Panoramica introduttiva

NetApp Solutions

NetApp
April 26, 2024

Sommario

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

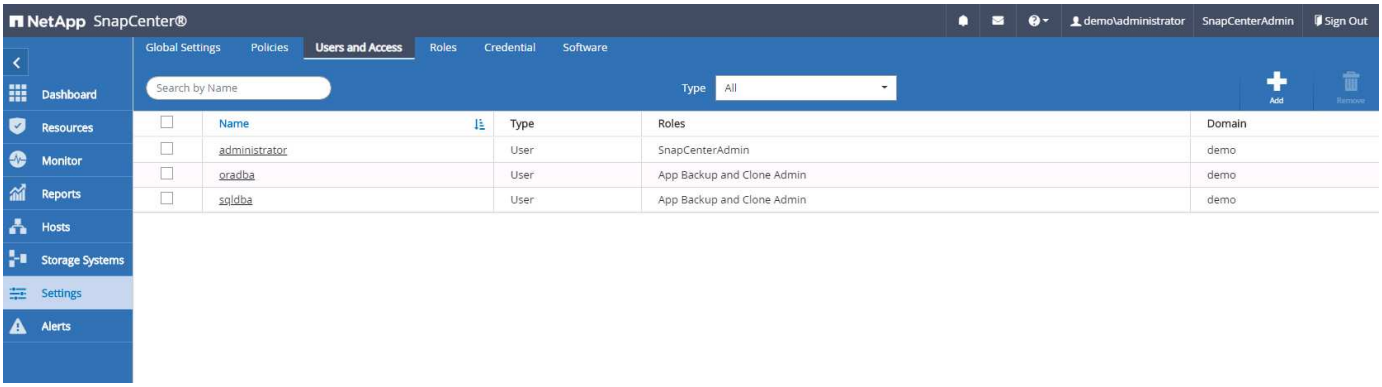
1. Configurare l'utente amministratore del database in SnapCenter

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.

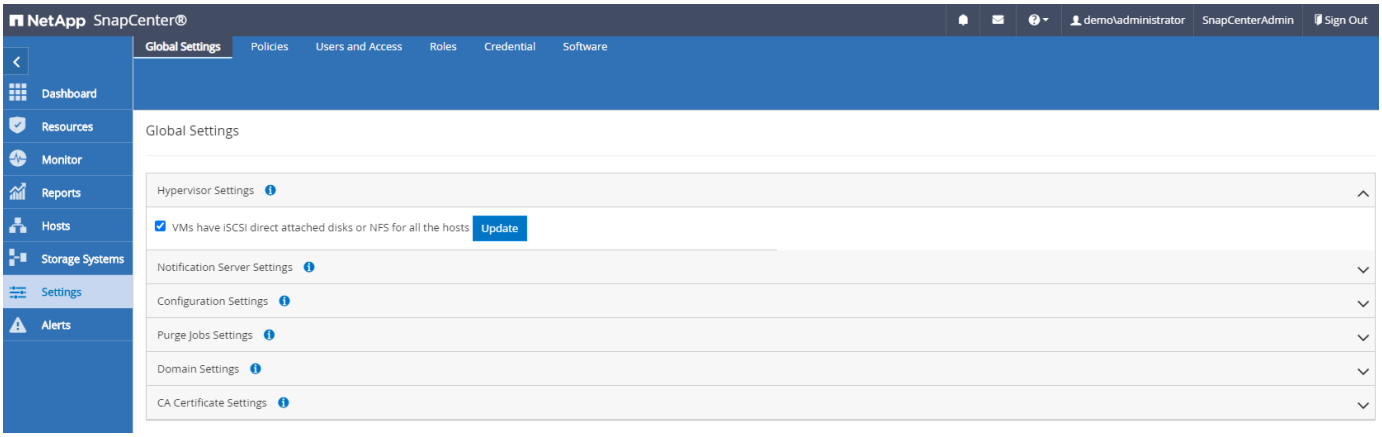
3. Installazione del plug-in host SnapCenter

> 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

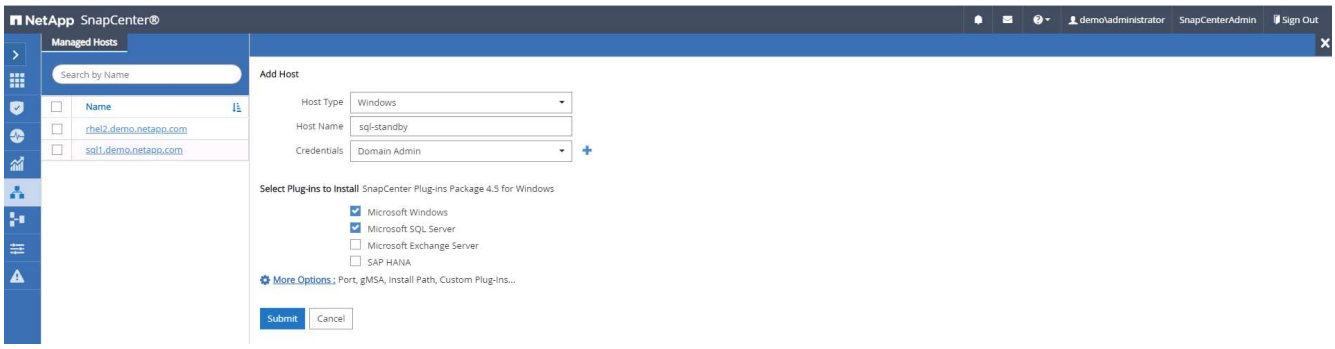
Accedere a Impostazioni > Impostazioni globali. Selezionare "VM con iSCSI direct attached disks o NFS per tutti gli host" in Impostazioni hypervisor e fare clic su Aggiorna.



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

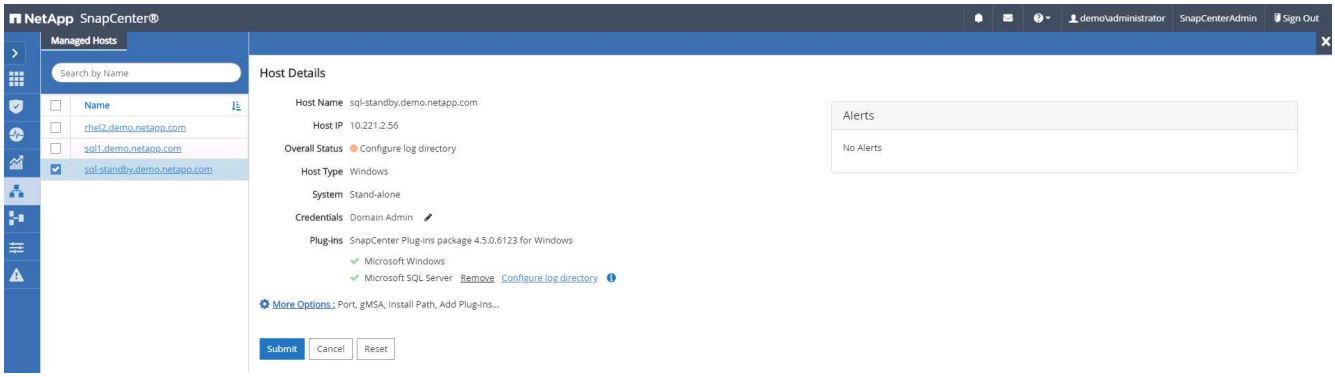
1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda host dal menu a sinistra, quindi fare clic su Add (Aggiungi) per aprire il flusso di lavoro Add host (Aggiungi host).

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.

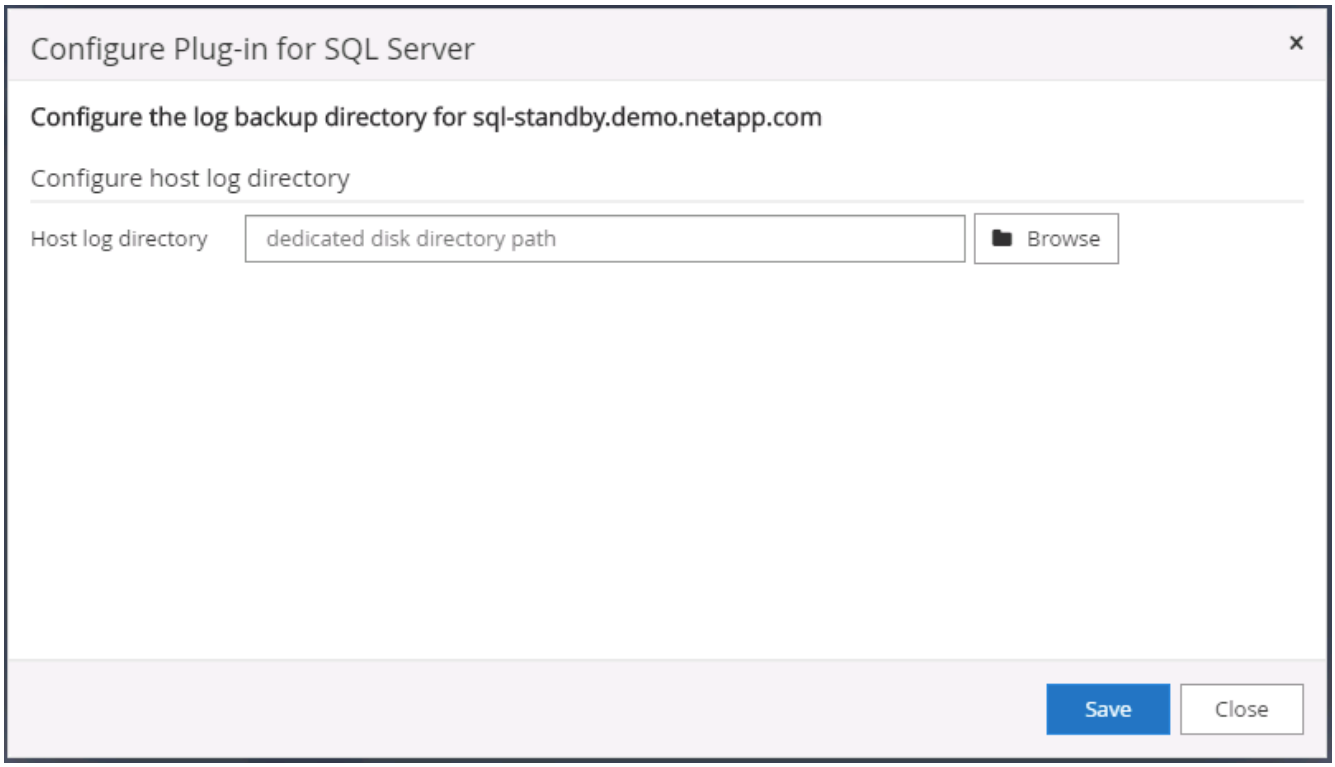


4. Una volta installato il plug-in su un host Windows, il relativo stato generale viene visualizzato come "Configure log directory" (Configura directory log).

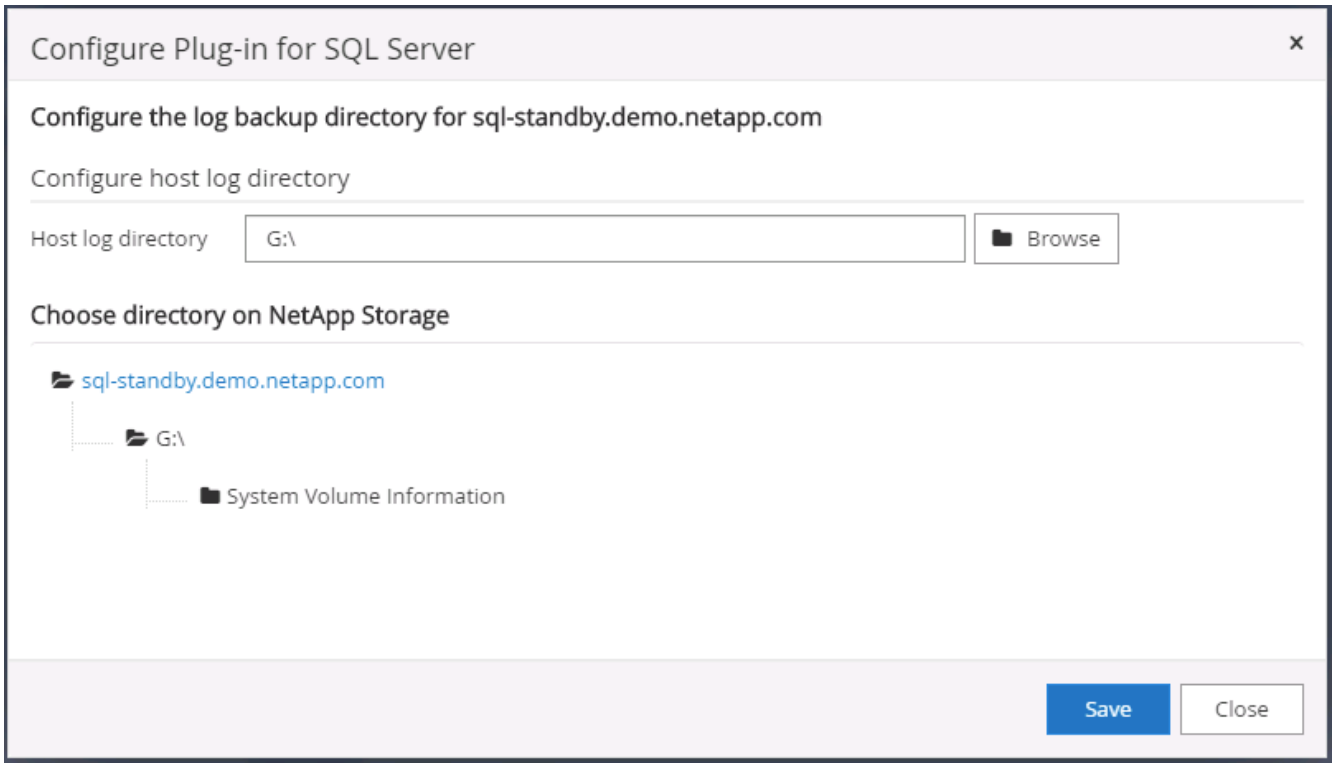
5. Fare clic su host Name (Nome host) per aprire la configurazione della directory di log di SQL Server.



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

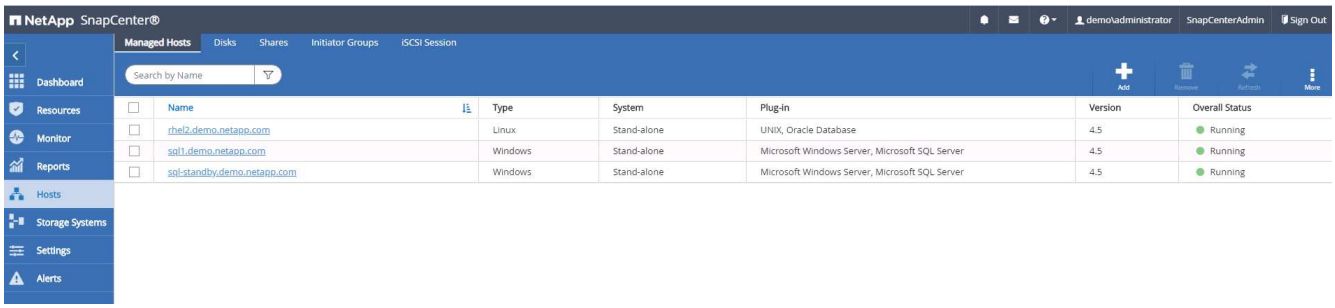


7. Fare clic su Browse (Sfoglia) per scoprire lo storage NetApp in modo da poter impostare una directory di log; SnapCenter utilizza questa directory di log per eseguire il rolloup dei file di log delle transazioni di SQL Server. Quindi fare clic su Save (Salva).

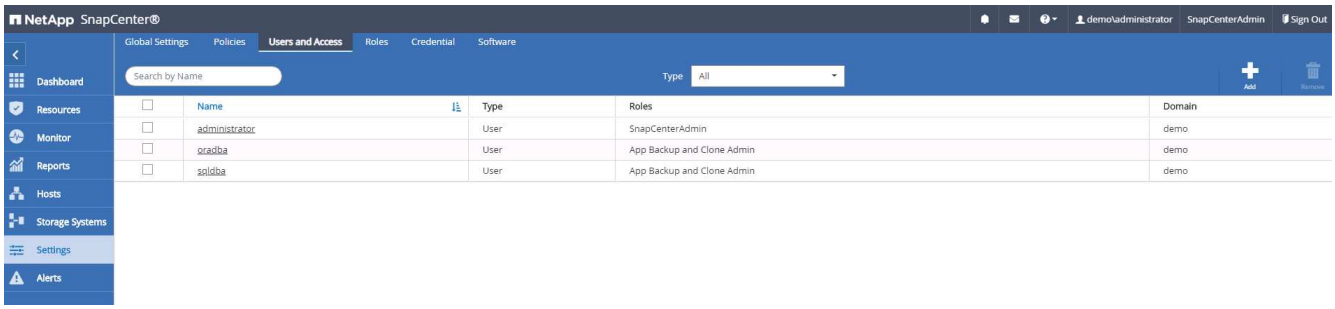


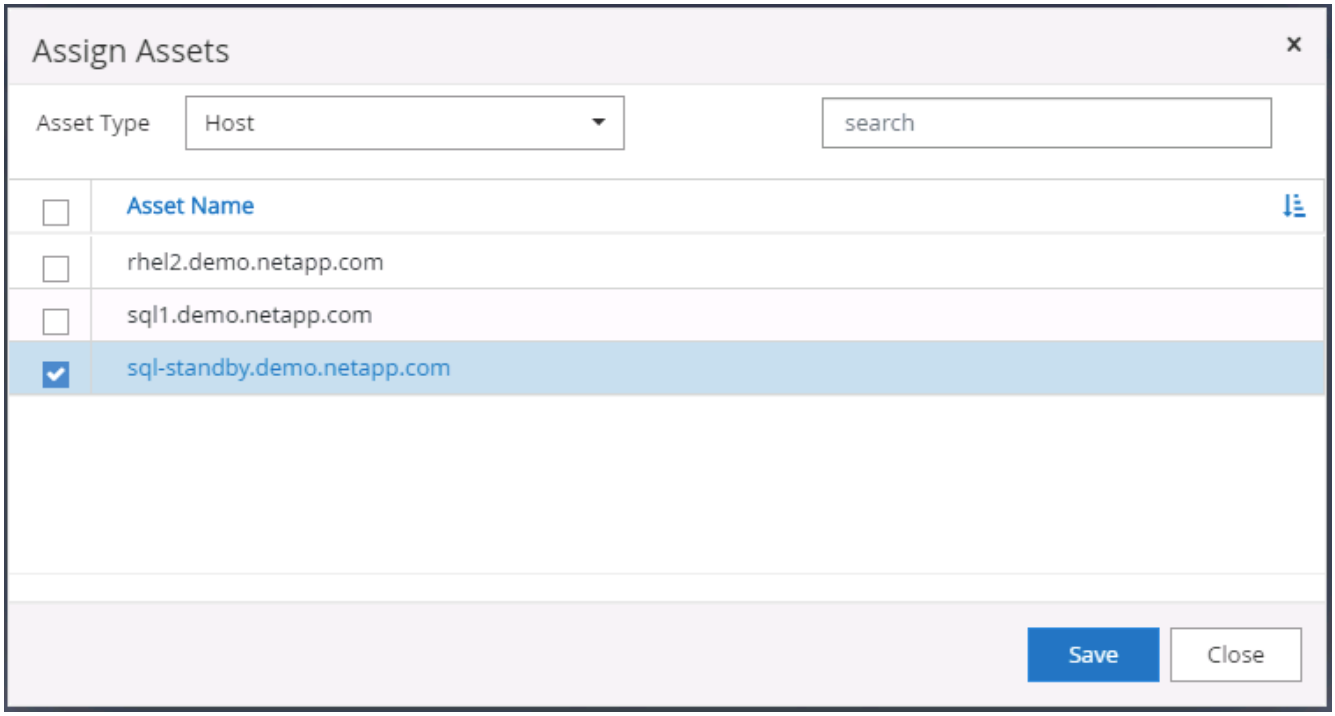
Affinché lo storage NetApp fornito a un host DB venga rilevato, lo storage (on-premise o CVO) deve essere aggiunto a SnapCenter, come illustrato nella fase 6 per CVO come esempio.

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.



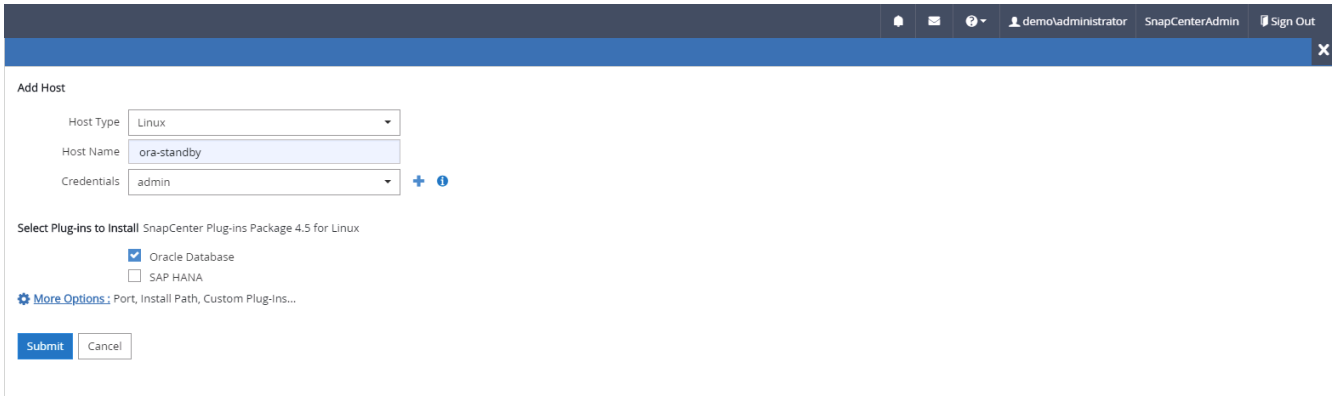


Aggiungere l'host Unix e l'installazione del plug-in sull'host

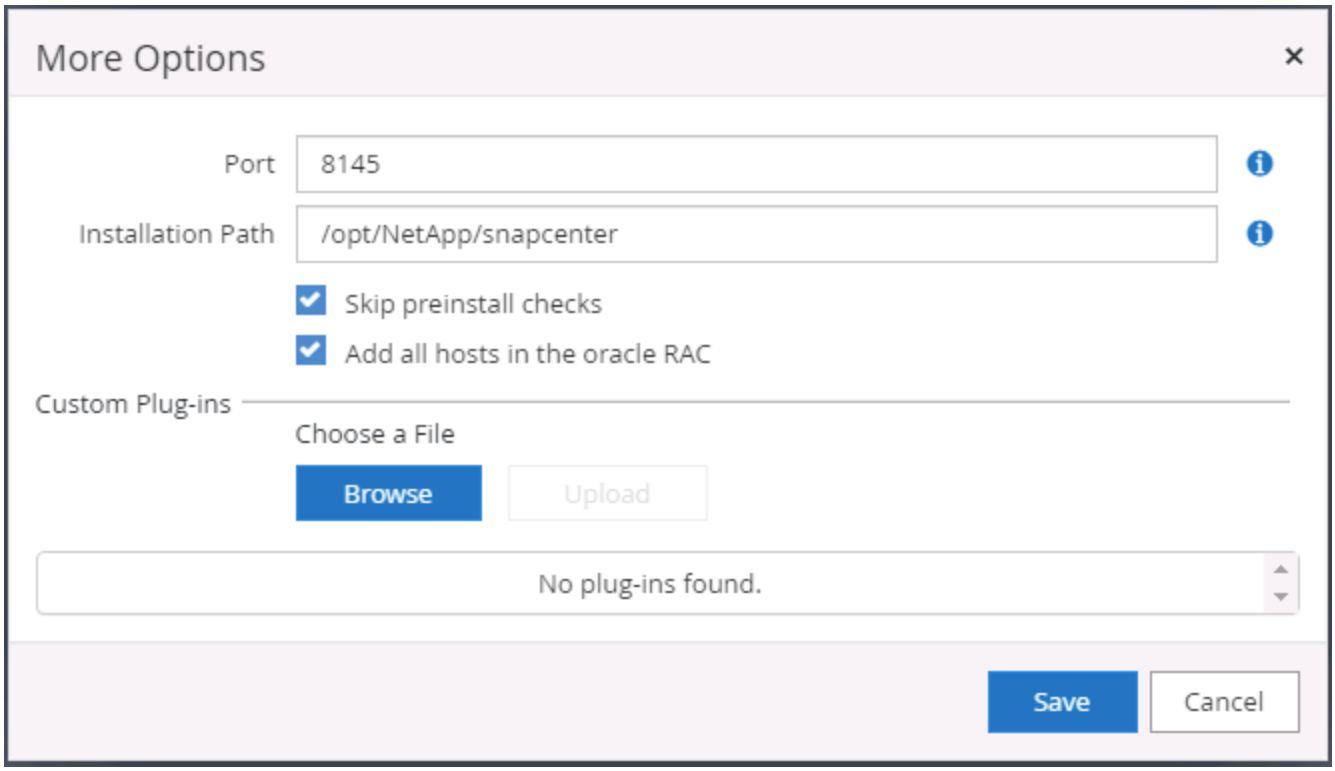
1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda host dal menu a sinistra, quindi fare clic su Add (Aggiungi) per aprire il flusso di

lavoro Add host (Aggiungi host).

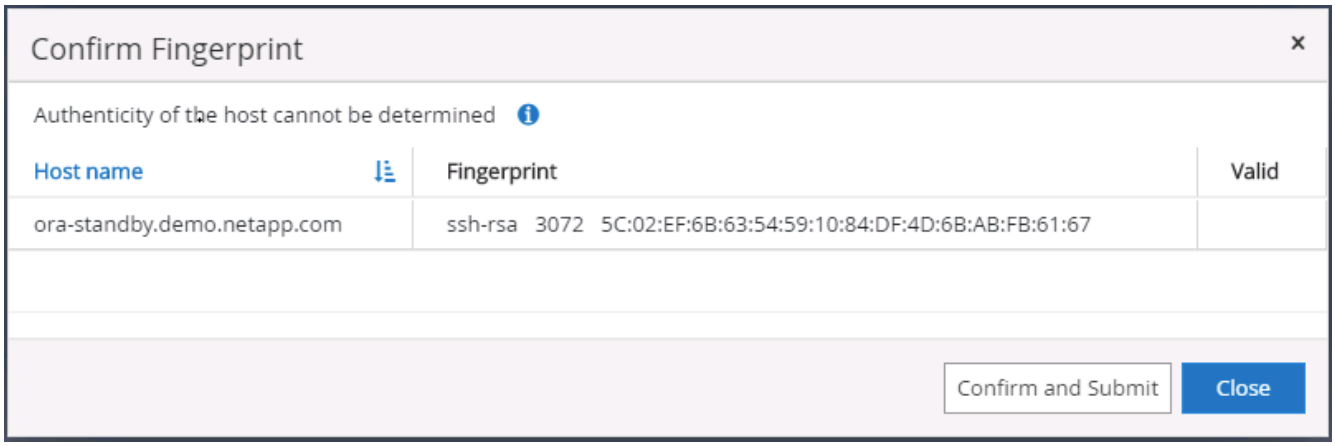
3. Scegliere Linux come tipo di host. Il nome host può essere il nome host o un indirizzo IP. Tuttavia, il nome host deve essere risolto per correggere l'indirizzo IP host dall'host SnapCenter. Scegliere le credenziali host create nel passaggio 2. Le credenziali host richiedono privilegi sudo. Selezionare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



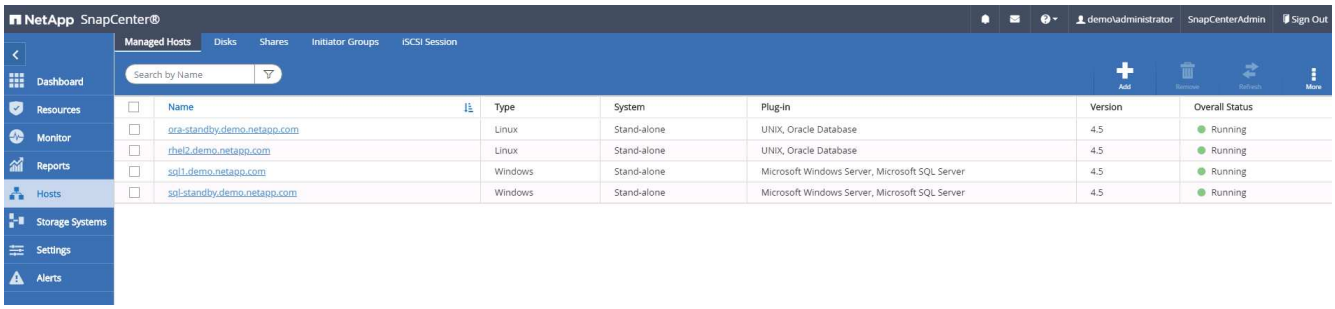
4. Fare clic su altre opzioni e selezionare "Ignora controlli di preinstallazione". Viene richiesto di confermare l'omissione del controllo di preinstallazione. Fare clic su Sì, quindi su Salva.



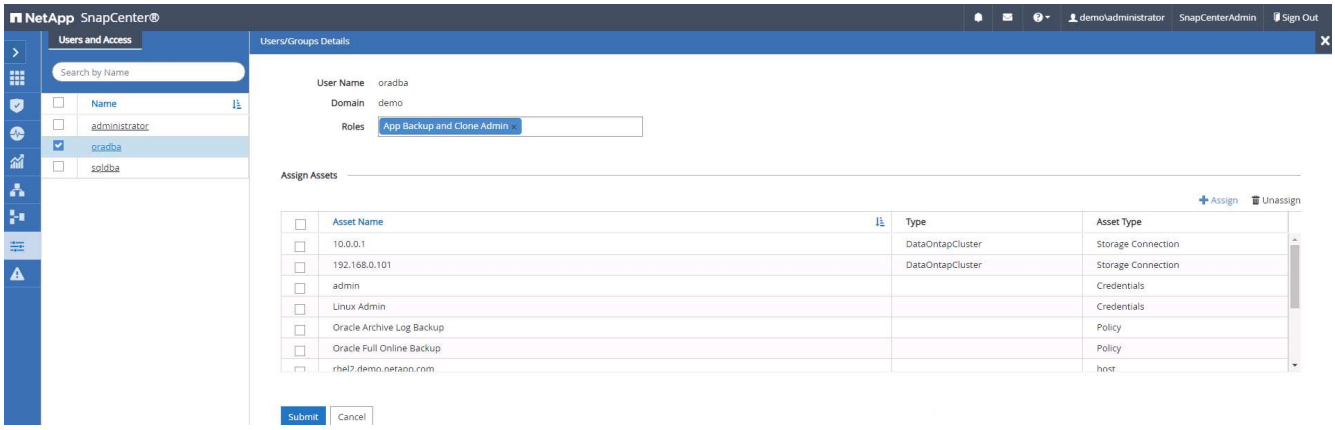
5. Fare clic su Submit (Invia) per avviare l'installazione del plug-in. Viene richiesto di confermare l'impronta digitale come mostrato di seguito.

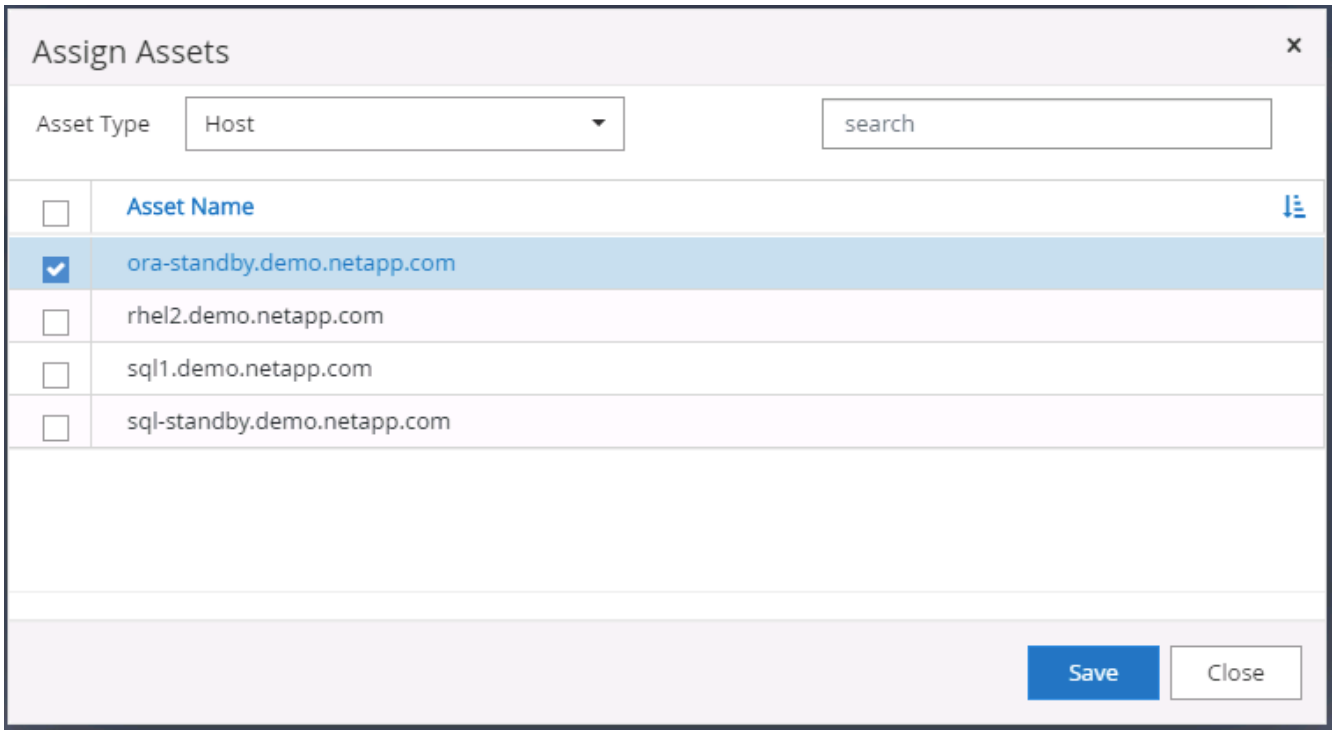


6. SnapCenter esegue la convalida e la registrazione dell'host, quindi il plug-in viene installato sull'host Linux. Lo stato cambia da Installing Plugin (Installazione del plug-in) a running (in esecuzione)



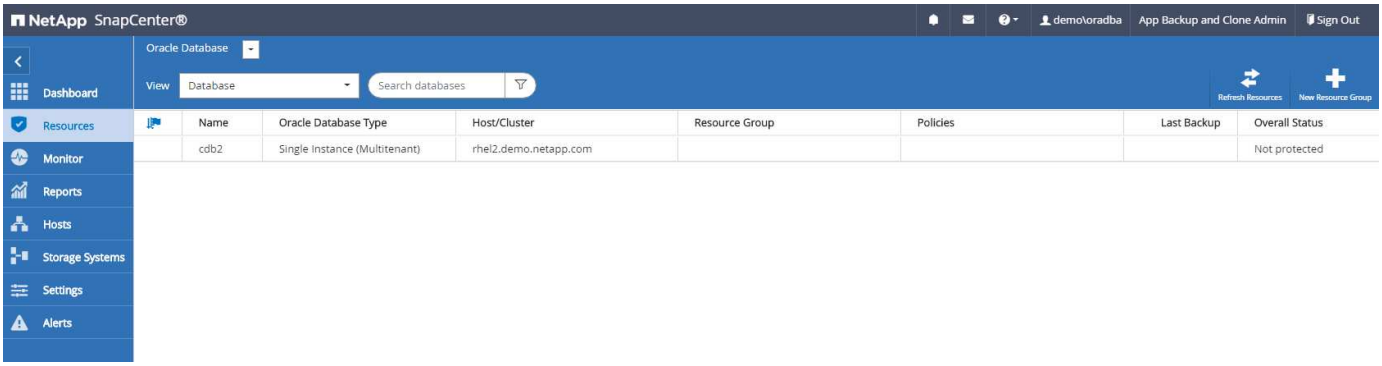
7. Assegnare l'host appena aggiunto all'ID utente corretto per la gestione del database (nel nostro caso, oradba).





4. Rilevamento delle risorse del database

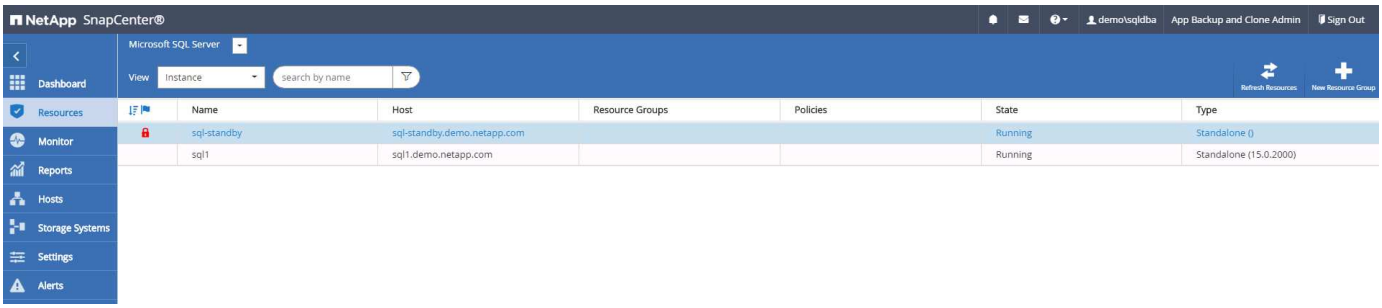
Una volta completata l'installazione del plug-in, è possibile rilevare immediatamente le risorse del database sull'host. Fare clic sulla scheda Resources (risorse) nel menu a sinistra. A seconda del tipo di piattaforma di database, sono disponibili diverse visualizzazioni, ad esempio il database, il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

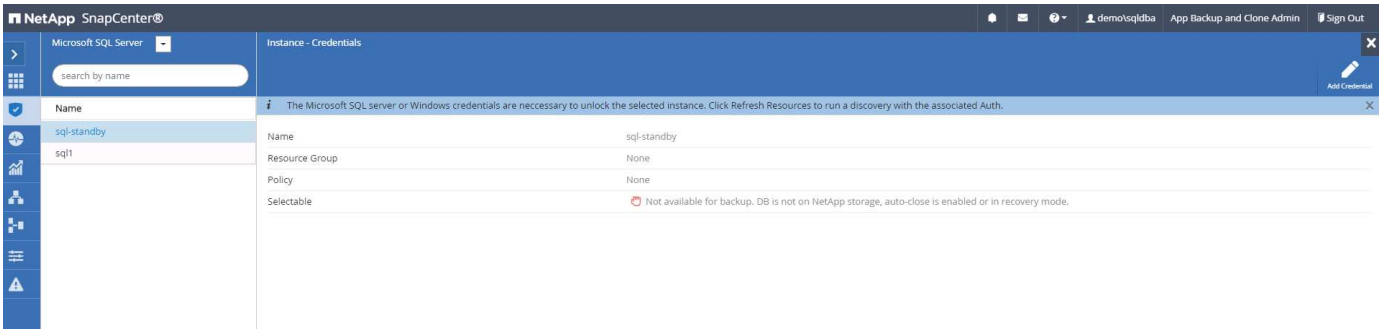


Quando il database viene rilevato inizialmente, lo stato generale viene visualizzato come "Not Protected" (non protetto). La schermata precedente mostra un database Oracle non ancora protetto da una policy di backup.

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.





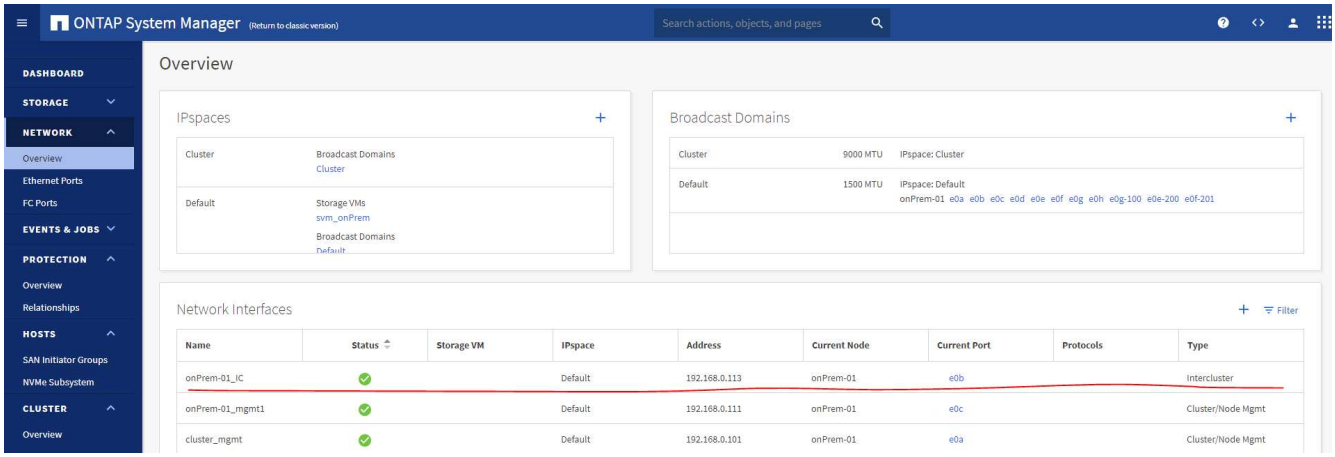
Una volta configurate le credenziali appropriate a livello di Windows o di database, il blocco rosso scompare e le informazioni sul tipo di SQL Server vengono raccolte e riviste.

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

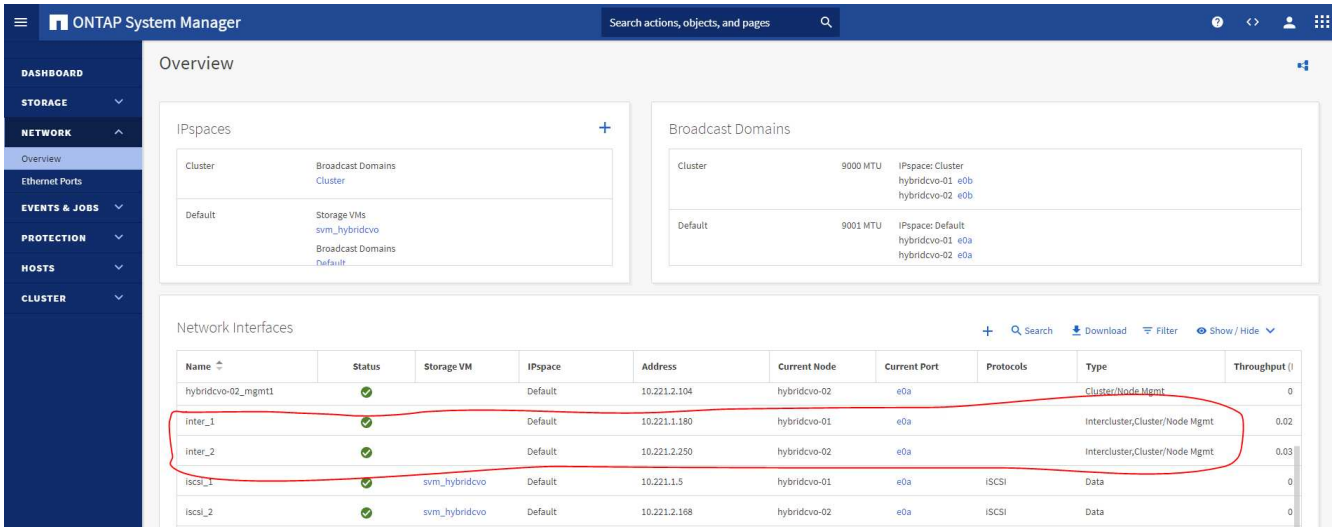
Per proteggere i dati del database on-premise utilizzando un cloud pubblico come destinazione di destinazione, i volumi di database del cluster ONTAP on-premise vengono replicati nel CVO del cloud utilizzando la tecnologia NetApp SnapMirror. I volumi di destinazione replicati possono quindi essere clonati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



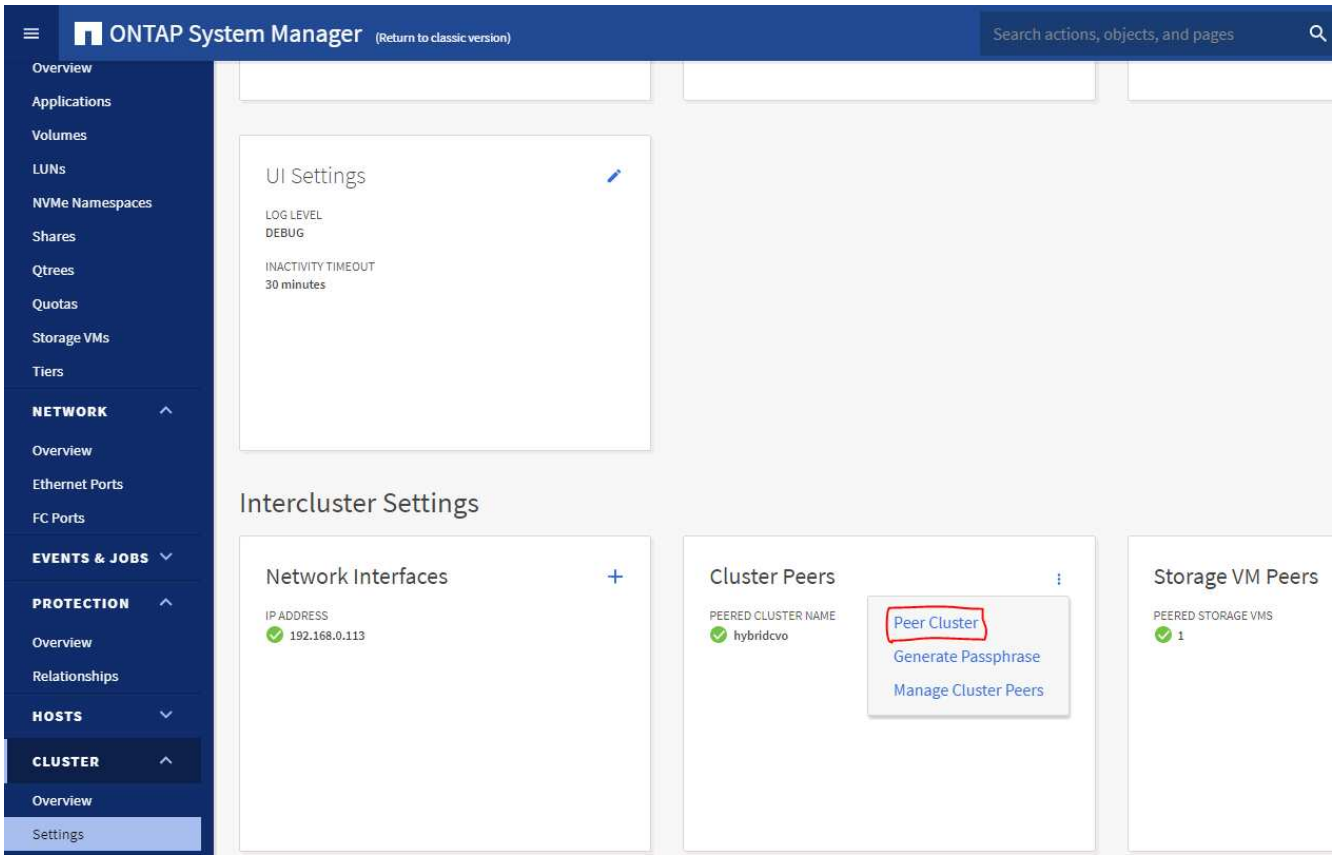
   Cluster CVO di destinazione:



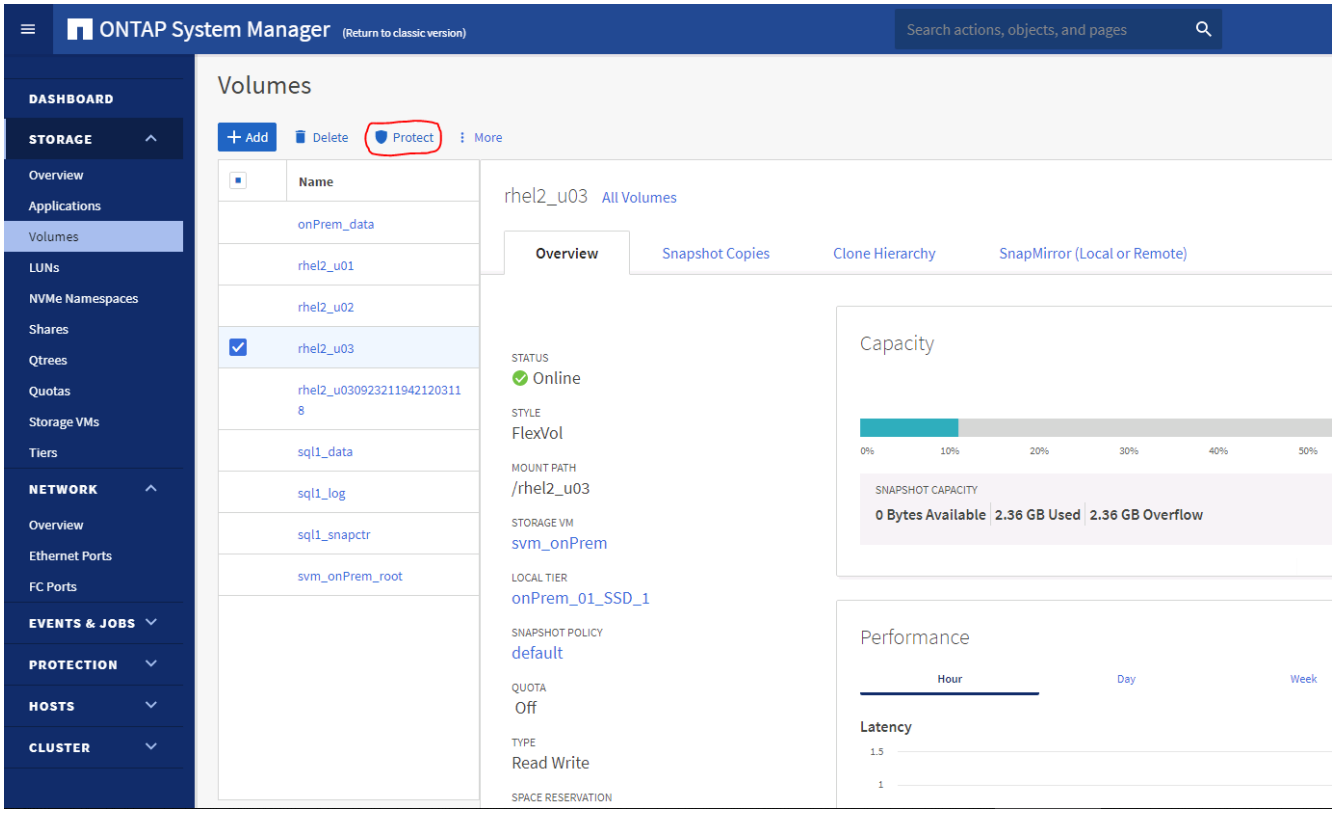
2. Con le LIF intercluster configurate, è possibile configurare il peering dei cluster e la replica dei volumi utilizzando la funzione di trascinamento della selezione in NetApp Cloud Manager. Vedere "Getting started - AWS Public Cloud" per ulteriori informazioni.

   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.

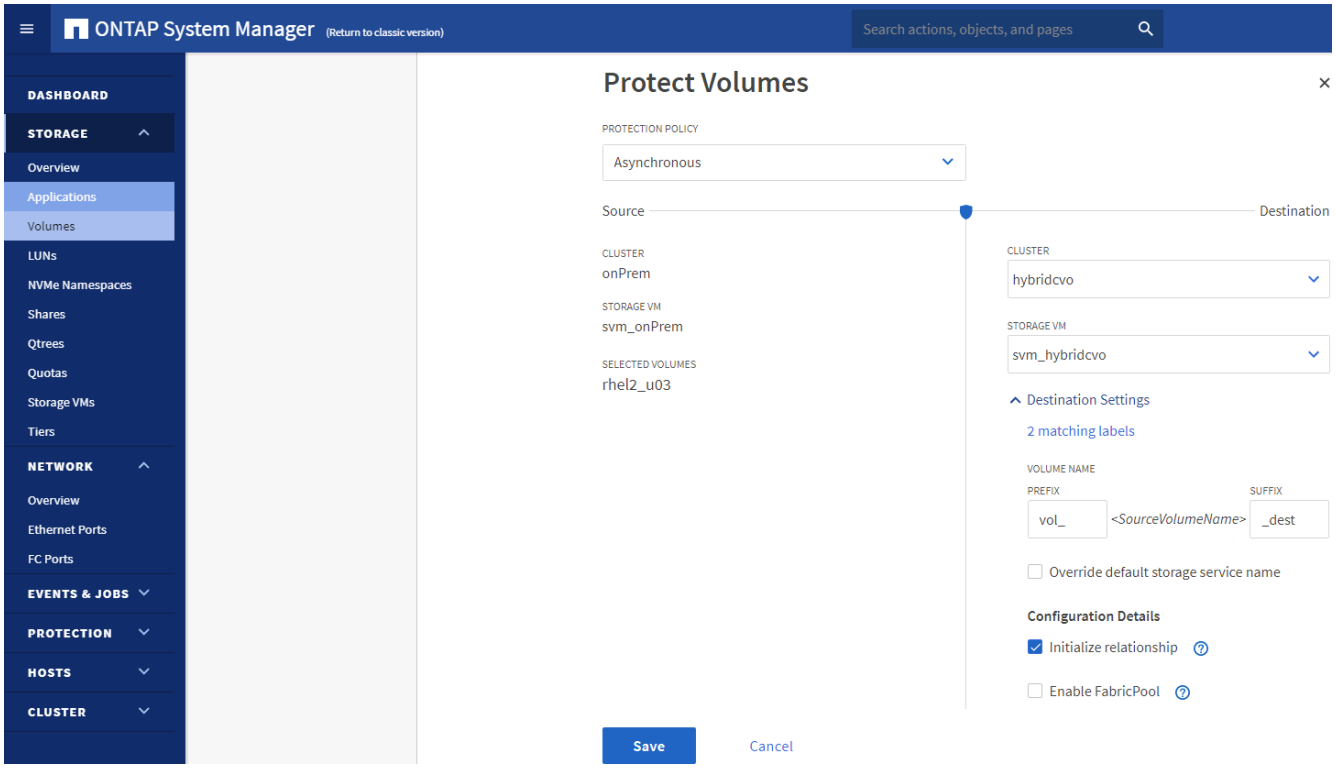


4. Accedere alla scheda Volumes (volumi). Selezionare il volume di database da replicare e fare clic su Proteggi.

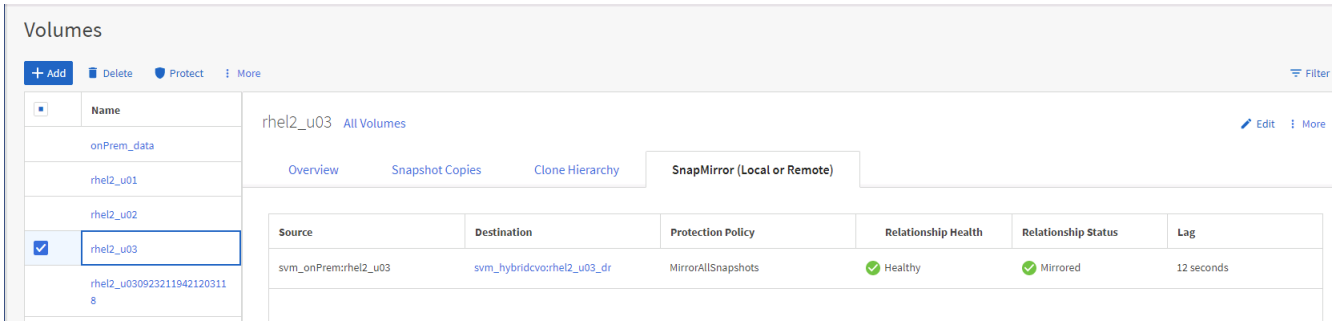


5. Impostare il criterio di protezione su asincrono. Selezionare la SVM del cluster e dello storage di

destinazione.

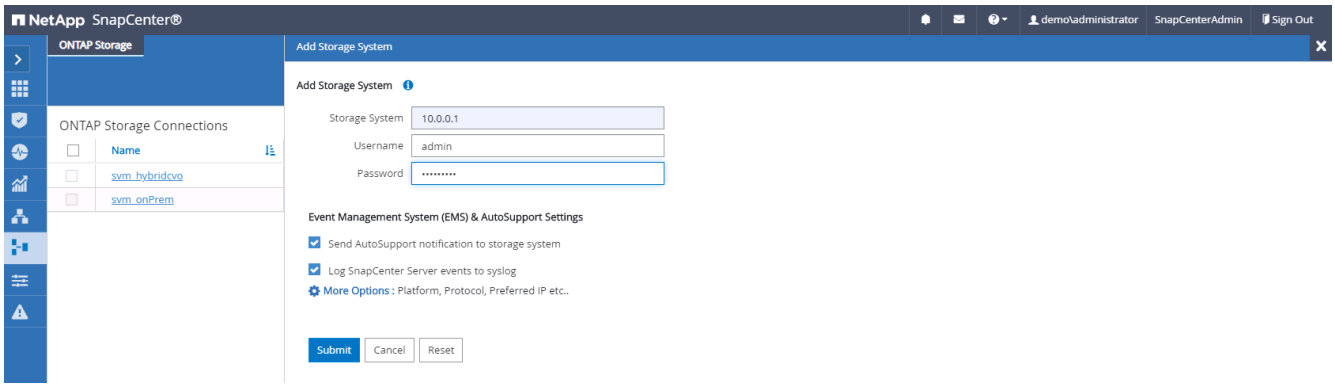


6. Verificare che il volume sia sincronizzato tra l'origine e la destinazione e che la relazione di replica sia corretta.

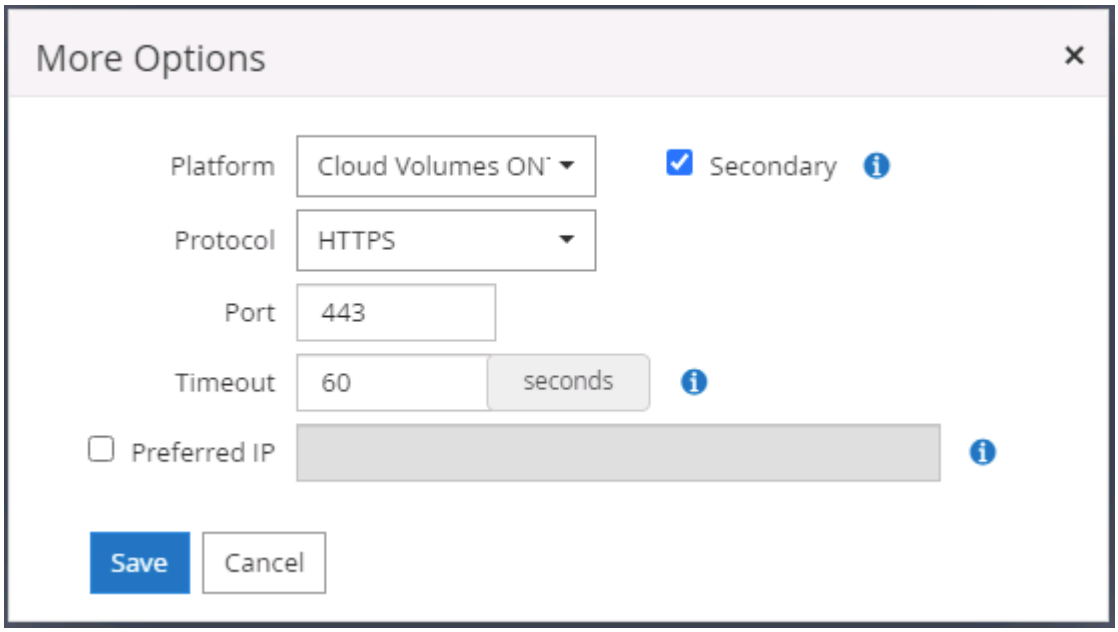


6. Aggiunta di SVM per lo storage di database CVO a SnapCenter

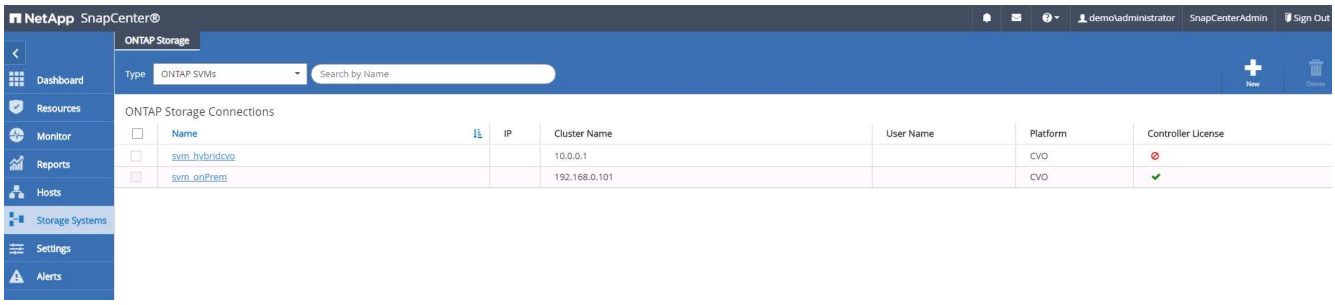
1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda sistema di storage dal menu, quindi fare clic su nuovo per aggiungere una SVM di storage CVO che ospita volumi di database di destinazione replicati in SnapCenter. Inserire l'IP di gestione del cluster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

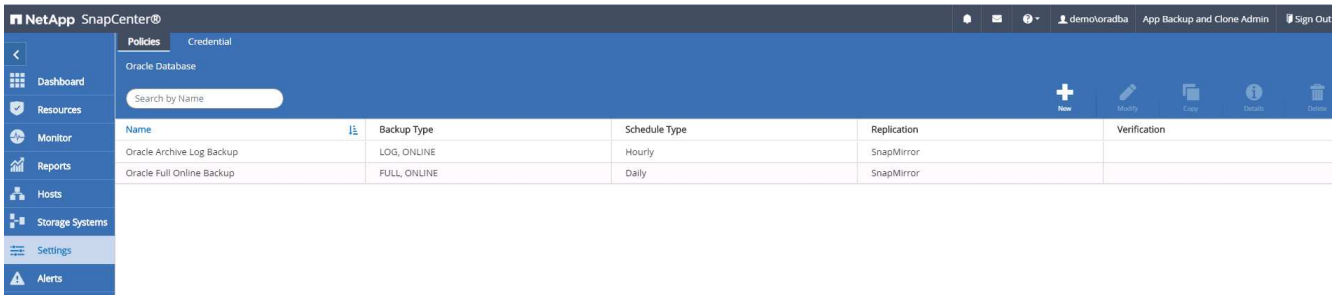


7. Configurare i criteri di backup del database in SnapCenter

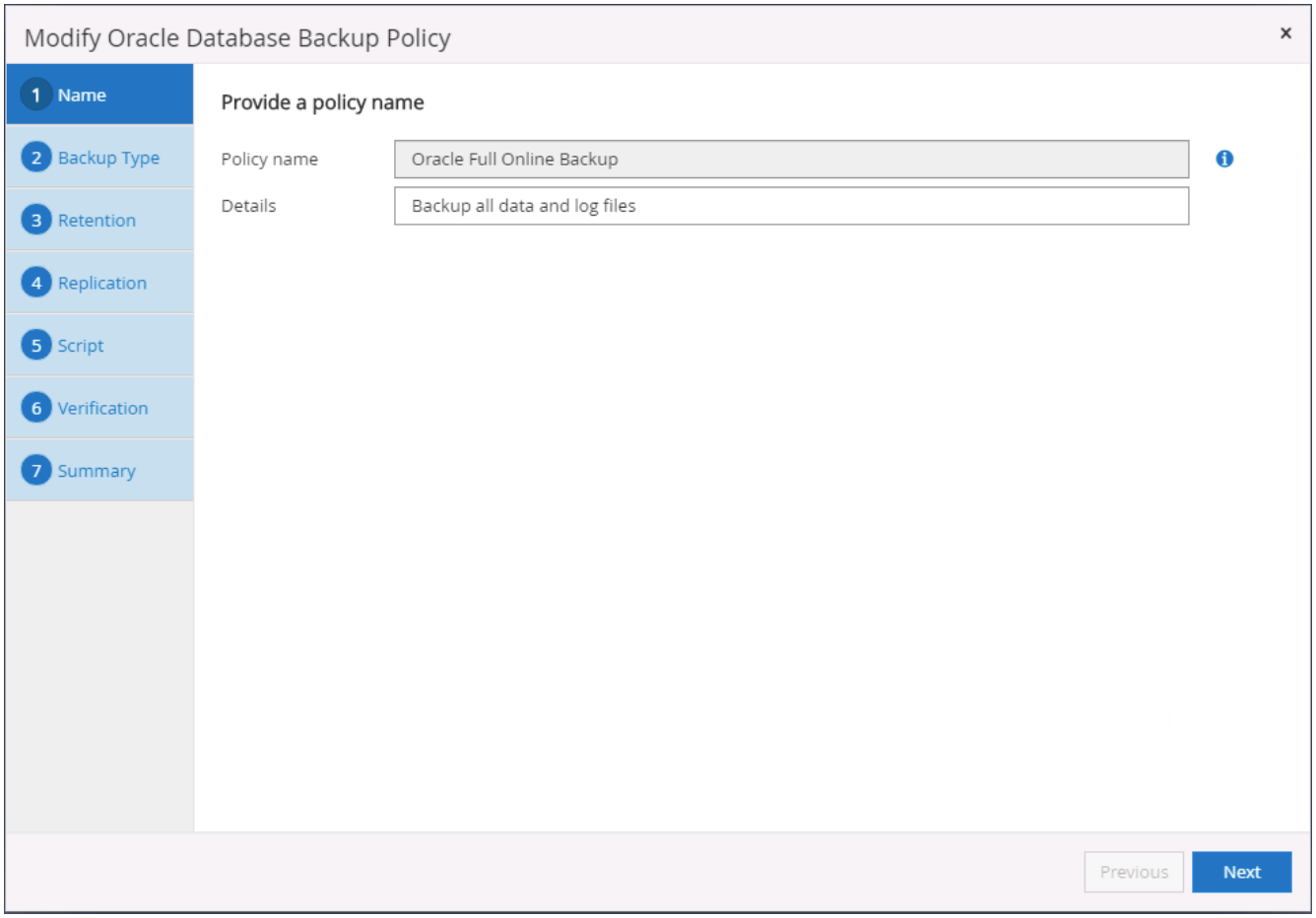
Le seguenti procedure illustrano come creare un database completo o un criterio di backup del file di log. Il criterio può quindi essere implementato per proteggere le risorse dei database. L'RPO (Recovery Point Objective) o RTO (Recovery Time Objective) determina la frequenza dei backup del database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

Creare una policy di backup completa del database per Oracle

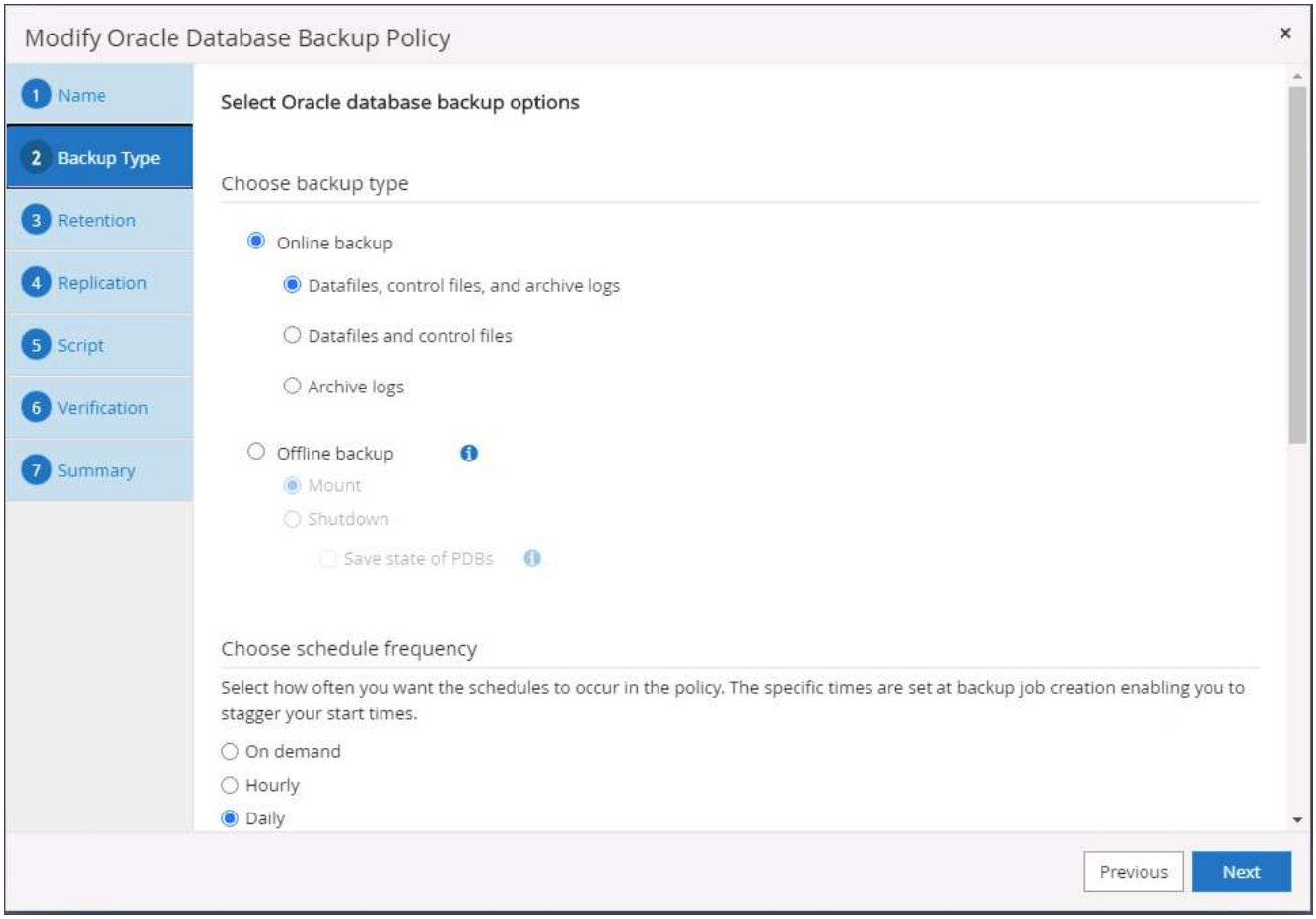
1. Accedere a SnapCenter come ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.



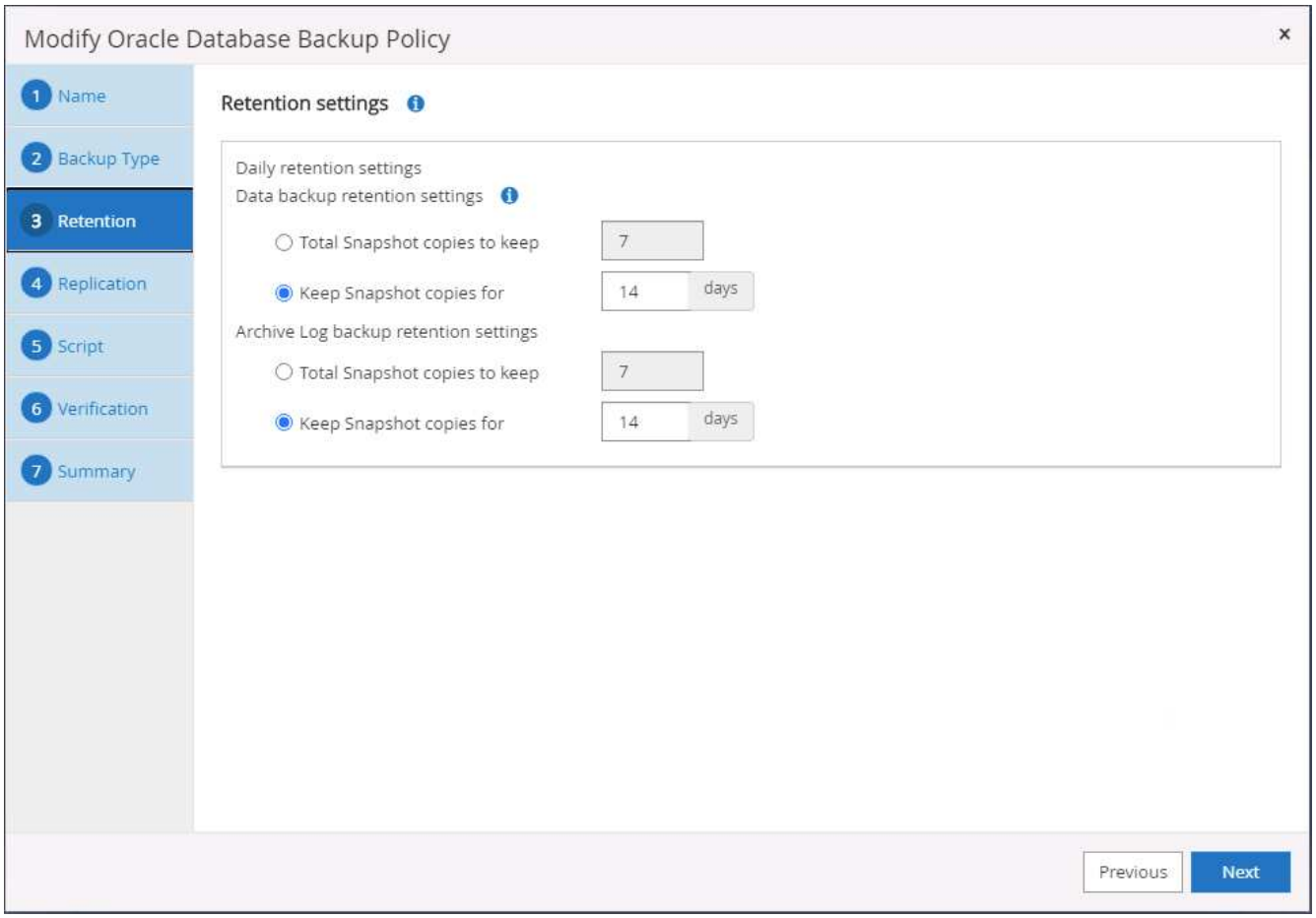
2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.



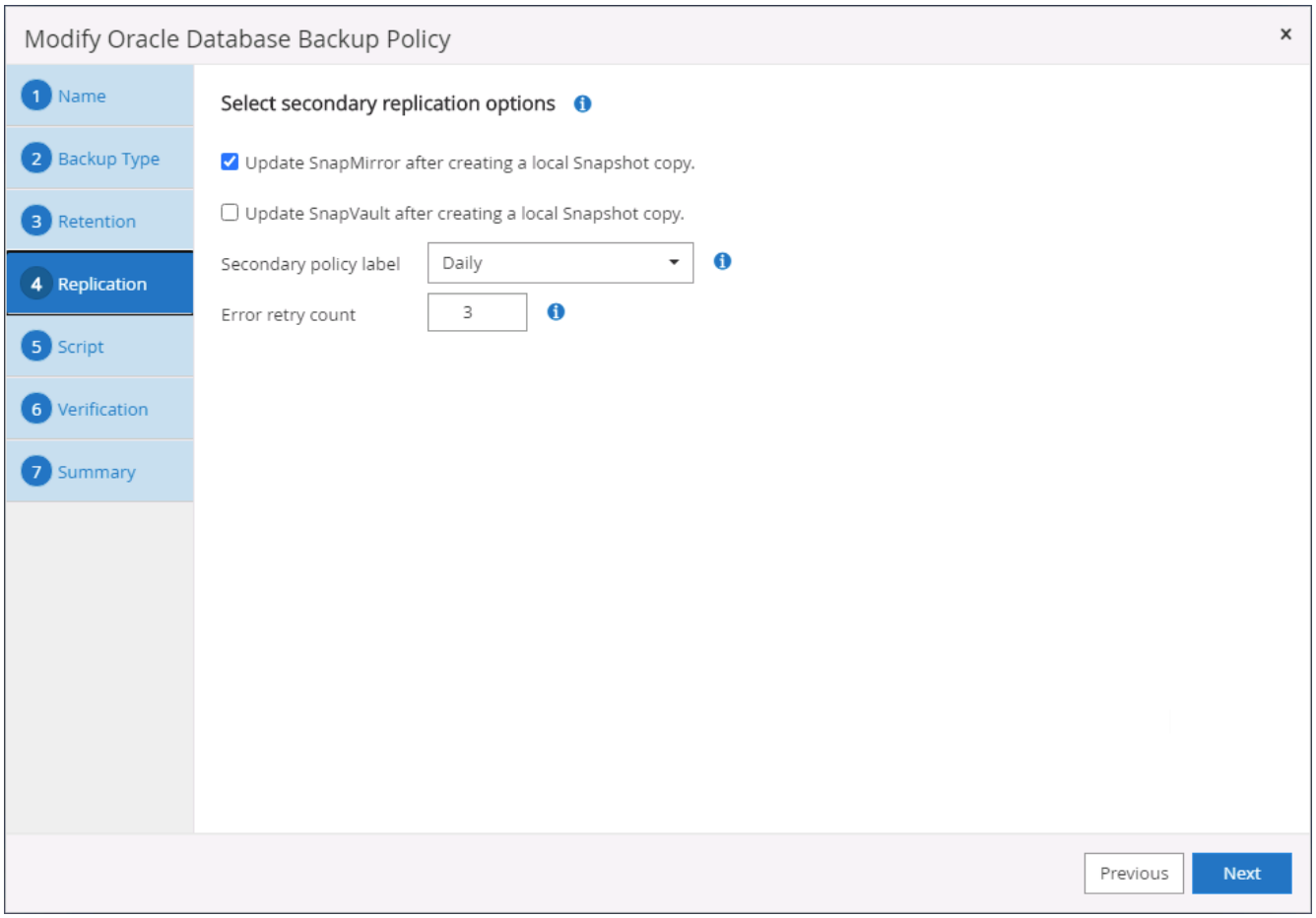
3. Selezionare il tipo di backup e la frequenza di pianificazione.



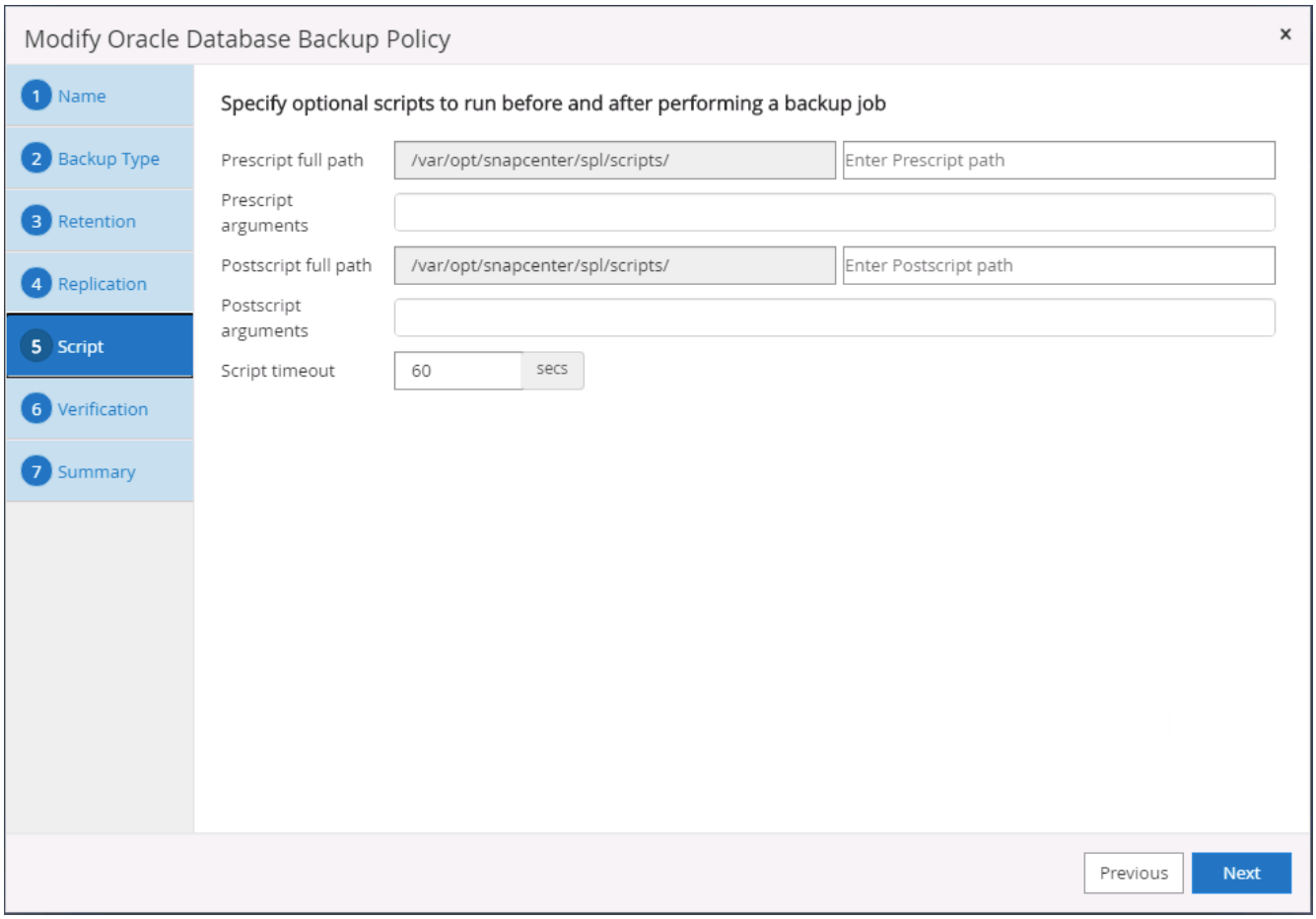
4. Impostare la conservazione del backup. Definisce il numero di copie di backup complete del database da conservare.



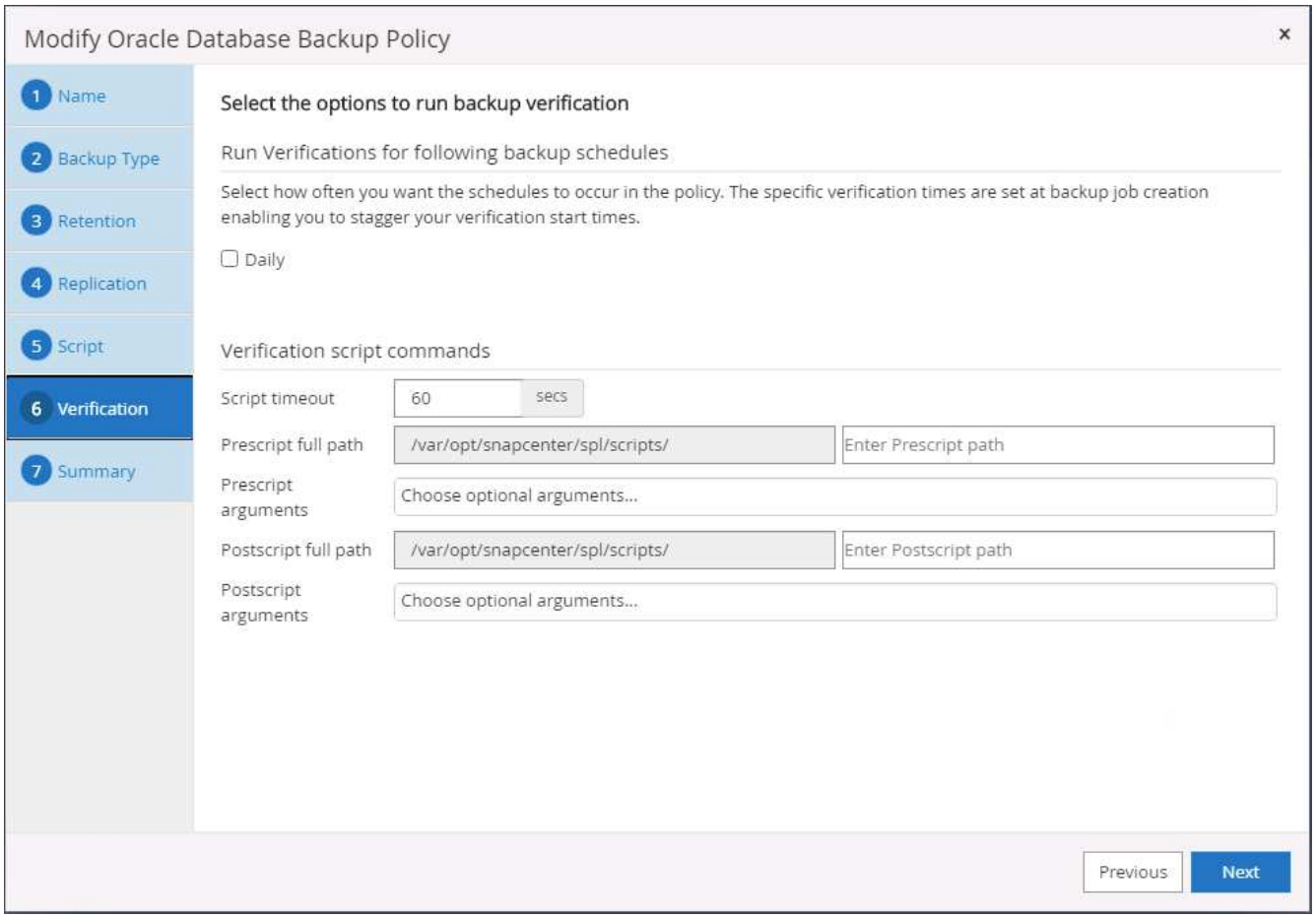
5. Selezionare le opzioni di replica secondaria per inviare i backup delle snapshot primarie locali da replicare in una posizione secondaria nel cloud.



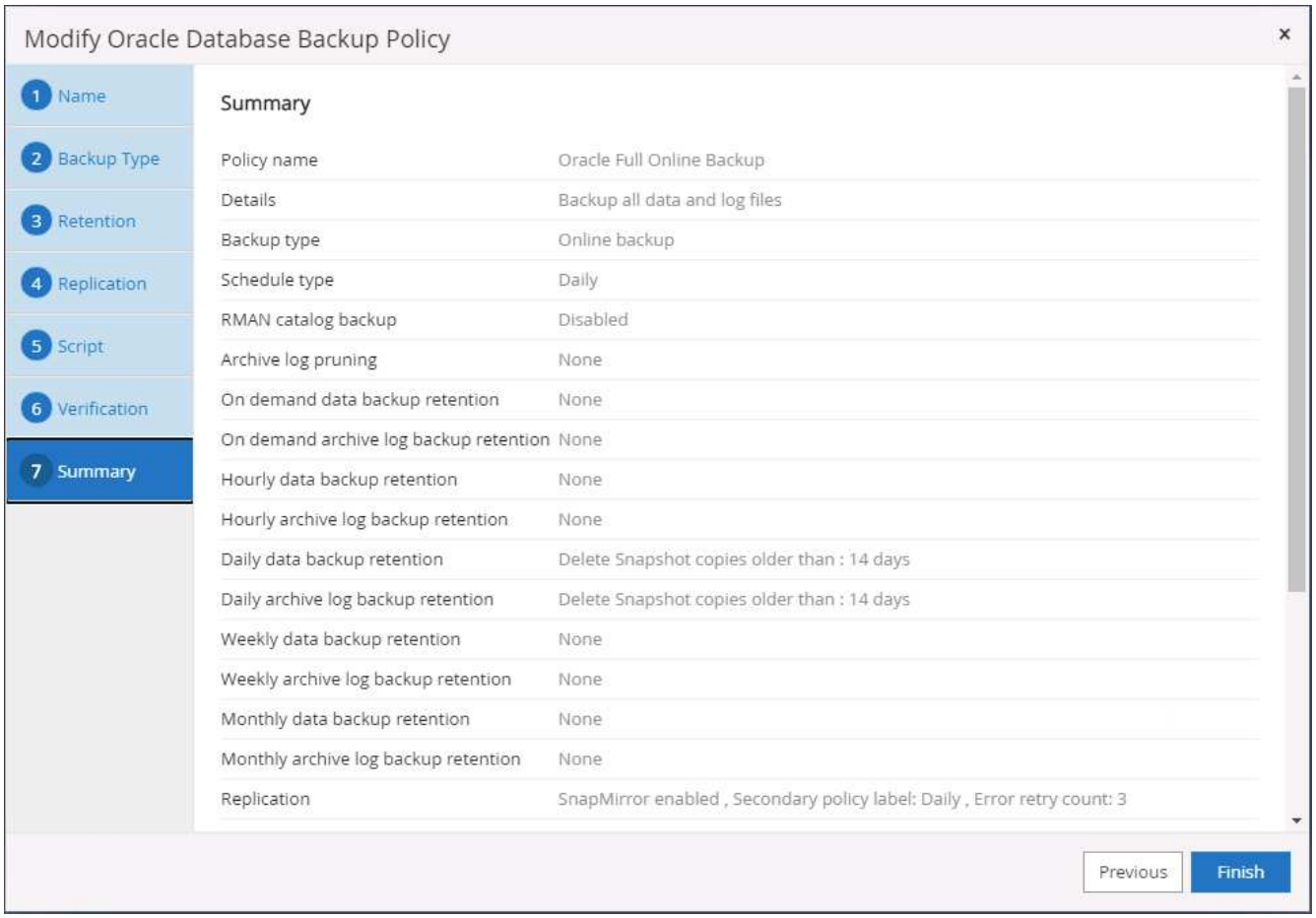
6. Specificare qualsiasi script opzionale da eseguire prima e dopo l'esecuzione di un backup.



7. Eseguire la verifica del backup, se necessario.

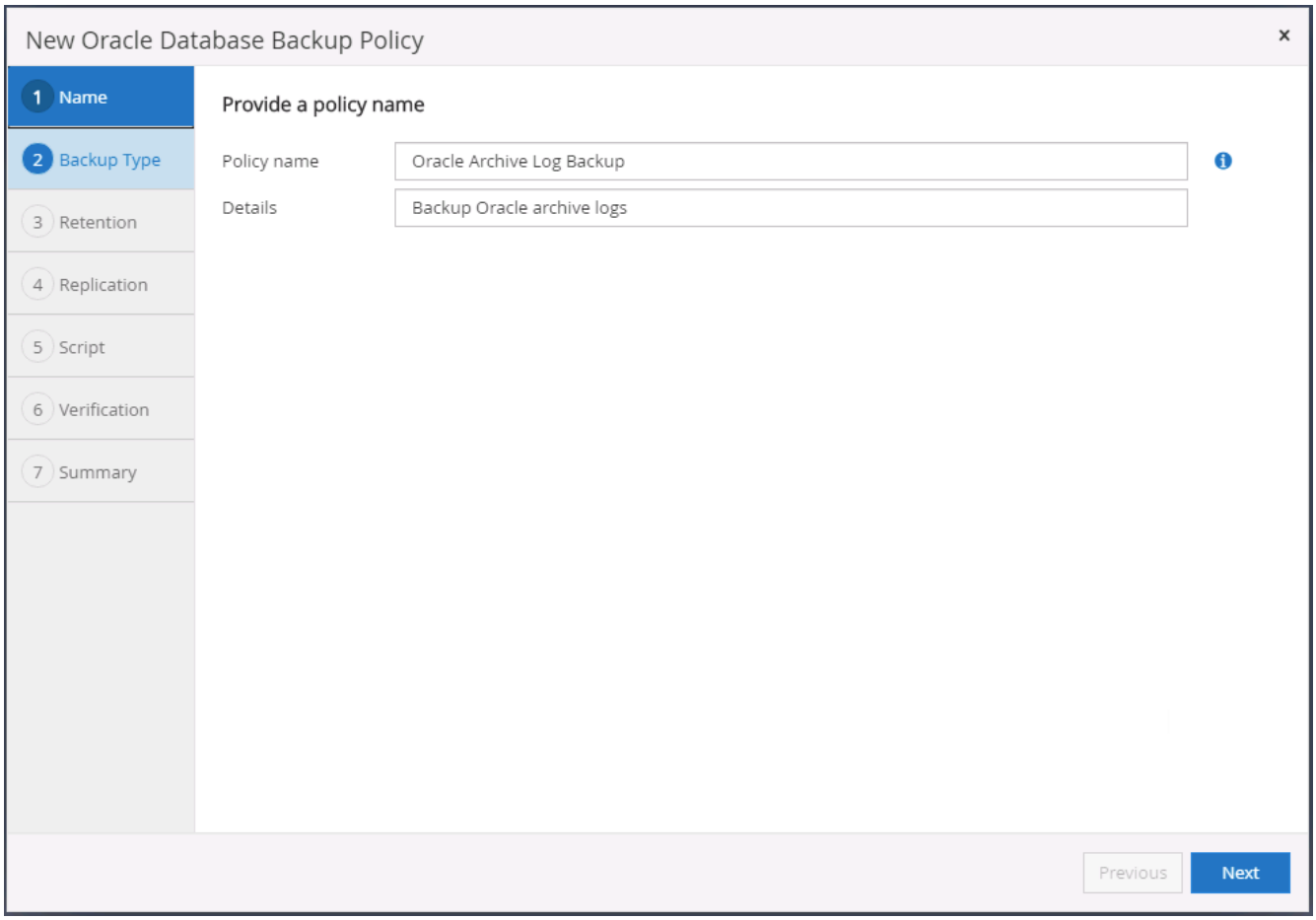

Modify Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification 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.

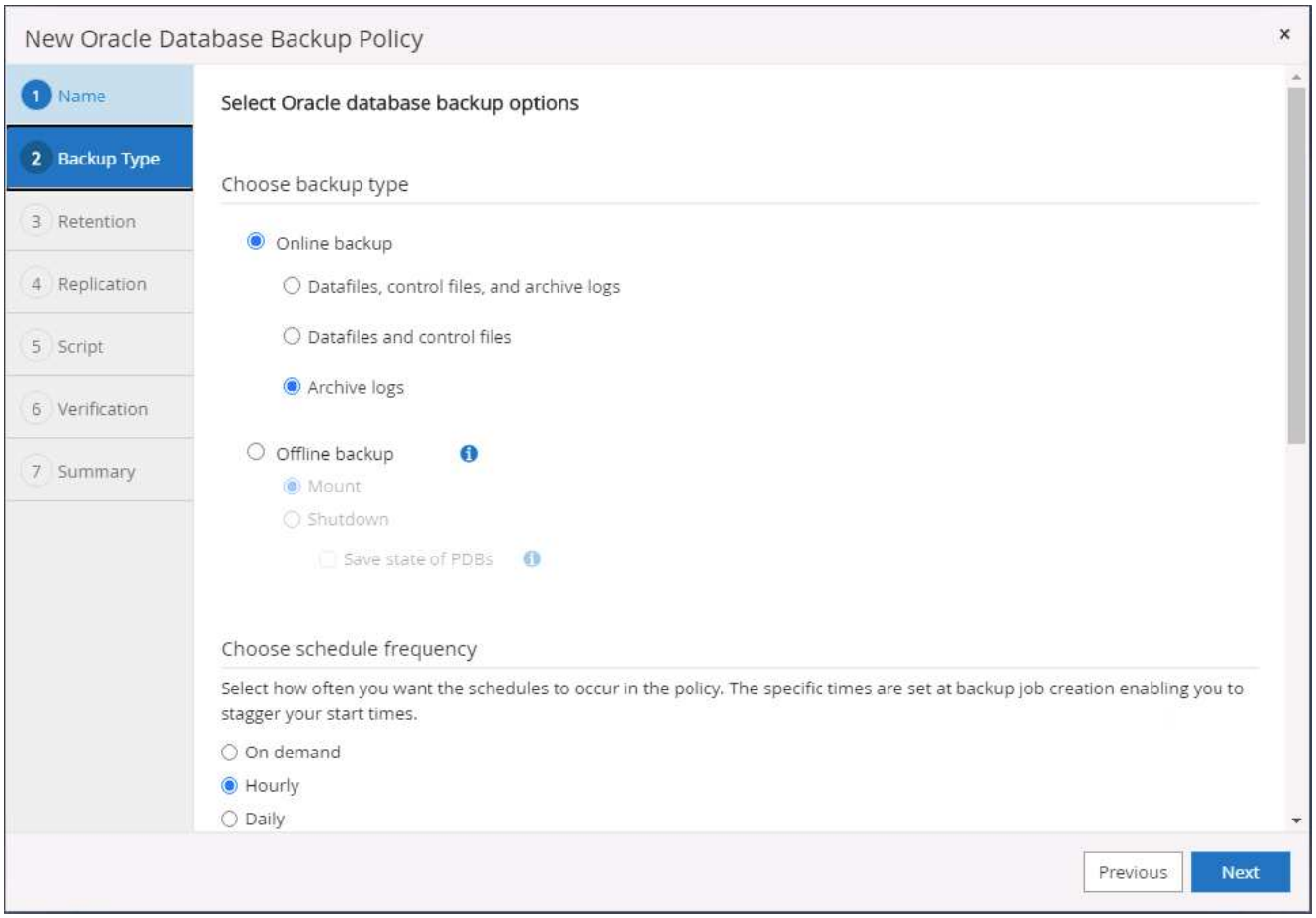


Creare una policy di backup del log del database per Oracle

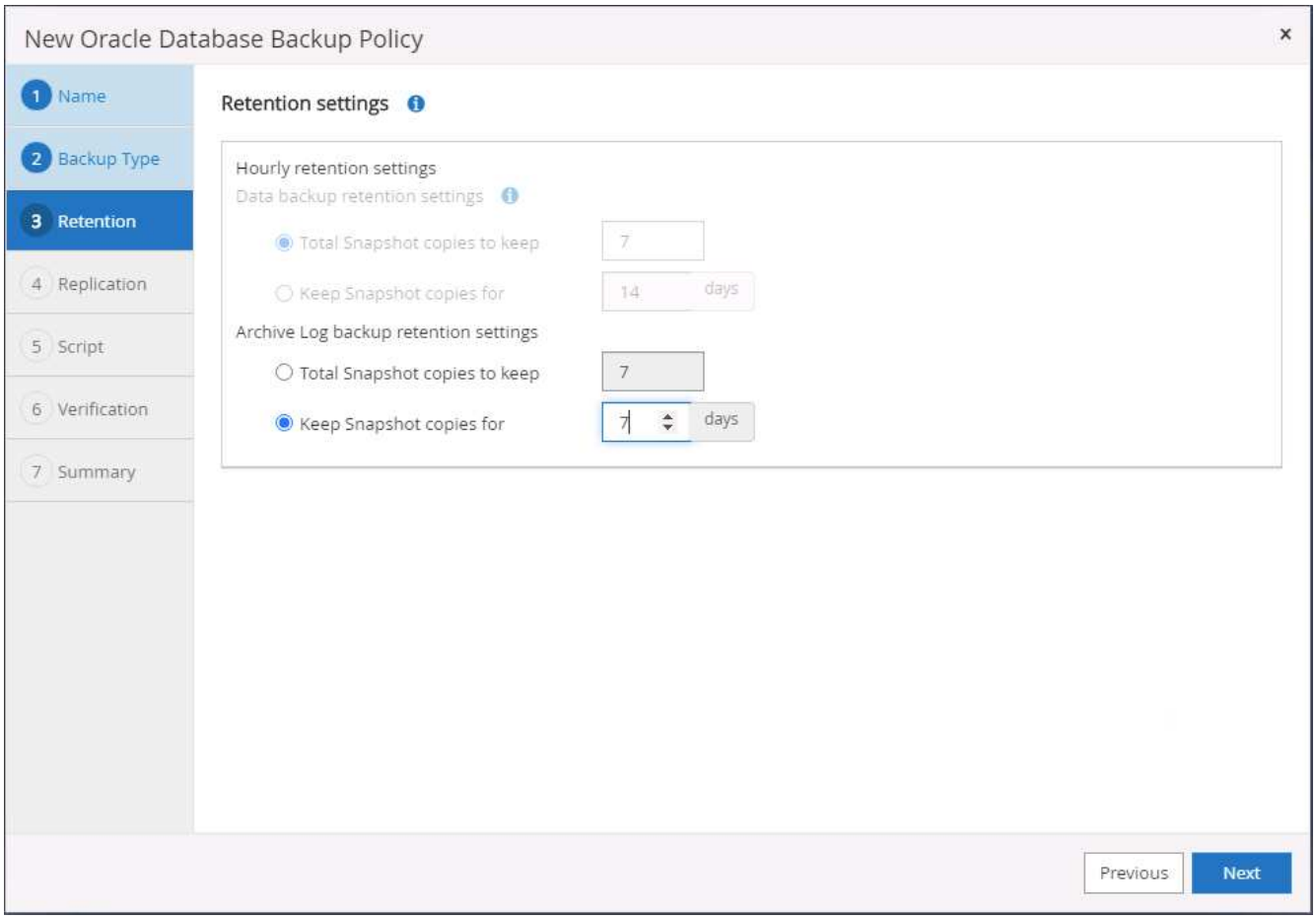
1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.
2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.



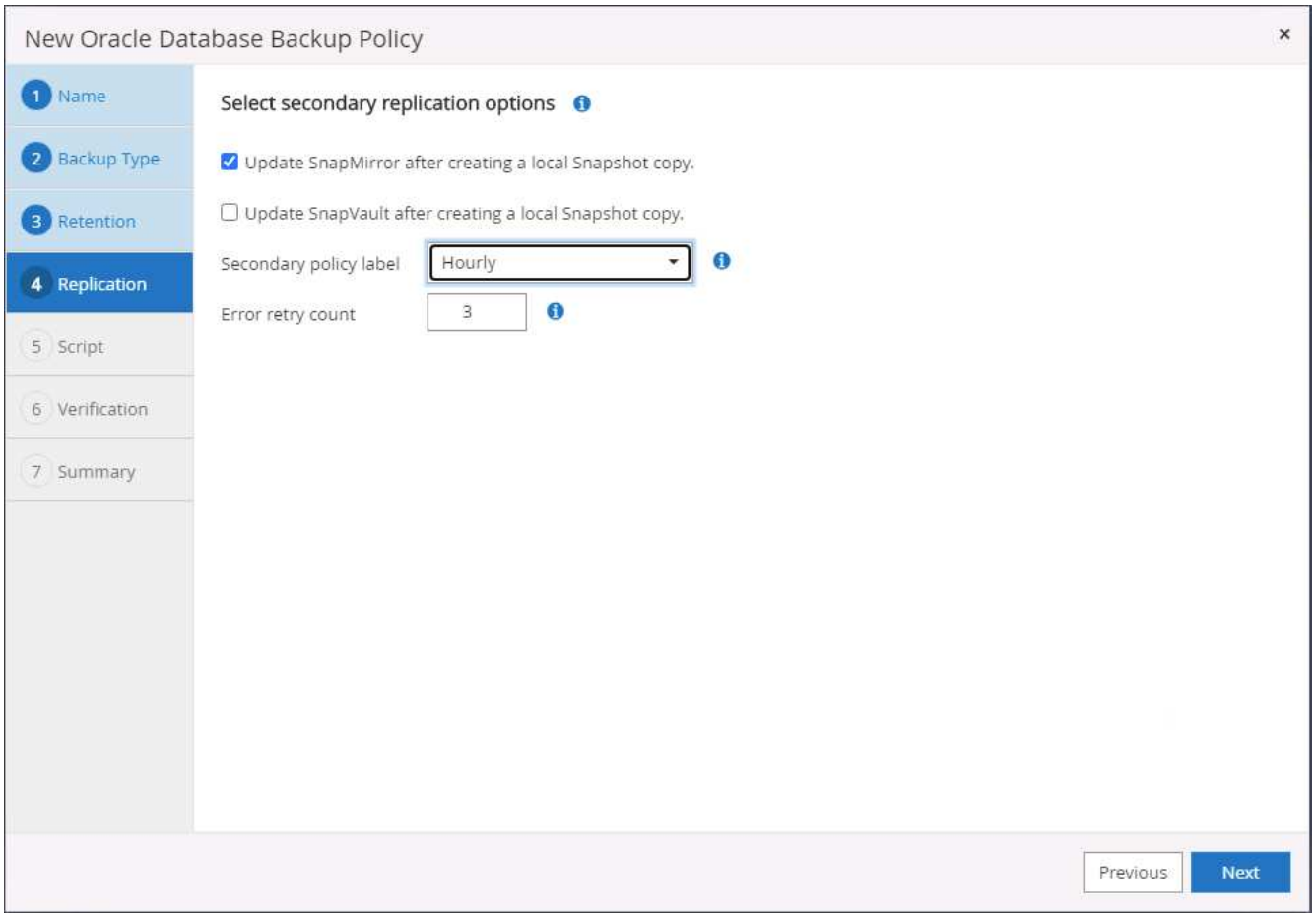
3. Selezionare il tipo di backup e la frequenza di pianificazione.



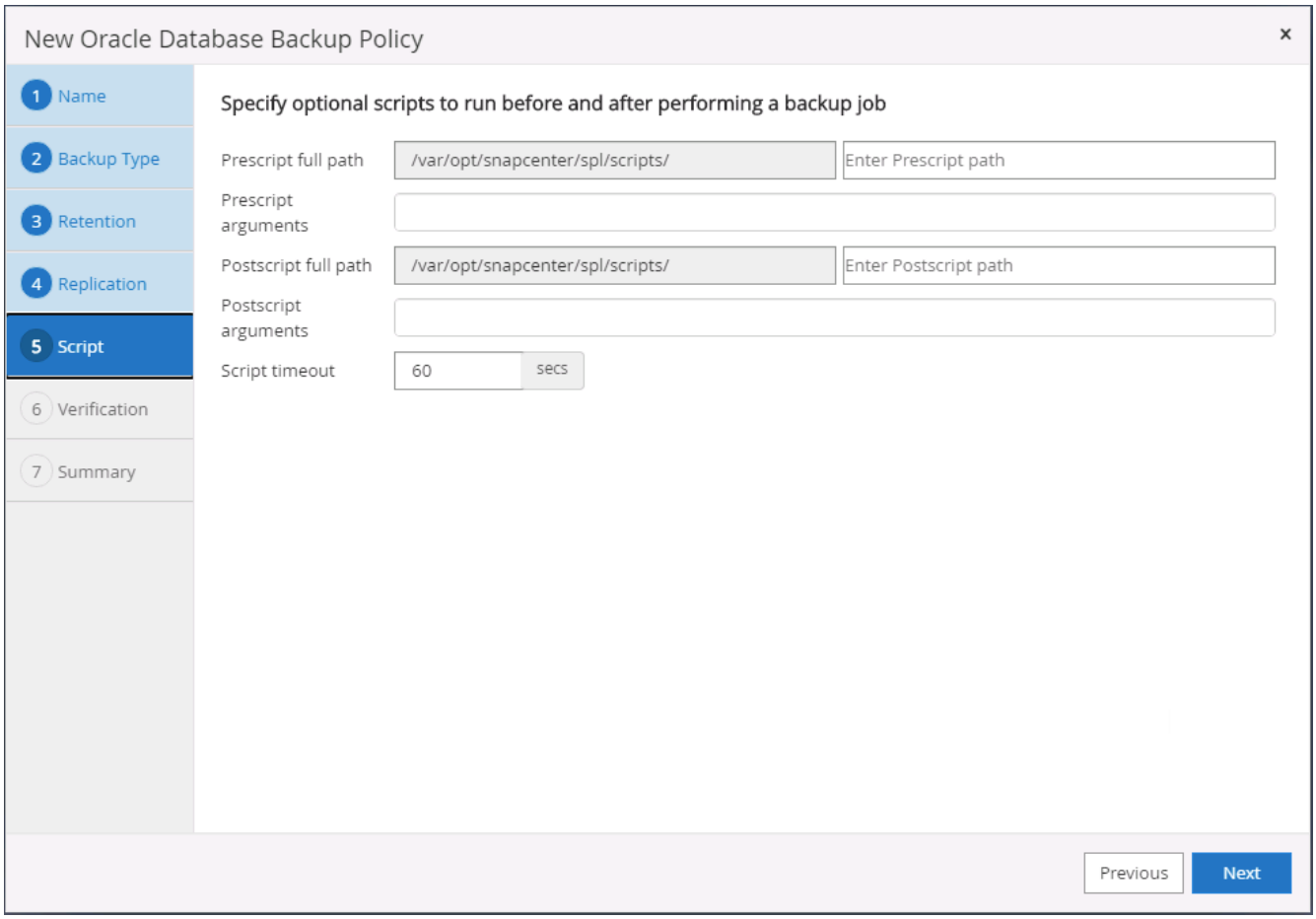
4. Impostare il periodo di conservazione del registro.



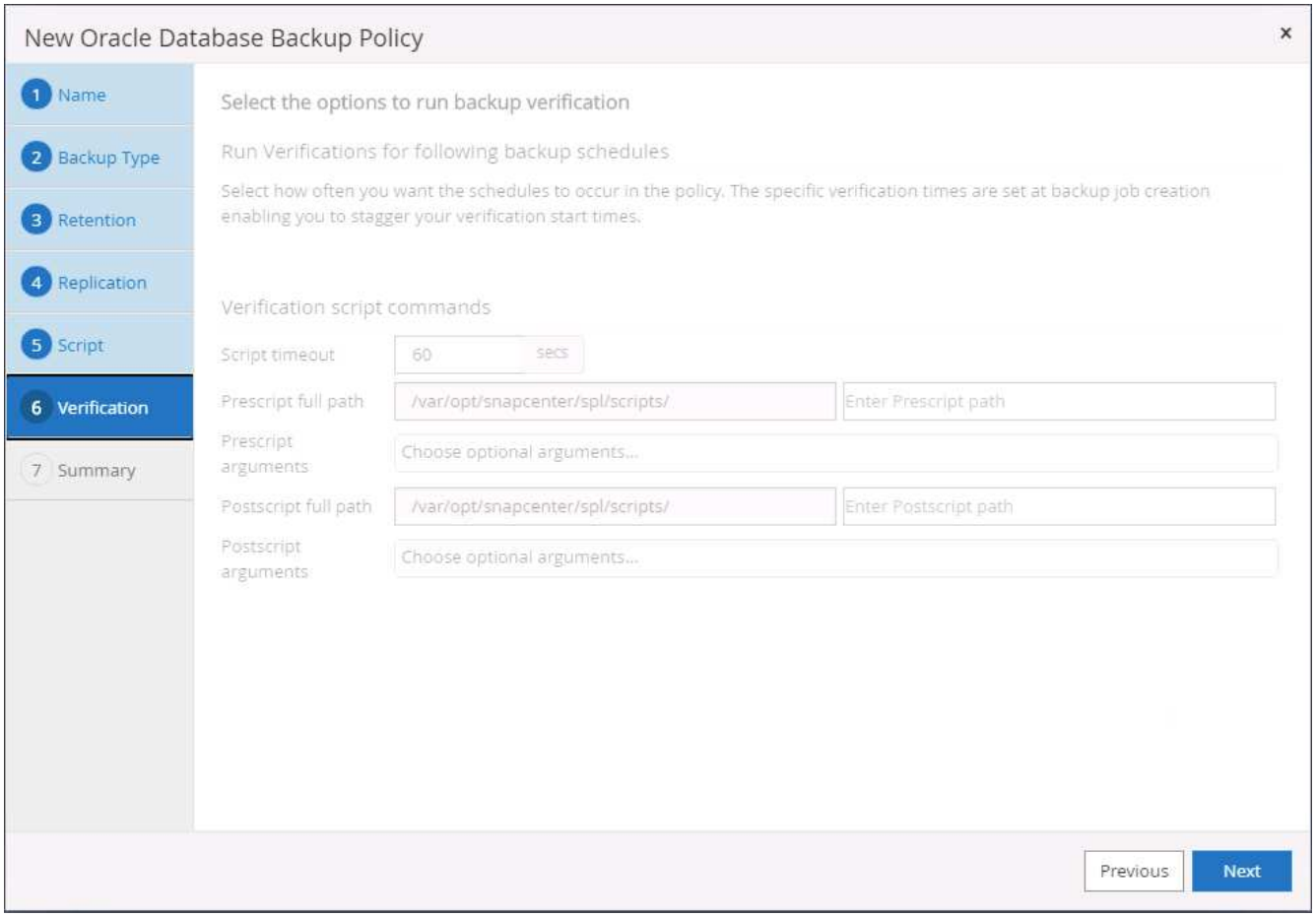
5. Abilitare la replica in una posizione secondaria nel cloud pubblico.



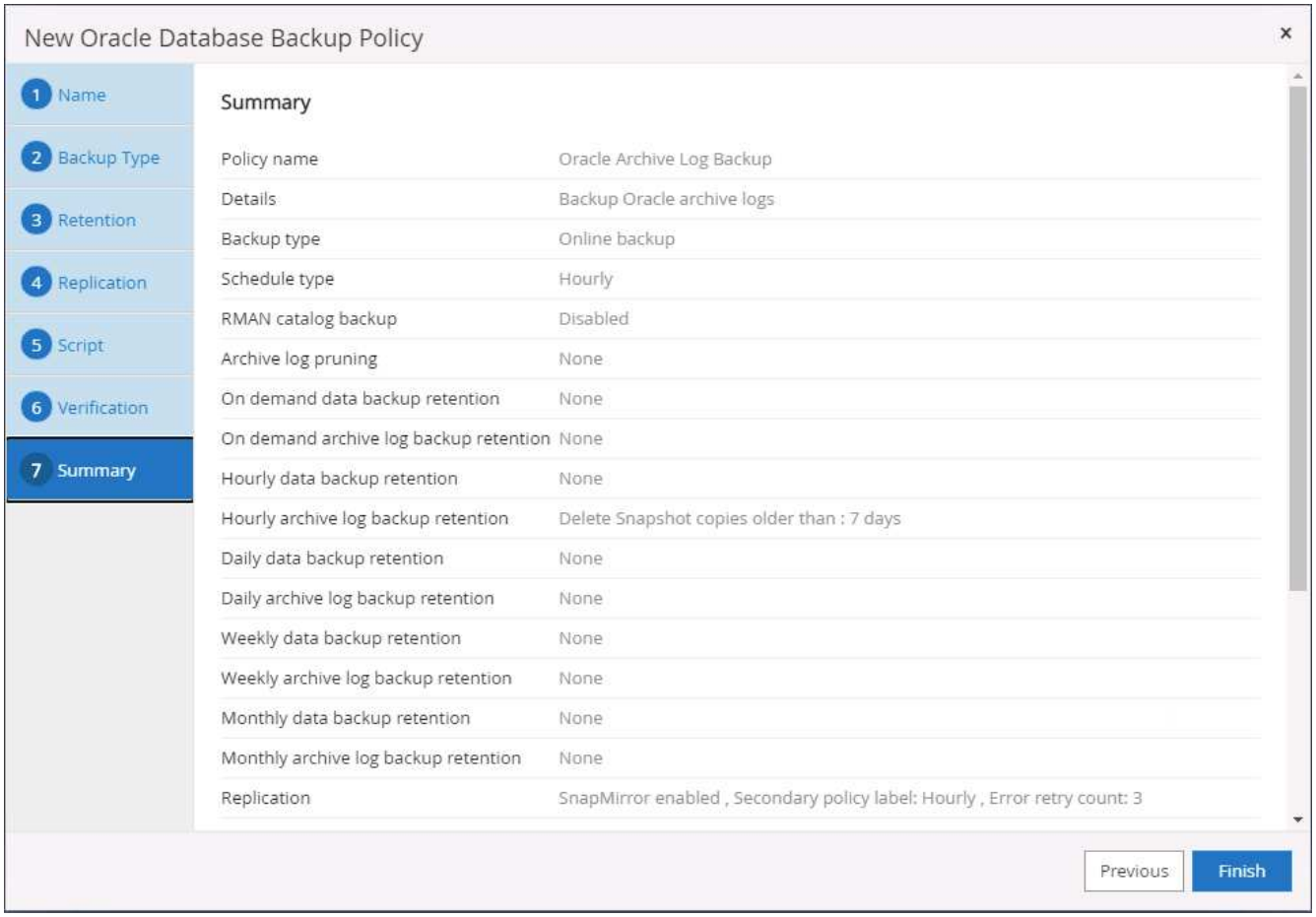
6. Specificare eventuali script opzionali da eseguire prima e dopo il backup del registro.



7. Specificare eventuali script di verifica del backup.

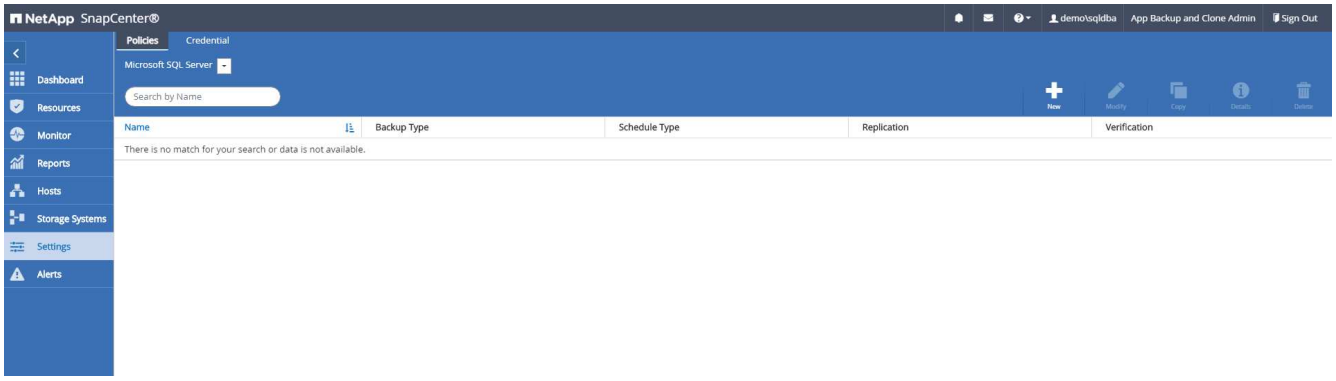

New Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times 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.

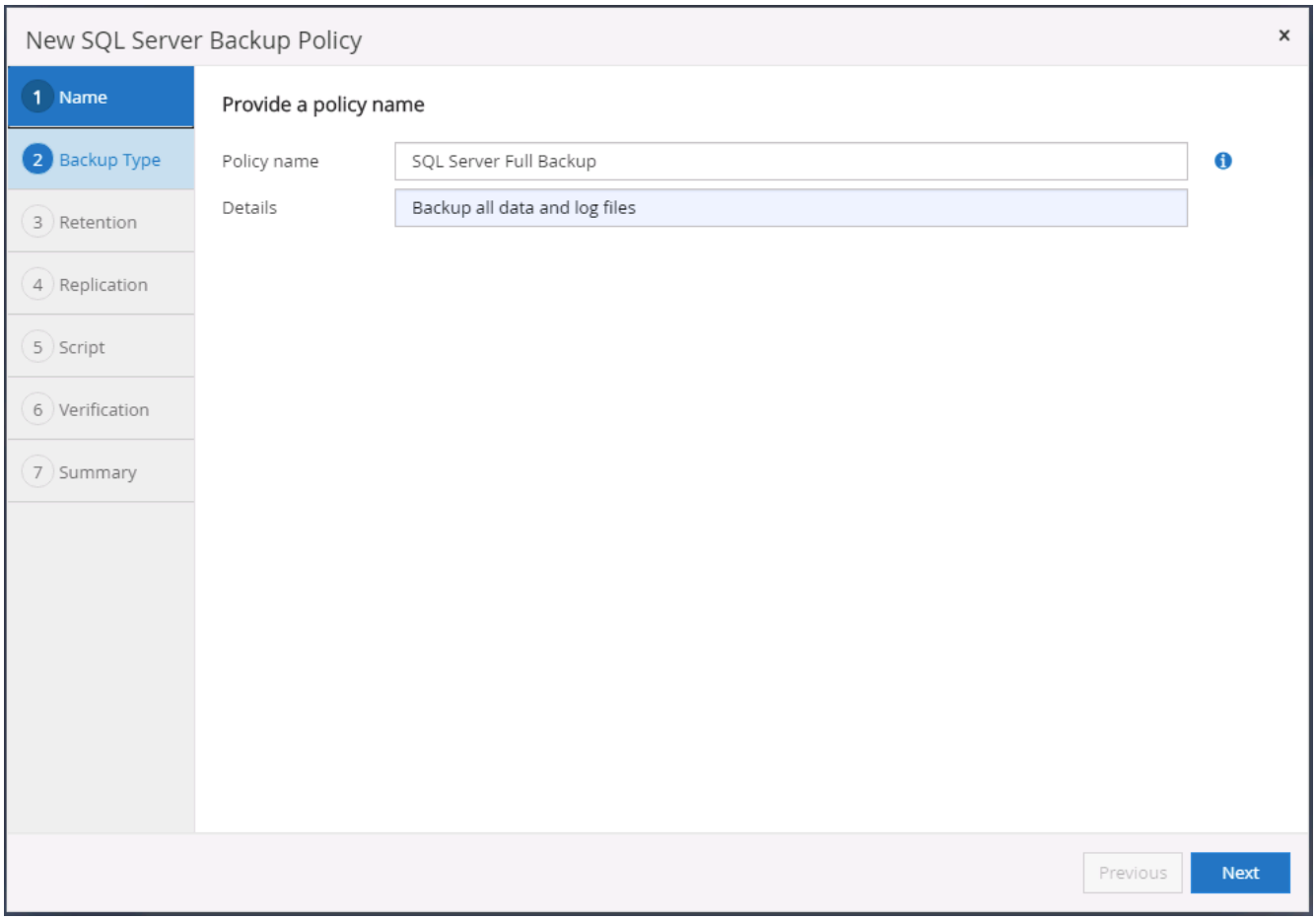


Creare una policy di backup completa del database per SQL

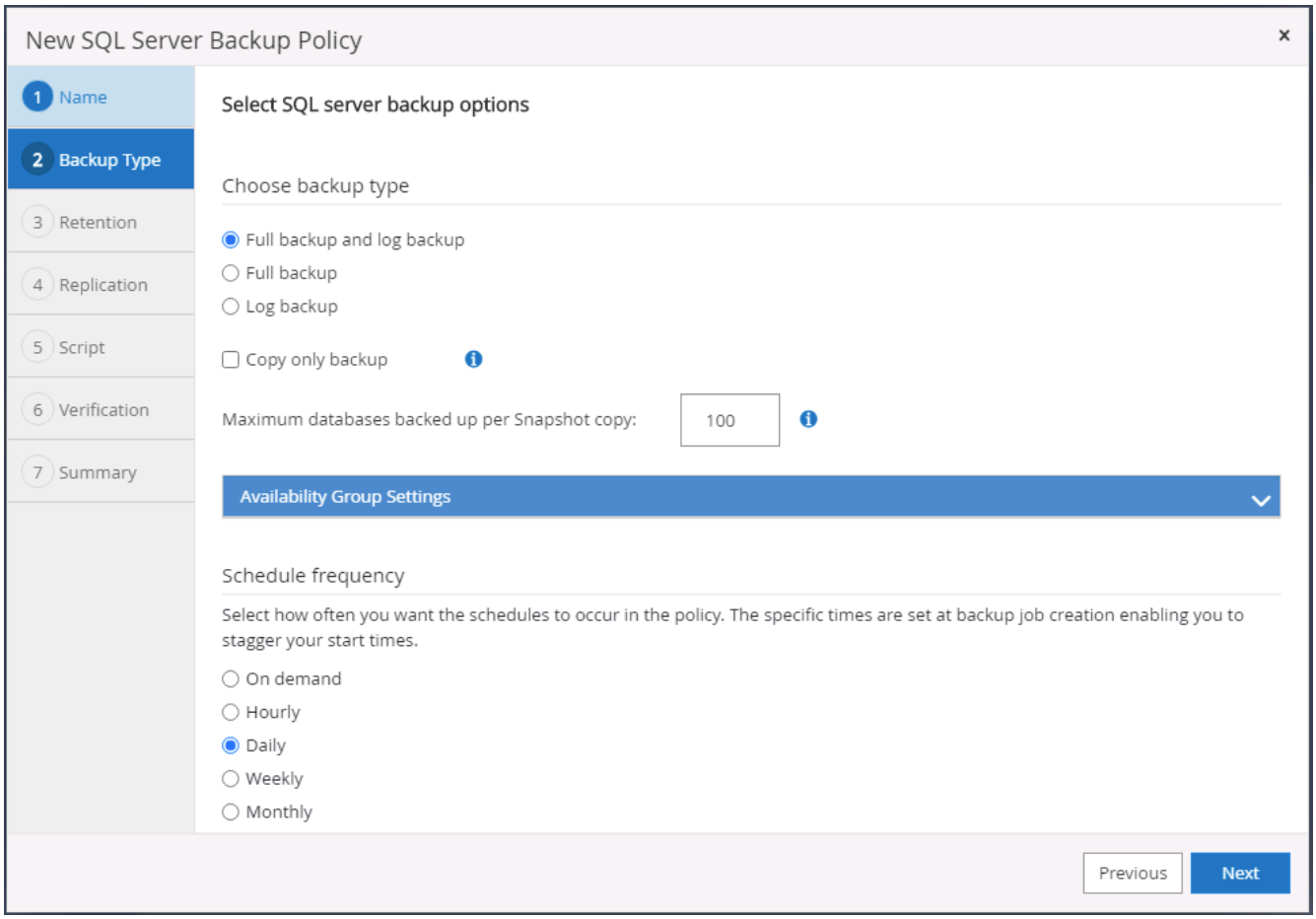
1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni, quindi su criteri.



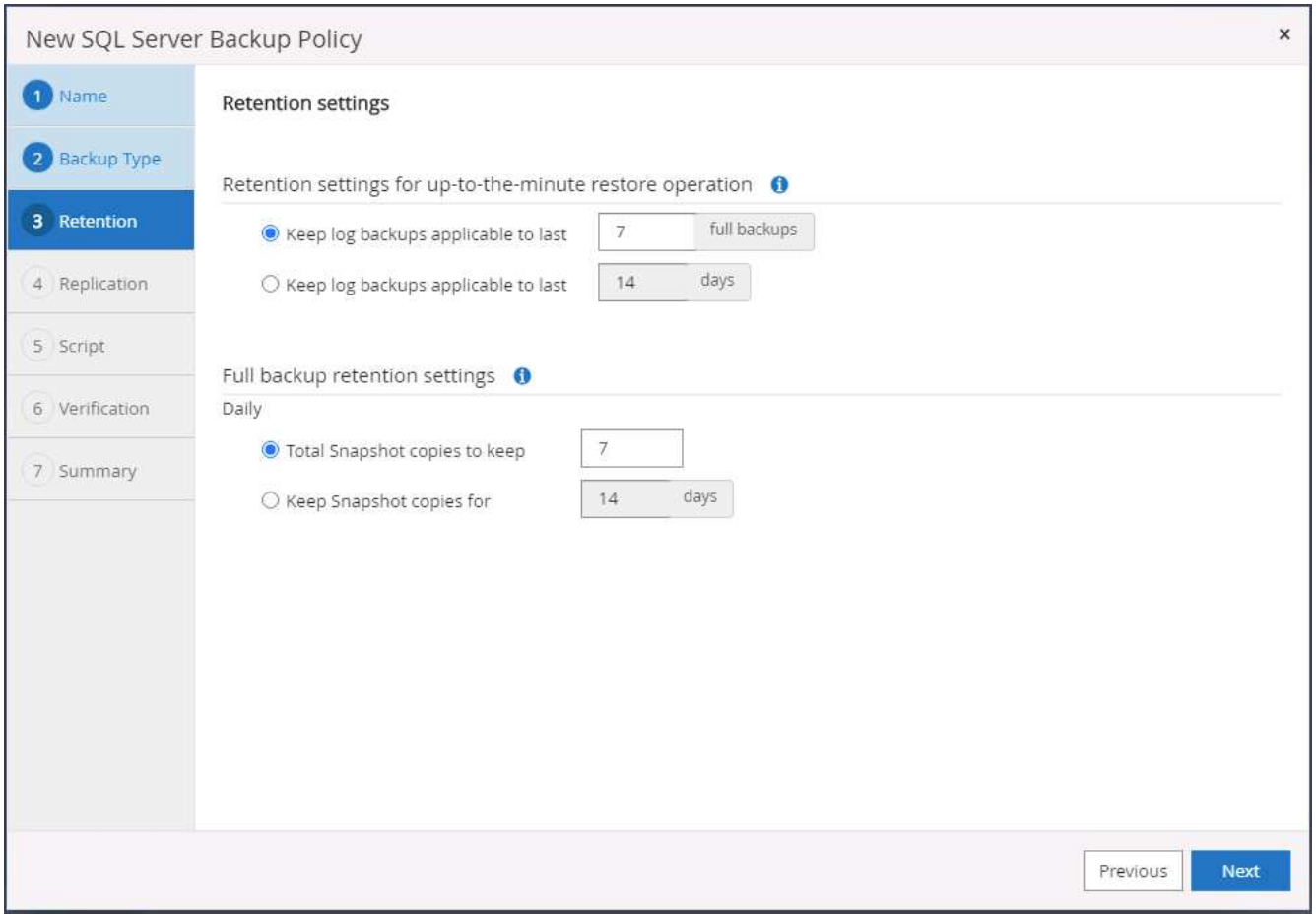
2. Fare clic su New (nuovo) per avviare un nuovo flusso di lavoro di creazione dei criteri di backup o scegliere un criterio esistente per la modifica.



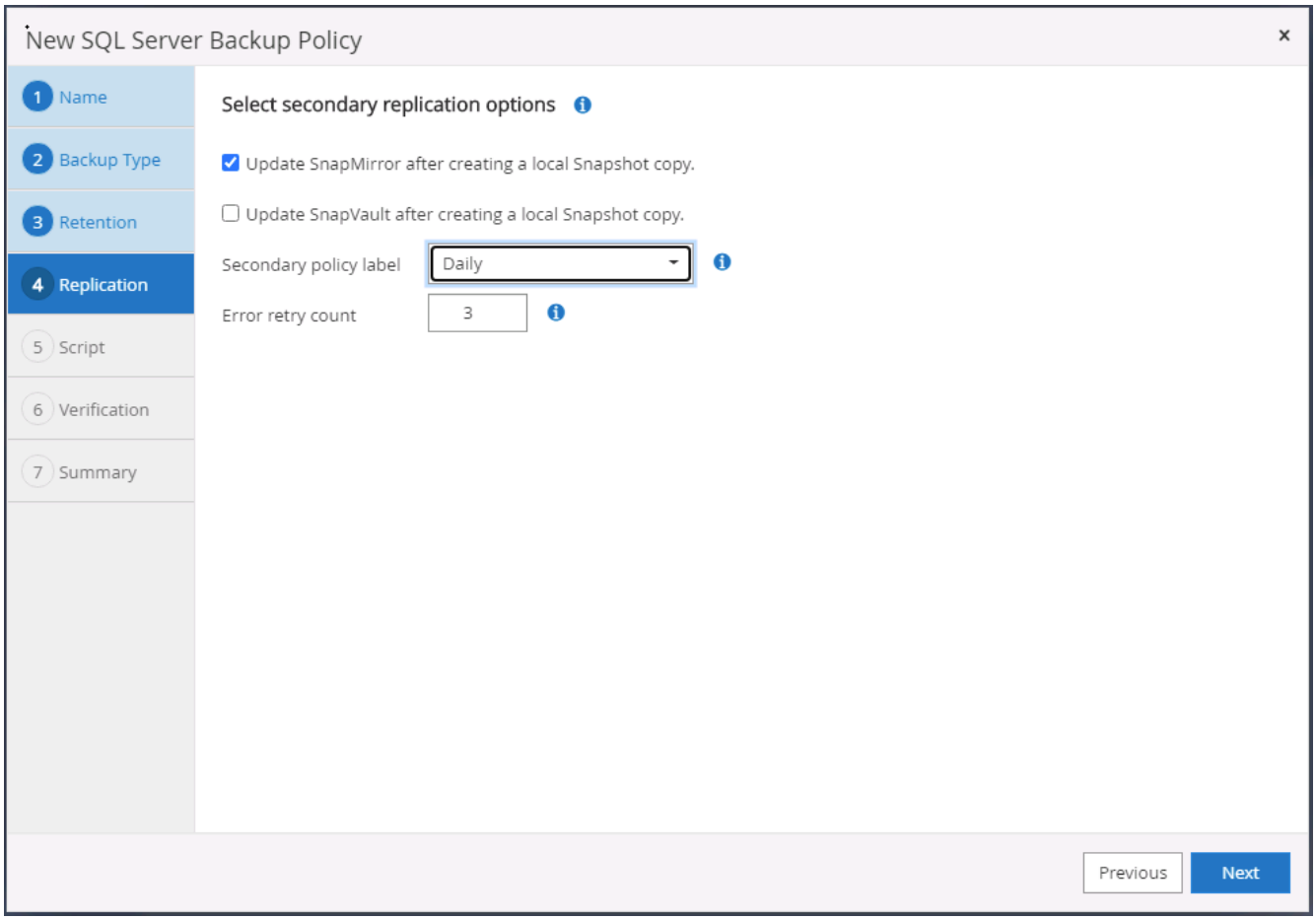
3. Definire l'opzione di backup e la frequenza di pianificazione. Per SQL Server configurato con un gruppo di disponibilità, è possibile impostare una replica di backup preferita.



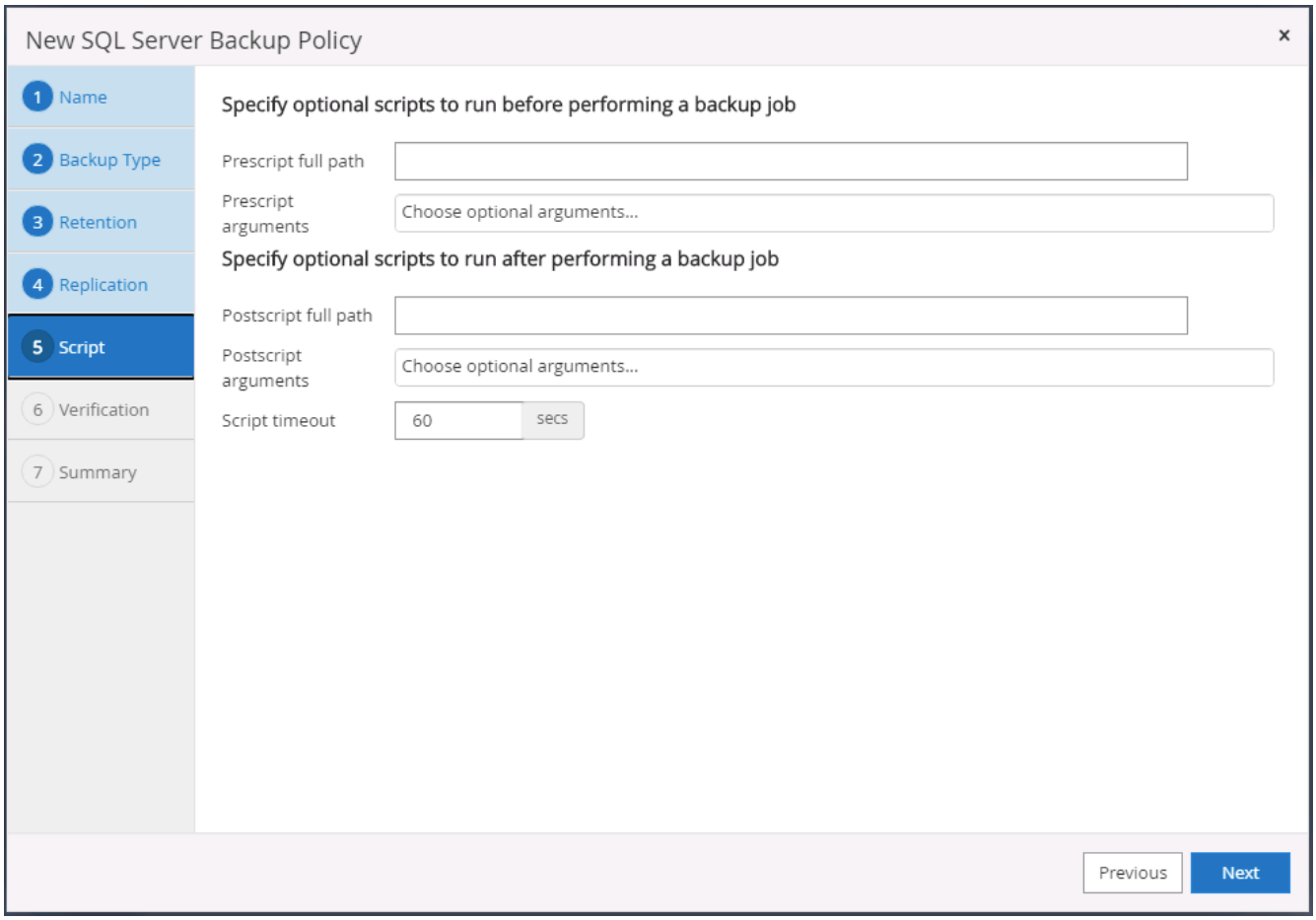
4. Impostare il periodo di conservazione del backup.



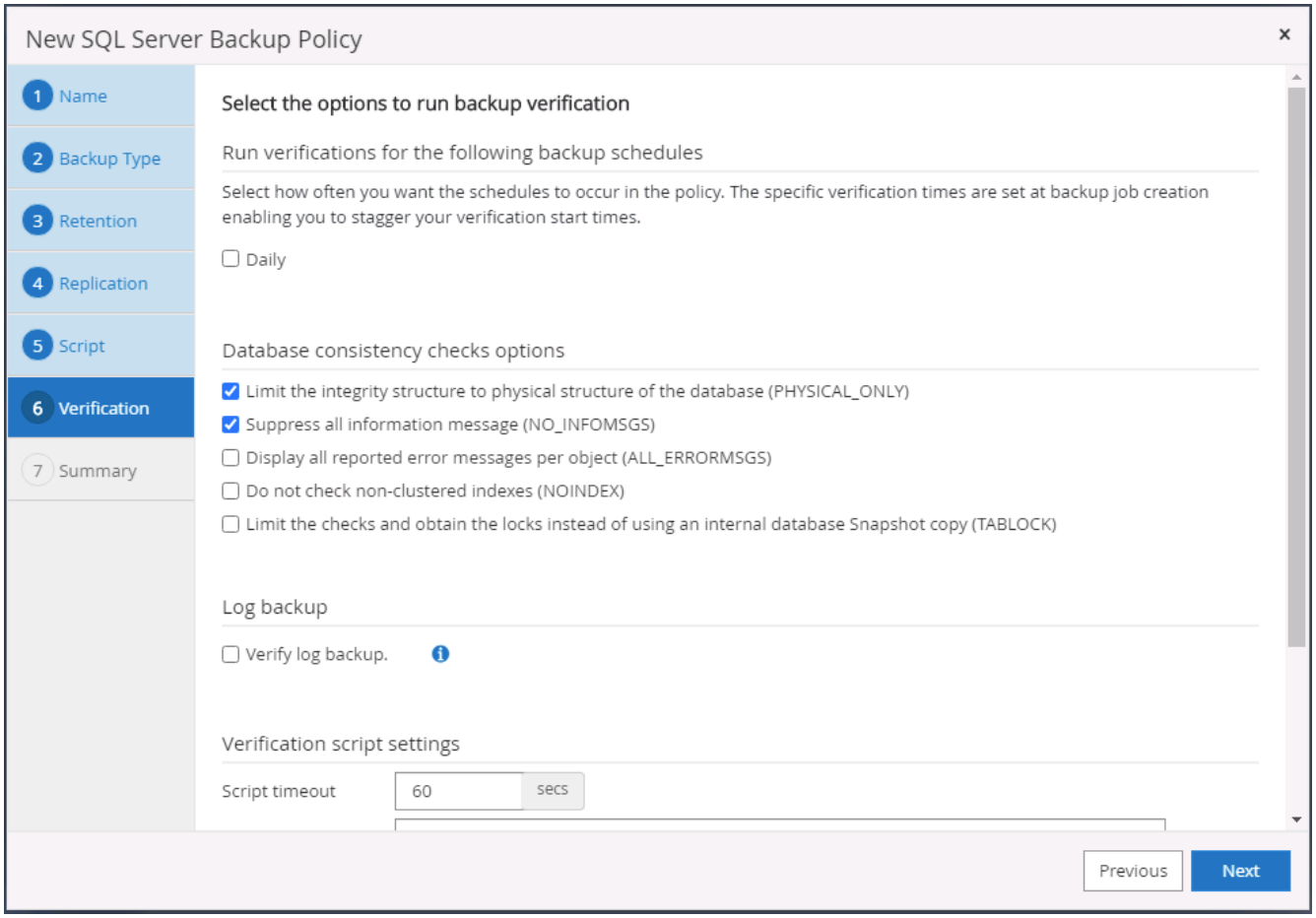
5. Abilitare la replica delle copie di backup in una posizione secondaria nel cloud.



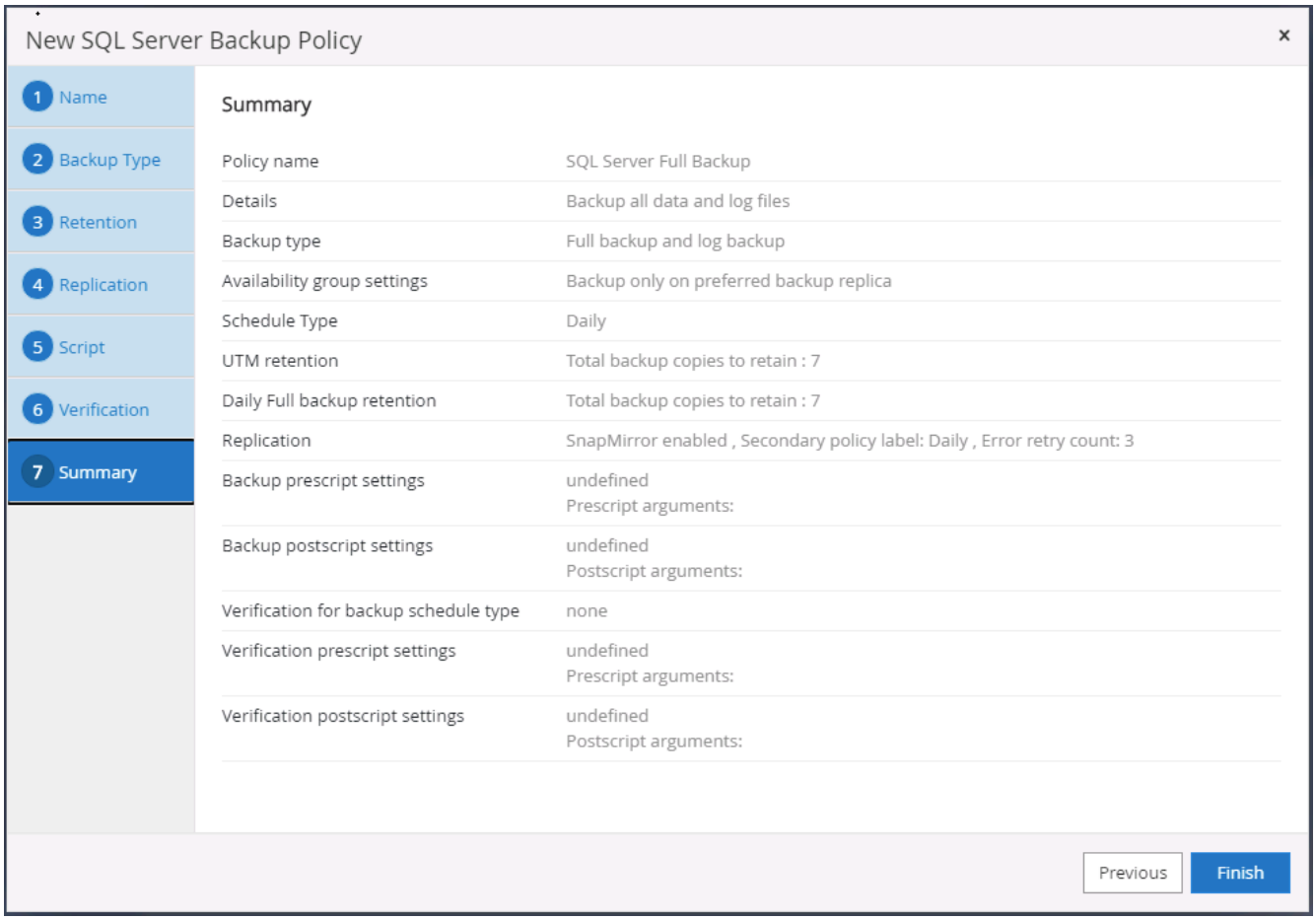
6. Specificare eventuali script opzionali da eseguire prima o dopo un processo di backup.



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

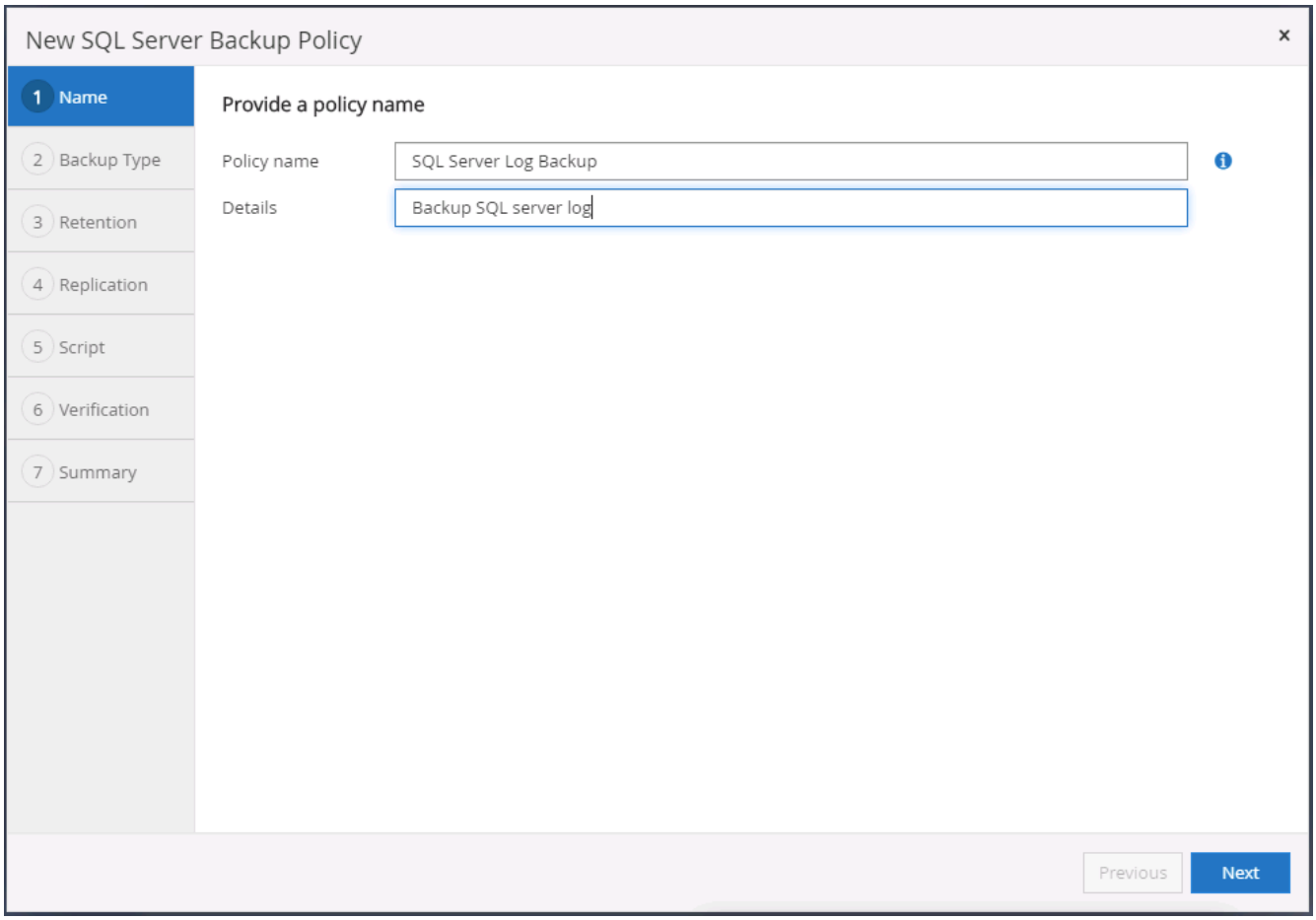

New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run verifications for the following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times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

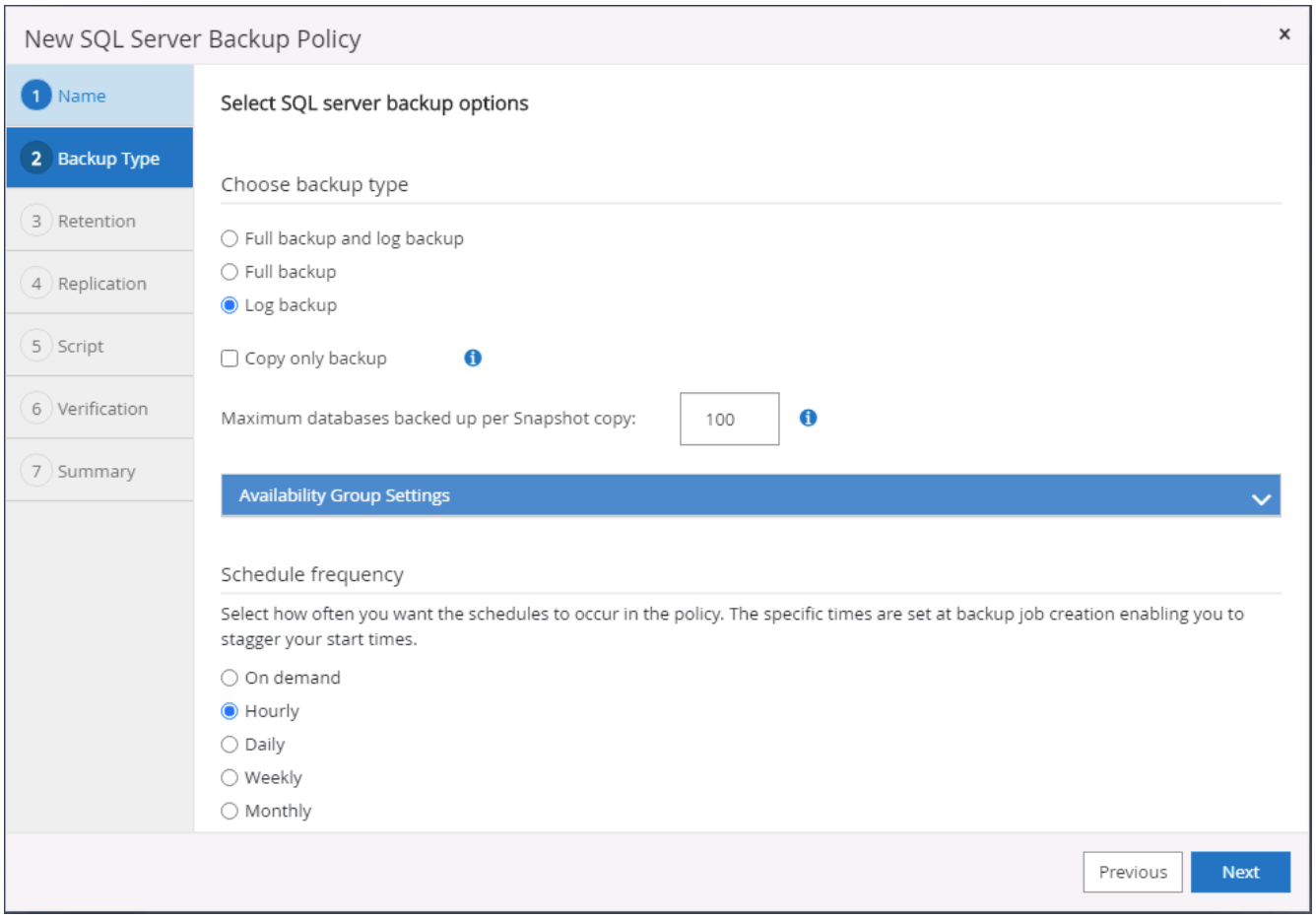


Creare un criterio di backup del log del database per SQL.

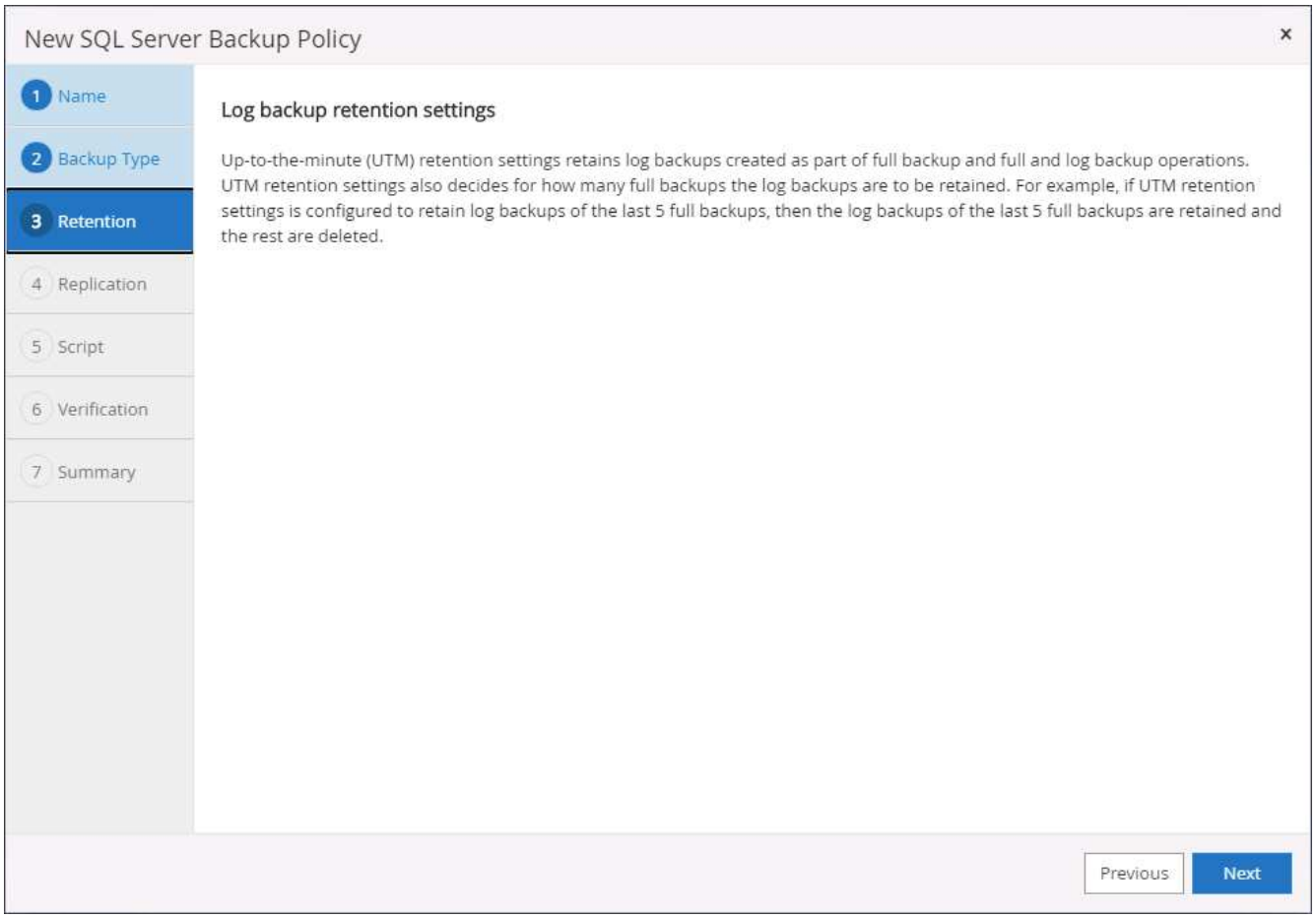
1. Accedere a SnapCenter con un ID utente per la gestione del database, fare clic su Impostazioni > Criteri, quindi su nuovo per avviare un nuovo flusso di lavoro per la creazione di policy.



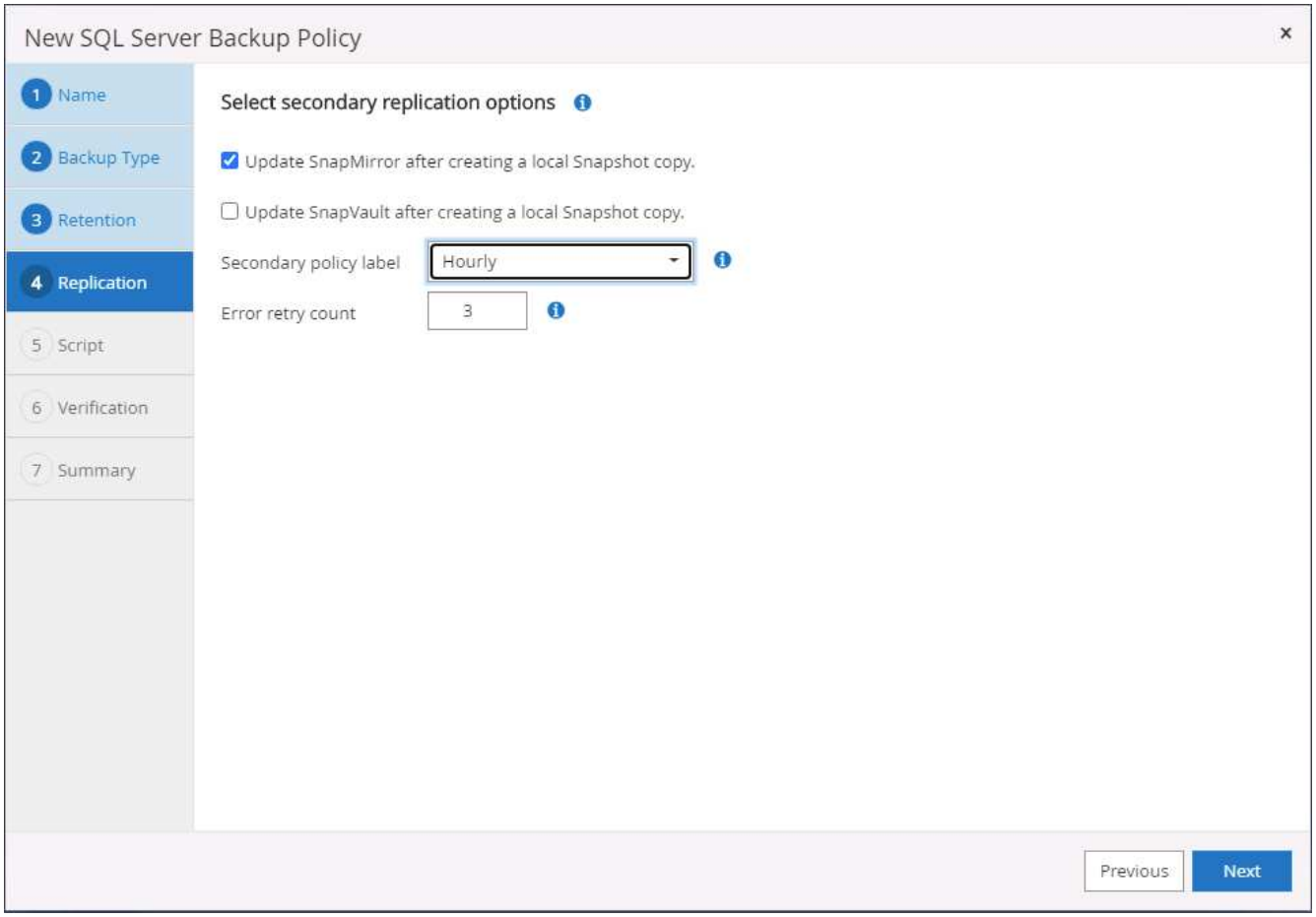
2. Definire l'opzione di backup del registro e la frequenza di pianificazione. Per SQL Server configurato con un gruppo di disponibilità, è possibile impostare una replica di backup preferita.



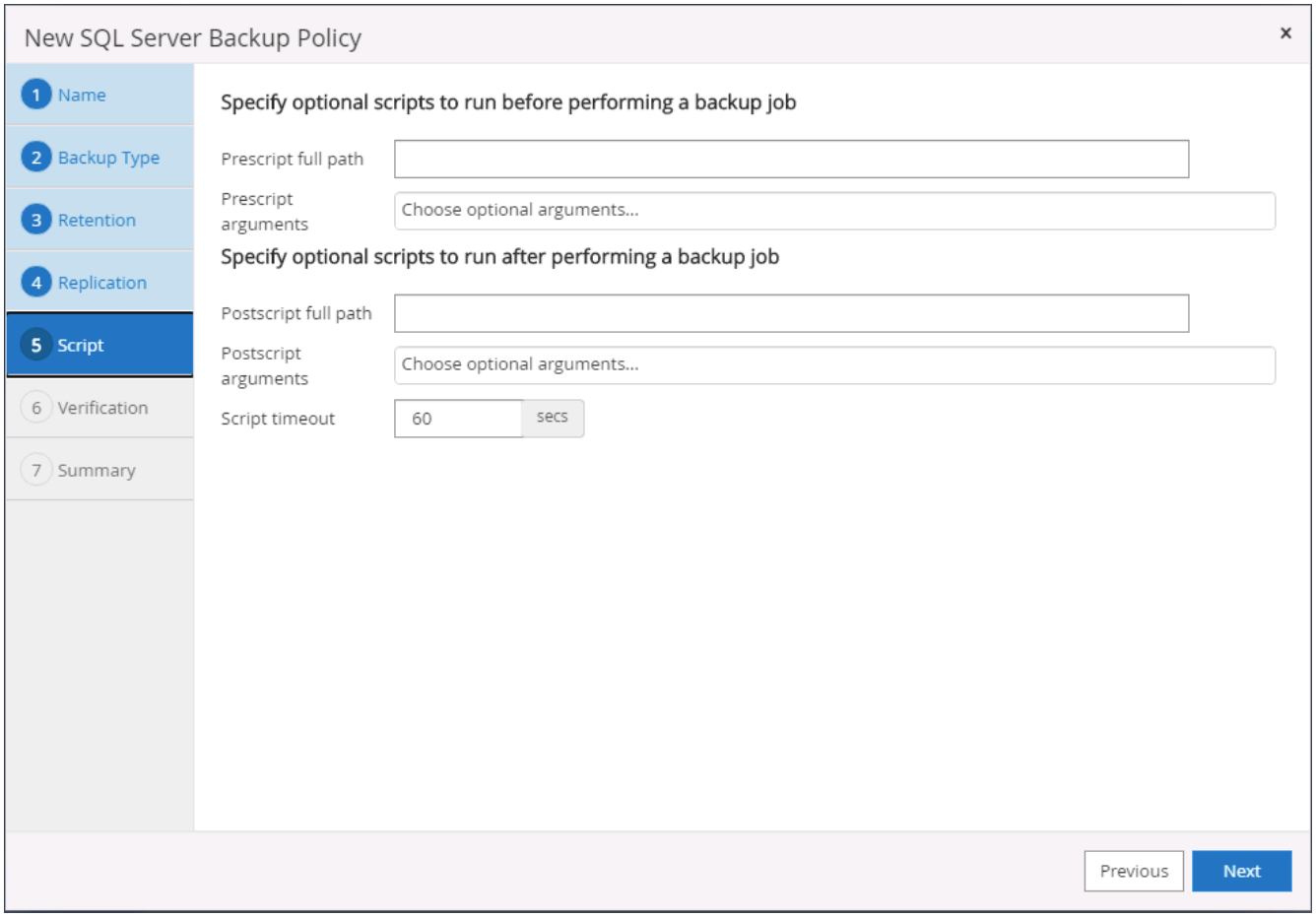
3. Il criterio di backup dei dati di SQL Server definisce la conservazione del backup del registro; accettare i valori predefiniti qui.



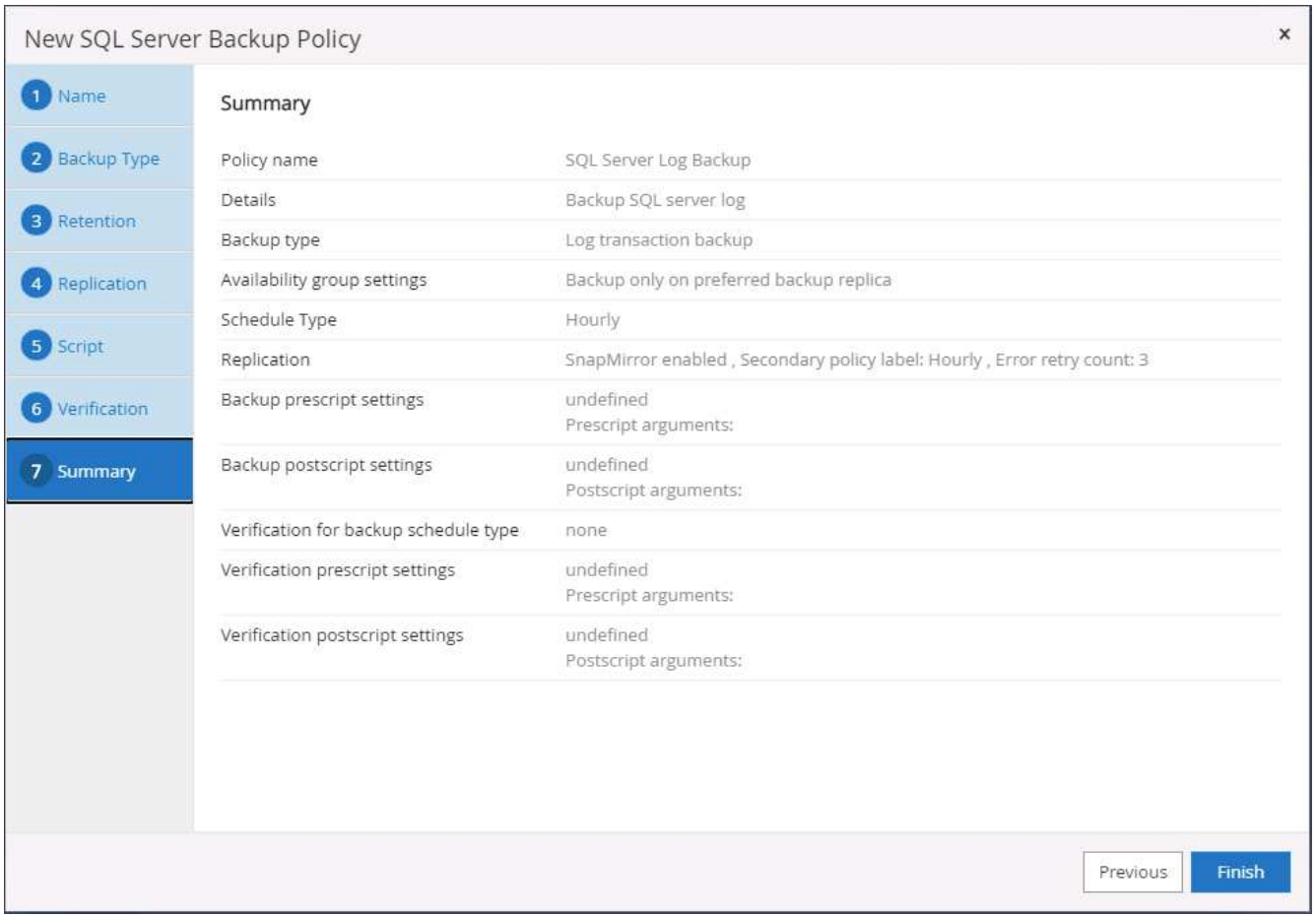
4. Abilitare la replica del backup dei log su secondario nel cloud.



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.

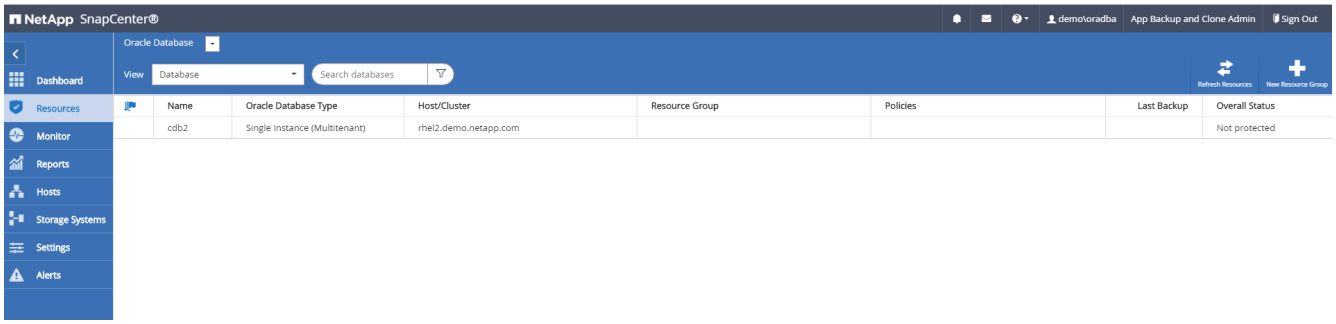


8. Implementare policy di backup per proteggere il database

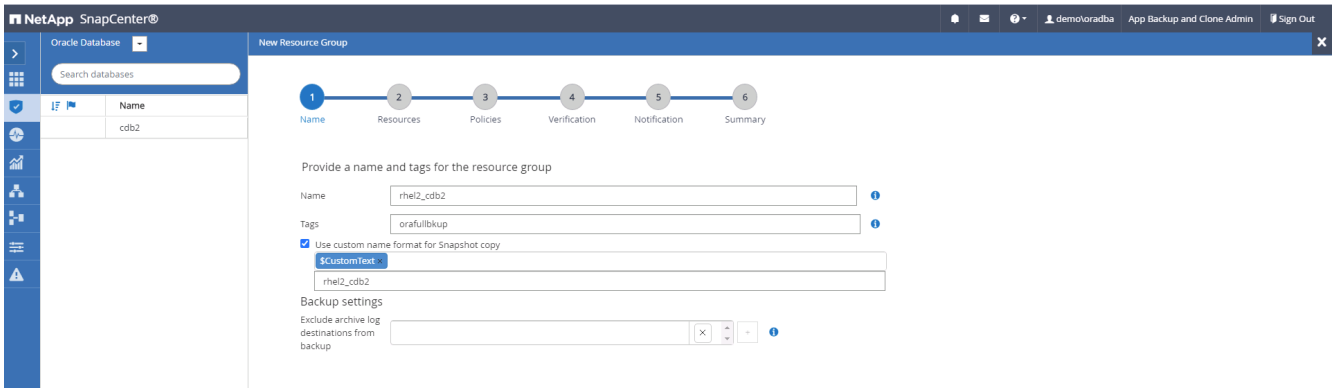
SnapCenter utilizza un gruppo di risorse per eseguire il backup di un database in un gruppo logico di risorse di database, ad esempio più database ospitati su un server, un database che condivide gli stessi volumi di storage, più database che supportano un'applicazione di business e così via. La protezione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

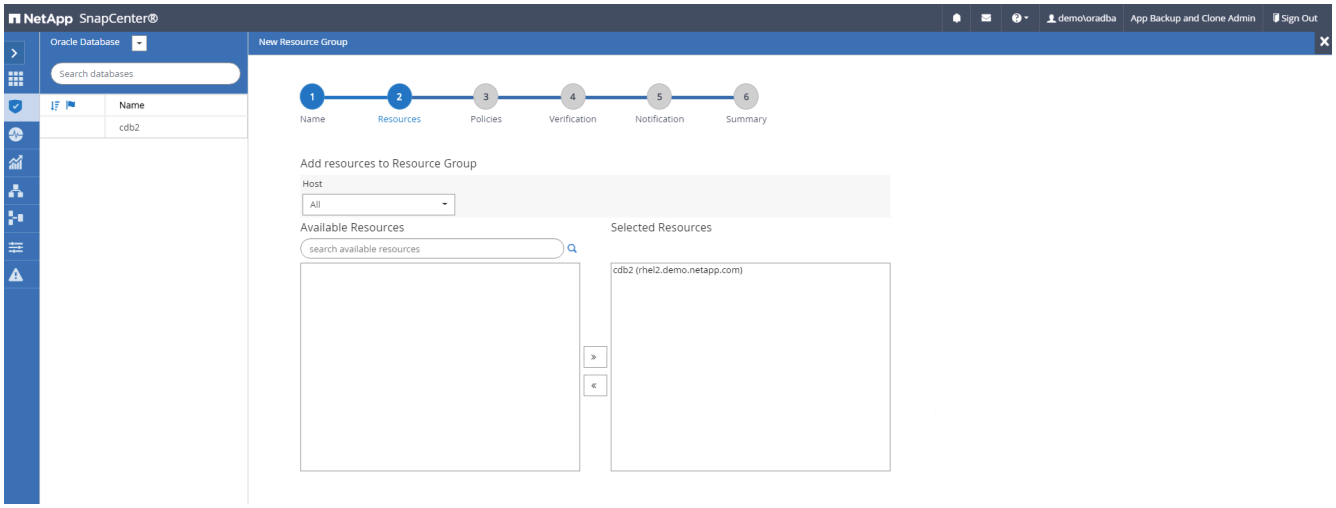
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.



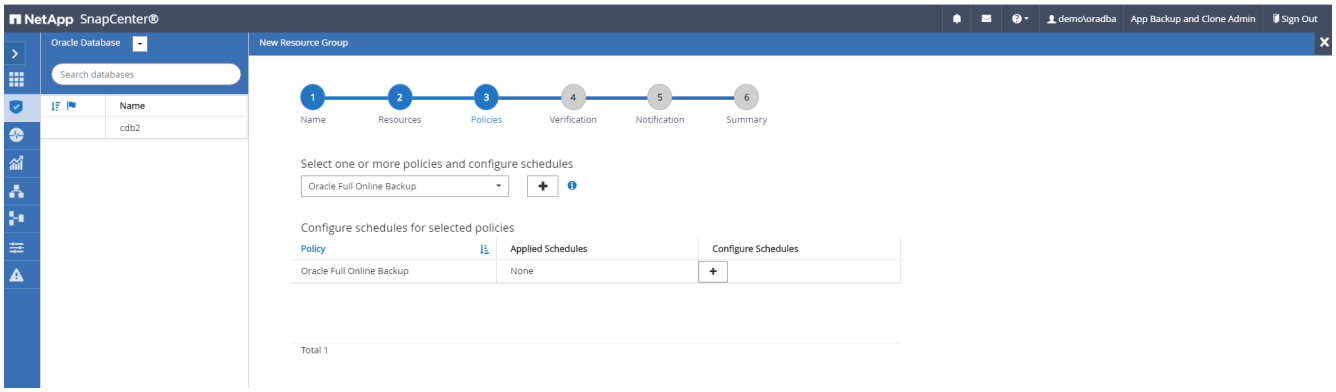
2. Fornire un nome e tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archiviazione ridondante, se configurata.



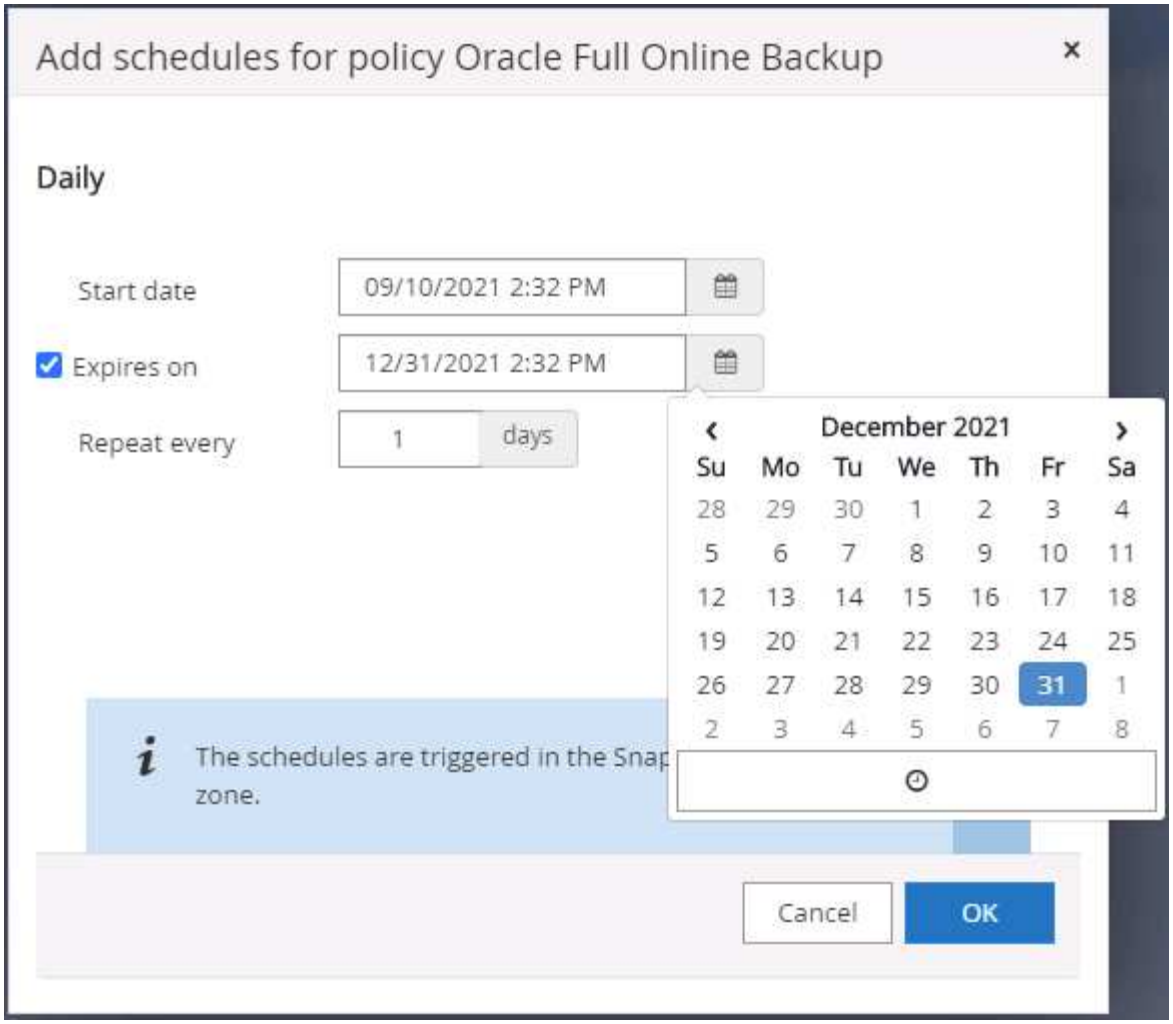
3. Aggiungere risorse di database al gruppo di risorse.



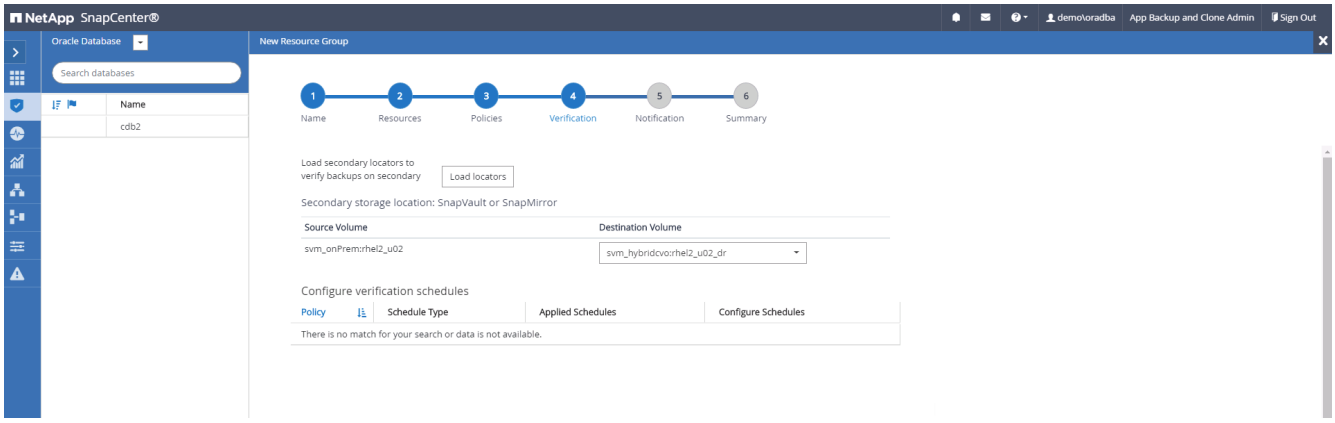
4. Selezionare una policy di backup completa creata nella sezione 7 dall'elenco a discesa.



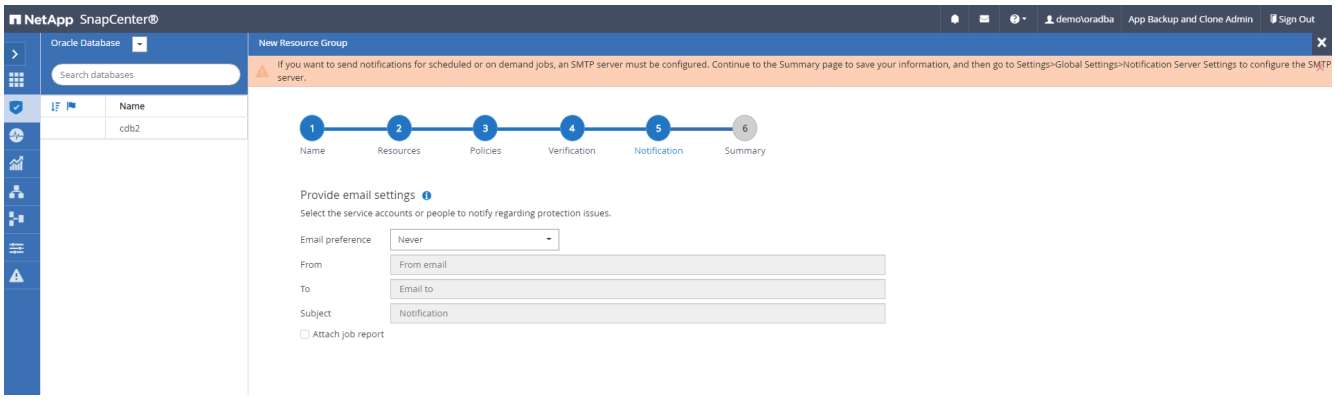
5. Fare clic sul segno (+) per configurare la pianificazione di backup desiderata.



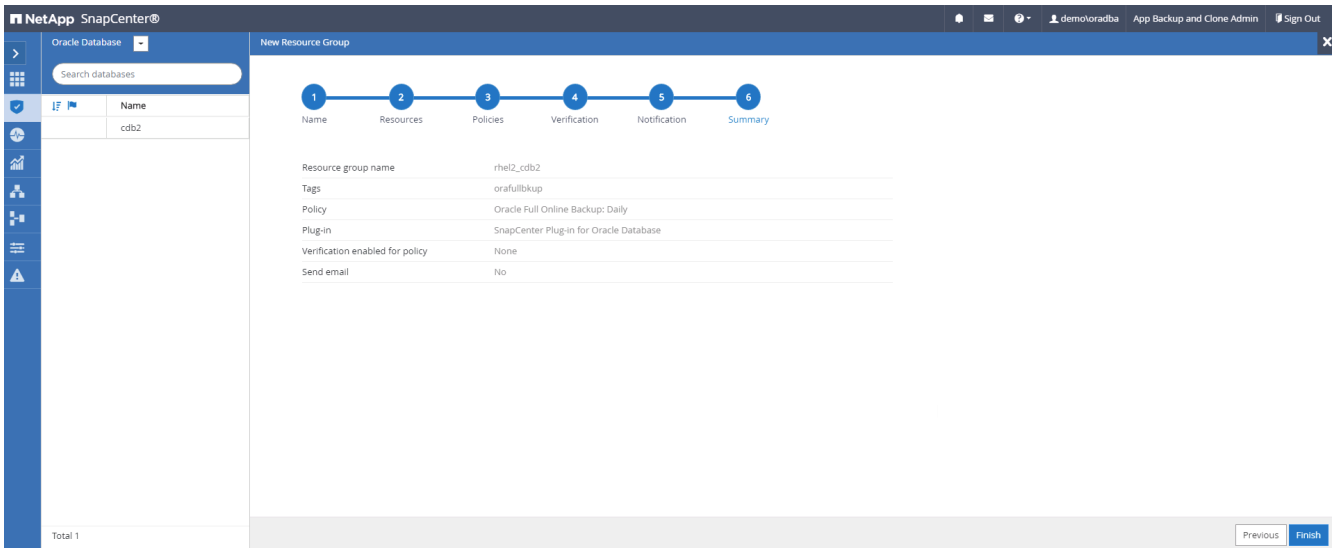
6. Fare clic su Load Locators (carica locatori) per caricare il volume di origine e di destinazione.



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

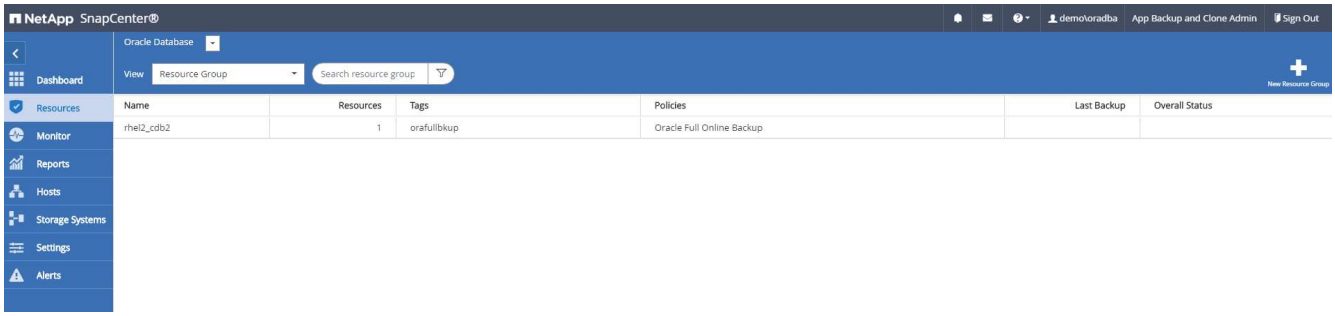


8. Riepilogo.

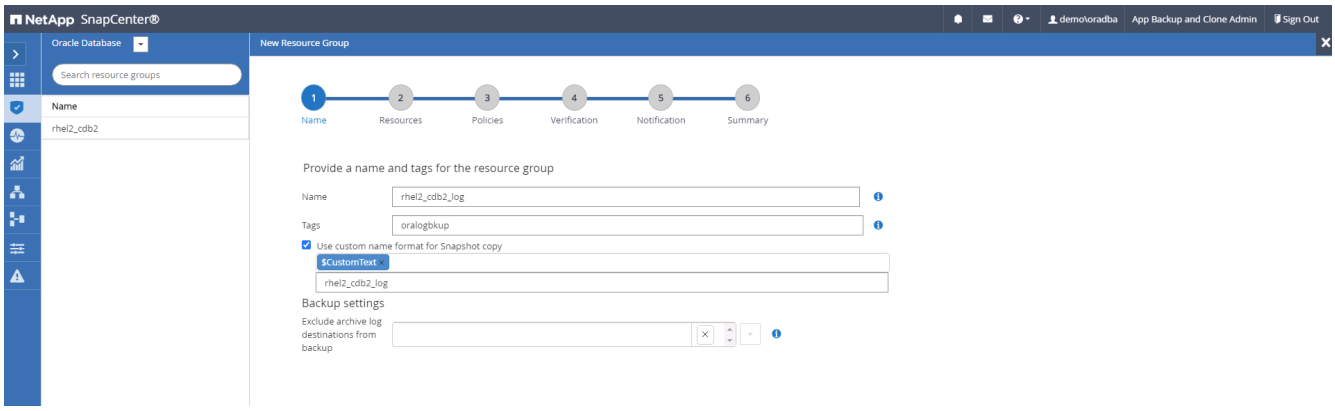


Creare un gruppo di risorse per il backup dei log di Oracle

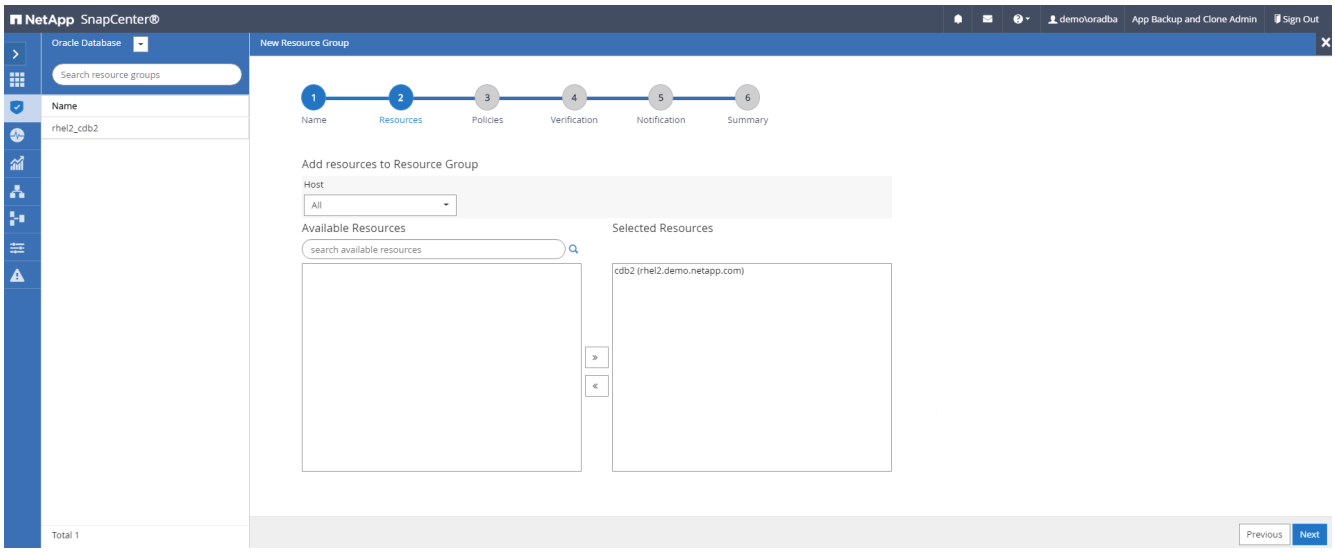
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.



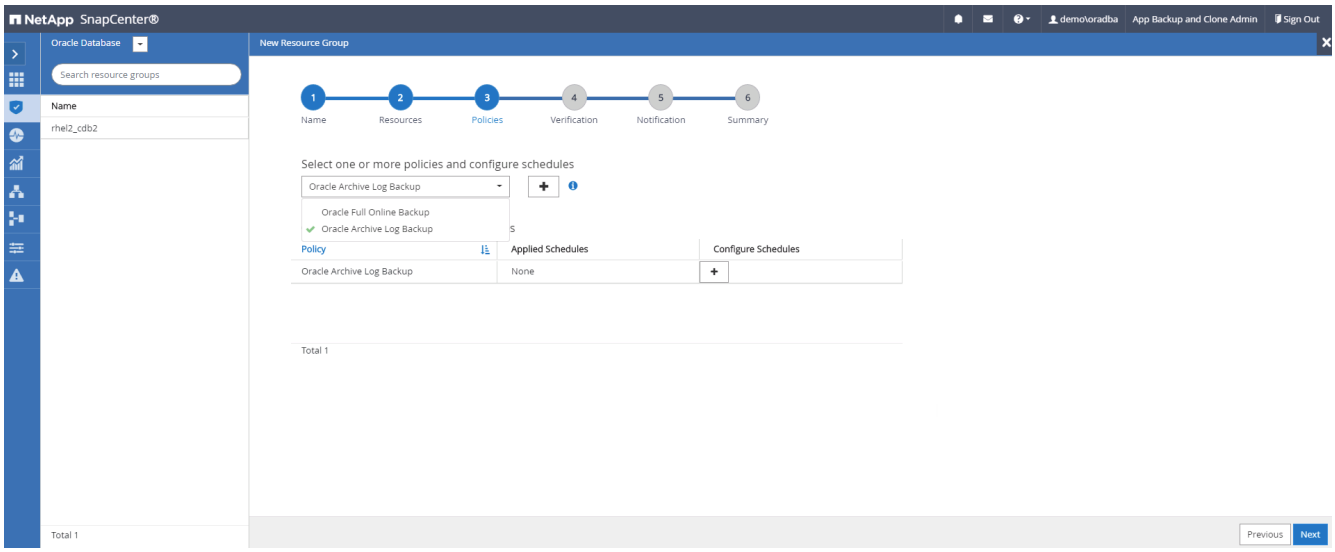
2. Fornire un nome e tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archiviazione ridondante, se configurata.



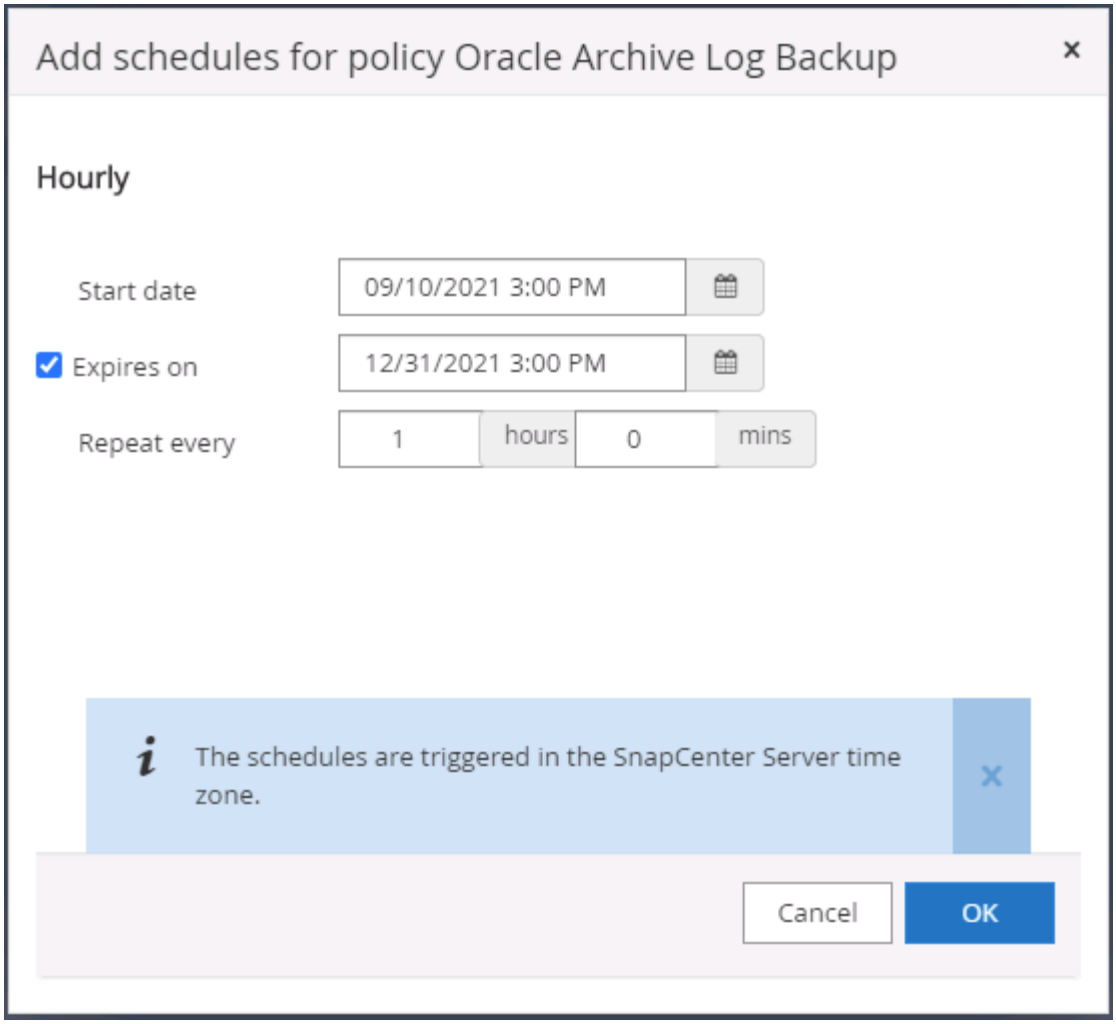
3. Aggiungere risorse di database al gruppo di risorse.



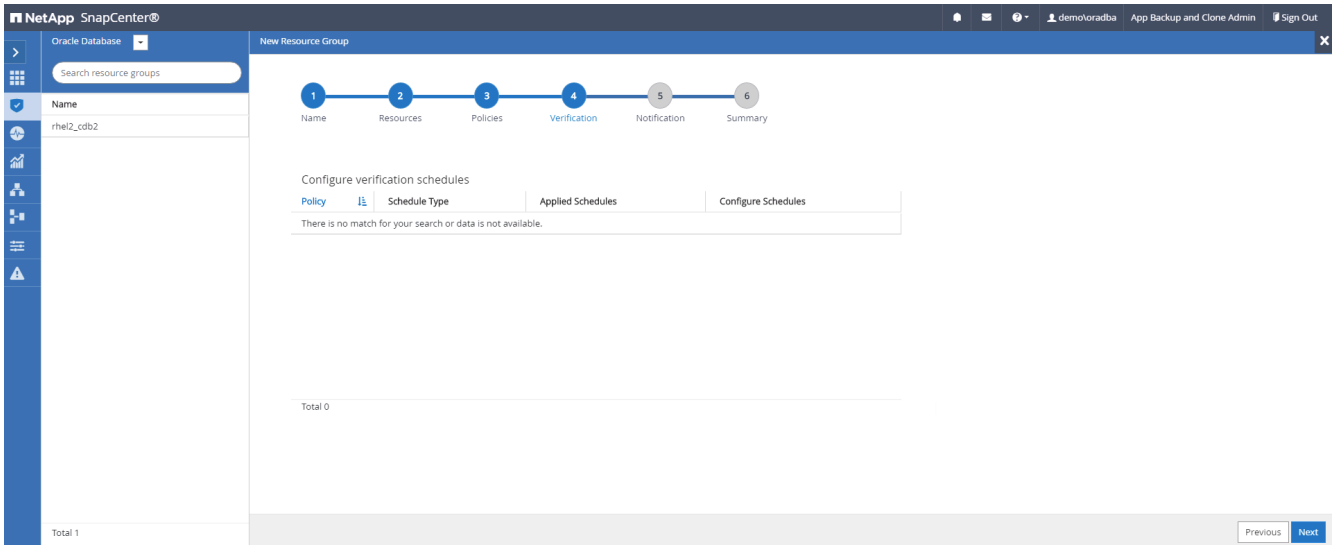
4. Selezionare un criterio di backup del registro creato nella sezione 7 dall'elenco a discesa.



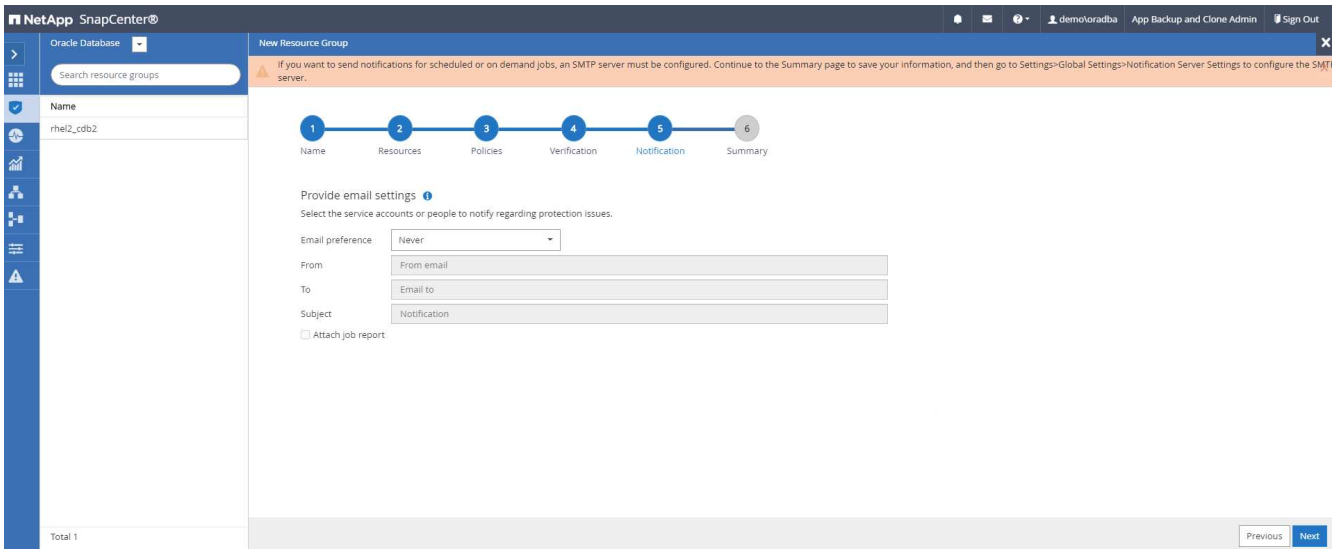
5. Fare clic sul segno (+) per configurare la pianificazione di backup desiderata.



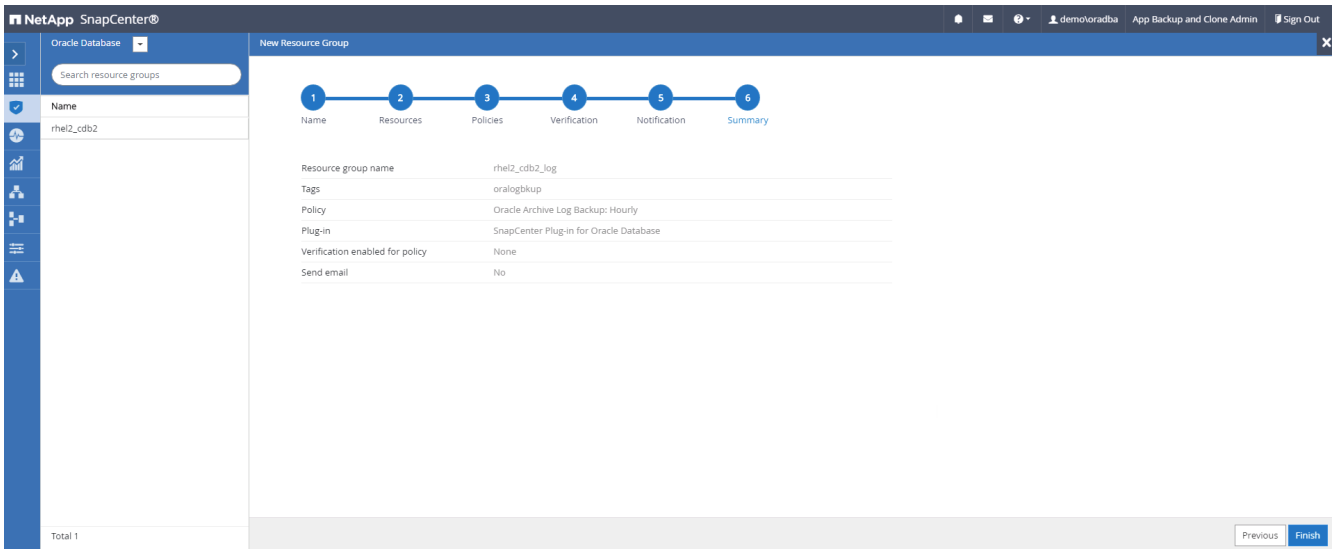
6. Se la verifica del backup è configurata, viene visualizzata qui.



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

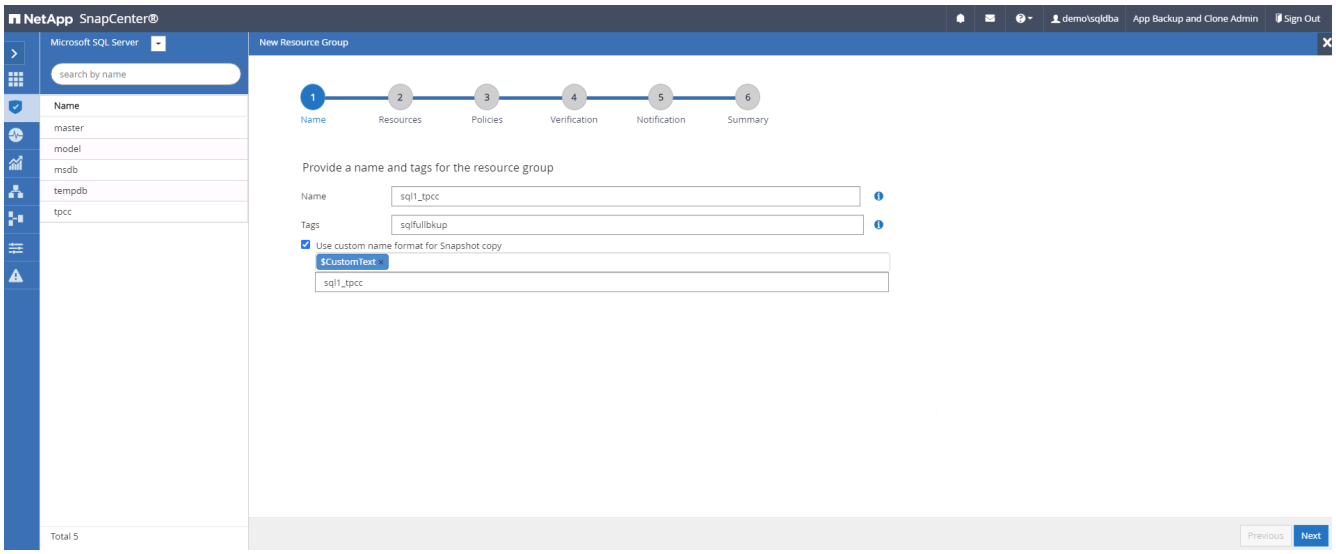


8. Riepilogo.

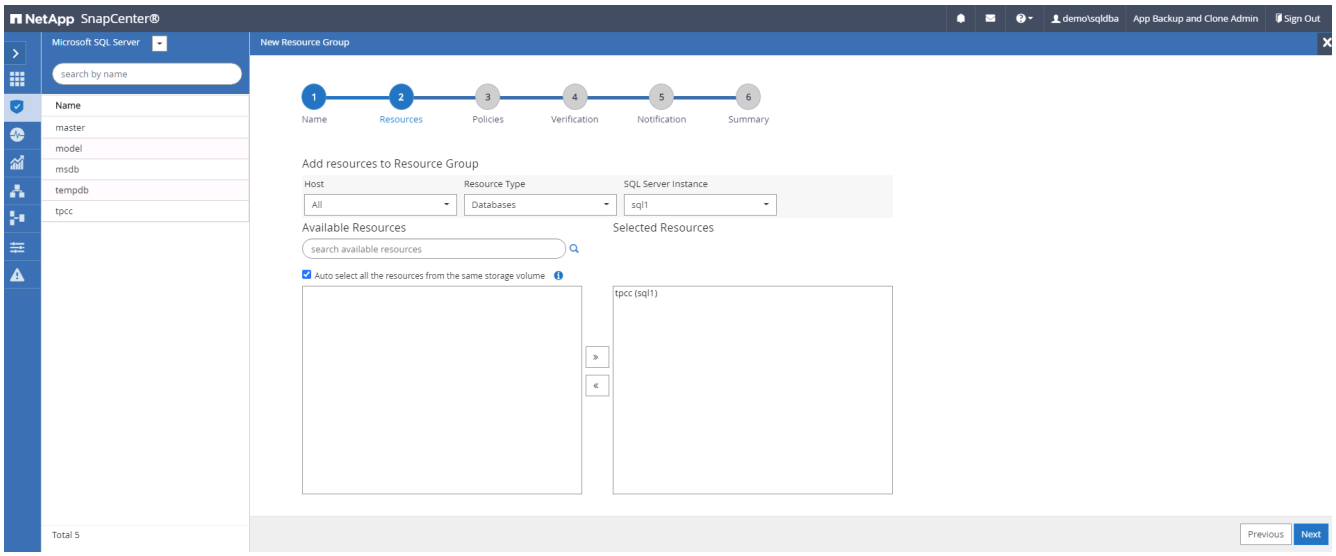


Creare un gruppo di risorse per il backup completo di SQL Server

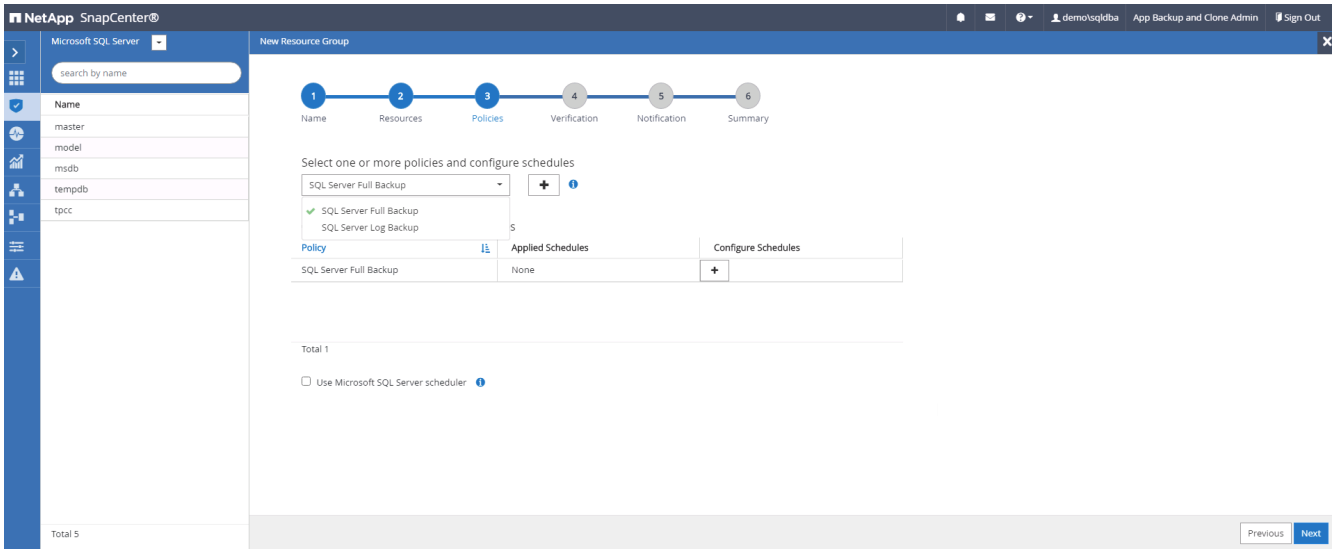
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire un nome e tag per il gruppo di risorse. È possibile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



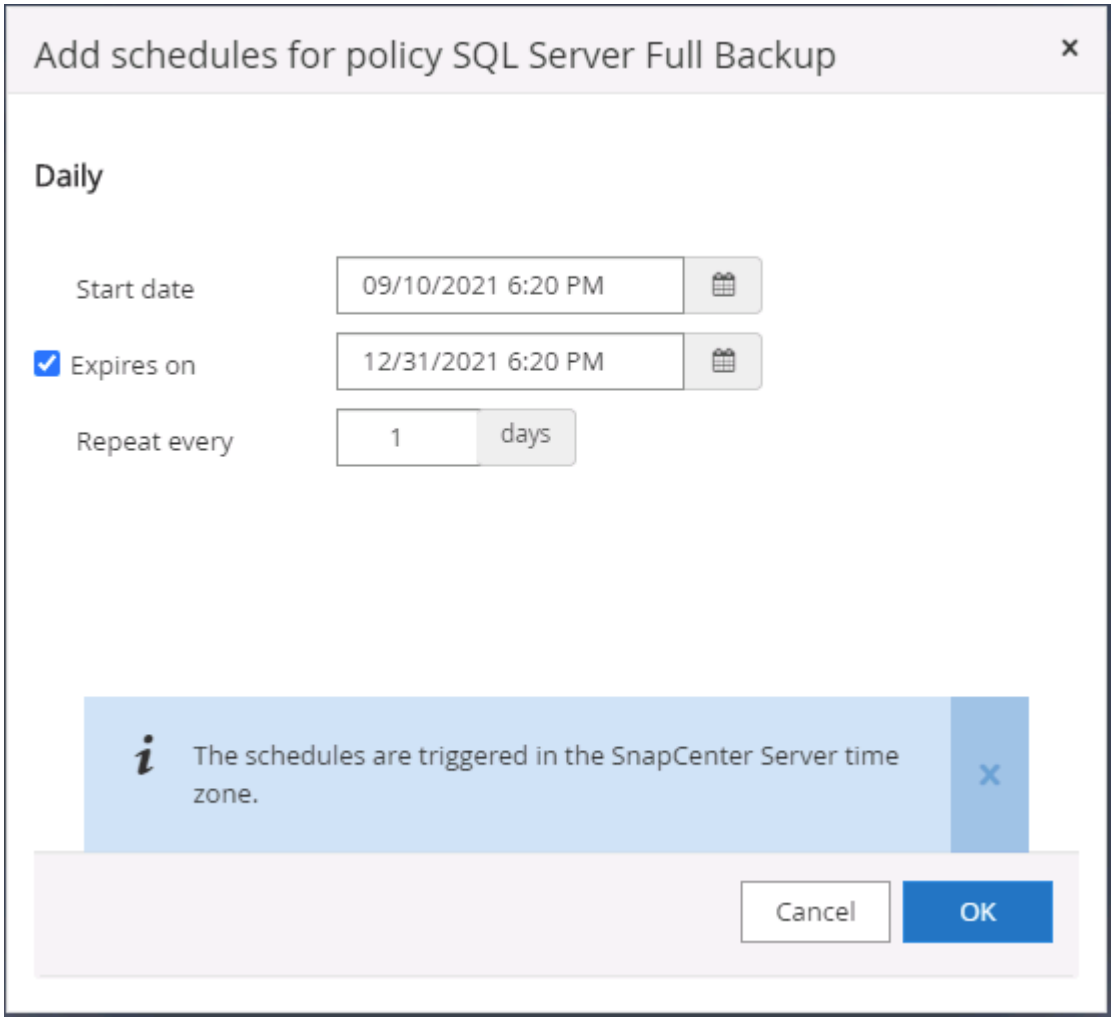
2. Selezionare le risorse di database di cui eseguire il backup.



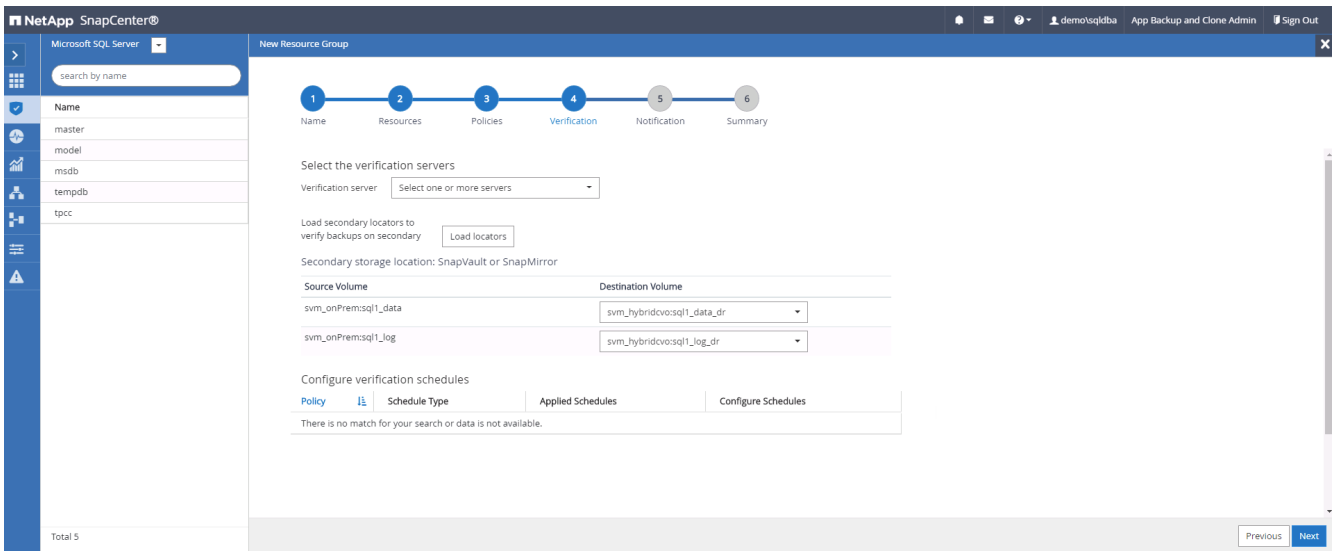
3. Selezionare una policy di backup SQL completa creata nella sezione 7.



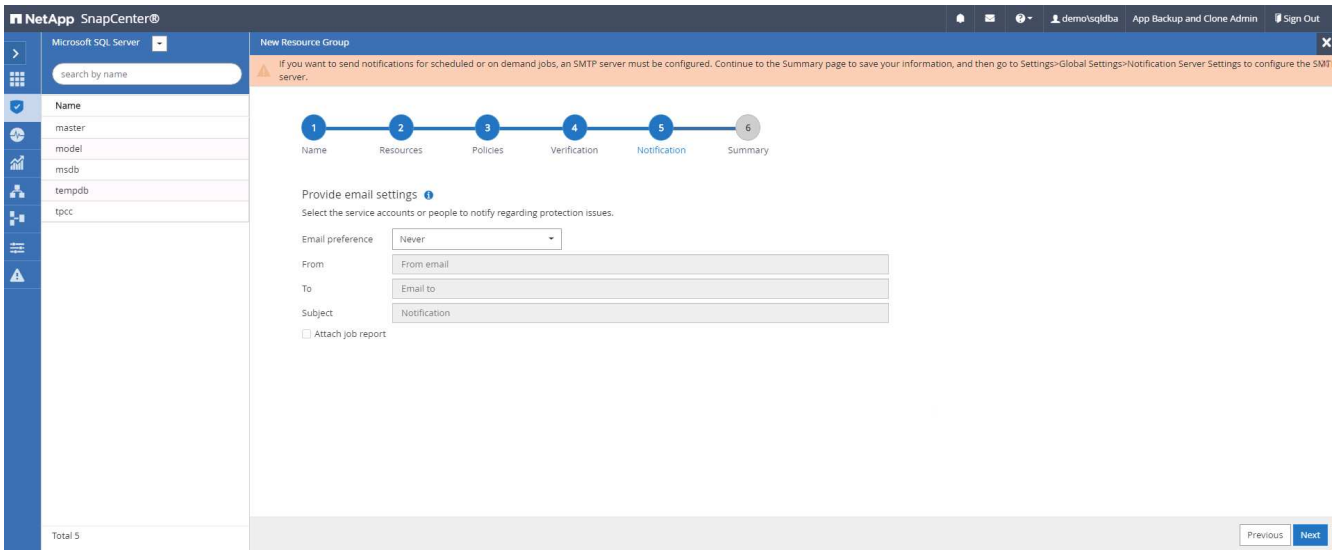
4. Aggiungi tempi esatti per i backup e la frequenza.



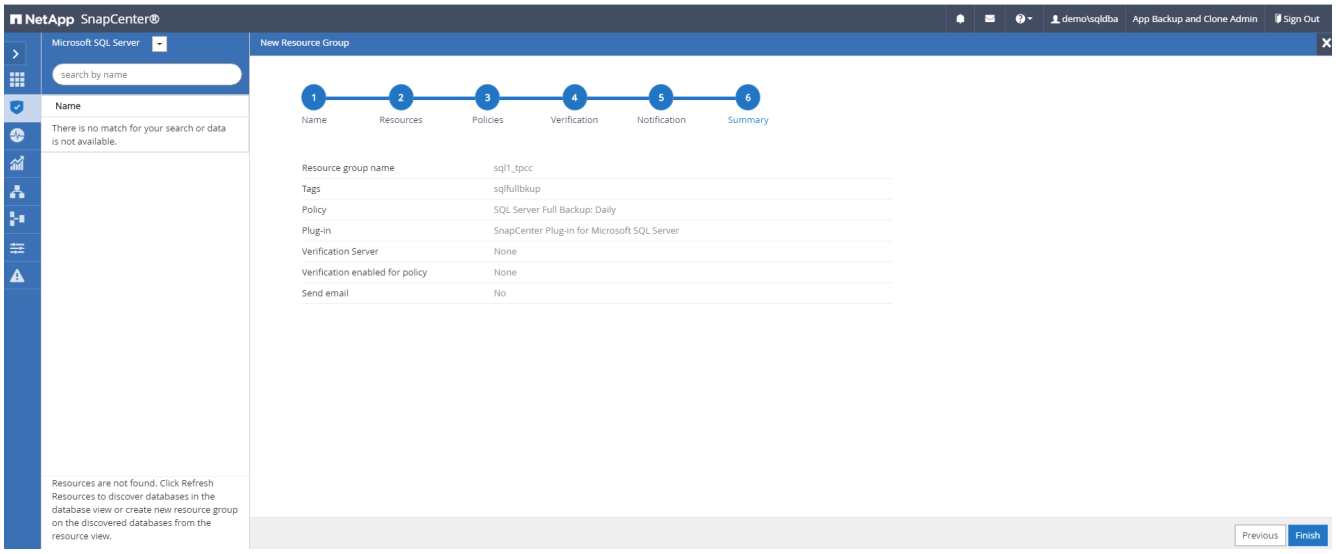
5. Scegliere il server di verifica per il backup su secondario se deve essere eseguita la verifica del backup. Fare clic su Load Locator (carica localizzatore) per popolare la posizione dello storage secondario.



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

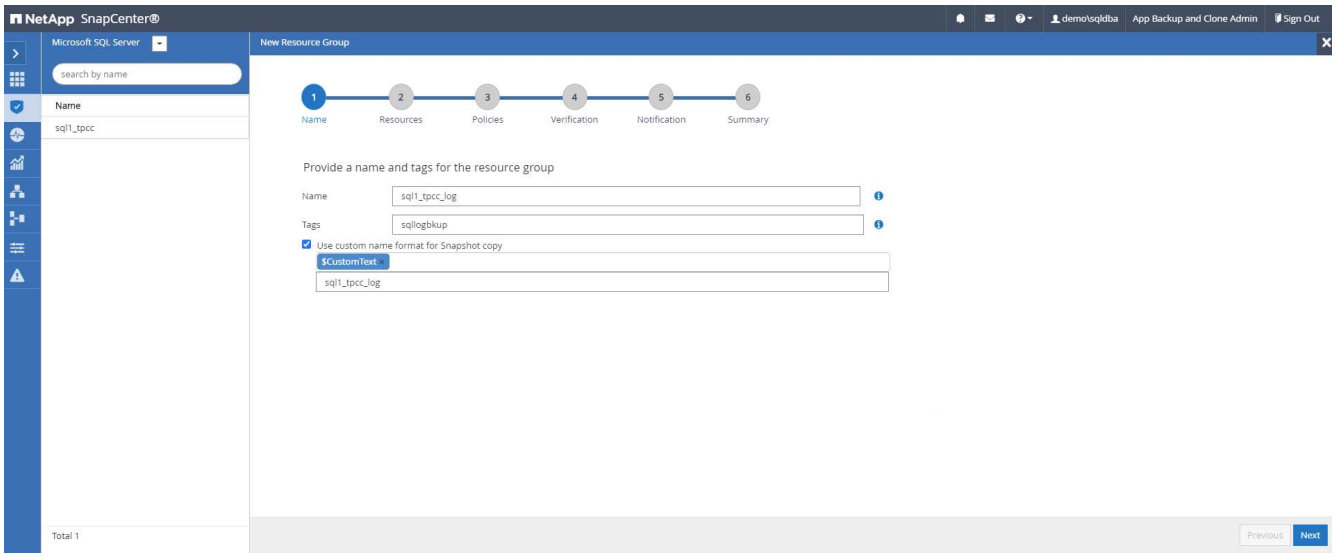


7. Riepilogo.

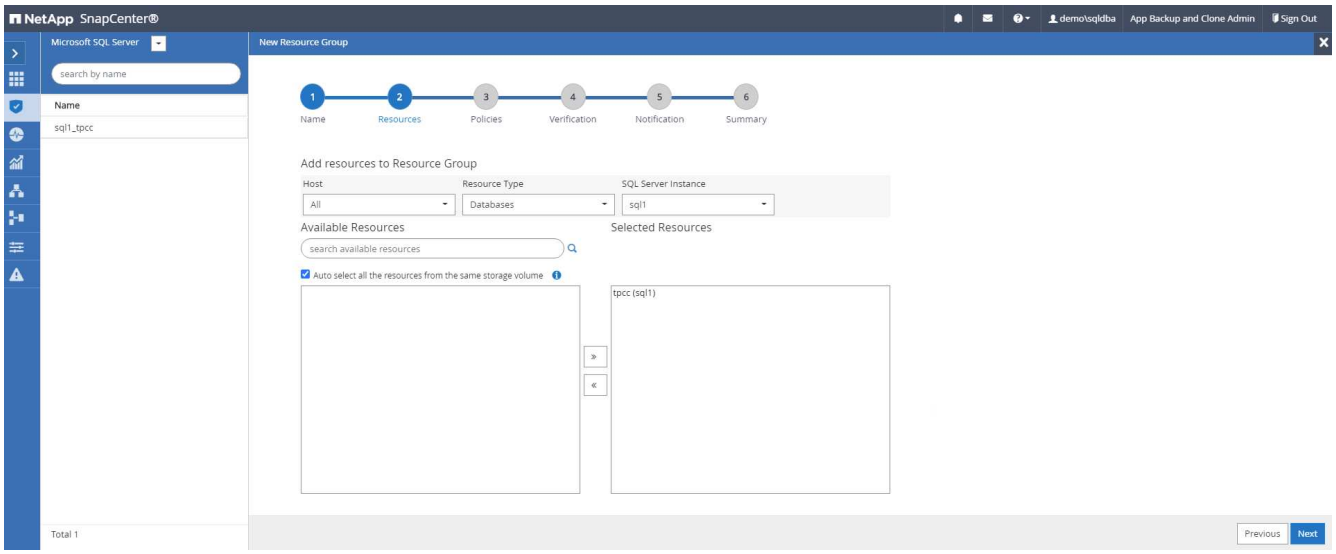


Creare un gruppo di risorse per il backup del log di SQL Server

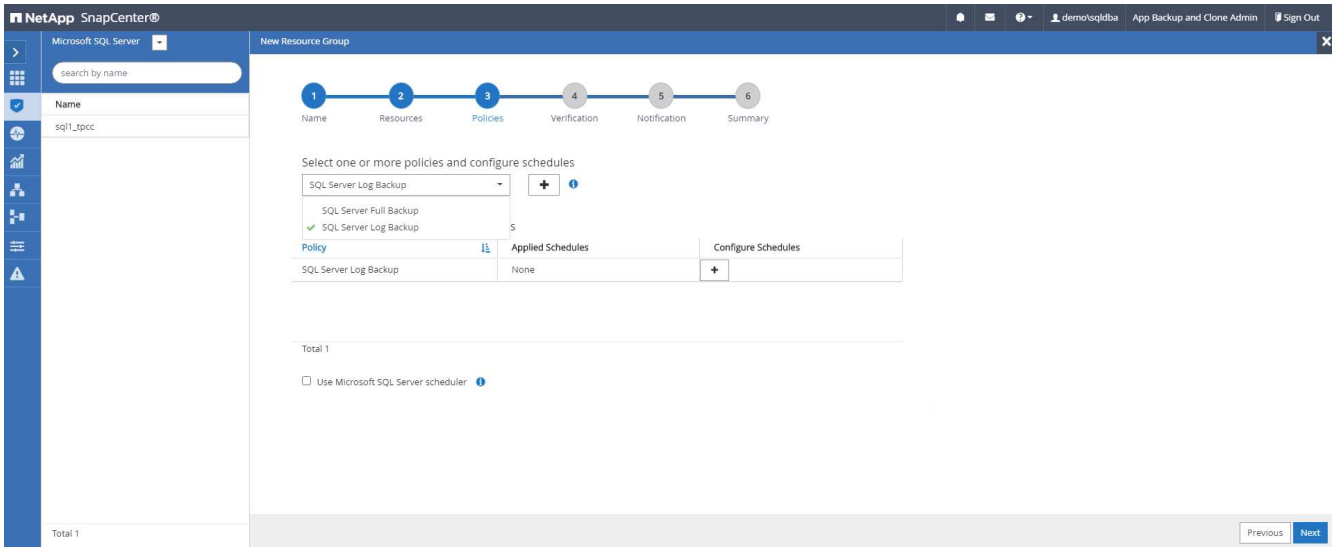
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire il nome e i tag per il gruppo di risorse. È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



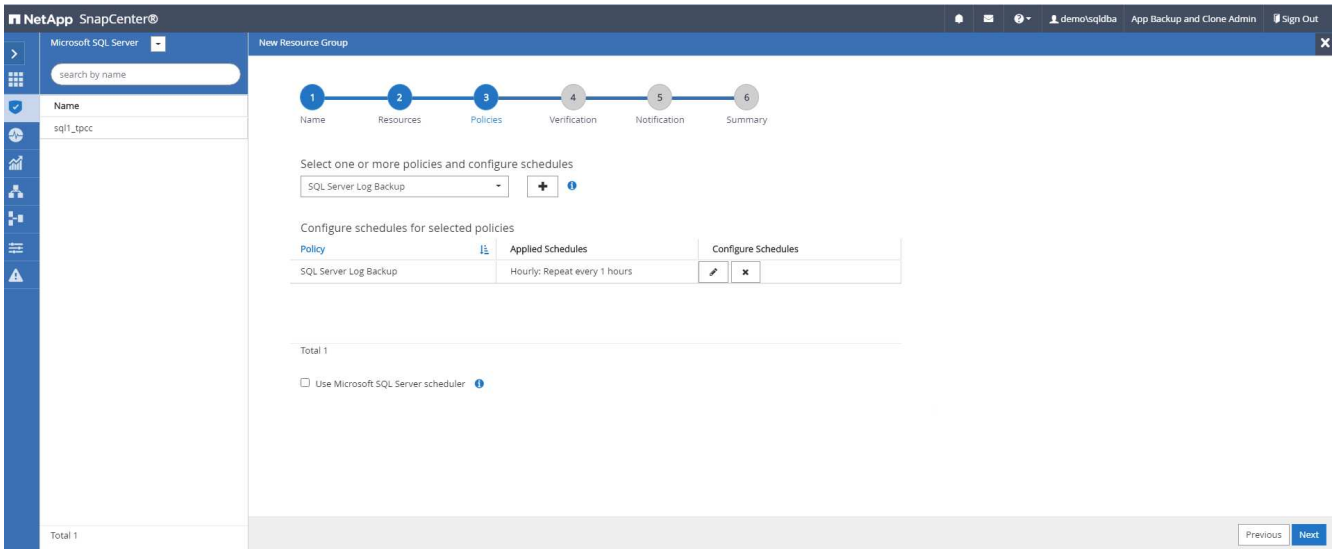
2. Selezionare le risorse di database di cui eseguire il backup.



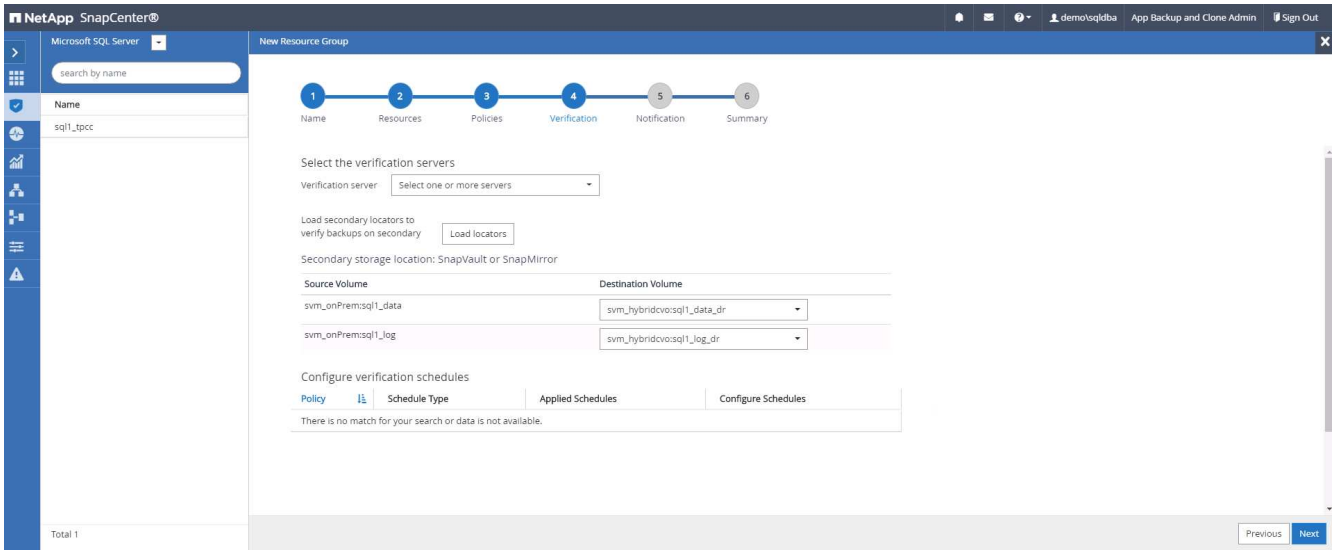
3. Selezionare un criterio di backup del registro SQL creato nella sezione 7.



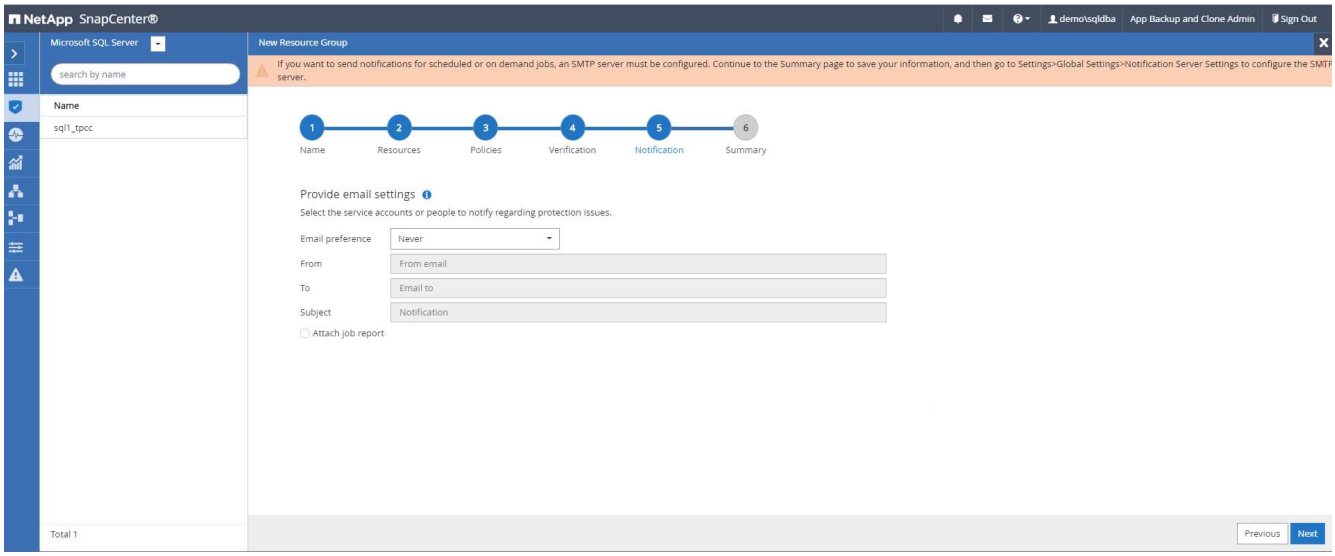
4. Aggiungere la tempistica esatta per il backup e la frequenza.



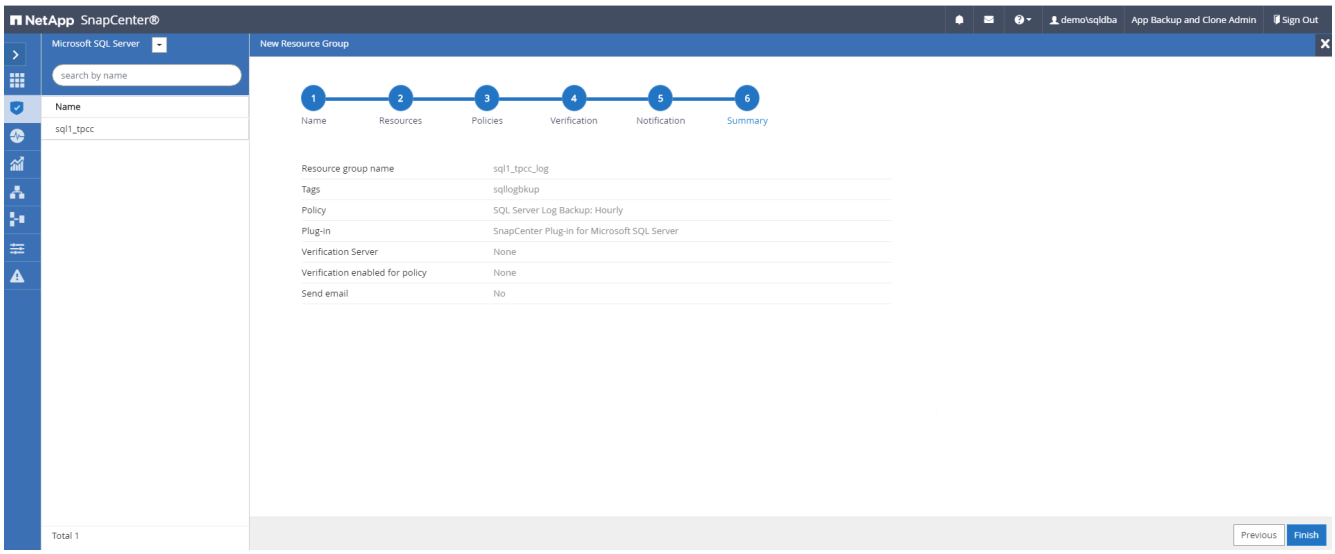
5. Scegliere il server di verifica per il backup su secondario se deve essere eseguita la verifica del backup. Fare clic su Load Locator per popolare la posizione dello storage secondario.



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

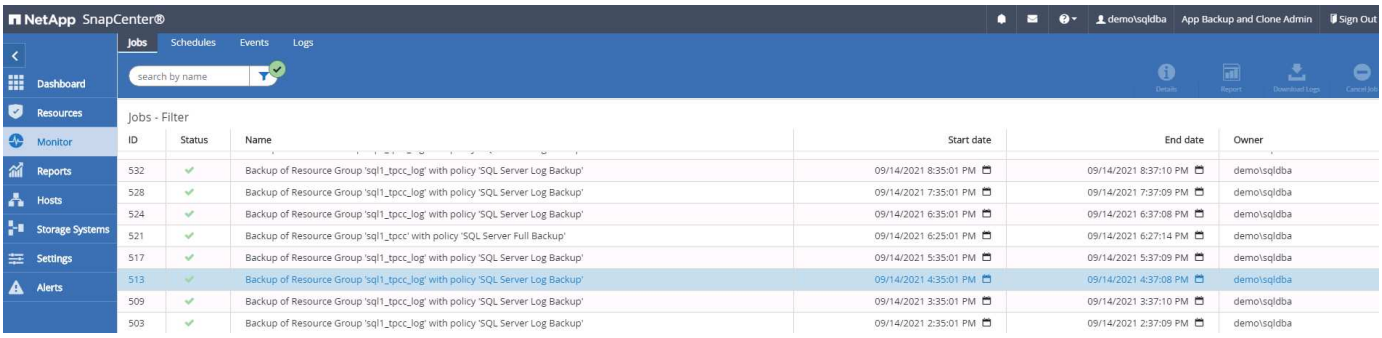


7. Riepilogo.



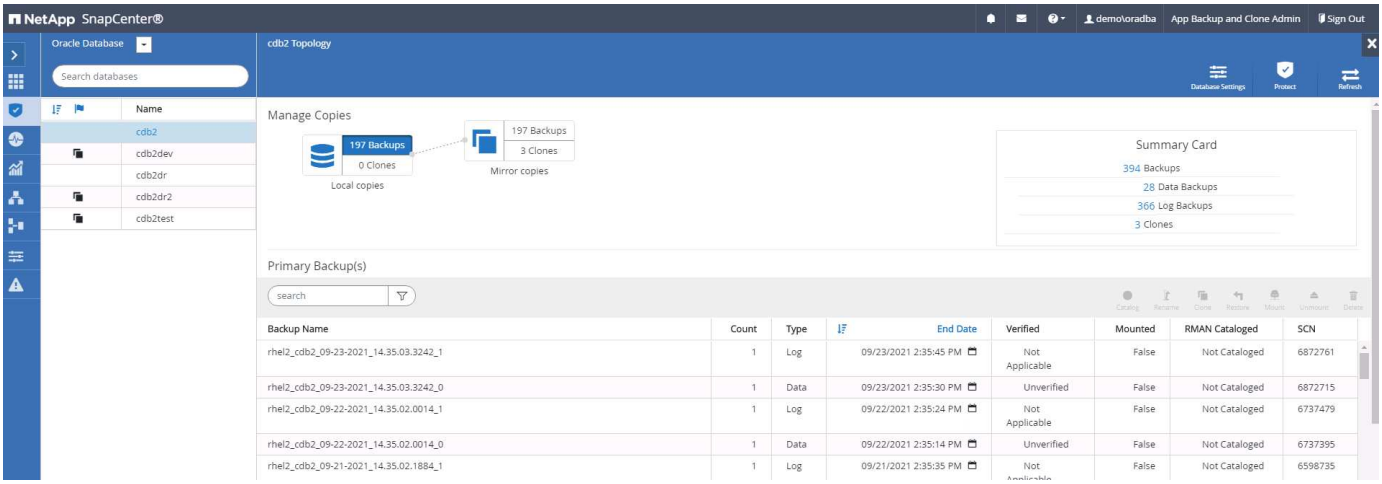
9. Convalidare il backup

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:

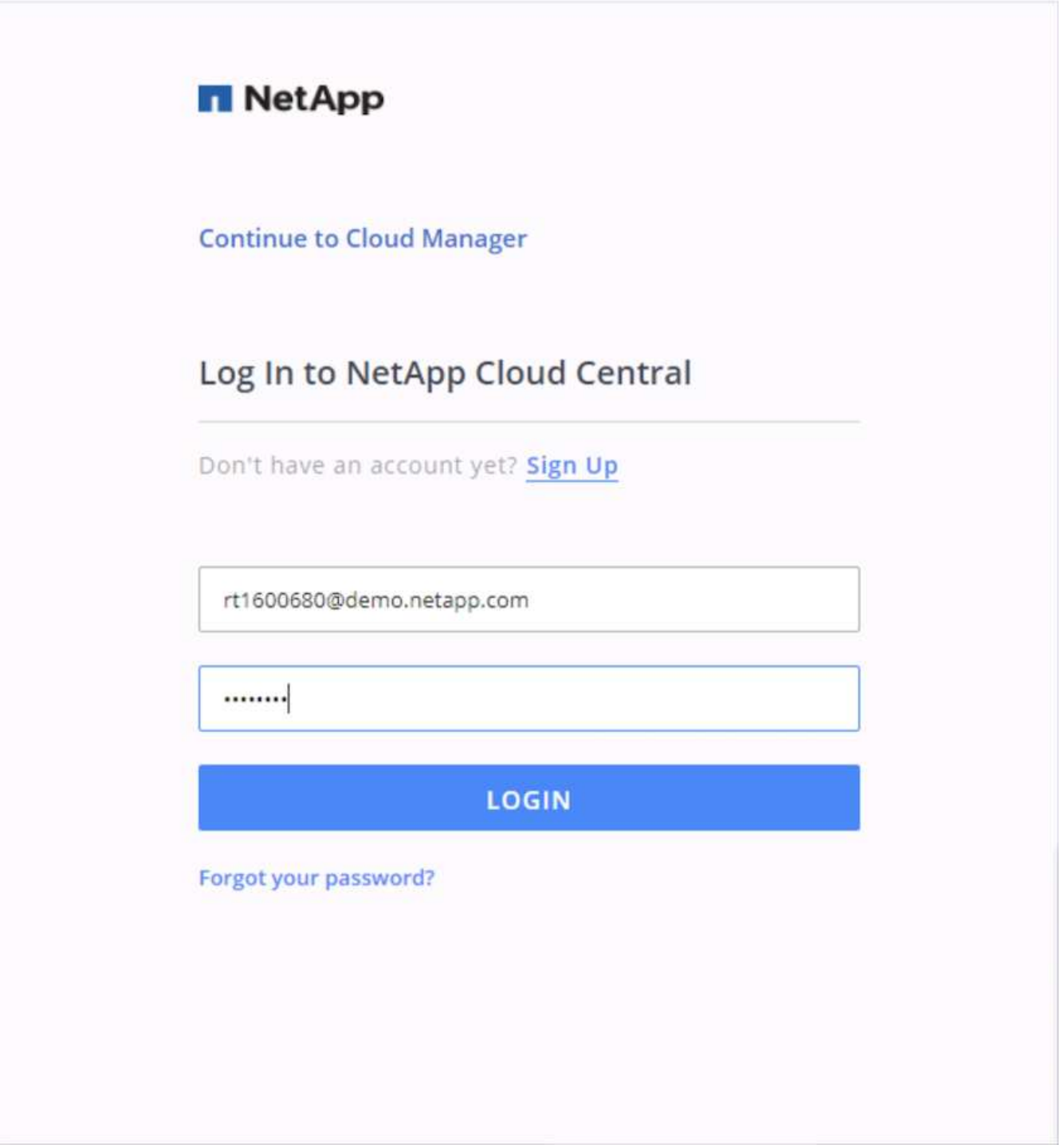
- Account AWS
- VPC nella tua regione di scelta
- Subnet con accesso a Internet pubblico
- Autorizzazioni per aggiungere ruoli IAM all'account AWS
- Chiave segreta e chiave di accesso per l'utente AWS

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

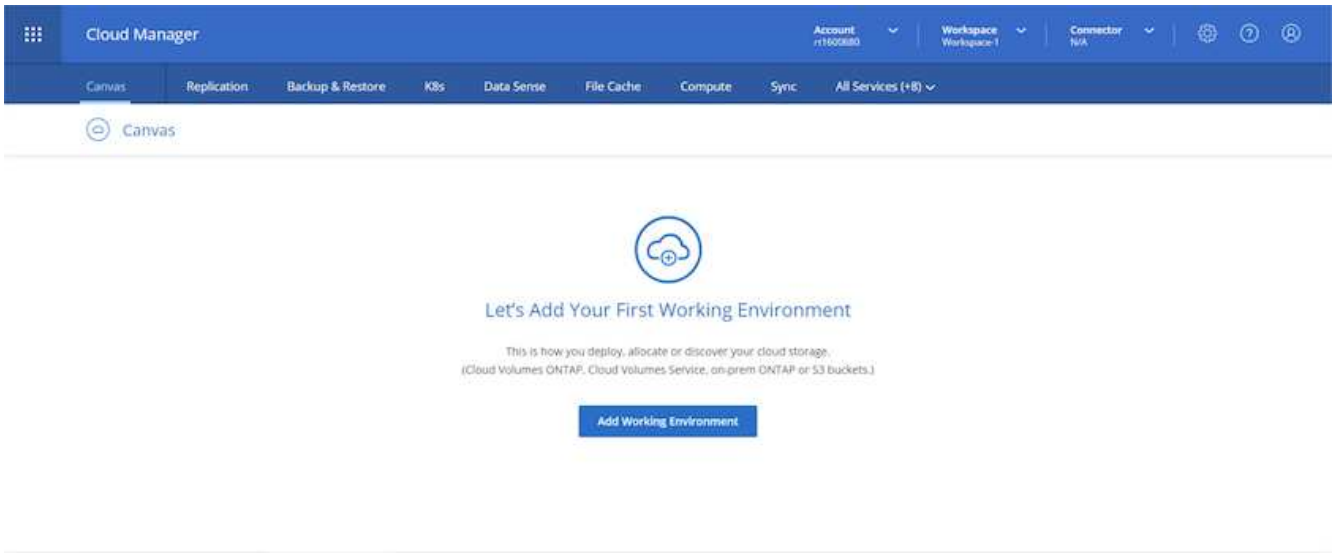
> Esistono molti metodi per implementare Cloud Manager e Cloud Volumes ONTAP; questo metodo è il più semplice ma richiede la maggior parte delle autorizzazioni. Se questo metodo non è appropriato per l'ambiente AWS in uso, consultare "Documentazione cloud di NetApp".

Implementare Cloud Manager Connector

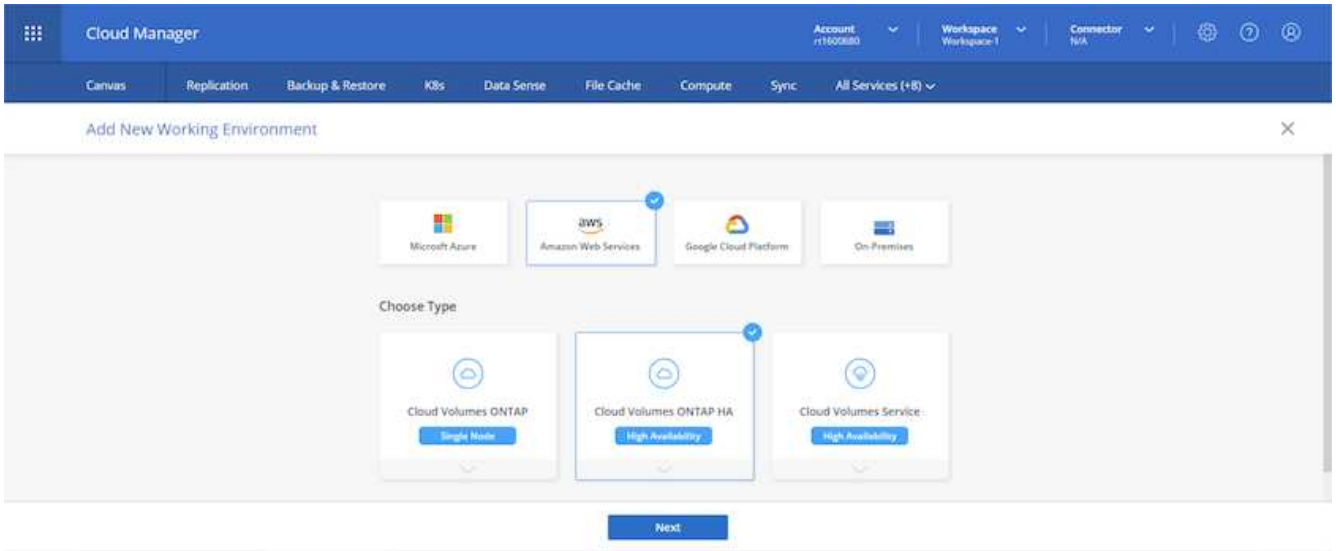
1. Selezionare "NetApp Cloud Central" ed effettuare l'accesso o l'iscrizione.



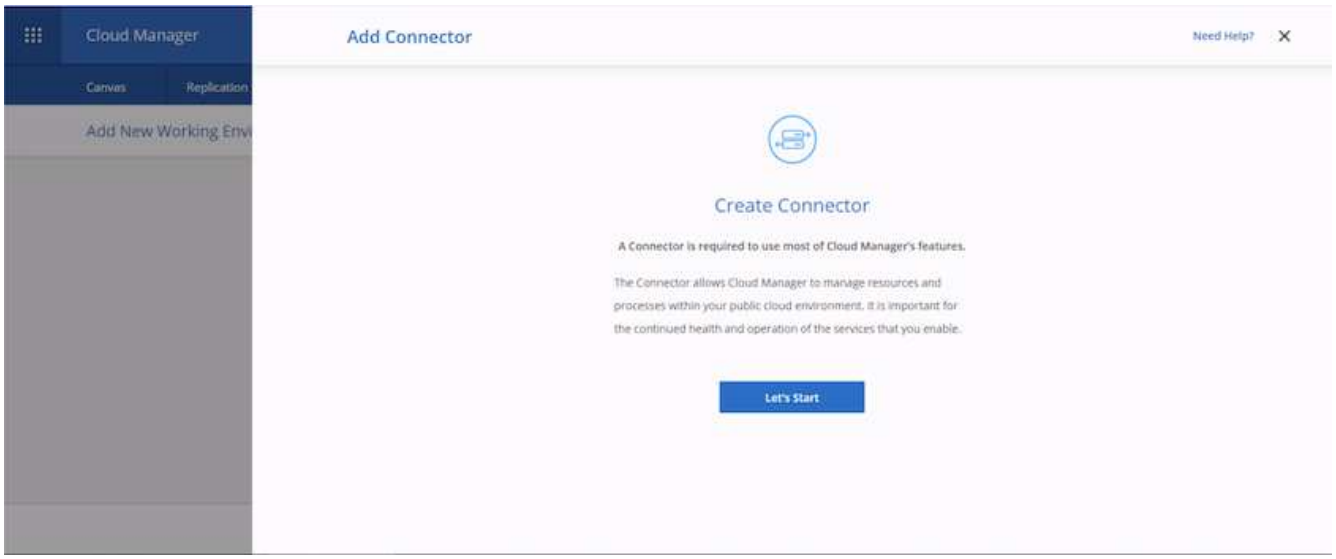
2. Dopo aver effettuato l'accesso, si dovrebbe essere portati a Canvas.



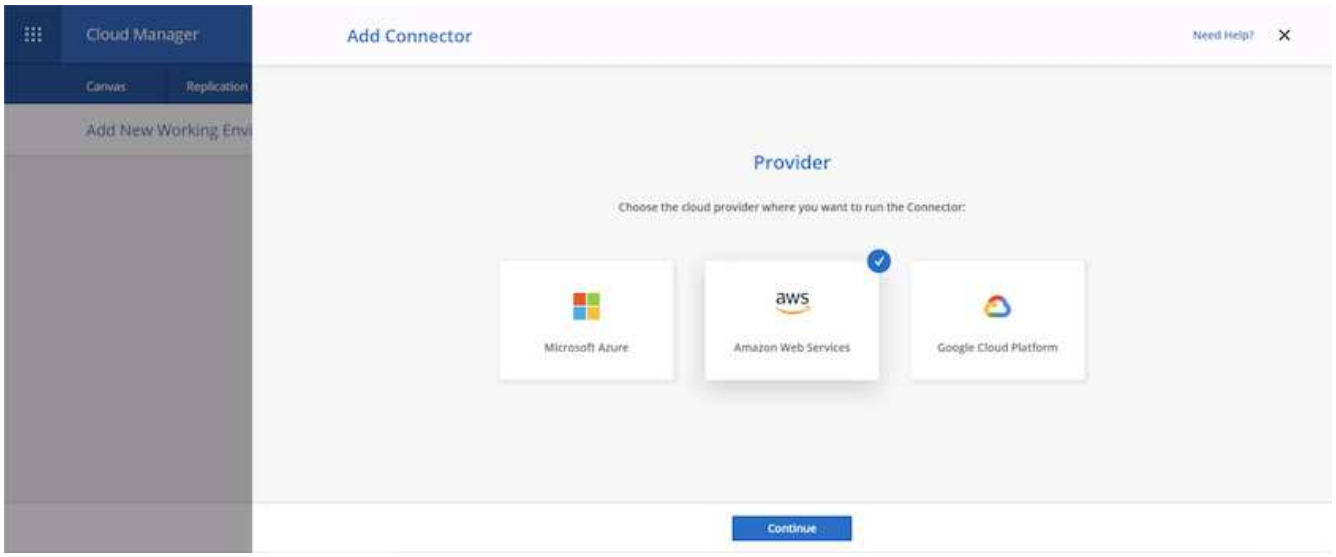
3. Fai clic su "Aggiungi ambiente di lavoro" e scegli Cloud Volumes ONTAP in AWS. In questo caso, è anche possibile scegliere se implementare un sistema a nodo singolo o una coppia ad alta disponibilità. Ho scelto di implementare una coppia ad alta disponibilità.



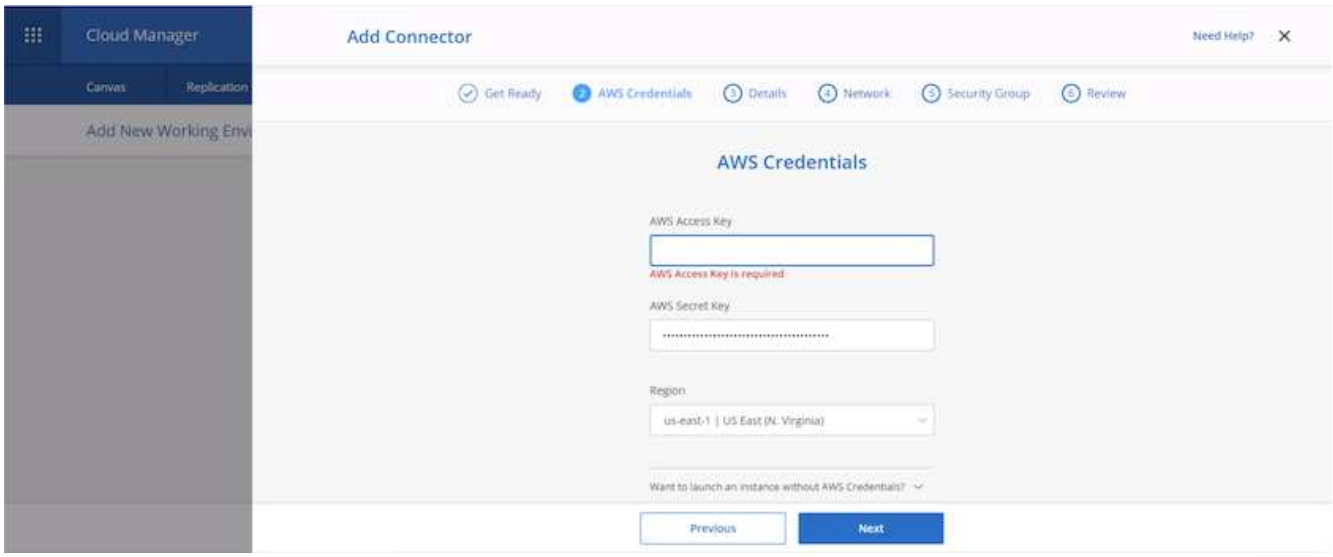
4. Se non è stato creato alcun connettore, viene visualizzata una finestra a comparsa che richiede di creare un connettore.



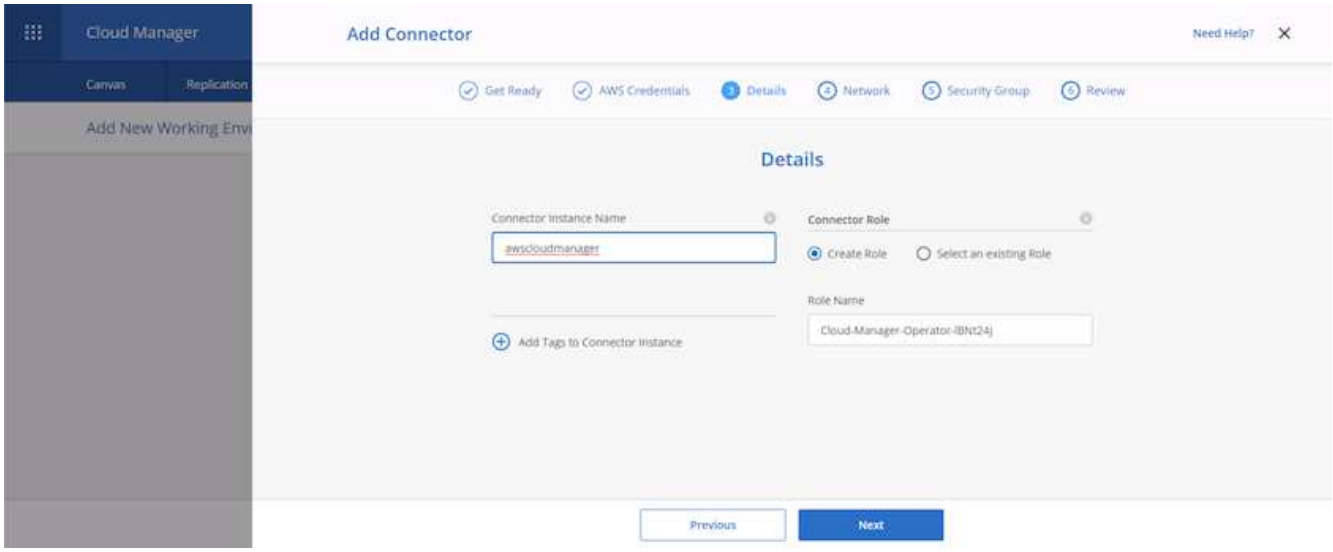
5. Fare clic su Avvia, quindi scegliere AWS.



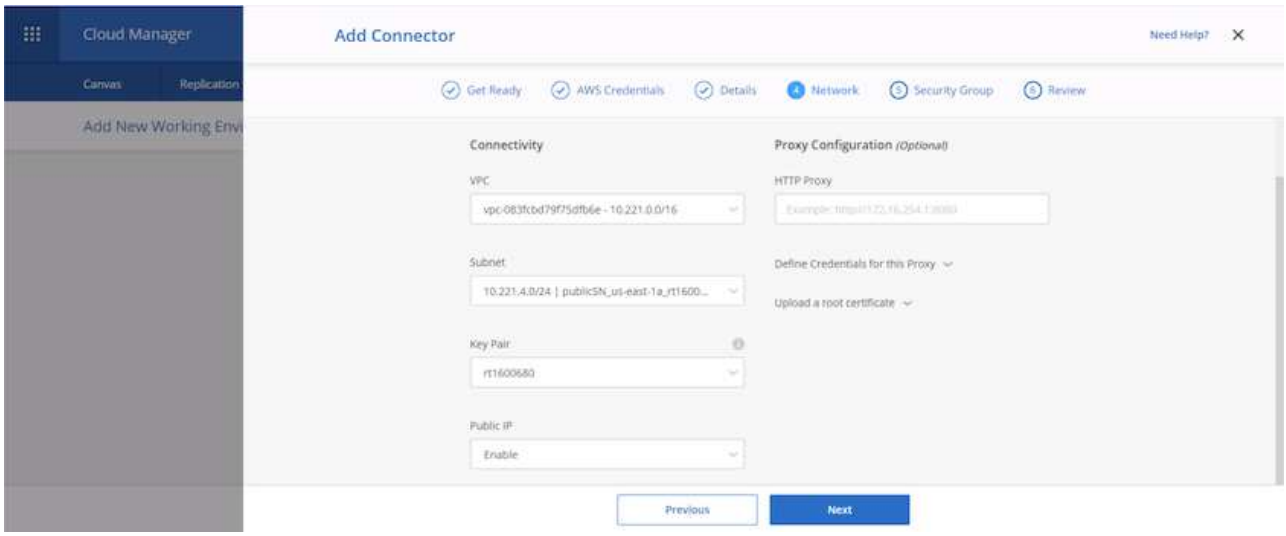
6. Inserire la chiave segreta e la chiave di accesso. Assicurarsi che l'utente disponga delle autorizzazioni corrette descritte in "Pagina delle policy di NetApp".



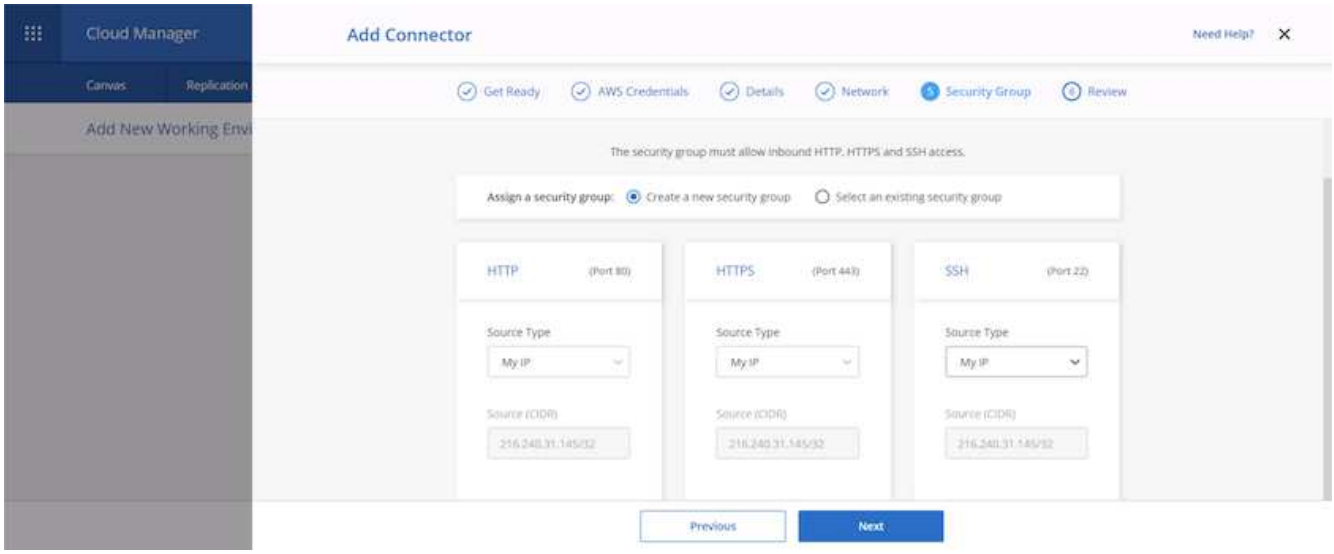
7. Assegnare un nome al connettore e utilizzare un ruolo predefinito come descritto in "Pagina delle policy di NetApp" Oppure chiedi a Cloud Manager di creare il tuo ruolo.



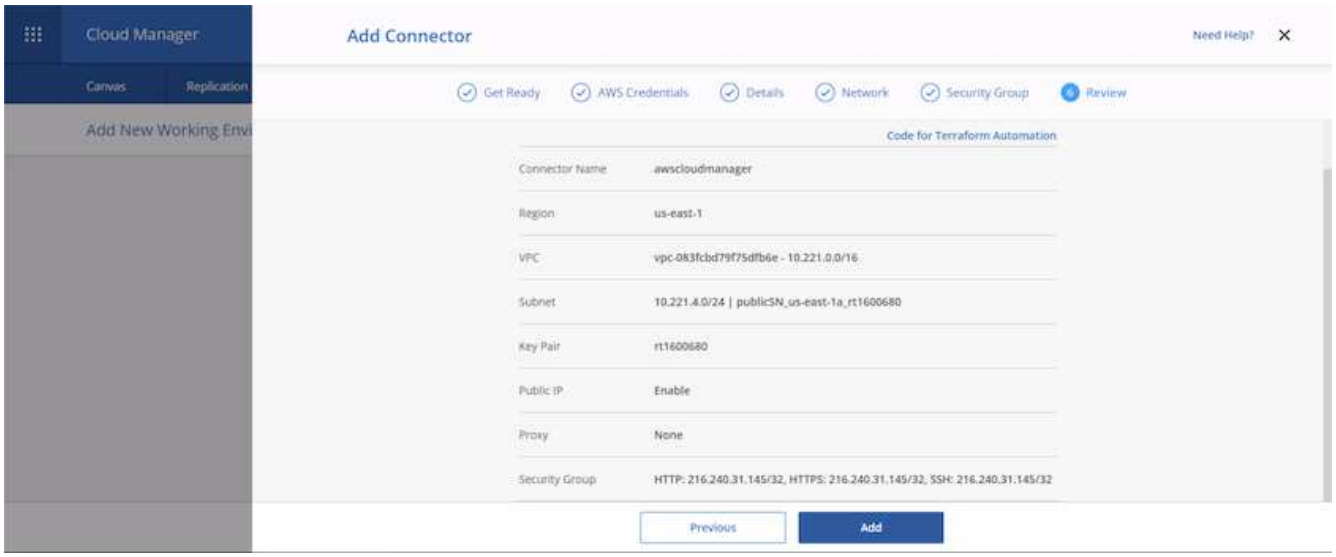
8. Fornire le informazioni di rete necessarie per implementare il connettore. Verificare che l'accesso a Internet in uscita sia attivato:
   a. Fornire al connettore un indirizzo IP pubblico
   b. Fornire al connettore un proxy da utilizzare
   c. Fornire al connettore un percorso verso Internet pubblico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



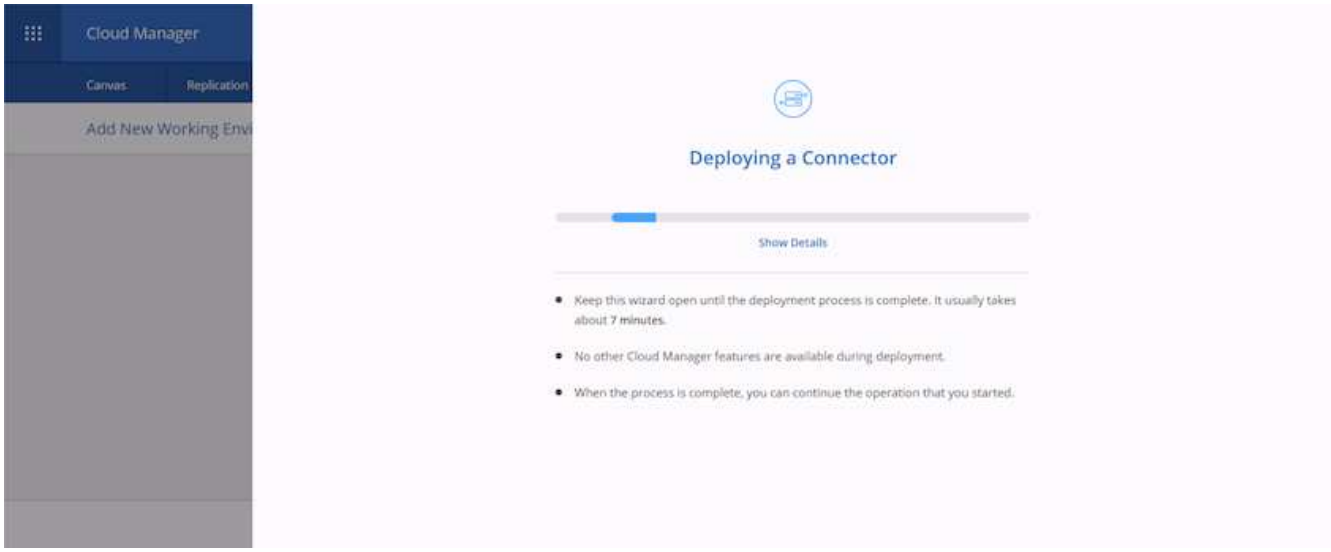
9. Fornire la comunicazione con il connettore tramite SSH, HTTP e HTTPS fornendo un gruppo di protezione o creando un nuovo gruppo di protezione. È stato attivato l'accesso al connettore solo dall'indirizzo IP.



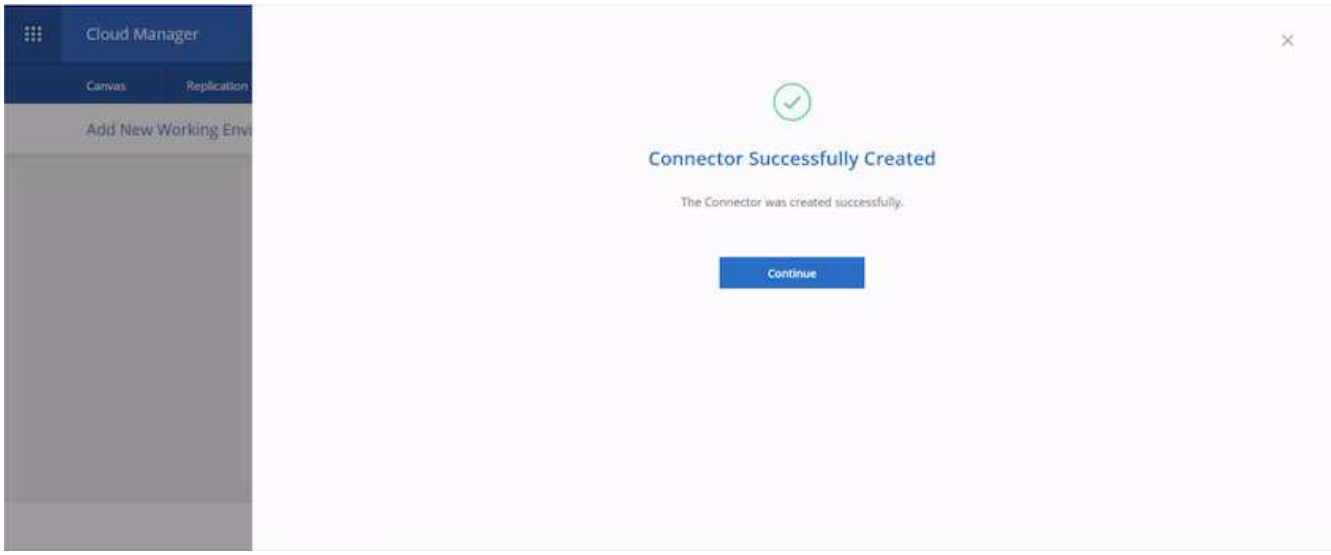
10. Esaminare le informazioni nella pagina di riepilogo e fare clic su Add (Aggiungi) per implementare il connettore.



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

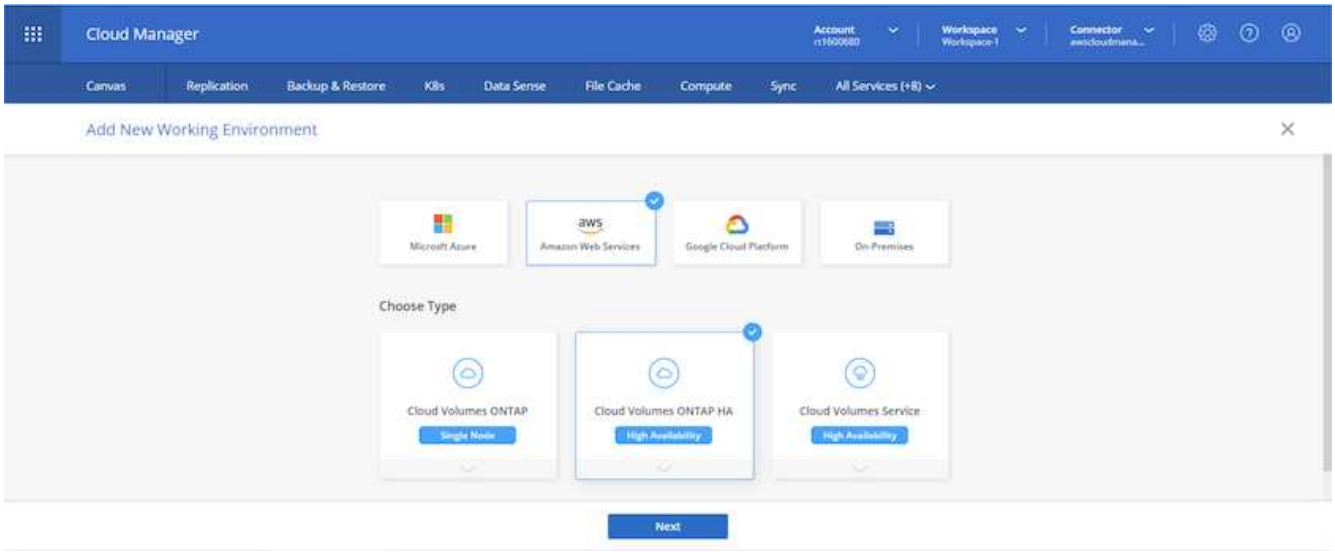


12. Una volta completata l'implementazione, viene visualizzata una pagina di successo.

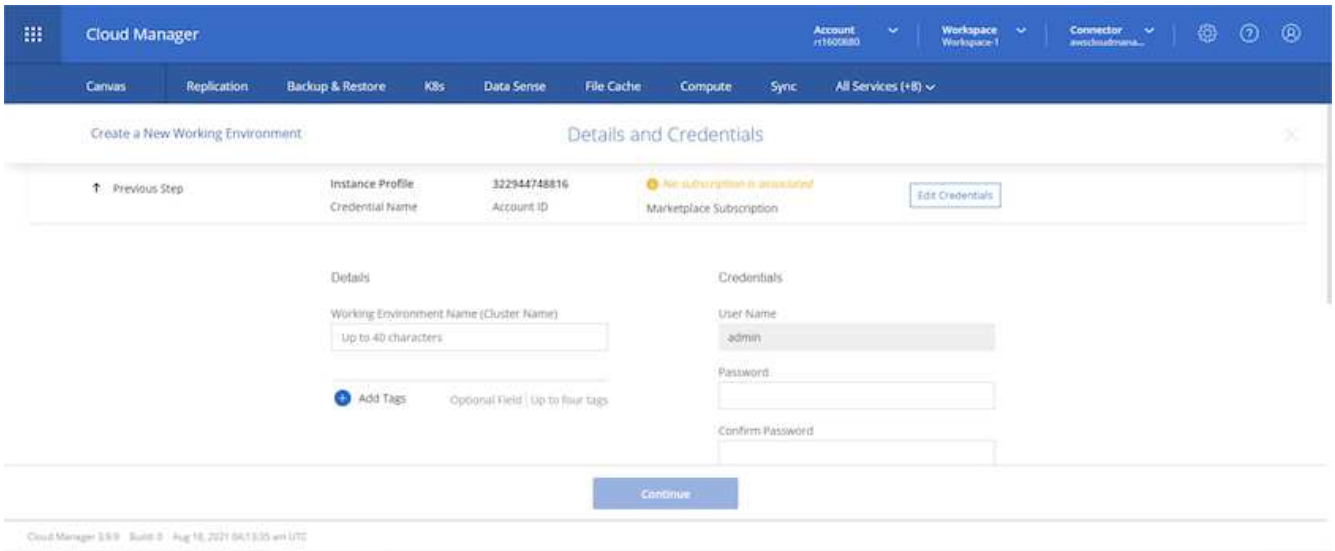


Implementare Cloud Volumes ONTAP

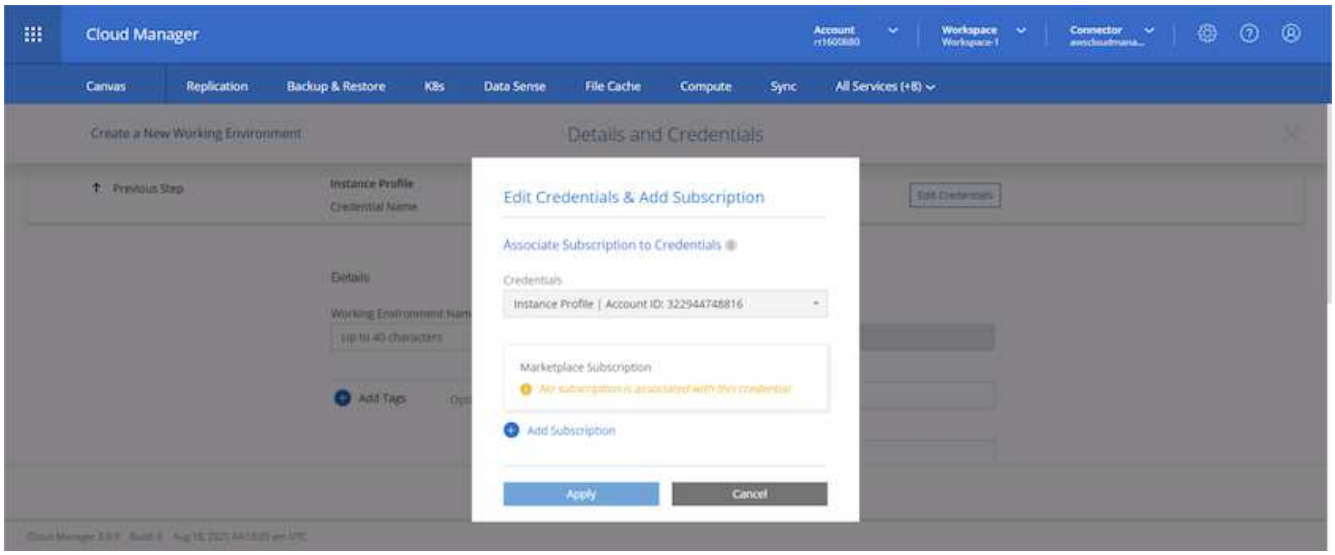
1. Selezionare AWS e il tipo di implementazione in base ai requisiti.



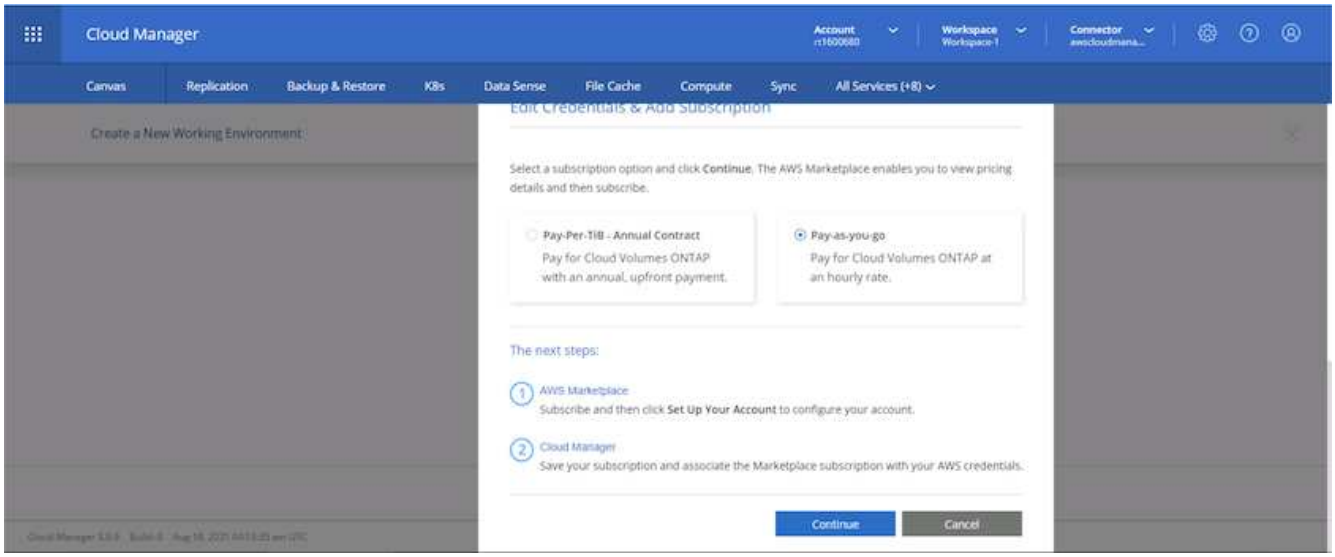
2. Se non è stato assegnato alcun abbonamento e si desidera effettuare l'acquisto con PAYGO, scegliere Modifica credenziali.



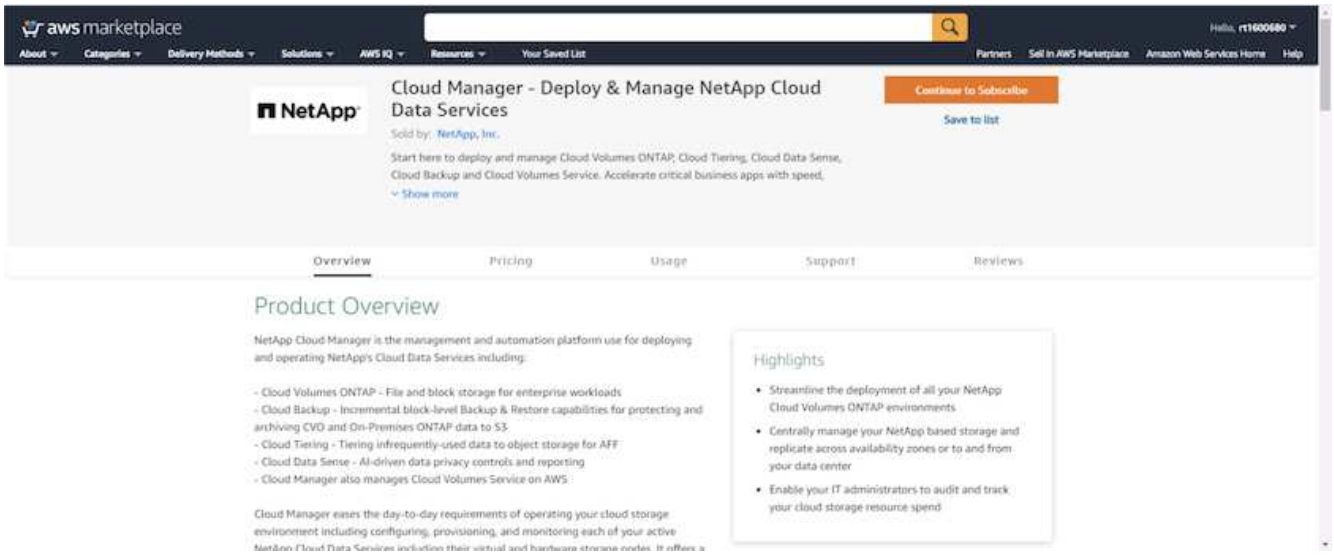
3. Scegliere Aggiungi abbonamento.



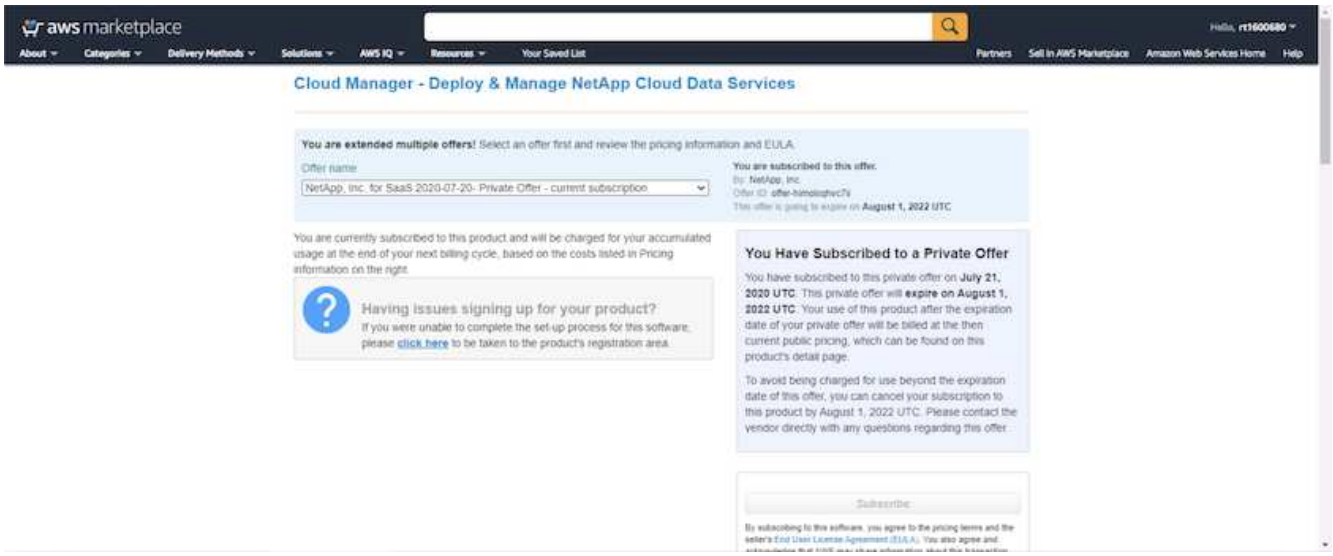
4. Scegliere il tipo di contratto a cui si desidera sottoscrivere. Ho scelto il pay-as-you-go.



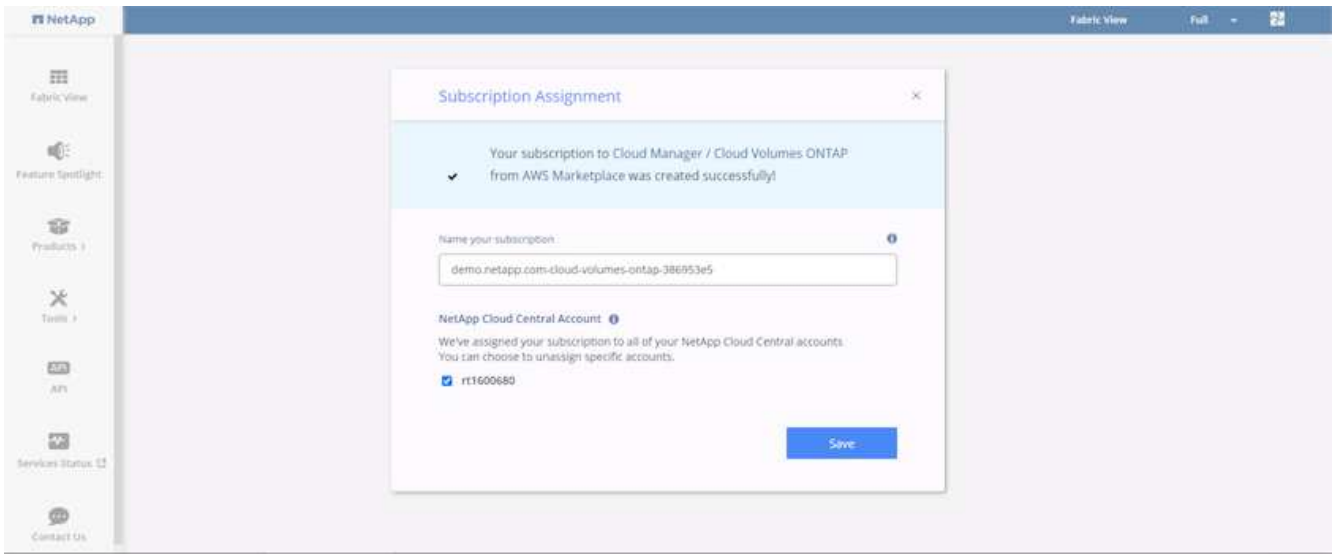
5. Si viene reindirizzati ad AWS; scegliere continua per iscriversi.



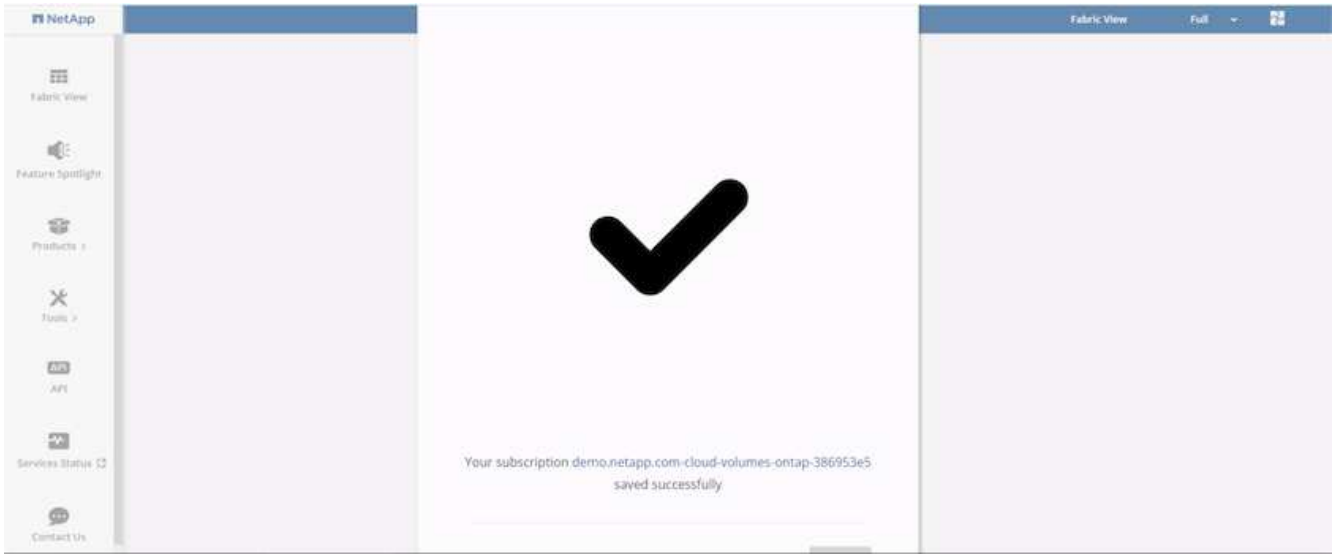
6. Iscriviti e verrai reindirizzato a NetApp Cloud Central. Se sei già iscritto e non ricevi il reindirizzamento, scegli il link "Clicca qui".



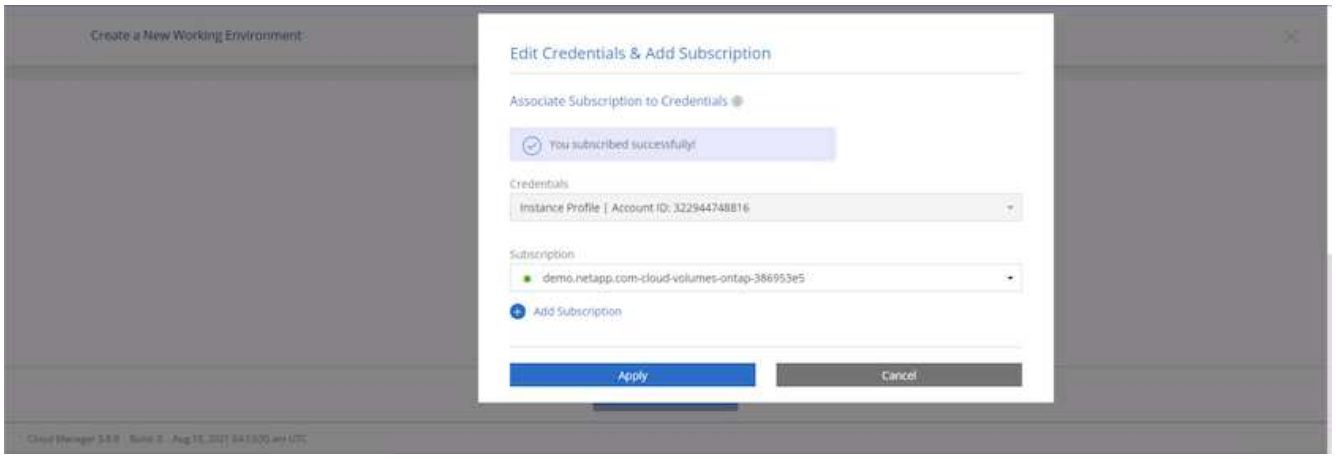
7. Verrai reindirizzato a Cloud Central dove devi assegnare un nome all'abbonamento e assegnarlo al tuo account Cloud Central.



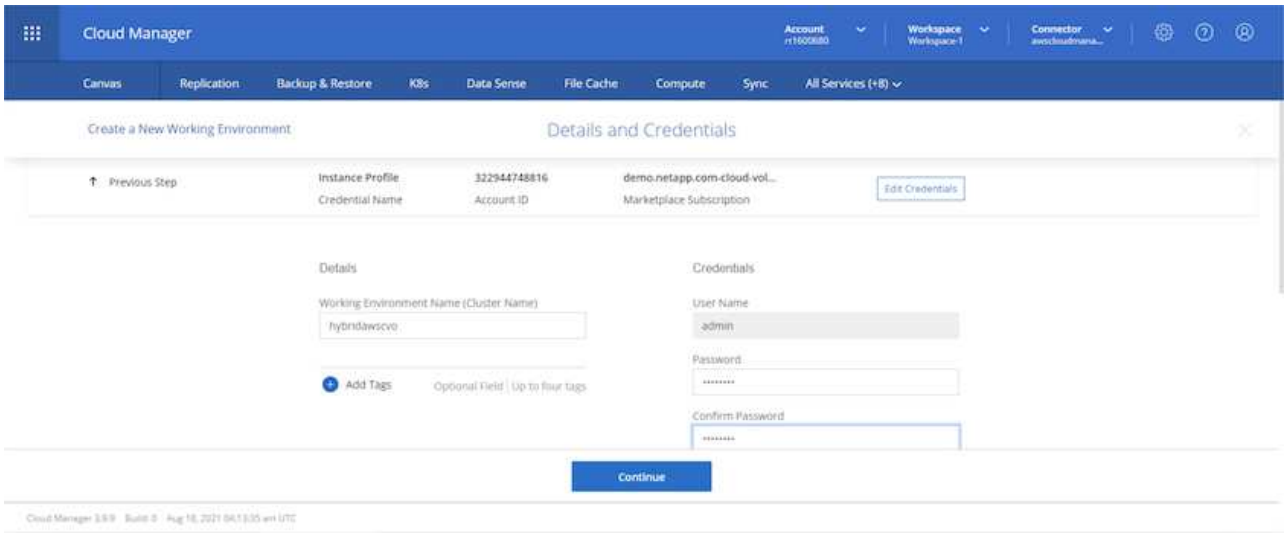
8. Una volta completata la stampa, viene visualizzata una pagina con un segno di spunta. Tornare alla scheda Cloud Manager.



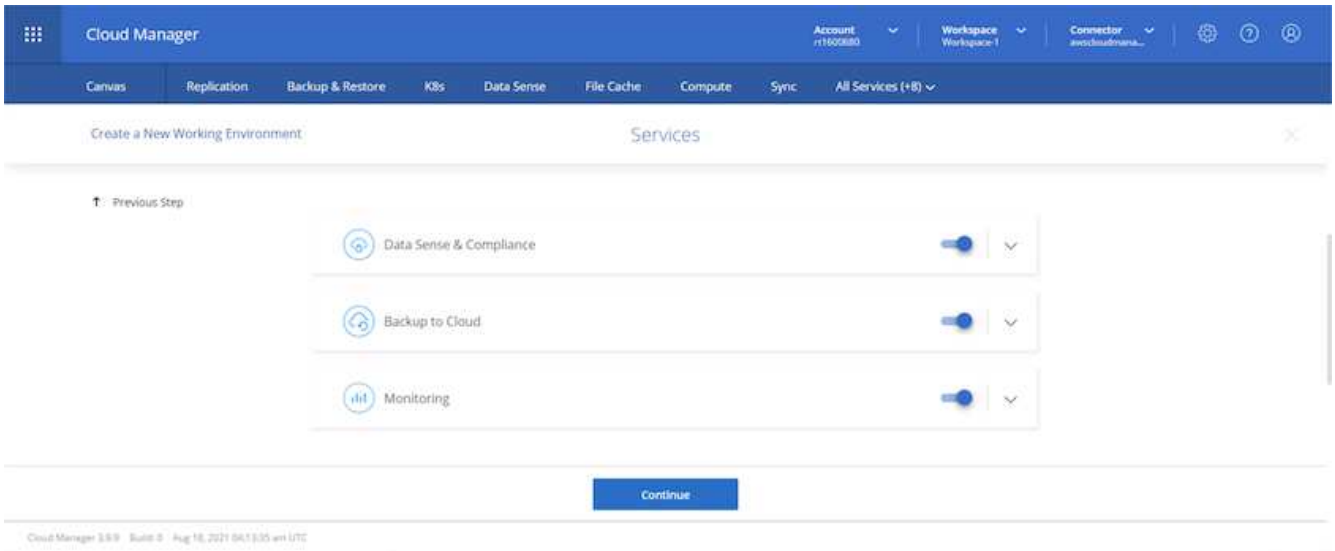
9. L'abbonamento viene ora visualizzato in Cloud Central. Fare clic su Apply (Applica) per continuare.



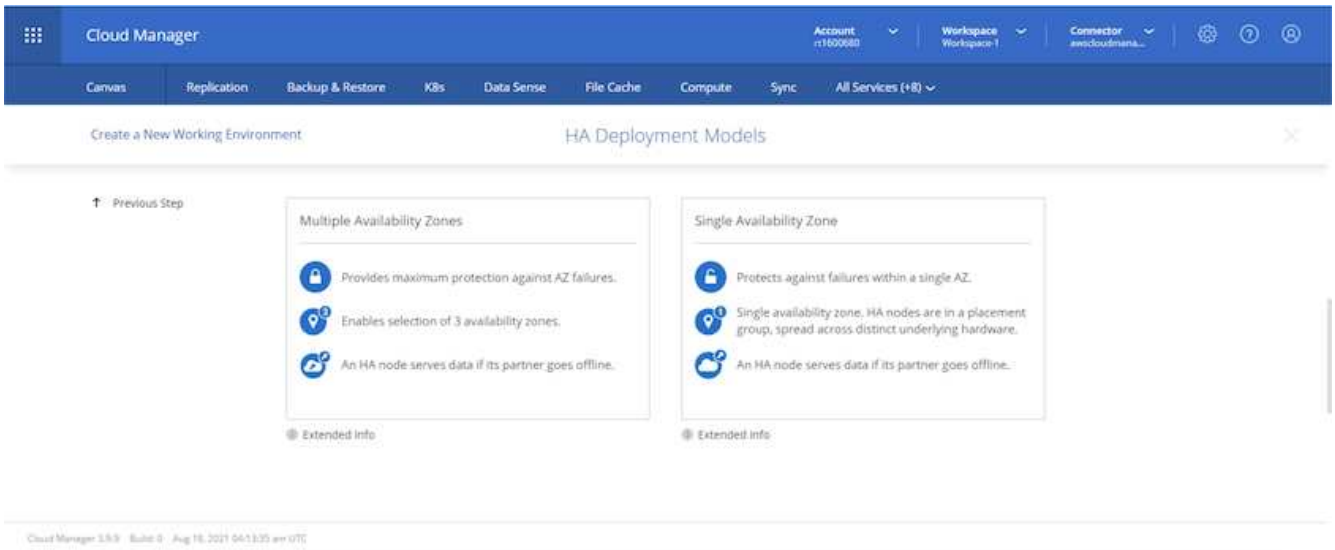
10. Inserire i dettagli dell'ambiente di lavoro, ad esempio:
    a. Nome del cluster
    b. Password del cluster
    c. Tag AWS (opzionale)



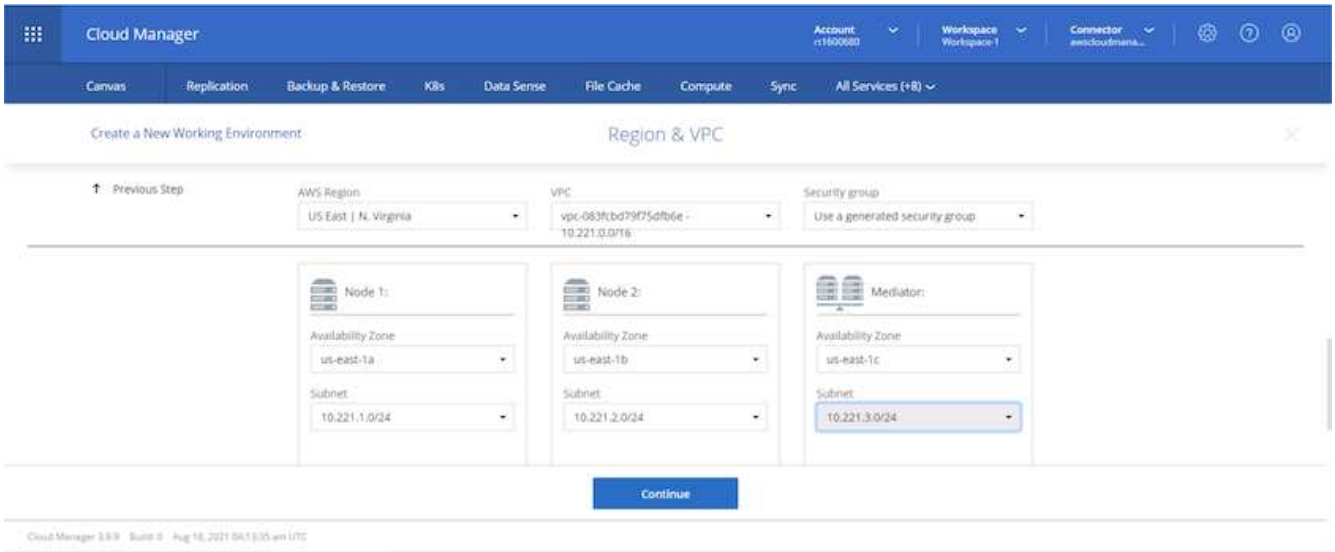
11. Scegliere i servizi aggiuntivi che si desidera implementare. Per ulteriori informazioni su questi servizi, visitare il "Homepage di NetApp Cloud".



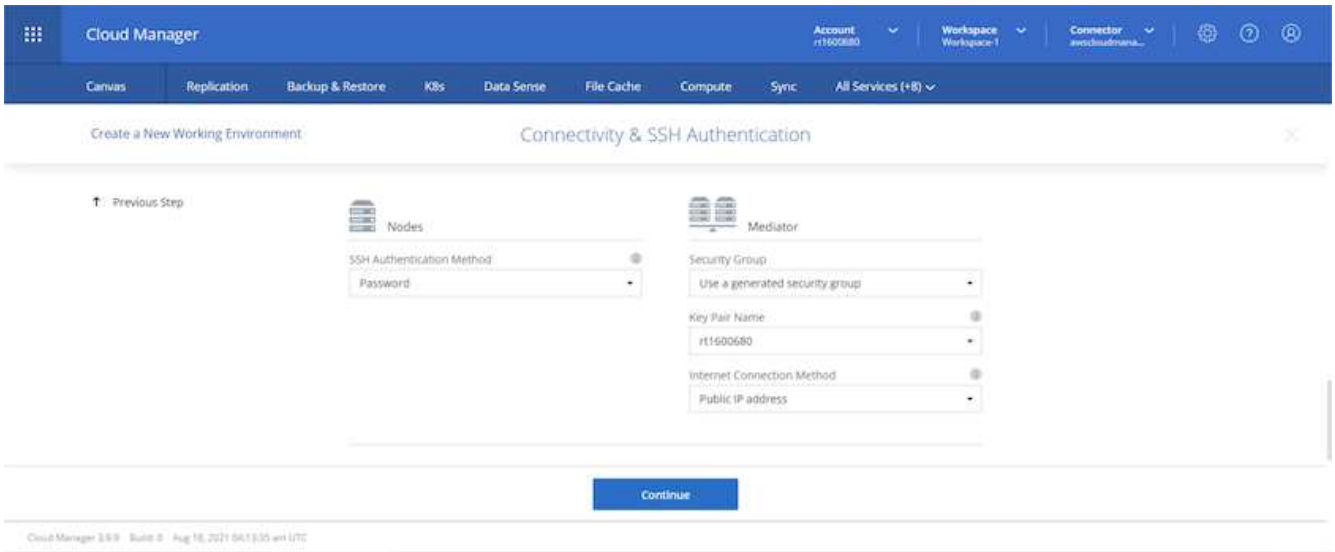
12. Scegliere se eseguire l'implementazione in più zone di disponibilità (si recuperano tre subnet, ciascuna in un AZ diverso) o in una singola zona di disponibilità. Ho scelto più AZS.



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.

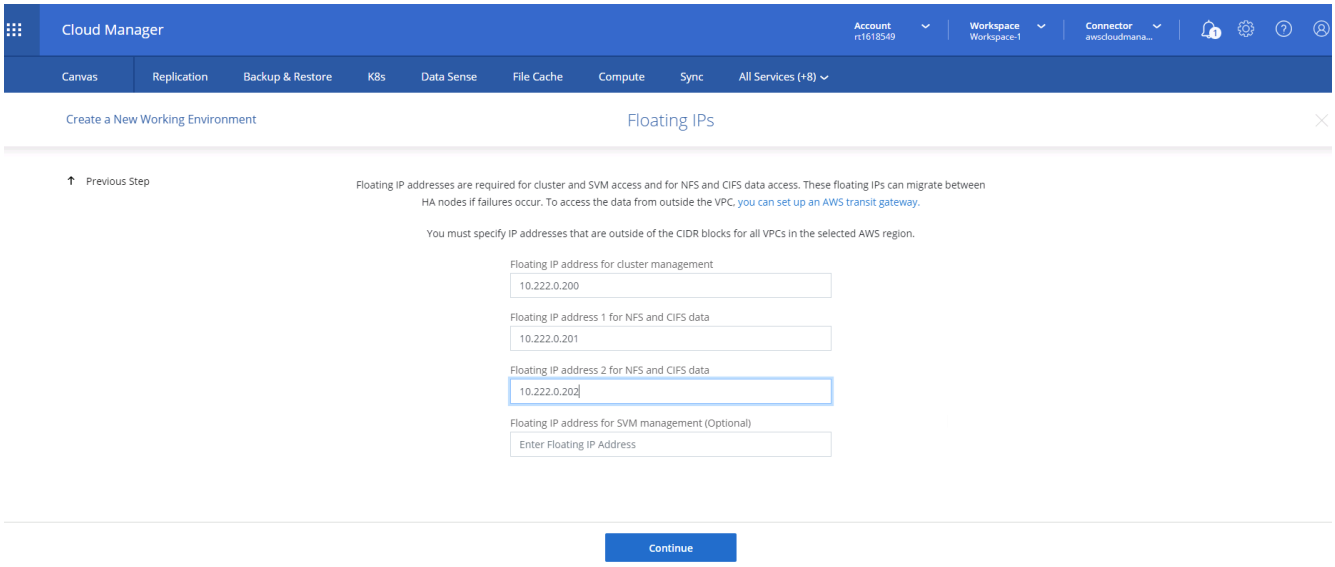


14. Scegliere i metodi di connessione per i nodi e il mediatore.

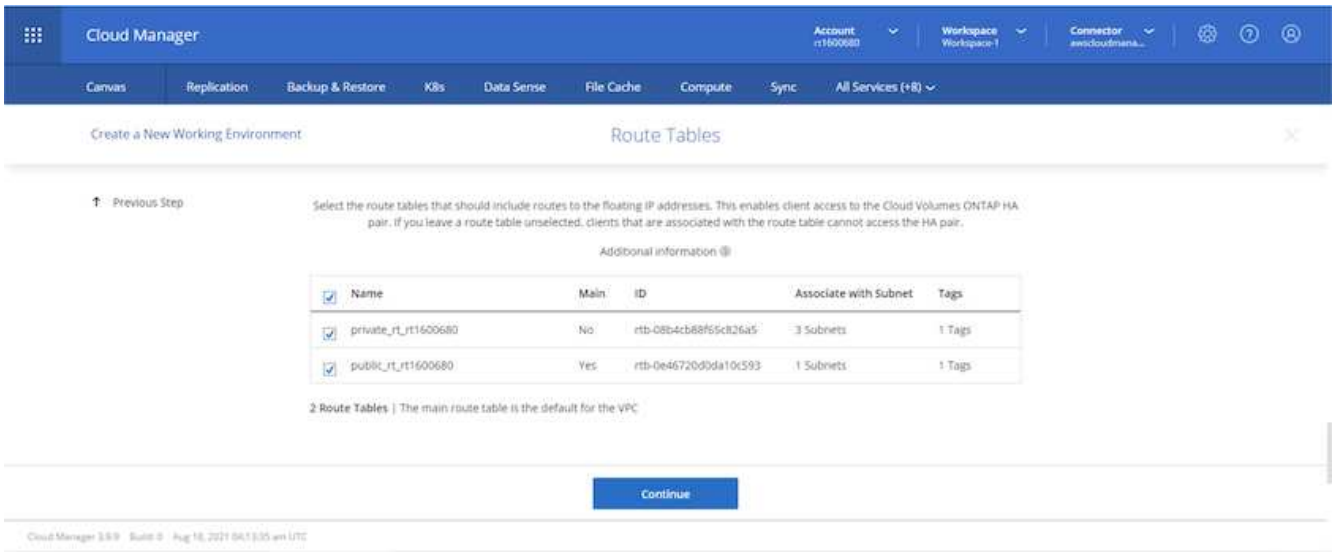


Il mediatore richiede la comunicazione con le API AWS. Non è richiesto un indirizzo IP pubblico, purché le API siano raggiungibili dopo l'implementazione dell'istanza EC2 del mediatore.

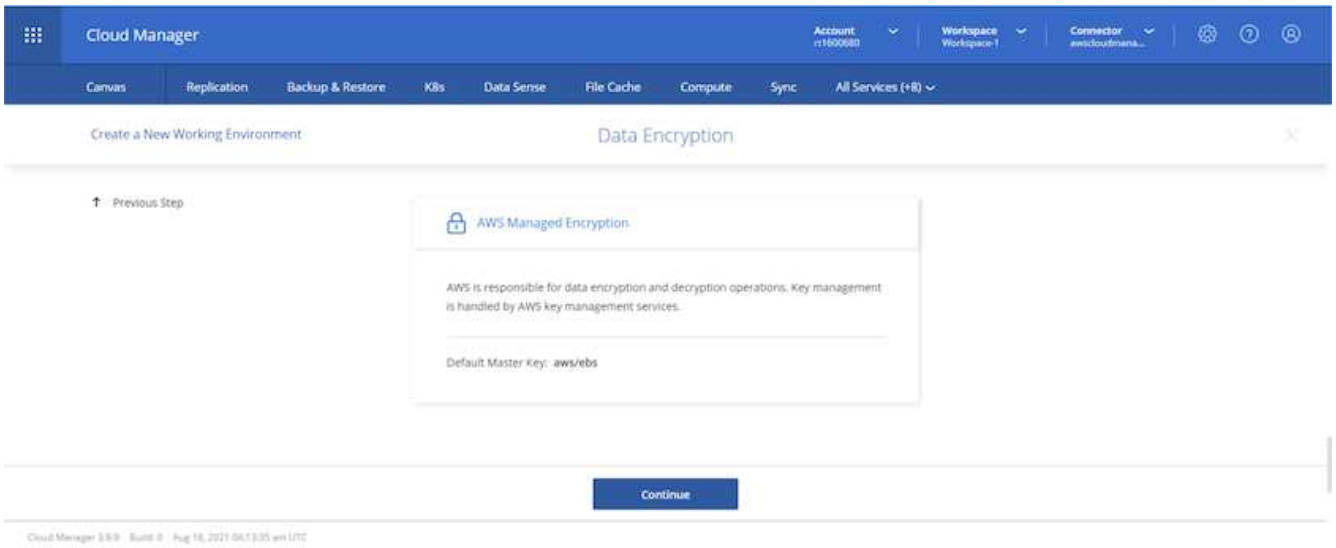
1. Gli indirizzi IP mobili vengono utilizzati per consentire l'accesso ai vari indirizzi IP utilizzati da Cloud Volumes ONTAP, inclusi gli IP di gestione del cluster e di erogazione dei dati. Devono essere indirizzi non ancora instradabili all'interno della rete e aggiunti alle tabelle di routing nell'ambiente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



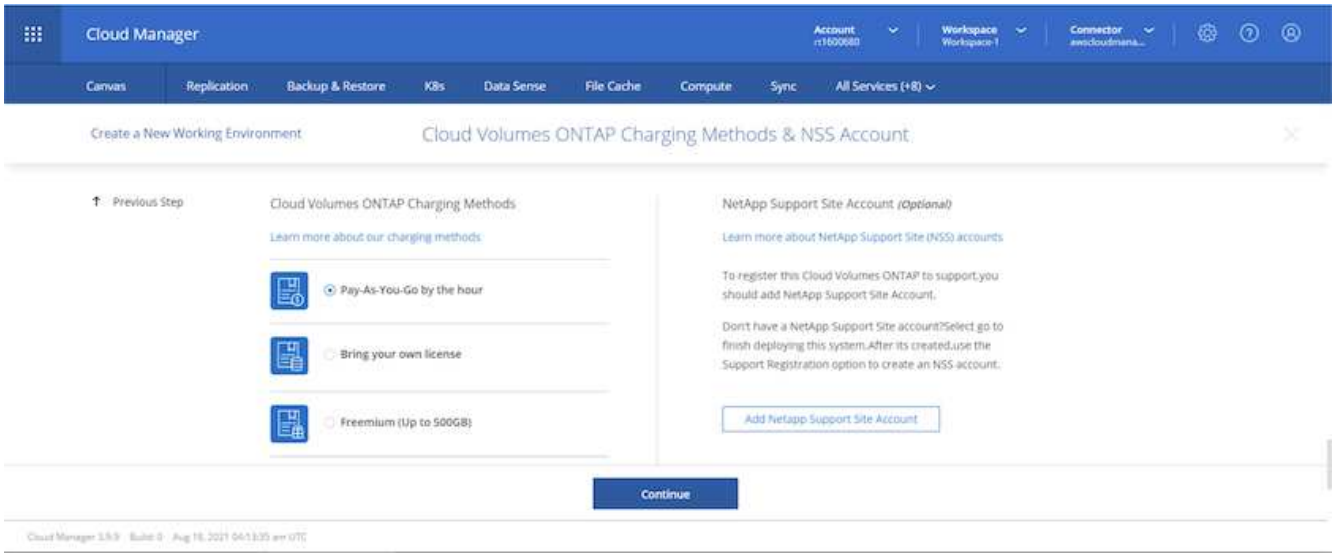
2. Selezionare le tabelle di routing a cui aggiungere gli indirizzi IP mobili. Queste tabelle di routing vengono utilizzate dai client per comunicare con Cloud Volumes ONTAP.



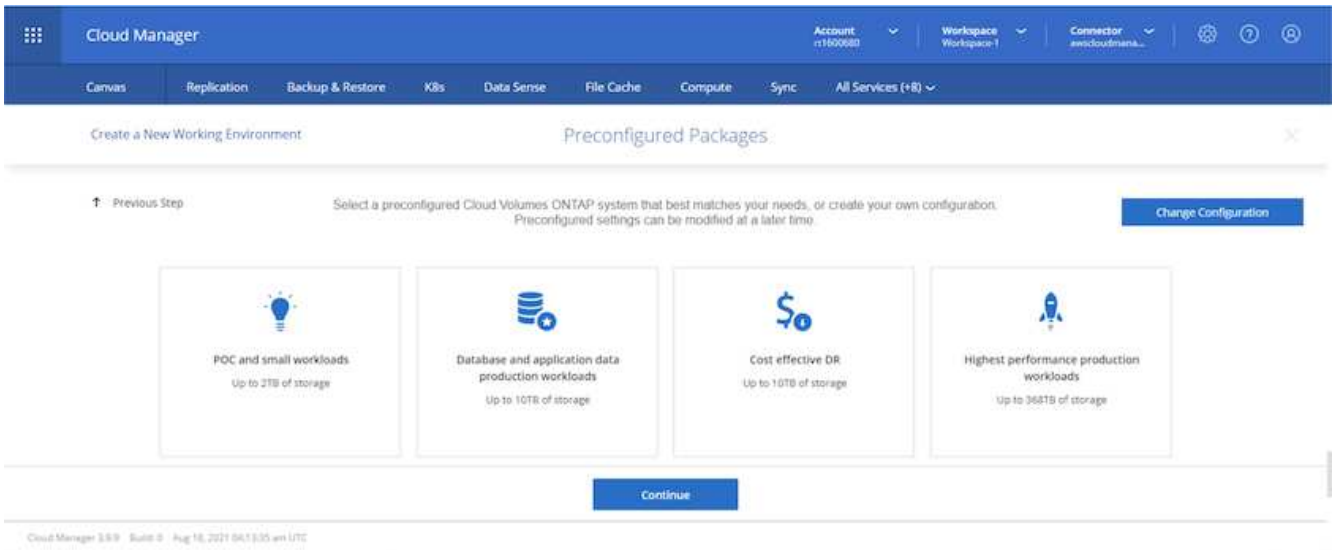
3. Scegliere se attivare la crittografia gestita AWS o AWS KMS per crittografare i dischi root, boot e dati ONTAP.



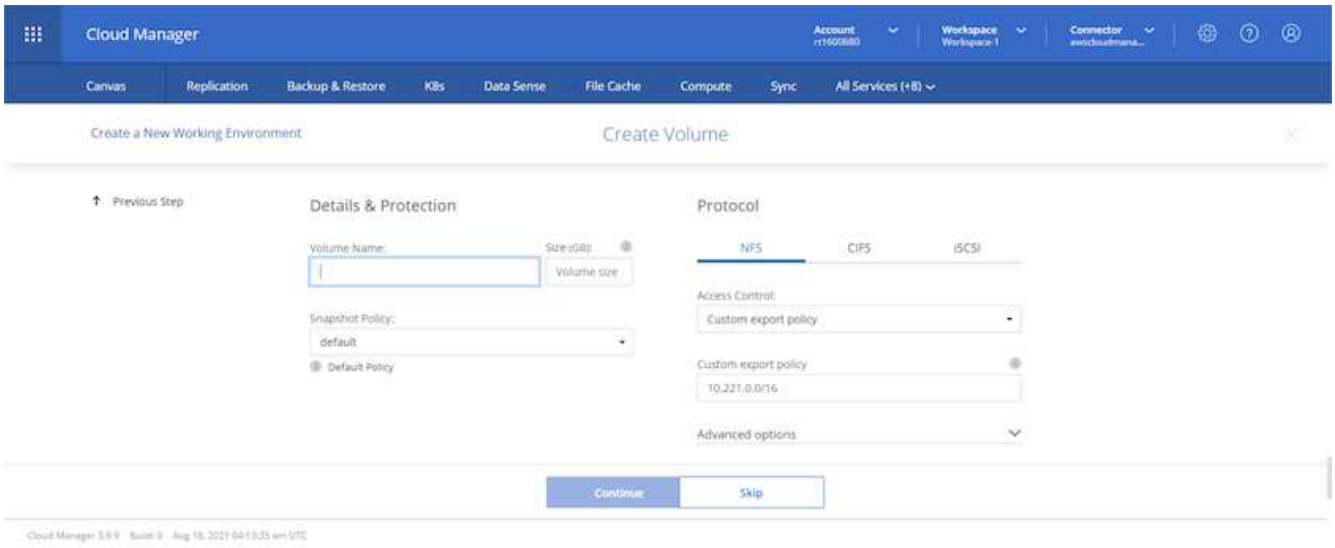
4. Scegli il tuo modello di licenza. Se non sai quale scegliere, contatta il tuo rappresentante NetApp.



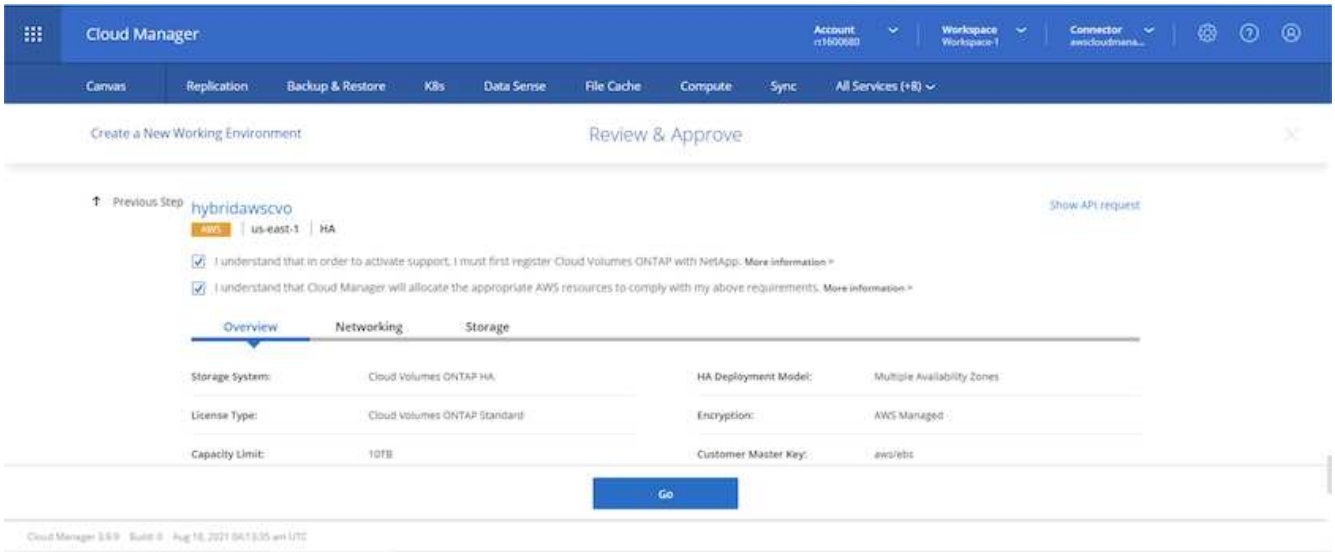
5. Selezionare la configurazione più adatta al caso d'utilizzo. Ciò è correlato alle considerazioni sul dimensionamento trattate nella pagina dei prerequisiti.



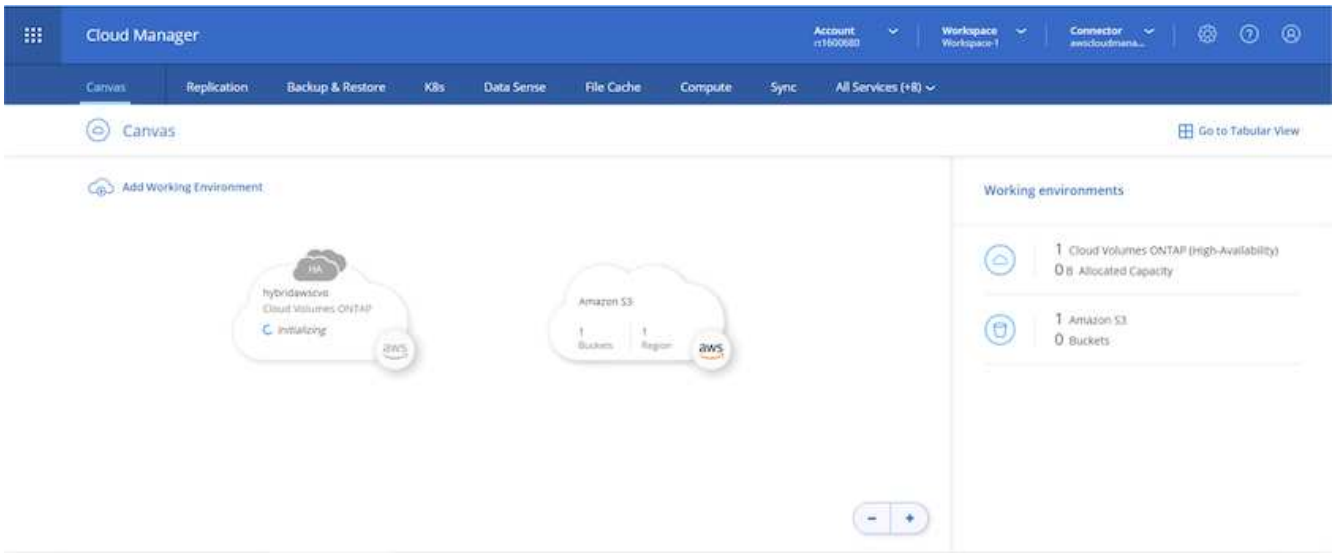
6. Se si desidera, creare un volume. Questo non è necessario, perché le fasi successive utilizzano SnapMirror, che crea i volumi per noi.



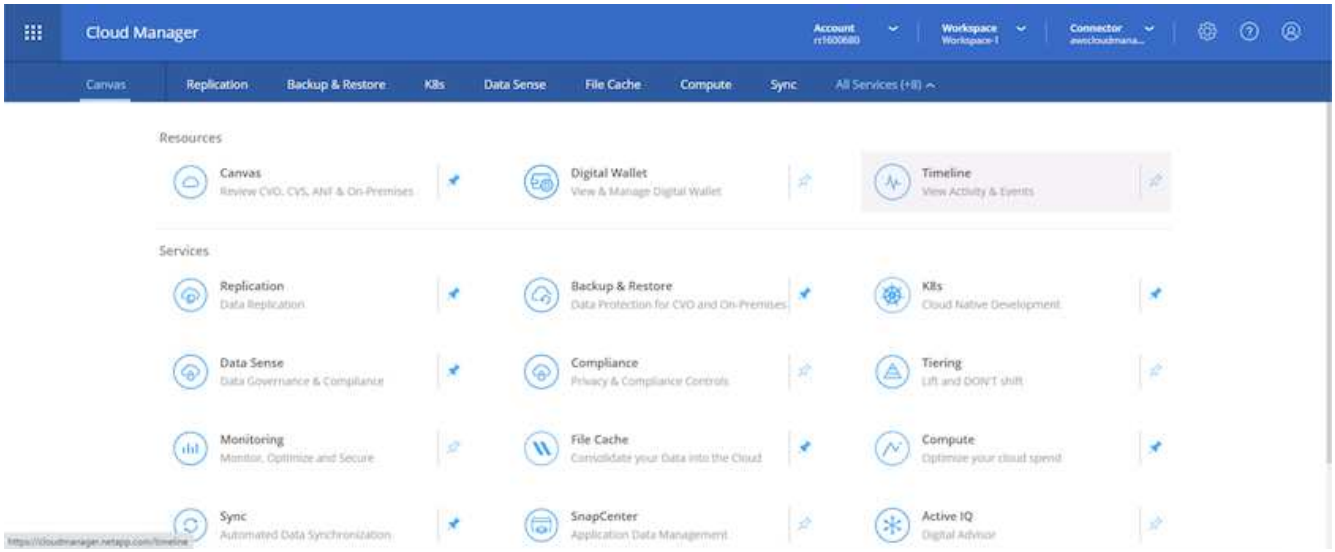
7. Esaminare le selezioni effettuate e spuntare le caselle per verificare che Cloud Manager implementa le risorse nel proprio ambiente AWS. Quando si è pronti, fare clic su Go (Vai).



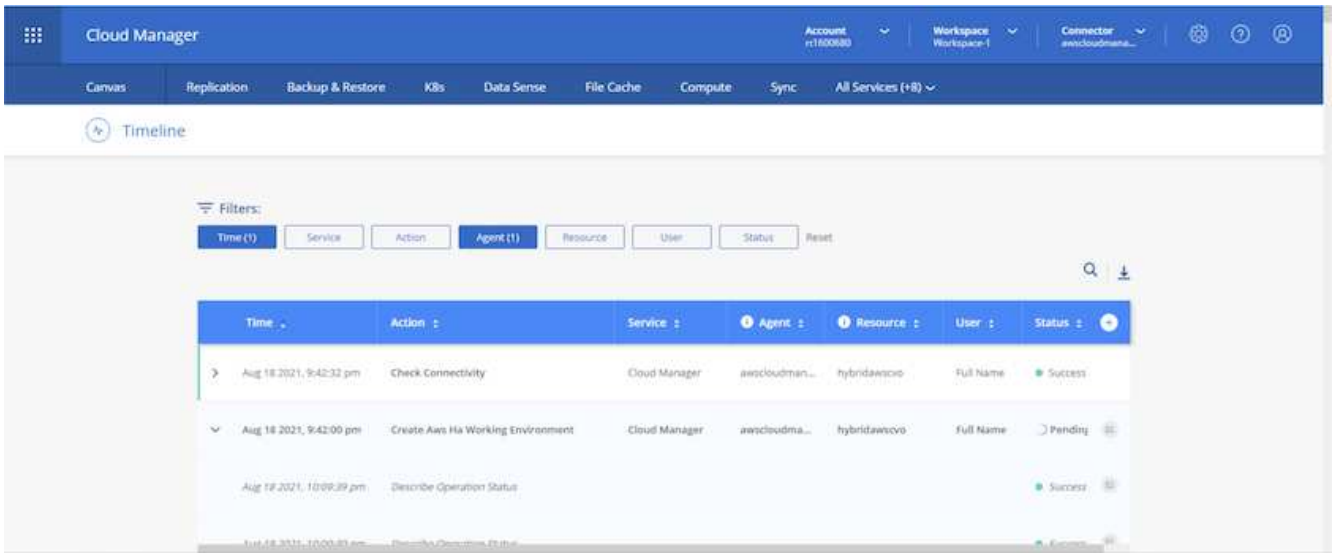
8. Cloud Volumes ONTAP avvia ora il processo di implementazione. Cloud Manager utilizza le API AWS e gli stack di formazione del cloud per implementare Cloud Volumes ONTAP. Quindi, configura il sistema in base alle tue specifiche, offrendo un sistema pronto all'uso che può essere utilizzato immediatamente.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



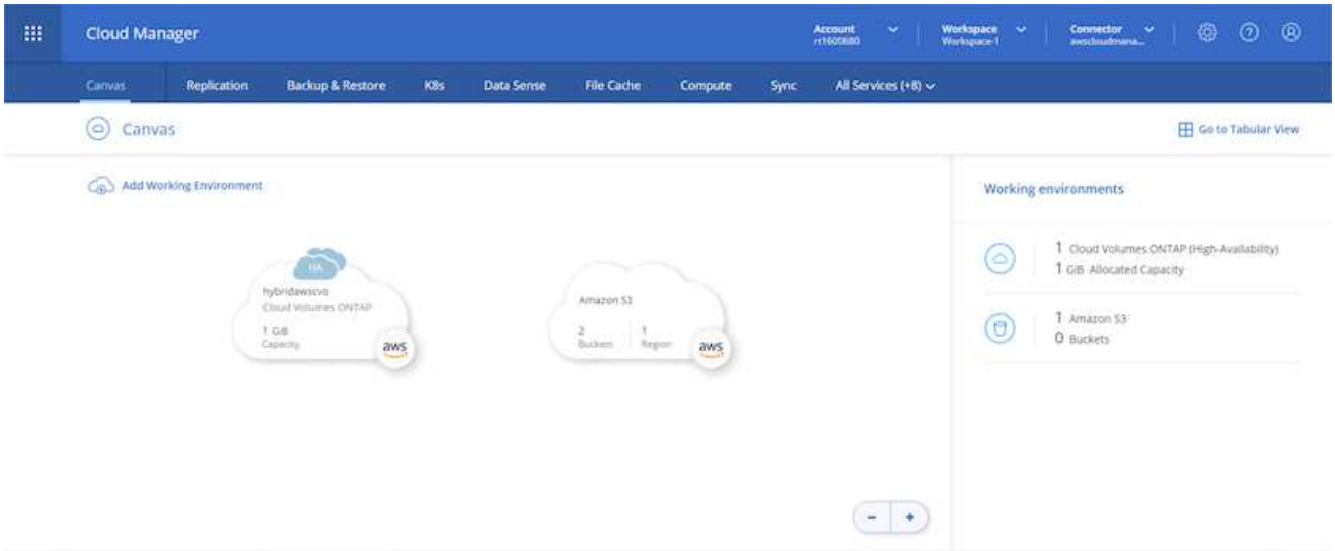
9. È possibile monitorare l'avanzamento passando alla Timeline.



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.

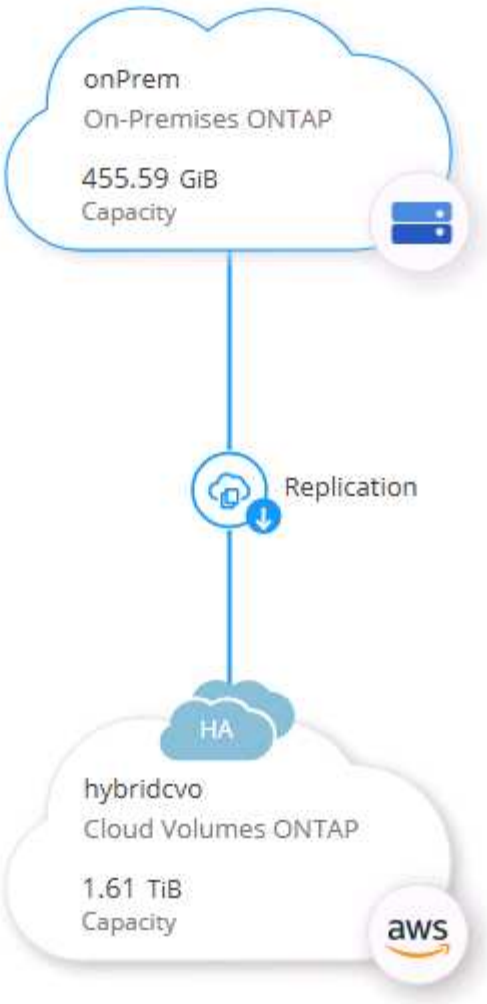


Configurare SnapMirror da on-premise a cloud

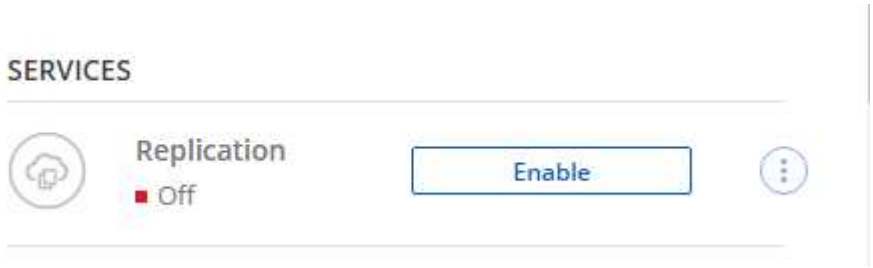
Ora che hai implementato un sistema ONTAP di origine e un sistema ONTAP di destinazione, puoi replicare volumi contenenti dati di database nel cloud.

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

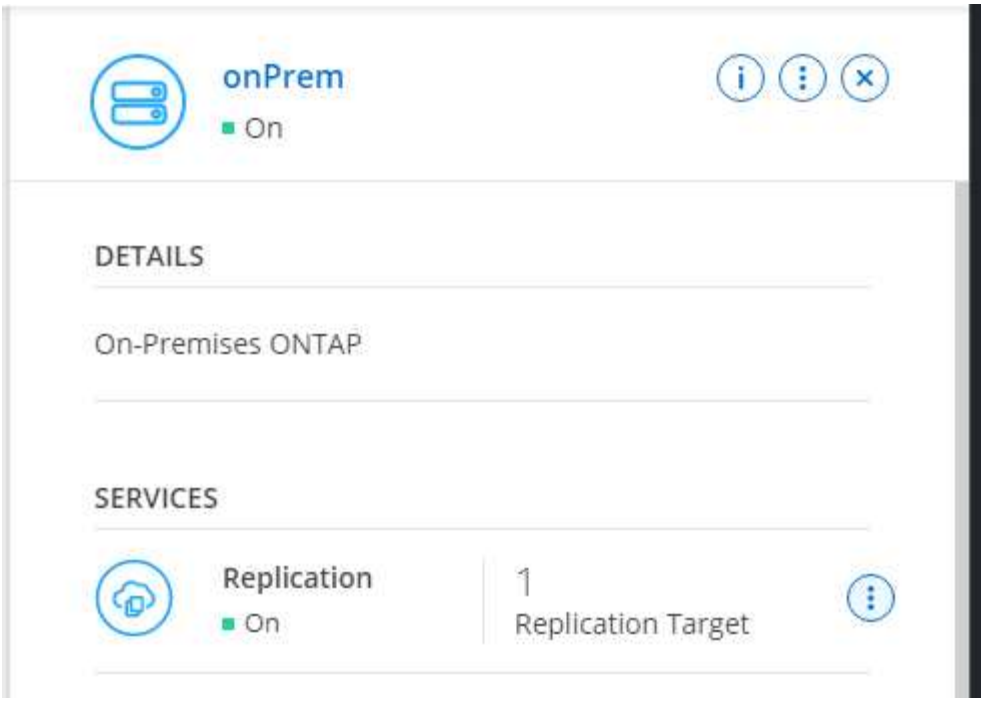
1. Fare clic sul sistema ONTAP di origine (on-premise) e trascinarlo nella destinazione, selezionare Replication > Enable (Replica > attiva) oppure selezionare Replication > Menu > Replicate (Replica > Menu > Replica).



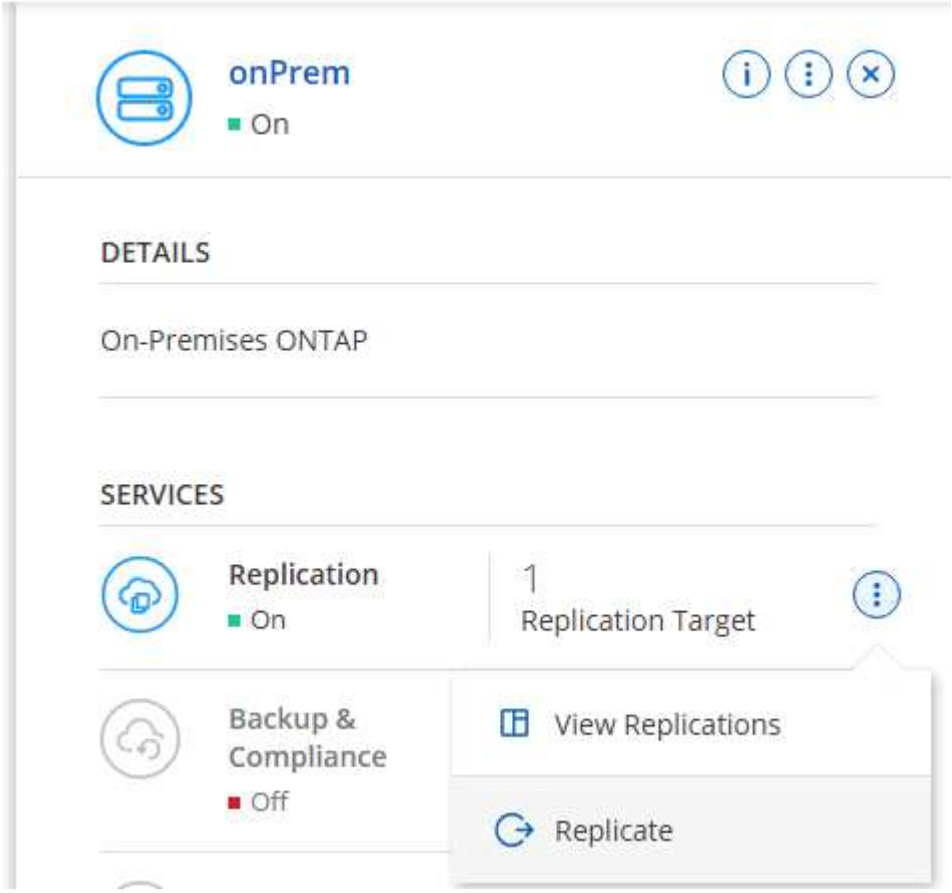
Selezionare Enable (attiva).



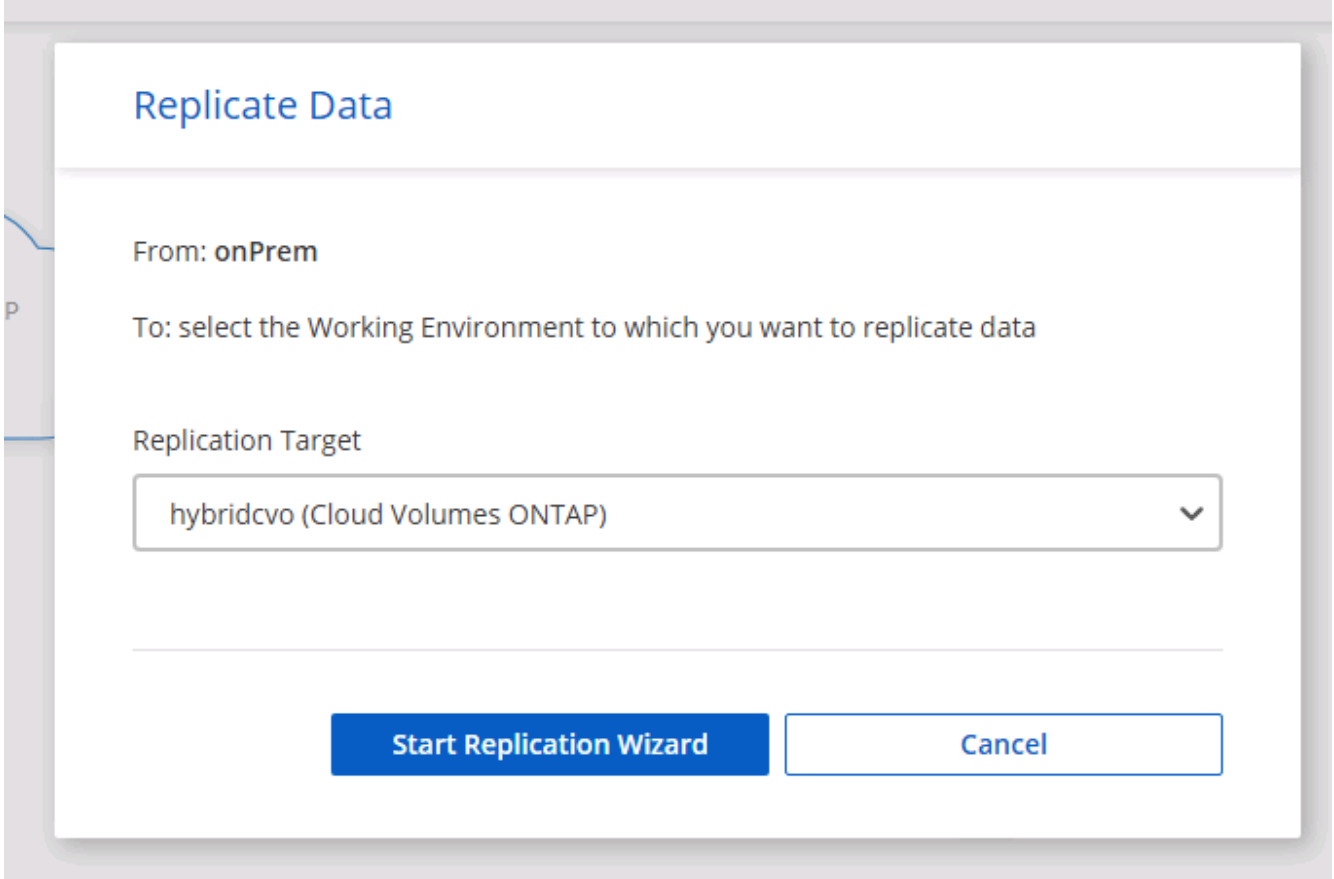
O Opzioni.



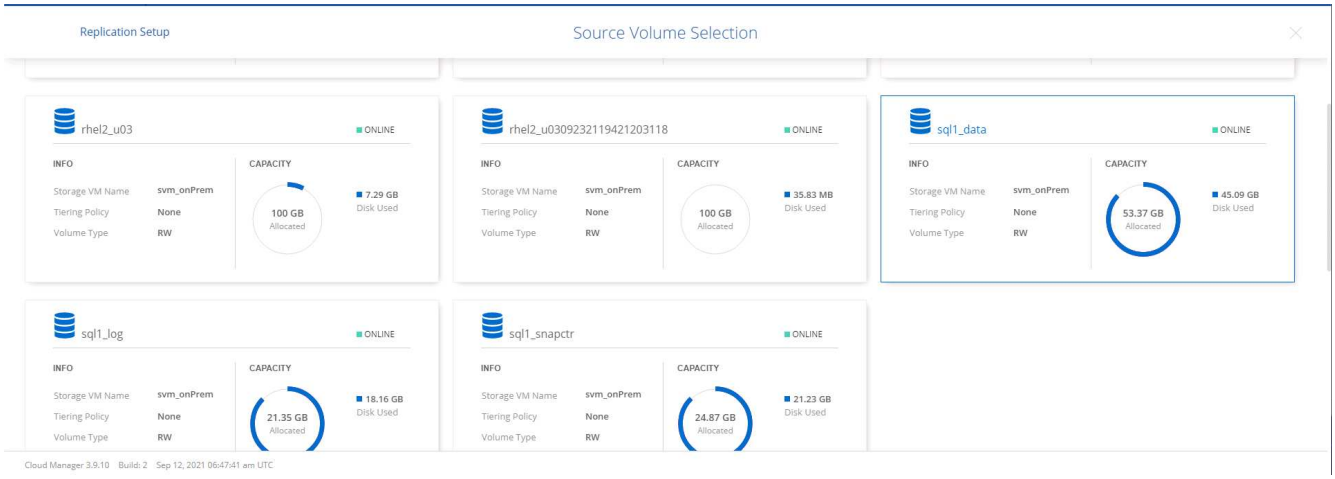
Replicare.



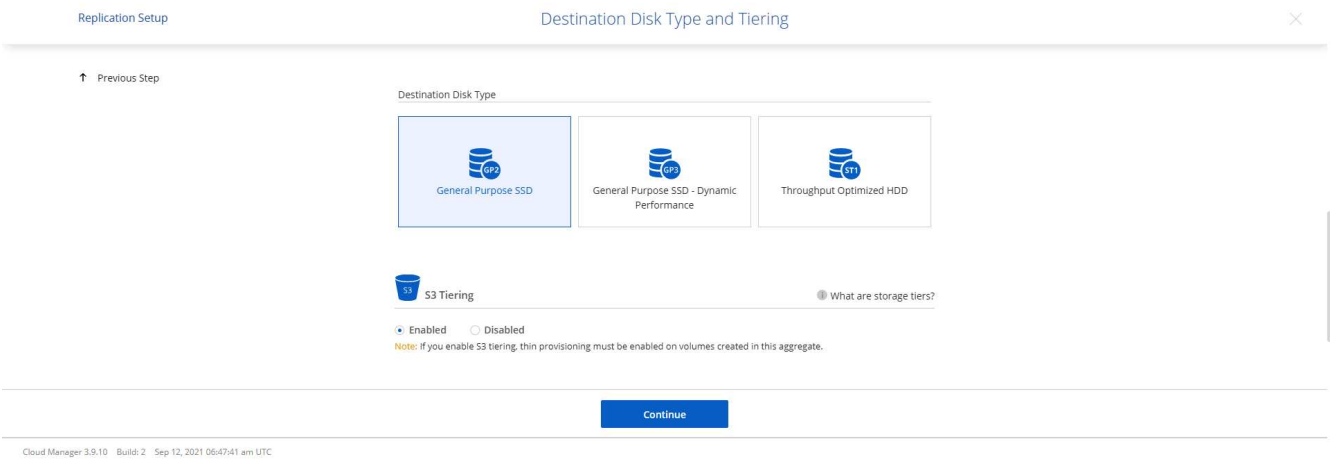
2. Se non è stato trascinato, scegliere il cluster di destinazione in cui replicare.



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

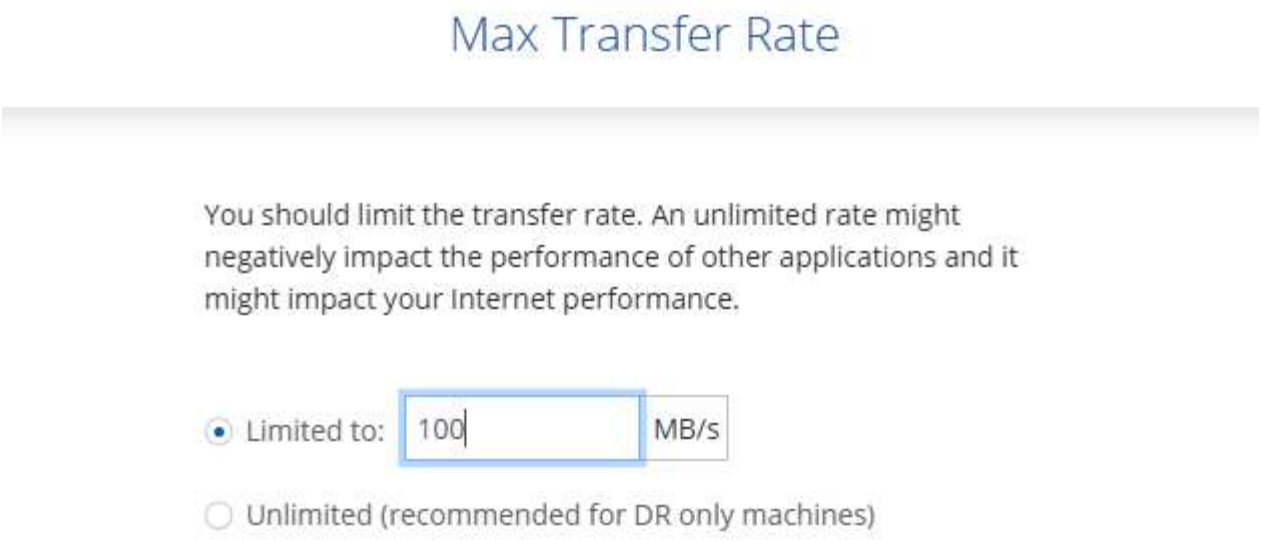


4. Scegliere il tipo di disco di destinazione e il criterio di tiering. Per il disaster recovery, consigliamo un SSD come tipo di disco e per mantenere il tiering dei dati. Il tiering dei dati tiering i dati mirrorati in storage a oggetti a basso costo e consente di risparmiare denaro sui dischi locali.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

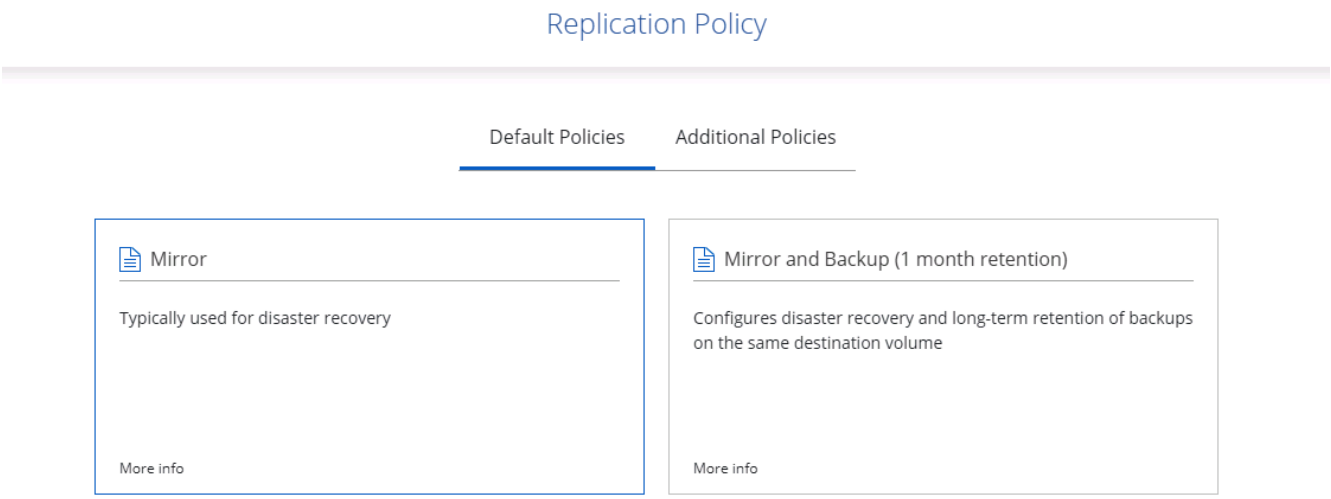


5. Selezionare il nome del volume di destinazione scelto `[source_volume_name]_dr`.

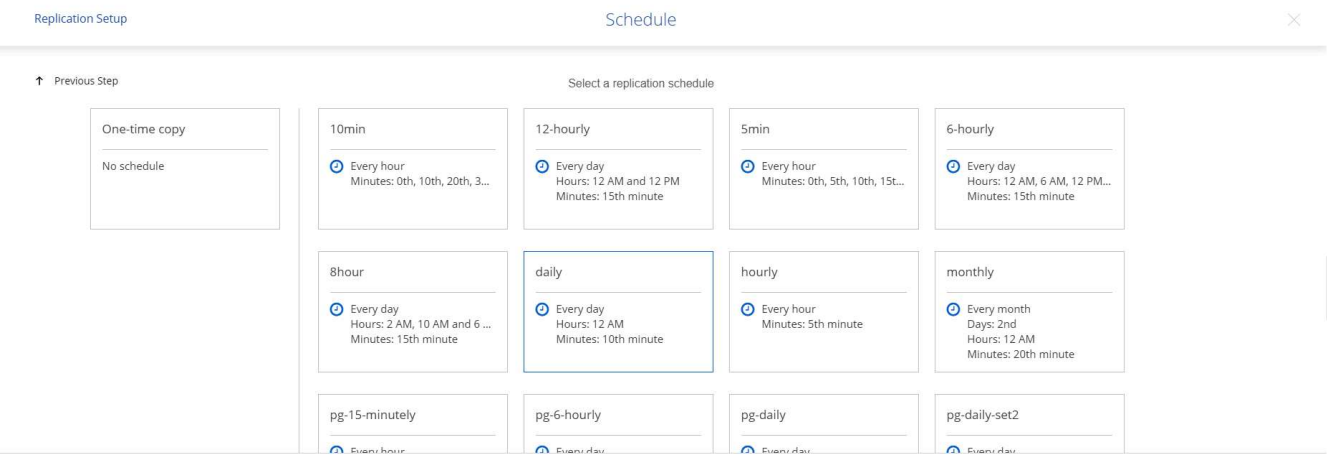
6. Selezionare la velocità di trasferimento massima per la replica. Ciò consente di risparmiare larghezza di banda se si dispone di una connessione a bassa larghezza di banda al cloud, ad esempio una VPN.



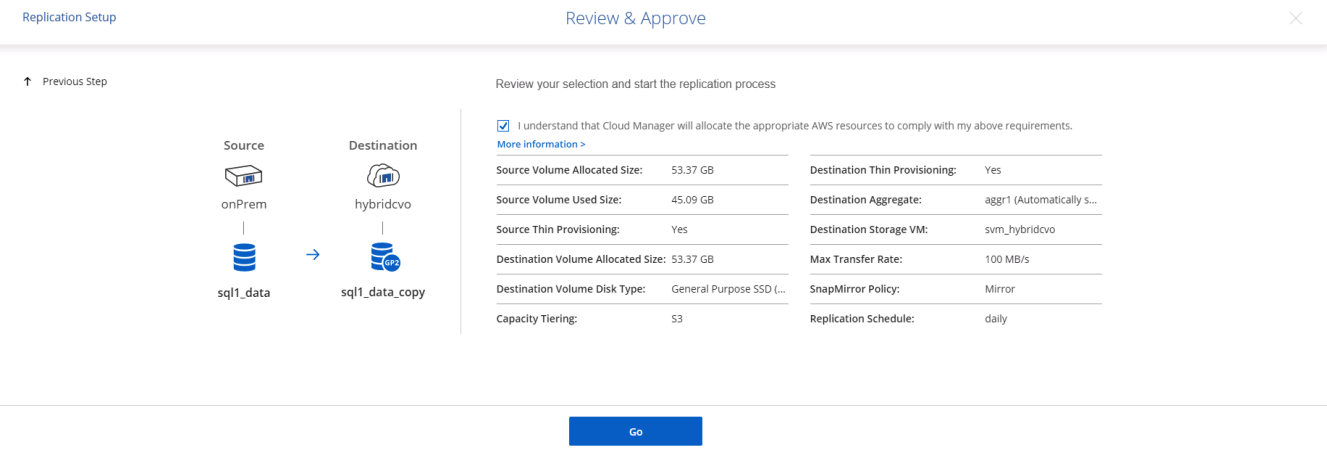
7. Definire il criterio di replica. Abbiamo scelto un Mirror, che prende i dataset più recenti e li replica nel volume di destinazione. Puoi anche scegliere una policy diversa in base ai tuoi requisiti.



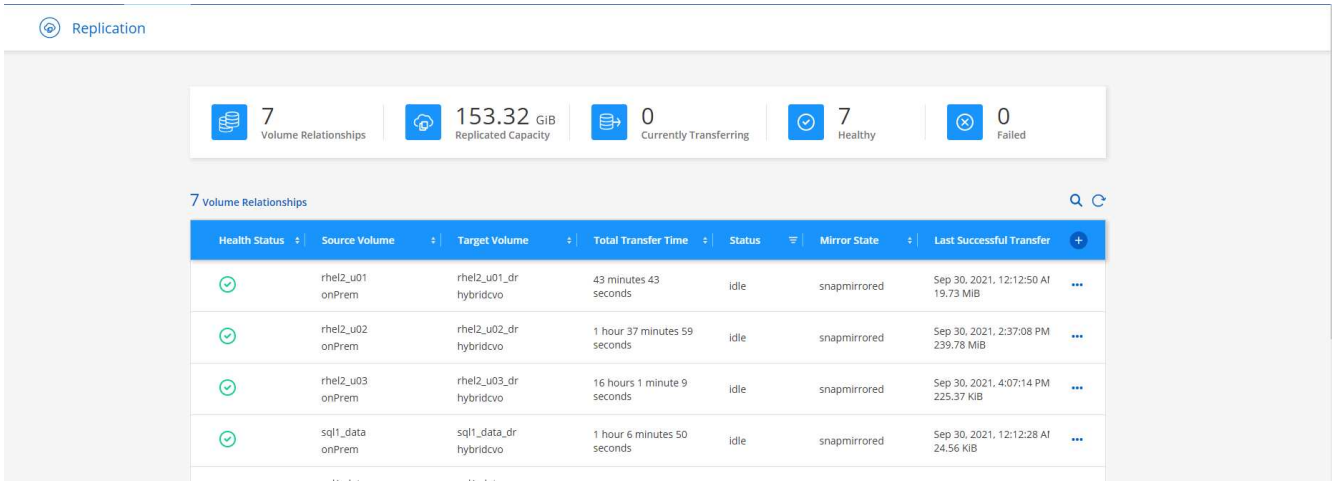
8. Scegliere la pianificazione per l'attivazione della replica. NetApp consiglia di impostare una pianificazione "giornaliera" di per il volume di dati e una pianificazione "oraria" per i volumi di log, sebbene sia possibile modificarla in base ai requisiti.



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".