



# Configuring data backups

## Snap Creator Framework

NetApp  
August 30, 2024

This PDF was generated from [https://docs.netapp.com/us-en/snap-creator-framework/sap-hana-ops/task\\_configuring\\_the\\_backup\\_user\\_and\\_hdbuserstore.html](https://docs.netapp.com/us-en/snap-creator-framework/sap-hana-ops/task_configuring_the_backup_user_and_hdbuserstore.html) on August 30, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Configuring data backups. . . . . 1
  - Configuring the backup user and hdbuserstore . . . . . 1
  - Configuring SnapVault relationships . . . . . 2
  - Starting the SnapVault relationships . . . . . 3
  - Configuring the Snap Creator Framework and SAP HANA database backup . . . . . 5

# Configuring data backups

After you install the required software components, follow these steps to complete the configuration:

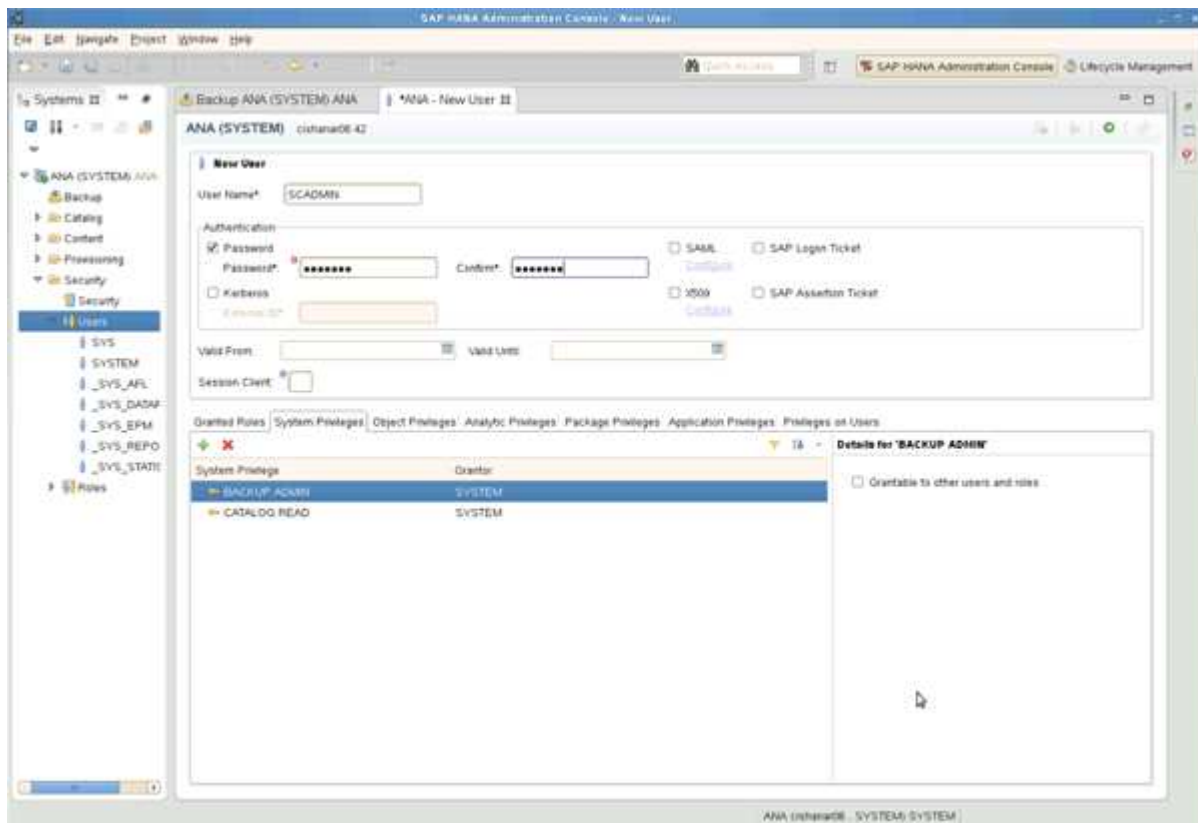
1. Configure a dedicated database user and the SAP HANA userstore.
2. Prepare SnapVault replication on all storage controllers.
3. Create volumes at secondary storage controller.
4. Initialize the SnapVault relationships for database volumes.
5. Configure Snap Creator.

## Configuring the backup user and hdbuserstore

You should configure a dedicated database user within the HANA database to run the backup operations with Snap Creator. In a second step, you should configure a SAP HANA userstore key for this backup user. This userstore key is used within the configuration of the Snap Creator SAP HANA plug-in.

The backup user must have the following privileges:

- BACKUP ADMIN
- CATALOG READ



1. At the administration host, the host where Snap Creator got installed, a userstore key is configured for all database hosts that belong to the SAP HANA database. The userstore key is configured with the OS root user: `hdbuserstore set keyhost 3[instance]15 userpassword`

## 2. Configure a key for all four database 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
```

## Configuring SnapVault relationships

When you configure SnapVault relationships, the primary storage controllers must have a valid SnapRestore and SnapVault license installed. The secondary storage must have a valid SnapVault license installed.

1. Enable SnapVault and NDMP on the primary and the secondary storage controllers.

```
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. On all primary storage controllers, configure the access to the secondary storage controller.

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



Using a dedicated network for replication traffic is recommended. In such cases, the host name of this interface at the secondary storage controller needs to be configured. Instead of hana2b, the host name could be hana2b-rep.

3. On the secondary storage controller, configure the access for all primary storage controllers.

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



Using a dedicated network for replication traffic is recommended. In such cases, the host name of this interface at the primary storage controllers needs to be configured. Instead of hana1b and hana1a the host name could be hana1a-rep and hana1b-rep.

## Starting the SnapVault relationships

You need to start the SnapVault relationship with Data ONTAP operating in 7-Mode and clustered Data ONTAP.

### Starting the SnapVault relationships with Data ONTAP operating in 7-Mode

You can start a SnapVault relationship with commands executed on the secondary storage system.

1. For storage systems running Data ONTAP operating in 7-Mode, you start the SnapVault relationships by running the following command:

```
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>
```



It is recommended that you use a dedicated network for replication traffic. In that case, configure the host name of this interface at the primary storage controllers. Instead of hana1b and hana1a, the host name could be hana1a-rep and hana1b-rep.

## Starting the SnapVault relationships with clustered Data ONTAP

You need to define a SnapMirror policy before you start a SnapVault relationship.

1. For storage systems running clustered Data ONTAP, you start the SnapVault relationships by running the following command.

```
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
```

The policy must contain rules for all retention classes (labels) that are used in the Snap Creator configuration. The above commands show how to create a dedicated SnapMirror policy SV\_HANA

2. To create and start the SnapVault relationship on the cluster console of the backup cluster, run the following commands.

```
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.

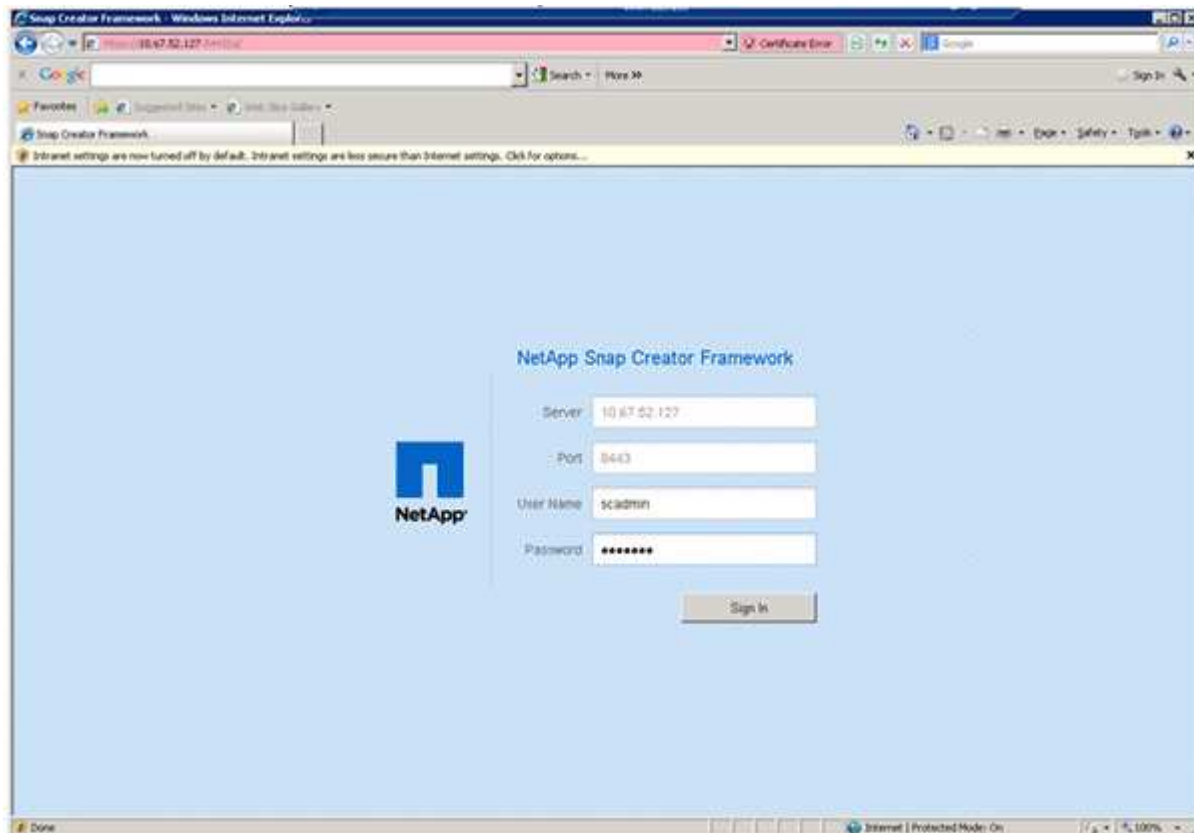
hana::> snapmirror initialize -destination-path hana2b:backup_hana_data
-type XDP
```

## Configuring the Snap Creator Framework and SAP HANA database backup

You must configure the Snap Creator Framework and the SAP HANA database backup.

1. Connect to the Snap Creator graphical user interface (GUI): <https://host:8443/ui/>.

2. Log in using the user name and password that were configured during the installation. Click **Sign in**.



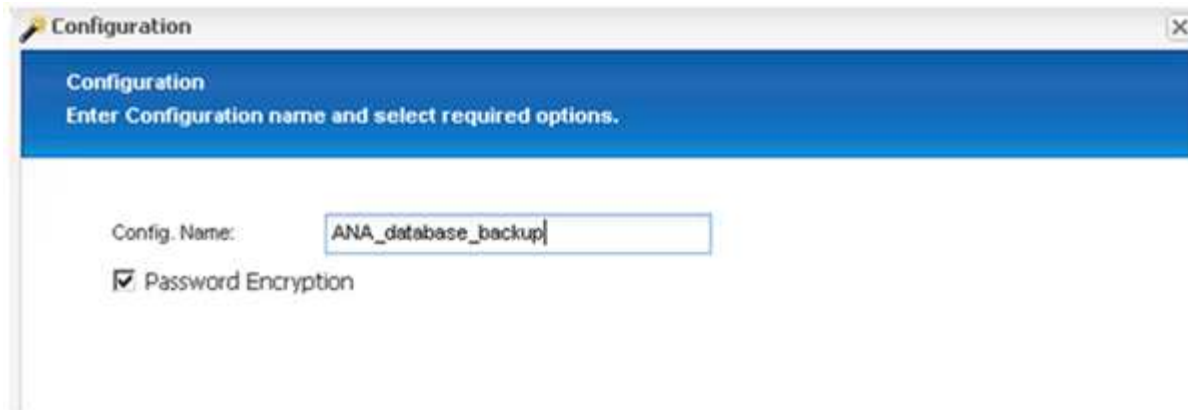
3. Enter a profile name and click **OK**.



For example, "ANA" is the SID of the database.

4. Enter the configuration name, and click **Next**.





The image shows a 'Configuration' dialog box with a blue header bar containing the title 'Configuration' and a close button. Below the header, the text 'Enter Configuration name and select required options.' is displayed. The main area contains a text input field labeled 'Config. Name:' with the value 'ANA\_database\_backup' entered. Below the input field, there is a checked checkbox labeled 'Password Encryption'.

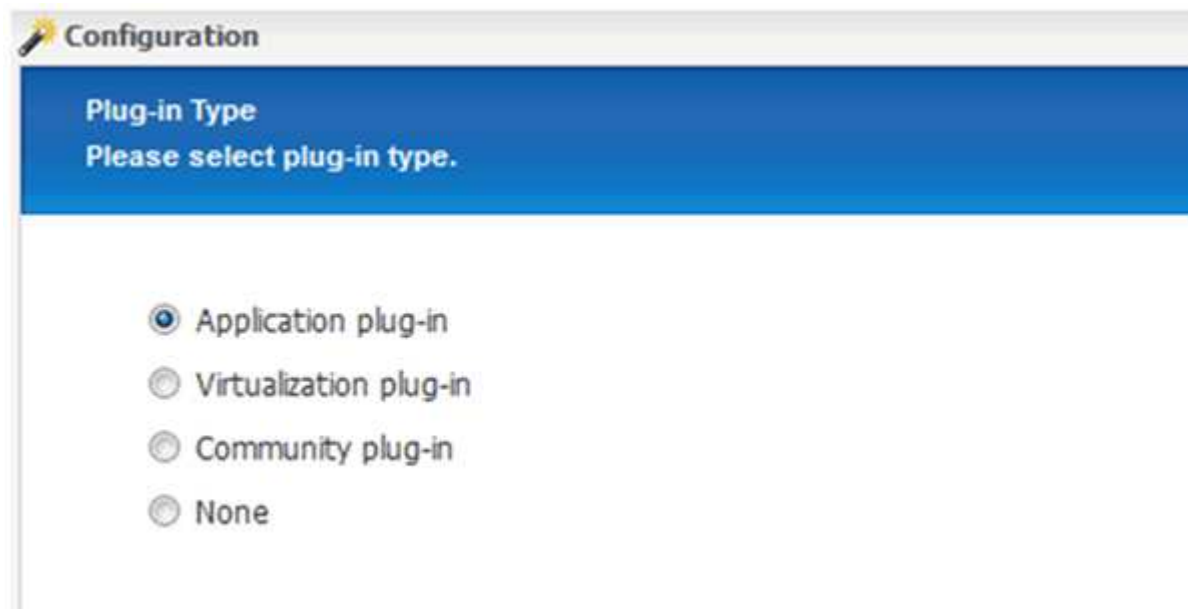
Configuration

Enter Configuration name and select required options.

Config. Name: ANA\_database\_backup

☒ Password Encryption

5. Select **Application plug-in** as the plug-in type, and click **Next**.



The image shows a 'Configuration' dialog box with a blue header bar containing the title 'Configuration' and a close button. Below the header, the text 'Plug-in Type' and 'Please select plug-in type.' is displayed. The main area contains four radio button options: 'Application plug-in' (selected), 'Virtualization plug-in', 'Community plug-in', and 'None'.

Configuration

Plug-in Type

Please select plug-in type.

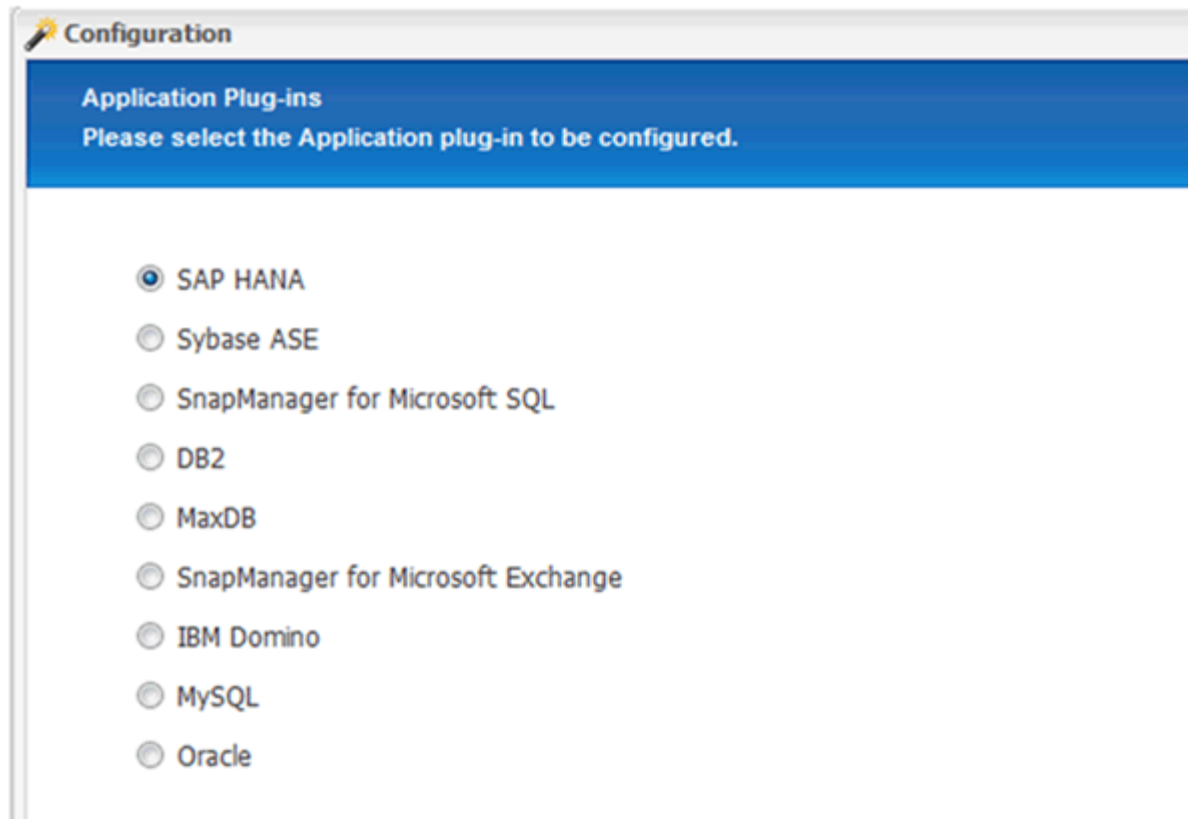
☒ Application plug-in

☐ Virtualization plug-in

☐ Community plug-in

☐ None

6. Select **SAP HANA** as the application plug-in, and click **Next**.



7. Enter the following configuration details:

- a. Select **Yes** from the drop-down menu to use the configuration with a multitenant database. For a single container database select **No**.
- b. If Multitenant Database Container is set to **No**, you must provide the database SID.
- c. If Multitenant Database Container is set to **Yes**, you must add the hdbuserstore keys for each SAP HANA node.
- d. Add the name of the tenant database.
- e. Add the HANA nodes on which the hdbsql statement must be executed.
- f. Enter the HANA node instance number.
- g. Provide the path to the hdbsql executable file.
- h. Add the OSDB user.
- i. Select **Yes** from the drop-down list to Enable LOG Cleanup.

NOTE:

- Parameter `HANA_SID` is available only if the value for parameter `HANA_MULTITENANT_DATABASE` is set to `N`
- For multitenant database containers (MDC) with a “Single Tenant” resource type, the SAP HANA Snapshot copies work with UserStore Key based authentication. If the `HANA_MULTITENANT_DATABASE` parameter is set to `Y`, then the `HANA_USERSTORE_KEYS` parameter must be set to the appropriate value.
- Similar to non-multitenant database containers, the file-based backup and integrity check feature is supported

j. Click **Next**.

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. Enable the File-Based Backup operation:
  - a. Set the File-Backup Location.
  - b. Specify the file-backup prefix.
  - c. Select the **Enable File-Backup** checkbox.
  - d. Click **Next**.

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'.

Configuration

File-Based Backup Configuration Details  
Provide File-Based Backup Details

File-Backup Location:

File-Backup prefix:

Enable File-Backup: ☐

Back Next Cancel

9. Enable the Database Integrity Check operation:
  - a. Set the temporary File-Backup location.
  - b. Select the **Enable DB Integrity Check** checkbox.
  - c. Click **Next**.

**Configuration**

**Integrity Check Configuration Details**  
Provide Integrity Check Details

Temporary File-Backup Location:

Enable DB Integrity Check: ☐

10. Enter the details for the agent configuration parameter, and click **Next**.

**Agent Configuration**  
Enter agent configuration details

IP/DNS:

Port:

Timeout (secs):

11. Enter the storage connection settings, and click **Next**.

**Storage Connection Settings**  
Please Provide Storage Connection Settings

Use OnCommand Proxy: ☐

Transport:

Controller/Vserver Port:

12. Enter the storage login credentials, and click **Next**.

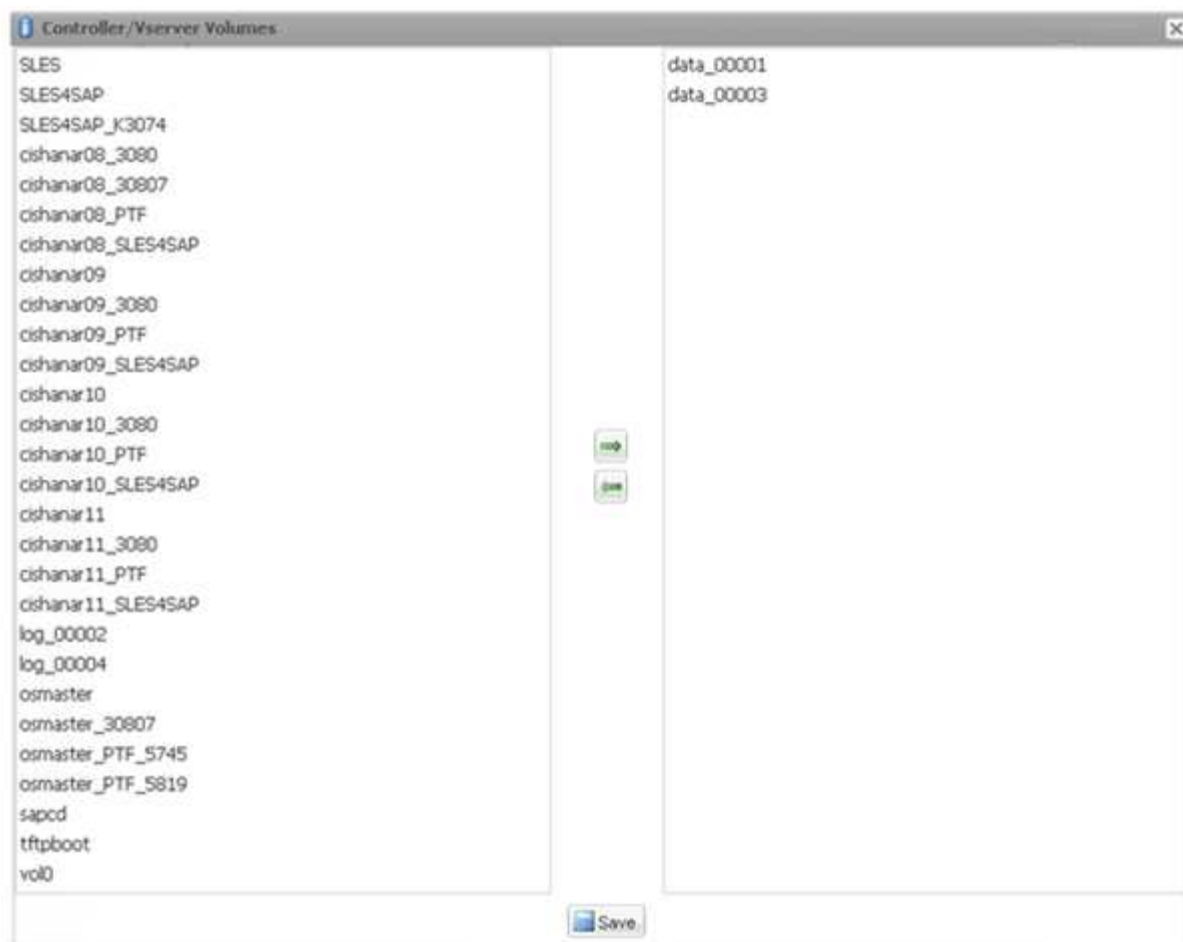
**Controller/Vserver Credentials**  
Add one or more Controller/Vserver credentials to the configuration.

**Controller/Vserver Login Credentials**

 Add  Edit  Delete

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

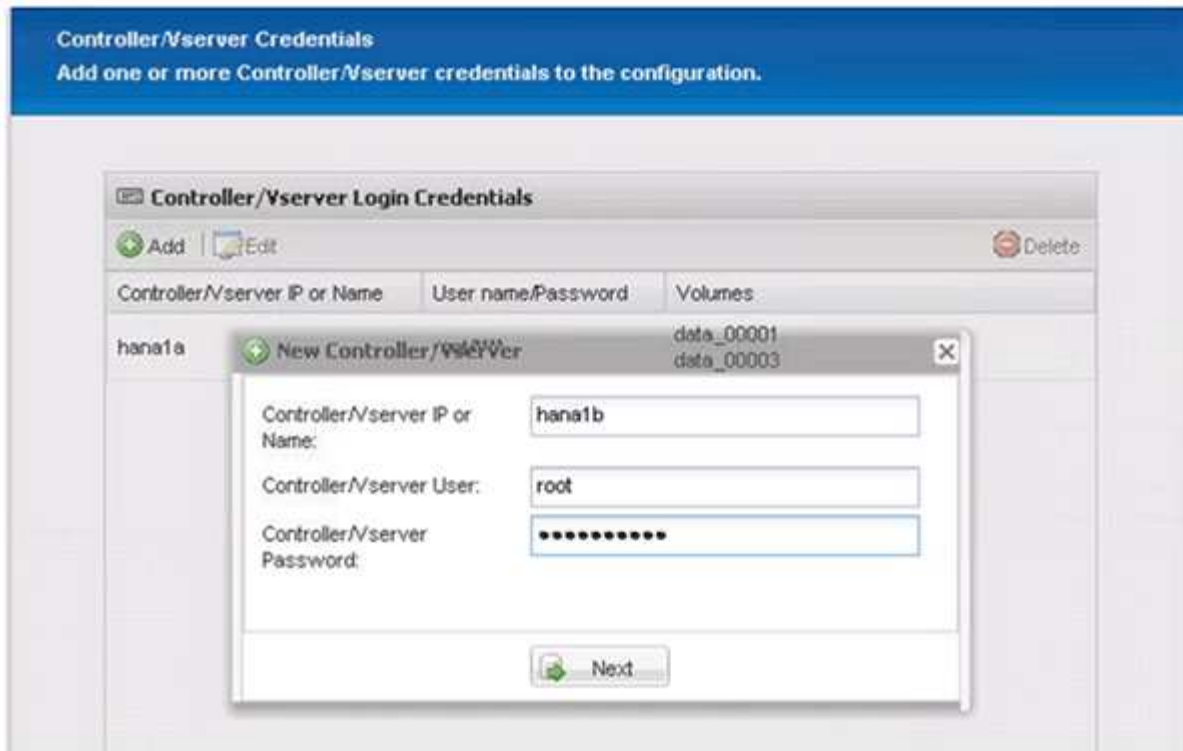
13. Select the data volumes that are stored on this storage controller, and click **Save**.



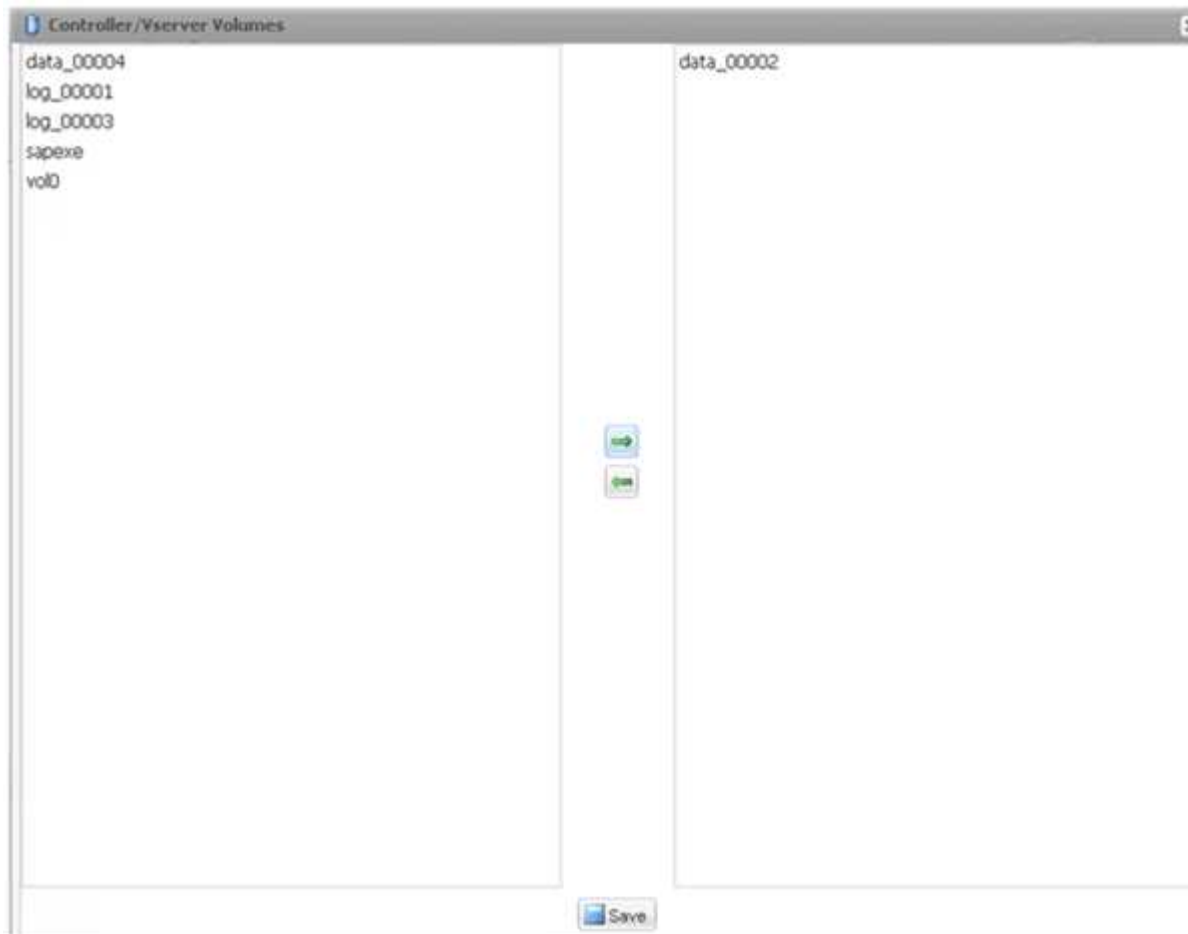
14. Click **Add** to add another storage controller.



15. Enter the storage login credentials, and click **Next**.



16. Select the data volumes that are stored on the second storage controller that you created, and click **Save**.



17. The Controller/Vserver Credentials window displays the storage controllers and volumes that you added.



Click **Next**.

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

18. Enter the Snapshot policy and retention configuration.

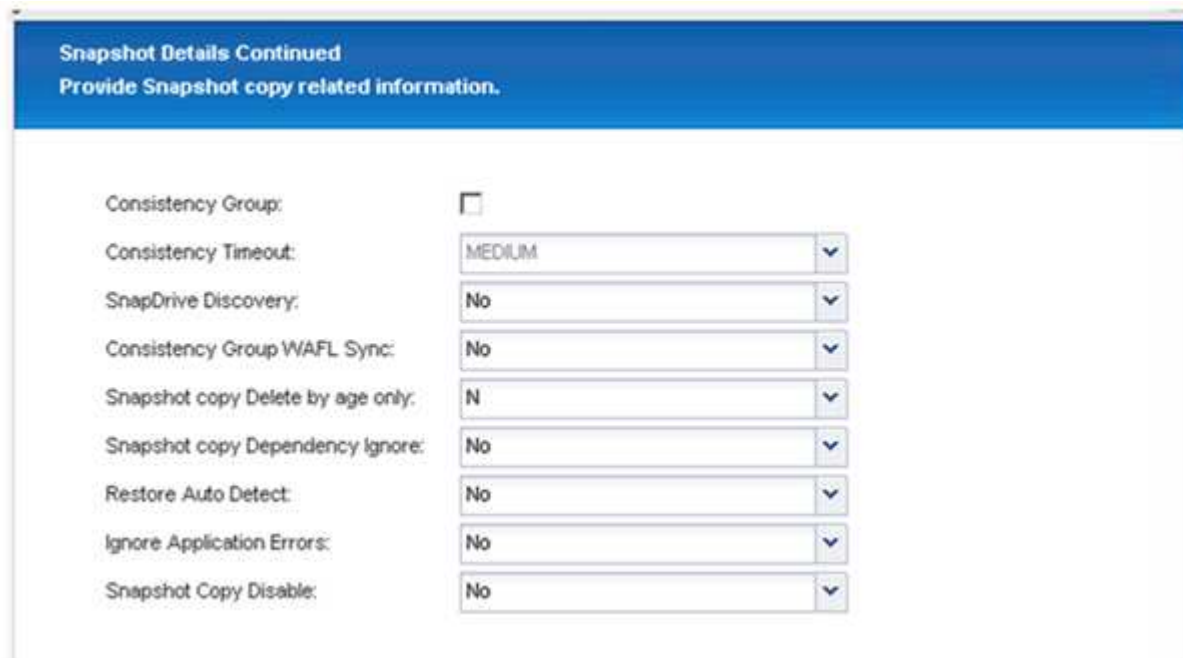
The retention of three daily and eight hourly Snapshot copies is just an example and could be configured differently depending on the customer requirements.



Select **Timestamp** as the naming convention. The use of the naming convention **Recent** is not supported with the SAP HANA plug-in, because the timestamp of the Snapshot copy is also used for the SAP HANA backup catalog entries.

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

19. No changes required. Click **Next**.



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

Consistency Group: ☐

Consistency Timeout: MEDIUM

SnapDrive Discovery: No

Consistency Group WAFL Sync: No

Snapshot copy Delete by age only: N

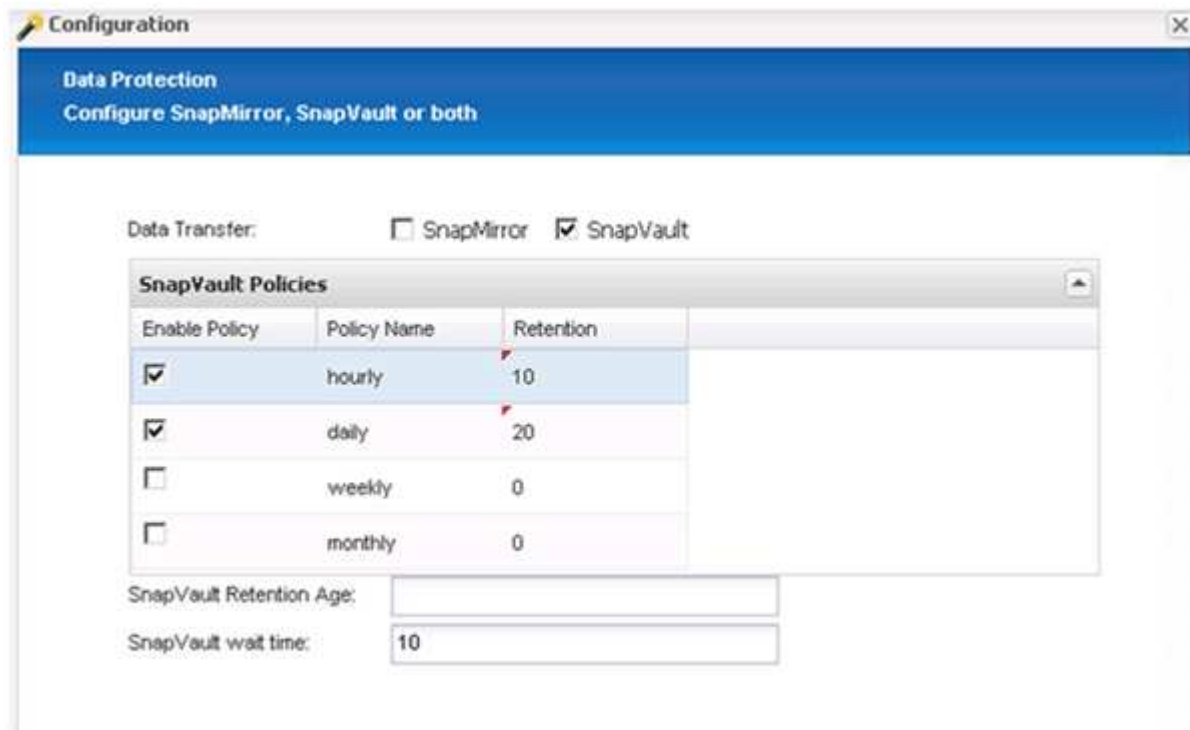
Snapshot copy Dependency ignore: No

Restore Auto Detect: No

Ignore Application Errors: No

Snapshot Copy Disable: No

20. Select **SnapVault**, and configure the SnapVault retention policies and the SnapVault wait time.



**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

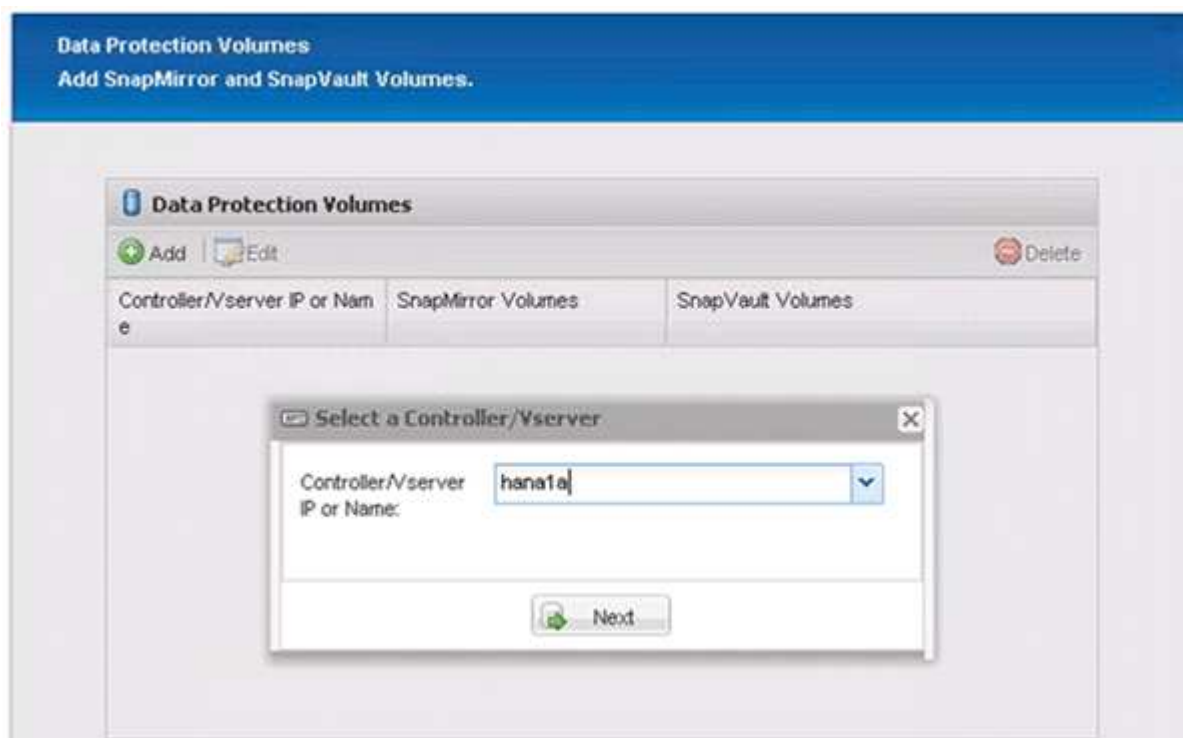
SnapVault Retention Age:

SnapVault wait time: 10

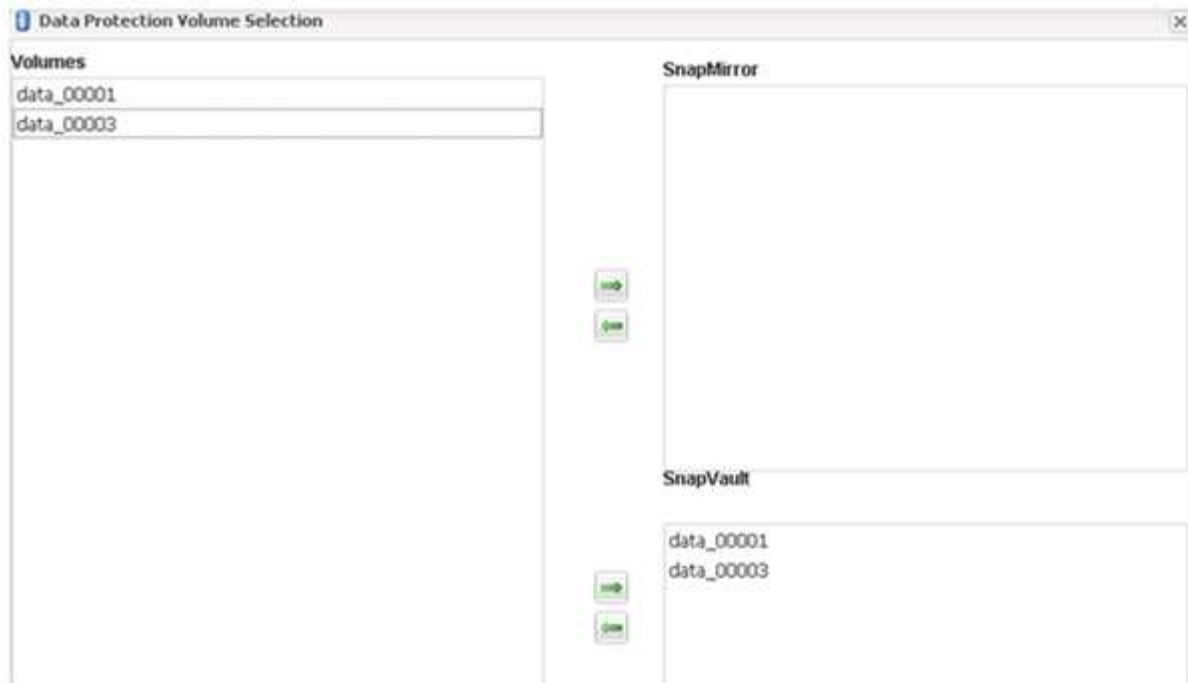
21. Click **Add**.



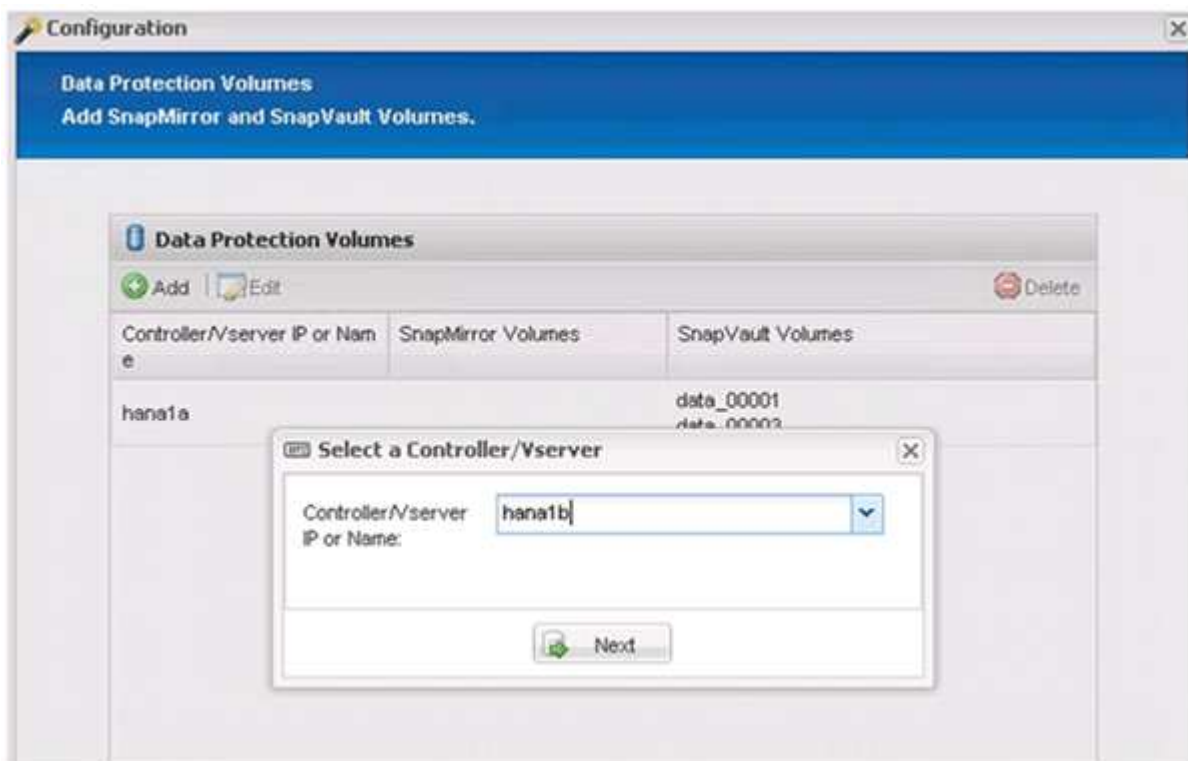
22. Select a source storage controller from the list, and click **Next**.



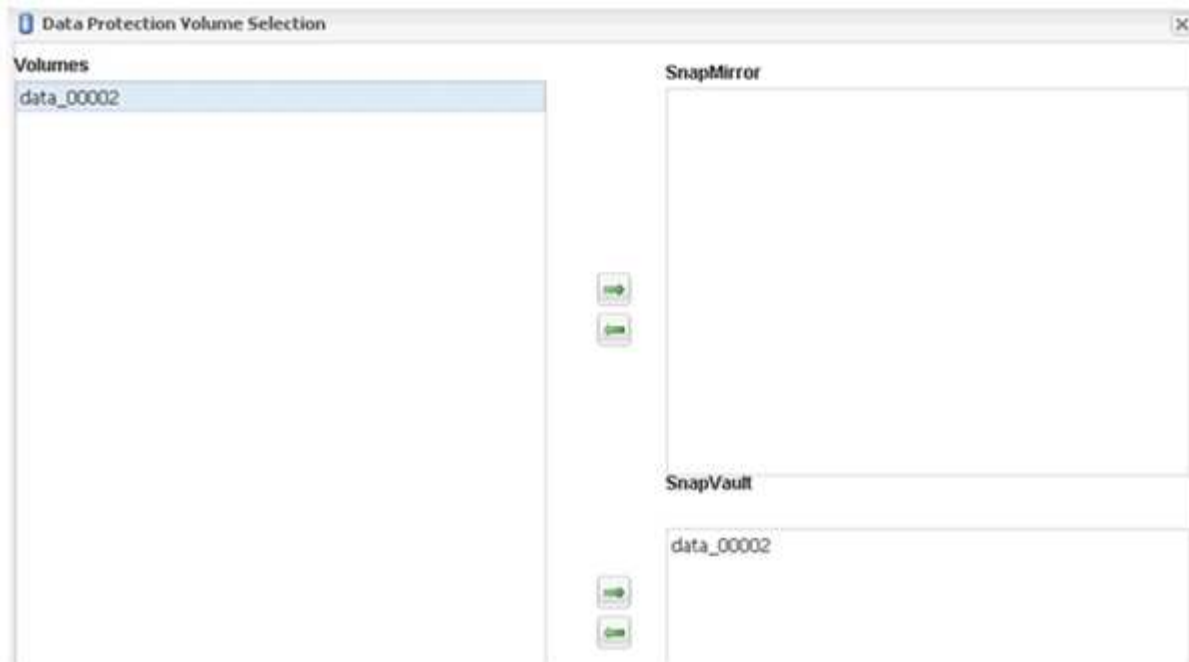
23. Select all the volumes that are stored on the source storage controller, and click **Save**.



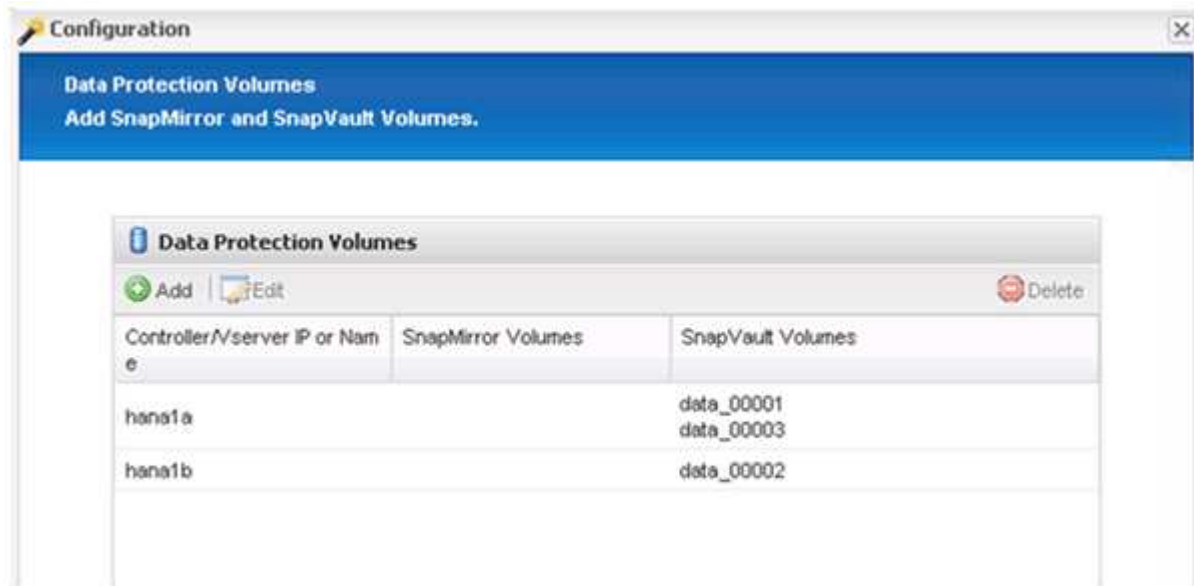
24. Click **Add**, and select the second source storage controller from the list, and then click **Next**.



25. Select all the volumes that are stored on the second source storage controller, and click **Save**.



26. The Data Protection Volumes window displays all the volumes that should be protected in the configuration that you created. Click **Next**.



27. Enter the credentials for the target storage controllers, and click **Next**. In this example, the “root” user credentials are used to access the storage system. Typically, a dedicated backup user is configured on the storage system and is then used with Snap Creator.

The screenshot shows a 'Configuration' window with a blue header bar containing the text 'Data protection relationships' and 'SnapMirror and SnapVault relationships'. Below the header, it states 'Verified all SnapMirror relationships.' and 'Verified all SnapVault relationships.'. A section titled 'hana2b' is expanded, showing two input fields: 'Controller/server User:' with the value 'root' and 'Controller/server Password:' with a masked password represented by dots.

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. Click **Next**.

The screenshot shows a 'DFM/OnCommand Settings' window with a blue header bar containing the text 'DFM/OnCommand Settings' and 'Enter OnCommand credentials and other details and settings.'. Below the header, there are two checkboxes: 'Operations Manager console Alert' (unchecked) and 'NetApp Management Console data protection capability' (checked). Below these are five input fields: 'Host:', 'User:', 'Password:', 'Transport:' (with a dropdown arrow), and 'Port:'.

DFM/OnCommand Settings  
Enter OnCommand credentials and other details and settings.

☐ Operations Manager console Alert

☒ NetApp Management Console data protection capability

Host:

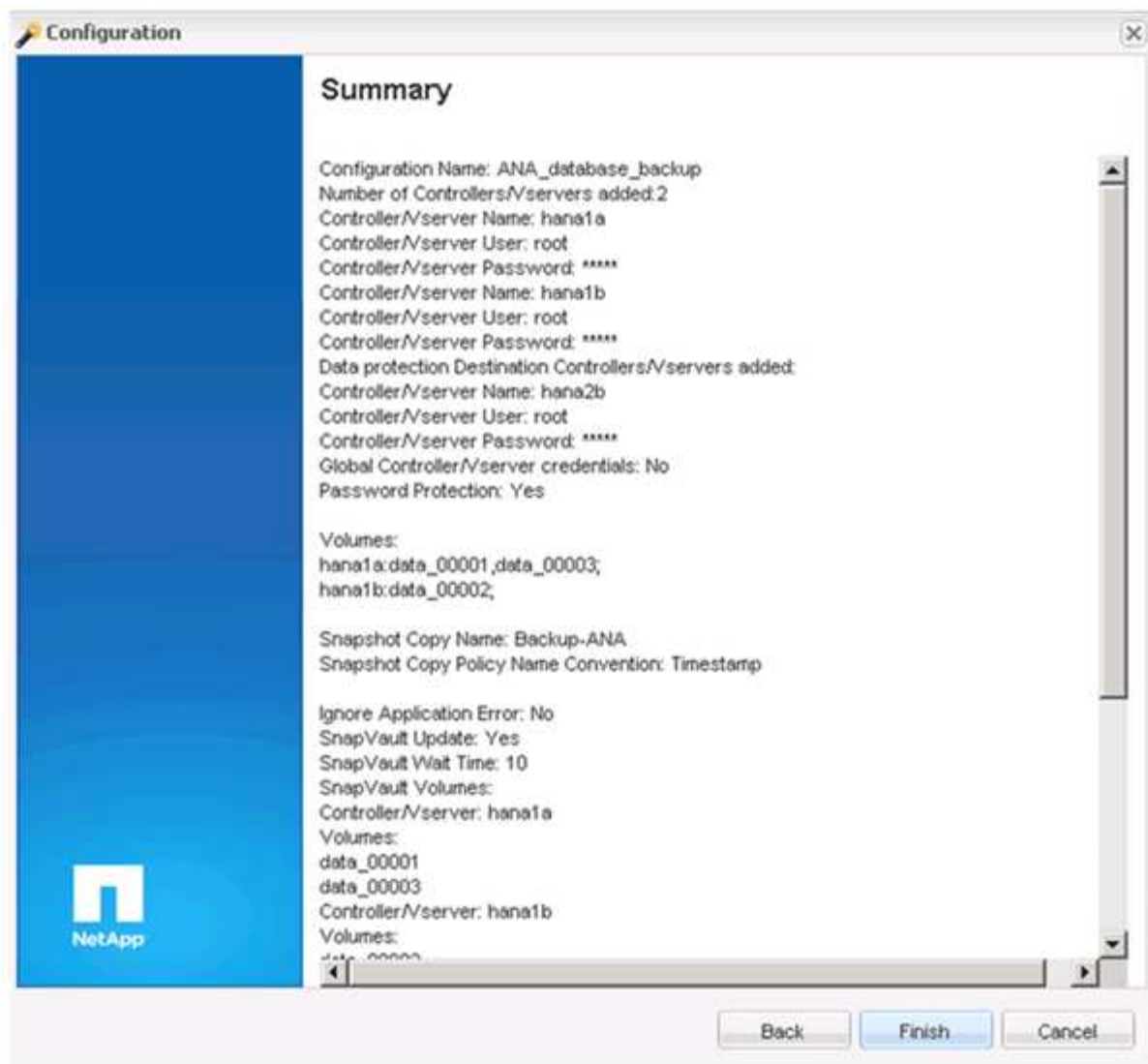
User:

Password:

Transport:  ▼

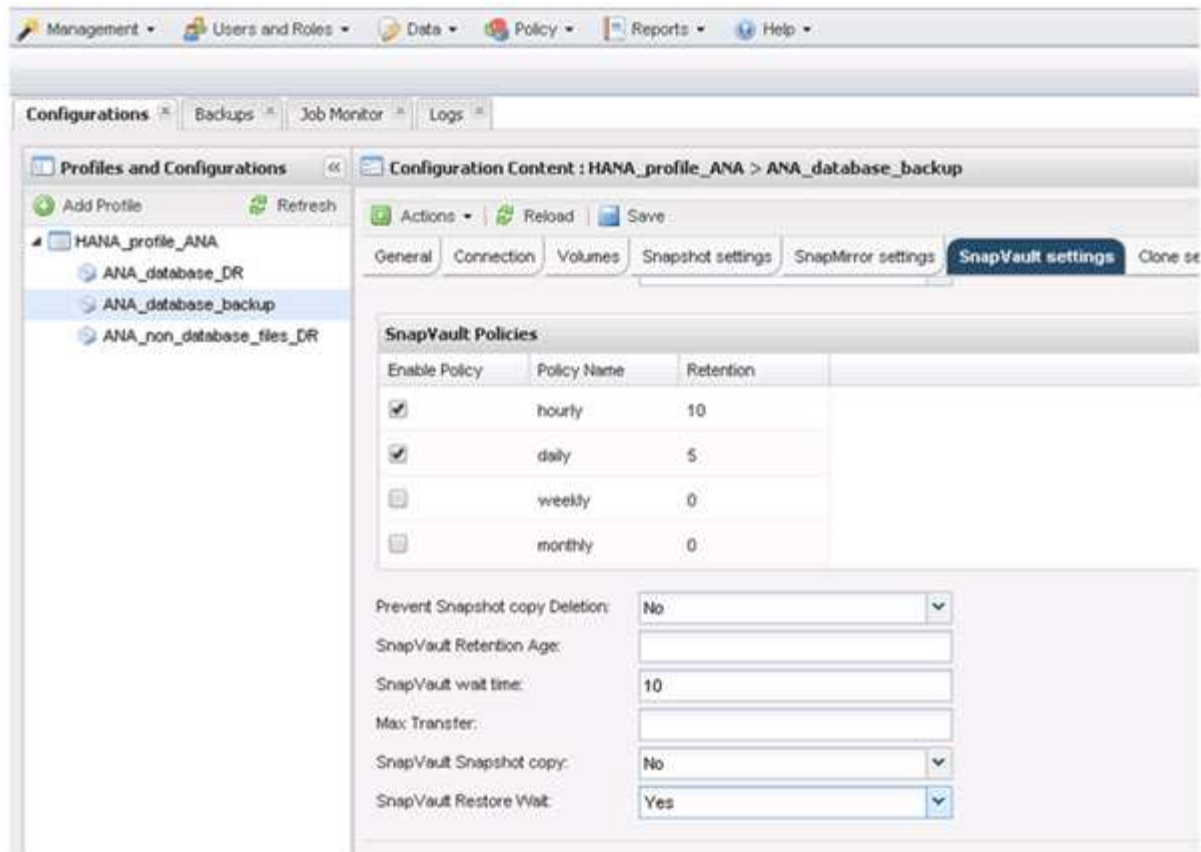
Port:

29. Click **Finish** to complete the configuration.



30. Click the **SnapVault settings** tab.

31. Select **Yes** from the drop-down list of the **SnapVault Restore Wait** option, and click **Save**.



It is recommended that you use a dedicated network for replication traffic. If you decide to do so, you should include this interface in the Snap Creator configuration file as a secondary interface.

You can also configure dedicated management interfaces so that Snap Creator can access the source or the target storage system by using a network interface that is not bound to the storage controller's host name.

```
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
```



## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.