



Panoramica introduttiva

NetApp Solutions

NetApp
April 26, 2024

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions/databases/hybrid_dbops_snapcenter_getting_started_onprem.html on April 26, 2024. Always check docs.netapp.com for the latest.

Sommario

- Panoramica introduttiva 1
 - On-premise..... 1
 - Cloud pubblico AWS..... 1
- Introduzione on-premise 1
- Introduzione al cloud pubblico AWS..... 54

Panoramica introduttiva

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

On-premise

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

Cloud pubblico AWS

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

Per ulteriori informazioni, fare clic sui seguenti collegamenti:

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

Introduzione on-premise

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

On-premise

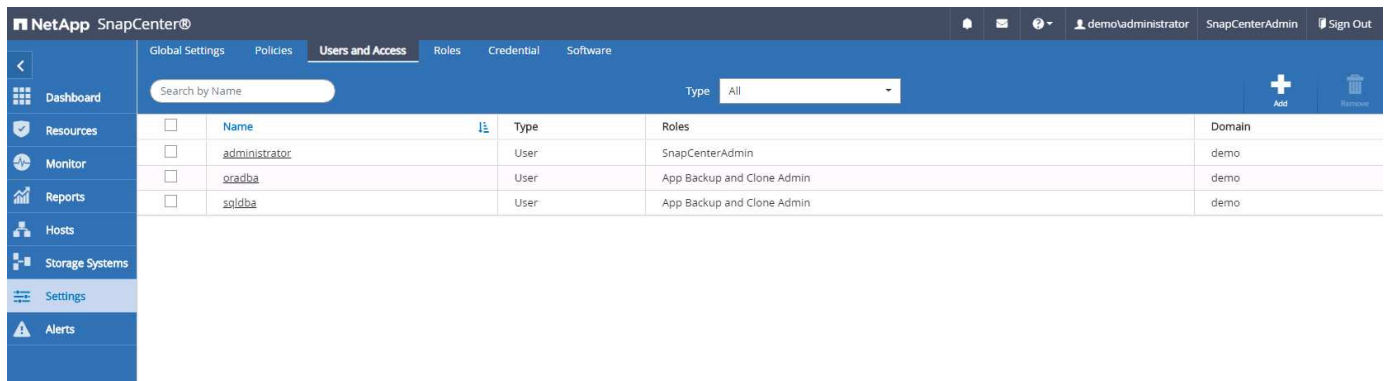
1. Configurare l'utente amministratore del database in SnapCenter

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

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

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

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



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

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

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

Host Windows per SQL Server:

1. Se si utilizzano credenziali Windows per l'autenticazione, è necessario impostare le credenziali prima di installare i plug-in.
2. Se si utilizza un'istanza di SQL Server per l'autenticazione, è necessario aggiungere le credenziali dopo l'installazione dei plug-in.
3. Se è stata attivata l'autenticazione SQL durante la configurazione delle credenziali, l'istanza o il database rilevato viene visualizzato con un'icona a forma di lucchetto rosso. Se viene visualizzata l'icona a forma di lucchetto, è necessario specificare le credenziali dell'istanza o del database per aggiungere correttamente l'istanza o il database a un gruppo di risorse.

4. È necessario assegnare la credenziale a un utente RBAC senza accesso sysadmin quando vengono soddisfatte le seguenti condizioni:
 - La credenziale viene assegnata a un'istanza SQL.
 - L'istanza o l'host SQL viene assegnato a un utente RBAC.
 - L'utente amministratore DB RBAC deve disporre sia del gruppo di risorse che dei privilegi di backup.

Host UNIX per Oracle:

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

3. Installazione del plug-in host SnapCenter

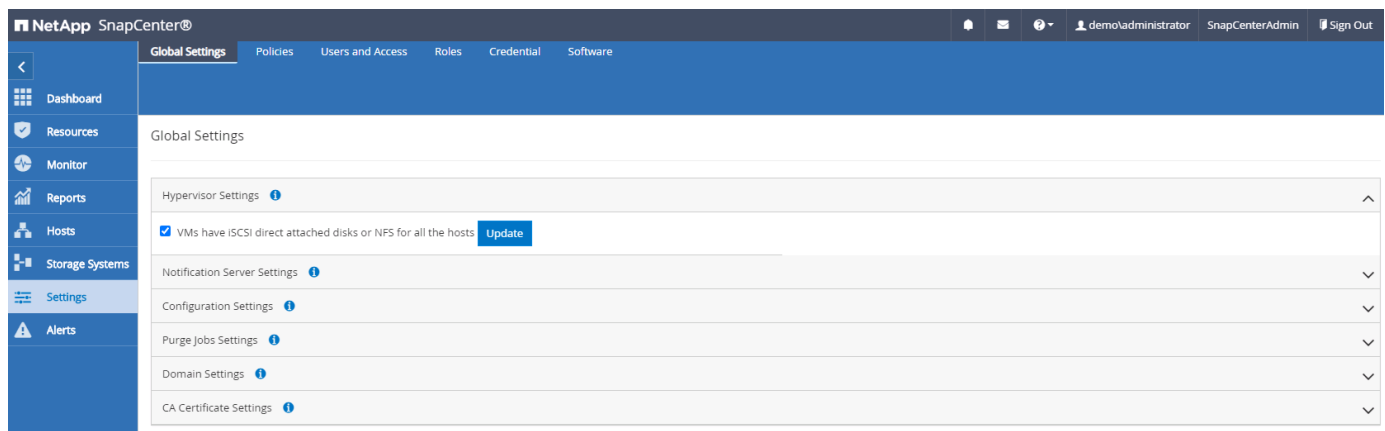


Prima di tentare di installare i plug-in SnapCenter sulle istanze del server DB cloud, assicurarsi che tutte le fasi di configurazione siano state completate come indicato nella relativa sezione cloud per l'implementazione dell'istanza di calcolo.

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

Configurare le impostazioni globali di SnapCenter

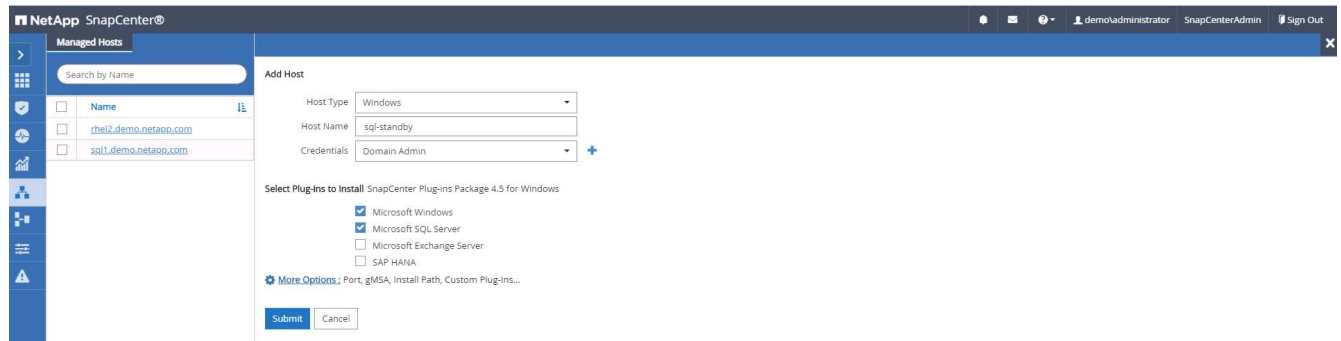
Accedere a Impostazioni > Impostazioni globali. Selezionare "VM con iSCSI direct attached disks o NFS per tutti gli host" in Impostazioni hypervisor e fare clic su Aggiorna.



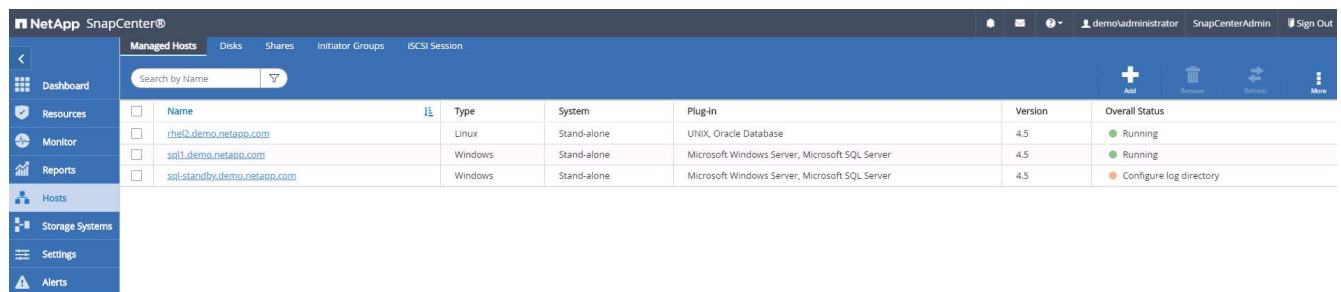
Aggiungere l'host Windows e l'installazione del plug-in sull'host

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

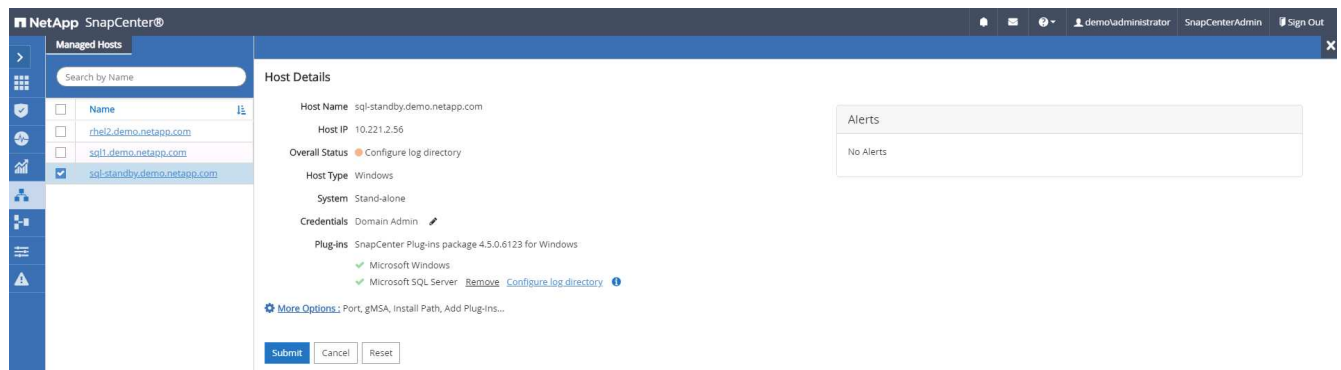
3. Scegliere Windows come tipo di host; il nome host può essere un nome host o un indirizzo IP. Il nome host deve essere risolto con l'indirizzo IP host corretto dall'host SnapCenter. Scegliere le credenziali host create al punto 2. Scegliere Microsoft Windows e Microsoft SQL Server come pacchetti di plug-in da installare.



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



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



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

Configure Plug-in for SQL Server

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

Configure host log directory

Host log directory

dedicated disk directory path

Browse

Save

Close

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

Configure Plug-in for SQL Server

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

Configure host log directory

Host log directory

G:\

Browse

Choose directory on NetApp Storage

sql-standby.demo.netapp.com

G:\

System Volume Information

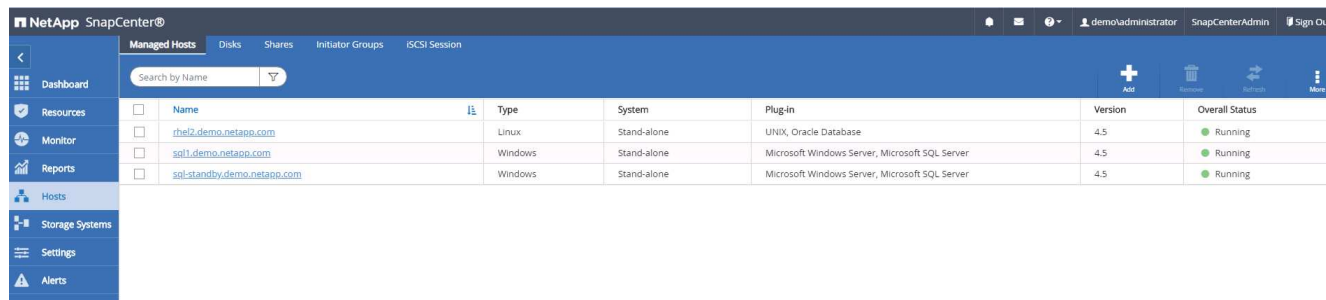
Save

Close

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

5

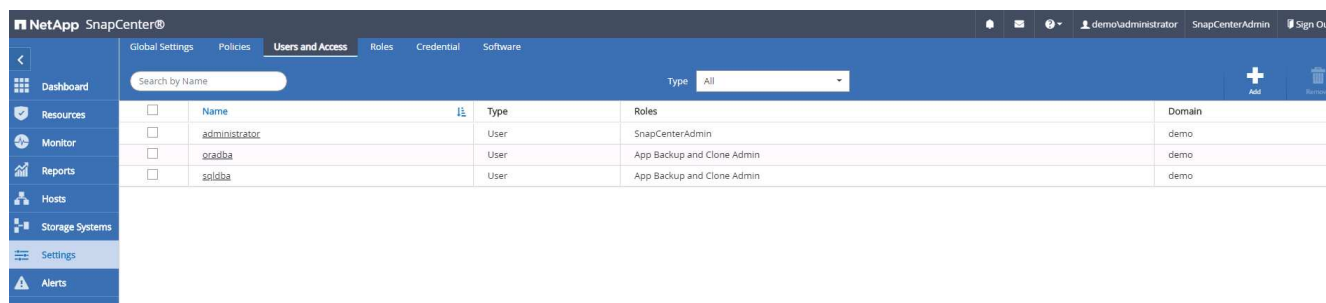
8. Una volta configurata la directory di log, lo stato generale del plug-in host di Windows viene modificato in in esecuzione.



The screenshot shows the NetApp SnapCenter interface with the 'Managed Hosts' tab selected. The table lists three hosts: 'rhel2.demo.netapp.com' (Linux, Stand-alone), 'sql1.demo.netapp.com' (Windows, Stand-alone), and 'sql-standby.demo.netapp.com' (Windows, Stand-alone). All hosts have a 'Running' status.

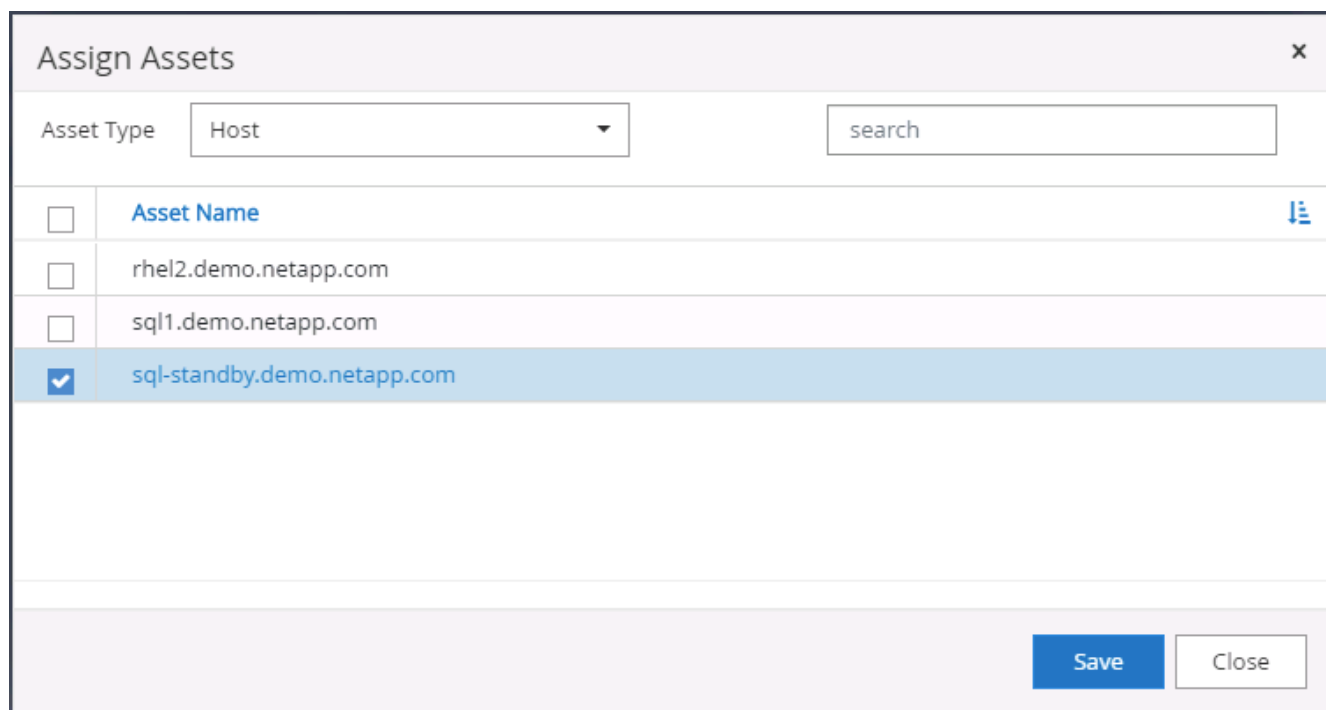
Name	Type	System	Plug-in	Version	Overall Status
rhel2.demo.netapp.com	Linux	Stand-alone	UNIX, Oracle Database	4.5	Running
sql1.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft SQL Server	4.5	Running
sql-standby.demo.netapp.com	Windows	Stand-alone	Microsoft Windows Server, Microsoft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

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



The screenshot shows the NetApp SnapCenter interface with the 'Users and Access' tab selected. The table lists three users: 'administrator', 'oraoba', and 'sqloba'. The 'sqloba' user is selected.

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



The screenshot shows the 'Assign Assets' dialog box. The 'Asset Type' is set to 'Host'. The search results show three hosts: 'rhel2.demo.netapp.com', 'sql1.demo.netapp.com', and 'sql-standby.demo.netapp.com'. The 'sql-standby.demo.netapp.com' host is selected.

Asset Type: Host

search

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

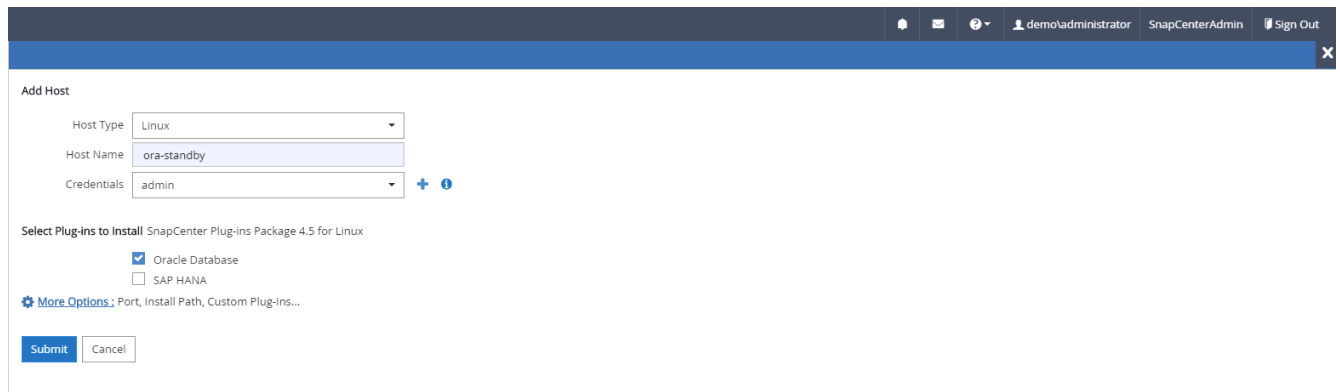
Save Close

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

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

lavoro Add host (Aggiungi host).

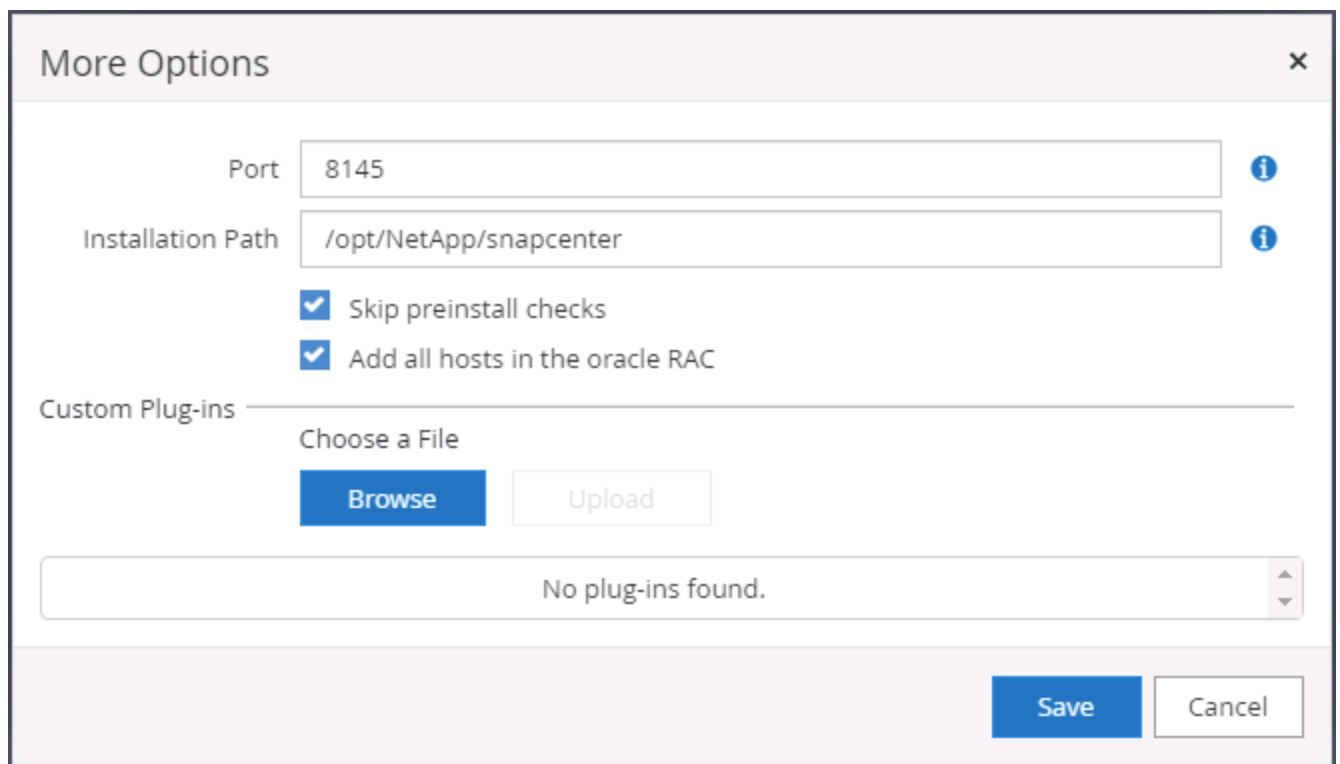
3. Scegliere Linux come tipo di host. Il nome host può essere il nome host o un indirizzo IP. Tuttavia, il nome host deve essere risolto per correggere l'indirizzo IP host dall'host SnapCenter. Scegliere le credenziali host create nel passaggio 2. Le credenziali host richiedono privilegi sudo. Selezionare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



The screenshot shows the 'Add Host' form in the SnapCenter Admin interface. The form is titled 'Add Host' and has a close button (X) in the top right corner. It contains the following fields and options:

- Host Type:** A dropdown menu with 'Linux' selected.
- Host Name:** A text input field with 'ora-standby' entered.
- Credentials:** A dropdown menu with 'admin' selected, followed by a '+' icon and an information icon (i).
- Select Plug-ins to Install:** A section titled 'SnapCenter Plug-ins Package 4.5 for Linux' with two checkboxes: 'Oracle Database' (checked) and 'SAP HANA' (unchecked).
- More Options:** A link labeled 'More Options' with a gear icon, followed by the text 'Port, Install Path, Custom Plug-ins...'. Below this link are 'Submit' and 'Cancel' buttons.

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



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

- Port:** A text input field with '8145' entered, followed by an information icon (i).
- Installation Path:** A text input field with '/opt/NetApp/snapcenter' entered, followed by an information icon (i).
- Checkboxes:** Two checked checkboxes: 'Skip preinstall checks' and 'Add all hosts in the oracle RAC'.
- Custom Plug-ins:** A section with a 'Choose a File' label, a 'Browse' button, and an 'Upload' button.
- Plug-ins List:** A text area displaying 'No plug-ins found.' with up and down arrow icons on the right.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

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

Confirm Fingerprint

Authenticity of the host cannot be determined

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

Confirm and Submit

Close

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

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

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

NetApp SnapCenter®

Users and Access

Users/Groups Details

Search by Name

Name
administrator
oradba
sqlidba

User Name

Domain

Roles

oradba

demo

App Backup and Clone Admin

Assign Assets

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

Submit

Cancel

Assign Assets

Asset Type
Host
search

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

Save
Close

4. Rilevamento delle risorse del database

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

NetApp SnapCenter®
demoloradba
App Backup and Clone Admin
Sign Out

Oracle Database
View Database Search databases

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

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

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

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

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

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

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

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

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

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

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

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

Cluster on-premise:

Overview

IPspaces

Cluster	Broadcast Domains
Default	Storage VMS svm_onPrem Broadcast Domains Default

Broadcast Domains

Cluster	9000 MTU	IPspace: Cluster
Default	1500 MTU	IPspace: Default onPrem-01 e0a e0b e0c e0d e0e e0f e0g e0h e0i-100 e0e-200 e0f-201

Network Interfaces

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

Cluster CVO di destinazione:

ONTAP System Manager

Search actions, objects, and pages

DASHBOARD

STORAGE

NETWORK

Overview

Ethernet Ports

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Overview

IPspaces

Cluster	Broadcast Domains Cluster
Default	Storage VMs svm_hybridcvo Broadcast Domains Default

Broadcast Domains

Cluster	9000 MTU	IPspace: Cluster hybridcvo-01 e0b hybridcvo-02 e0b
Default	9001 MTU	IPspace: Default hybridcvo-01 e0a hybridcvo-02 e0a

Network Interfaces

Search

Download

Filter

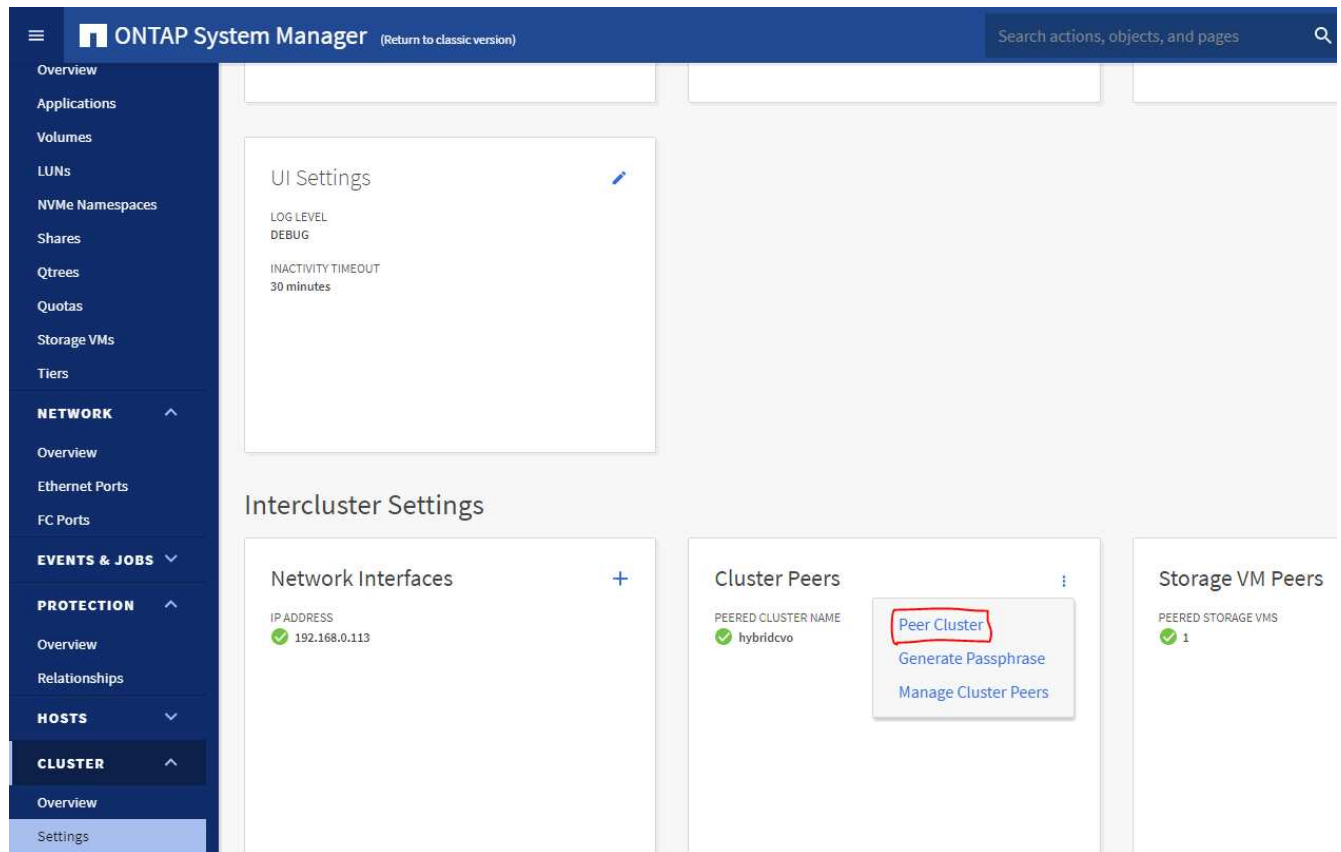
Show / Hide

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

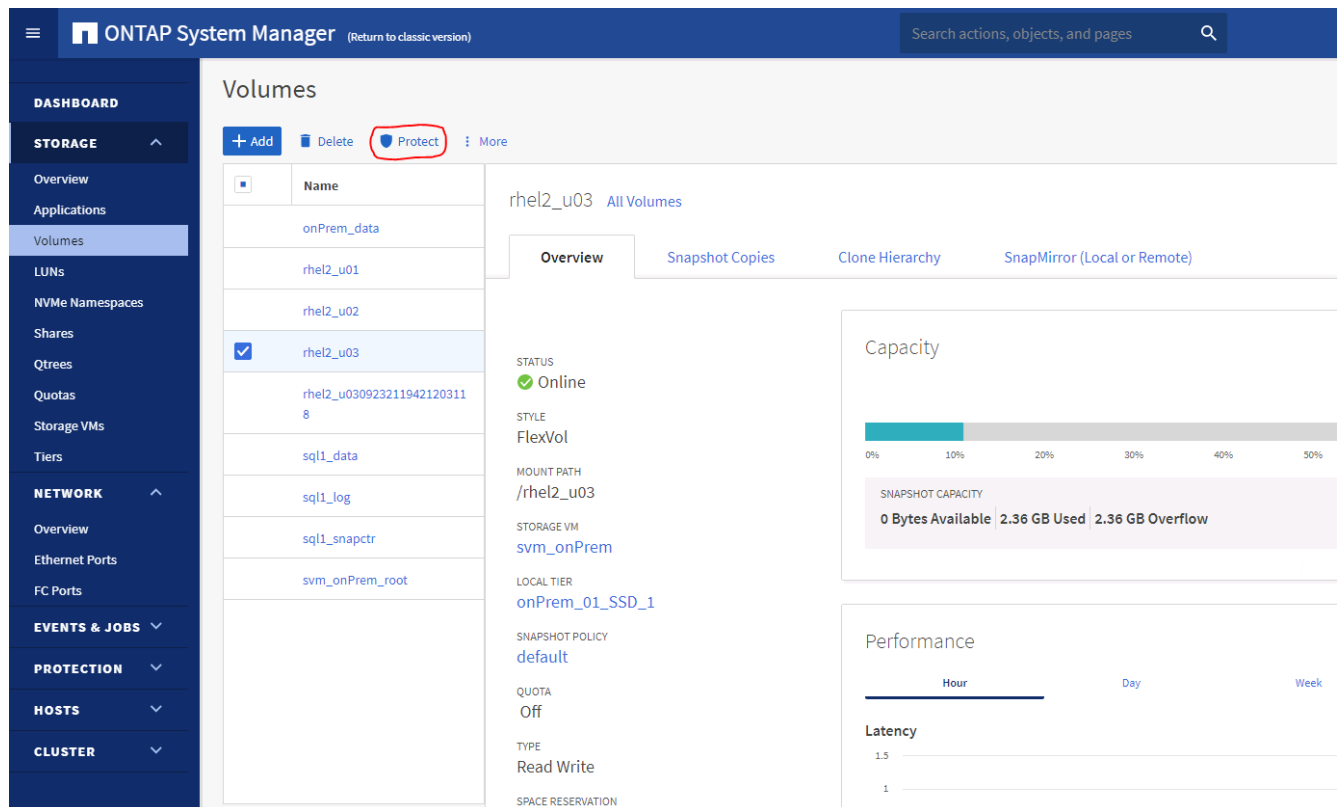
2. Con le LIF intercluster configurate, è possibile configurare il peering dei cluster e la replica dei volumi utilizzando la funzione di trascinamento della selezione in NetApp Cloud Manager. Vedere ["Getting started - AWS Public Cloud"](#) per ulteriori informazioni.

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

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



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



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

destinazione.

ONTAP System Manager

(Return to classic version)

Search actions, objects, and pages

DASHBOARD

STORAGE

Overview

Applications

Volumes

LUNs

NVMe Namespaces

Shares

Qtrees

Quotas

Storage VMs

Tiers

NETWORK

Overview

Ethernet Ports

FC Ports

EVENTS & JOBS

PROTECTION

HOSTS

CLUSTER

Protect Volumes

PROTECTION POLICY

Asynchronous

Source

CLUSTER
onPrem

STORAGE VM
svm_onPrem

SELECTED VOLUMES
rhel2_u03

Destination

CLUSTER
hybridcvo

STORAGE VM
svm_hybridcvo

Destination Settings

2 matching labels

VOLUME NAME

PREFIX
vol_

SUFFIX
<SourceVolumeName>_dest

☐ Override default storage service name

Configuration Details

☒ Initialize relationship

☐ Enable FabricPool

Save

Cancel

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

Volumes

+ Add

Delete

Protect

More

Name

rhel2_u03

onPrem_data

rhel2_u01

rhel2_u02

☒ rhel2_u03

rhel2_u0309232119421203118

All Volumes

Edit

More

Overview

Snapshot Copies

Clone Hierarchy

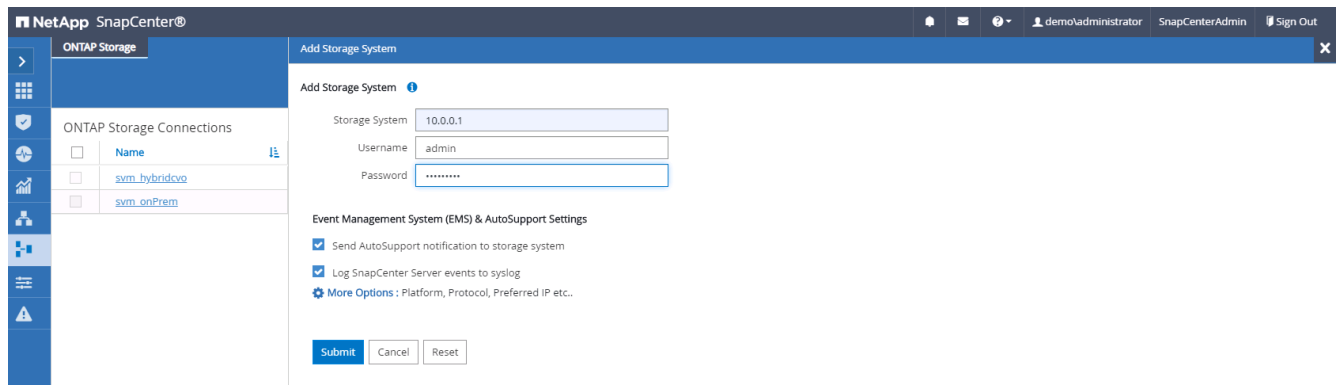
SnapMirror (Local or Remote)

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

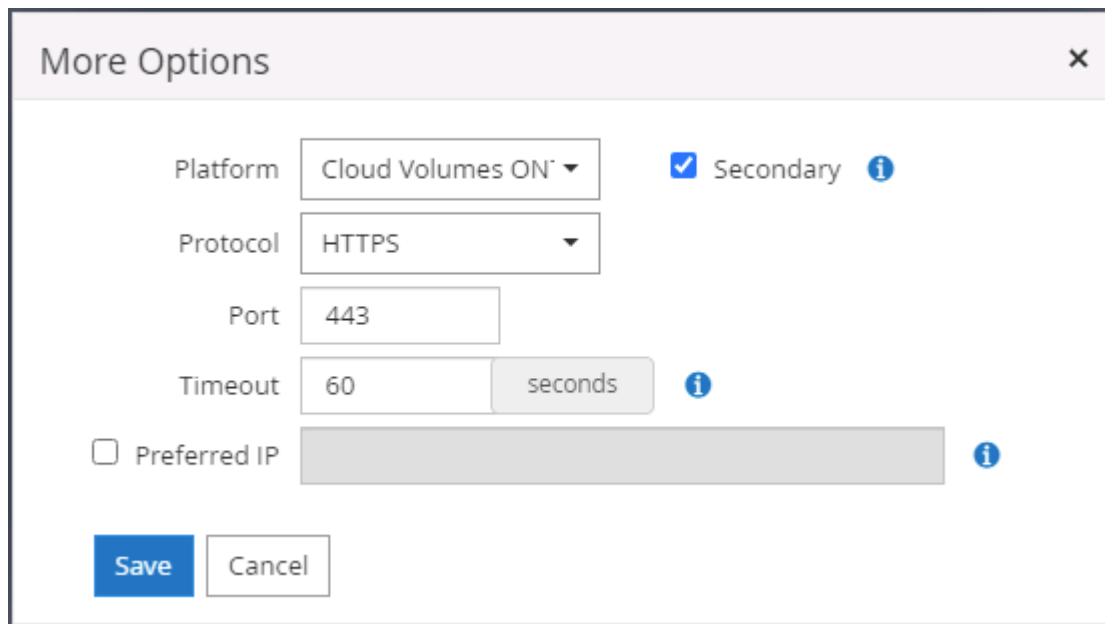
6. Aggiunta di SVM per lo storage di database CVO a SnapCenter

1. Accedere a SnapCenter con un ID utente con privilegi SnapCenterAdmin.

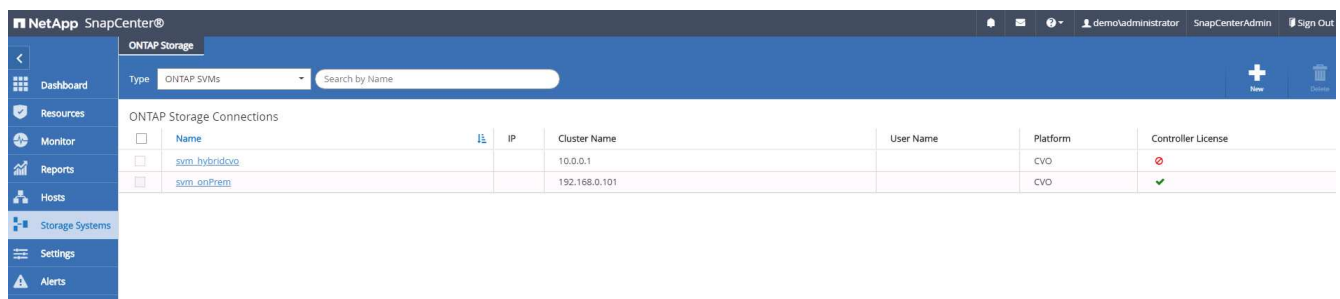
2. Fare clic sulla scheda sistema di storage dal menu, quindi fare clic su nuovo per aggiungere una SVM di storage CVO che ospita volumi di database di destinazione replicati in SnapCenter. Inserire l'IP di gestione del cluster nel campo Storage System (sistema di storage) e immettere il nome utente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



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



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

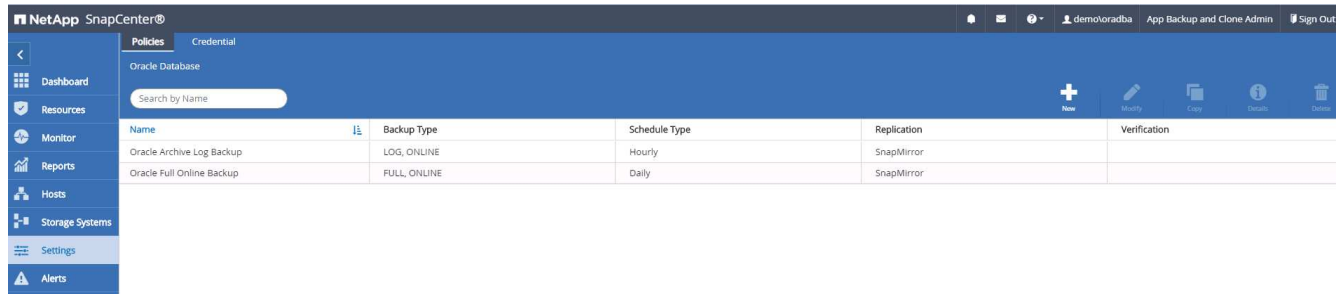


7. Configurare i criteri di backup del database in SnapCenter

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

Creare una policy di backup completa del database per Oracle

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



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

The screenshot shows a 'Modify Oracle Database Backup Policy' dialog box. It has a close button (X) in the top right corner. On the left, there is a vertical list of steps: 1 Name, 2 Backup Type, 3 Retention, 4 Replication, 5 Script, 6 Verification, and 7 Summary. The 'Name' step is currently selected and highlighted in blue. The main area of the dialog is titled 'Provide a policy name'. It contains two input fields: 'Policy name' with the value 'Oracle Full Online Backup' and an information icon (i) to its right, and 'Details' with the value 'Backup all data and log files'. At the bottom right of the dialog, there are two buttons: 'Previous' and 'Next'.

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

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☒ Datafiles, control files, and archive logs

☐ Datafiles and control files

☐ Archive logs

☐ Offline backup

i

☒ Mount

☐ Shutdown

☐ Save state of PDBs

i

Choose schedule frequency

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

☐ On demand

☐ Hourly

☒ Daily

Previous

Next

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

16

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Daily retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14

days

Previous

Next

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

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options i

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily i

Error retry count

3 i

Previous

Next

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

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

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

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Eseguire la verifica del backup, se necessario.

19

Modify Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run Verifications for following backup schedules

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

☐ Daily

Verification script commands

Script timeout

60secs

Prescript full path

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

Prescript arguments

Choose optional arguments...

Postscript full path

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

Postscript arguments

Choose optional arguments...

Previous

Next

8. Riepilogo.

20

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

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

Previous

Finish

Creare una policy di backup del log del database per Oracle

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

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

Oracle Archive Log Backup

Backup Oracle archive logs

Previous

Next

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

22

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select Oracle database backup options

Choose backup type

☒ Online backup

☐ Datafiles, control files, and archive logs

☐ Datafiles and control files

☒ Archive logs

☐ Offline backup

i

☒ Mount

☐ Shutdown

☐ Save state of PDBs

i

Choose schedule frequency

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

☐ On demand

☒ Hourly

☐ Daily

Previous

Next

4. Impostare il periodo di conservazione del registro.

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

Hourly retention settings

Data backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

14 days

Archive Log backup retention settings

Total Snapshot copies to keep

7

Keep Snapshot copies for

7 days

Previous

Next

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

24

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Hourly

Error retry count

3

Previous

Next

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

New Oracle Database Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

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

Prescript full path

/var/opt/snapcenter/spl/scripts/

Enter Prescript path

Prescript arguments

Postscript full path

/var/opt/snapcenter/spl/scripts/

Enter Postscript path

Postscript arguments

Script timeout

60

secs

Previous

Next

7. Specificare eventuali script di verifica del backup.

26

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.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

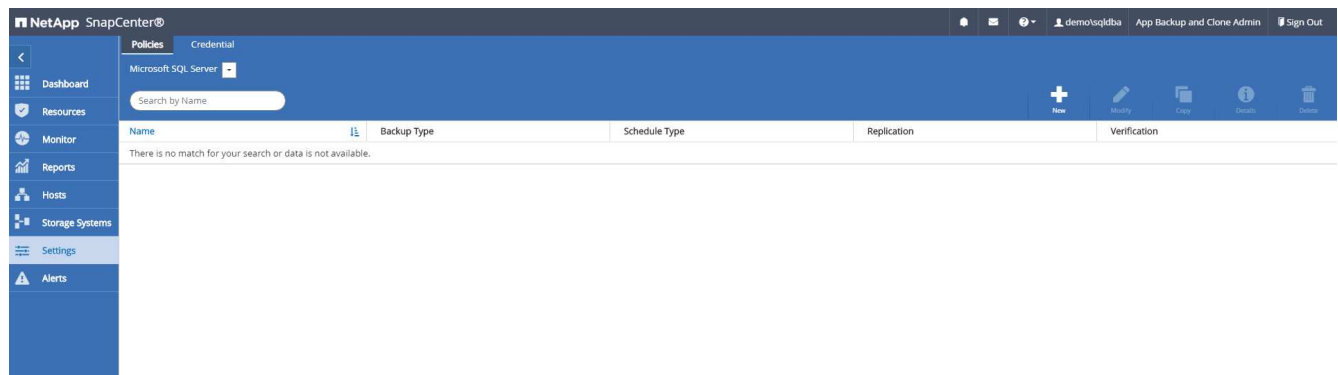
Policy name	Oracle Archive Log Backup
Details	Backup Oracle archive logs
Backup type	Online backup
Schedule type	Hourly
RMAN catalog backup	Disabled
Archive log pruning	None
On demand data backup retention	None
On demand archive log backup retention	None
Hourly data backup retention	None
Hourly archive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

Previous

Finish

Creare una policy di backup completa del database per SQL

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



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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

SQL Server Full Backup

Details

Backup all data and log files

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☒ Full backup and log backup

☐ Full backup

☐ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

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

☐ On demand

☐ Hourly

☒ Daily

☐ Weekly

☐ Monthly

Previous

Next

4. Impostare il periodo di conservazione del backup.

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Retention settings

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

☒ Keep log backups applicable to last

7

full backups

☐ Keep log backups applicable to last

14

days

Full backup retention settings ⓘ

Daily

☒ Total Snapshot copies to keep

7

☐ Keep Snapshot copies for

14

days

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Daily

Error retry count

3

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

Specify optional scripts to run after performing a backup job

Postscript full path

Postscript arguments

Script timeout

Choose optional arguments...

Choose optional arguments...

60secs

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select the options to run backup verification

Run verifications for the following backup schedules

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

☐ Daily

Database consistency checks options

☒ Limit the integrity structure to physical structure of the database (PHYSICAL_ONLY)

☒ Suppress all information message (NO_INFOMSGS)

☐ Display all reported error messages per object (ALL_ERRORMSGSGS)

☐ Do not check non-clustered indexes (NOINDEX)

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

Log backup

☐ Verify log backup.

Verification script settings

Script timeout secs

Previous

Next

8. Riepilogo.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

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

Previous

Finish

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

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Provide a policy name

Policy name

Details

SQL Server Log Backup

Backup SQL server log

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select SQL server backup options

Choose backup type

☐ Full backup and log backup

☐ Full backup

☒ Log backup

☐ Copy only backup

Maximum databases backed up per Snapshot copy:

Availability Group Settings

Schedule frequency

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

☐ On demand

☒ Hourly

☐ Daily

☐ Weekly

☐ Monthly

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Log backup retention settings

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

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Select secondary replication options

☒ Update SnapMirror after creating a local Snapshot copy.

☐ Update SnapVault after creating a local Snapshot copy.

Secondary policy label

Hourly

Error retry count

3

Previous

Next

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

New SQL Server Backup Policy

1 Name

2 Backup Type

3 Retention

4 Replication

5 Script

6 Verification

7 Summary

Specify optional scripts to run before performing a backup job

Prescript full path

Prescript arguments

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.

1

Name

2

Backup Type

3

Retention

4

Replication

5

Script

6

Verification

7

Summary

Summary

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

Previous

Finish

8. Implementare policy di backup per proteggere il database

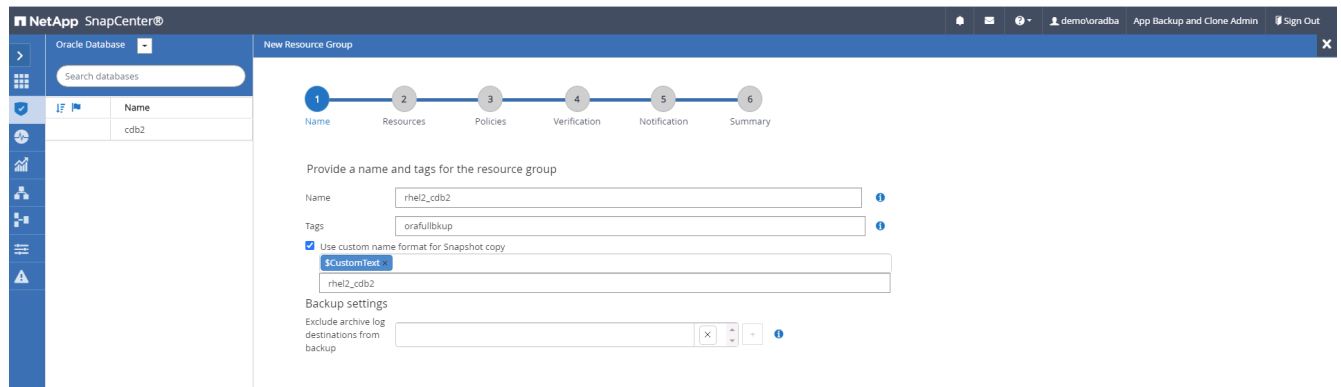
SnapCenter utilizza un gruppo di risorse per eseguire il backup di un database in un gruppo logico di risorse di database, ad esempio più database ospitati su un server, un database che condivide gli stessi volumi di storage, più database che supportano un'applicazione di business e così via. La protezione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

Creare un gruppo di risorse per il backup completo di Oracle

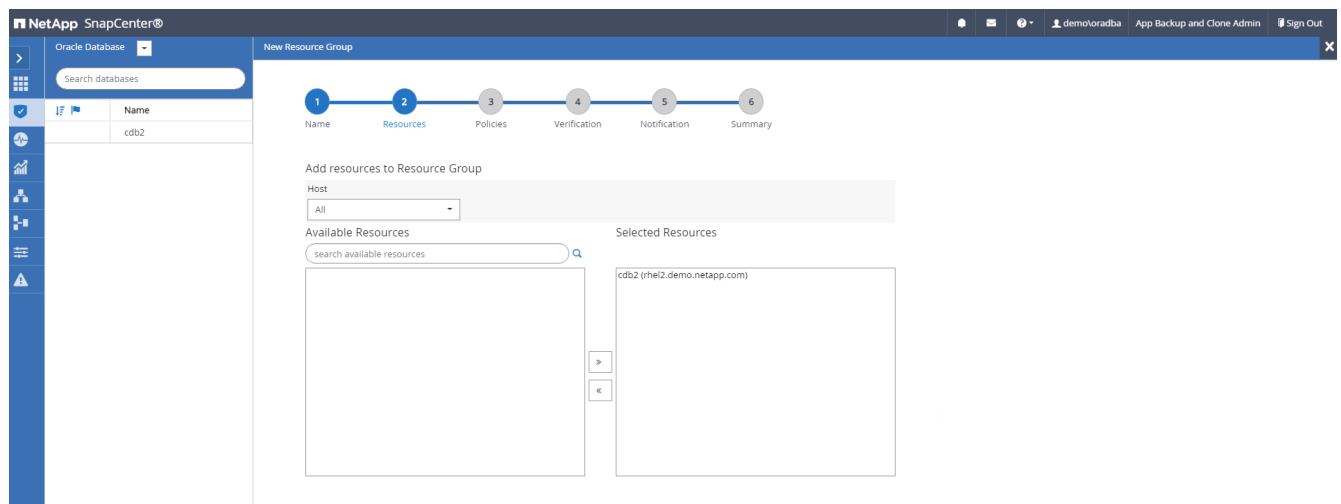
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere Database o Gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse.

NetApp SnapCenter®							
Oracle Database							
View Database Search databases							
Resources	Name	Oracle Database Type	Host/Cluster	Resource Group	Policies	Last Backup	Overall Status
Monitor	cdb2	Single instance (Multitenant)	rhe12.demo.netapp.com				Not protected
Reports							
Hosts							
Storage Systems							
Settings							
Alerts							

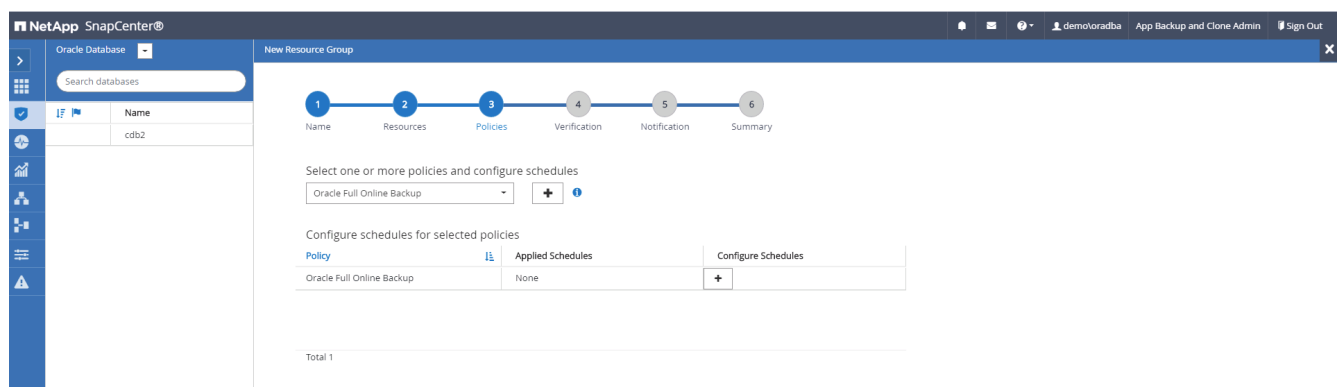
2. Fornire un nome e tag per il gruppo di risorse. È possibile definire un formato di denominazione per la copia Snapshot e ignorare la destinazione del registro di archiviazione ridondante, se configurata.



3. Aggiungere risorse di database al gruppo di risorse.



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



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

NetApp SnapCenter®

Oracle Database

New Resource Group

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

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

Provide email settings

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

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

8. Riepilogo.

NetApp SnapCenter®

Oracle Database

New Resource Group

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

Resource group name: rhel2_cdb2

Tags: orafullbkup

Policy: Oracle Full Online Backup: Daily

Plug-in: SnapCenter Plug-in for Oracle Database

Verification enabled for policy: None

Send email: No

Previous Finish

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

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

NetApp SnapCenter®

Oracle Database

View: Resource Group Search resource group

Name	Resources	Tags	Policies	Last Backup	Overall Status
rhel2_cdb2	1	orafullbkup	Oracle Full Online Backup		

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

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhe12_cdb2

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

Provide a name and tags for the resource group

Name rhe12_cdb2_log

Tags oralogbkup

☒ Use custom name format for Snapshot copy

\$CustomText rhe12_cdb2_log

Backup settings

Exclude archive log destinations from backup

3. Aggiungere risorse di database al gruppo di risorse.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhe12_cdb2

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

Add resources to Resource Group

Host All

Available Resources

search available resources

Selected Resources

cdb2 (rhe12.demo.netapp.com)

Total 1

Previous Next

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

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhe12_cdb2

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

Select one or more policies and configure schedules

Oracle Archive Log Backup

Oracle Full Online Backup

Oracle Archive Log Backup

Policy

Applied Schedules

None

Configure Schedules

Total 1

Previous Next

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

Add schedules for policy Oracle Archive Log Backup

Hourly

Start date

09/10/2021 3:00 PM

☒ Expires on

12/31/2021 3:00 PM

Repeat every

1

hours

0

mins

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

Cancel
OK

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

NetApp SnapCenter®
demolatordba
App Backup and Clone Admin
Sign Out

Oracle Database
Search resource groups
Name
rhe2_cdb2
Total 1

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

Configure verification schedules
Policy Schedule Type Applied Schedules Configure Schedules
There is no match for your search or data is not available.
Total 0
Previous Next

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

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

Total 1

New Resource Group

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

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

Provide email settings ⓘ

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

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

8. Riepilogo.

NetApp SnapCenter®

Oracle Database

Search resource groups

Name

rhel2_cdb2

Total 1

New Resource Group

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

Resource group name: rhel2_cdb2_log

Tags: oralogbkup

Policy: Oracle Archive Log Backup: Hourly

Plug-in: SnapCenter Plug-in for Oracle Database

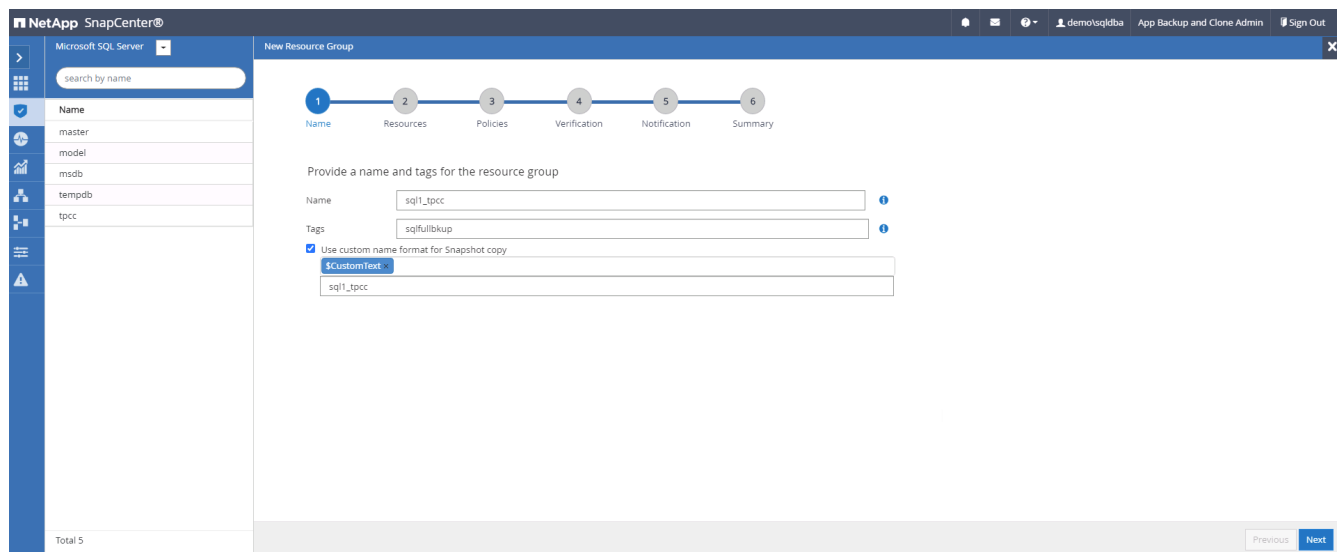
Verification enabled for policy: None

Send email: No

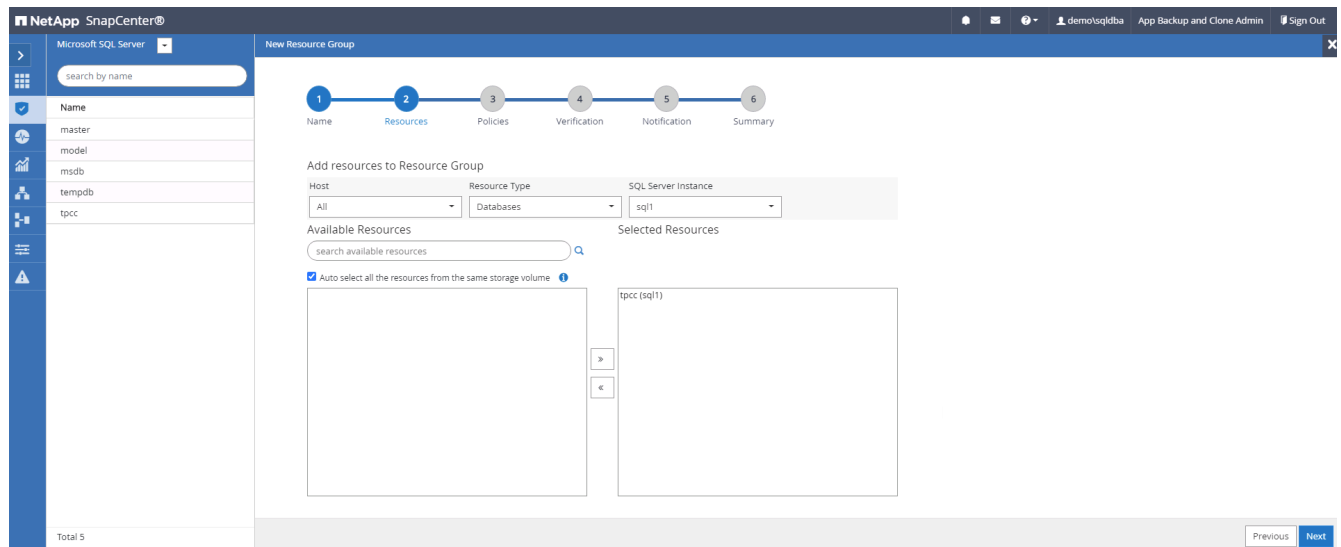
Previous Finish

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

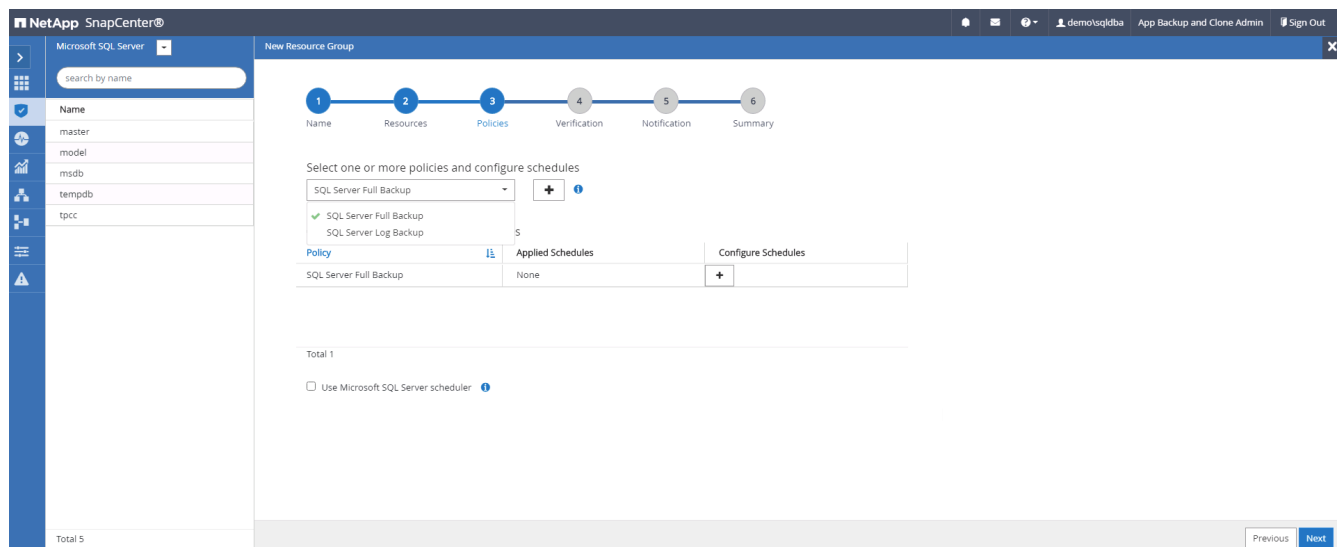
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire un nome e tag per il gruppo di risorse. È possibile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



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



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



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

Add schedules for policy SQL Server Full Backup

Daily

Start date 09/10/2021 6:20 PM

☒ Expires on 12/31/2021 6:20 PM

Repeat every 1 days

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

Cancel OK

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

NetApp SnapCenter®

Microsoft SQL Server

New Resource Group

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

Select the verification servers

Verification server Select one or more servers

Load secondary locators to verify backups on secondary Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridcvosql1_data_dr
svm_onPrem:sql1_log	svm_hybridcvosql1_log_dr

Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

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

Total 5

Previous Next

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

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

master

model

msdb

tempdb

tpcc

Total 5

New Resource Group

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

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

Provide email settings

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

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

7. Riepilogo.

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

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

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

New Resource Group

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

Resource group name: sql1_tpcc

Tags: sqlfullbkup

Policy: SQL Server Full Backup: Daily

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

Verification Server: None

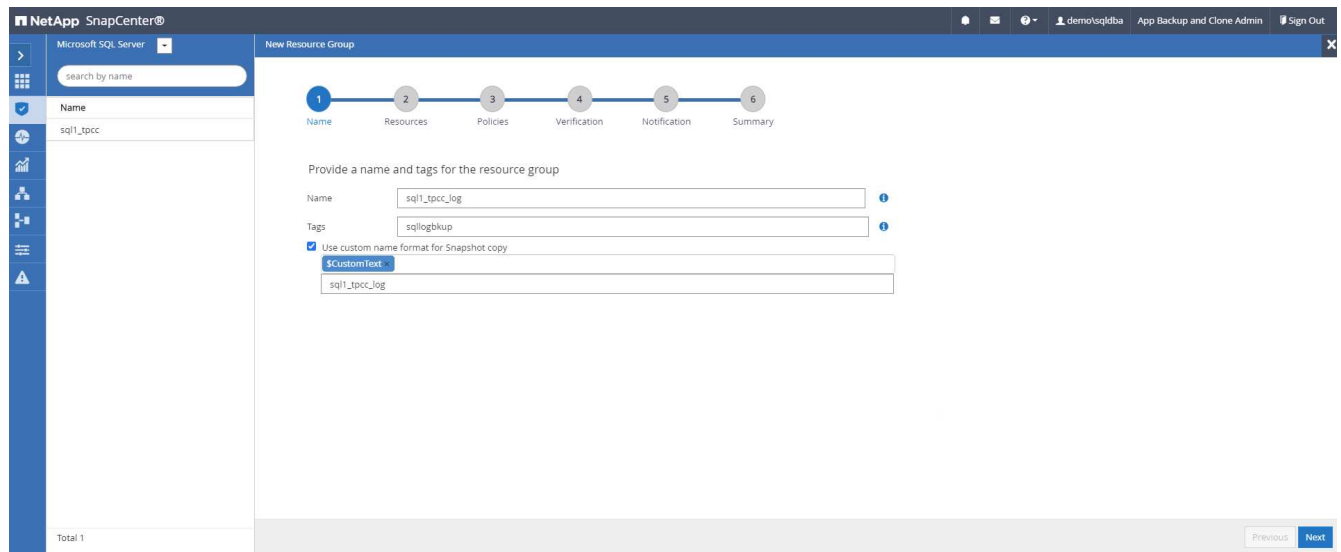
Verification enabled for policy: None

Send email: No

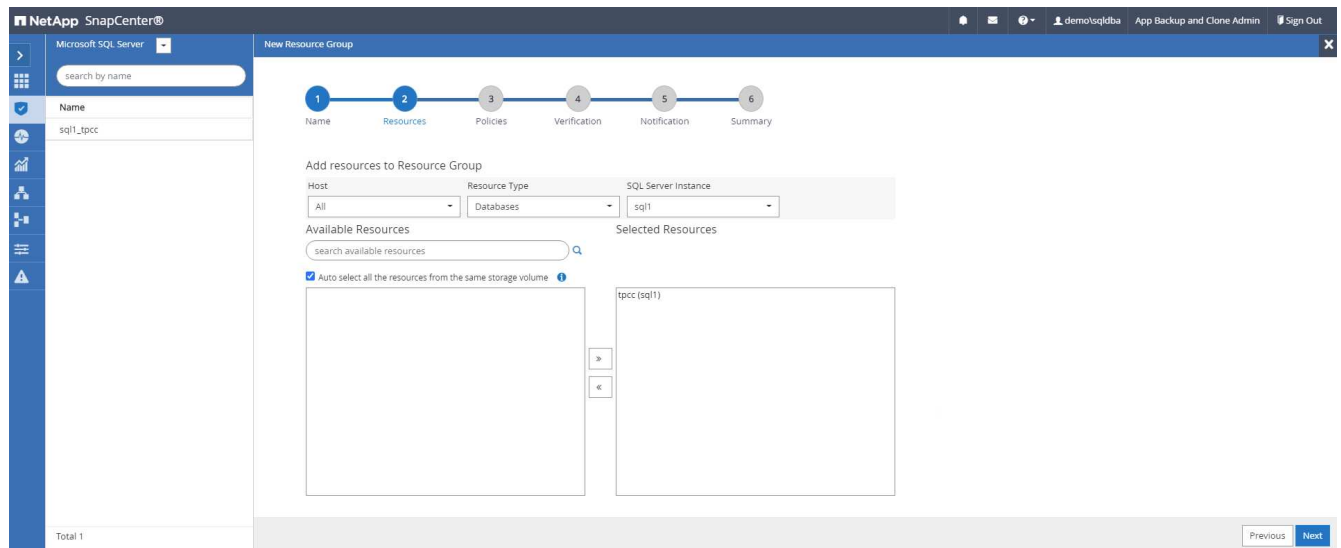
Previous Finish

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

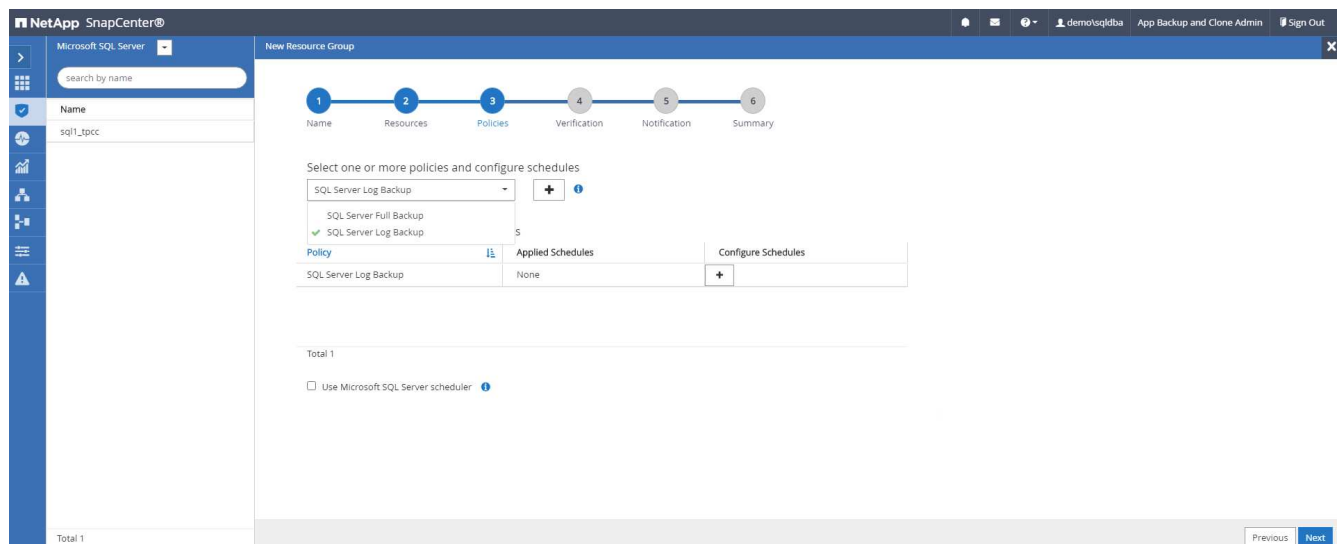
1. Accedere a SnapCenter con un ID utente per la gestione del database e accedere alla scheda risorse. Nell'elenco a discesa Visualizza, scegliere un database o un gruppo di risorse per avviare il flusso di lavoro di creazione del gruppo di risorse. Fornire il nome e i tag per il gruppo di risorse. È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



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



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



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

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1_tpcc

Total 1

New Resource Group

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

Select one or more policies and configure schedules

SQL Server Log Backup

Configure schedules for selected policies

Policy	Applied Schedules	Configure Schedules
SQL Server Log Backup	Hourly: Repeat every 1 hours	✎ ✕

Total 1

☐ Use Microsoft SQL Server scheduler

Previous Next

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

NetApp SnapCenter®

Microsoft SQL Server

search by name

Name

sql1_tpcc

Total 1

New Resource Group

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

Select the verification servers

Verification server: Select one or more servers

Load secondary locators to verify backups on secondary

Load locators

Secondary storage location: SnapVault or SnapMirror

Source Volume	Destination Volume
svm_onPrem:sql1_data	svm_hybridv:sql1_data_dr
svm_onPrem:sql1_log	svm_hybridv:sql1_log_dr

Configure verification schedules

Policy Schedule Type Applied Schedules Configure Schedules

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

Previous Next

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

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1_tpcc

Total 1

New Resource Group

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

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

Provide email settings

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

Email preference: Never

From: From email

To: Email to

Subject: Notification

☐ Attach job report

Previous Next

7. Riepilogo.

NetApp SnapCenter®

Microsoft SQL Server

search by name

sql1_tpcc

Total 1

New Resource Group

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

Resource group name: sql1_tpcc_log

Tags: sqllogbkup

Policy: SQL Server Log Backup: Hourly

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

Verification Server: None

Verification enabled for policy: None

Send email: No

Previous Finish

9. Convalidare il backup

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

NetApp SnapCenter®

Jobs Schedules Events Logs

search by name

Dashboard Resources Monitor Reports Hosts Storage Systems Settings Alerts

Jobs - Filter

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

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

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

The screenshot shows the NetApp SnapCenter interface. On the left, there's a sidebar with navigation icons. The main area is titled 'Oracle Database' and 'cdb2 Topology'. It displays a 'Manage Copies' section with a diagram showing 'Local copies' (197 Backups, 0 Clones) and 'Mirror copies' (197 Backups, 3 Clones). A 'Summary Card' on the right shows: 394 Backups, 28 Data Backups, 366 Log Backups, and 3 Clones. Below this is a 'Primary Backup(s)' section with a search bar and a table of backups.

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

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

Introduzione al cloud pubblico AWS

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

Cloud pubblico AWS



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

1. Controllo prima del volo

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

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

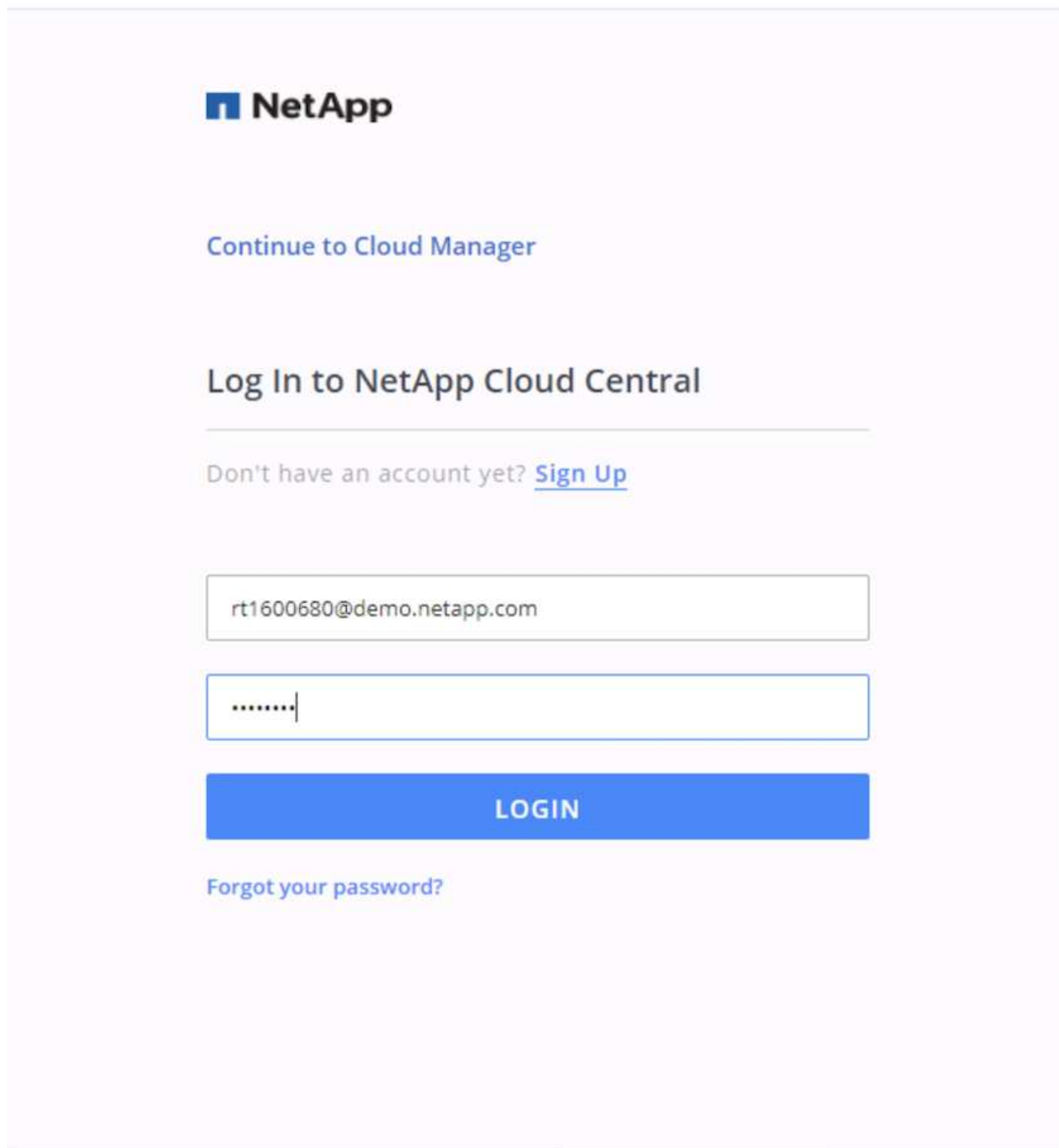
2. Fasi per implementare Cloud Manager e Cloud Volumes ONTAP in AWS



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

Implementare Cloud Manager Connector

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



The image shows the NetApp Cloud Central login page. At the top is the NetApp logo. Below it is a link to "Continue to Cloud Manager". The main heading is "Log In to NetApp Cloud Central". Below the heading is a link for "Don't have an account yet? Sign Up". There are two input fields: the first contains the email "rt1600680@demo.netapp.com" and the second contains a masked password ".....". Below the password field is a blue "LOGIN" button. At the bottom is a link for "Forgot your password?".

NetApp

[Continue to Cloud Manager](#)

Log In to NetApp Cloud Central

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

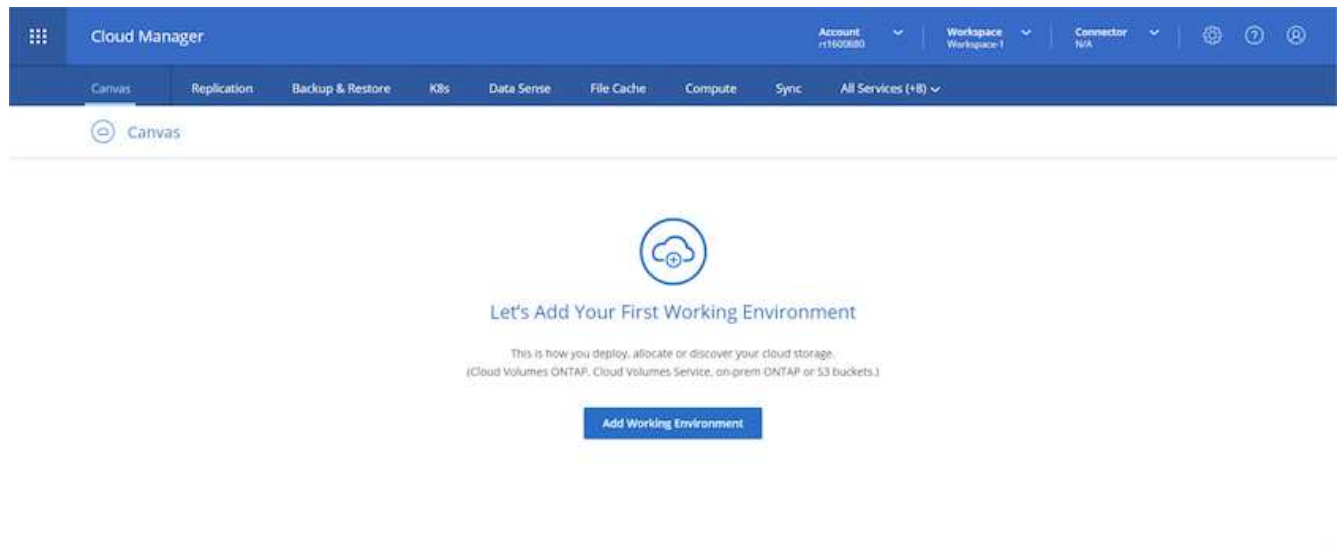
rt1600680@demo.netapp.com

.....

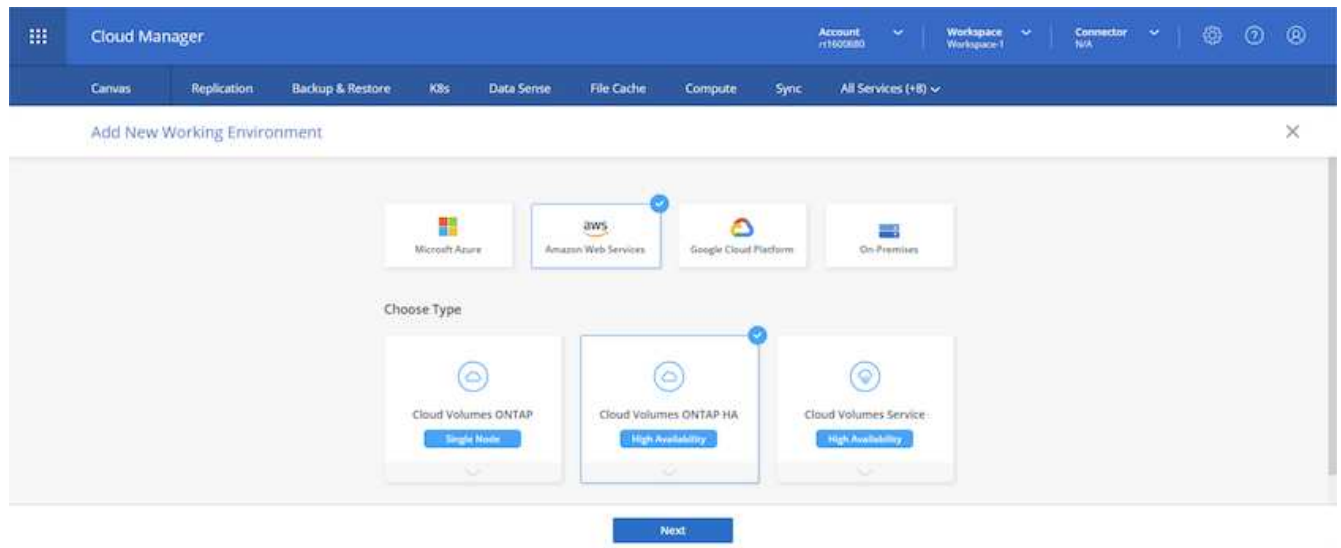
LOGIN

[Forgot your password?](#)

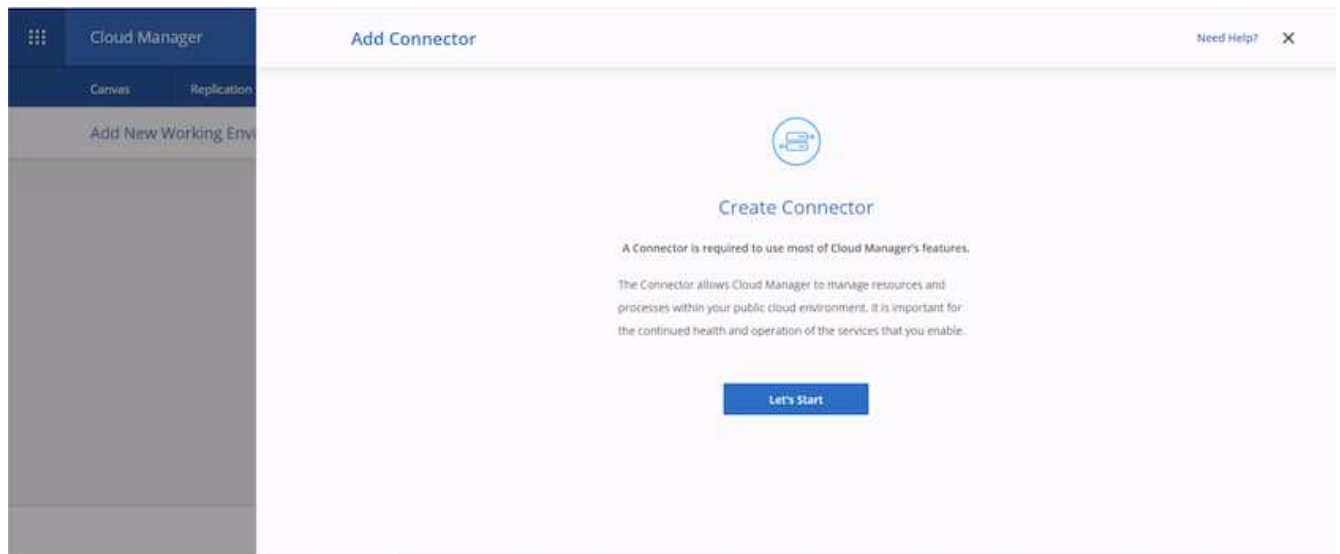
2. Dopo aver effettuato l'accesso, si dovrebbe essere portati a Canvas.



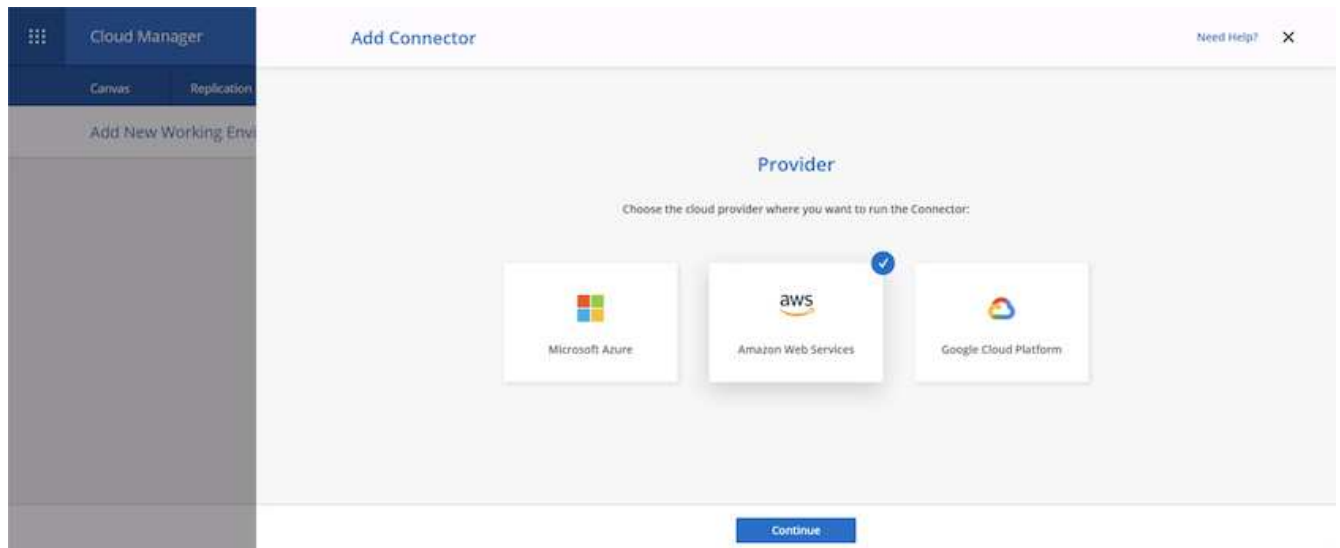
3. Fai clic su "Aggiungi ambiente di lavoro" e scegli Cloud Volumes ONTAP in AWS. In questo caso, è anche possibile scegliere se implementare un sistema a nodo singolo o una coppia ad alta disponibilità. Ho scelto di implementare una coppia ad alta disponibilità.



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



5. Fare clic su Avvia, quindi scegliere AWS.



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

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

AWS Credentials

AWS Access Key

AWS Access Key is required

AWS Secret Key

Region

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

Want to launch an instance without AWS Credentials?

Previous Next

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

Cloud Manager

Add Connector

Need Help? X

Get Ready AWS Credentials Details Network Security Group Review

Details

Connector Instance Name

awscloudmanager

Connector Role

Create Role Select an existing Role

Role Name

Cloud-Manager-Operator-IBHt24j

Add Tags to Connector Instance

Previous Next

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

Cloud Manager | Add Connector | Need Help? X

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

Connectivity

VPC: vpc-083fcd79f75dfb6e - 10.221.0.0/16

Subnet: 10.221.4.0/24 | publicSN-us-east-1a-rt1600...

Key Pair: rt1600680

Public IP: Enable

Proxy Configuration (Optional)

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

Define Credentials for this Proxy

Upload a root certificate

Previous Next

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

Cloud Manager | Add Connector | Need Help? X

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

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

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

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

Previous Next

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

Cloud Manager

Canvas Replication

Add New Working Env

Add Connector

Need Help? X

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

Code for Terraform Automation

Connector Name	awscloudmanager
Region	us-east-1
VPC	vpc-083fcbd79f75dfb6e - 10.221.0.0/16
Subnet	10.221.4.0/24 publicSN_us-east-1a_rt1600680
Key Pair	rt1600680
Public IP	Enable
Proxy	None
Security Group	HTTP: 216.240.31.145/32, HTTPS: 216.240.31.145/32, SSH: 216.240.31.145/32

Previous Add

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

Cloud Manager

Canvas Replication

Add New Working Env

Deploying a Connector

Show Details

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

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

Cloud Manager

Canvas Replication

Add New Working Env

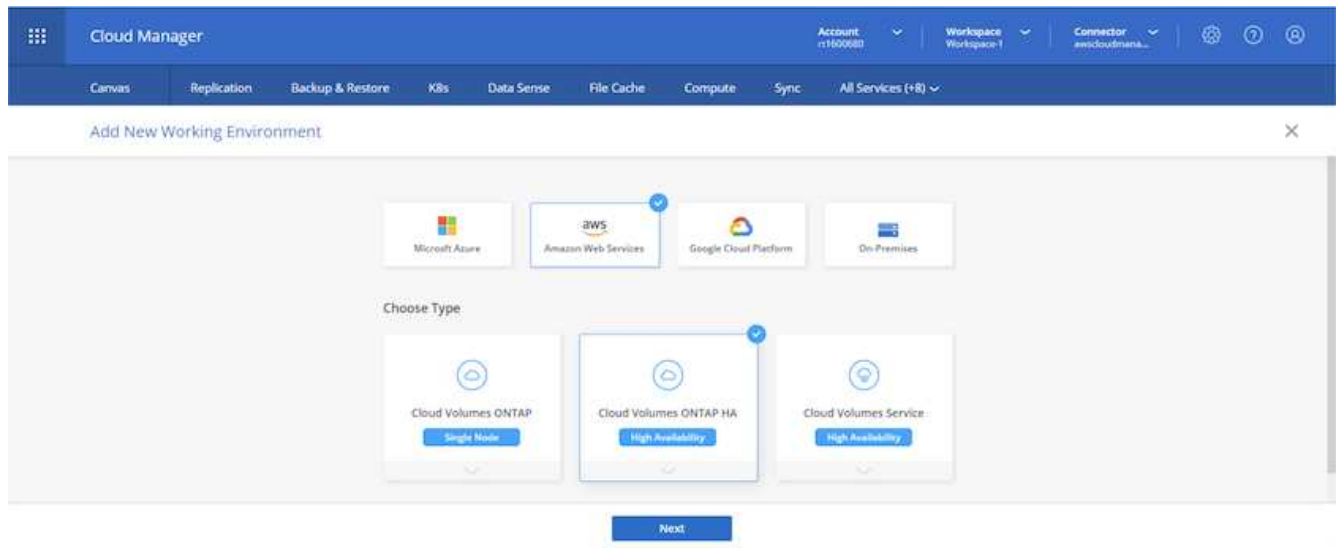
Connector Successfully Created

The Connector was created successfully.

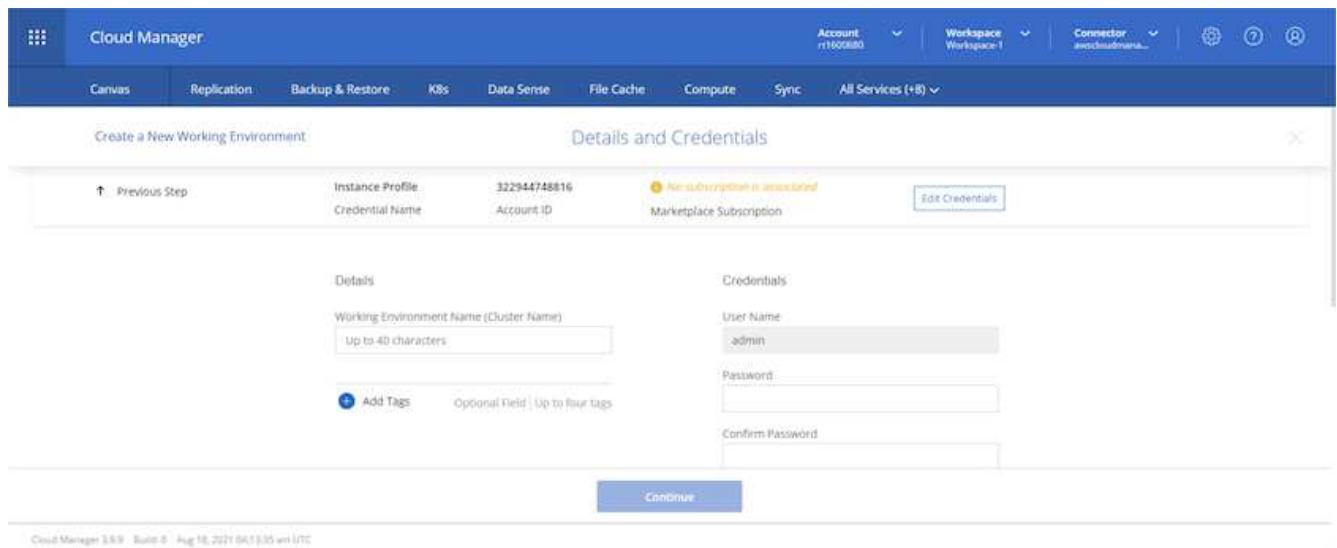
Continue

Implementare Cloud Volumes ONTAP

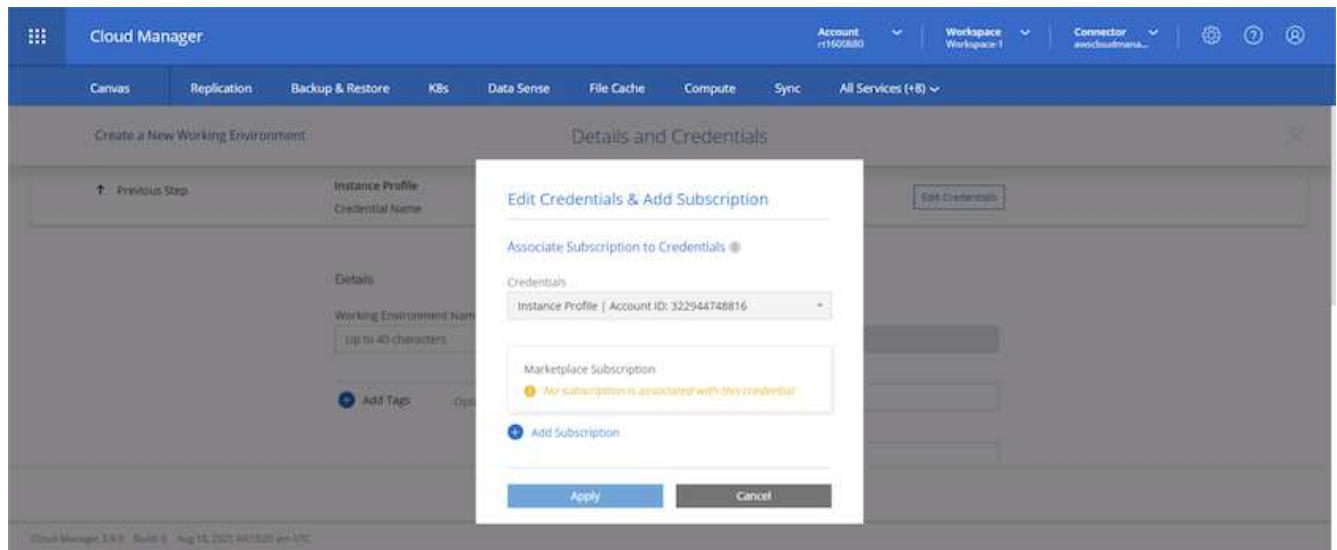
1. Selezionare AWS e il tipo di implementazione in base ai requisiti.



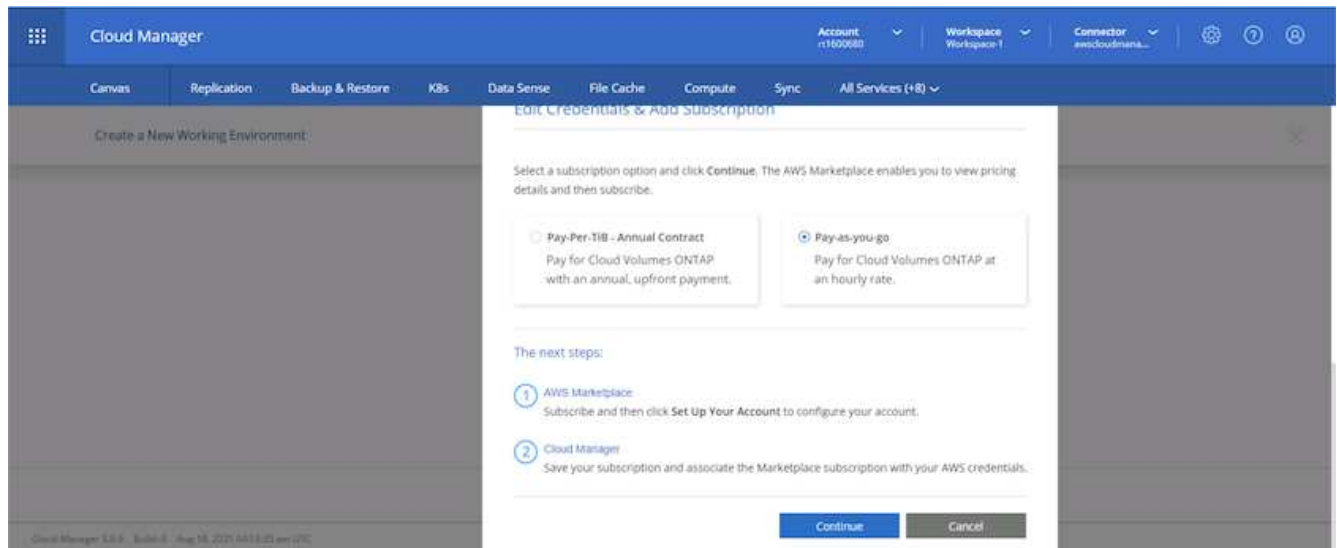
2. Se non è stato assegnato alcun abbonamento e si desidera effettuare l'acquisto con PAYGO, scegliere Modifica credenziali.



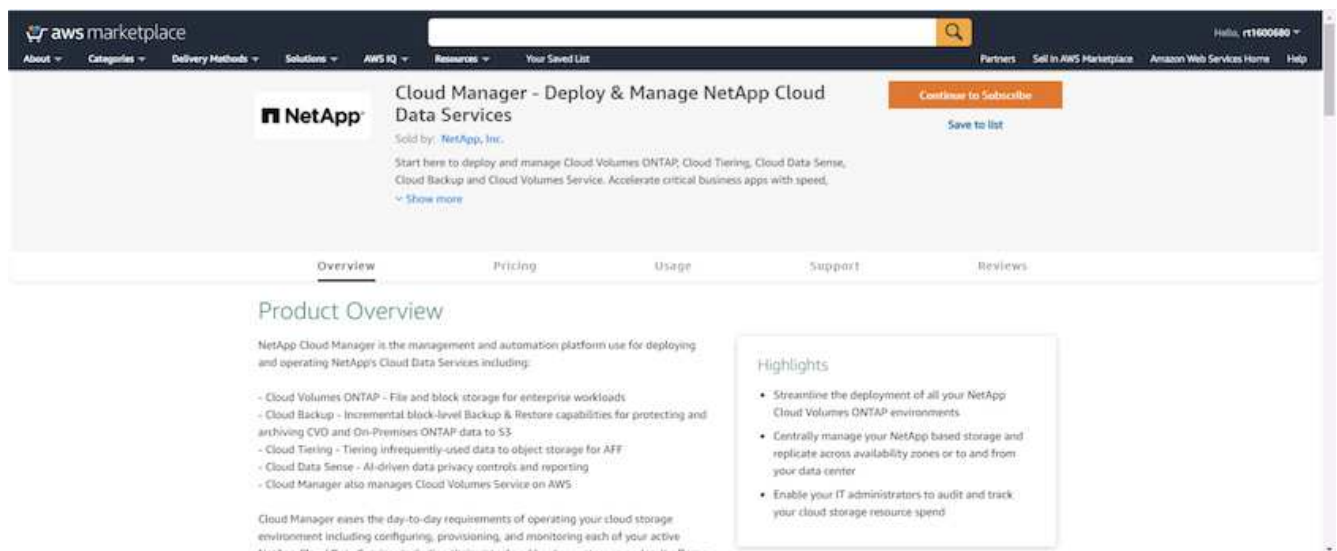
3. Scegliere Aggiungi abbonamento.



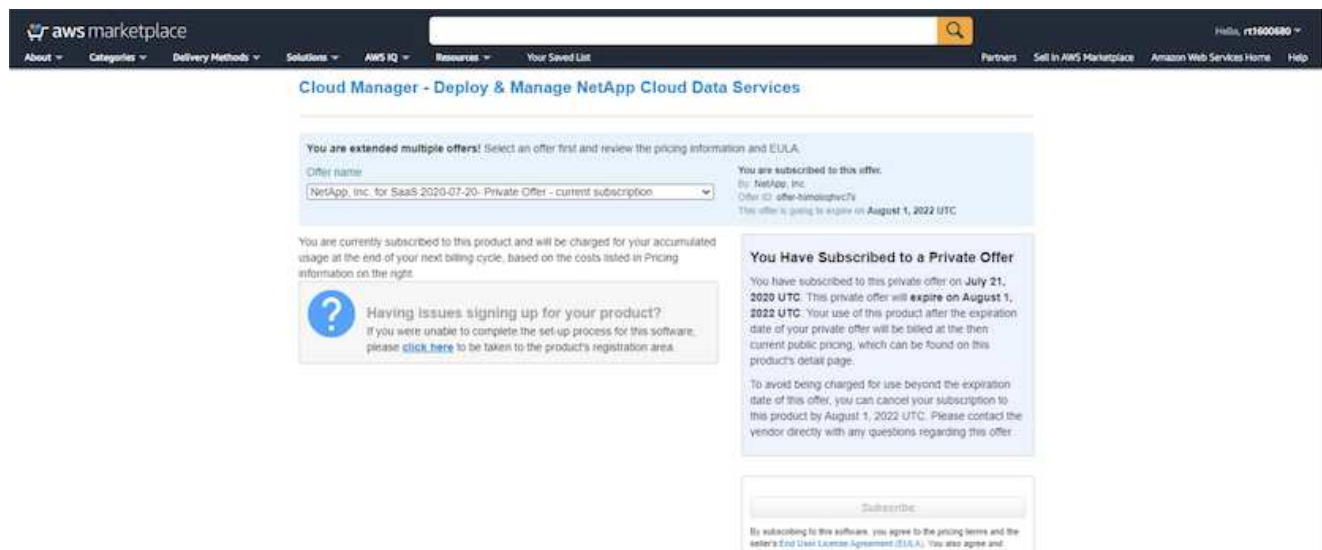
4. Scegliere il tipo di contratto a cui si desidera sottoscrivere. Ho scelto il pay-as-you-go.



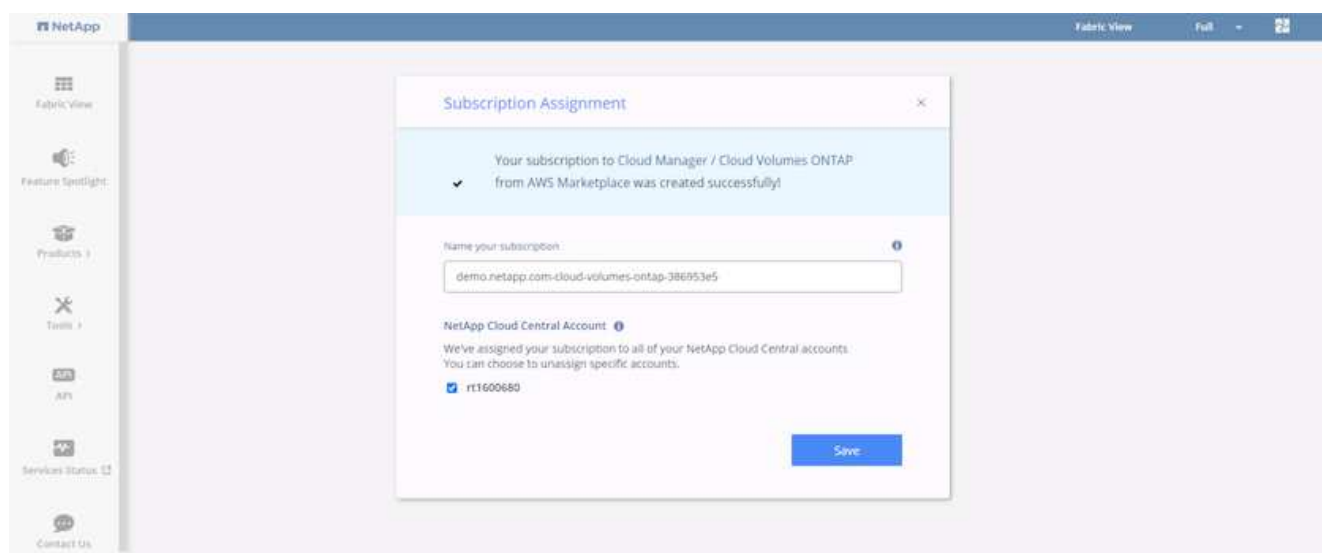
5. Si viene reindirizzati ad AWS; scegliere continua per iscriversi.



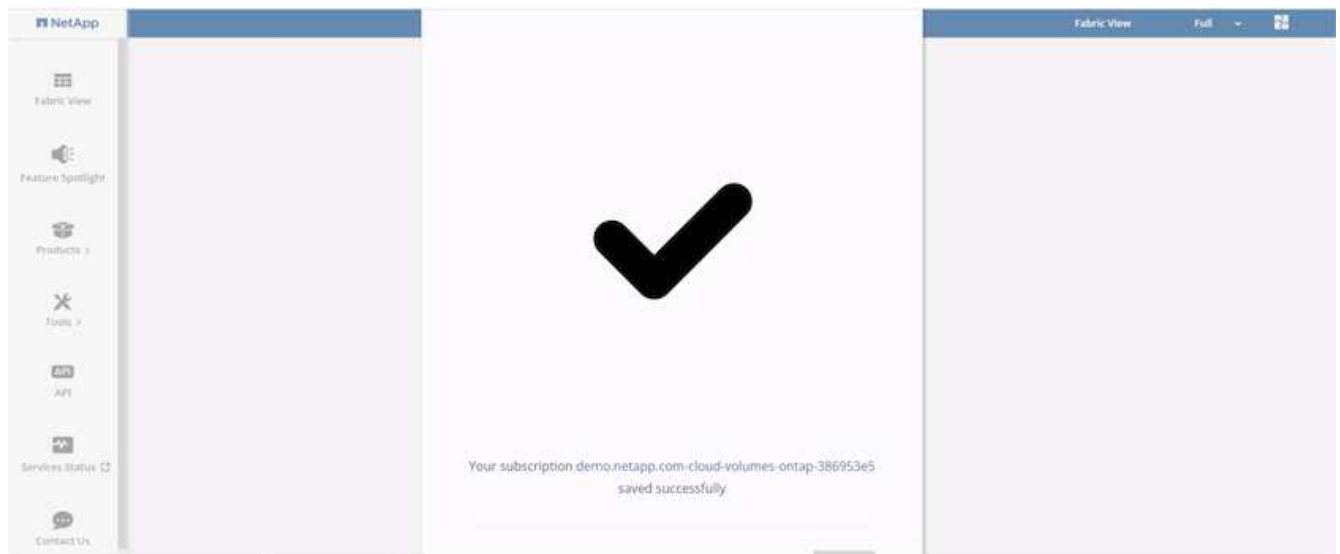
6. Iscriviti e verrai reindirizzato a NetApp Cloud Central. Se sei già iscritto e non ricevi il reindirizzamento, scegli il link "Clicca qui".



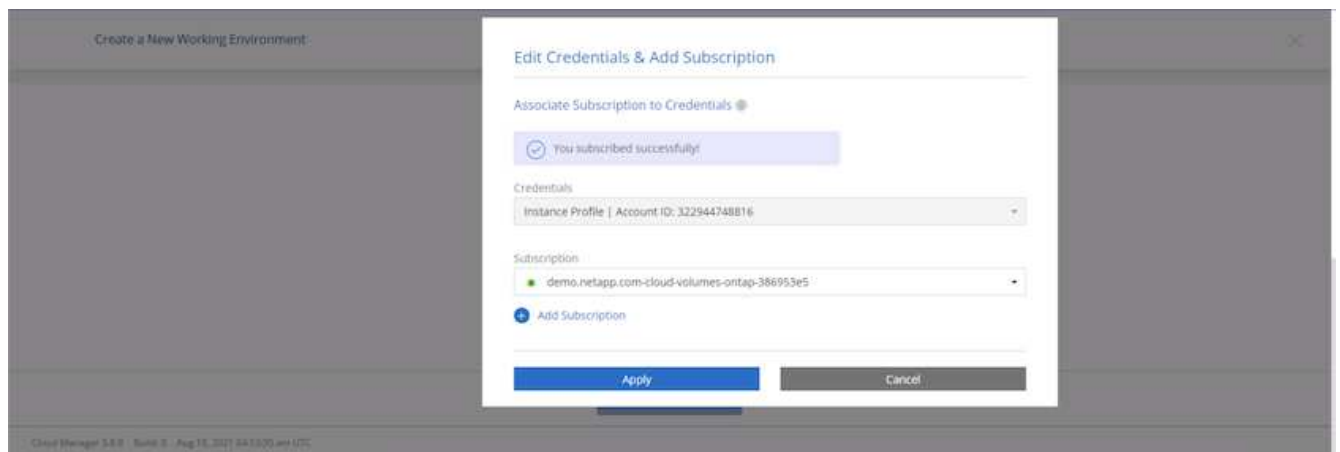
7. Verrai reindirizzato a Cloud Central dove devi assegnare un nome all'abbonamento e assegnarlo al tuo account Cloud Central.



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



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



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

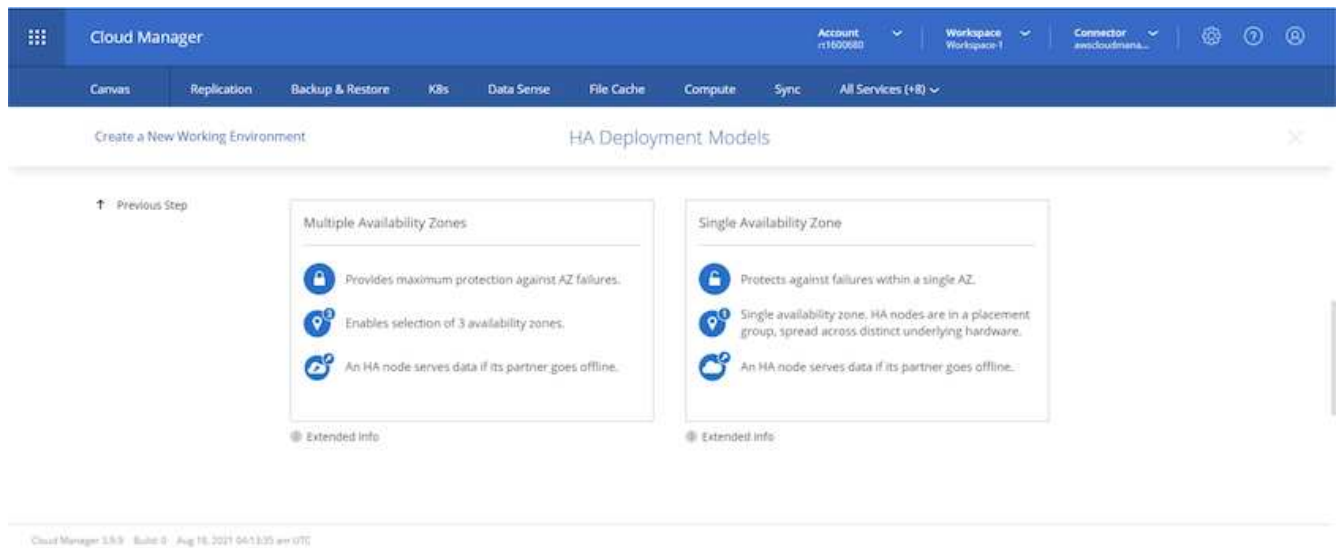
- a. Nome del cluster
- b. Password del cluster
- c. Tag AWS (opzionale)

The screenshot shows the 'Details and Credentials' step in the NetApp Cloud Manager interface. The top navigation bar includes 'Cloud Manager' and various service tabs like 'Canvas', 'Replication', 'Backup & Restore', etc. The main content area is titled 'Create a New Working Environment' and 'Details and Credentials'. It features a 'Previous Step' button and a table with instance profile details. Below this, there are two sections: 'Details' with a 'Working Environment Name (Cluster Name)' field set to 'hybridawsco' and an 'Add Tags' button, and 'Credentials' with 'User Name' (admin), 'Password', and 'Confirm Password' fields. A 'Continue' button is at the bottom.

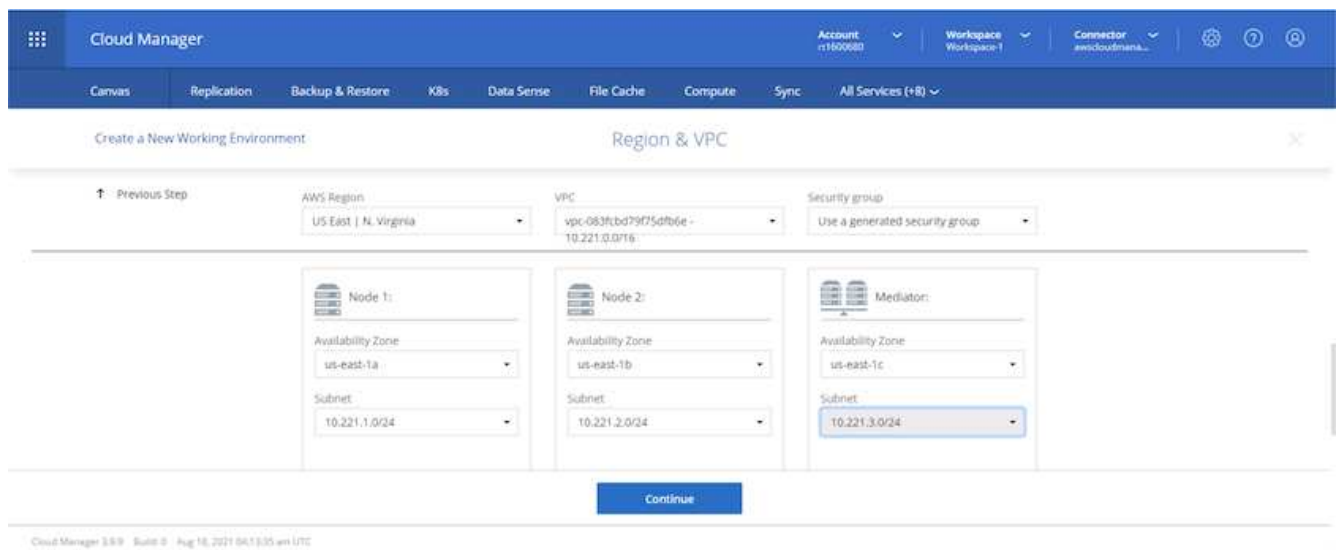
11. Scegliere i servizi aggiuntivi che si desidera implementare. Per ulteriori informazioni su questi servizi, visitare il ["Homepage di NetApp Cloud"](#).

The screenshot shows the 'Services' step in the NetApp Cloud Manager interface. The top navigation bar is the same as the previous screenshot. The main content area is titled 'Create a New Working Environment' and 'Services'. It features a 'Previous Step' button and a list of three services: 'Data Sense & Compliance', 'Backup to Cloud', and 'Monitoring'. Each service has a toggle switch and a dropdown arrow, all of which are currently turned on. A 'Continue' button is at the bottom.

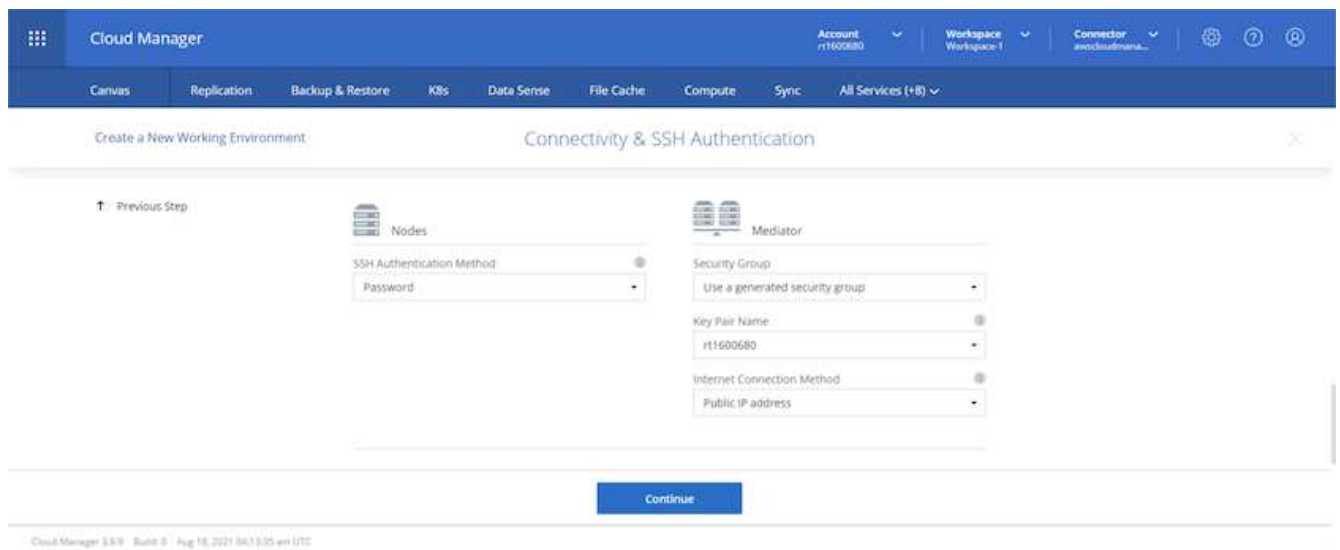
12. Scegliere se eseguire l'implementazione in più zone di disponibilità (si recuperano tre subnet, ciascuna in un AZ diverso) o in una singola zona di disponibilità. Ho scelto più AZS.



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



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





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

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

Cloud Manager Account: r1618349 Workspace: Workspace-1 Connector: awscloudmana...

Create a New Working Environment Floating IPs

↑ Previous Step

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

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

Floating IP address for cluster management
10.222.0.200

Floating IP address 1 for NFS and CIFS data
10.222.0.201

Floating IP address 2 for NFS and CIFS data
10.222.0.202

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

Continue

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

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

Create a New Working Environment Route Tables

↑ Previous Step

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

Additional information ⓘ

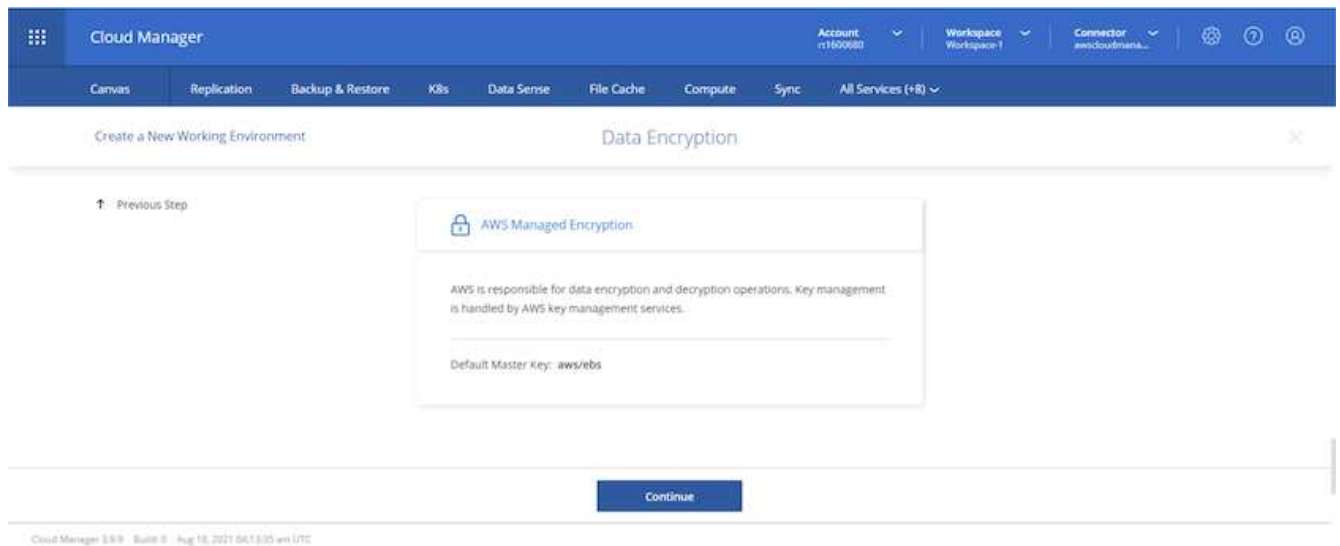
<input checked="" type="checkbox"/>	Name	Main	ID	Associate with Subnet	Tags
<input checked="" type="checkbox"/>	private_rt_r1600680	No	rtb-08b4cb88f5c826a5	3 Subnets	1 Tags
<input checked="" type="checkbox"/>	public_rt_r1600680	Yes	rtb-0e46720d0da10c593	1 Subnets	1 Tags

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

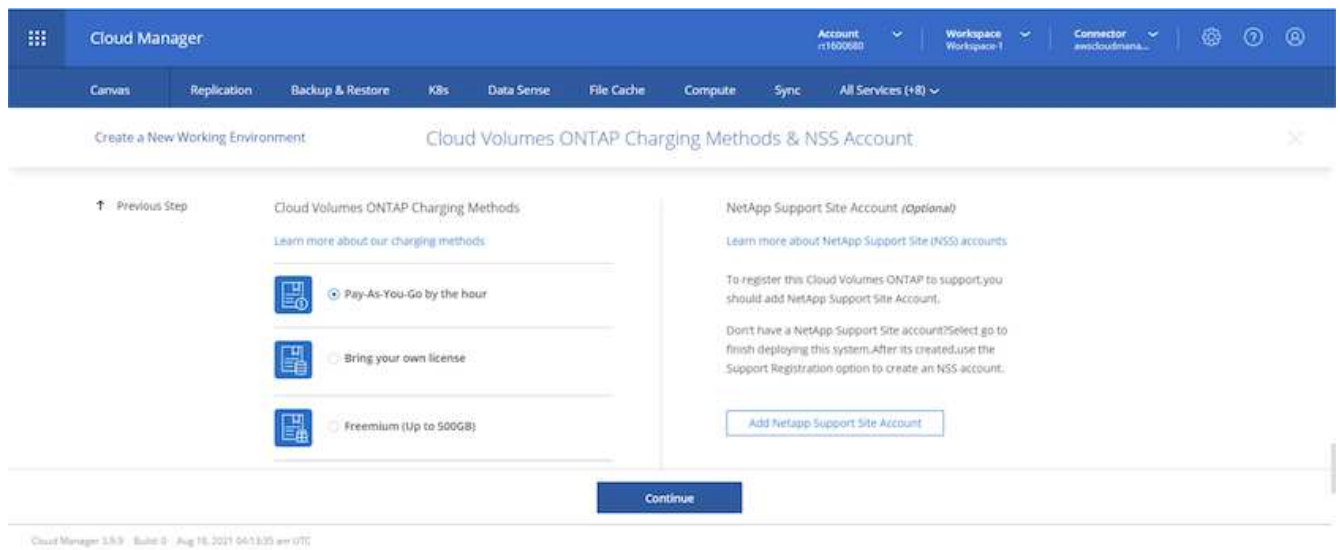
Continue

Cloud Manager 3.8.9 Build 0 Aug 18, 2021 06:13:35 am UTC

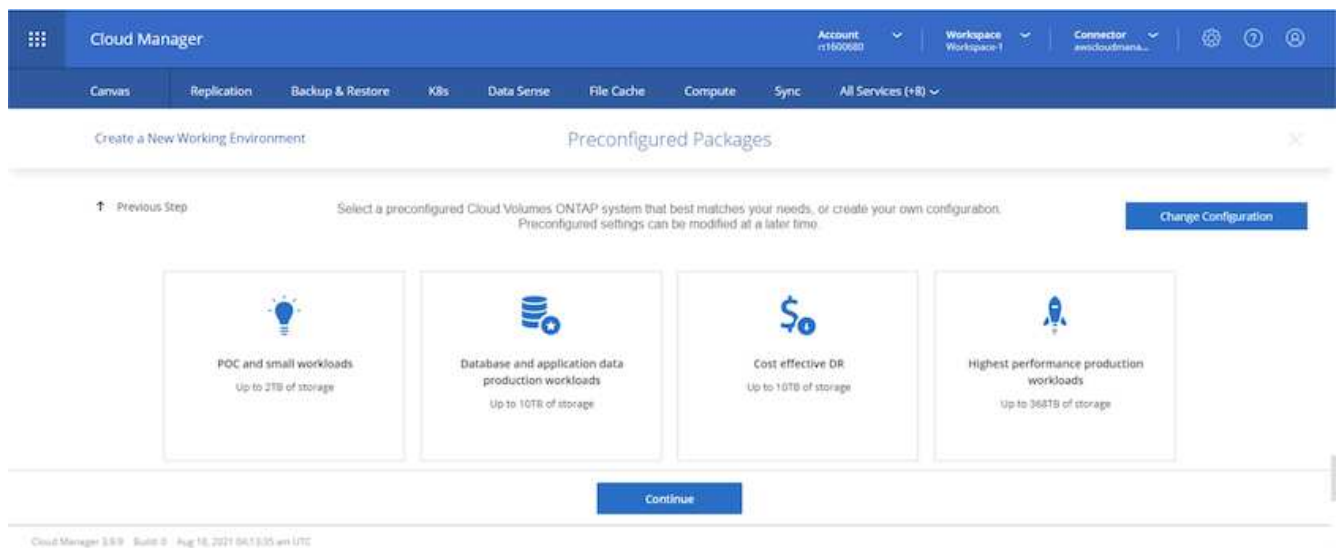
3. Scegliere se attivare la crittografia gestita AWS o AWS KMS per crittografare i dischi root, boot e dati ONTAP.



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



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



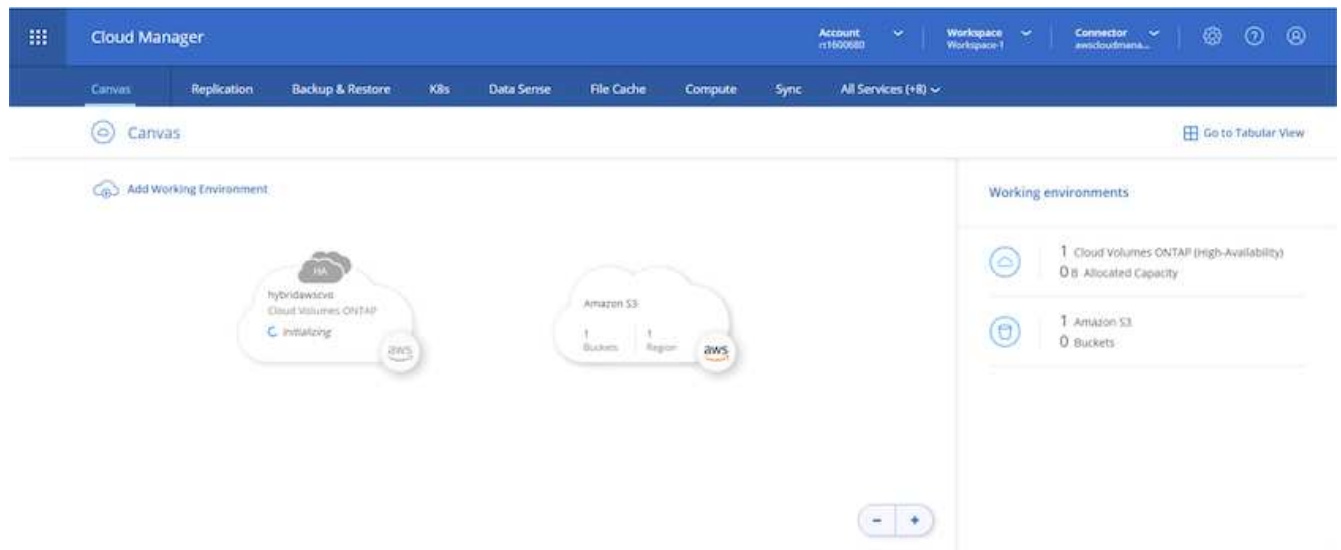
6. Se si desidera, creare un volume. Questo non è necessario, perché le fasi successive utilizzano SnapMirror, che crea i volumi per noi.

The screenshot shows the 'Create Volume' wizard in the Cloud Manager interface. The top navigation bar includes 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+8)'. The main header shows 'Create a New Working Environment' and 'Create Volume'. The 'Details & Protection' section includes a 'Volume Name' field, a 'Size (GiB)' field with a 'Volume size' button, a 'Snapshot Policy' dropdown set to 'default', and a 'Default Policy' button. The 'Protocol' section has tabs for 'NFS', 'CIFS', and 'iSCSI'. Under 'NFS', there is an 'Access Control' dropdown set to 'Custom export policy', a 'Custom export policy' field with the value '10.221.0.0/16', and an 'Advanced options' dropdown. At the bottom, there are 'Continue' and 'Skip' buttons. The footer indicates 'Cloud Manager 5.8.9 Build 0 Aug 18, 2021 04:13:35 am UTC'.

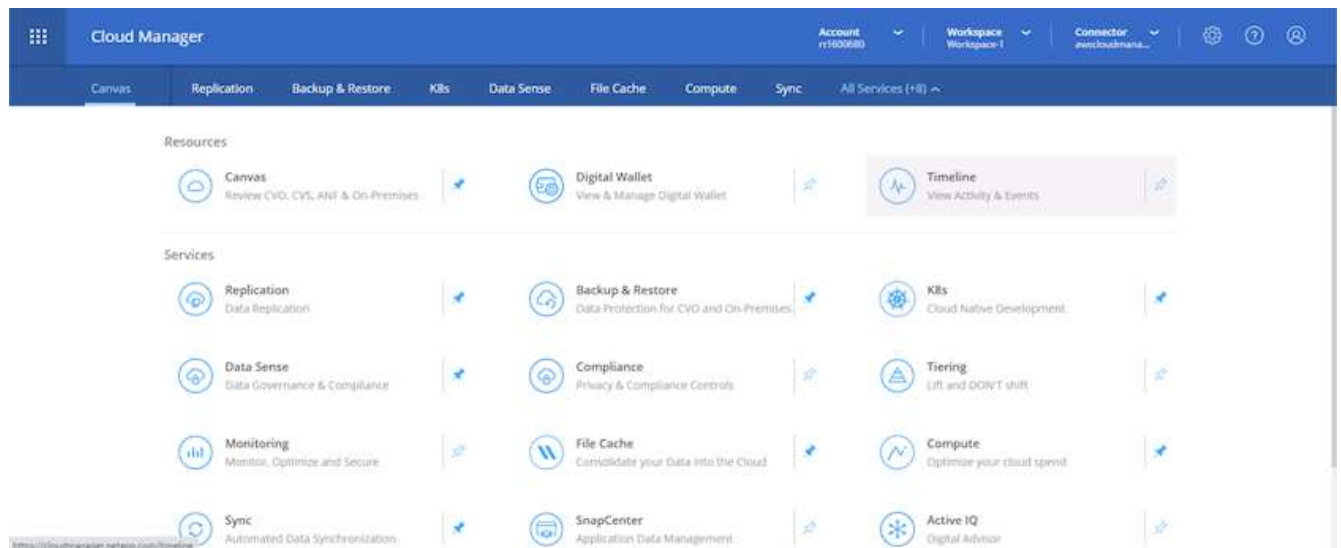
7. Esaminare le selezioni effettuate e spuntare le caselle per verificare che Cloud Manager implementa le risorse nel proprio ambiente AWS. Quando si è pronti, fare clic su Go (Vai).

The screenshot shows the 'Review & Approve' wizard in the Cloud Manager interface. The top navigation bar is the same as the previous screenshot. The main header shows 'Create a New Working Environment' and 'Review & Approve'. The 'Previous Step' section shows 'hybridawscvo' with tabs for 'AWS', 'us-east-1', and 'HA'. There are two checkboxes: 'I understand that in order to activate support, I must first register Cloud Volumes ONTAP with NetApp. More information >' and 'I understand that Cloud Manager will allocate the appropriate AWS resources to comply with my above requirements. More information >'. Below these are three tabs: 'Overview', 'Networking', and 'Storage'. The 'Overview' tab is active, showing a table with the following details: 'Storage System: Cloud Volumes ONTAP HA', 'License Type: Cloud Volumes ONTAP Standard', 'Capacity Limit: 10TB', 'HA Deployment Model: Multiple Availability Zones', 'Encryption: AWS Managed', and 'Customer Master Key: aws/ebs'. At the bottom, there is a 'Go' button. The footer indicates 'Cloud Manager 5.8.9 Build 0 Aug 18, 2021 04:13:35 am UTC'.

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



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



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

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

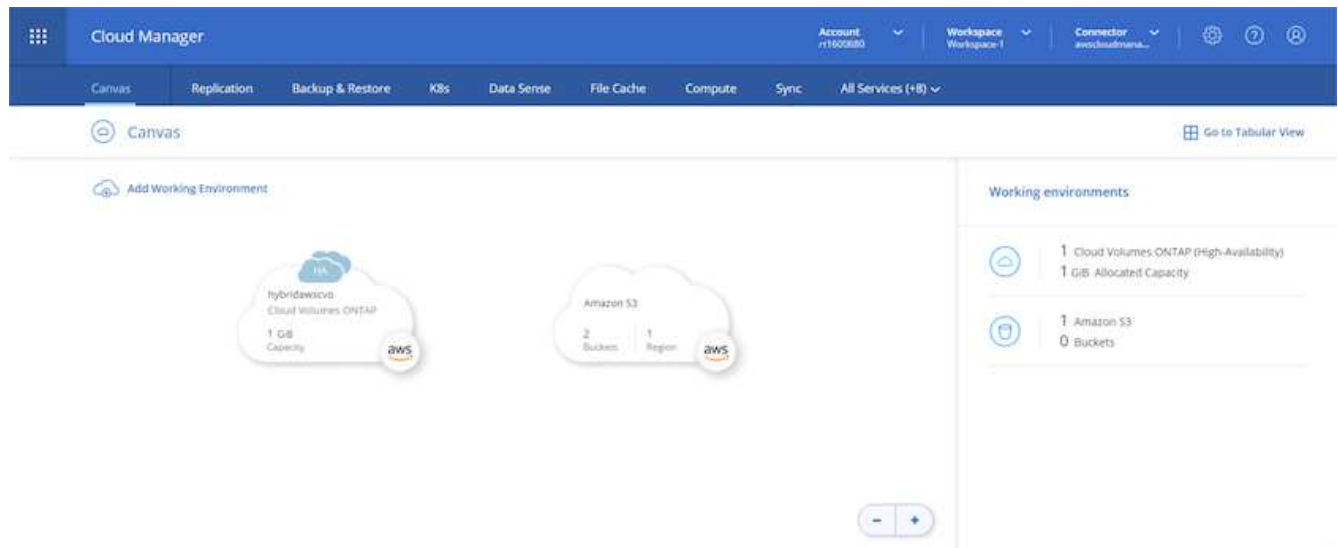
Canvas | Replication | Backup & Restore | K8s | Data Sense | File Cache | Compute | Sync | All Services (+8) v

Timeline

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

Time	Action	Service	Agent	Resource	User	Status
Aug 18 2021, 9:42:32 pm	Check Connectivity	Cloud Manager	awscloudmana...	hybridawsco	Full Name	Success
Aug 18 2021, 9:42:00 pm	Create Aws Ha Working Environment	Cloud Manager	awscloudma...	hybridawsco	Full Name	Pending
Aug 18 2021, 10:09:39 pm	Describe Operation Status					Success
Aug 18 2021, 10:00:03 pm	Describe Operation Status					Success

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

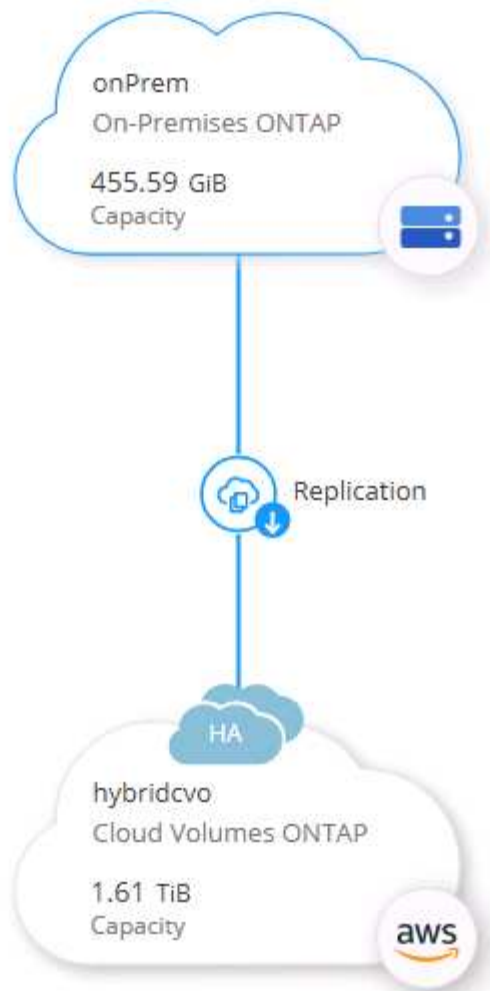


Configurare SnapMirror da on-premise a cloud

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

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

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



Selezionare Enable (attiva).

SERVICES



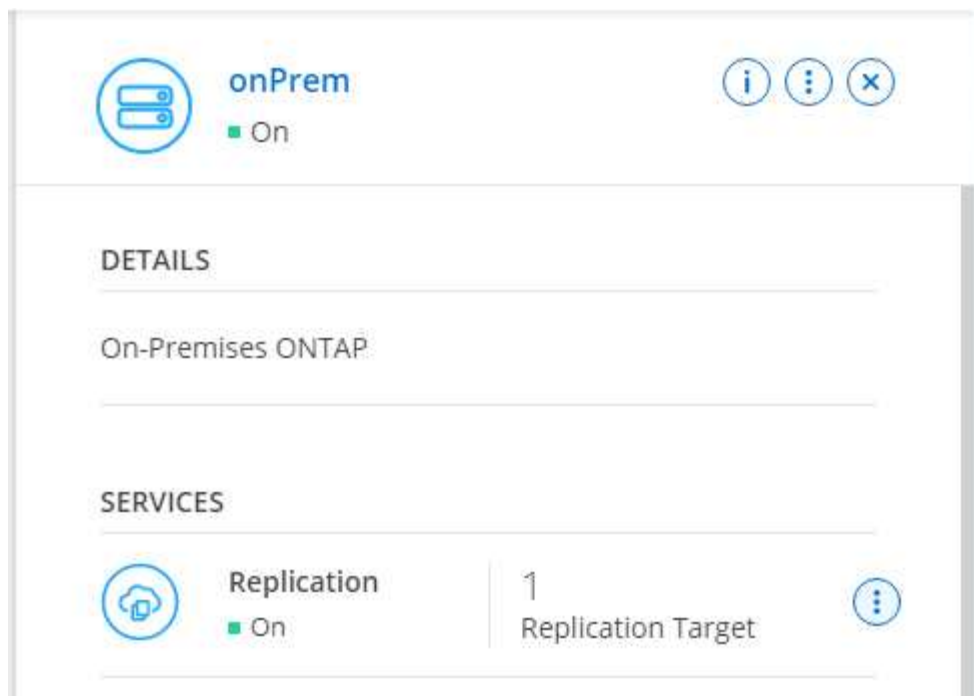
Replication

■ Off

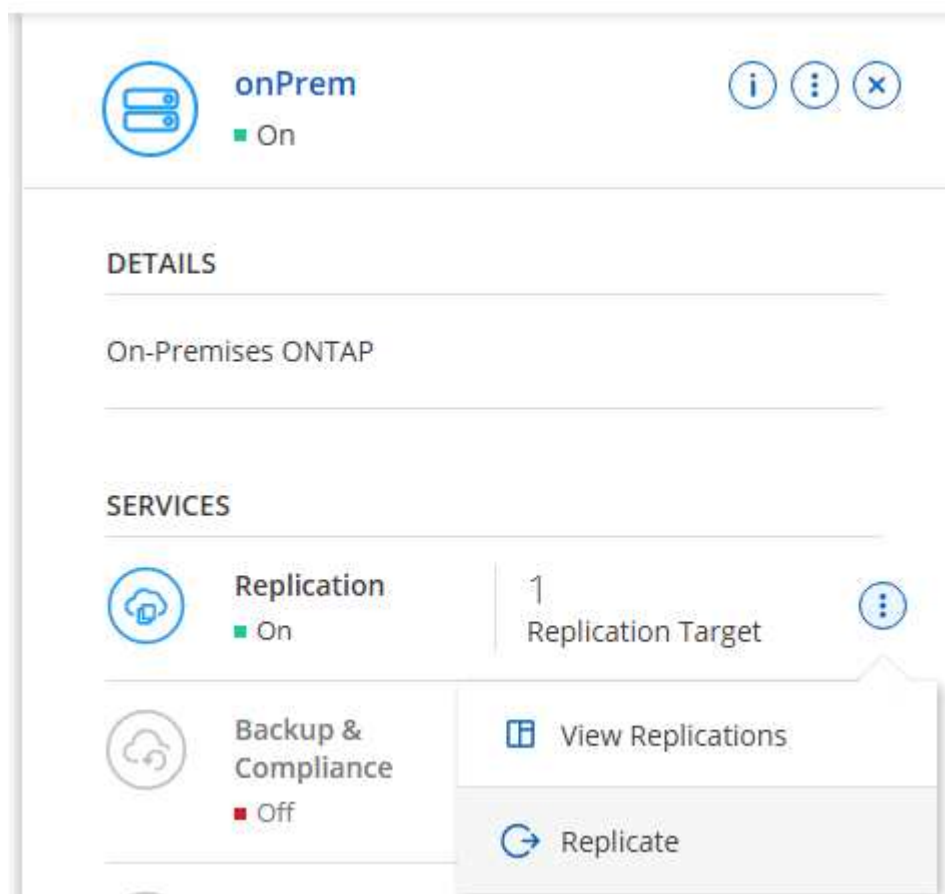
Enable



O Opzioni.



Replicare.



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

Replicate Data

From: onPrem

To: select the Working Environment to which you want to replicate data

Replication Target

hybridcvo (Cloud Volumes ONTAP) ✓

Start Replication Wizard Cancel

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

Replication Setup Source Volume Selection

Volume Name	Storage VM Name	Tiering Policy	Volume Type	Capacity	Allocated	Disk Used	Status
rhel2_u03	svm_onPrem	None	RW	100 GB	7.29 GB	7.29 GB	ONLINE
rhel2_u0309232119421203118	svm_onPrem	None	RW	100 GB	35.83 MB	35.83 MB	ONLINE
sql1_data	svm_onPrem	None	RW	53.37 GB	45.09 GB	45.09 GB	ONLINE
sql1_log	svm_onPrem	None	RW	21.35 GB	18.16 GB	18.16 GB	ONLINE
sql1_snapctr	svm_onPrem	None	RW	24.87 GB	21.23 GB	21.23 GB	ONLINE


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


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


Replication Setup Destination Disk Type and Tiering ×


[↑ Previous Step](#)

Destination Disk Type


General Purpose SSD


General Purpose SSD - Dynamic Performance


Throughput Optimized HDD

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

☒ Enabled ☐ Disabled

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

Continue

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

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

Destination Volume Name

Destination Volume Name

`sql1_data_dr`

Destination Aggregate

Automatically select the best aggregate ▼

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

Max Transfer Rate

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


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

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

Replication Policy


Default Policies

Additional Policies

 Mirror

Typically used for disaster recovery

More info

 Mirror and Backup (1 month retention)

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

More info

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

Replication Setup Schedule

↑ Previous Step Select a replication schedule

One-time copy

No schedule

10min

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

12-hourly

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

5min

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

6-hourly

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

8hour

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

daily

Every day
Hours: 12 AM
Minutes: 10th minute

hourly

Every hour
Minutes: 5th minute

monthly

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

pg-15-minutely

Every hour

pg-6-hourly

Every day

pg-daily

Every day

pg-daily-set2

Every day

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

Replication Setup Review & Approve

↑ Previous Step Review your selection and start the replication process

Source

onPrem

sql1_data

Destination

hybridcvo

sql1_data_copy

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

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

[Go](#)

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

Replication

7 Volume Relationships

153.32 GiB Replicated Capacity

0 Currently Transferring

7 Healthy

0 Failed

7 Volume Relationships

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

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

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

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

Dimensionamento dell'istanza di calcolo

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

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

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

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

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

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

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

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.