



Configurazione dei backup dei dati

Snap Creator Framework

NetApp
October 04, 2023

This PDF was generated from https://docs.netapp.com/it-it/snap-creator-framework/sap-hana-ops/task_configuring_the_backup_user_and_hdbuserstore.html on October 04, 2023. Always check docs.netapp.com for the latest.

Sommario

- Configurazione dei backup dei dati 1
 - Configurazione dell'utente di backup e di hdbuserstore 1
 - Configurazione delle relazioni SnapVault..... 2
 - Avvio delle relazioni SnapVault 3
 - Configurazione di Snap Creator Framework e backup del database SAP HANA 5

Configurazione dei backup dei dati

Dopo aver installato i componenti software richiesti, attenersi alla seguente procedura per completare la configurazione:

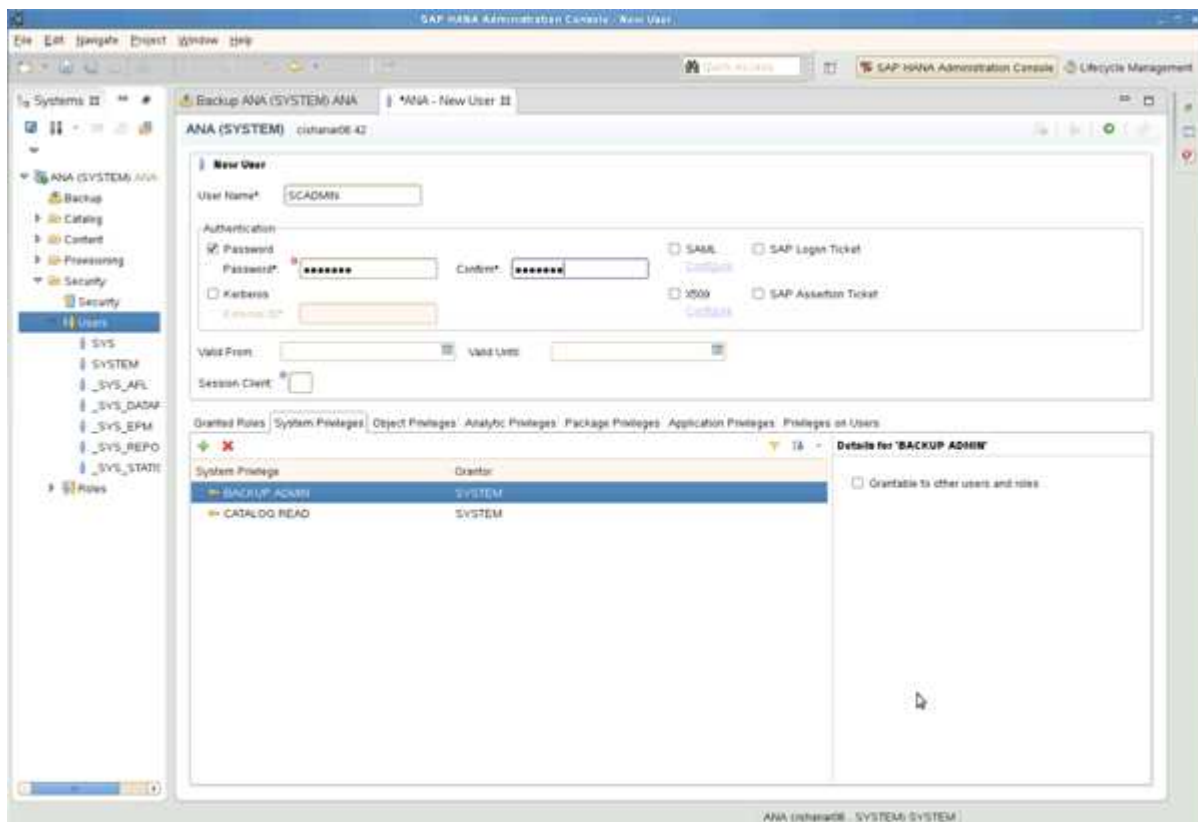
1. Configurare un utente di database dedicato e l'archivio utenti SAP HANA.
2. Preparare la replica SnapVault su tutti i controller di storage.
3. Creazione di volumi nel controller dello storage secondario.
4. Inizializzare le relazioni SnapVault per i volumi di database.
5. Configurare Snap Creator.

Configurazione dell'utente di backup e di hdbuserstore

È necessario configurare un utente di database dedicato all'interno del database HANA per eseguire le operazioni di backup con Snap Creator. In una seconda fase, è necessario configurare una chiave dell'archivio utenti SAP HANA per questo utente di backup. Questa chiave dell'archivio utenti viene utilizzata all'interno della configurazione del plug-in SAP HANA di Snap Creator.

L'utente del backup deve disporre dei seguenti privilegi:

- AMMINISTRATORE BACKUP
- CATALOGO LETTO



1. Nell'host di amministrazione, l'host in cui è stato installato Snap Creator, viene configurata una chiave

userstore per tutti gli host di database che appartengono al database SAP HANA. La chiave dello userstore è configurata con l'utente root del sistema operativo: Hdbuserstore set keyhost 3[instance]15 userpassword

2. Configurare una chiave per tutti e quattro i nodi di database.

```
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore set SCADMIN08
cishanar08:34215 SCADMIN Password
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore set SCADMIN09
cishanar09:34215 SCADMIN Password
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore set SCADMIN10
cishanar10:34215 SCADMIN password
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore set SCADMIN11
cishanar11:34215 SCADMIN Password
mgmtsrv01:/usr/sap/hdbclient32 # ./hdbuserstore LIST
DATA FILE          : /root/.hdb/mgmtsrv01/SSFS_HDB.DAT

KEY SCADMIN08
  ENV : cishanar08:34215
  USER: SCADMIN
KEY SCADMIN09
  ENV : cishanar09:34215
  USER: SCADMIN
KEY SCADMIN10
  ENV : cishanar10:34215
  USER: SCADMIN
KEY SCADMIN11
  ENV : cishanar11:34215
  USER: SCADMIN
mgmtsrv01:/usr/sap/hdbclient32
```

Configurazione delle relazioni SnapVault

Quando si configurano le relazioni SnapVault, i controller di storage primari devono avere una licenza SnapRestore e SnapVault valida installata. Lo storage secondario deve disporre di una licenza SnapVault valida.

1. Abilitare SnapVault e NDMP sui controller dello storage primario e secondario.

```

hana1a> options snapvault.enable on
hana1a> ndmp on
hana1a>
hana1b> options snapvault.enable on
hana1b> ndmpd on
hana1b>
hana2b> options snapvault.enable on
hana2b> ndmpd on
hana2b>

```

2. Su tutti i controller dello storage primario, configurare l'accesso al controller dello storage secondario.

```

hana1a> options snapvault.access host=hana2b
hana1a>
hana1b> options snapvault.access host=hana2b
hana1b>

```



Si consiglia di utilizzare una rete dedicata per il traffico di replica. In questi casi, è necessario configurare il nome host di questa interfaccia nel controller dello storage secondario. Invece di hana2b, il nome host potrebbe essere hana2b-REP.

3. Sul controller dello storage secondario, configurare l'accesso per tutti i controller dello storage primario.

```

hana2b> options snapvault.access host=hana1a,hana1b
hana2b>

```



Si consiglia di utilizzare una rete dedicata per il traffico di replica. In questi casi, è necessario configurare il nome host di questa interfaccia nei controller di storage primari. Invece di hana1b e hana1a il nome host potrebbe essere hana1a-REP e hana1b-REP.

Avvio delle relazioni SnapVault

È necessario avviare la relazione SnapVault con Data ONTAP che opera in 7-Mode e Clustered Data ONTAP.

Avvio delle relazioni SnapVault con Data ONTAP in 7-Mode

È possibile avviare una relazione SnapVault con i comandi eseguiti sul sistema di storage secondario.

1. Per i sistemi storage che eseguono Data ONTAP in 7-Mode, è possibile avviare le relazioni SnapVault eseguendo il seguente comando:

```

hana2b> snapvault start -S hana1a:/vol/data_00001/mnt00001
/vol/backup_data_00001/mnt00001
Snapvault configuration for the qtree has been set.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
hana2b>
hana2b> snapvault start -S hana1a:/vol/data_00003/mnt00003
/vol/backup_data_00003/mnt00003
Snapvault configuration for the qtree has been set.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
hana2b>
hana2b> snapvault start -S hana1b:/vol/data_00002/mnt00002
/vol/backup_data_00002/mnt00002
Snapvault configuration for the qtree has been set.
Transfer started.
Monitor progress with 'snapvault status' or the snapmirror log.
hana2b>

```



Si consiglia di utilizzare una rete dedicata per il traffico di replica. In tal caso, configurare il nome host di questa interfaccia sui controller di storage primari. Invece di hana1b e hana1a, il nome host potrebbe essere hana1a-REP e hana1b-REP.

Avvio delle relazioni SnapVault con Clustered Data ONTAP

È necessario definire un criterio SnapMirror prima di avviare una relazione SnapVault.

1. Per i sistemi storage che eseguono Clustered Data ONTAP, avviare le relazioni SnapVault eseguendo il seguente comando.

```
hana::> snapmirror policy create -vserver hana2b -policy SV_HANA
hana::> snapmirror policy add-rule -vserver hana2b -policy SV_HANA
-snapmirror-label daily -keep 20
hana::> snapmirror policy add-rule -vserver hana2b -policy SV_HANA
-snapmirror-label hourly -keep 10
```

```
hana::> snapmirror policy show -vserver hana2b -policy SV_HANA
```

```

                Vserver: hana2b
    SnapMirror Policy Name: SV_HANA
                Policy Owner: vserver-admin
                Tries Limit: 8
        Transfer Priority: normal
Ignore accesstime Enabled: false
    Transfer Restartability: always
                Comment: -
    Total Number of Rules: 2
                Total Keep: 8
                Rules: Snapmirror-label  Keep  Preserve  Warn
                      -----  -----  -----  ----
                      daily           20   false      0
                      hourly          10   false      0

```

Il criterio deve contenere regole per tutte le classi di conservazione (etichette) utilizzate nella configurazione di Snap Creator. I comandi sopra riportati mostrano come creare una policy SnapMirror dedicata SV_HANA

2. Per creare e avviare la relazione SnapVault sulla console del cluster di backup, eseguire i seguenti comandi.

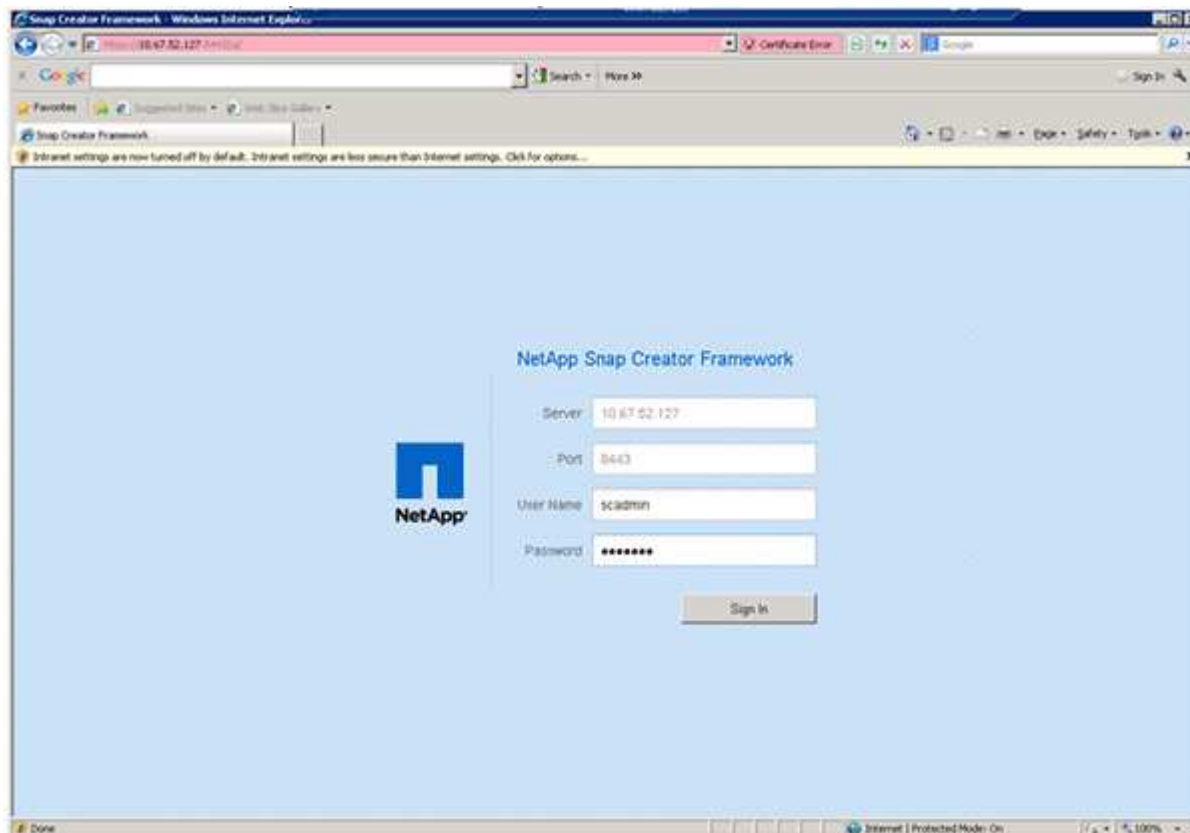
```
hana::> snapmirror create -source-path hanala:hana_data -destination
-path
hana2b:backup_hana_data -type XDP -policy SV_HANA
Operation succeeded: snapmirror create the relationship with destination
hana2b:backup_hana_data.

hana::> snapmirror initialize -destination-path hana2b:backup_hana_data
-type XDP
```

Configurazione di Snap Creator Framework e backup del database SAP HANA

È necessario configurare Snap Creator Framework e il backup del database SAP HANA.

1. Connettersi all'interfaccia grafica utente (GUI) di Snap Creator: <https://host:8443/ui/>.
2. Accedere utilizzando il nome utente e la password configurati durante l'installazione. Fare clic su **Accedi**.

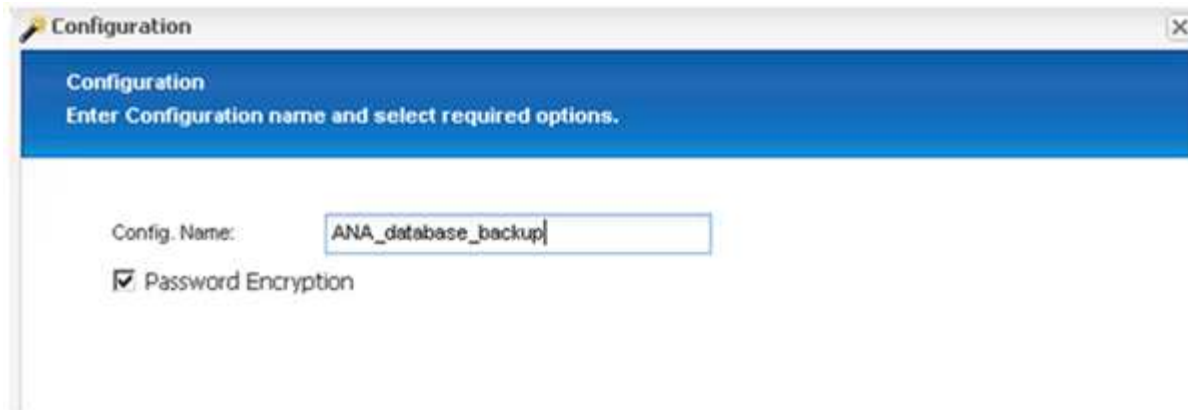


3. Immettere un nome per il profilo e fare clic su **OK**.



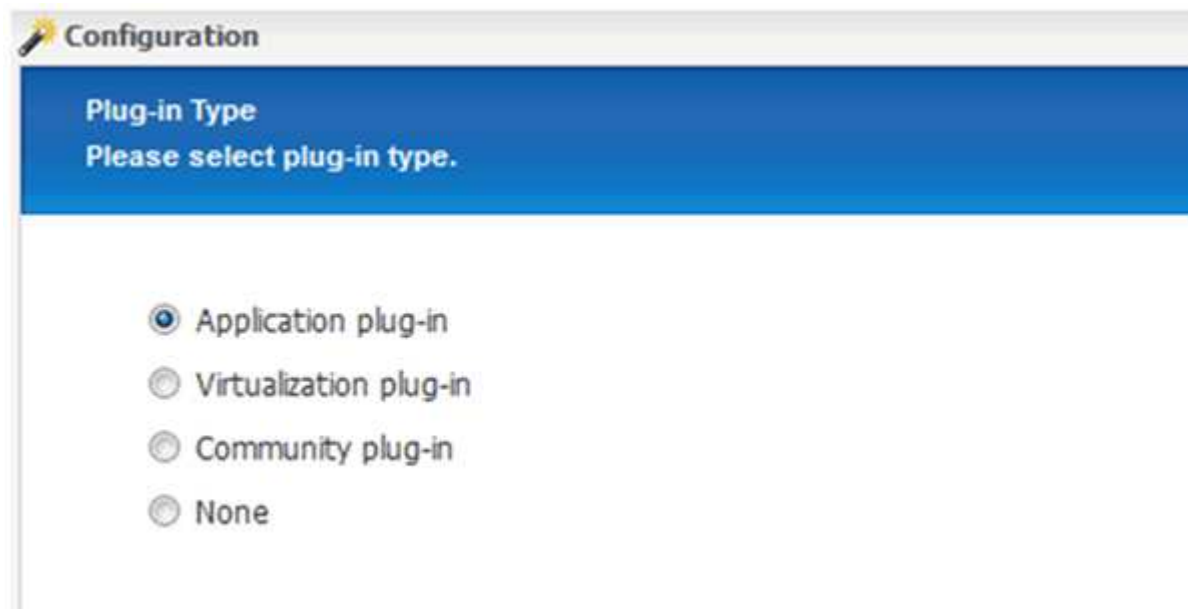
Ad esempio, "ANA" è il SID del database.

4. Inserire il nome della configurazione e fare clic su **Avanti**.



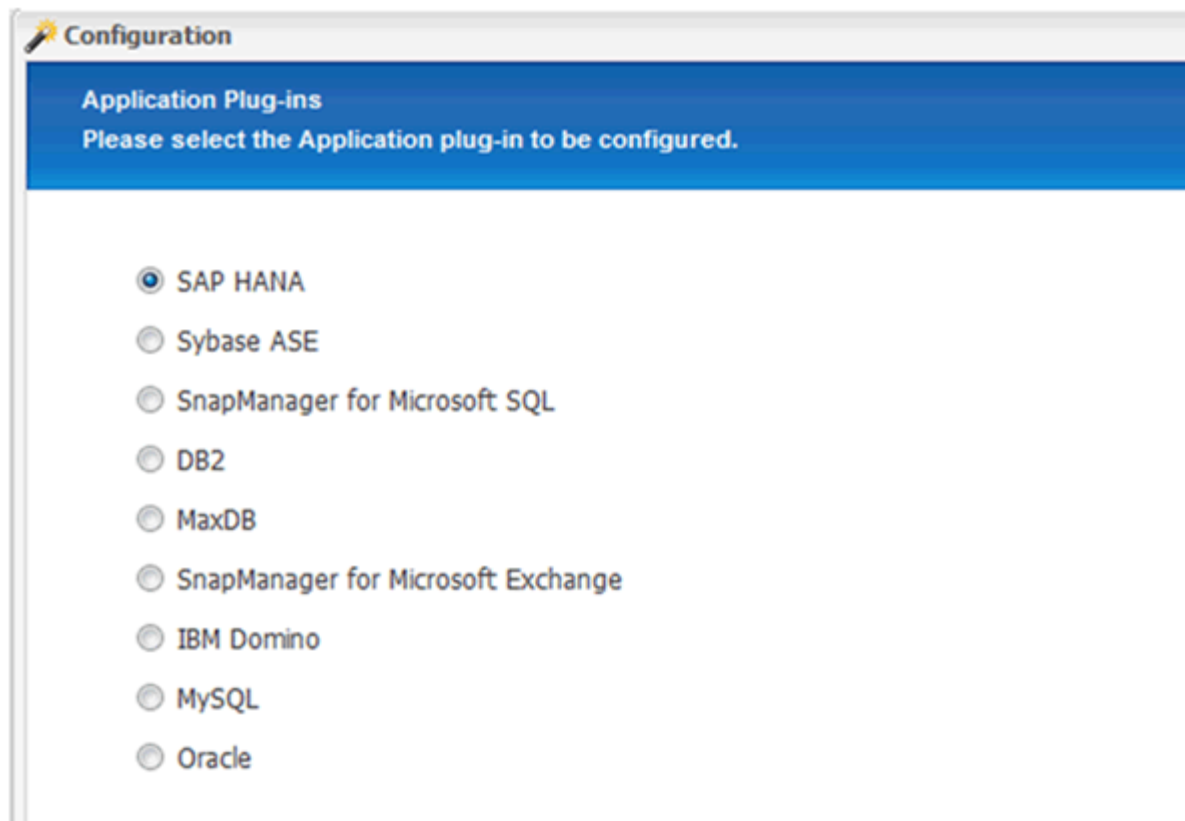
A screenshot of a 'Configuration' dialog box. The title bar says 'Configuration' with a close button. The main area has a blue header with the text 'Configuration' and 'Enter Configuration name and select required options.' Below this, there is a text field labeled 'Config. Name:' containing the text 'ANA_database_backup'. Below the text field is a checkbox labeled 'Password Encryption' which is checked.

5. Selezionare **Application plug-in** come tipo di plug-in e fare clic su **Next**.



A screenshot of a 'Configuration' dialog box titled 'Plug-in Type' with the instruction 'Please select plug-in type.' Below the header, there are four radio button options: 'Application plug-in' (which is selected), 'Virtualization plug-in', 'Community plug-in', and 'None'.

6. Selezionare **SAP HANA** come plug-in dell'applicazione e fare clic su **Avanti**.



7. Immettere i seguenti dettagli di configurazione:

- a. Selezionare **Sì** dal menu a discesa per utilizzare la configurazione con un database multi-tenant. Per un singolo database container, selezionare **No**.
- b. Se il contenitore di database multitenant è impostato su **No**, è necessario fornire il SID del database.
- c. Se il contenitore di database multitenant è impostato su **Sì**, è necessario aggiungere le chiavi hdbuserstore per ogni nodo SAP HANA.
- d. Aggiungere il nome del database tenant.
- e. Aggiungere i nodi HANA su cui deve essere eseguita l'istruzione hdbsql.
- f. Inserire il numero di istanza del nodo HANA.
- g. Fornire il percorso del file eseguibile hdbsql.
- h. Aggiungere l'utente OSDB.
- i. Selezionare **Sì** dall'elenco a discesa per attivare la pulizia DEL REGISTRO.

NOTA:

- Parametro HANA_SID è disponibile solo se il valore per il parametro HANA_MULTITENANT_DATABASE è impostato su N
- Per i container di database multi-tenant (MDC) con un tipo di risorsa "Ssingolo tenant", le copie Snapshot di SAP HANA funzionano con l'autenticazione basata su chiave di UserStore. Se il HANA_MULTITENANT_DATABASE il parametro è impostato su Y, quindi il HANA_USERSTORE_KEYS il parametro deve essere impostato sul valore appropriato.
- Analogamente ai container di database non multitenant, è supportata la funzionalità di backup basato su file e di controllo dell'integrità

j. Fare clic su **Avanti**.

Multitenant Database Container (MDC) - Single Tenant:	No
SID:	H66
hdbuserstore Keys:	
Tenant Database Name:	
Nodes:	10.235.220.66
Username:	SYSTEM
Password:	*****
Instance number:	66
Path to hdbsql:	/usr/sap/H66/HDB66/exe/hdbsql
OSDB User:	
Enable LOG Cleanup:	Yes

8. Abilitare l'operazione di backup basato su file:

- Impostare il percorso di backup del file.
- Specificare il prefisso file-backup.
- Selezionare la casella di controllo **Enable file-Backup** (Abilita backup file).
- Fare clic su **Avanti**.

The screenshot shows a 'Configuration' window with a blue header bar containing the text 'File-Based Backup Configuration Details' and 'Provide File-Based Backup Details'. Below the header, there are three input fields: 'File-Backup Location:', 'File-Backup prefix:', and 'Enable File-Backup:'. The 'Enable File-Backup:' field is a checkbox. At the bottom right of the window, there are three buttons: 'Back', 'Next', and 'Cancel'.

9. Abilitare l'operazione di verifica dell'integrità del database:
 - a. Impostare la posizione di file-Backup temporanea.
 - b. Selezionare la casella di controllo **attiva controllo integrità DB**.
 - c. Fare clic su **Avanti**.

The screenshot shows a window titled "Configuration" with a sub-header "Integrity Check Configuration Details" and the instruction "Provide Integrity Check Details". Below this, there are two configuration options: "Temporary File-Backup Location:" followed by an empty text input field, and "Enable DB Integrity Check:" followed by an unchecked checkbox.

10. Inserire i dettagli del parametro di configurazione dell'agente e fare clic su **Avanti**.

The screenshot shows a window titled "Agent Configuration" with the instruction "Enter agent configuration details". It contains three input fields: "IP/DNS:" with the value "localhost", "Port:" with the value "9090", and "Timeout (secs):" with the value "300". Below these fields is a button labeled "Test agent connection".

11. Inserire le impostazioni di connessione dello storage e fare clic su **Avanti**.

Storage Connection Settings
Please Provide Storage Connection Settings

Use OnCommand Proxy: ☐

Transport:

Controller/Vserver Port:

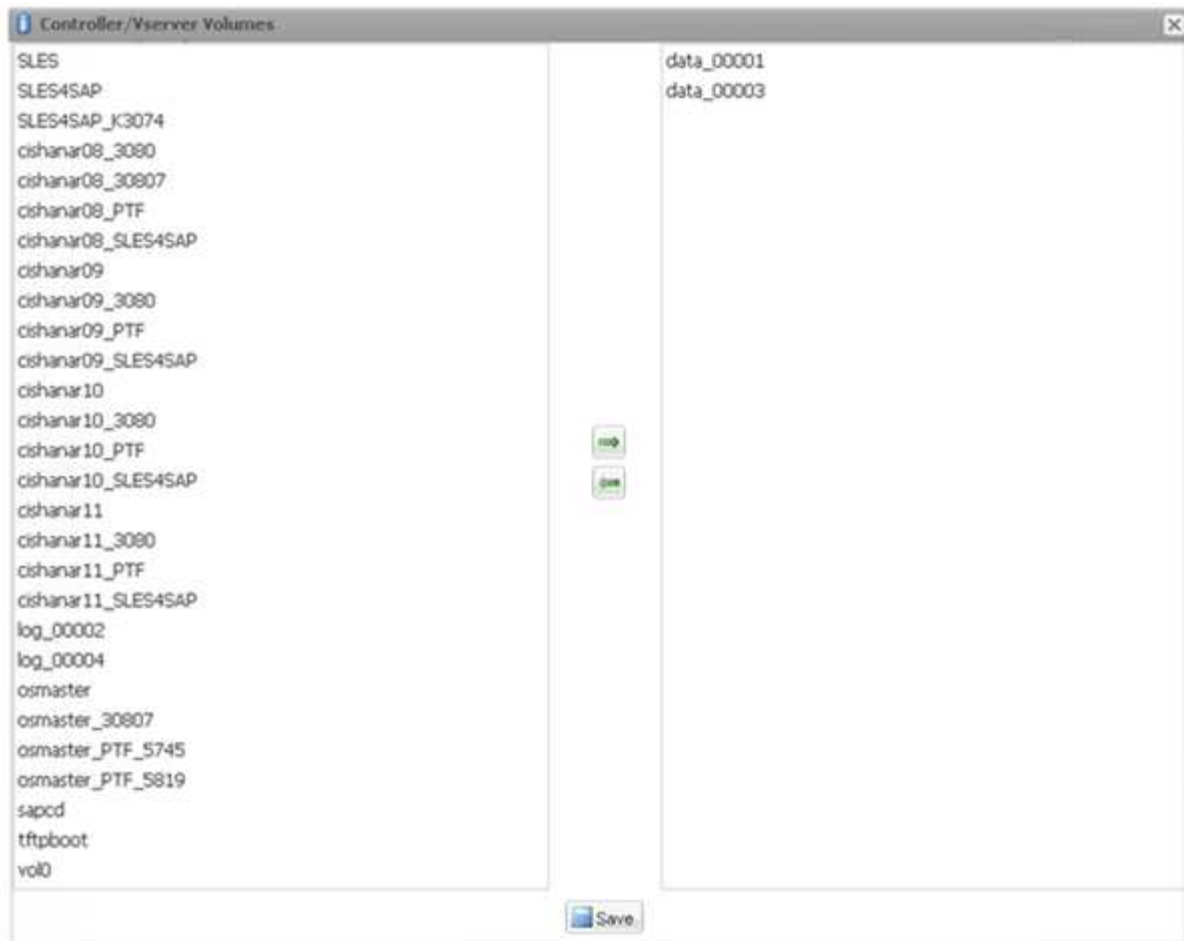
12. Immettere le credenziali di accesso allo storage e fare clic su **Avanti**.

Controller/Vserver Credentials
Add one or more Controller/Vserver credentials to the configuration.

Controller/Vserver Login Credentials

Controller/Vserver IP or Name	User name/Password	Volumes
<div><div>New Controller/Vserver</div><div>Controller/Vserver IP or Name: <input type="text" value="hana1a"/></div><div>Controller/Vserver User: <input type="text" value="root"/></div><div>Controller/Vserver Password: <input type="password" value="....."/></div><div><input type="button" value="Next"/></div></div>		

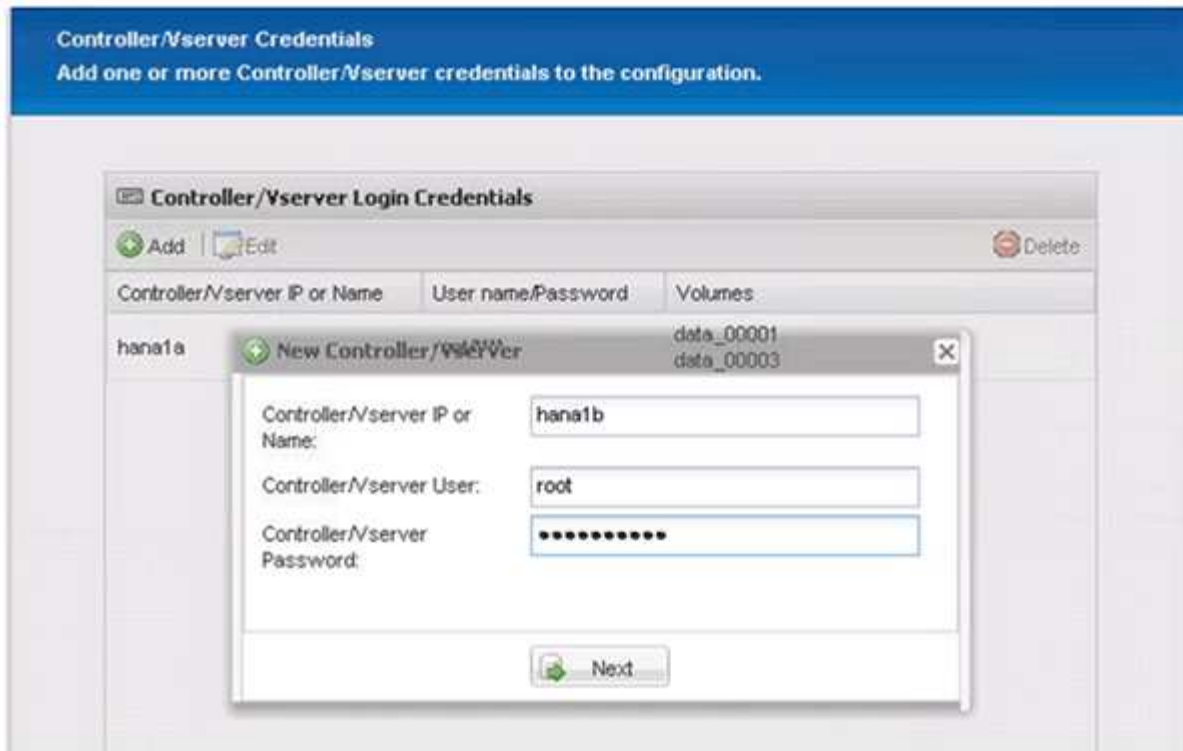
13. Selezionare i volumi di dati memorizzati su questo controller di storage e fare clic su **Save** (Salva).



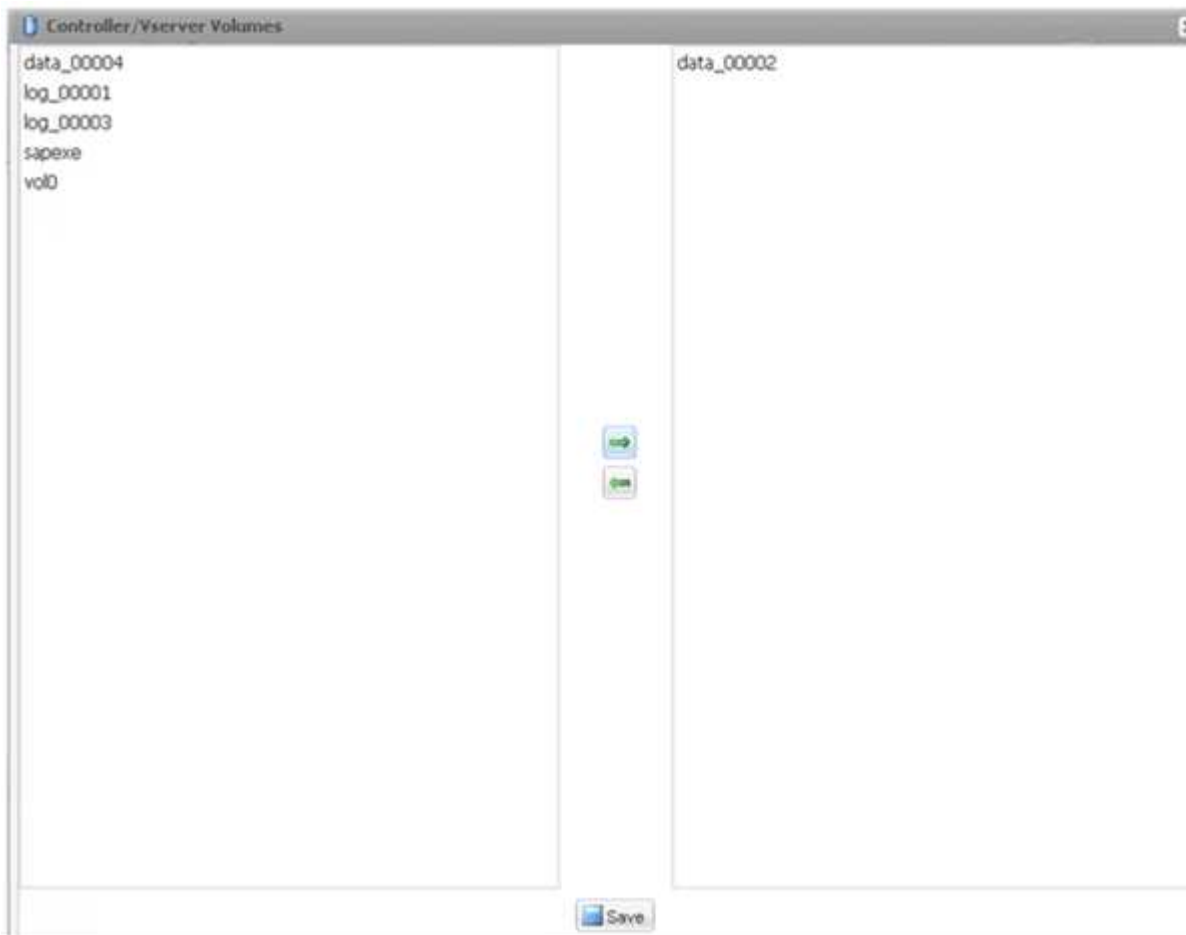
14. Fare clic su **Add** (Aggiungi) per aggiungere un altro controller di storage.



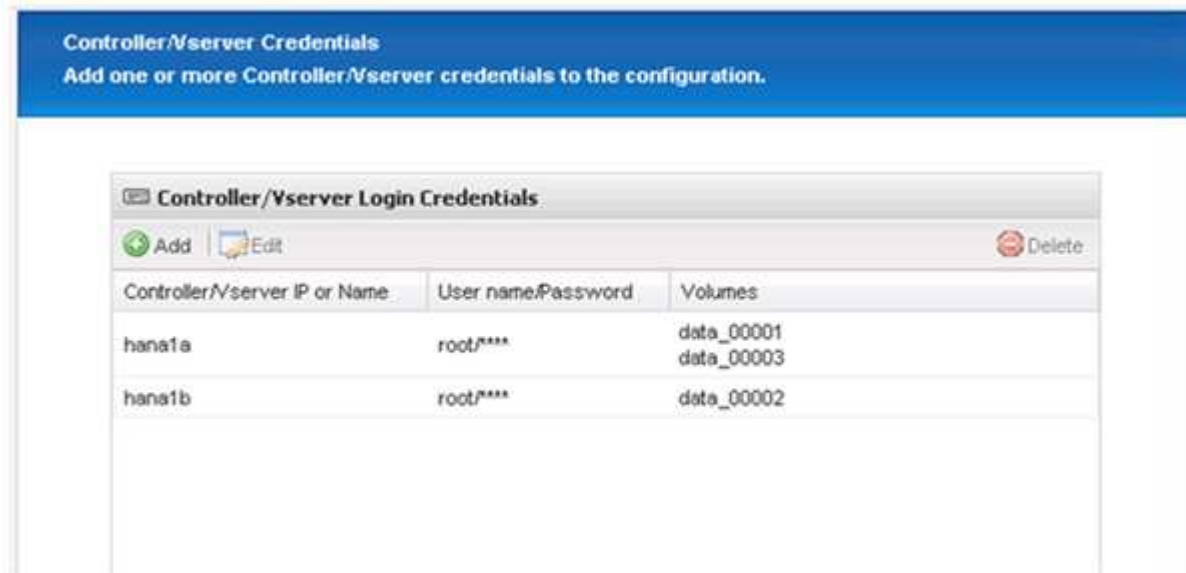
15. Immettere le credenziali di accesso allo storage e fare clic su **Avanti**.



16. Selezionare i volumi di dati memorizzati nel secondo controller di storage creato e fare clic su **Save** (Salva).



17. La finestra Controller/Vserver Credentials (credenziali controller/server virtuale) visualizza i controller e i volumi di storage aggiunti. Fare clic su **Avanti**.



18. Inserire il criterio Snapshot e la configurazione di conservazione.

La conservazione di tre copie Snapshot giornaliere e otto copie Snapshot orarie è solo un esempio e può essere configurata in modo diverso a seconda delle esigenze del cliente.



Selezionare **Timestamp** come convenzione di denominazione. L'utilizzo della convenzione di denominazione **Recent** non è supportato con il plug-in SAP HANA, in quanto la data e l'ora della copia Snapshot viene utilizzata anche per le voci del catalogo di backup SAP HANA.

Configuration

Snapshot Details
Provide Snapshot copy related information.

Snapshot copy Name:

Snapshot copy Label:

Policy Type: ☒ Use Policy ☐ Use Policy Object

Snapshot copy Policies		
Enable Policy	Policy Name	Retention
<input checked="" type="checkbox"/>	hourly	12
<input checked="" type="checkbox"/>	daily	3
<input type="checkbox"/>	weekly	0
<input type="checkbox"/>	monthly	0

Prevent Snapshot copy Deletion:

Policy Retention Age:

Naming Convention: ☐ Recent ☒ Timestamp

19. Non sono richieste modifiche. Fare clic su **Avanti**.

Snapshot Details Continued
Provide Snapshot copy related information.

Consistency Group: ☐

Consistency Timeout:

SnapDrive Discovery:

Consistency Group WAFL Sync:

Snapshot copy Delete by age only:

Snapshot copy Dependency Ignore:

Restore Auto Detect:

Ignore Application Errors:

Snapshot Copy Disable:

20. Selezionare **SnapVault** e configurare i criteri di conservazione SnapVault e il tempo di attesa SnapVault.

Configuration

Data Protection
Configure SnapMirror, SnapVault or both

Data Transfer: ☐ SnapMirror ☒ SnapVault

SnapVault Policies		
Enable Policy	Policy Name	Retention
<input checked="" type="checkbox"/>	hourly	10
<input checked="" type="checkbox"/>	daily	20
<input type="checkbox"/>	weekly	0
<input type="checkbox"/>	monthly	0

SnapVault Retention Age:

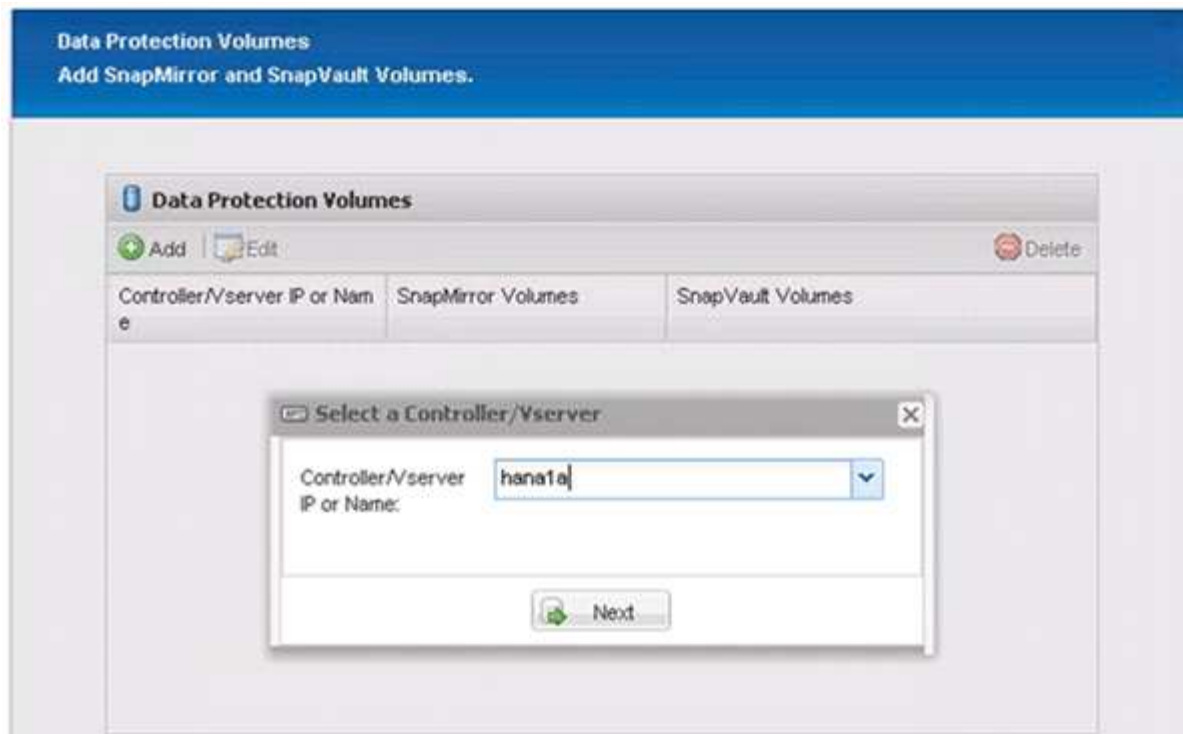
SnapVault wait time:

21. Fare clic su **Aggiungi**.

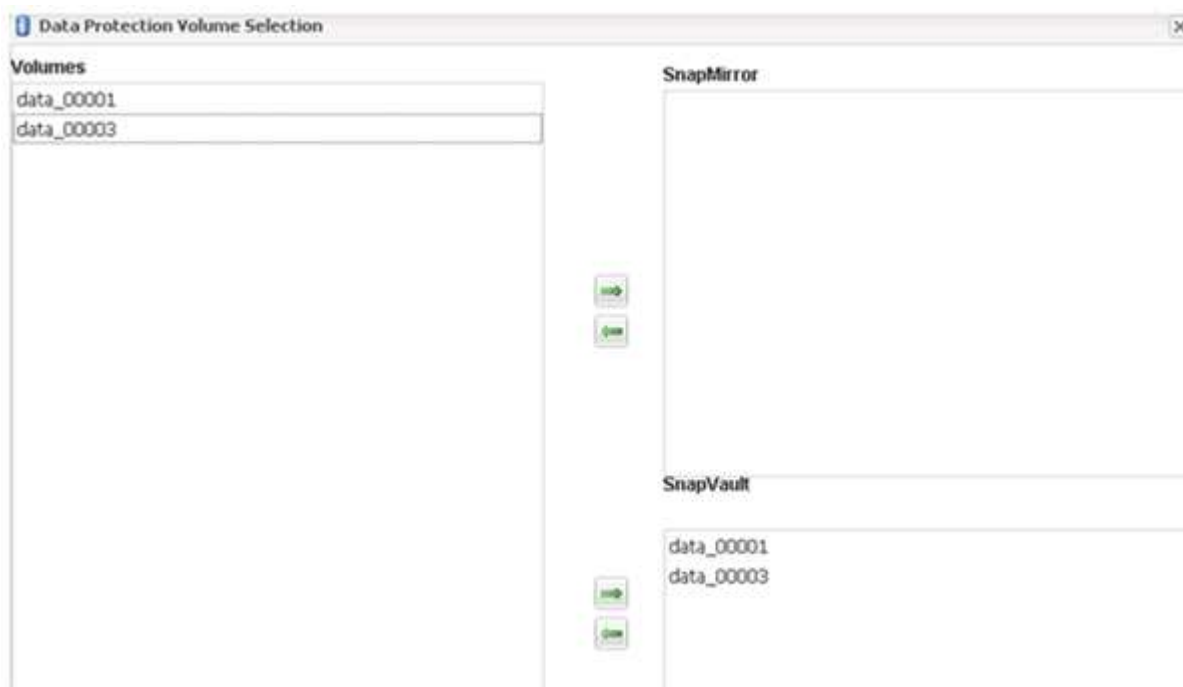
Data Protection Volumes
Add SnapMirror and SnapVault Volumes.

Data Protection Volumes		
Controller/Vserver IP or Name	SnapMirror Volumes	SnapVault Volumes

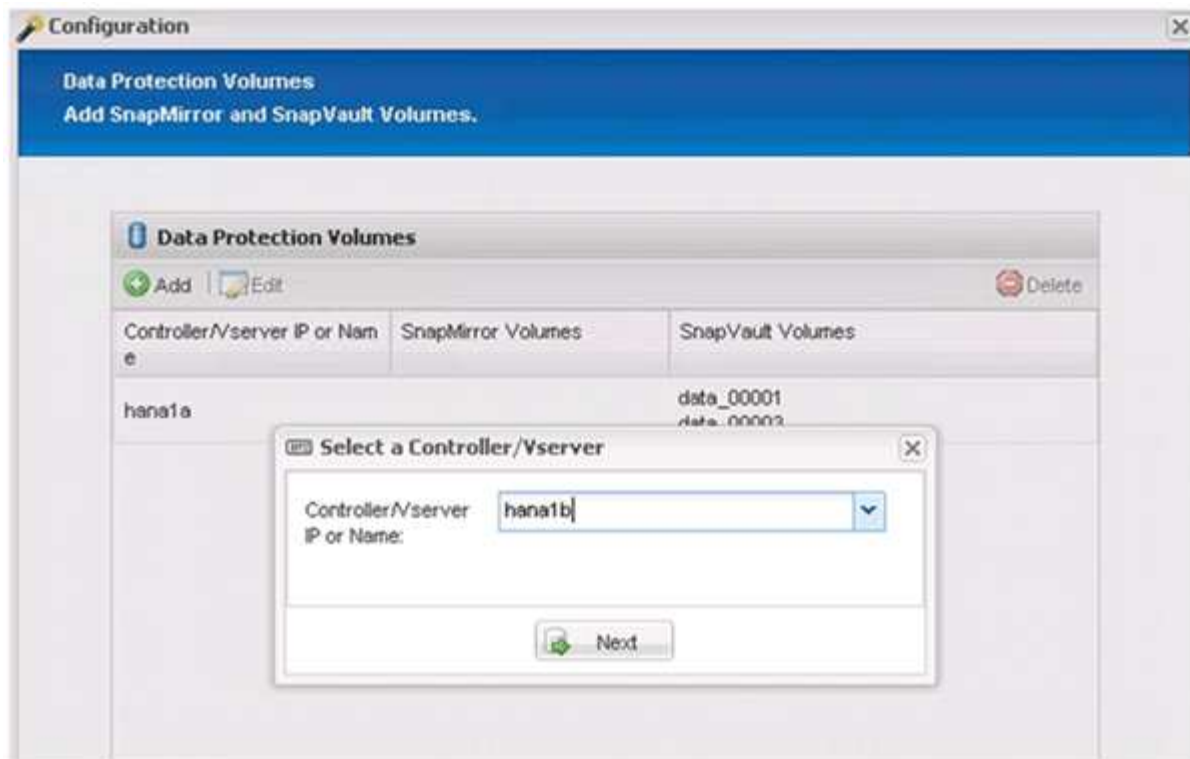
22. Selezionare un controller di storage di origine dall'elenco e fare clic su **Avanti**.



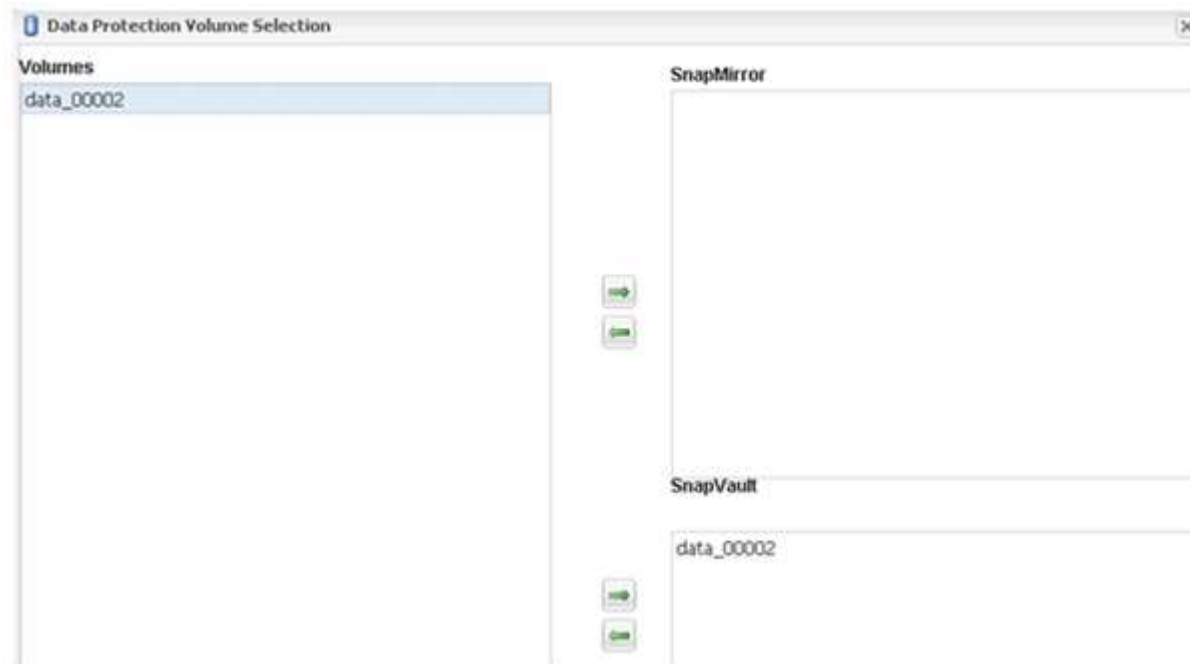
23. Selezionare tutti i volumi memorizzati nel controller dello storage di origine e fare clic su **Save** (Salva).



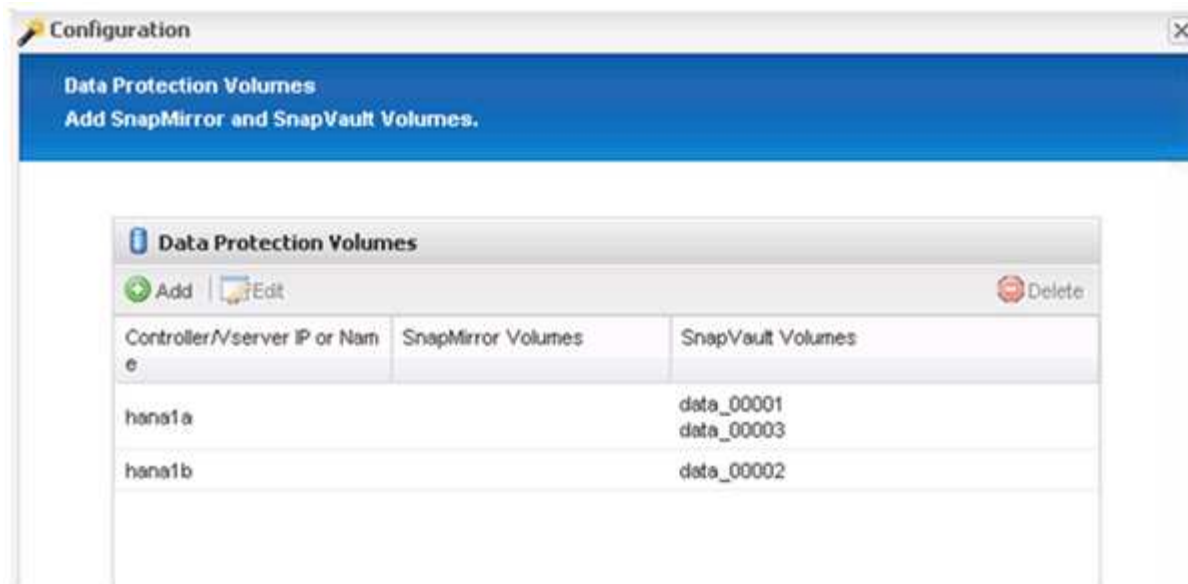
24. Fare clic su **Aggiungi**, selezionare il secondo controller storage di origine dall'elenco, quindi fare clic su **Avanti**.



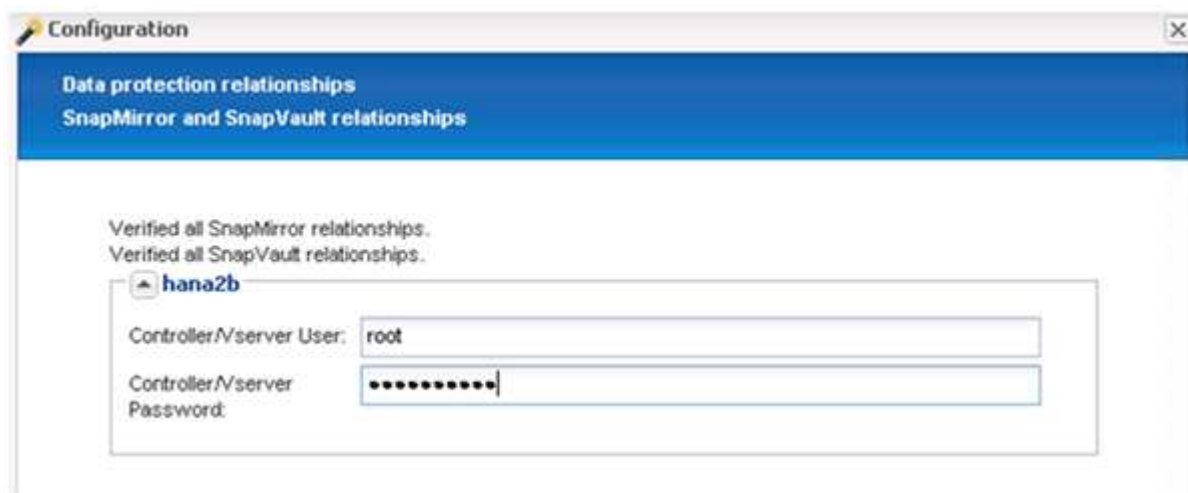
25. Selezionare tutti i volumi memorizzati nel secondo controller di storage di origine e fare clic su **Save** (Salva).



26. La finestra Data Protection Volumes (volumi di protezione dati) visualizza tutti i volumi che devono essere protetti nella configurazione creata. Fare clic su **Avanti**.



27. Immettere le credenziali per i controller di storage di destinazione e fare clic su **Avanti**. In questo esempio, le credenziali utente “root” vengono utilizzate per accedere al sistema di storage. In genere, un utente di backup dedicato viene configurato sul sistema di storage e quindi utilizzato con Snap Creator.



28. Fare clic su **Avanti**.

DFM/OnCommand Settings

Enter OnCommand credentials and other details and settings.

☐ Operations Manager console Alert
 ☒ NetApp Management Console data protection capability

Host:

User:

Password:

Transport:

Port:

29. Fare clic su **fine** per completare la configurazione.

Configuration

Summary

Configuration Name: ANA_database_backup
 Number of Controllers/Vservers added: 2
 Controller/Vserver Name: hana1a
 Controller/Vserver User: root
 Controller/Vserver Password: *****
 Controller/Vserver Name: hana1b
 Controller/Vserver User: root
 Controller/Vserver Password: *****
 Data protection Destination Controllers/Vservers added:
 Controller/Vserver Name: hana2b
 Controller/Vserver User: root
 Controller/Vserver Password: *****
 Global Controller/Vserver credentials: No
 Password Protection: Yes

Volumes:
 hana1a: data_00001, data_00003;
 hana1b: data_00002;

Snapshot Copy Name: Backup-ANA
 Snapshot Copy Policy Name Convention: Timestamp

Ignore Application Error: No
 SnapVault Update: Yes
 SnapVault Wait Time: 10
 SnapVault Volumes:
 Controller/Vserver: hana1a
 Volumes:
 data_00001
 data_00003
 Controller/Vserver: hana1b
 Volumes:
 data_00002

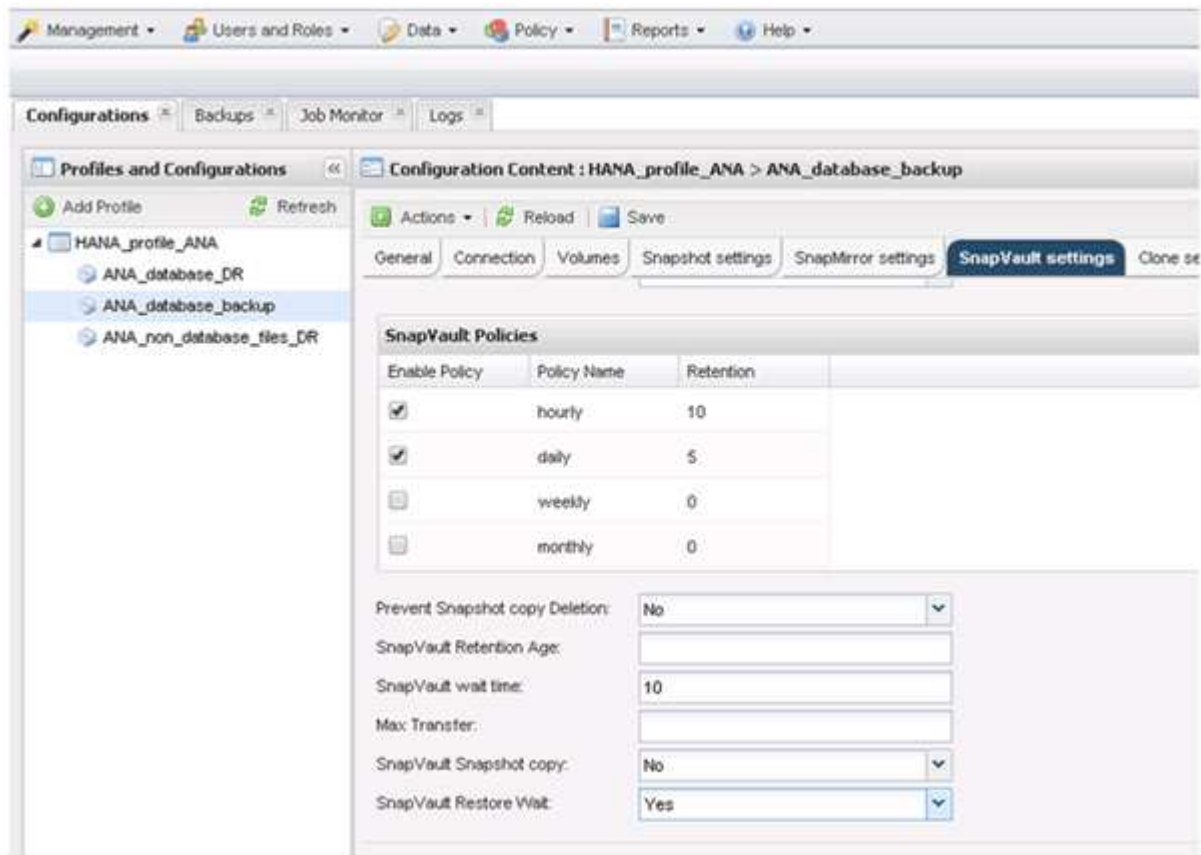
Back

Finish

Cancel

30. Fare clic sulla scheda **SnapVault settings**.

31. Selezionare **Sì** dall'elenco a discesa dell'opzione **attesa ripristino SnapVault** e fare clic su **Salva**.



Si consiglia di utilizzare una rete dedicata per il traffico di replica. Se si decide di farlo, è necessario includere questa interfaccia nel file di configurazione di Snap Creator come interfaccia secondaria.

È inoltre possibile configurare interfacce di gestione dedicate in modo che Snap Creator possa accedere al sistema di storage di origine o di destinazione utilizzando un'interfaccia di rete non associata al nome host del controller di storage.

```
mgmtsrv01:/opt/NetApp/Snap_Creator_Framework_411/scServer4.1.1c/engine/c
onfigs/HANA_profile_ANA
# vi ANA_database_backup.conf

#####
#####
#      Connection Options                                #
#####
#####
PORT=443
SECONDARY_INTERFACES=hana1a:hana1a-rep/hana2b;hana1b:hana1b-rep/hana2b
MANAGEMENT_INTERFACES=hana2b:hana2b-mgmt
```


Informazioni sul copyright

Copyright © 2023 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.