Soluzioni di database cloud ibrido con SnapCenter

NetApp database solutions

NetApp
August 18, 2025

Sommario

Soluzioni di database cloud ibrido con SnapCenter

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

Alan Cao, Felix Melligan, NetApp

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

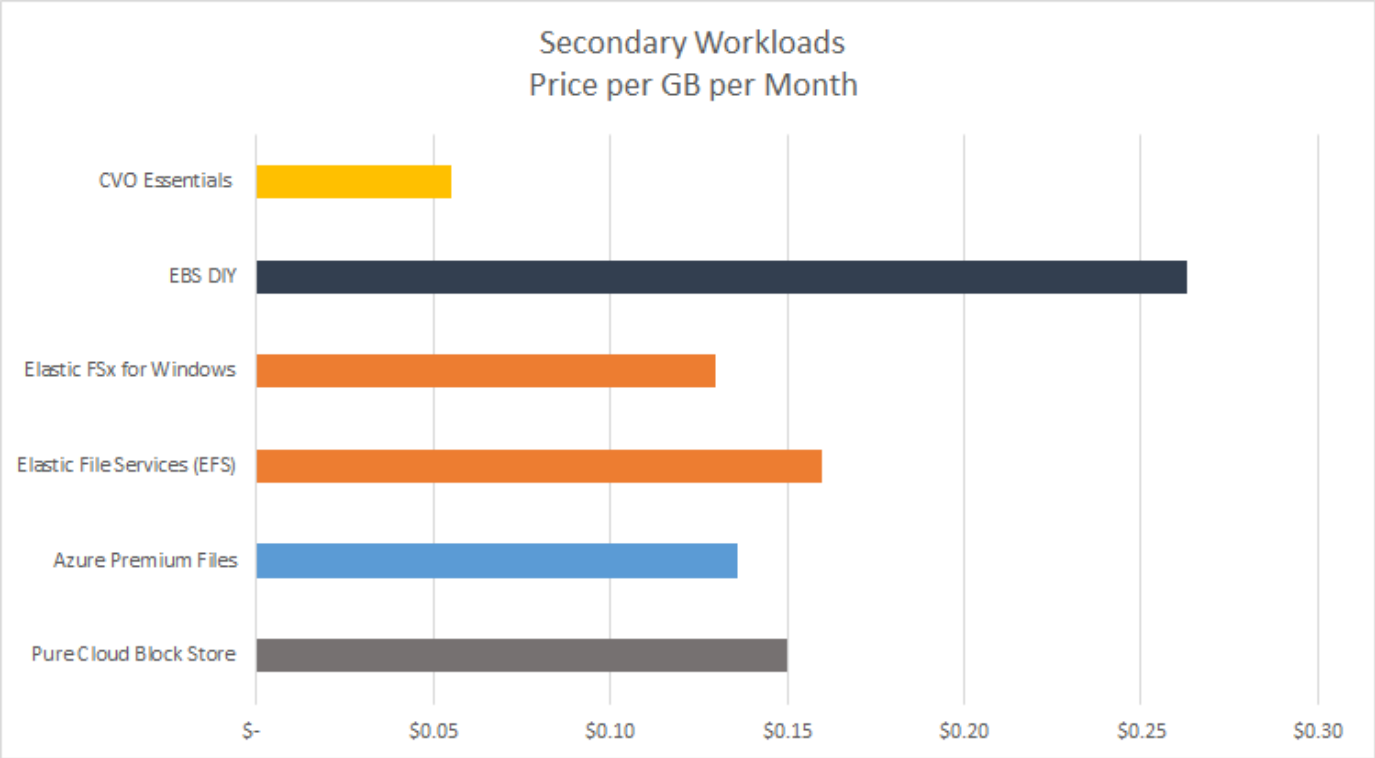
- Operazioni di sviluppo/test del database nel cloud ibrido
- Ripristino di emergenza del database nel cloud ibrido

Oggigiorno, molti database aziendali risiedono ancora in data center aziendali privati per motivi di prestazioni, sicurezza e/o altri motivi. Questa soluzione di database cloud ibrido consente alle aziende di gestire i propri database primari in loco, utilizzando al contempo un cloud pubblico per le operazioni di sviluppo/test del database e per il disaster recovery, riducendo così i costi operativi e di licenza.

Molti database aziendali, come Oracle, SQL Server, SAP HANA e così via, comportano costi di licenza e operativi elevati. Molti clienti pagano una quota di licenza una tantum e costi di supporto annuali in base al numero di core di elaborazione presenti nel loro ambiente di database, indipendentemente dal fatto che i core vengano utilizzati per sviluppo, test, produzione o ripristino di emergenza. Molti di questi ambienti potrebbero non essere sfruttati appieno durante l'intero ciclo di vita dell'applicazione.

Le soluzioni offrono ai clienti la possibilità di ridurre potenzialmente il numero di core concessi in licenza spostando sul cloud i propri ambienti di database dedicati allo sviluppo, ai test o al ripristino di emergenza. Utilizzando la scalabilità del cloud pubblico, la ridondanza, l'elevata disponibilità e un modello di fatturazione basato sul consumo, il risparmio sui costi di licenza e operatività può essere sostanziale, senza sacrificare l'usabilità o la disponibilità dell'applicazione.

Oltre al potenziale risparmio sui costi delle licenze del database, il modello di licenza CVO basato sulla capacità di NetApp consente ai clienti di risparmiare sui costi di storage per GB, offrendo loro al contempo un elevato livello di gestibilità del database non disponibile nei servizi di storage concorrenti. Il grafico seguente mostra un confronto dei costi di archiviazione dei servizi di archiviazione più diffusi disponibili nel cloud pubblico.



Questa soluzione dimostra che, utilizzando lo strumento software basato su GUI SnapCenter e la tecnologia NetApp SnapMirror , le operazioni di database cloud ibrido possono essere facilmente configurate, implementate e gestite.

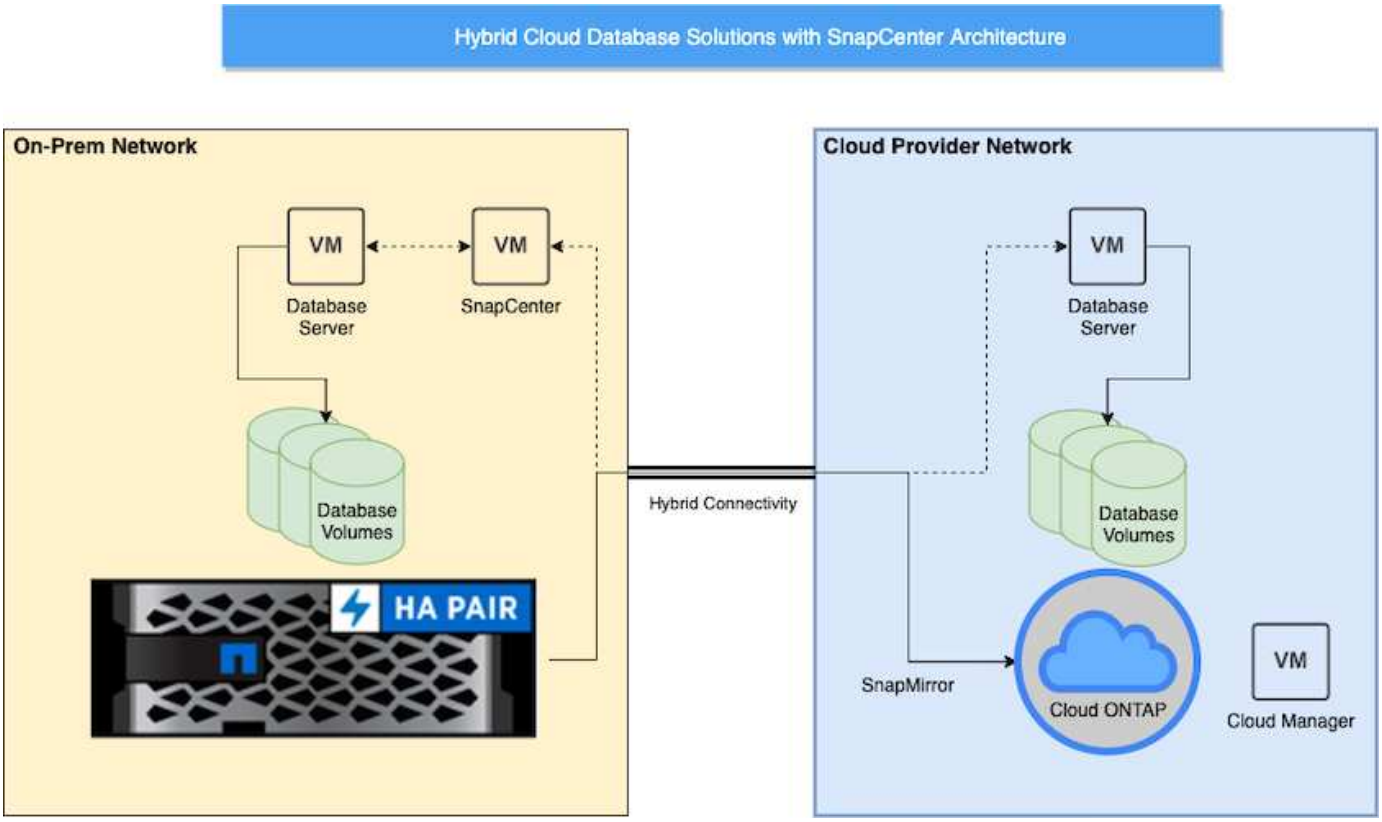
I seguenti video mostrano SnapCenter in azione:

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

In particolare, sebbene le illustrazioni presenti in questo documento mostrino CVO come istanza di storage di destinazione nel cloud pubblico, la soluzione è completamente convalidata anche per la nuova versione del motore di storage FSx ONTAP per AWS.

Architettura della soluzione

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



Nelle normali operazioni aziendali, 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 del database sincronizzati nel cloud possono essere attivati per il ripristino di emergenza.

Requisiti SnapCenter

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

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

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

Requisiti

Ambiente	Requisiti
In sede	Tutti i database e le versioni supportati da SnapCenter
	SnapCenter v4.4 o superiore
	Ansible v2.09 o superiore
	Cluster ONTAP 9.x
	Intercluster LIF configurati
	Connettività da locale 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"
	Abbinamento delle istanze DB OS EC2 a quelle locali
Cloud - Azzurro	"Connettore Cloud Manager"
	"Cloud Volumes ONTAP"
	Abbinamento delle macchine virtuali di Azure del sistema operativo DB a quelle locali
Cloud - GCP	"Connettore Cloud Manager"
	"Cloud Volumes ONTAP"
	Abbinamento delle istanze di Google Compute Engine del sistema operativo DB a quelle locali

Configurazione dei prerequisiti

Configurazione dei prerequisiti

Prima di eseguire carichi di lavoro di database cloud ibridi, è necessario configurare determinati prerequisiti sia in locale che nel cloud. La sezione seguente fornisce un riepilogo di alto livello di questo processo e i seguenti link forniscono ulteriori informazioni sulla configurazione di sistema necessaria.

In loco

- Installazione e configurazione SnapCenter
- Configurazione dell'archiviazione del server di database locale
- Requisiti di licenza
- Rete e sicurezza
- Automazione

Cloud pubblico

- Un accesso a NetApp Cloud Central

- Accesso alla rete da un browser web a più endpoint
- Una posizione di rete per un connettore
- Autorizzazioni del provider cloud
- Networking per servizi individuali

Considerazioni importanti:

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

Per ulteriori dettagli, consultare i seguenti "In sede"

"Cloud pubblico"

Prerequisiti in sede

Per preparare l'ambiente di carico di lavoro del database cloud ibrido SnapCenter , è necessario completare le seguenti attività in locale.

Installazione e configurazione SnapCenter

Lo strumento NetApp SnapCenter è un'applicazione basata su Windows che in genere viene eseguita in un ambiente di dominio Windows, sebbene sia possibile anche la distribuzione in gruppi di lavoro. Si basa su un'architettura multilivello che include un server di gestione centralizzato (il server SnapCenter) e un plug-in SnapCenter sugli host del server del database per i carichi di lavoro del database. Ecco alcune considerazioni chiave per l'implementazione del cloud ibrido.

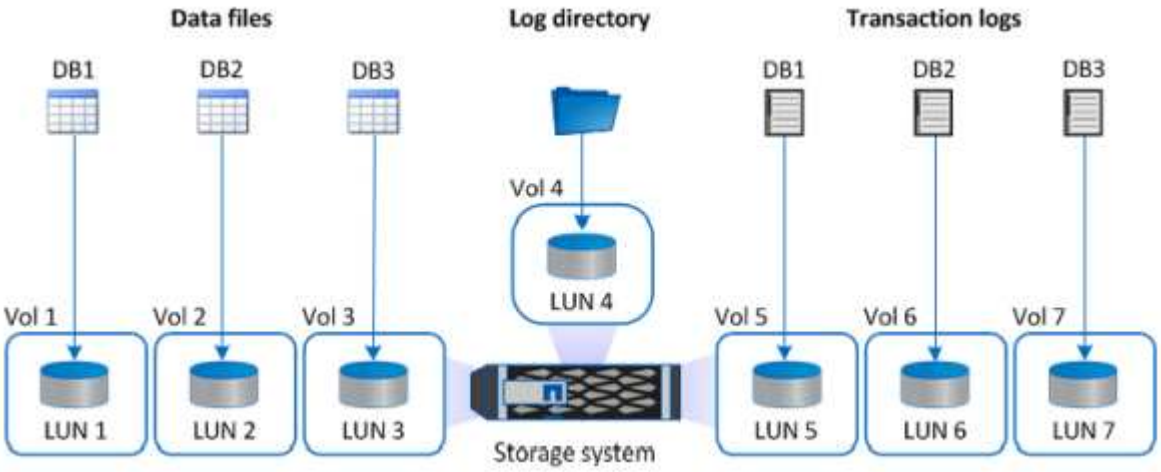
- **Distribuzione a istanza singola o HA.** L'implementazione HA garantisce ridondanza in caso di guasto di un singolo server di istanza SnapCenter .
- **Risoluzione del nome.** Il DNS deve essere configurato sul server SnapCenter per risolvere tutti gli host del database e anche sull'SVM di archiviazione per la ricerca diretta e inversa. Il DNS deve essere configurato anche sui server del database per risolvere il server SnapCenter e l'SVM di archiviazione per la ricerca diretta e inversa.
- **Configurazione del controllo degli accessi basato sui ruoli (RBAC).** Per carichi di lavoro di database misti, potrebbe essere opportuno utilizzare RBAC per separare la responsabilità di gestione per diverse piattaforme DB, ad esempio un amministratore per il database Oracle o un amministratore per SQL Server. È necessario concedere le autorizzazioni necessarie all'utente amministratore del database.
- **Abilita la 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 locale di comunicare con gli agenti installati nell'host del database cloud.
- **Le porte devono essere aperte per consentire il traffico SnapMirror tra il cloud locale e quello pubblico.** Il server SnapCenter si basa su ONTAP SnapMirror per replicare i backup Snapshot in loco su SVM di storage CVO cloud.

Dopo un'attenta pianificazione e valutazione pre-installazione, fare clic qui"Prerequisiti per l'installazione di SnapCenter" per i dettagli sull'installazione e la configurazione di SnapCenter .

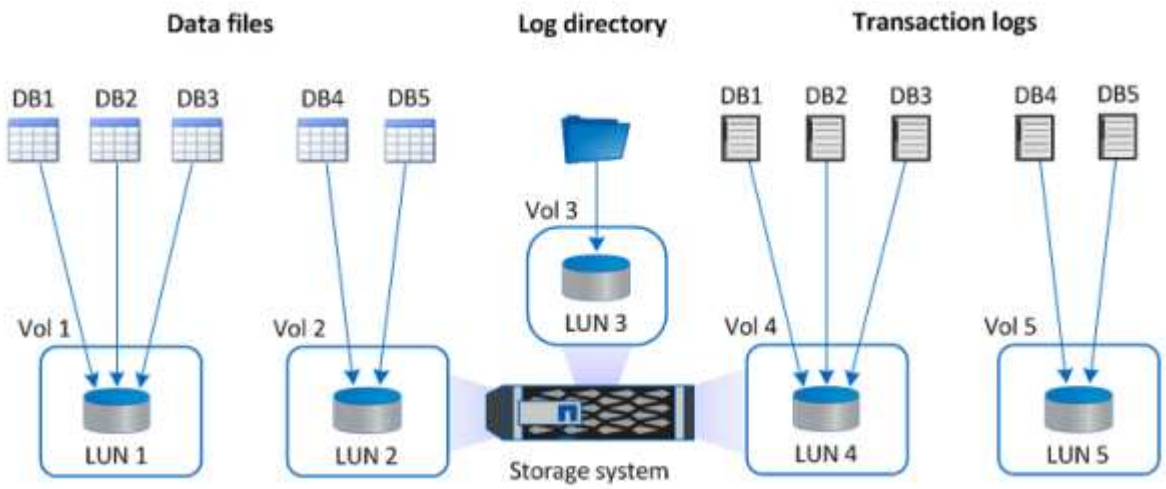
Configurazione dell'archiviazione del server di database locale

Le prestazioni di archiviazione svolgono un ruolo importante nelle prestazioni complessive di database e applicazioni. Un layout di archiviazione ben progettato può non solo migliorare le prestazioni del database, ma anche semplificare la gestione del backup e del ripristino del database. Quando si definisce il layout di archiviazione, è necessario considerare diversi fattori, tra cui le dimensioni del database, la frequenza di modifica prevista dei dati per il database e la frequenza con cui si eseguono i backup.

Il collegamento diretto di LUN di storage alla VM guest tramite NFS o iSCSI per carichi di lavoro di database virtualizzati garantisce in genere prestazioni migliori rispetto allo storage allocato tramite VMDK. NetApp consiglia il layout di archiviazione per un database SQL Server di grandi dimensioni su LUN illustrato nella figura seguente.



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



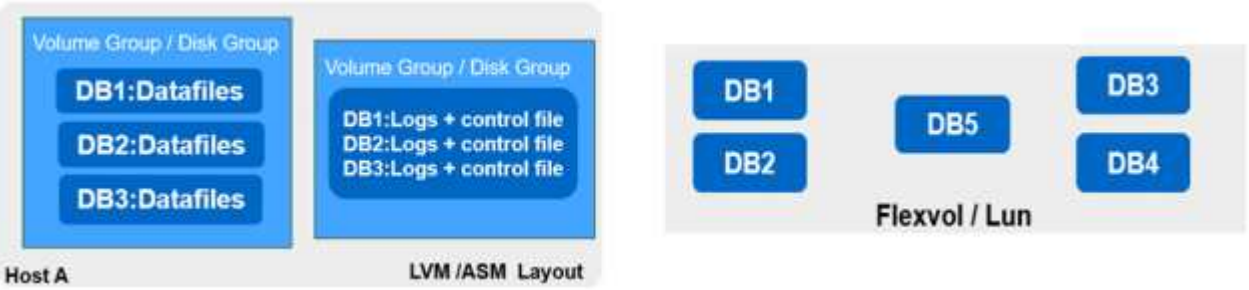
La directory Log è dedicata a SnapCenter per eseguire il rollup del registro delle transazioni per il ripristino del database. Per un database di grandi dimensioni, è possibile allocare più LUN a un volume per ottenere prestazioni migliori.

Per i carichi di lavoro del database Oracle, SnapCenter supporta ambienti di database supportati da storage ONTAP montati sull'host come dispositivi fisici o virtuali. È possibile ospitare l'intero database su uno o più dispositivi di archiviazione in base alla criticità dell'ambiente. In genere, i clienti isolano i file di dati su un

archivio dedicato da tutti gli altri file, come i file di controllo, i file di ripristino e i file di registro di archivio. Ciò aiuta gli amministratori a ripristinare rapidamente (ONTAP single-file SnapRestore) o a clonare un database critico di grandi dimensioni (su scala petabyte) utilizzando la tecnologia Snapshot in pochi secondi o minuti.

Per carichi di lavoro critici per la missione sensibili alla latenza, è opportuno distribuire un volume di archiviazione 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 ne consiglia fino a otto) per volume ai file di dati.

Per i database Oracle più piccoli, SnapCenter supporta layout di archiviazione condivisi in cui è possibile ospitare più database o parte di un database sullo stesso volume di archiviazione 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 su un gruppo di volumi. I file rimanenti (redo, registro di archivio e file di controllo) possono essere ospitati su un altro gruppo di dischi o gruppo di volumi (LVM) dedicato. Di seguito è illustrato uno scenario di distribuzione di questo tipo.



Per facilitare lo spostamento dei database Oracle, il binario Oracle deve essere installato su una LUN separata inclusa nella normale policy di backup. Ciò garantisce che, in caso di trasferimento del database su un nuovo host server, lo stack Oracle possa 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. In genere è incluso in una licenza ONTAP locale. Tuttavia, per la distribuzione cloud ibrida, è necessaria anche una licenza cloud per SnapCenter per aggiungere CVO a SnapCenter come destinazione di replicazione dei dati. Per maggiori dettagli, consultare i seguenti link per la licenza basata sulla capacità standard SnapCenter :

"Licenze basate sulla capacità standard SnapCenter"

Rete e sicurezza

In un'operazione di database ibrido che richiede un database di produzione locale con supporto burst nel cloud per sviluppo/test e ripristino di emergenza, la rete e la sicurezza sono fattori importanti da considerare quando si configura l'ambiente e ci si connette al cloud pubblico da un data center locale.

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

La connettività dal data center locale alla VPC può essere protetta tramite un tunnel VPN. Sul gateway VPN, la sicurezza può essere rafforzata utilizzando 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 alla rete e alla sicurezza, rivedi le regole CVO in entrata e in uscita pertinenti per il cloud pubblico che hai scelto:

- "Regole del gruppo di sicurezza per CVO - AWS"
- "Regole del gruppo di sicurezza per CVO - Azure"
- "Regole del firewall per CVO - GCP"

Utilizzo dell'automazione Ansible per sincronizzare le istanze DB tra locale e cloud (facoltativo)

Per semplificare la gestione di un ambiente di database cloud ibrido, NetApp consiglia vivamente, ma non richiede, di distribuire un controller Ansible per automatizzare alcune attività di gestione, come mantenere sincronizzate le istanze di elaborazione in locale e nel cloud. Ciò è particolarmente importante perché un'istanza di elaborazione non sincronizzata nel cloud potrebbe rendere il database recuperato nel cloud soggetto a errori a causa di pacchetti kernel mancanti e altri problemi.

La capacità di automazione di un controller Ansible può essere utilizzata anche per potenziare SnapCenter per determinate attività, ad esempio suddividendo l'istanza di SnapMirror per attivare la copia dei dati DR per la produzione.

Segui queste istruzioni per configurare il tuo nodo di controllo Ansible per macchine RedHat o CentOS:

1. Requisiti per il nodo di controllo Ansible:
    a. Una macchina RHEL/CentOS con i seguenti pacchetti installati:
        i. Python3
        ii. Pip3
        iii. Ansible (versione successiva alla 2.10.0)
        iv. Git

Se si dispone di una nuova macchina RHEL/CentOS senza i requisiti sopra indicati installati, seguire i passaggi sottostanti per configurare tale macchina come nodo di controllo Ansible:

1. Abilita il repository Ansible per RHEL-8/RHEL-7
    a. Per RHEL-8 (eseguire il comando sottostante come root)

```
subscription-manager repos --enable ansible-2.9-for-rhel-8-x86_64-
rpms
```

b. Per RHEL-7 (eseguire il comando sottostante come root)

```
subscription-manager repos --enable rhel-7-server-ansible-2.9-rpms
```

2. Incolla il contenuto sottostante nel Terminale

```
sudo yum -y install python3 >> install.log
sudo yum -y install python3-pip >> install.log
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
install.log
sudo yum -y install git >> install.log
```

Segui queste istruzioni per configurare il tuo nodo di controllo Ansible per macchine Ubuntu o Debian:

1. Requisiti per il nodo di controllo Ansible:
   a. Una macchina Ubuntu/Debian con i seguenti pacchetti installati:
      i. Python3
      ii. Pip3
      iii. Ansible (versione successiva alla 2.10.0)
      iv. Git

Se si dispone di una nuova macchina Ubuntu/Debian senza i requisiti sopra indicati installati, seguire i passaggi sottostanti per configurare tale macchina come nodo di controllo Ansible:

1. Incolla il contenuto sottostante nel terminale

```
sudo apt-get -y install python3 >> outputlog.txt
sudo apt-get -y install python3-pip >> outputlog.txt
python3 -W ignore -m pip --disable-pip-version-check install ansible >>
outputlog.txt
sudo apt-get -y install git >> outputlog.txt
```

Prerequisiti per il cloud pubblico

Prima di installare il connettore Cloud Manager e Cloud Volumes ONTAP e configurare SnapMirror, dobbiamo eseguire alcune operazioni di preparazione per il nostro ambiente cloud. Questa pagina descrive il lavoro da svolgere e le considerazioni da tenere a mente quando si distribuisce Cloud Volumes ONTAP.

Elenco di controllo dei prerequisiti per la distribuzione di Cloud Manager e Cloud Volumes ONTAP

- Un accesso a NetApp Cloud Central
- Accesso alla rete da un browser web a più endpoint
- Una posizione di rete per un connettore
- Autorizzazioni del provider cloud
- Networking per servizi individuali

Per maggiori 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, l'amministratore di un account Cloud Central deve distribuire un connettore nel cloud o nella rete locale. Il connettore consente a Cloud Manager di gestire risorse e processi all'interno del tuo ambiente cloud pubblico.

Per maggiori informazioni sui connettori, visita il nostro "documentazione cloud" .

2. Dimensionamento e architettura Cloud Volumes ONTAP

Quando si distribuisce Cloud Volumes ONTAP, è possibile scegliere tra un pacchetto predefinito o la creazione di una configurazione personalizzata. Sebbene molti di questi valori possano essere modificati in un secondo momento senza interruzioni, ci sono alcune decisioni chiave che devono essere prese prima della distribuzione in base ai carichi di lavoro da distribuire nel cloud.

Ogni provider cloud offre diverse opzioni di distribuzione e quasi ogni carico di lavoro ha le sue proprietà uniche. NetApp ha un "Calcolatore TCO" che può aiutare a dimensionare correttamente le distribuzioni in base alla capacità e alle prestazioni, ma è stato costruito attorno ad alcuni concetti di base che vale la pena considerare:

- Capacità richiesta
- Capacità di rete della macchina virtuale cloud
- Caratteristiche prestazionali dell'archiviazione cloud

La chiave è pianificare una configurazione che non solo soddisfi i requisiti attuali di capacità e prestazioni, ma che tenga anche conto della crescita futura. Questo è generalmente noto come margine di capacità e margine di prestazioni.

Se desideri ulteriori informazioni, leggi la documentazione sulla pianificazione corretta per "AWS" , "Azzurro" , E "GCP" .

3. Nodo singolo o alta disponibilità?

In tutti i cloud è possibile distribuire CVO in un singolo nodo o in una coppia ad alta disponibilità in cluster con due nodi. A seconda del caso d'uso, potrebbe essere opportuno distribuire un singolo nodo per risparmiare sui costi oppure una coppia HA per garantire maggiore disponibilità e ridondanza.

Per un caso d'uso di DR o per l'avvio di un archivio temporaneo per lo sviluppo e il test, i nodi singoli sono comuni poiché l'impatto di un'interruzione improvvisa di una zona o dell'infrastruttura è inferiore. Tuttavia, per qualsiasi caso d'uso di produzione, quando i dati si trovano in un'unica posizione o quando il set di dati deve avere maggiore ridondanza e disponibilità, si consiglia l'elevata disponibilità.

Per ulteriori informazioni sull'architettura di ogni versione di alta disponibilità del cloud, visitare la documentazione per "AWS" , "Azzurro" E "GCP" .

Panoramica introduttiva

Panoramica introduttiva

Questa sezione fornisce un riepilogo delle attività che devono essere completate per soddisfare i requisiti preliminari descritti nella sezione precedente. La sezione seguente fornisce un elenco di attività di alto livello per le operazioni sia in locale che nel cloud pubblico. È possibile accedere ai processi e alle procedure dettagliate cliccando sui link pertinenti.

In sede

- Imposta l'utente amministratore del database in SnapCenter
- Prerequisiti per l'installazione del plugin SnapCenter
- Installazione del plugin host SnapCenter
- Rilevamento delle risorse del database
- Configurazione del peering del cluster di archiviazione e della replica del volume DB
- Aggiungere l'SVM di archiviazione del database CVO a SnapCenter
- Imposta la policy di backup del database in SnapCenter
- Implementare una politica di backup per proteggere il database
- Convalida il backup

Cloud pubblico AWS

- Controllo pre-volo
- Passaggi per distribuire Cloud Manager e Cloud Volumes ONTAP in AWS
- Distribuisci l'istanza di elaborazione EC2 per il carico di lavoro del database

Per maggiori dettagli cliccare sui seguenti "In sede","Cloud pubblico - AWS"

Iniziare in sede

Lo strumento NetApp SnapCenter utilizza il controllo degli accessi basato sui ruoli (RBAC) per gestire l'accesso alle risorse utente e le concessioni di autorizzazioni, mentre l'installazione SnapCenter crea ruoli precompilati. Puoi anche creare ruoli personalizzati in base alle tue esigenze o applicazioni.

In sede

1. Imposta l'utente amministratore del database in SnapCenter

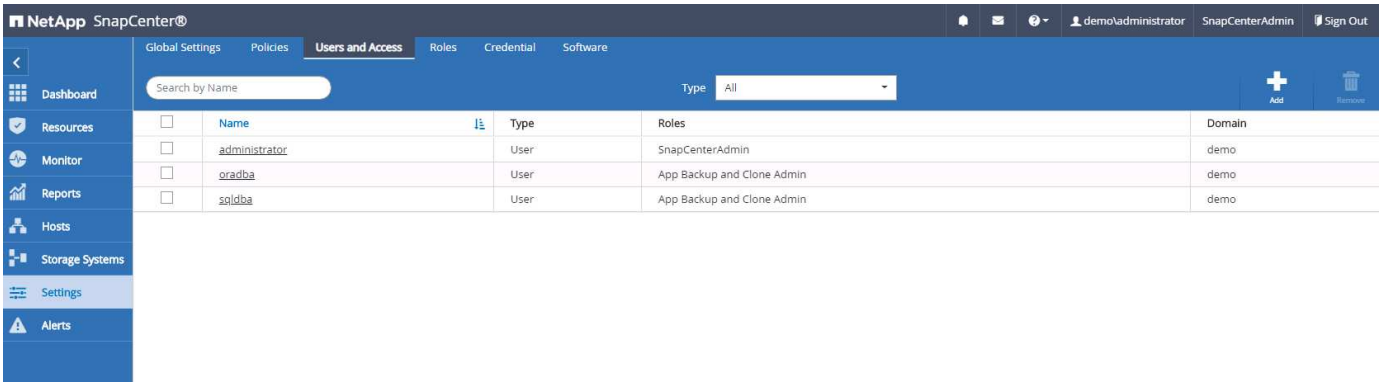
Ha senso avere un ID utente amministratore dedicato per ogni piattaforma di database supportata da SnapCenter per il backup, il ripristino e/o il ripristino di emergenza del database. È anche possibile utilizzare

un unico ID per gestire tutti i database. Nei nostri casi di prova e nella dimostrazione, abbiamo creato un utente amministratore dedicato rispettivamente per Oracle e SQL Server.

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, procedere come segue per creare un utente amministratore del database:

1. Aggiungere l'utente amministratore a Windows Active Directory.
2. Accedi a SnapCenter utilizzando un ID concesso con il ruolo SnapCenterAdmin.
3. Passare alla scheda Accesso in Impostazioni e Utenti e fare clic su Aggiungi per aggiungere un nuovo utente. Il nuovo ID utente è collegato all'utente amministratore creato in Windows Active Directory nel passaggio 1. . Assegnare il ruolo appropriato all'utente, secondo necessità. Assegnare le risorse all'utente amministratore, se applicabile.



2. Prerequisiti per l'installazione del plugin SnapCenter

SnapCenter esegue backup, ripristino, clonazione e altre funzioni utilizzando un agente plugin 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 dei plugin e altre funzioni di gestione. Esistono requisiti di privilegi specifici 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 plugin SnapCenter . In genere, è consigliabile utilizzare un account utente amministratore sull'host DB come credenziali di connessione all'host per l'installazione del plugin. È anche possibile concedere lo stesso ID utente per l'accesso al database utilizzando l'autenticazione basata sul sistema operativo. D'altro canto, è anche 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, all'ID utente amministratore del sistema operativo deve essere concesso l'accesso al database. Per l'installazione di SQL Server basata su dominio Windows, è possibile utilizzare un account amministratore di dominio per gestire tutti i server SQL all'interno del dominio.

Host Windows per SQL Server:

1. Se si utilizzano le credenziali di Windows per l'autenticazione, è necessario impostare le credenziali prima di installare i plugin.
2. Se si utilizza un'istanza di SQL Server per l'autenticazione, è necessario aggiungere le credenziali dopo aver installato i plugin.
3. Se hai abilitato l'autenticazione SQL durante la configurazione delle credenziali, l'istanza o il database individuato viene visualizzato con un'icona a forma di lucchetto rosso. Se viene visualizzata l'icona del

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 le credenziali a un utente RBAC senza accesso sysadmin quando sono 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 del database RBAC deve disporre sia dei privilegi di gruppo di risorse che di backup.

Host Unix per Oracle:

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

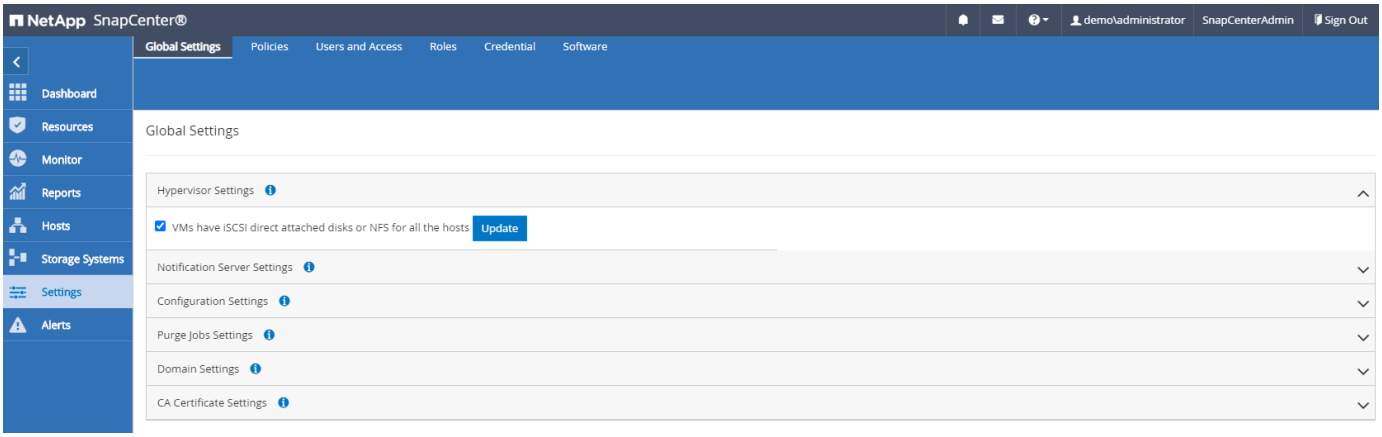
3. Installazione del plugin host SnapCenter

Prima di provare a installare i plugin SnapCenter sulle istanze del server DB cloud, assicurarsi che tutti i passaggi di configurazione siano stati completati come elencato nella sezione cloud pertinente per la distribuzione delle istanze di calcolo.

I passaggi seguenti illustrano come aggiungere un host di database a SnapCenter mentre un plug-in SnapCenter è installato sull'host. La procedura si applica sia all'aggiunta di host locali che di host cloud. La seguente dimostrazione aggiunge un host Windows o Linux residente in AWS.

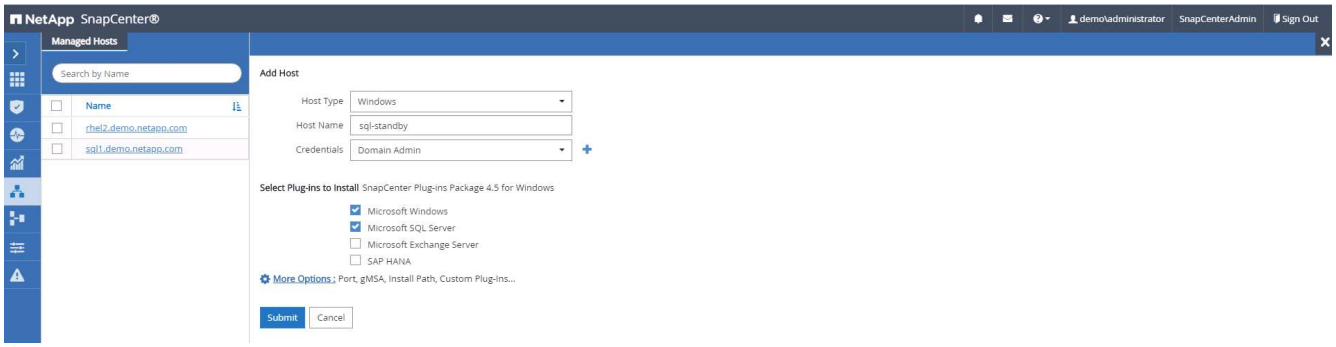
Configurare le impostazioni globali di SnapCenter VMware

Vai su Impostazioni > Impostazioni globali. Selezionare "Le VM hanno dischi collegati direttamente iSCSI o NFS per tutti gli host" in Impostazioni hypervisor e fare clic su Aggiorna.



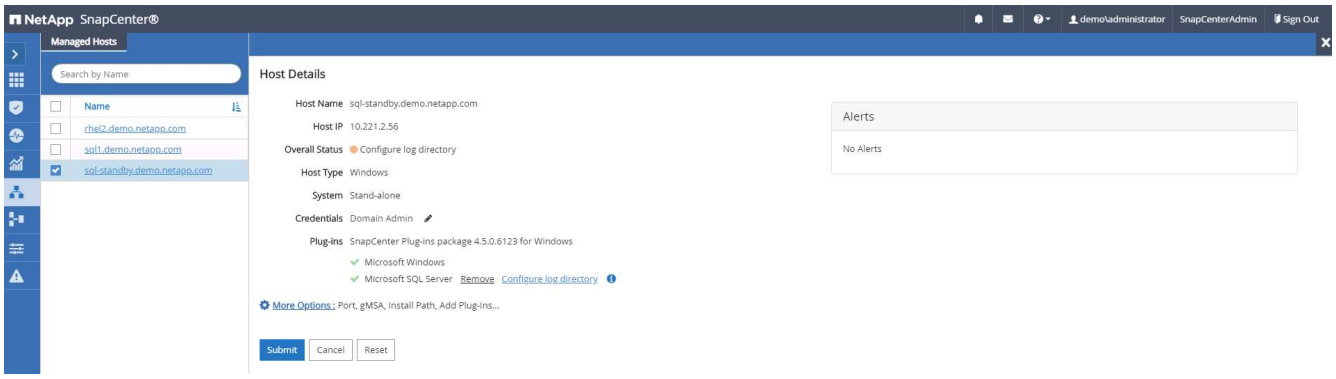
Aggiungi host Windows e installazione del plugin sull'host

1. Accedi a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda Host dal menu a sinistra, quindi fare clic su Aggiungi per aprire il flusso di lavoro Aggiungi host.
3. Selezionare Windows per Tipo di host; il Nome host può essere un nome host o un indirizzo IP. Il nome host deve essere risolto nell'indirizzo IP host corretto dall'host SnapCenter . Selezionare le credenziali host create nel passaggio 2. Selezionare Microsoft Windows e Microsoft SQL Server come pacchetti plugin da installare.

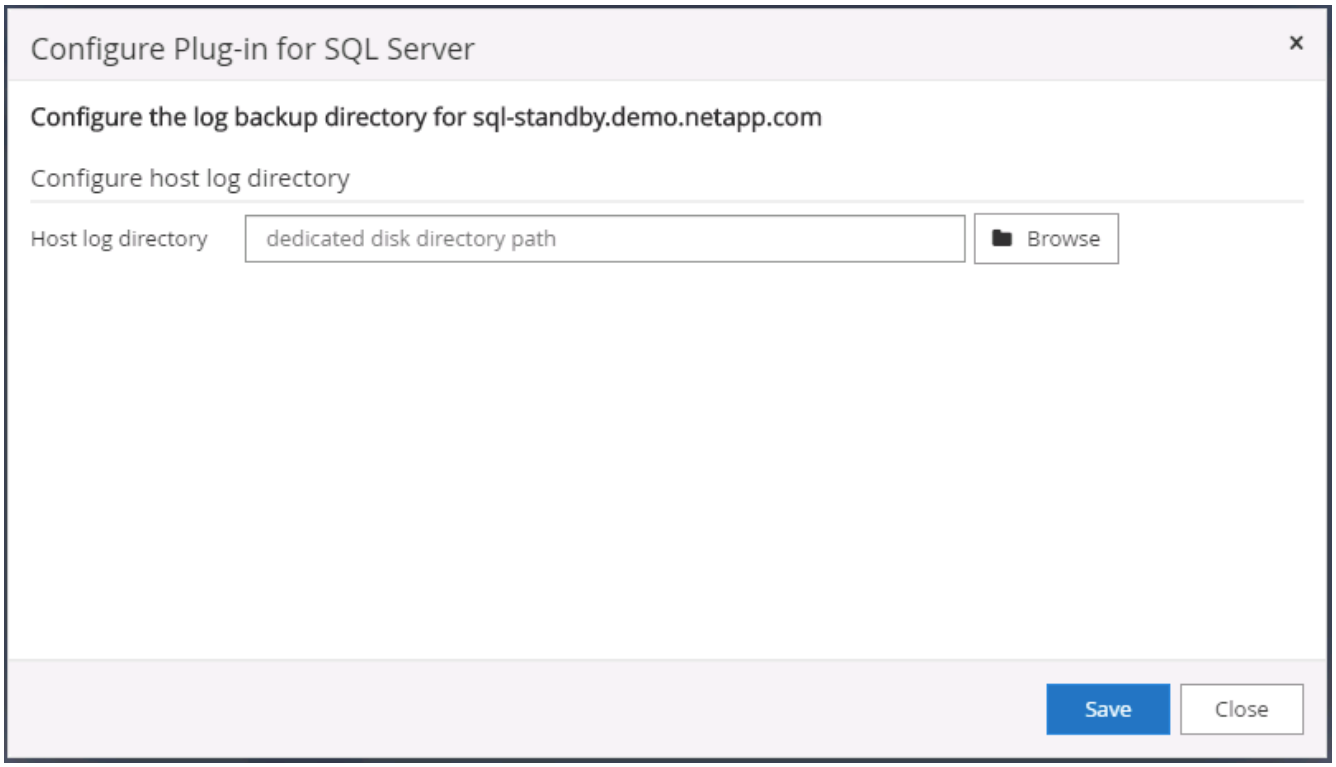


4. Dopo aver installato il plugin su un host Windows, il suo stato generale viene visualizzato come "Configura directory di registro".

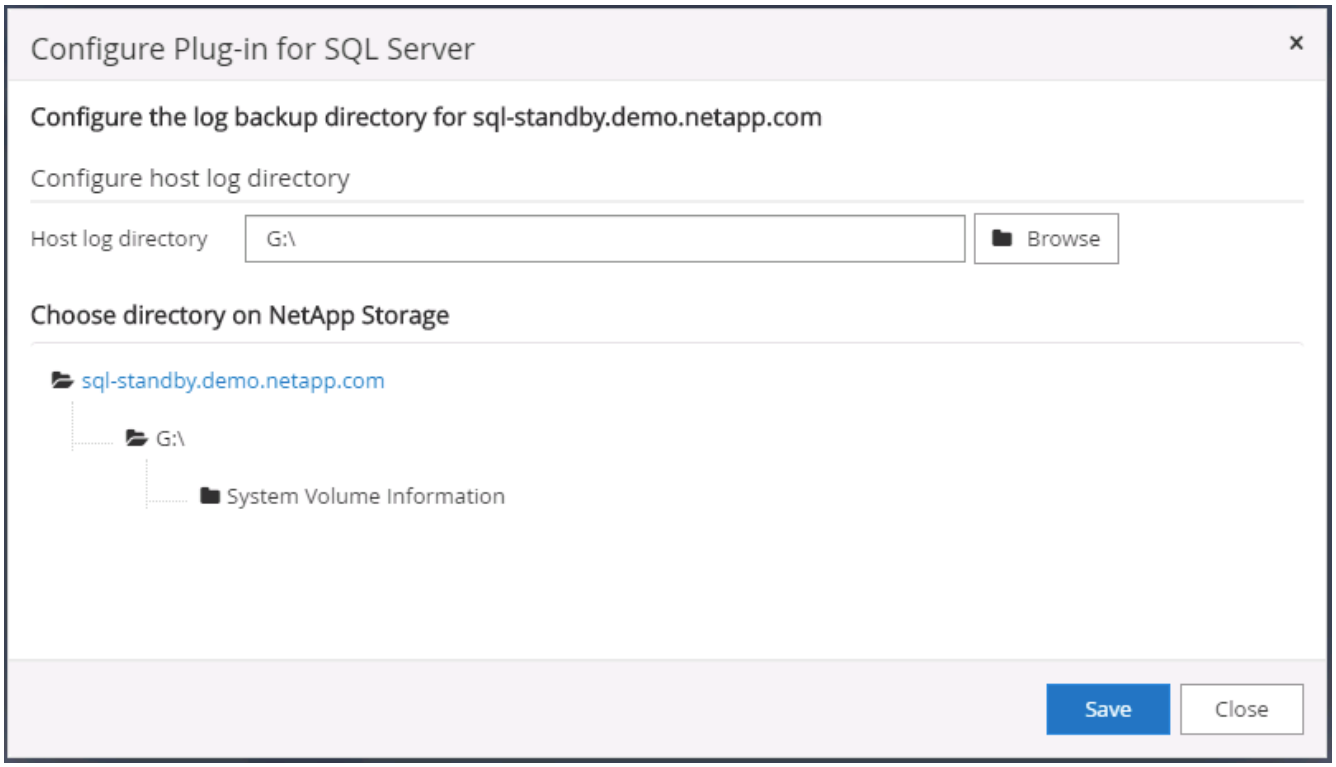
5. Fare clic sul nome host per aprire la configurazione della directory dei log di SQL Server.



6. Fare clic su "Configura directory di registro" per aprire "Configura plug-in per SQL Server".

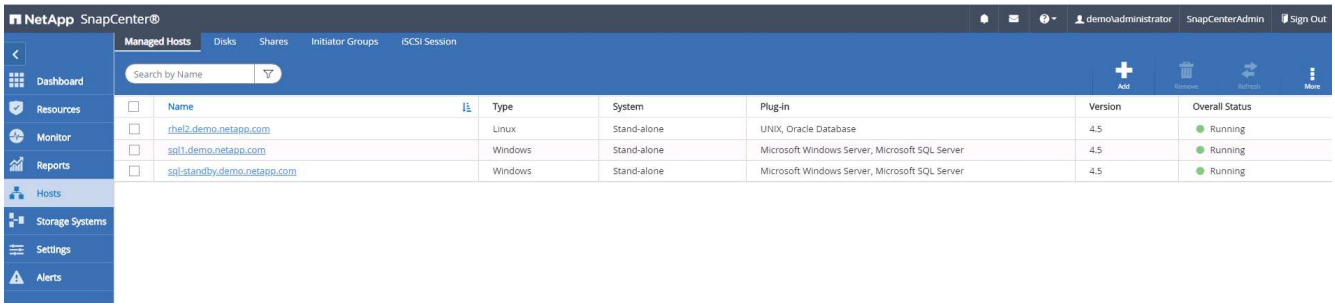


7. Fare clic su Sfoglia per individuare lo storage NetApp in modo da poter impostare una directory di registro; SnapCenter utilizza questa directory di registro per eseguire il rollup dei file di registro delle transazioni del server SQL. Quindi fare clic su Salva.

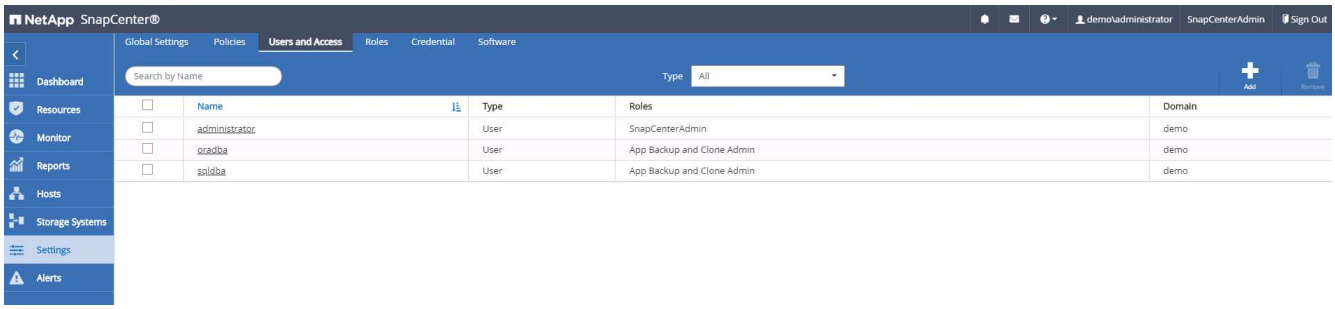


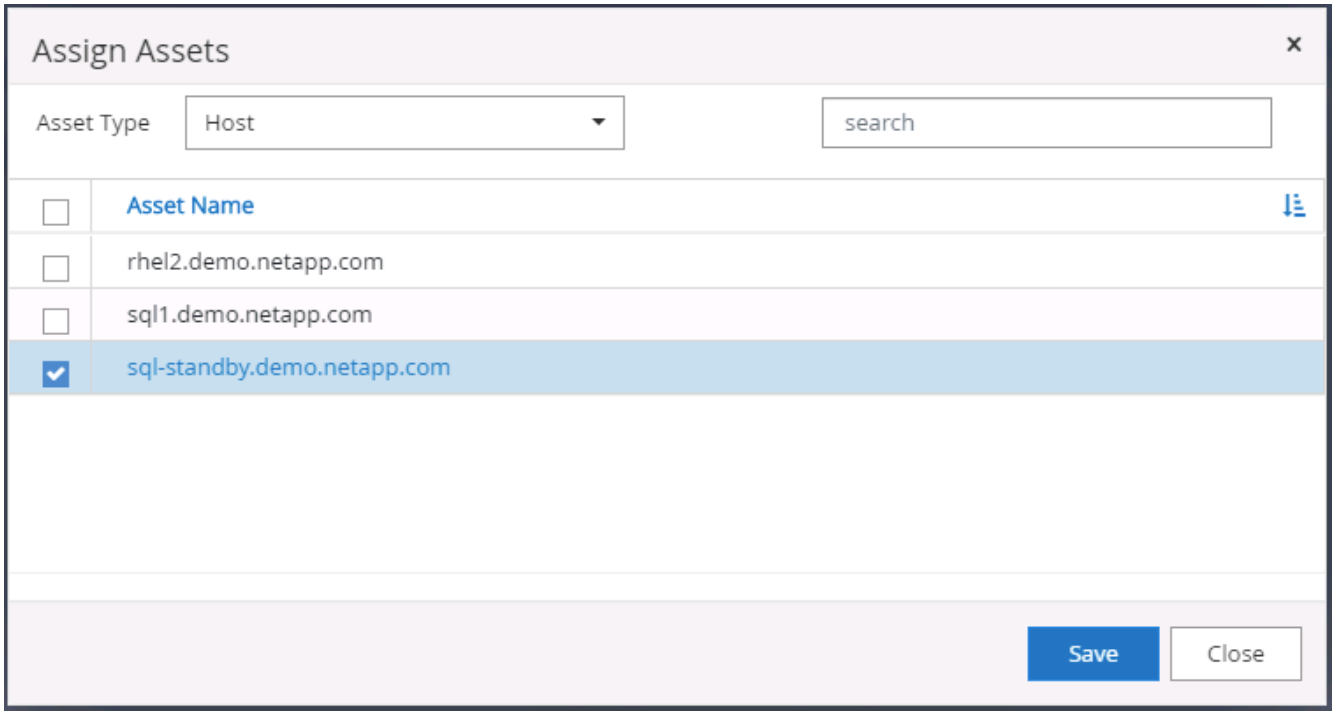
Per poter rilevare lo storage NetApp fornito a un host DB, è necessario aggiungere lo storage (on-prem o CVO) a SnapCenter, come illustrato nel passaggio 6 per CVO come esempio.

8. Dopo aver configurato la directory del registro, lo stato generale del plug-in host di Windows viene modificato in In esecuzione.



9. Per assegnare l'host all'ID utente di gestione del database, accedere alla scheda Accesso in Impostazioni e utenti, fare clic sull'ID utente di gestione del database (nel nostro caso l'sqldba a cui deve essere assegnato l'host) e fare clic su Salva per completare l'assegnazione delle risorse dell'host.

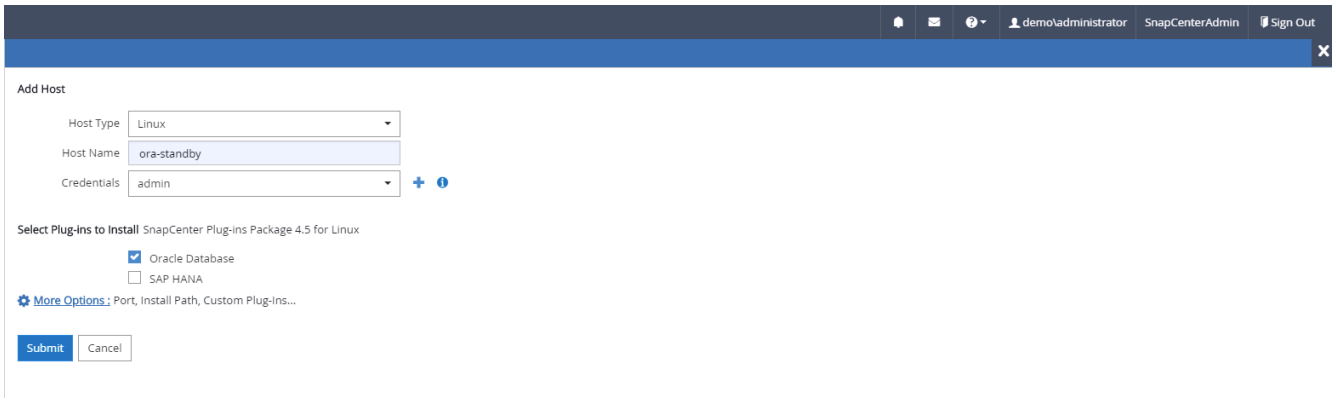




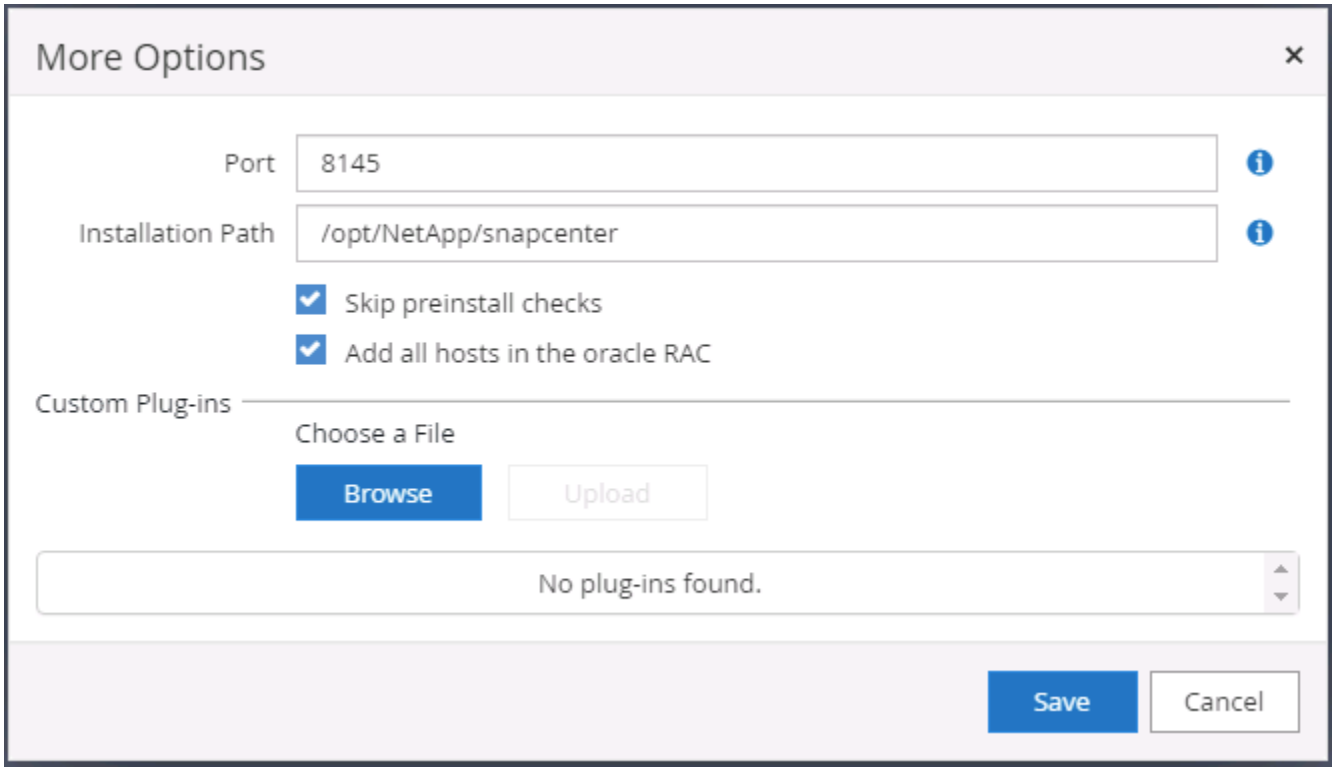
Aggiungi host Unix e installazione del plugin sull'host

1. Accedi a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda Host dal menu a sinistra e fare clic su Aggiungi per aprire il flusso di lavoro Aggiungi host.

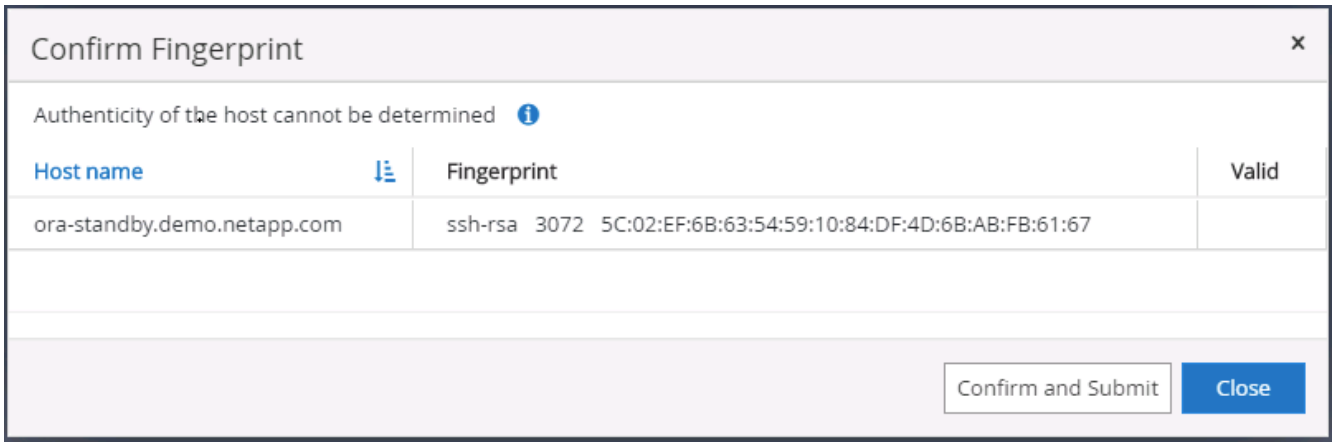
3. Selezionare Linux come tipo di host. Il nome host può essere il nome host o un indirizzo IP. Tuttavia, il nome host deve essere risolto nell'indirizzo IP host corretto dall'host SnapCenter . Selezionare le credenziali host create nel passaggio 2. Le credenziali host richiedono privilegi sudo. Selezionare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



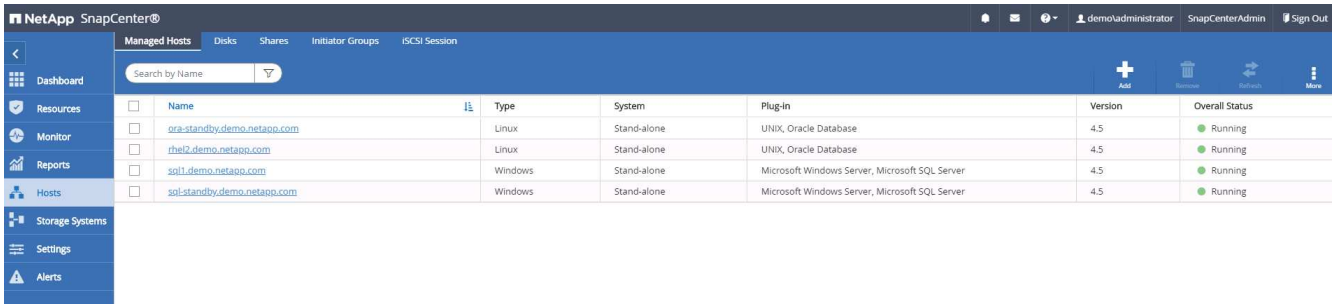
4. Fai clic su Altre opzioni e seleziona "Salta controlli preinstallazione". Ti verrà chiesto di confermare l'esclusione del controllo pre-installazione. Fare clic su Sì e poi su Salva.



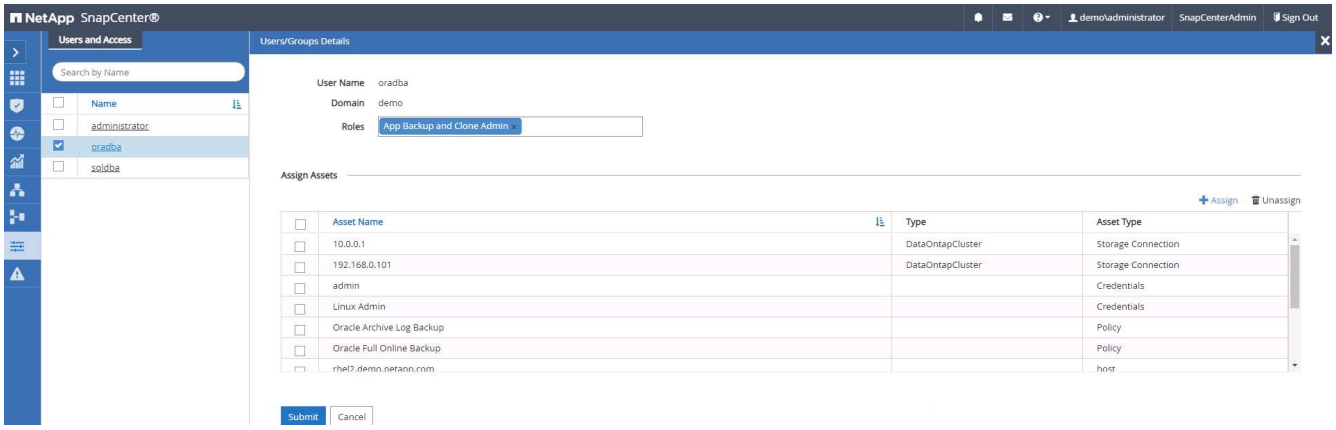
5. Fare clic su Invia per avviare l'installazione del plugin. Ti verrà chiesto di confermare l'impronta digitale come mostrato di seguito.

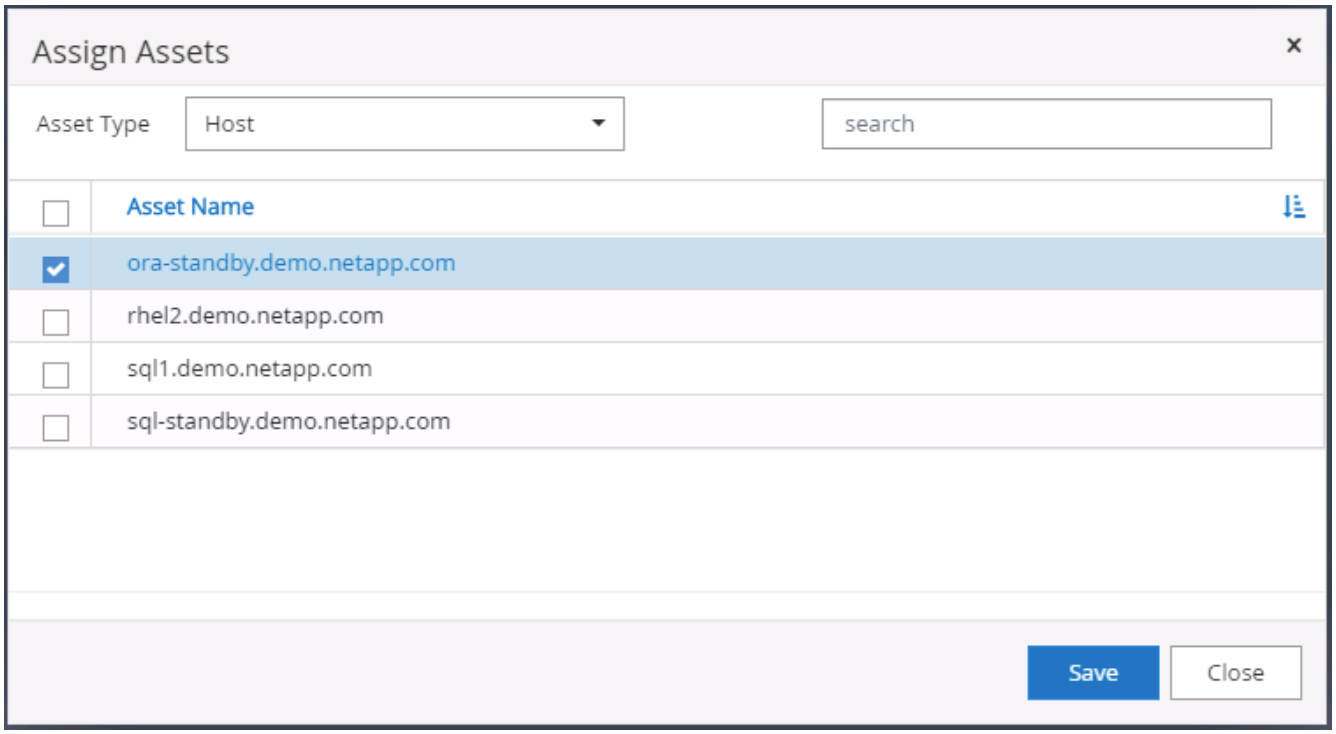


6. SnapCenter esegue la convalida e la registrazione dell'host, dopodiché il plugin viene installato sull'host Linux. Lo stato è cambiato da Installazione plugin a In esecuzione.



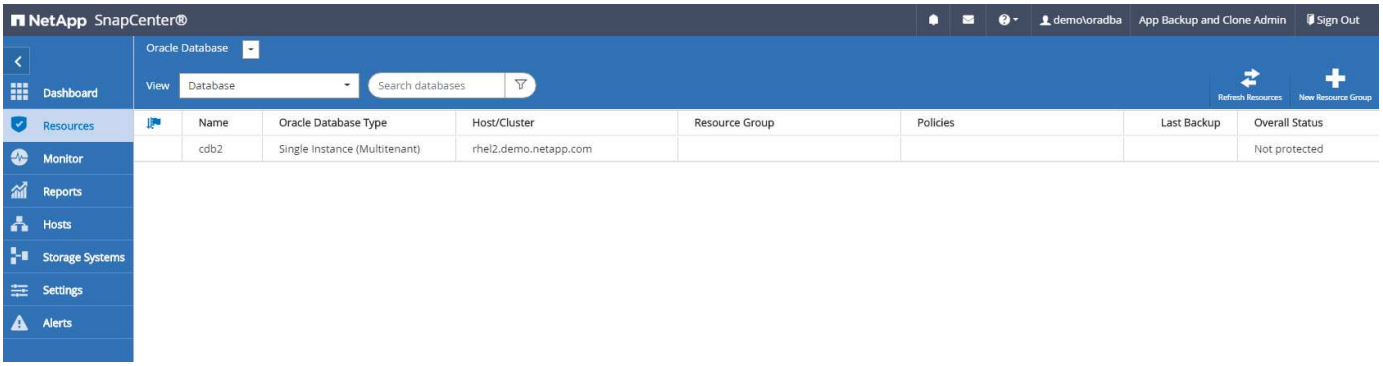
7. Assegnare all'host appena aggiunto l'ID utente di gestione del database appropriato (nel nostro caso, oradba).





4. Scoperta delle risorse del database

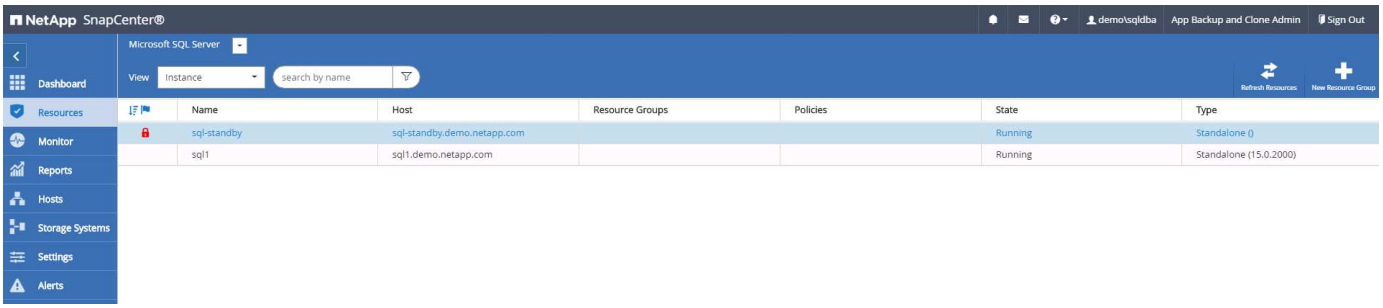
Una volta installato correttamente il plugin, le risorse del database sull'host possono essere immediatamente scoperte. Fare clic sulla scheda Risorse nel menu a sinistra. A seconda del tipo di piattaforma di database, sono disponibili diverse viste, ad esempio quella del database, del gruppo di risorse e così via. Potrebbe essere necessario fare clic sulla scheda Aggiorna risorse se le risorse sull'host non vengono rilevate e visualizzate.

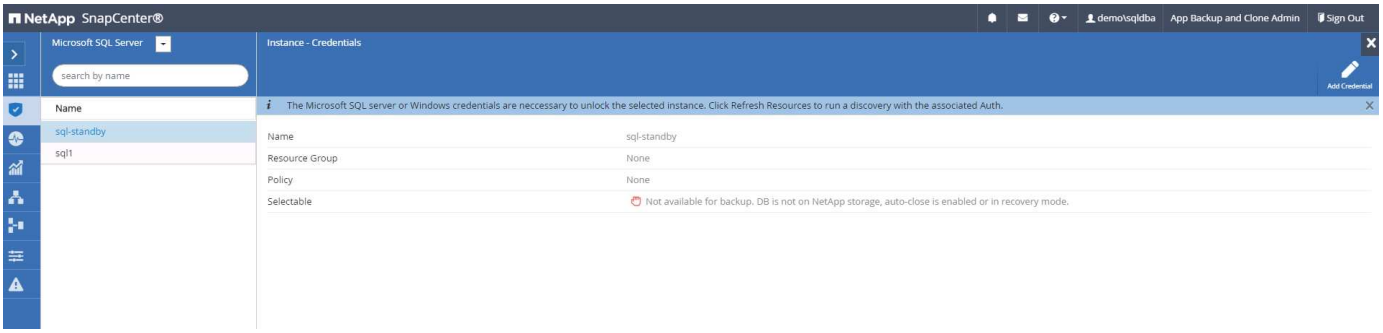


Quando il database viene inizialmente scoperto, lo stato generale viene visualizzato come "Non protetto". Lo screenshot precedente mostra un database Oracle non ancora protetto da una policy di backup.

Quando viene impostata una configurazione o una policy di backup e viene eseguito un backup, lo Stato complessivo del database mostra lo stato del backup come "Backup riuscito" e il timestamp dell'ultimo backup. La seguente schermata mostra lo stato del backup di un database utente di SQL Server.

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





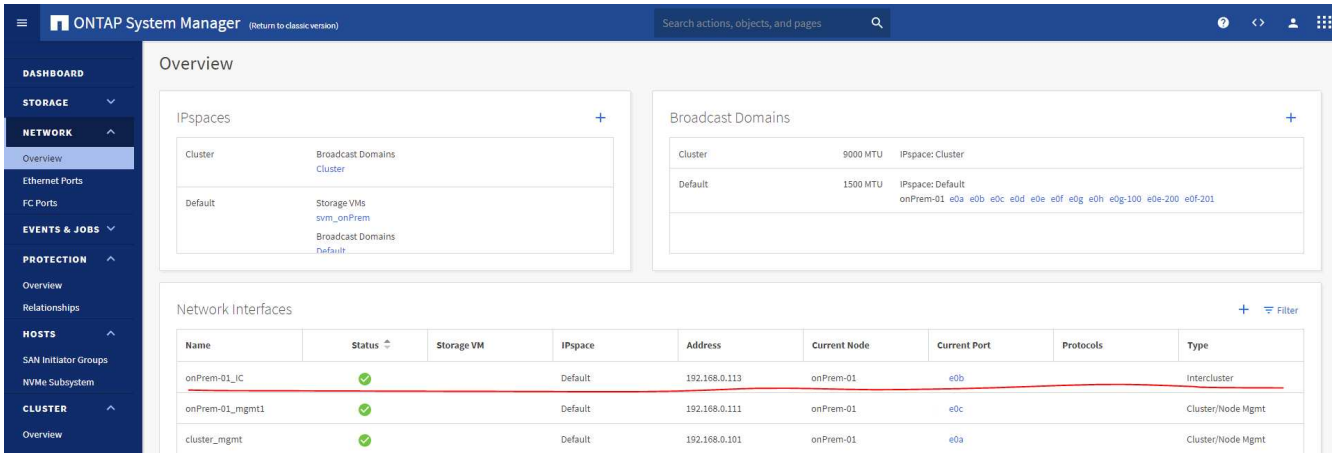
Dopo aver configurato le credenziali appropriate a livello di Windows o di database, il lucchetto rosso scompare e le informazioni sul tipo di SQL Server vengono raccolte e riviste.

5. Configurazione del peering del cluster di archiviazione e della replica dei volumi DB

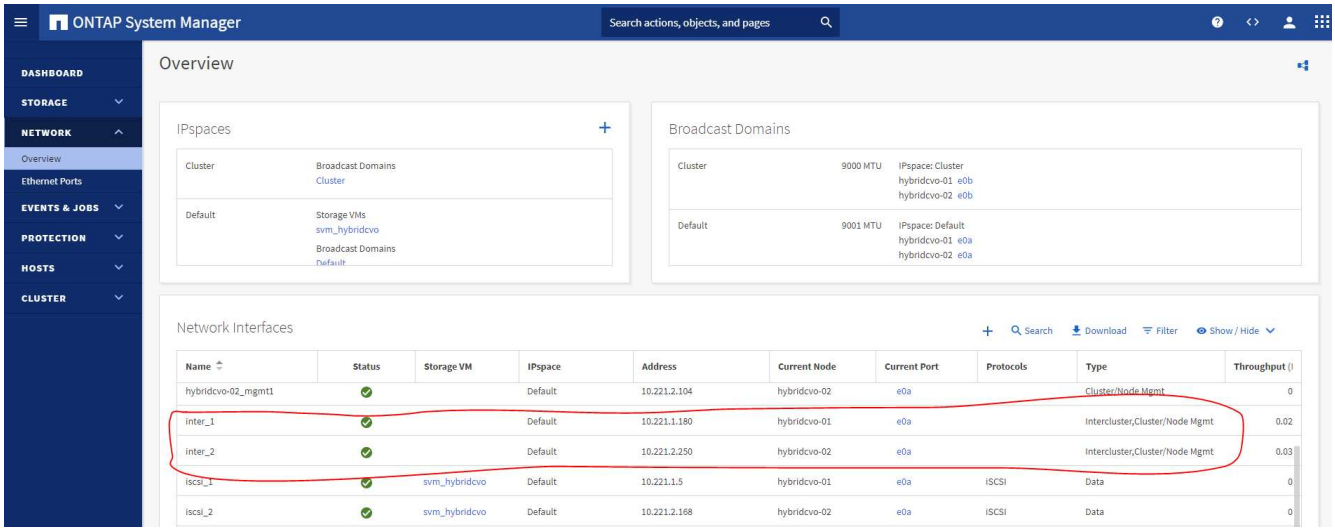
Per proteggere i dati del database locale utilizzando un cloud pubblico come destinazione, i volumi del database del cluster ONTAP locale vengono replicati sul CVO del cloud utilizzando la tecnologia NetApp SnapMirror . I volumi di destinazione replicati possono quindi essere clonati per DEV/OPS o per il ripristino di emergenza. I seguenti passaggi di alto livello consentono di configurare il peering del cluster e la replica dei volumi DB.

1. Configurare i LIF intercluster per il peering dei cluster sia sul cluster locale che sull'istanza del cluster CVO. Questo passaggio può essere eseguito con ONTAP System Manager. Una distribuzione CVO predefinita prevede la configurazione automatica dei LIF inter-cluster.

   Cluster on-premise:



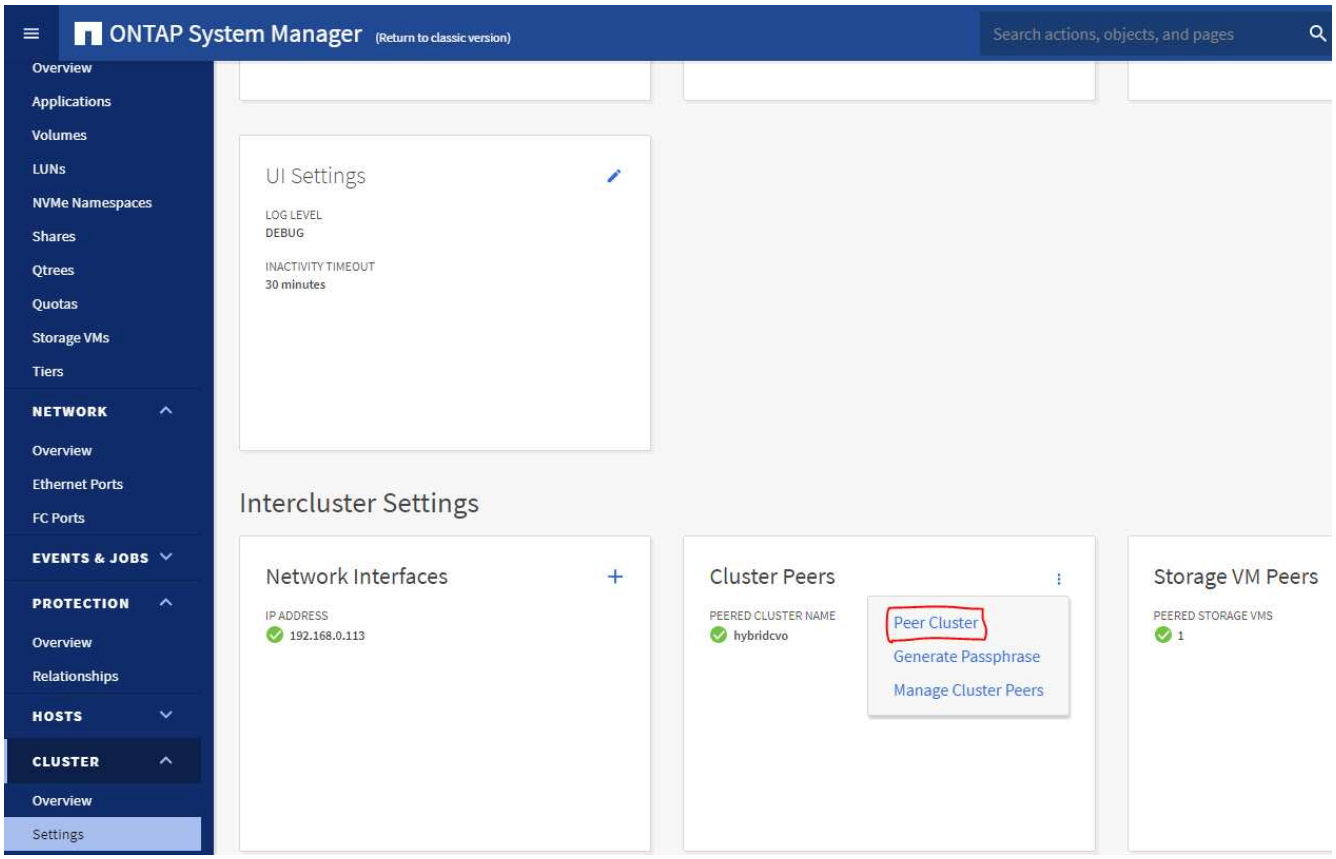
   Cluster CVO di destinazione:



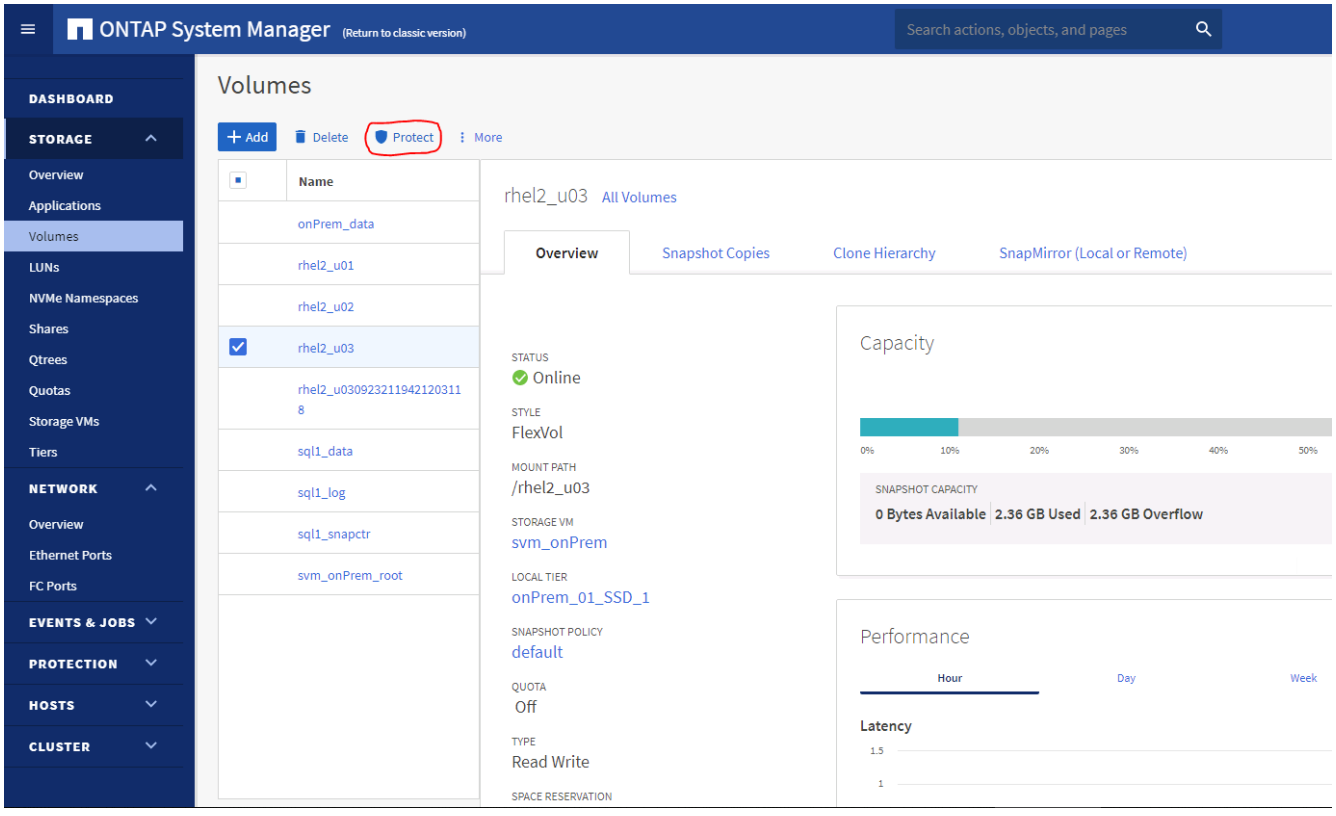
2. Una volta configurati i LIF intercluster, è possibile impostare il peering dei cluster e la replica dei volumi tramite trascinamento della selezione in NetApp Cloud Manager. Vedere"Per iniziare - AWS Public Cloud" per i dettagli.

   In alternativa, il peering del cluster e la replica del volume DB possono essere eseguiti utilizzando ONTAP System Manager come segue:

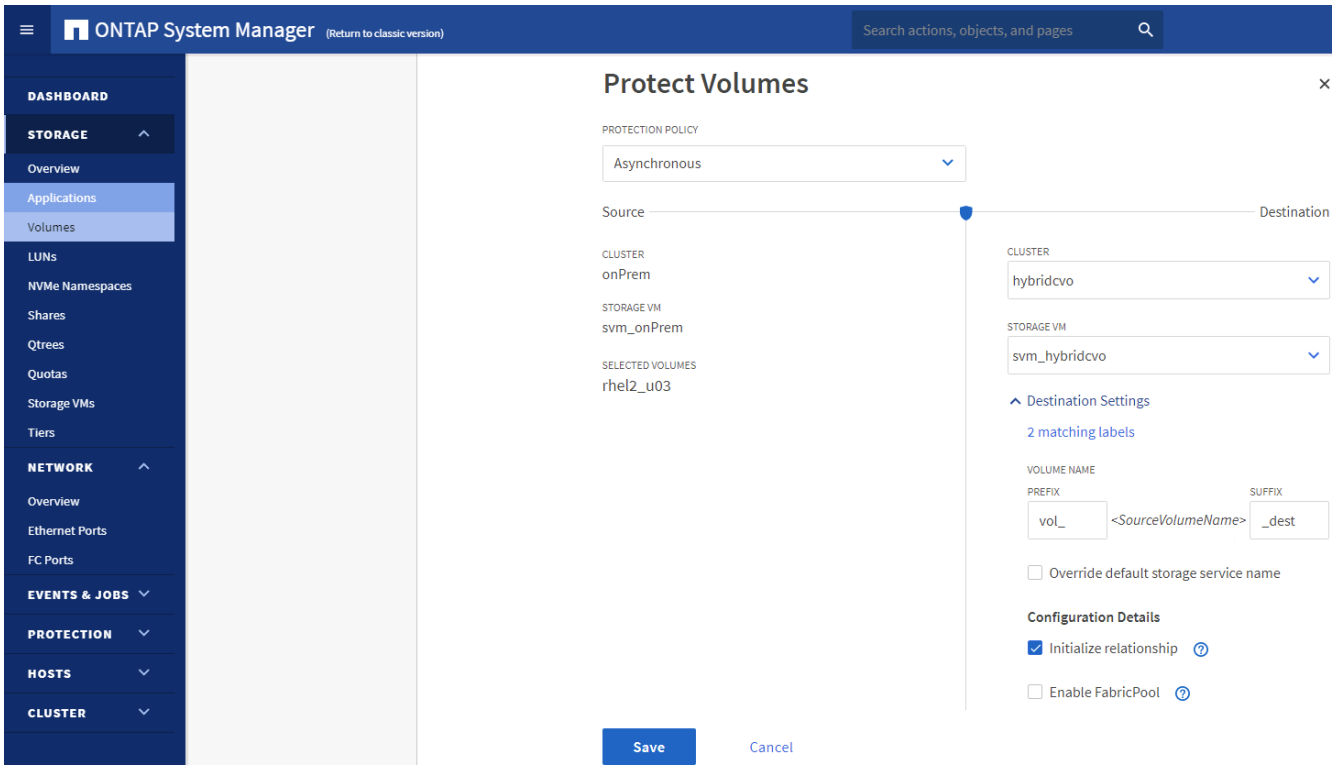
3. Accedere a ONTAP System Manager. Vai su Cluster > Impostazioni e fai clic su Cluster peer per configurare il peering del cluster con l'istanza CVO nel cloud.



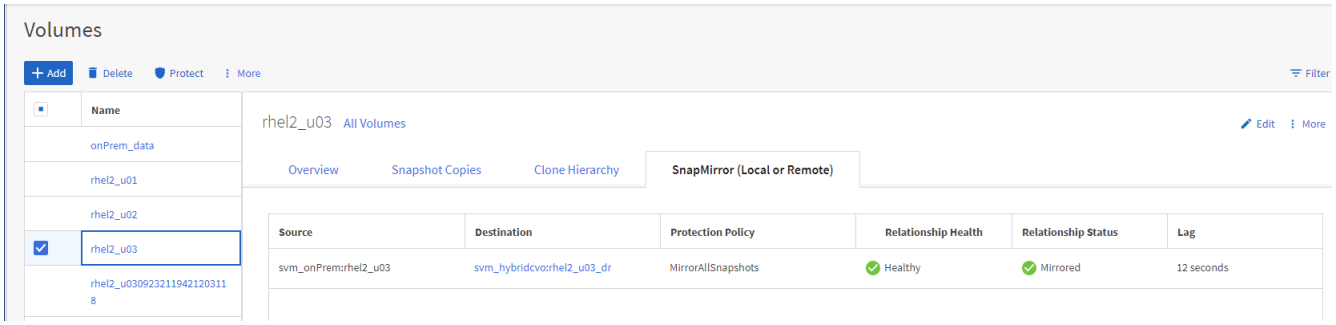
4. Vai alla scheda Volumi. Selezionare il volume del database da replicare e fare clic su Proteggi.



5. Impostare la policy di protezione su Asincrona. Selezionare il cluster di destinazione e l'SVM di archiviazione.

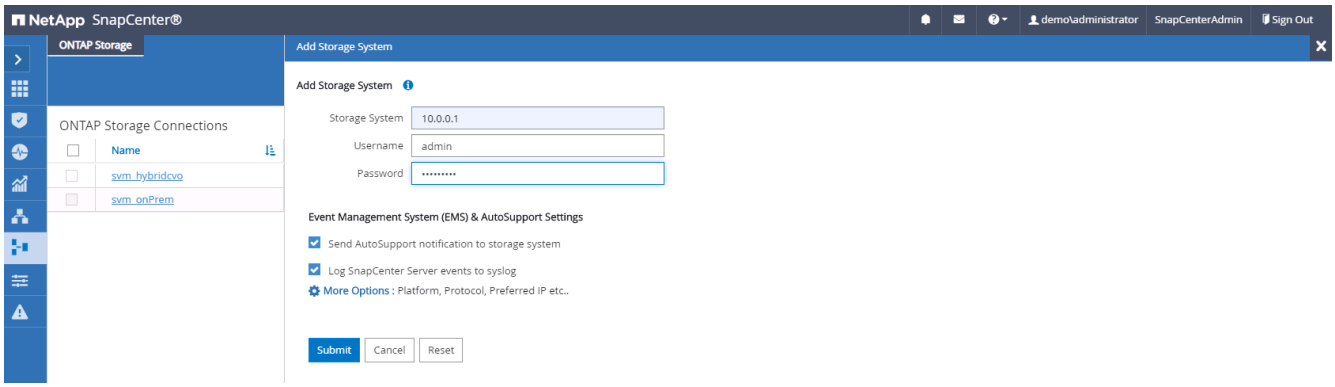


6. Verificare che il volume sia sincronizzato tra l'origine e la destinazione e che la relazione di replica sia integra.

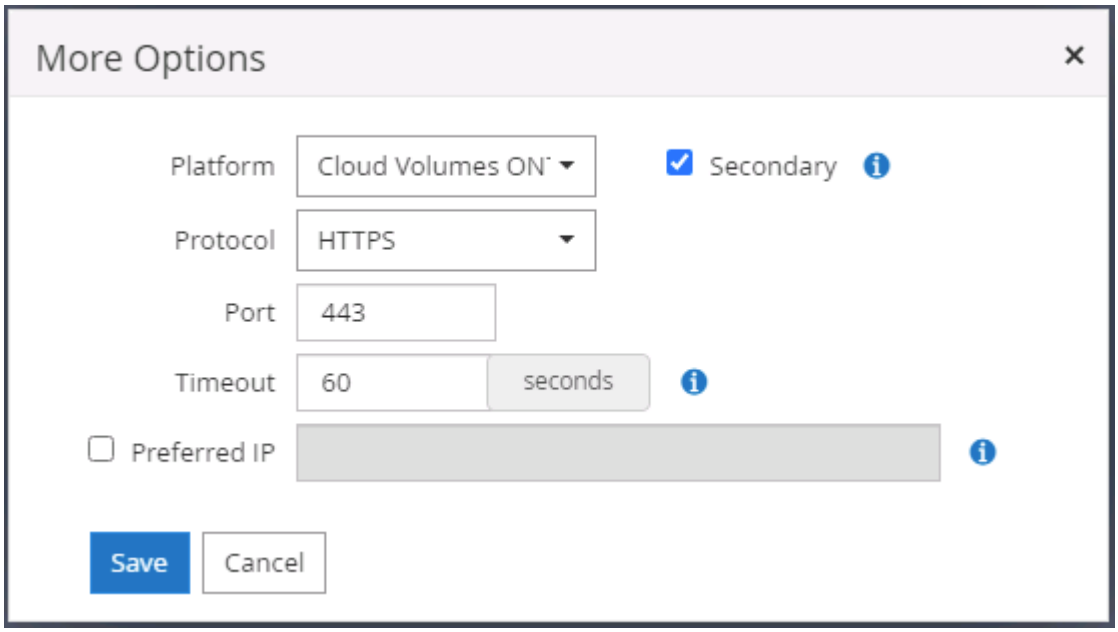


6. Aggiungere l'SVM di archiviazione del database CVO a SnapCenter

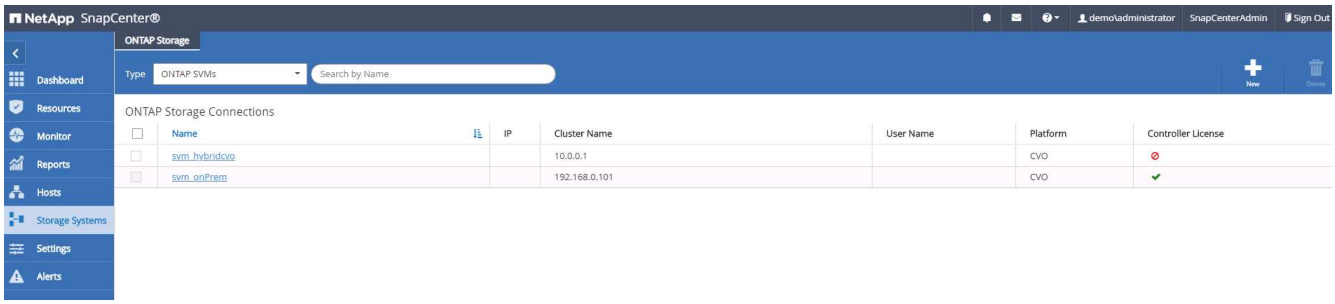
1. Accedi a SnapCenter con un ID utente con privilegi SnapCenterAdmin.
2. Fare clic sulla scheda Sistema di archiviazione dal menu, quindi fare clic su Nuovo per aggiungere un SVM di archiviazione CVO che ospita volumi di database di destinazione replicati a SnapCenter. Immettere l'IP di gestione del cluster nel campo Sistema di archiviazione e immettere il nome utente e la password appropriati.



3. Fare clic su Altre opzioni per aprire ulteriori opzioni di configurazione dell'archiviazione. Nel campo Piattaforma, seleziona Cloud Volumes ONTAP, seleziona Secondario e quindi fai clic su Salva.



4. Assegnare i sistemi di archiviazione agli ID utente di gestione del database SnapCenter come mostrato in3. Installazione del plugin host SnapCenter .

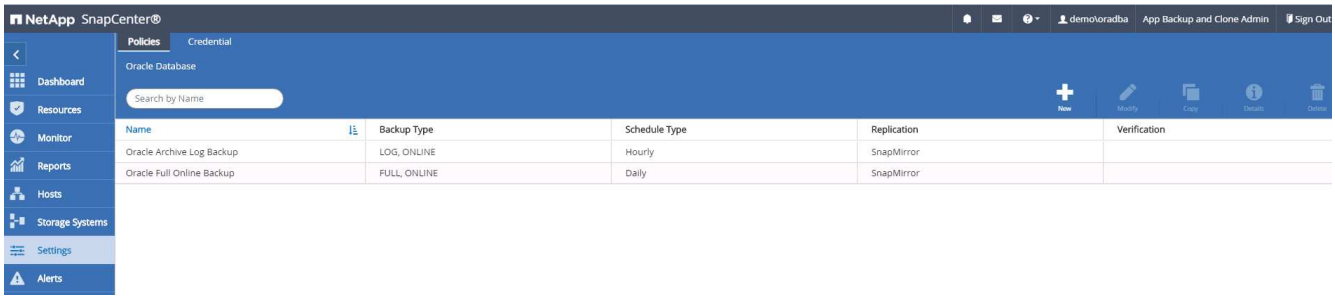


7. Imposta la policy di backup del database in SnapCenter

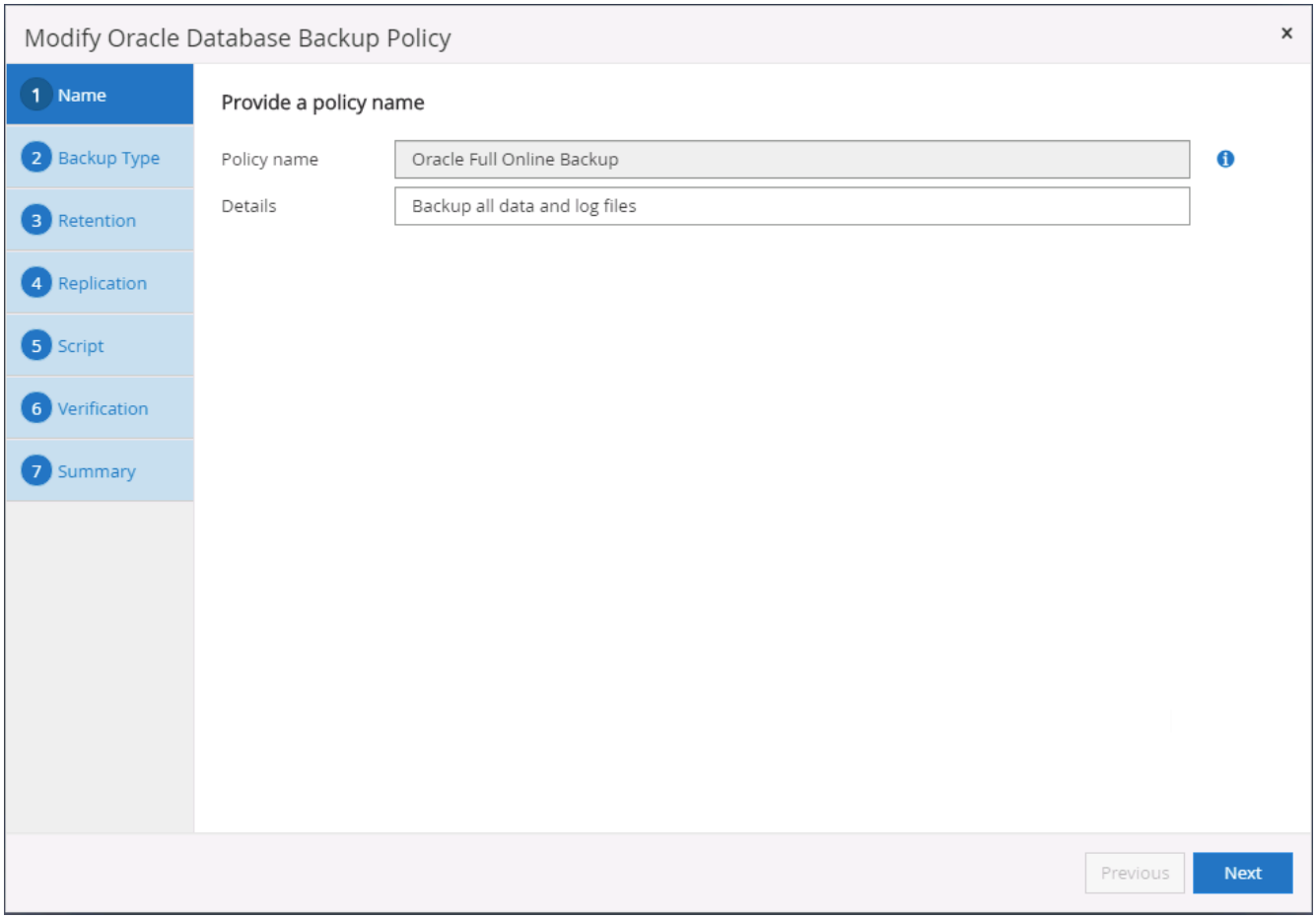
Le seguenti procedure illustrano come creare un criterio di backup completo del database o del file di registro. La politica può quindi essere implementata per proteggere le risorse dei database. L'obiettivo del punto di ripristino (RPO) o l'obiettivo del tempo di ripristino (RTO) determinano la frequenza dei backup del database e/o del log.

Creare una policy di backup completa del database per Oracle

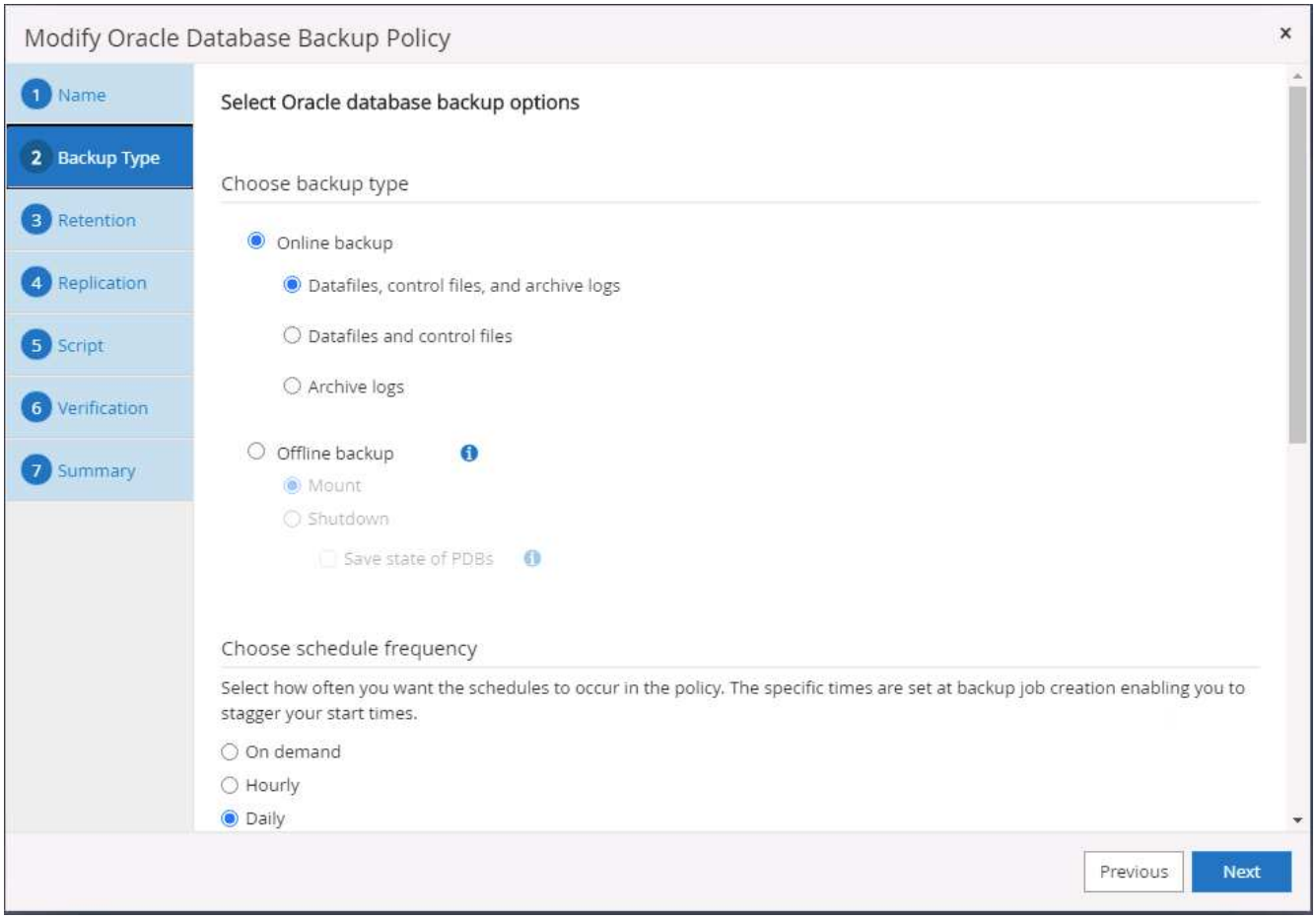
1. Accedi a SnapCenter come ID utente di gestione del database, fai clic su Impostazioni, quindi su Criteri.



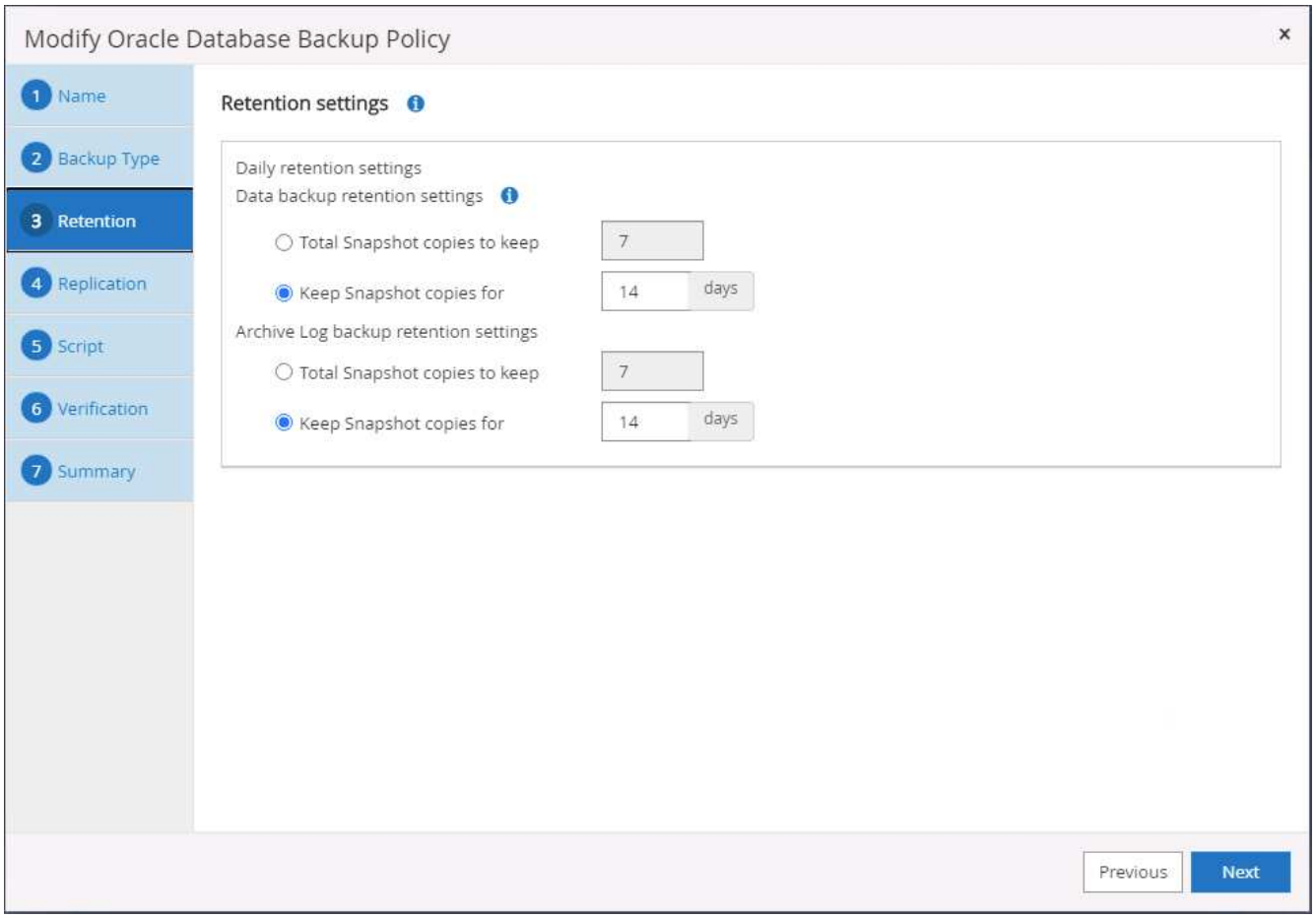
2. Fare clic su Nuovo per avviare un nuovo flusso di lavoro per la creazione di una policy di backup oppure scegliere una policy esistente da modificare.



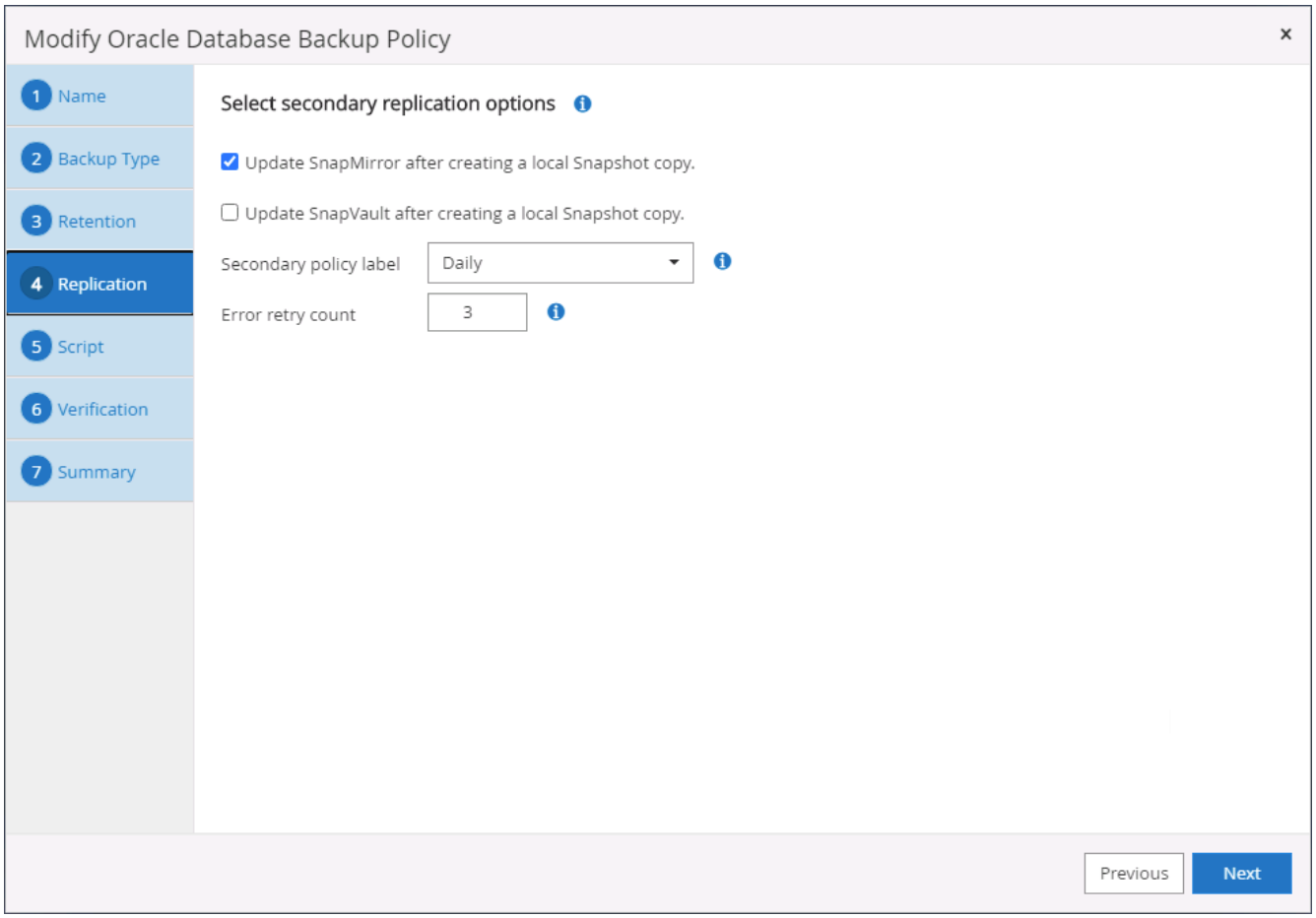
3. Selezionare il tipo di backup e la frequenza di pianificazione.



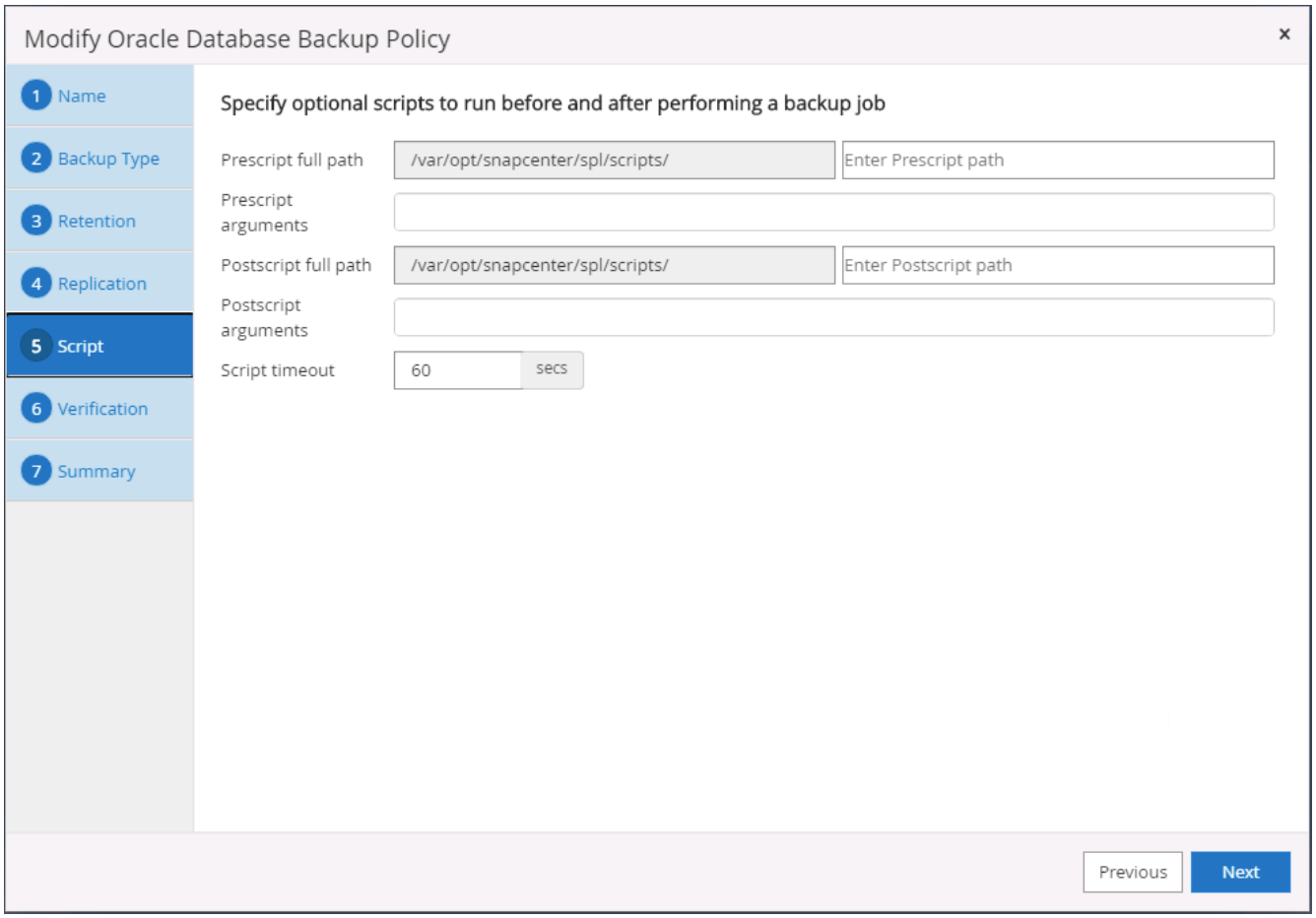
4. Imposta le impostazioni di conservazione del backup. Definisce quante copie di backup complete del database conservare.



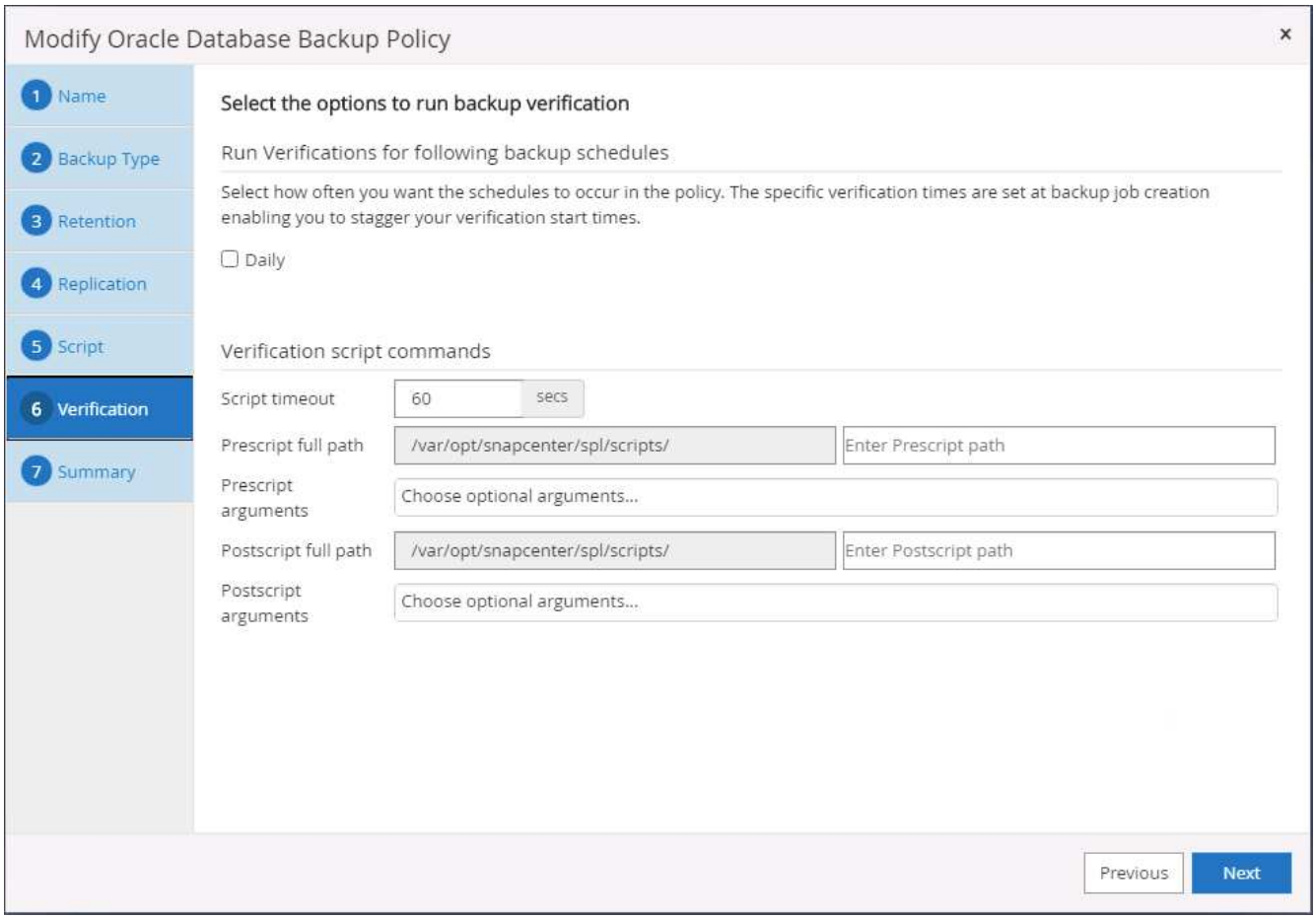
5. Selezionare le opzioni di replicazione secondaria per inviare i backup degli snapshot primari locali da replicare in una posizione secondaria nel cloud.



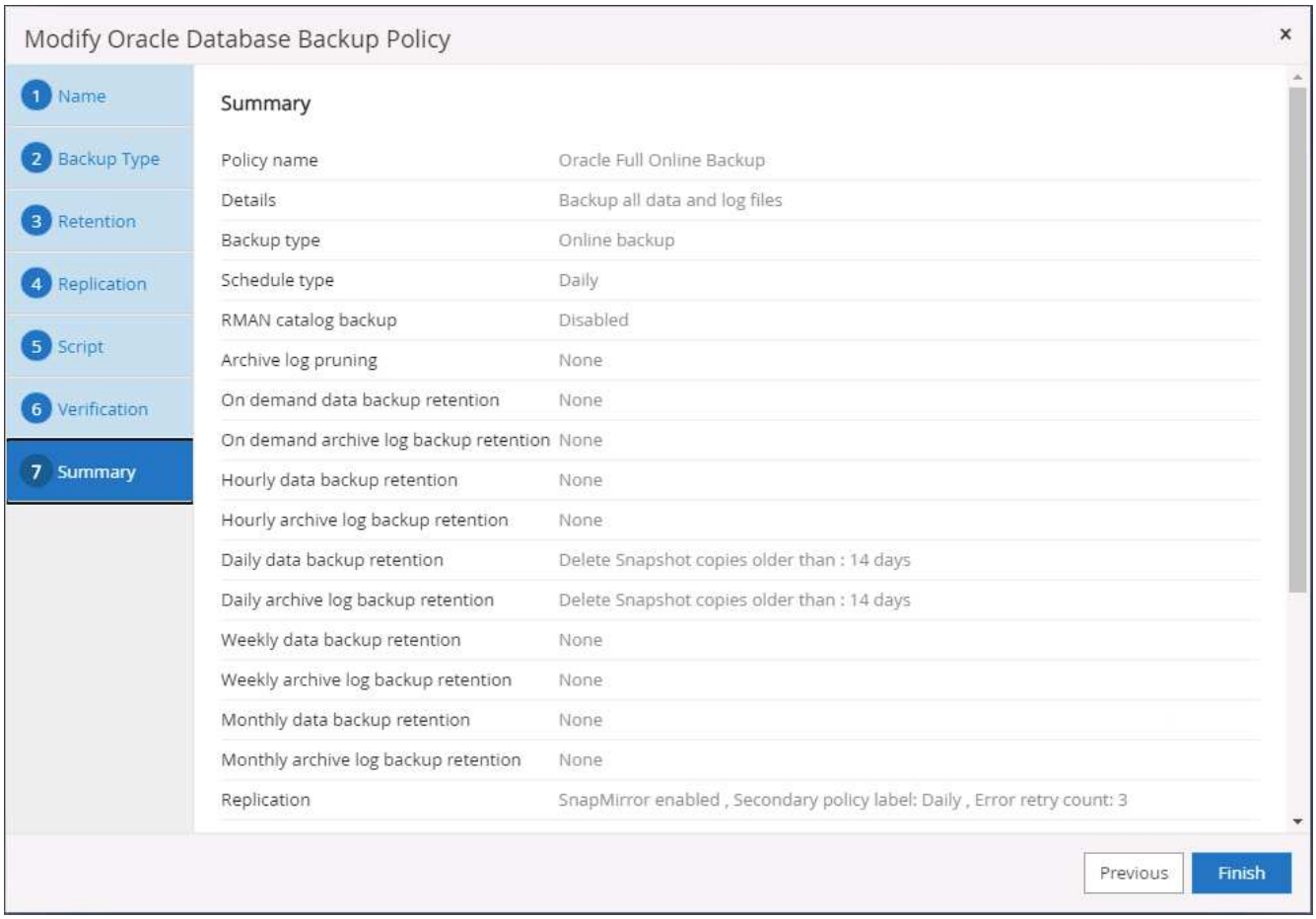
6. Specificare eventuali script facoltativi da eseguire prima e dopo l'esecuzione di un backup.



7. Se lo si desidera, eseguire la verifica del backup.

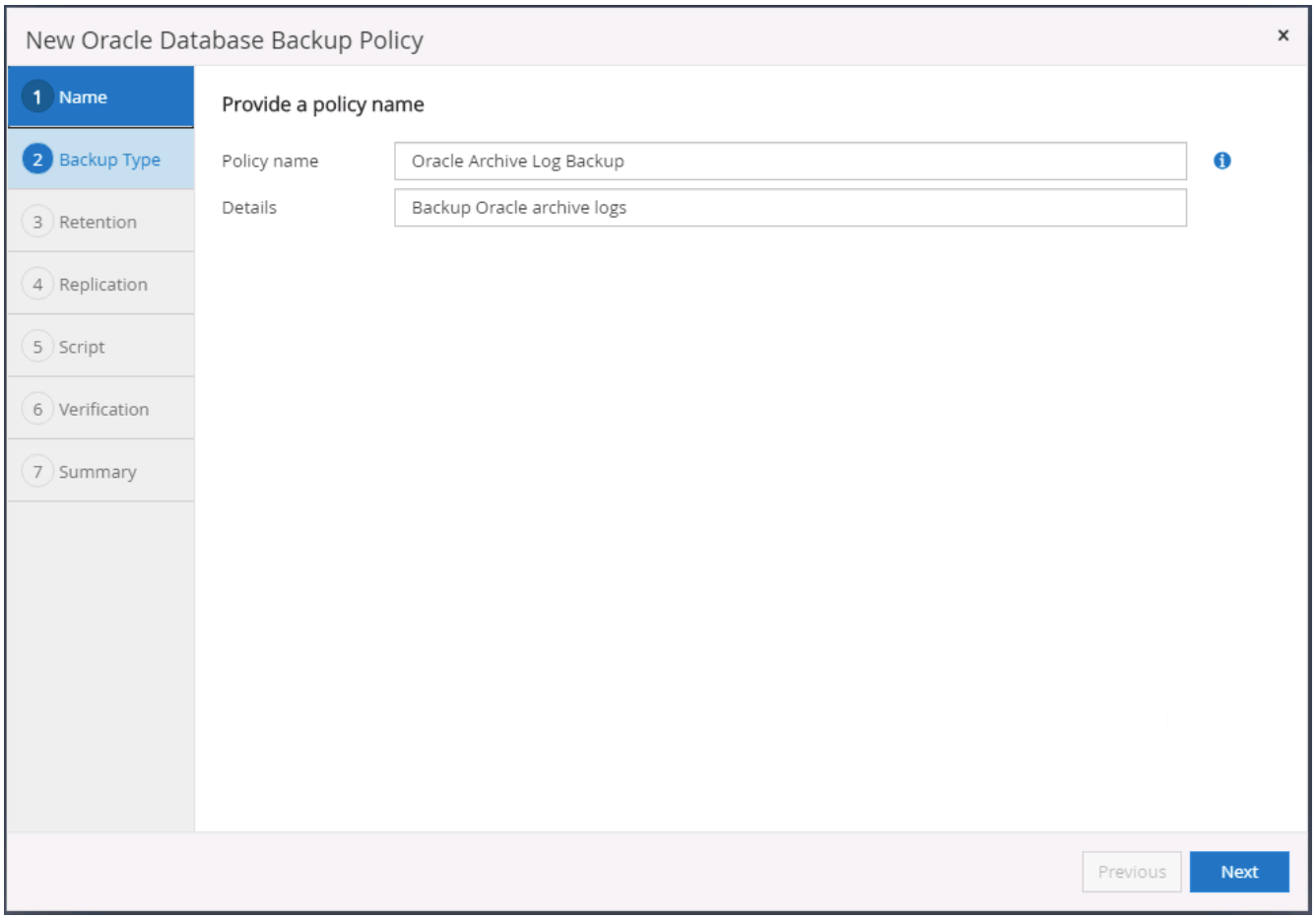

Modify Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification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

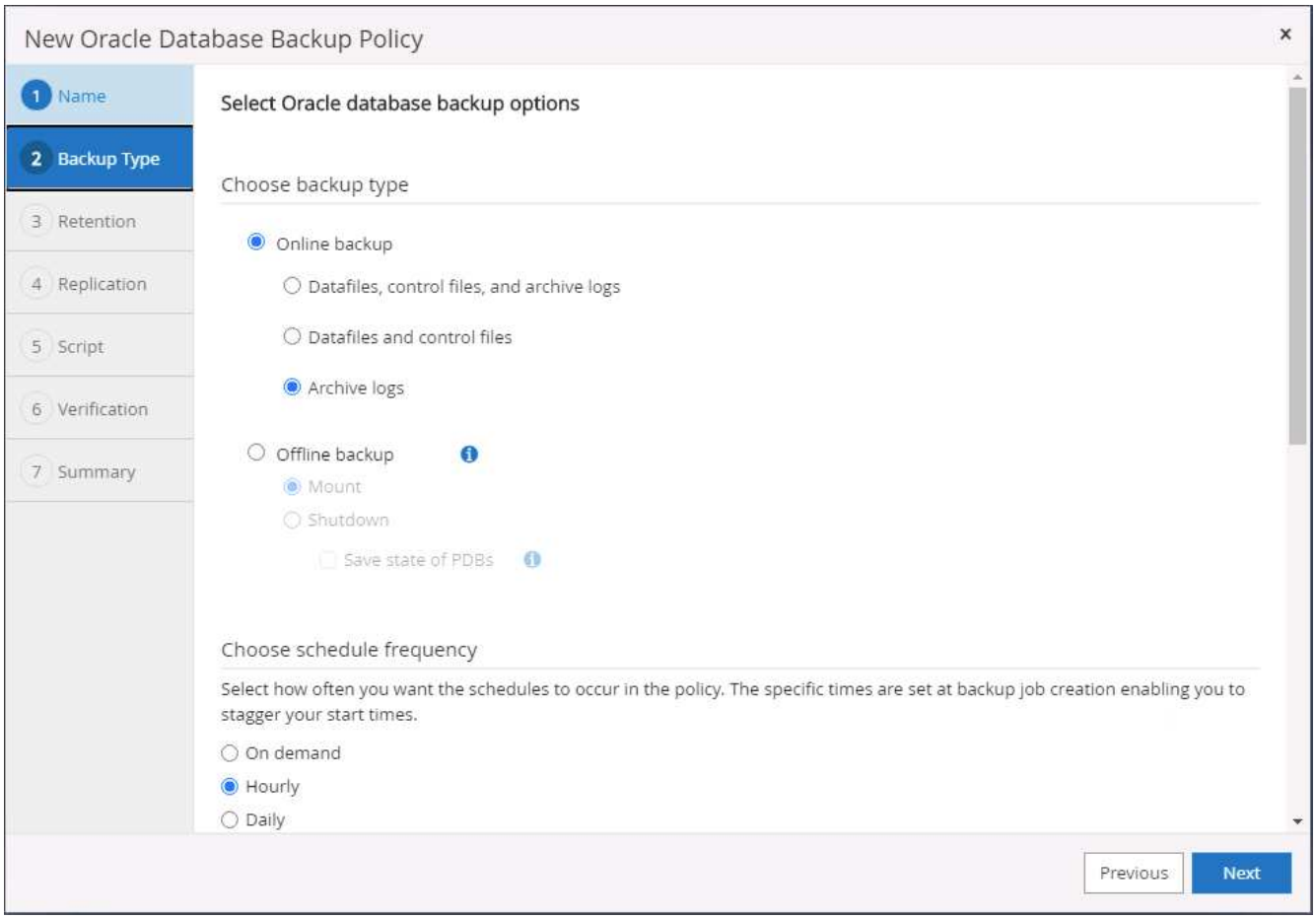


Creare una policy di backup del registro del database per Oracle

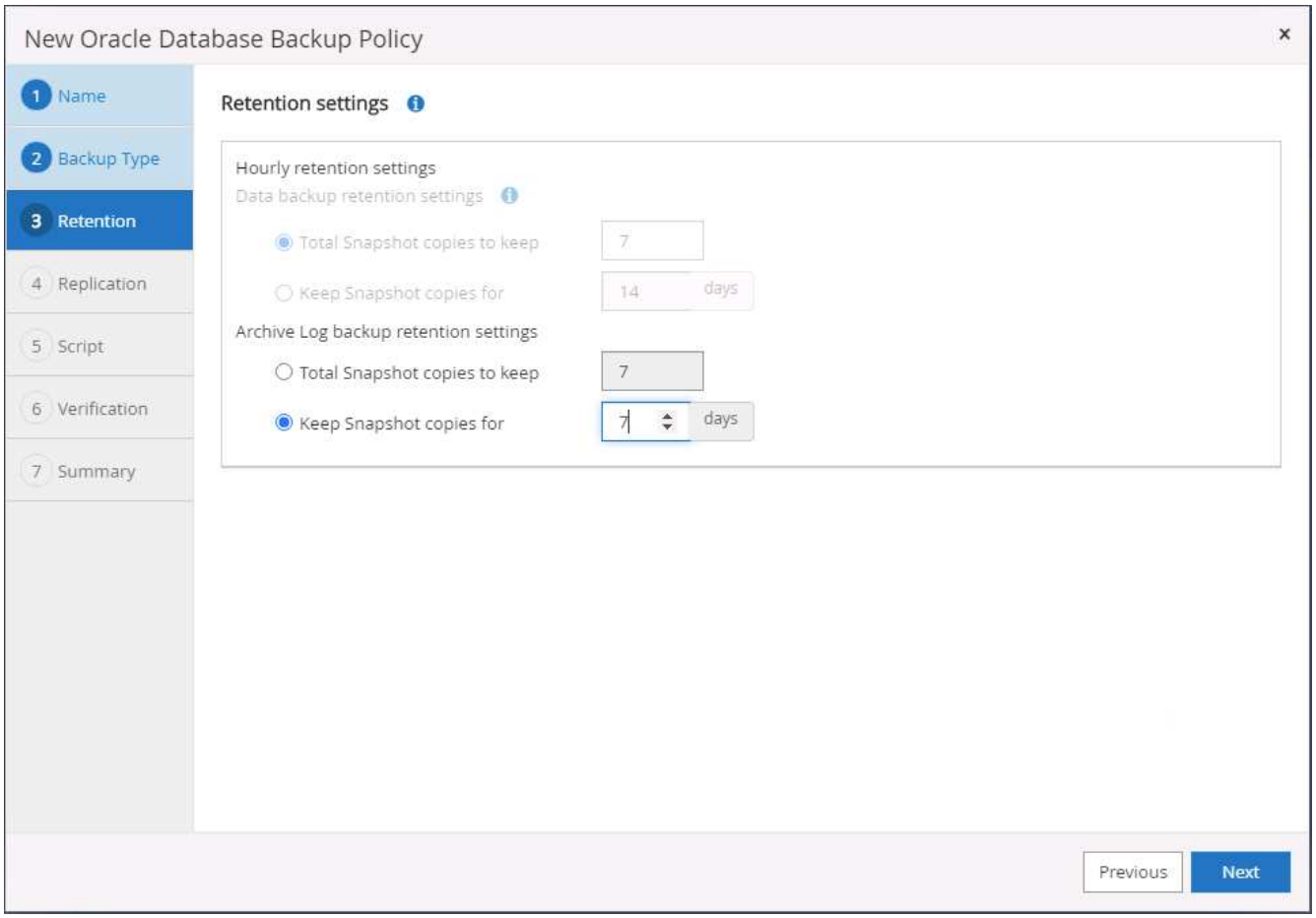
1. Accedi a SnapCenter con un ID utente di gestione del database, fai clic su Impostazioni, quindi su Criteri.
2. Fare clic su Nuovo per avviare un nuovo flusso di lavoro per la creazione di una policy di backup oppure scegliere una policy esistente da modificare.



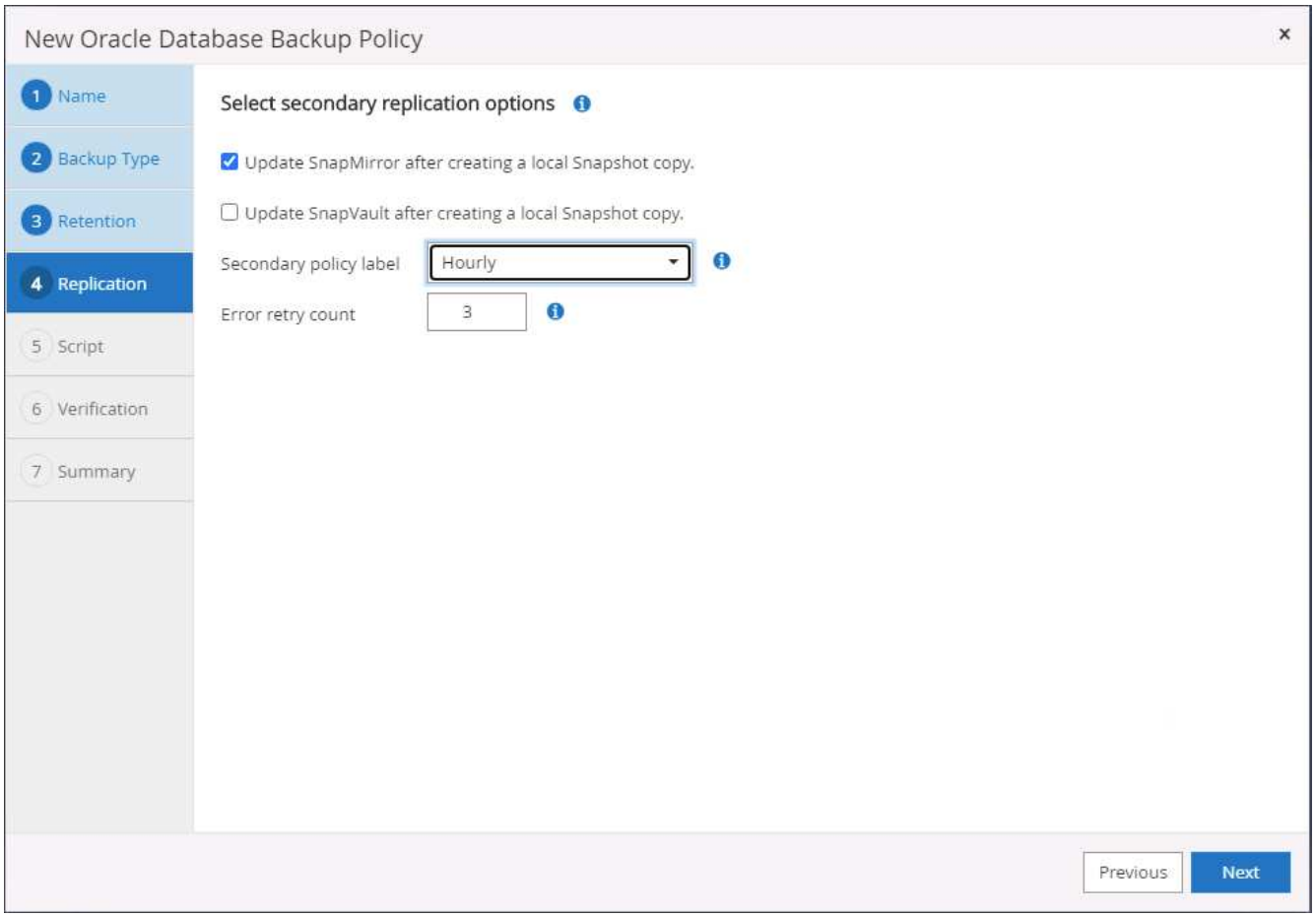
3. Selezionare il tipo di backup e la frequenza di pianificazione.



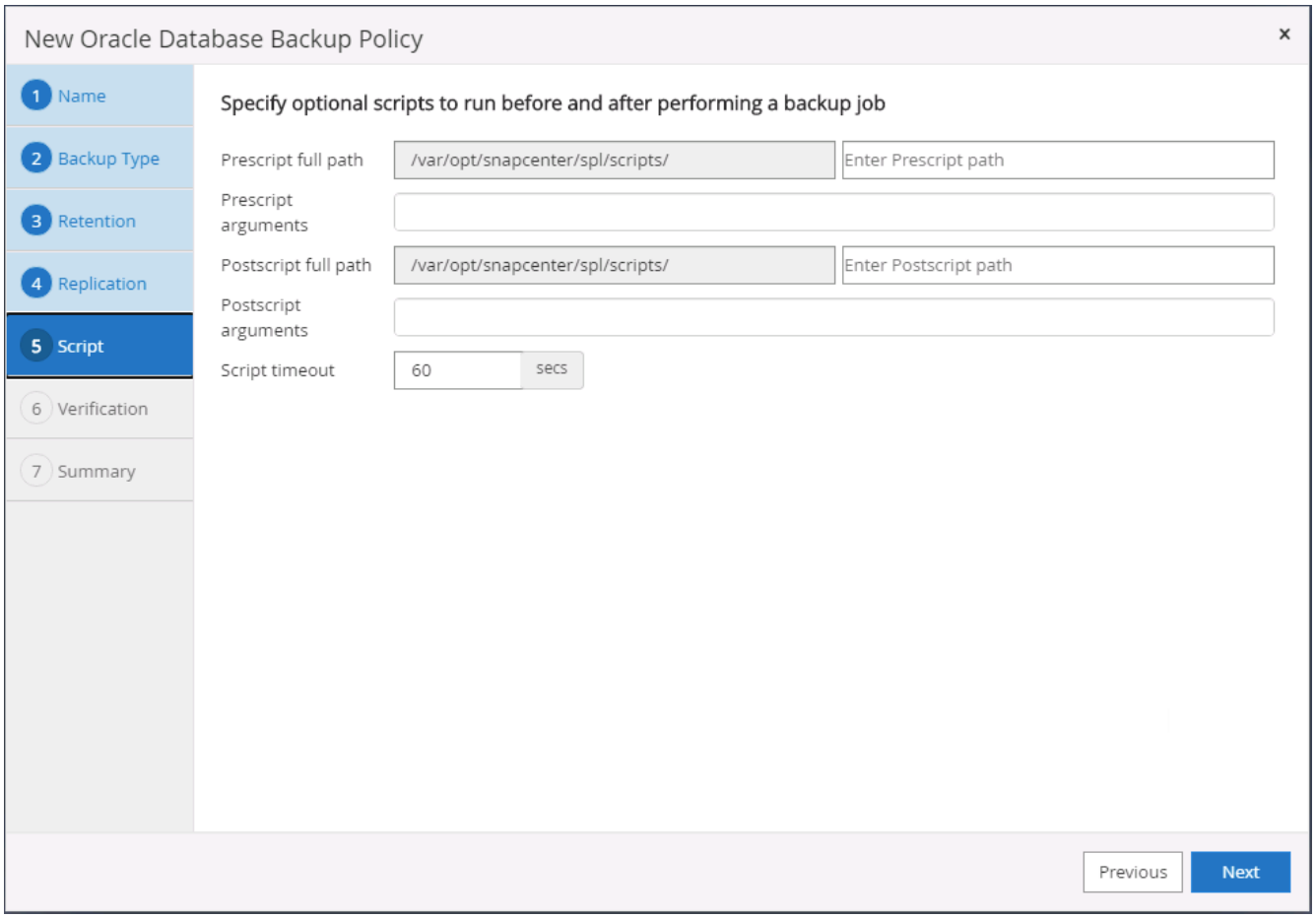
4. Imposta il periodo di conservazione del registro.



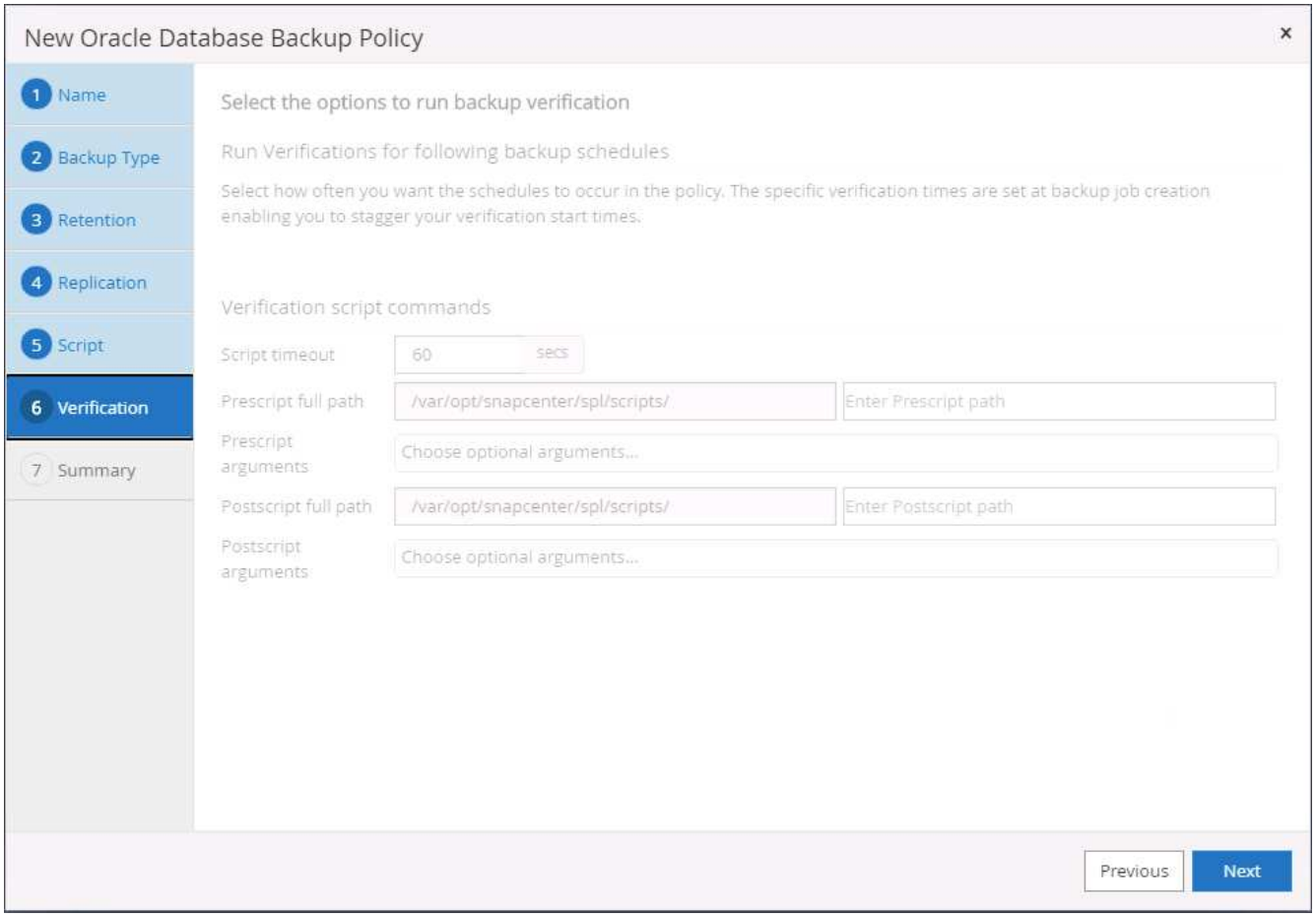
5. Abilita la replica in una posizione secondaria nel cloud pubblico.



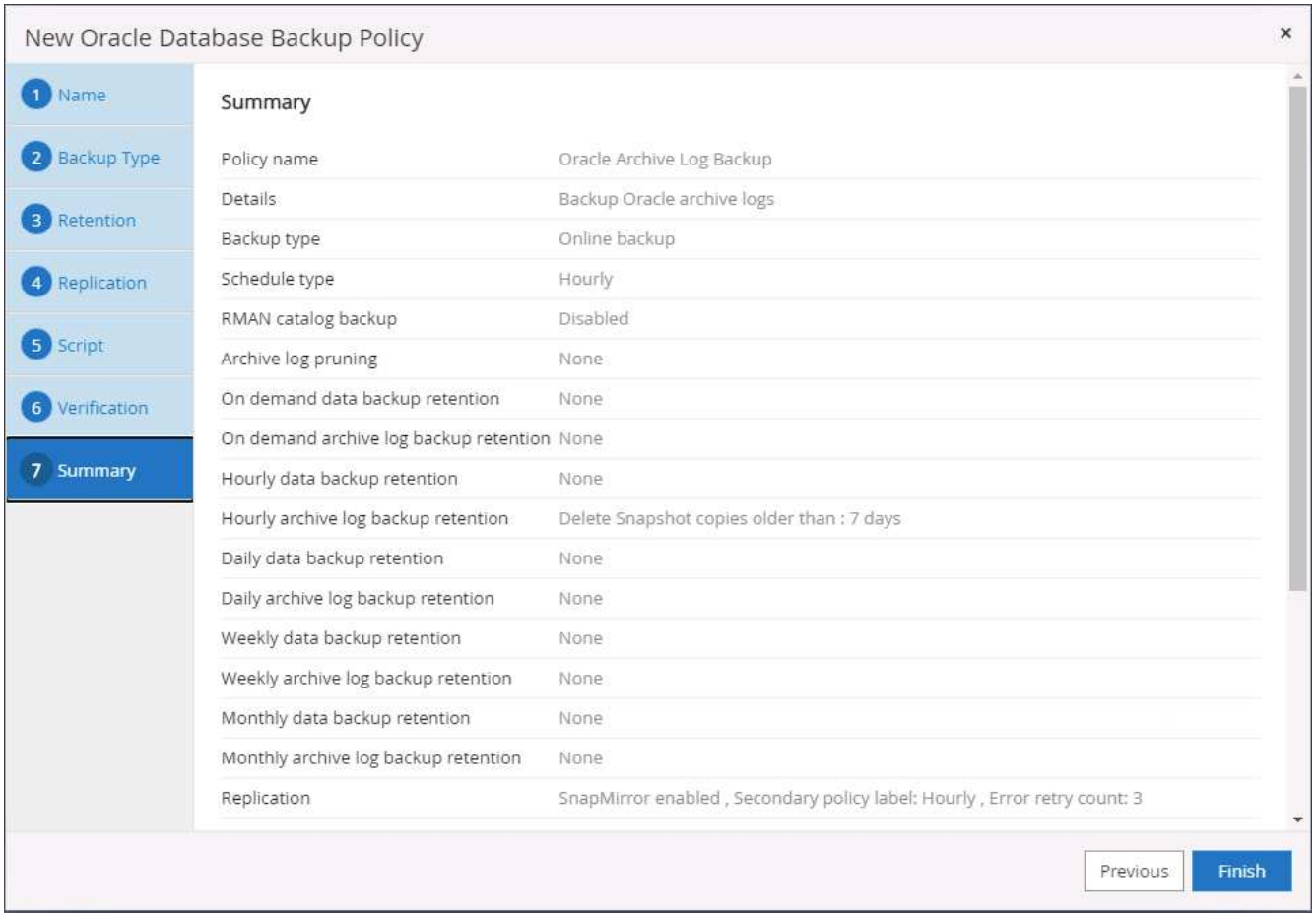
6. Specificare eventuali script facoltativi da eseguire prima e dopo il backup del registro.



7. Specificare eventuali script di verifica del backup.

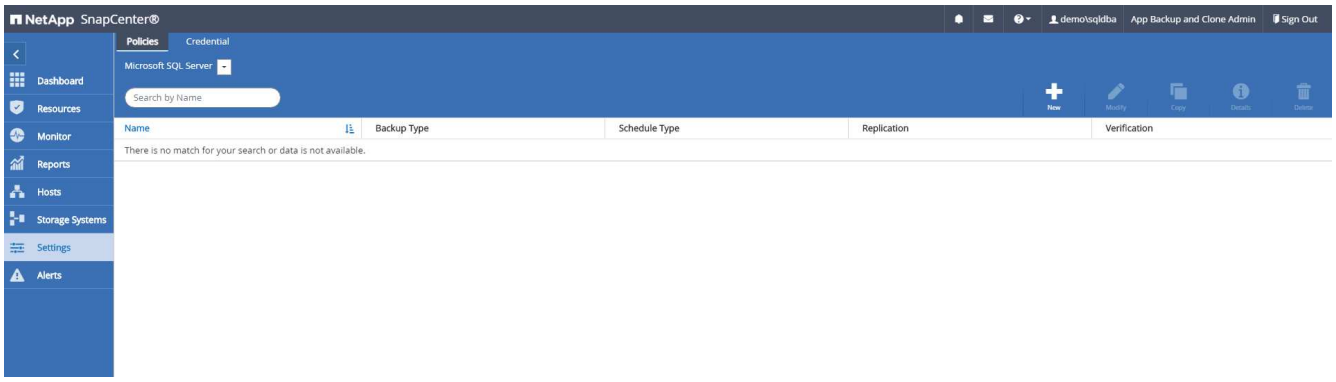

New Oracle Database Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run Verifications for following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times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

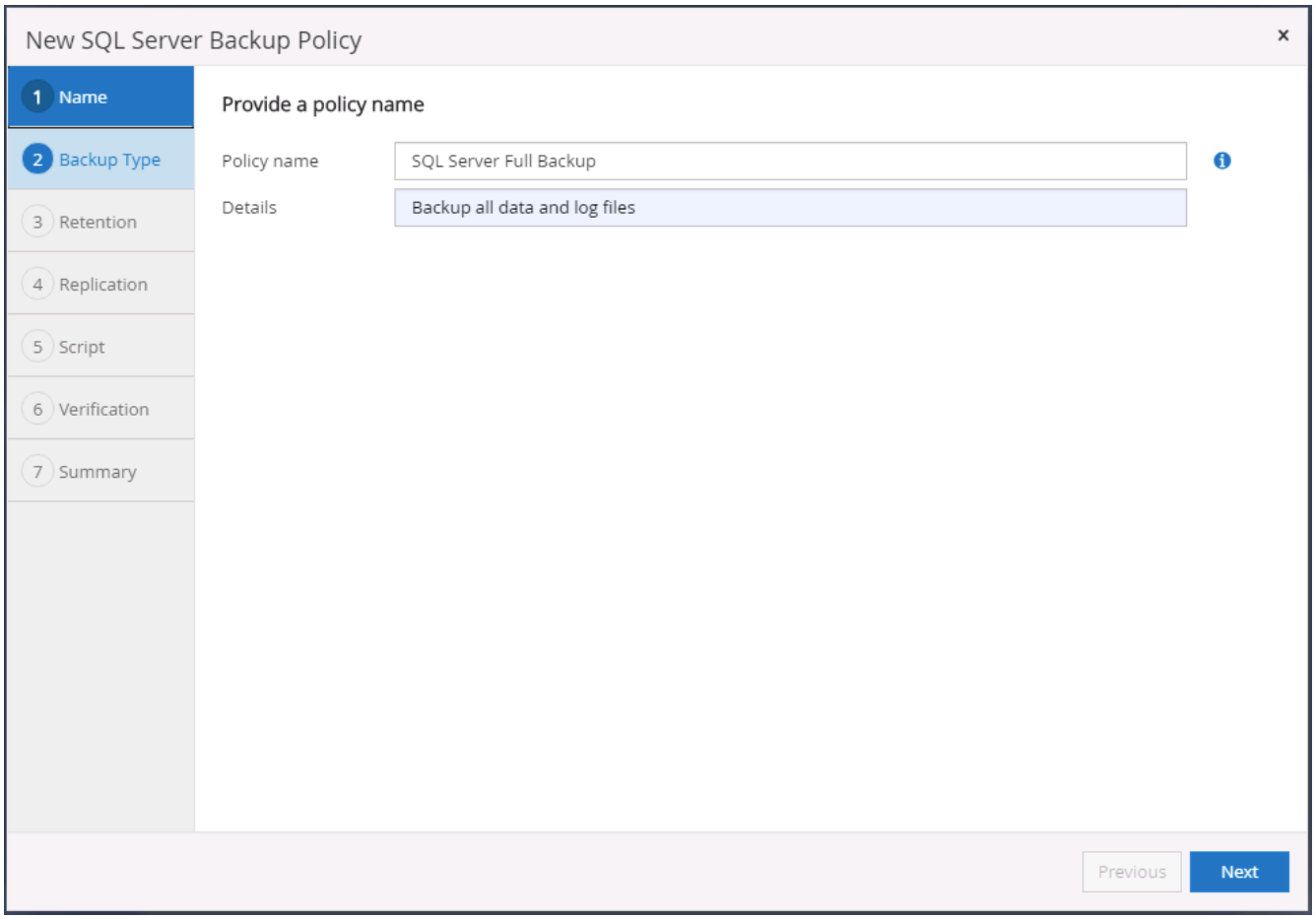


Creare una policy di backup completo del database per SQL

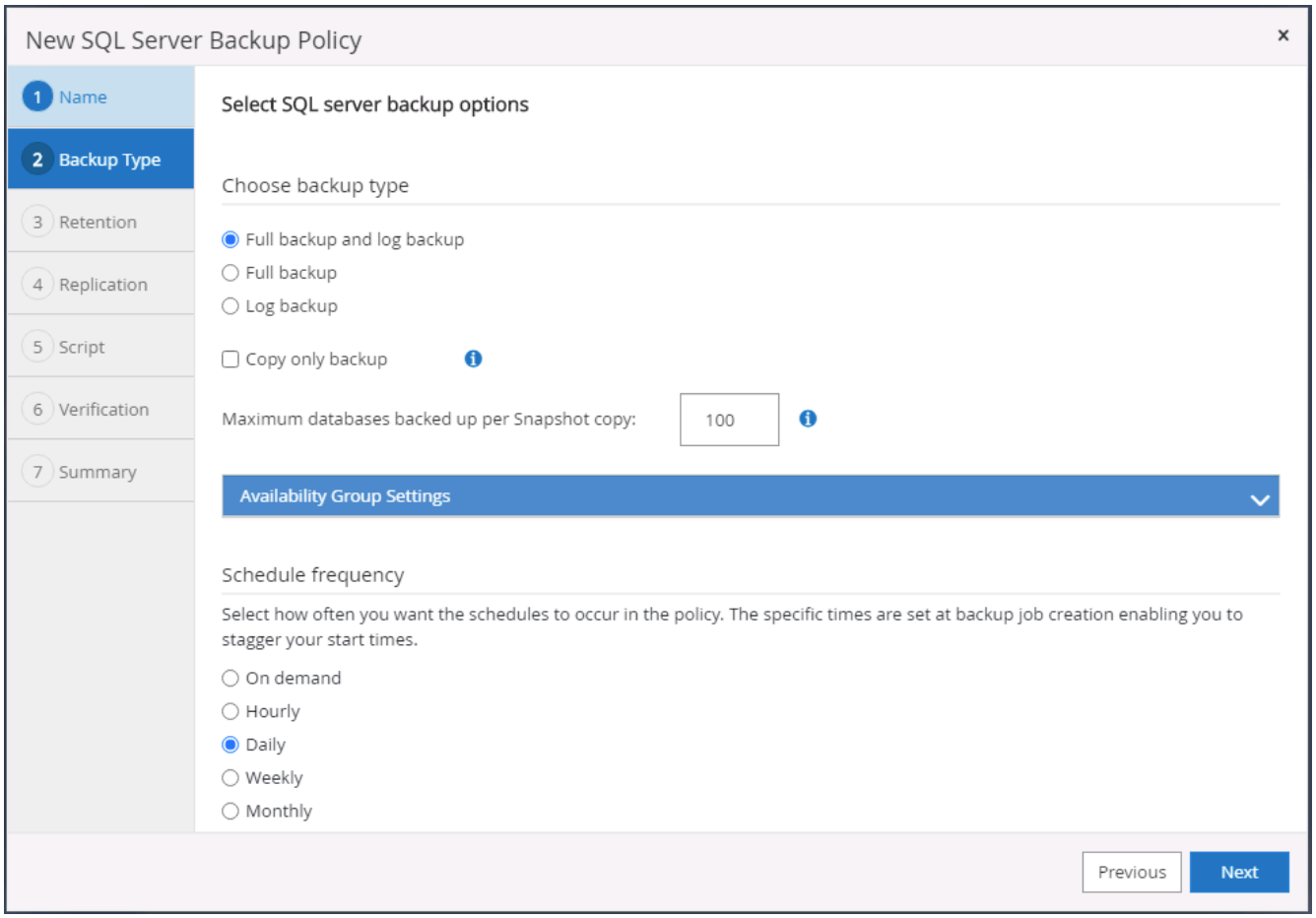
1. Accedi a SnapCenter con un ID utente di gestione del database, fai clic su Impostazioni, quindi su Criteri.



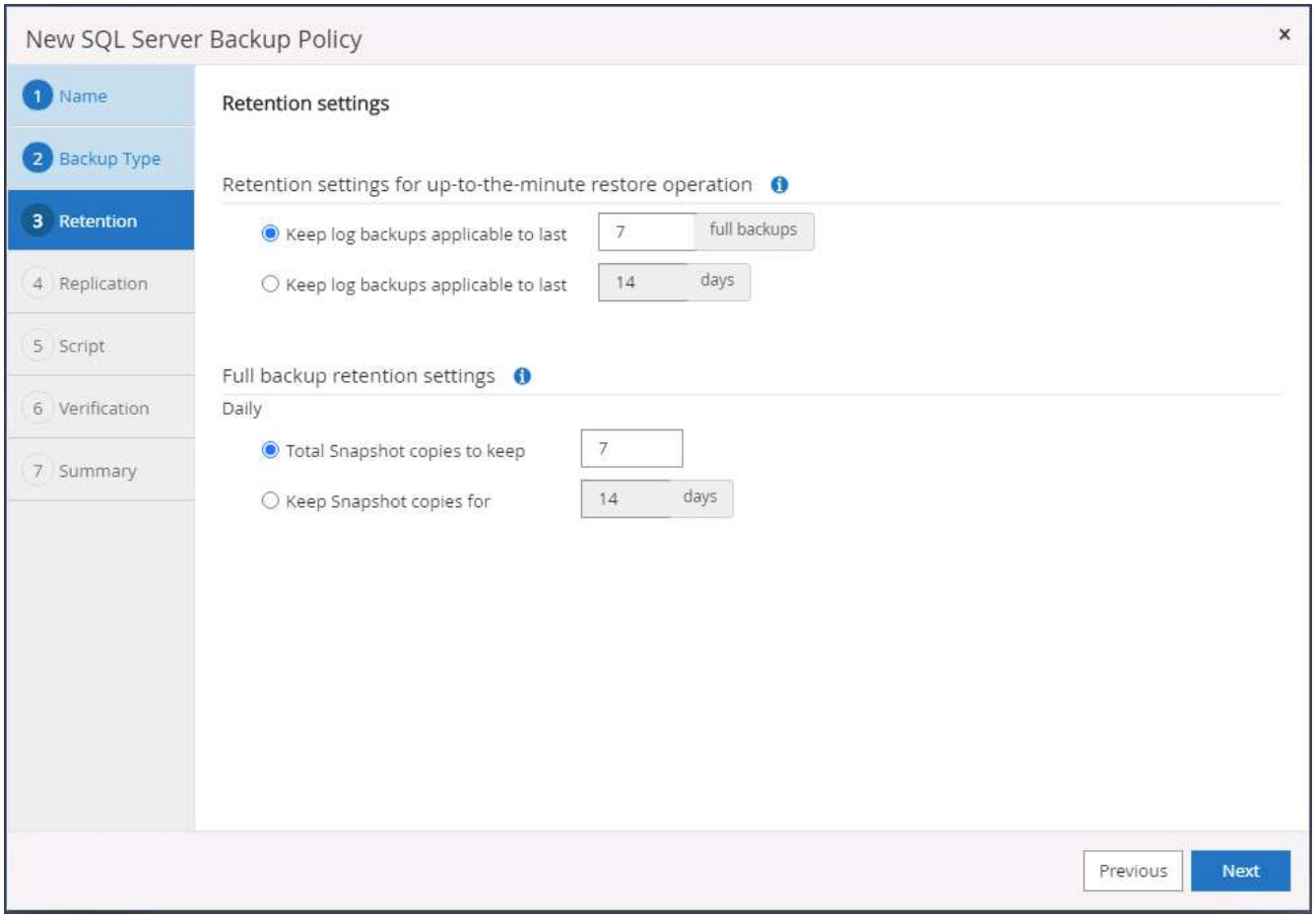
2. Fare clic su Nuovo per avviare un nuovo flusso di lavoro per la creazione di una policy di backup oppure scegliere una policy esistente da modificare.



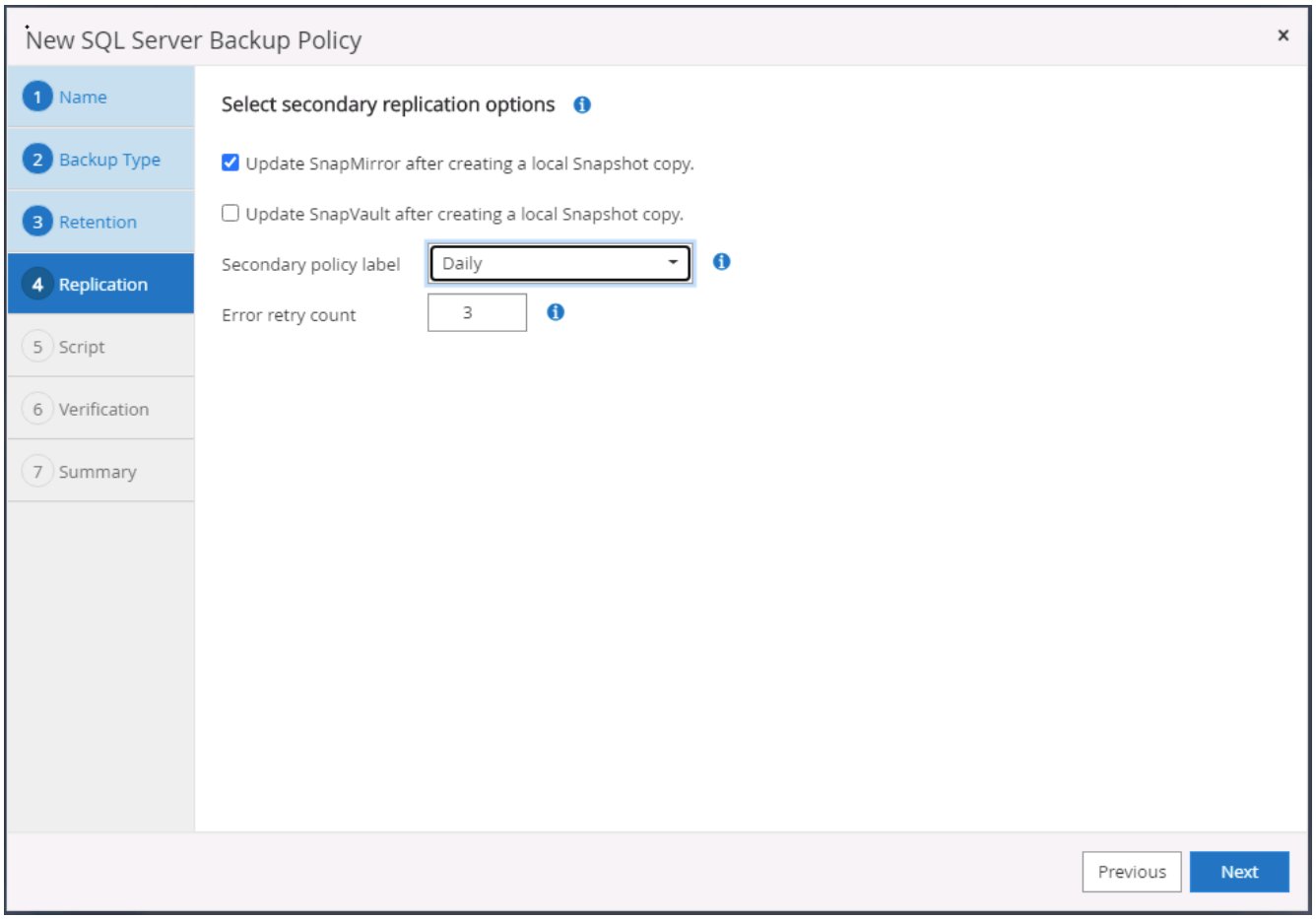
3. Definisci l'opzione di backup e la frequenza di pianificazione. Per SQL Server configurato con un gruppo di disponibilità, è possibile impostare una replica di backup preferita.



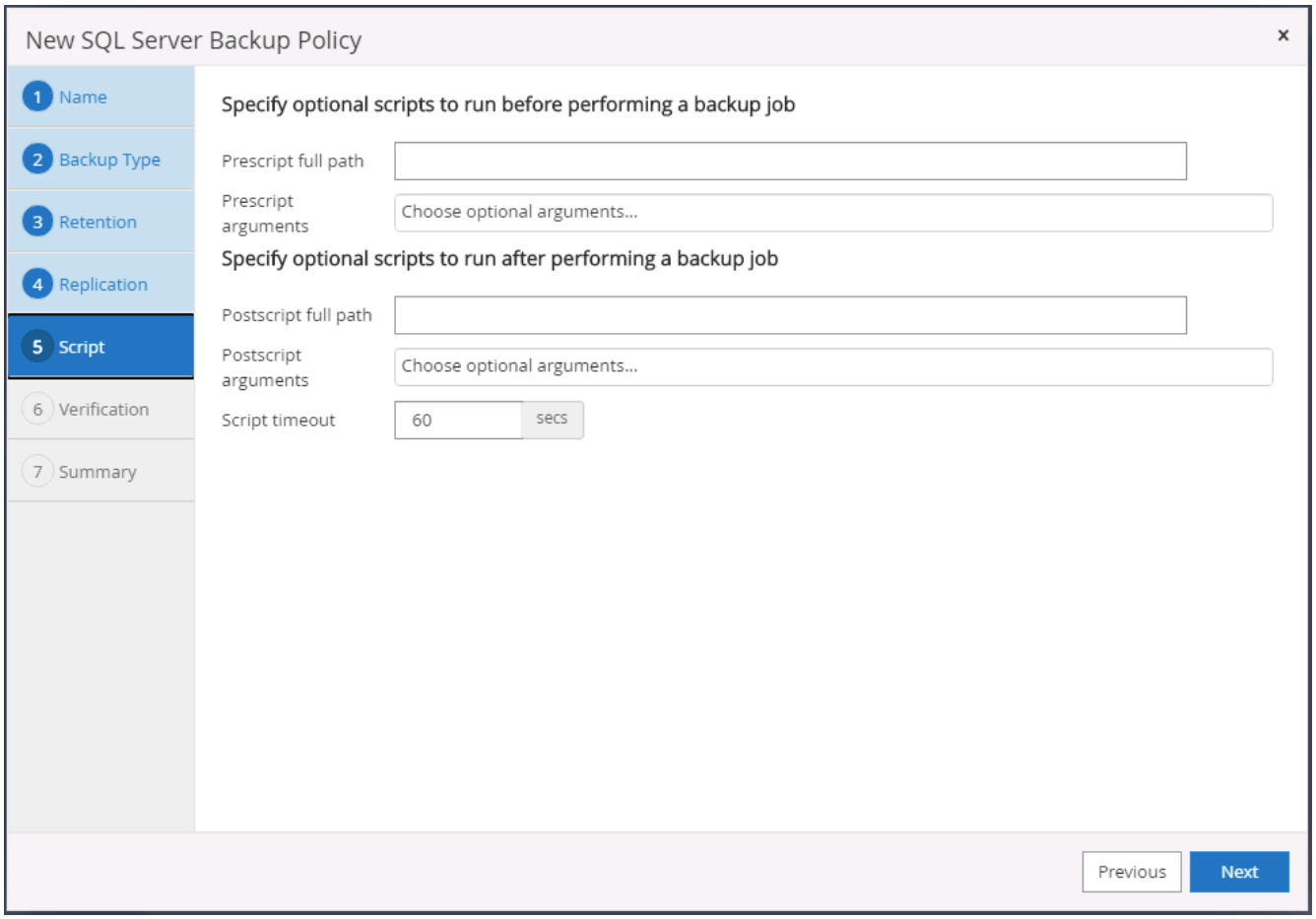
4. Imposta il periodo di conservazione del backup.



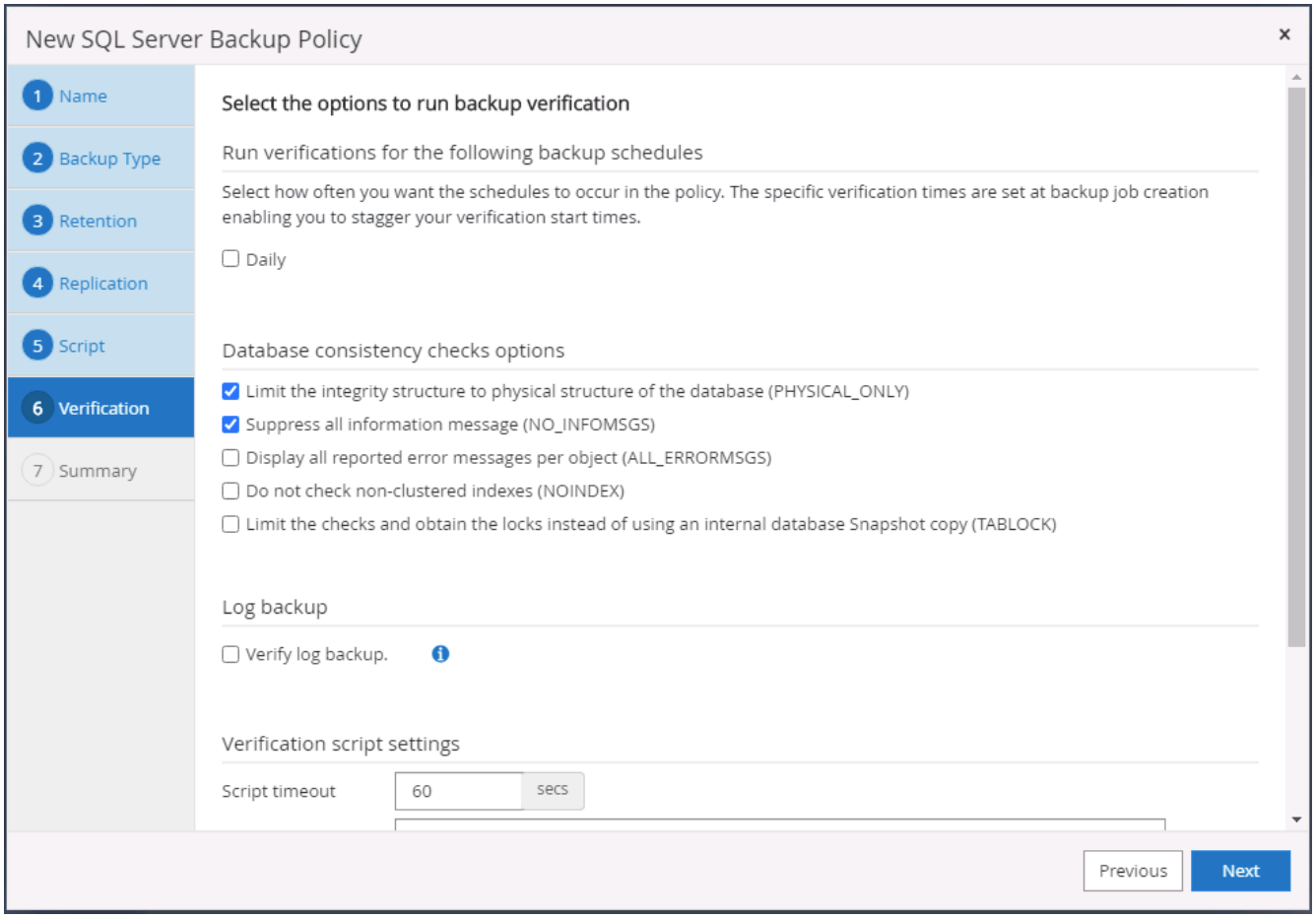
5. Abilita la replica della copia di backup in una posizione secondaria nel cloud.



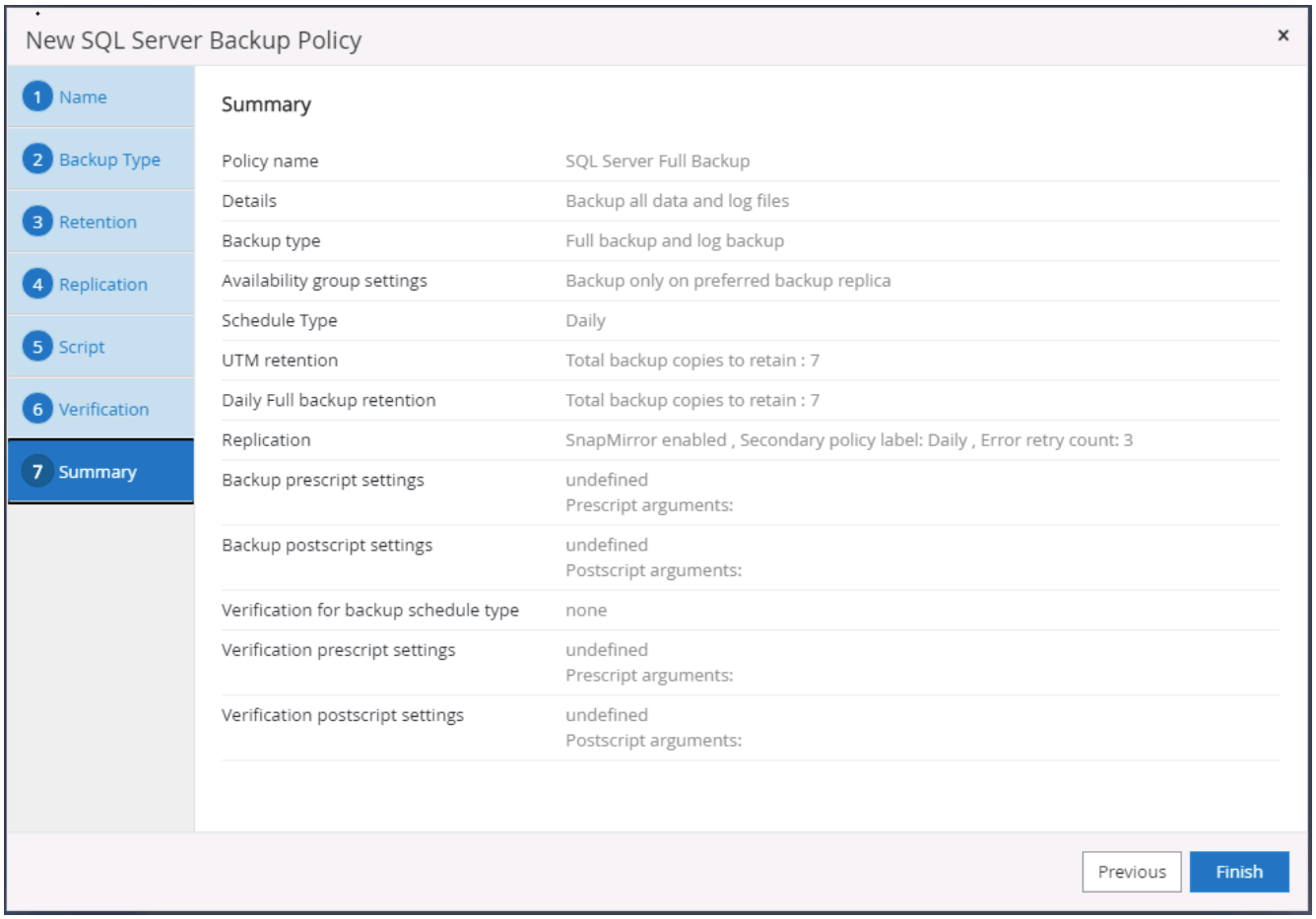
6. Specificare eventuali script facoltativi da eseguire prima o dopo un processo di backup.



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

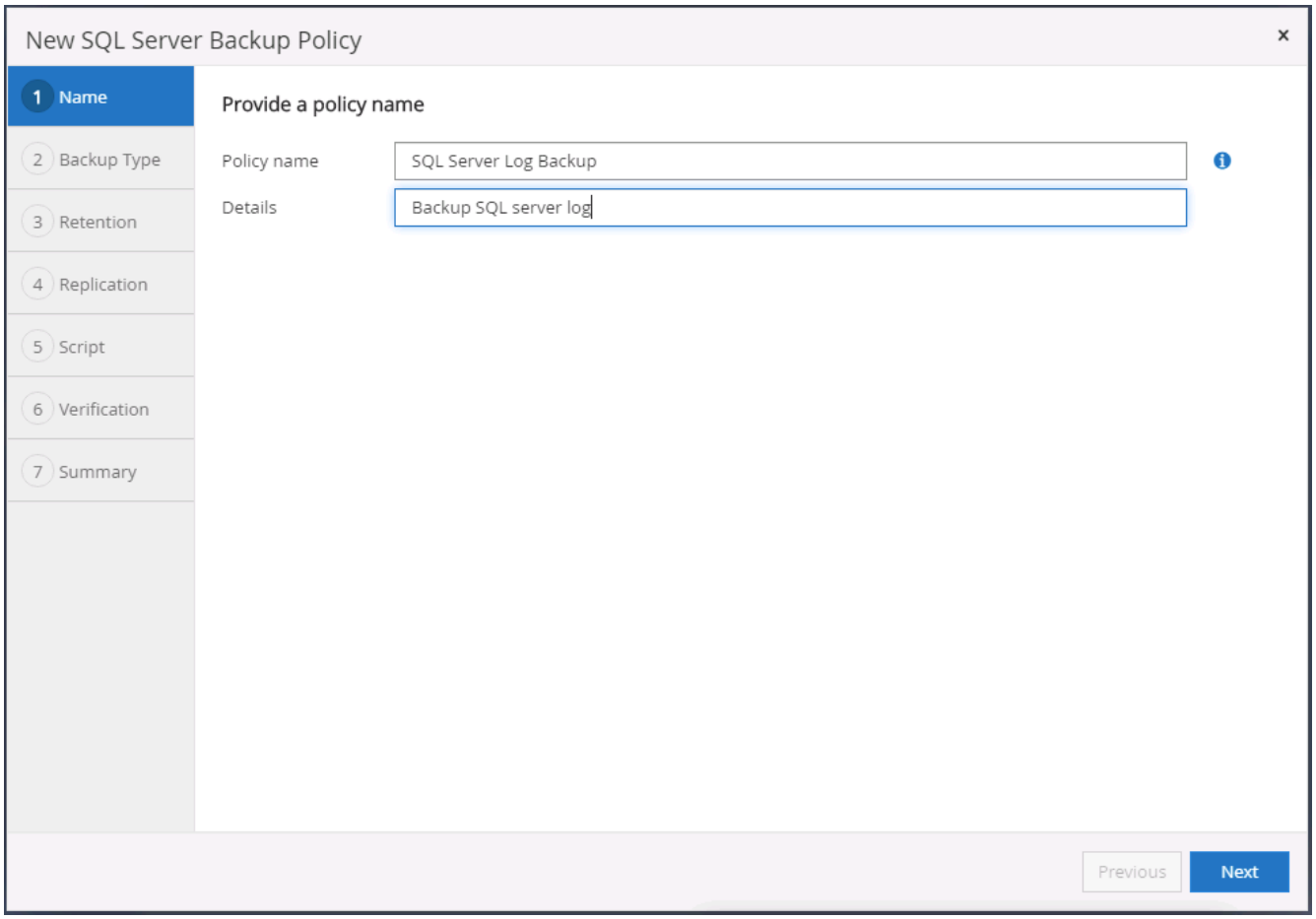

New SQL Server Backup Policy
1 Name
2 Backup Type
3 Retention
4 Replication
5 Script
6 Verification
7 Summary
Select the options to run backup verification
Run verifications for the following backup schedules
Select how often you want the schedules to occur in the policy. The specific verification times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

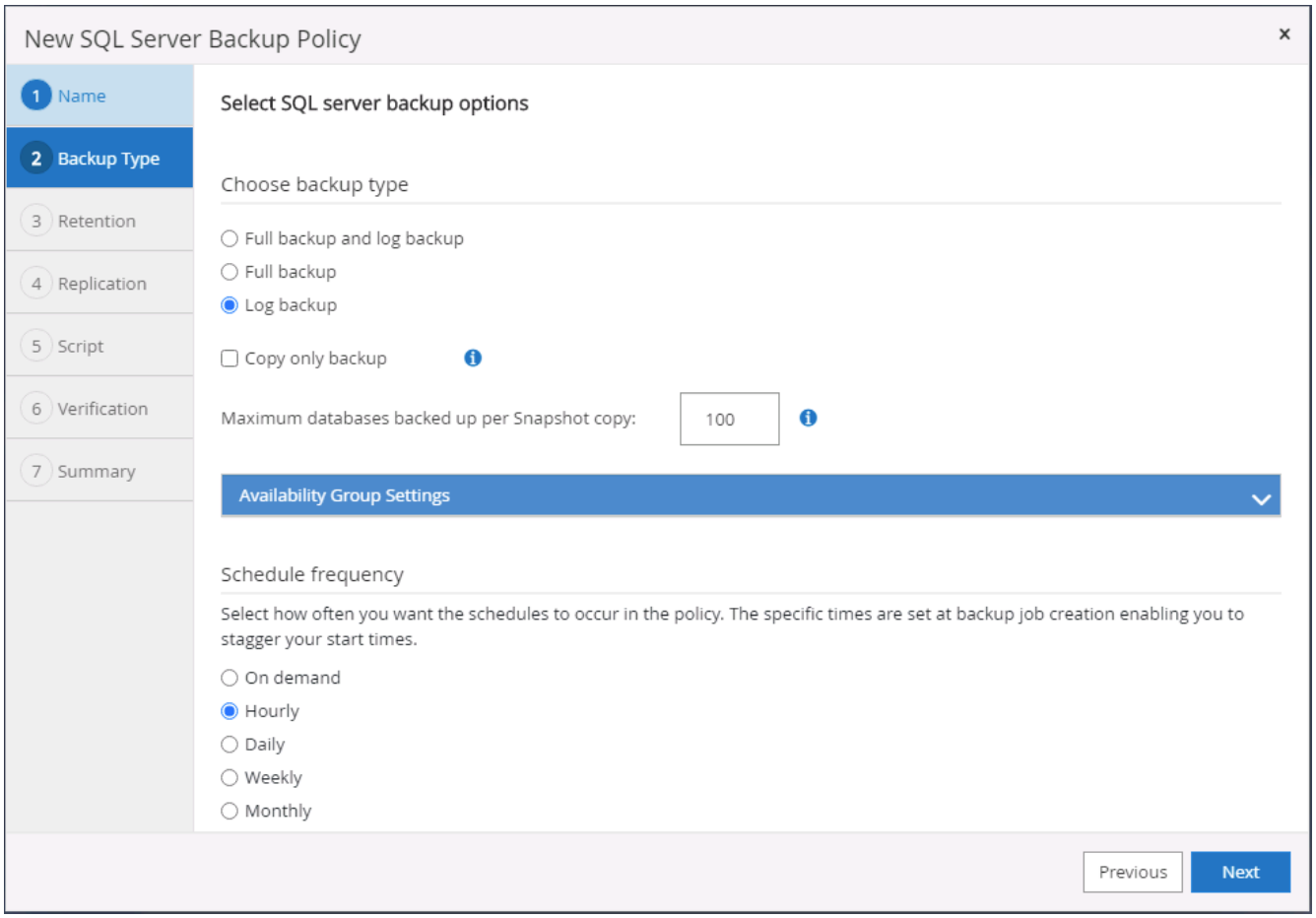


Creare un criterio di backup del log del database per SQL.

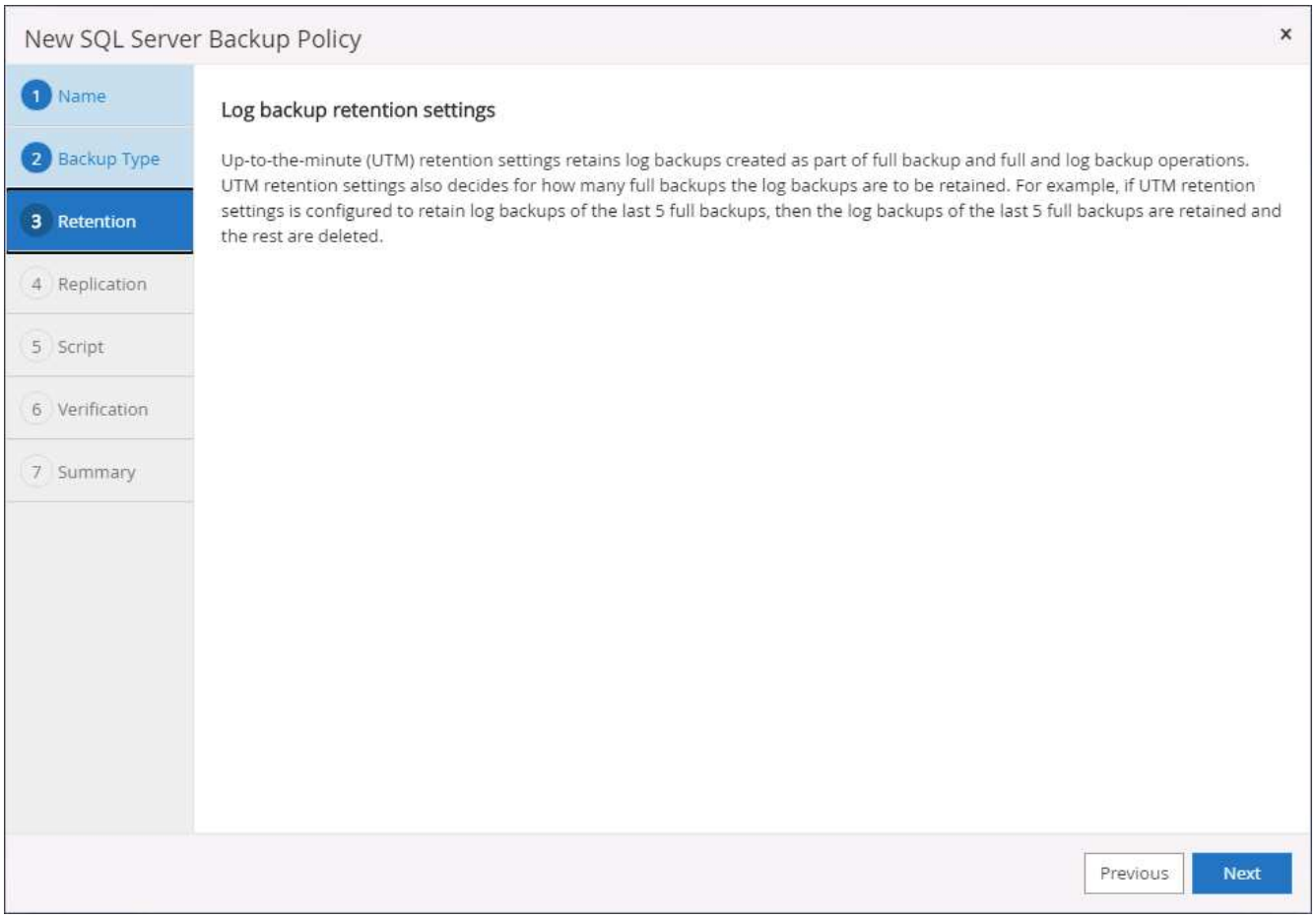
1. Accedi a SnapCenter con un ID utente di gestione del database, fai clic su Impostazioni > Criteri, quindi su Nuovo per avviare un nuovo flusso di lavoro per la creazione di criteri.



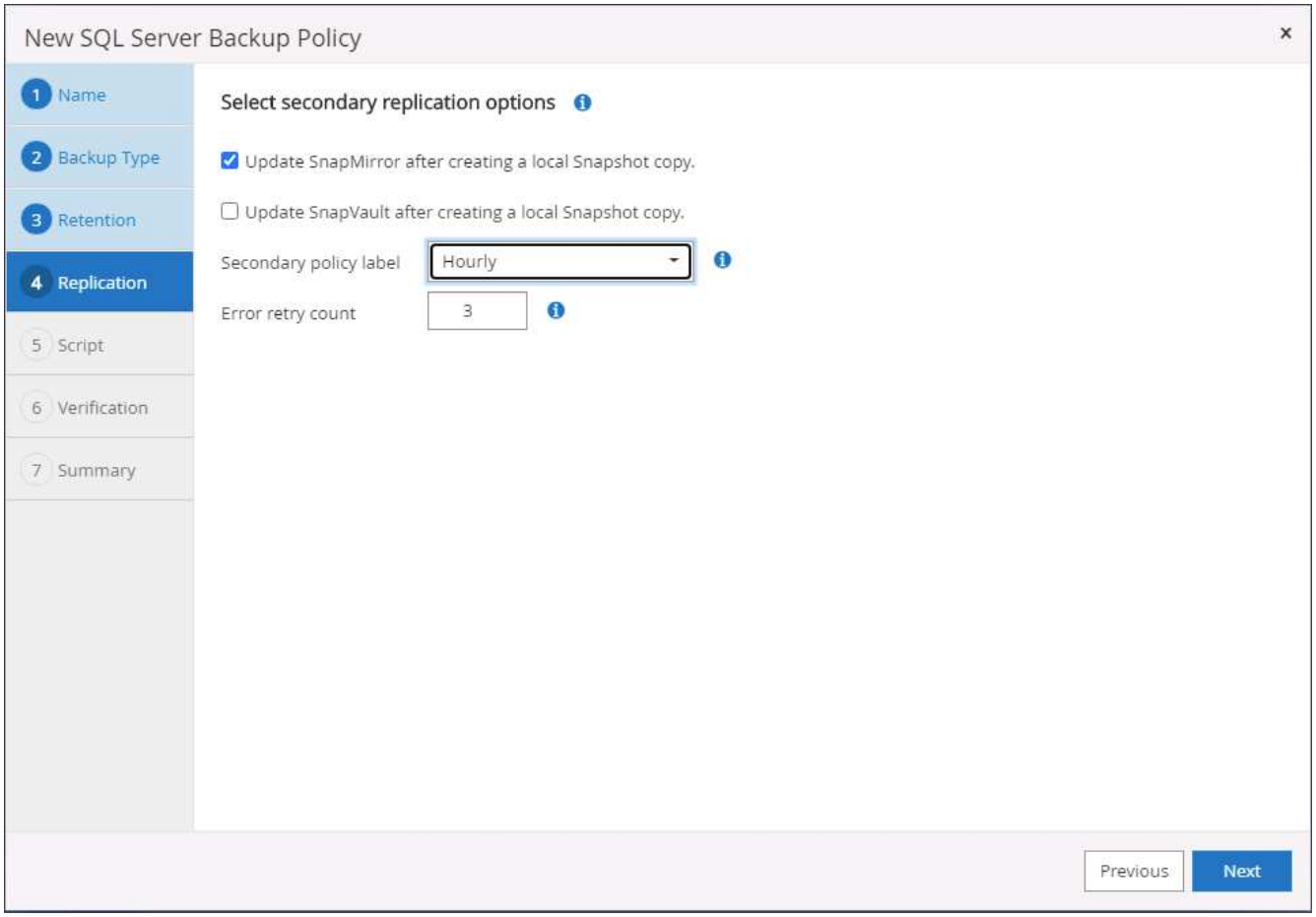
2. Definire l'opzione di backup del registro e la frequenza di pianificazione. Per SQL Server configurato con un gruppo di disponibilità, è possibile impostare una replica di backup preferita.



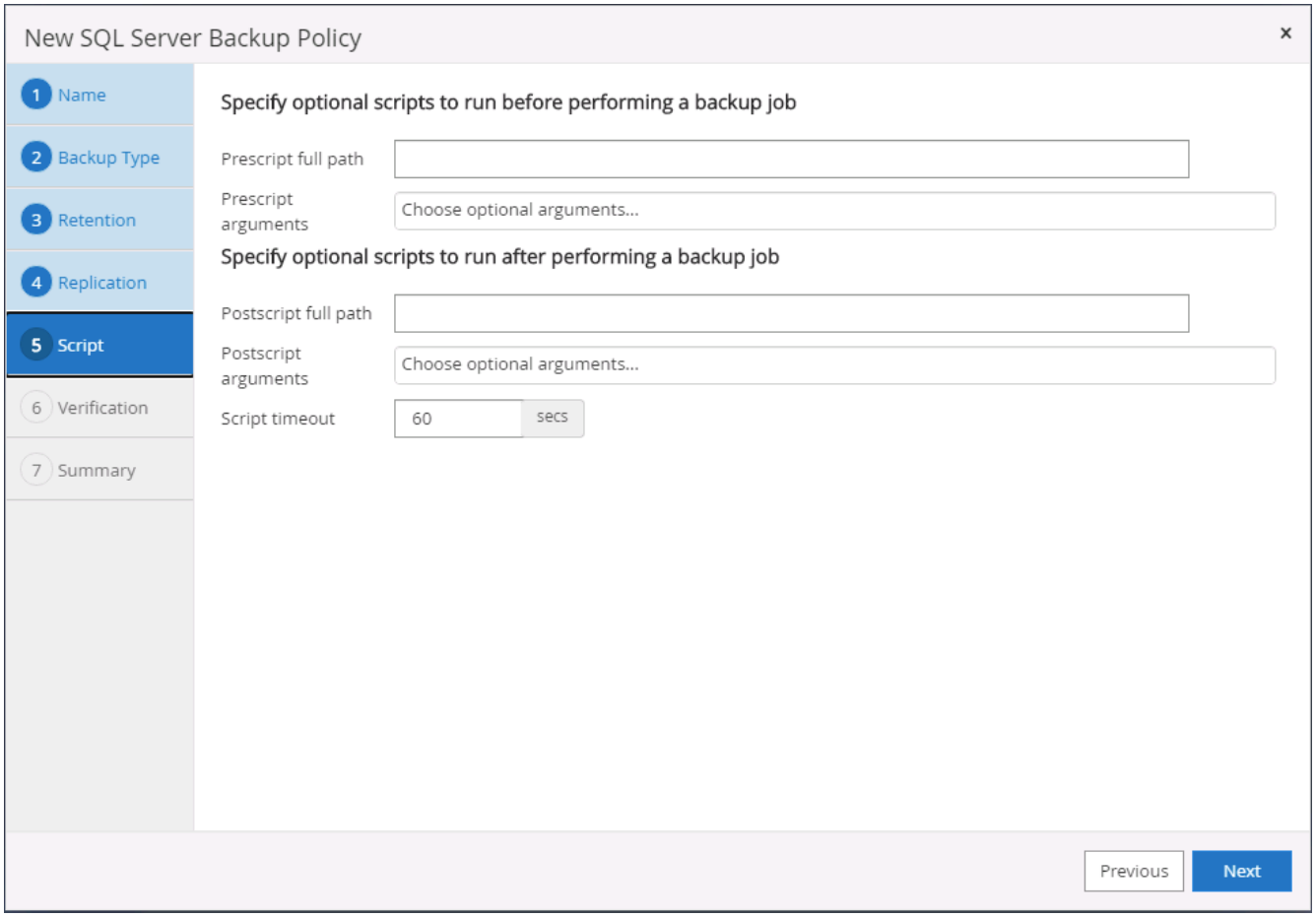
3. I criteri di backup dei dati di SQL Server definiscono la conservazione del backup del log; accettare i valori predefiniti.



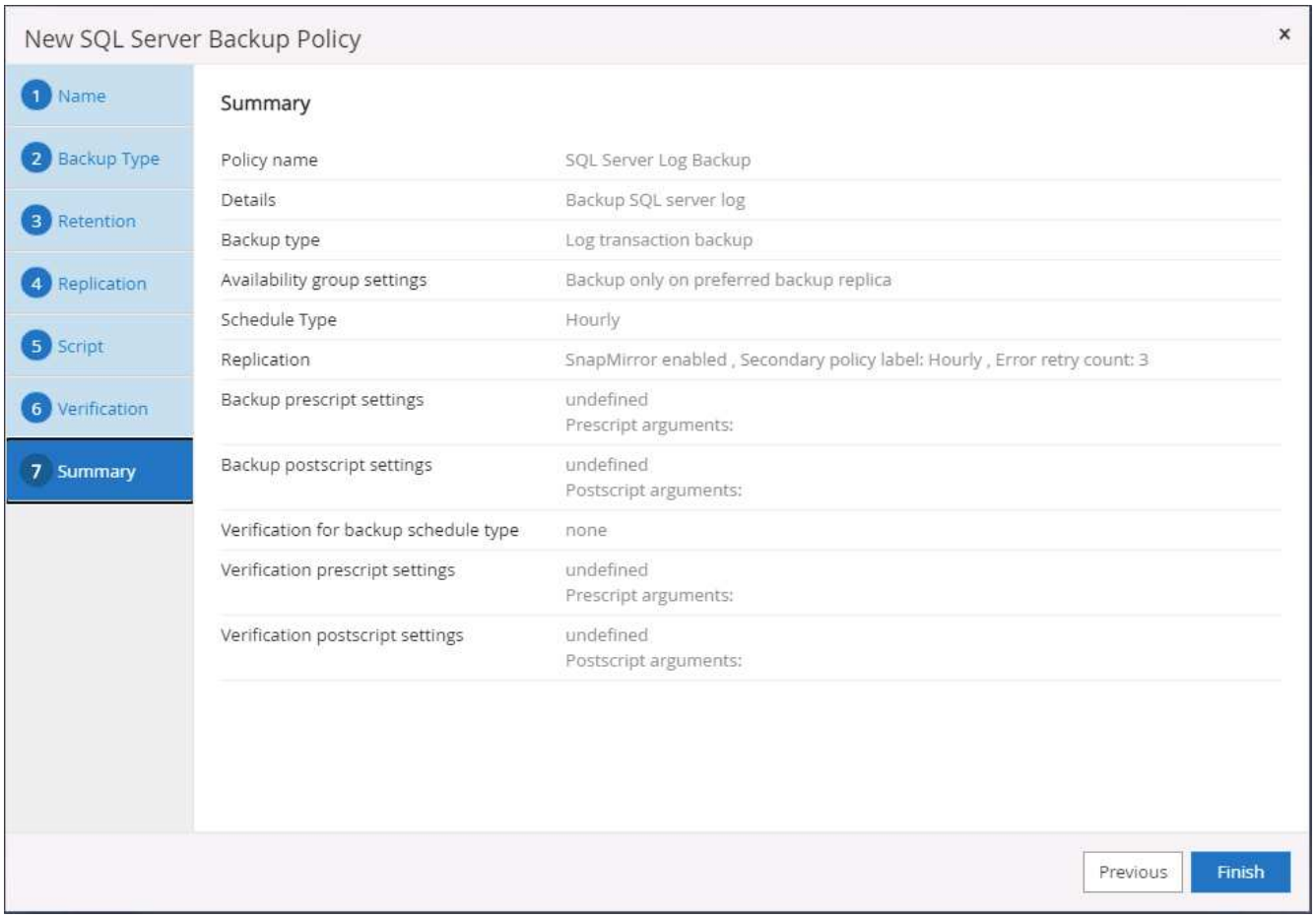
4. Abilita la replica del backup del registro sul server secondario nel cloud.



5. Specificare eventuali script facoltativi 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.

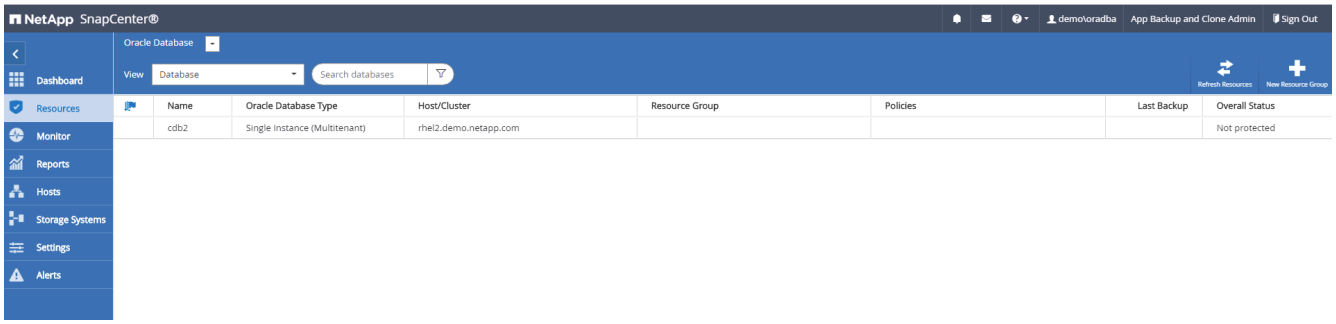


8. Implementare una politica di backup per proteggere il database

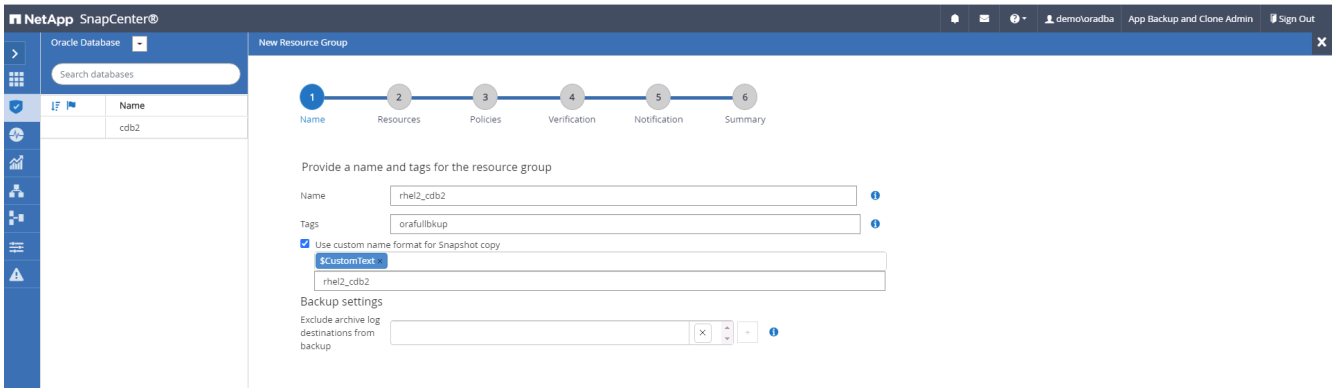
SnapCenter utilizza un gruppo di risorse per eseguire il backup di un database in un raggruppamento logico di risorse del database, ad esempio più database ospitati su un server, un database che condivide gli stessi volumi di archiviazione, più database che supportano un'applicazione aziendale e così via. La protezione di un singolo database crea un gruppo di risorse a sé stante. Le seguenti procedure illustrano 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

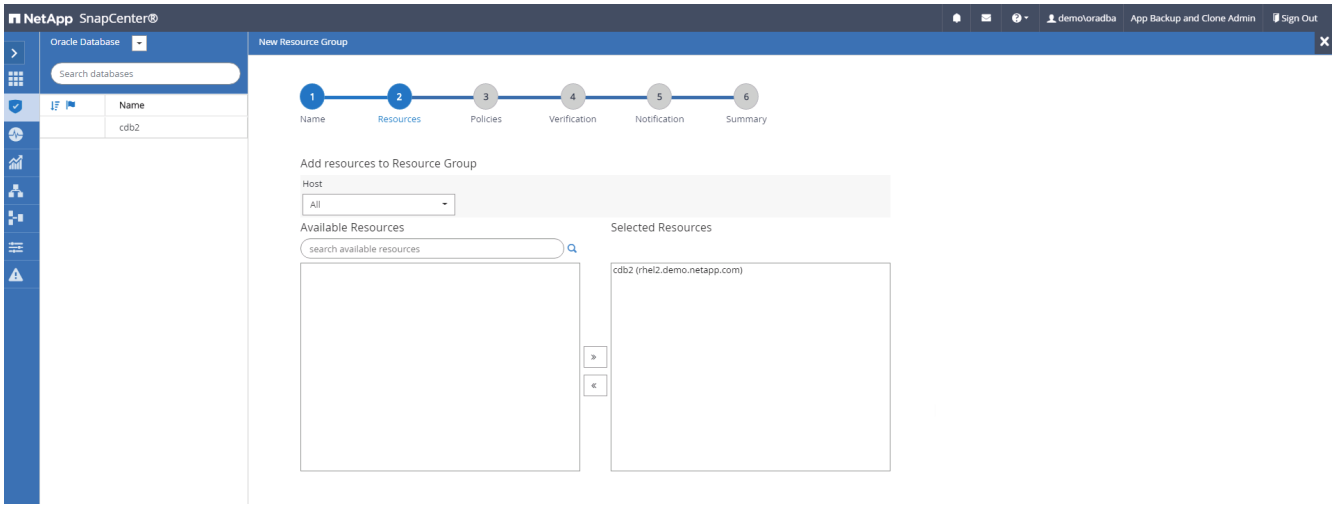
1. Accedi a SnapCenter con un ID utente di gestione del database e vai alla scheda Risorse. Nell'elenco a discesa Visualizza, seleziona Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.



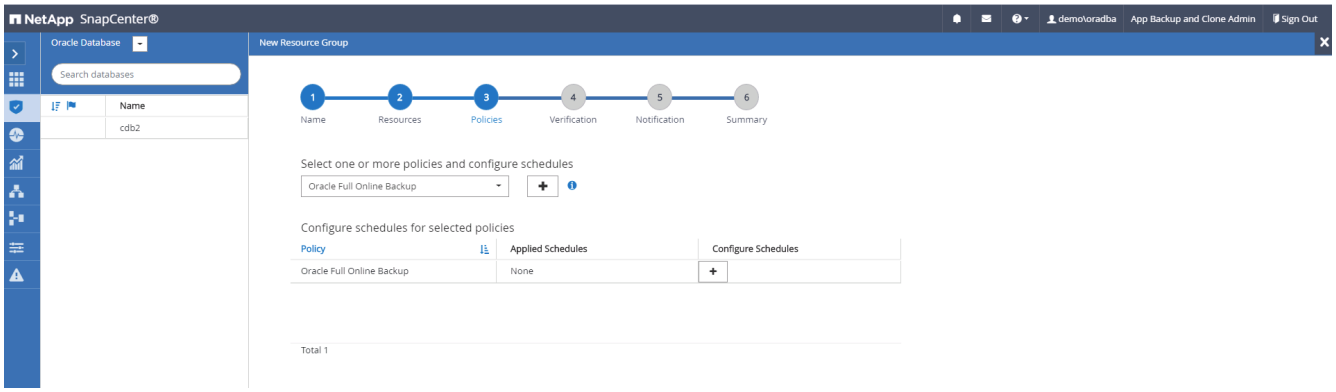
2. Fornire un nome e dei tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archivio ridondante, se configurata.



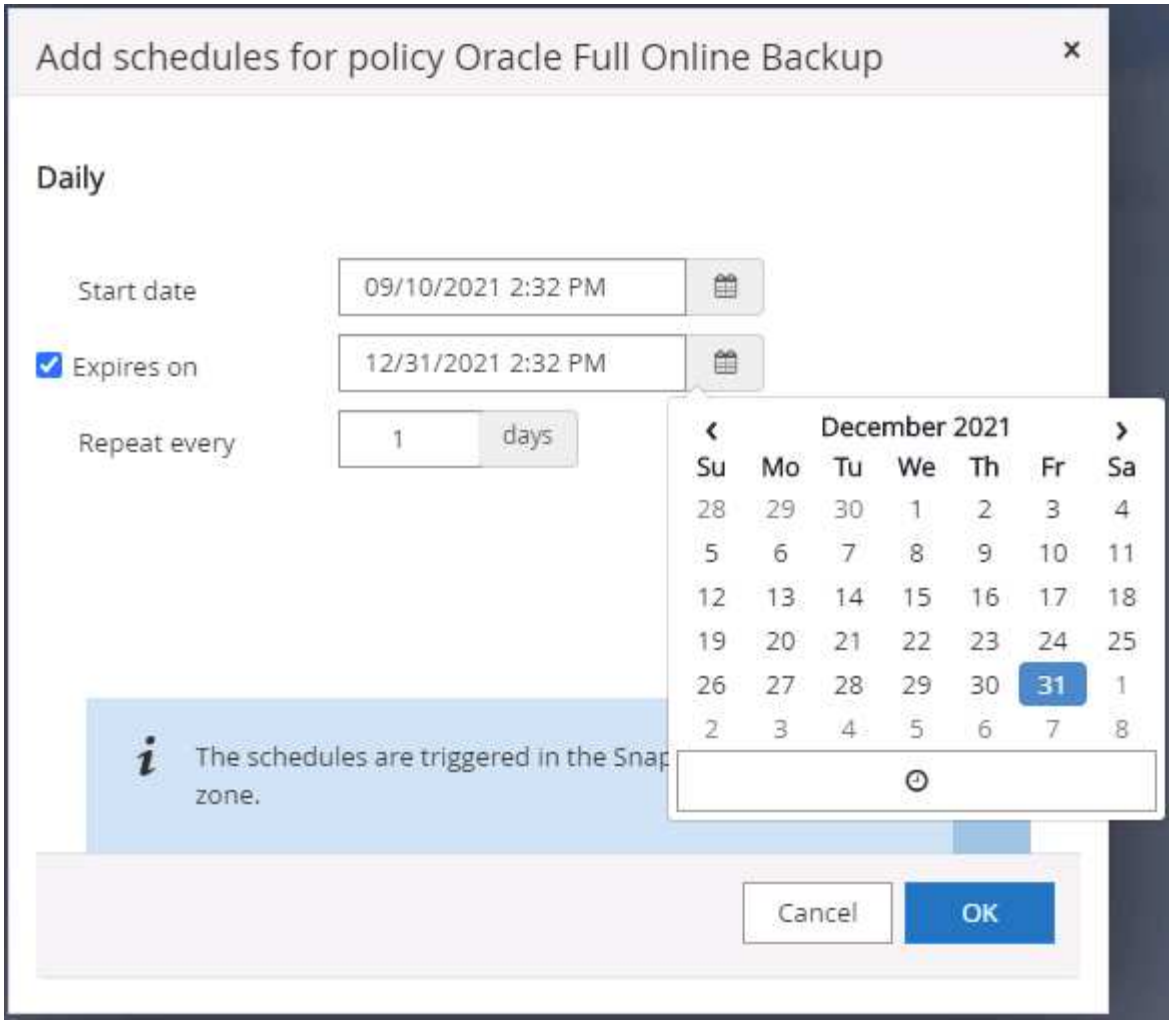
3. Aggiungere risorse del database al gruppo di risorse.



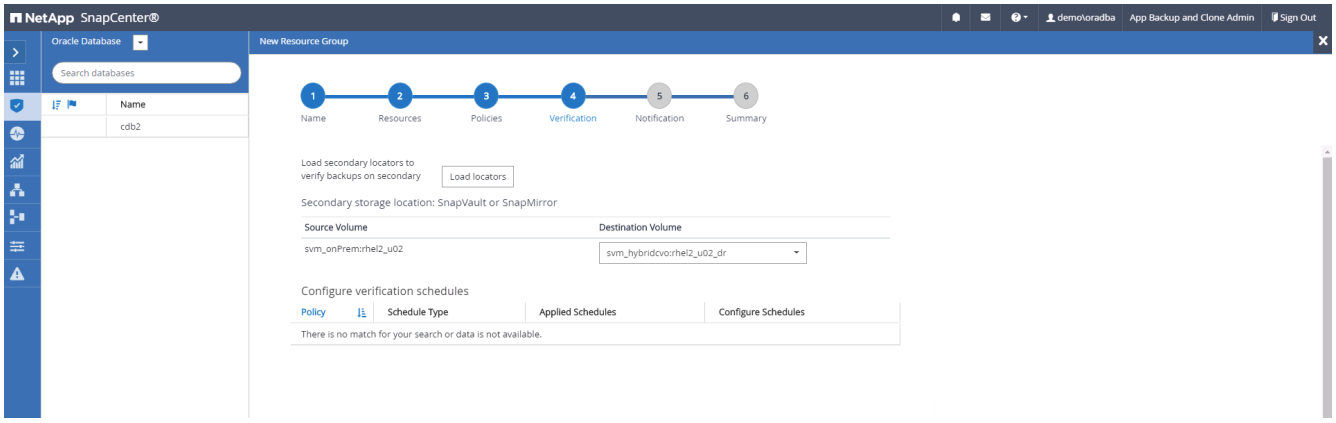
4. Selezionare dall'elenco a discesa un criterio di backup completo creato nella sezione 7.



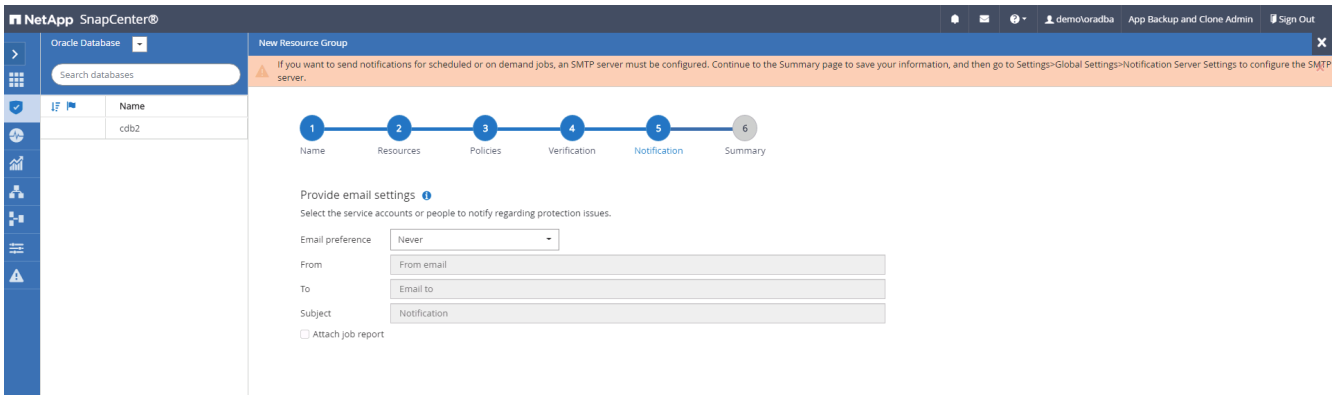
5. Fare clic sul segno (+) per configurare la pianificazione del backup desiderata.



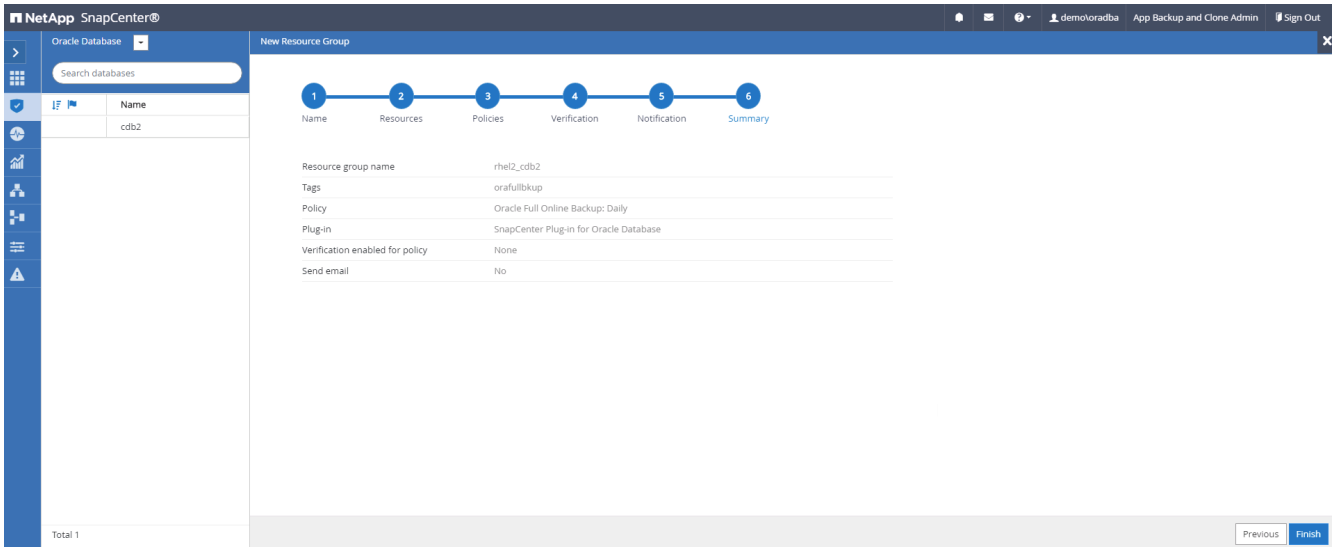
6. Fare clic su Carica localizzatori per caricare il volume di origine e di destinazione.



7. Se lo si desidera, configurare il server SMTP per la notifica via e-mail.

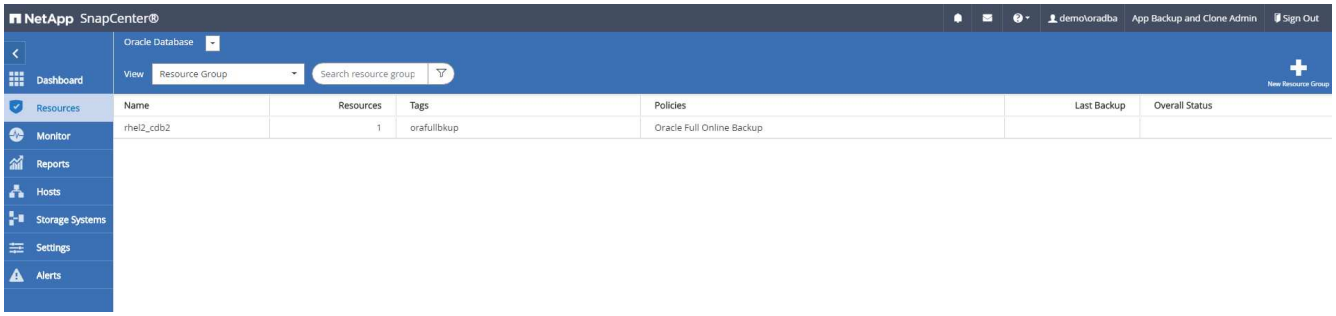


8. Riepilogo.

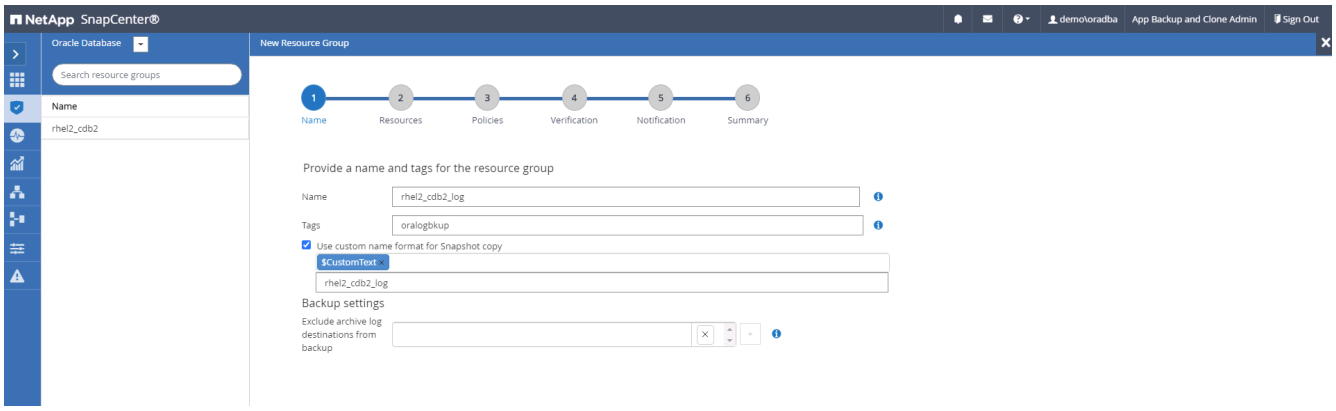


Creare un gruppo di risorse per il backup del log di Oracle

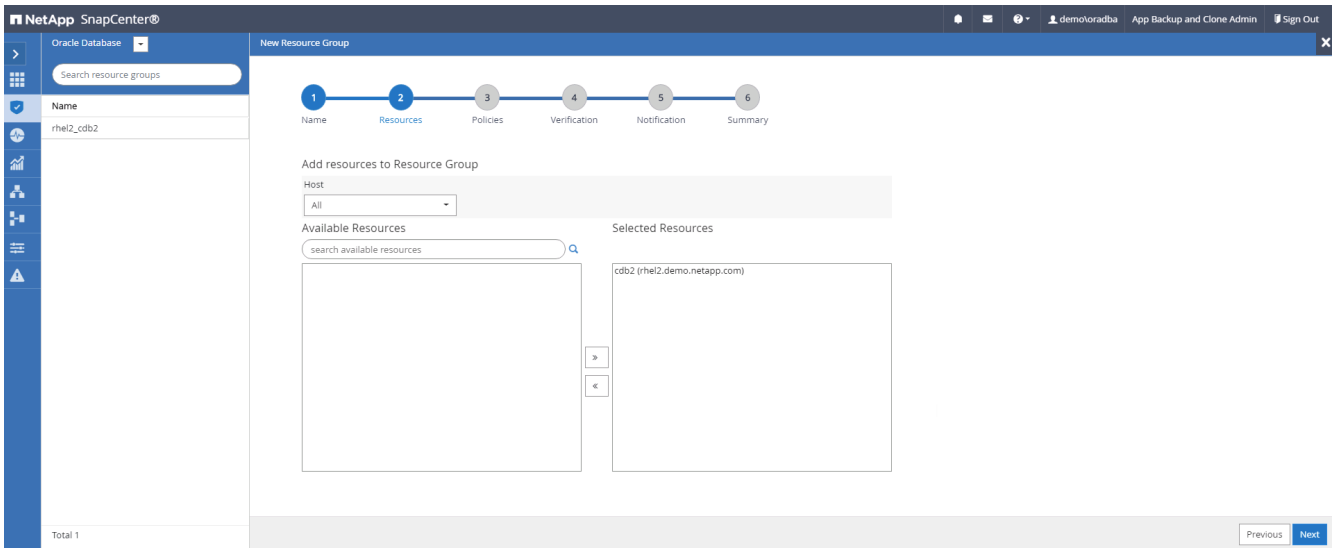
1. Accedi a SnapCenter con un ID utente di gestione del database e vai alla scheda Risorse. Nell'elenco a discesa Visualizza, seleziona Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.



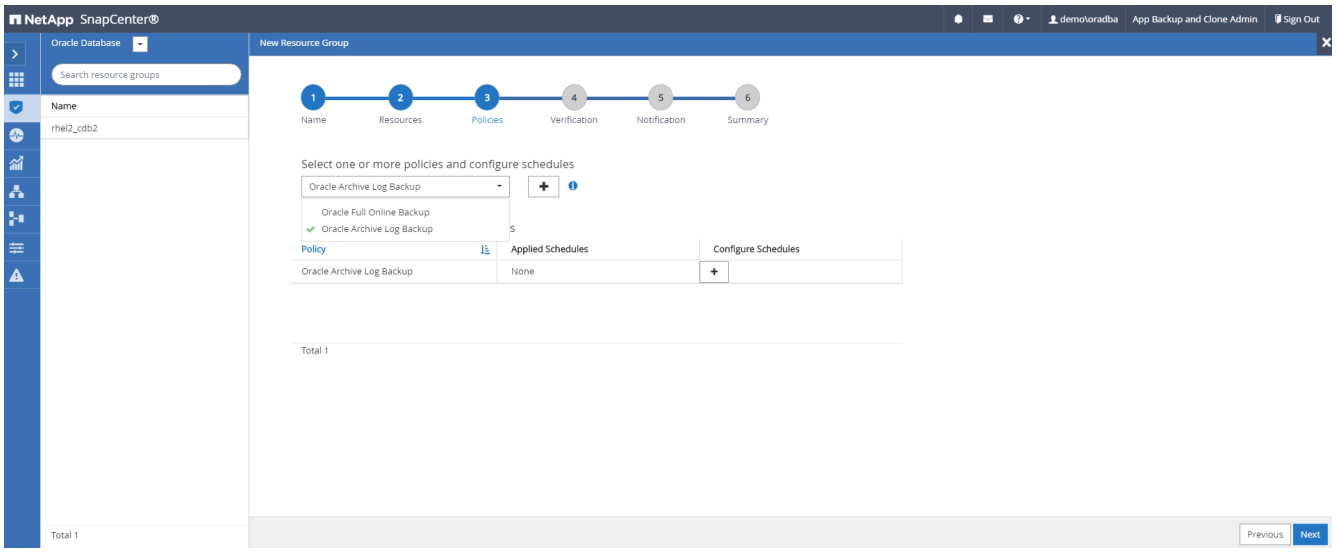
2. Fornire un nome e dei tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archivio ridondante, se configurata.



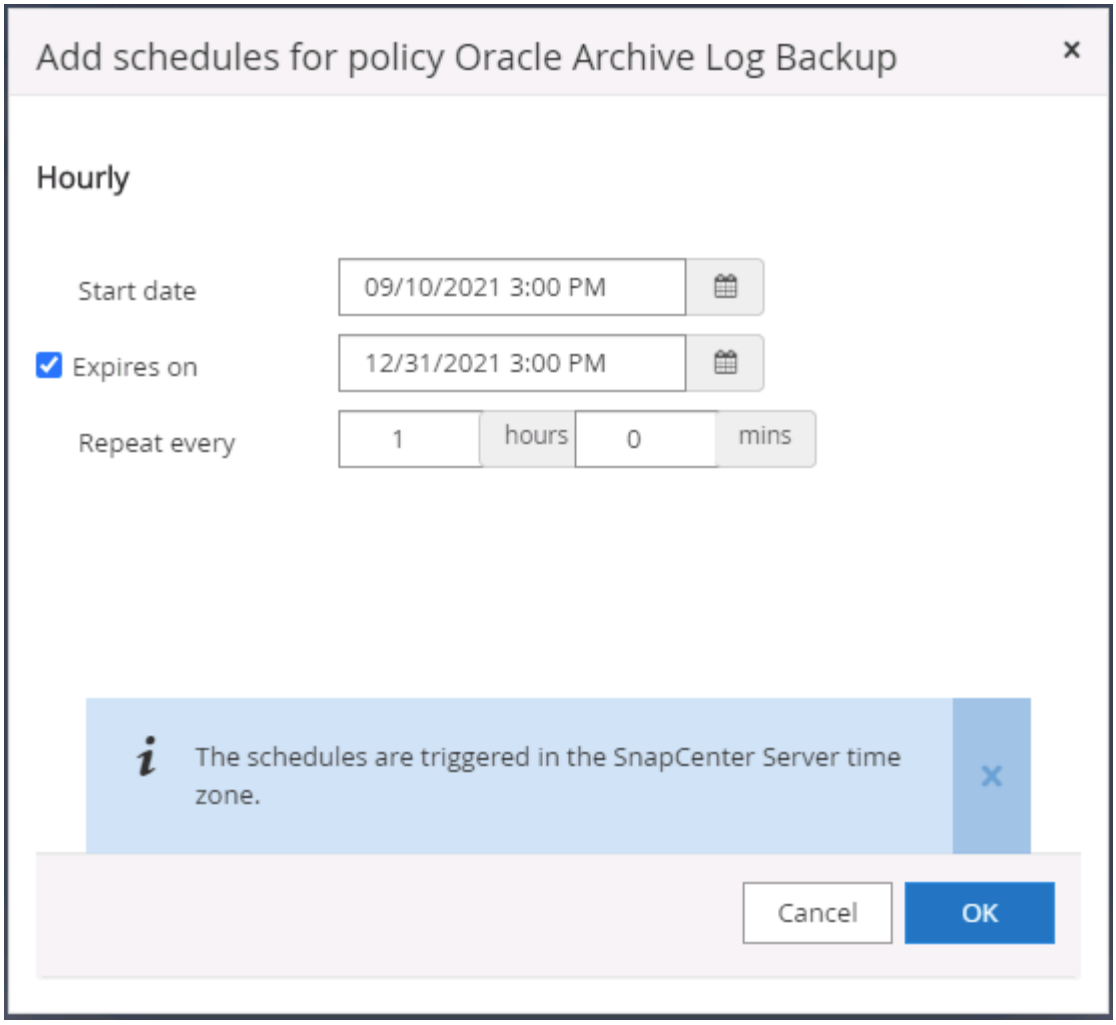
3. Aggiungere risorse del database al gruppo di risorse.



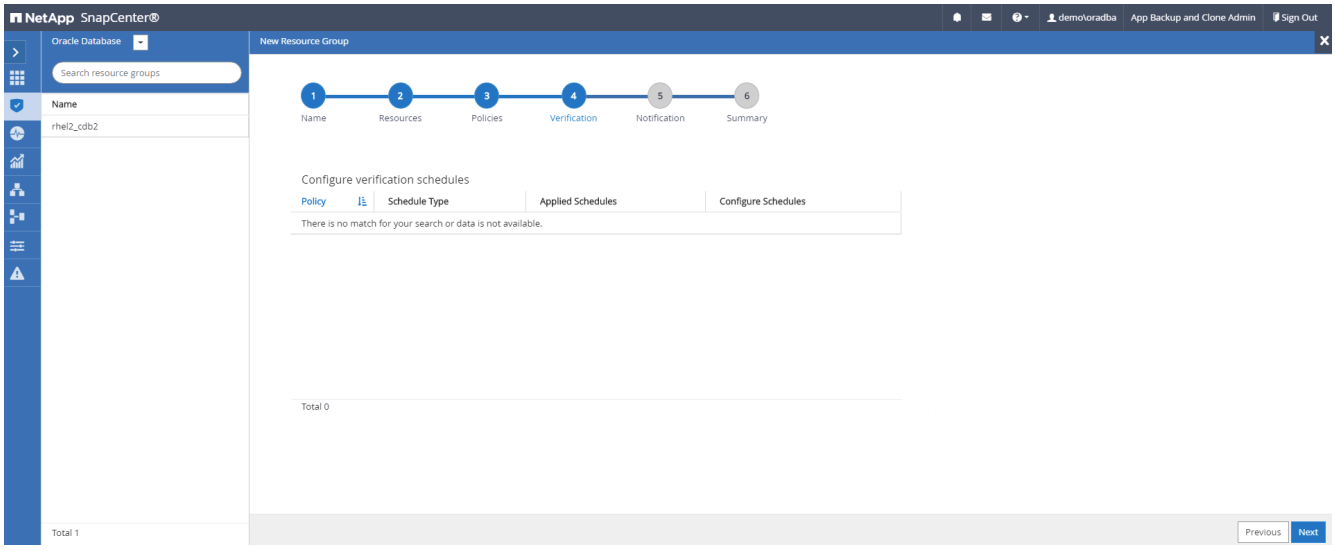
4. Selezionare dall'elenco a discesa un criterio di backup del registro creato nella sezione 7.



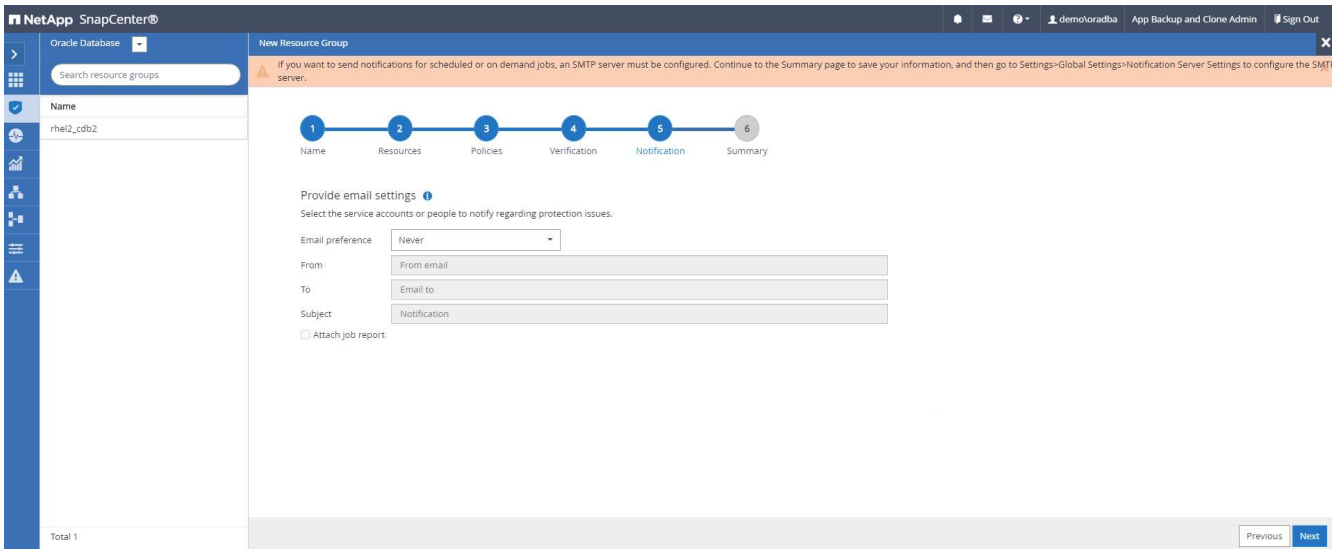
5. Fare clic sul segno (+) per configurare la pianificazione del backup desiderata.



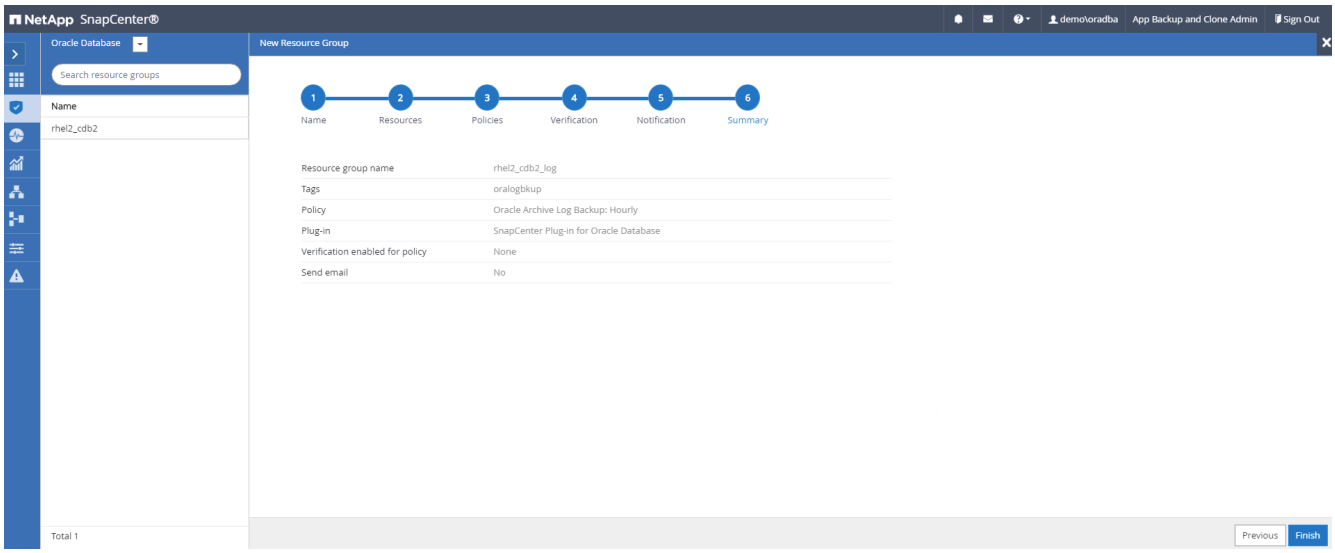
6. Se è configurata la verifica del backup, questa viene visualizzata qui.



7. Se lo si desidera, configurare un server SMTP per la notifica via e-mail.

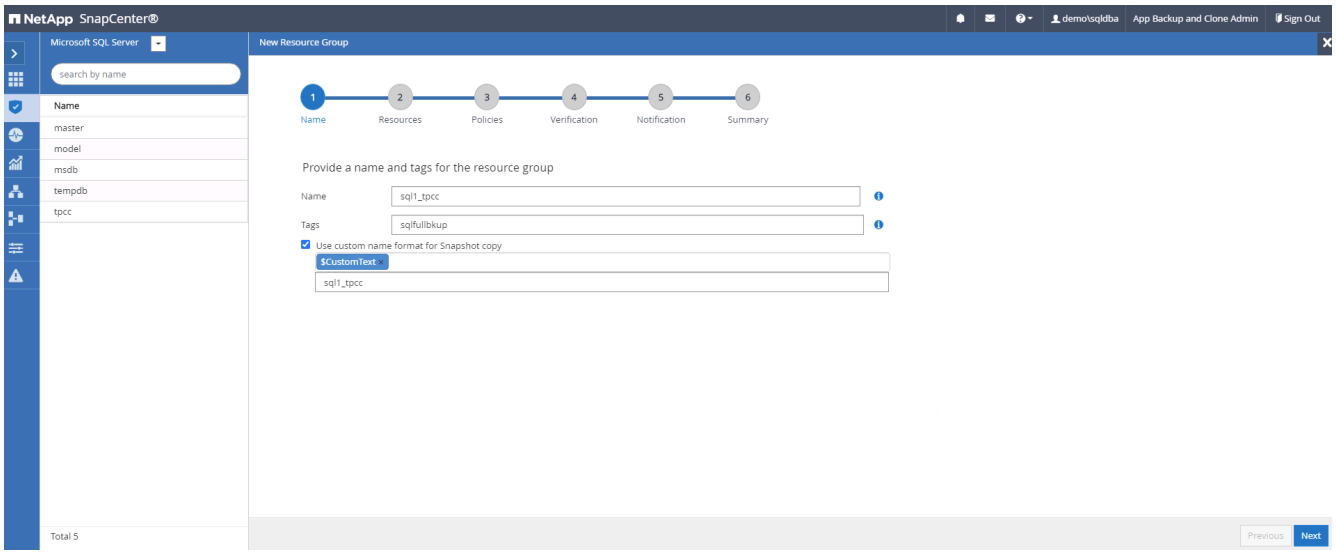


8. Riepilogo.

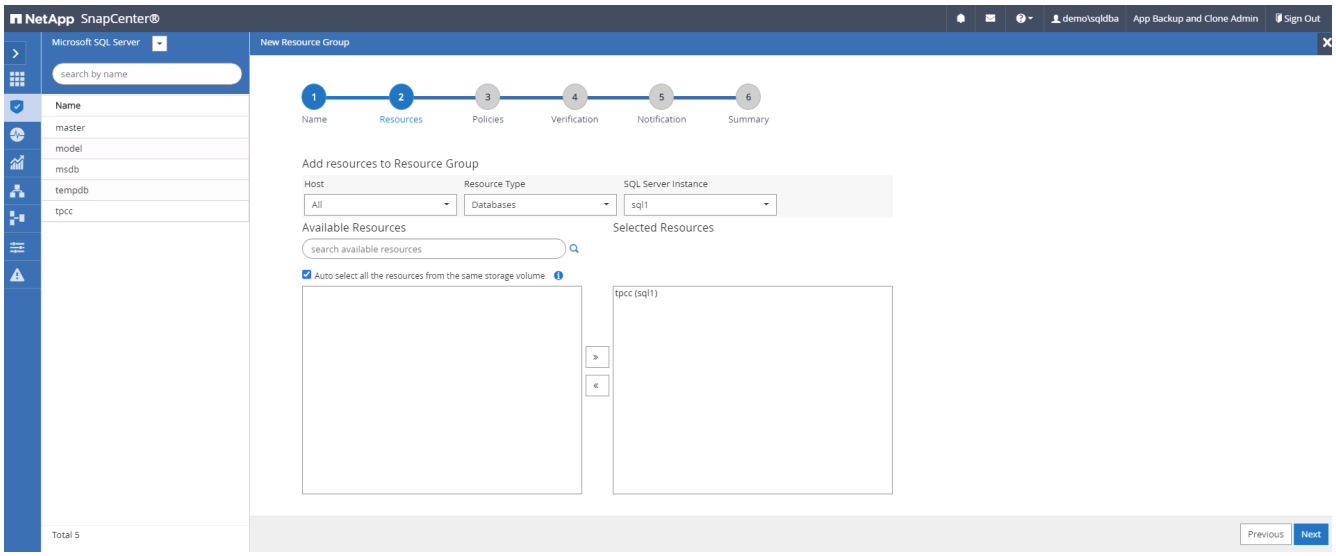


Creare un gruppo di risorse per il backup completo di SQL Server

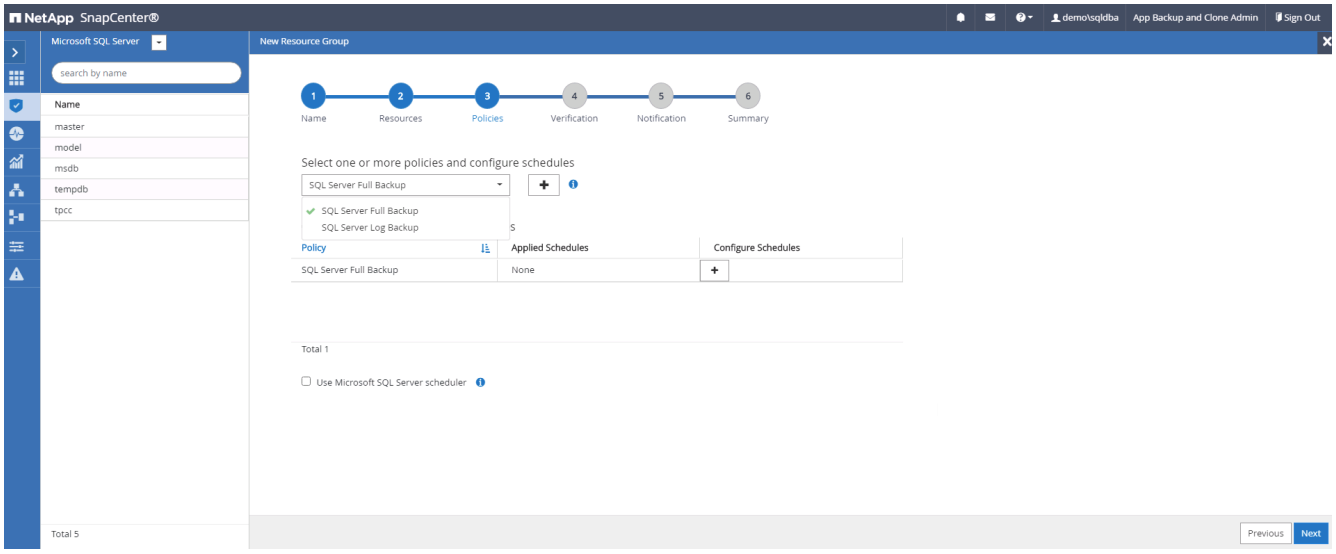
1. Accedi a SnapCenter con un ID utente di gestione del database e vai alla scheda Risorse. Nell'elenco a discesa Visualizza, seleziona un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire un nome e dei tag per il gruppo di risorse. È possibile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



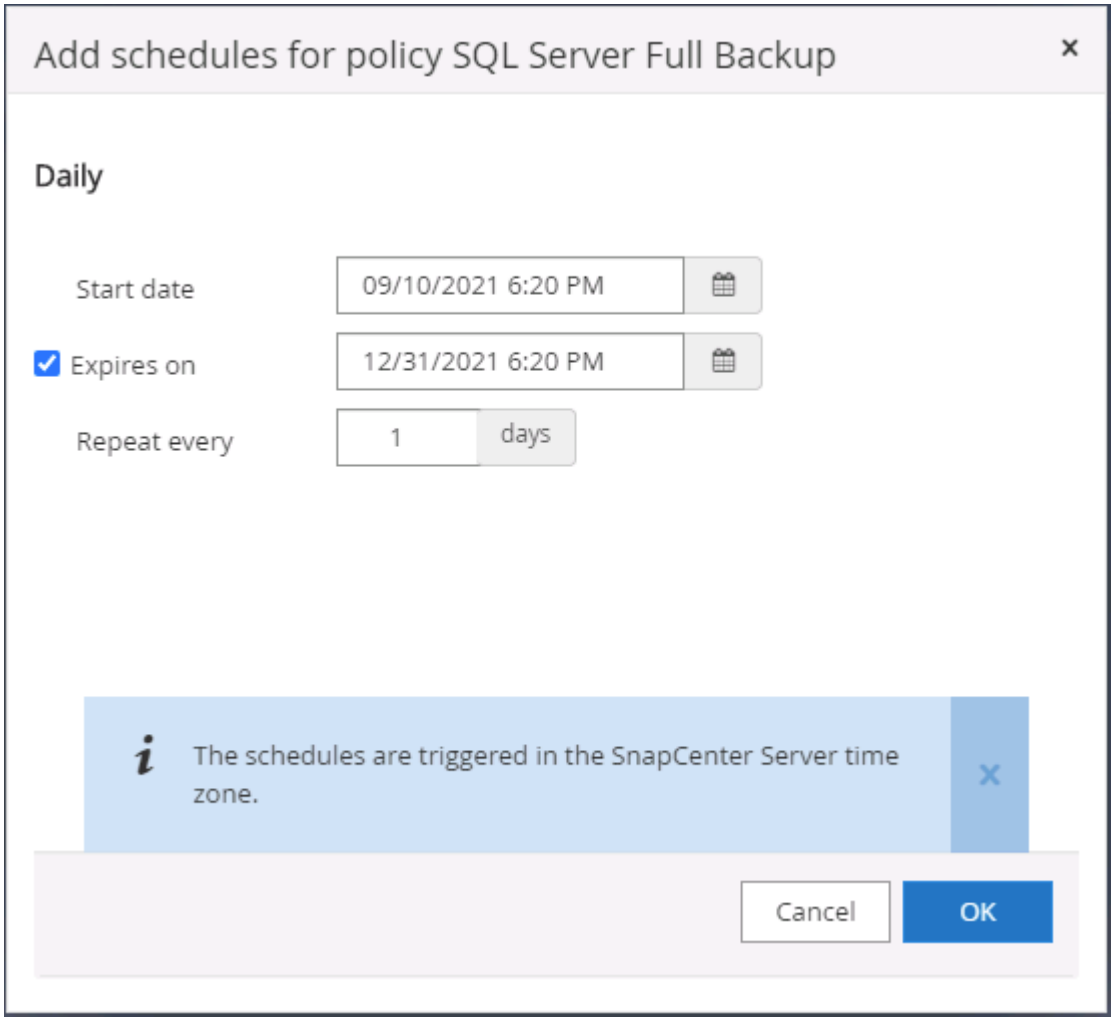
2. Selezionare le risorse del database di cui eseguire il backup.



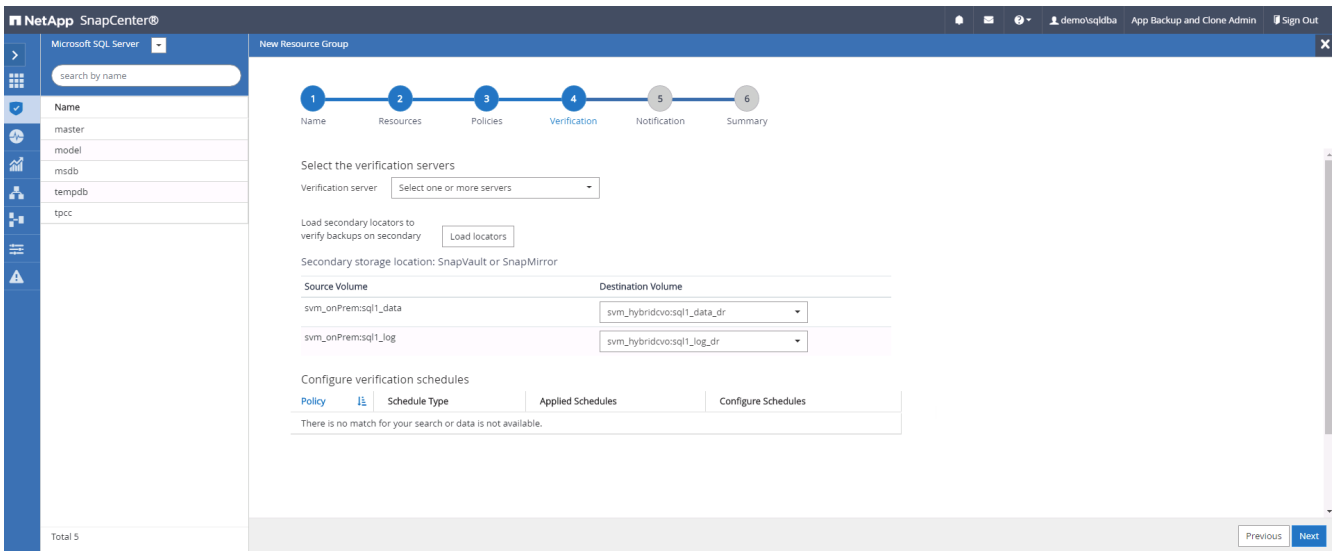
3. Selezionare un criterio di backup SQL completo creato nella sezione 7.



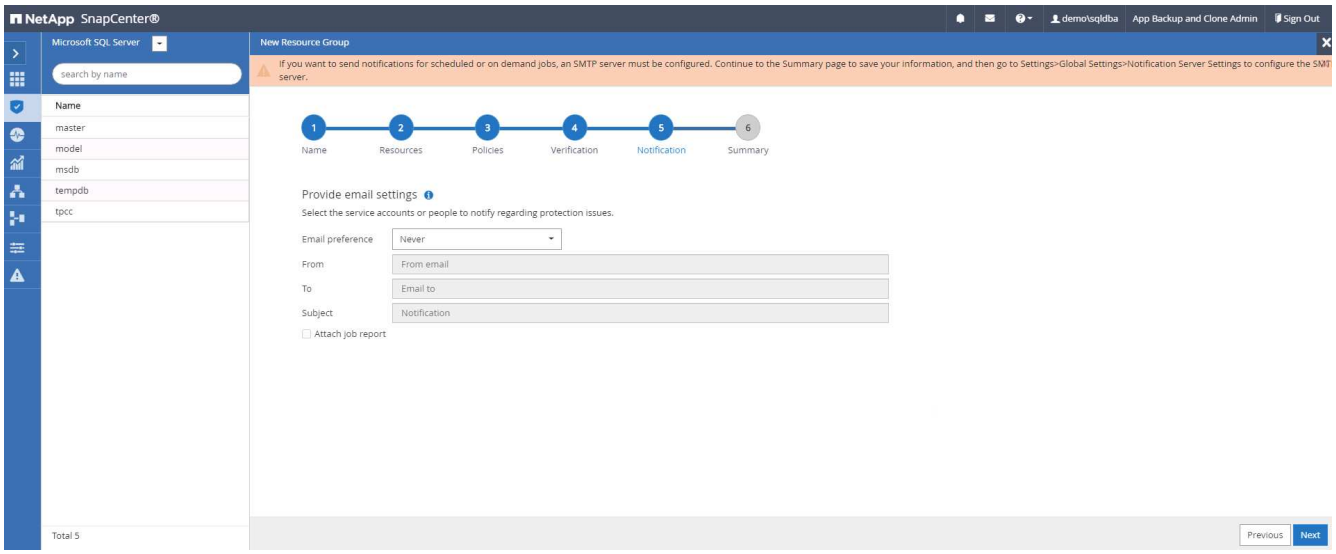
4. Aggiungere i tempi esatti per i backup e la frequenza.



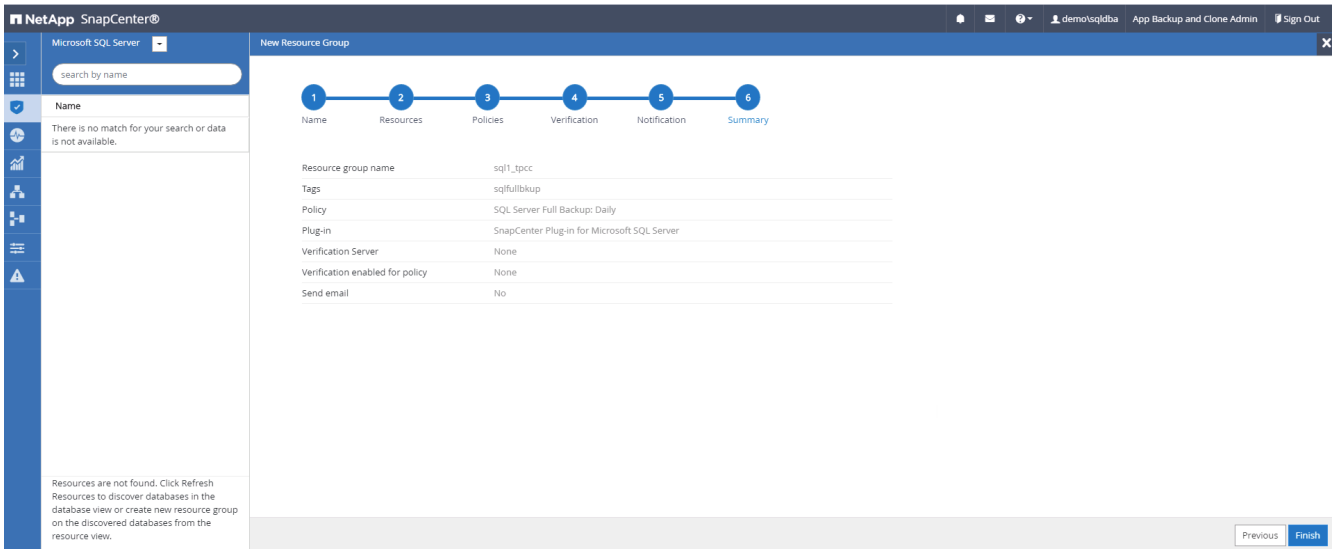
5. Selezionare il server di verifica per il backup secondario se si desidera eseguire la verifica del backup. Fare clic su Carica localizzatore per popolare la posizione di archiviazione secondaria.



6. Se lo si desidera, configurare il server SMTP per la notifica via e-mail.

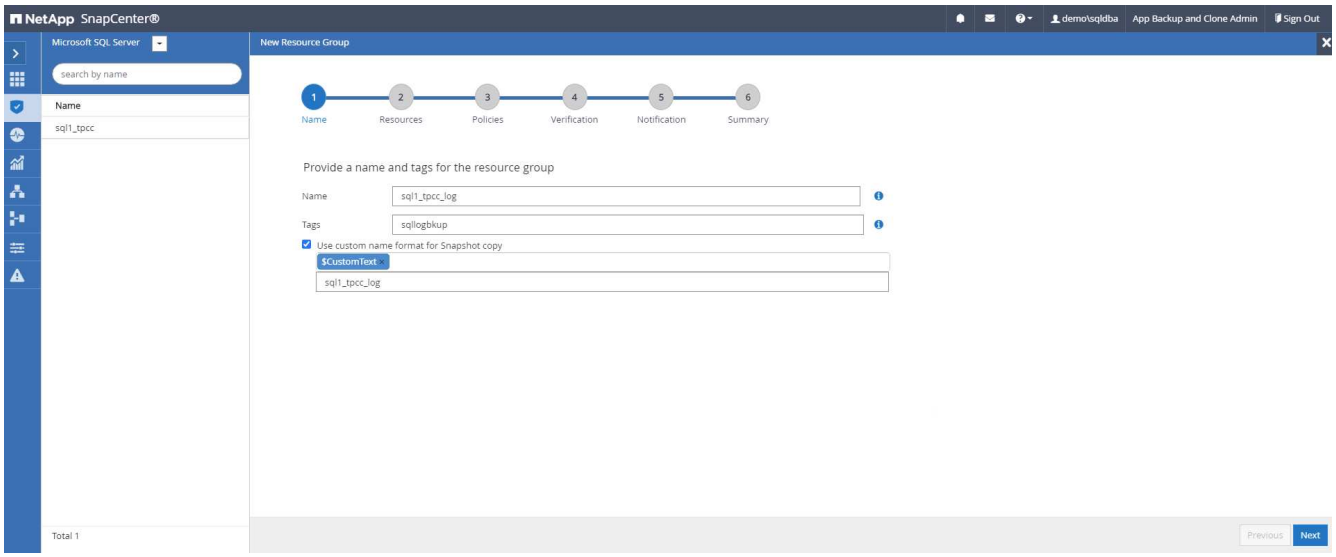


7. Riepilogo.

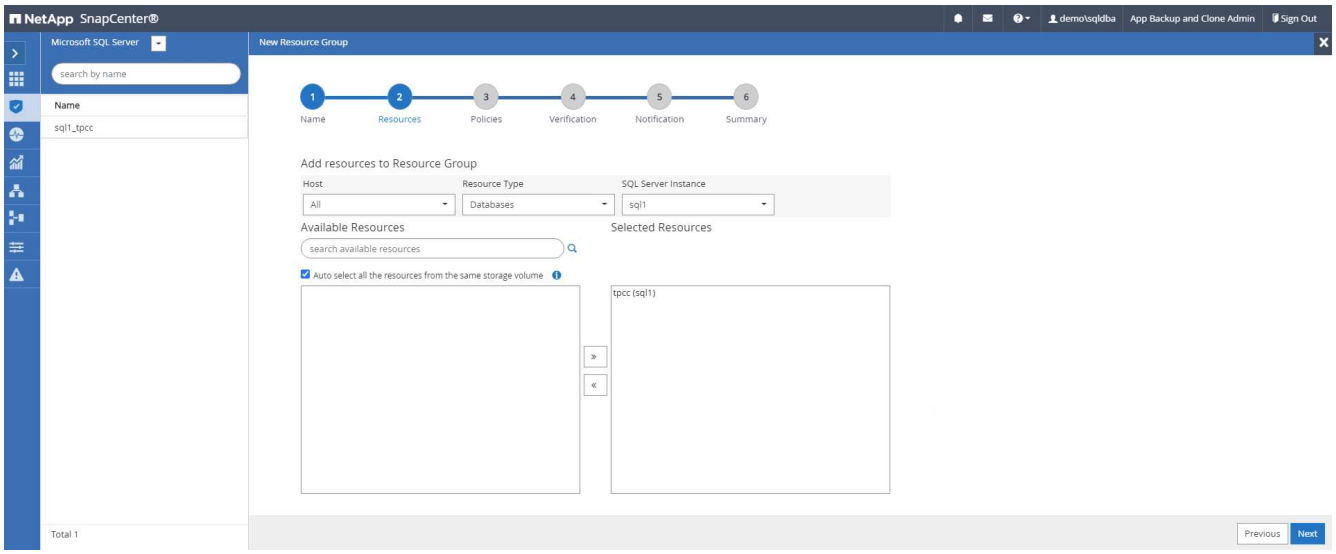


Creare un gruppo di risorse per il backup del log di SQL Server

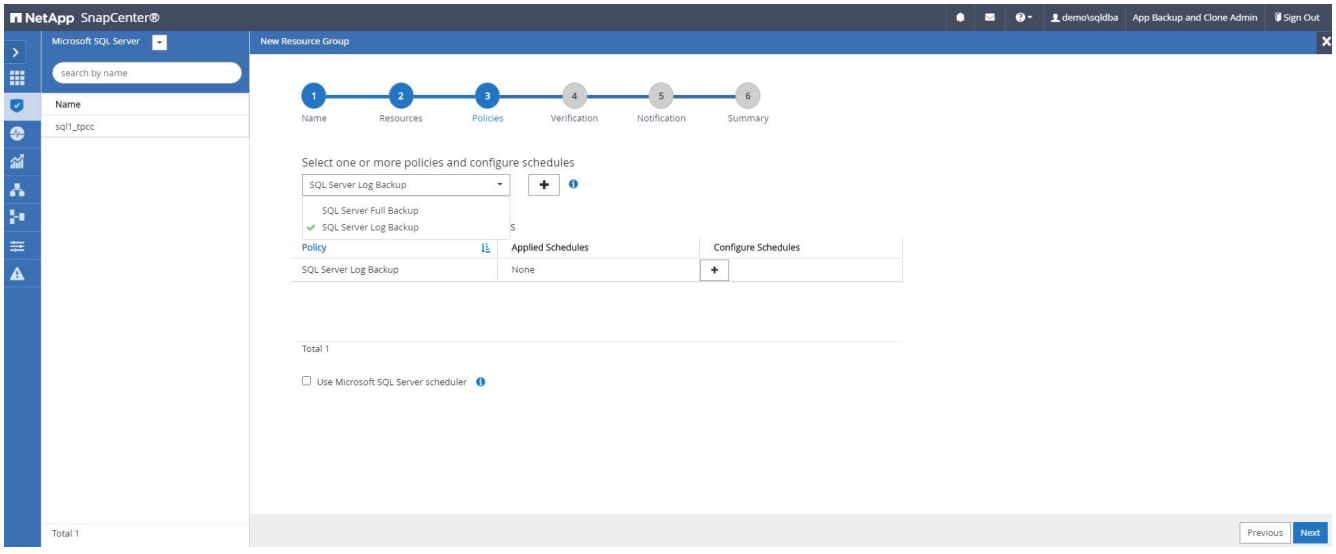
1. Accedi a SnapCenter con un ID utente di gestione del database e vai alla scheda Risorse. Nell'elenco a discesa Visualizza, seleziona un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire il nome e i tag per il gruppo di risorse. È possibile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



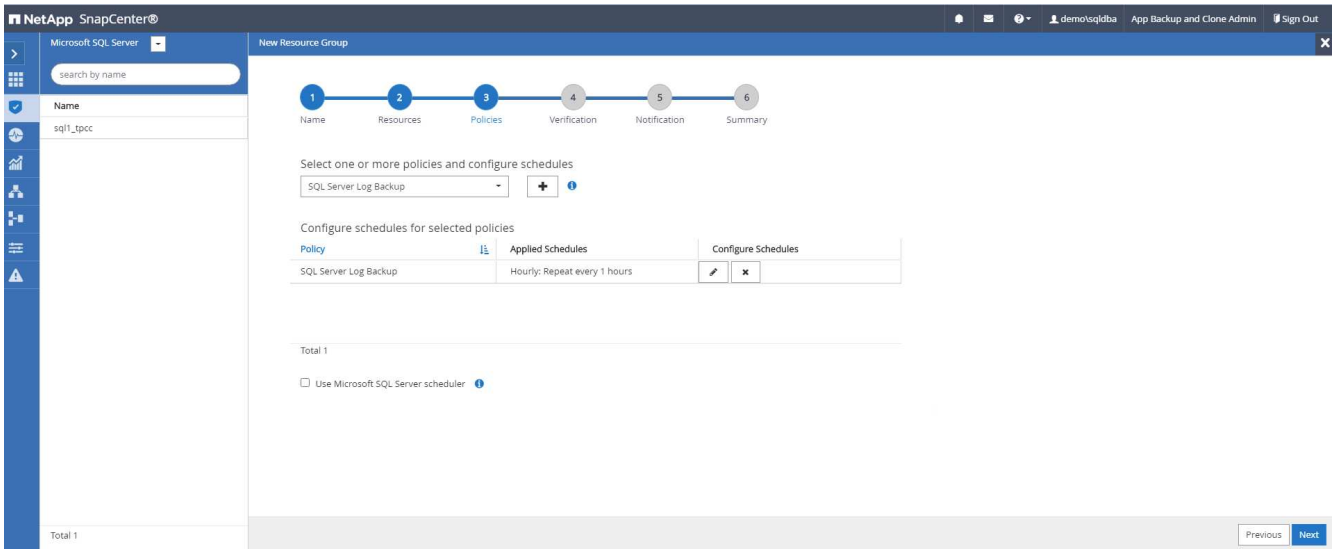
2. Selezionare le risorse del database di cui eseguire il backup.



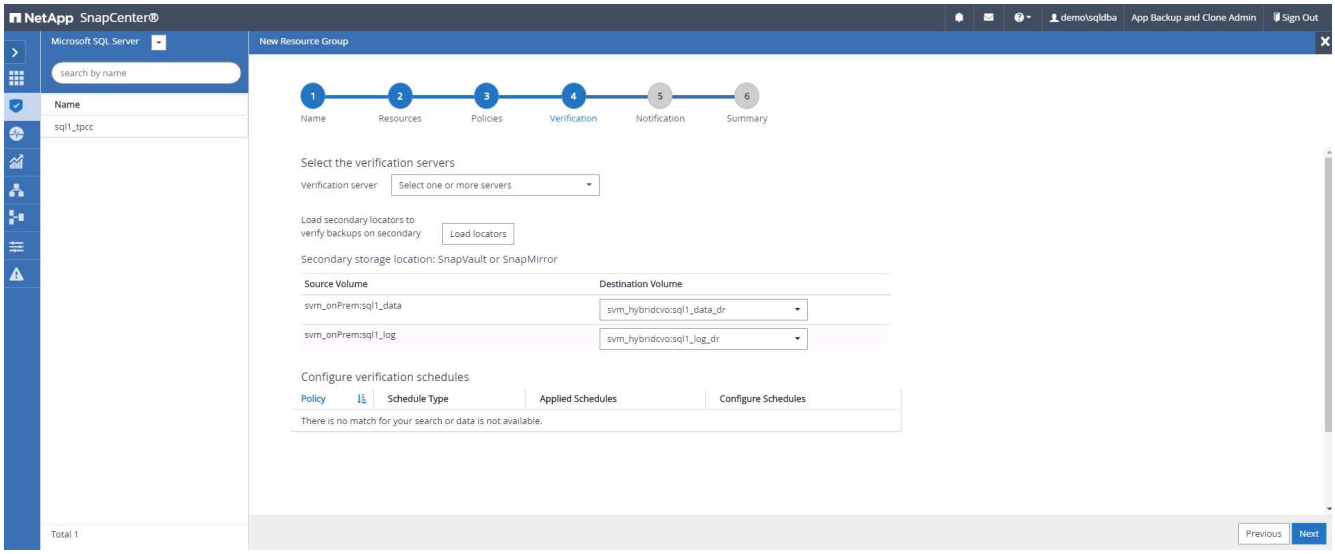
3. Selezionare un criterio di backup del log SQL creato nella sezione 7.



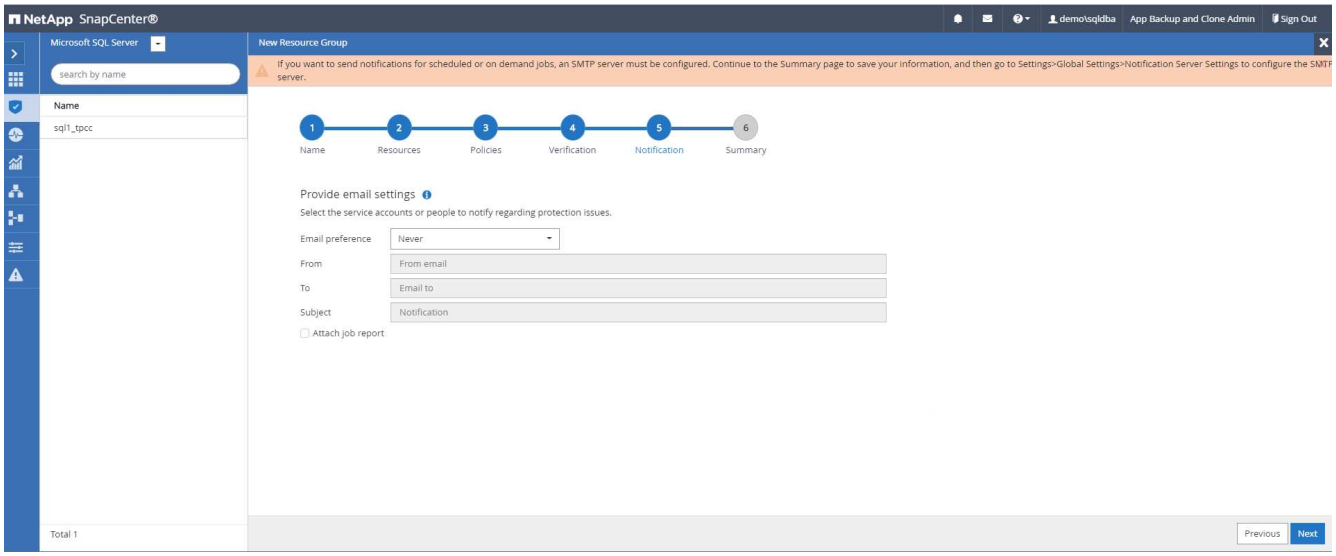
4. Aggiungere l'orario esatto per il backup e la frequenza.



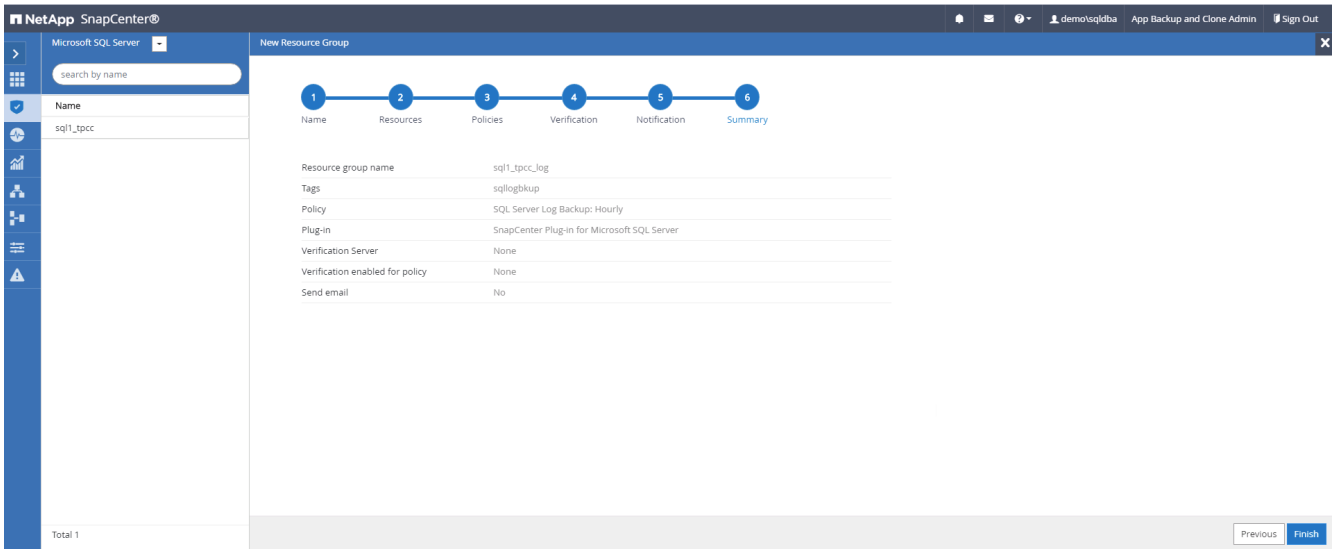
5. Selezionare il server di verifica per il backup secondario se si desidera eseguire la verifica del backup. Fare clic su Load Locator per popolare la posizione di archiviazione secondaria.



6. Se lo si desidera, configurare il server SMTP per la notifica via e-mail.



7. Riepilogo.

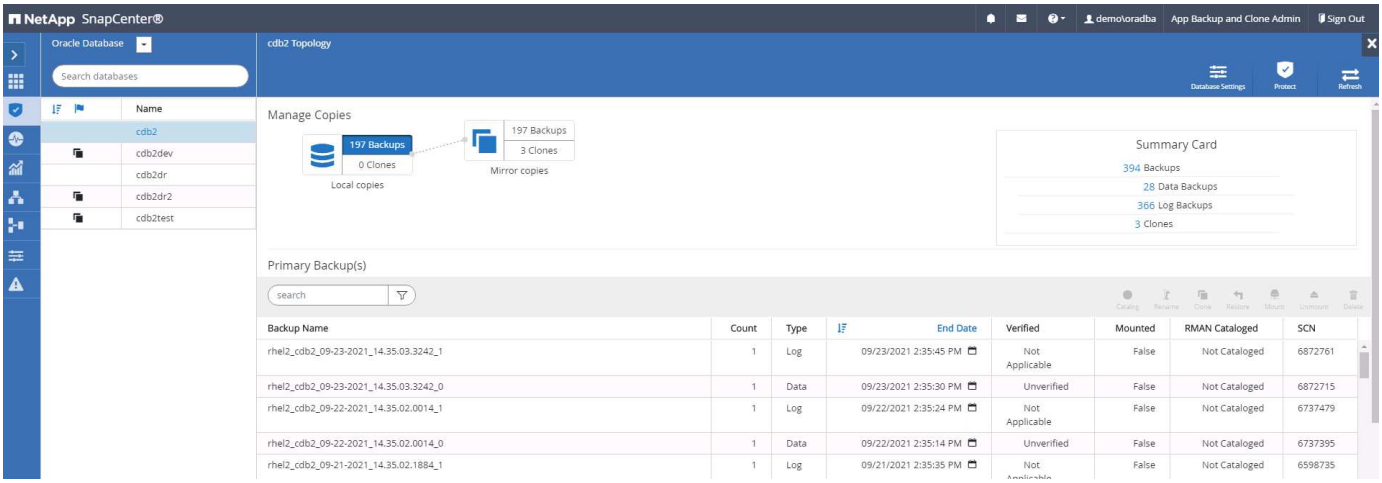


9. Convalida il backup

Dopo aver creato 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.

Vai alla scheda Risorse, fai clic sul nome del database per visualizzare i dettagli del backup del database e alterna tra copie locali e copie mirror per verificare che i backup snapshot vengano 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 ripristino di emergenza in caso di un errore primario.

Introduzione al cloud pubblico AWS

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

Cloud pubblico AWS

Per semplificare la comprensione, abbiamo creato questo documento basandoci su una distribuzione in AWS. Tuttavia, il processo è molto simile per Azure e GCP.

1. Controllo pre-volo

Prima della distribuzione, accertarsi che l'infrastruttura sia pronta per consentire la distribuzione nella fase successiva. Ciò include quanto segue:

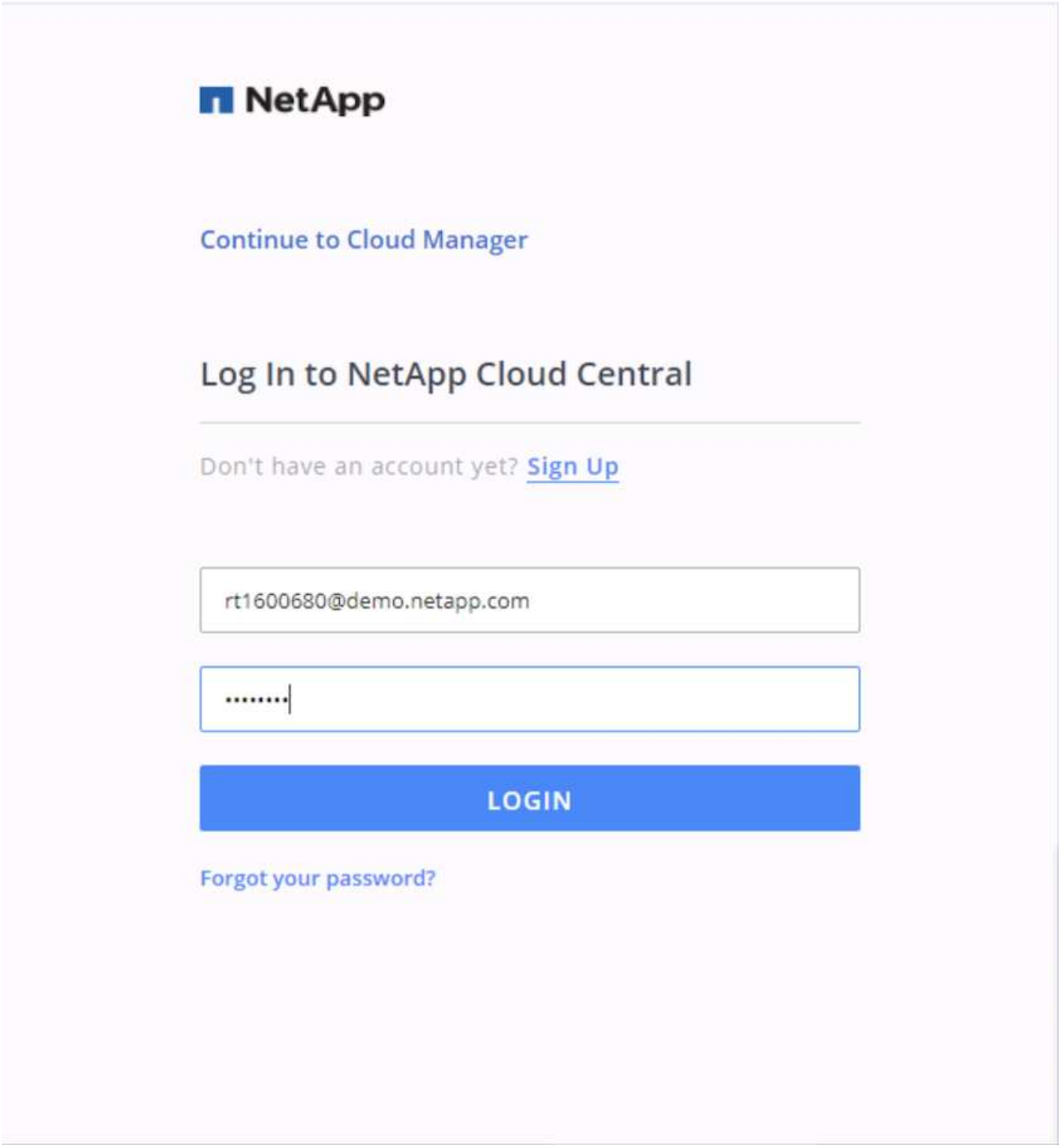
- Account AWS
- VPC nella regione di tua scelta
- Subnet con accesso a Internet pubblico
- Autorizzazioni per aggiungere ruoli IAM al tuo account AWS
- Una chiave segreta e una chiave di accesso per il tuo utente AWS

2. Passaggi per distribuire Cloud Manager e Cloud Volumes ONTAP in AWS

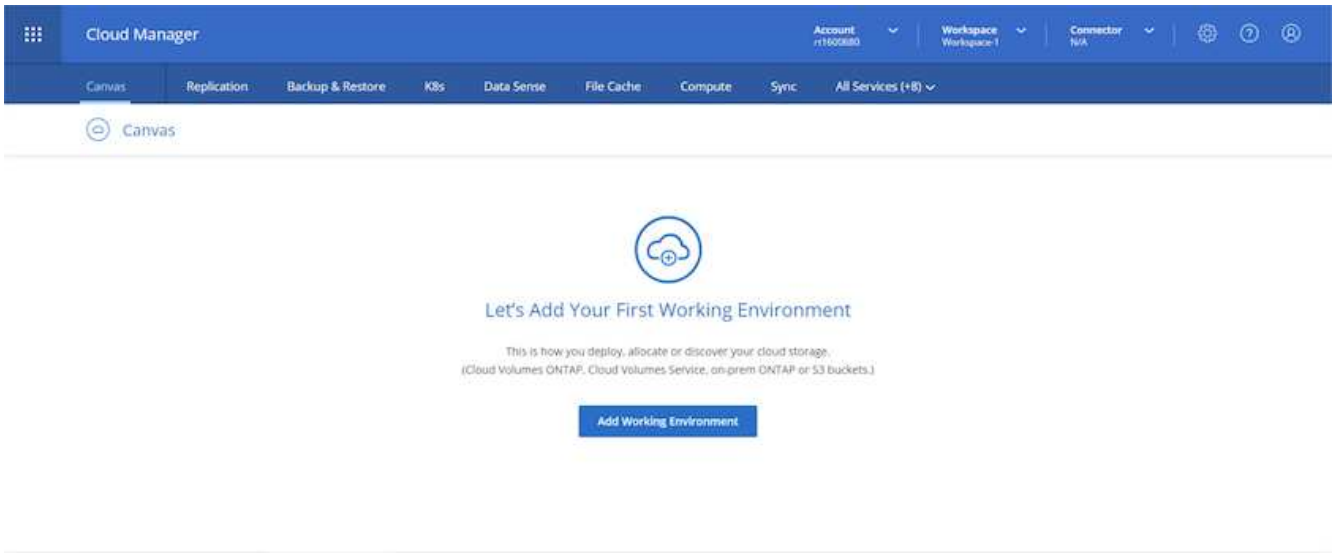
Esistono molti metodi per distribuire Cloud Manager e Cloud Volumes ONTAP; questo metodo è il più semplice, ma richiede la maggior parte delle autorizzazioni. Se questo metodo non è appropriato per il tuo ambiente AWS, consulta il "Documentazione NetApp Cloud" .

Distribuisci il connettore Cloud Manager

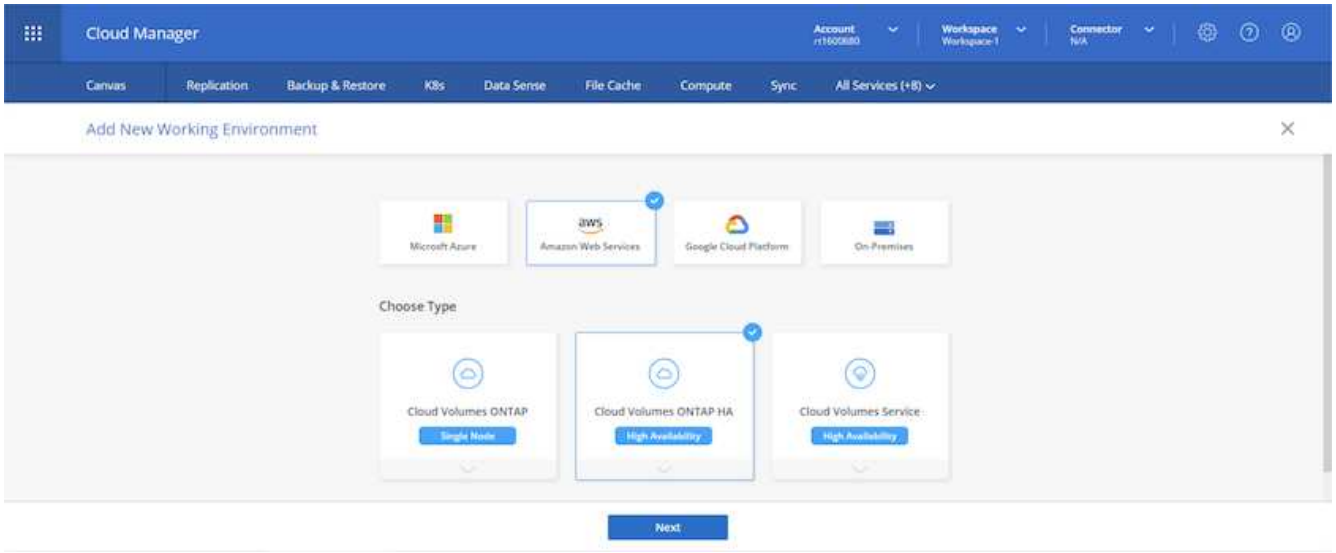
1. Vai a "NetApp BlueXP" e accedi o registrati.



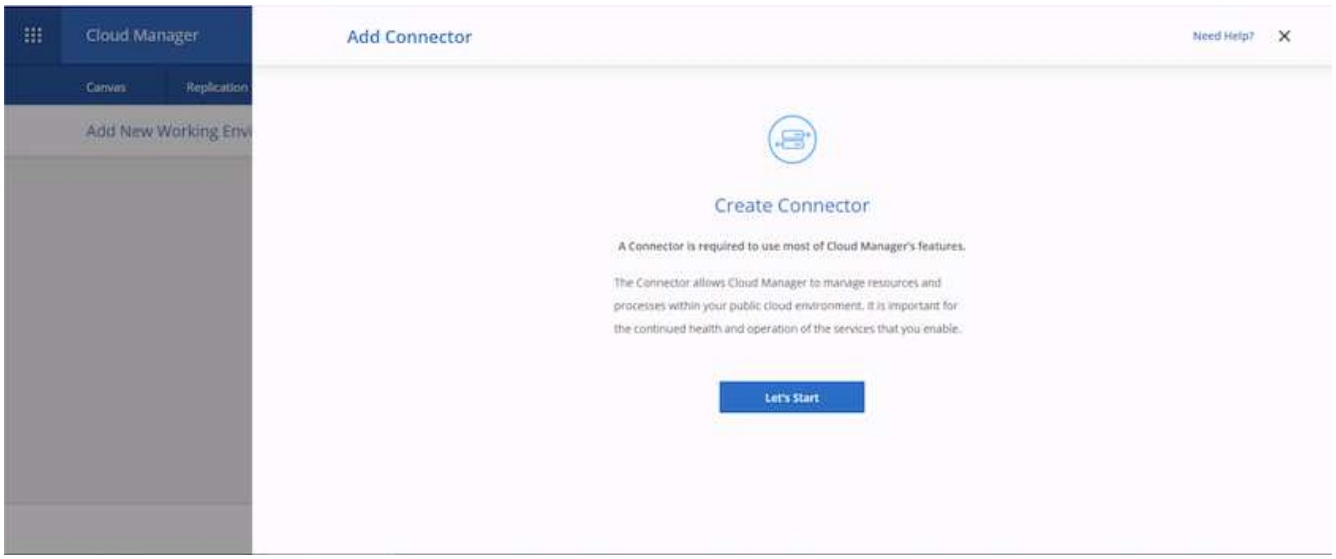
2. Dopo aver effettuato l'accesso, dovresti essere indirizzato a Canvas.



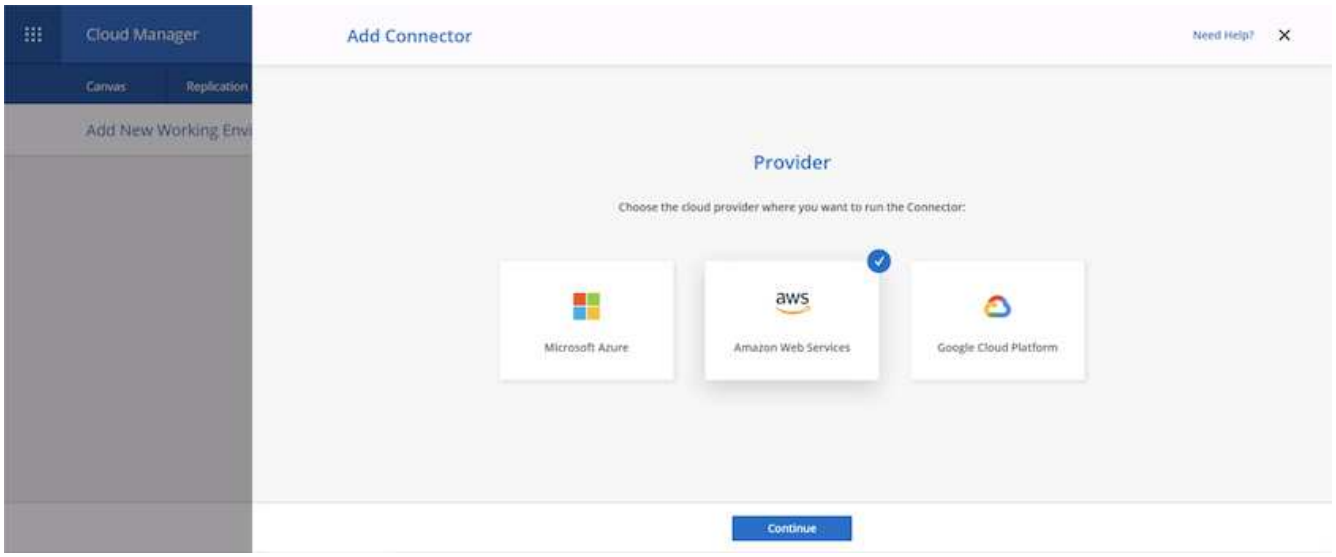
3. Fare clic su "Aggiungi ambiente di lavoro" e scegliere Cloud Volumes ONTAP in AWS. Qui puoi anche scegliere se vuoi distribuire un sistema a nodo singolo o una coppia ad alta disponibilità. Ho scelto di implementare una coppia ad alta disponibilità.



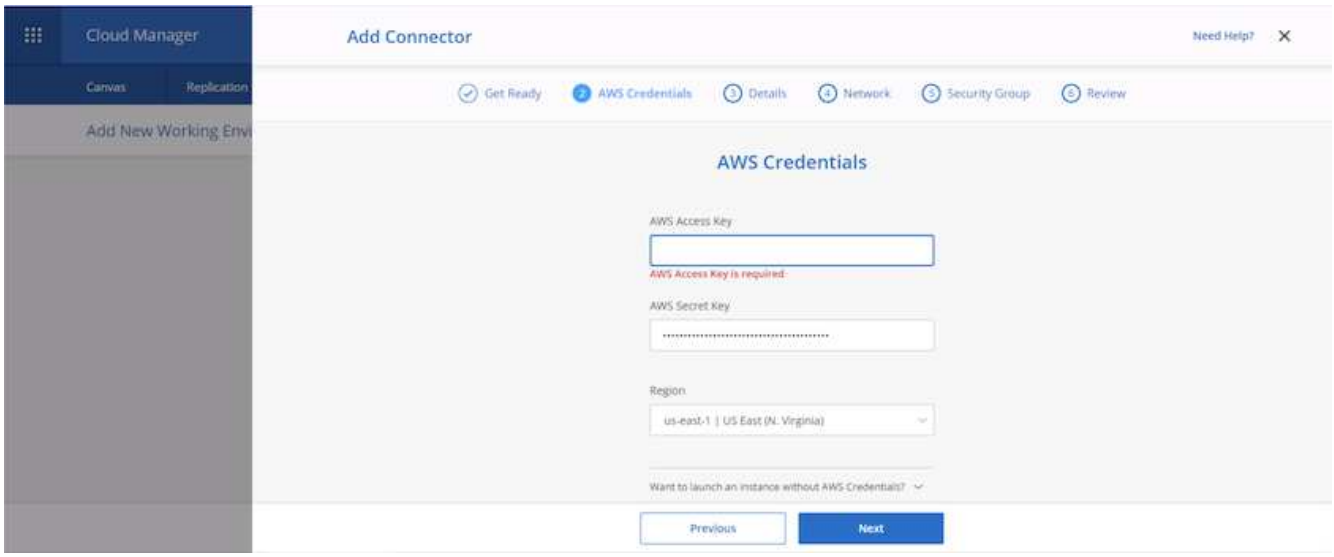
4. Se non è stato creato alcun connettore, viene visualizzato un pop-up che chiede di crearne uno.



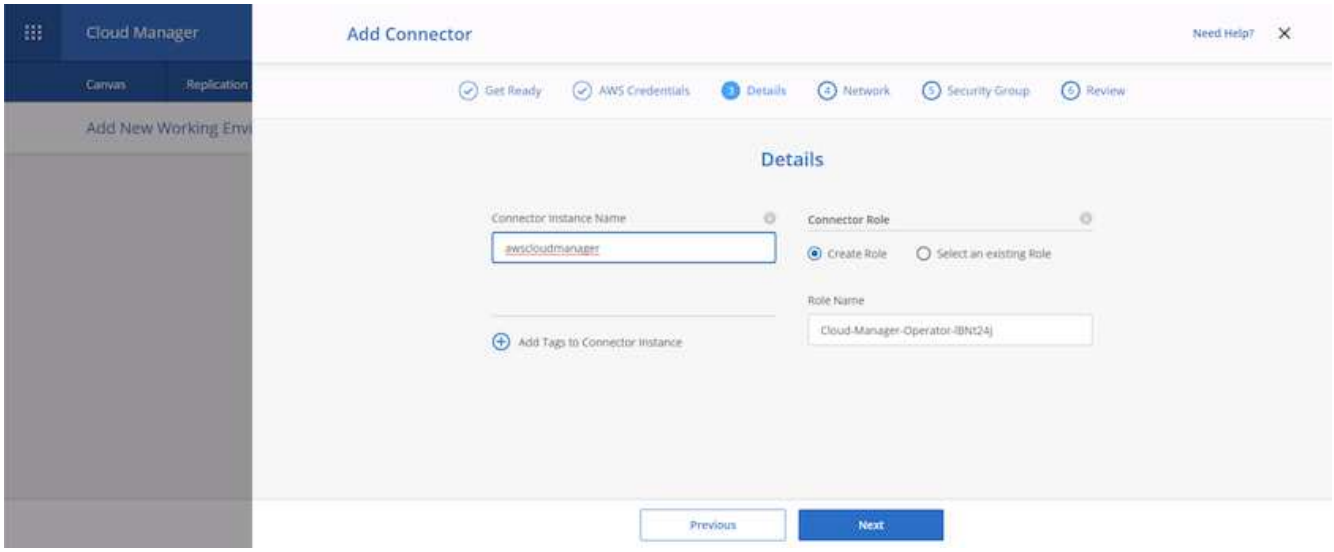
5. Fare clic su Iniziamo, quindi scegliere AWS.



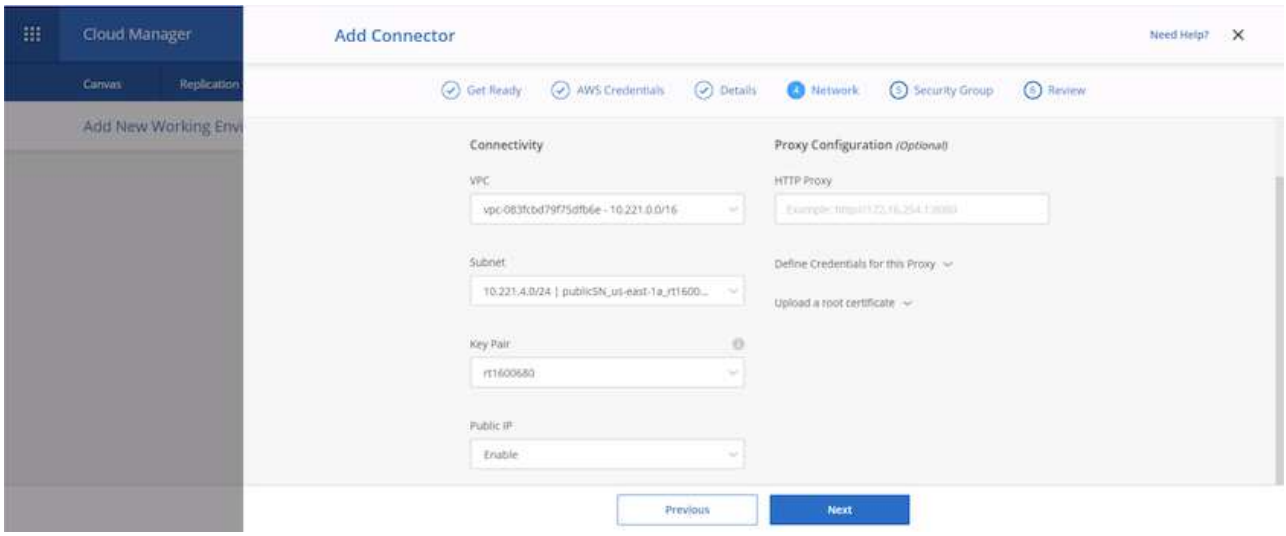
6. Inserisci la tua chiave segreta e la chiave di accesso. Assicurati che il tuo utente abbia le autorizzazioni corrette descritte in "Pagina delle policy NetApp" .



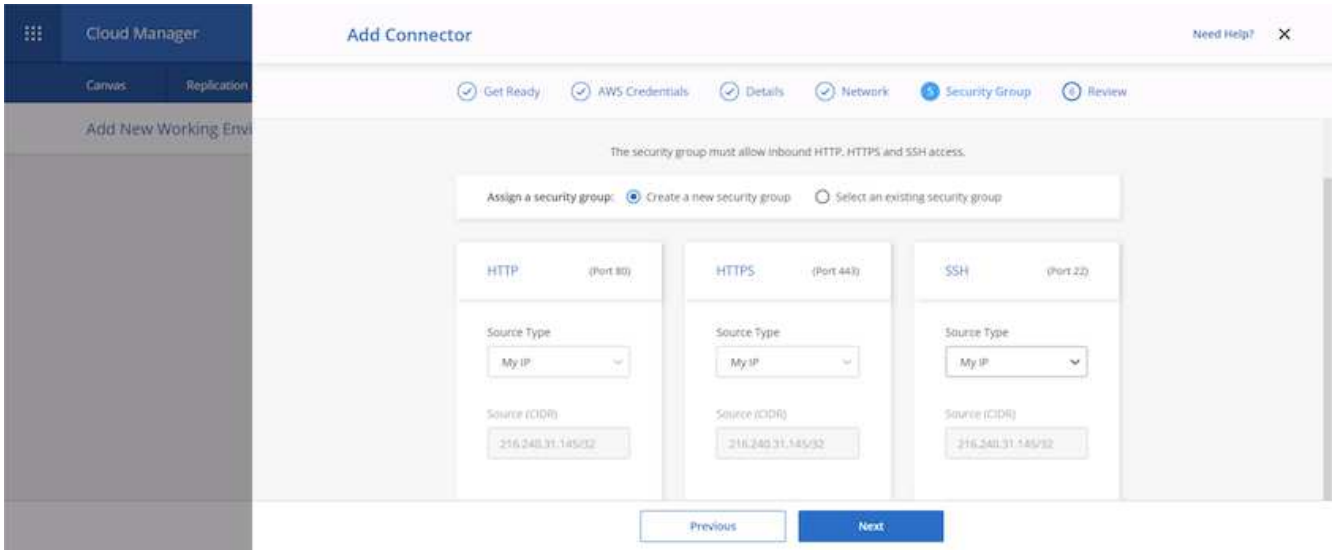
7. Assegna un nome al connettore e utilizza un ruolo predefinito come descritto nel "Pagina delle policy NetApp" oppure chiedi a Cloud Manager di creare il ruolo per te.



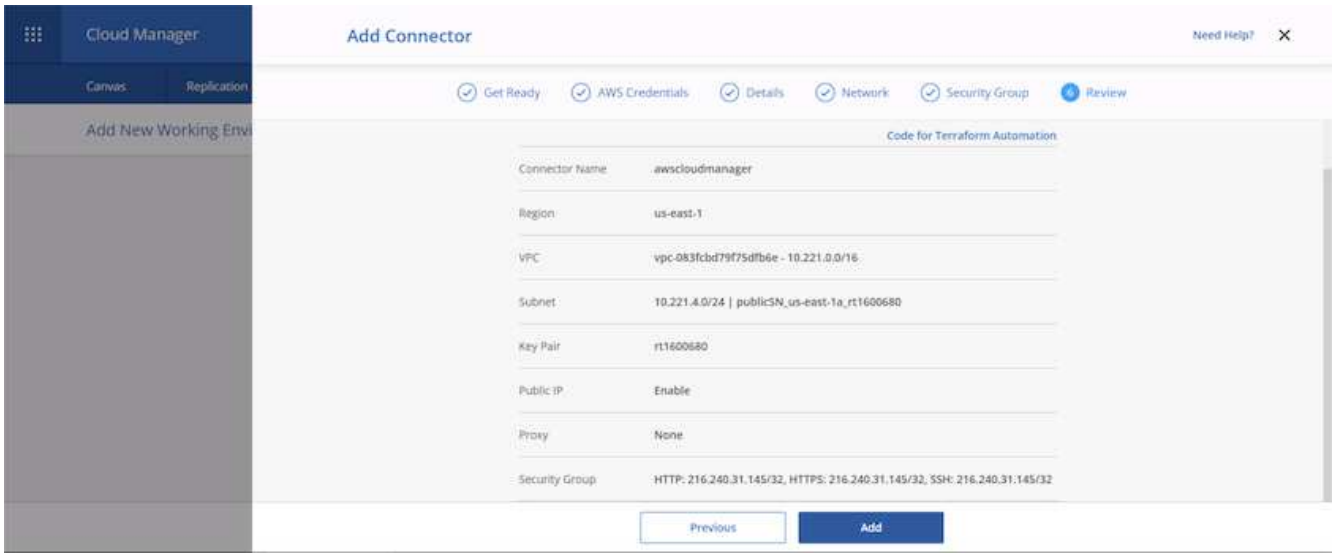
8. Fornire le informazioni di rete necessarie per distribuire il connettore. Verificare che l'accesso a Internet in uscita sia abilitato:
   a. Assegnare al connettore un indirizzo IP pubblico
   b. Fornire al connettore un proxy attraverso cui lavorare
   c. Fornire al connettore un percorso verso Internet pubblico tramite un gateway Internet



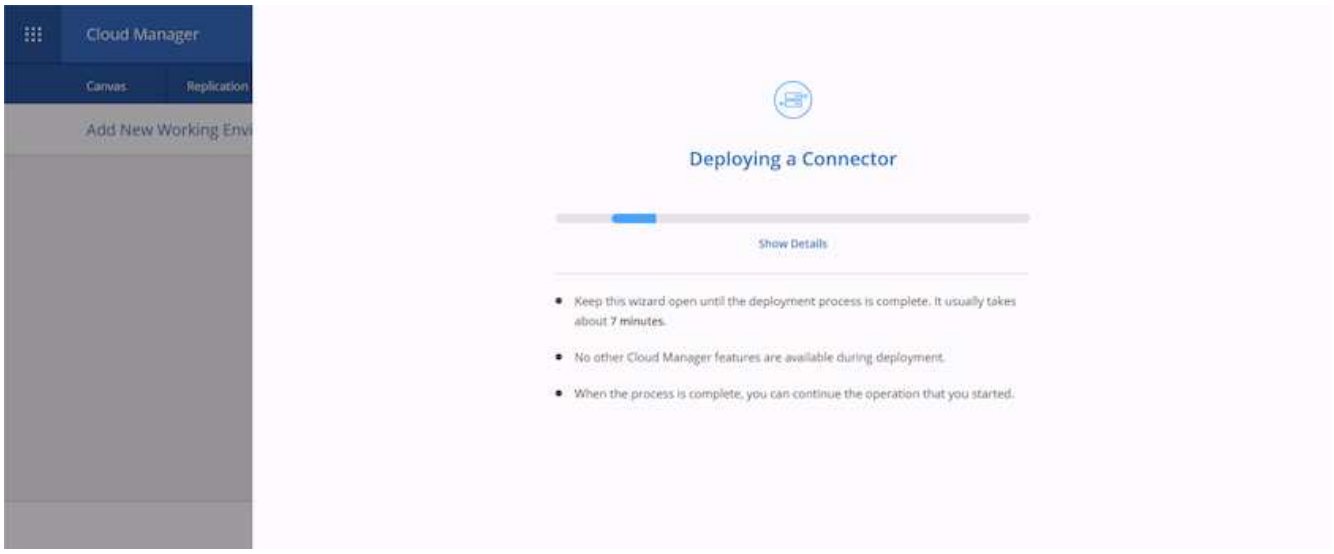
9. Fornire la comunicazione con il connettore tramite SSH, HTTP e HTTPs fornendo un gruppo di sicurezza o creandone uno nuovo. Ho abilitato l'accesso al connettore solo dal mio indirizzo IP.



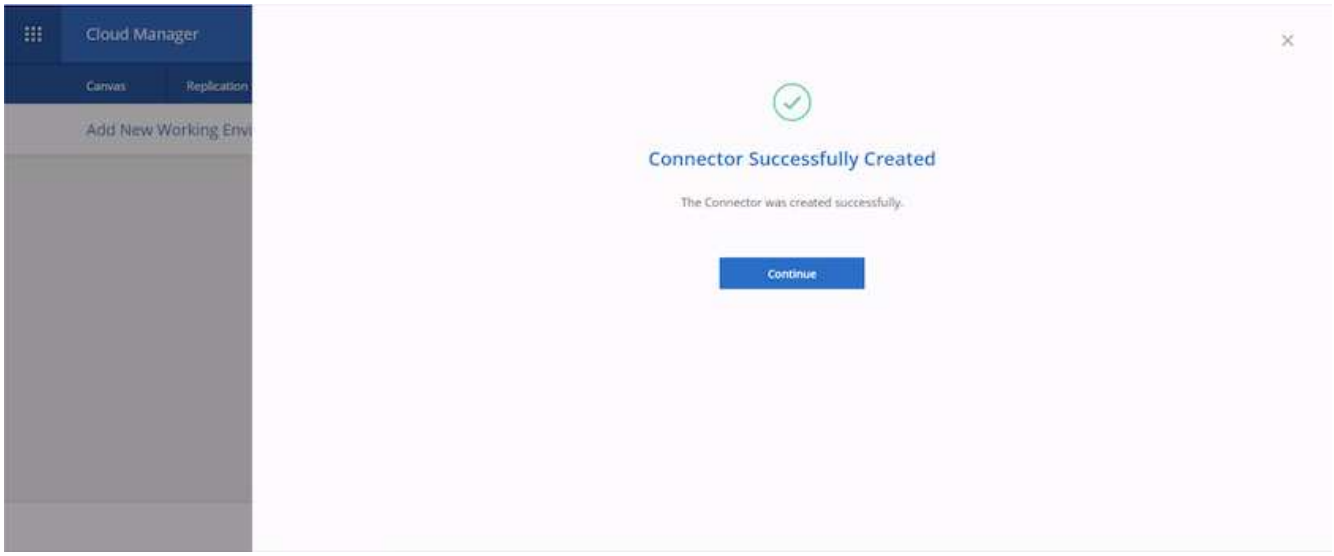
10. Esaminare le informazioni nella pagina di riepilogo e fare clic su Aggiungi per distribuire il connettore.



11. Il connettore ora viene distribuito utilizzando uno stack di formazione cloud. È possibile monitorarne l'avanzamento tramite Cloud Manager o AWS.

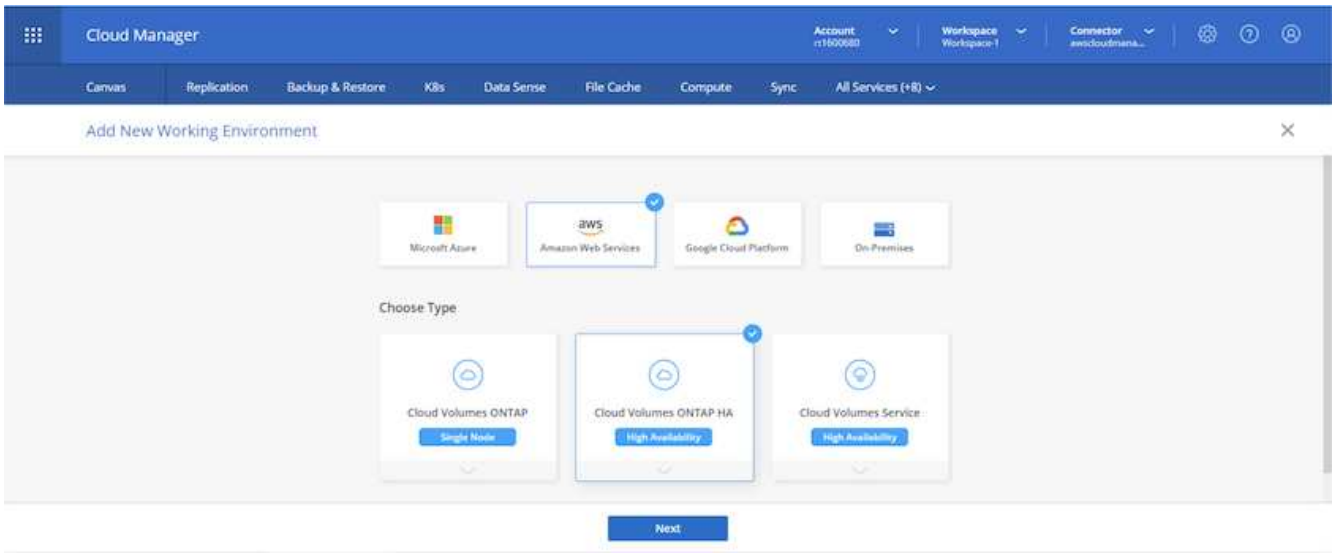


12. Una volta completata la distribuzione, verrà visualizzata una pagina di conferma.

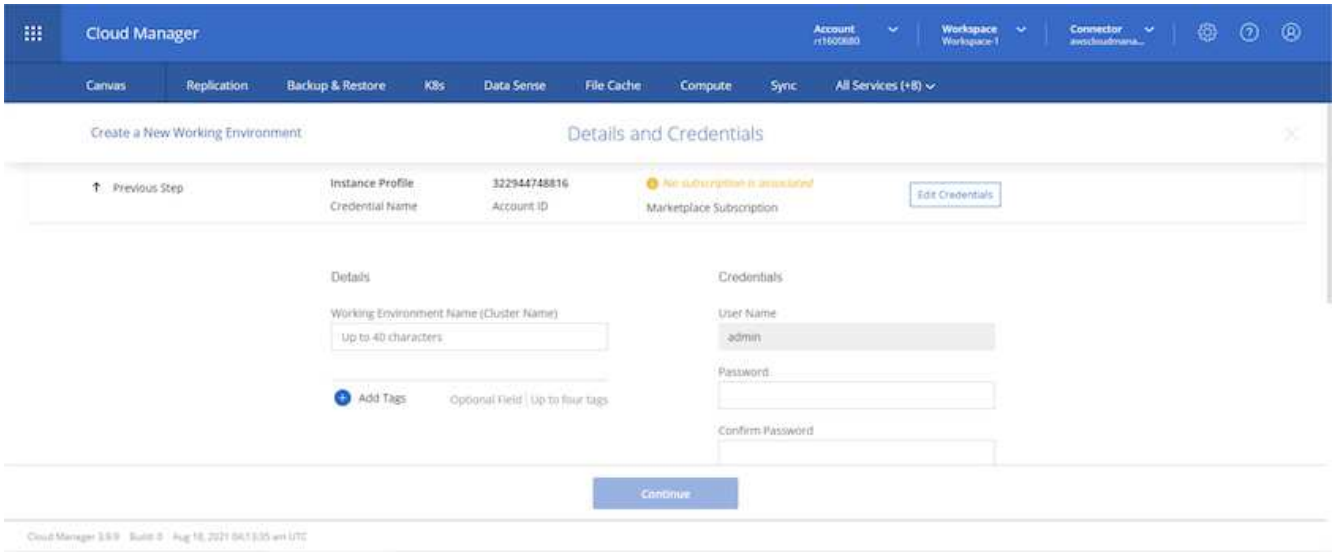


Distribuisci Cloud Volumes ONTAP

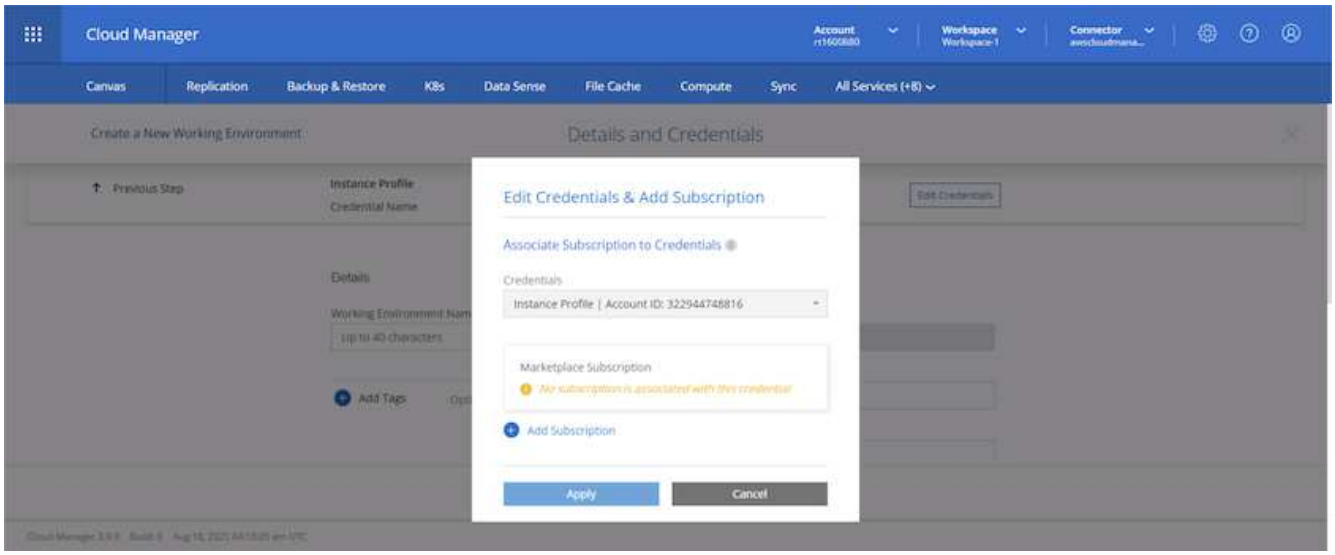
1. Seleziona AWS e il tipo di distribuzione in base alle tue esigenze.



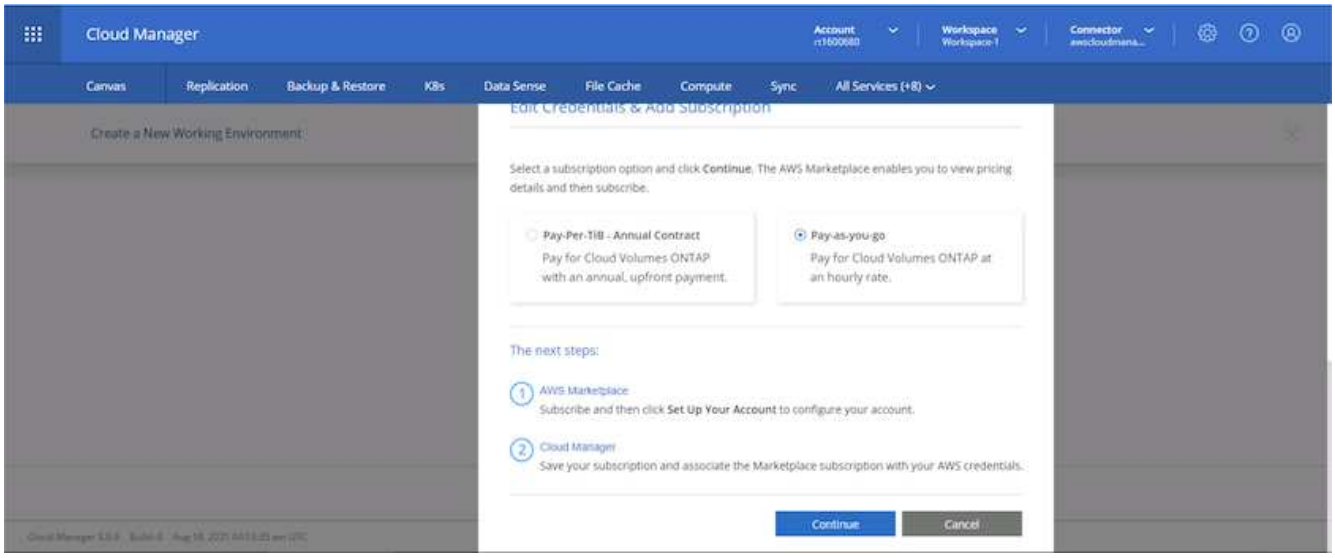
2. Se non è stato assegnato alcun abbonamento e si desidera acquistare con PAYGO, selezionare Modifica credenziali.



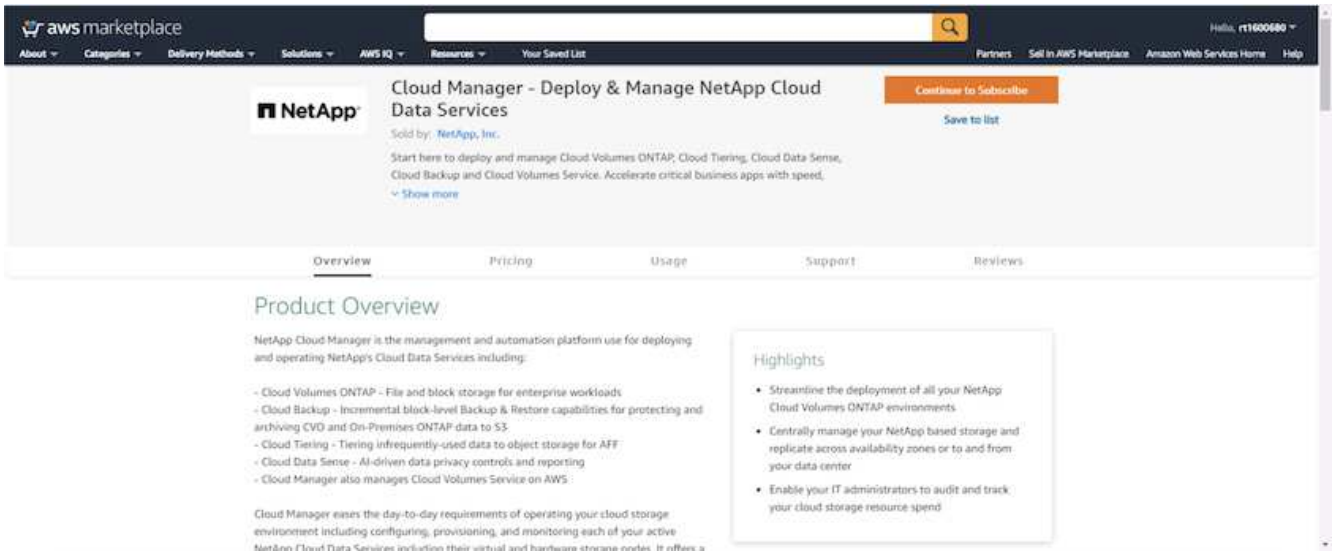
3. Seleziona Aggiungi abbonamento.



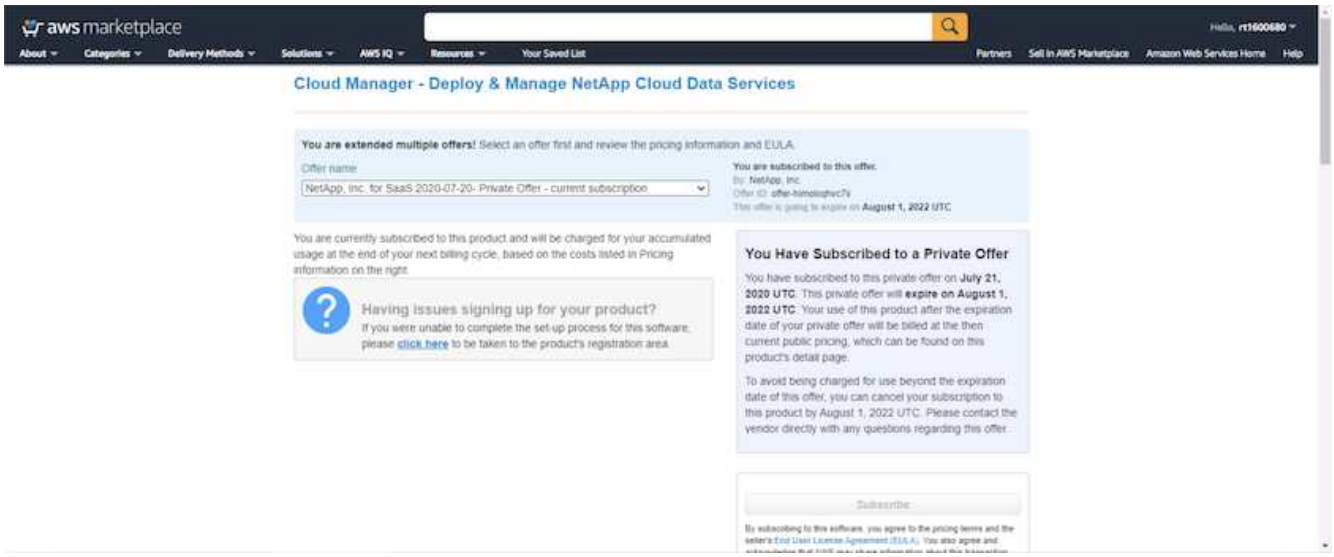
4. Scegli il tipo di contratto che desideri sottoscrivere. Ho scelto il pagamento a consumo.



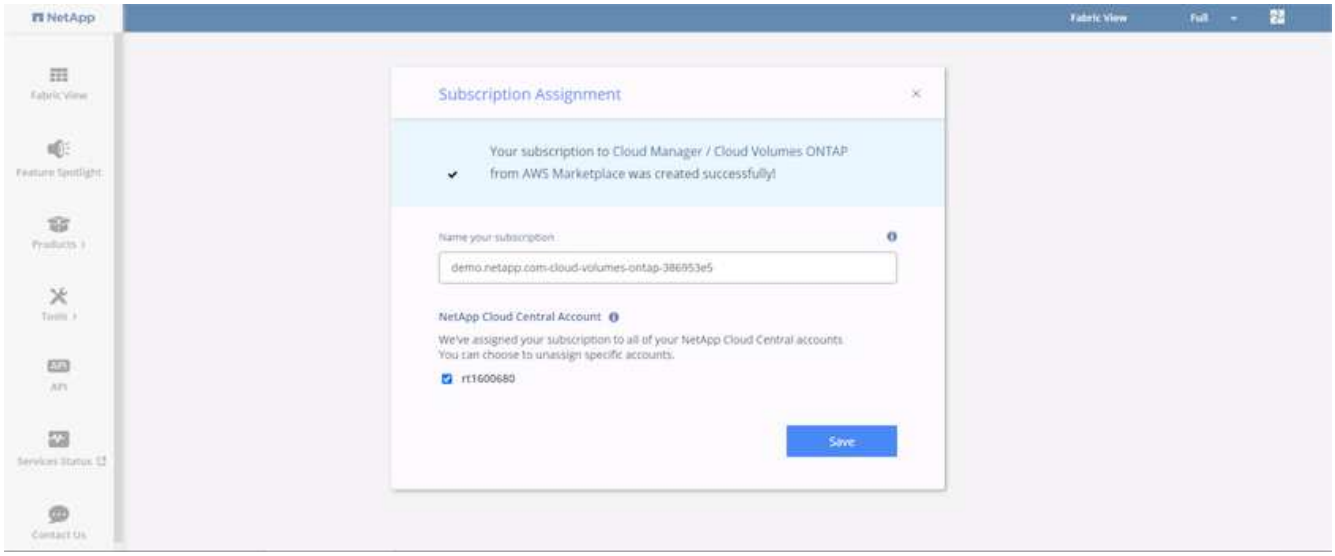
5. Verrai reindirizzato ad AWS; seleziona Continua per iscriverti.



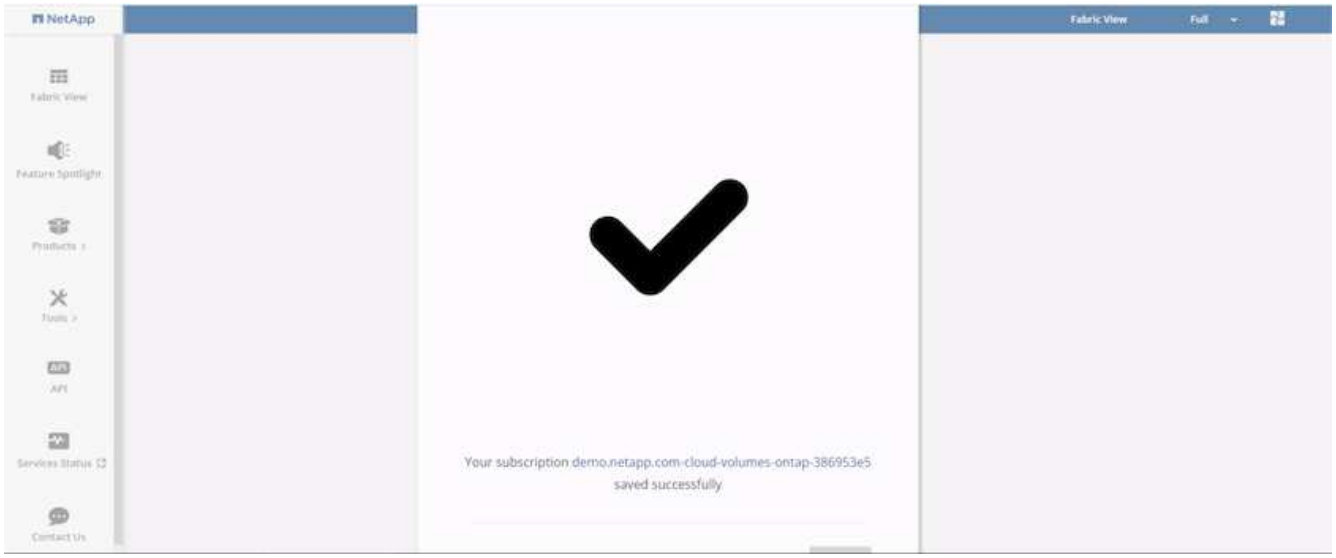
6. Iscriviti e verrai reindirizzato a NetApp Cloud Central. Se ti sei già iscritto e non vieni reindirizzato, seleziona il link "Clicca qui".



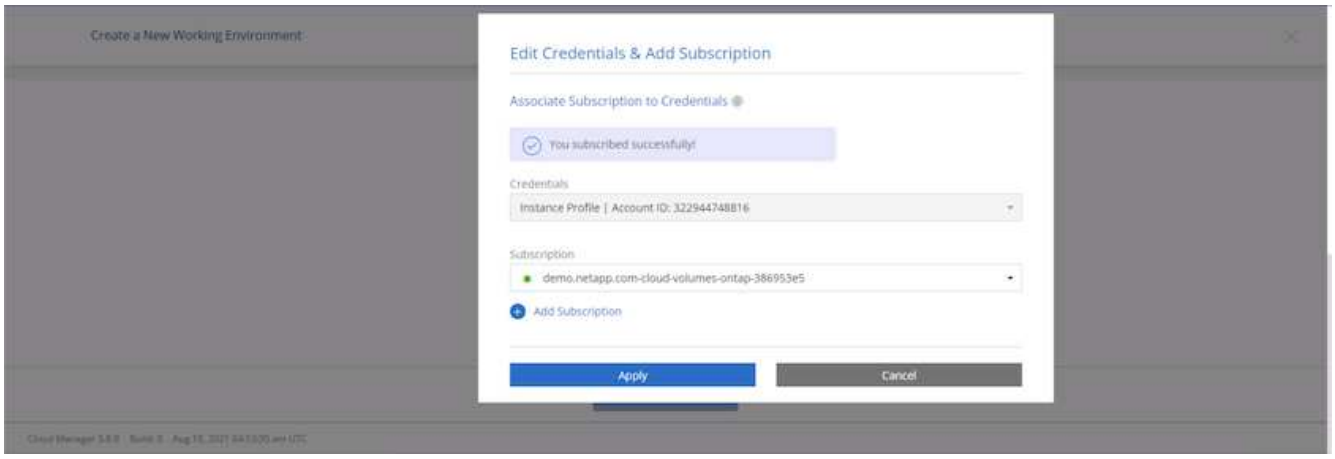
7. Verrai reindirizzato a Cloud Central, dove dovrai assegnare un nome al tuo abbonamento e assegnarlo al tuo account Cloud Central.



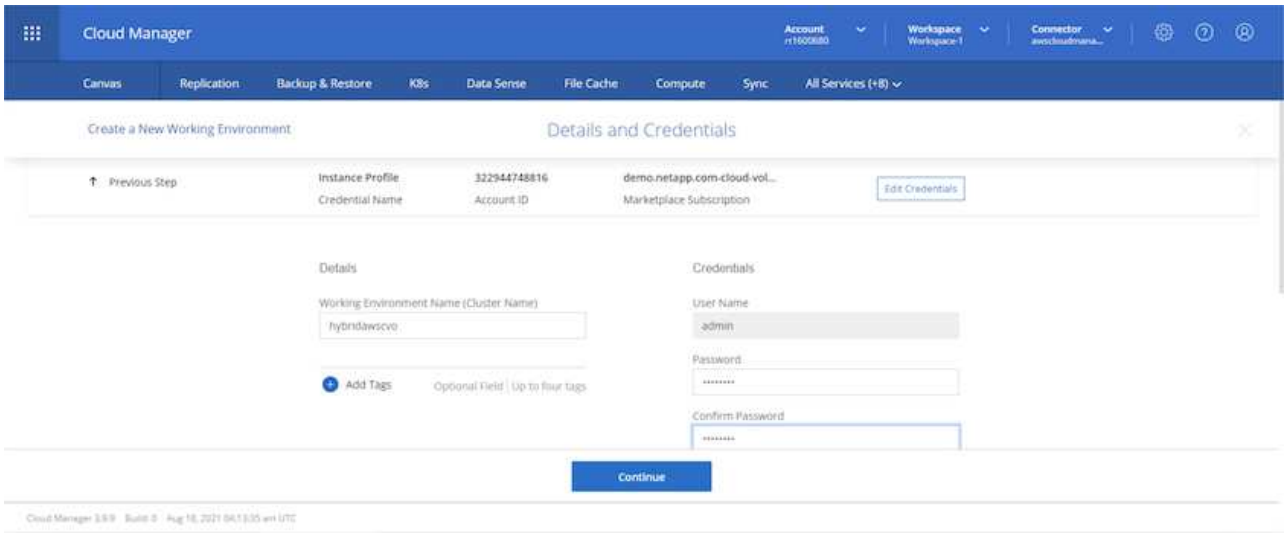
8. Se l'operazione riesce, viene visualizzata una pagina con un segno di spunta. Torna alla scheda Cloud Manager.



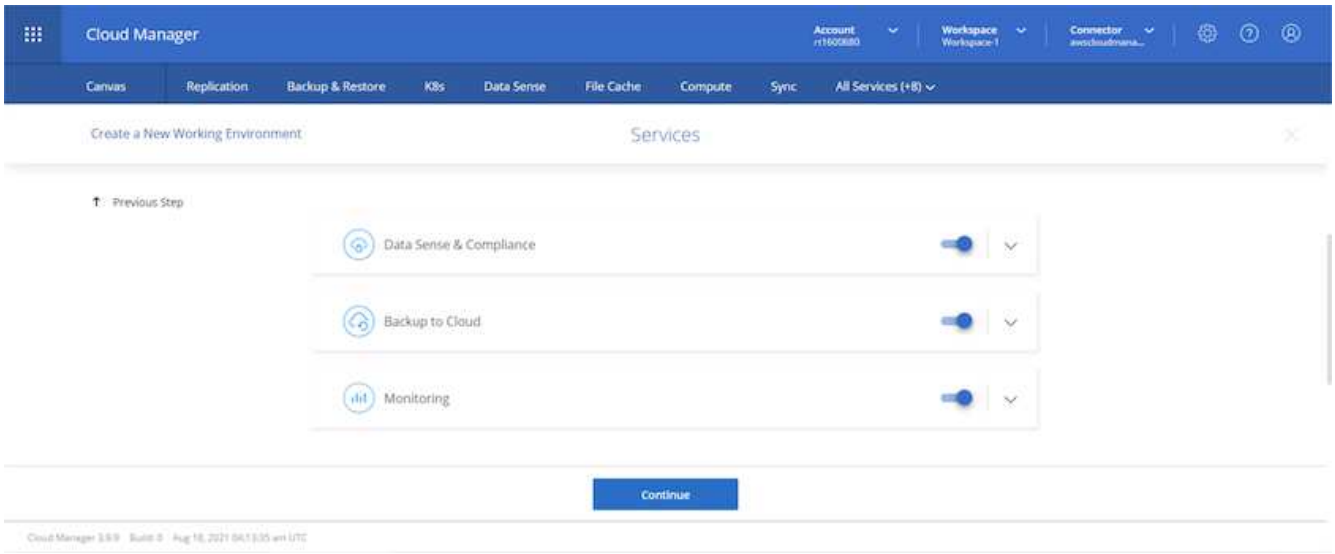
9. L’abbonamento ora appare in Cloud Central. Fare clic su Applica per continuare.



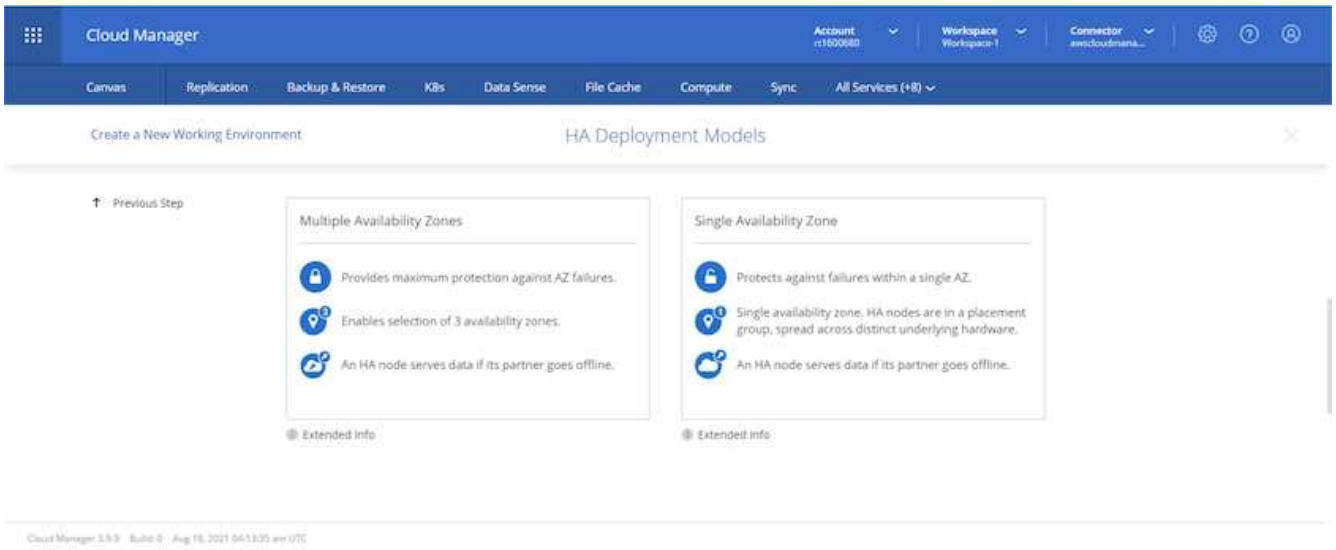
10. Inserisci i dettagli dell’ambiente di lavoro, ad esempio:
    a. Nome del cluster
    b. Password del cluster
    c. Tag AWS (facoltativo)



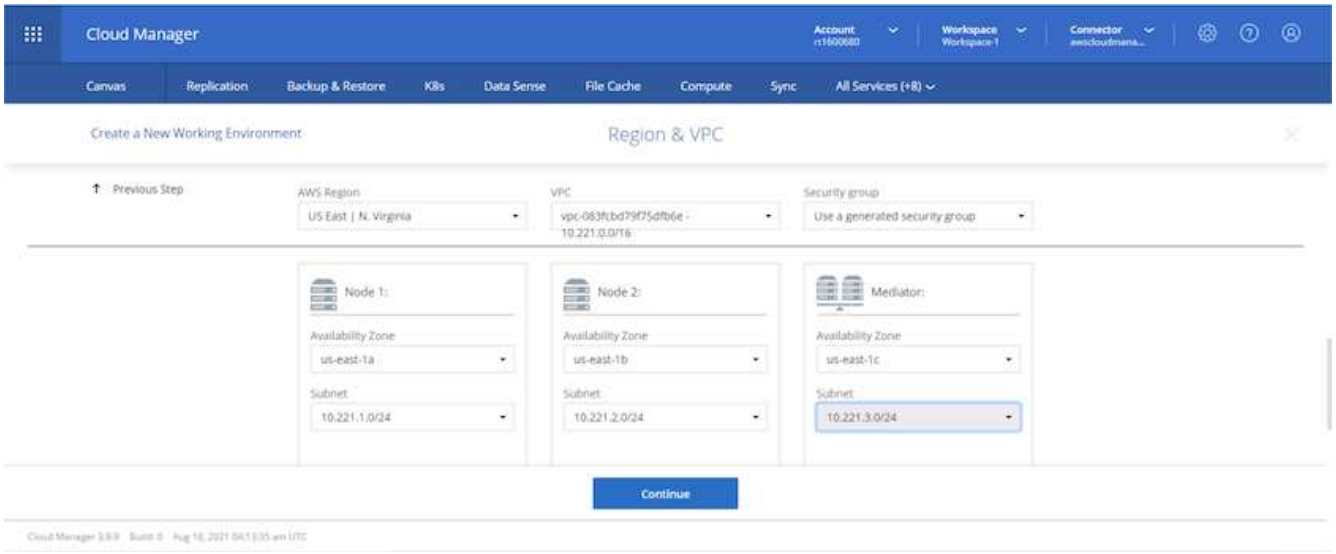
11. Scegli quali servizi aggiuntivi desideri implementare. Per scoprire di più su questi servizi, visita il "BlueXP: le moderne operazioni di gestione dei dati semplificate" .



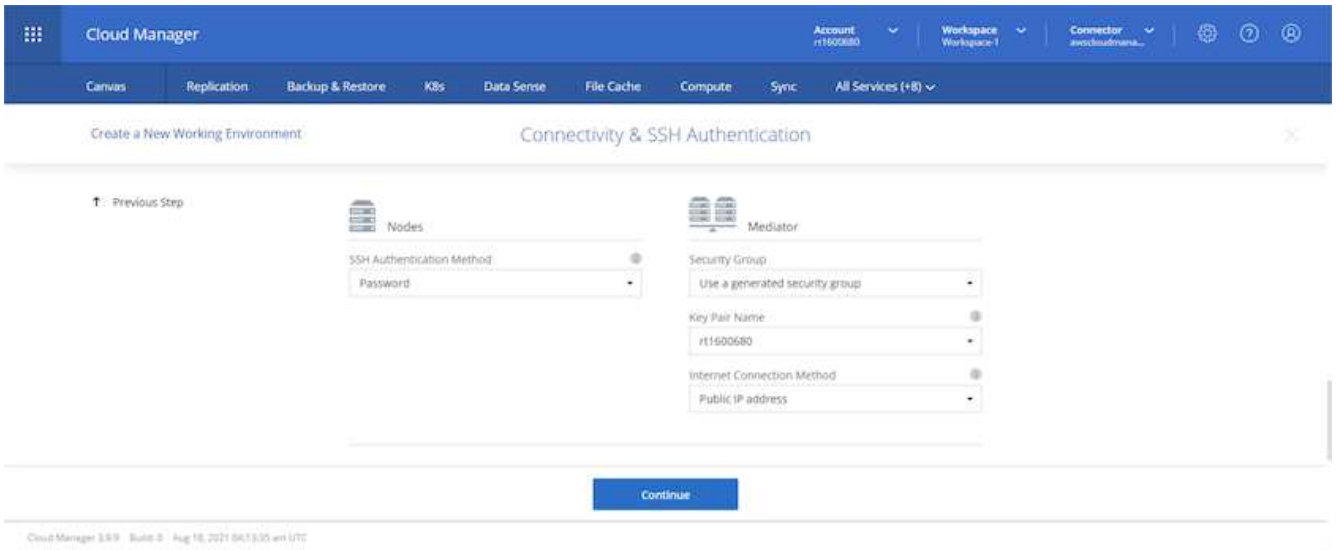
12. Scegliere se eseguire la distribuzione in più zone di disponibilità (sono necessarie tre subnet, ciascuna in una AZ diversa) o in una singola zona di disponibilità. Ho scelto più AZ.



13. Selezionare la regione, la VPC e il gruppo di sicurezza in cui verrà distribuito il cluster. In questa sezione si assegnano anche le zone di disponibilità per nodo (e mediatore), nonché le subnet che occupano.

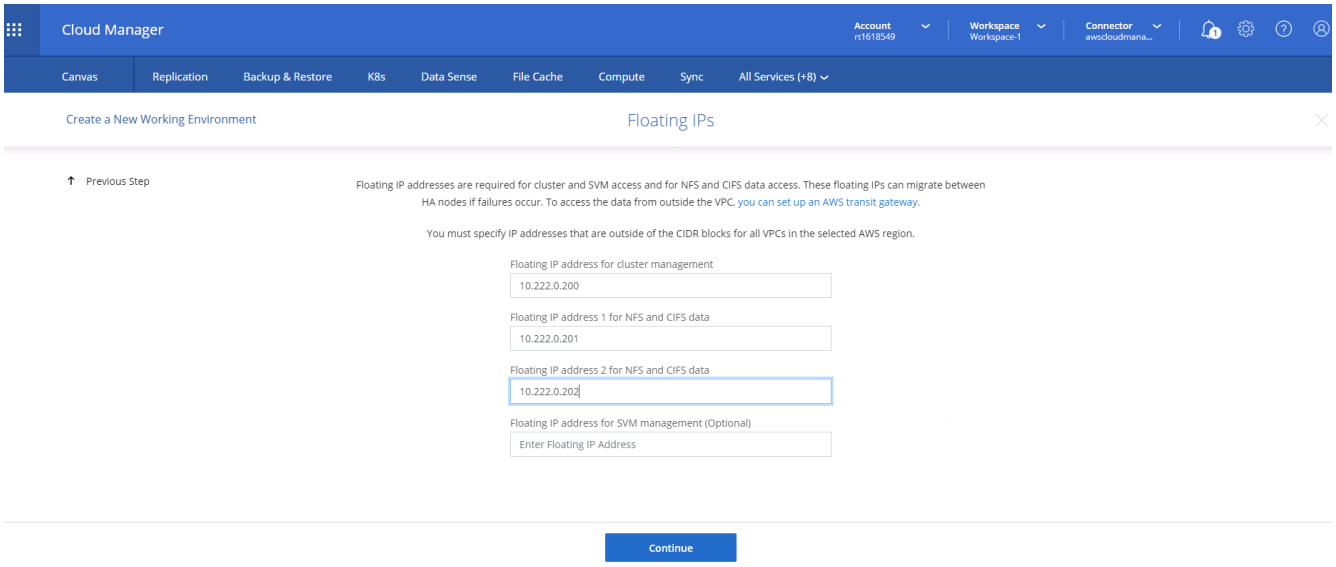


14. Scegliere i metodi di connessione per i nodi e per il mediatore.

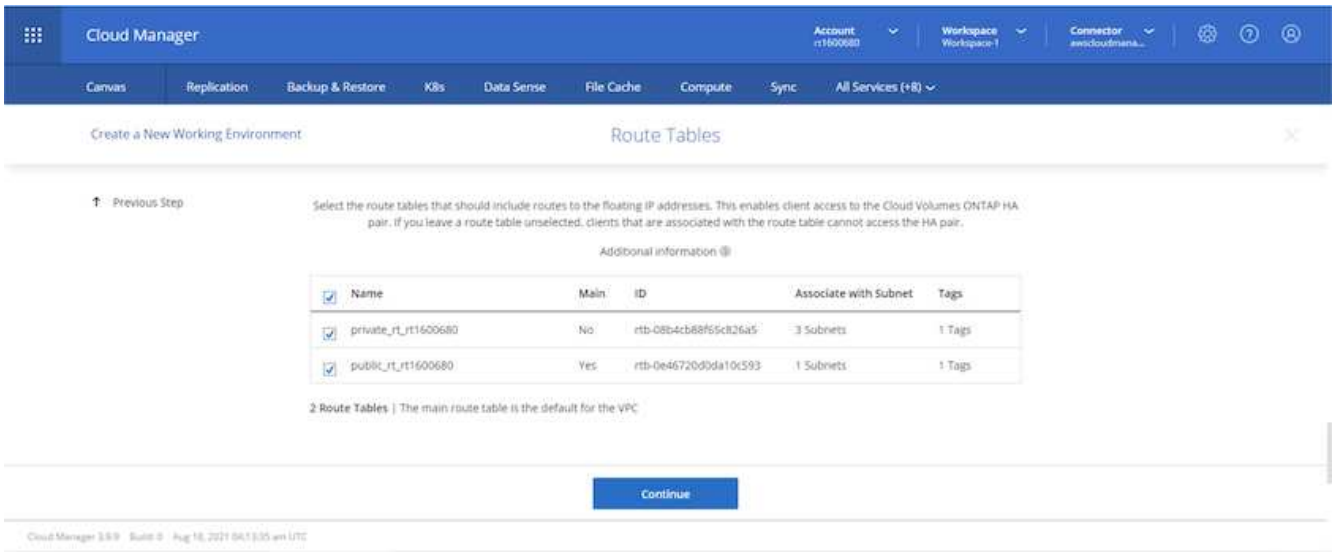


Il mediatore richiede la comunicazione con le API AWS. Non è necessario un indirizzo IP pubblico, purché le API siano raggiungibili dopo la distribuzione dell'istanza EC2 del mediatore.

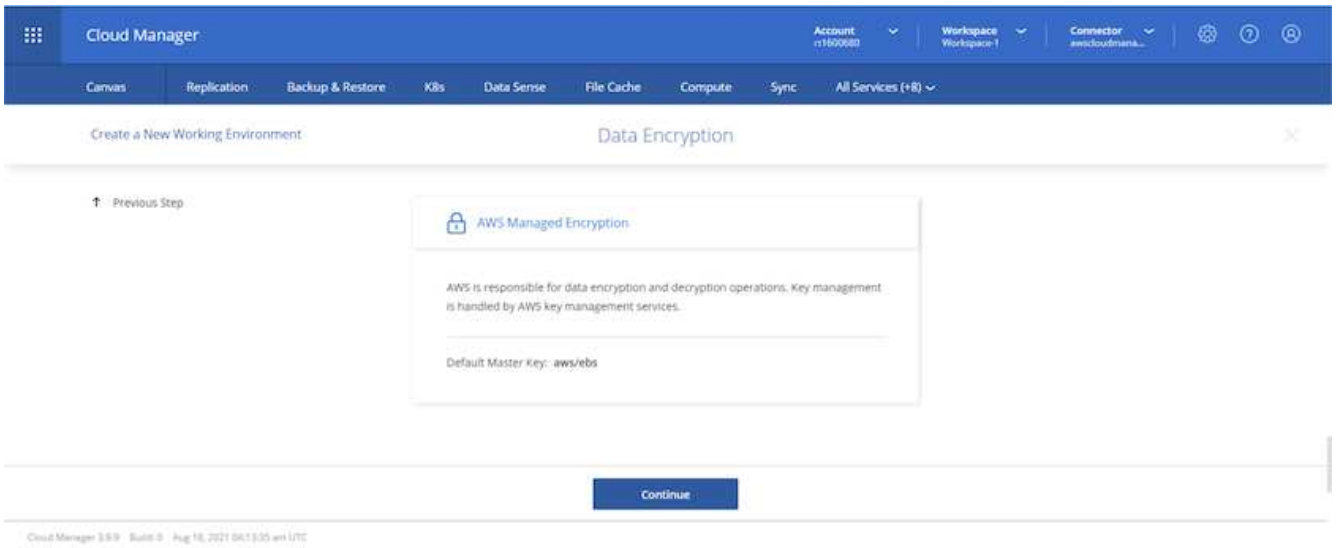
1. Gli indirizzi IP flottanti vengono utilizzati per consentire l'accesso ai vari indirizzi IP utilizzati da Cloud Volumes ONTAP , inclusi gli IP di gestione dei cluster e di fornitura dei dati. Devono essere indirizzi che non sono già instradabili all'interno della rete e che vengono aggiunti alle tabelle di routing nel tuo ambiente AWS. Sono necessari per abilitare indirizzi IP coerenti per una coppia HA durante il failover. Ulteriori informazioni sugli indirizzi IP flottanti possono essere trovate in "Documentazione NetApp Cloud" .



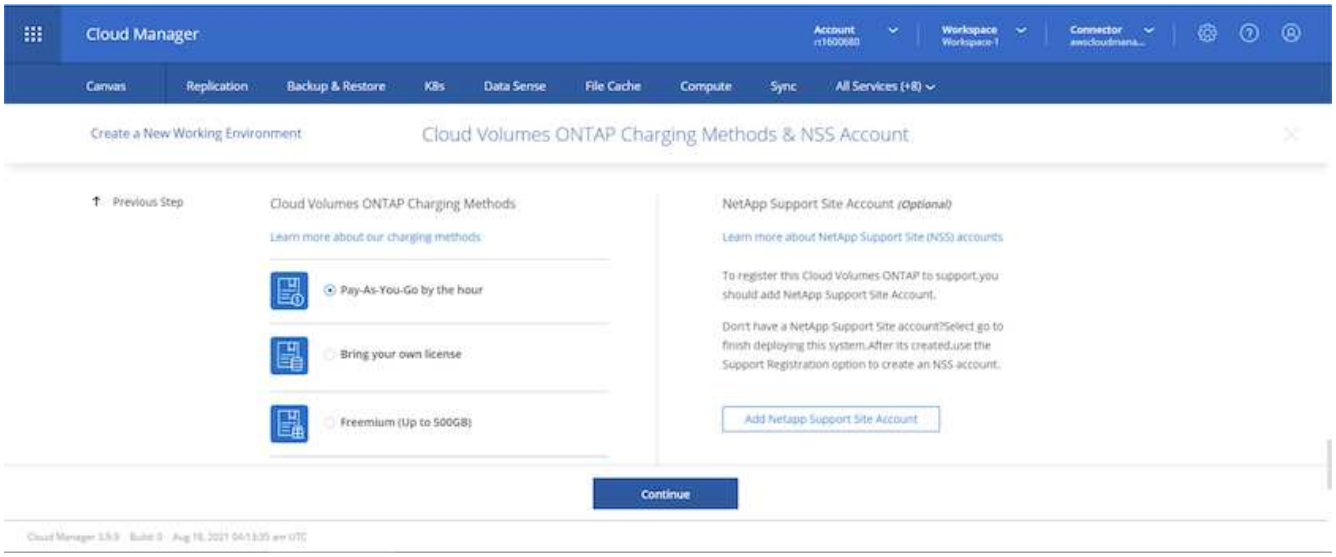
2. Selezionare a quali tabelle di routing aggiungere gli indirizzi IP mobili. Queste tabelle di routing vengono utilizzate dai client per comunicare con Cloud Volumes ONTAP.



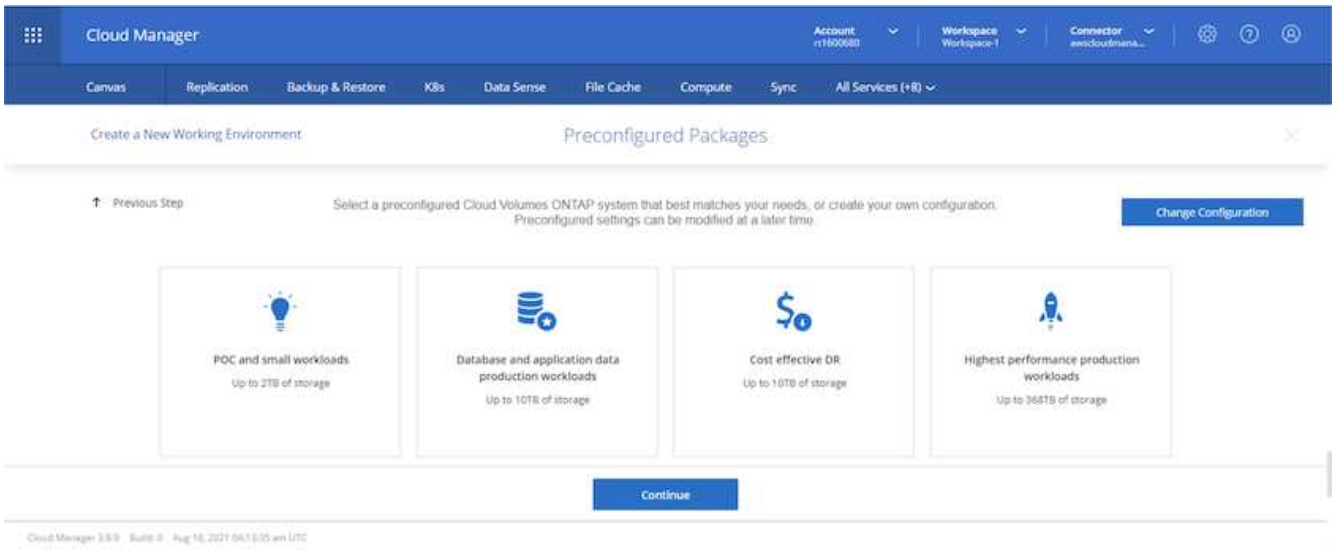
3. Scegliere se abilitare la crittografia gestita da AWS o AWS KMS per crittografare i dischi radice, di avvio e dati ONTAP .



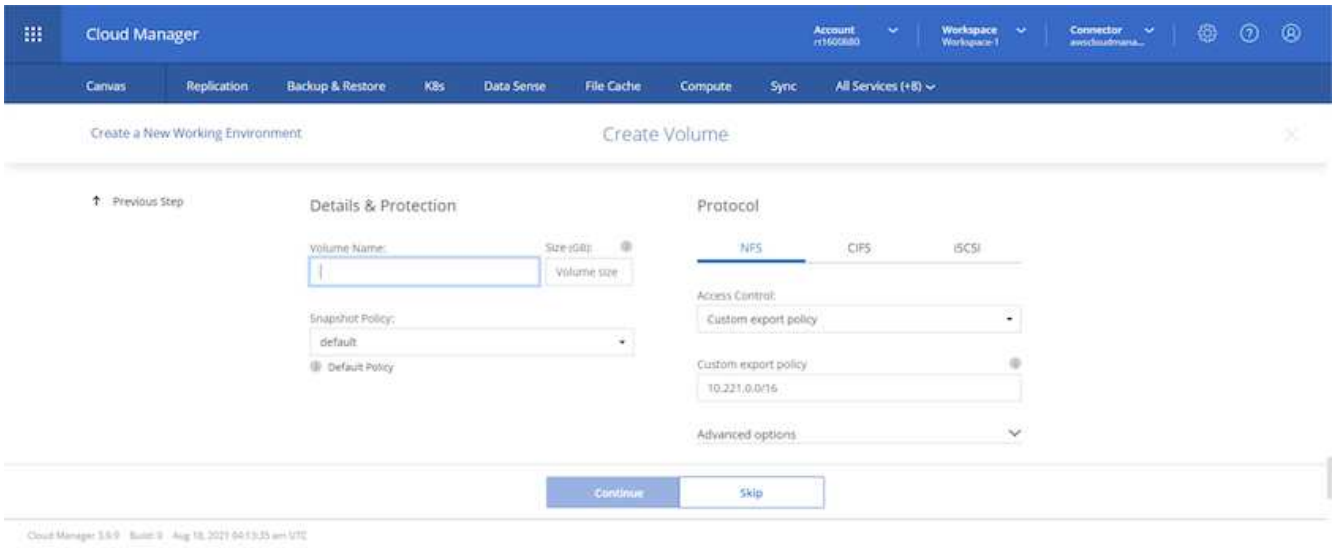
4. Scegli il tuo modello di licenza. Se non sai quale scegliere, contatta il tuo rappresentante NetApp .



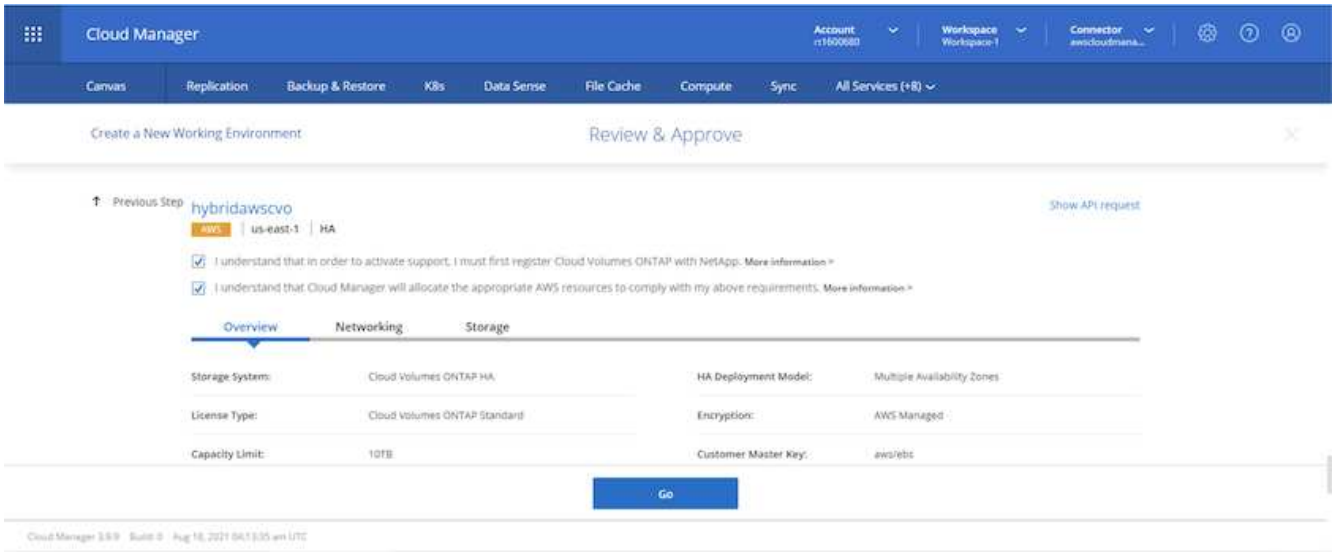
5. Seleziona la configurazione più adatta al tuo caso d'uso. Ciò è correlato alle considerazioni sulle dimensioni trattate nella pagina dei prerequisiti.



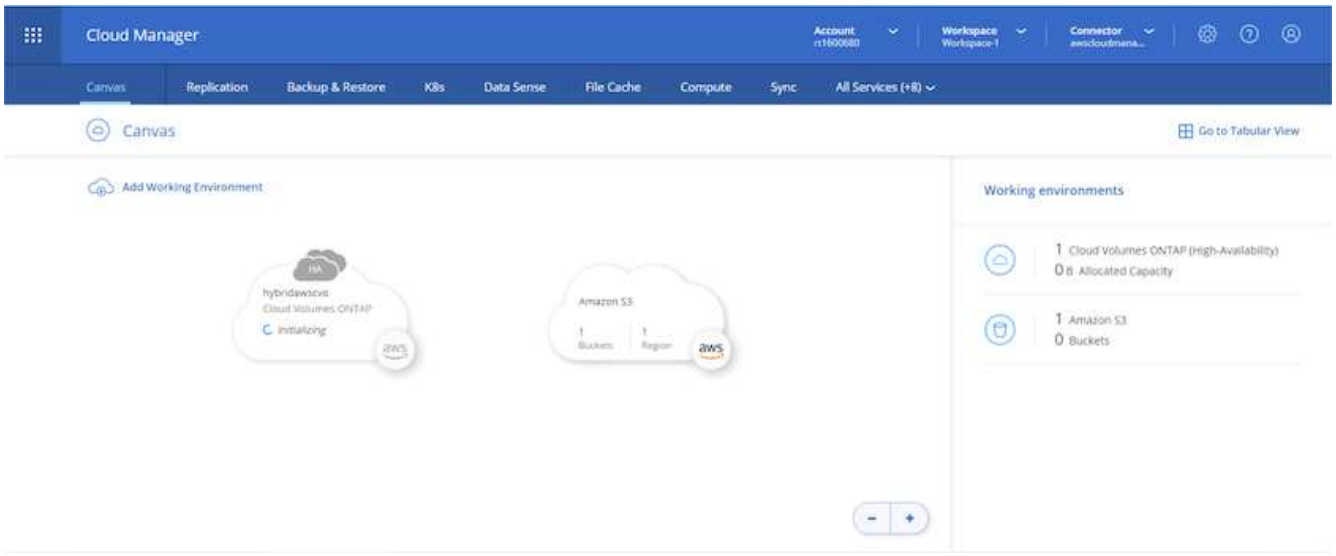
6. Facoltativamente, creare un volume. Questa operazione non è necessaria, perché i passaggi successivi utilizzano SnapMirror, che crea i volumi per noi.



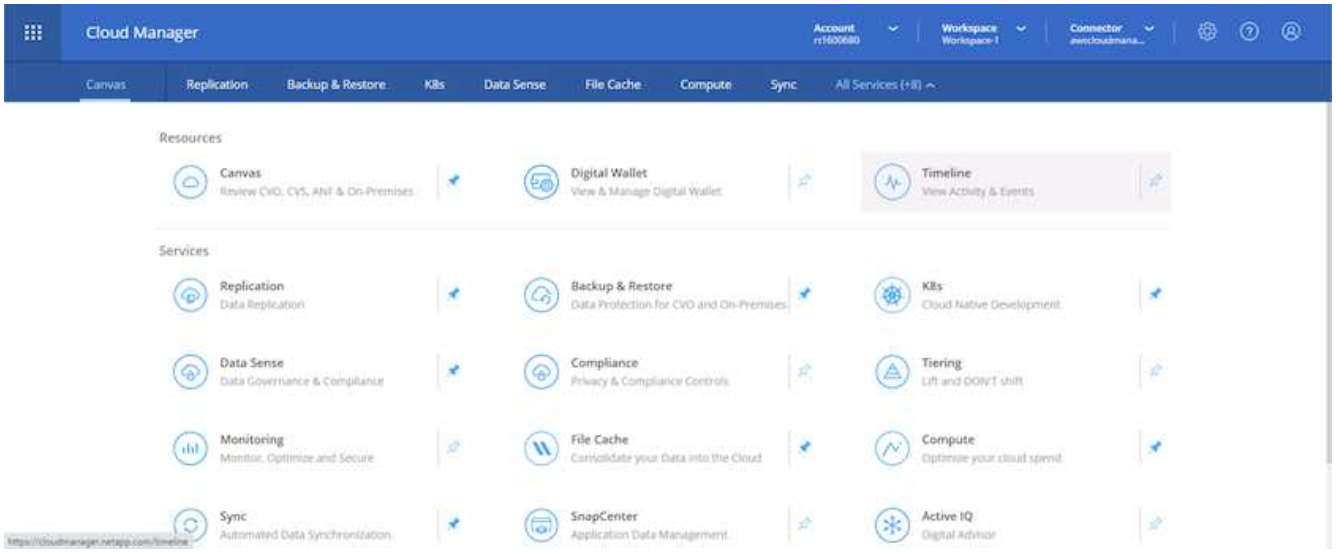
7. Rivedi le selezioni effettuate e seleziona le caselle per verificare di aver compreso che Cloud Manager distribuisce risorse nel tuo ambiente AWS. Quando sei pronto, clicca su Vai.



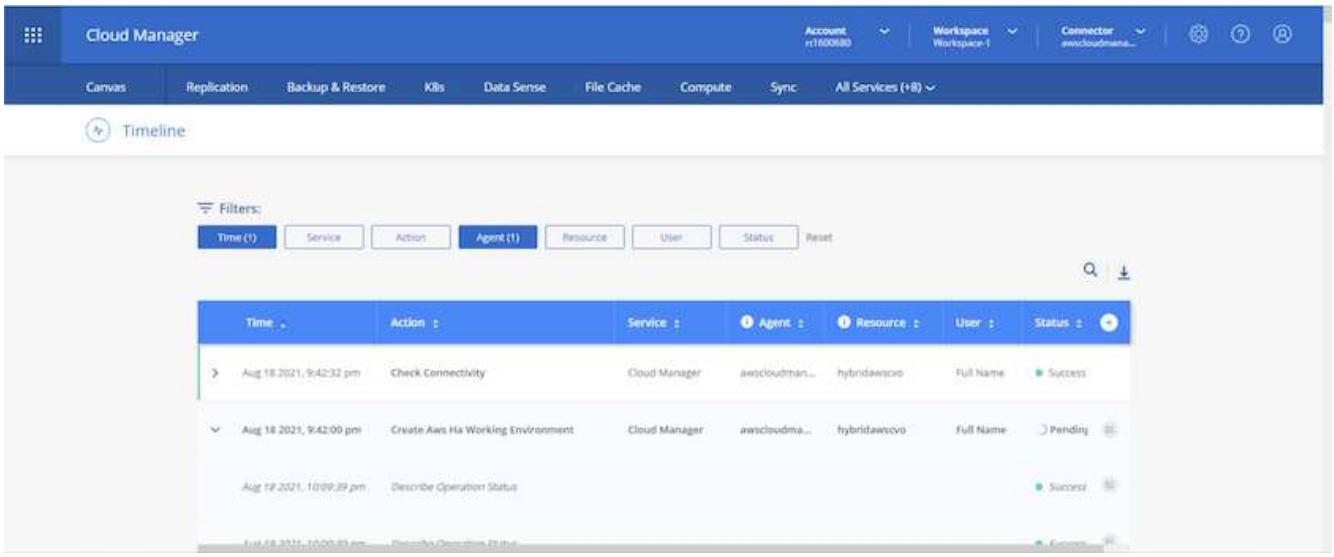
8. Cloud Volumes ONTAP avvia ora il processo di distribuzione. Cloud Manager utilizza le API AWS e gli stack di formazione cloud per distribuire Cloud Volumes ONTAP. Quindi configura il sistema in base alle tue specifiche, fornendoti un sistema pronto all'uso che puoi utilizzare immediatamente. I tempi di questo processo variano a seconda delle selezioni effettuate.



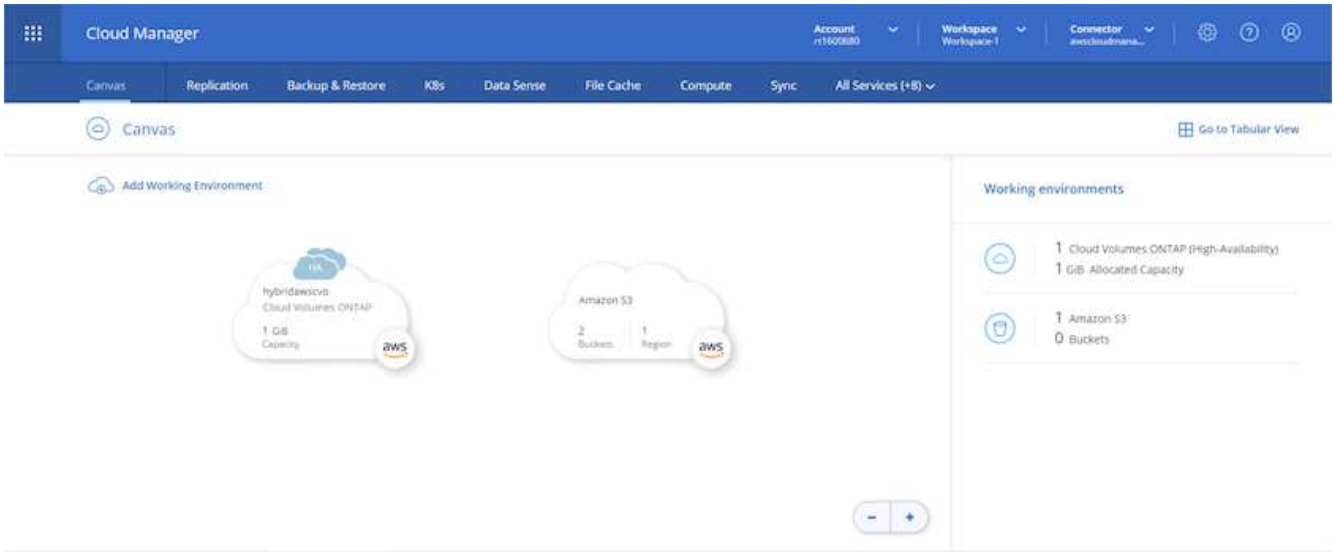
9. È possibile monitorare i progressi accedendo alla Timeline.



10. La cronologia funge da controllo di tutte le azioni eseguite in Cloud Manager. È possibile visualizzare tutte le chiamate API effettuate da Cloud Manager durante la configurazione sia su AWS che sul cluster ONTAP . Può essere utilizzato efficacemente anche per risolvere eventuali problemi che si possono riscontrare.



11. Una volta completata la distribuzione, il cluster CVO appare su Canvas, con la capacità corrente. Il cluster ONTAP nel suo stato attuale è completamente configurato per consentire un'esperienza reale e immediata.

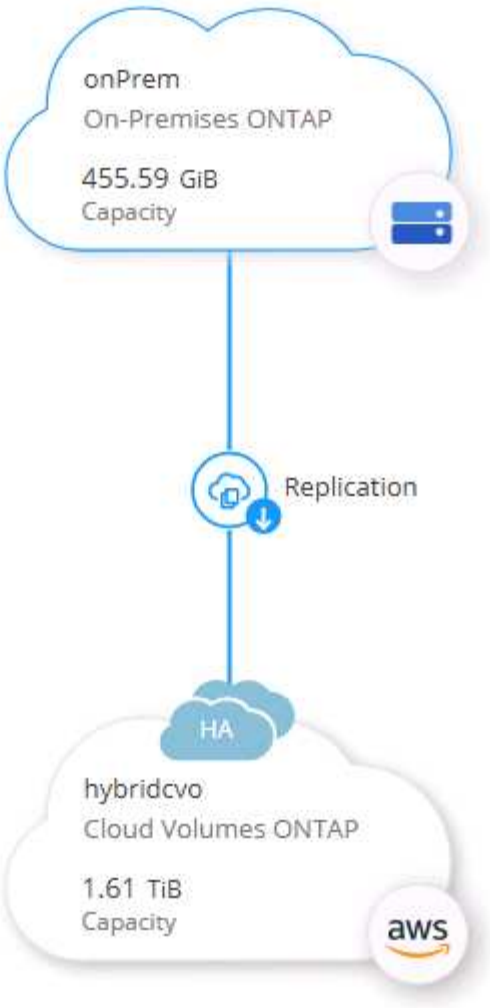


Configura SnapMirror da locale a cloud

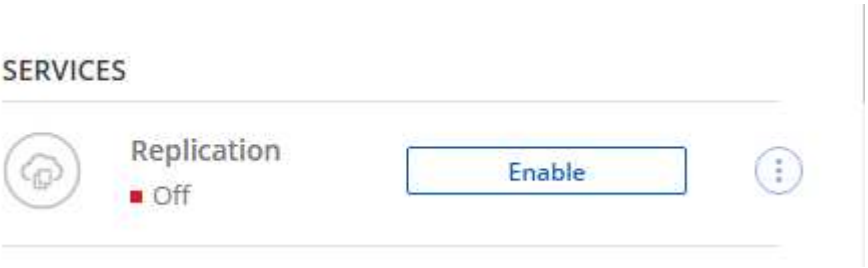
Ora che hai distribuito un sistema ONTAP di origine e un sistema ONTAP di destinazione, puoi replicare i volumi contenenti i dati del database nel cloud.

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

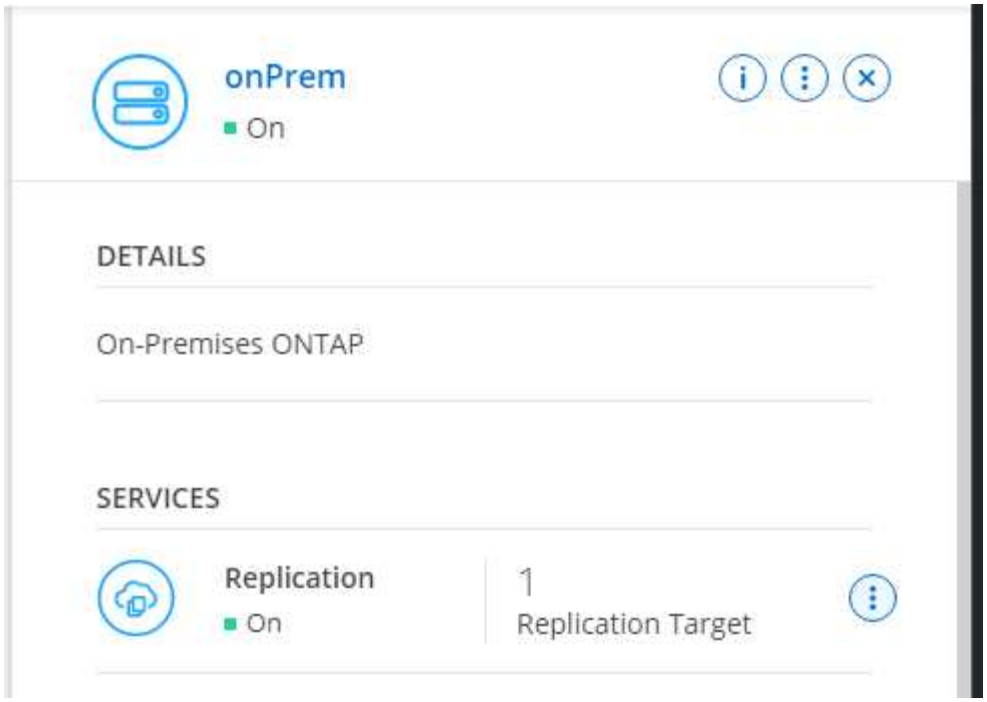
1. Fare clic sul sistema ONTAP di origine (in locale) e trascinarlo nella destinazione, selezionare Replica > Abilita oppure selezionare Replica > Menu > Replica.



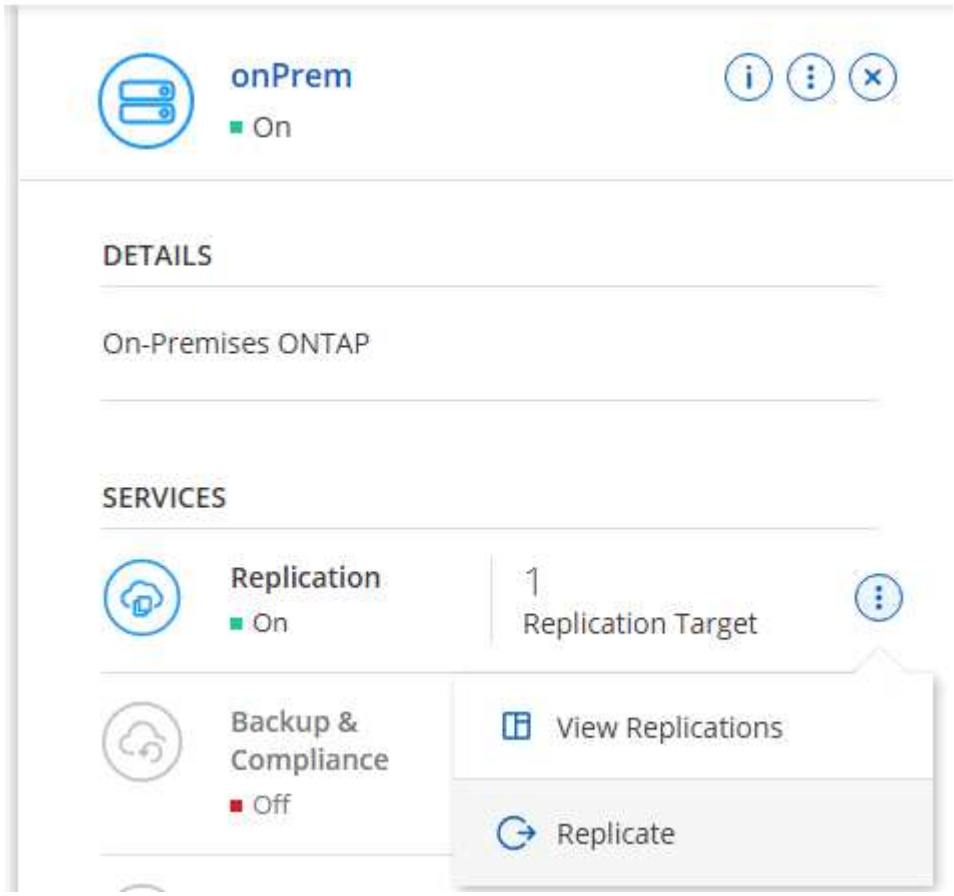
Selezionare Abilita.



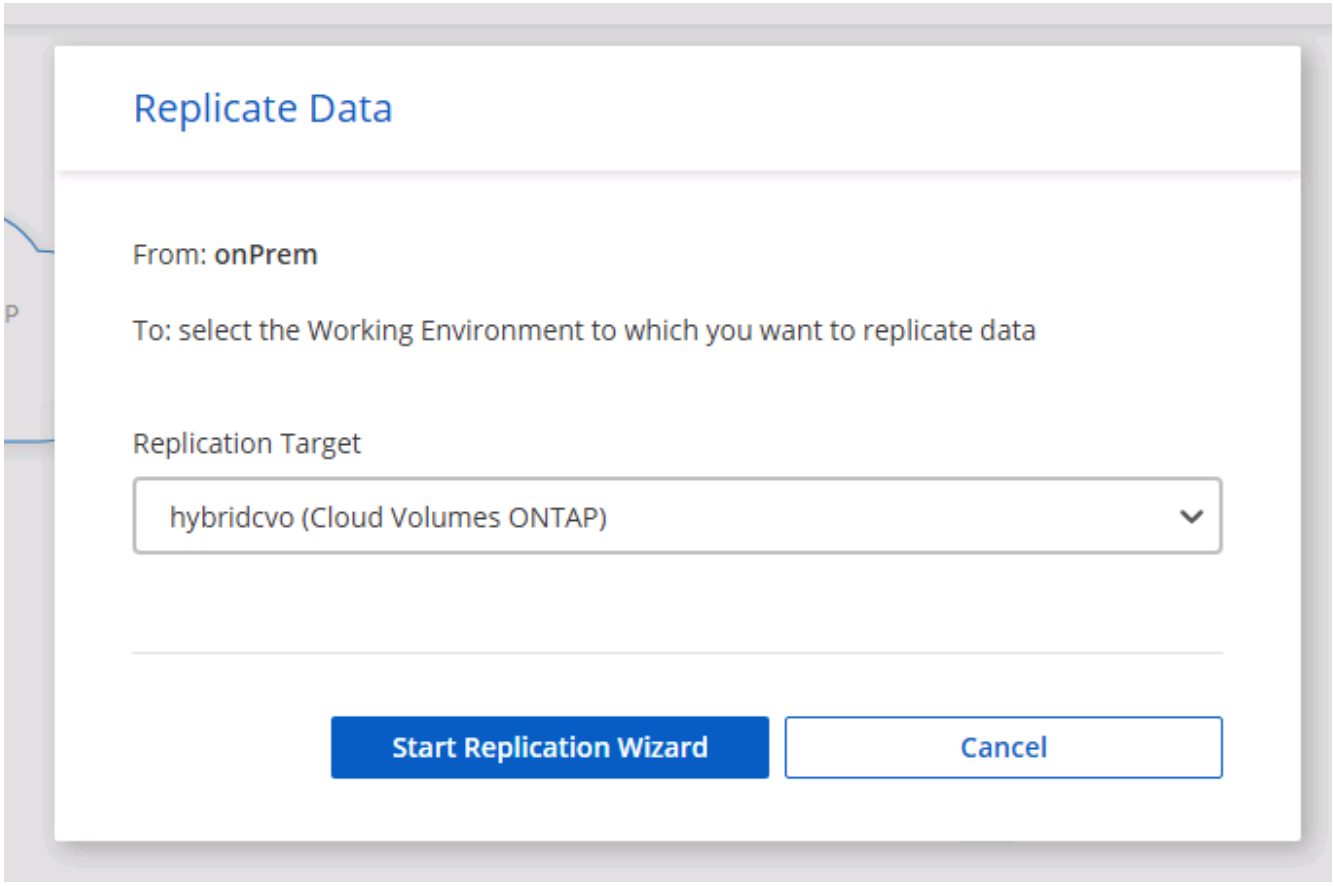
Oppure Opzioni.



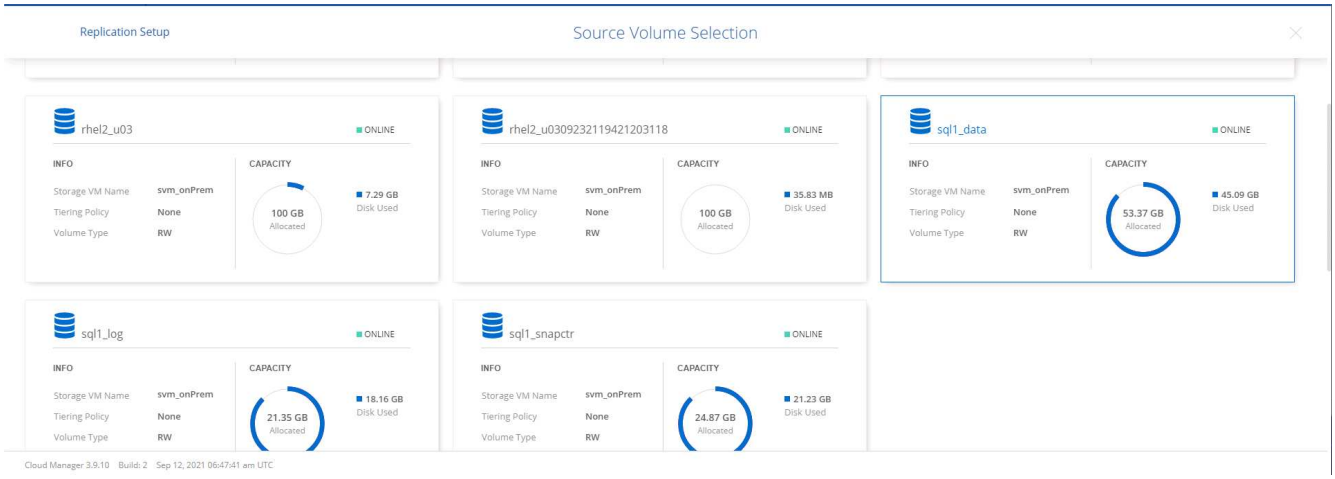
Replicare.



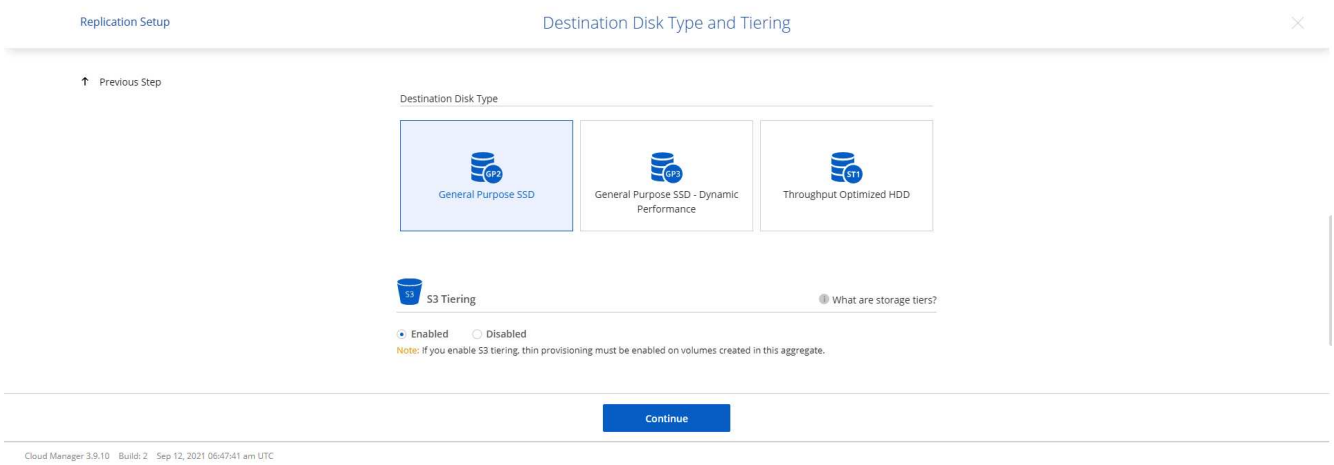
2. Se non hai eseguito il trascinamento della selezione, seleziona il cluster di destinazione su cui effettuare la replica.



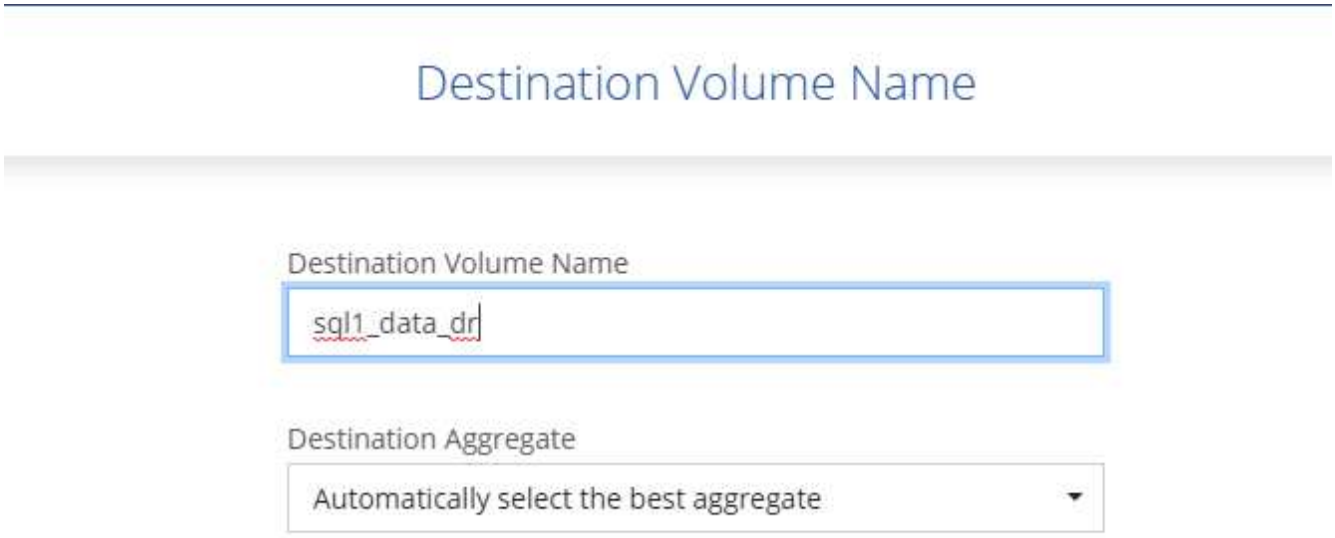
3. Scegli il volume che desideri replicare. Abbiamo replicato i dati e tutti i volumi di registro.



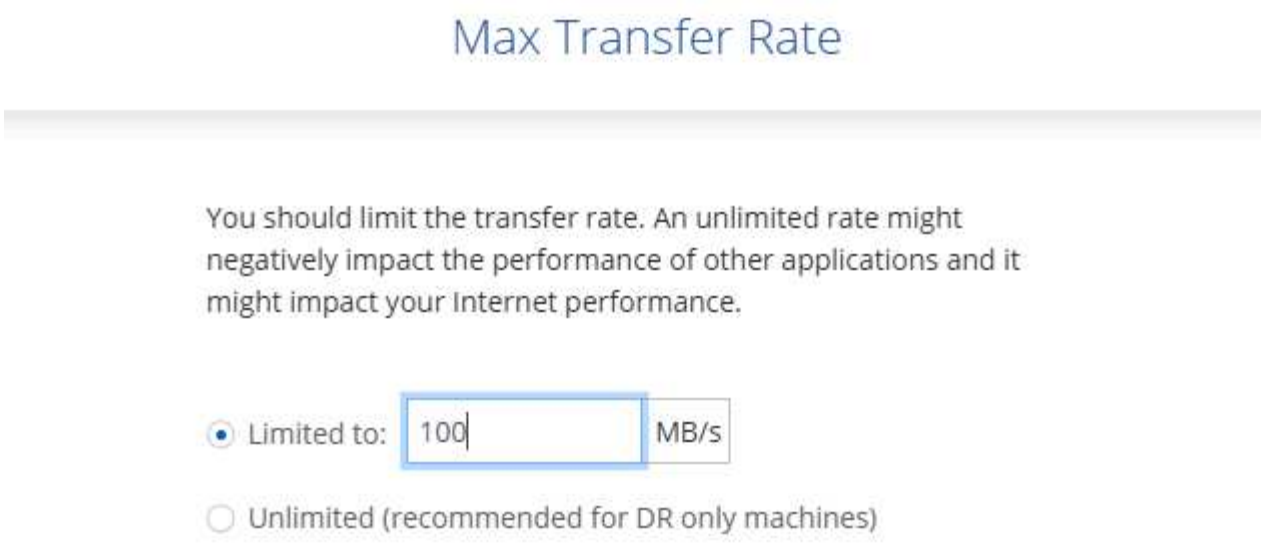
4. Selezionare il tipo di disco di destinazione e la politica di suddivisione in livelli. Per il disaster recovery, consigliamo un SSD come tipo di disco e per mantenere la suddivisione in livelli dei dati. Il data tiering suddivide i dati speculari in un archivio di oggetti a basso costo e consente di risparmiare denaro sui dischi locali. Quando si interrompe la relazione o si clona il volume, i dati utilizzano l'archiviazione locale veloce.



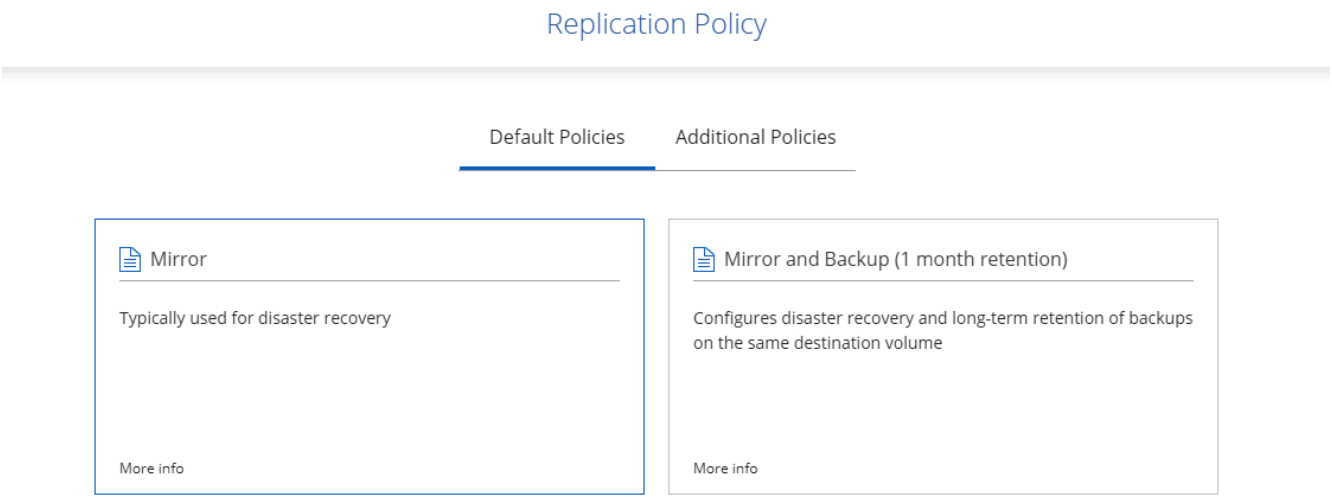
5. Seleziona il nome del volume di destinazione: abbiamo scelto `[source_volume_name]_dr`.



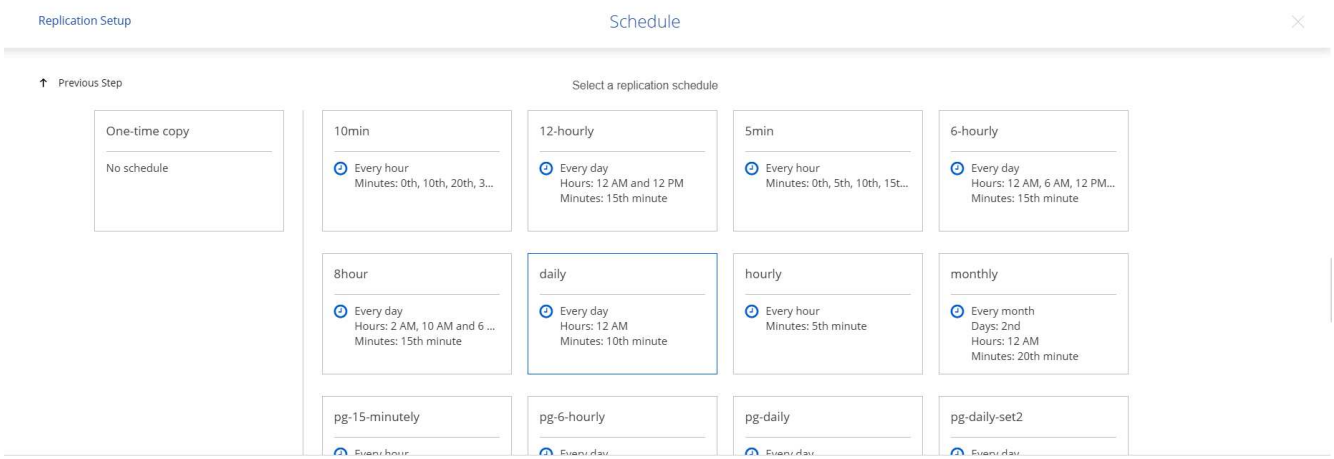
6. Selezionare la velocità di trasferimento massima per la replica. Ciò consente di risparmiare larghezza di banda se si dispone di una connessione al cloud con larghezza di banda ridotta, come una VPN.



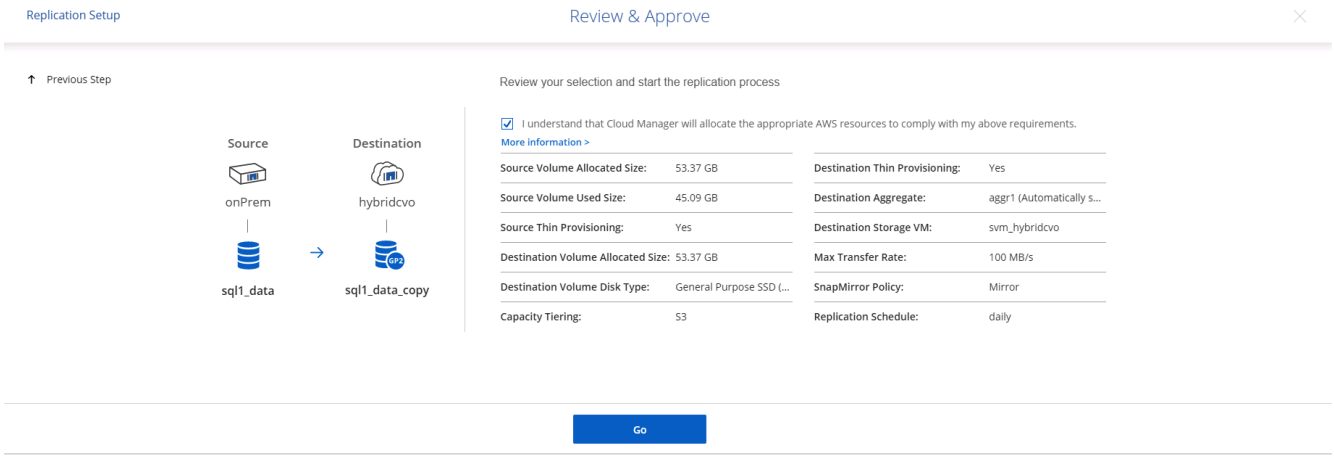
7. Definire la politica di replicazione. Abbiamo scelto un Mirror, che prende il set di dati più recente e lo replica nel volume di destinazione. Potresti anche scegliere una polizza diversa in base alle tue esigenze.



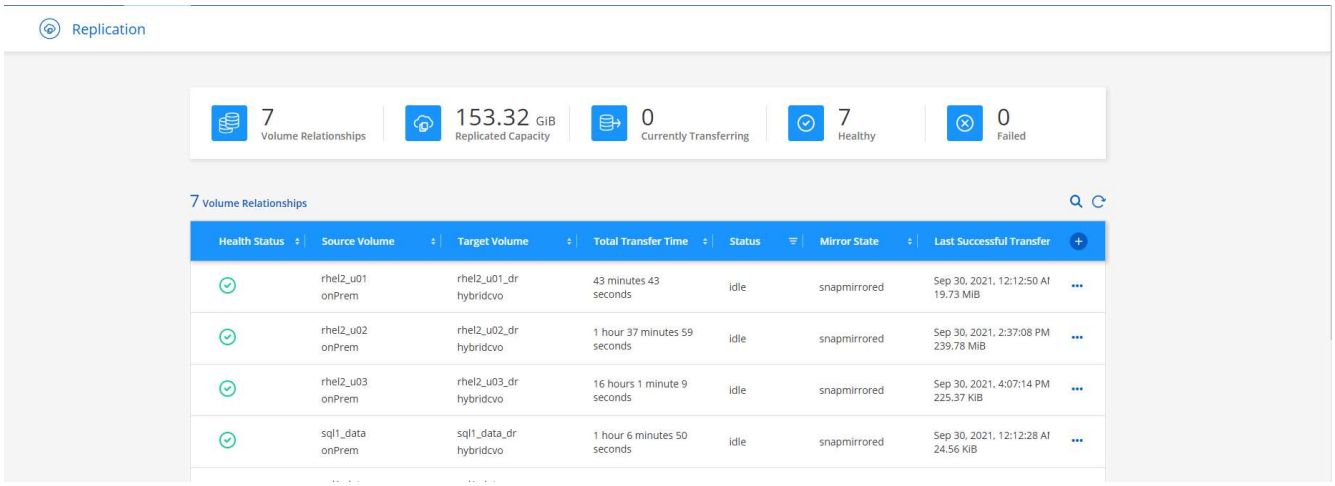
8. Selezionare la pianificazione per l'attivazione della replica. NetApp consiglia di impostare una pianificazione "giornaliera" per il volume di dati e una pianificazione "oraria" per i volumi di log, anche se è possibile modificarla in base alle esigenze.



9. Rivedere le informazioni immesse, fare clic su Vai per attivare il peer del cluster e il peer SVM (se è la prima volta che si esegue una replica tra i due cluster), quindi implementare e inizializzare la relazione SnapMirror .



10. Continuare questo processo per i volumi di dati e i volumi di registro.
11. Per controllare tutte le relazioni, vai alla scheda Replicazione in Cloud Manager. Qui puoi gestire le tue relazioni e controllarne lo stato.



12. Dopo aver replicato tutti i volumi, si è in uno stato stabile e si è pronti a passare ai flussi di lavoro di disaster recovery e sviluppo/test.

3. Distribuisci l'istanza di elaborazione EC2 per il carico di lavoro del database

AWS ha preconfigurato istanze di elaborazione EC2 per vari carichi di lavoro. La scelta del tipo di istanza determina il numero di core della CPU, la capacità di memoria, il tipo e la capacità di archiviazione e le prestazioni della rete. Per i casi d'uso, 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, della memoria e del livello di prestazioni della rete. I tipi tipici di istanze 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. Tra i fattori da considerare rientrano il numero di transazioni commerciali da supportare, il numero di utenti contemporanei, le dimensioni del set di dati e così via.
2. La distribuzione delle istanze EC2 può essere avviata tramite la Dashboard EC2. Le procedure di distribuzione esatte vanno oltre lo scopo di questa soluzione. Vedere "Amazon EC2" per i dettagli.

Configurazione dell'istanza Linux per il carico di lavoro Oracle

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

1. Aggiungere un'istanza standby di 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. Abilitare l'ID con autenticazione tramite password SSH sull'istanza EC2. (Per impostazione predefinita, l'autenticazione tramite password SSH e sudo senza password sono disattivati nelle istanze EC2.)
3. Configurare l'installazione di Oracle in modo che corrisponda all'installazione di Oracle in locale, ad esempio patch del sistema operativo, versioni e patch di Oracle e così via.
4. I ruoli di automazione del database NetApp Ansible possono essere sfruttati per configurare istanze EC2 per casi d'uso di sviluppo/test del database e di disaster recovery. Il codice di automazione può essere scaricato dal sito pubblico GitHub NetApp : "Distribuzione automatizzata di Oracle 19c" . L'obiettivo è installare e configurare uno stack software di database su un'istanza EC2 in modo che corrisponda alle configurazioni del sistema operativo e del database locali.

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

In questa sezione sono elencati i passaggi di configurazione aggiuntivi successivi alla distribuzione iniziale di un'istanza EC2 Windows.

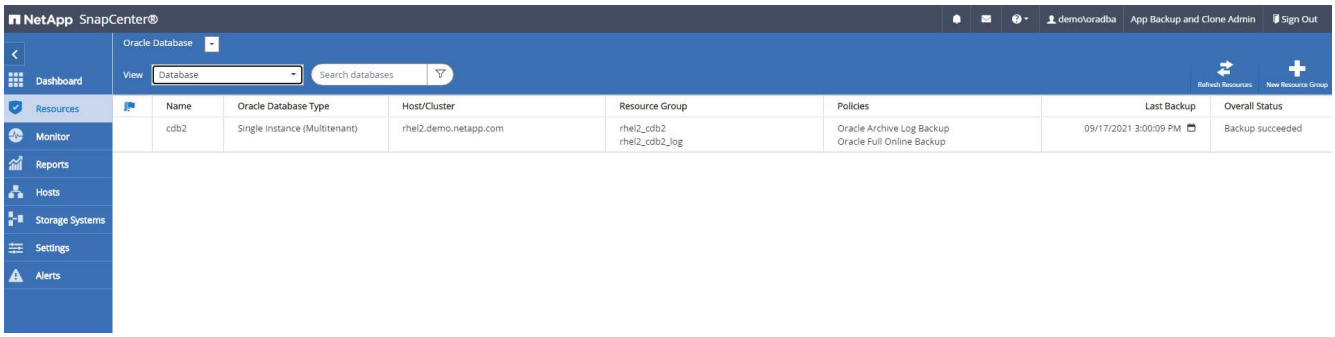
1. Recupera la password dell'amministratore di Windows per accedere a un'istanza tramite RDP.
2. Disattivare il firewall di Windows, unire l'host al dominio Windows SnapCenter e aggiungere l'istanza al server DNS per la risoluzione dei nomi.
3. Fornire un volume di registro SnapCenter per archiviare i file di registro di SQL Server.
4. Configurare iSCSI sull'host Windows per montare il volume e formattare l'unità disco.
5. Anche in questo caso, molte delle attività precedenti possono essere automatizzate con la soluzione di automazione NetApp per SQL Server. Consulta il sito GitHub pubblico di NetApp Automation per i ruoli e le soluzioni appena pubblicati: "Automazione NetApp" .

Flusso di lavoro per lo sviluppo/test che si espande nel cloud

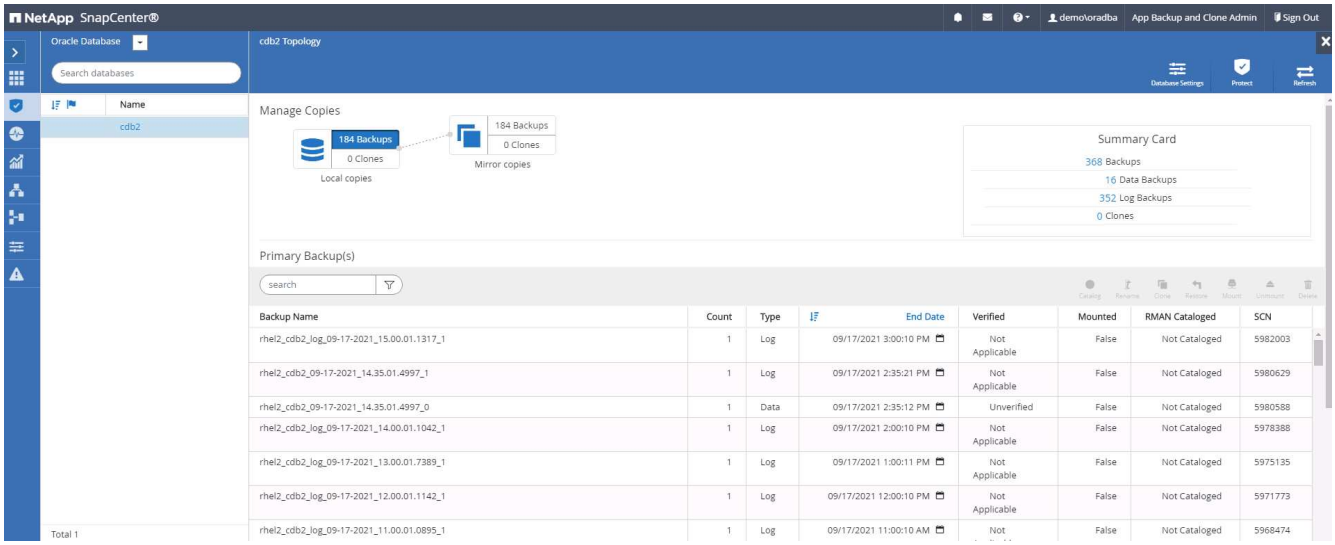
L'agilità del cloud pubblico, il time-to-value e il risparmio sui costi sono tutte proposte di valore significative per le aziende che adottano il cloud pubblico per lo sviluppo e il test delle applicazioni di database. Non esiste strumento migliore di SnapCenter per rendere tutto questo realtà. SnapCenter non solo può proteggere il tuo database di produzione in locale, ma può anche clonarne rapidamente una copia per lo sviluppo di applicazioni o per il test del codice nel cloud pubblico, consumando pochissimo spazio di archiviazione aggiuntivo. Di seguito sono riportati i dettagli dei processi passo dopo passo per utilizzare questo strumento.

Clona un database Oracle per sviluppo/test da un backup snapshot replicato

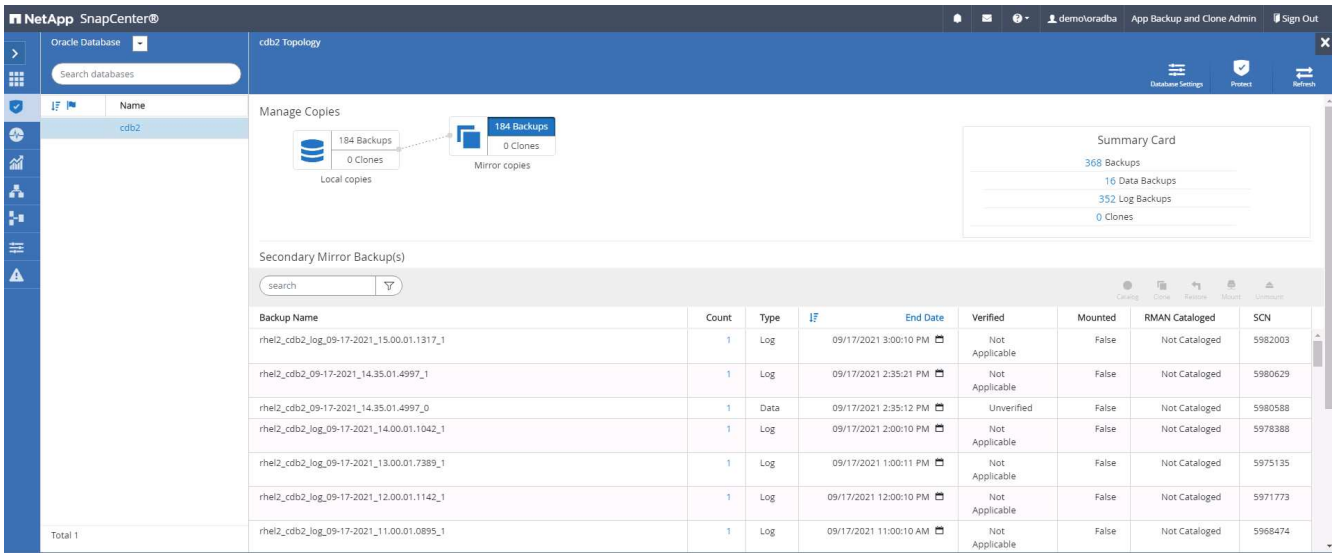
1. Accedi a SnapCenter con un ID utente di gestione del database per Oracle. Passare alla scheda Risorse, che mostra i database Oracle protetti da SnapCenter.



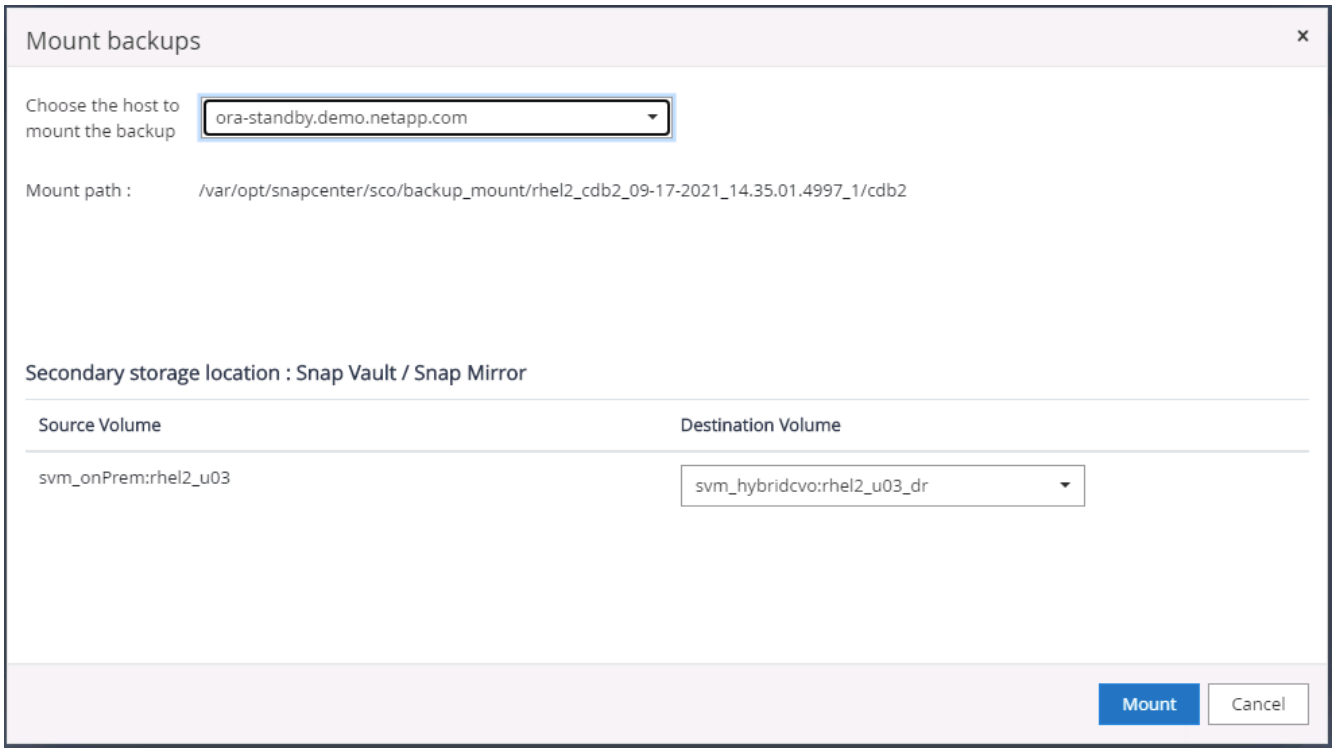
2. Fare clic sul nome del database locale desiderato per la topologia di backup e la vista dettagliata. Se è abilitata una posizione replicata secondaria, vengono mostrati i backup mirror collegati.

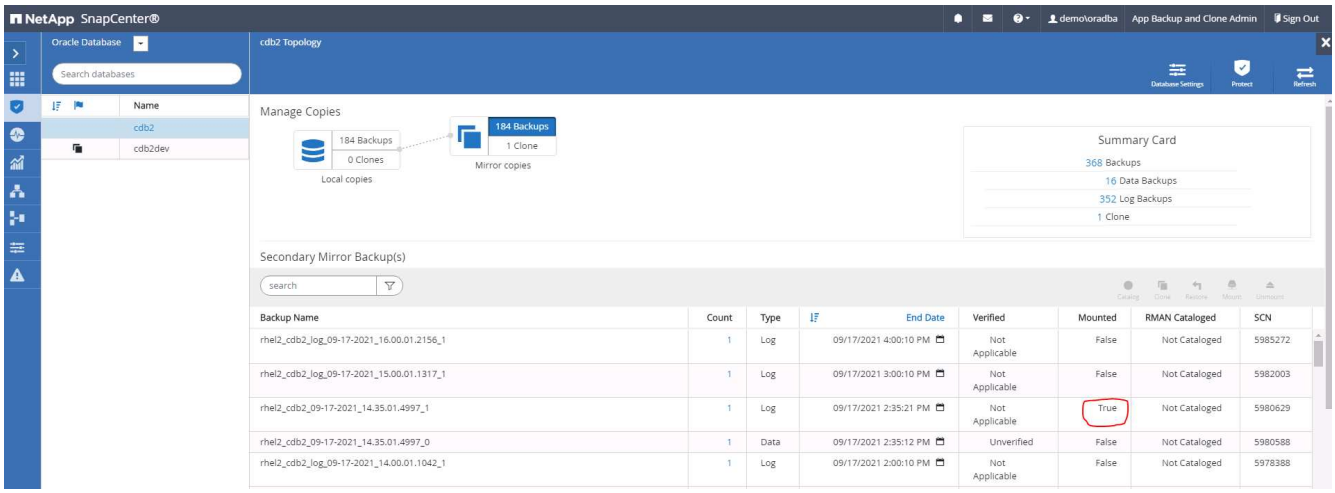


3. È possibile passare alla visualizzazione dei backup speculari facendo clic su Backup speculari. Vengono quindi visualizzati i backup dello specchio secondario.



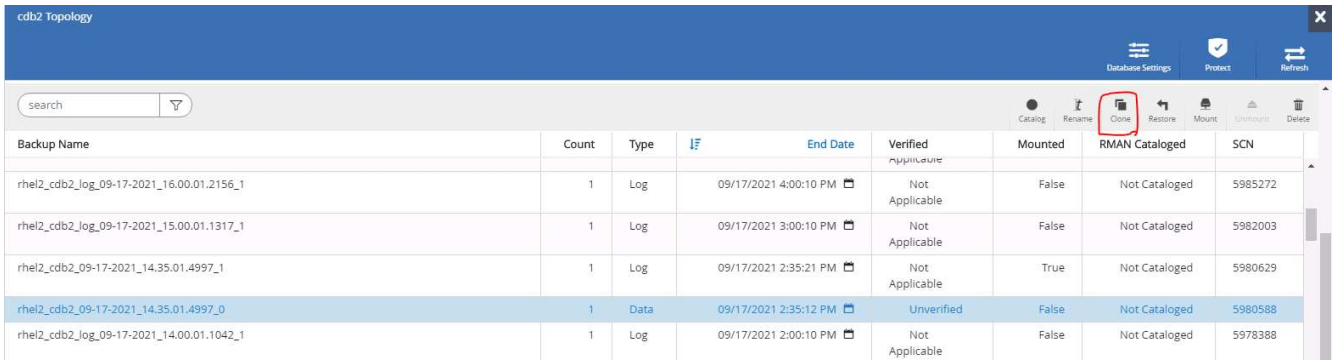
4. Selezionare una copia di backup del database secondario con mirroring da clonare e determinare un punto di ripristino in base all'ora e al numero di modifica del sistema oppure in base all'SCN. In genere, il punto di ripristino dovrebbe essere successivo al momento del backup completo del database o all'SCN da clonare. Dopo aver deciso un punto di ripristino, è necessario montare il backup del file di registro richiesto per il ripristino. Il backup del file di registro deve essere montato sul server DB di destinazione in cui verrà ospitato il database clone.



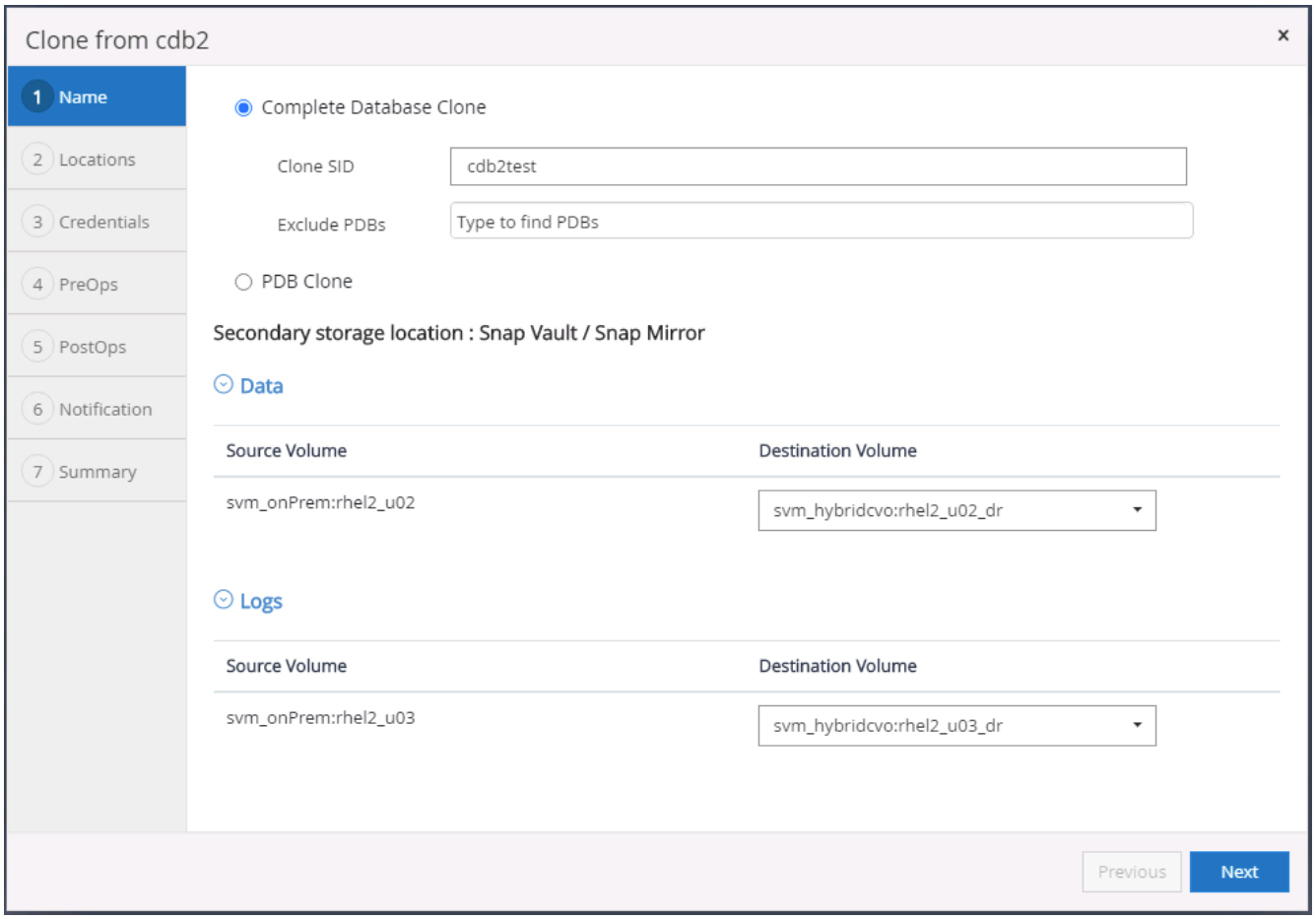


Se è abilitata la potatura del registro e il punto di ripristino viene esteso oltre l'ultima potatura del registro, potrebbe essere necessario montare più backup del registro di archivio.

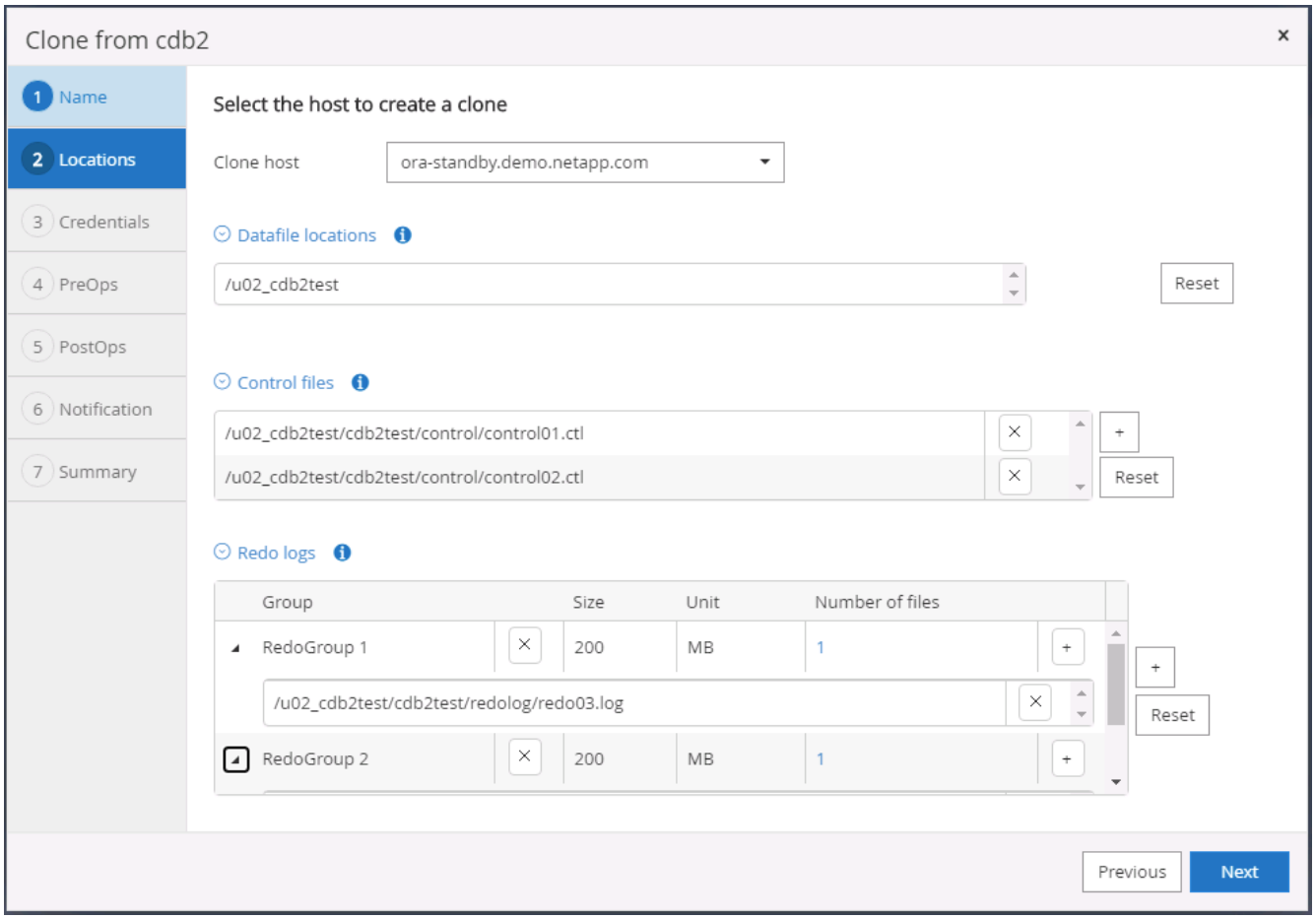
5. Evidenziare la copia di backup completa del database da clonare, quindi fare clic sul pulsante Clona per avviare il flusso di lavoro di clonazione del database.



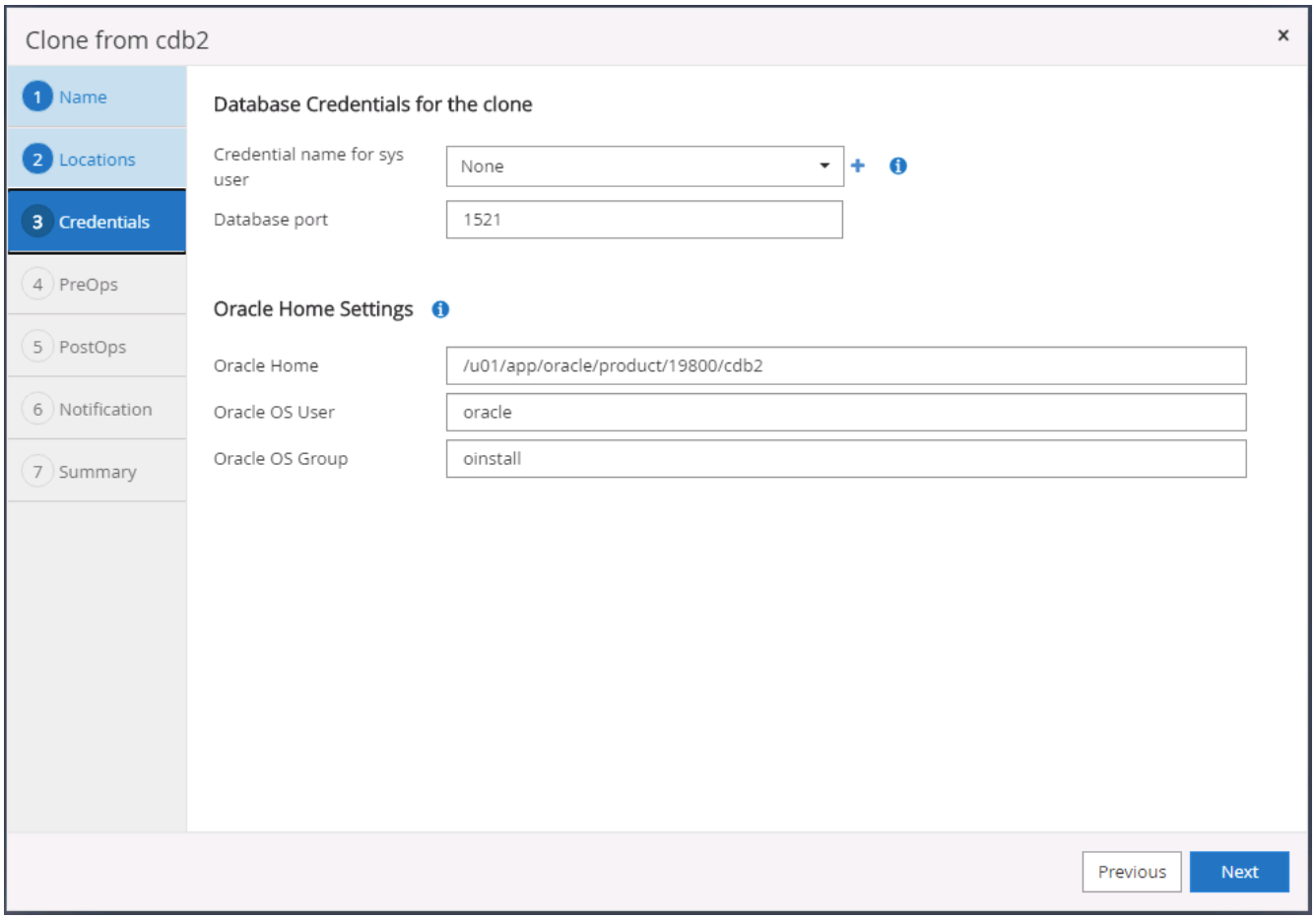
6. Scegliere un SID DB clone appropriato per un database contenitore completo o un clone CDB.



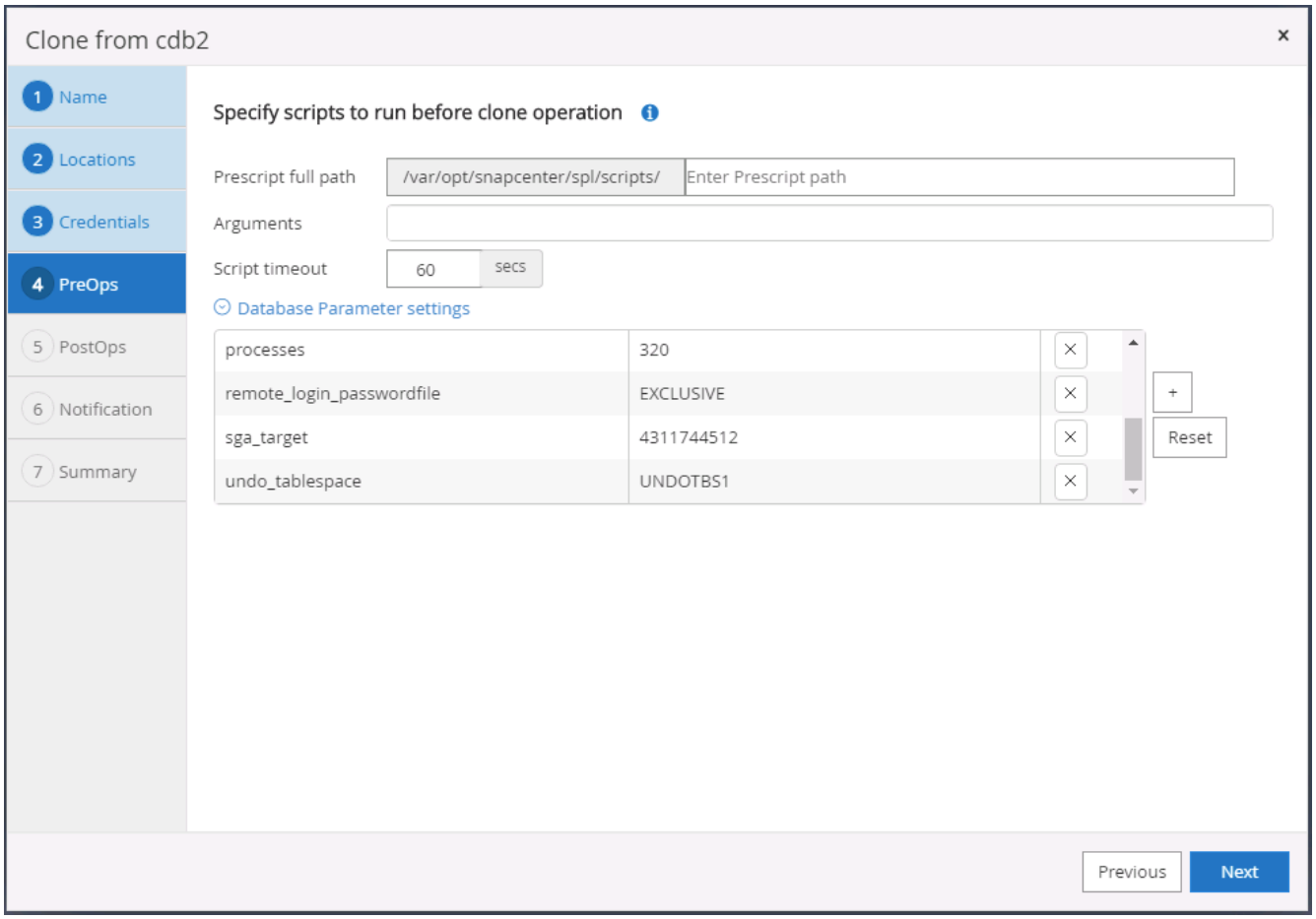
7. Selezionando l'host clone di destinazione nel cloud, il flusso di lavoro di clonazione creerà le directory dei file di dati, dei file di controllo e dei log redo.



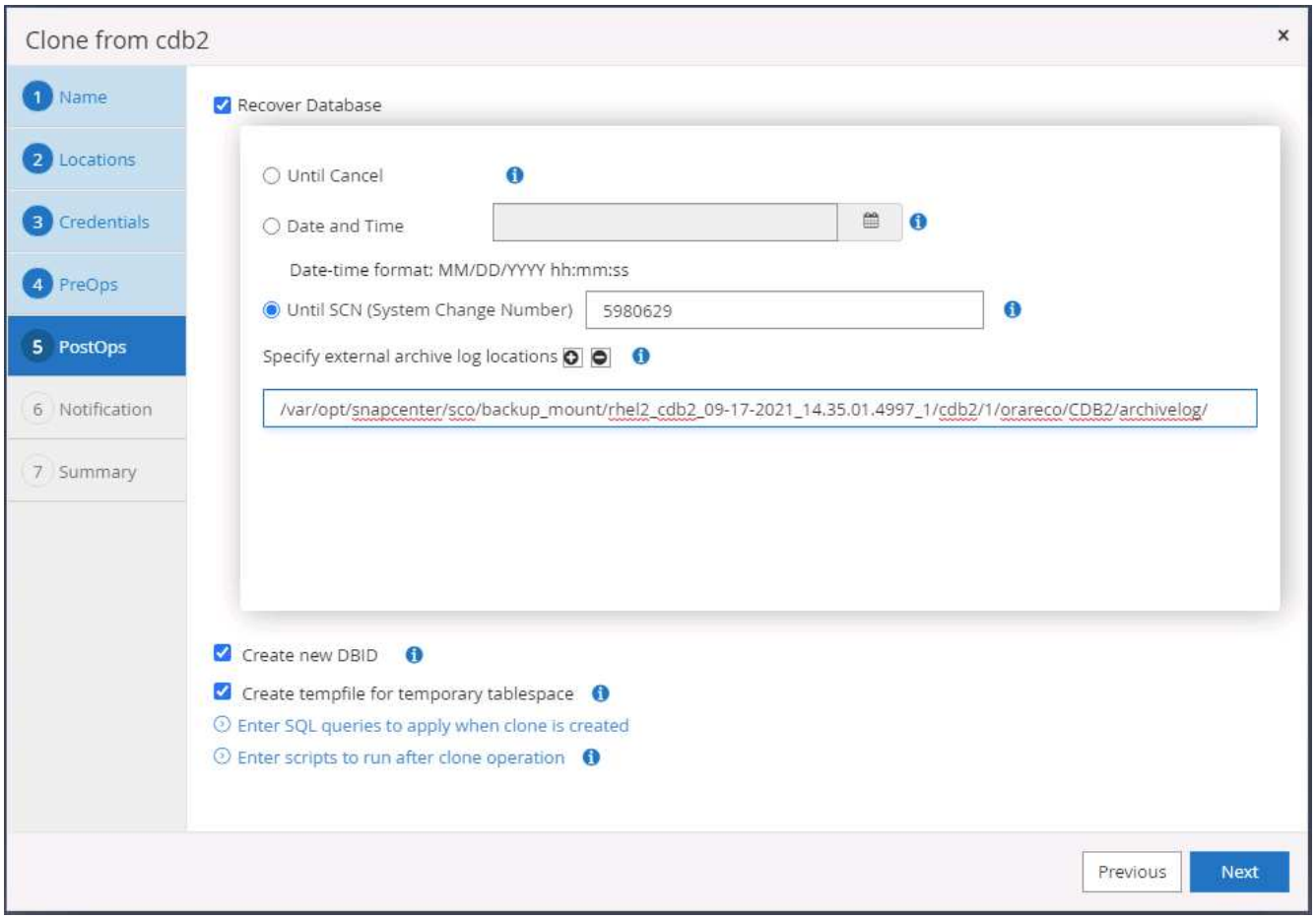
8. Il nome della credenziale Nessuno viene utilizzato per l'autenticazione basata sul sistema operativo, il che rende irrilevante la porta del database. Inserire i dati corretti per Oracle Home, Oracle OS User e Oracle OS Group, come configurato nel server DB clone di destinazione.

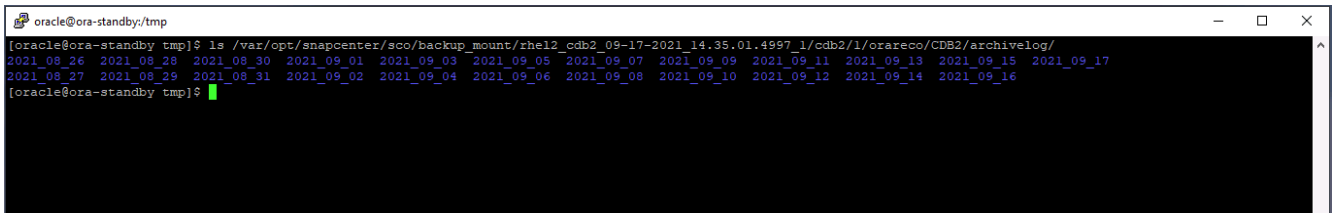


9. Specificare gli script da eseguire prima dell'operazione di clonazione. Ancora più importante, il parametro dell'istanza del database può essere modificato o definito qui.

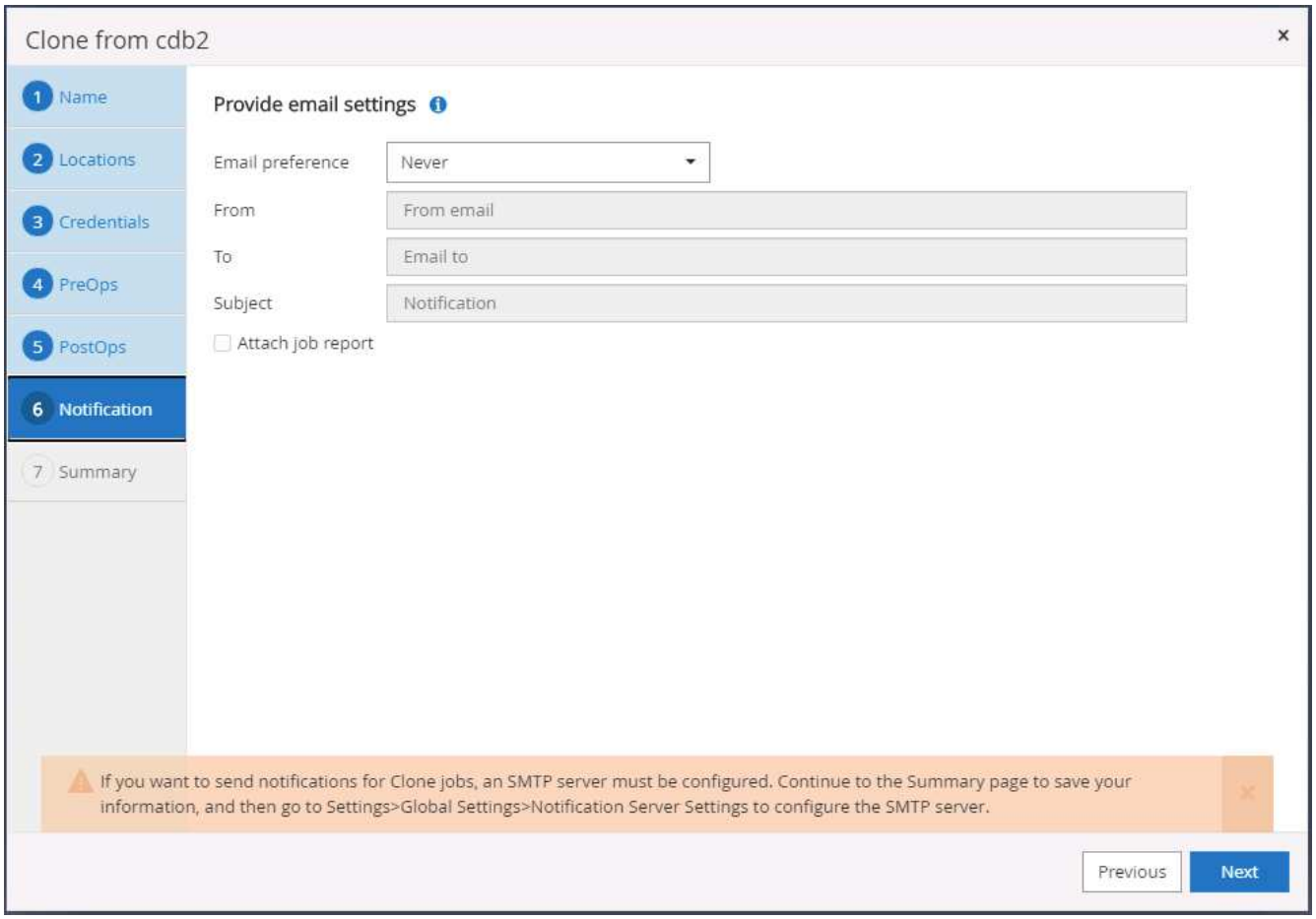


10. Specificare il punto di ripristino in base alla data e all'ora oppure tramite SCN. Finché Annulla ripristina il database fino ai registri di archivio disponibili. Specificare la posizione del registro di archivio esterno dall'host di destinazione in cui è montato il volume del registro di archivio. Se il proprietario Oracle del server di destinazione è diverso dal server di produzione locale, verificare che la directory del registro di archivio sia leggibile dal proprietario Oracle del server di destinazione.

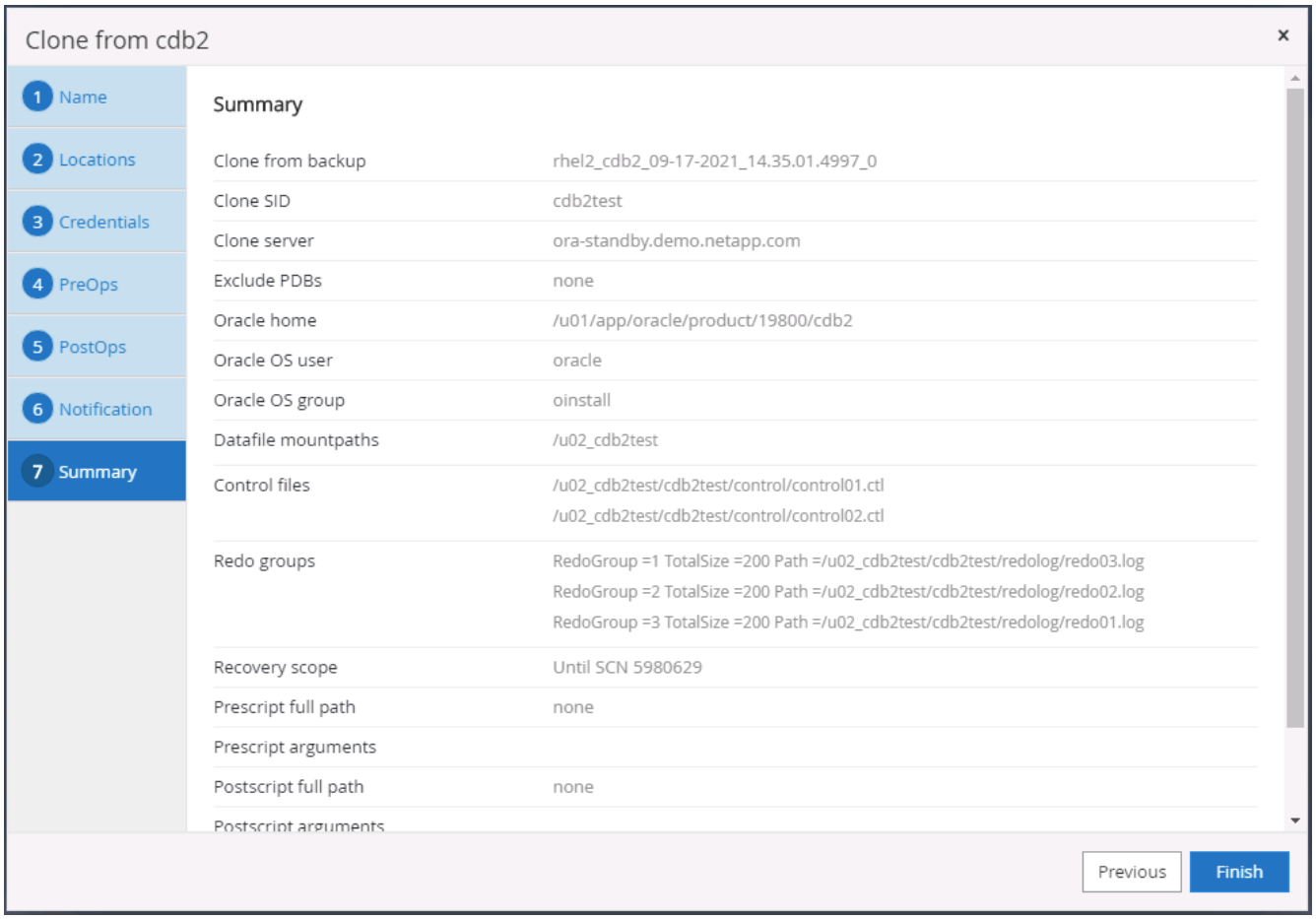




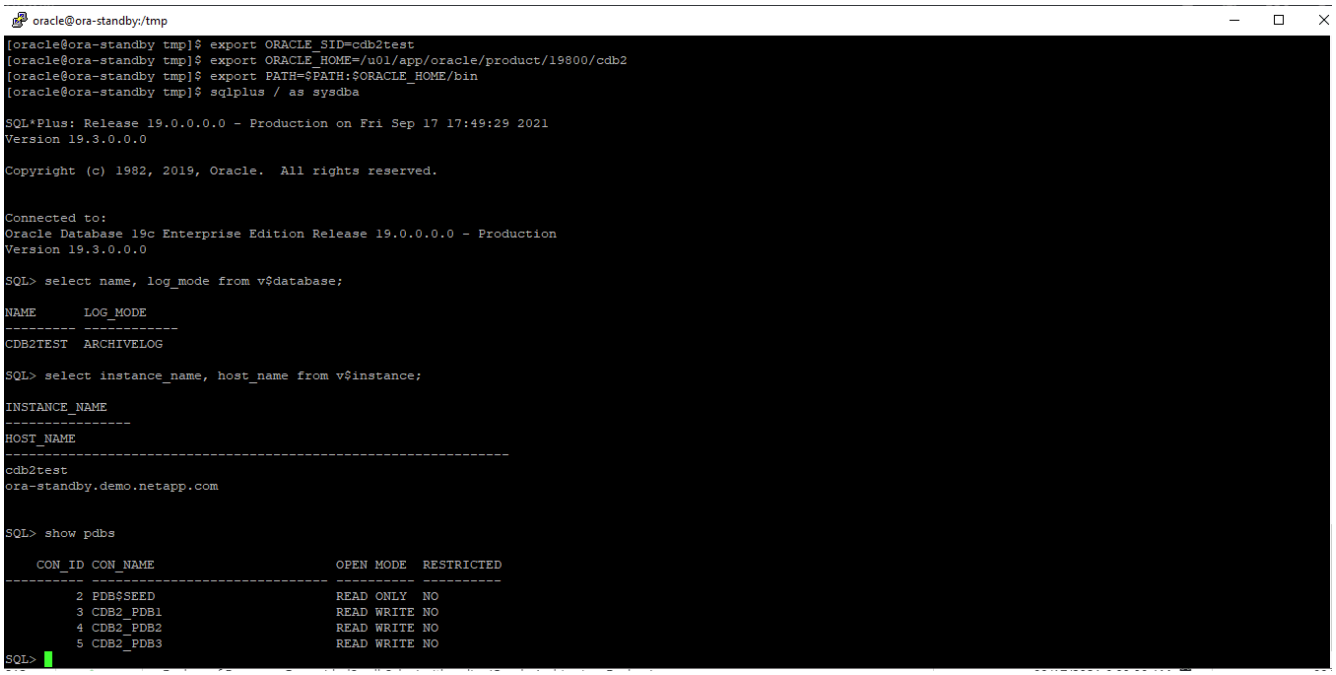
11. Se lo si desidera, configurare il server SMTP per la notifica via e-mail.



12. Riepilogo del clone.

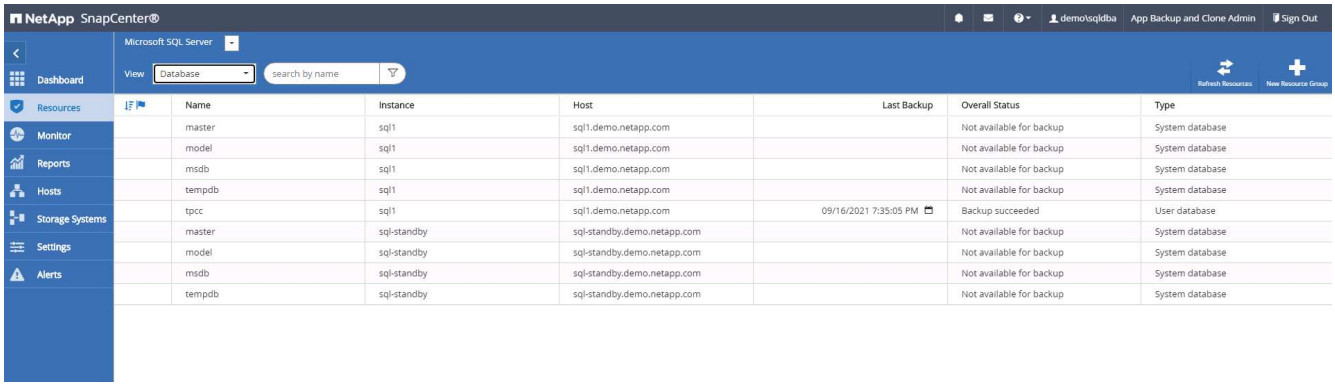


13. Dopo la clonazione è necessario convalidare per assicurarsi che il database clonato sia operativo. Alcune attività aggiuntive, come l'avvio del listener o la disattivazione della modalità di archiviazione del log del DB, possono essere eseguite sul database di sviluppo/test.

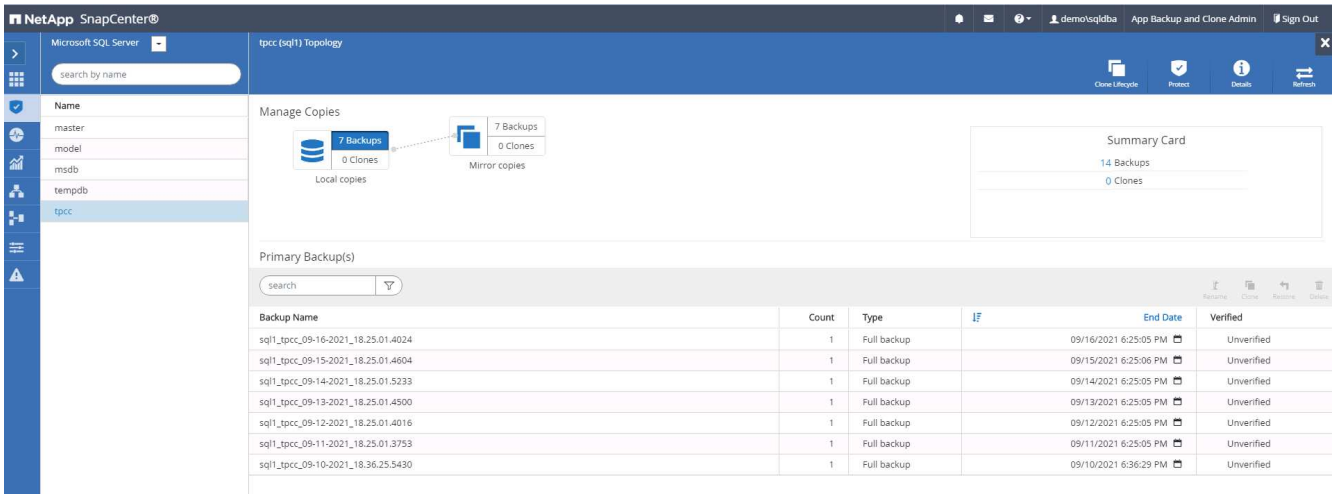


Clona un database SQL per sviluppo/test da un backup Snapshot replicato

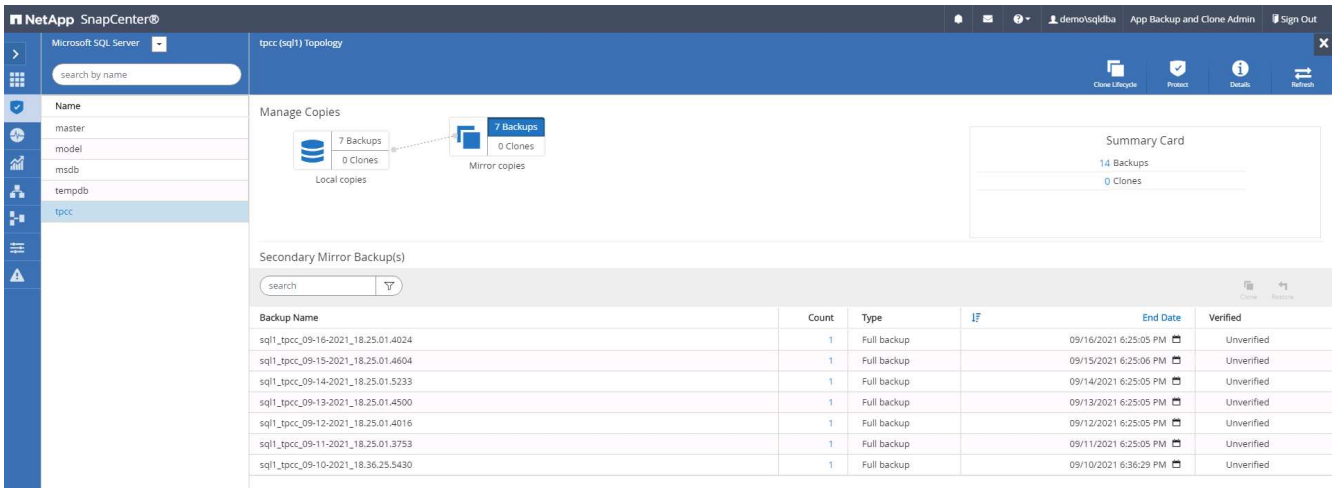
1. Accedi a SnapCenter con un ID utente di gestione del database per SQL Server. Passare alla scheda Risorse, che mostra i database utente di SQL Server protetti da SnapCenter e un'istanza SQL di standby di destinazione nel cloud pubblico.



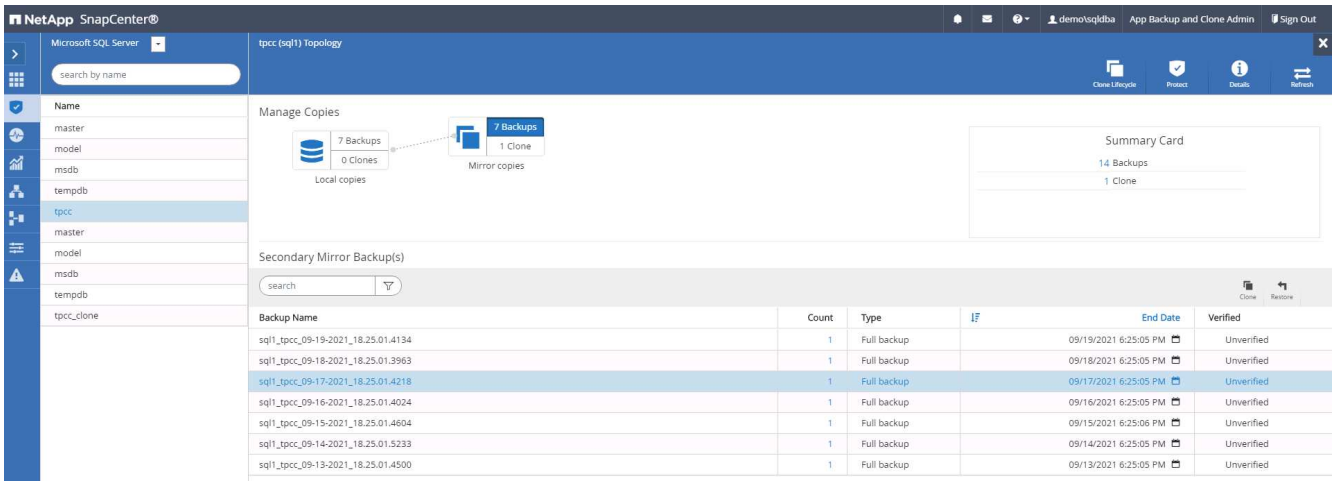
2. Fare clic sul nome del database utente SQL Server locale desiderato per la topologia dei backup e la visualizzazione dettagliata. Se è abilitata una posizione replicata secondaria, vengono mostrati i backup mirror collegati.

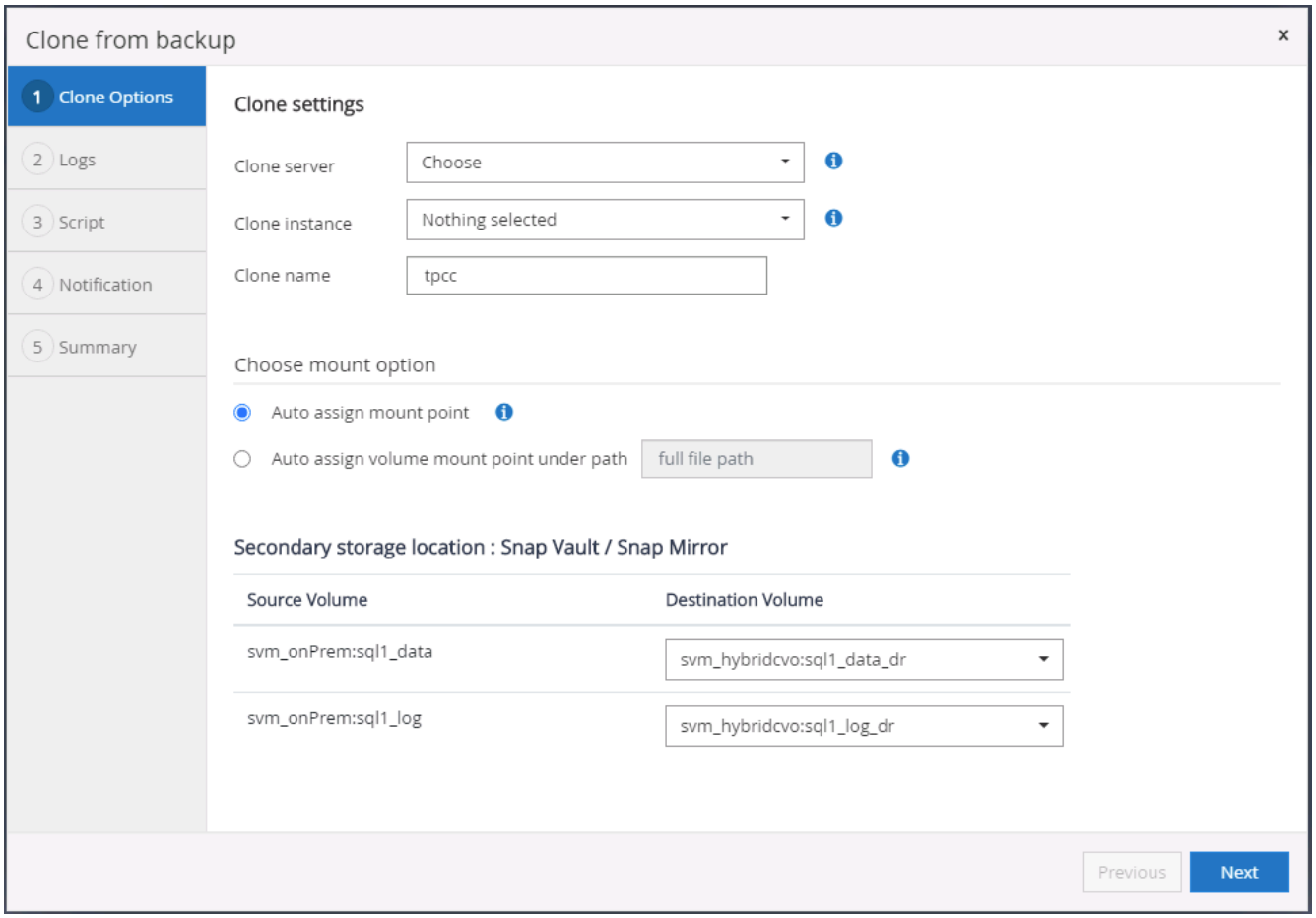


3. Passare alla visualizzazione Backup speculari facendo clic su Backup speculari. Vengono quindi visualizzati i backup mirror secondari. Poiché SnapCenter esegue il backup del registro delle transazioni di SQL Server su un'unità dedicata per il ripristino, qui vengono visualizzati solo i backup completi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

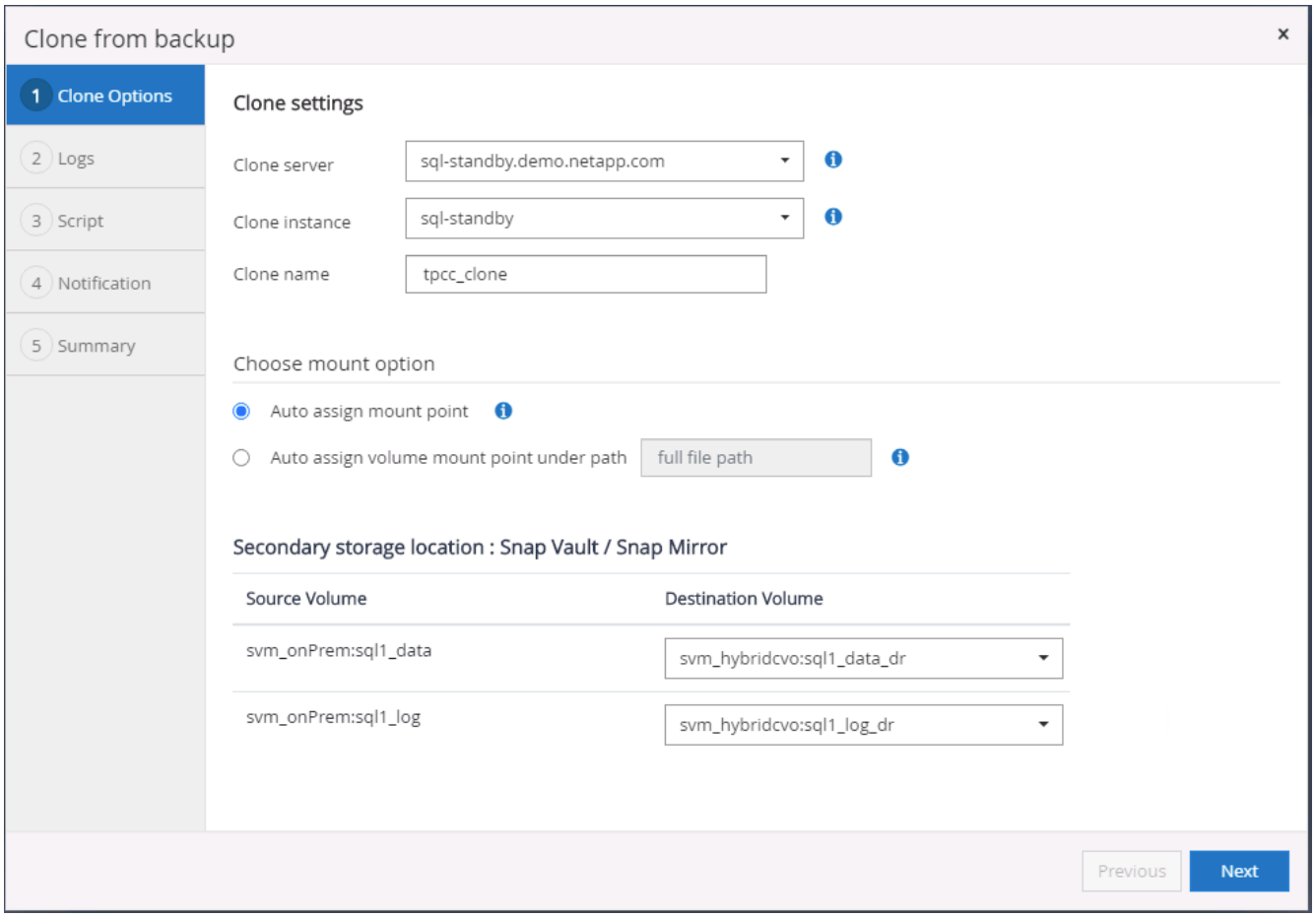


4. Scegli una copia di backup, quindi fai clic sul pulsante Clona per avviare il flusso di lavoro Clona da backup.

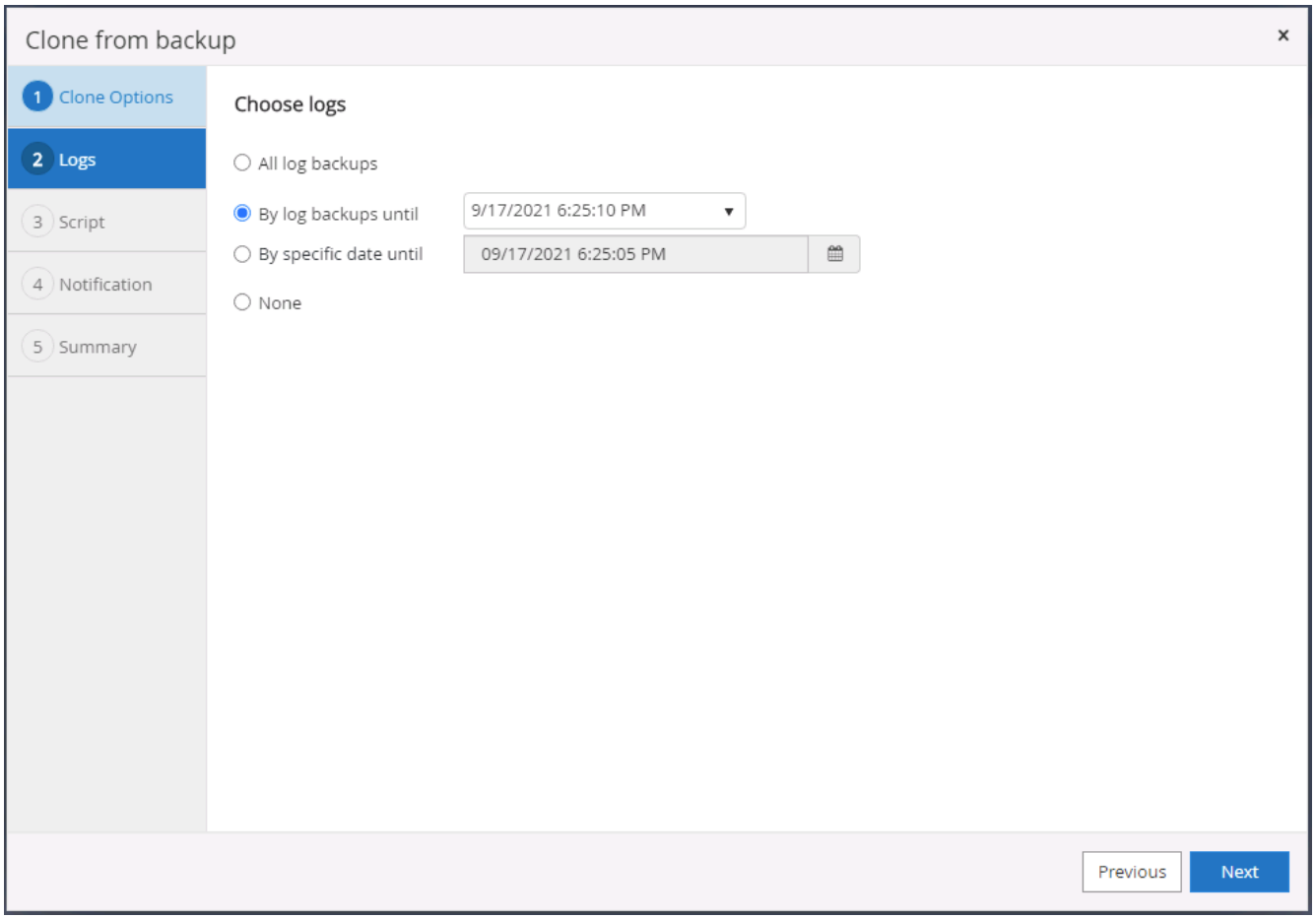




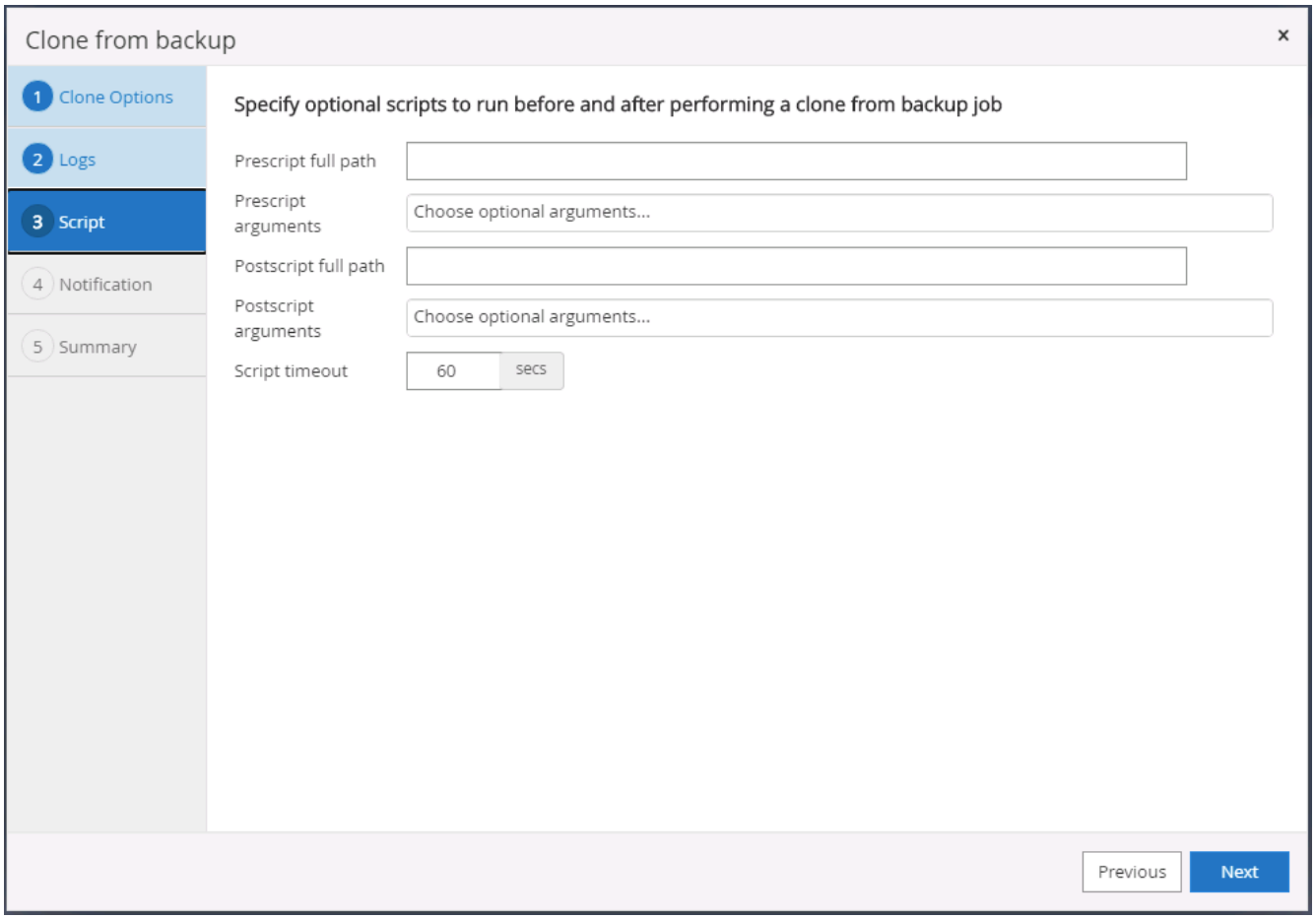
5. Selezionare un server cloud come server clone di destinazione, il nome dell'istanza clone e il nome del database clone. Scegliere un punto di montaggio assegnato automaticamente o un percorso di punto di montaggio definito dall'utente.



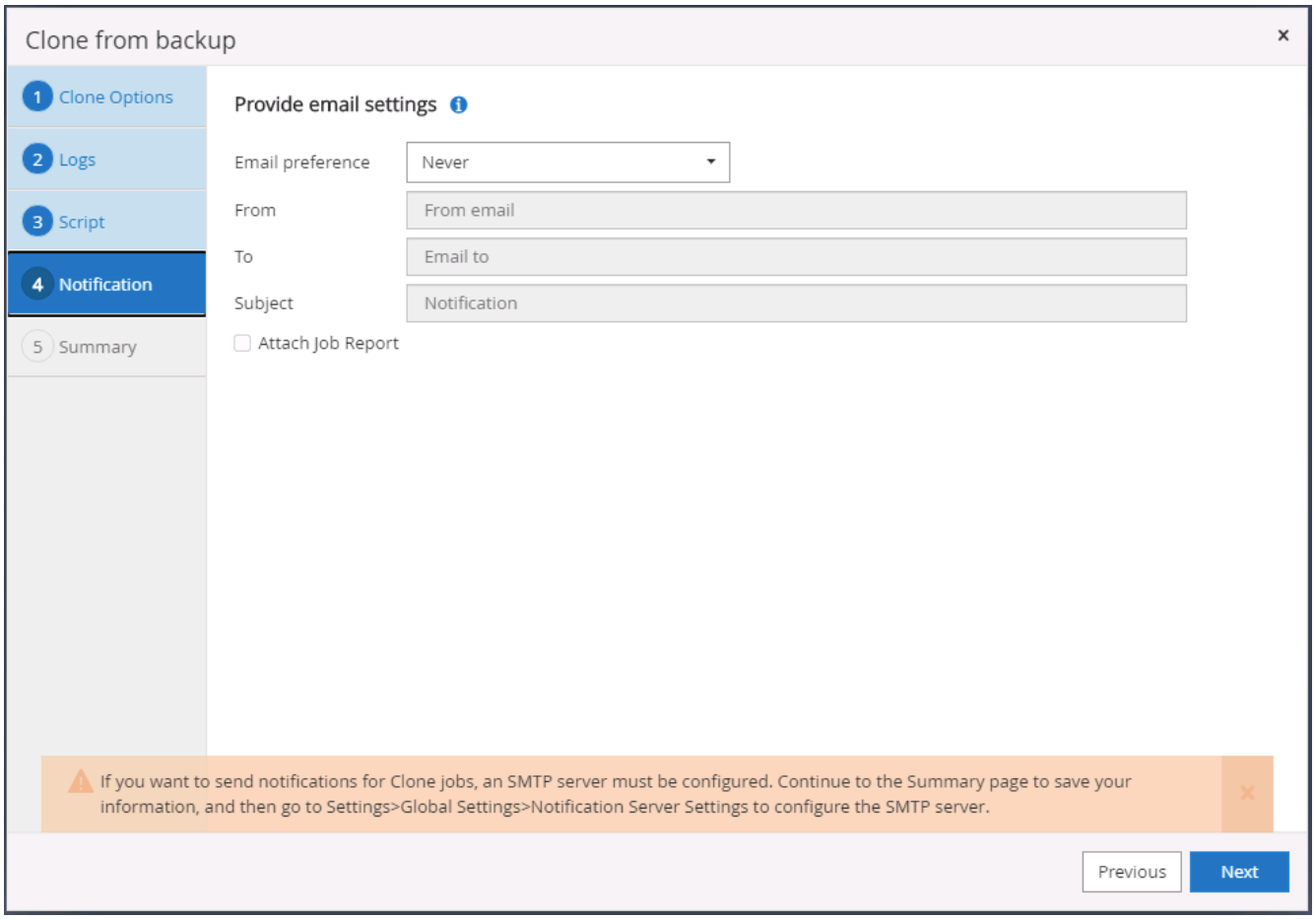
6. Determinare un punto di ripristino in base all'ora di backup del registro o in base a una data e un'ora specifiche.



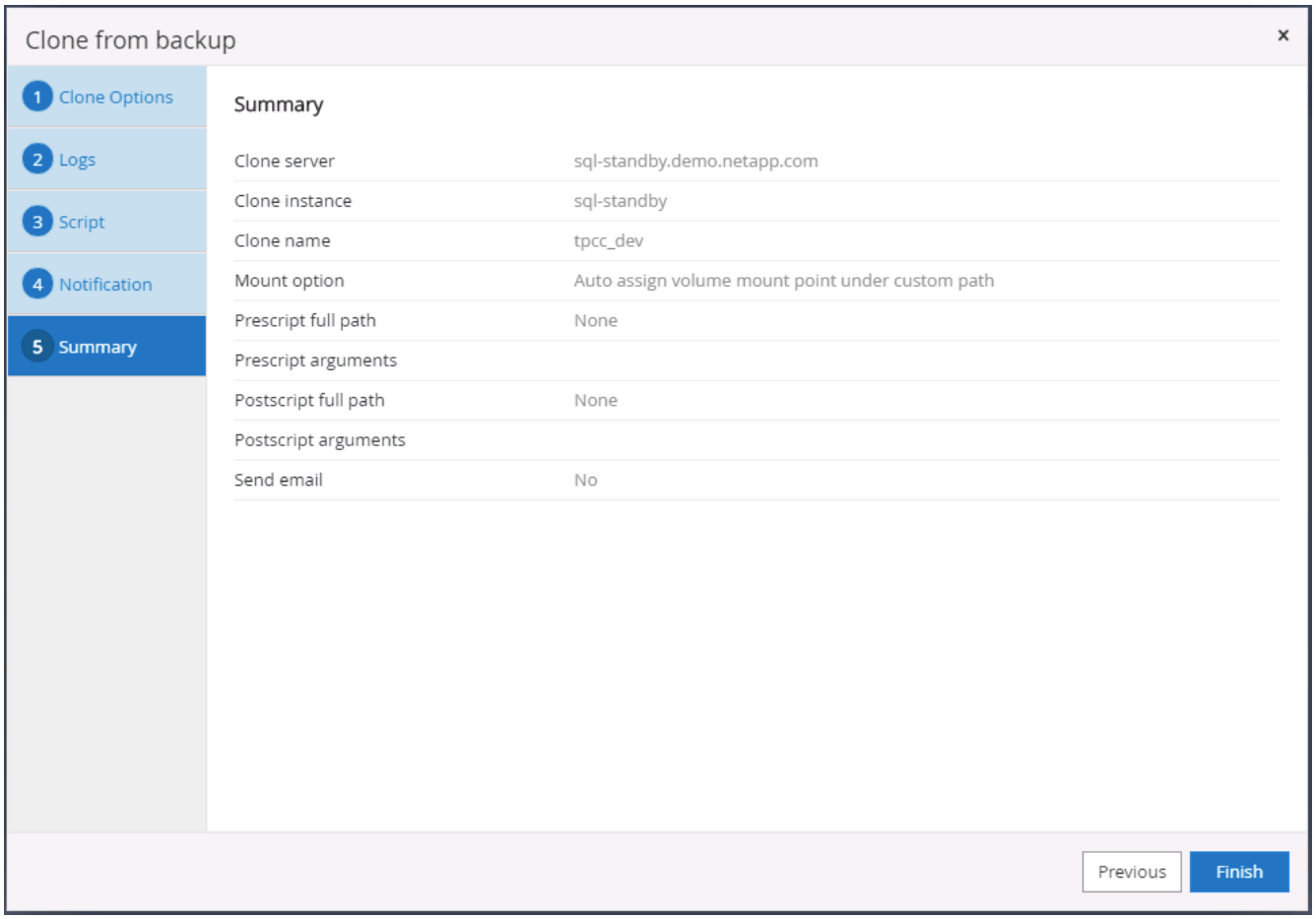
7. Specificare gli script facoltativi da eseguire prima e dopo l'operazione di clonazione.



8. Configurare un server SMTP se si desidera la notifica via e-mail.



9. Riepilogo del clone.



10. Monitorare lo stato del processo e verificare che il database utente previsto sia stato collegato a un'istanza SQL di destinazione nel server clone cloud.

Configurazione post-clone

1. Un database di produzione Oracle in locale viene solitamente eseguito in modalità di archiviazione dei log. Questa modalità non è necessaria per un database di sviluppo o di test. Per disattivare la modalità di archiviazione dei log, accedere al database Oracle come sysdba, eseguire un comando di modifica della modalità di log e avviare il database per l'accesso.
2. Configurare un listener Oracle oppure registrare il DB appena clonato con un listener esistente per l'accesso utente.
3. Per SQL Server, modificare la modalità di registrazione da Completa a Semplice in modo che il file di registro di sviluppo/test di SQL Server possa essere facilmente ridotto quando riempie il volume di registro.

Aggiorna il database clone

1. Eliminare i database clonati e ripulire l'ambiente del server DB cloud. Quindi seguire le procedure precedenti per clonare un nuovo DB con dati aggiornati. Per clonare un nuovo database bastano pochi minuti.
2. Arrestare il database clone, eseguire un comando di aggiornamento clone tramite la CLI. Per maggiori dettagli, consultare la seguente documentazione SnapCenter :"Aggiorna un clone" .

Dove rivolgersi per chiedere aiuto?

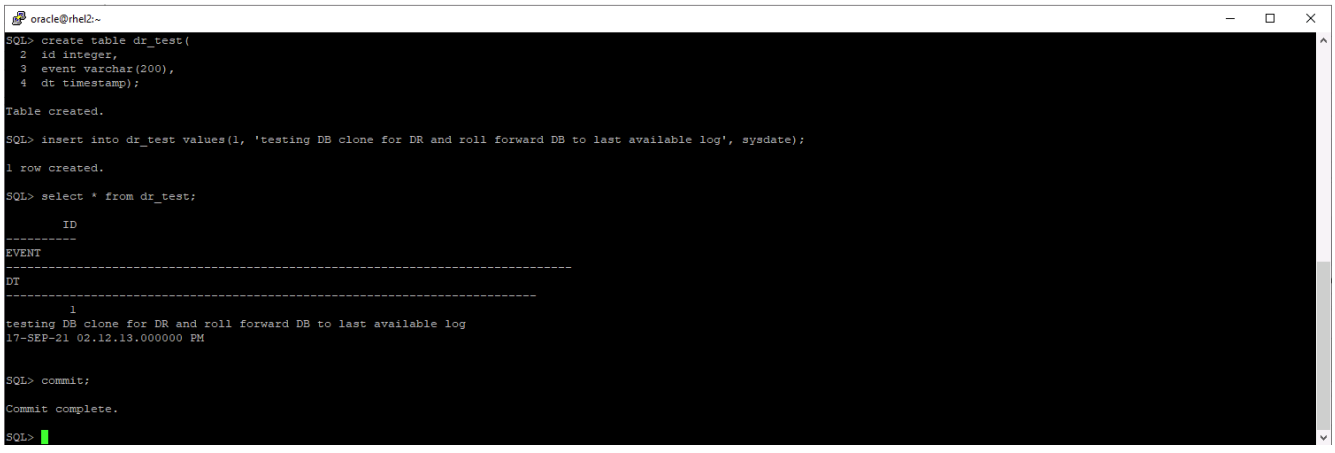
Se hai bisogno di aiuto con questa soluzione e casi d'uso, unisciti a"Canale Slack di supporto della community NetApp Solution Automation" e cerca il canale solution-automation per pubblicare le tue domande o richieste.

Flusso di lavoro di ripristino di emergenza

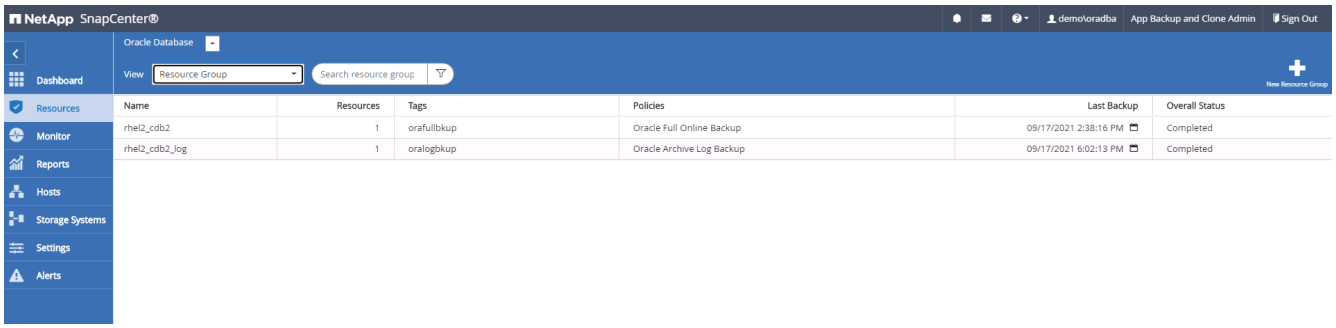
Le aziende hanno adottato il cloud pubblico come risorsa e destinazione valida per il disaster recovery. SnapCenter rende questo processo il più fluido possibile. Questo flusso di lavoro di disaster recovery è molto simile al flusso di lavoro di clonazione, ma il ripristino del database viene eseguito tramite l'ultimo registro disponibile che è stato replicato sul cloud per recuperare tutte le transazioni aziendali possibili. Tuttavia, per il disaster recovery sono previsti ulteriori passaggi di pre-configurazione e post-configurazione.

Clona un database di produzione Oracle locale sul cloud per il DR

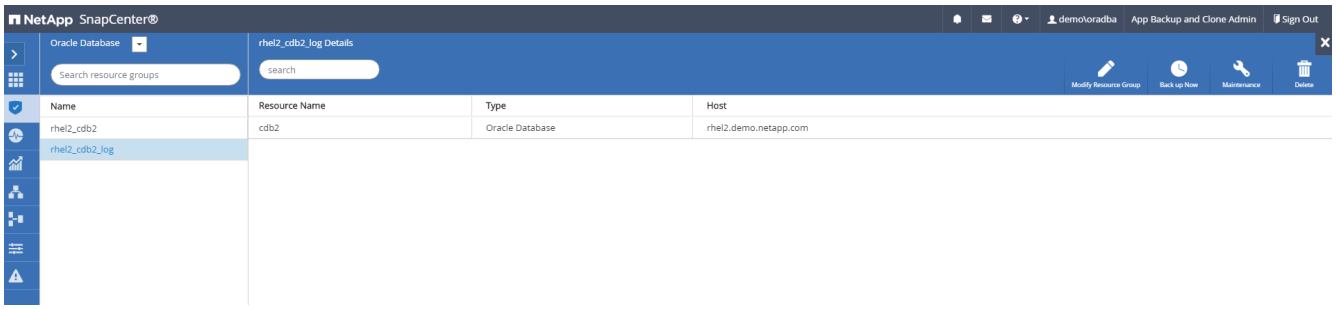
1. Per verificare che il ripristino del clone venga eseguito tramite l'ultimo registro disponibile, abbiamo creato una piccola tabella di prova e inserito una riga. I dati di prova verrebbero recuperati dopo un ripristino completo dell'ultimo registro disponibile.

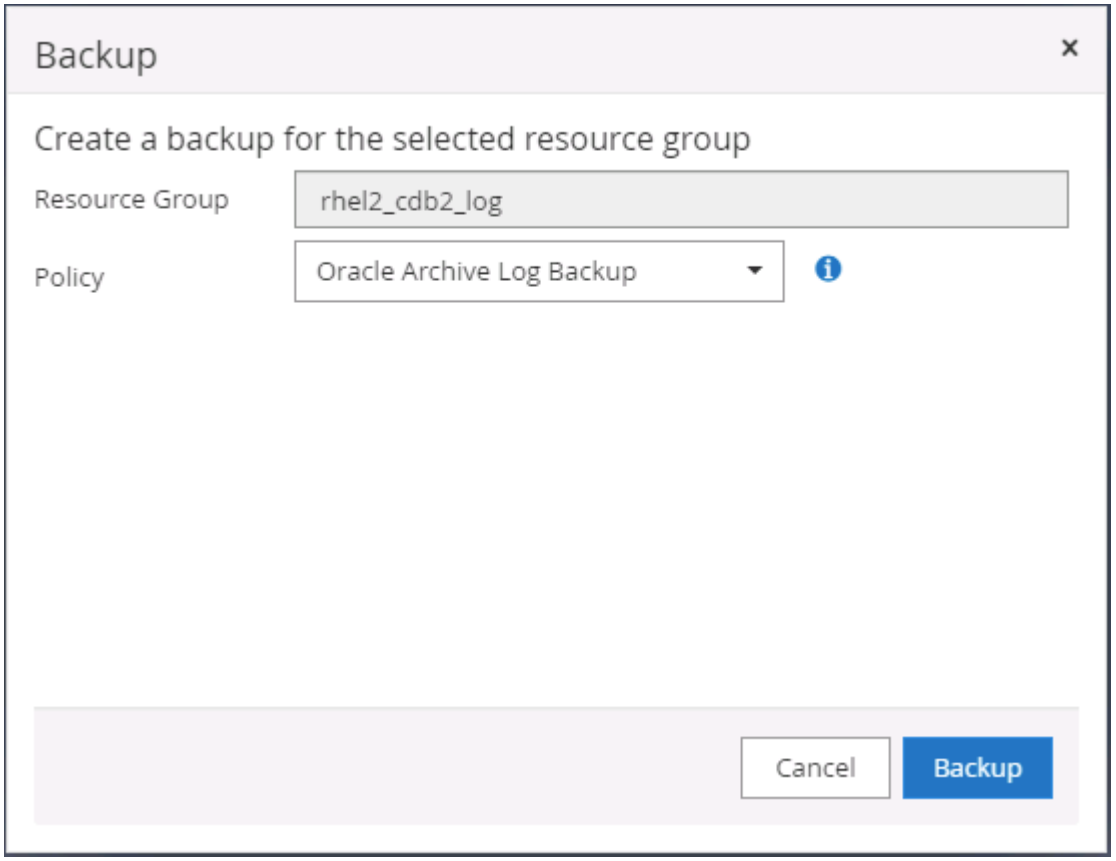


2. Accedi a SnapCenter come ID utente di gestione del database per Oracle. Passare alla scheda Risorse, che mostra i database Oracle protetti da SnapCenter.



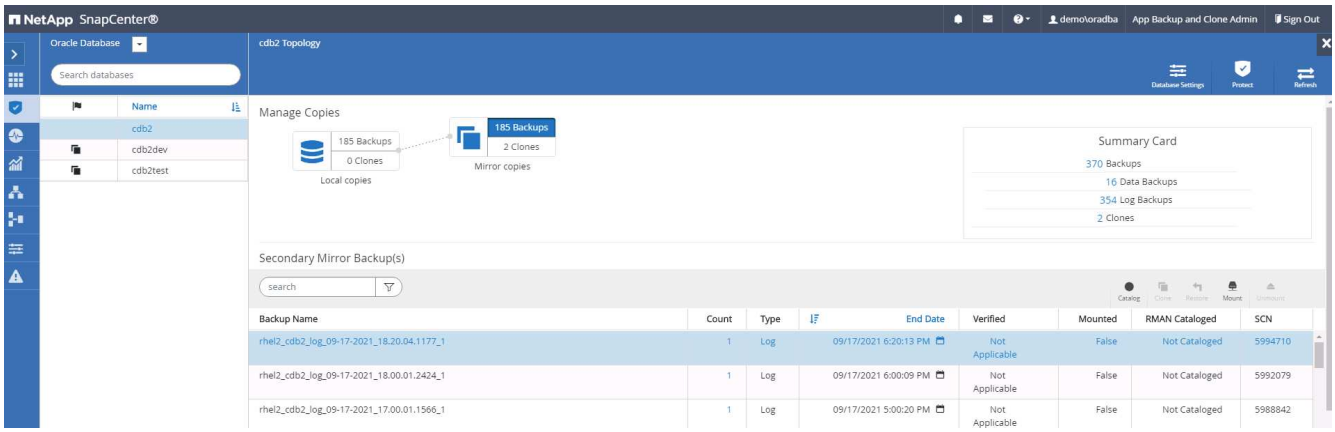
3. Selezionare il gruppo di risorse del registro Oracle e fare clic su Esegui backup ora per eseguire manualmente un backup del registro Oracle per scaricare l'ultima transazione nella destinazione nel cloud. In uno scenario DR reale, l'ultima transazione recuperabile dipende dalla frequenza di replicazione del volume del registro del database sul cloud, che a sua volta dipende dalla politica RTO o RPO dell'azienda.

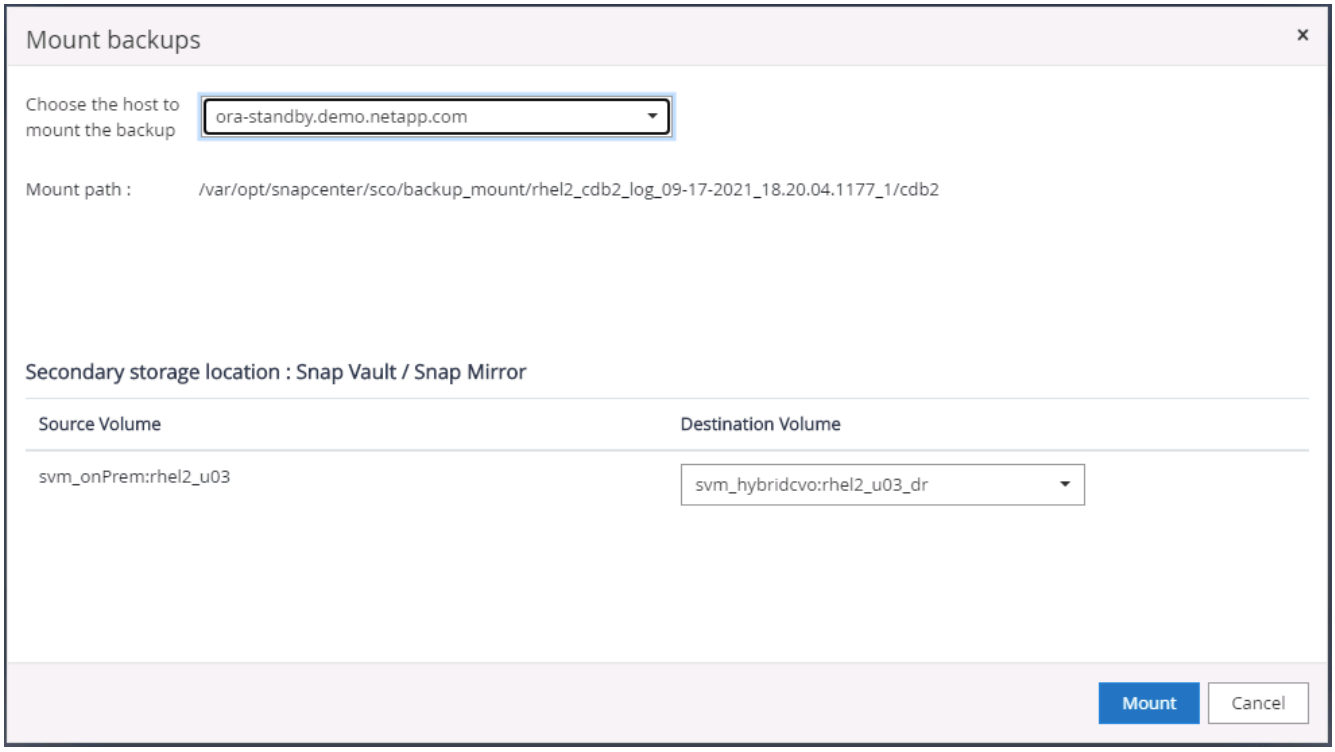




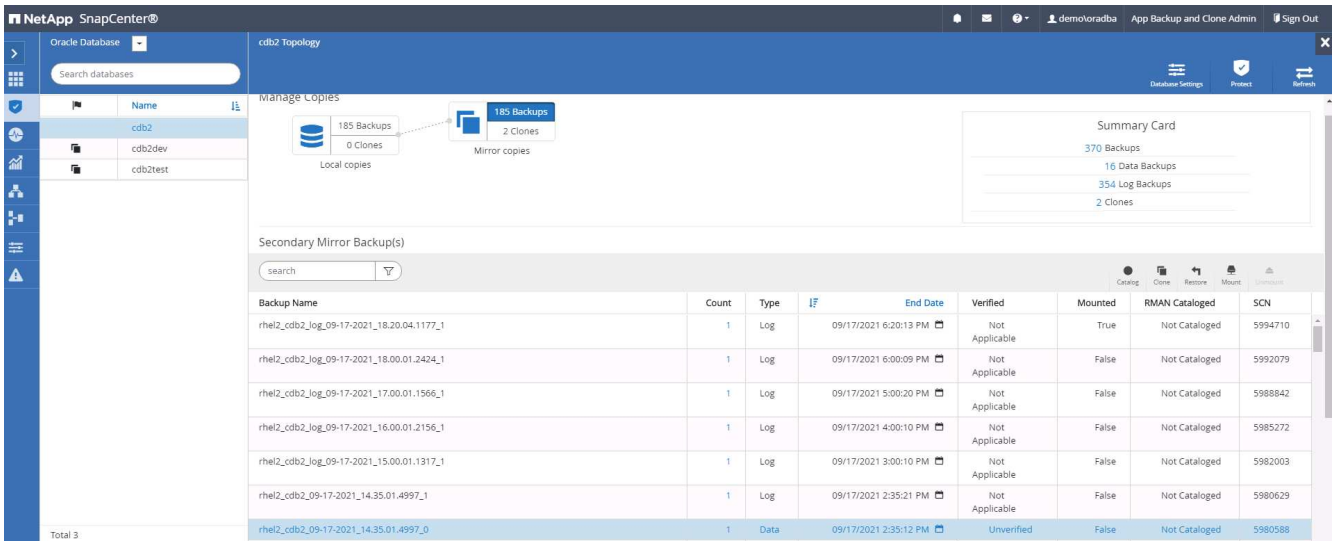
SnapMirror asincrono perde i dati che non sono arrivati alla destinazione cloud nell'intervallo di backup del registro del database in uno scenario di ripristino di emergenza. Per ridurre al minimo la perdita di dati, è possibile pianificare backup del registro più frequenti. Tuttavia, esiste un limite alla frequenza di backup del registro tecnicamente realizzabile.

4. Selezionare l'ultimo backup del log sul/sui backup mirror secondario/i e montare il backup del log.

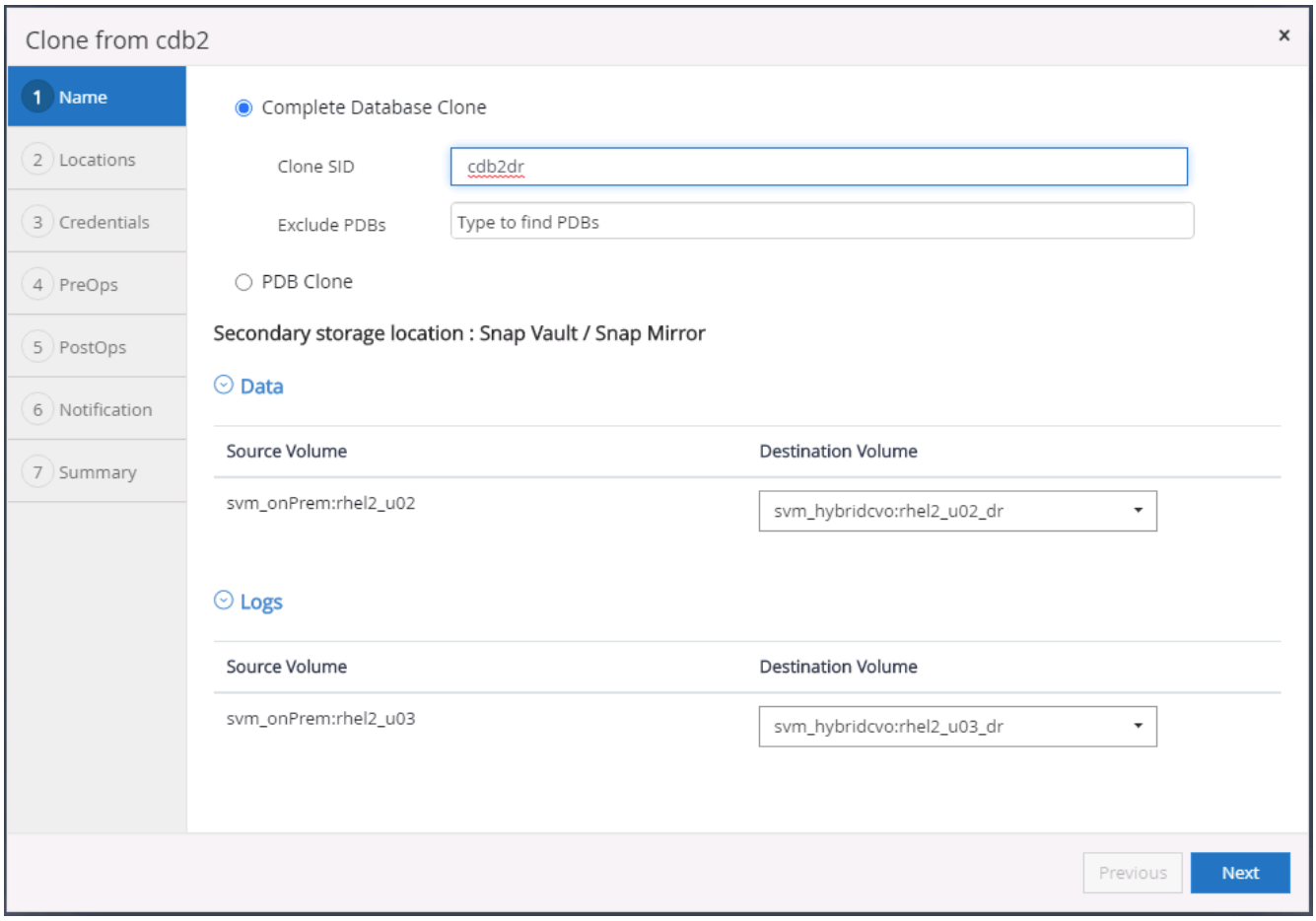




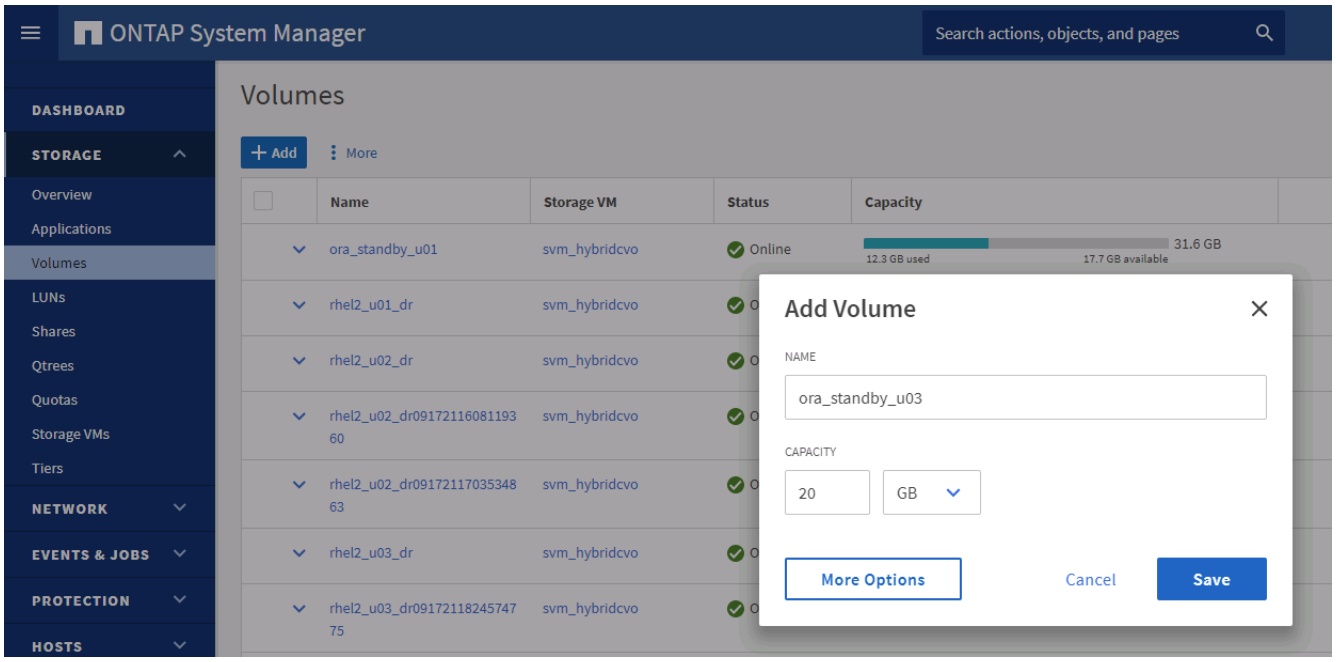
5. Selezionare l'ultimo backup completo del database e fare clic su Clona per avviare il flusso di lavoro di clonazione.

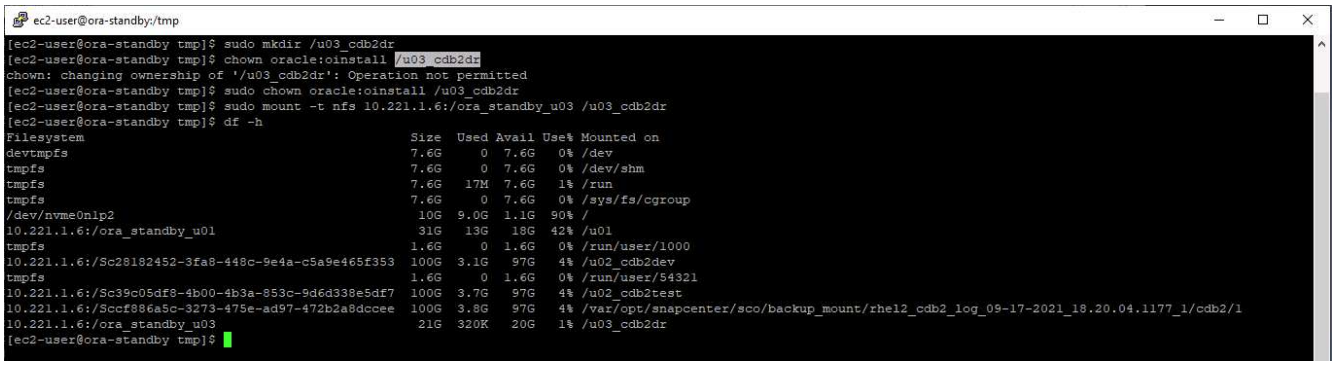


6. Selezionare un ID DB clone univoco sull'host.



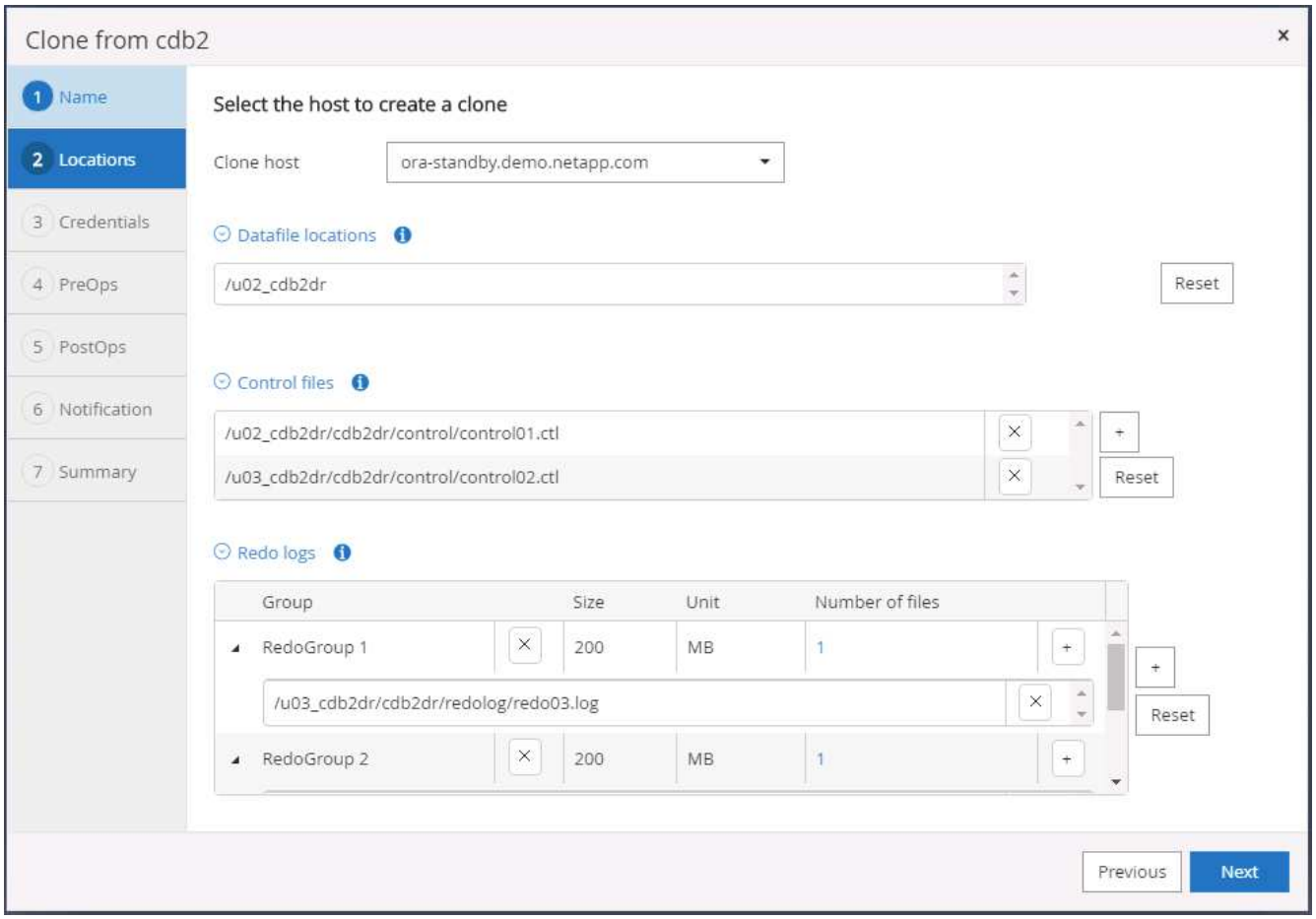
7. Fornire un volume di registro e montarlo sul server DR di destinazione per l'area di ripristino flash Oracle e i registri online.



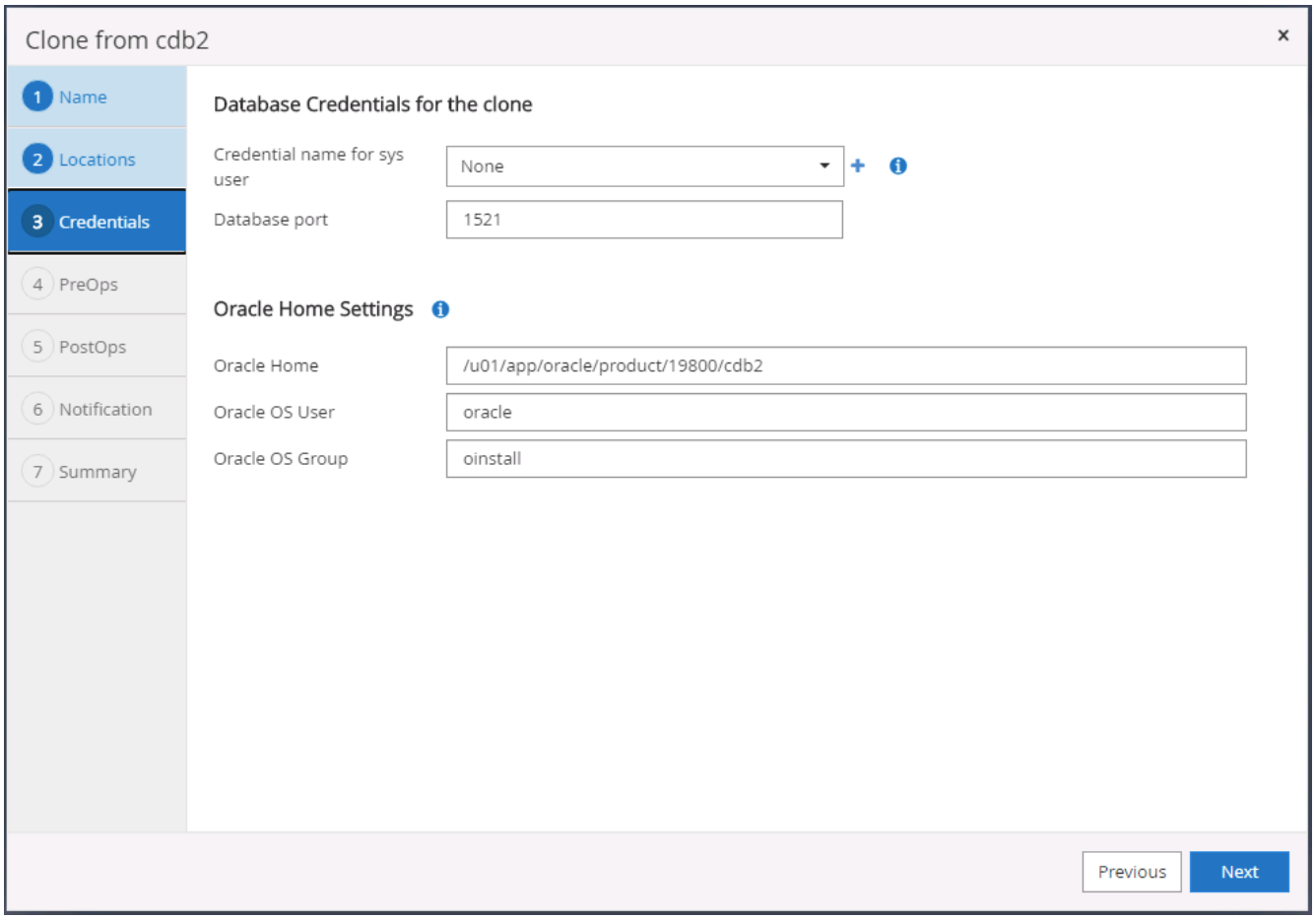


La procedura di clonazione di Oracle non crea un volume di registro, che deve essere predisposto sul server DR prima della clonazione.

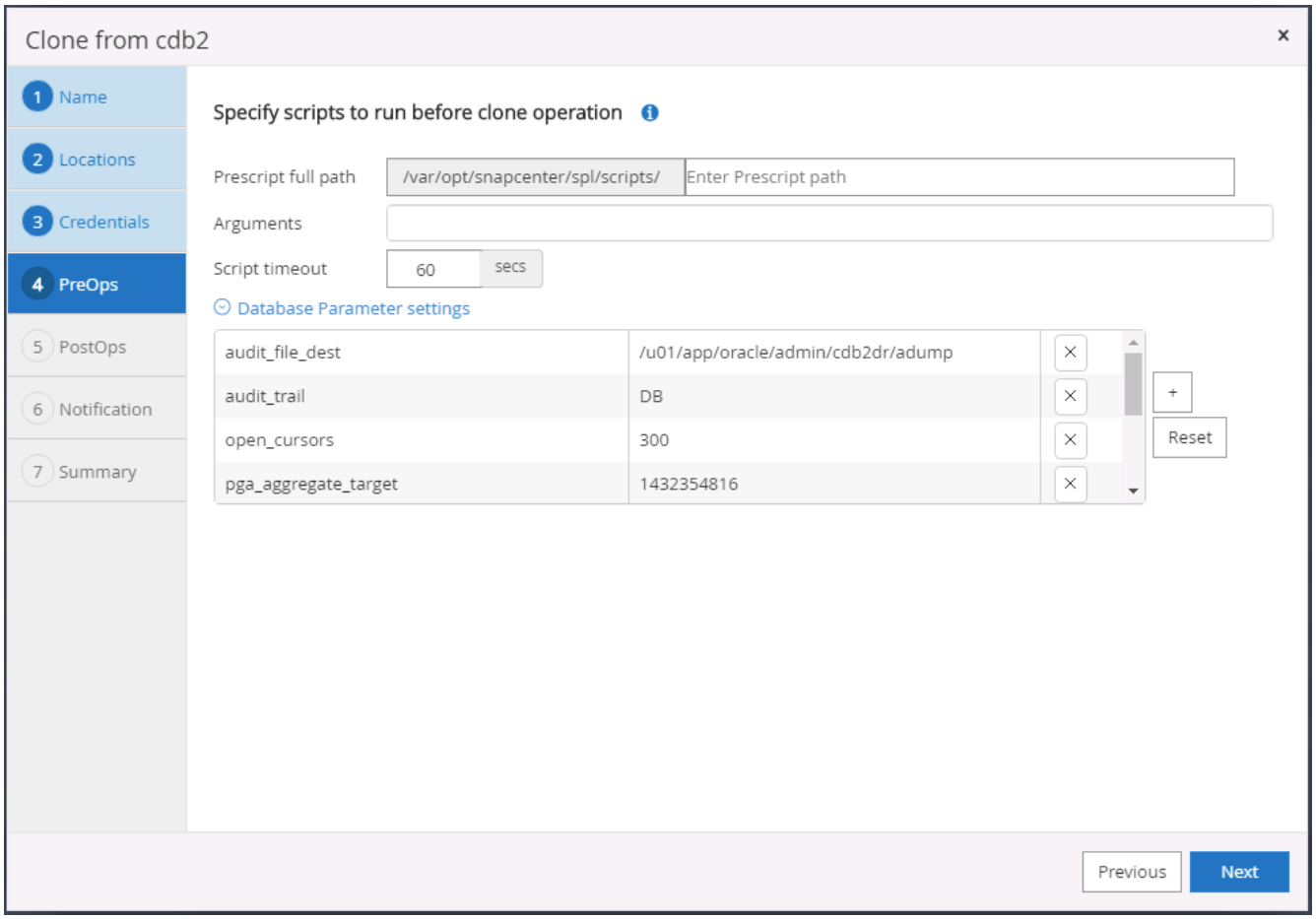
8. Selezionare l'host clone di destinazione e la posizione in cui posizionare i file di dati, i file di controllo e i redo log.



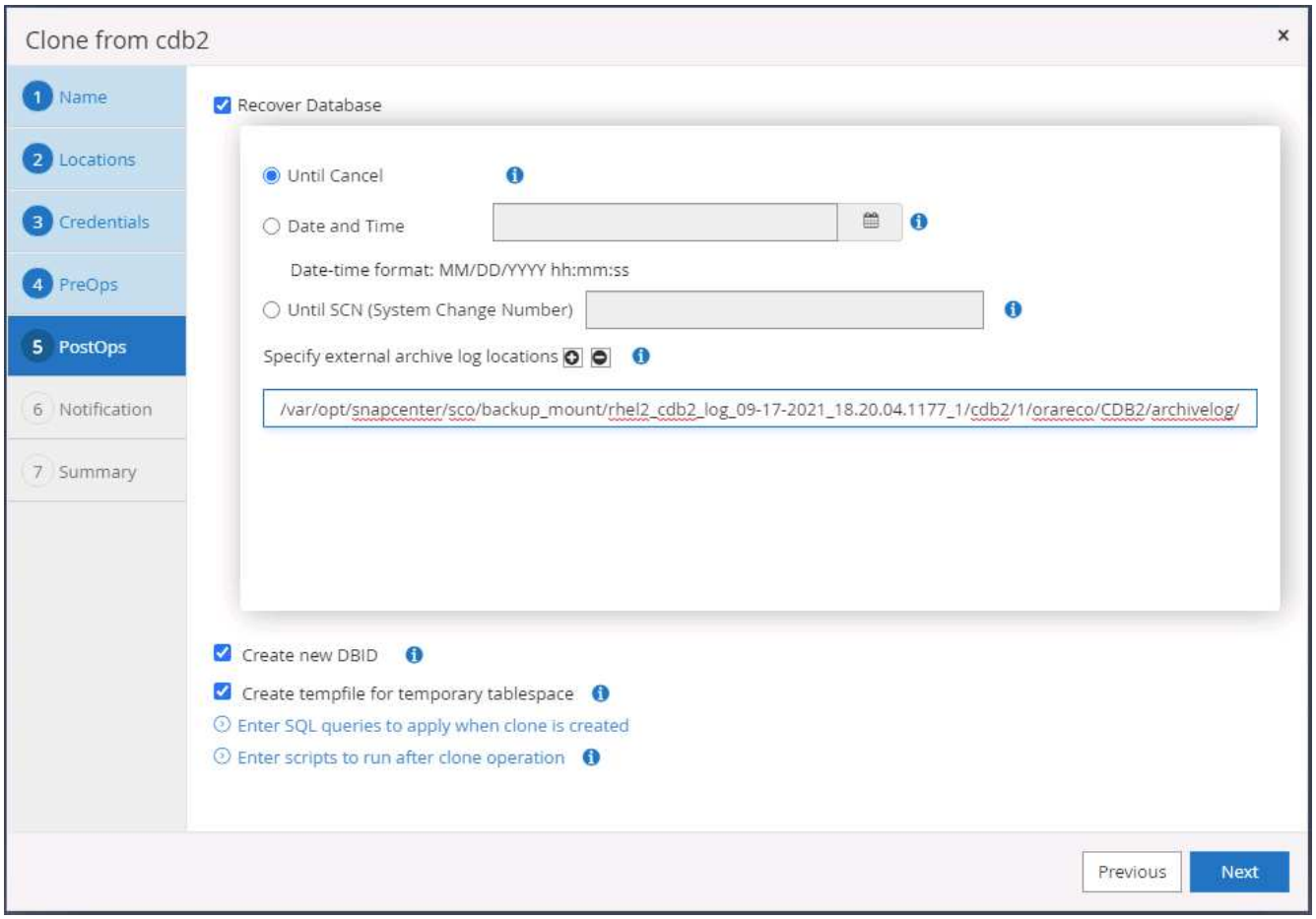
9. Selezionare le credenziali per il clone. Compilare i dettagli della configurazione Oracle home sul server di destinazione.



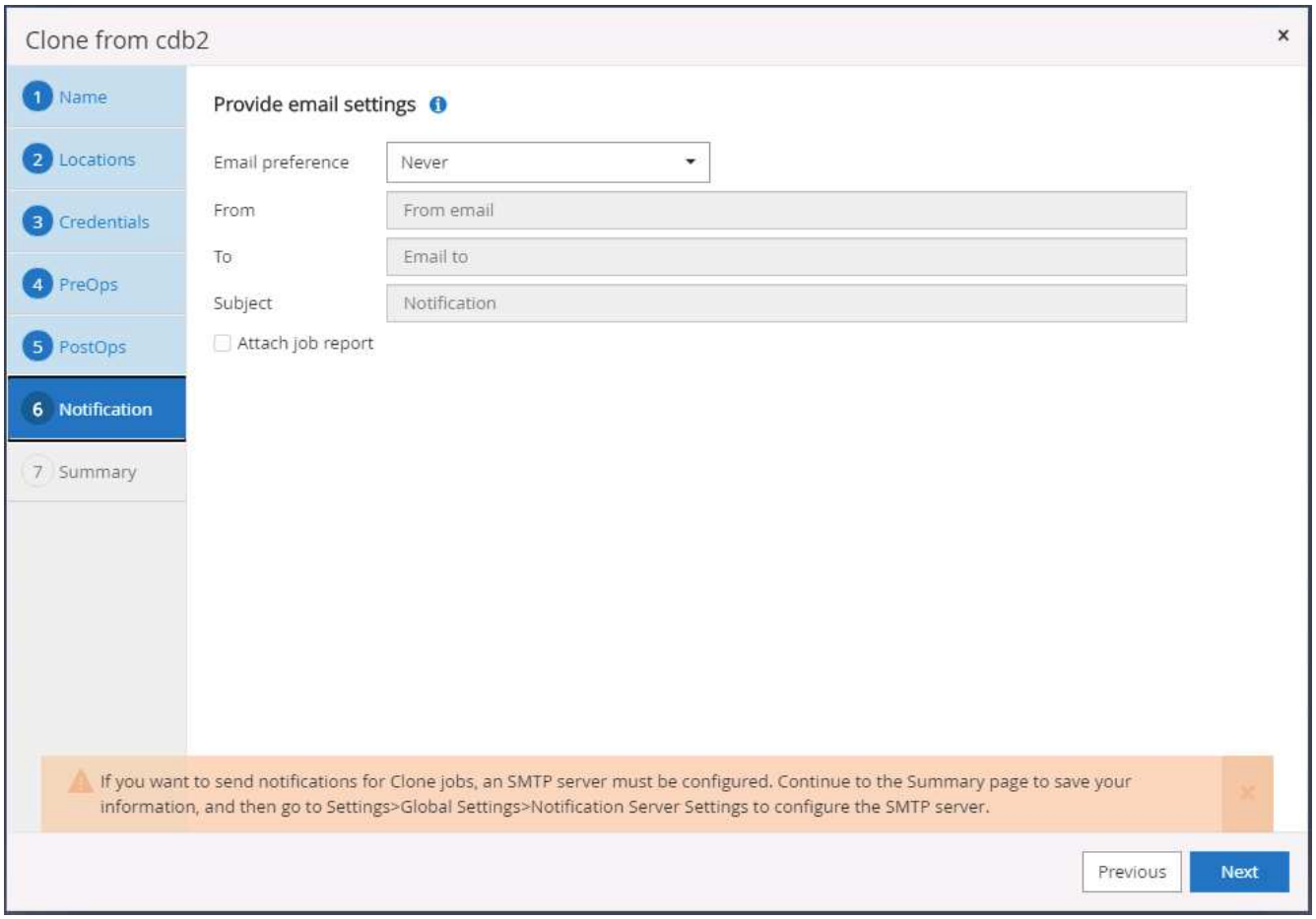
10. Specificare gli script da eseguire prima della clonazione. Se necessario, è possibile modificare i parametri del database.



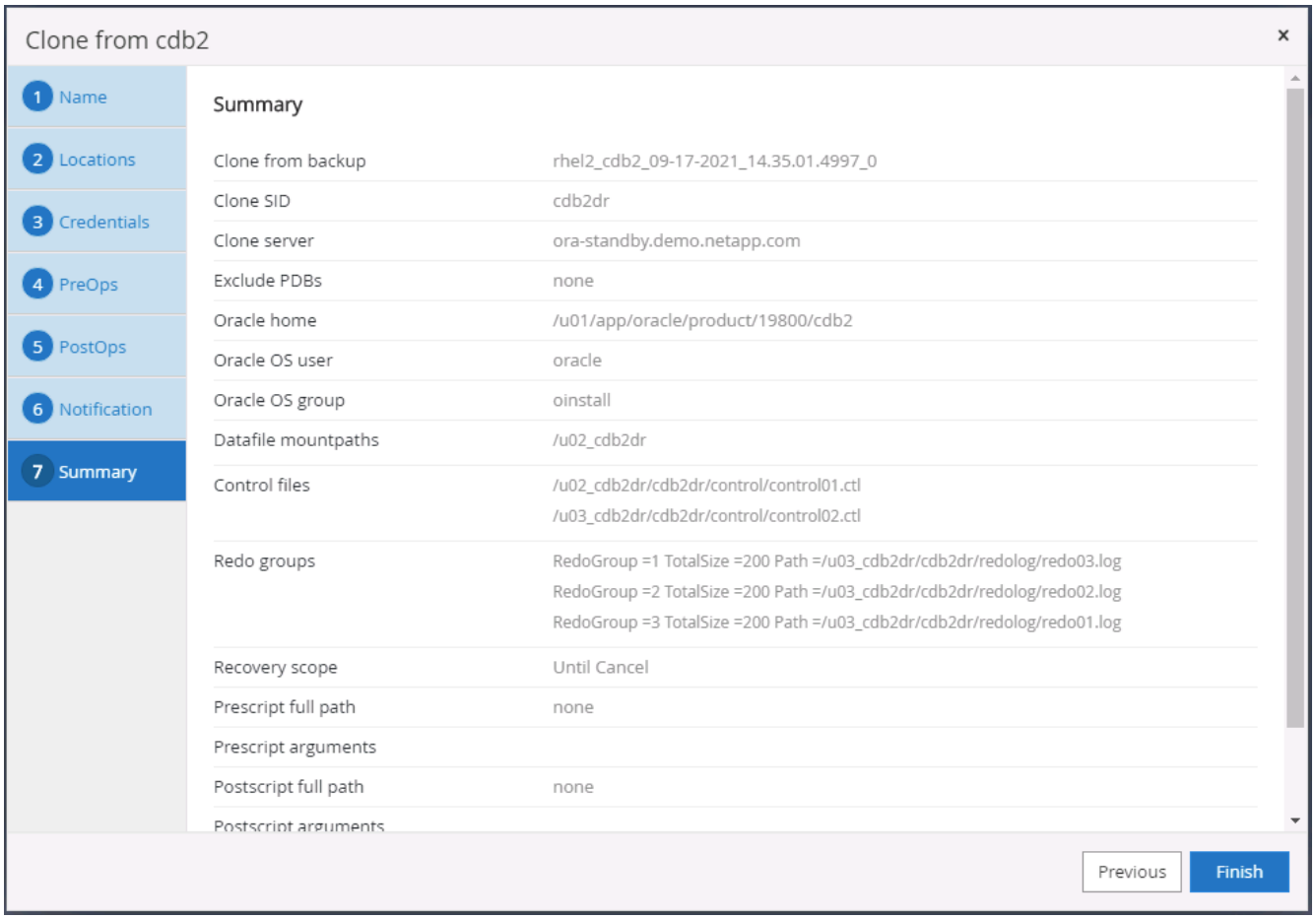
11. Selezionare Fino all'annullamento come opzione di ripristino in modo che il ripristino venga eseguito attraverso tutti i registri di archivio disponibili per recuperare l'ultima transazione replicata nella posizione cloud secondaria.



12. Se necessario, configurare il server SMTP per la notifica via e-mail.



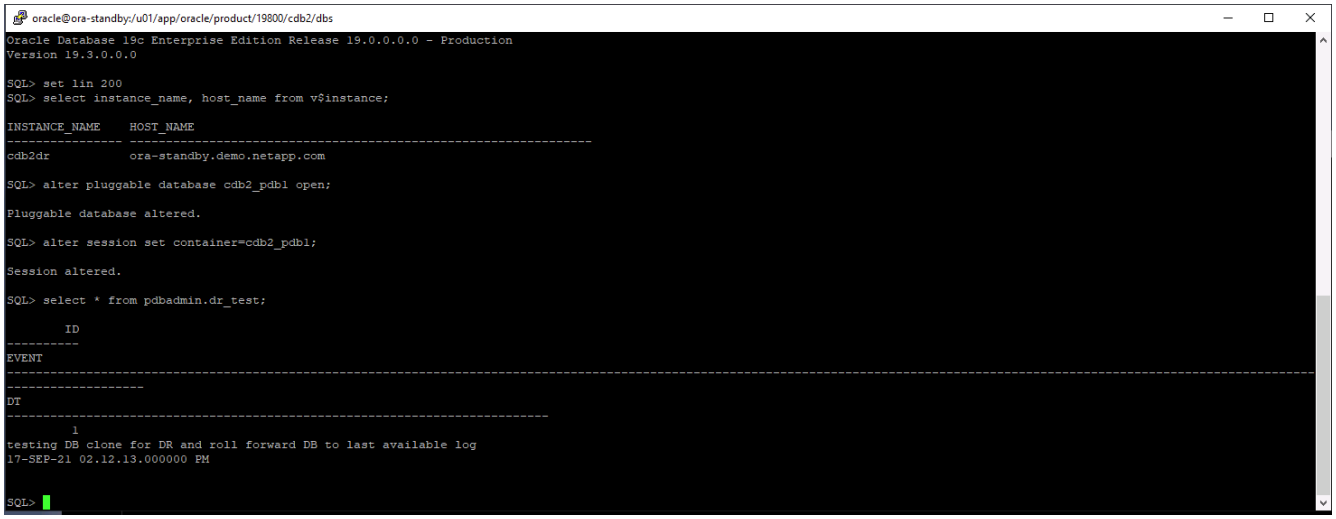
13. Riepilogo del clone DR.



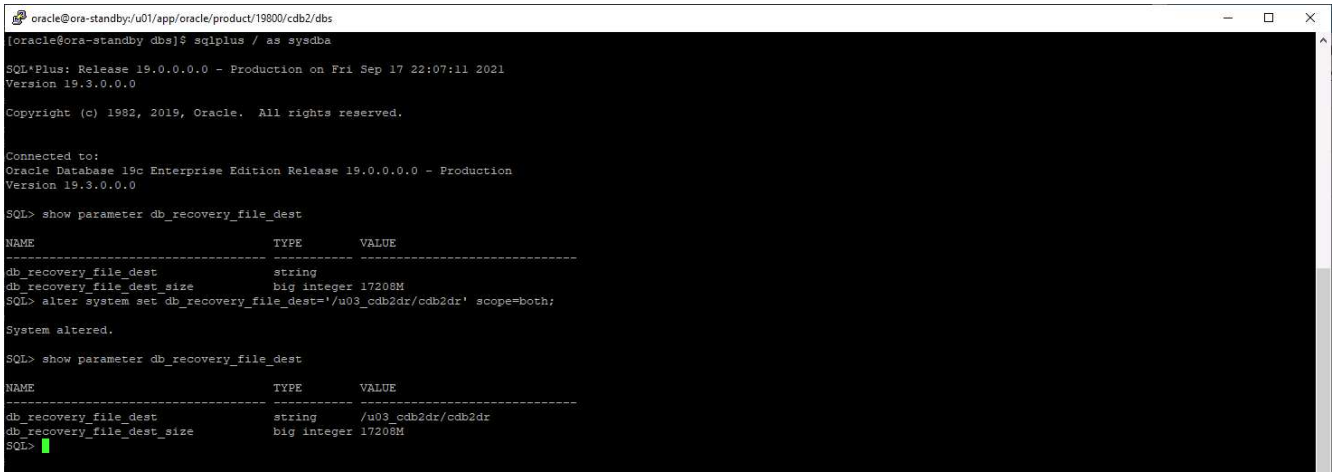
14. I DB clonati vengono registrati con SnapCenter subito dopo il completamento della clonazione e sono quindi disponibili per la protezione tramite backup.

Convalida e configurazione del clone post-DR per Oracle

1. Convalida l'ultima transazione di prova che è stata svuotata, replicata e ripristinata nella posizione DR nel cloud.



2. Configurare l'area di ripristino flash.

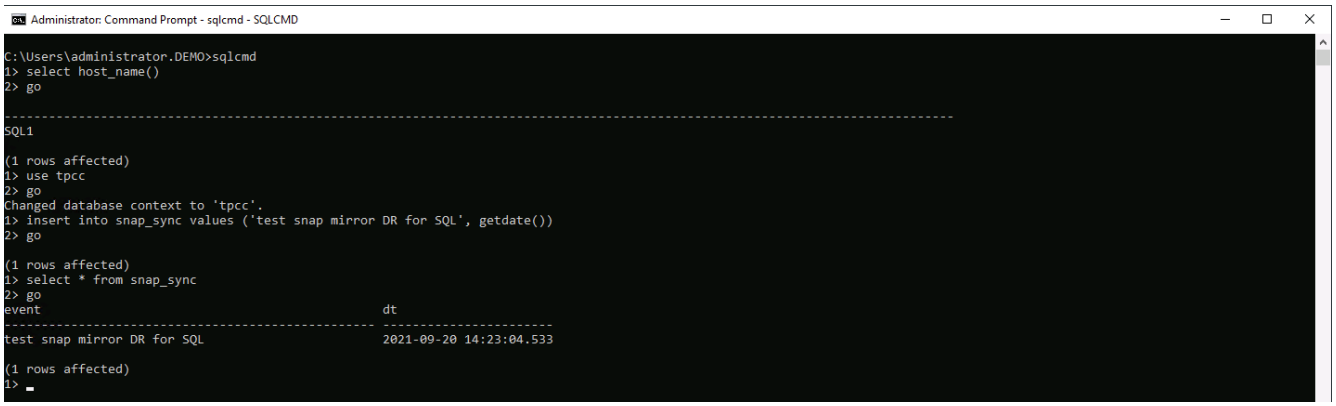


3. Configurare l'ascoltatore Oracle per l'accesso utente.
4. Dividere il volume clonato dal volume sorgente replicato.
5. Replica inversa dal cloud all'ambiente locale e ricostruzione del server di database locale non funzionante.

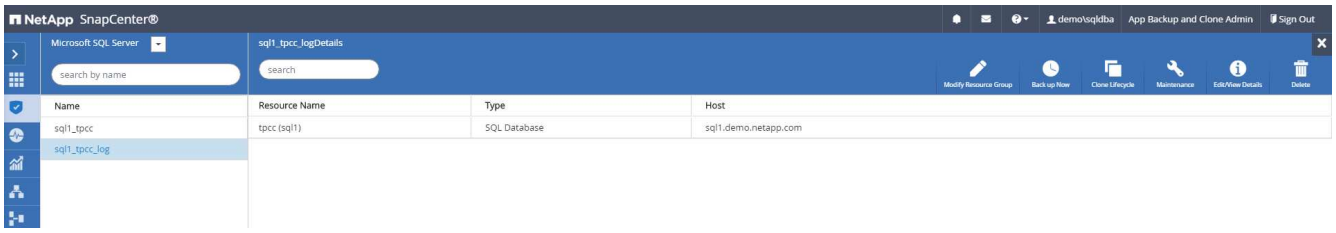
> La suddivisione dei cloni può comportare un utilizzo temporaneo dello spazio di archiviazione molto più elevato rispetto al normale funzionamento. Tuttavia, dopo aver ricostruito il server DB locale, è possibile liberare spazio extra.

Clona un database di produzione SQL locale sul cloud per il ripristino di emergenza

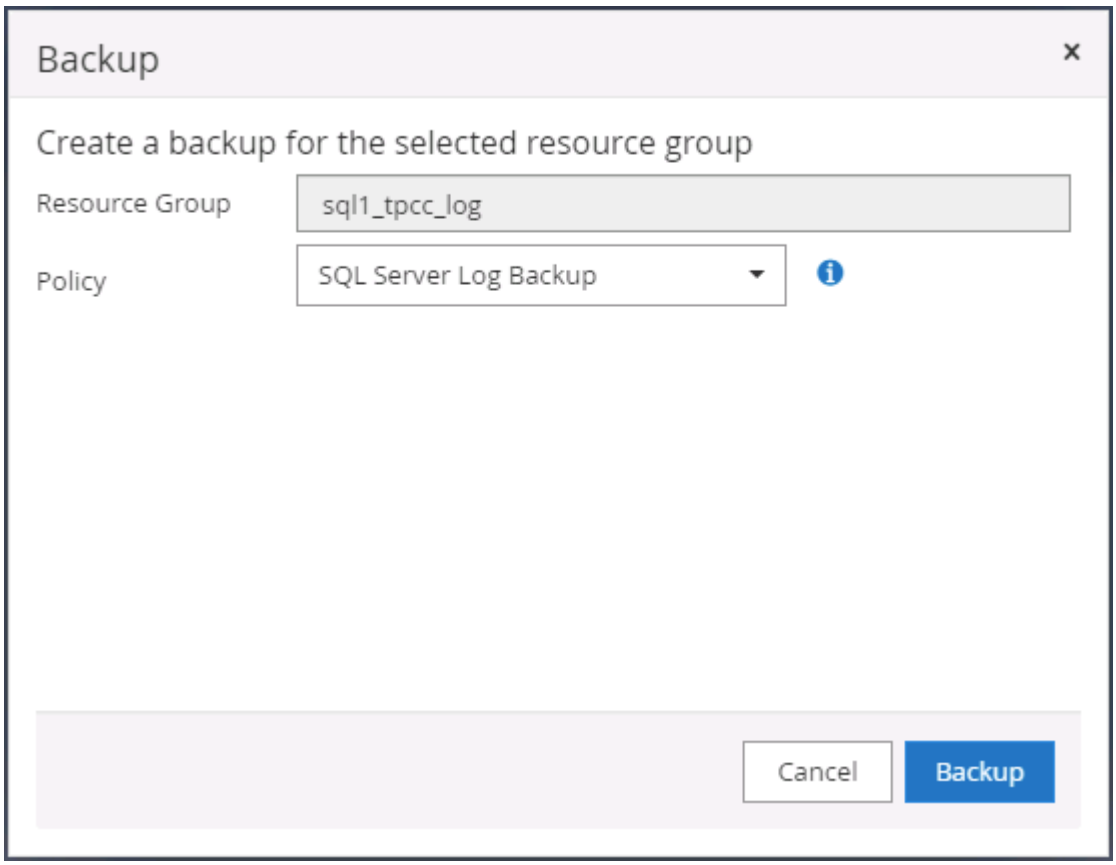
1. Allo stesso modo, per convalidare che il ripristino del clone SQL fosse stato eseguito tramite l'ultimo log disponibile, abbiamo creato una piccola tabella di prova e inserito una riga. I dati di prova verrebbero recuperati dopo un ripristino completo dell'ultimo registro disponibile.



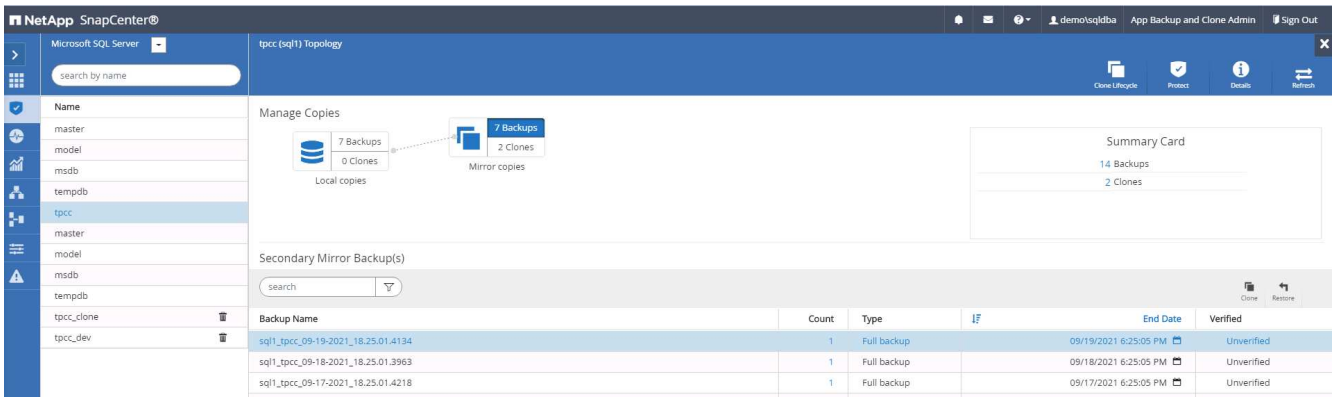
2. Accedi a SnapCenter con un ID utente di gestione del database per SQL Server. Passare alla scheda Risorse, che mostra il gruppo di risorse di protezione di SQL Server.



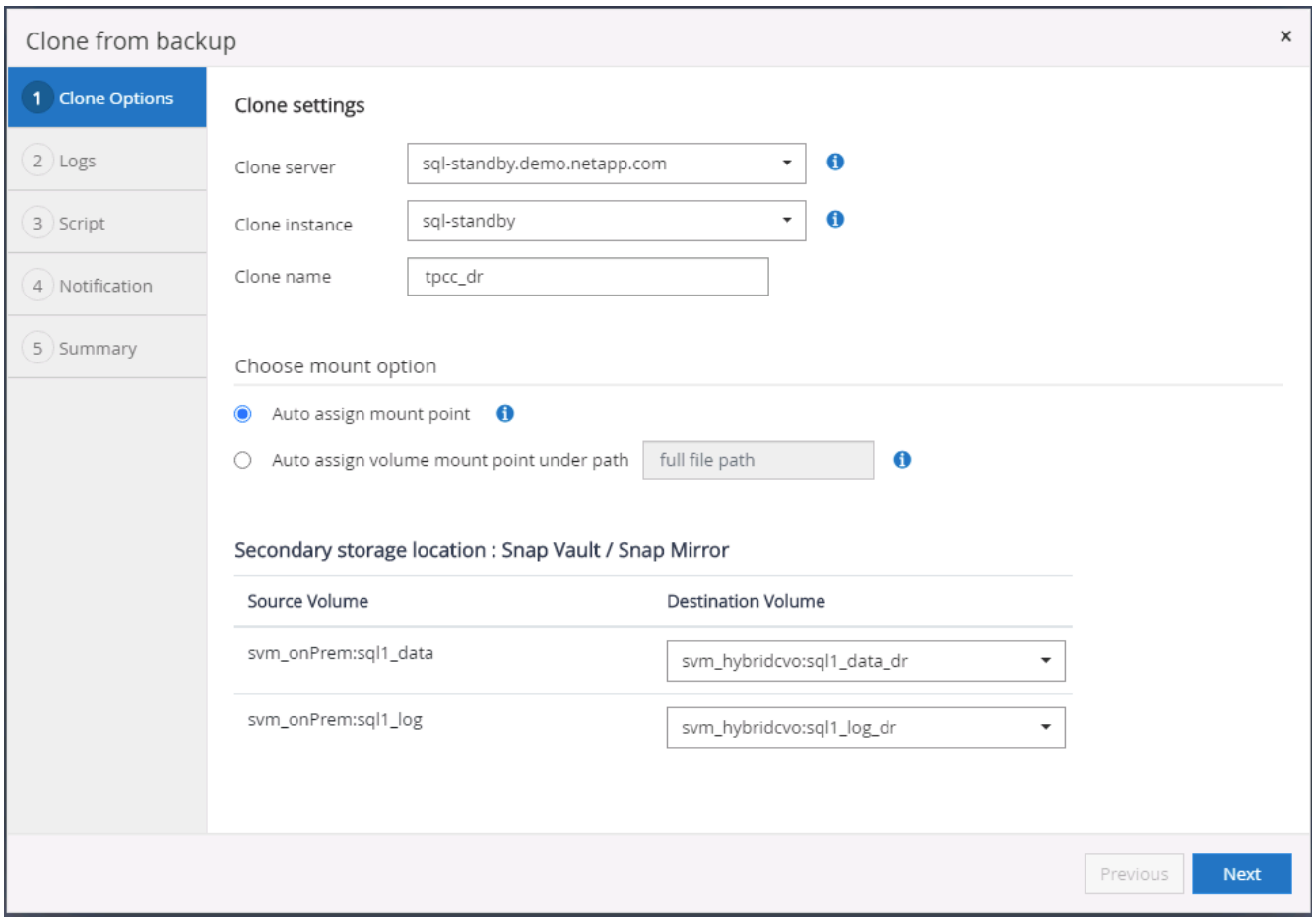
3. Eseguire manualmente un backup del registro per eliminare l'ultima transazione da replicare nell'archivio secondario nel cloud pubblico.



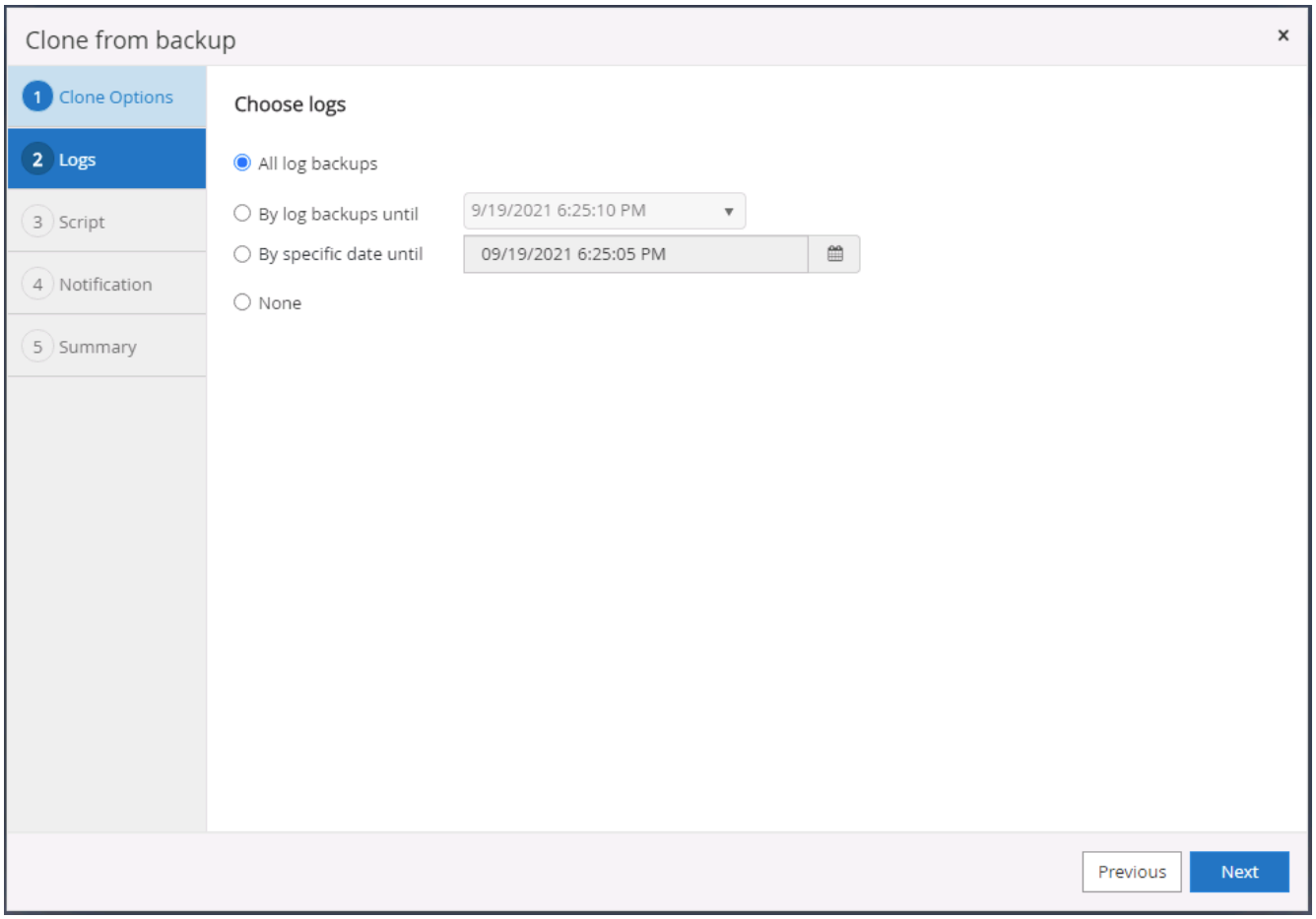
4. Selezionare l'ultimo backup completo di SQL Server per il clone.



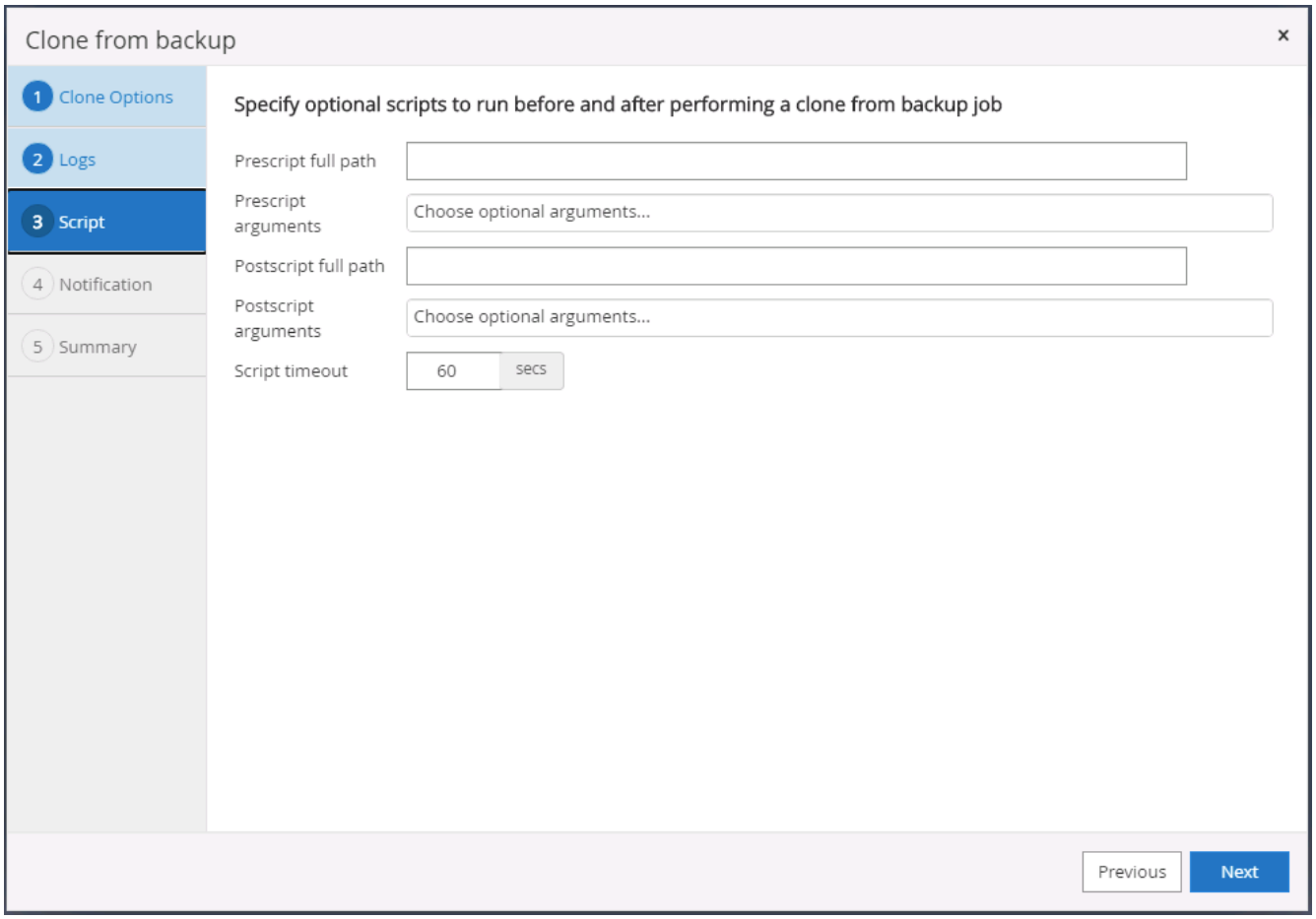
5. Imposta le impostazioni di clonazione, come il server di clonazione, l'istanza di clonazione, il nome di clonazione e l'opzione di montaggio. La posizione di archiviazione secondaria in cui viene eseguita la clonazione viene popolata automaticamente.



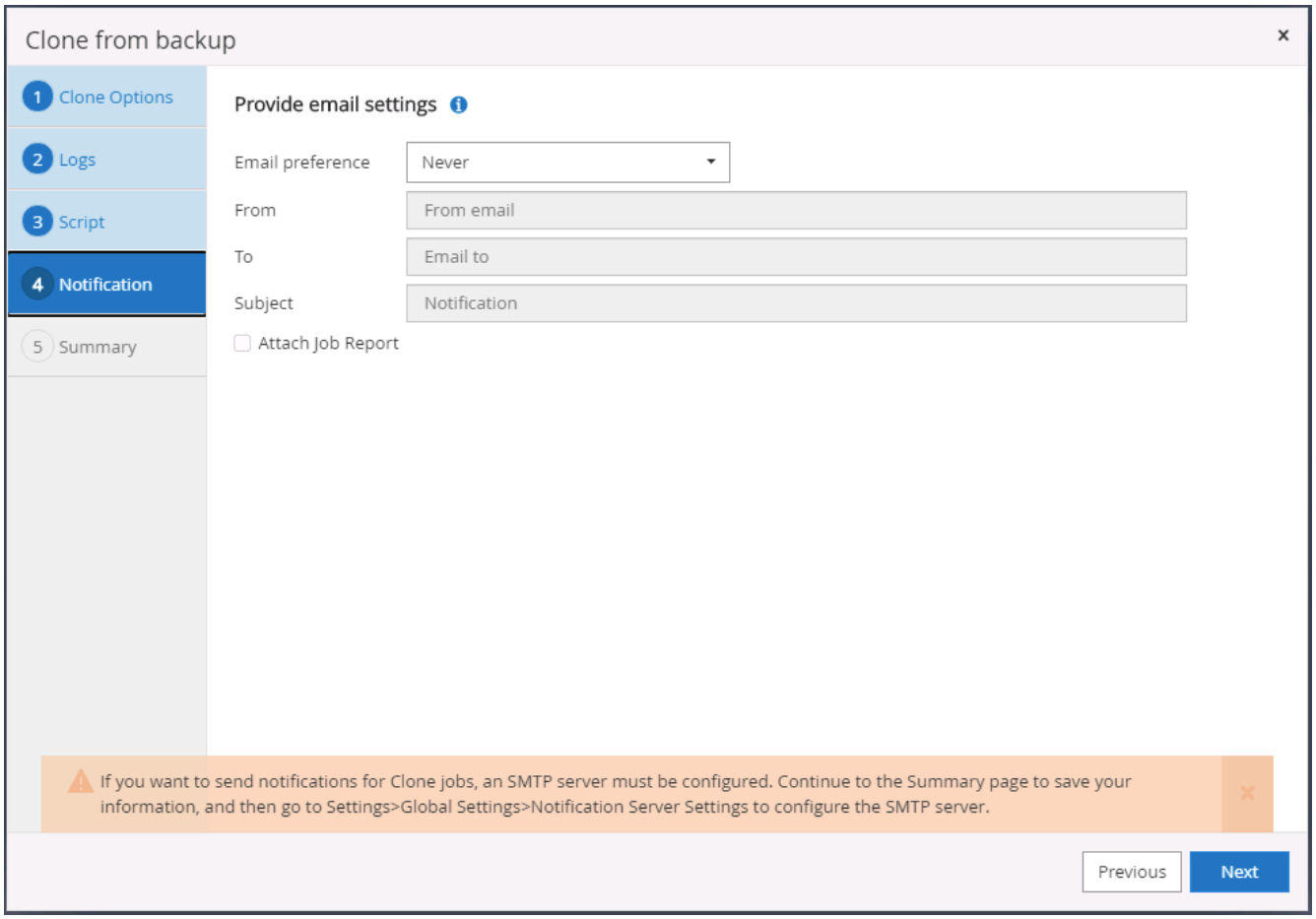
6. Seleziona tutti i backup del registro da applicare.



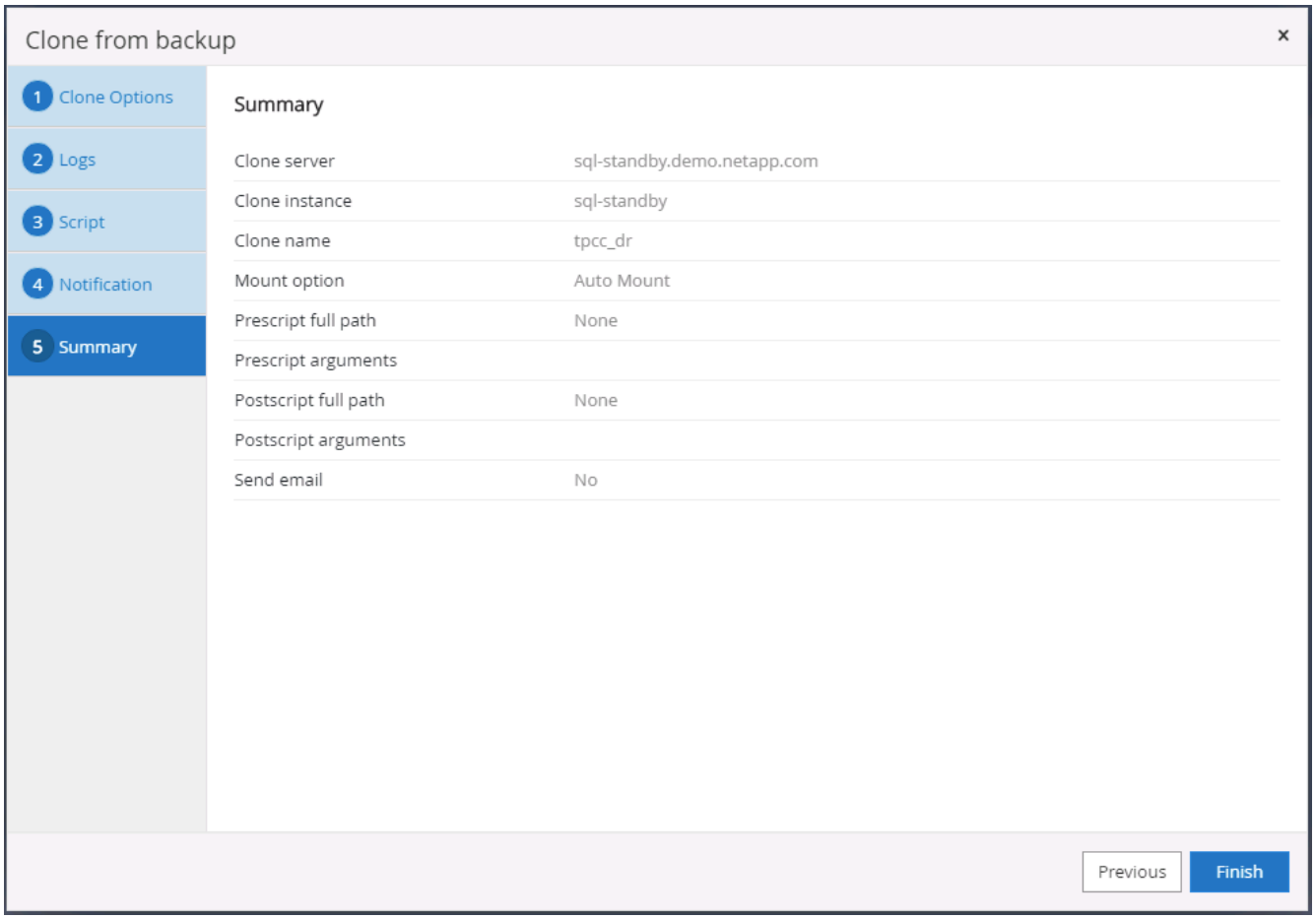
7. Specificare eventuali script facoltativi da eseguire prima o dopo la clonazione.

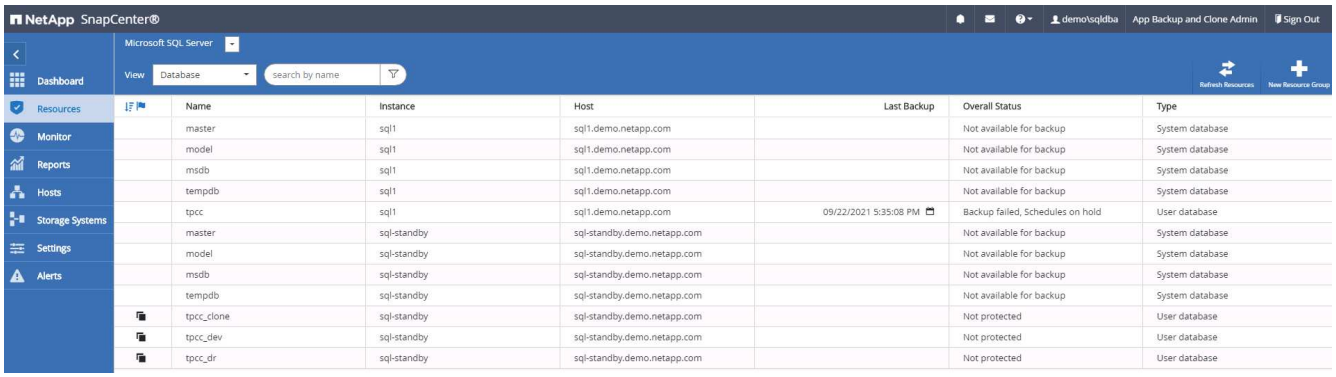


8. Specificare un server SMTP se si desidera la notifica via e-mail.



9. Riepilogo del clone DR. I database clonati vengono immediatamente registrati con SnapCenter e disponibili per la protezione tramite backup.



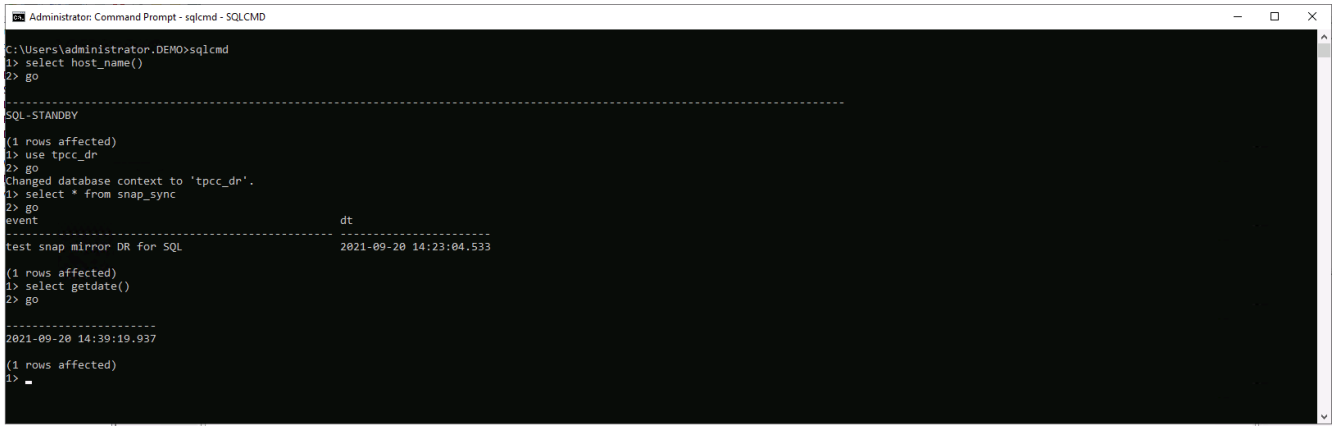


Convalida e configurazione del clone post-DR per SQL

1. Monitorare lo stato del processo di clonazione.

2. Convalidare che l'ultima transazione sia stata replicata e recuperata con tutti i cloni dei file di registro e il

recupero.



3. Configurare una nuova directory di log di SnapCenter sul server DR per il backup del log di SQL Server.
4. Dividere il volume clonato dal volume sorgente replicato.
5. Replica inversa dal cloud all'ambiente locale e ricostruzione del server di database locale non funzionante.

Dove rivolgersi per chiedere aiuto?

Se hai bisogno di aiuto con questa soluzione e casi d'uso, unisciti a"Canale Slack di supporto della community NetApp Solution Automation" e cerca il canale solution-automation per pubblicare le tue domande o richieste.

Informazioni sul copyright

Informazioni sul marchio commerciale