



# **Configuración de backups de datos**

Snap Creator Framework

NetApp  
January 20, 2026

This PDF was generated from [https://docs.netapp.com/es-es/snap-creator-framework/sap-hana-ops/task\\_configuring\\_the\\_backup\\_user\\_and\\_hdbuserstore.html](https://docs.netapp.com/es-es/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.

# Tabla de contenidos

Configuración de backups de datos .....	1
Configuración del usuario de copia de seguridad y hdbuserstore .....	1
Configurar las relaciones de SnapVault .....	2
Iniciar las relaciones de SnapVault .....	3
Iniciar las relaciones de SnapVault con Data ONTAP funcionando en 7-Mode .....	3
Inicio de las relaciones de SnapVault con Clustered Data ONTAP .....	4
Configurar el backup de la base de datos SAP HANA y Snap Creator Framework .....	5

# Configuración de backups de datos

Después de instalar los componentes de software necesarios, siga estos pasos para completar la configuración:

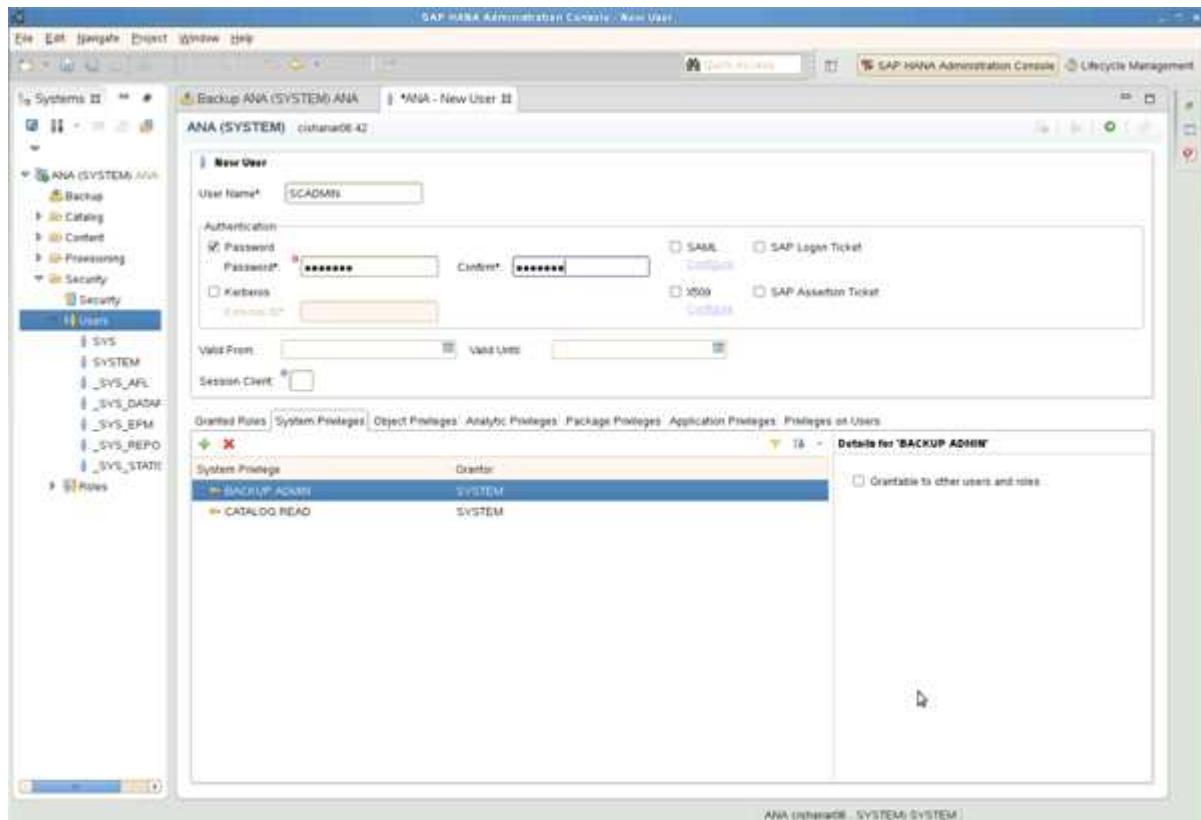
1. Configure un usuario de base de datos dedicado y el almacén de usuarios de SAP HANA.
2. Preparar la replicación de SnapVault en todas las controladoras de almacenamiento.
3. Crear volúmenes en la controladora de almacenamiento secundario.
4. Inicialice las relaciones de SnapVault para volúmenes de base de datos.
5. Configure Snap Creator.

## Configuración del usuario de copia de seguridad y hdbuserstore

Debe configurar un usuario con base de datos dedicada dentro de la base de datos de HANA para ejecutar las operaciones de backup con Snap Creator. En un segundo paso, debe configurar una clave de almacenamiento de usuarios de SAP HANA para este usuario de backup. Esta clave del almacén de usuarios se usa en la configuración del complemento SAP HANA para Snap Creator.

El usuario de backup debe tener los siguientes privilegios:

- ADMINISTRADOR DE BACKUPS
- CATÁLOGO LEÍDO



1. En el host de administración, el host en el que se instaló Snap Creator, se configura una clave de almacenamiento de usuario para todos los hosts de bases de datos que pertenecen a la base de datos SAP HANA. La clave userstore se configura con el usuario raíz del SO: Hdbuserstore set keyhost 3[Instance]15 userpassword
2. Configure una clave para los cuatro nodos de base de datos.

```

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

```

## Configurar las relaciones de SnapVault

Una vez instaladas las relaciones de SnapVault, las controladoras de almacenamiento primario deben tener una licencia válida de SnapRestore y SnapVault. El almacenamiento secundario debe tener instalada una licencia de SnapVault válida.

1. Habilite SnapVault y NDMP en las controladoras de almacenamiento principal y secundario.

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

2. En todas las controladoras de almacenamiento principal, configure el acceso a la controladora de almacenamiento secundario.

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



Se recomienda utilizar una red dedicada para el tráfico de replicación. En estos casos, es necesario configurar el nombre de host de esta interfaz en la controladora de almacenamiento secundario. En lugar de hana2b, el nombre de host podría ser hana2b-rep.

3. En la controladora de almacenamiento secundario, configure el acceso para todas las controladoras de almacenamiento primario.

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



Se recomienda utilizar una red dedicada para el tráfico de replicación. En estos casos, es necesario configurar el nombre de host de esta interfaz en las controladoras de almacenamiento primarias. En lugar de hanalb y hanala, el nombre de host podría ser hanala-rep y hanalb-rep.

## Iniciar las relaciones de SnapVault

Es necesario iniciar la relación de SnapVault con Data ONTAP en 7-Mode y Clustered Data ONTAP.

### Iniciar las relaciones de SnapVault con Data ONTAP funcionando en 7-Mode

Puede iniciar una relación de SnapVault con comandos ejecutados en el sistema de almacenamiento secundario.

1. En los sistemas de almacenamiento que ejecutan Data ONTAP en 7-Mode, se deben iniciar las relaciones de SnapVault ejecutando el siguiente comando:

```
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 recomendable utilizar una red dedicada para el tráfico de replicación. En ese caso, configure el nombre de host de esta interfaz en las controladoras de almacenamiento principales. En lugar de hana1b y hana1a, el nombre del host podría ser hana1arep y hana1brep.

## Inicio de las relaciones de SnapVault con Clustered Data ONTAP

Debe definir una política de SnapMirror antes de iniciar una relación de SnapVault.

1. En el caso de los sistemas de almacenamiento que ejecutan Clustered Data ONTAP, puede iniciar las relaciones de SnapVault ejecutando el siguiente 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

```

La directiva debe contener reglas para todas las clases de retención (etiquetas) que se utilicen en la configuración de Snap Creator. Los comandos anteriores muestran cómo crear una política de SnapMirror dedicada SV\_HANA

2. Para crear e iniciar la relación de SnapVault en la consola de clústeres del clúster de backup, ejecute los siguientes comandos.

```

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.

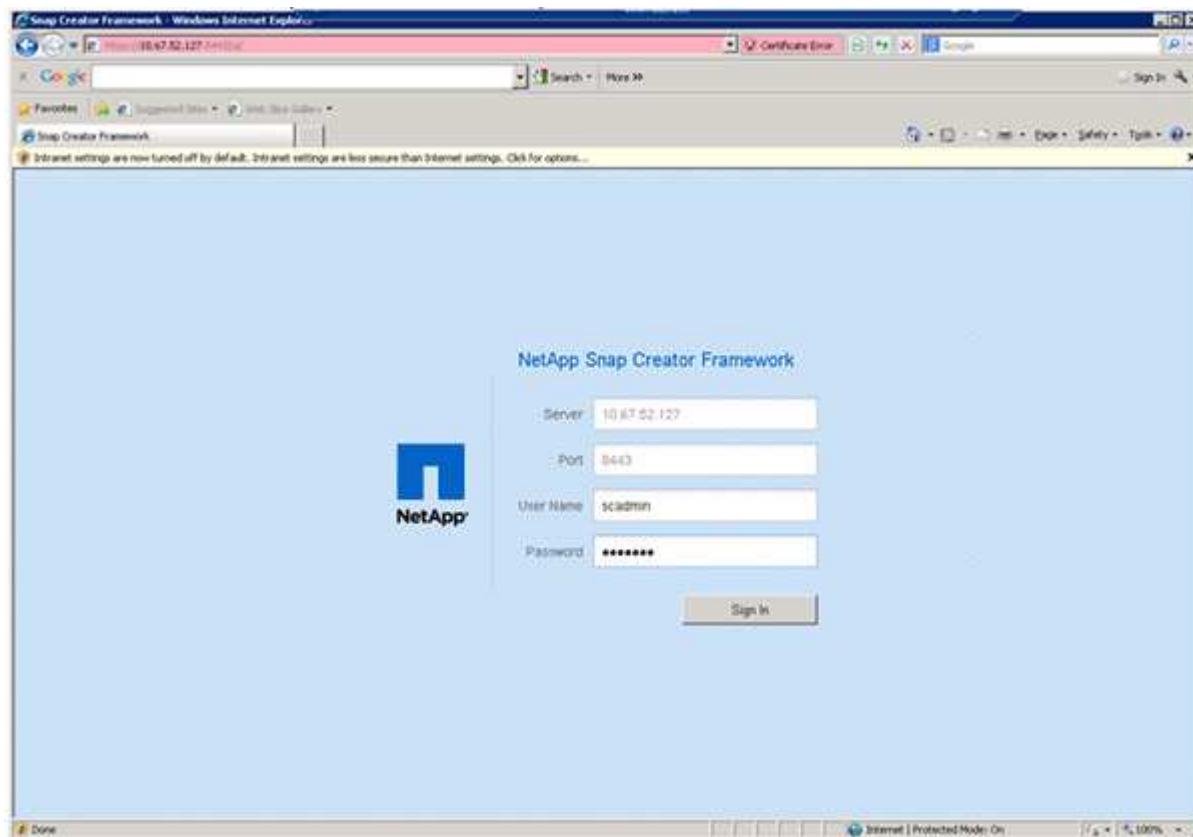
hana::> snapmirror initialize -destination-path hana2b:backup_hana_data
-type XDP

```

## Configurar el backup de la base de datos SAP HANA y Snap Creator Framework

Debe configurar Snap Creator Framework y el backup de la base de datos SAP HANA.

1. Conectarse a la interfaz gráfica de usuario (GUI) de Snap Creator: <https://host:8443/ui/>.
2. Inicie sesión con el nombre de usuario y la contraseña configurados durante la instalación. Haga clic en **Iniciar sesión**.

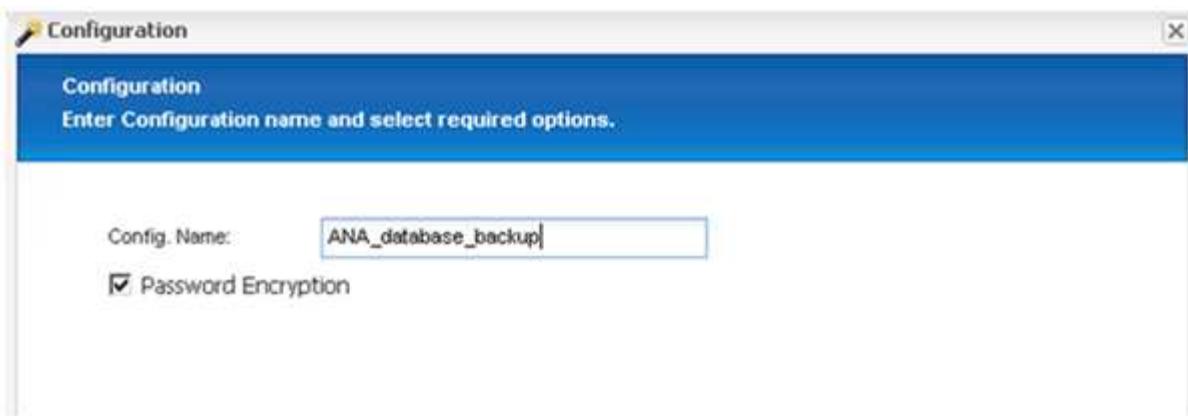


3. Introduzca un nombre de perfil y haga clic en **Aceptar**.

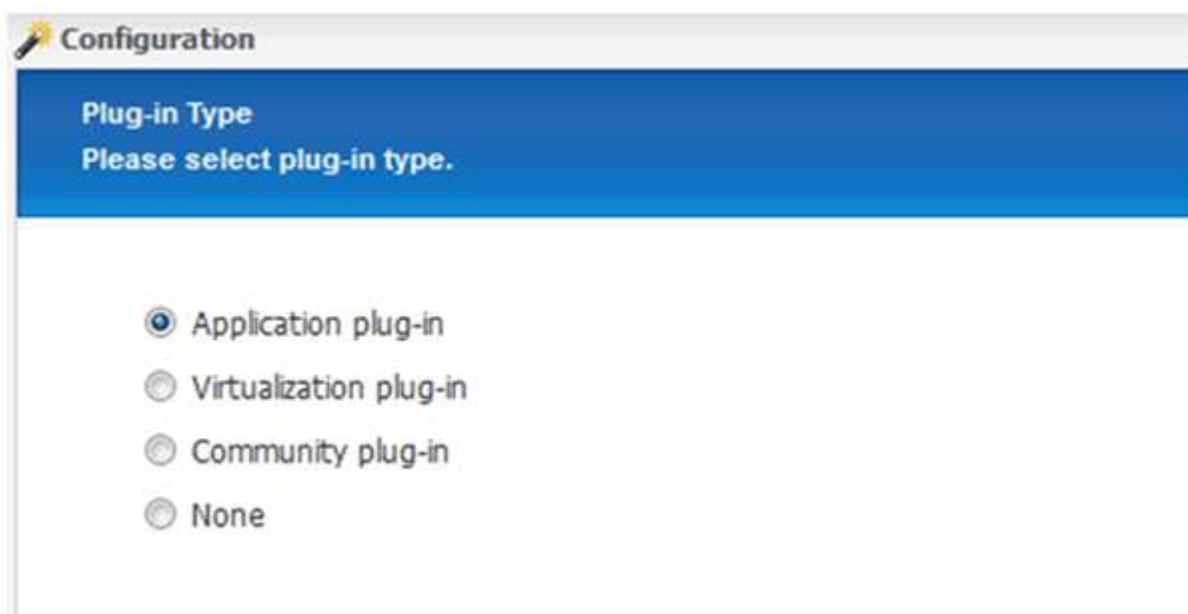


Por ejemplo, "ANAL" es el SID de la base de datos.

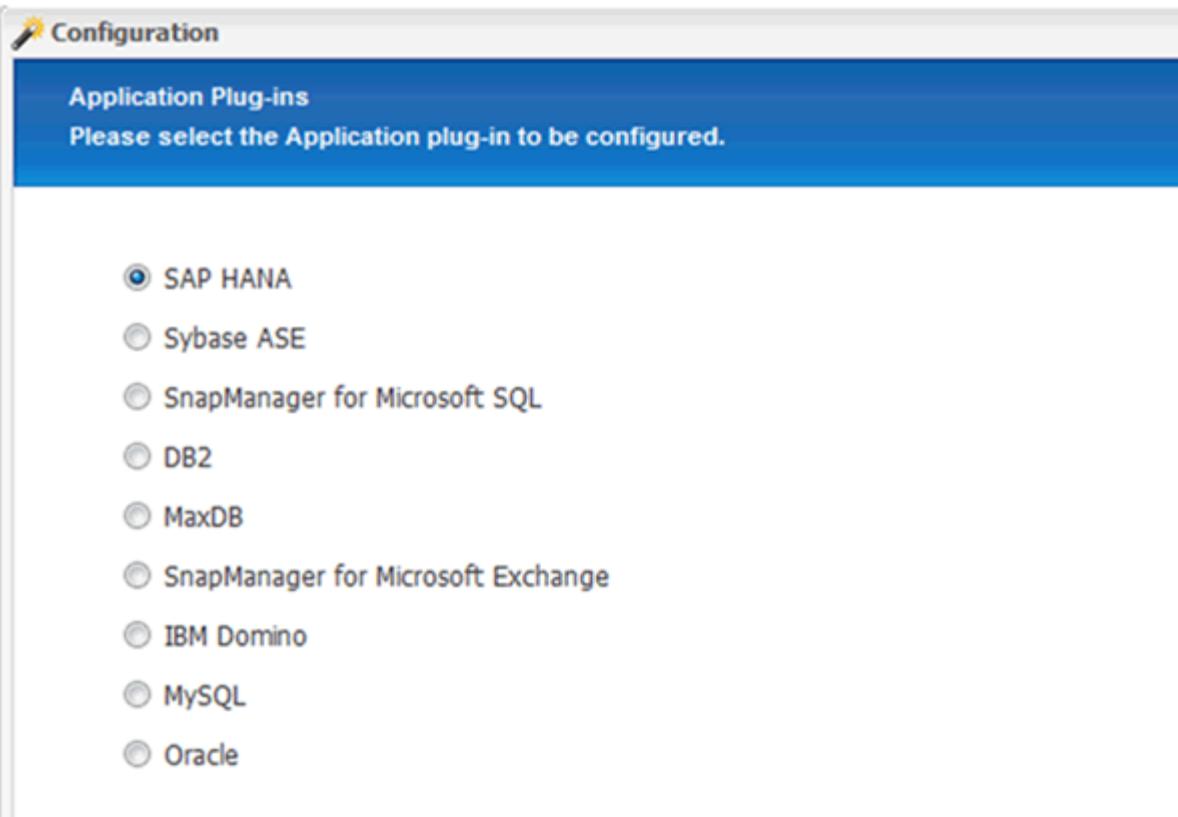
4. Introduzca el nombre de la configuración y haga clic en **Siguiente**.



5. Seleccione **Application Plug-in** como tipo de plug-in y haga clic en **Siguiente**.



6. Seleccione **SAP HANA** como complemento de aplicación y haga clic en **Siguiente**.



7. Introduzca los siguientes detalles de configuración:

- a. Seleccione **Sí** en el menú desplegable para utilizar la configuración con una base de datos multitenant. Para una base de datos de contenedor único, seleccione **no**.
- b. Si contenedor de base de datos multitenant está establecido en **no**, debe proporcionar el SID de la base de datos.
- c. Si contenedor de base de datos multitenant está establecido en **Sí**, debe agregar las claves hdbuserstore para cada nodo SAP HANA.
- d. Agregue el nombre de la base de datos de arrendatarios.
- e. Añada los nodos HANA en los que se debe ejecutar la sentencia hdbsql.
- f. Introduzca el número de instancia del nodo HANA.
- g. Proporcione la ruta al archivo ejecutable hdbsql.
- h. Agregue el usuario OSDB.
- i. Seleccione **Sí** en la lista desplegable para activar el Liberador de espacio DE REGISTRO.

NOTA:

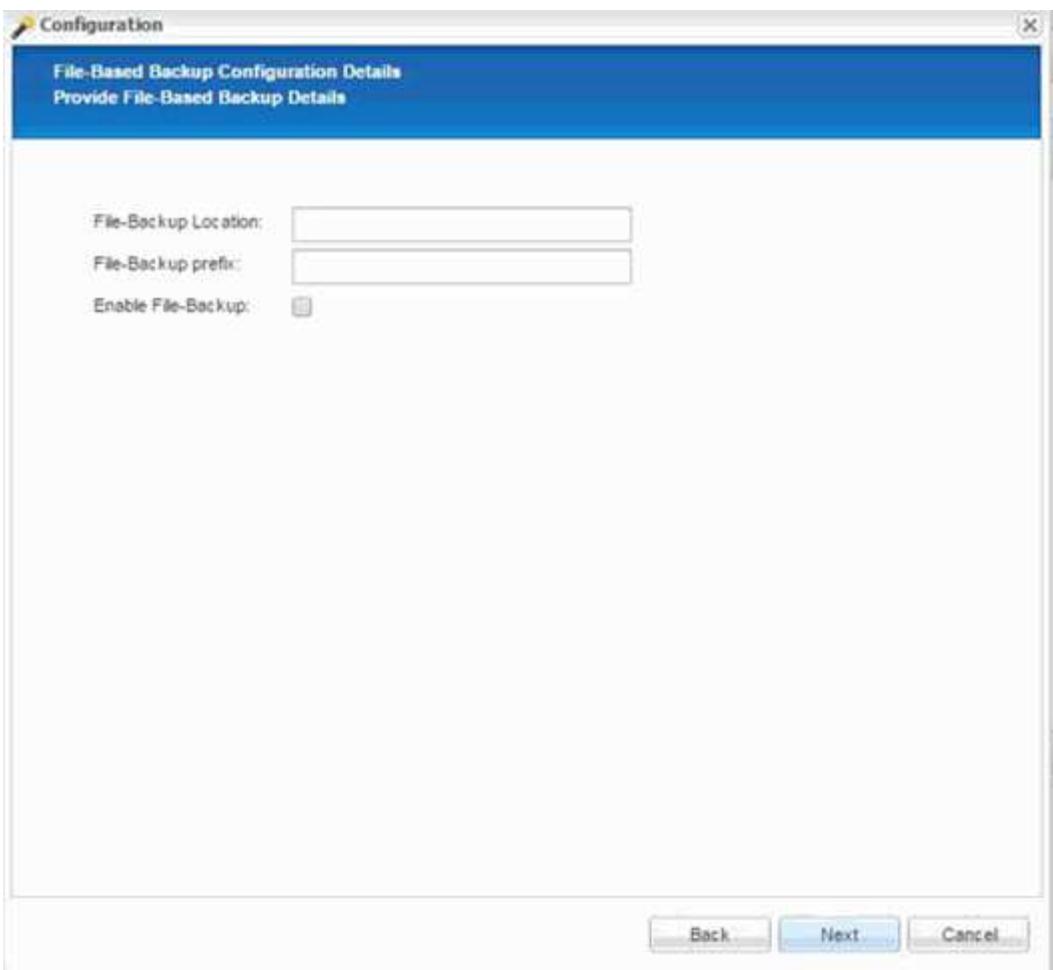
- Parámetro HANA\_SID está disponible solo si el valor para parámetro HANA\_MULTITENANT\_DATABASE se establece en N
- Para contenedores de bases de datos multitenant (MDC) con un tipo de recurso "SingTenant", las copias Snapshot de SAP HANA funcionan con la autenticación basada en UserStore Key. Si la HANA\_MULTITENANT\_DATABASE el parámetro se establece en Y, a continuación, la HANA\_USERSTORE\_KEYS el parámetro debe estar configurado con el valor apropiado.
- Al igual que con los contenedores de bases de datos que no son multi-tenant, se admite la función de backup basado en archivos y comprobación de integridad

j. Haga clic en **Siguiente**.

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

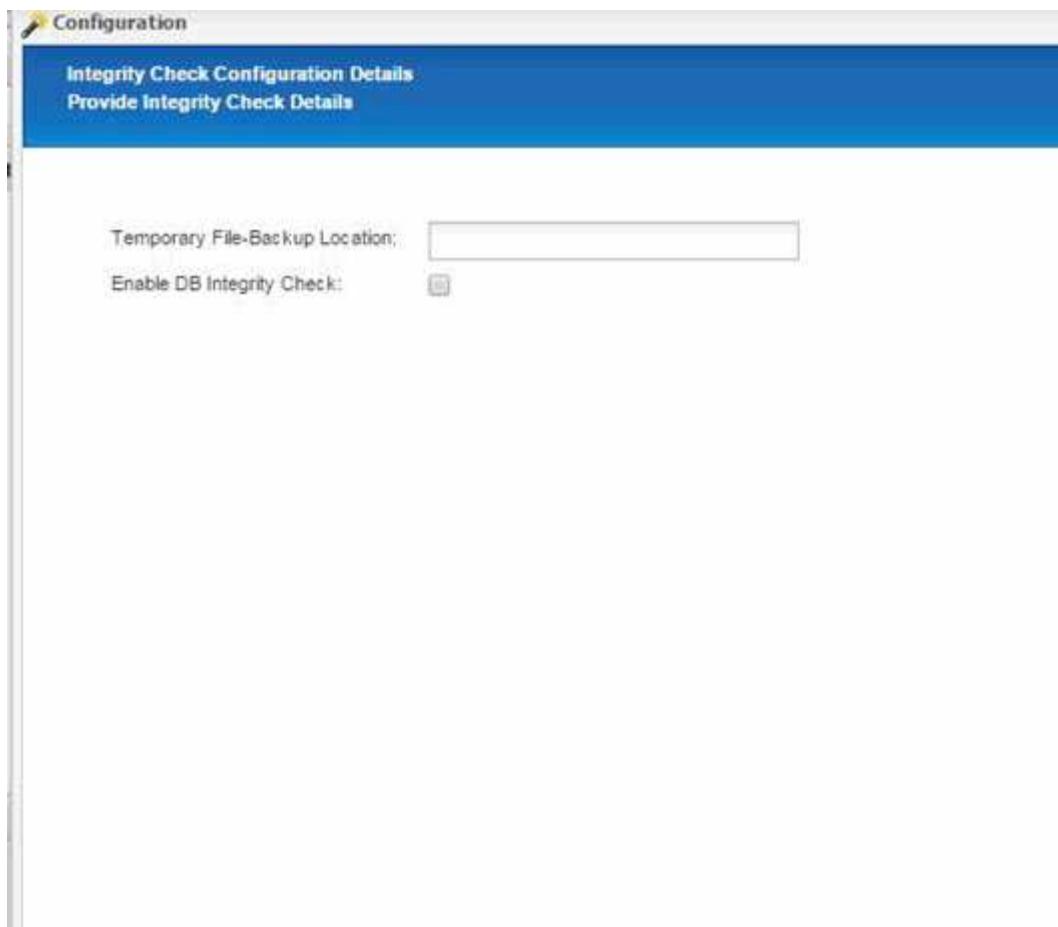
8. Active la operación de backup basado en archivos:

- a. Establezca la ubicación de la copia de seguridad de archivos.
- b. Especifique el prefijo de backup de archivos.
- c. Seleccione la casilla de verificación **Activar copia de seguridad de archivo**.
- d. Haga clic en **Siguiente**.



9. Activar la operación Database Integrity Check:

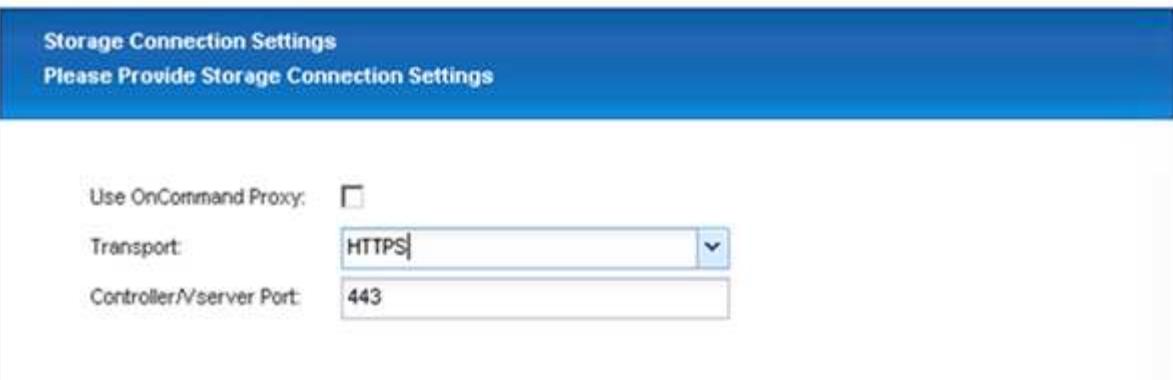
- Establezca la ubicación temporal de copia de seguridad de archivos.
- Seleccione la casilla de verificación **Activar integridad de base de datos**.
- Haga clic en **Siguiente**.



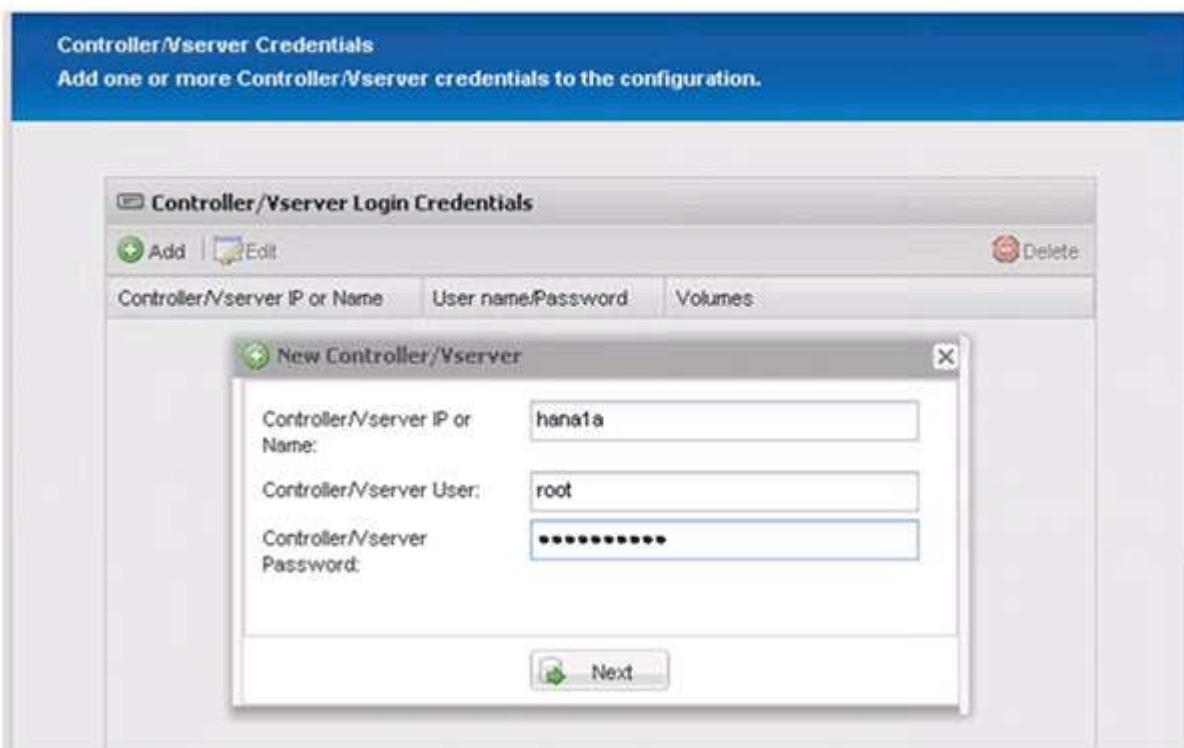
10. Introduzca los detalles del parámetro de configuración del agente y haga clic en **Siguiente**.

The screenshot shows an "Agent Configuration" screen with a blue header bar. The header text is "Agent Configuration" and "Enter agent configuration details". The form contains three fields: "IP/DNS" with the value "localhost", "Port" with the value "9090", and "Timeout (secs)" with the value "300". Below the form is a button labeled "Test agent connection".

11. Introduzca la configuración de la conexión de almacenamiento y haga clic en **Siguiente**.



12. Introduzca las credenciales de inicio de sesión de almacenamiento y haga clic en **Siguiente**.



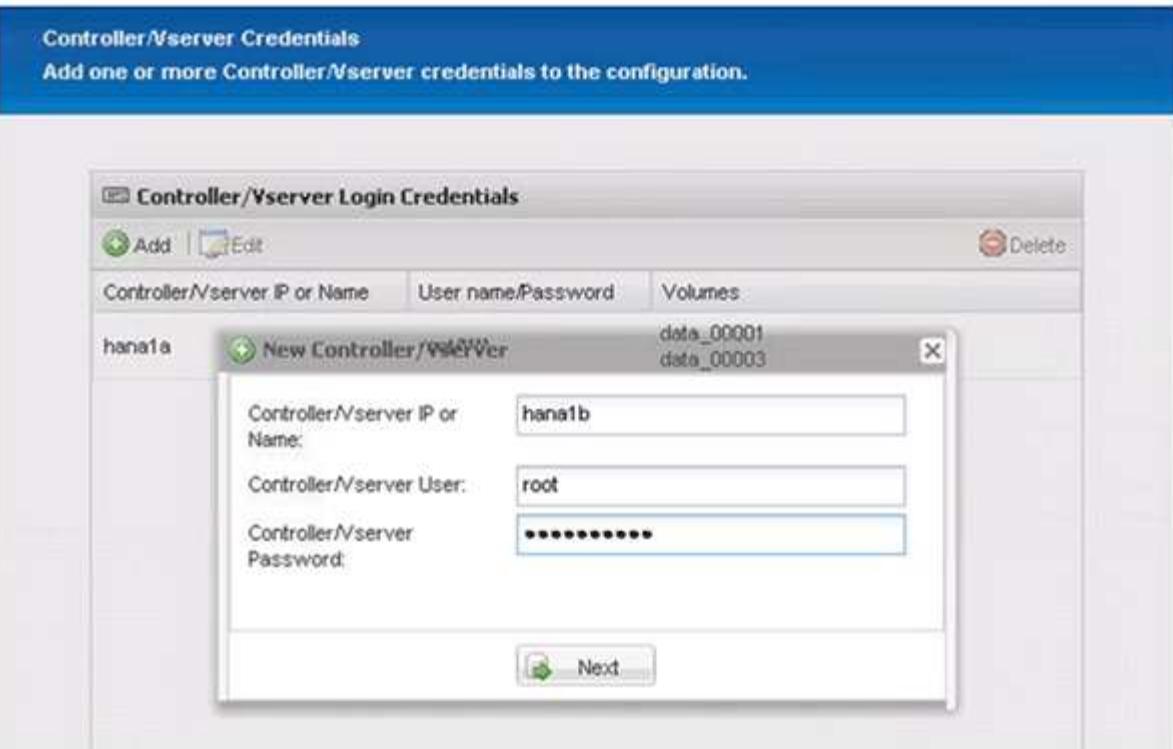
13. Seleccione los volúmenes de datos almacenados en este controlador de almacenamiento y haga clic en **Guardar**.

Controller/Vserver Volumes	
SLES	
SLES4SAP	
SLES4SAP_K3074	
cishanar08_3080	
cishanar08_30807	
cishanar08_PTF	
cishanar08_SLES4SAP	
cishanar09	
cishanar09_3080	
cishanar09_PTF	
cishanar09_SLES4SAP	
cishanar10	
cishanar10_3080	
cishanar10_PTF	
cishanar10_SLES4SAP	
cishanar11	
cishanar11_3080	
cishanar11_PTF	
cishanar11_SLES4SAP	
log_00002	
log_00004	
osmaster	
osmaster_30807	
osmaster_PTF_S745	
osmaster_PTF_S819	
sapcd	
tftpboot	
vol0	
<input type="button" value="Save"/>	

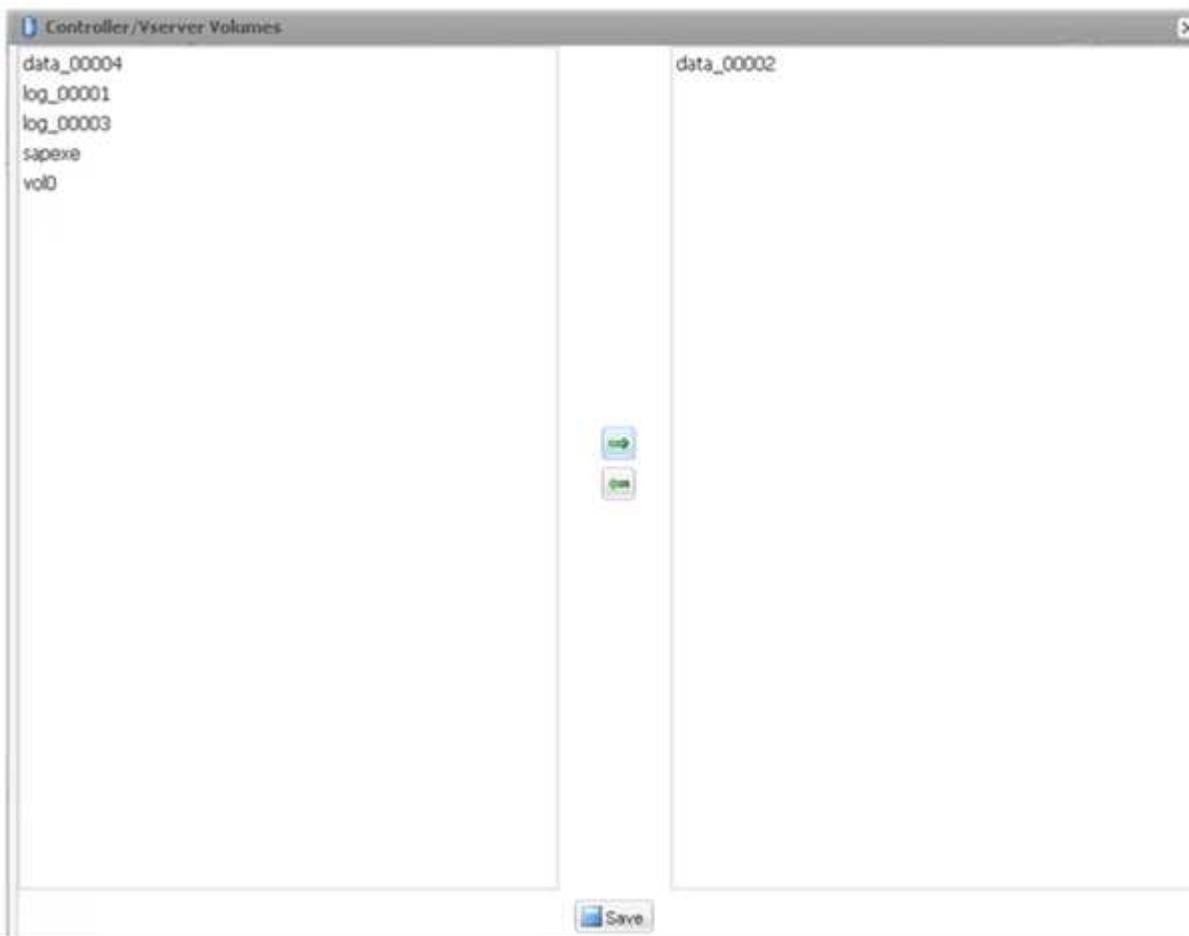
14. Haga clic en **Agregar** para agregar otro controlador de almacenamiento.

Controller/Vserver Credentials		
Add one or more Controller/Vserver credentials to the configuration.		
<input type="checkbox"/> Controller/Vserver Login Credentials		
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
Controller/Vserver IP or Name	User name/Password	Volumes
hanaf1a	root/****	data_00001 data_00003

15. Introduzca las credenciales de inicio de sesión de almacenamiento y haga clic en **Siguiente**.



16. Seleccione los volúmenes de datos almacenados en el segundo controlador de almacenamiento que creó y haga clic en **Guardar**.



17. La ventana Controller/Vserver Credentials muestra las controladoras de almacenamiento y los volúmenes que añadió. Haga clic en **Siguiente**.

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, there is a table titled "Controller/Vserver Login Credentials". The table has three columns: "Controller/Vserver IP or Name", "User name/Password", and "Volumes". There are two rows of data:

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

18. Introduzca la política de Snapshot y la configuración de retención.

La retención de tres copias Snapshot diarias y ocho horas es solo un ejemplo y se puede configurar de manera diferente en función de los requisitos del cliente.



Seleccione **Timestamp** como convención de nomenclatura. El uso de la convención de nomenclatura **Recent** no es compatible con el plugin SAP HANA, ya que la Marca de hora de la copia Snapshot también se usa para las entradas del catálogo de 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. No es necesario realizar cambios. Haga clic en **Siguiente**.

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

Consistency Group:

Consistency Timeout:

SnapDrive Discovery:

Consistency Group WAFL Sync:

Snapshot copy Delete by age only:

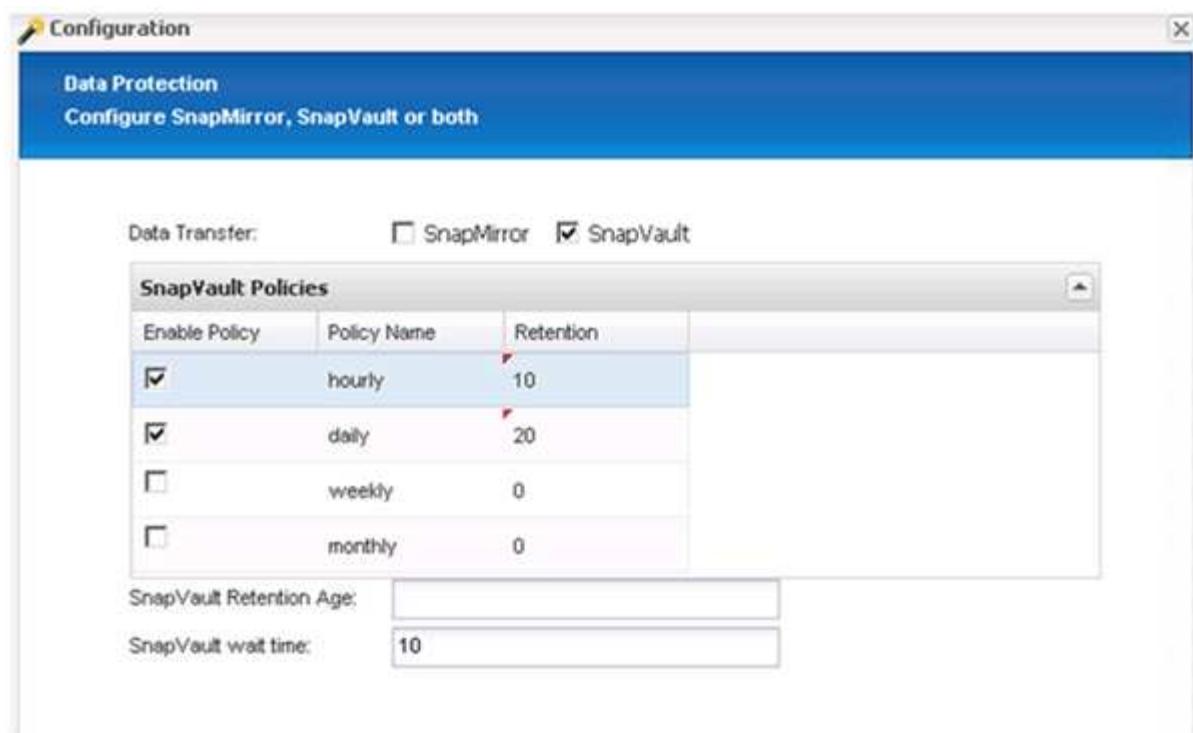
Snapshot copy Dependency Ignore:

Restore Auto Detect:

Ignore Application Errors:

Snapshot Copy Disable:

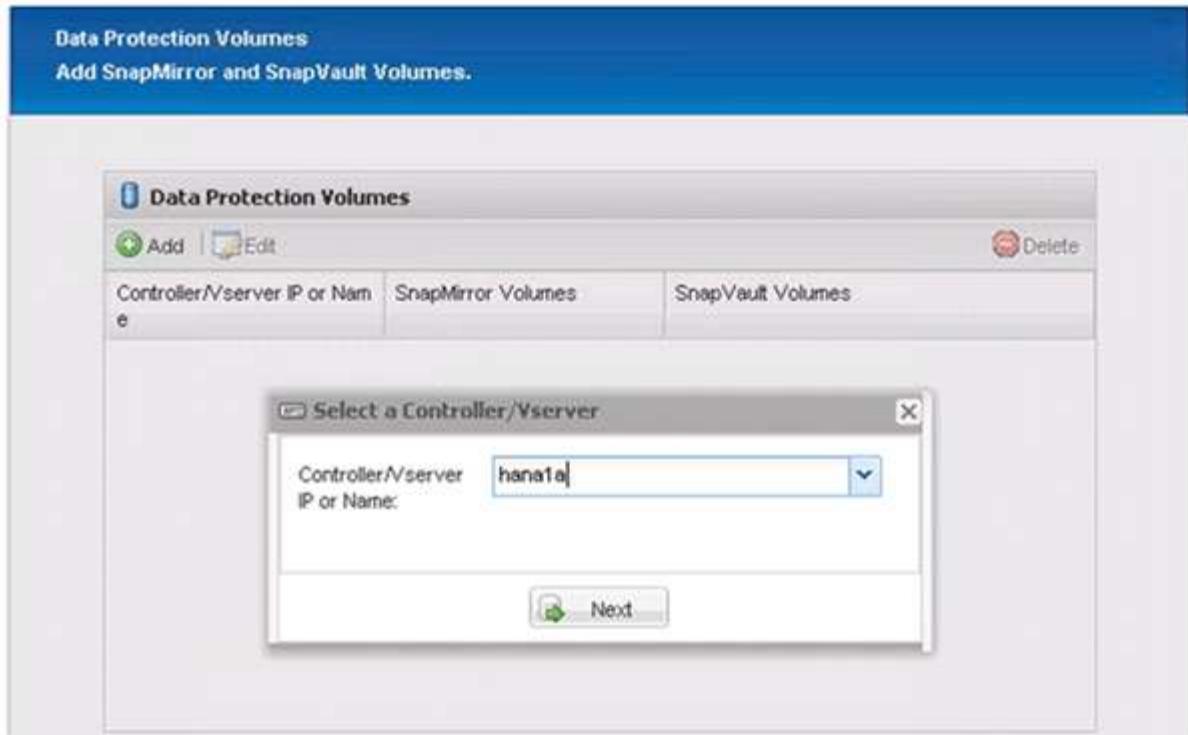
20. Seleccione **SnapVault** y configure las directivas de retención de SnapVault y el tiempo de espera de SnapVault.



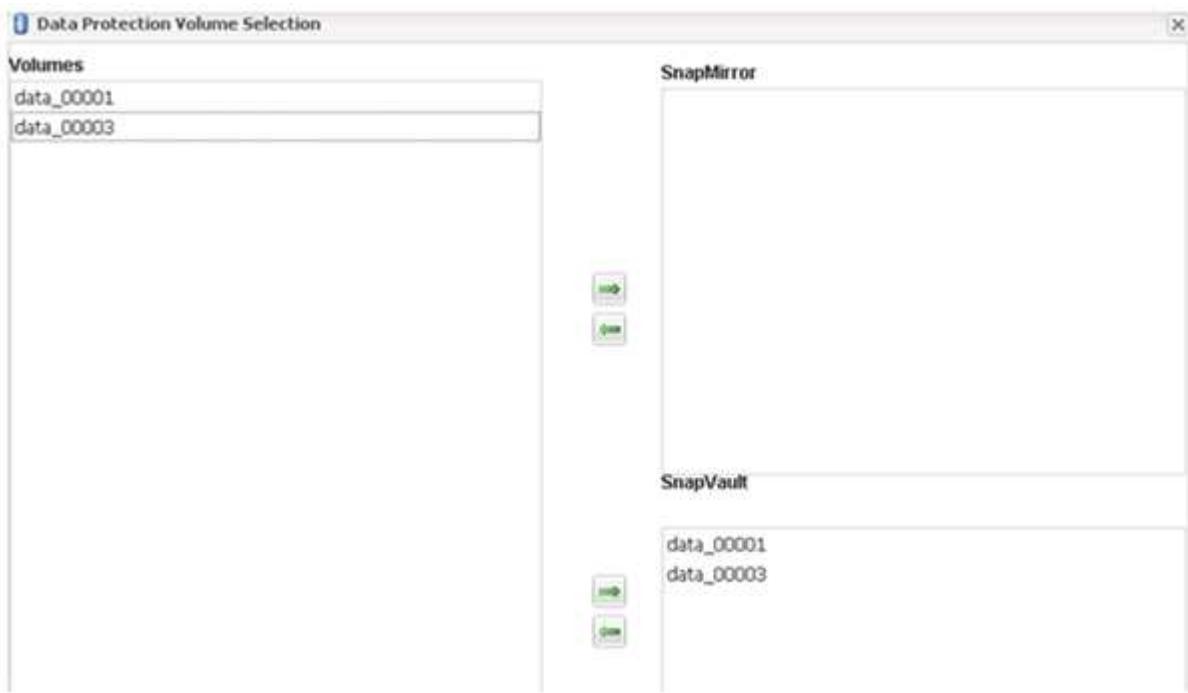
21. Haga clic en **Agregar**.



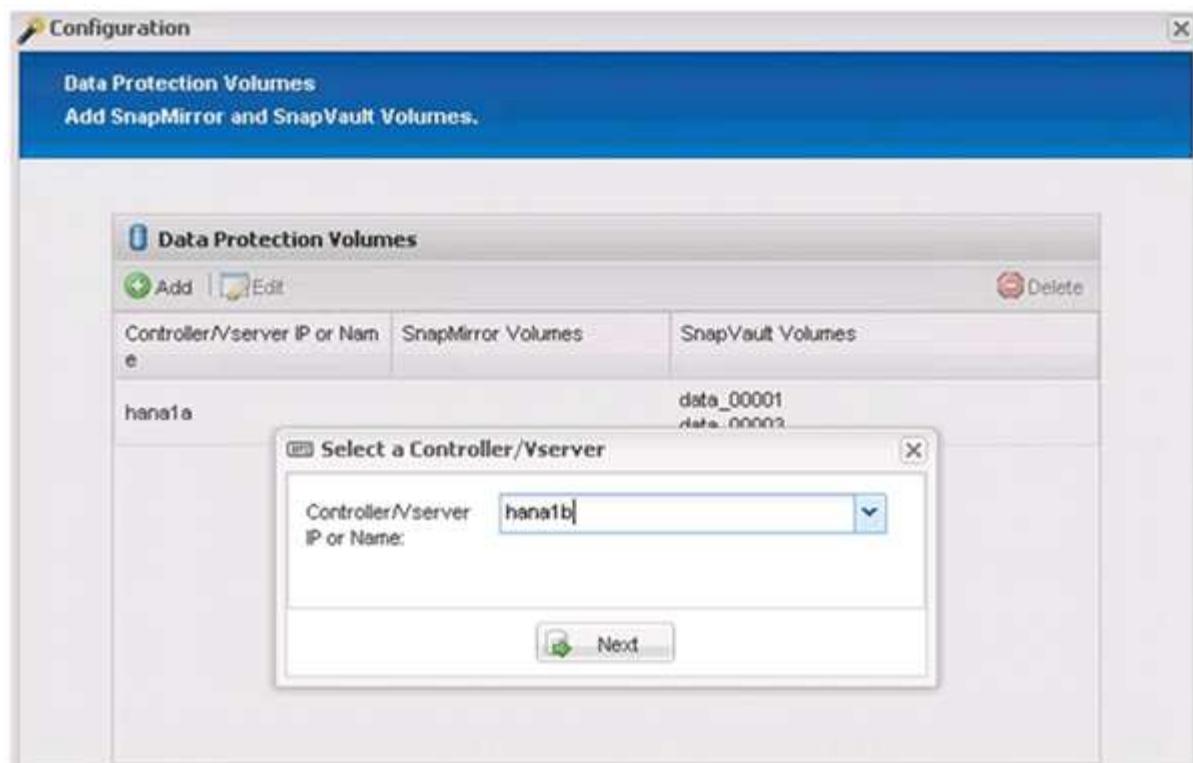
22. Seleccione un controlador de almacenamiento de origen de la lista y haga clic en **Siguiente**.



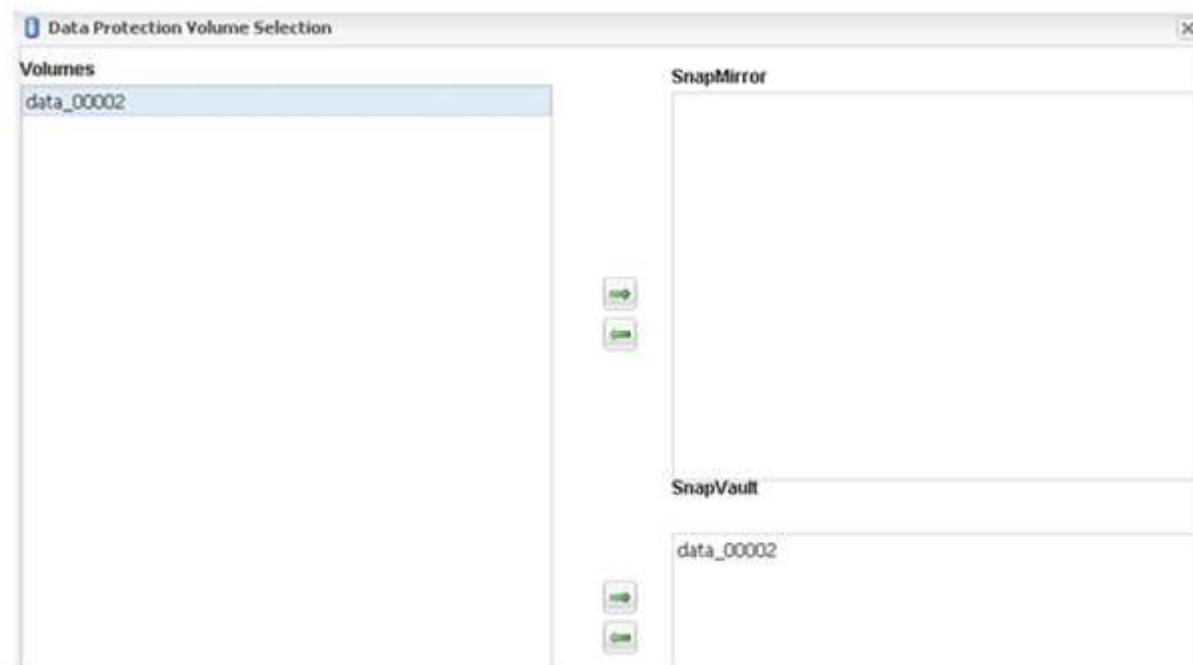
23. Seleccione todos los volúmenes almacenados en el controlador de almacenamiento de origen y haga clic en **Guardar**.



24. Haga clic en **Agregar**, seleccione el segundo controlador de almacenamiento de origen de la lista y, a continuación, haga clic en **Siguiente**.



25. Seleccione todos los volúmenes que se almacenan en el segundo controlador de almacenamiento de origen y haga clic en **Guardar**.



26. La ventana Data Protection Volumes muestra todos los volúmenes que deben protegerse en la configuración que ha creado. Haga clic en **Siguiente**.

**Configuration**

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

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

27. Introduzca las credenciales de los controladores de almacenamiento de destino y haga clic en **Siguiente**. En este ejemplo, se utilizan las credenciales de usuario «'root'» para acceder al sistema de almacenamiento. Normalmente, se configura un usuario de backup dedicado en el sistema de almacenamiento y, a continuación, se utiliza con Snap Creator.

**Configuration**

**Data protection relationships**  
SnapMirror and SnapVault relationships

Verified all SnapMirror relationships.  
Verified all SnapVault relationships.

**hana2b**

Controller/Server User:	<input type="text" value="root"/>
Controller/Server Password:	<input type="password" value="*****"/>

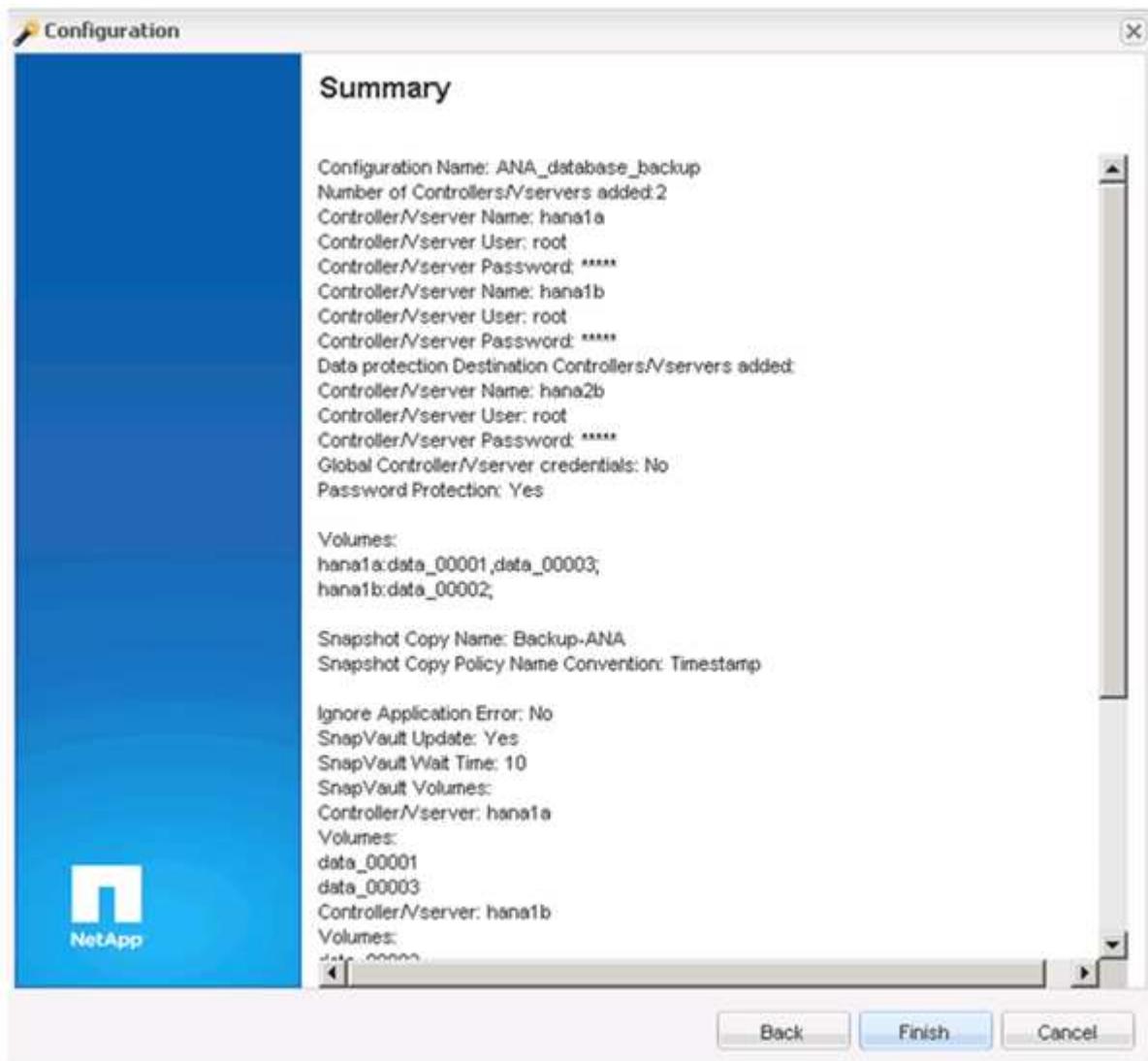
28. Haga clic en **Siguiente**.

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

- Operations Manager console Alert  
 NetApp Management Console data protection capability

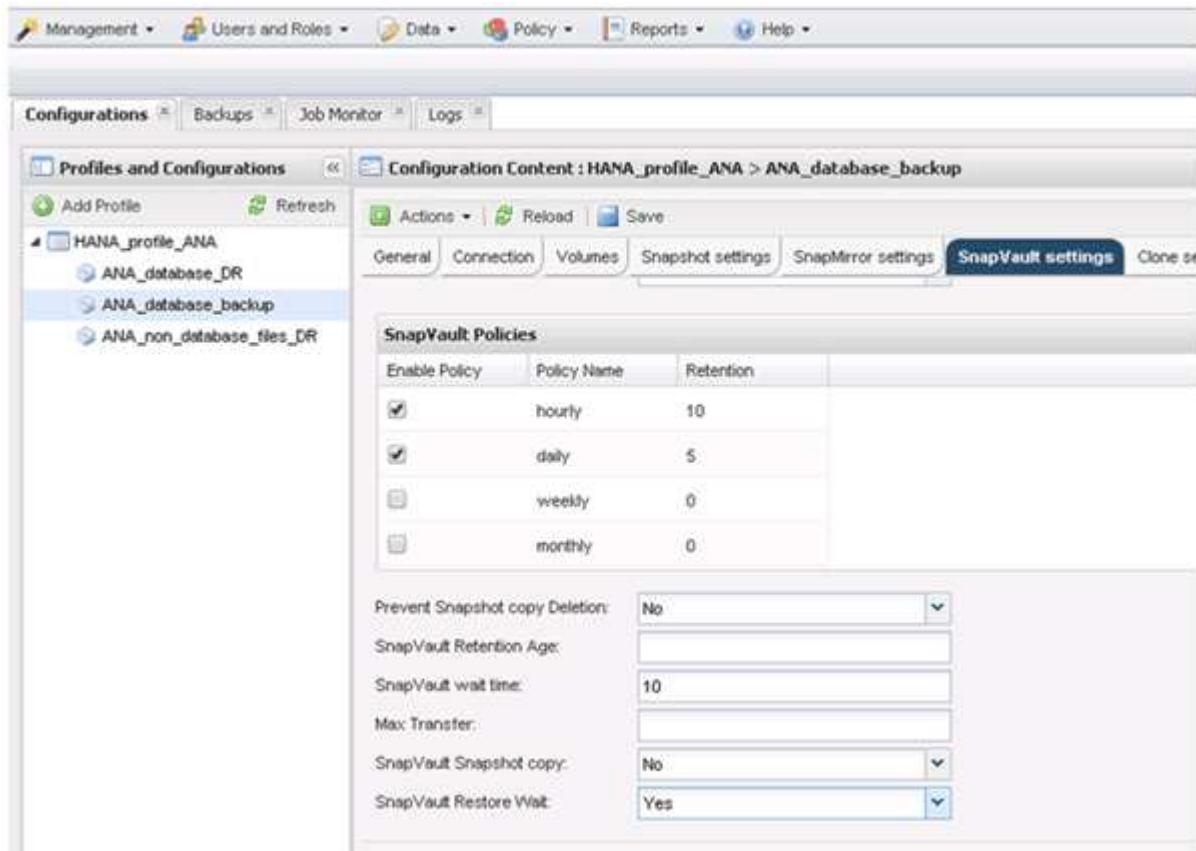
Host:   
User:   
Password:   
Transport:   
Port:

29. Haga clic en **Finalizar** para completar la configuración.



30. Haga clic en la ficha **Configuración de SnapVault**.

31. Seleccione **Sí** en la lista desplegable de la opción **Restaurar espera** de SnapVault y haga clic en **Guardar**.



Es recomendable utilizar una red dedicada para el tráfico de replicación. Si decide hacerlo, debe incluir esta interfaz en el archivo de configuración de Snap Creator como una interfaz secundaria.

También puede configurar interfaces de gestión dedicadas para que Snap Creator pueda acceder al sistema de almacenamiento de origen o de destino mediante una interfaz de red que no está vinculada al nombre de host de la controladora de almacenamiento.

```
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
```

## **Información de copyright**

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

**ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.**

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

**LEYENDA DE DERECHOS LIMITADOS:** el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## **Información de la marca comercial**

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.