

Configuring data backups

Snap Creator Framework

NetApp August 28, 2025

This PDF was generated from https://docs.netapp.com/us-en/snap-creator-framework/sap-hanaops/task_configuring_the_backup_user_and_hdbuserstore.html on August 28, 2025. 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
Starting the SnapVault relationships with Data ONTAP operating in 7-Mode	 . 3
Starting the SnapVault relationships with clustered Data ONTAP	 . 4
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

	GAP HABA Administration Currente A	Am Vast	-
Ele Est gaugate Briest	Rautow Date		
() - () () - ()	1 C 227 195	🚯 (Sero et Sero) 👘 👔 🐃 SAP ISANA Administration Canada 🖉 Obrigita Managam	east.
la Systems II	Eachup ANA (SVSTEN) ANA MNA - New User II	- 0	1
B. H H. B.	ANA (SYSTEM) cisturade 42	5 6 0 C	c
	New Own User Name* SCADARS Authoritication Passend Passend Netherin Contern* Contern* Velot From Weld From Second Cont	SAME SAP Legen Ticket Contract Contract	9
SVS_AR	Session Charter		
SYS EPM	Granted Roles System Polleges Object Polleges' Analytic Polleges' Package Po	weges Application Privileges Privileges of Users	
1_SVS_REPO	* X	7 18 - Details for 'BACKUP ADMIN'	
SVS_SVS_STATE	System Protege Drants:	Van Strate - 200 States	
* #2 Adves	BERNAR ASSAULT TYTEM	C Orantable to other users and roles	
	- CATALOG NEAD SYSTEM		
		4	
	<u></u>	ANA Inclumente System, bystem	

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.

```
hanala> options snapvault.enable on
hanala> ndmp on
hanala>
hanalb> options snapvault.enable on
hanalb> ndmpd on
hana2b> options snapvault.enable on
hana2b> ndmpd on
hana2b>
```

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

```
hanala> options snapvault.access host=hana2b
hanala>
hanalb> options snapvault.access host=hana2b
hanalb>
```



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
                           ----- ---- ----- -----
                                             20 false
                           daily
                                                            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**.

Stop Creative Framework Windows Internet Explores	- 22	China	and the second se	RIG IS
C		• Q Contractor	B 9 8 10 mile	1P-
· Conge	· (Tseet	Plane 34		
Another a suggested best + g and the later +				
a Ship Create Pranework			Q • D • ⇒ # • be	e - Salety - Typin - 🖗 -
Intranet settings are now turoed all by default. Intranet settings are less secure than bitamet astrongs.	Cleb for options			×
	NetApp 3	Snap Creator Framework		
	للمحمد			
	server	10.00.000.000		
	Port	3443		
	User Name	scadmin		
NetApp [*]		Contract (
	Patreord	******		
		Sign W		
# Done		P P P P P P	Transvet Protected Hode: On	/A + 1% 100%

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

O New Profile		×
Enter new profile name:	HANA_profile_ANA	
	OK	Canaal
	OK	Cancel

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

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

	anna anna anna anna anna anna anna ann	
Config. Name:	ANA_database_backup	
Password End	ryption	

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

Plug-in Type Please select	plug-in type.	
Applic	ation plug-in	
Ø Virtua	lization plug-in	
Comn	nunity plug-in	
None		

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

App Plea	lication Plug-ins ise select the Application plug-in to be configured.
	SAP HANA
	Sybase ASE
	SnapManager for Microsoft SQL
	© DB2
	C MaxDB
	SnapManager for Microsoft Exchange
	IBM Domino
	MySQL
	Oracle

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 $\ensuremath{\text{Yes}}$ 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/e	xe/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.

onnguration		
File-Based Backup Config Provide File-Based Backu	puration Details p Details	
File-Backup Location:		
File-Backup prefix:		
Enable File-Backup:		

- 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.

Integration		
Provide Integrity Check Details		
Tamanan Ede Baston Landlan	1	
Temporary File-Dackup Location.		
Enable DB Integrity Check:		

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

IP/DNS:	localhost	
Port:	9090	
Timeout (secs):	300	
Test agent conn	ection	

11. Enter the storage connection settings, and click $\ensuremath{\textbf{Next}}.$

	NUMBER OF STREET		
Use OnCommand Proxy:			
Transport:	HTTPS	~	

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

Contr	oller/Vserver Login	Credenti	als		
Add	Edit				Oelete
Controller/Vserver IP or Name		User na	me/Password	Volumes	
	Controller/Vserver Controller/Vserver IP or Name: Controller/Vserver User: Controller/Vserver Password		hana1a		
			root	•	

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

Controller/Vserver Volumes		×
SLES	data_00001	
SLES4SAP	data_00003	
SLES4SAP_K3074		
cishanar08_3080		
cishanar08_30807		
cishanar08_PTF		
cithanar08_SLES4SAP		
cishanar09		
cishanar09_3080		
cishanar09_PTF		
cishanar09_SLES4SAP		
cishanar 10		
cishanar10_3080	(m)	
cishanar10_PTF	000	
cishanar10_SLE54SAP	(cm)	
cishanar 11	6229	
cishanar11_3080		
cishanar11_PTF		
cishanar11_SLES4SAP		
50000_gol		
log_00004		
osmaster		
osmaster_30807		
osmaster_PTF_S745		
osmaster_PTF_S819		
saped		
tftpboot		
Olov		
	Sava	

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

Controller/Vserver Login	Credentials	
🔘 Add 🔂 Edit		😂 Dele
Controller/Vserver IP or Name	User name/Password	Volumes
hanata	root/****	data_00001

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

Contr	oller/¥server Login	Credenti	als			
Add	[⊒ Eat				0	Delete
Controller/	Controller/Vserver IP or Name User name/		me/Password	Volumes		
hana1a	New Control	er/996990	er	data_00001 data_00003	×	
	Controller/Vserver IP or Name:		hana1b			
	Controller/Vserv	er User:	root			
	Controller/Vserv	er	•••••	•		

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

1) Controller/Vserver Volumes		×
data_00004 log_00003 sapexe vol0		data_00002
	Save	

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

Click Next.

📼 Controller/Vserver Login	Credentials		
🔕 Add 🔂 Edit			😂 Delete
Controller/Vserver IP or Name	User name/Password	Volumes	
hanata	root/****	data_00001 data_00003	
hanatb	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.

Snapshot copy Ne	me:	Backup-ANA		
Snapshot copy La	bet			
Policy Type:	Policies	Use Policy C Use Pol	cy Object	
Enable Policy	Policy Name	Retention		
N	hourly	12		
5	daily	3		
	weekly	0		
П	monthly	0		

19. No changes required. Click Next.

- 6	BUDIN.	
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	*
Spanshot Conv Disable	No	

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

Data Transfer:	□ Sna	pMirror 🔽 SnapVault	
Snap¥ault Poli	icies		(
Enable Policy	Policy Name	Retention	
V	hourly	10	
5	daily	20	
	weekly	0	
E	manthly	0	

21. Click Add.

Data Protection Volum	ies	
🔾 Add 🏹 Edit		0
Controller/Vserver IP or Nam e	SnapMirror Volumes	SnapVault Volumes

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

				🔵 Deiet
Controller/Vserver IP or Nam		r Volumes	SnapVault Volumes	
Controller	Vserver	hanata		*
IP or Nam	e:			
	r IP or Nam	r IP or Nam ShapMirro Select a Controll Controller/Vserver IP or Name:	r IP or Nam SnapMirror Volumes	r IP or Nam SnapMirror Volumes SnapVault Volume Select a Controllier/Vserver Controller/Vserver hana1a IP or Name:

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

	×
SnapMirror	
1000	
SnapVault	
data_00001 data_00003	
	SnapMirror SnapVault Gata_00001 Gata_00003

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

0 Data Pro	otection Volum	ies			
🖉 Add 🛛 🌄	Edit				🙆 Delete
Controller/Vs	erver IP or Nam	SnapMirror Volumes SnapVault Vo		SnapVault Volumes	
hanata				data_00001	
	I Select	a Controller/Vserver			×
Control IP or No		Nserver e:	hana1b	*	

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

Data Protection Volume Selection		×
Volumes data_00002	SnapMirror	
	SnapVault	
	data_00002	

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

SnapMirror and SnapVault \	/olumes.	
1 Data Protection Volum	ies	
Add Treat		() D
Controller/Vserver IP or Nam e	SnapMirror Volumes	SnapVault Volumes
hanala		data_00001 data_00003
hanatb		deta_00002

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.

Data protection relationships	•	
SnapMirror and SnapVault re	lationships	
Verified all SnapMirror relati	ionships.	
hana2b	onsneps.	
- 2777 K	root	
Controller/Vserver User	1974	
Controller/Vserver User:		
Controller/Vserver User: Controller/Vserver	*******	

28. Click Next.

	Alart	
E tisting timesees Court		
NetApp Management Consol	e data protection capability	
Host		
User:		
User: Password:		
User: Password: Transport:		

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

Lonnguration		
	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 Walt Time: 10	
	SnapVault Volumes:	
	Controller/Vserver: hana1a	
	Volumes:	
1 N	data_00001	
	data_00003	
	Controller/Vserver: hana1b	
NetApp	Volumes:	
		1.1
		<u> </u>

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

Configurations * Backups * Job Mo	nitor * Logs *						
Profiles and Configurations	Configuration	Content : HAN	A_profile_ANA > At	A_database_back	up		
Add Profile	Actions - 🖉 Reload 📄 Save						
HANA_profile_ANA ANA_database_DR	General Connec	tion Volumes	Snapshot settings	SnapMirror settings	SnapVault settings	Clone s	
S ANA_database_backup							
ANA_non_database_files_DR	SnapYault Policies						
	Enable Policy	Policy Name	Retention				
	8	hourly	10				
	2	daily	5				
	8	weekty	0				
	8	monthly	0				
	Prevent Snapshot	copy Deletion:	No		1		
	SnapVault Retention Age: SnapVault wait time: Max Transfer: SnapVault Snapshot copy: SnapVault Restore Wait						
			10		1		
			No		1		
			Yes				

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.

Copyright information

Copyright © 2025 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.