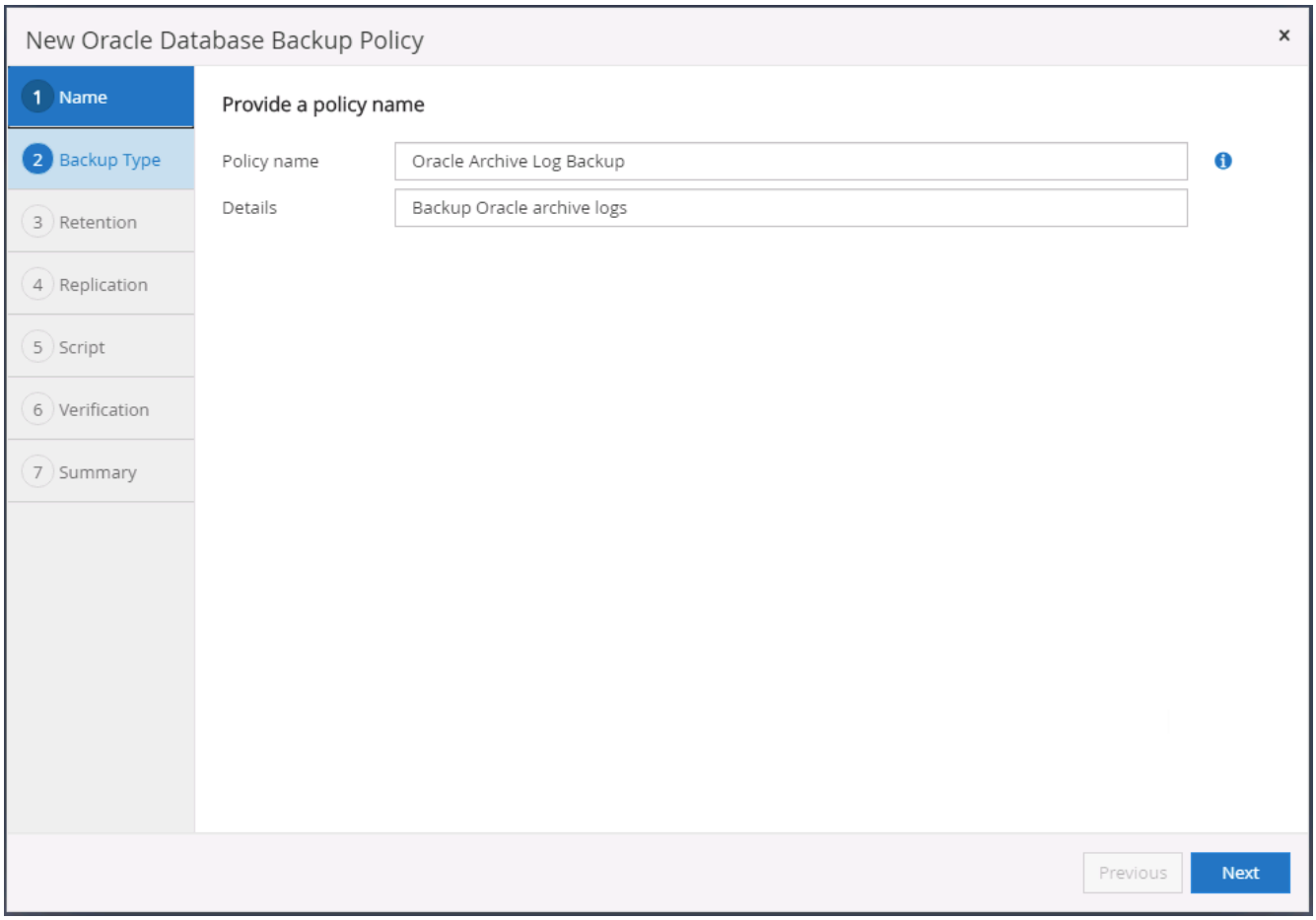

Modify Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Daily
Verification script commands
Script timeout
60
secs
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.

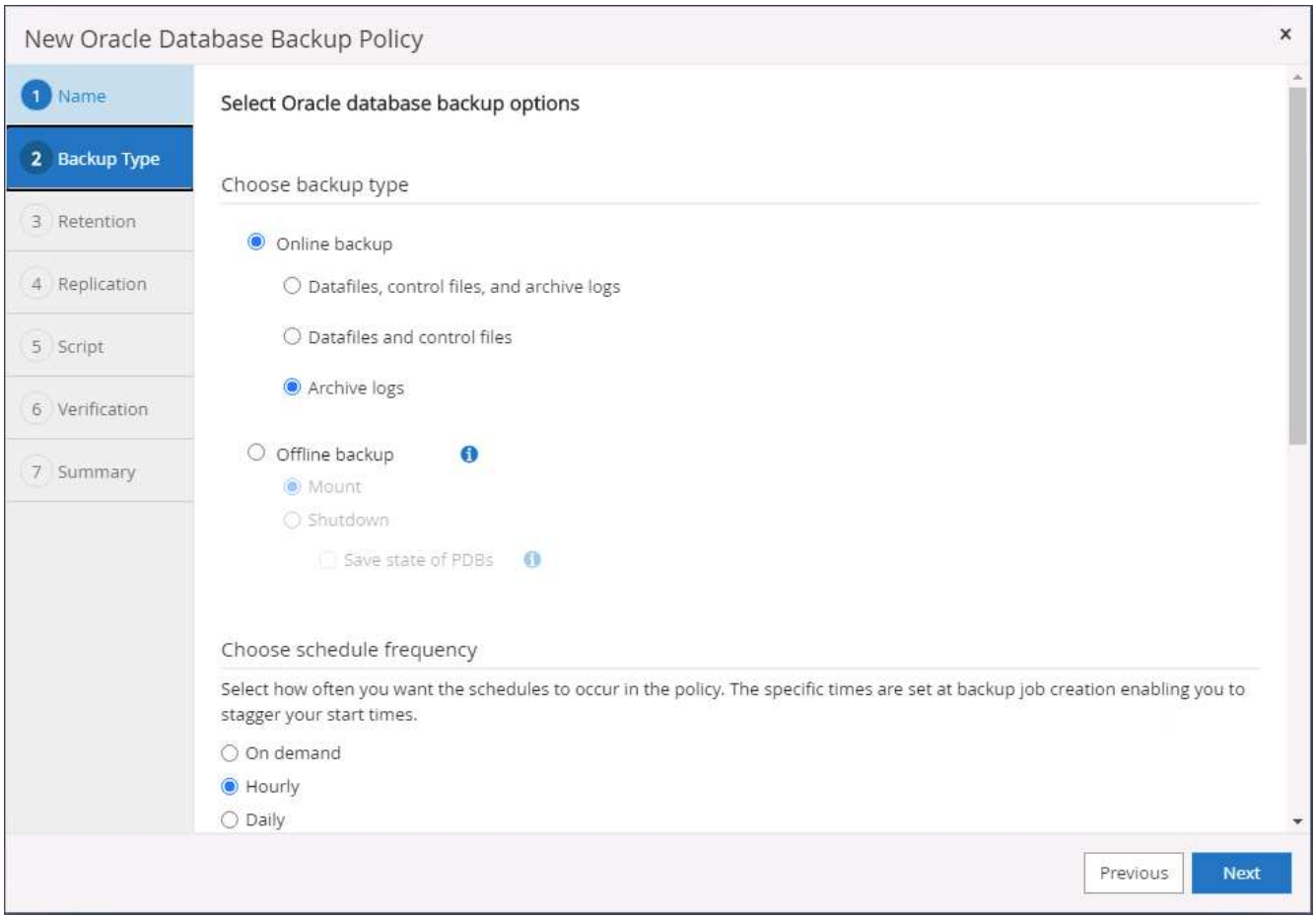


Creare una policy di backup del log del database per Oracle

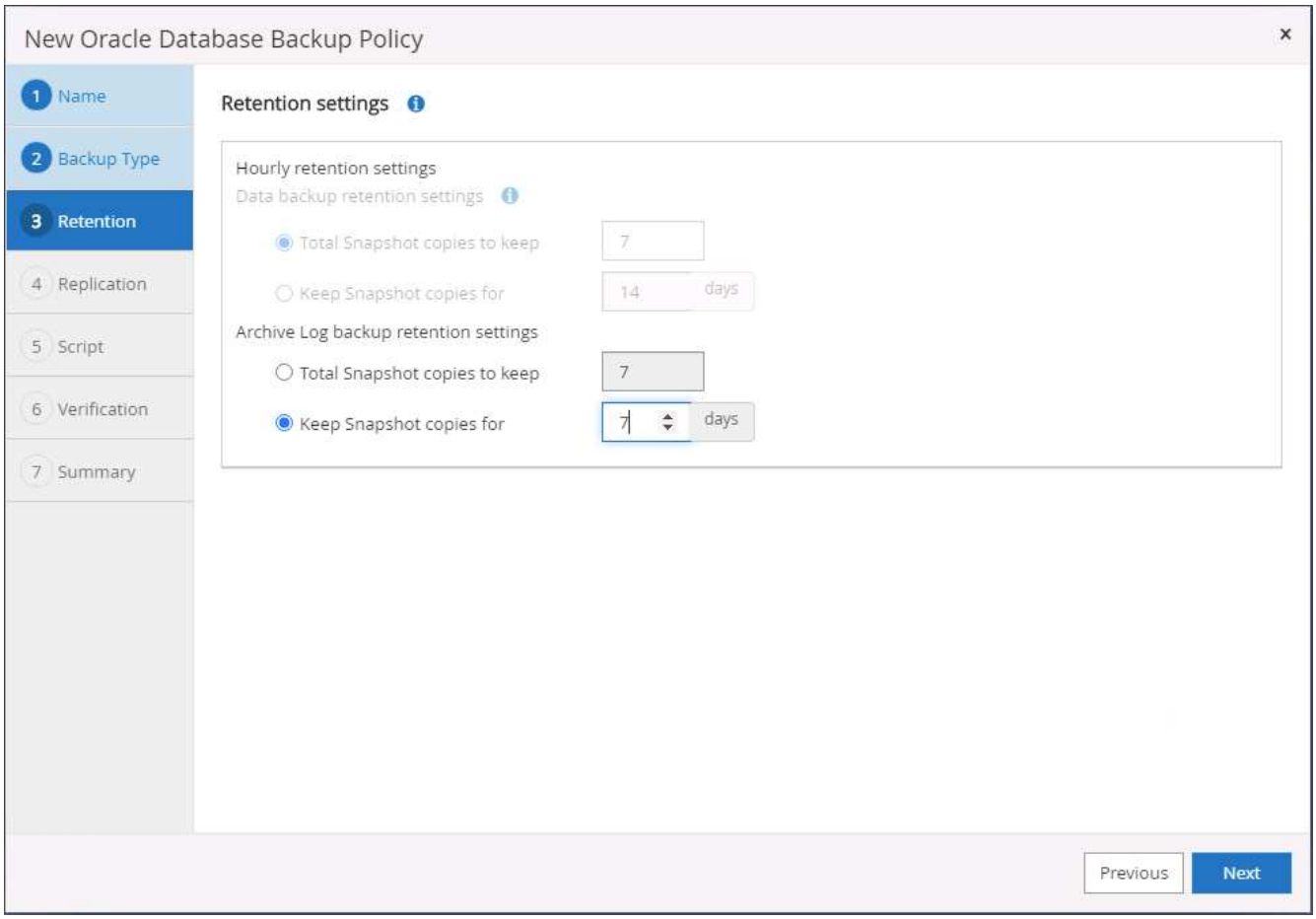
1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.
2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.



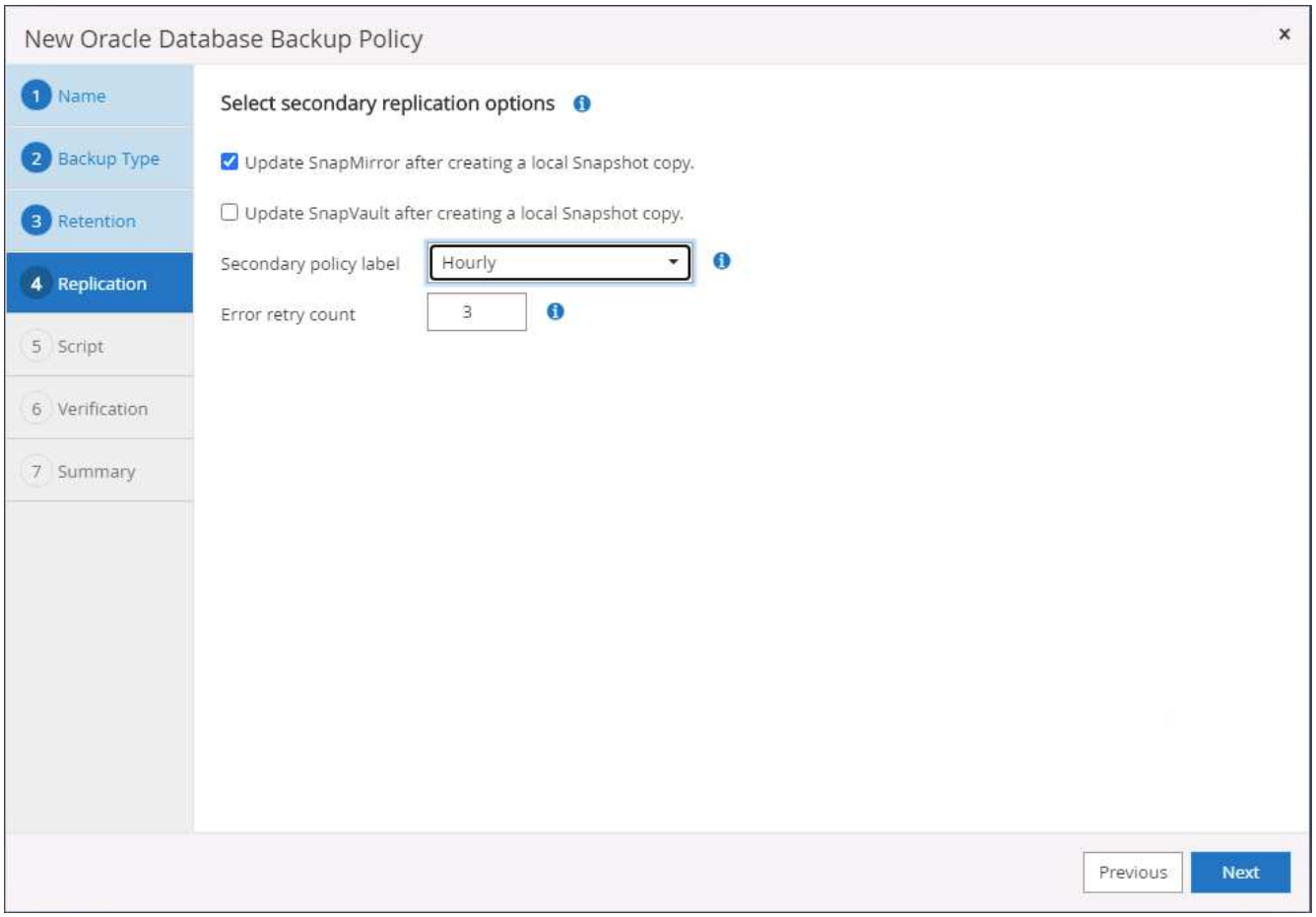
3. Selezionare il tipo di backup e la frequenza di pianificazione.



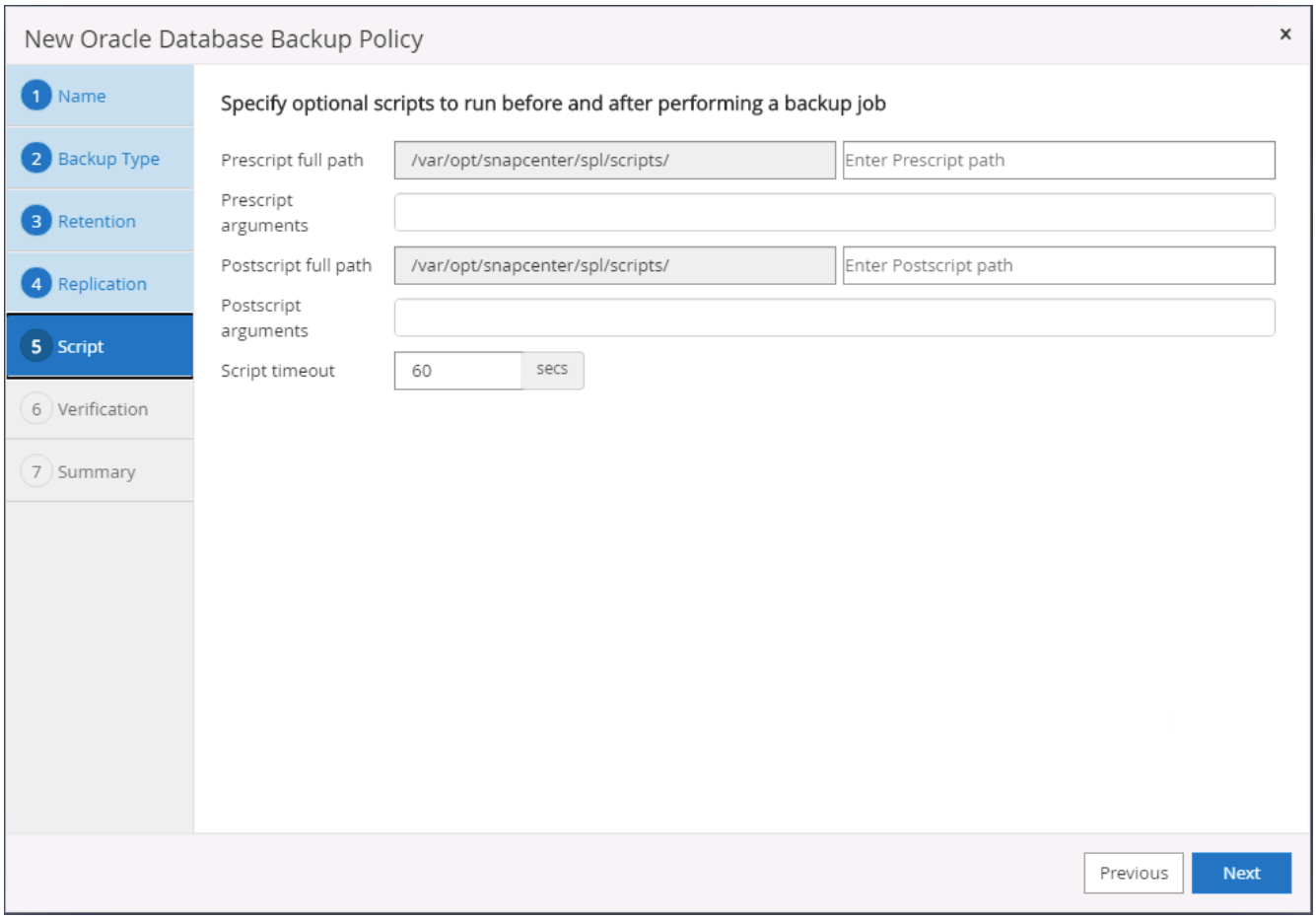
4. Impostare il periodo di conservazione del registro.



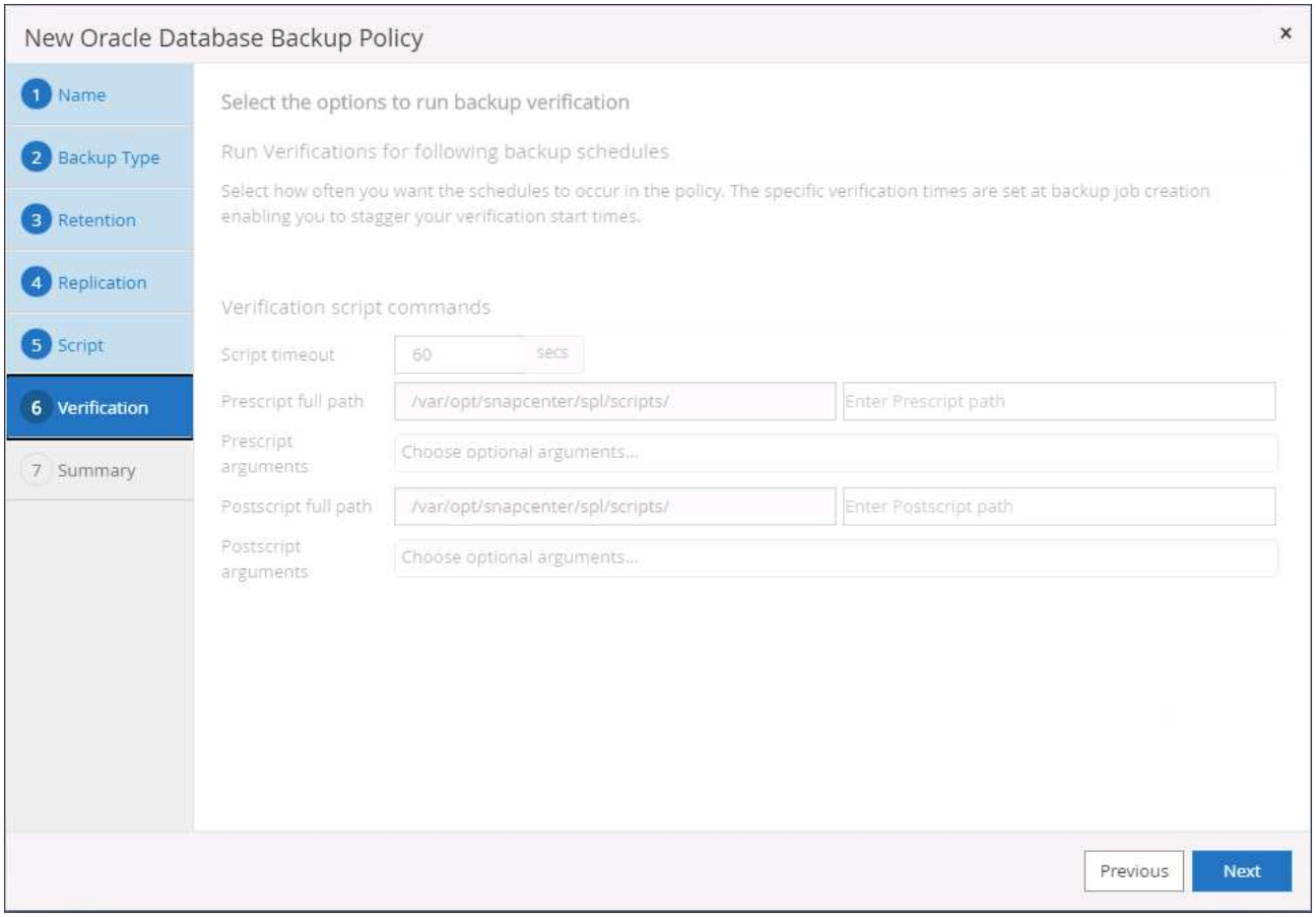
5. Abilitare la replica in una posizione secondaria nel cloud pubblico.



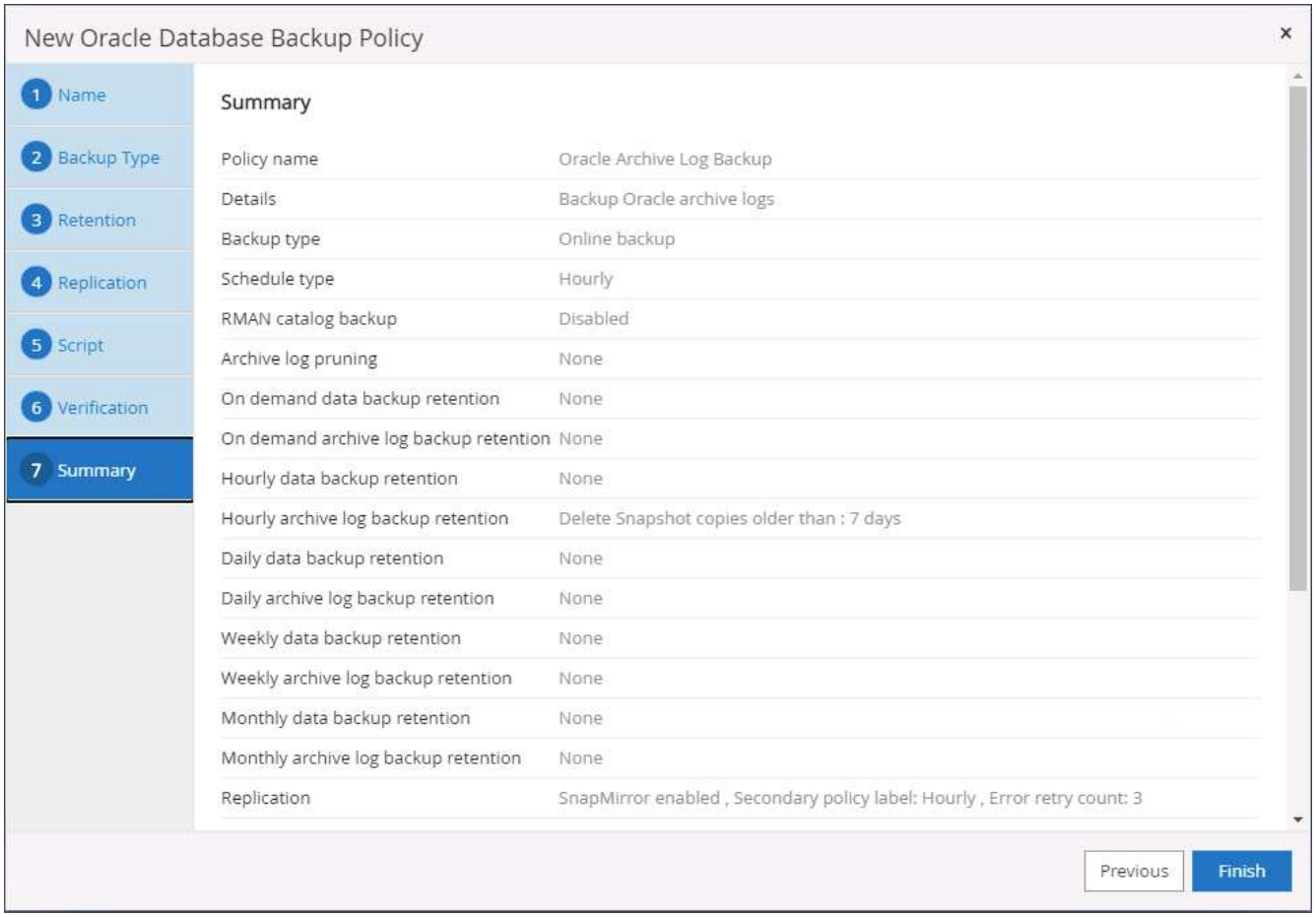
6. Specificare eventuali script opzionali da eseguire prima e dopo il backup del registro.



7. Specificare eventuali script di verifica del backup.

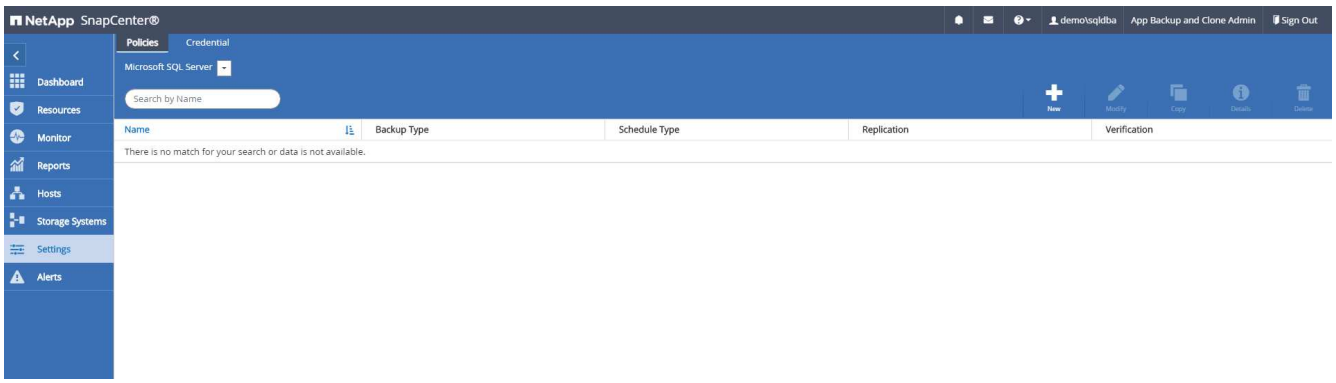

New Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times are set at backup job creation enabling you to stagger your verification start times.
Verification script commands
Script timeout
60
secs
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.

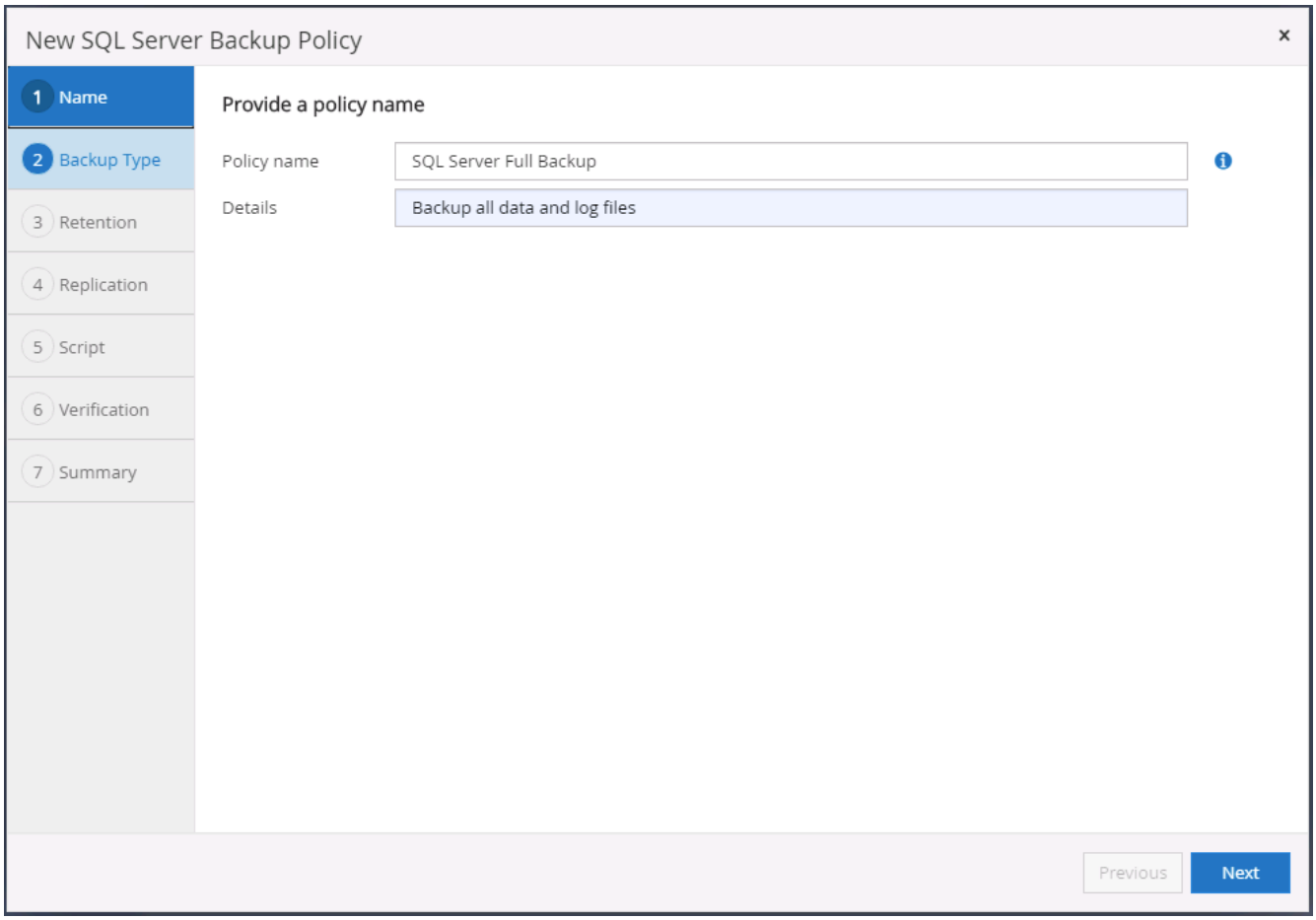


Creare una policy di backup completa del database per SQL

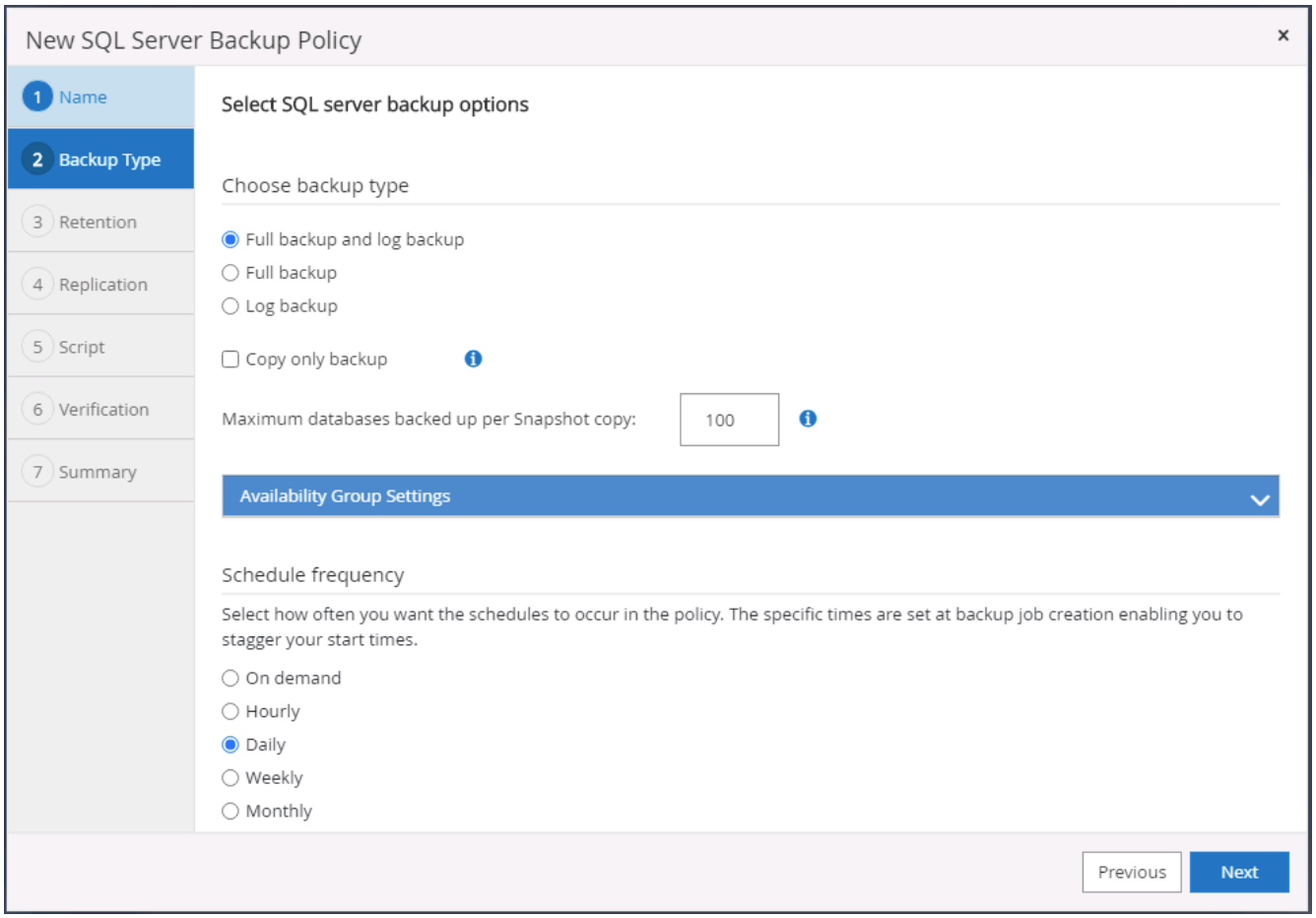
1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.



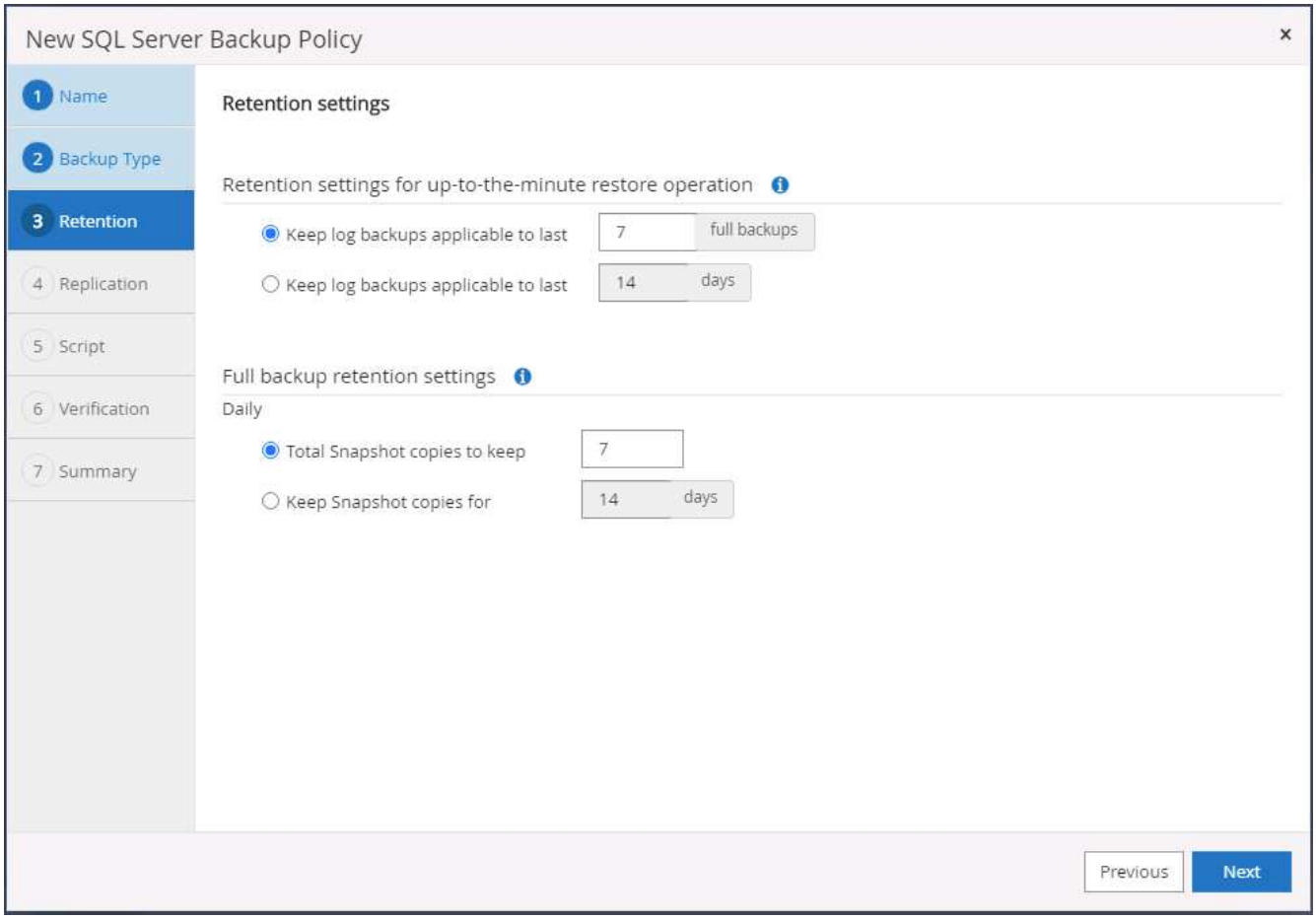
2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.



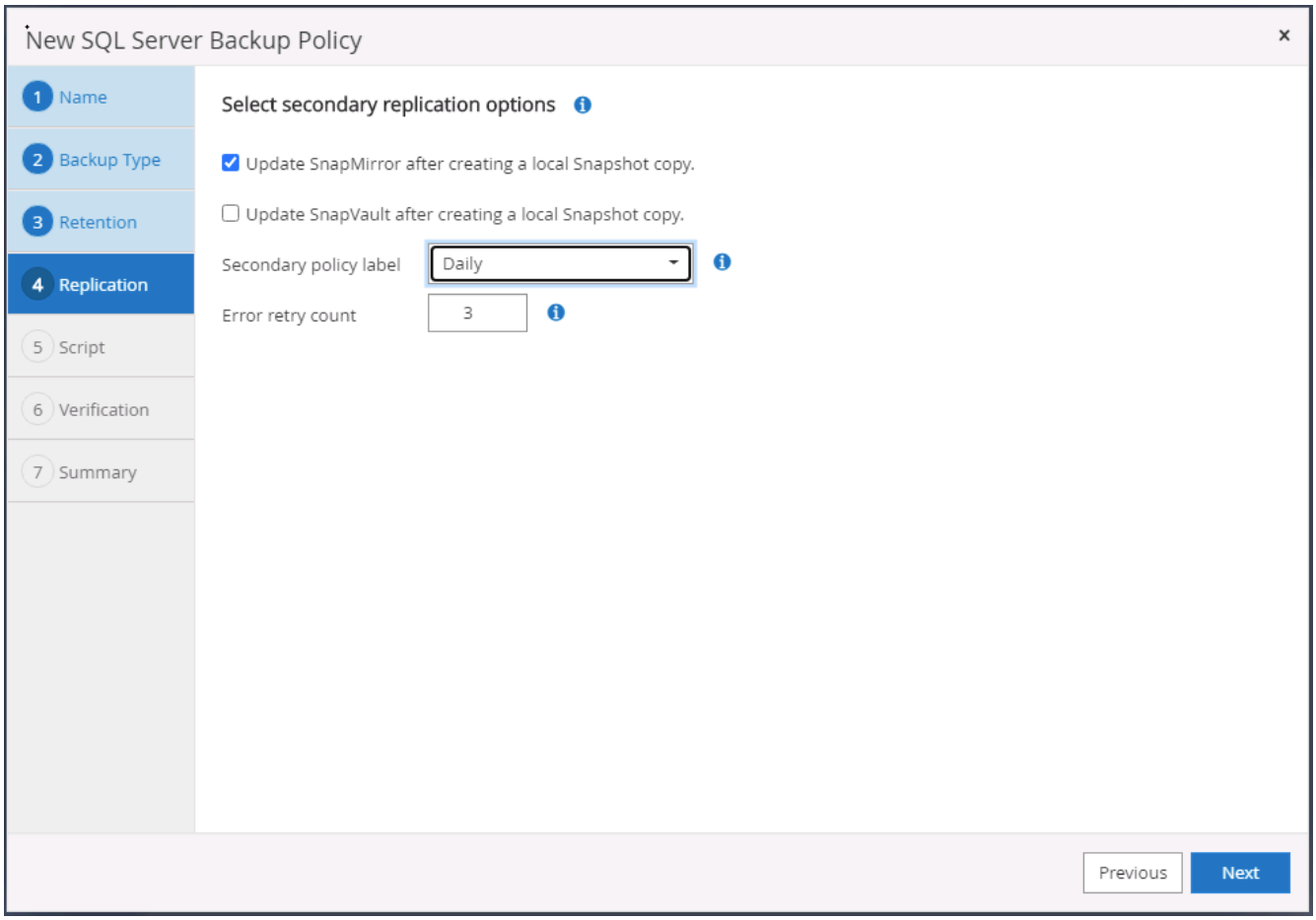
3. Definire l'opzione di backup e la frequenza di pianificazione. Per SQL Server configurato con un gruppo di disponibilità, è possibile impostare una replica di backup preferita.



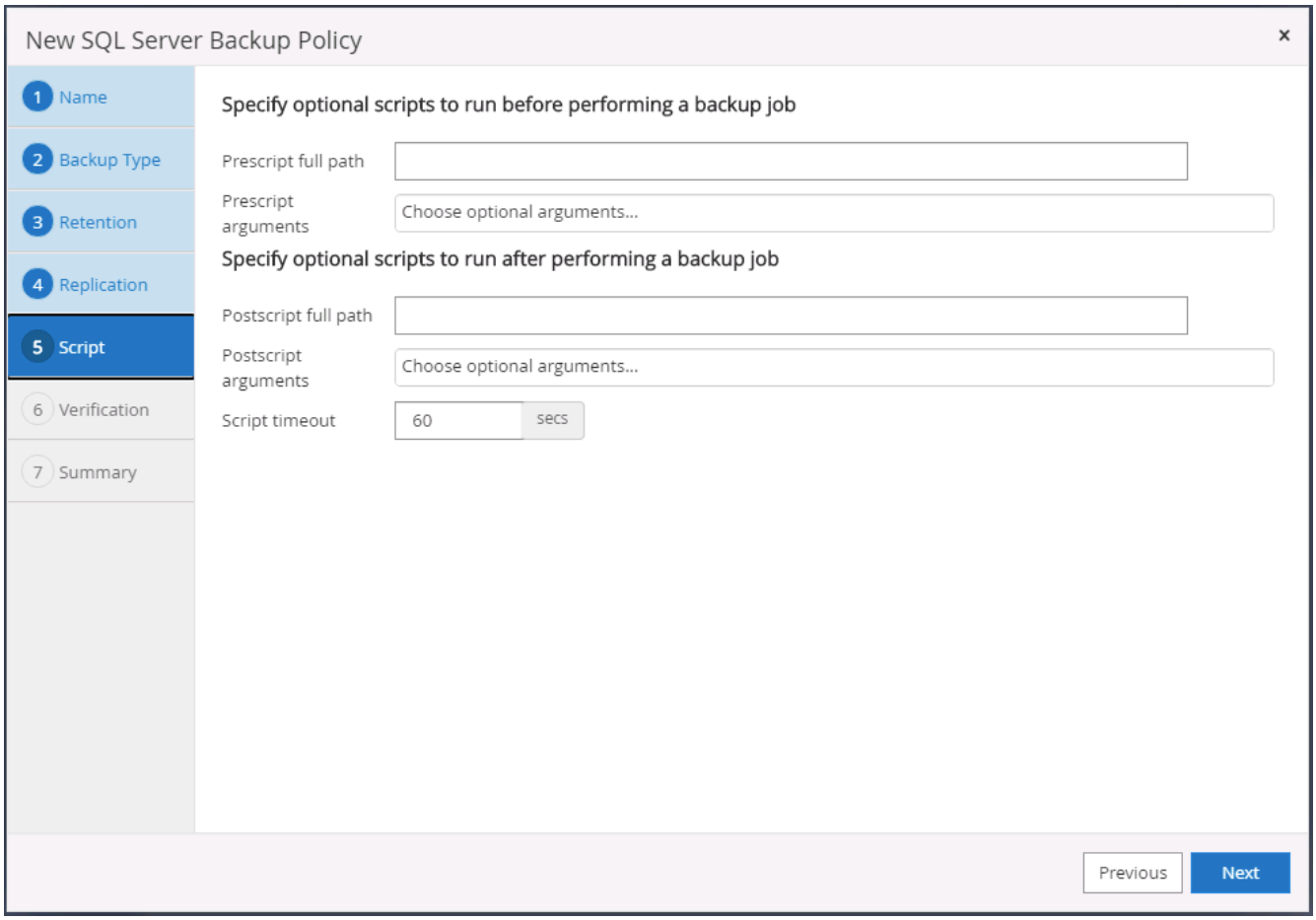
4. Impostare il periodo di conservazione del backup.



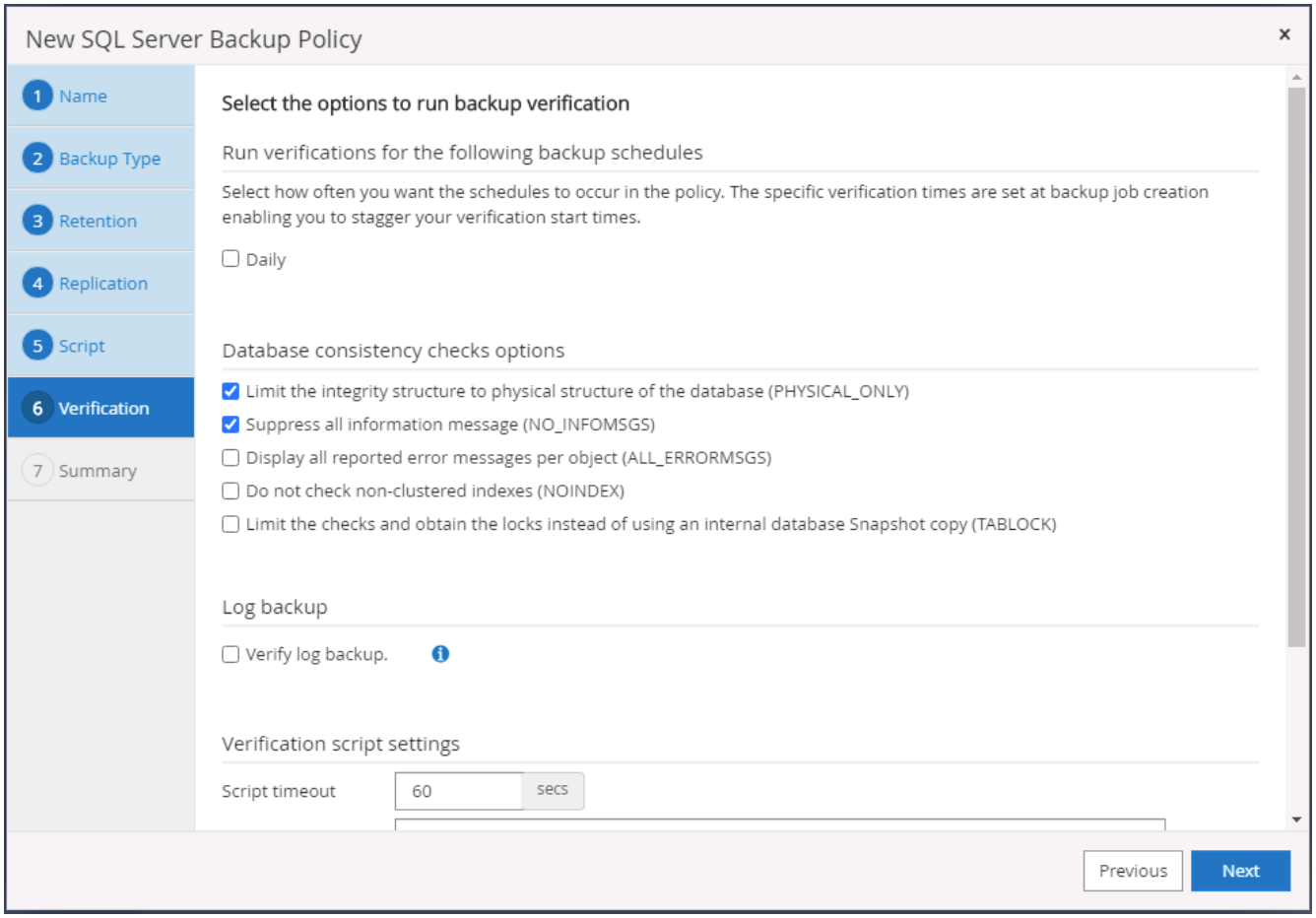
5. Abilitare la replica delle copie di backup in una posizione secondaria nel cloud.



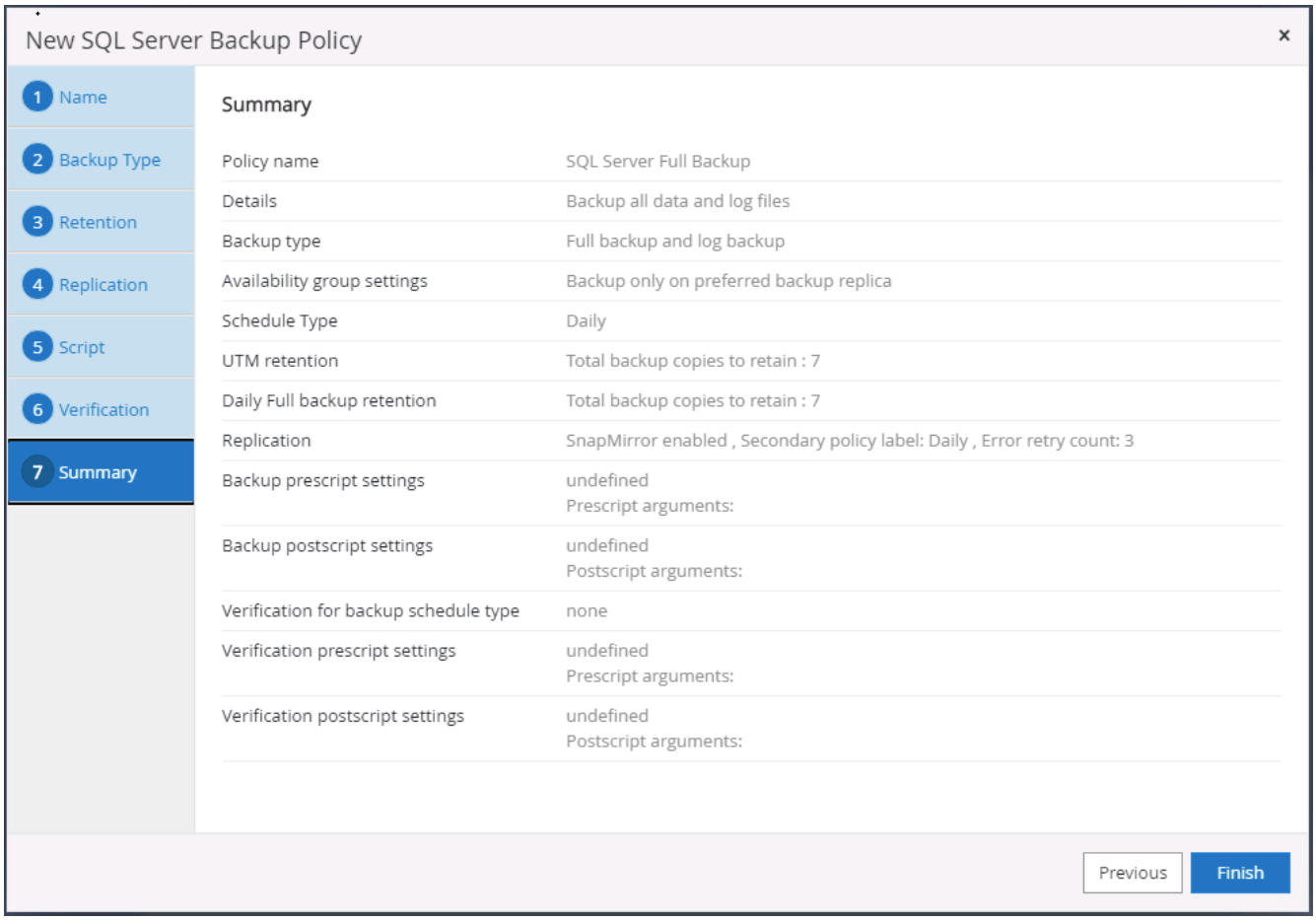
6. Specificare eventuali script opzionali da eseguire prima o dopo un processo di backup.



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

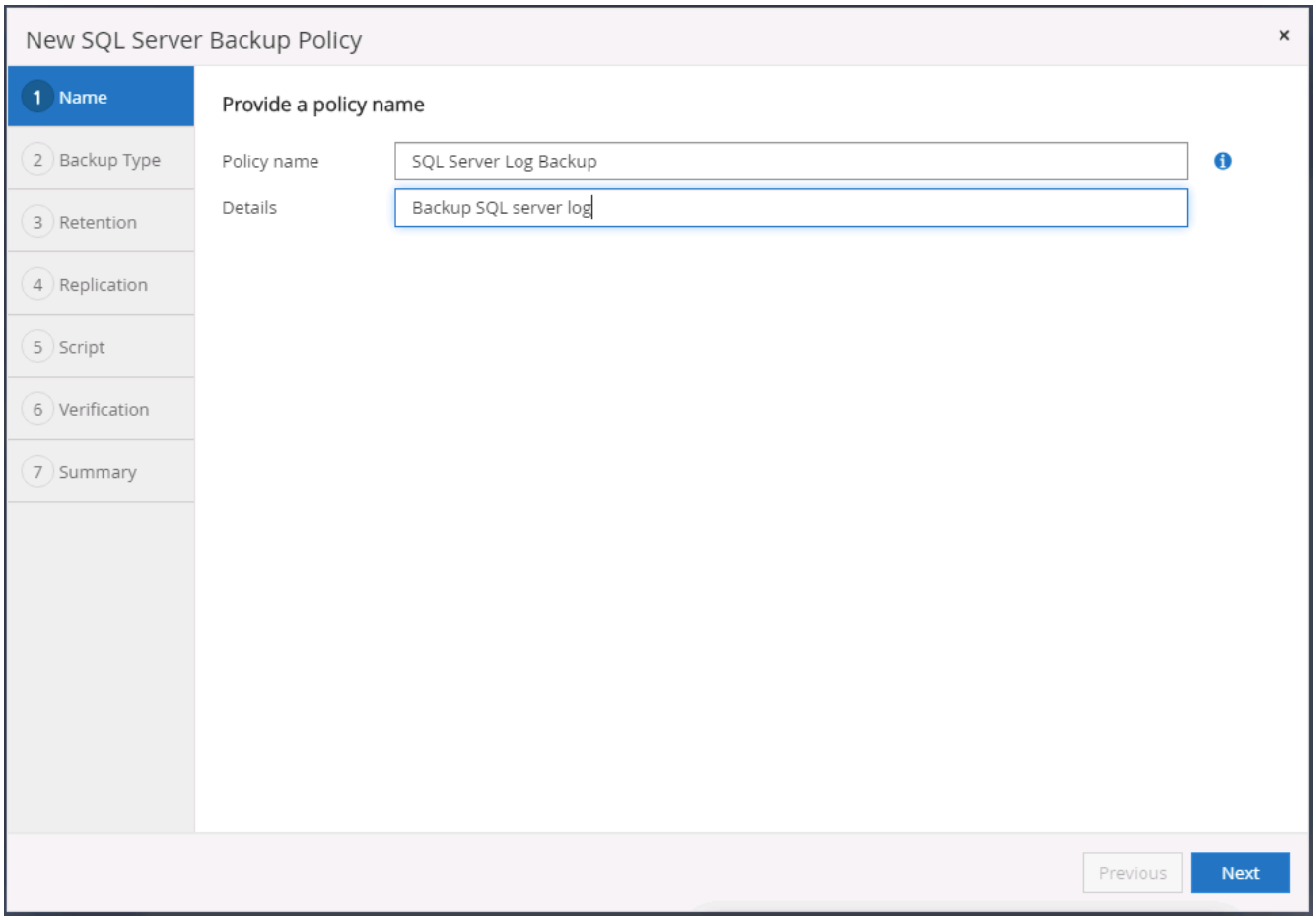

New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run verifications for the following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times 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_ERRORMSGS)
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
60
secs
Previous
Next

8. Riepilogo.

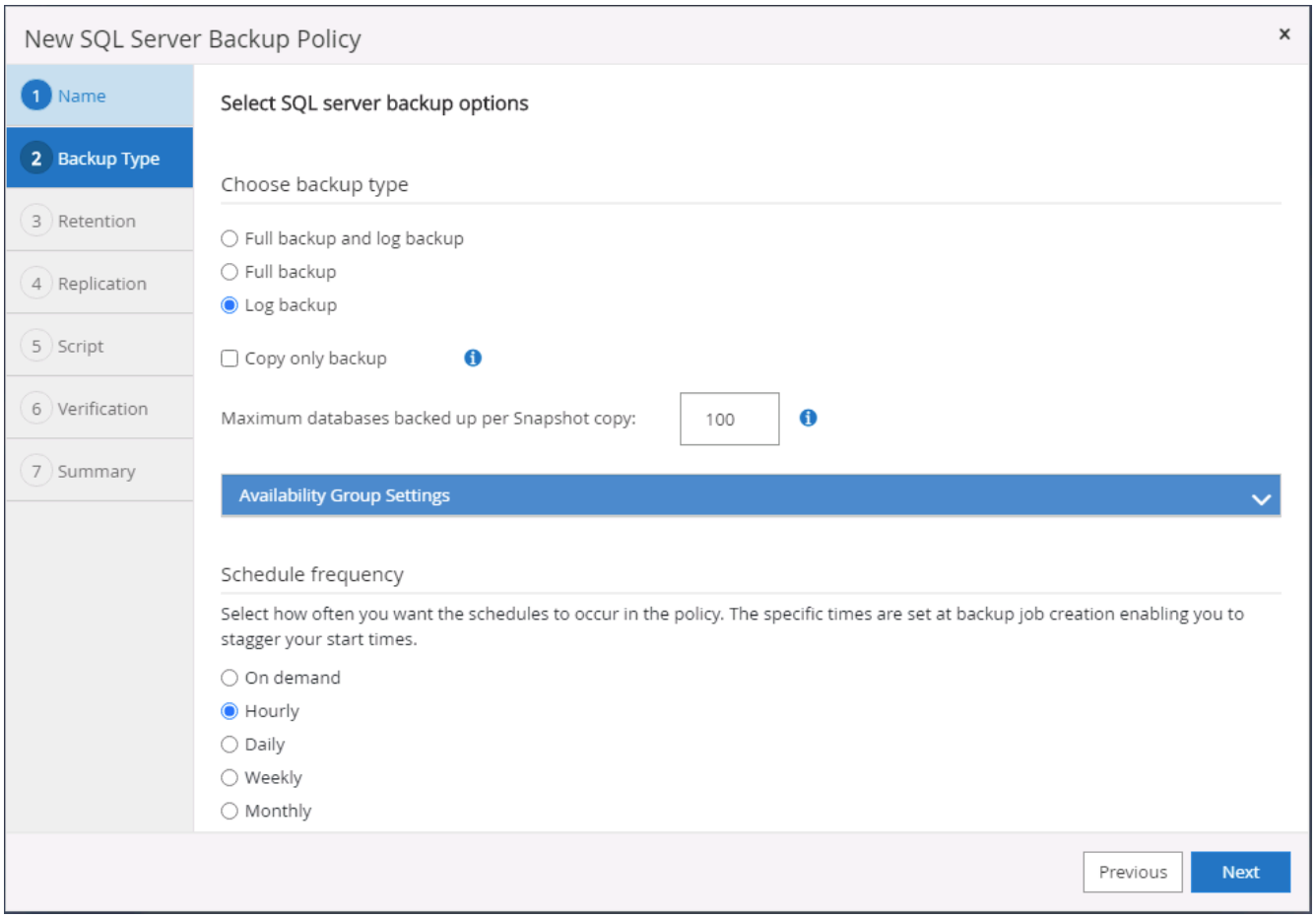


Creare un criterio di backup del log del database per SQL.

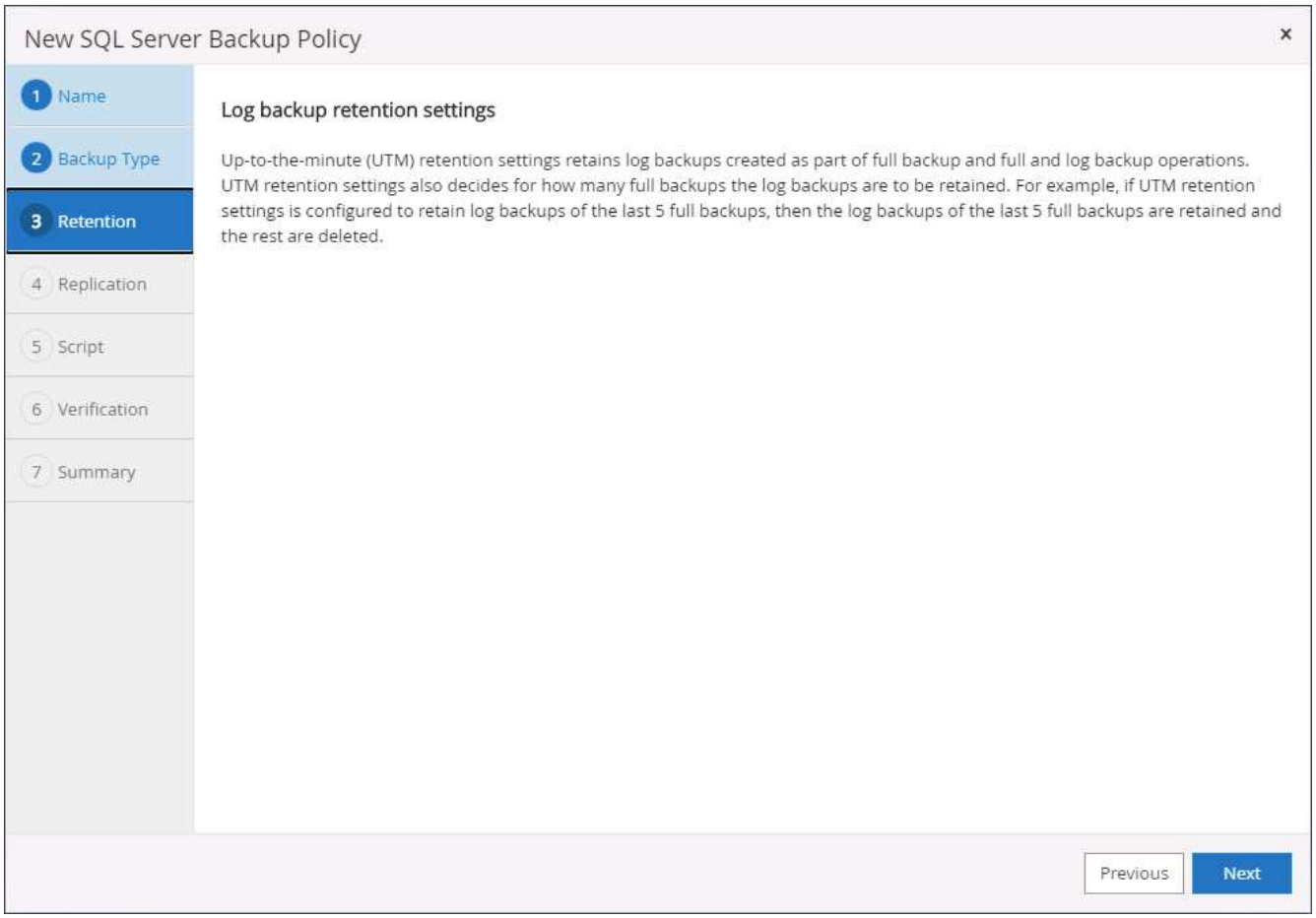
1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni > Criteri, quindi su nuovo per avviare un nuovo flusso di lavoro per la creazione di policy.



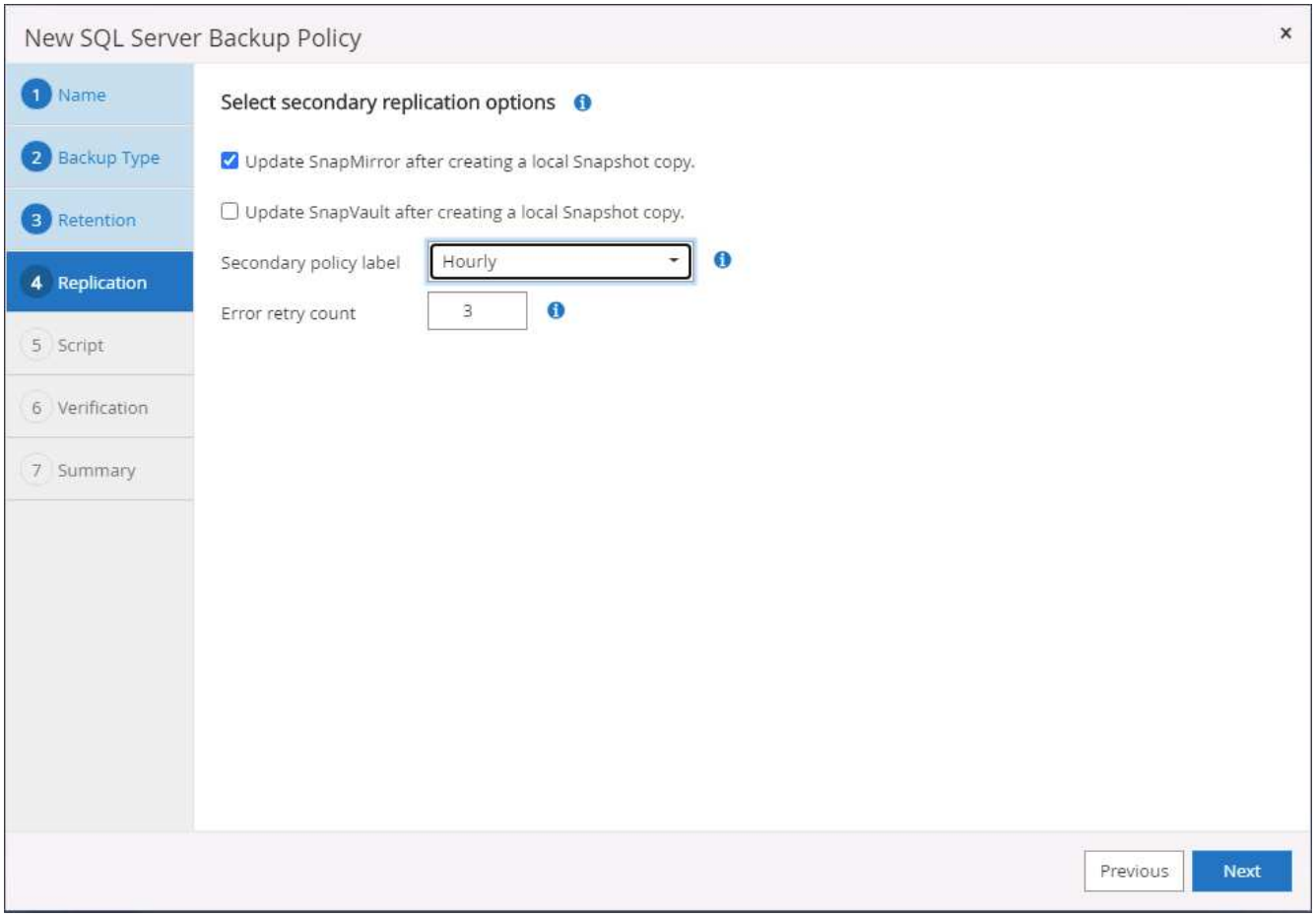
2. Definire l'opzione di backup del registro e la frequenza di pianificazione. Per SQL Server configurato con un gruppo di disponibilità, è possibile impostare una replica di backup preferita.



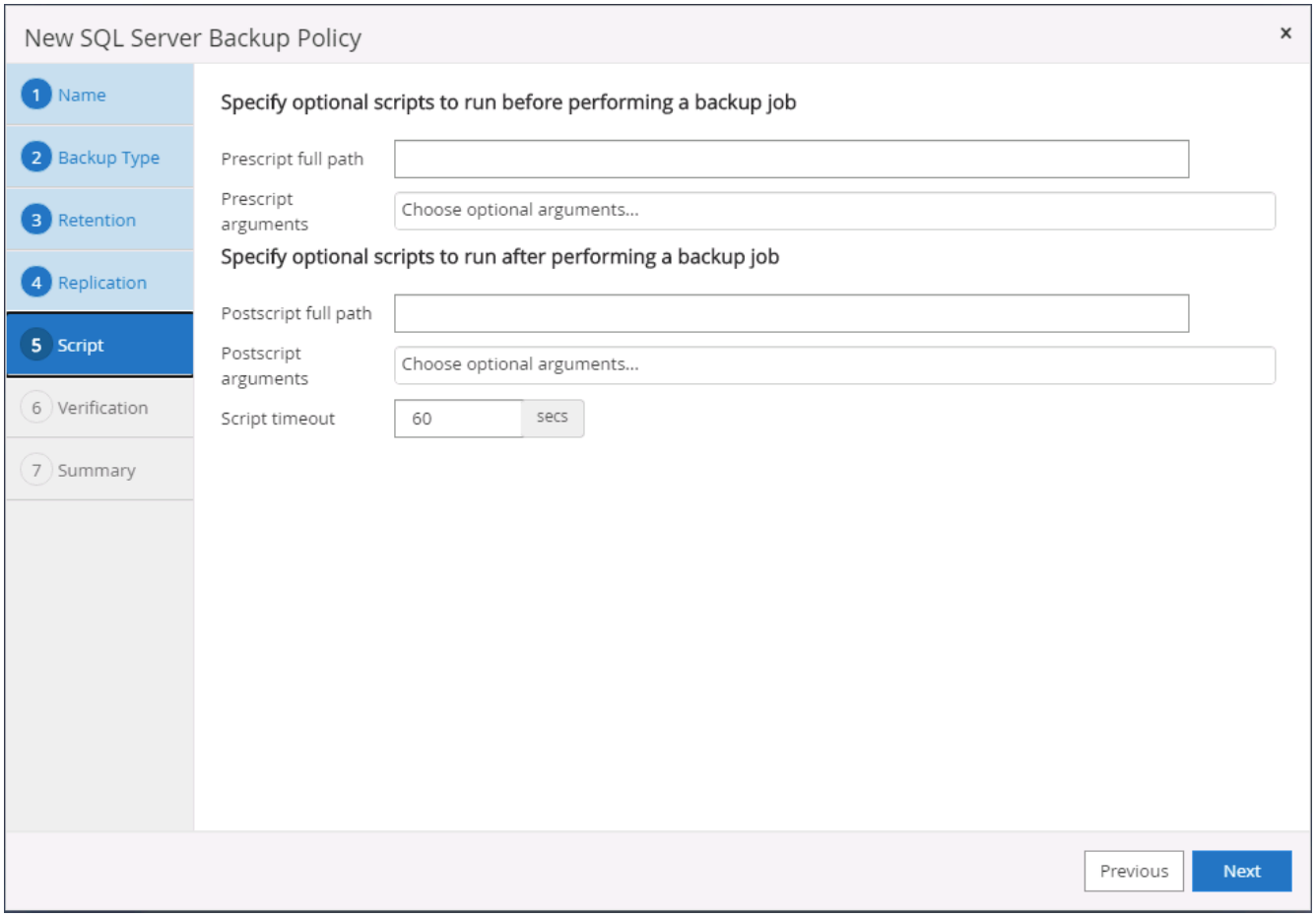
3. Il criterio di backup dei dati di SQL Server definisce la conservazione del backup del registro; accettare i valori predefiniti qui.



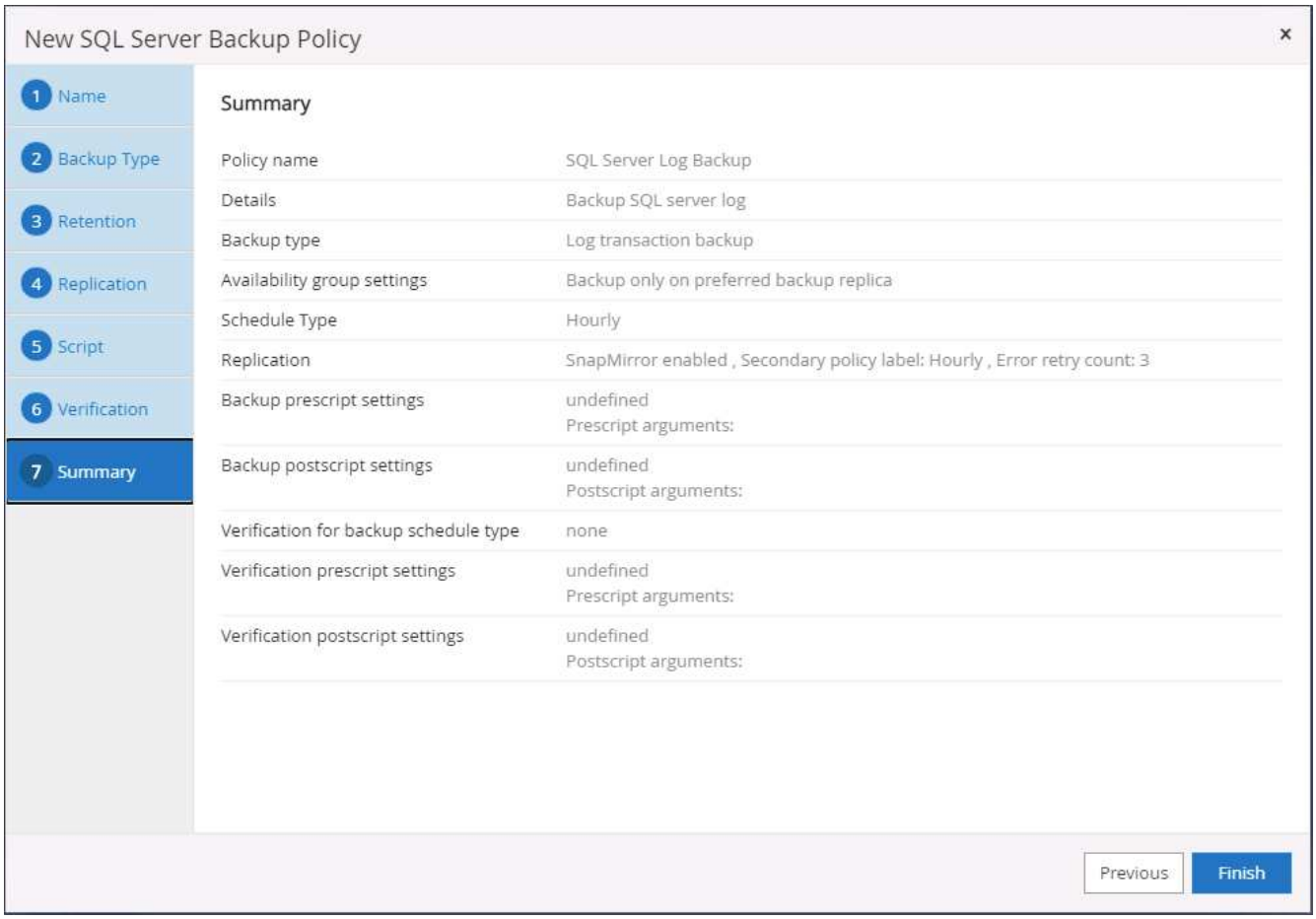
4. Abilitare la replica del backup dei log su secondario nel cloud.



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
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

6. Riepilogo.

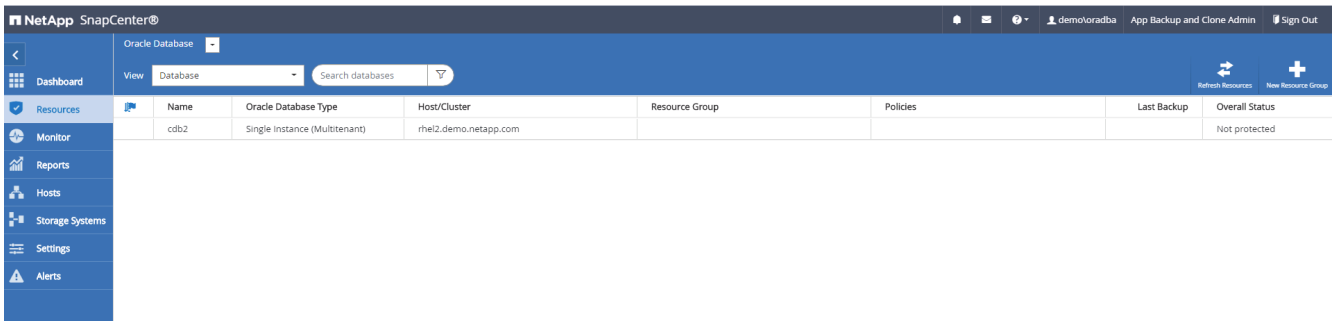


8. Implementare policy di backup per proteggere il database

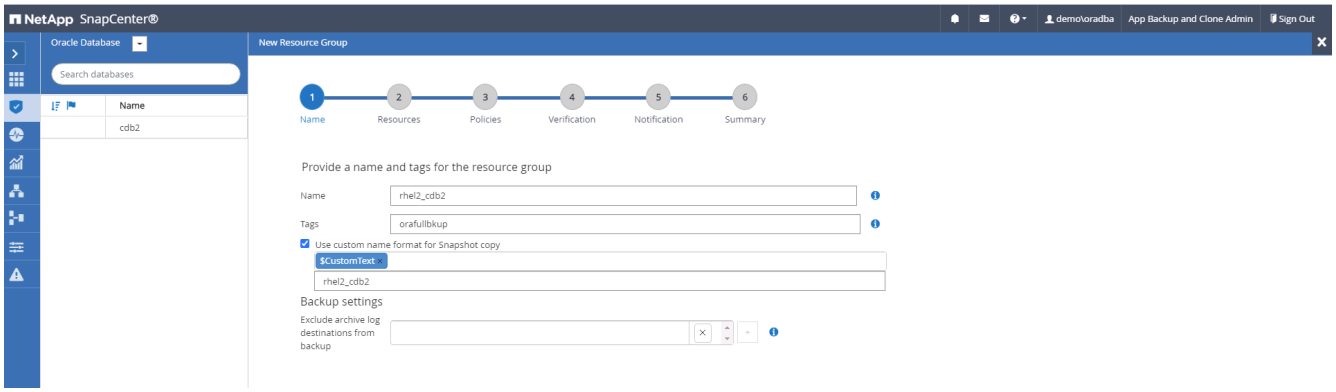
SnapCenter utilizza un gruppo di risorse per eseguire il backup di un database in un gruppo logico di risorse di database, ad esempio più database ospitati su un server, un database che condivide gli stessi volumi di storage, più database che supportano un'applicazione di business e così via. La protezione 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

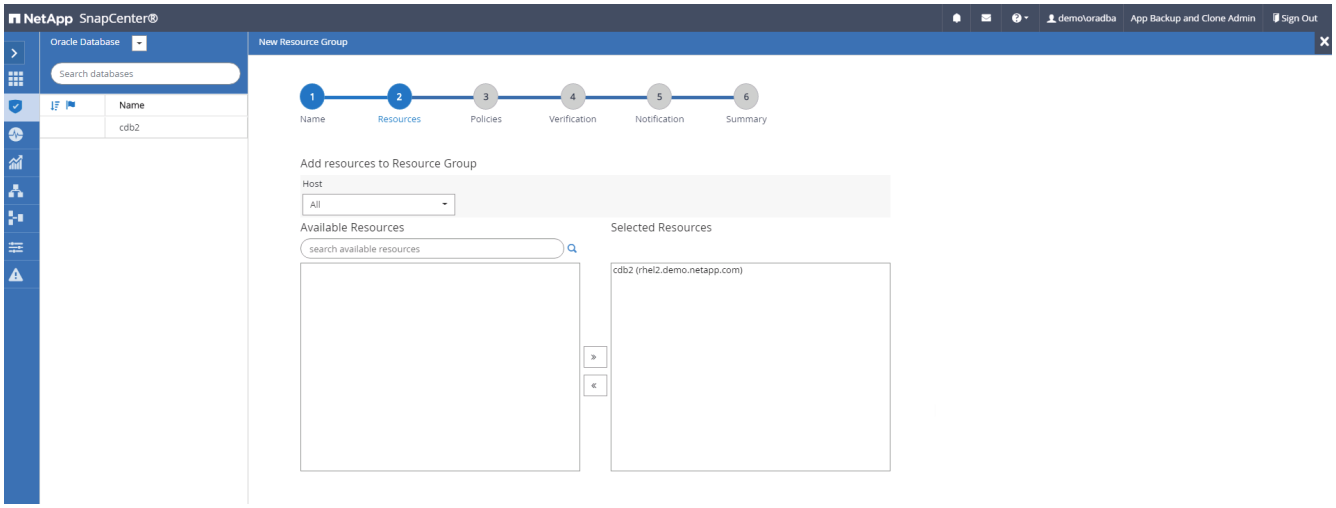
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.



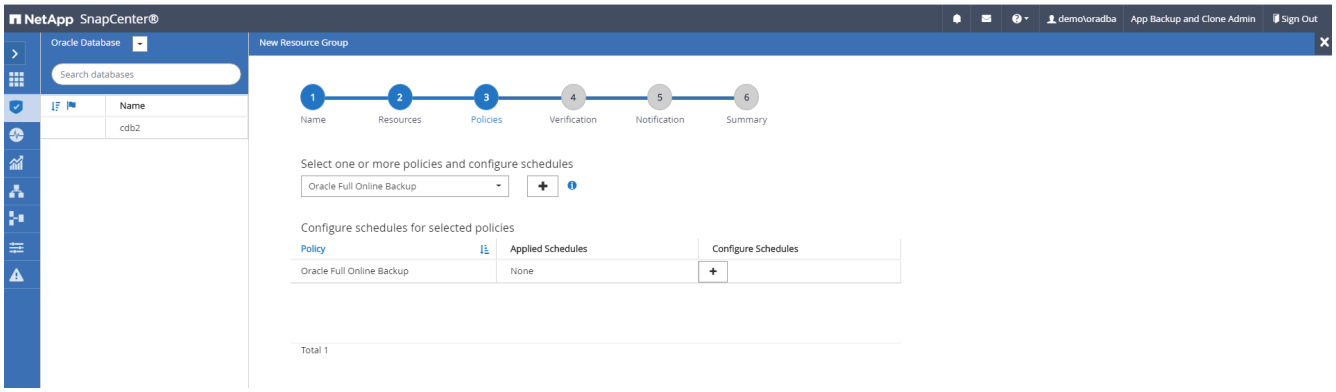
2. Fornire un nome e tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archiviazione ridondante, se configurata.



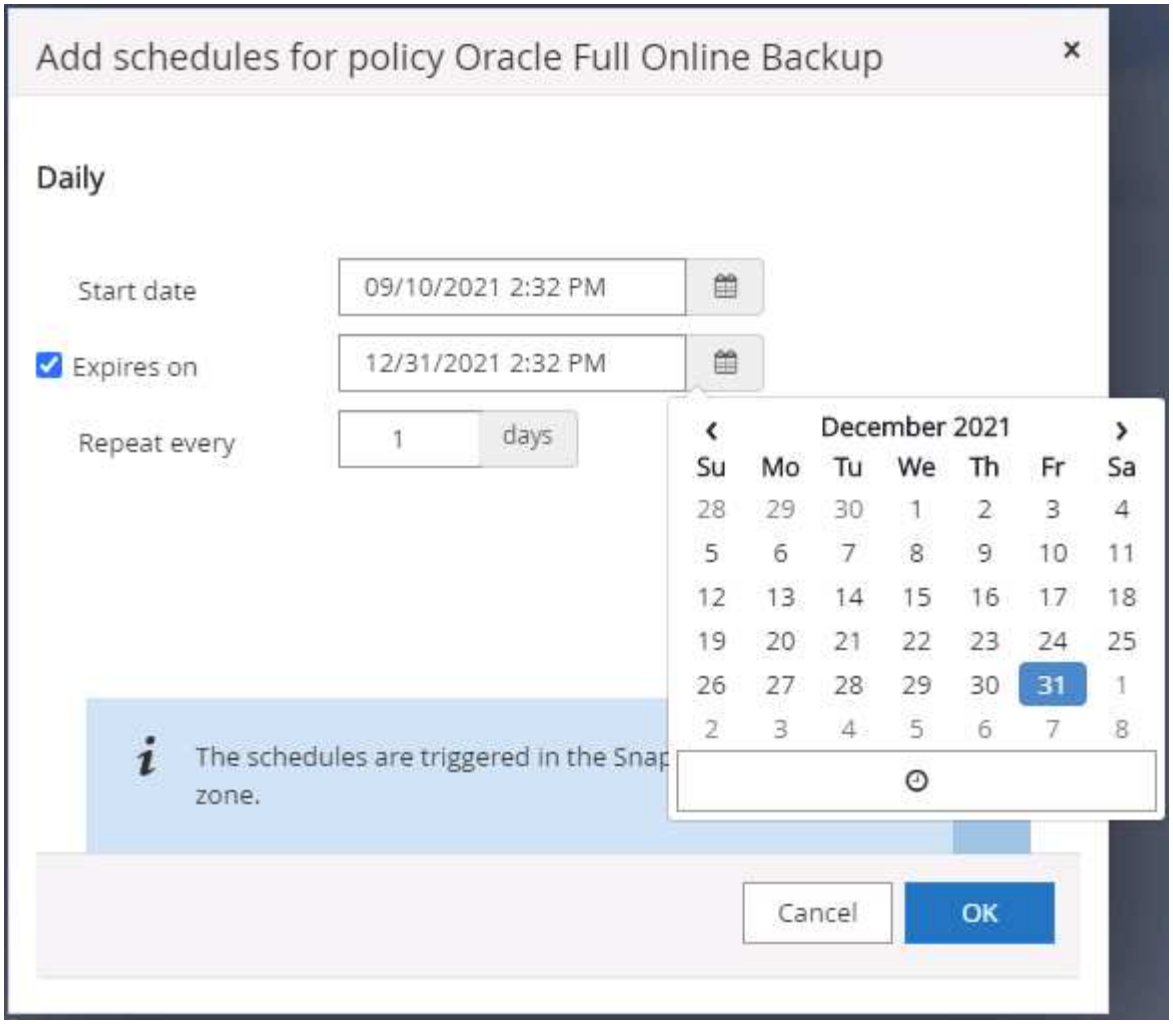
3. Aggiungere risorse di database al gruppo di risorse.



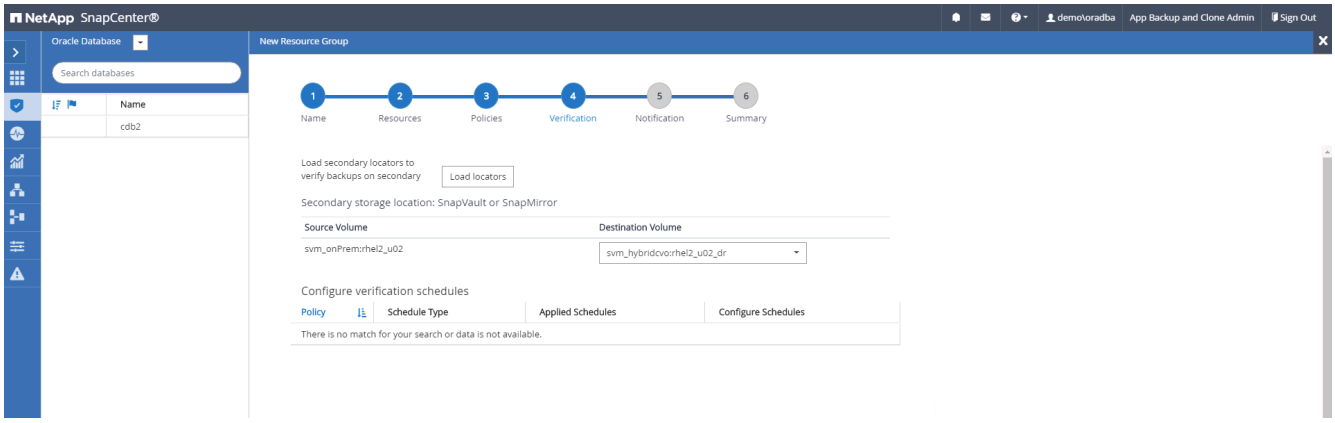
4. Selezionare una policy di backup completa creata nella sezione 7 dall'elenco a discesa.



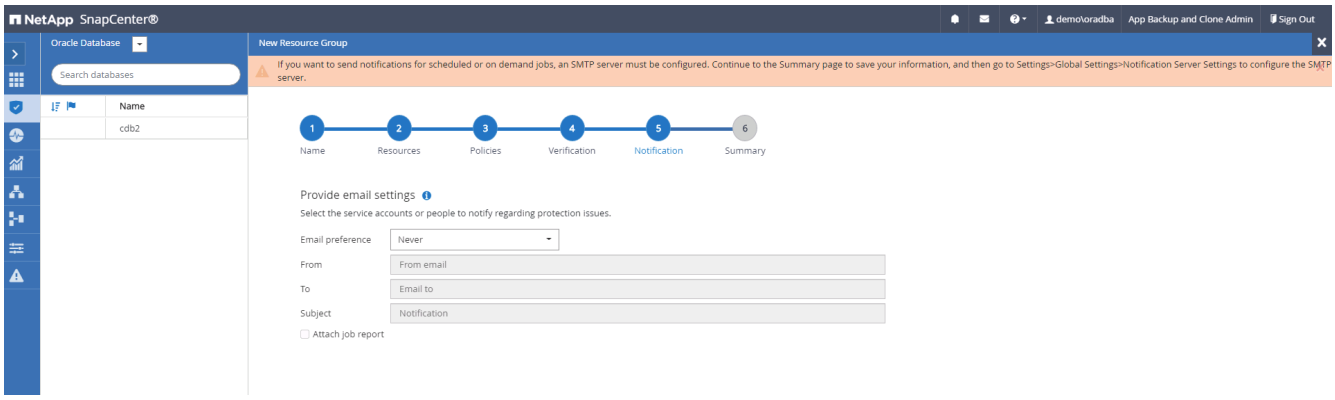
5. Fare clic sul segno (+) per configurare la pianificazione di backup desiderata.



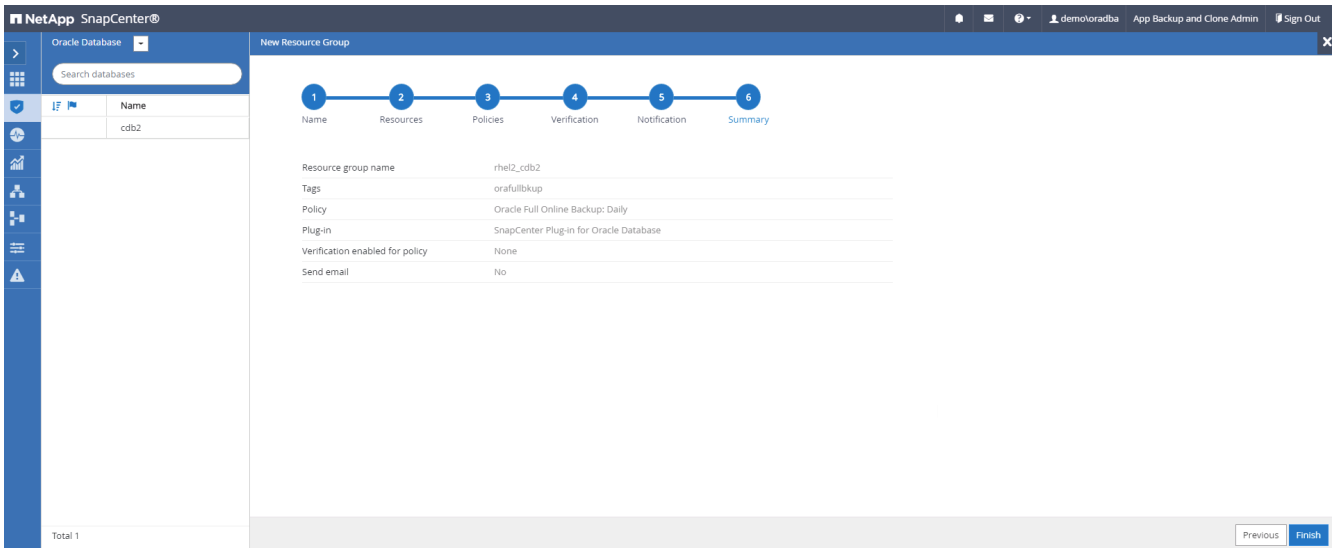
6. Fare clic su Load Locators (carica locatori) per caricare il volume di origine e di destinazione.



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

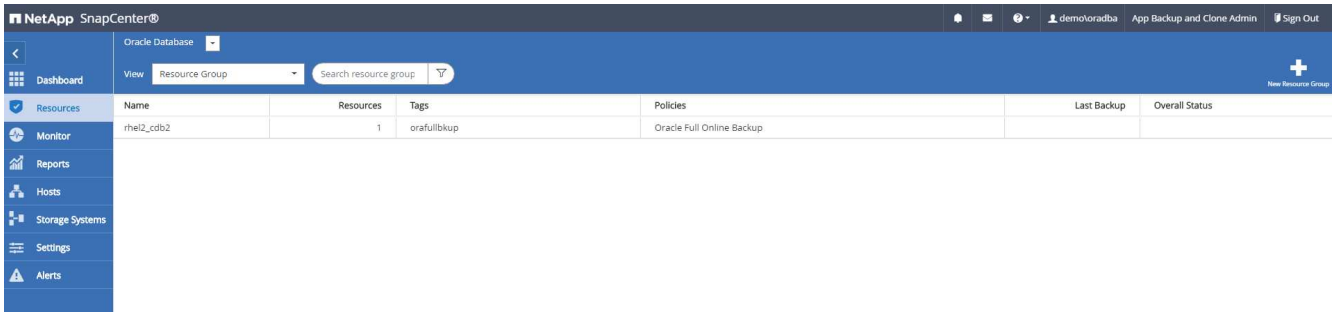


8. Riepilogo.

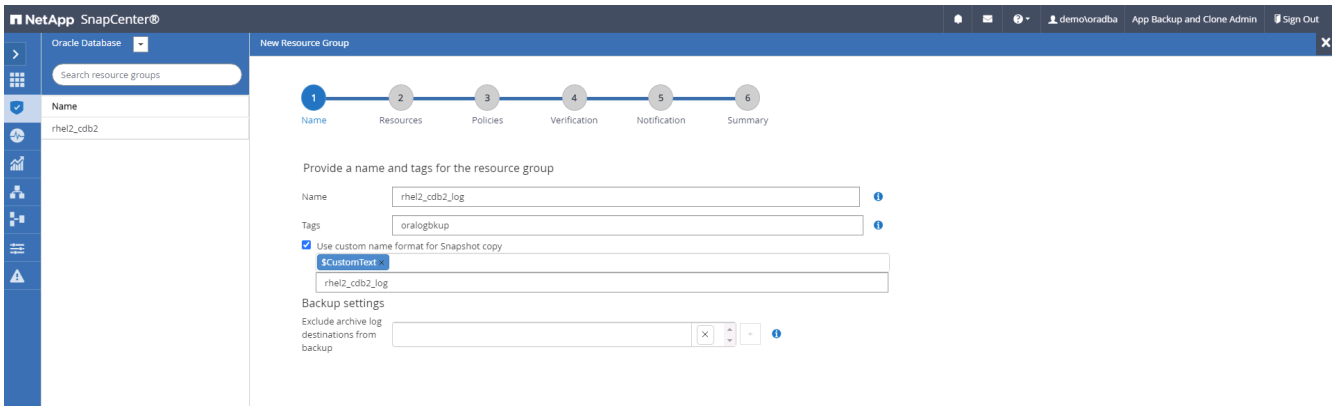


Creare un gruppo di risorse per il backup dei log di Oracle

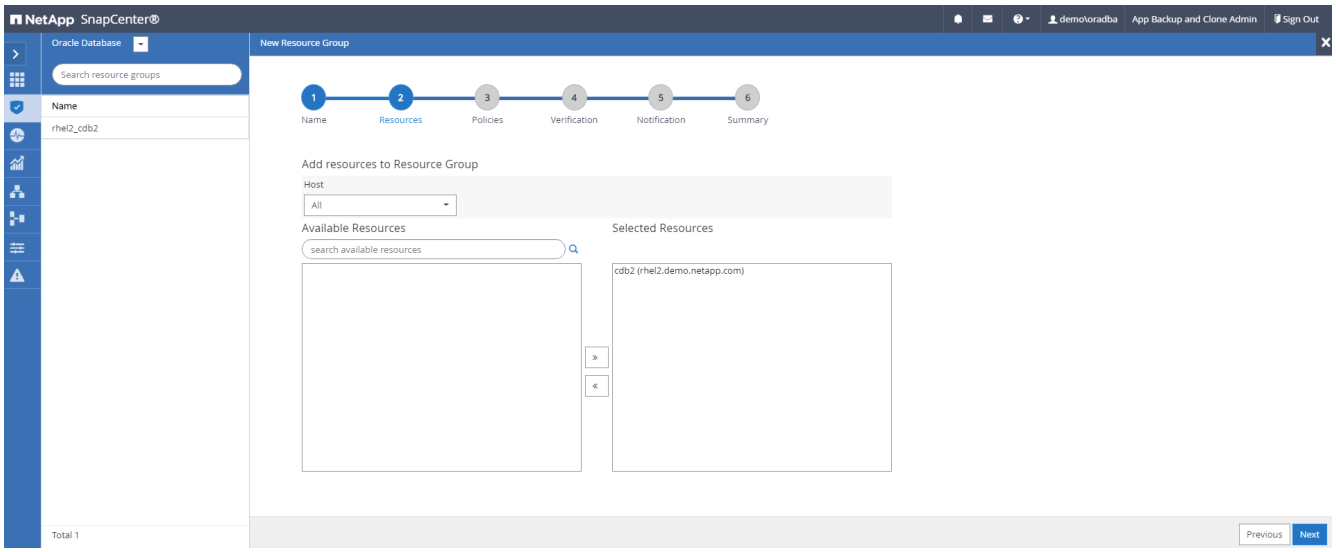
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.



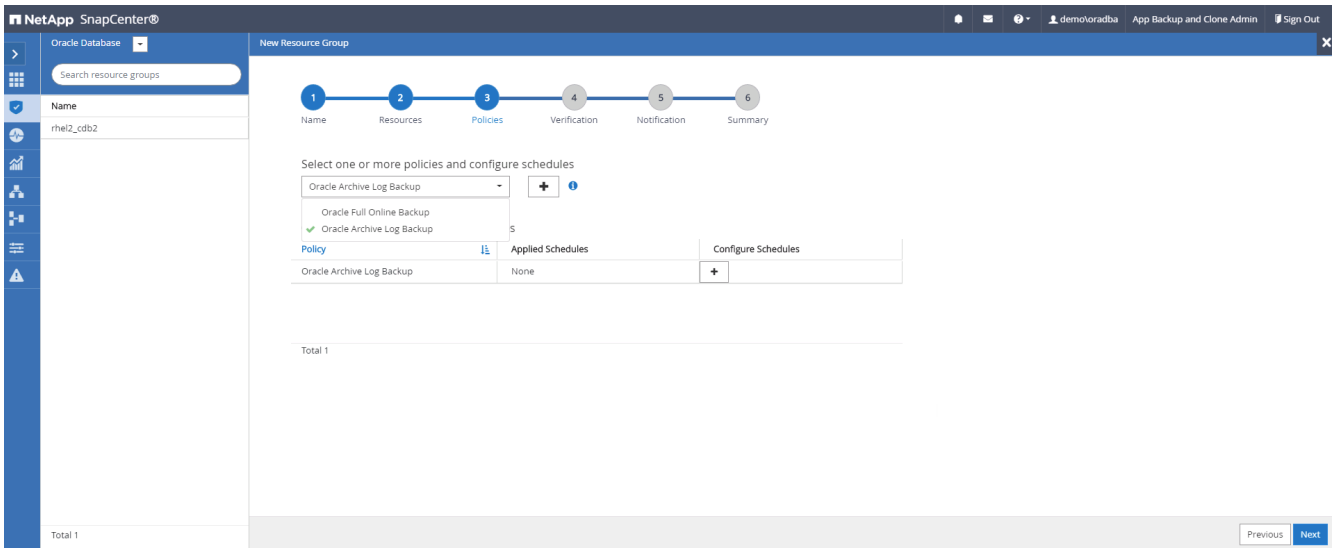
2. Fornire un nome e tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archiviazione ridondante, se configurata.



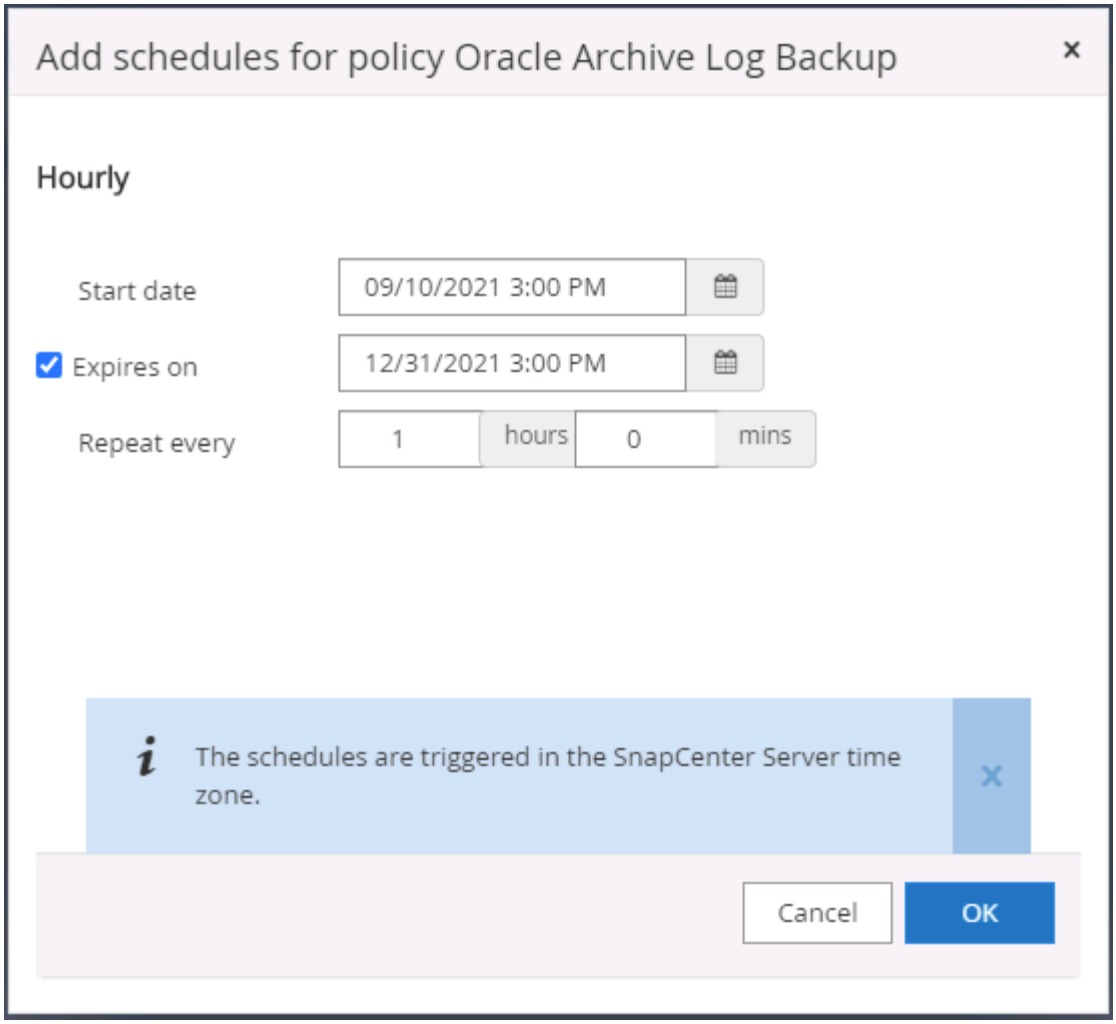
3. Aggiungere risorse di database al gruppo di risorse.



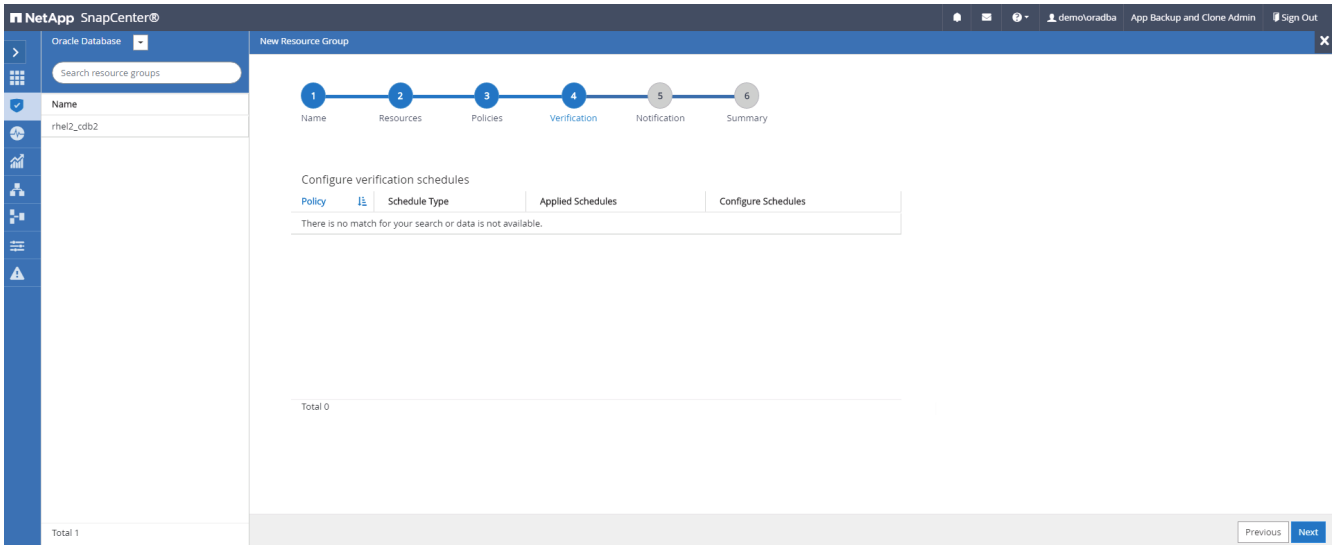
4. Selezionare un criterio di backup del registro creato nella sezione 7 dall'elenco a discesa.



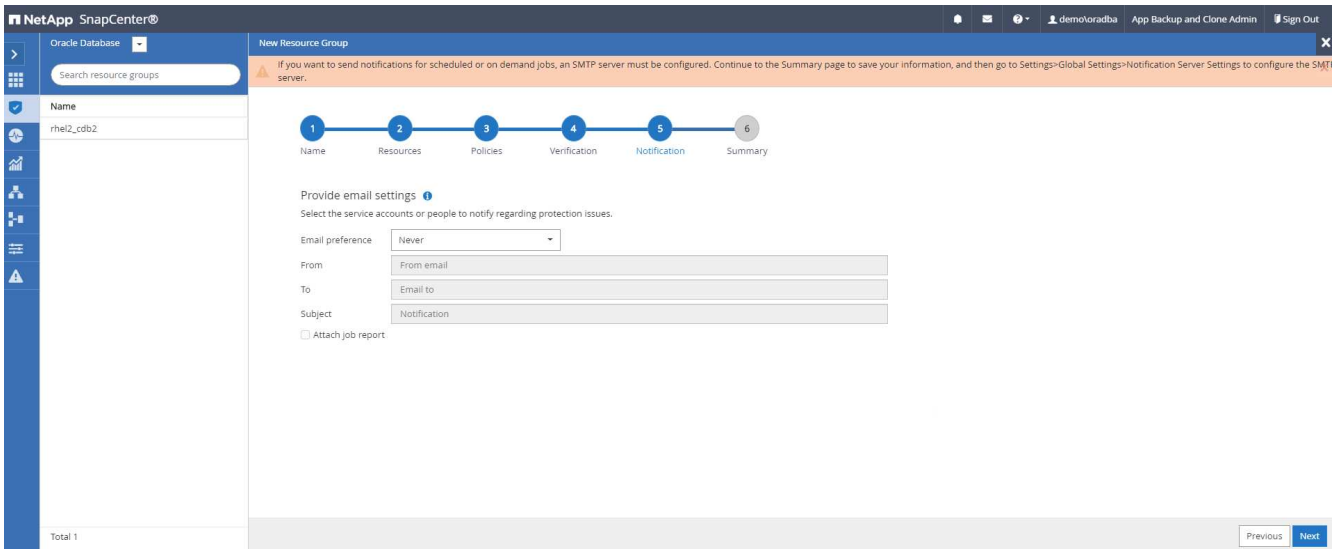
5. Fare clic sul segno (+) per configurare la pianificazione di backup desiderata.



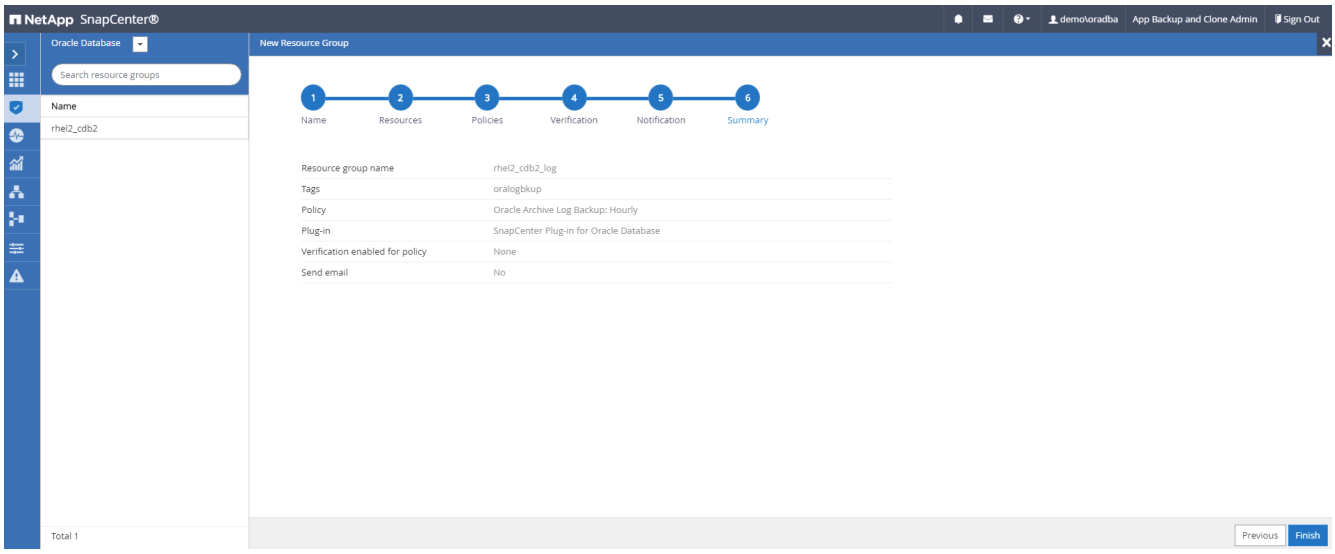
6. Se la verifica del backup è configurata, viene visualizzata qui.



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

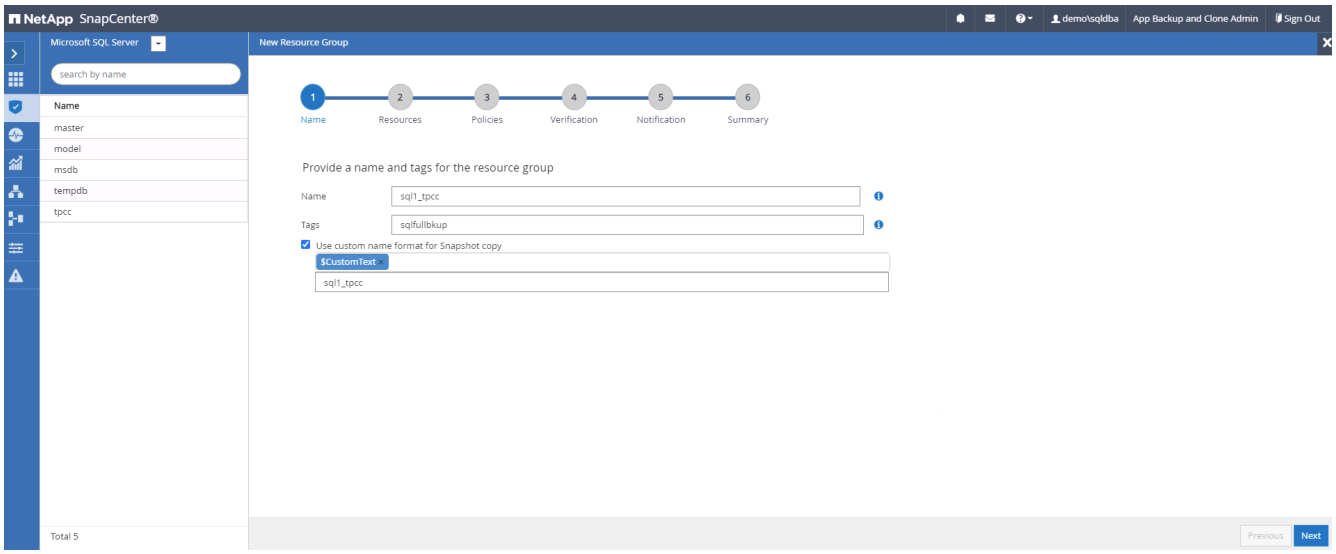


8. Riepilogo.

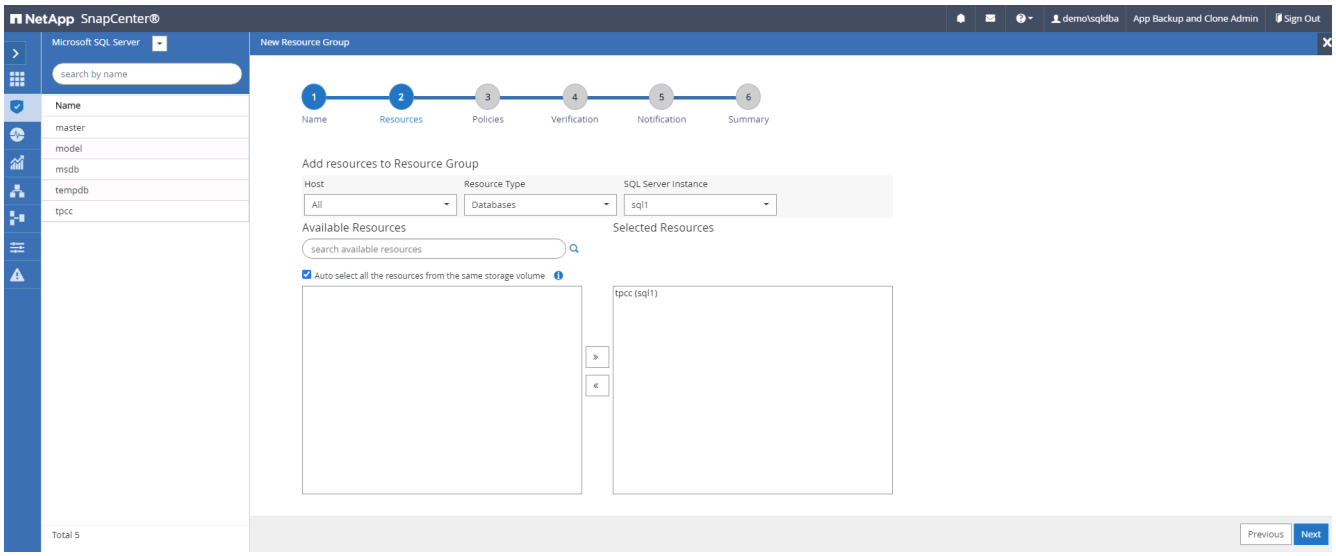


Creare un gruppo di risorse per il backup completo di SQL Server

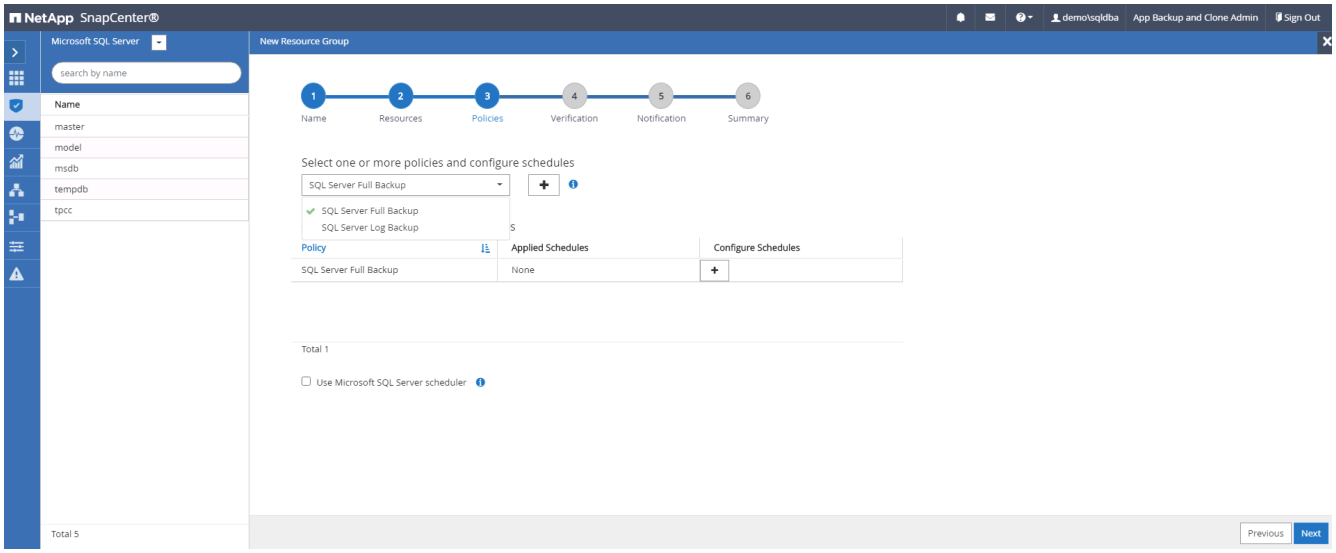
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire un nome e tag per il gruppo di risorse. È possibile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



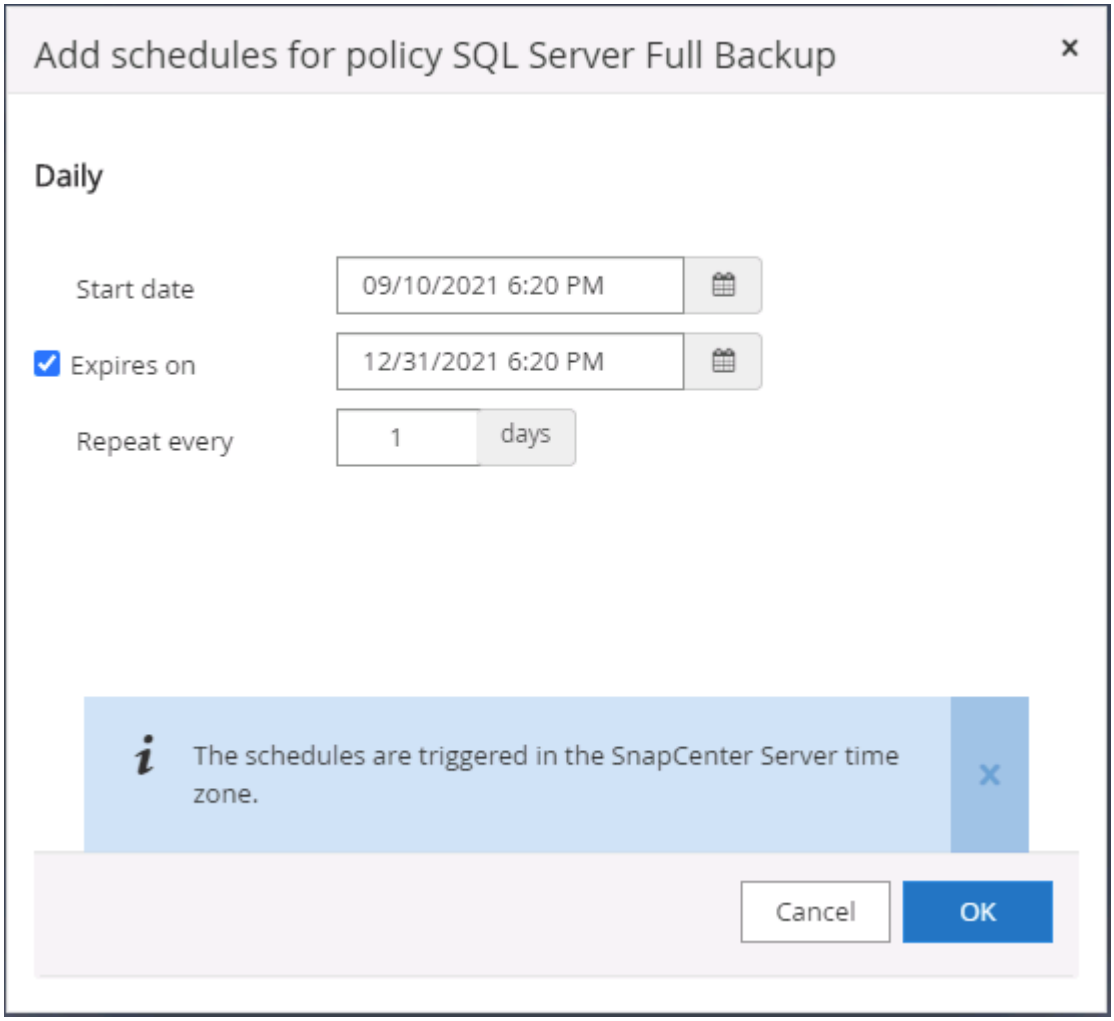
2. Selezionare le risorse di database di cui eseguire il backup.



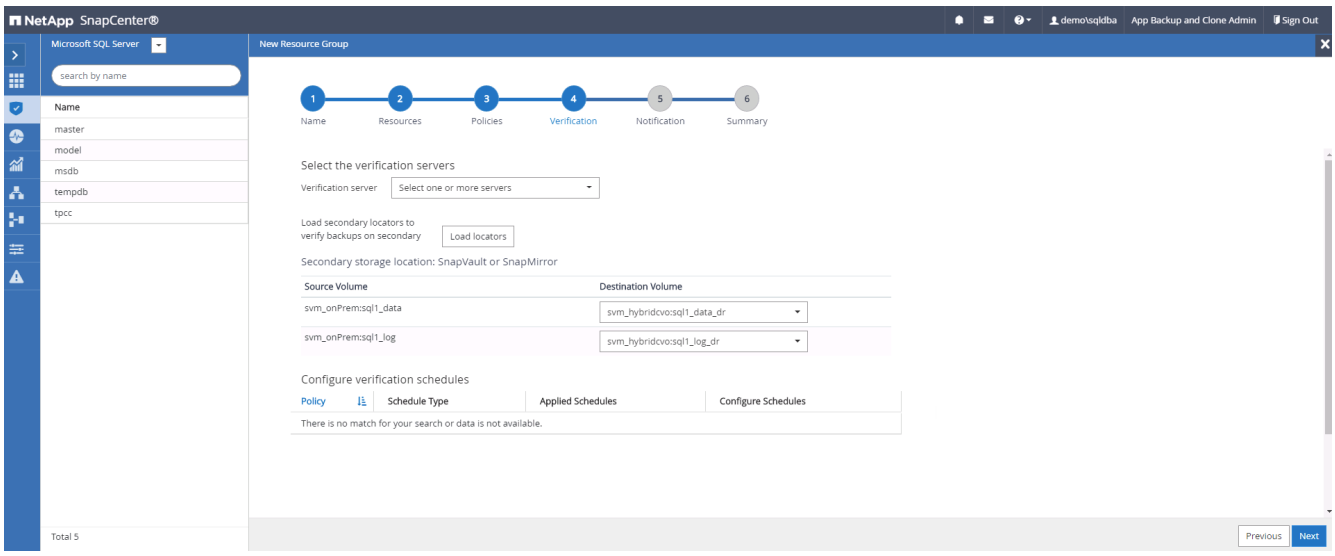
3. Selezionare una policy di backup SQL completa creata nella sezione 7.



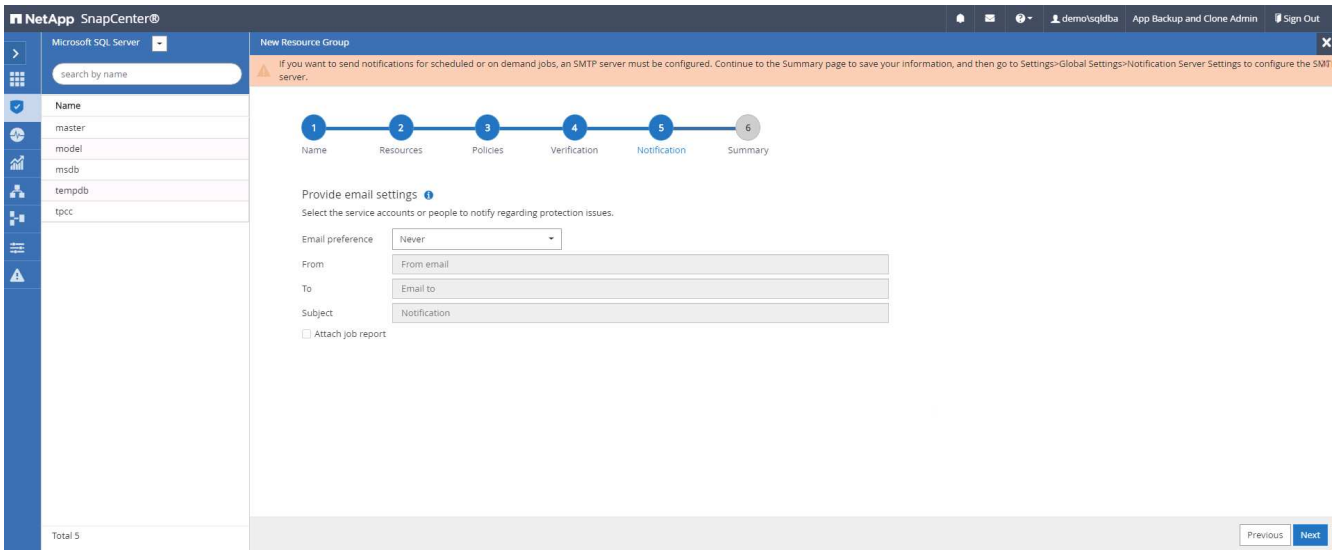
4. Aggiungi tempi esatti per i backup e la frequenza.



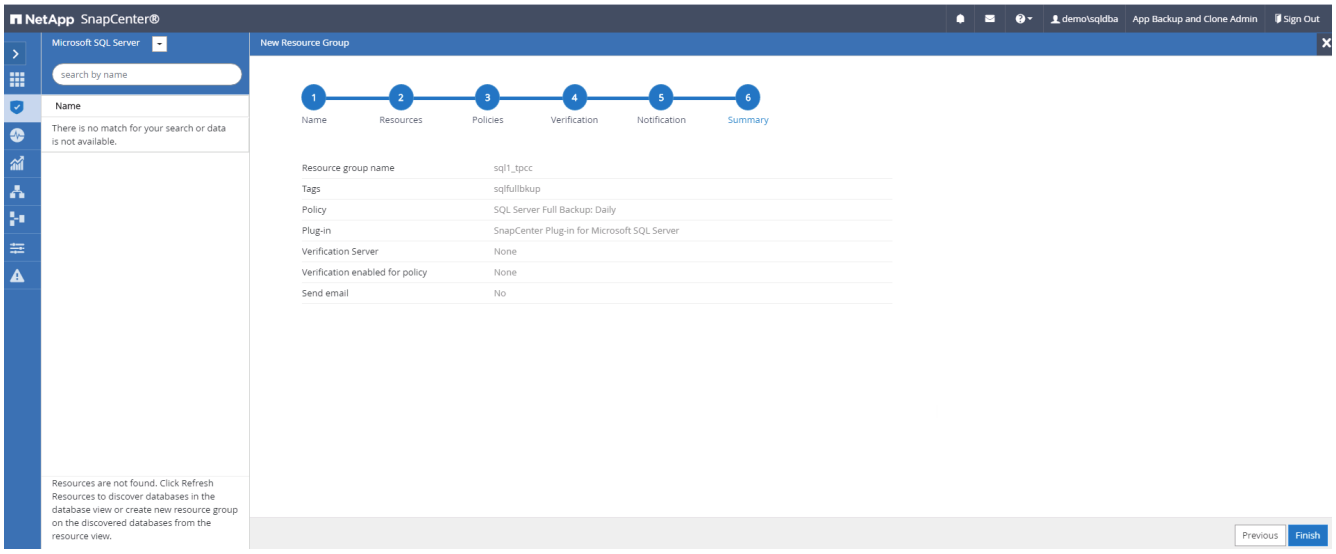
5. Scegliere il server di verifica per il backup su secondario se deve essere eseguita la verifica del backup. Fare clic su Load Locator (carica localizzatore) per popolare la posizione dello storage secondario.



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

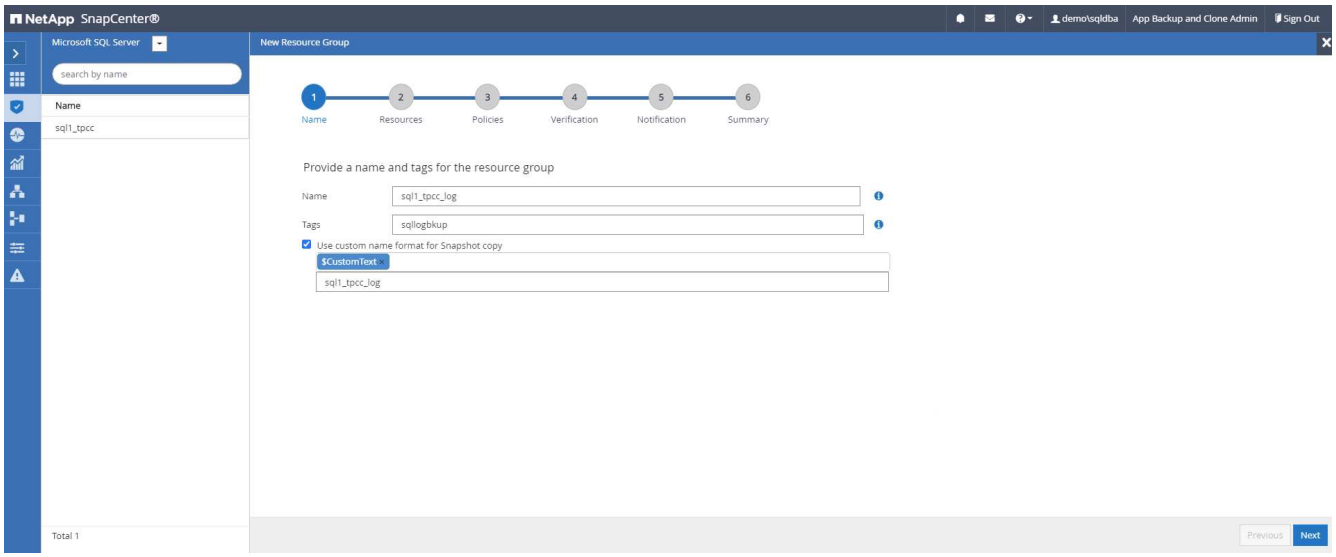


7. Riepilogo.

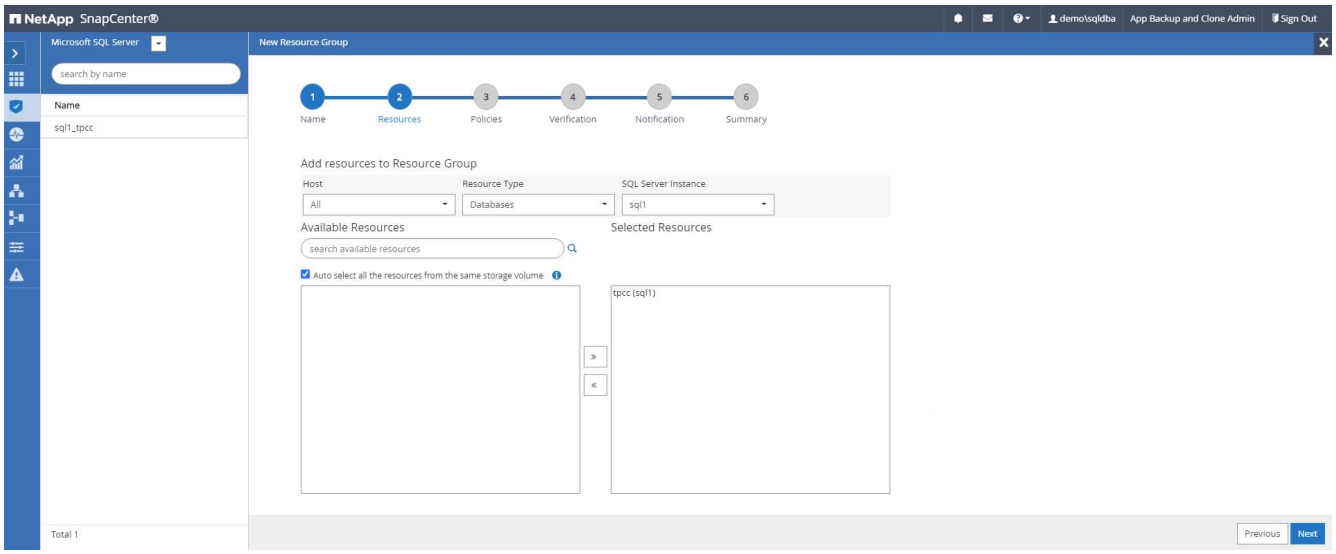


Creare un gruppo di risorse per il backup del log di SQL Server

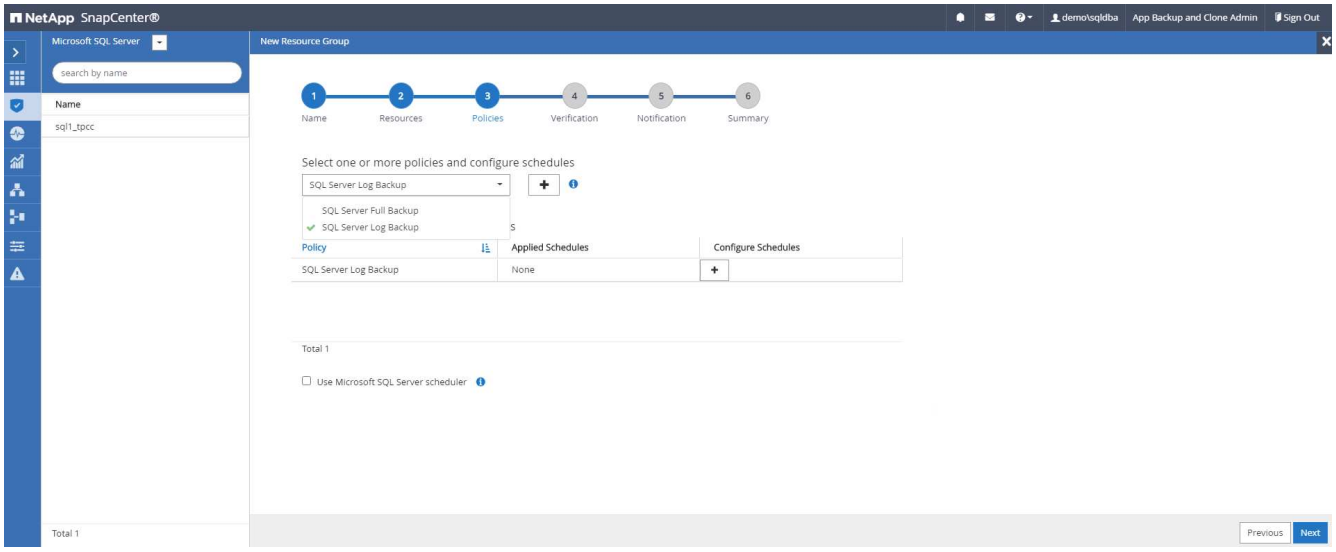
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire il nome e i tag per il gruppo di risorse. È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



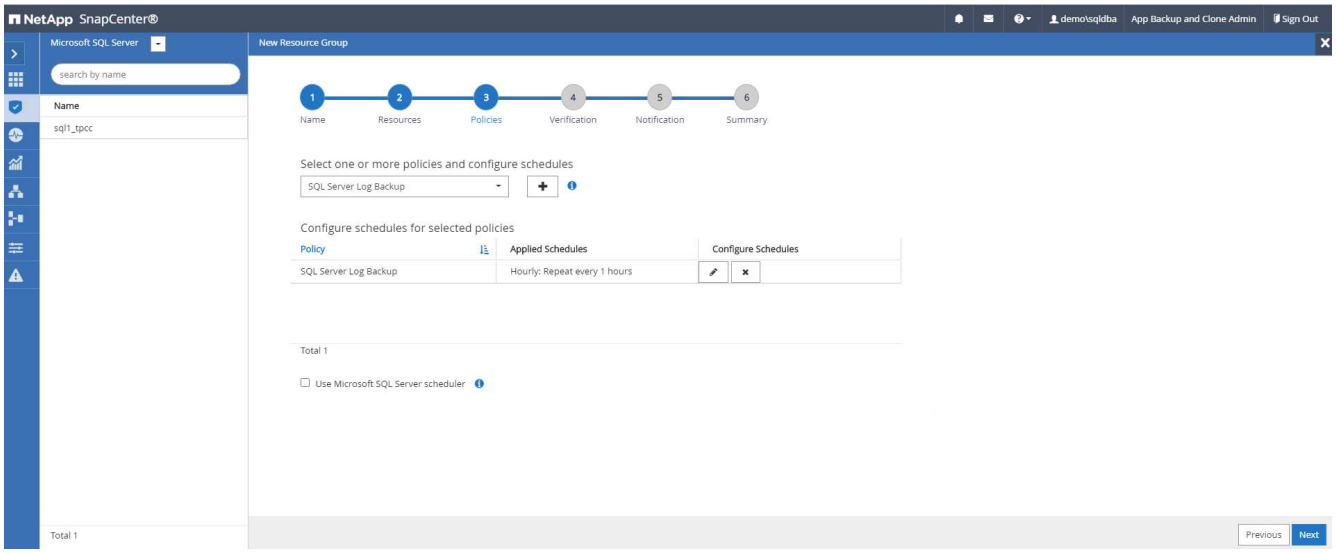
2. Selezionare le risorse di database di cui eseguire il backup.



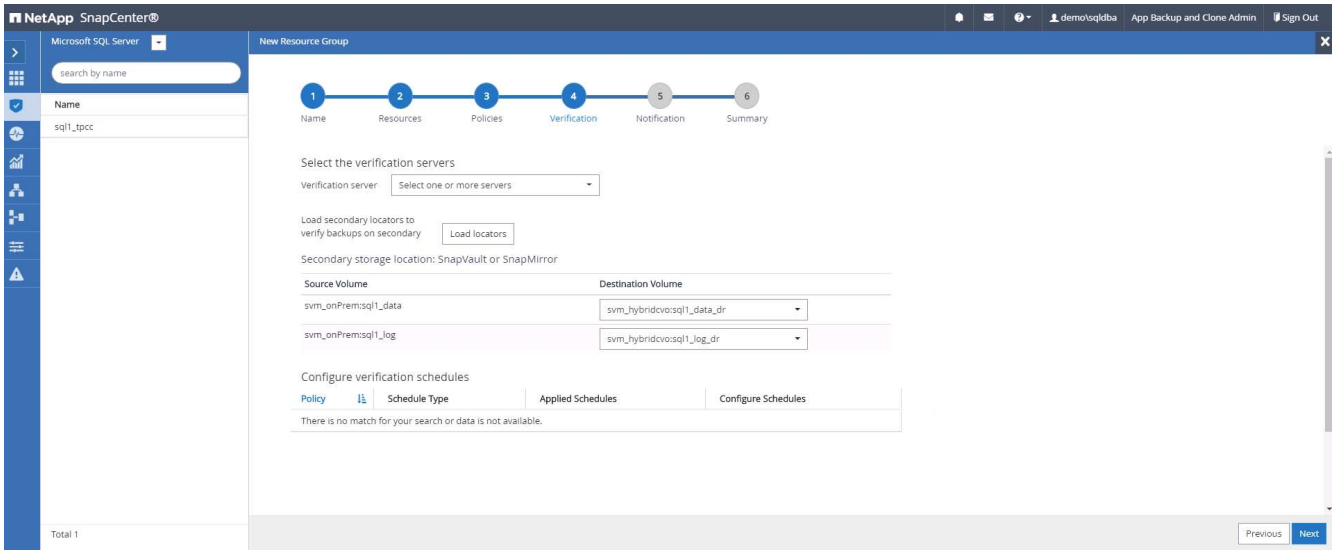
3. Selezionare un criterio di backup del registro SQL creato nella sezione 7.



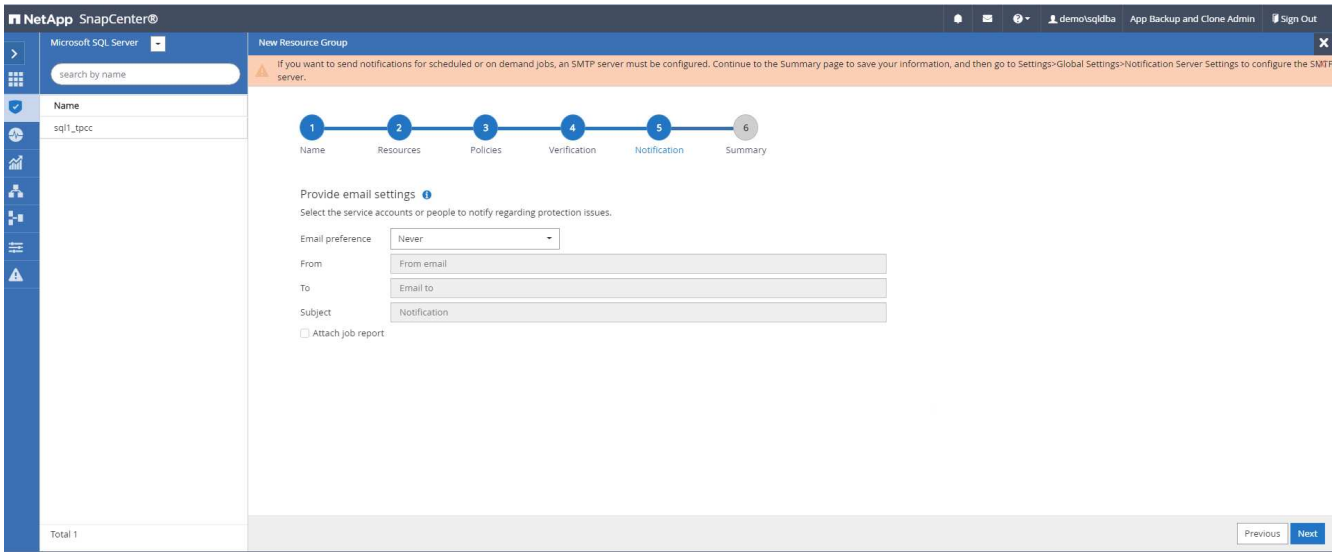
4. Aggiungere la tempistica esatta per il backup e la frequenza.



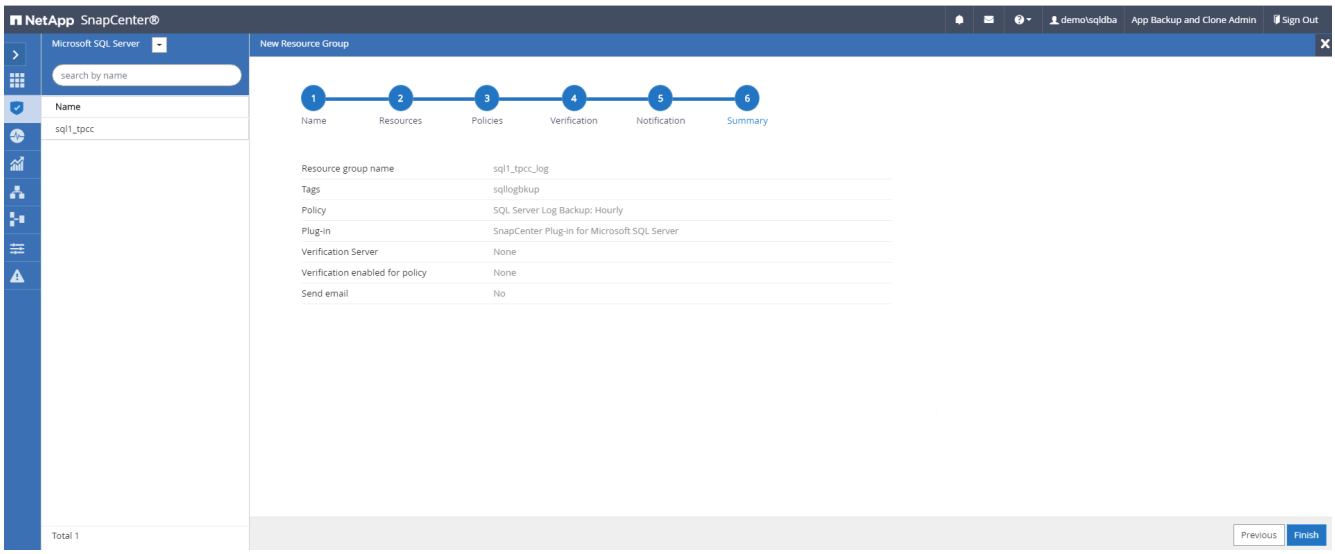
5. Scegliere il server di verifica per il backup su secondario se deve essere eseguita la verifica del backup. Fare clic su Load Locator per popolare la posizione dello storage secondario.



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

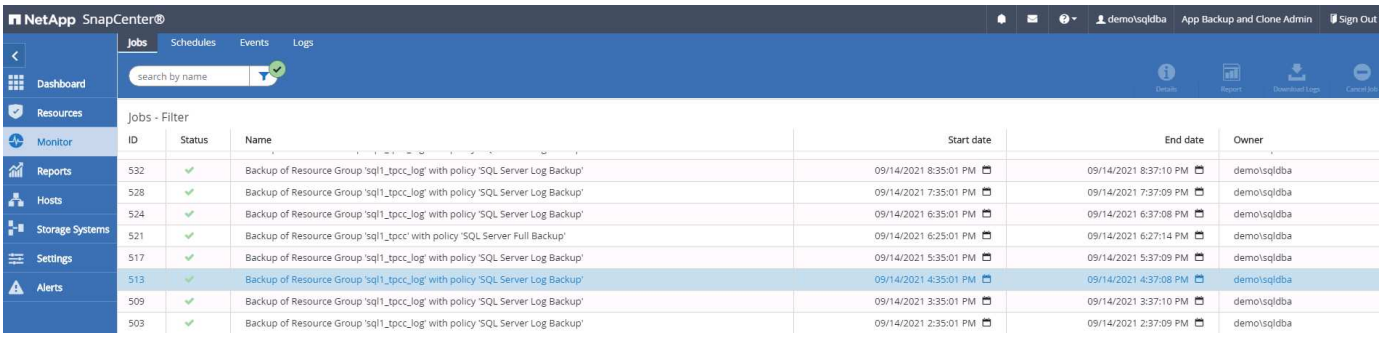


7. Riepilogo.



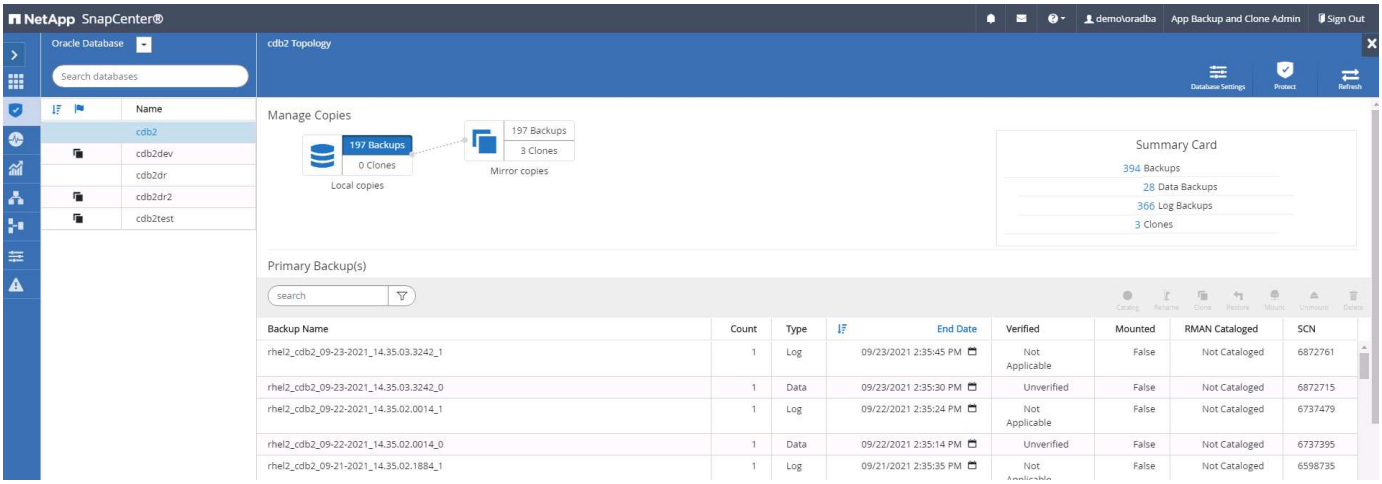
9. Convalidare il backup

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.



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.



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:

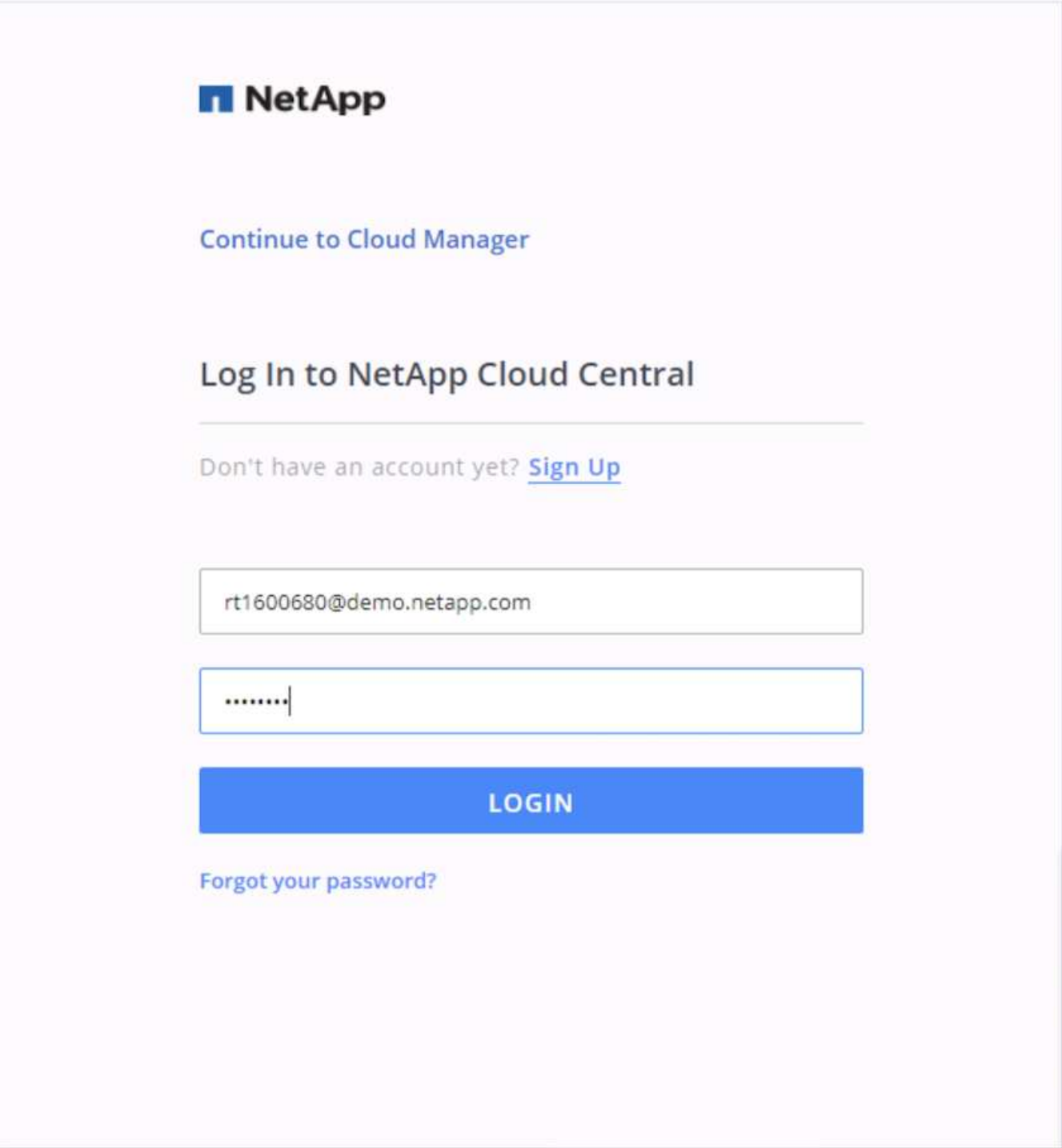
- Account AWS
- VPC nella tua regione di scelta
- Subnet con accesso a Internet pubblico
- Autorizzazioni per aggiungere ruoli IAM all'account AWS
- Chiave segreta e chiave di accesso per l'utente AWS

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

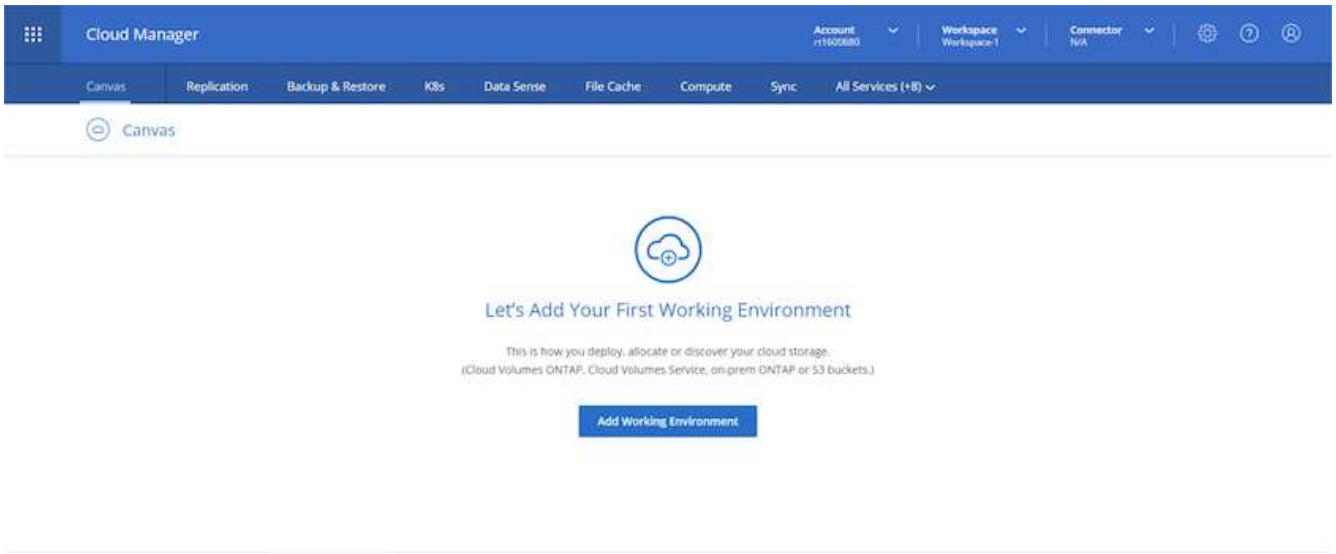
> Esistono molti metodi per implementare Cloud Manager e Cloud Volumes ONTAP; questo metodo è il più semplice ma richiede la maggior parte delle autorizzazioni. Se questo metodo non è appropriato per l'ambiente AWS in uso, consultare "Documentazione cloud di NetApp".

Implementare Cloud Manager Connector

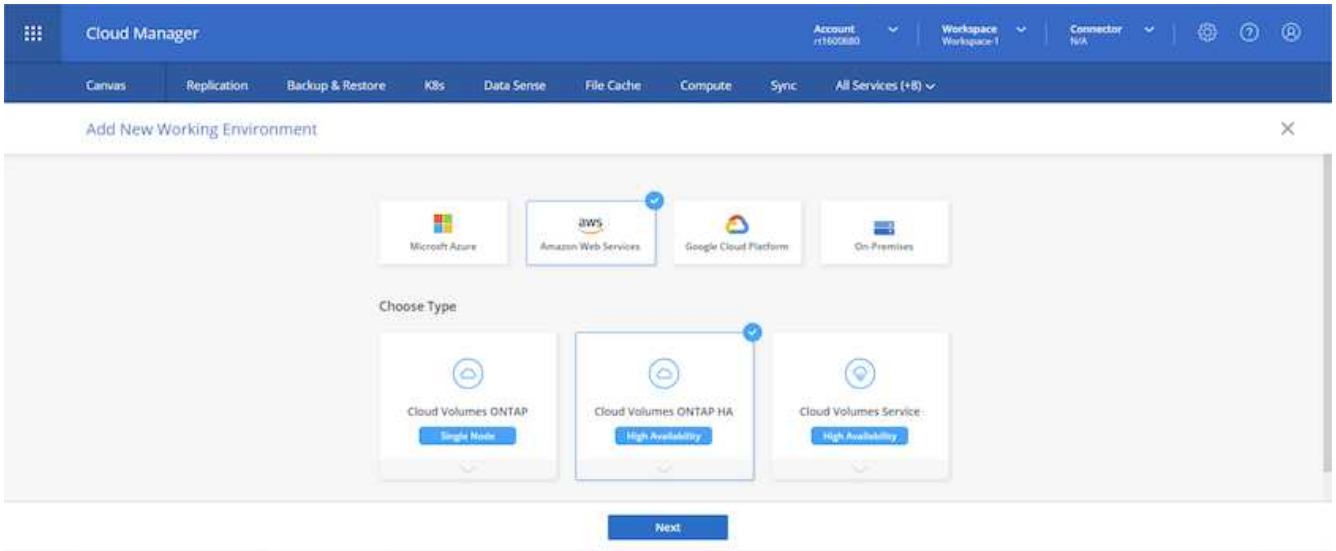
1. Selezionare "NetApp Cloud Central" ed effettuare l'accesso o l'iscrizione.



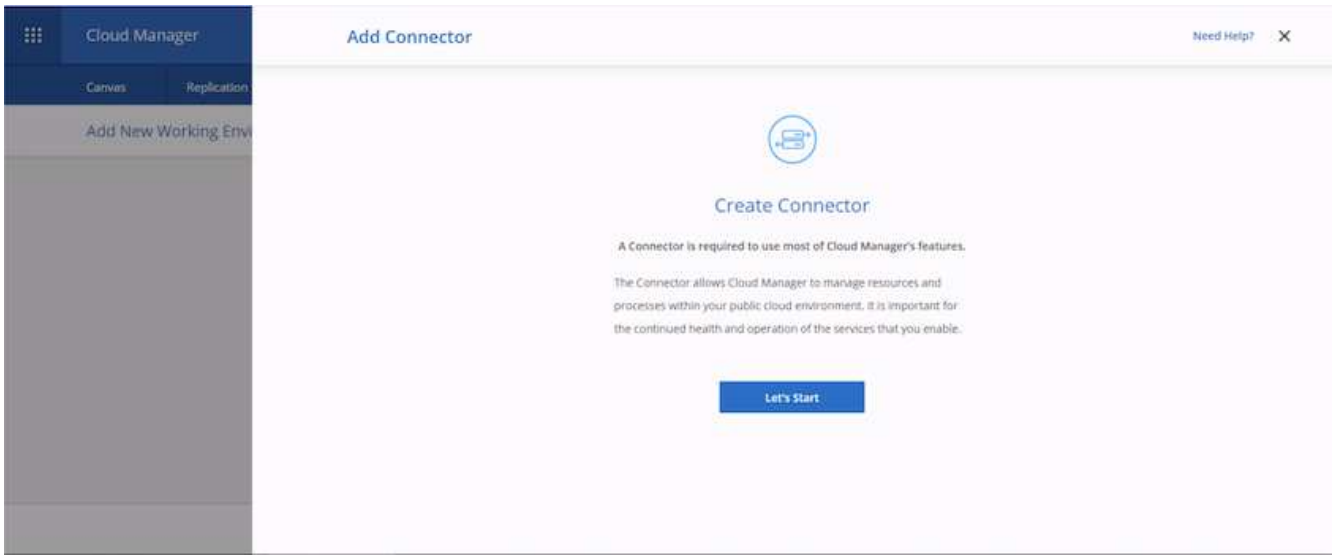
2. Dopo aver effettuato l’accesso, si dovrebbe essere portati a Canvas.



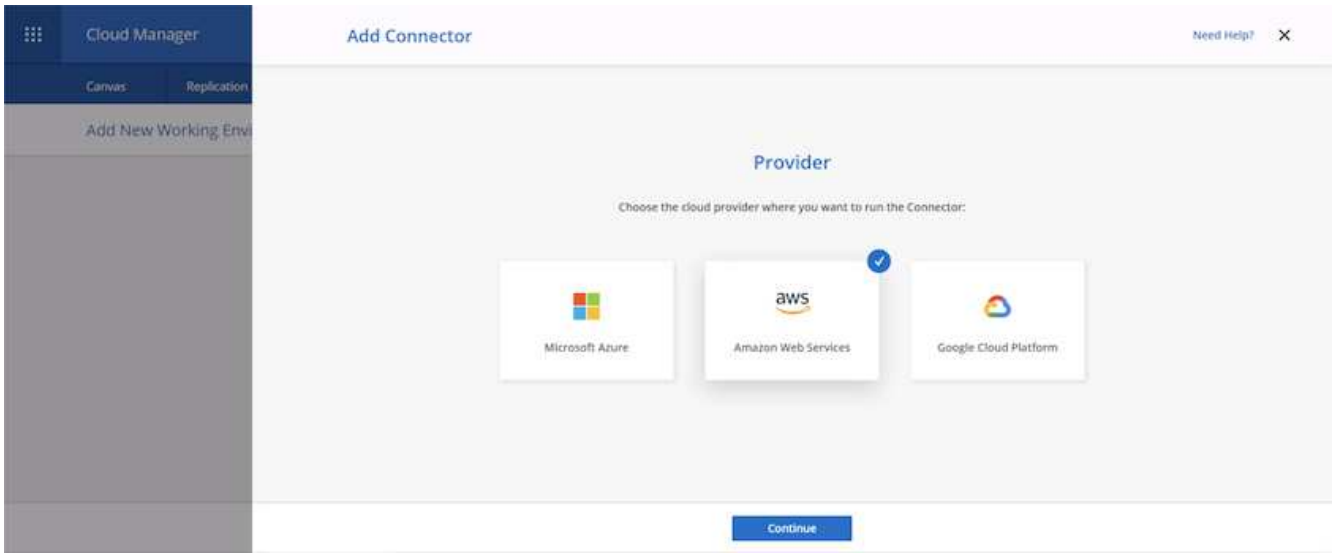
3. Fai clic su "Aggiungi ambiente di lavoro" e scegli Cloud Volumes ONTAP in AWS. In questo caso, è anche possibile scegliere se implementare un sistema a nodo singolo o una coppia ad alta disponibilità. Ho scelto di implementare una coppia ad alta disponibilità.



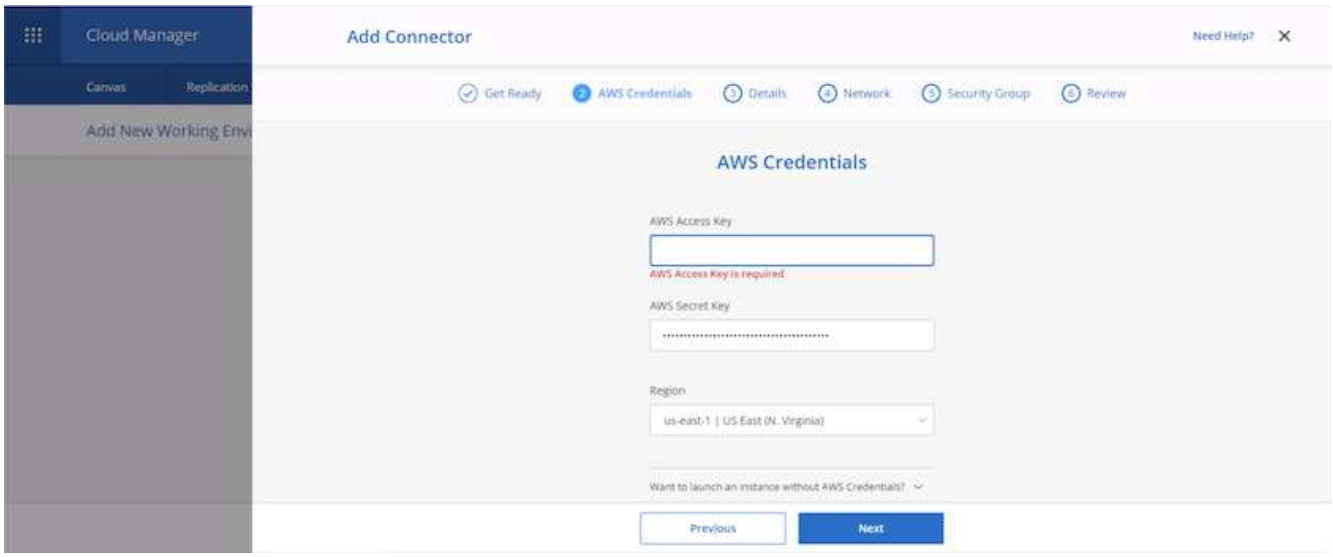
4. Se non è stato creato alcun connettore, viene visualizzata una finestra a comparsa che richiede di creare un connettore.



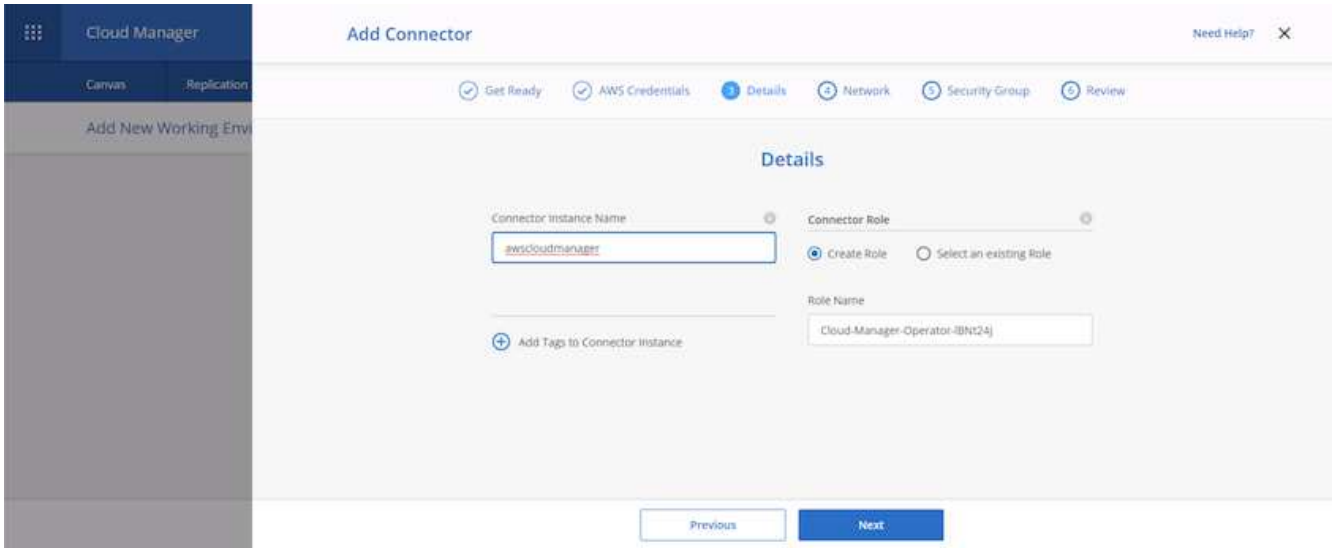
5. Fare clic su Avvia, quindi scegliere AWS.



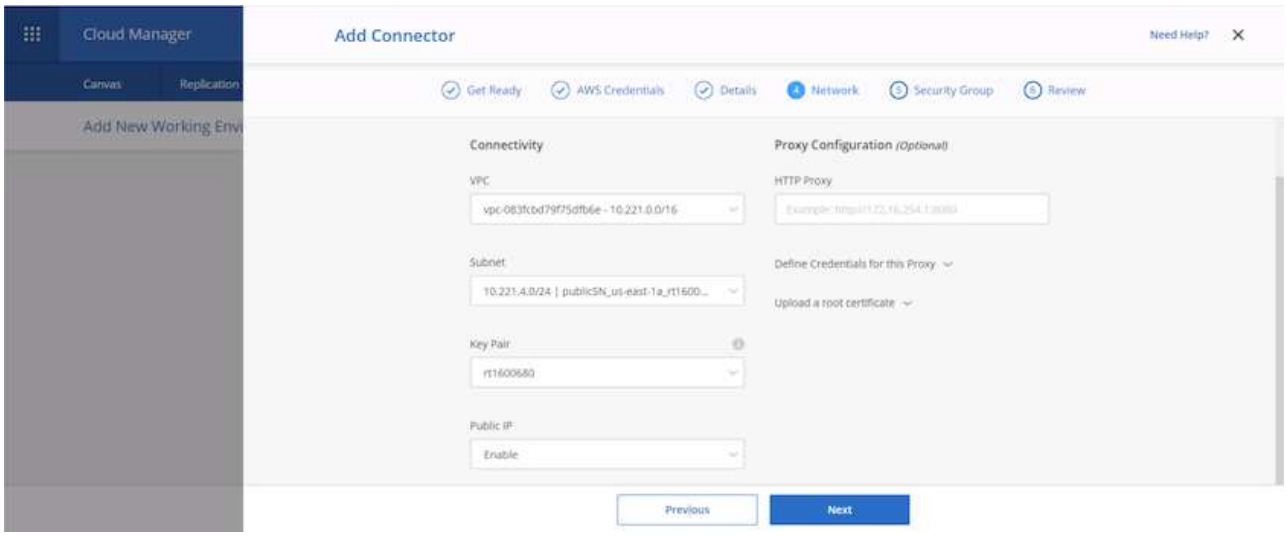
6. Inserire la chiave segreta e la chiave di accesso. Assicurarsi che l'utente disponga delle autorizzazioni corrette descritte in "Pagina delle policy di NetApp".



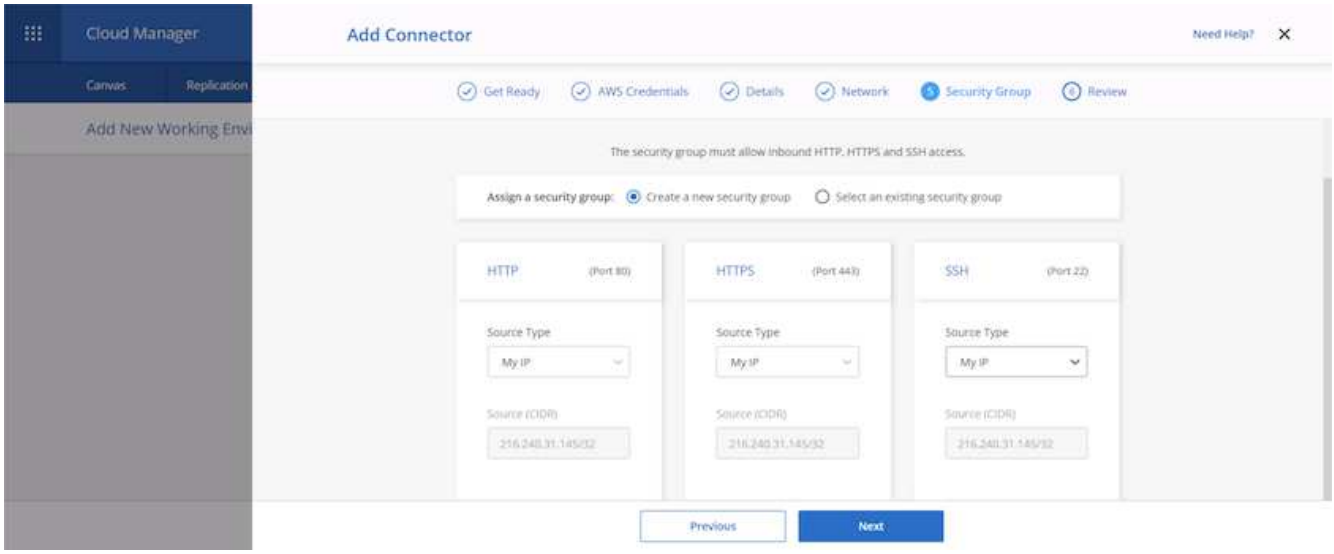
7. Assegnare un nome al connettore e utilizzare un ruolo predefinito come descritto in "Pagina delle policy di NetApp" Oppure chiedi a Cloud Manager di creare il tuo ruolo.



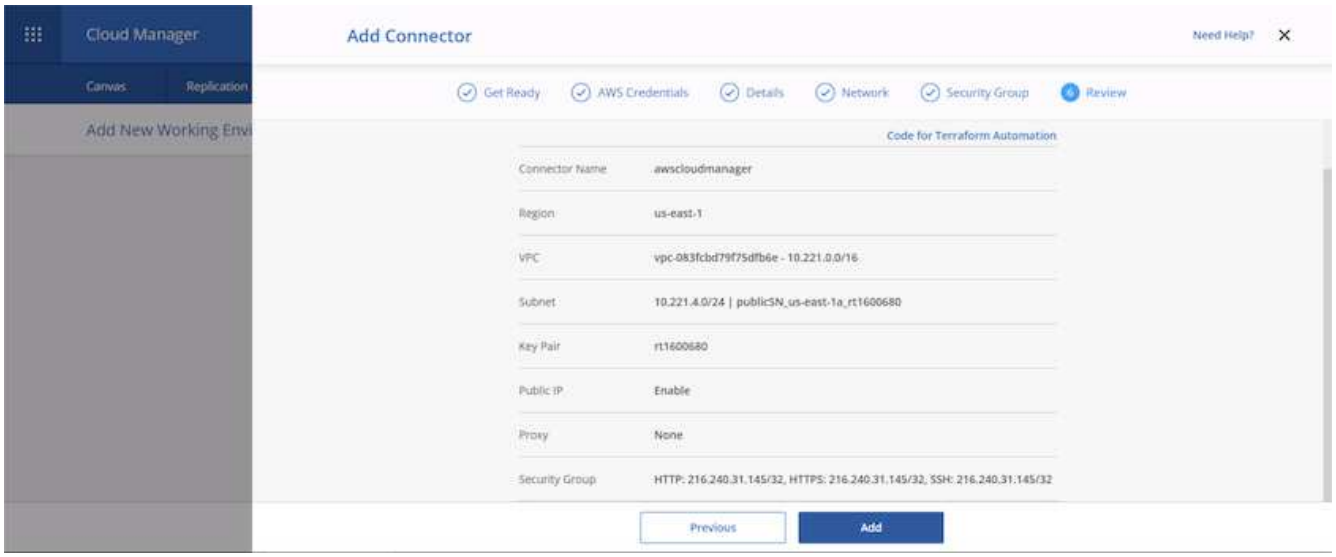
8. Fornire le informazioni di rete necessarie per implementare il connettore. Verificare che l'accesso a Internet in uscita sia attivato:
   a. Fornire al connettore un indirizzo IP pubblico
   b. Fornire al connettore un proxy da utilizzare
   c. Fornire al connettore un percorso verso Internet pubblico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



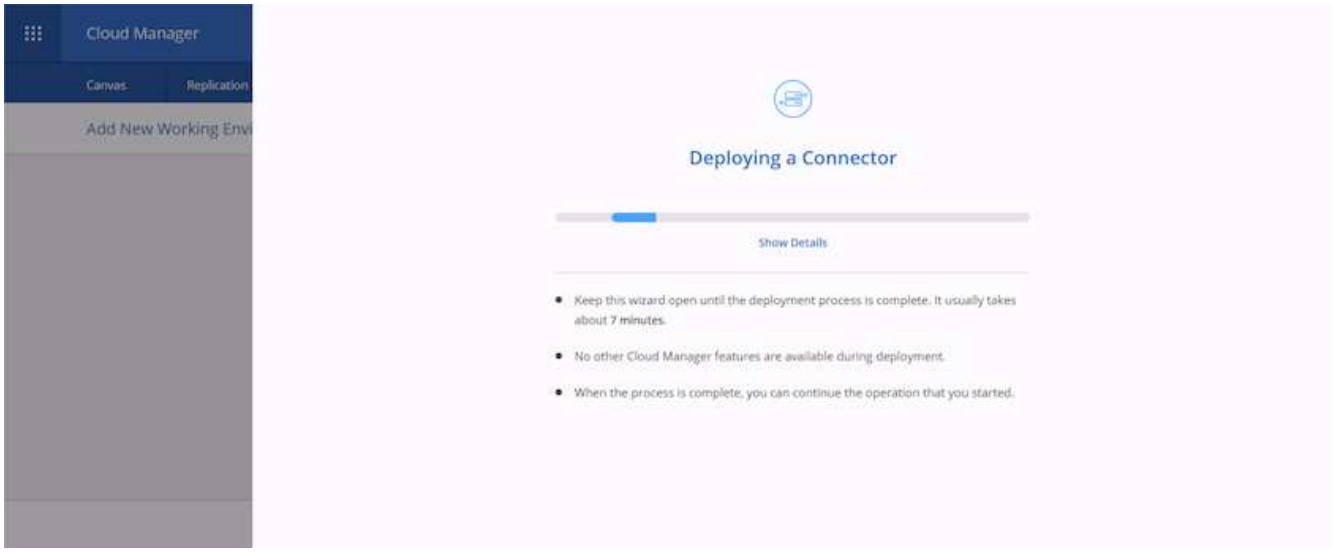
9. Fornire la comunicazione con il connettore tramite SSH, HTTP e HTTPS fornendo un gruppo di protezione o creando un nuovo gruppo di protezione. È stato attivato l'accesso al connettore solo dall'indirizzo IP.



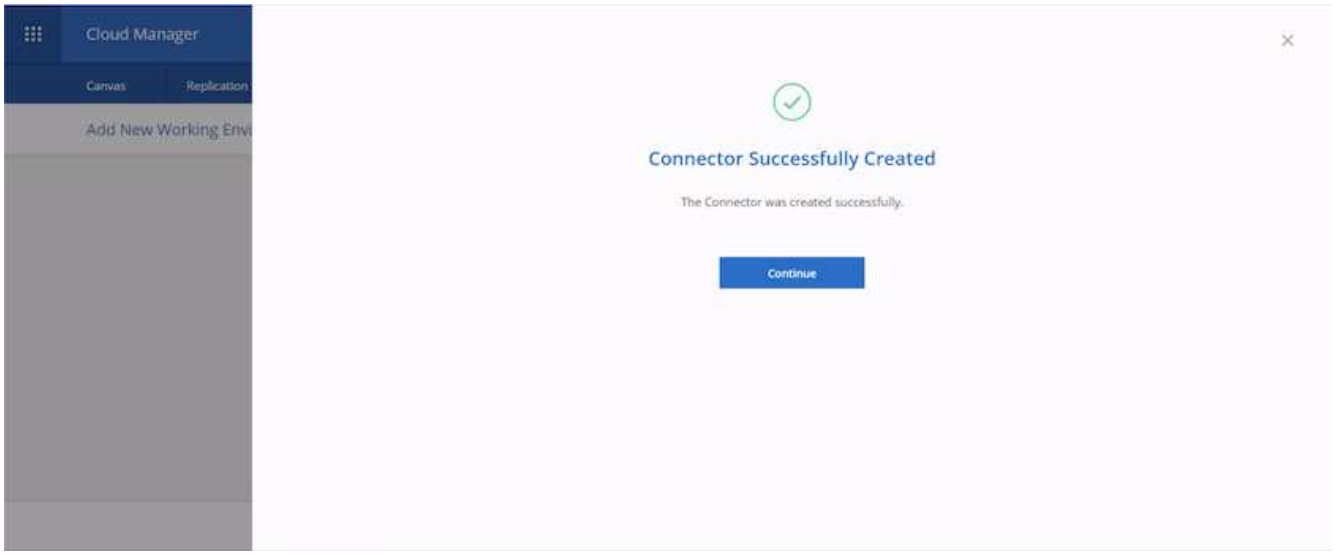
10. Esaminare le informazioni nella pagina di riepilogo e fare clic su Add (Aggiungi) per implementare il connettore.



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

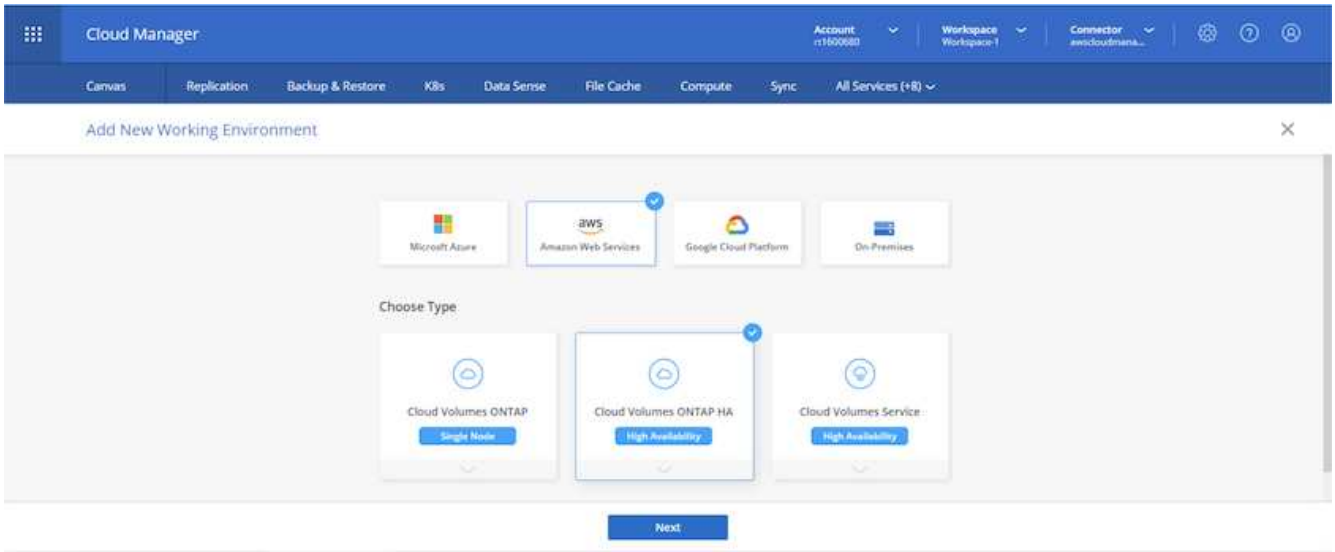


12. Una volta completata l'implementazione, viene visualizzata una pagina di successo.

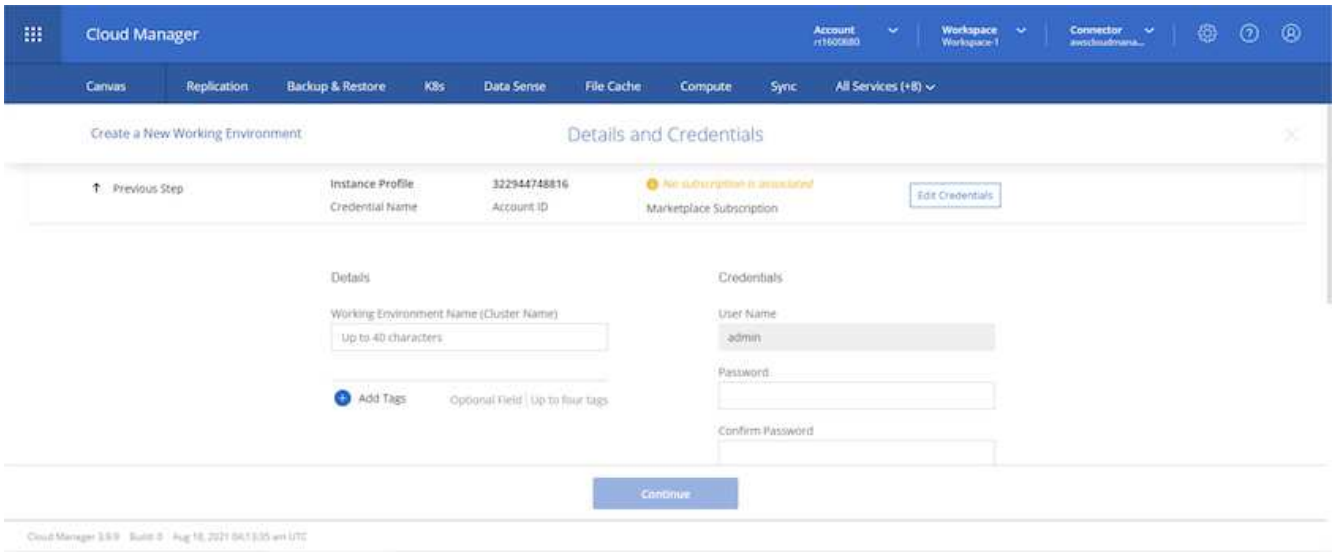


Implementare Cloud Volumes ONTAP

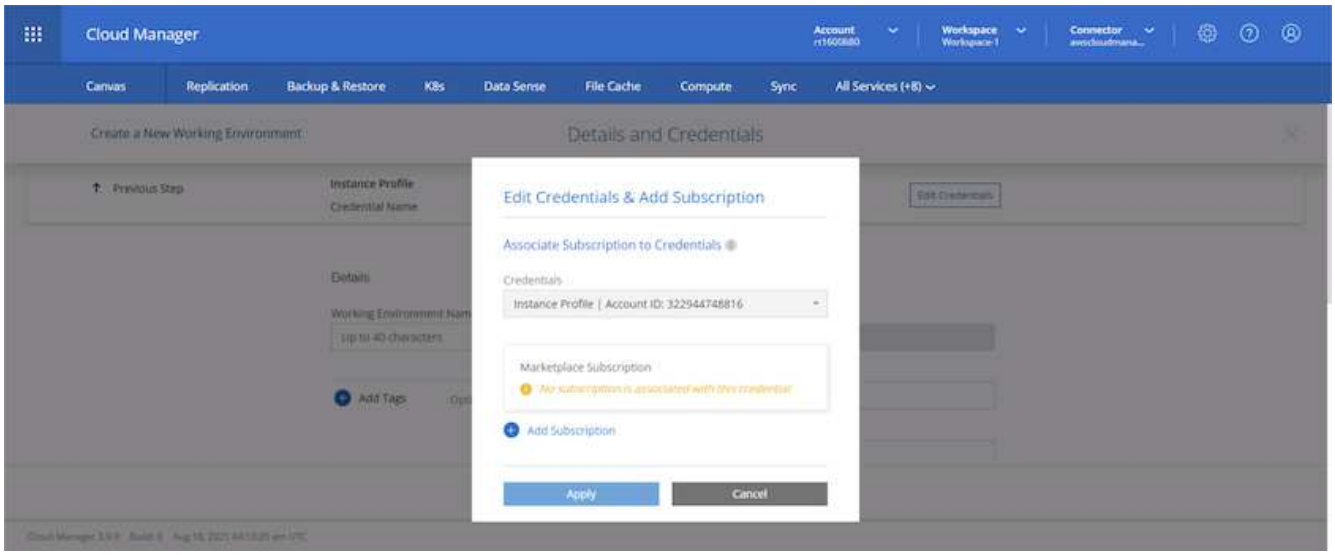
1. Selezionare AWS e il tipo di implementazione in base ai requisiti.



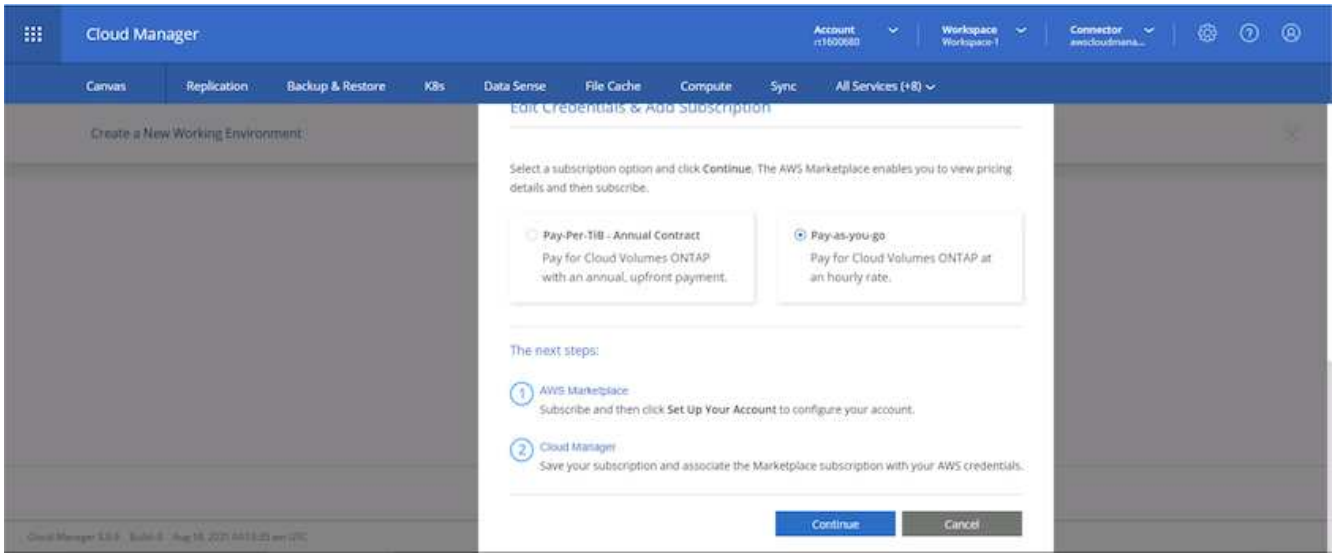
2. Se non è stato assegnato alcun abbonamento e si desidera effettuare l'acquisto con PAYGO, scegliere Modifica credenziali.



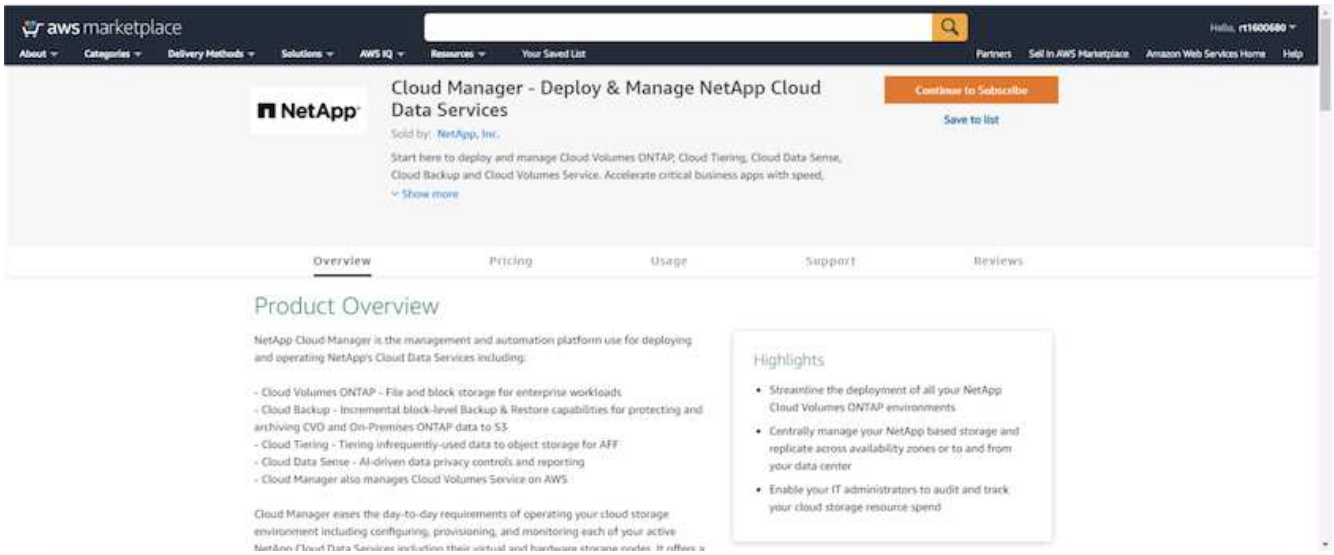
3. Scegliere Aggiungi abbonamento.



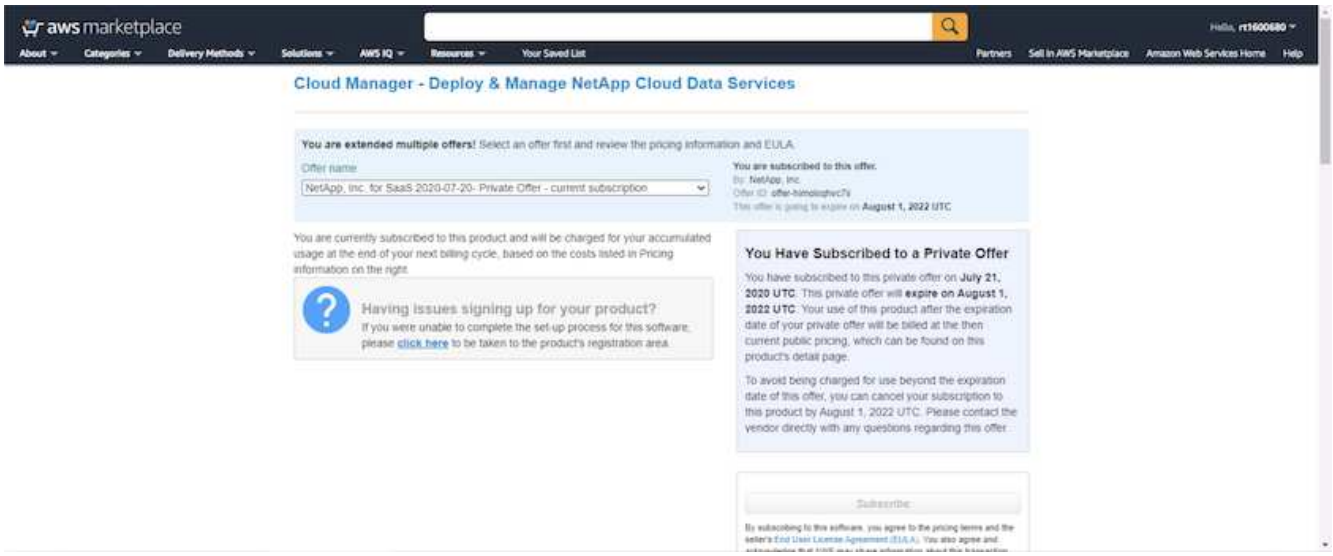
4. Scegliere il tipo di contratto a cui si desidera sottoscrivere. Ho scelto il pay-as-you-go.



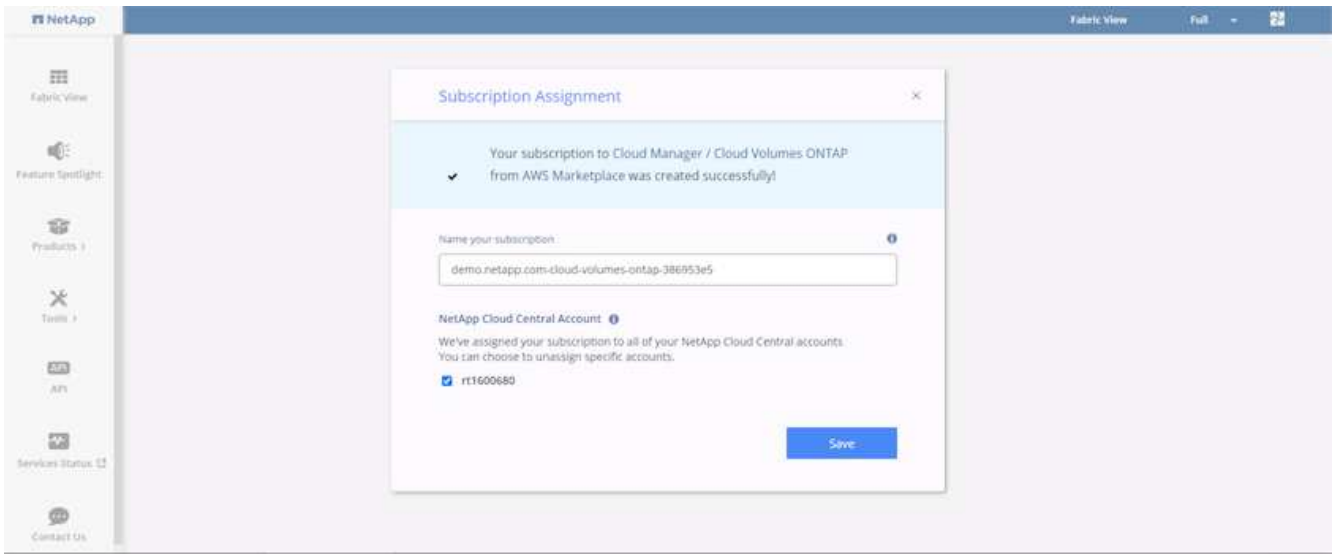
5. Si viene reindirizzati ad AWS; scegliere continua per iscriversi.



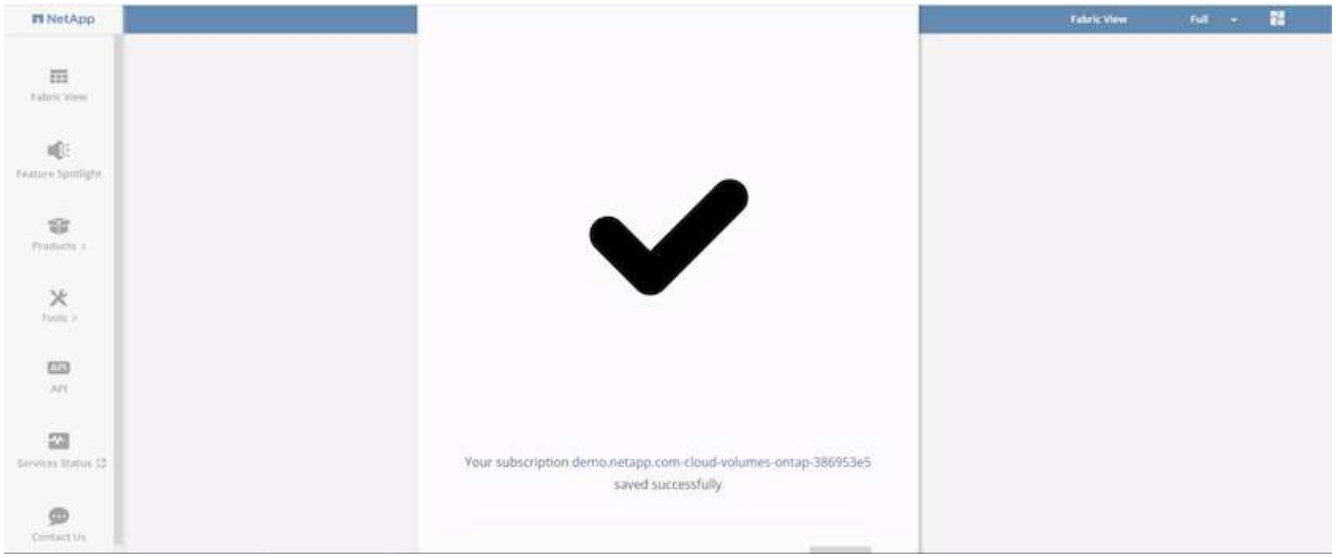
6. Iscriviti e verrai reindirizzato a NetApp Cloud Central. Se sei già iscritto e non ricevi il reindirizzamento, scegli il link "Clicca qui".



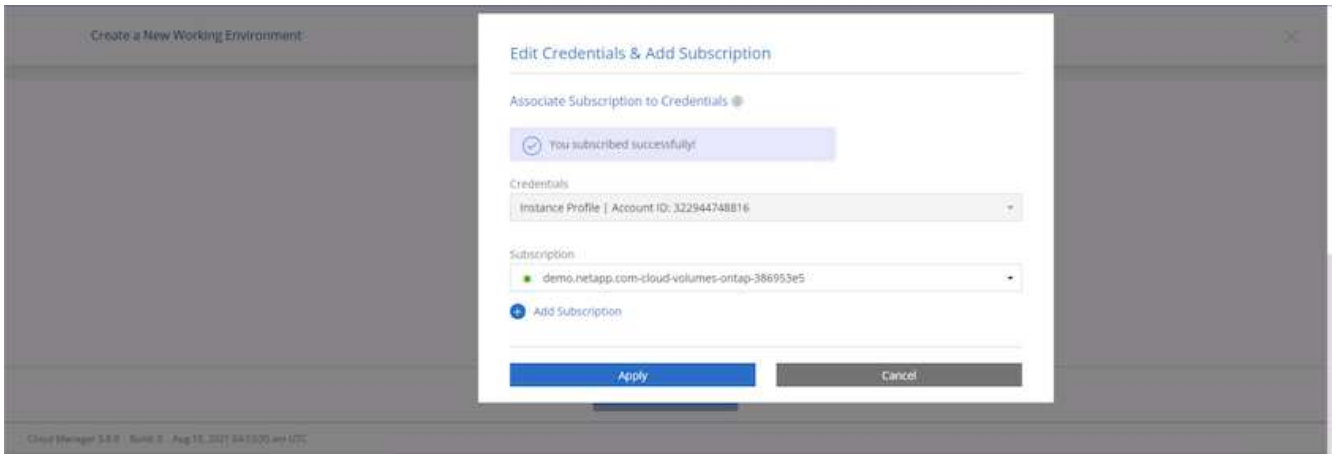
7. Verrai reindirizzato a Cloud Central dove devi assegnare un nome all'abbonamento e assegnarlo al tuo account Cloud Central.



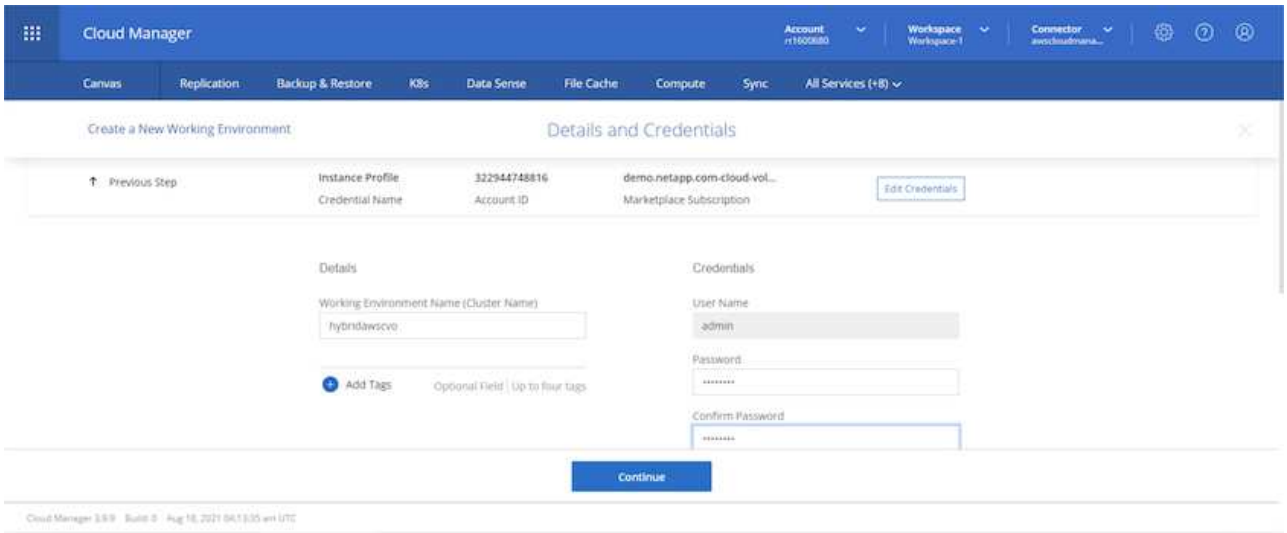
8. Una volta completata la stampa, viene visualizzata una pagina con un segno di spunta. Tornare alla scheda Cloud Manager.



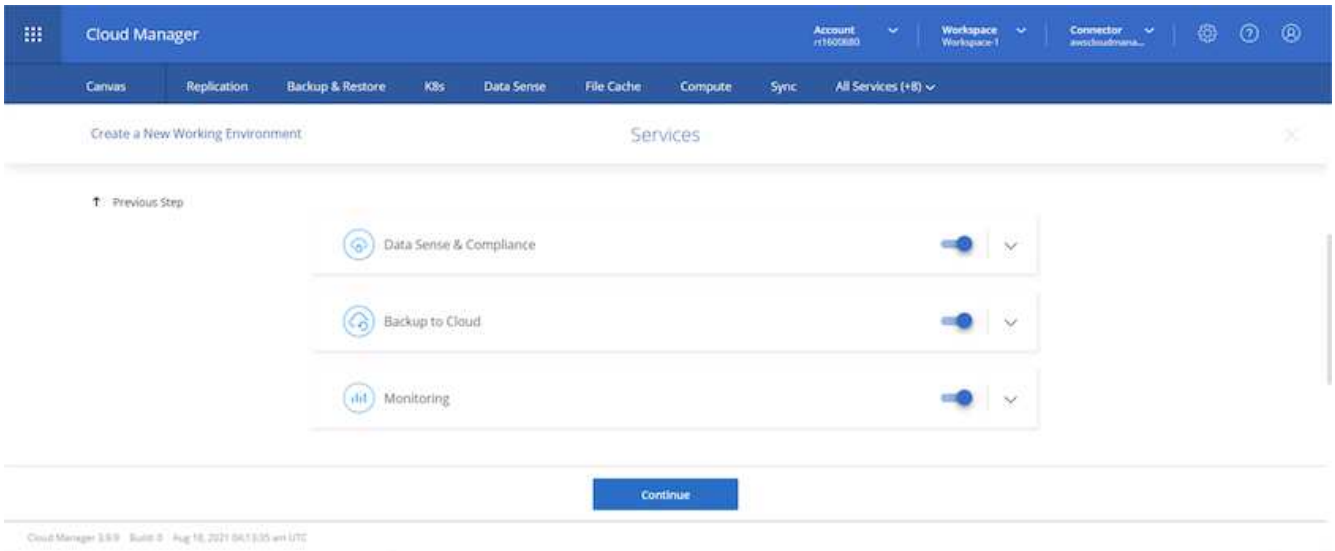
9. L'abbonamento viene ora visualizzato in Cloud Central. Fare clic su Apply (Applica) per continuare.



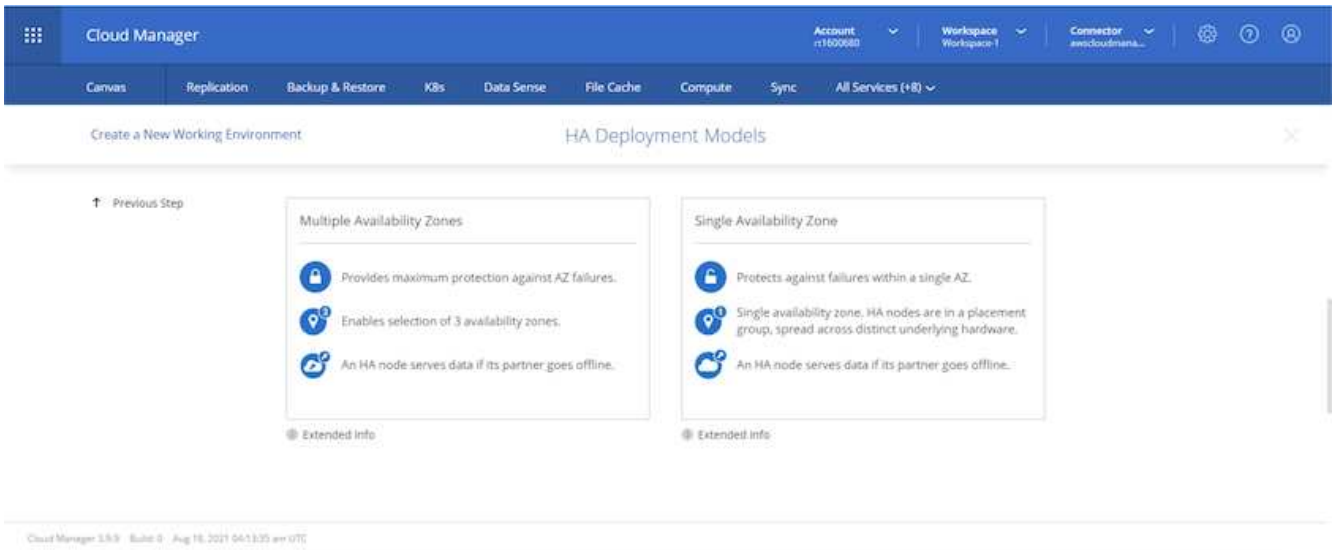
10. Inserire i dettagli dell'ambiente di lavoro, ad esempio:
    a. Nome del cluster
    b. Password del cluster
    c. Tag AWS (opzionale)



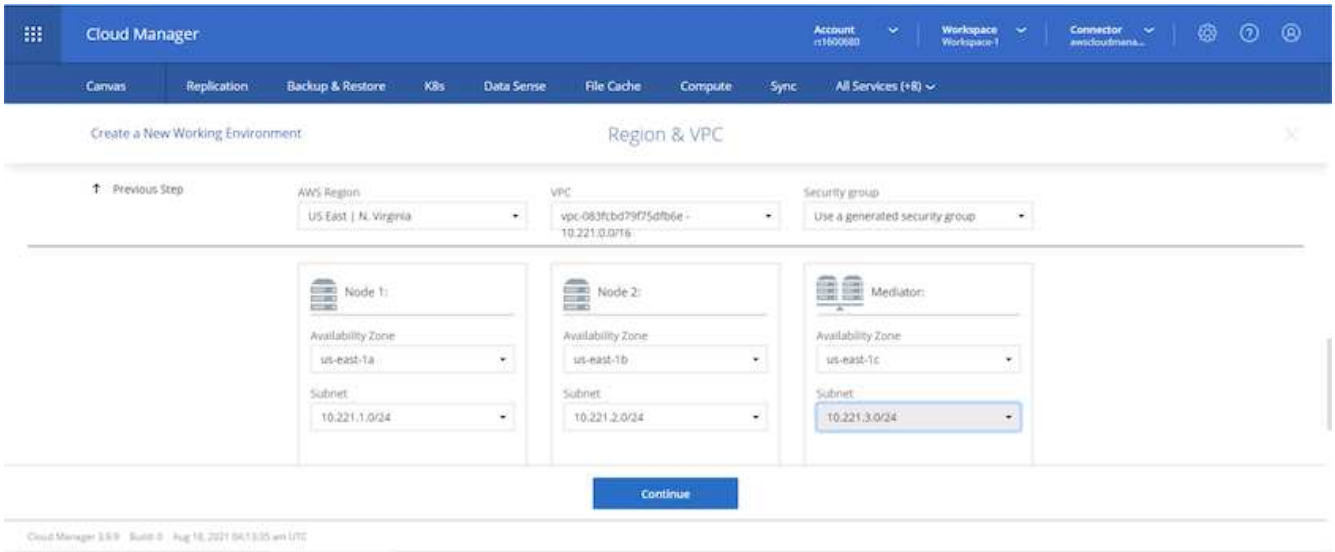
11. Scegliere i servizi aggiuntivi che si desidera implementare. Per ulteriori informazioni su questi servizi, visitare il "Homepage di NetApp Cloud".



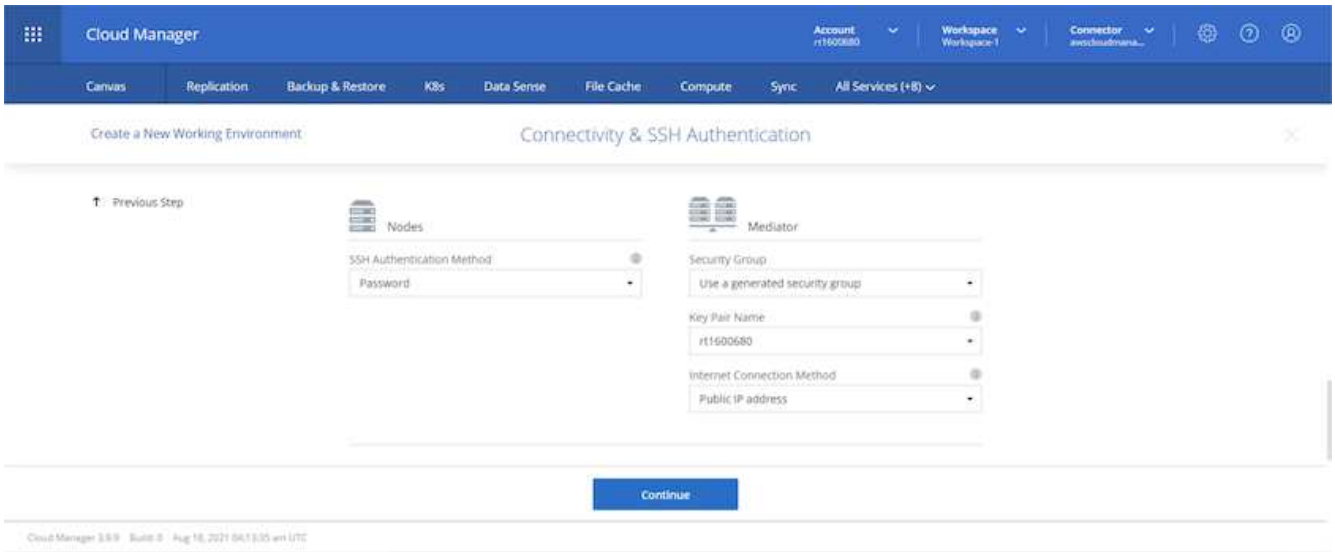
12. Scegliere se eseguire l'implementazione in più zone di disponibilità (si recuperano tre subnet, ciascuna in un AZ diverso) o in una singola zona di disponibilità. Ho scelto più AZS.



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.

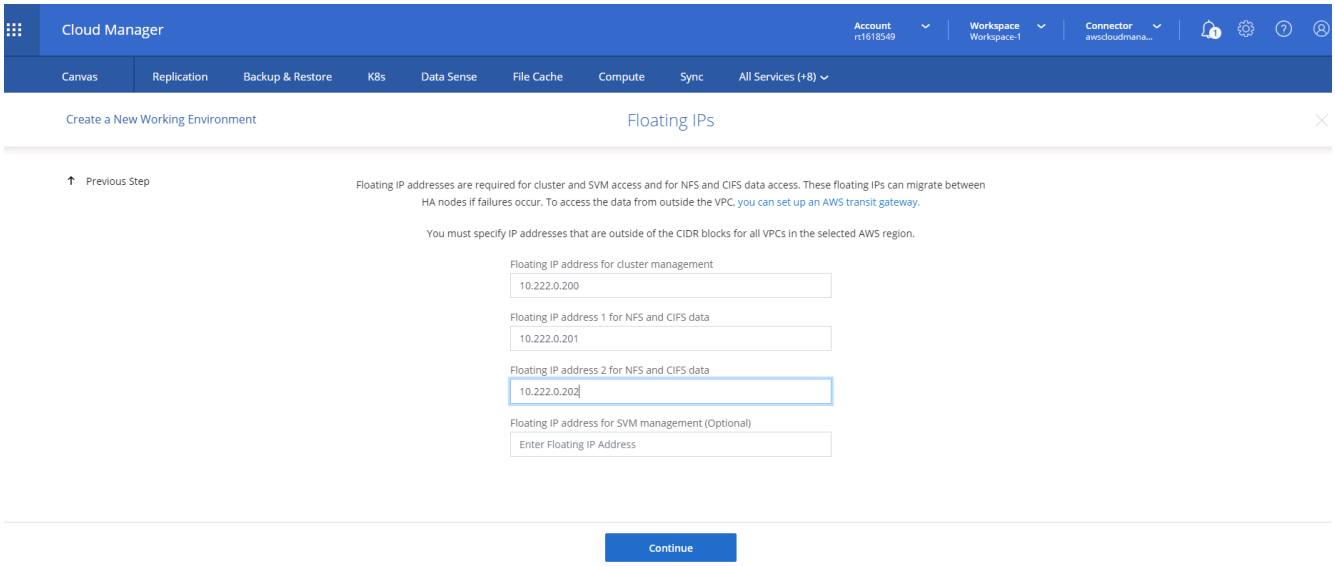


14. Scegliere i metodi di connessione per i nodi e il mediatore.

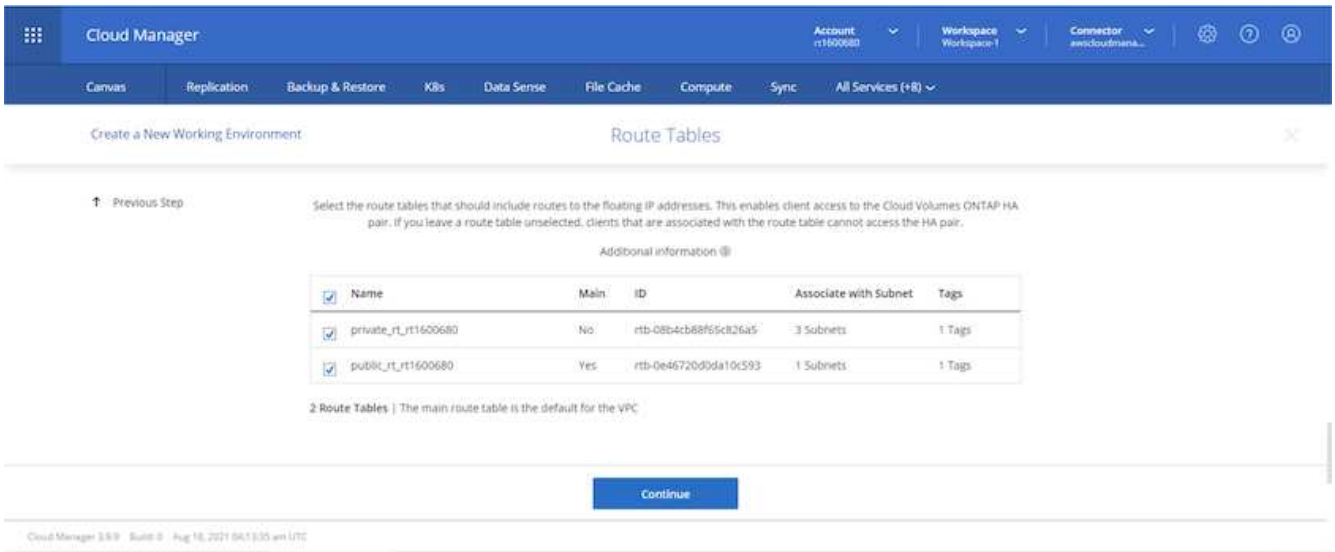


Il mediatore richiede la comunicazione con le API AWS. Non è richiesto un indirizzo IP pubblico, purché le API siano raggiungibili dopo l'implementazione dell'istanza EC2 del mediatore.

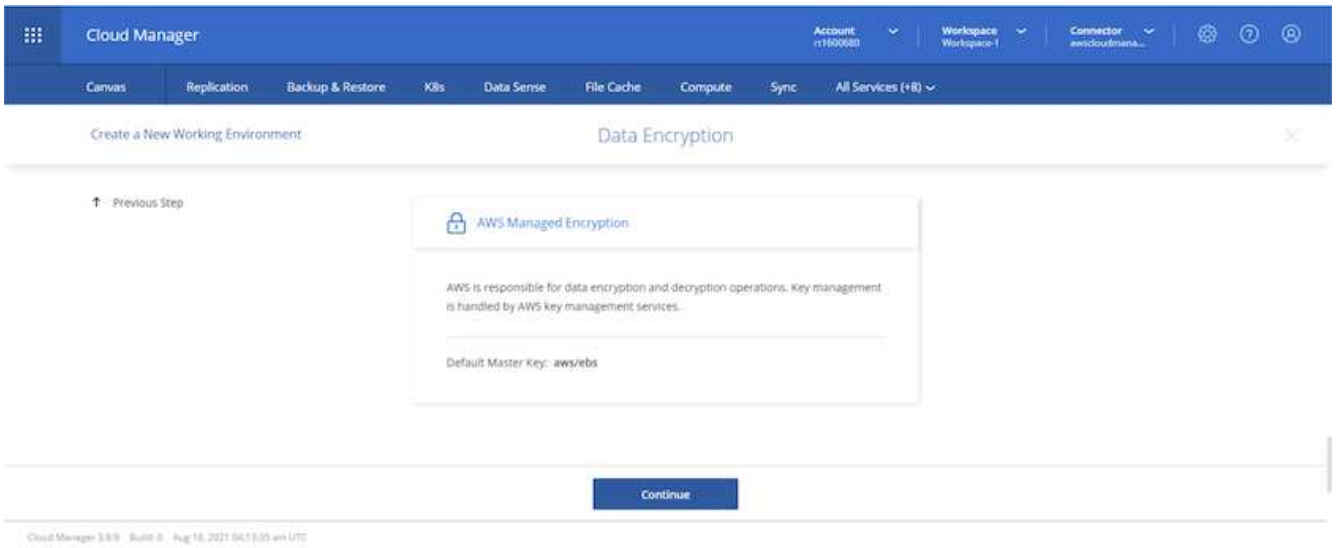
1. Gli indirizzi IP mobili vengono utilizzati per consentire l'accesso ai vari indirizzi IP utilizzati da Cloud Volumes ONTAP, inclusi gli IP di gestione del cluster e di erogazione dei dati. Devono essere indirizzi non ancora instradabili all'interno della rete e aggiunti alle tabelle di routing nell'ambiente 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".



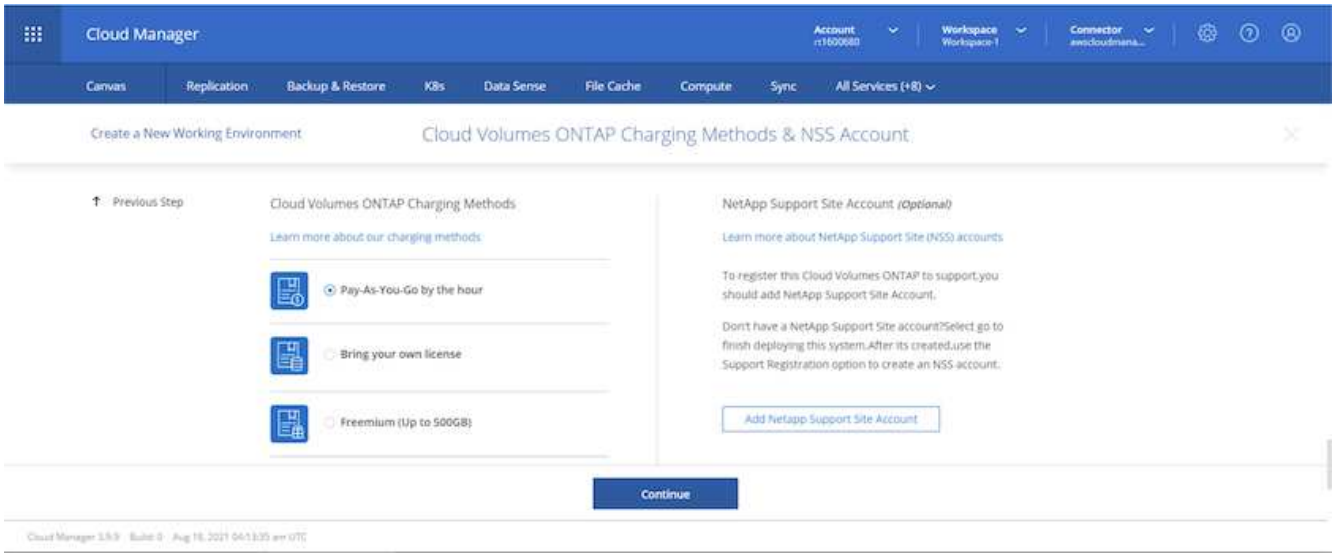
2. Selezionare le tabelle di routing a cui aggiungere gli indirizzi IP mobili. Queste tabelle di routing vengono utilizzate dai client per comunicare con Cloud Volumes ONTAP.



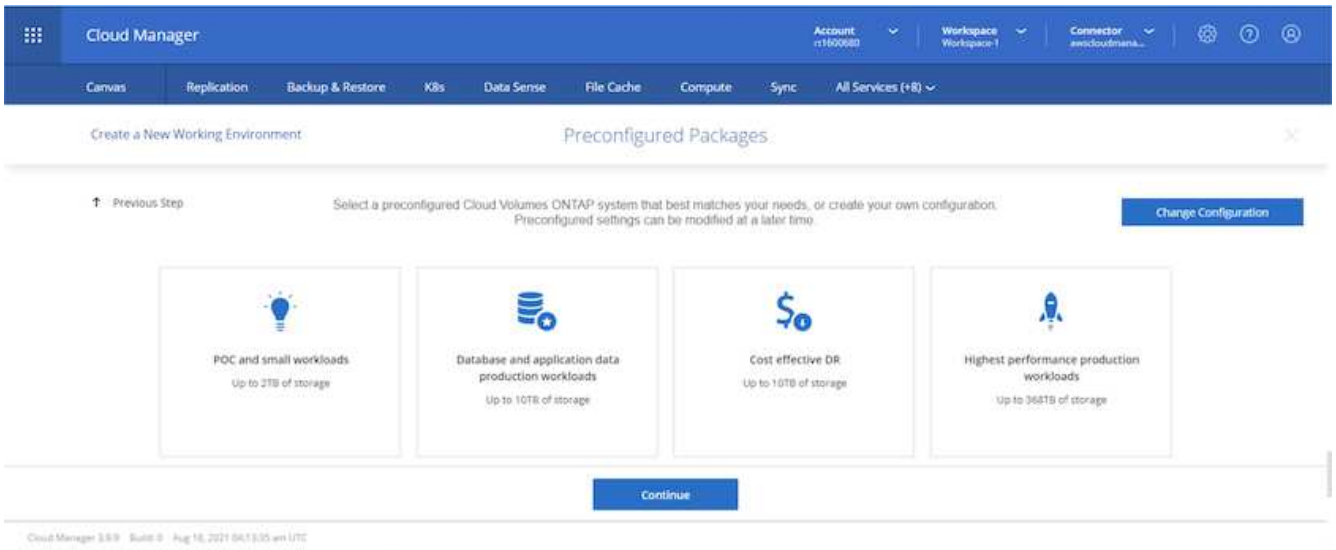
3. Scegliere se attivare la crittografia gestita AWS o AWS KMS per crittografare i dischi root, boot e dati ONTAP.



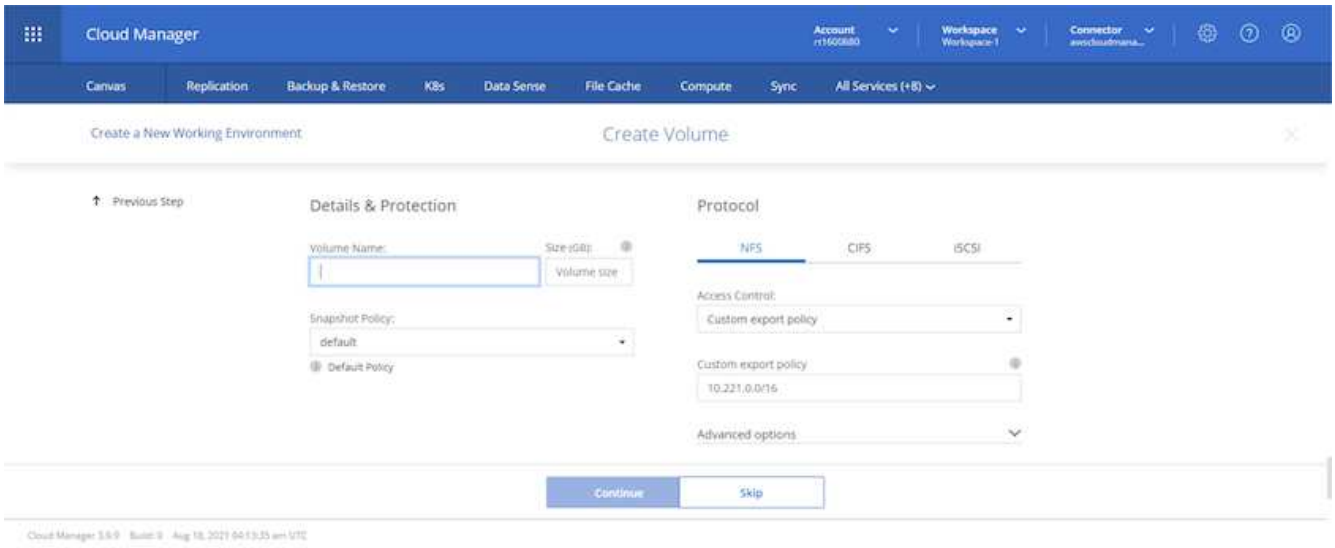
4. Scegli il tuo modello di licenza. Se non sai quale scegliere, contatta il tuo rappresentante NetApp.



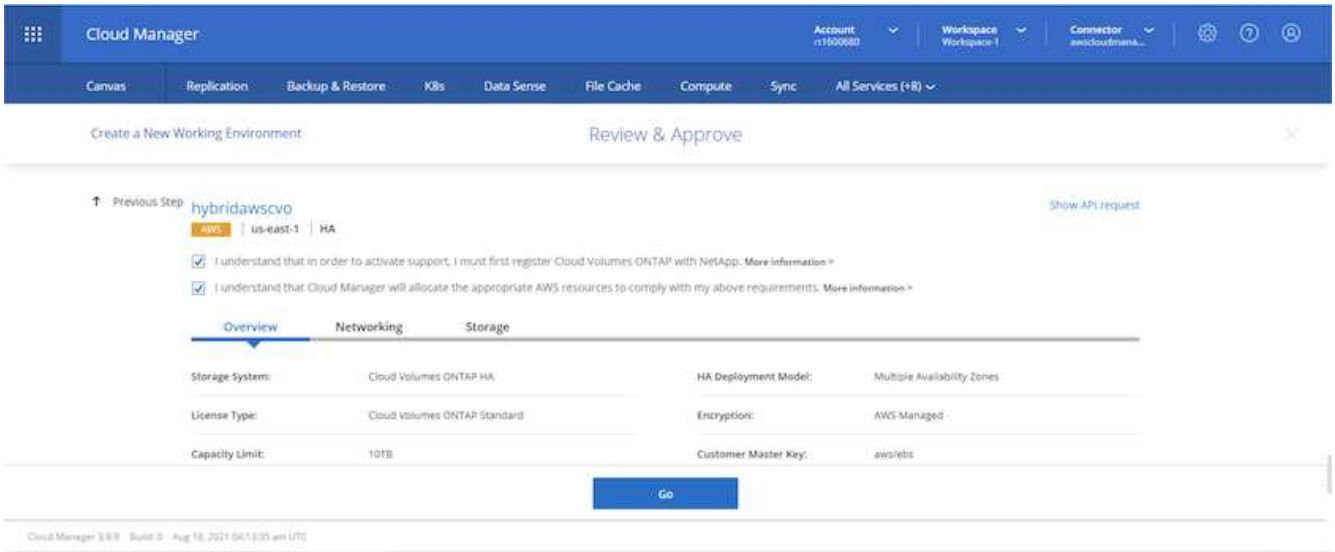
5. Selezionare la configurazione più adatta al caso d'utilizzo. Ciò è correlato alle considerazioni sul dimensionamento trattate nella pagina dei prerequisiti.



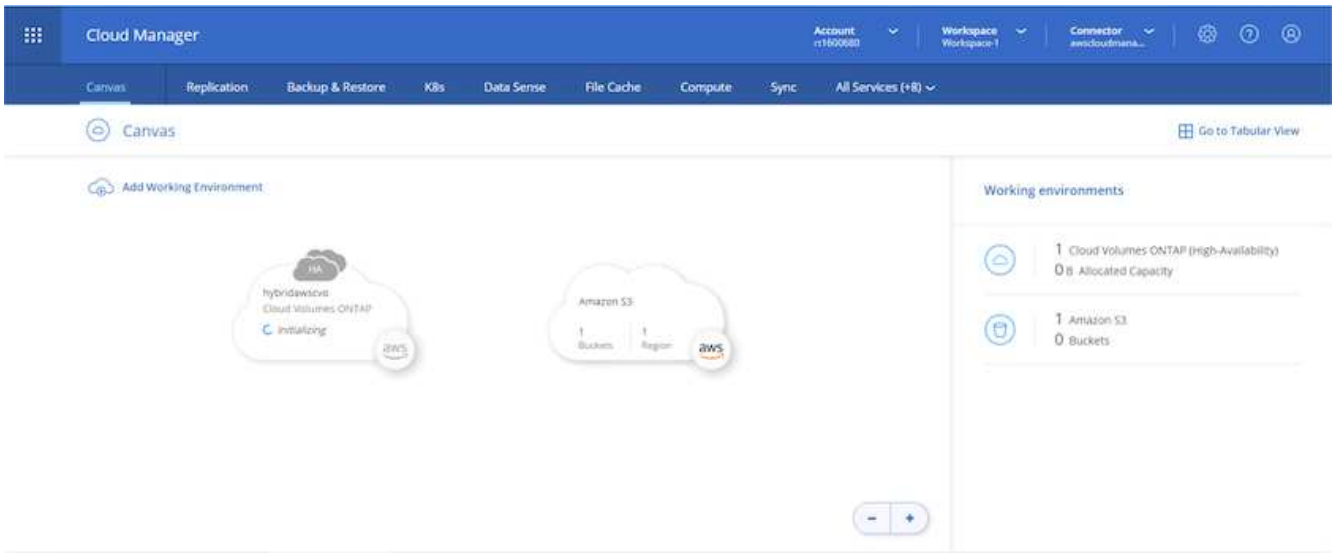
6. Se si desidera, creare un volume. Questo non è necessario, perché le fasi successive utilizzano SnapMirror, che crea i volumi per noi.



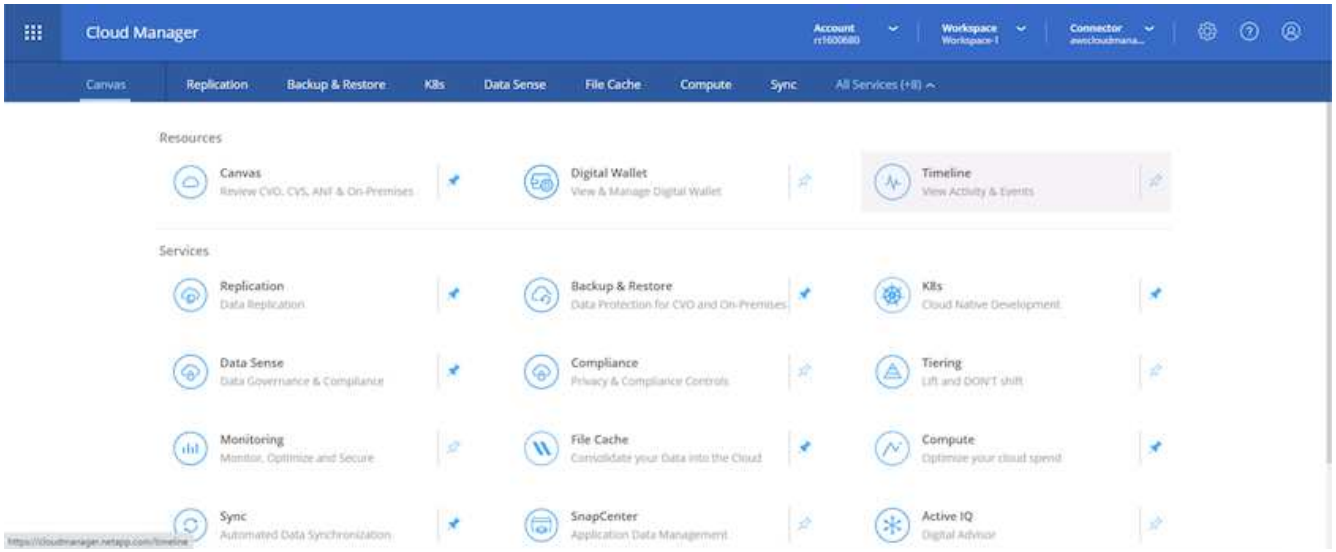
7. Esaminare le selezioni effettuate e spuntare le caselle per verificare che Cloud Manager implementa le risorse nel proprio ambiente AWS. Quando si è pronti, fare clic su Go (Vai).



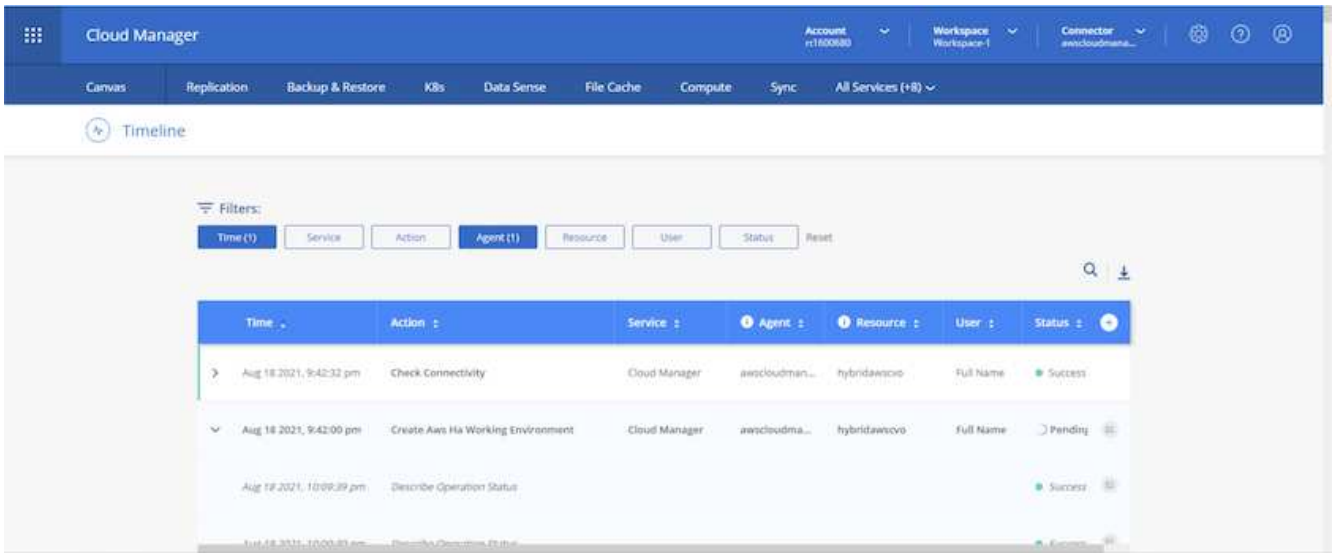
8. Cloud Volumes ONTAP avvia ora il processo di implementazione. Cloud Manager utilizza le API AWS e gli stack di formazione del cloud per implementare Cloud Volumes ONTAP. Quindi, configura il sistema in base alle tue specifiche, offrendo un sistema pronto all'uso che può essere utilizzato immediatamente.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



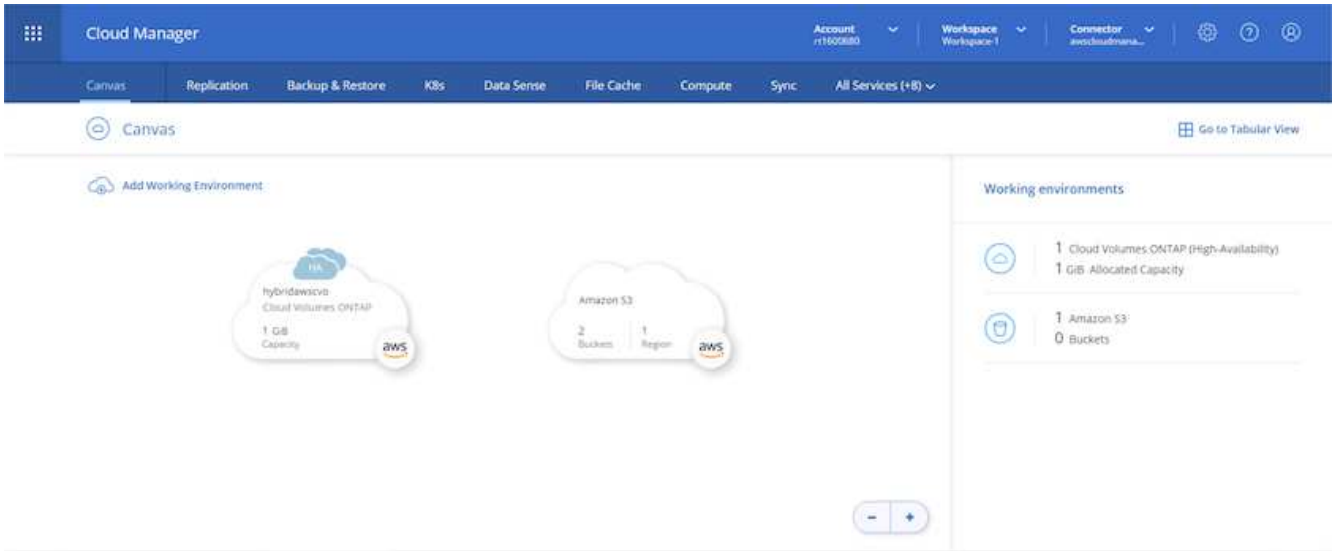
9. È possibile monitorare l'avanzamento passando alla Timeline.



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.



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.

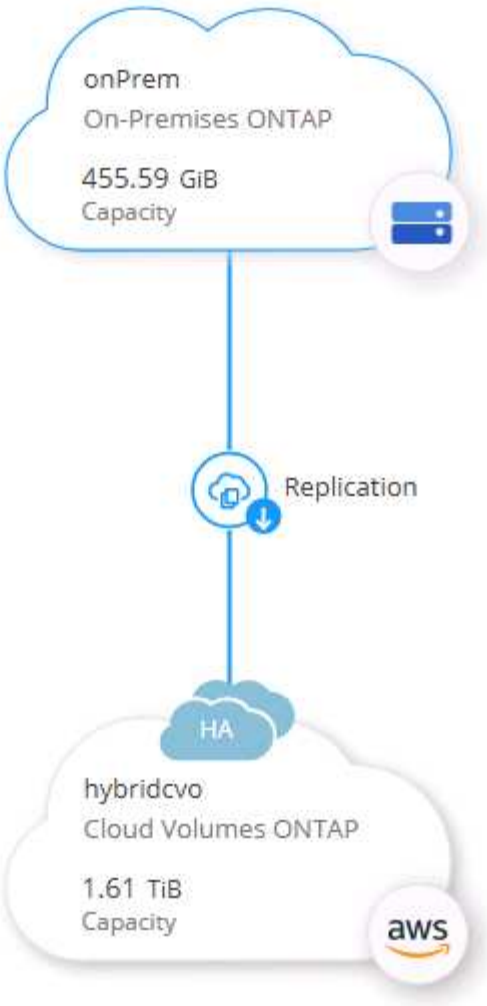


Configurare SnapMirror da on-premise a cloud

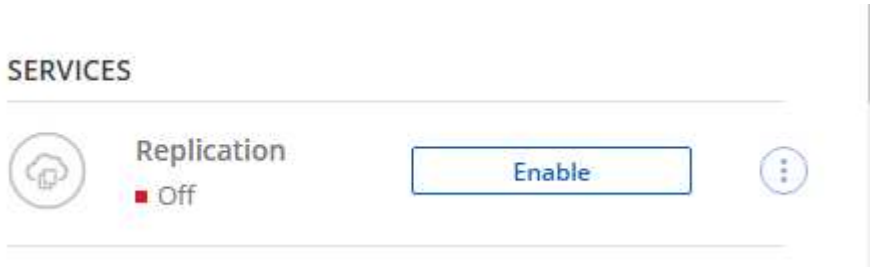
Ora che hai implementato un sistema ONTAP di origine e un sistema ONTAP di destinazione, puoi replicare volumi contenenti dati di database nel cloud.

Per una guida sulle versioni compatibili di ONTAP per SnapMirror, consultare "Matrice di compatibilità di SnapMirror".

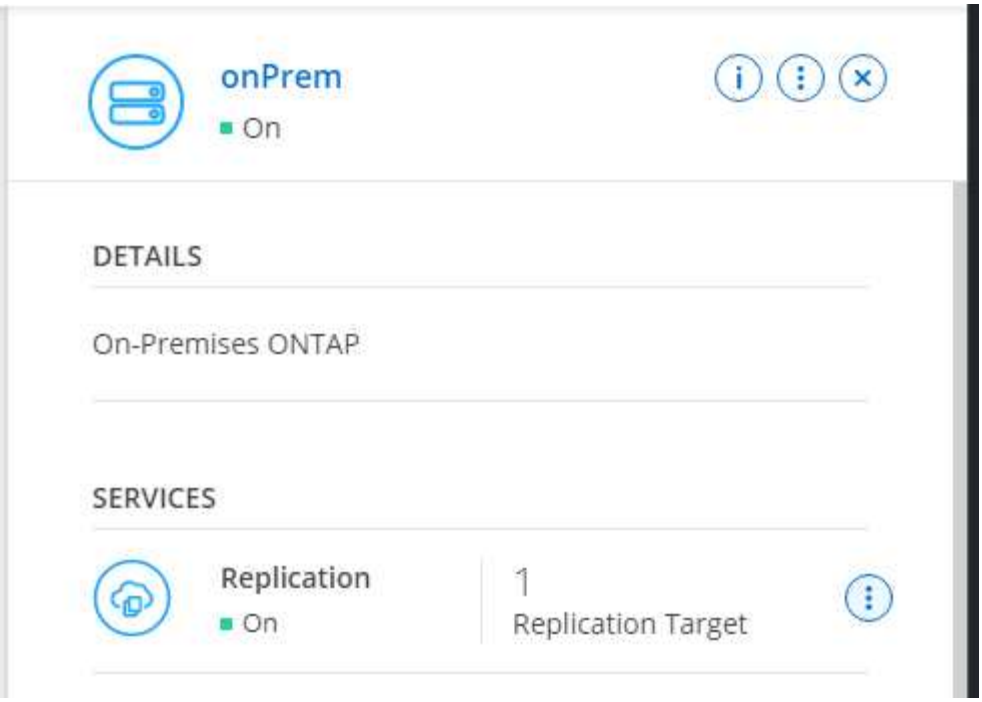
1. Fare clic sul sistema ONTAP di origine (on-premise) e trascinarlo nella destinazione, selezionare Replication > Enable (Replica > attiva) oppure selezionare Replication > Menu > Replicate (Replica > Menu > Replica).



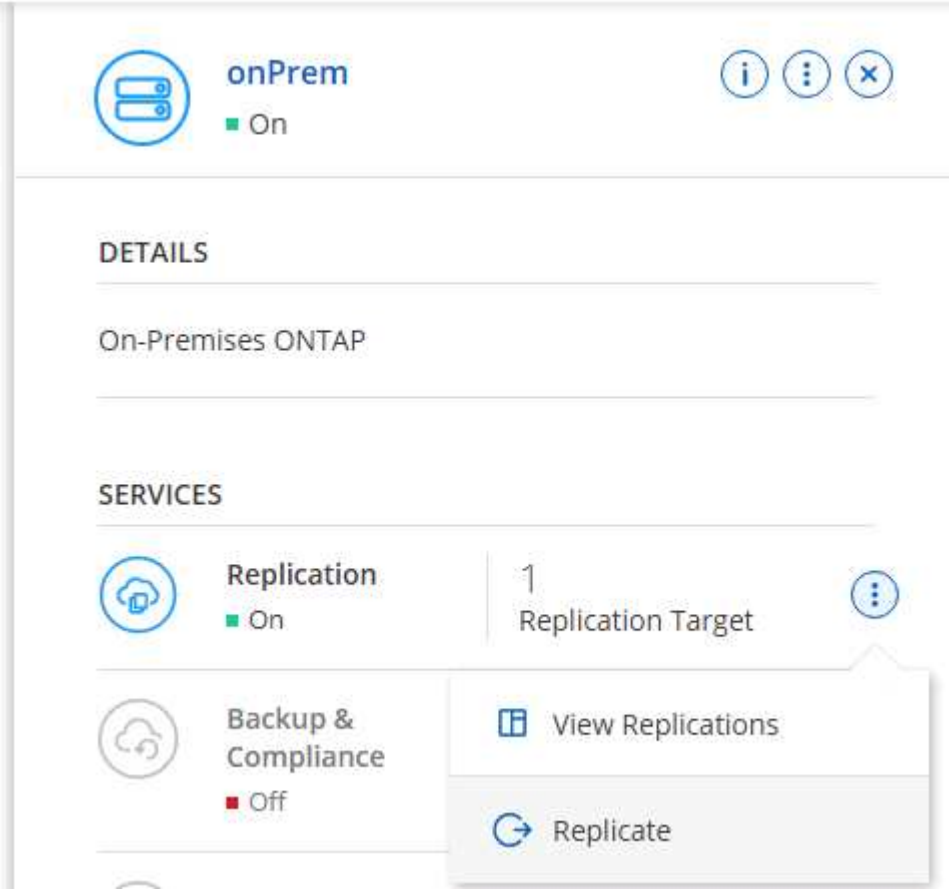
Selezionare Enable (attiva).



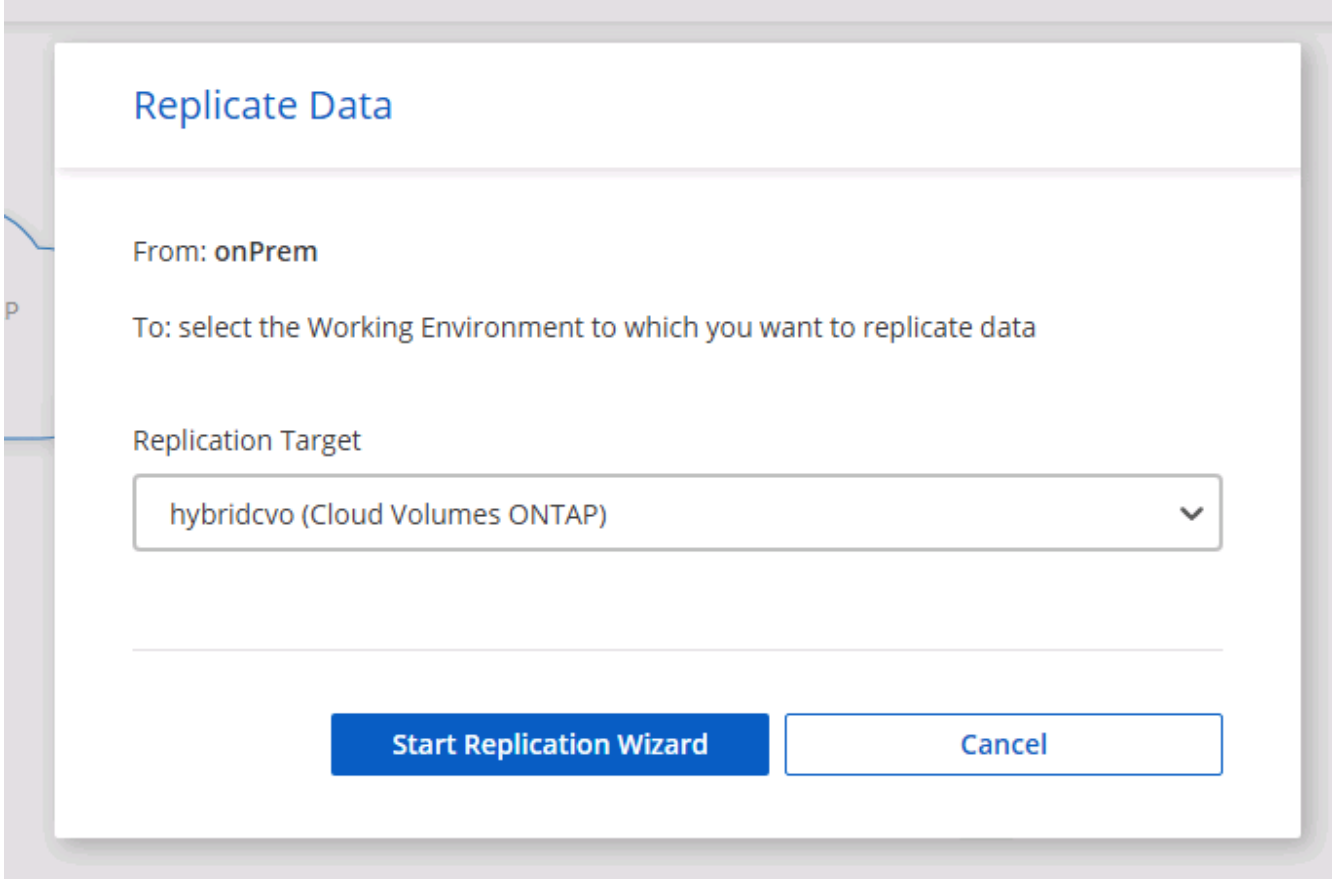
O Opzioni.



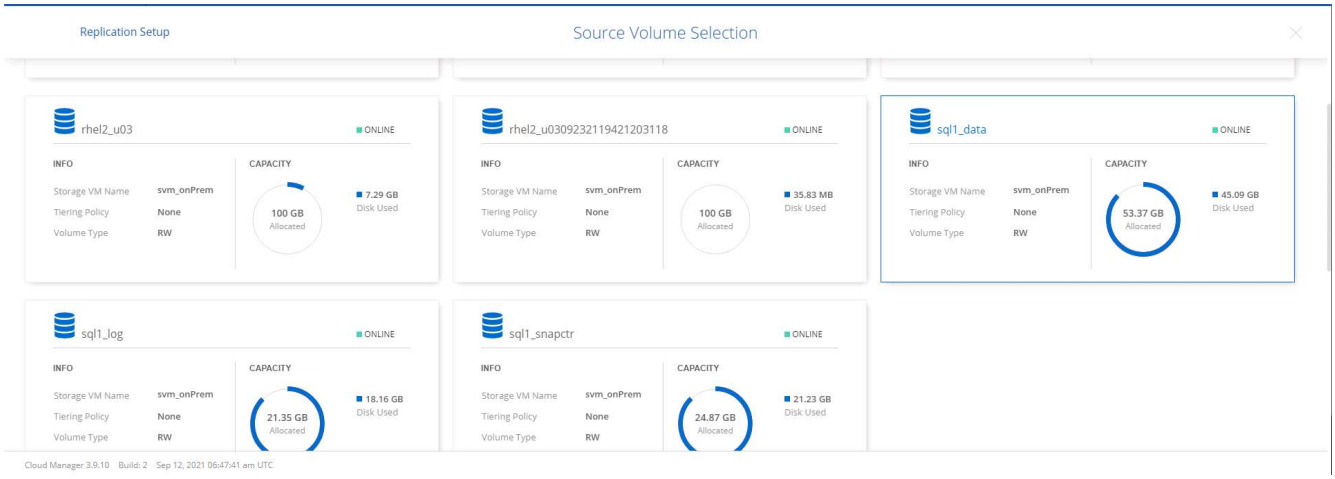
Replicare.



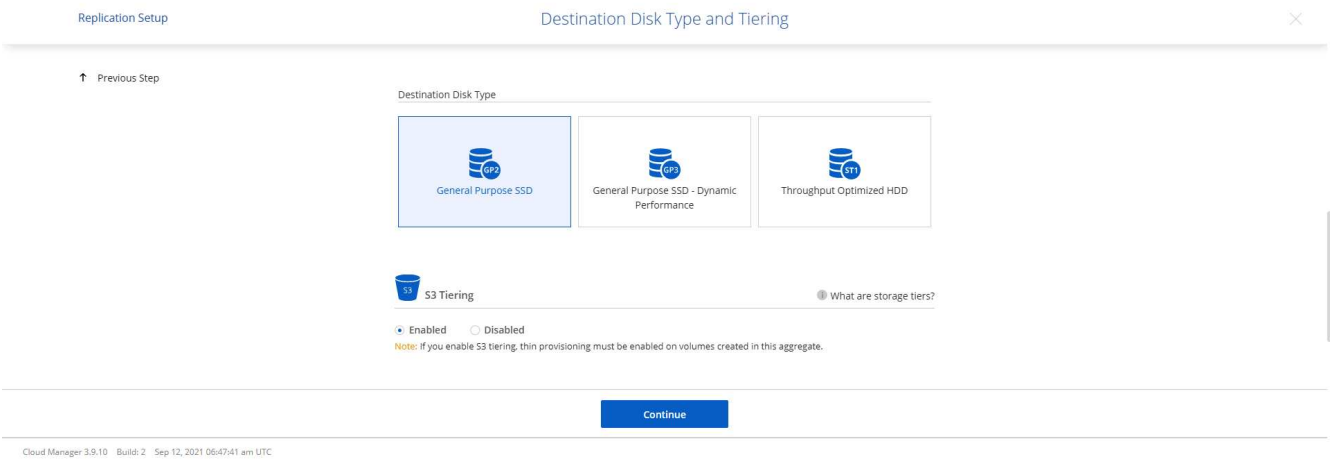
2. Se non è stato trascinato, scegliere il cluster di destinazione in cui replicare.



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

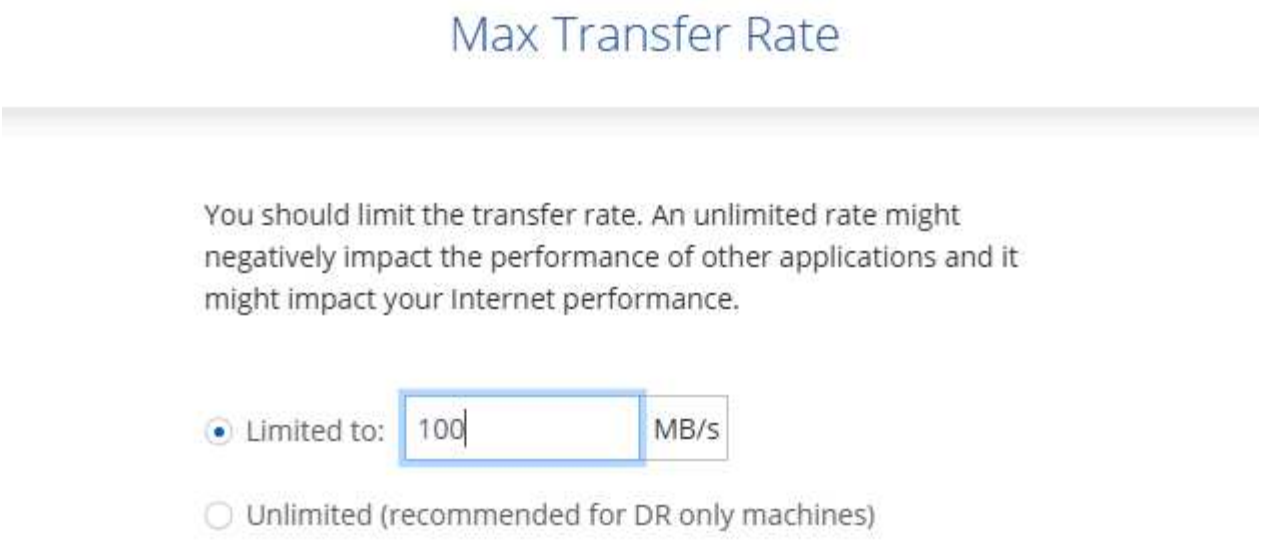


4. Scegliere il tipo di disco di destinazione e il criterio di tiering. Per il disaster recovery, consigliamo un SSD come tipo di disco e per mantenere il tiering dei dati. Il tiering dei dati tiering i dati mirrorati in storage a oggetti a basso costo e consente di risparmiare denaro sui dischi locali.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

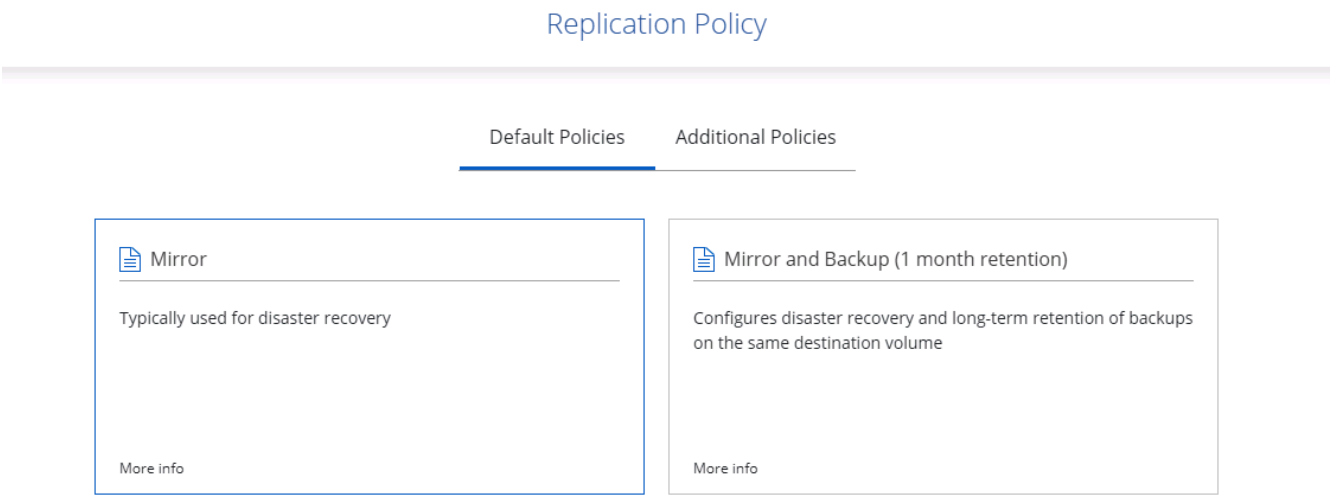


5. Selezionare il nome del volume di destinazione scelto `[source_volume_name]_dr`.

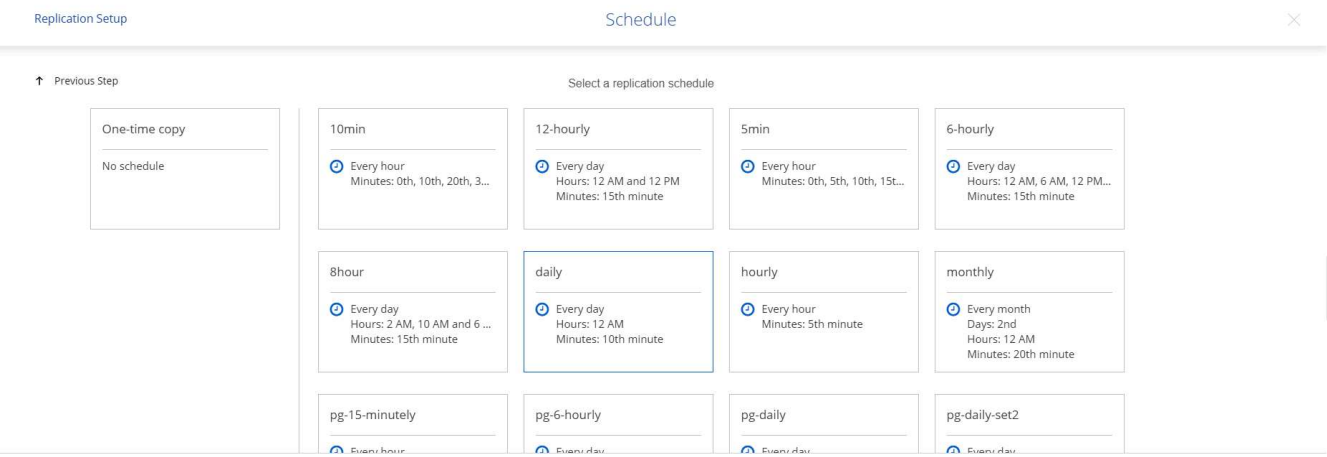
6. Selezionare la velocità di trasferimento massima per la replica. Ciò consente di risparmiare larghezza di banda se si dispone di una connessione a bassa larghezza di banda al cloud, ad esempio una VPN.



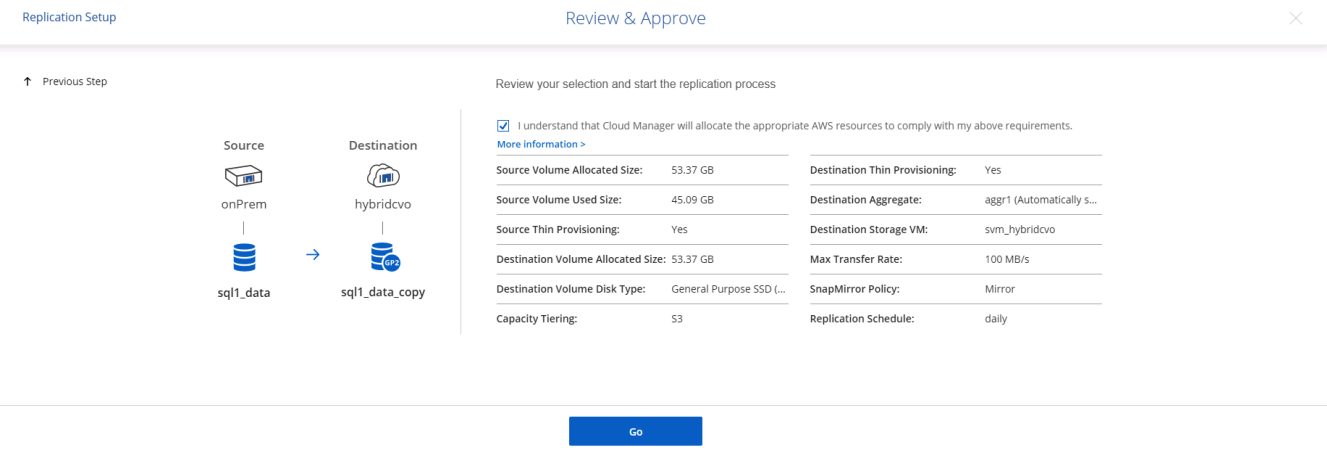
7. Definire il criterio di replica. Abbiamo scelto un Mirror, che prende i dataset più recenti e li replica nel volume di destinazione. Puoi anche scegliere una policy diversa in base ai tuoi requisiti.



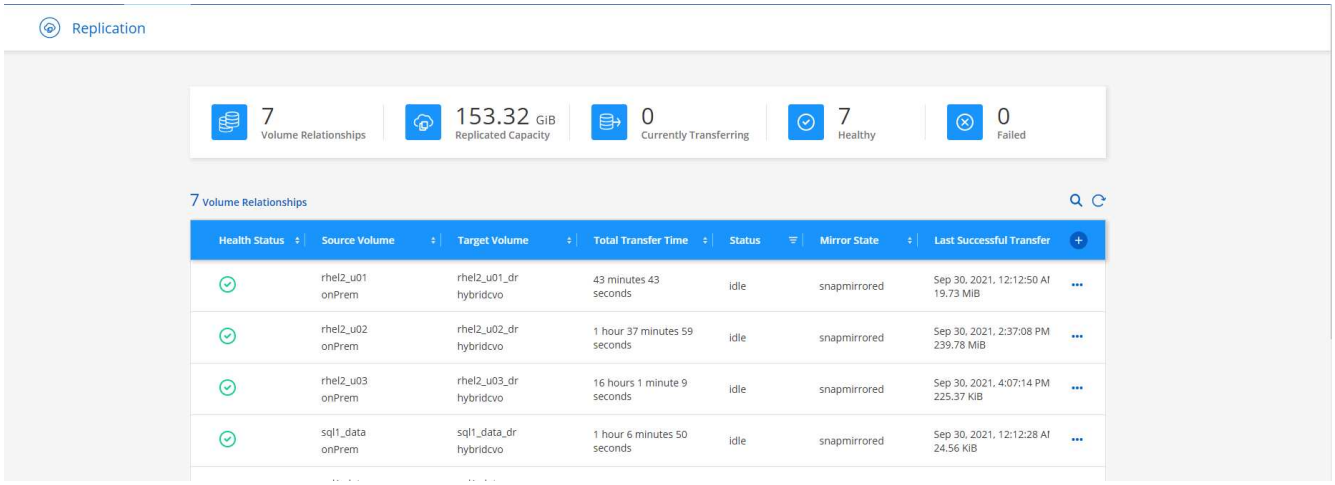
8. Scegliere la pianificazione per l'attivazione della replica. NetApp consiglia di impostare una pianificazione "giornaliera" di per il volume di dati e una pianificazione "oraria" per i volumi di log, sebbene sia possibile modificarla in base ai requisiti.



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.



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.



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.

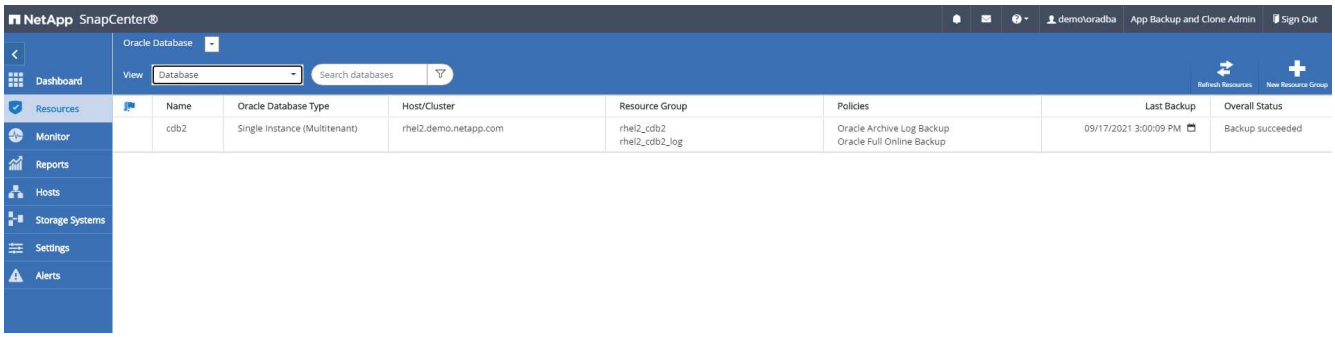
1. Recuperare la password dell'amministratore di Windows per accedere a un'istanza tramite RDP.
2. Disattivare il firewall Windows, unire l'host al dominio Windows SnapCenter e aggiungere l'istanza al server DNS per la risoluzione dei nomi.
3. Eseguire il provisioning di un volume di log di SnapCenter 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

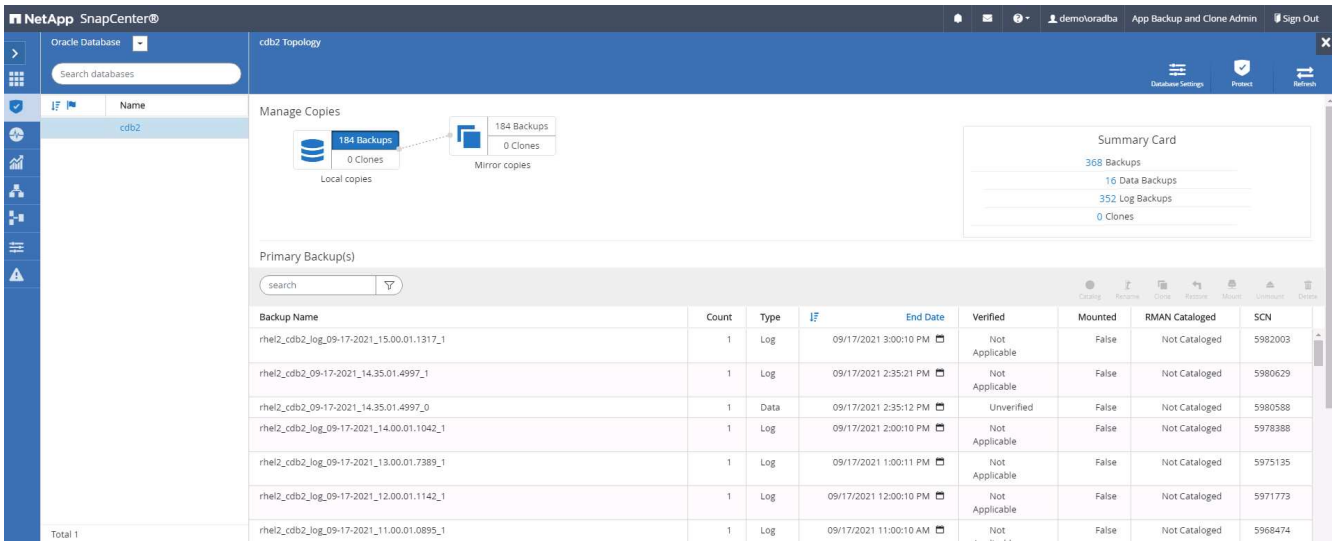
L'agilità del cloud pubblico, il time-to-value e i risparmi sui costi sono tutte proposte di valore significative per le aziende che adottano il cloud pubblico per lo sviluppo e il test delle applicazioni di database. Non esiste uno strumento migliore di SnapCenter per trasformare questo in realtà. SnapCenter 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

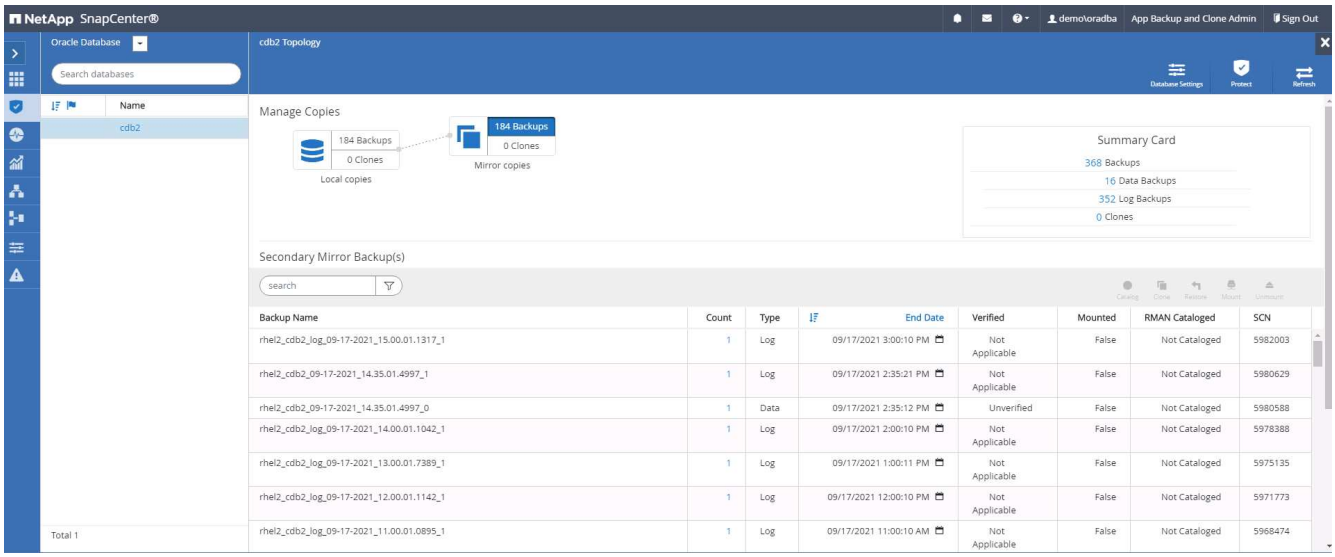
1. Accedere a SnapCenter con un ID utente per la gestione del database per Oracle. Accedere alla scheda risorse, che mostra i database Oracle protetti da SnapCenter.



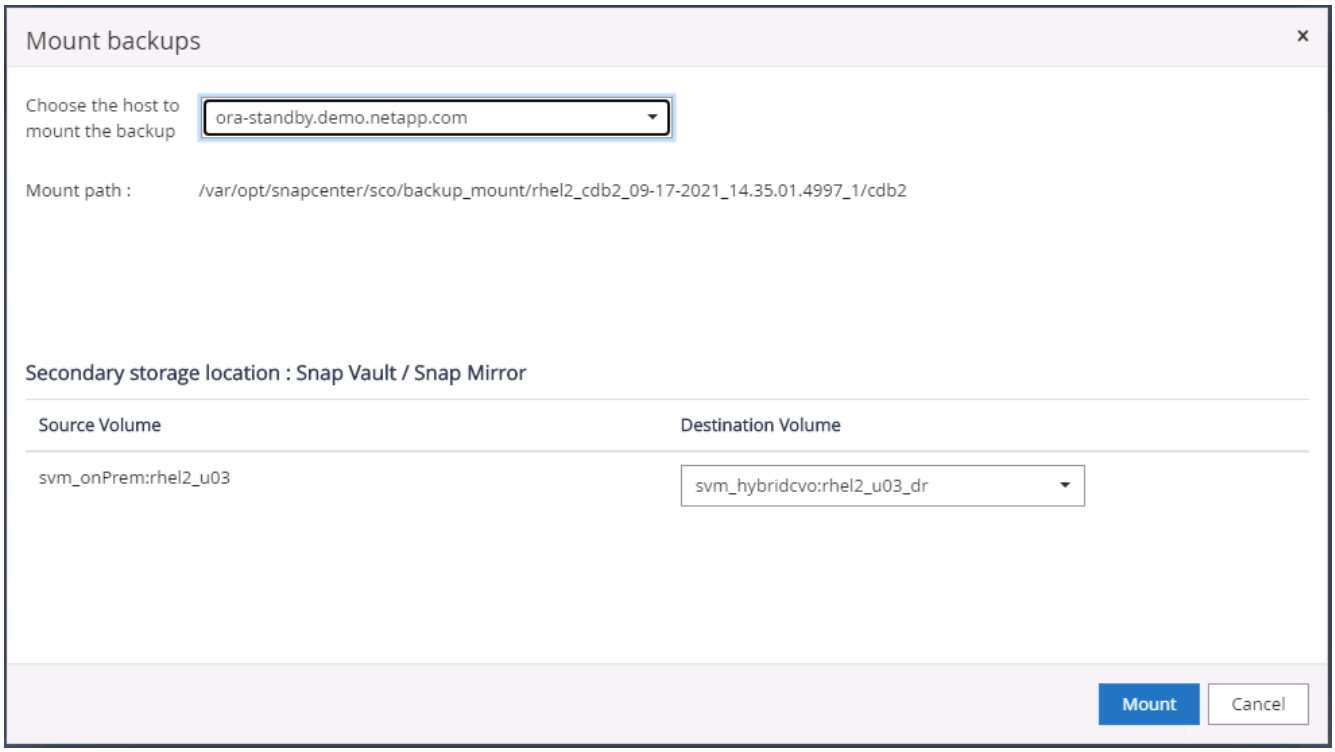
2. Fare clic sul nome del database on-premise desiderato per la topologia di backup e la vista dettagliata. Se è attivata una posizione replicata secondaria, vengono visualizzati i backup mirror collegati.

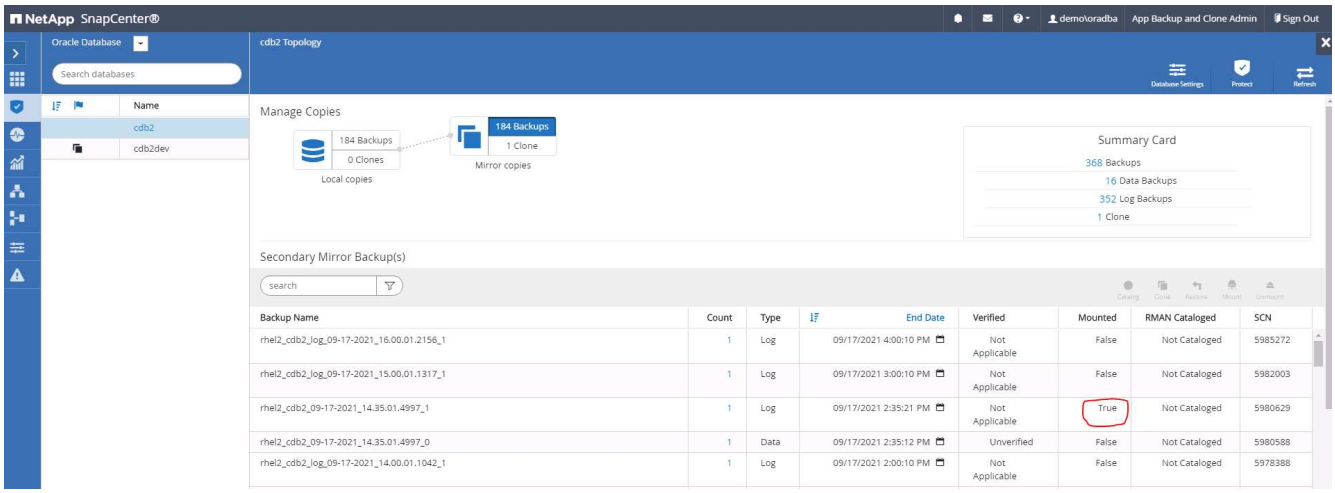


3. Per passare alla vista dei backup mirrorati, fare clic su Backup mirrorati. Vengono quindi visualizzati i backup dei mirror secondari.



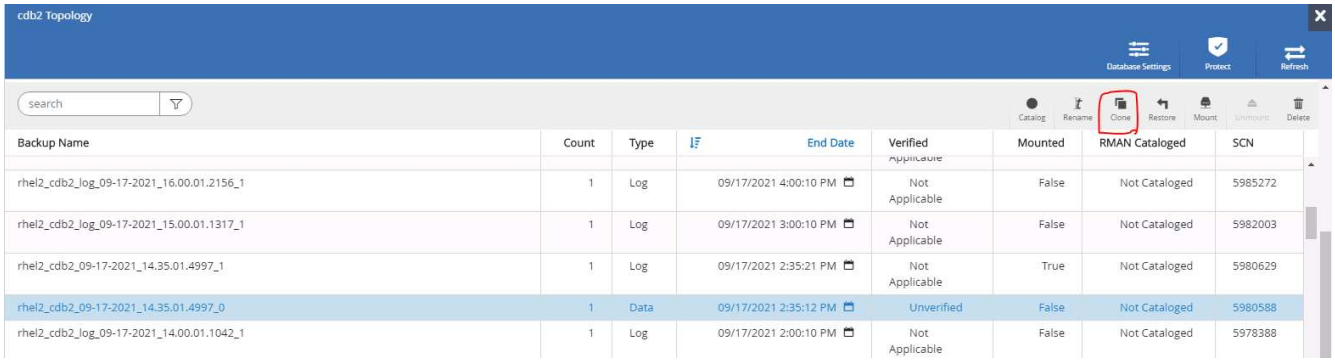
4. Scegliere una copia di backup del database secondario mirrorata da clonare e determinare un punto di ripristino in base all'ora e al numero di modifica del sistema o in base alla SCN. In genere, il punto di ripristino deve essere sottoposto a un periodo di tempo inferiore rispetto al tempo di backup 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.



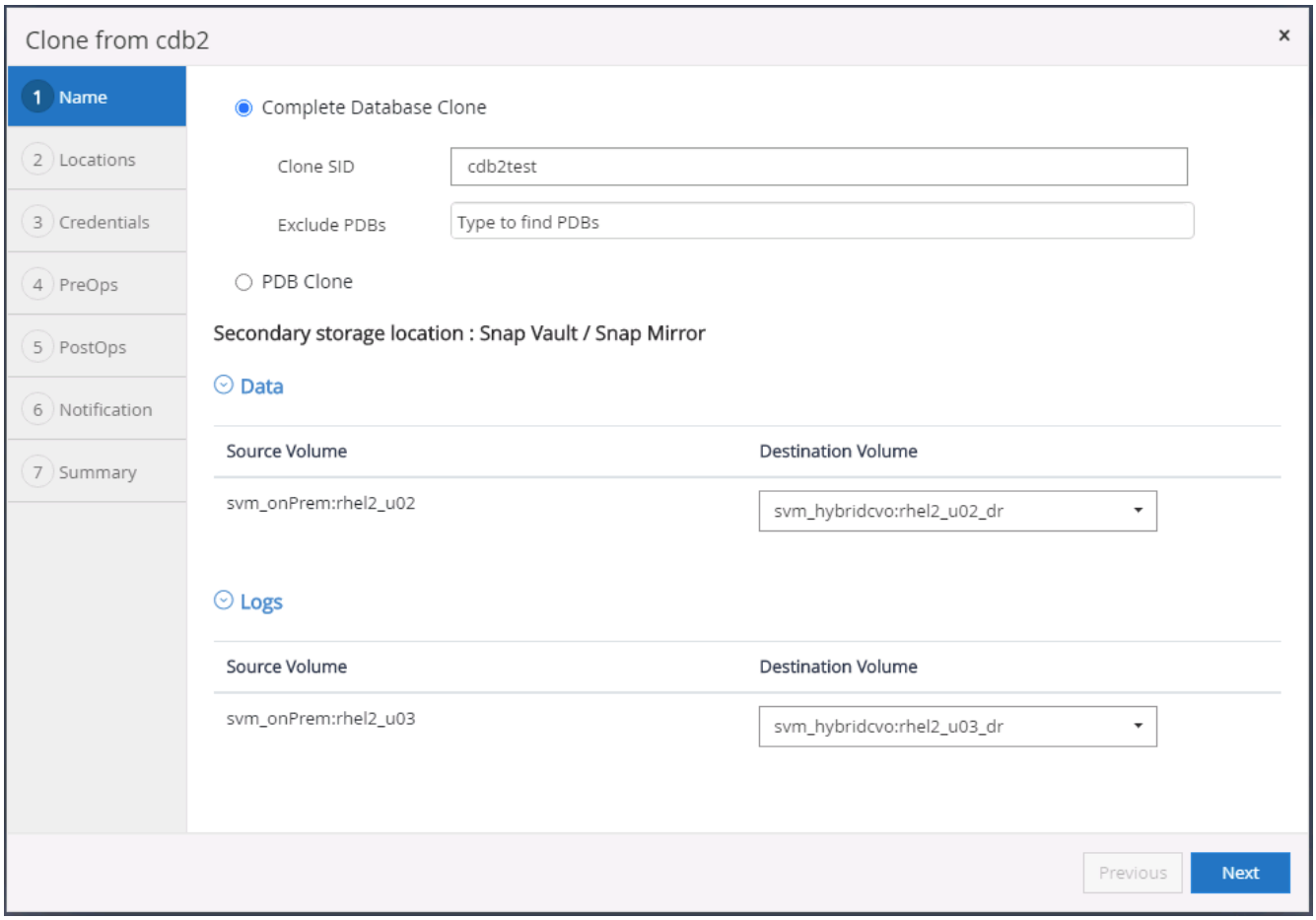


Se la funzione di eliminazione dei log è attivata e il punto di ripristino viene esteso oltre l'ultima eliminazione dei log, potrebbe essere necessario montare più backup dei log di archiviazione.

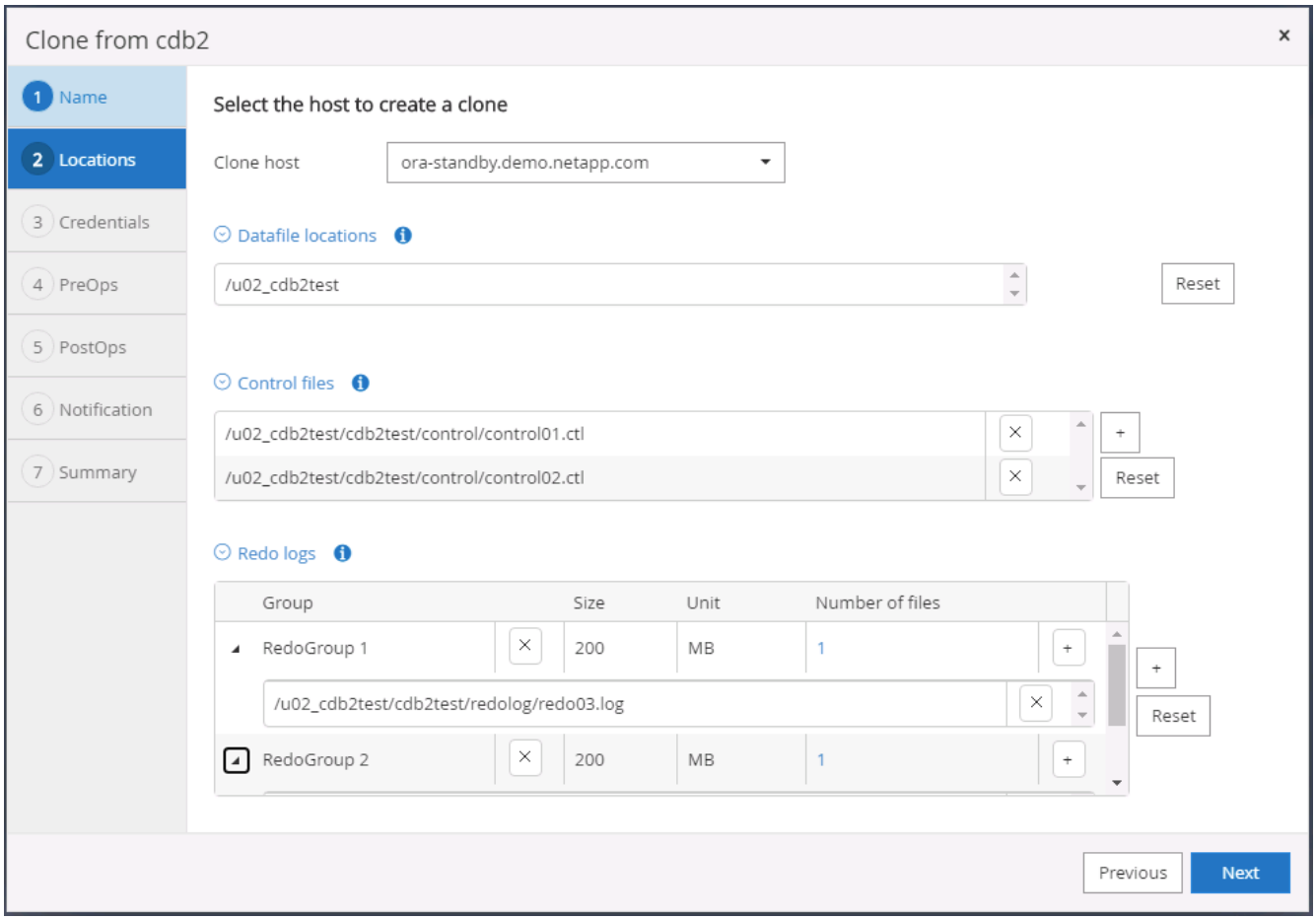
5. Evidenziare la copia di backup completa del database da clonare, quindi fare clic sul pulsante clone per avviare il flusso di lavoro del clone del database.



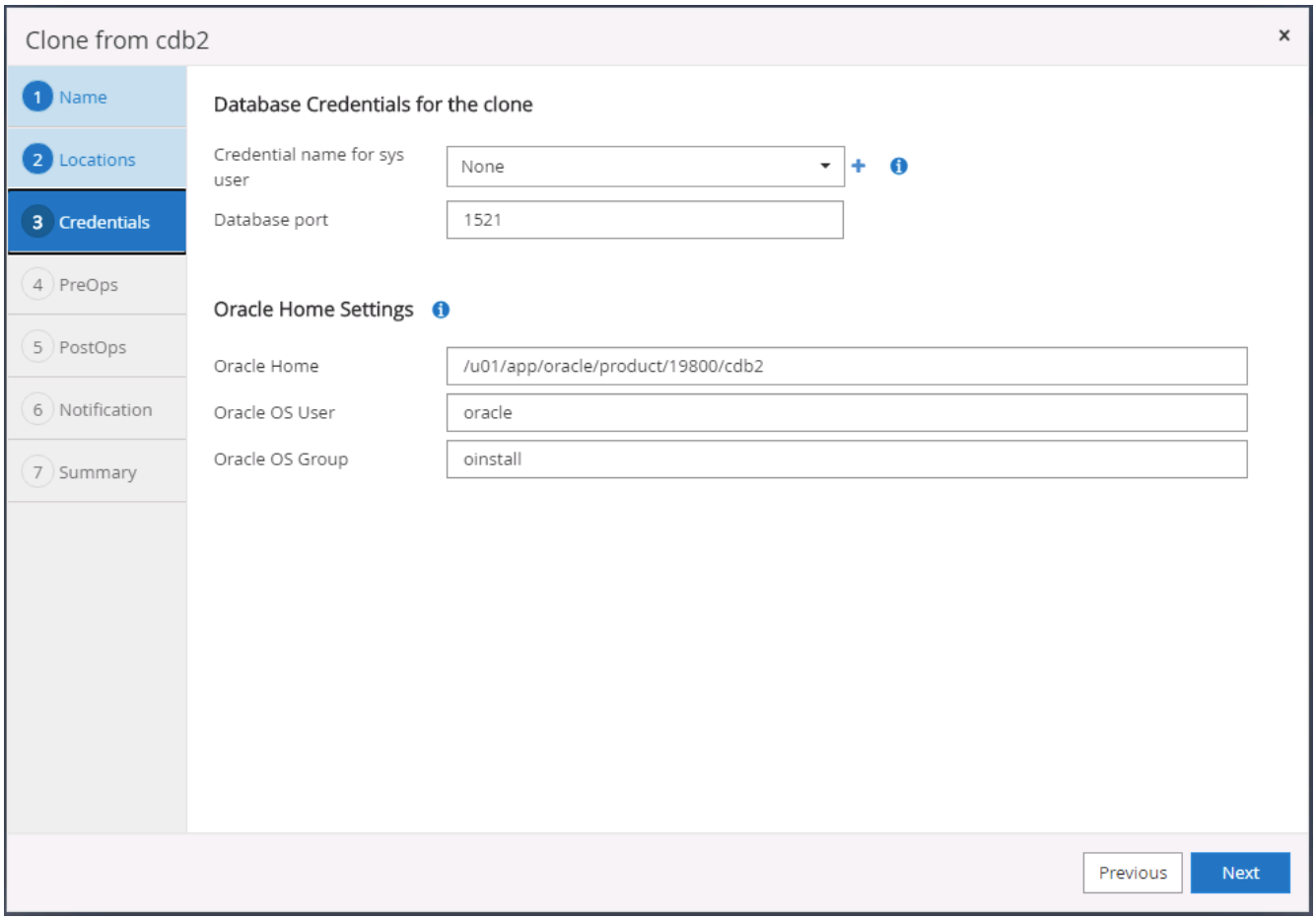
6. Scegliere un SID DB clone appropriato per un database container completo o un clone CDB.



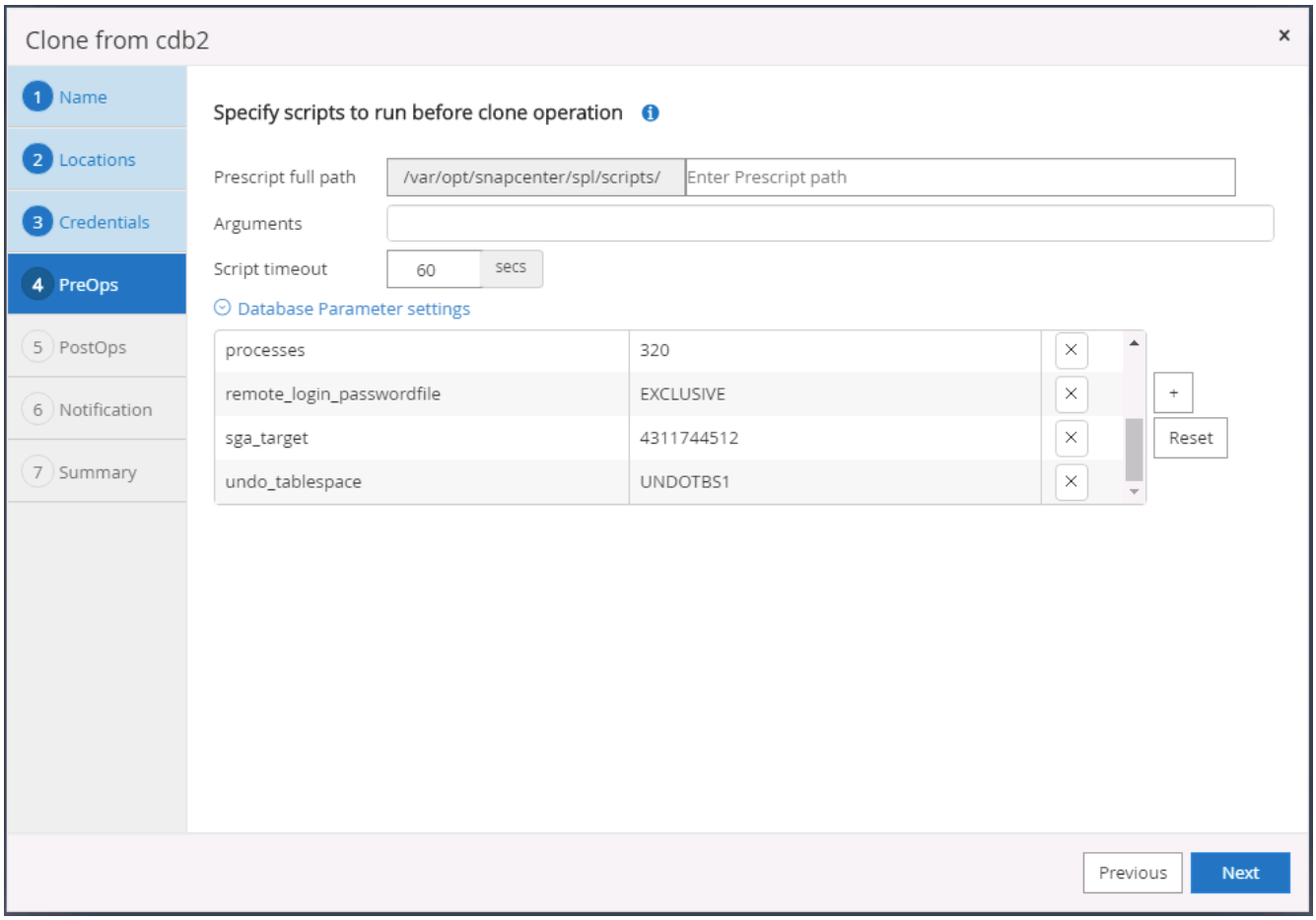
7. Selezionare l'host clone di destinazione nel cloud e le directory del file di dati, del file di controllo e del log di ripristino vengono create dal flusso di lavoro del clone.



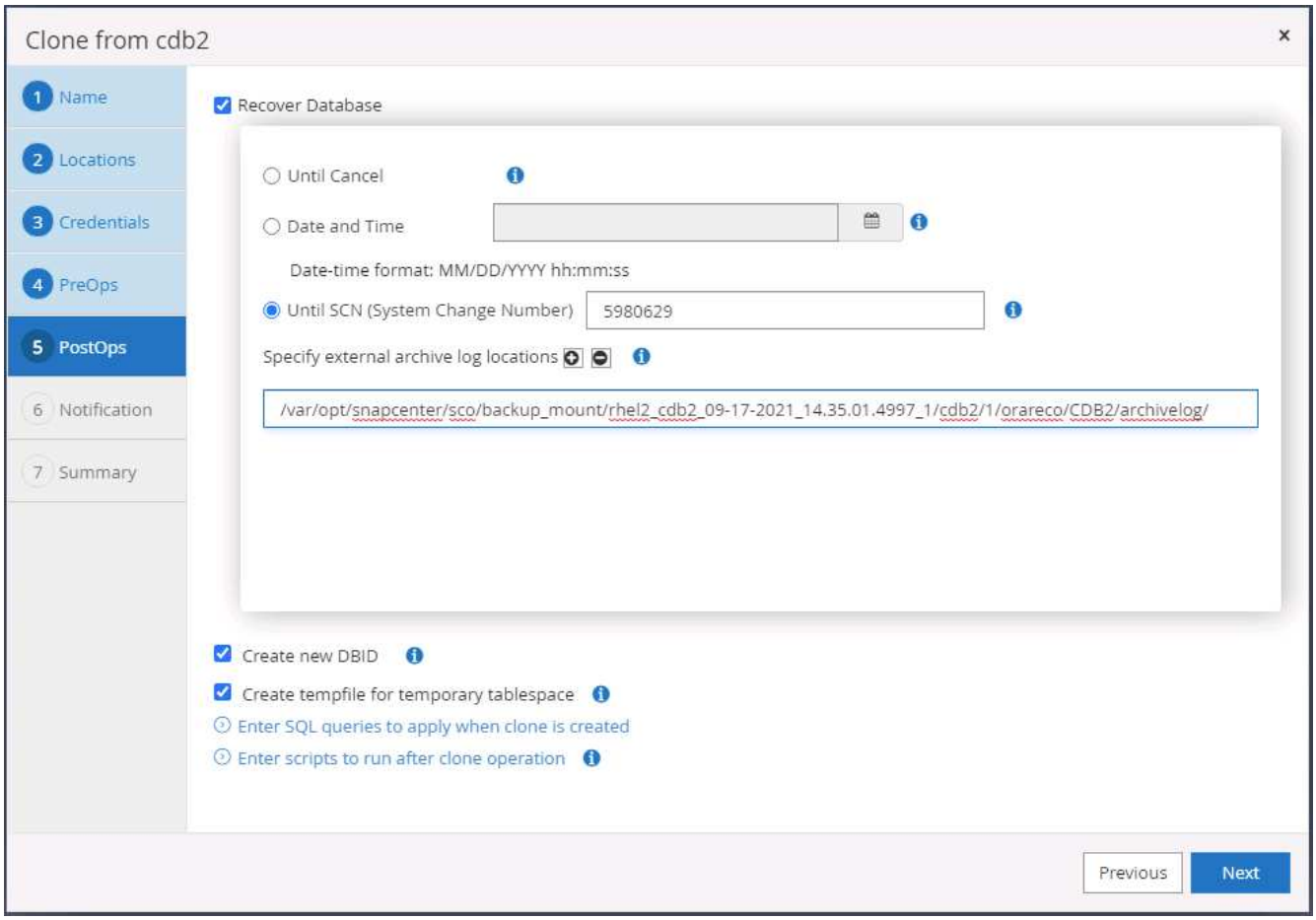
8. Il nome della credenziale Nessuno viene utilizzato per l'autenticazione basata sul sistema operativo, rendendo la porta del database irrilevante. Compilare i campi Oracle Home, Oracle OS User e Oracle OS Group appropriati, come configurati nel server DB clone di destinazione.

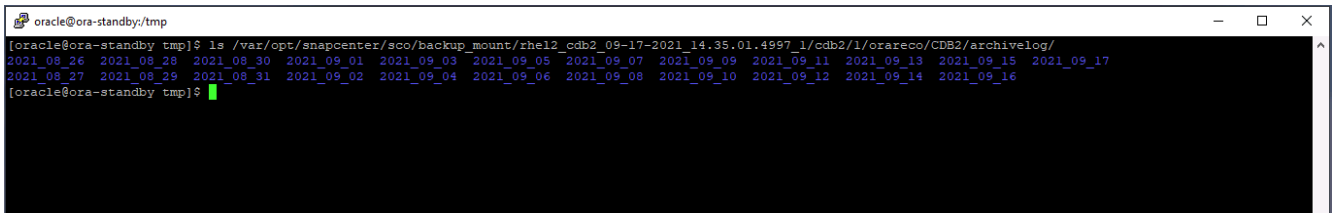


9. Specificare gli script da eseguire prima dell'operazione di clonazione. Cosa ancora più importante, il parametro dell'istanza del database può essere modificato o definito qui.

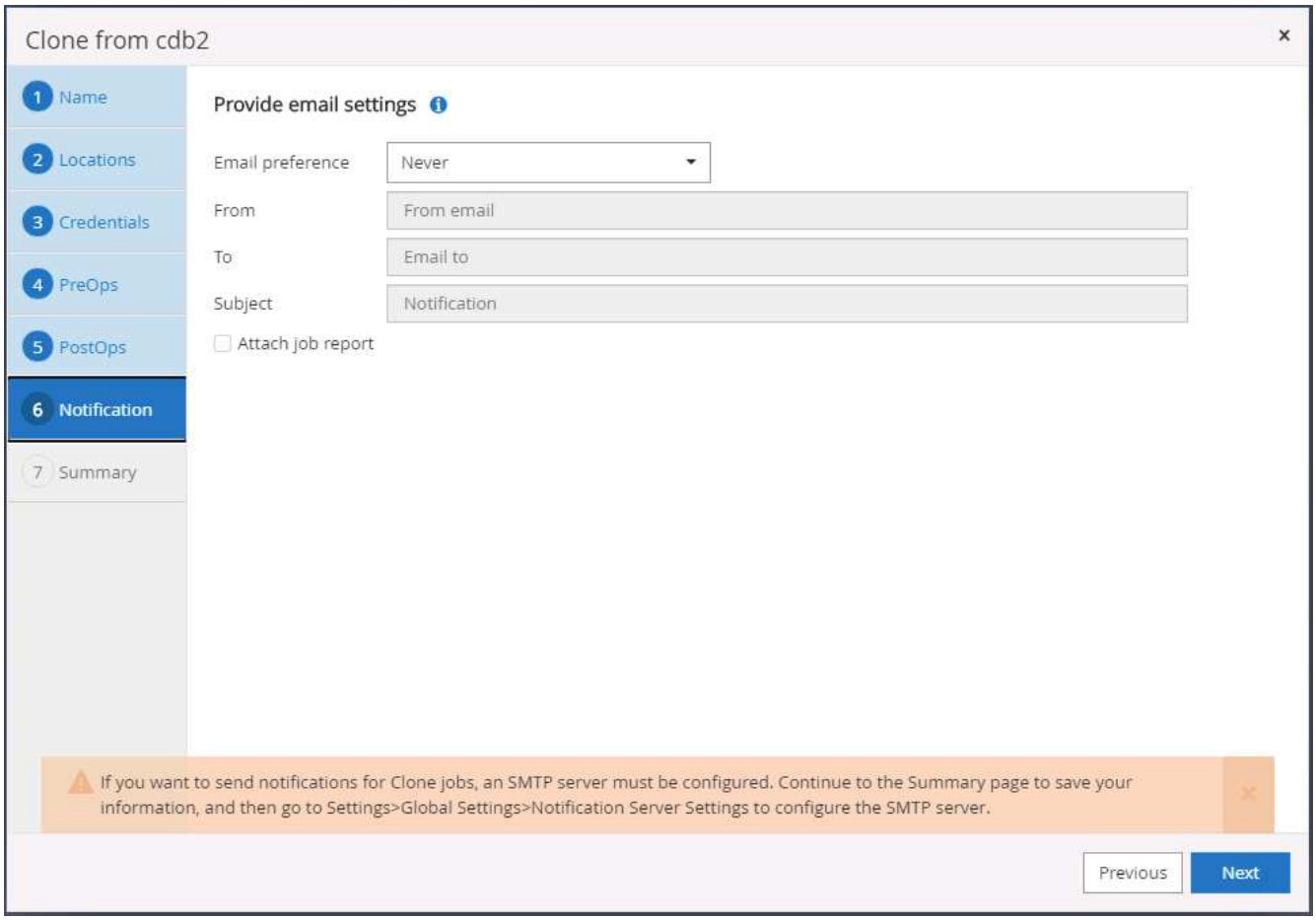


10. Specificare il punto di ripristino in base alla data e all'ora o alla SCN. Fino a quando Annulla ripristina il database fino ai log di archiviazione disponibili. Specificare la posizione del log di archiviazione esterno dall'host di destinazione in cui è montato il volume del log di archiviazione. 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.

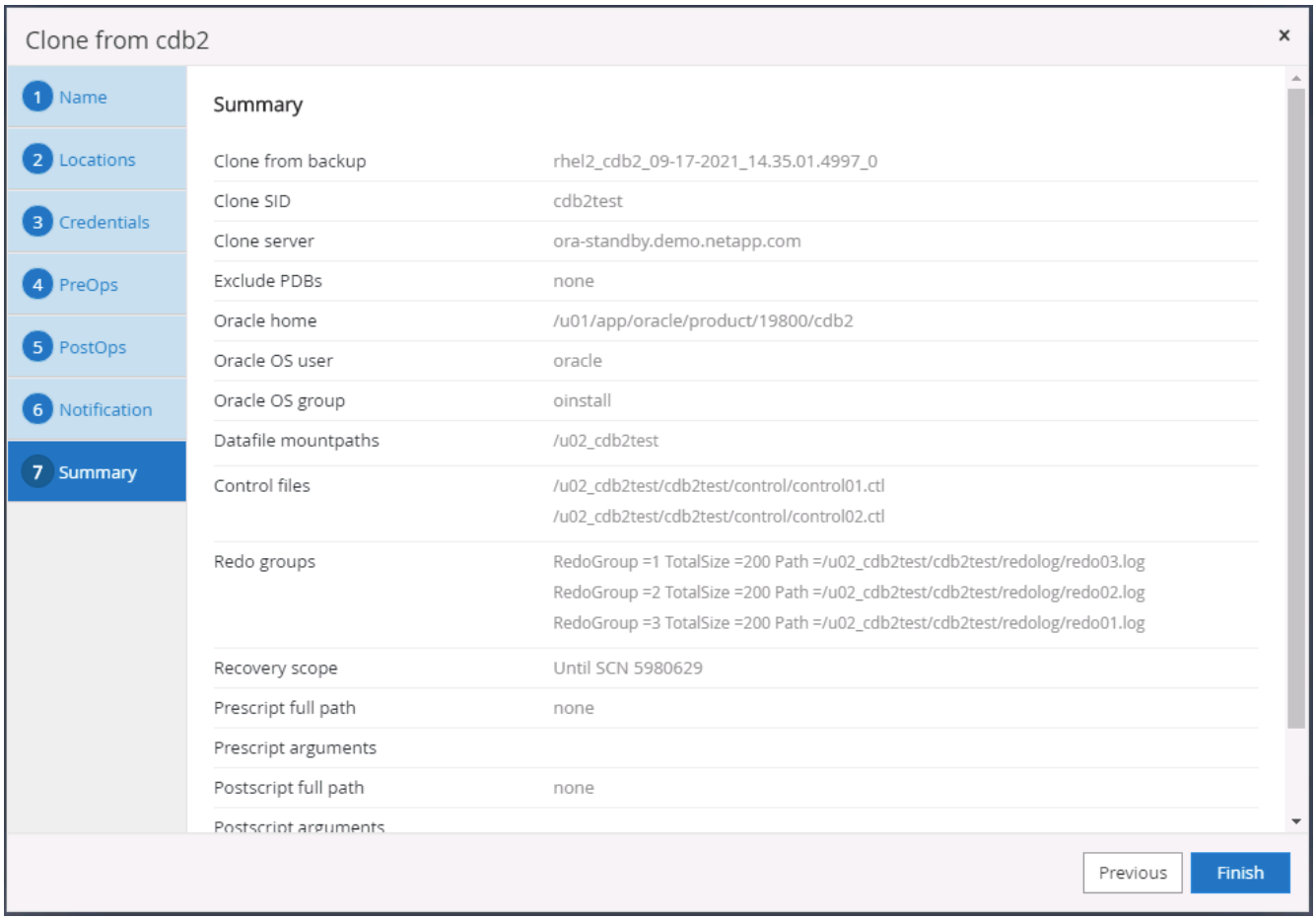




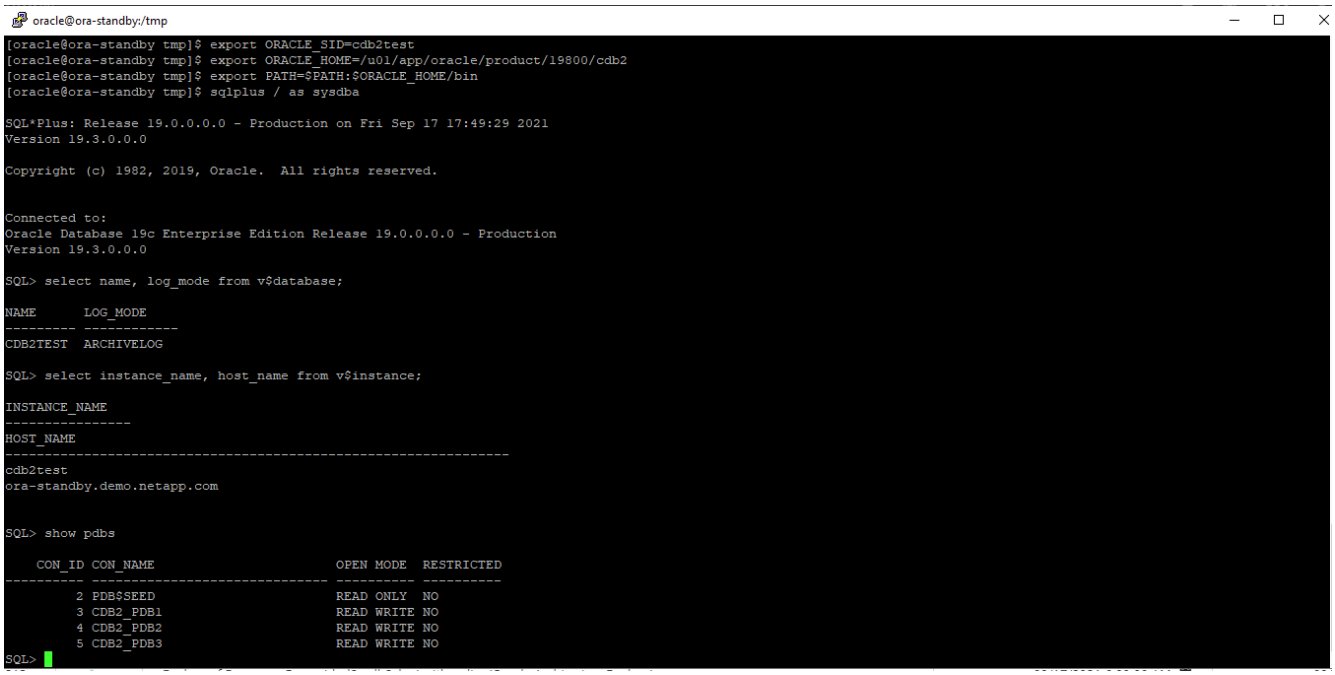
11. Configurare il server SMTP per la notifica via email, se lo si desidera.



12. Riepilogo dei cloni.

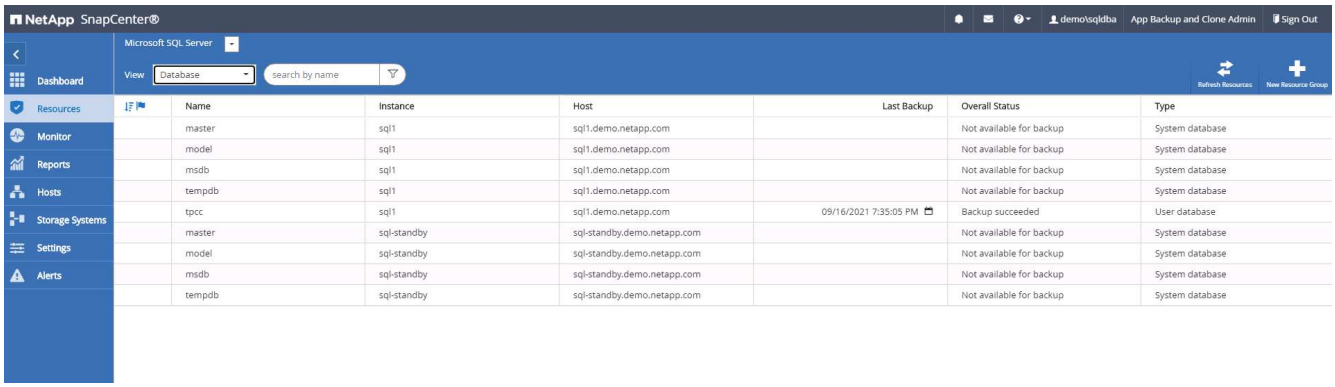


13. Dopo il cloning, è necessario eseguire la convalida per assicurarsi che il database clonato sia operativo. Alcune attività aggiuntive, come l'avvio del listener o la disattivazione della modalità di archiviazione del registro DB, possono essere eseguite sul database di sviluppo/test.

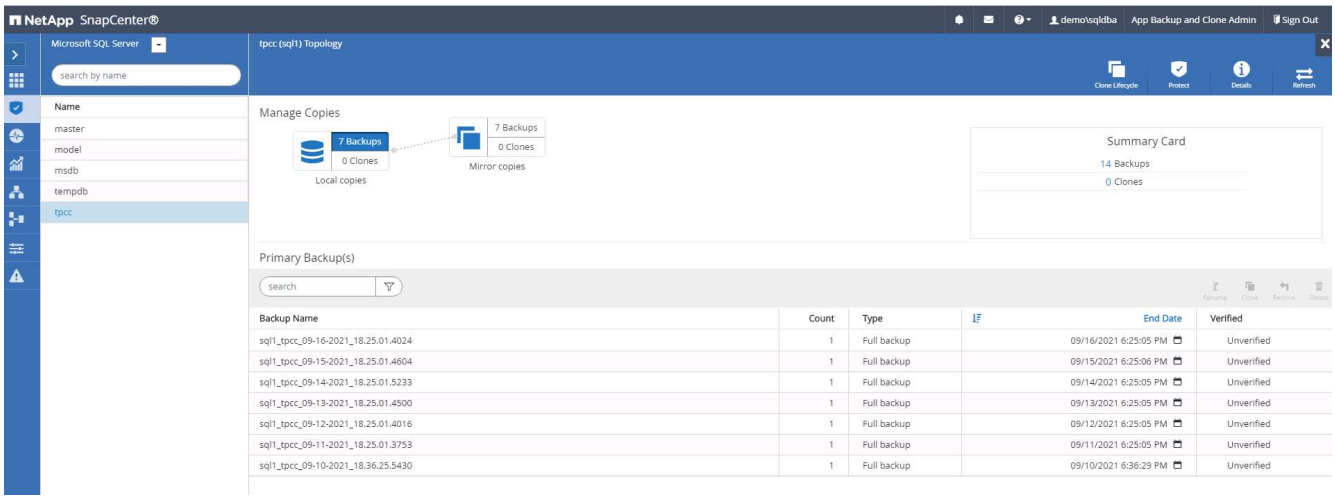


Clonare un database SQL per lo sviluppo/test da un backup Snapshot replicato

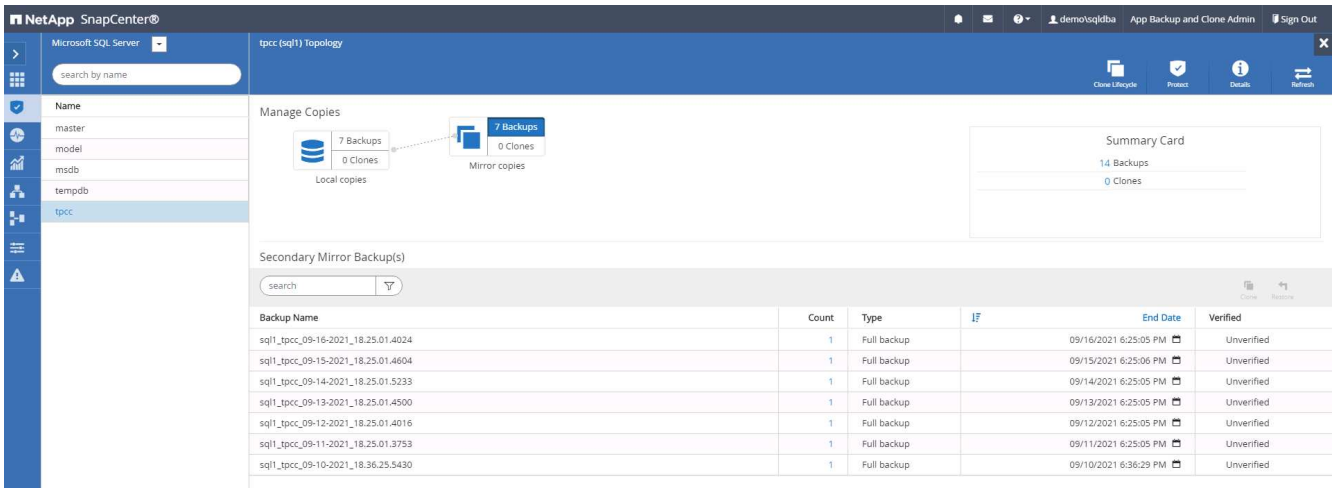
1. Accedere a SnapCenter con un ID utente per la gestione del database per SQL Server. Accedere alla scheda risorse, che mostra i database degli utenti SQL Server protetti da SnapCenter e un'istanza SQL di standby di destinazione nel cloud pubblico.



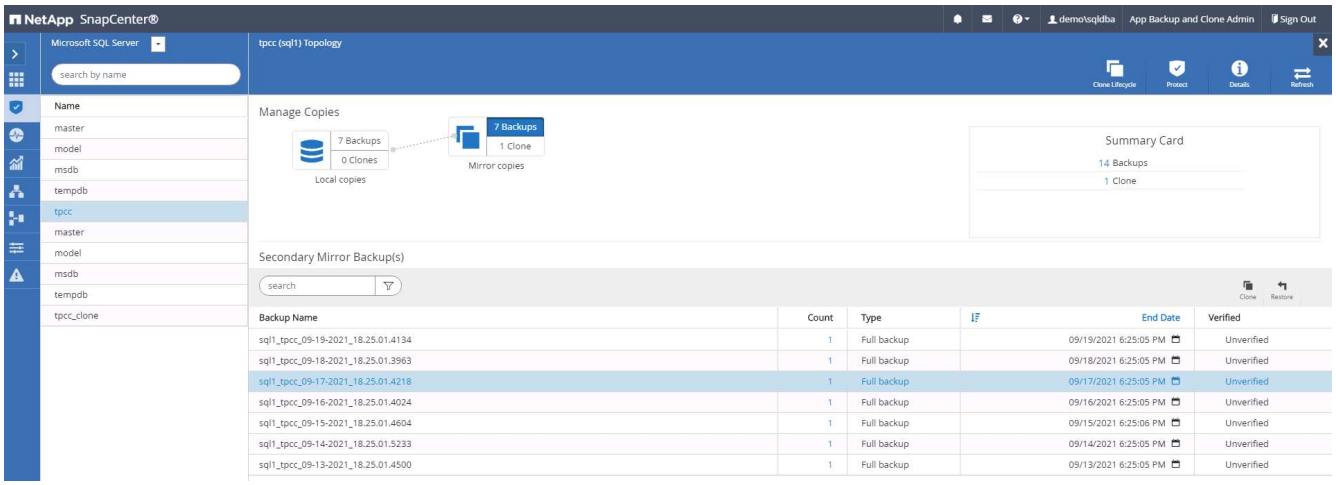
2. Fare clic sul nome del database utente SQL Server on-premise desiderato per la topologia dei backup e la vista dettagliata. Se è attivata una posizione replicata secondaria, vengono visualizzati i backup mirror collegati.

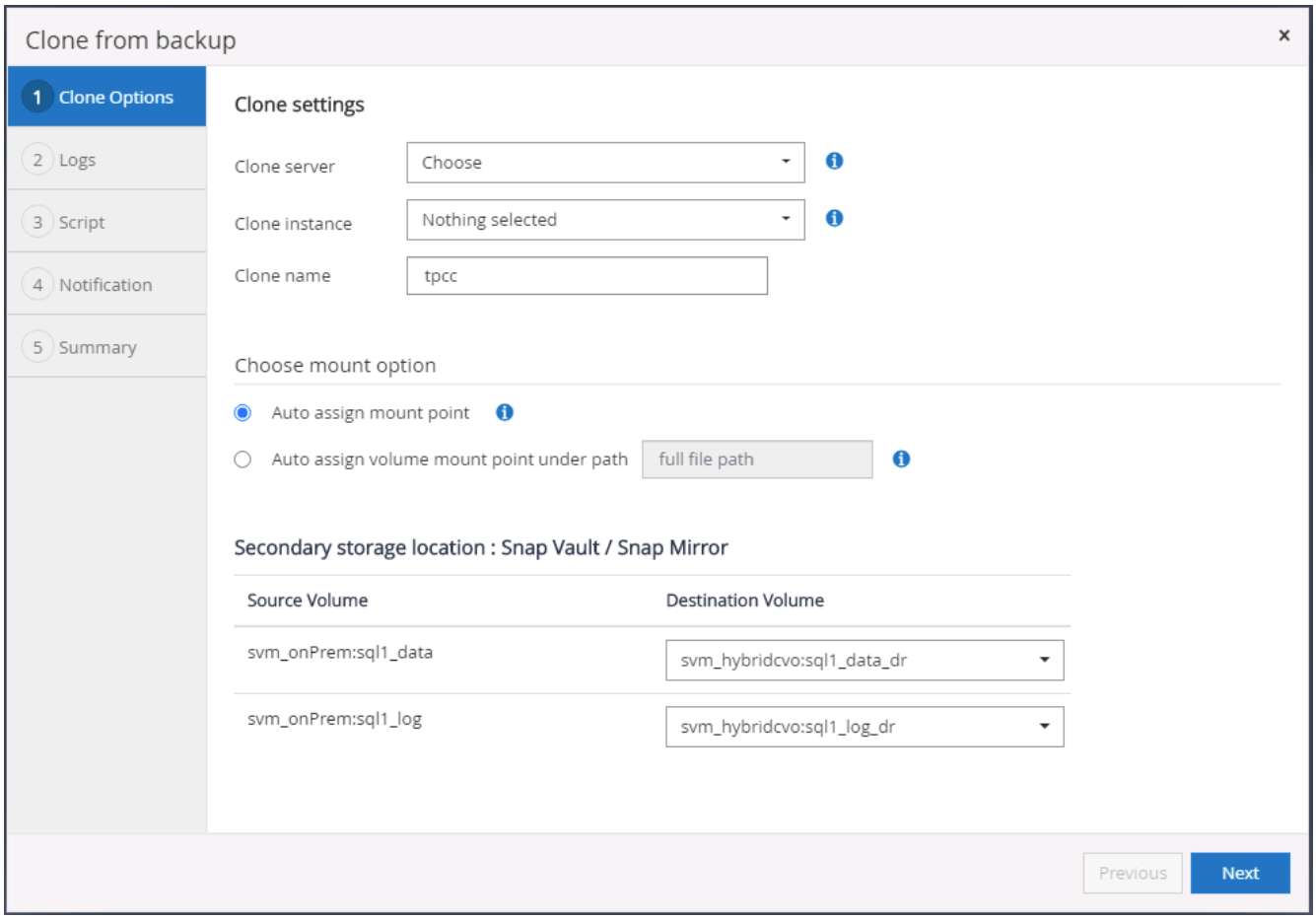


3. Passare alla vista dei backup mirrorati facendo clic su Backup mirrorati. Vengono quindi visualizzati i backup mirror secondari. Poiché SnapCenter esegue il backup del log delle transazioni di SQL Server su un'unità dedicata per il ripristino, vengono visualizzati solo i backup completi del database.

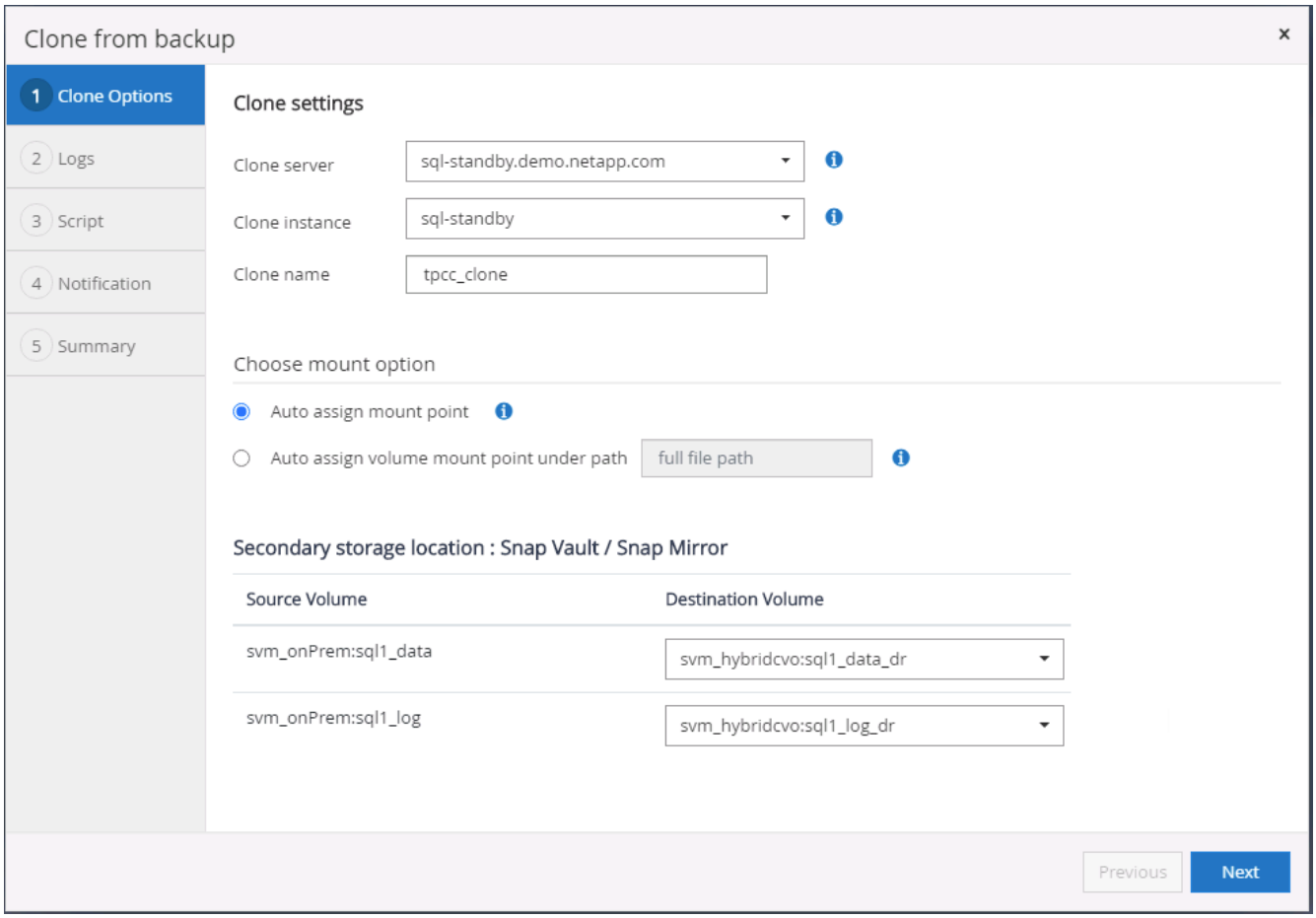


4. Scegliere una copia di backup, quindi fare clic sul pulsante Clone (Copia) per avviare il flusso di lavoro Clone from Backup (Copia da backup).

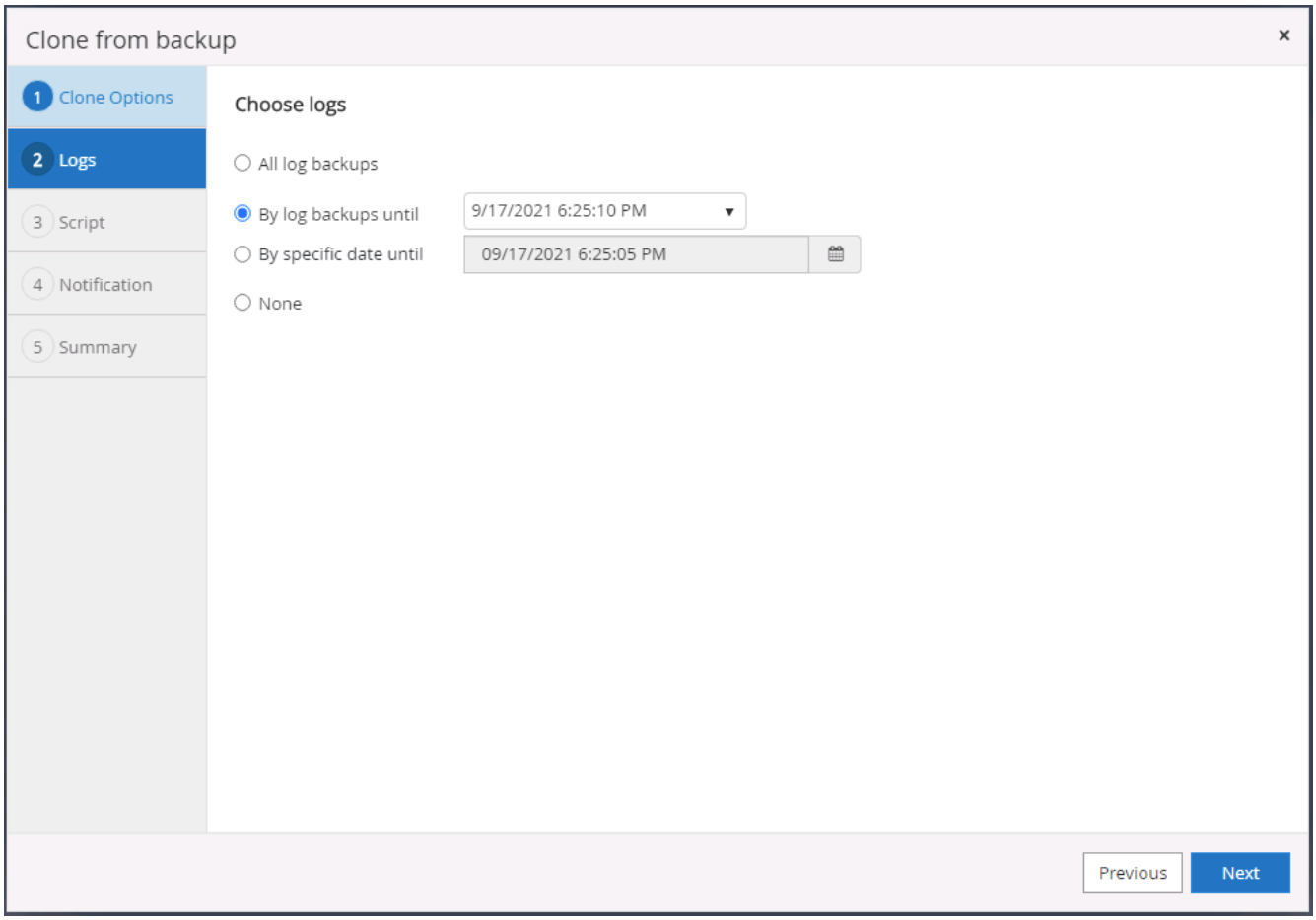




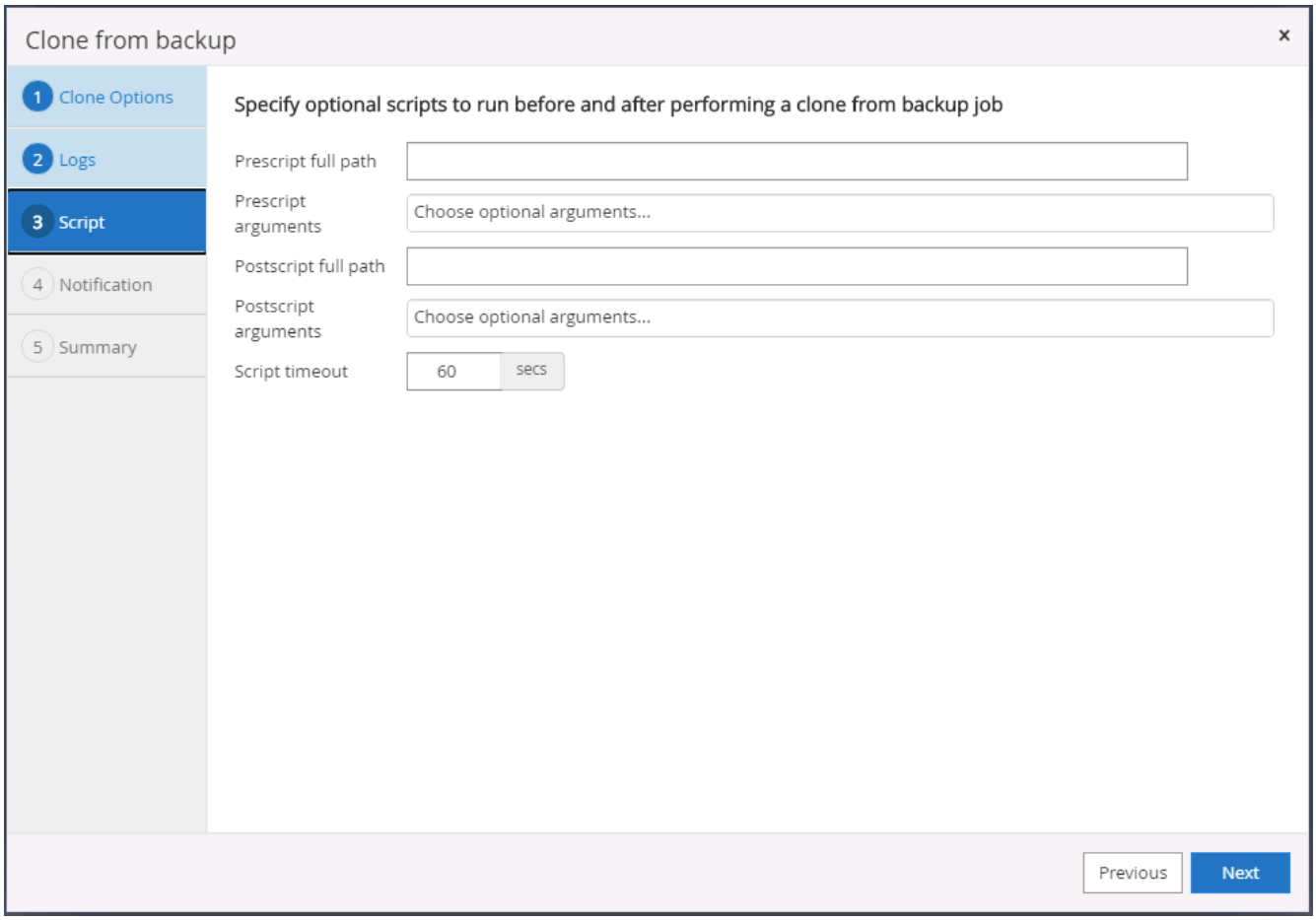
5. Selezionare un server cloud come server clone di destinazione, nome istanza clone e nome database clone. Scegliere un punto di montaggio ad assegnazione automatica o un percorso del punto di montaggio definito dall'utente.



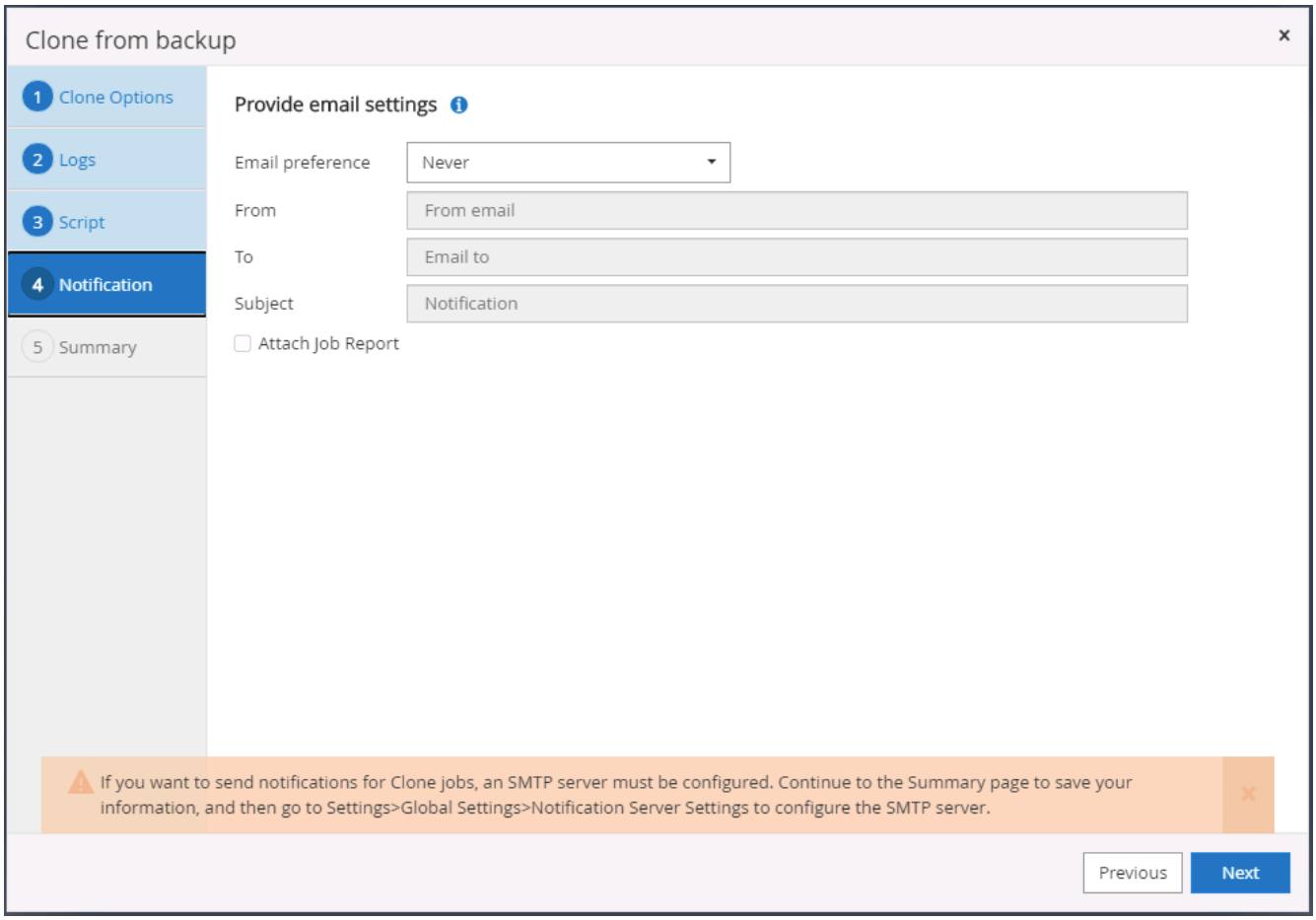
6. Determinare un punto di ripristino in base all'ora di backup del registro o a una data e un'ora specifiche.



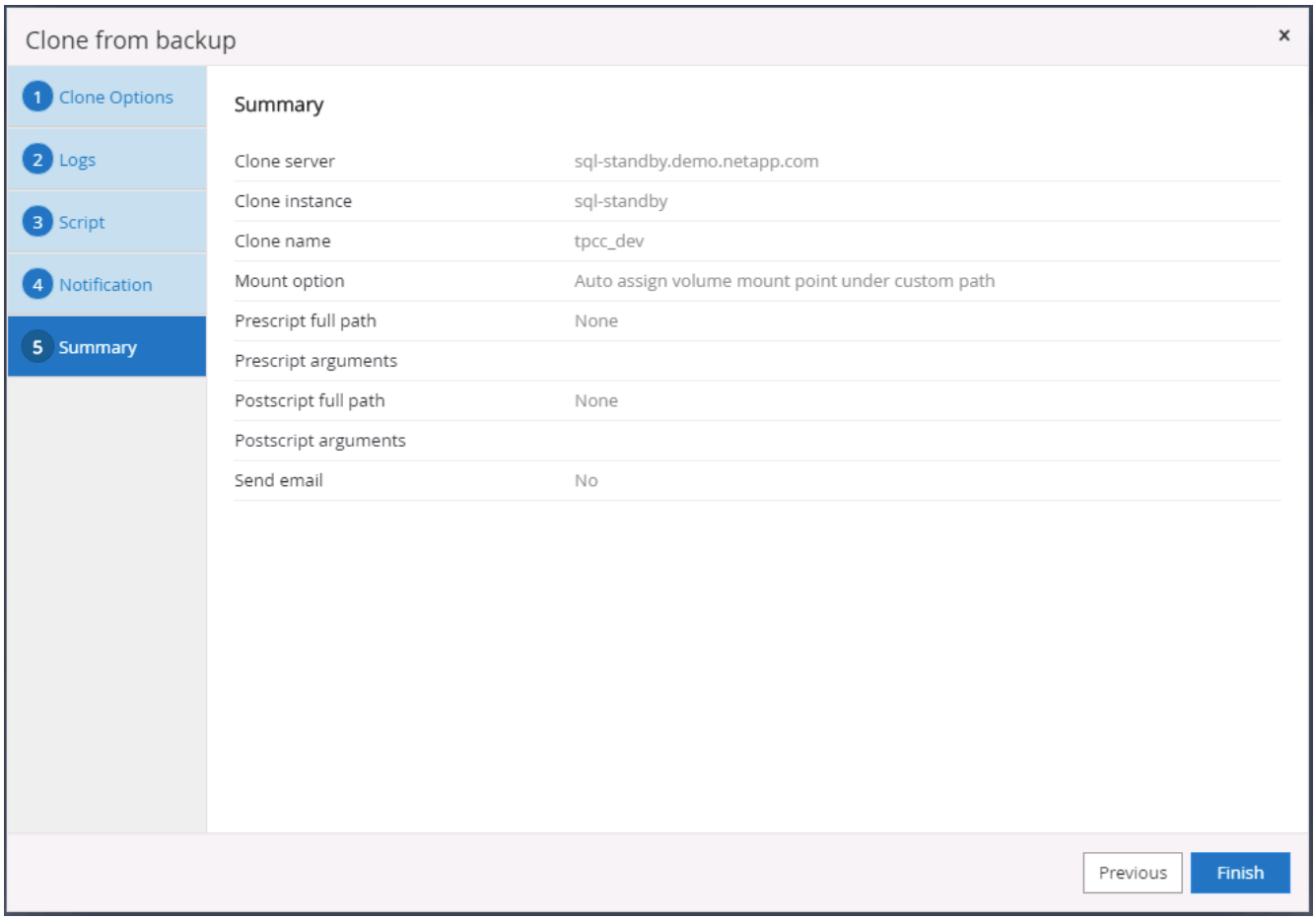
7. Specificare gli script opzionali da eseguire prima e dopo l'operazione di cloning.



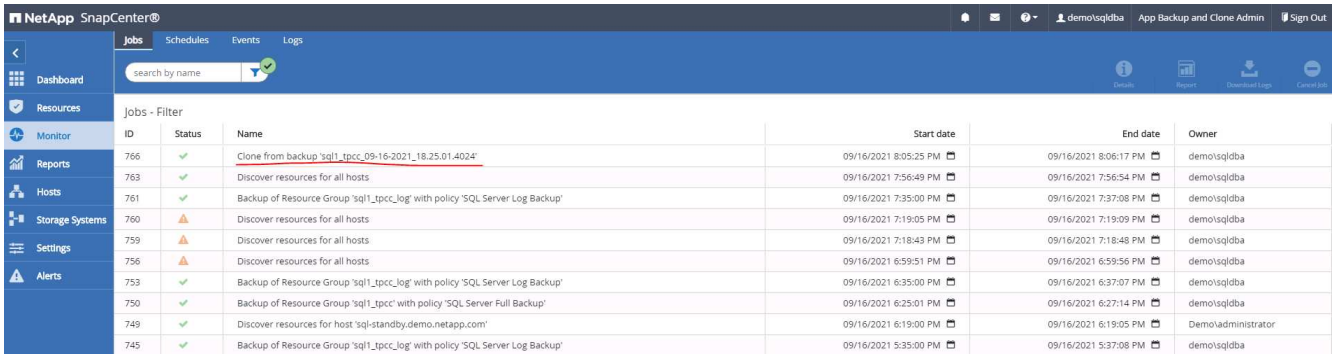
8. Configurare un server SMTP se si desidera inviare una notifica via email.



9. Riepilogo dei cloni.



10. 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.



Configurazione post-clone

1. 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.
2. Configurare un listener Oracle o registrare il database appena clonato con un listener esistente per l'accesso dell'utente.
3. 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?

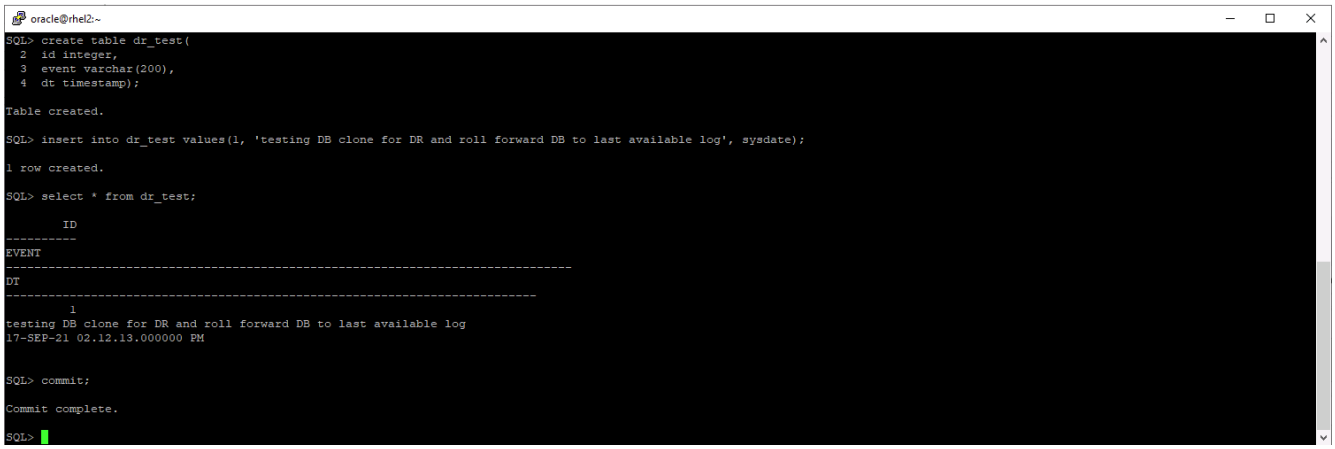
Se hai bisogno di aiuto per questa soluzione e per i casi d'utilizzo, partecipa a. "La community di NetApp Solution Automation supporta il canale slack" e cerca il canale di automazione della soluzione per inviare domande o domande.

Workflow di disaster recovery

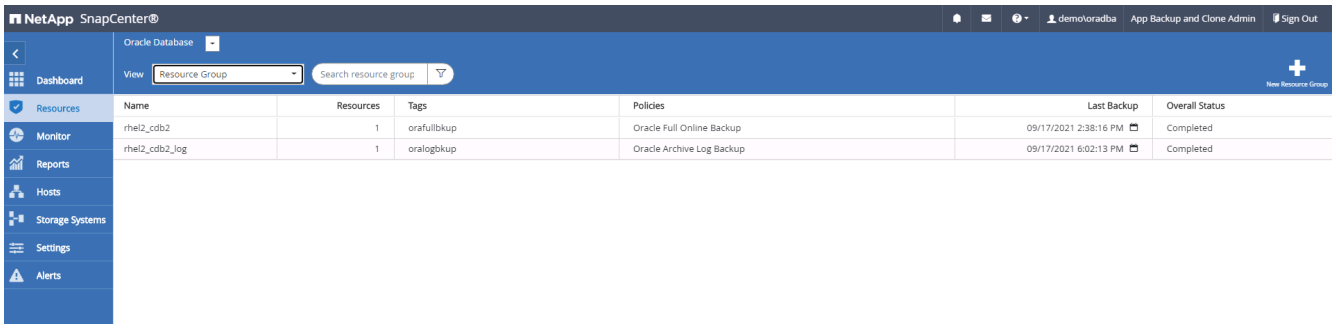
Le aziende hanno adottato il cloud pubblico come risorsa e destinazione praticabili per il disaster recovery. SnapCenter rende questo processo il più possibile perfetto. Questo flusso di lavoro di disaster recovery è molto simile al flusso di lavoro dei cloni, ma il ripristino del database viene eseguito 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

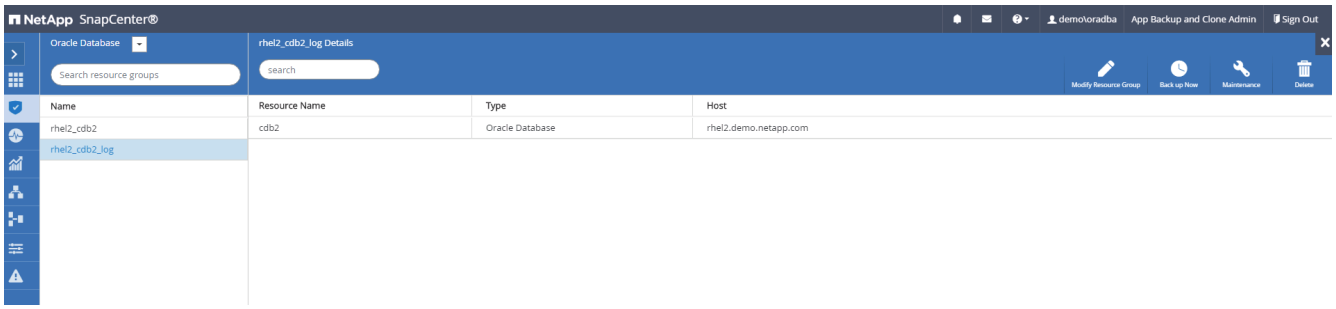
1. Per verificare che il ripristino del clone venga eseguito attraverso l'ultimo log disponibile, abbiamo creato una piccola tabella di test e inserito una riga. I dati del test vengono ripristinati dopo un ripristino completo dell'ultimo registro disponibile.

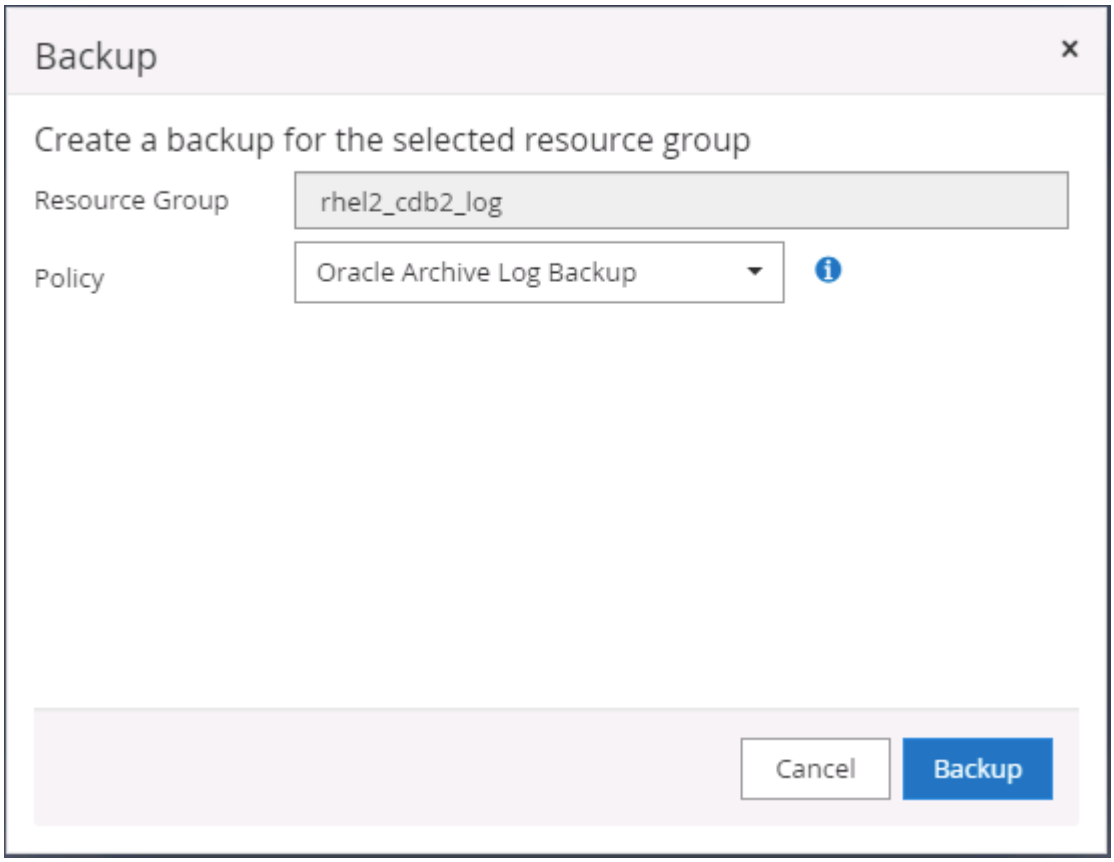


2. Accedere a SnapCenter come ID utente per la gestione del database per Oracle. Accedere alla scheda risorse, che mostra i database Oracle protetti da SnapCenter.



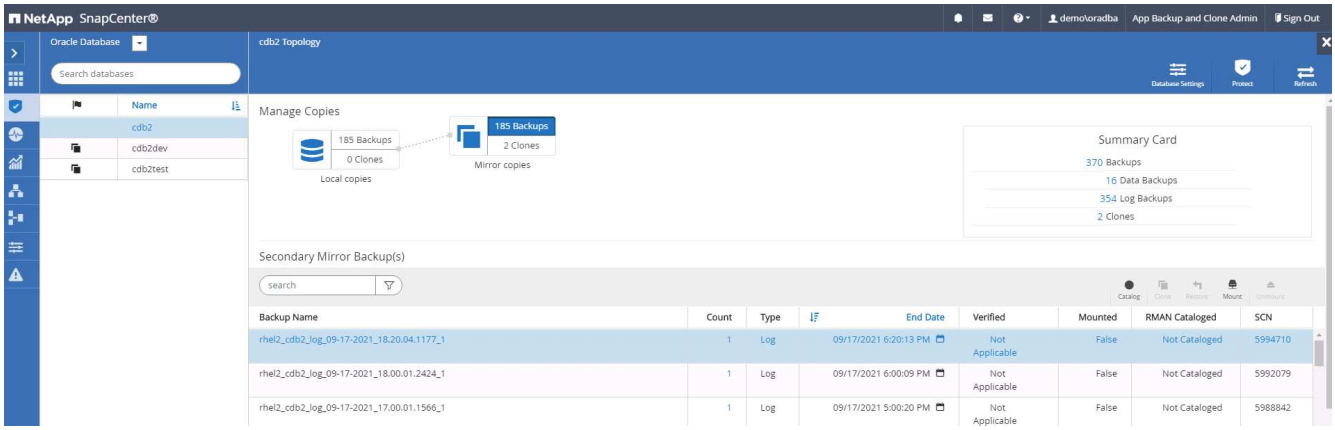
3. Selezionare il gruppo di risorse del registro Oracle e fare clic su Backup Now (Esegui backup ora) per eseguire manualmente un backup del registro Oracle per scaricare l'ultima transazione verso la destinazione nel cloud. In un vero scenario di DR, l'ultima transazione ripristinabile dipende dalla frequenza di replica del volume del log del database nel cloud, che a sua volta dipende dalla policy RTO o RPO dell'azienda.

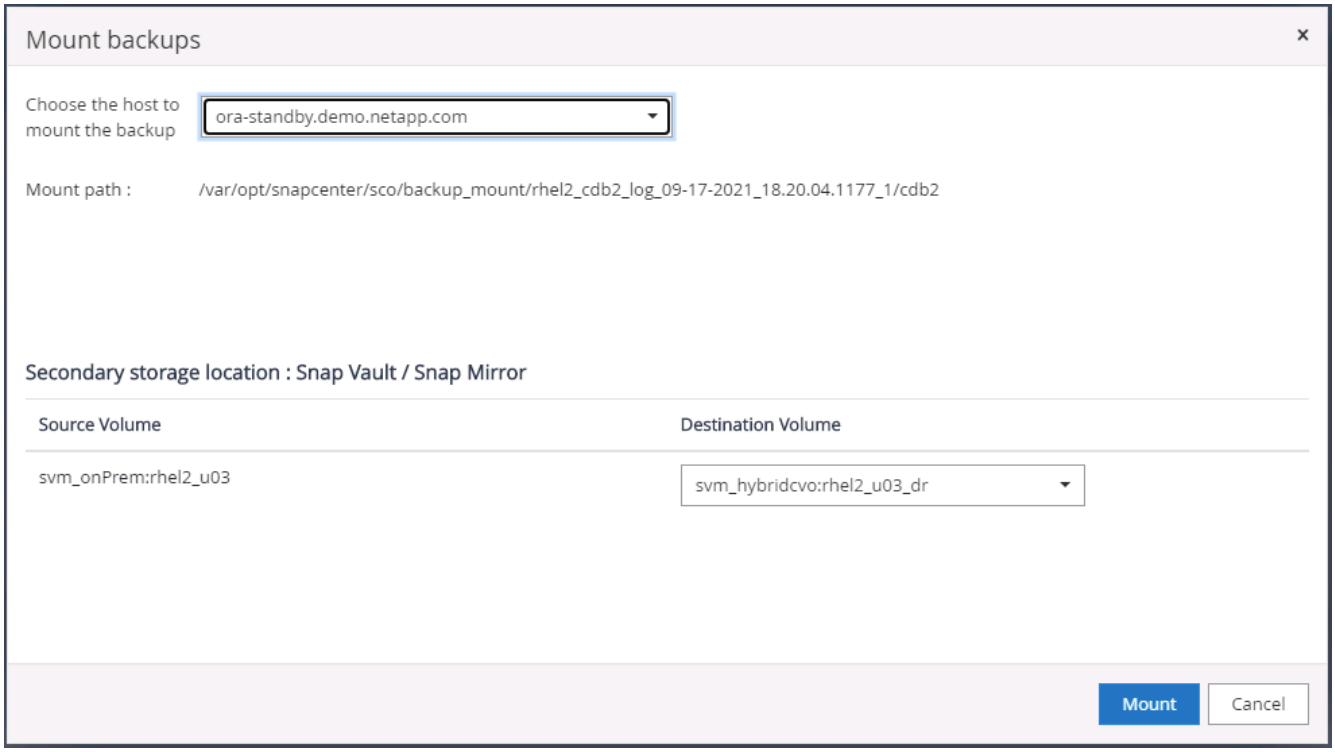




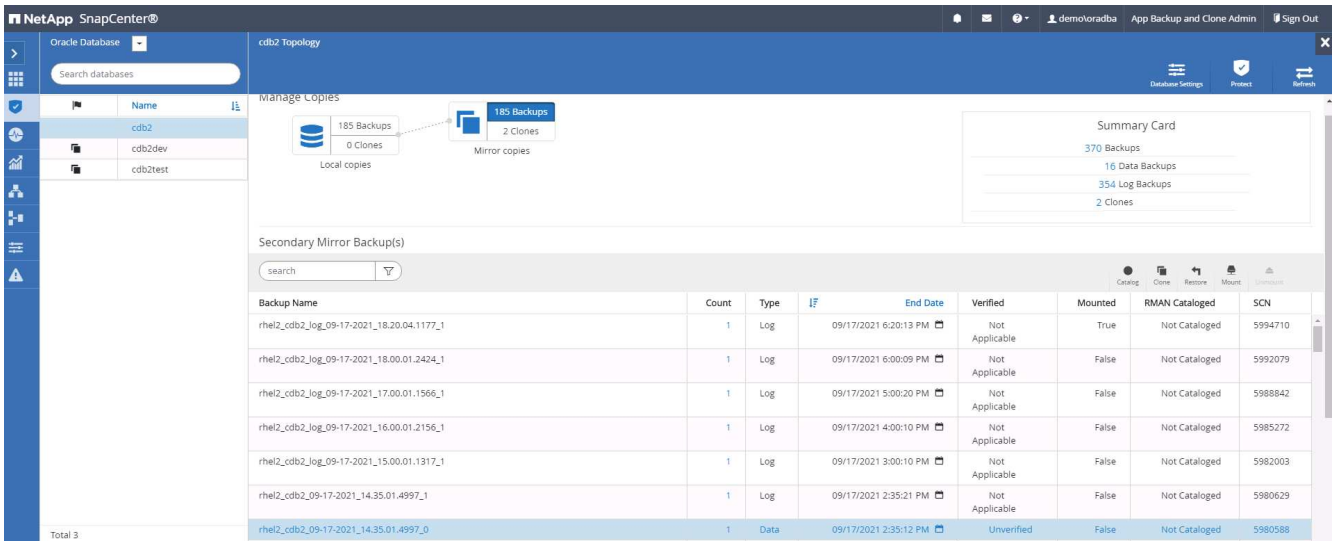
> SnapMirror asincrono perde i dati che non l'hanno fatto alla destinazione cloud nell'intervallo di backup del registro del database in uno scenario di disaster recovery. Per ridurre al minimo la perdita di dati, è possibile pianificare backup dei log più frequenti. Tuttavia, esiste un limite alla frequenza 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.

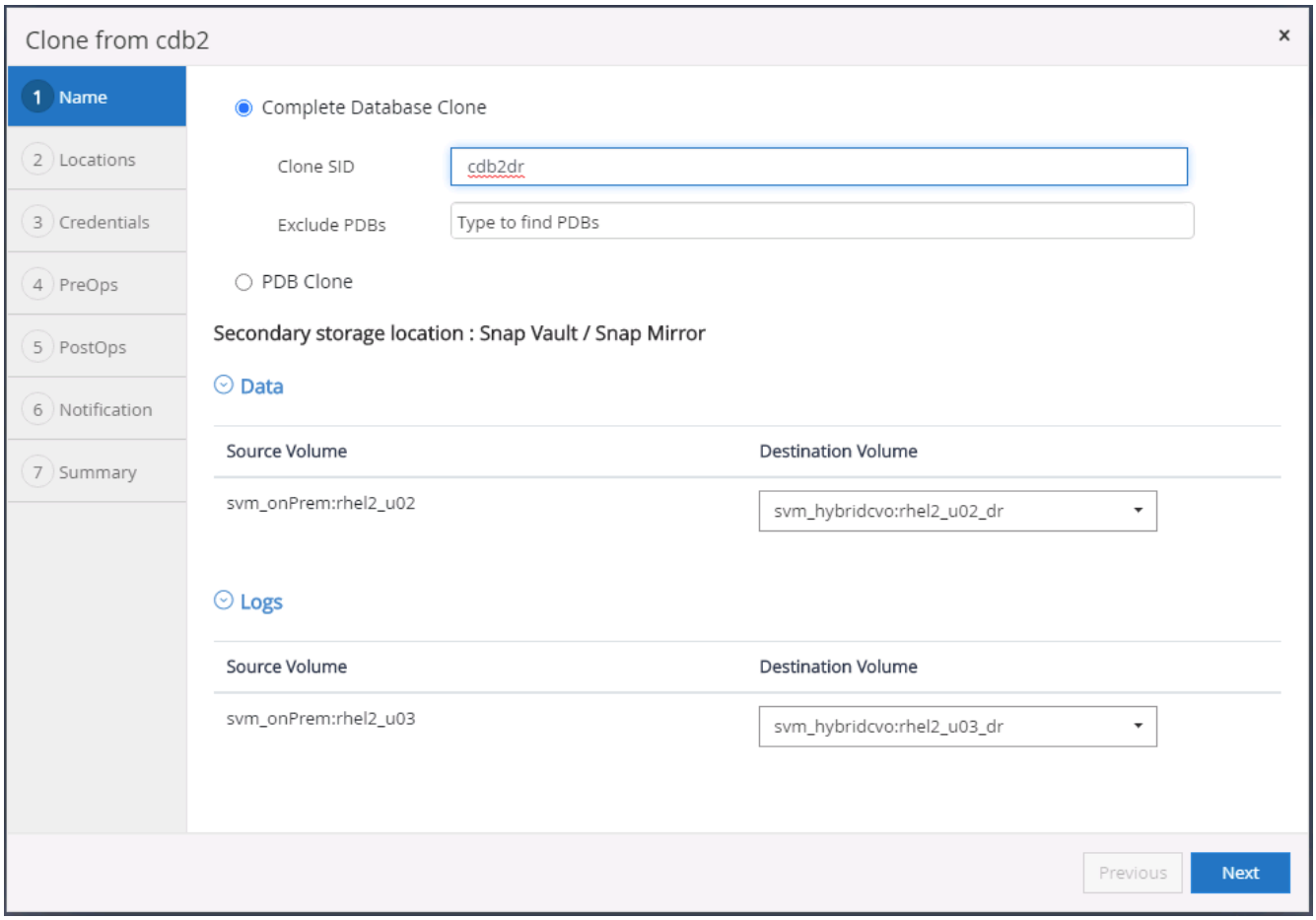




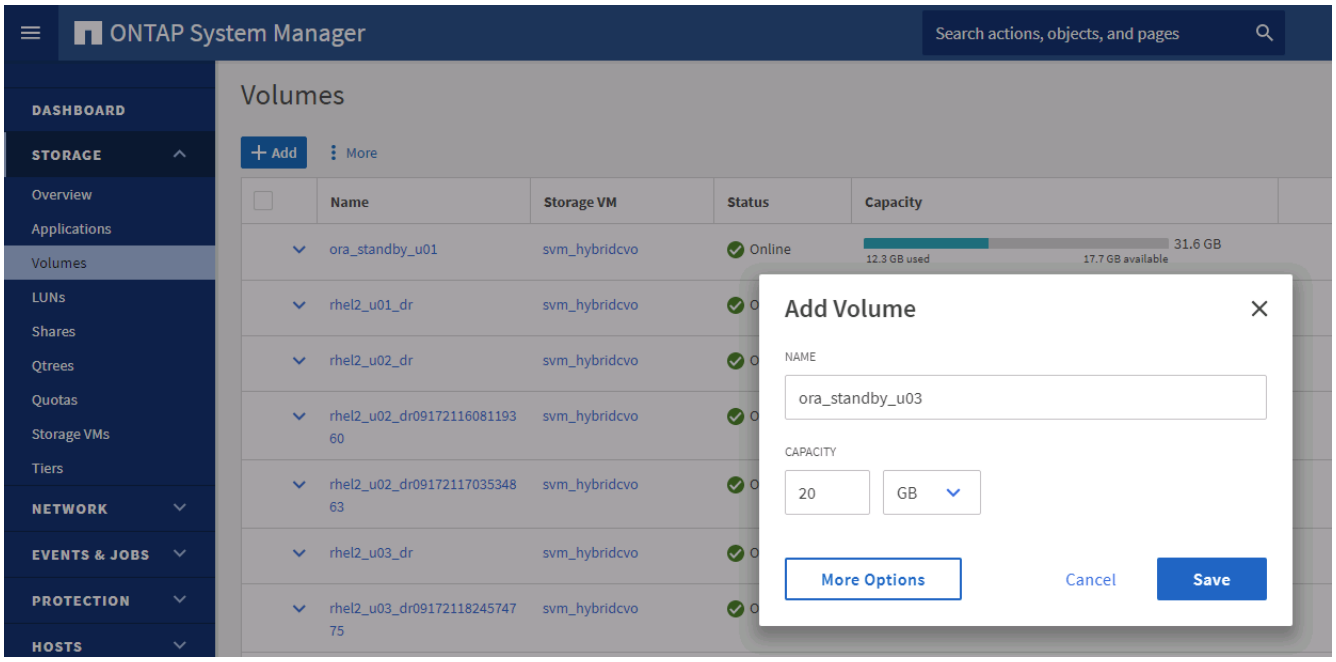
5. Selezionare l'ultimo backup completo del database e fare clic su Clone (Clona) per avviare il flusso di lavoro dei cloni.

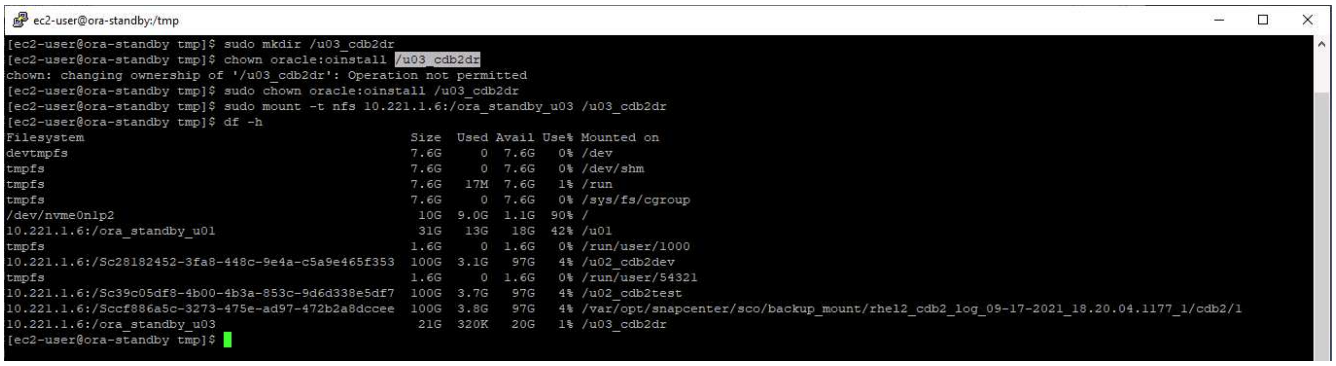


6. Selezionare un ID DB clone univoco sull'host.



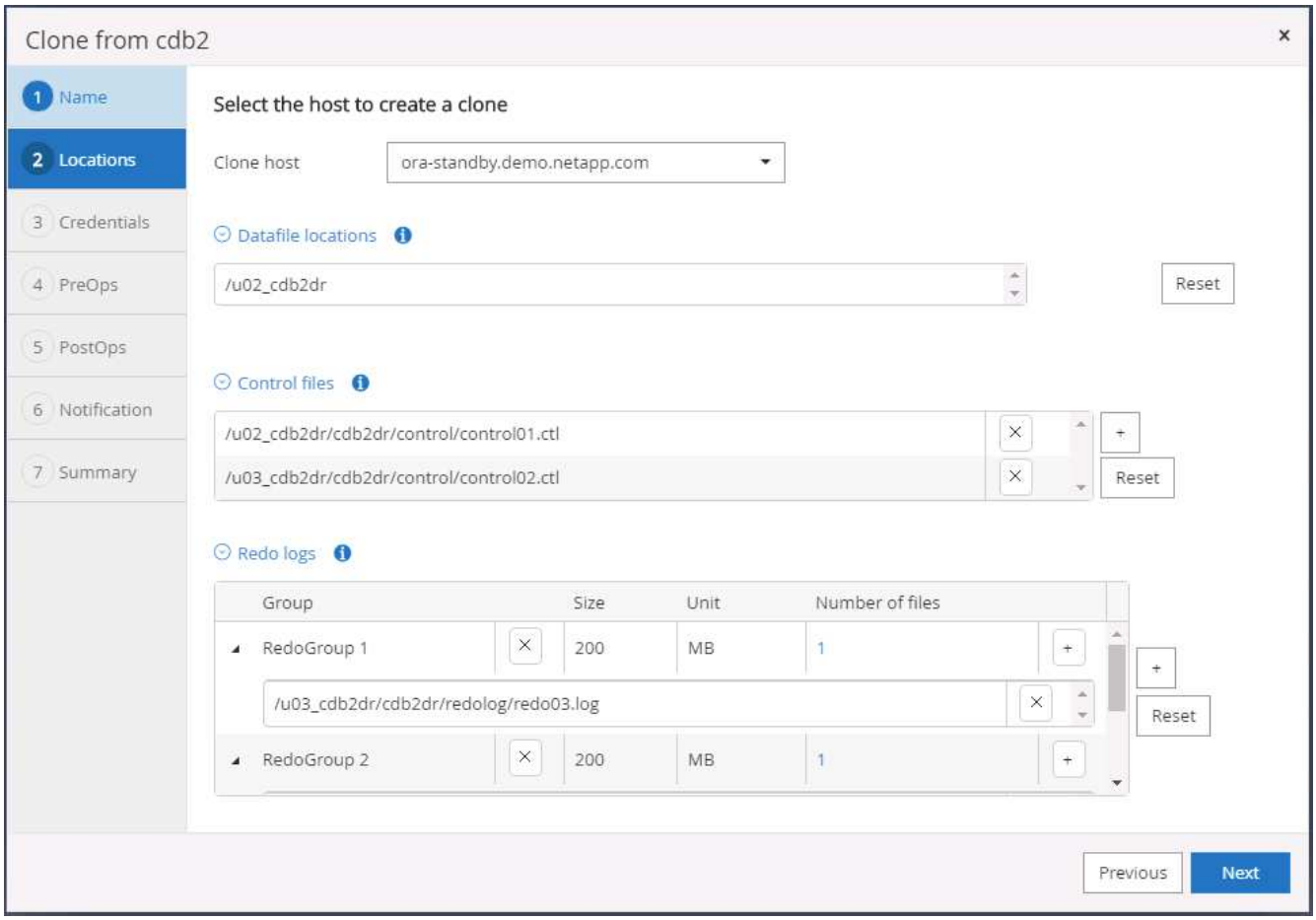
7. Eseguire il provisioning di un volume di log e montarlo sul server DR di destinazione per l'area di ripristino flash Oracle e i registri online.



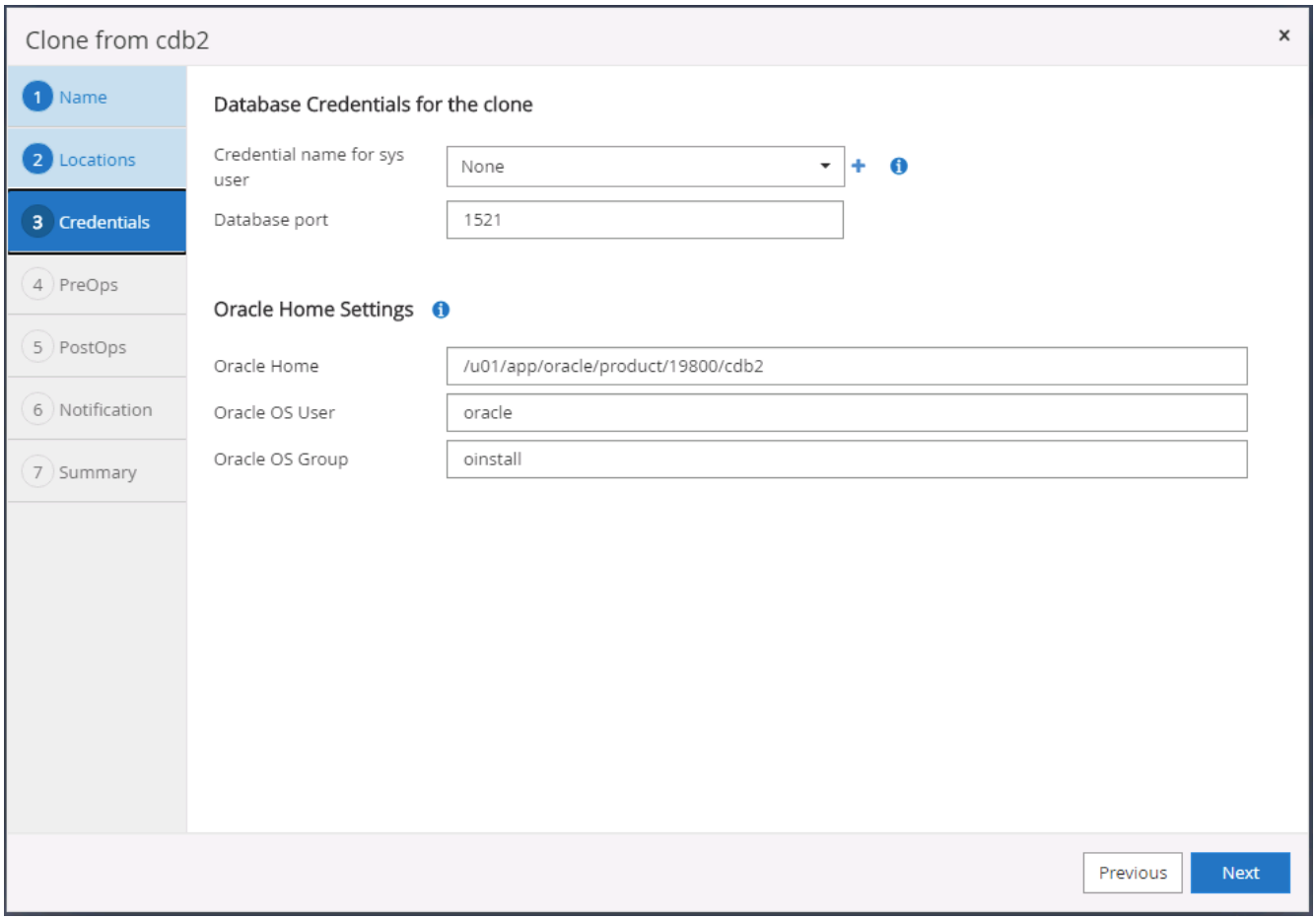


La procedura di clonazione Oracle non crea un volume di log, che deve essere fornito sul server DR prima della clonazione.

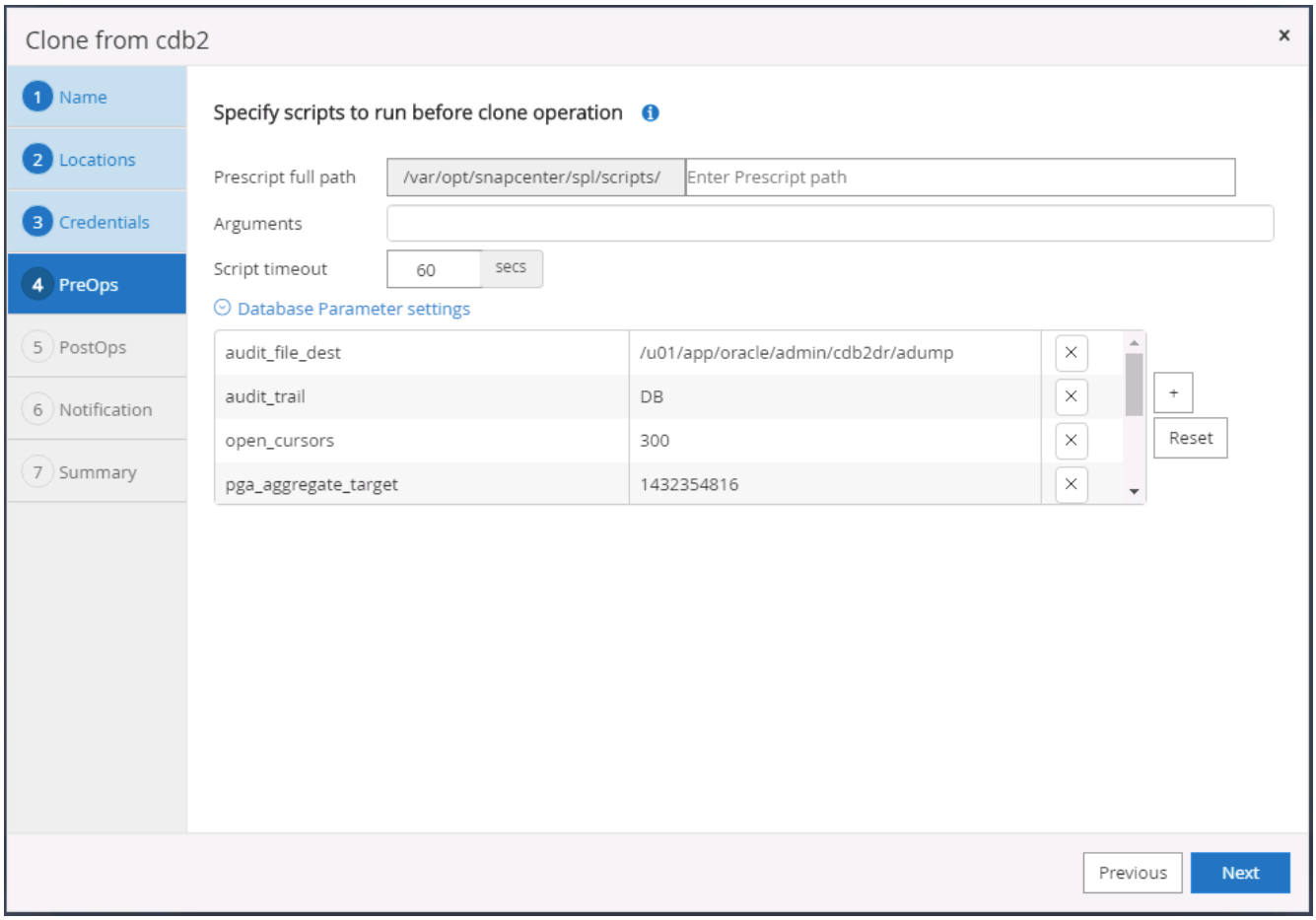
8. Selezionare l'host clone di destinazione e la posizione in cui inserire i file di dati, i file di controllo e i log di ripristino.



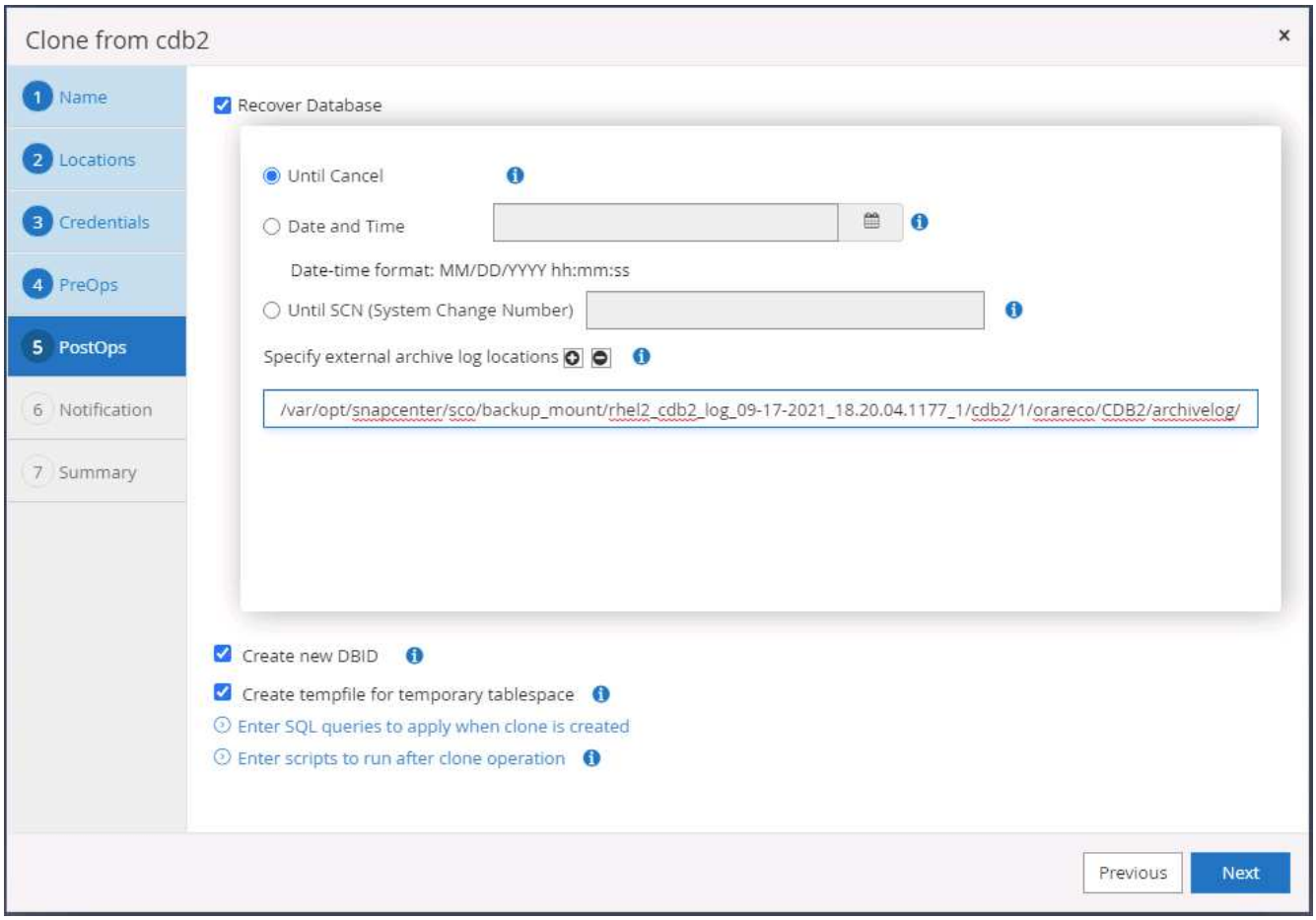
9. Selezionare le credenziali per il clone. Inserire i dettagli della configurazione Oracle home sul server di destinazione.



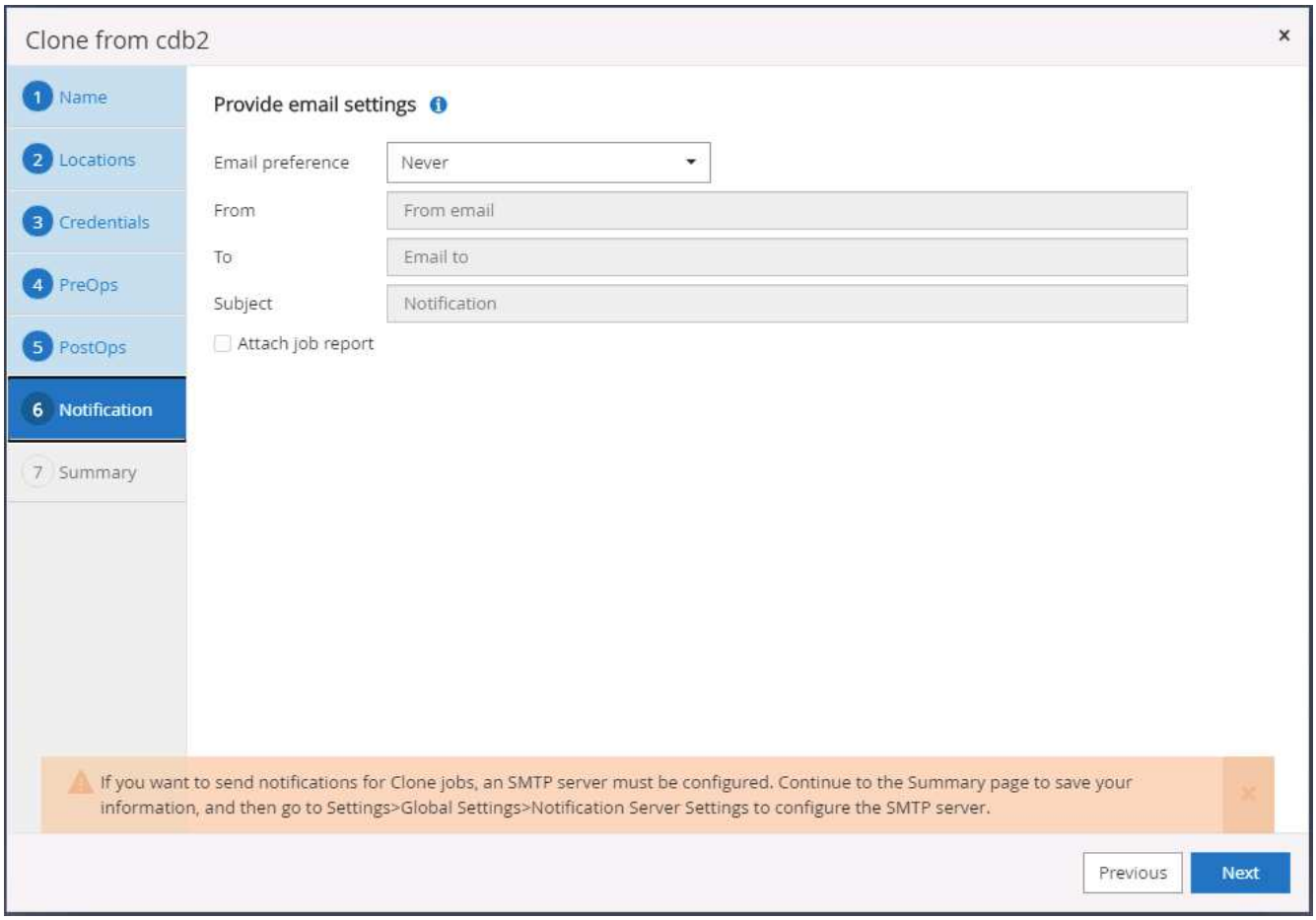
10. Specificare gli script da eseguire prima della clonazione. Se necessario, è possibile regolare i parametri del database.



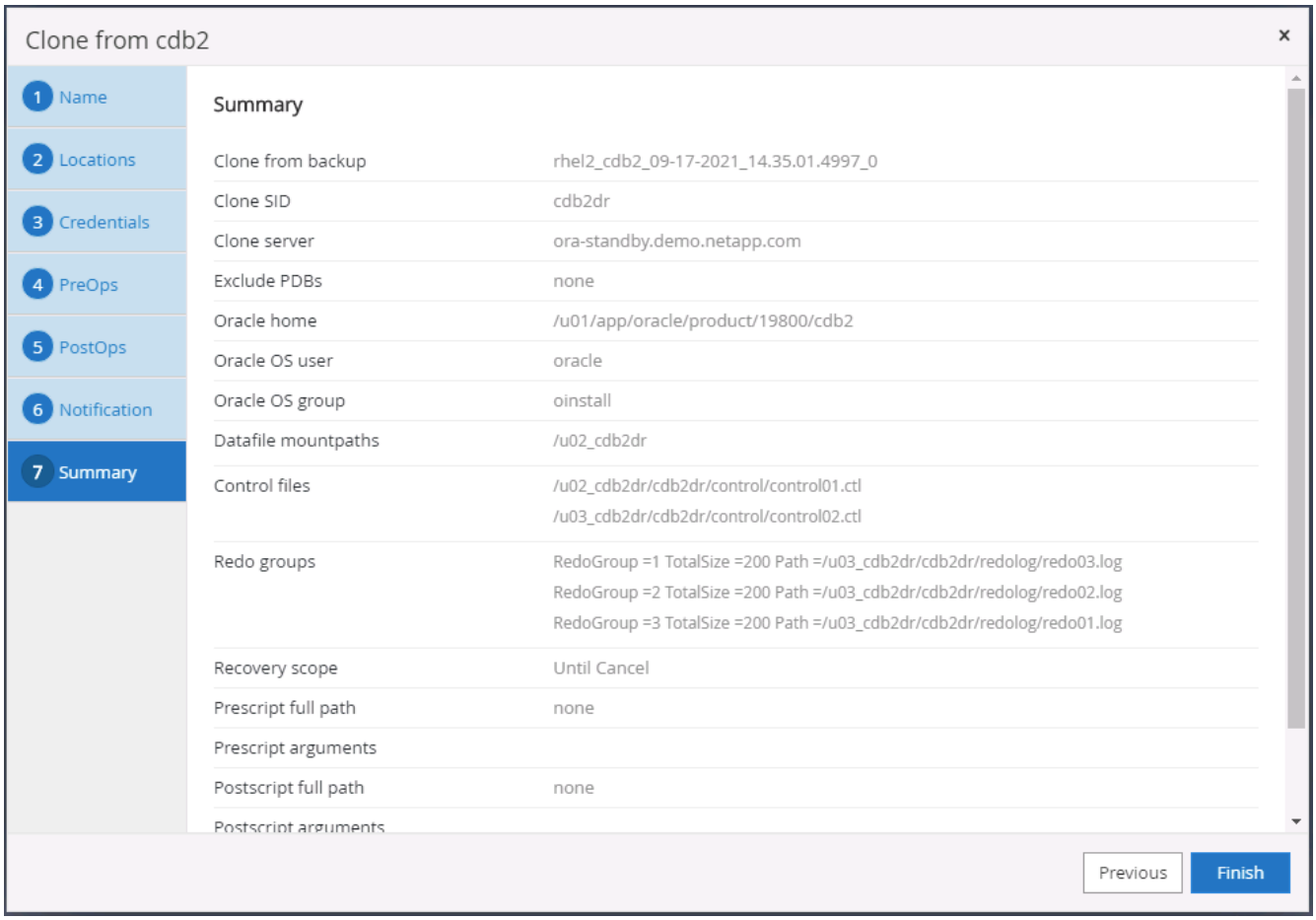
11. Selezionare l'opzione di ripristino fino a quando non viene eseguita l'opzione Cancel (Annulla), in modo che il ripristino venga eseguito attraverso tutti i log di archivio disponibili per recuperare l'ultima transazione replicata nella posizione del cloud secondario.



12. Configurare il server SMTP per la notifica via email, se necessario.



13. Riepilogo dei cloni DR.



14. I DBS clonati vengono registrati con SnapCenter subito dopo il completamento del clone e sono quindi disponibili per la protezione del backup.

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 dbs]$ 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
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.

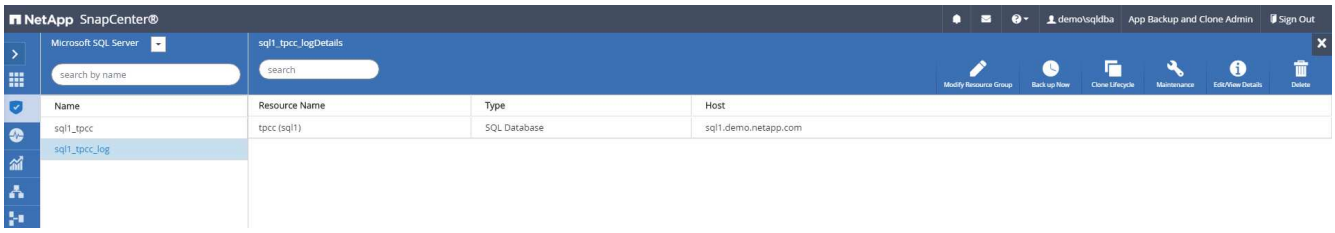
> La suddivisione dei cloni può comportare un utilizzo temporaneo dello spazio di storage molto più elevato del normale funzionamento. Tuttavia, dopo la ricostruzione del server DB on-premise, è possibile liberare spazio aggiuntivo.

Clonare un database di produzione SQL on-premise nel cloud per il DR

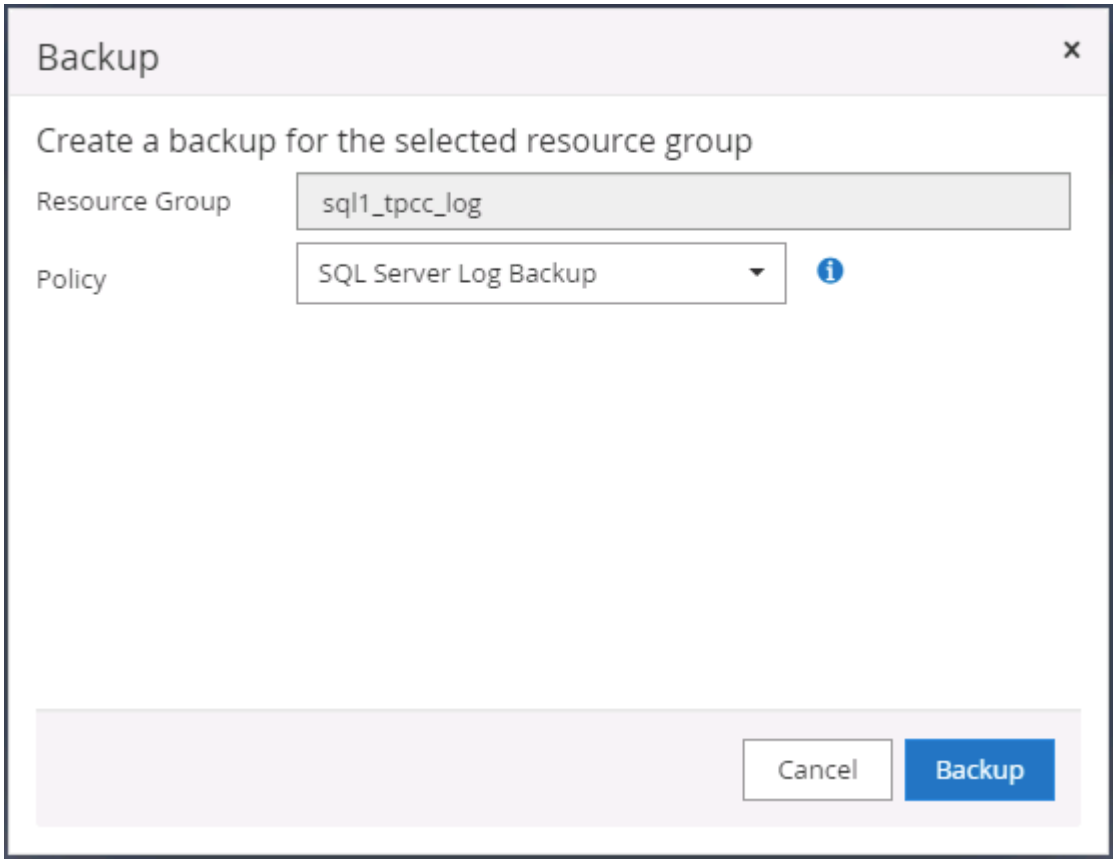
1. Allo stesso modo, per verificare che il ripristino del clone SQL sia stato eseguito attraverso l’ultimo log disponibile, abbiamo creato una piccola tabella di test e inserito una riga. I dati del test vengono ripristinati dopo un ripristino completo dell’ultimo registro disponibile.

```
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>
```

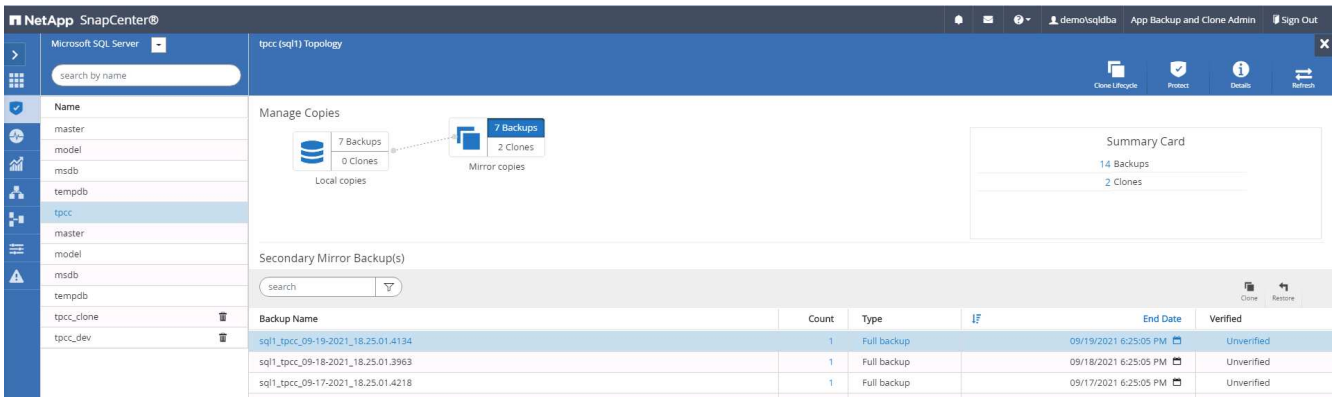
2. Accedere a SnapCenter con un ID utente per la gestione del database per SQL Server. Accedere alla scheda Resources (risorse), che mostra il gruppo di risorse di protezione di SQL Server.



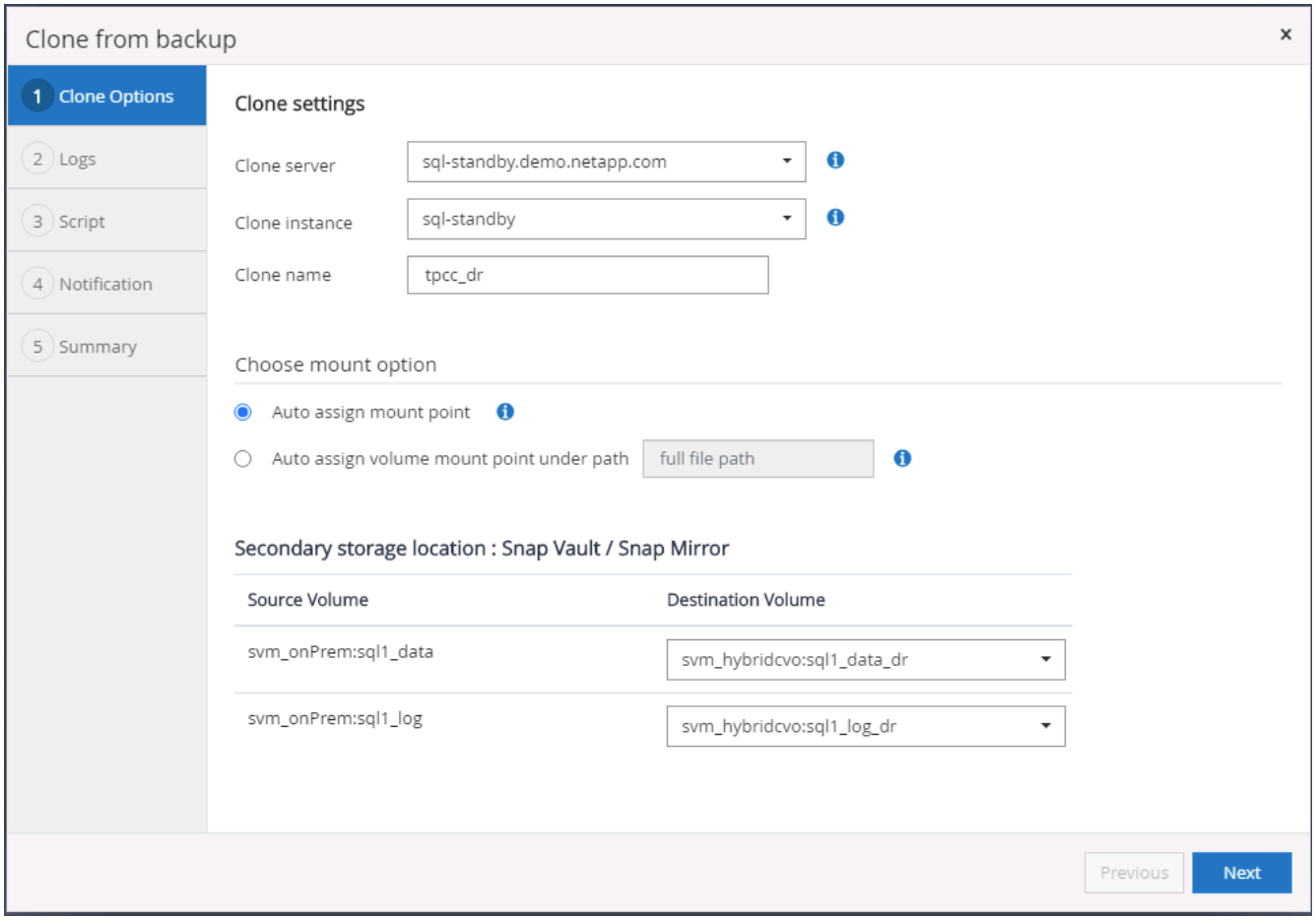
3. Eseguire manualmente un backup del log per svuotare l'ultima transazione da replicare sullo storage secondario nel cloud pubblico.



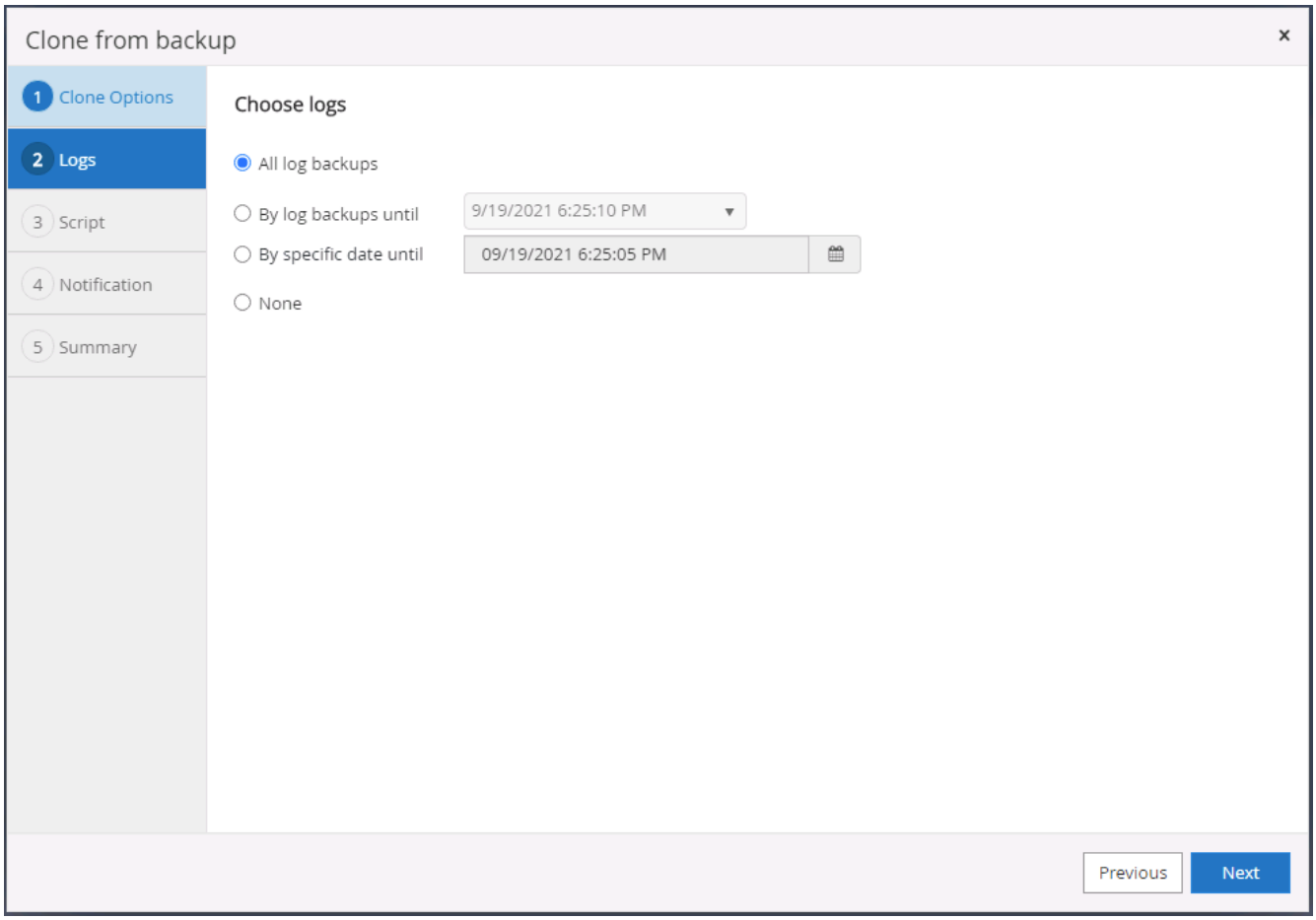
4. Selezionare l'ultimo backup completo di SQL Server per il clone.



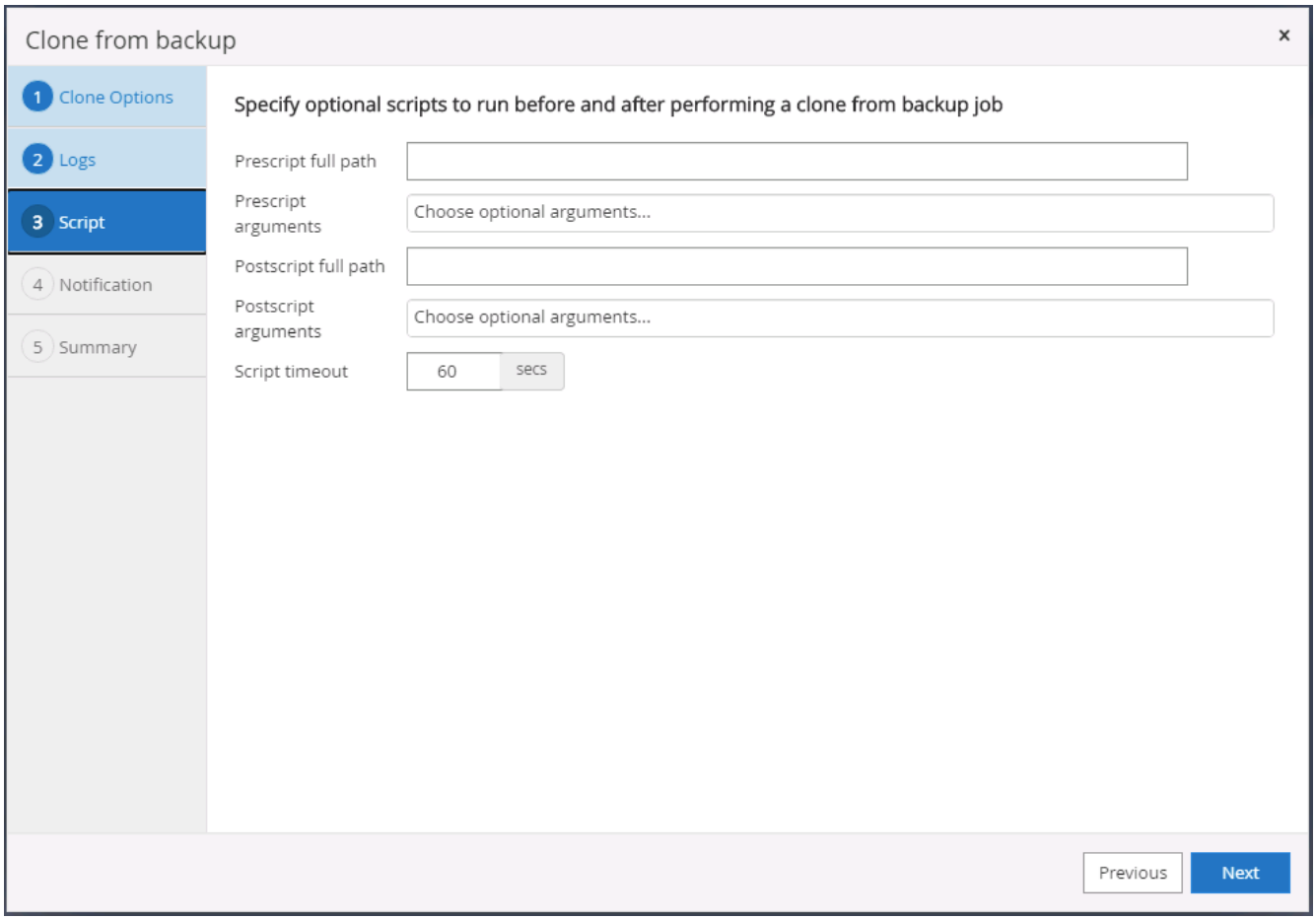
5. Impostare l'impostazione del clone, ad esempio Clone Server, Clone Instance, Clone Name e mount. Il percorso di storage secondario in cui viene eseguita la clonazione viene popolato automaticamente.



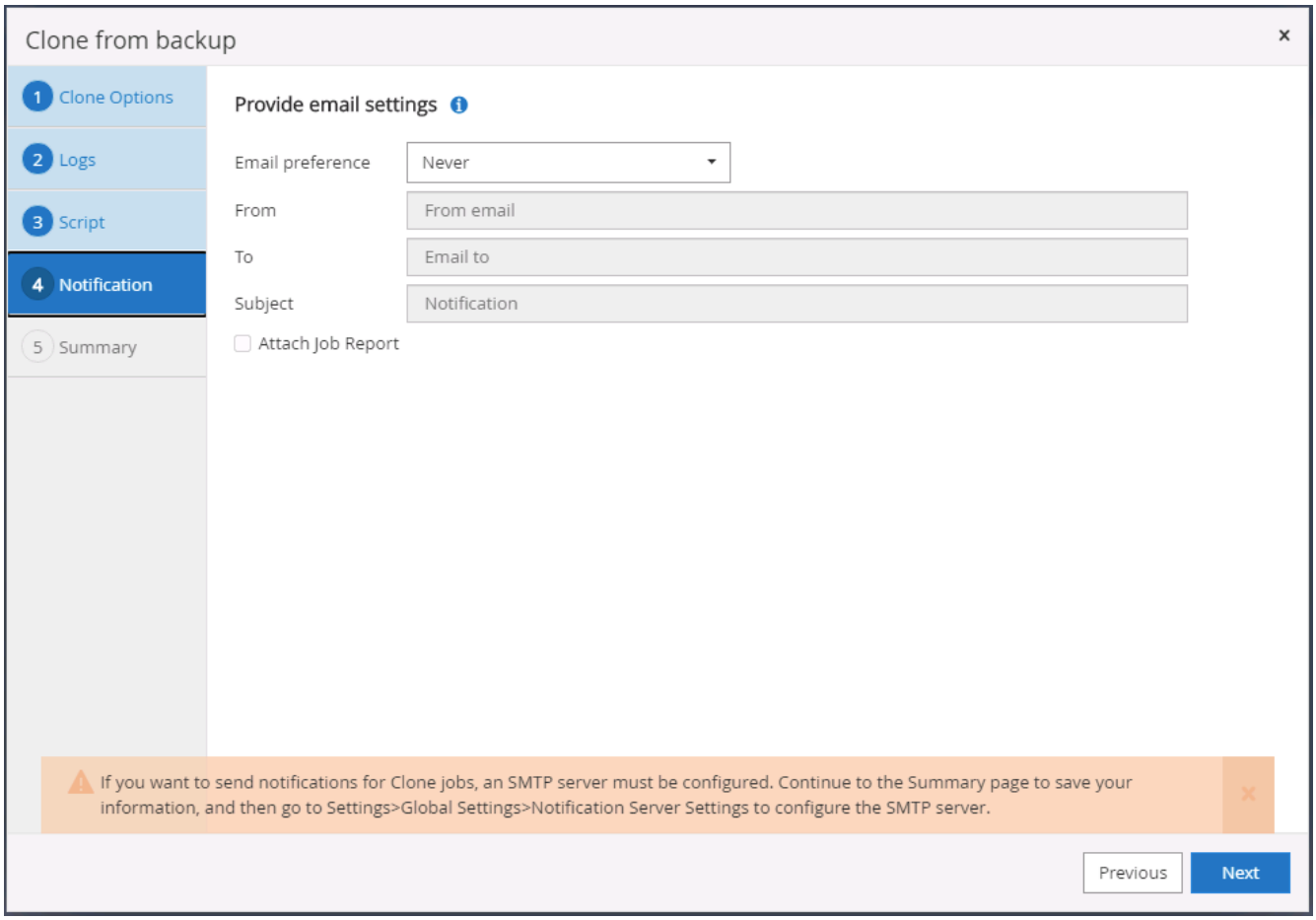
6. Selezionare tutti i backup del registro da applicare.



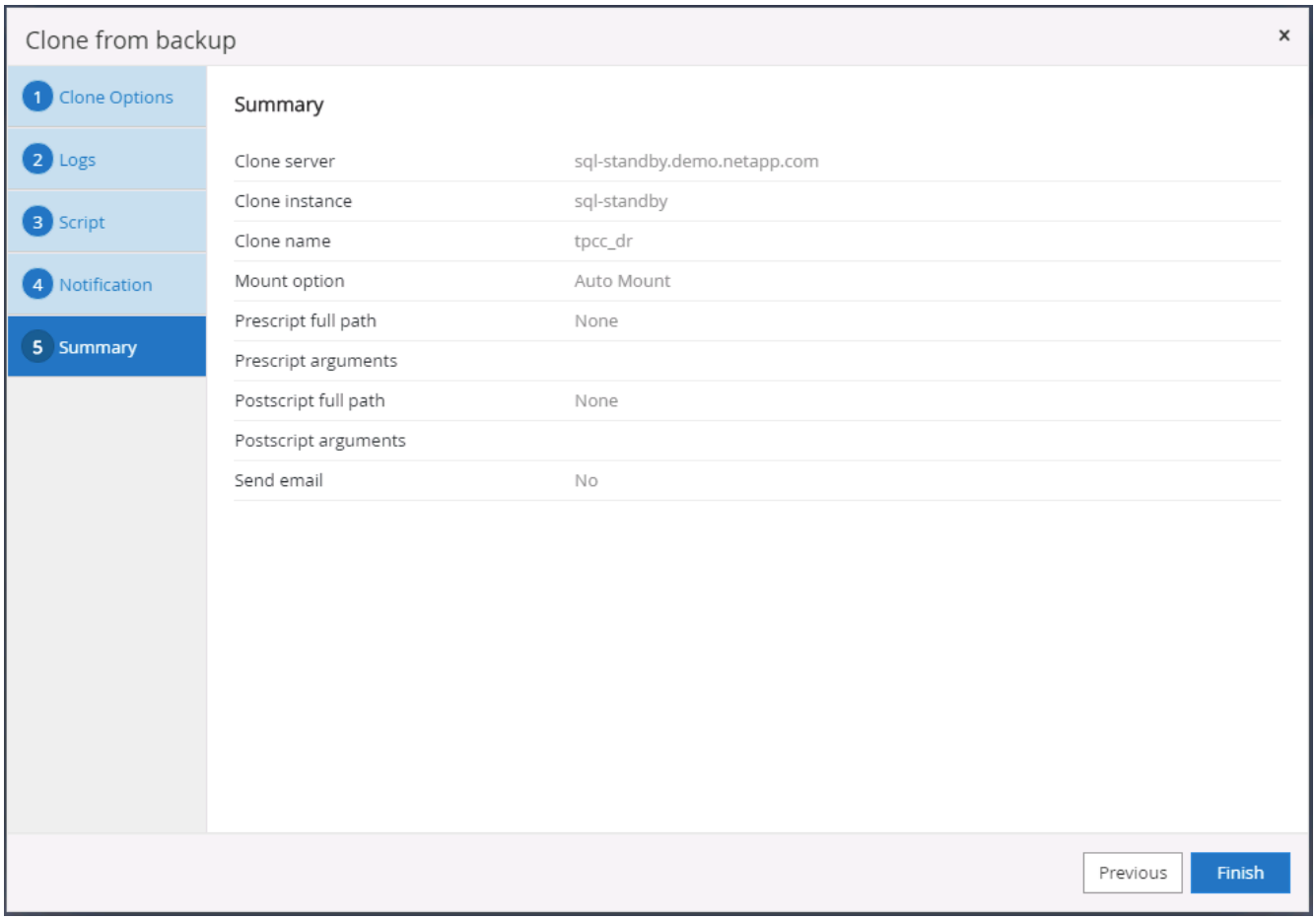
7. Specificare eventuali script opzionali da eseguire prima o dopo la clonazione.

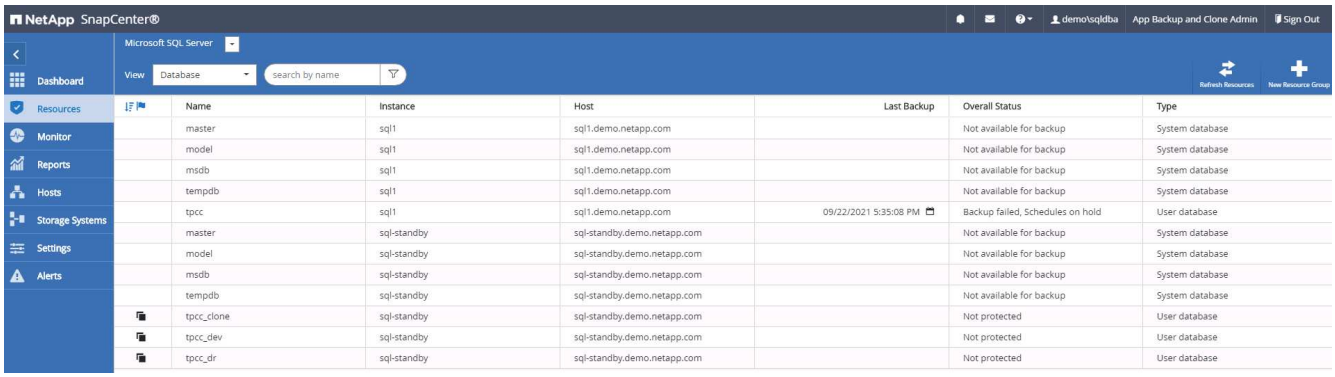


8. Specificare un server SMTP se si desidera inviare una notifica via e-mail.



9. Riepilogo dei cloni DR. I database clonati vengono immediatamente registrati con SnapCenter e sono disponibili per la protezione del backup.

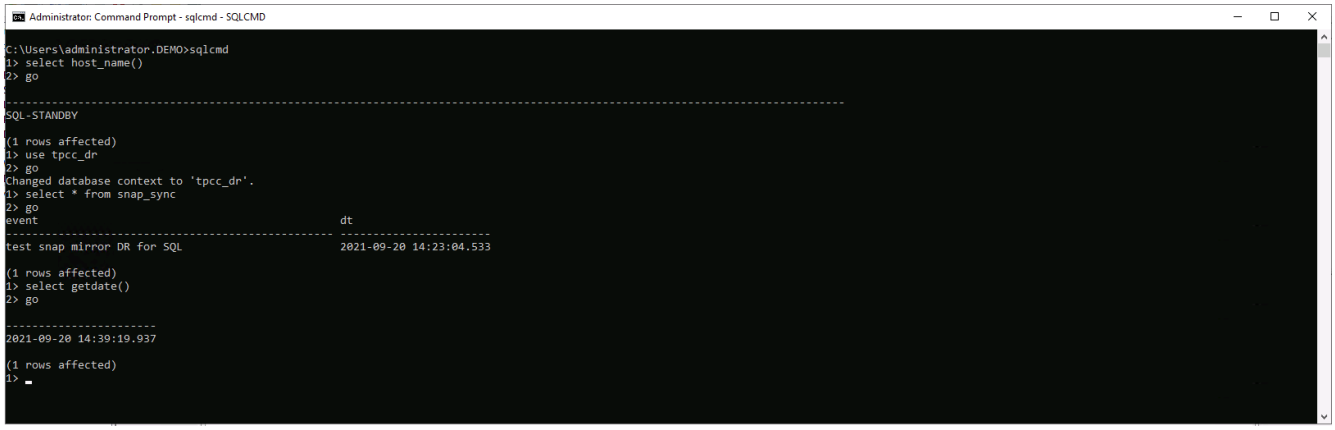




Convalida e configurazione dei cloni post-DR per SQL

1. Monitorare lo stato del lavoro clone.

2. Verificare che l’ultima transazione sia stata replicata e ripristinata con tutti i cloni dei file di log e il ripristino.



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.