



# Konfigurieren von Daten-Backups

Snap Creator Framework

NetApp

January 20, 2026

This PDF was generated from [https://docs.netapp.com/de-de/snap-creator-framework/sap-hana-ops/task\\_configuring\\_the\\_backup\\_user\\_and\\_hdbuserstore.html](https://docs.netapp.com/de-de/snap-creator-framework/sap-hana-ops/task_configuring_the_backup_user_and_hdbuserstore.html) on January 20, 2026. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Inhalt

Konfigurieren von Daten-Backups . . . . .	1
Konfigurieren des Backup-Benutzers und des hdbuserstore . . . . .	1
SnapVault Beziehungen werden konfiguriert . . . . .	2
Starten der SnapVault Beziehungen . . . . .	3
Starten der SnapVault Beziehungen mit Data ONTAP im 7-Mode . . . . .	3
Beginnen der Beziehungen zu SnapVault mit Clustered Data ONTAP . . . . .	4
Konfiguration des Snap Creator Framework und des Datenbank-Backups von SAP HANA . . . . .	5

# Konfigurieren von Daten-Backups

Führen Sie nach der Installation der erforderlichen Softwarekomponenten die folgenden Schritte aus, um die Konfiguration abzuschließen:

1. Konfigurieren Sie einen dedizierten Datenbankbenutzer und den SAP HANA Benutzerspeicher.
2. SnapVault-Replizierung auf allen Storage Controllern vorbereiten.
3. Erstellung von Volumes auf dem sekundären Storage Controller
4. SnapVault Beziehungen für Datenbank-Volumes initialisieren.
5. Konfigurieren Sie Snap Creator.

## Konfigurieren des Backup-Benutzers und des hdbuserstore

Sie sollten einen dedizierten Datenbankbenutzer in der HANA Datenbank konfigurieren, um die Backup-Vorgänge mit Snap Creator auszuführen. In einem zweiten Schritt sollten Sie für diesen Backup-Benutzer einen SAP HANA User Store Key konfigurieren. Dieser UserStore-Schlüssel wird in der Konfiguration des Snap Creator SAP HANA Plug-ins verwendet.

Der Backup-Benutzer muss über die folgenden Berechtigungen verfügen:

- BACKUP-ADMIN
- KATALOG GELESEN

1. Auf dem Administrationshost, dem Host, auf dem Snap Creator installiert wurde, ist ein Benutzerspeicherschlüssel für alle Datenbank-Hosts konfiguriert, die zur SAP HANA-Datenbank gehören. Der Userstore-Schlüssel wird mit dem OS-Root-Benutzer konfiguriert: Hdbuserstore Set keyhost 3[instance]15 userpassword
2. Konfigurieren Sie einen Schlüssel für alle vier Datenbank-Nodes.

```

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

```

## SnapVault Beziehungen werden konfiguriert

Wenn Sie SnapVault-Beziehungen konfigurieren, müssen für die primären Storage Controller eine gültige SnapRestore- und SnapVault-Lizenz installiert sein. Auf dem sekundären Storage muss eine gültige SnapVault-Lizenz installiert sein.

1. Aktivieren Sie SnapVault und NDMP auf den primären und sekundären Storage Controllern.

```

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

```

2. Konfigurieren Sie auf allen primären Storage Controllern den Zugriff auf den sekundären Storage Controller.

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



Die Verwendung eines dedizierten Netzwerks für den Replikationsverkehr wird empfohlen. In diesen Fällen muss der Host-Name dieser Schnittstelle am sekundären Storage Controller konfiguriert werden. Anstelle von hana2b könnte der Host Name hana2b-Rep sein.

3. Konfigurieren Sie auf dem sekundären Storage Controller den Zugriff für alle primären Storage Controller.

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



Die Verwendung eines dedizierten Netzwerks für den Replikationsverkehr wird empfohlen. In diesen Fällen muss der Host-Name dieser Schnittstelle auf den primären Storage Controllern konfiguriert werden. Anstelle von hana1b und hana1a könnte der Hostname hana1a-Rep und hana1b-rep sein.

## Starten der SnapVault Beziehungen

Sie müssen die SnapVault Partnerschaft mit Data ONTAP im 7-Mode und Clustered Data ONTAP starten.

### Starten der SnapVault Beziehungen mit Data ONTAP im 7-Mode

Sie können eine SnapVault Beziehung mit Befehlen starten, die auf dem sekundären Storage-System ausgeführt werden.

1. Für Storage-Systeme mit Data ONTAP 7-Mode starten Sie die SnapVault Beziehungen, indem Sie den folgenden Befehl ausführen:

```
hana2b> snapvault start -S hanala:/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 hanala:/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 hanalb:/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>
```



Es wird empfohlen, für den Replikationsverkehr ein dediziertes Netzwerk zu verwenden. In diesem Fall konfigurieren Sie den Host-Namen dieser Schnittstelle an den primären Storage Controllern. Anstelle von hana1b und hana1a könnte der Hostname hana1a-Vertreter und hana1brep sein.

## Beginnen der Beziehungen zu SnapVault mit Clustered Data ONTAP

Sie müssen eine SnapMirror-Richtlinie definieren, bevor Sie eine SnapVault-Beziehung starten.

1. Bei Storage-Systemen mit Clustered Data ONTAP starten Sie die SnapVault-Beziehungen, indem Sie den folgenden Befehl ausführen.

```

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

```

Die Richtlinie muss Regeln für alle Aufbewahrungsklassen (Labels) enthalten, die in der Snap Creator-Konfiguration verwendet werden. Die oben genannten Befehle zeigen, wie eine dedizierte SnapMirror-Richtlinie SV\_HANA erstellt wird

2. Führen Sie folgende Befehle aus, um die SnapVault-Beziehung auf der Cluster-Konsole des Backup-Clusters zu erstellen und zu starten.

```

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.

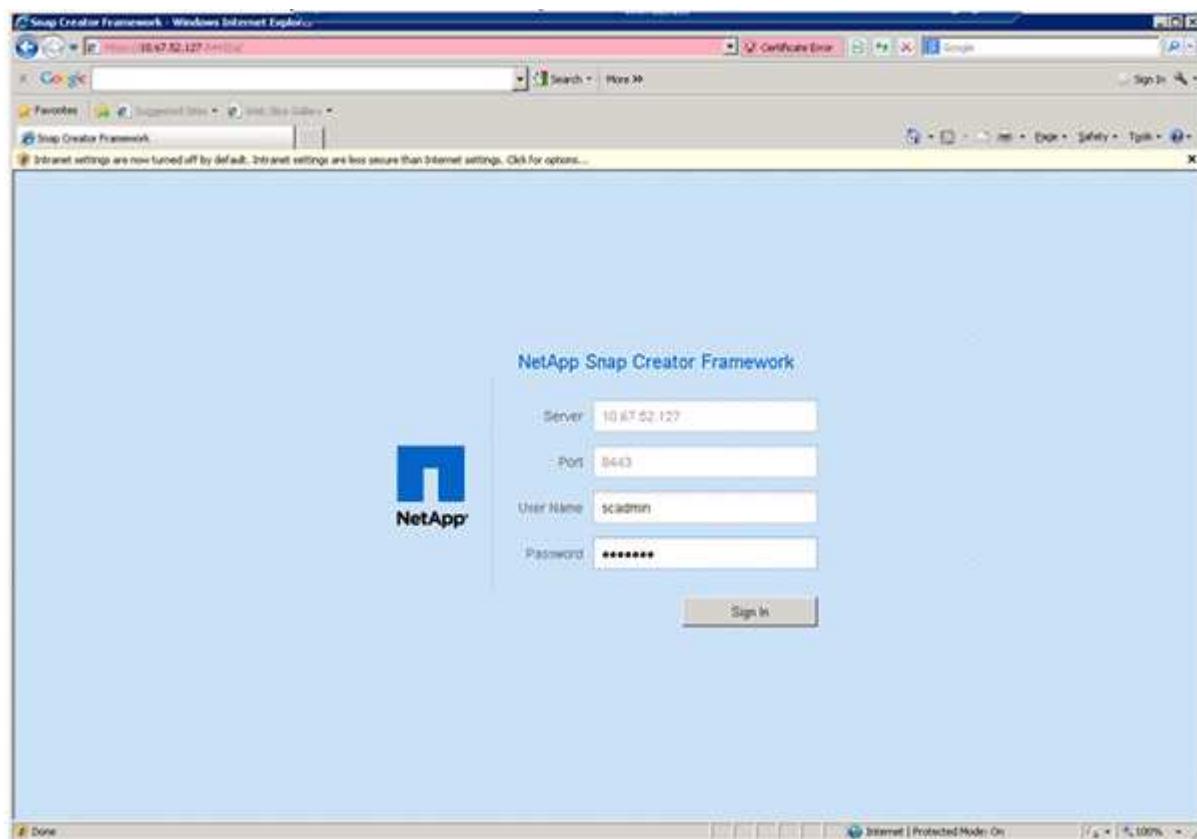
hana::> snapmirror initialize -destination-path hana2b:backup_hana_data
-type XDP

```

## Konfiguration des Snap Creator Framework und des Datenbank-Backups von SAP HANA

Sie müssen Snap Creator Framework und das SAP HANA Datenbank-Backup konfigurieren.

1. Verbinden Sie sich mit der grafischen Benutzeroberfläche des Snap Creator: <https://host:8443/ui/>.
2. Melden Sie sich mit dem Benutzernamen und Passwort an, die während der Installation konfiguriert wurden. Klicken Sie auf **Anmelden**.



3. Geben Sie einen Profilnamen ein und klicken Sie auf **OK**.



Beispiel: „ANA“ ist die SID der Datenbank.

4. Geben Sie den Konfigurationsnamen ein, und klicken Sie auf **Weiter**.

 Configuration

**Configuration**  
Enter Configuration name and select required options.

Config. Name:

Password Encryption

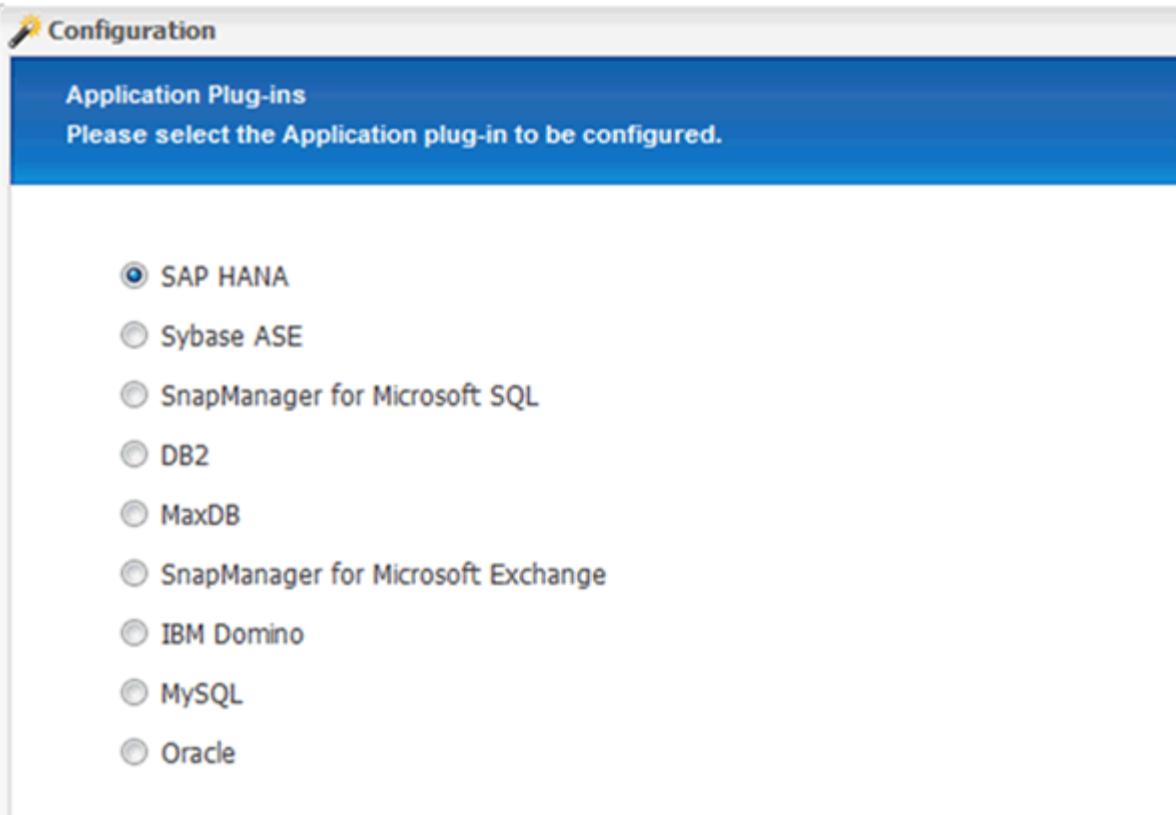
5. Wählen Sie als Plug-in-Typ \* Application Plug-in\* aus, und klicken Sie auf **Next**.

 Configuration

**Plug-in Type**  
Please select plug-in type.

Application plug-in  
 Virtualization plug-in  
 Community plug-in  
 None

6. Wählen Sie als Anwendungs-Plug-in \* SAP HANA\* aus und klicken Sie auf **Weiter**.



7. Geben Sie die folgenden Konfigurationsdetails ein:

- a. Wählen Sie im Dropdown-Menü \* Ja\* aus, um die Konfiguration mit einer mandantenfähigen Datenbank zu verwenden. Wählen Sie für eine einzelne Container-Datenbank **Nein**.
- b. Wenn der Multitenant-Datenbank-Container auf **Nein** gesetzt ist, müssen Sie die Datenbank-SID angeben.
- c. Wenn der Multitenant-Datenbank-Container auf **Ja** gesetzt ist, müssen Sie für jeden SAP HANA-Knoten die hdbuserstore-Schlüssel hinzufügen.
- d. Fügen Sie den Namen der Mandanten-Datenbank hinzu.
- e. Fügen Sie die HANA-Nodes hinzu, auf denen die hdbsql-Anweisung ausgeführt werden muss.
- f. Geben Sie die HANA-Node-Instanznummer ein.
- g. Geben Sie den Pfad zur ausführbaren Datei hdbsql an.
- h. Fügen Sie den OSDB-Benutzer hinzu.
- i. Wählen Sie in der Dropdown-Liste **Ja** aus, um DIE PROTOKOLLBEREINIGUNG zu aktivieren.

#### HINWEIS:

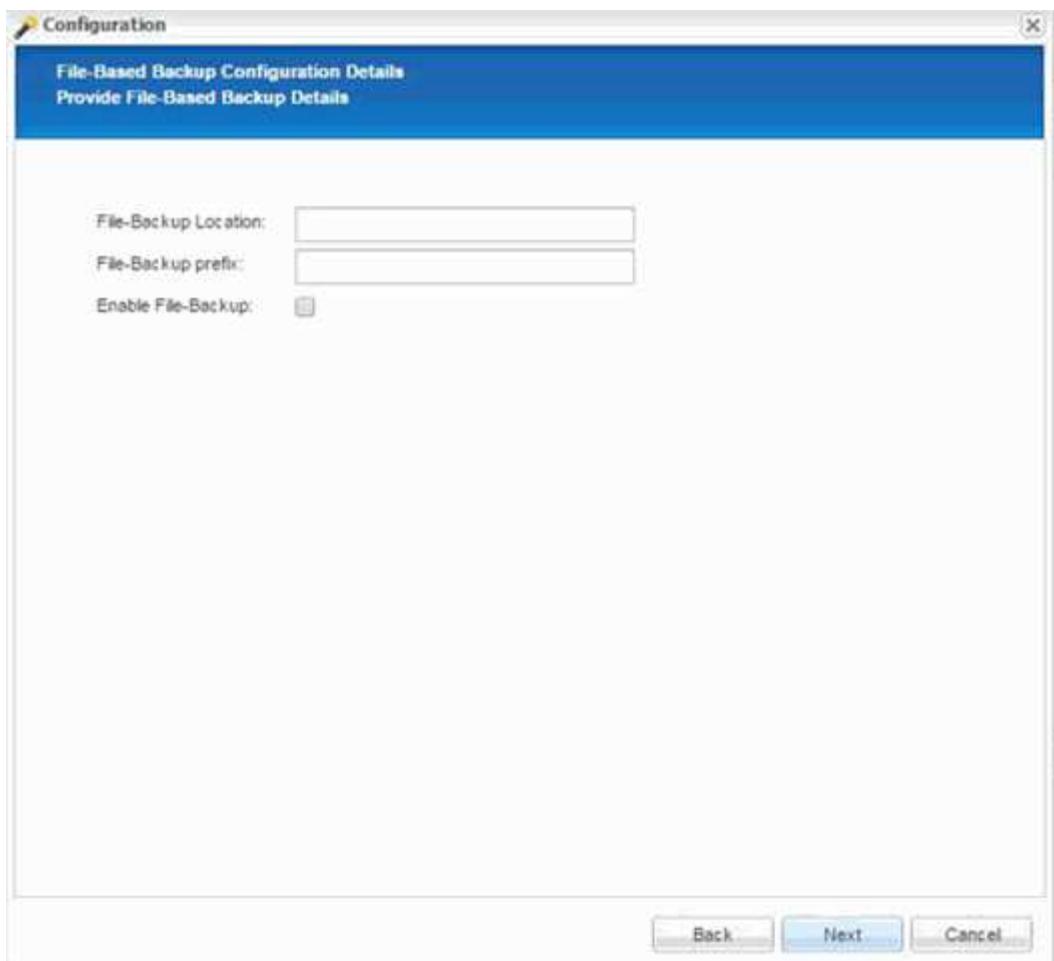
- Parameter `HANA_SID` Ist nur verfügbar, wenn der Wert für Parameter `HANA_MULTITENANT_DATABASE` Ist auf festgelegt `N`
- Für mandantenfähige Datenbank-Container (MDC) mit einem Ressourcentyp „Single Tenant“ arbeiten die SAP HANA Snapshot-Kopien mit der Key-basierten Authentifizierung von UserStore. Wenn der `HANA_MULTITENANT_DATABASE` Parameter ist auf festgelegt `Y`, Dann der `HANA_USERSTORE_KEYS` Parameter muss auf den entsprechenden Wert gesetzt werden.
- Ähnlich wie bei nicht-mandantenfähigen Datenbank-Containern wird die Funktion für dateibasiertes Backup und Integritätsprüfung unterstützt

j. Klicken Sie Auf **Weiter**.

Multitenant Database Container (MDC) - Single Tenant:	No
SID:	H66
hdbsql User 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

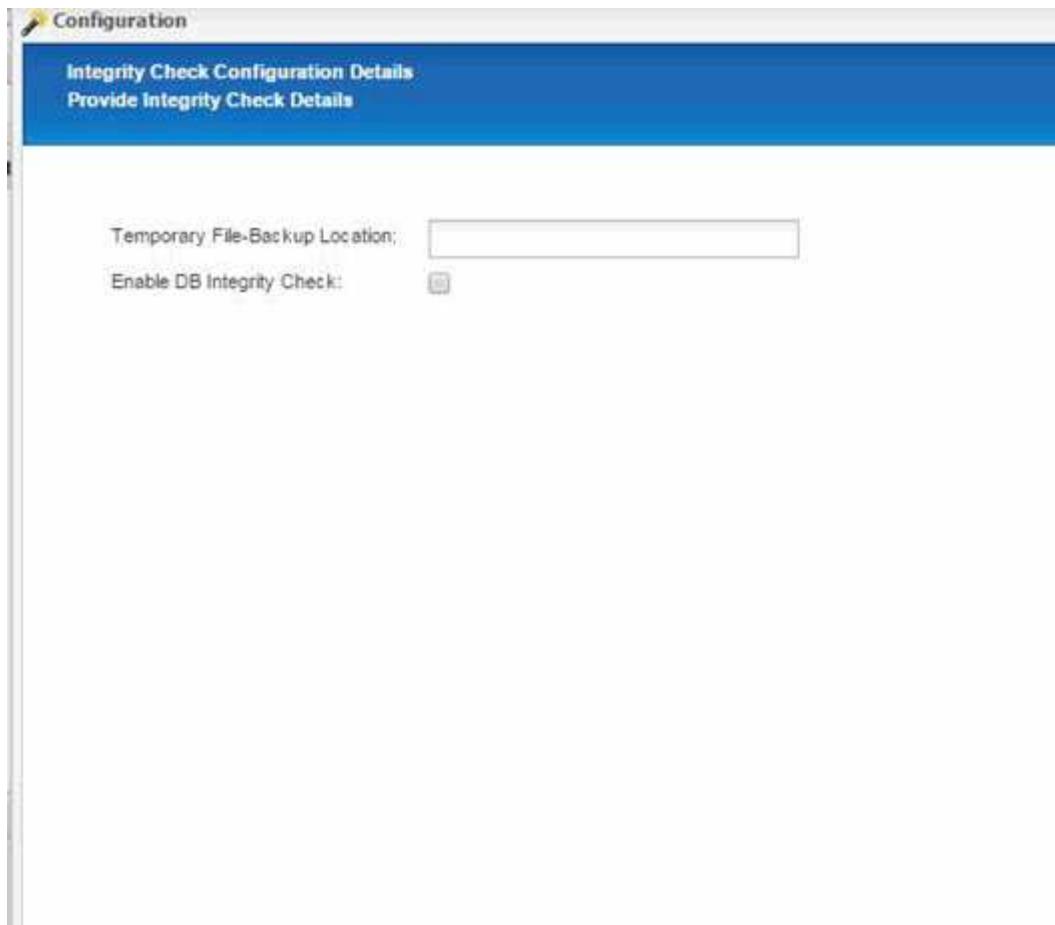
8. Aktivieren Sie den dateibasierten Backup-Vorgang:

- a. Legen Sie den Speicherort für die Dateisicherung fest.
- b. Geben Sie das Präfix für die Dateisicherung an.
- c. Aktivieren Sie das Kontrollkästchen **Datei-Backup aktivieren**.
- d. Klicken Sie Auf **Weiter**.



9. Aktivieren Sie die Datenbankintegritätsprüfung:

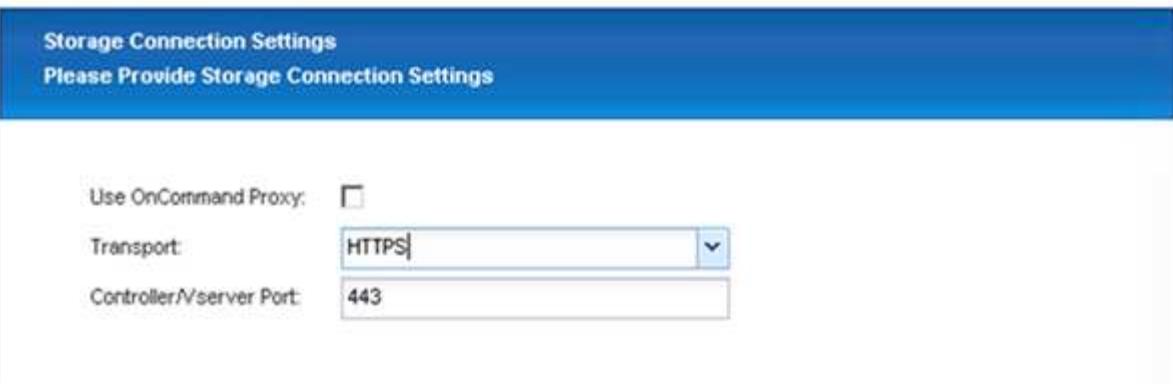
- Legen Sie den Speicherort für die temporäre Datei-Sicherung fest.
- Aktivieren Sie das Kontrollkästchen \* DB-Integritätsprüfung aktivieren\*.
- Klicken Sie Auf **Weiter**.



10. Geben Sie die Details für den Konfigurationsparameter des Agenten ein, und klicken Sie auf **Weiter**.

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

11. Geben Sie die Einstellungen für die Speicherverbindung ein, und klicken Sie auf **Weiter**.



12. Geben Sie die Anmelde Daten für den Speicher ein, und klicken Sie auf **Weiter**.



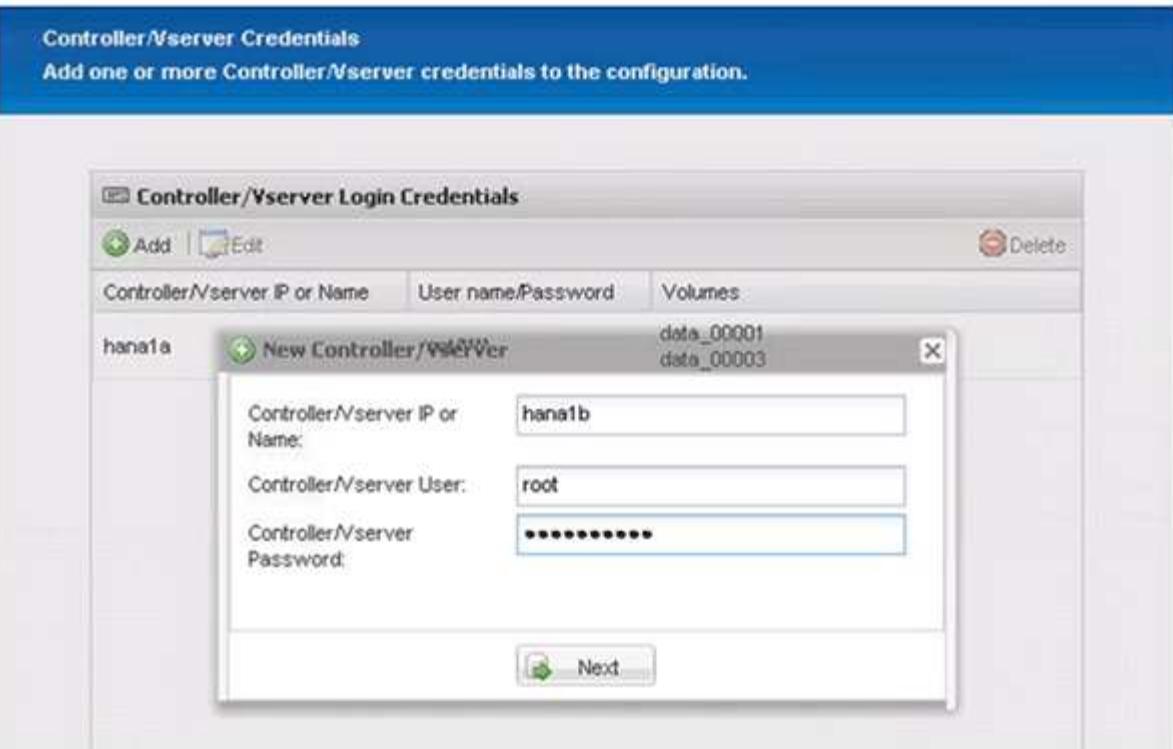
13. Wählen Sie die auf diesem Speicher-Controller gespeicherten Datenvolumen aus und klicken Sie auf **Speichern**.



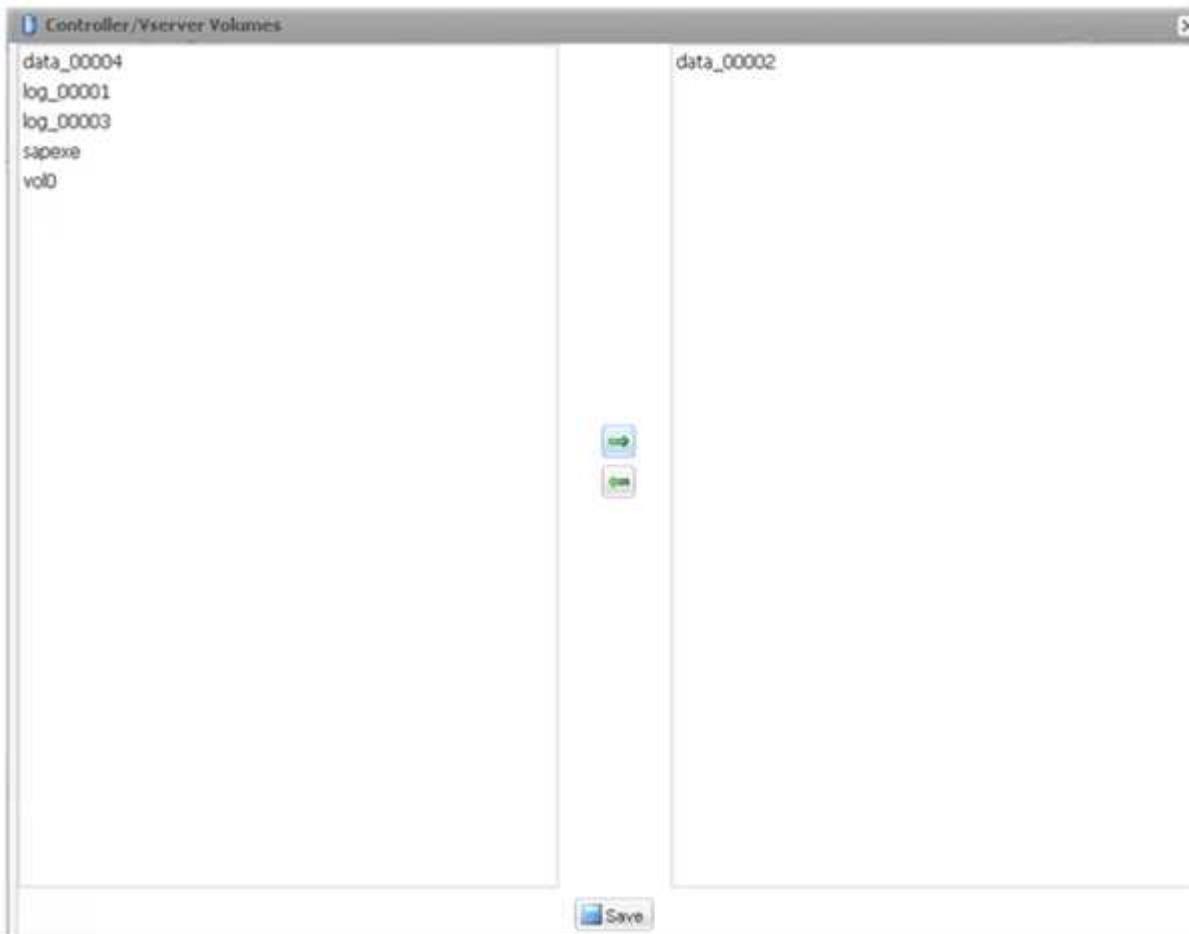
14. Klicken Sie auf **Hinzufügen**, um einen weiteren Speicher-Controller hinzuzufügen.

The screenshot shows a software window titled 'Controller/Vserver Credentials' with the sub-section 'Controller/Vserver Login Credentials'. It displays a table with three columns: 'Controller/Vserver IP or Name', 'User name/Password', and 'Volumes'. There is one entry: 'hanaf1a' in the first column, 'root/\*\*\*\*' in the second, and 'data\_00001' and 'data\_00003' in the third. At the top of the table are buttons for 'Add', 'Edit', and 'Delete'.

15. Geben Sie die Anmelddaten für den Speicher ein, und klicken Sie auf **Weiter**.



16. Wählen Sie die Datenvolumen aus, die auf dem zweiten Speicher-Controller gespeichert sind, den Sie erstellt haben, und klicken Sie auf **Speichern**.



17. Im Fenster Controller/Vserver Credentials werden die hinzugefügten Storage Controller und Volumes angezeigt. Klicken Sie Auf **Weiter**.

The screenshot shows a software interface titled 'Controller/Vserver Credentials' with the sub-instruction 'Add one or more Controller/Vserver credentials to the configuration.' Below this is a table titled 'Controller/Vserver Login Credentials'. The table has columns for 'Controller/Vserver IP or Name', 'User name/Password', and 'Volumes'. There are two rows: one for 'hana1a' with user 'root/\*\*\*\*' and volumes 'data\_00001' and 'data\_00003'; and another for 'hana1b' with user 'root/\*\*\*\*' and volume 'data\_00002'. At the top of the table are buttons for 'Add' (green plus), 'Edit' (pencil), and 'Delete' (red minus).

Controller/Vserver IP or Name	User name/Password	Volumes
hana1a	root/****	data_00001 data_00003
hana1b	root/****	data_00002

18. Geben Sie die Konfiguration der Snapshot-Richtlinie und -Aufbewahrung ein.

Die Aufbewahrung von drei täglichen und acht stündlichen Snapshot-Kopien ist nur ein Beispiel, das je nach Kundenanforderungen unterschiedlich konfiguriert werden könnte.



Wählen Sie als Namensgebungskonvention **Zeitstempel** aus. Die Verwendung der Namenskonvention **Recent** wird mit dem SAP HANA Plug-in nicht unterstützt, da der Zeitstempel der Snapshot Kopie auch für die SAP HANA Backup Katalog Einträge verwendet wird.

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. Es sind keine Änderungen erforderlich. Klicken Sie Auf **Weiter**.

**Snapshot Details Continued**  
Provide Snapshot copy related information.

Consistency Group:

Consistency Timeout:

SnapDrive Discovery:

Consistency Group WAFL Sync:

Snapshot copy Delete by age only:

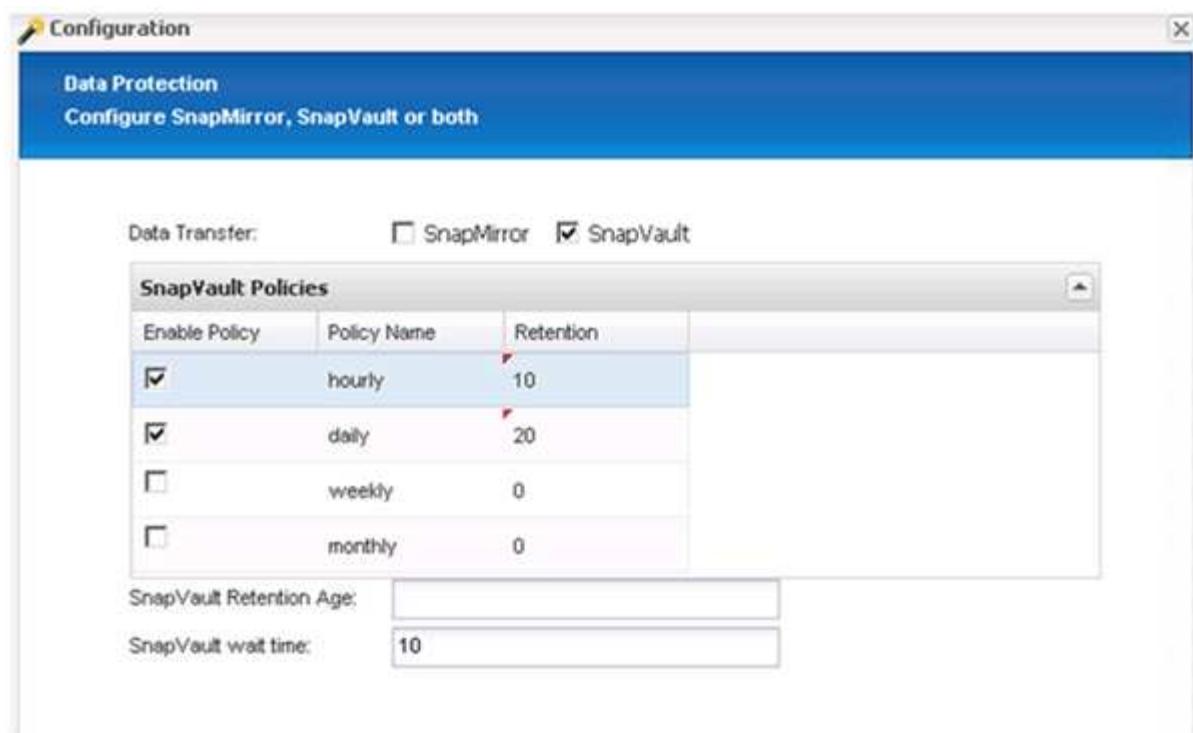
Snapshot copy Dependency Ignore:

Restore Auto Detect:

Ignore Application Errors:

Snapshot Copy Disable:

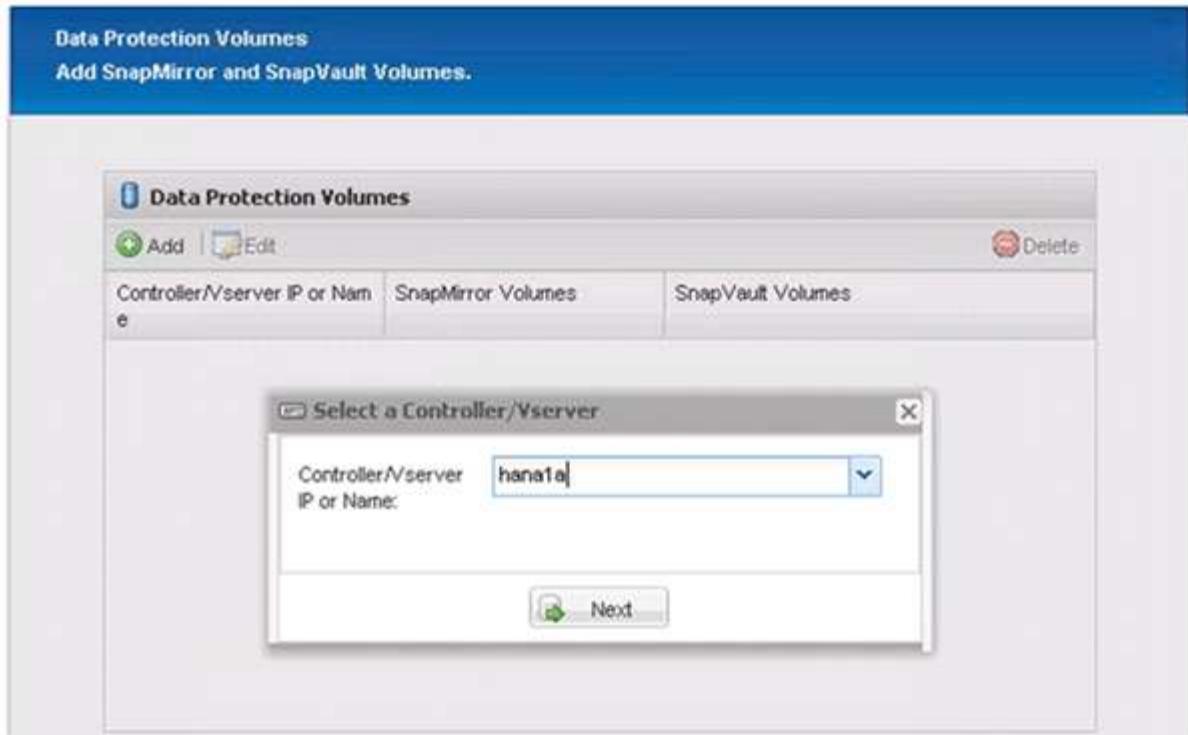
20. Wählen Sie **SnapVault** aus, und konfigurieren Sie die SnapVault-Aufbewahrungsrichtlinien und die SnapVault-Wartezeit.



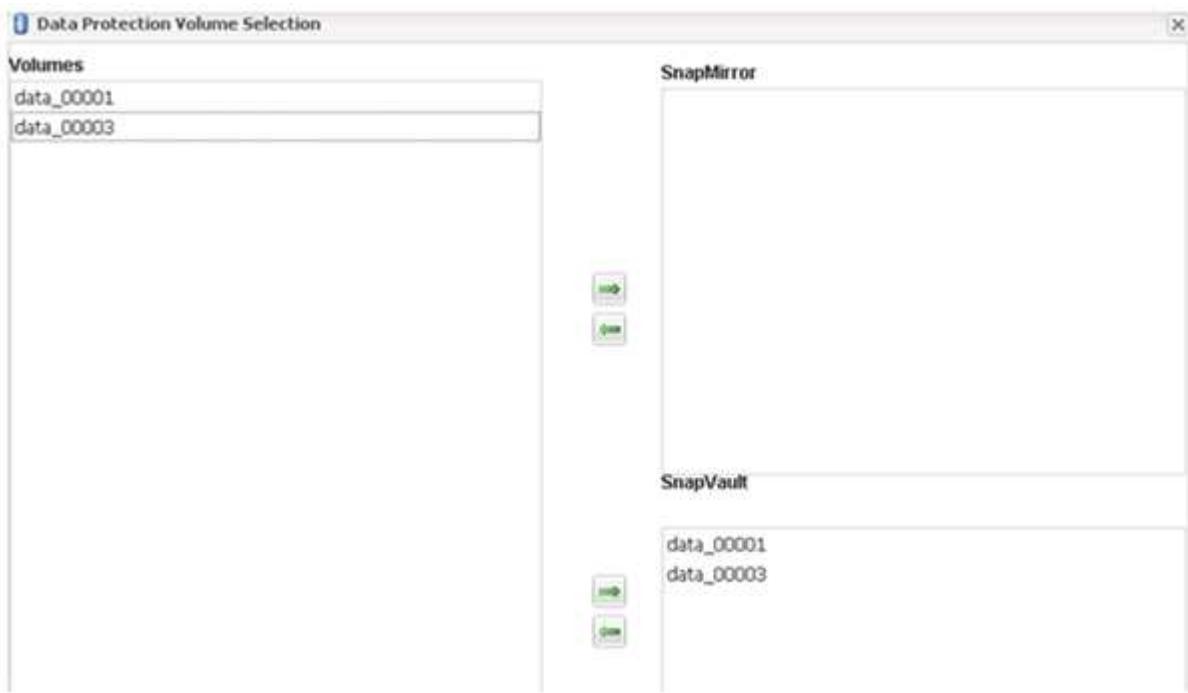
21. Klicken Sie Auf **Hinzufügen**.



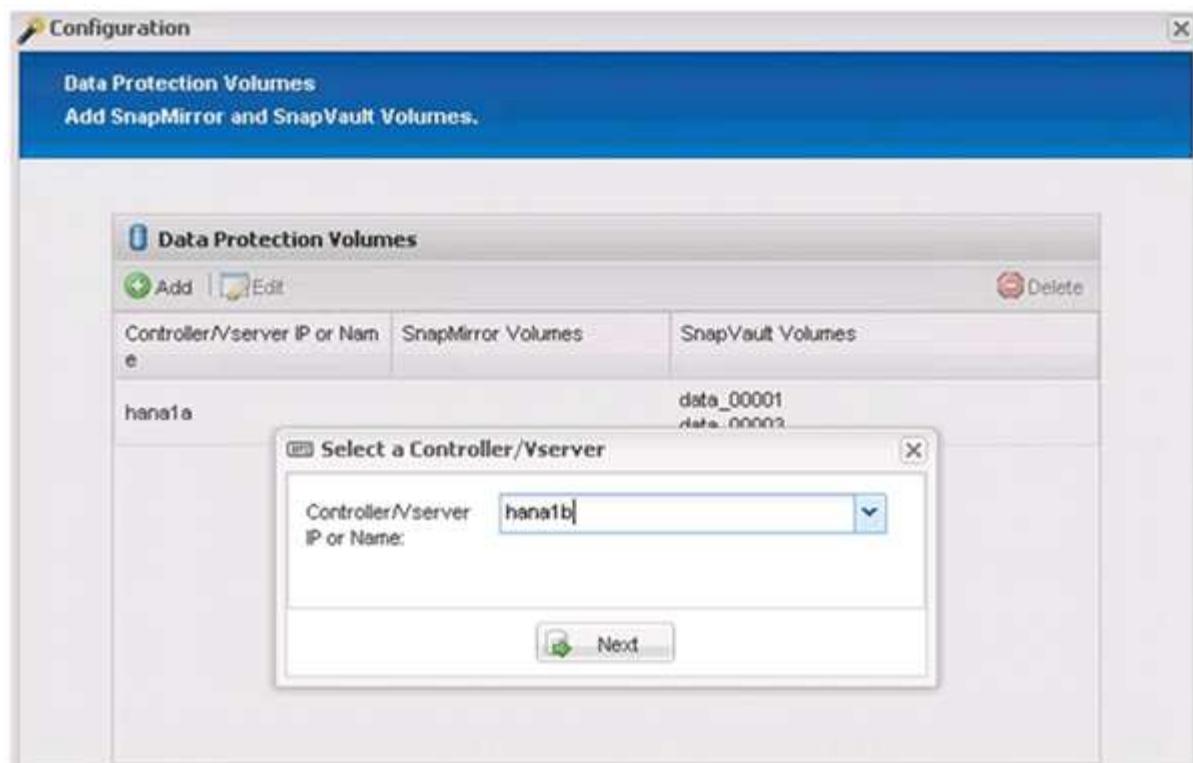
22. Wählen Sie einen Quell-Speicher-Controller aus der Liste aus, und klicken Sie auf **Weiter**.



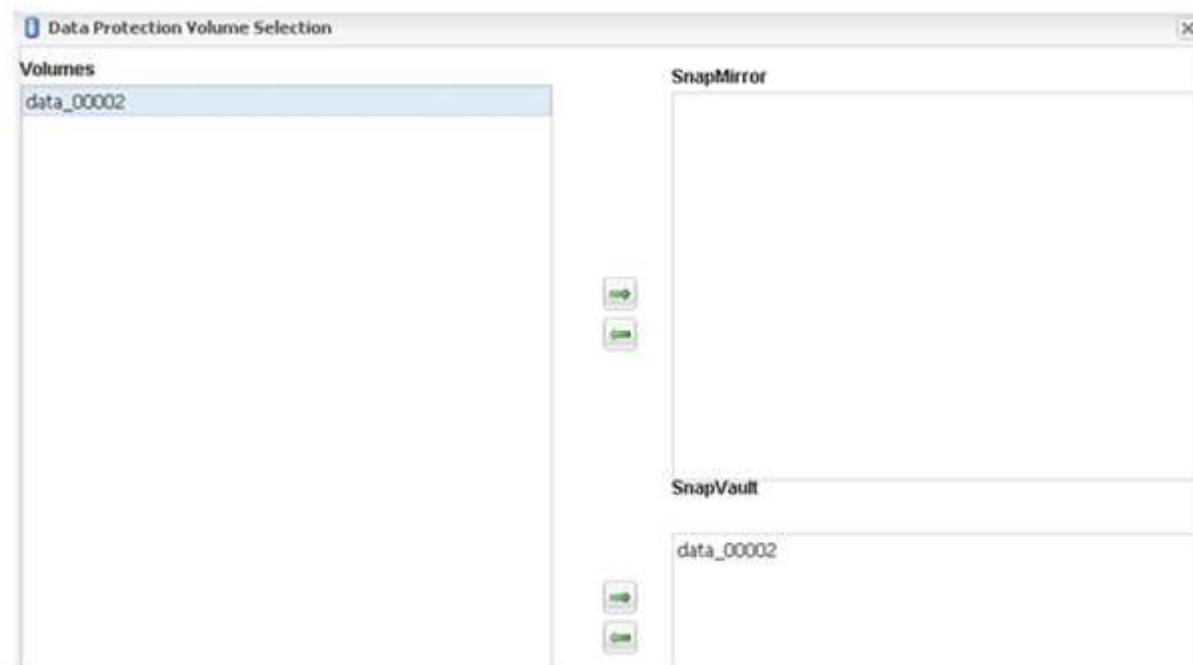
23. Wählen Sie alle Volumes aus, die auf dem Quell-Speicher-Controller gespeichert sind, und klicken Sie auf **Speichern**.



24. Klicken Sie auf **Hinzufügen**, und wählen Sie den zweiten Quell-Speicher-Controller aus der Liste aus, und klicken Sie dann auf **Weiter**.



25. Wählen Sie alle Volumes aus, die auf dem zweiten Quell-Speicher-Controller gespeichert sind, und klicken Sie auf **Speichern**.



26. Im Fenster Data Protection Volumes werden alle Volumes angezeigt, die in der von Ihnen erstellten Konfiguration geschützt werden sollten. Klicken Sie Auf **Weiter**.

**Configuration**

**Data Protection Volumes**  
Add SnapMirror and SnapVault Volumes.

Data Protection Volumes		
Add	Edit	Delete
Controller/Server IP or Name e	SnapMirror Volumes	SnapVault Volumes
hana1a		data_00001 data_00003
hana1b		data_00002

27. Geben Sie die Anmeldeinformationen für die Ziel-Storage-Controller ein, und klicken Sie auf **Weiter**. In diesem Beispiel werden die Benutzeranmeldeinformationen „root“ für den Zugriff auf das Speichersystem verwendet. Normalerweise wird ein dedizierter Backup-Benutzer auf dem Storage-System konfiguriert und dann mit Snap Creator verwendet.

**Configuration**

**Data protection relationships**  
SnapMirror and SnapVault relationships

Verified all SnapMirror relationships.  
Verified all SnapVault relationships.

**hana2b**

Controller/Server User:	root
Controller/Server Password:	*****

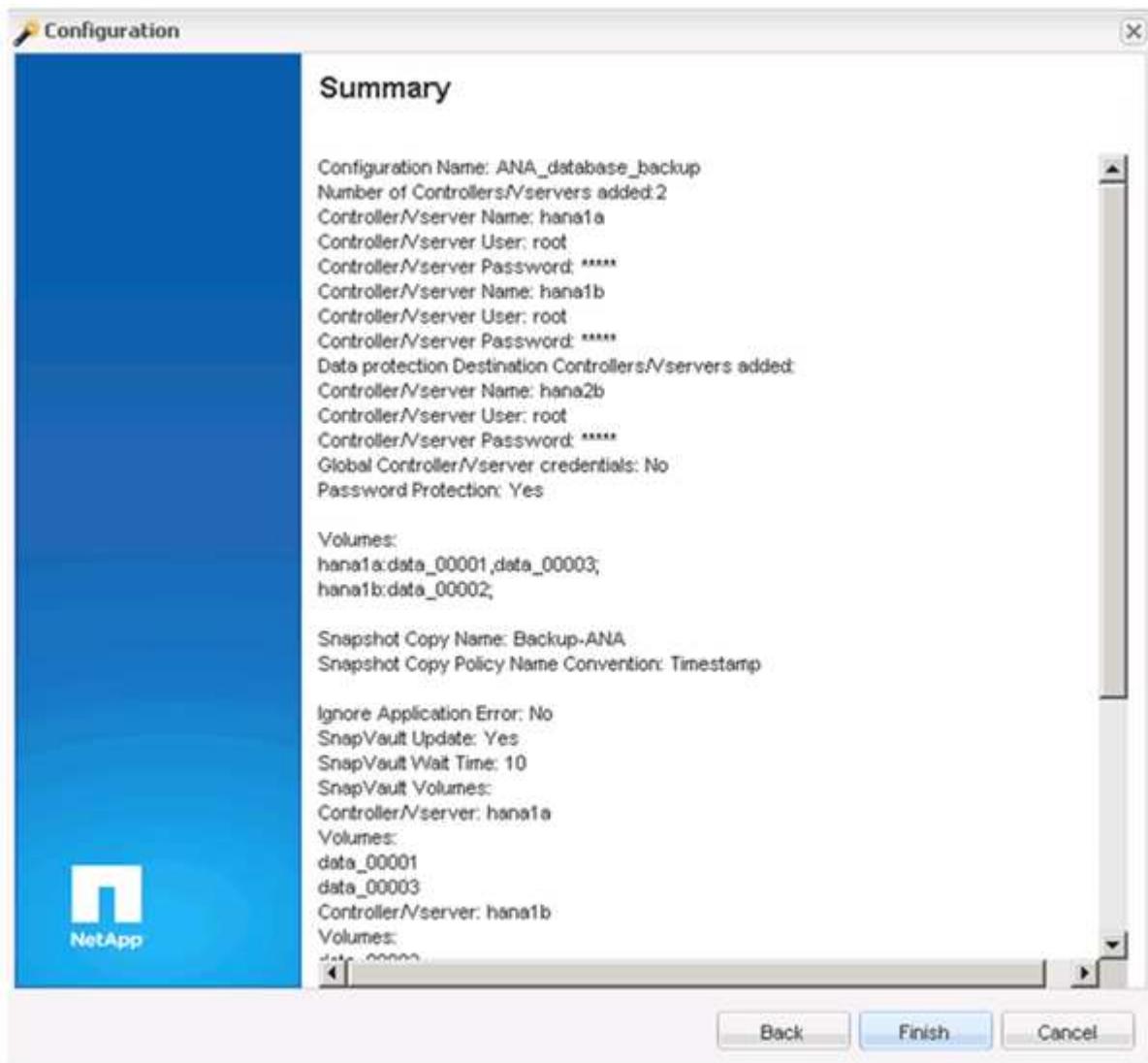
28. Klicken Sie Auf **Weiter**.

**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. Klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.



30. Klicken Sie auf die Registerkarte **SnapVault-Einstellungen**.

31. Wählen Sie in der Dropdown-Liste der Option **SnapVault-Wiederherstellung warten** \* Ja aus, und klicken Sie auf **Speichern**.

Enable Policy	Policy Name	Retention
<input checked="" type="checkbox"/>	hourly	10
<input checked="" type="checkbox"/>	daily	5
<input type="checkbox"/>	weekly	0
<input type="checkbox"/>	monthly	0

Prevent Snapshot copy Deletion: No

SnapVault Retention Age: [ ]

SnapVault wait time: 10

Max Transfer: [ ]

SnapVault Snapshot copy: No

SnapVault Restore Wait: Yes

Es wird empfohlen, für den Replikationsverkehr ein dediziertes Netzwerk zu verwenden. Wenn Sie sich dazu entscheiden, sollten Sie diese Schnittstelle in die Snap Creator-Konfigurationsdatei als sekundäre Schnittstelle aufnehmen.

Außerdem können Sie dedizierte Managementoberflächen konfigurieren, sodass Snap Creator über eine Netzwerkschnittstelle, die nicht an den Host-Namen des Storage Controllers gebunden ist, auf das Quell- oder Ziel-Storage-System zugreifen kann.

```
mgttsrv01:/opt/NetApp/Snap_Creator_Framework_411/scServer4.1.1c/engine/configs/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
```

## **Copyright-Informationen**

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDER EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

**ERLÄUTERUNG ZU „RESTRICTED RIGHTS“:** Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## **Markeninformationen**

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.