



Gestione el modo NDMP de ámbito SVM para volúmenes FlexVol

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from <https://docs.netapp.com/es-es/ontap/tape-backup/manage-svm-scoped-ndmp-mode-concept.html> on February 12, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Gestione el modo NDMP de ámbito SVM para volúmenes FlexVol 1
 - Obtenga información sobre cómo administrar el modo NDMP con ámbito SVM de ONTAP para volúmenes FlexVol 1
 - Comandos para administrar el modo NDMP con ámbito SVM de ONTAP 1
 - Obtenga información sobre la extensión Cluster Aware Backup para ONTAP NDMP 2
 - Disponibilidad de volúmenes ONTAP y dispositivos de cinta para realizar copias de seguridad y restaurar en diferentes tipos de LIF 3
 - La disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup no admite la extensión CAB 3
 - Disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup admite la extensión CAB 4
 - Obtenga información sobre la afinidad de ONTAP NDMP 4
 - Backup NDMP local y backup NDMP triple 4
 - El servidor NDMP admite conexiones de control ONTAP seguras en modo de ámbito SVM 5
 - Tipos de conexión de datos NDMP ONTAP 5
 - Tipo de conexión de datos NDMP cuando la aplicación de backup admite una extensión CAB 5
 - Tipo de conexión de datos NDMP cuando la aplicación de backup no admite la extensión CAB 6
 - Autenticación de usuarios de ONTAP en el modo NDMP con ámbito SVM 6
 - Generar una contraseña específica de NDMP para los usuarios de ONTAP NDMP 7
 - Cómo se ven afectadas las operaciones de copia de seguridad y restauración en cinta durante la recuperación ante desastres en las configuraciones de ONTAP MetroCluster 7

Gestione el modo NDMP de ámbito SVM para volúmenes FlexVol

Obtenga información sobre cómo administrar el modo NDMP con ámbito SVM de ONTAP para volúmenes FlexVol

Puede gestionar NDMP por SVM usando las opciones y los comandos de NDMP. Puede modificar las opciones de NDMP mediante `vserver services ndmp modify` el comando. En el modo NDMP con ámbito SVM, la autenticación del usuario está integrada con el mecanismo de control de acceso basado en roles.

Puede agregar NDMP en la lista de protocolos permitidos o no permitidos mediante `vserver modify` el comando. De forma predeterminada, NDMP se encuentra en la lista de protocolos permitidos. Si se agrega NDMP a la lista de protocolos no permitidos, no se podrán establecer sesiones NDMP.

Puede controlar el tipo de LIF en el que se establece una conexión de datos NDMP mediante `-preferred-interface-role` la opción. Durante una conexión de datos NDMP, NDMP elige una dirección IP que pertenece al tipo de LIF tal como especifica esta opción. Si las direcciones IP no pertenecen a ninguno de estos tipos de LIF, no se puede establecer la conexión de datos NDMP. Obtenga más información sobre `vserver services ndmp modify` en el ["Referencia de comandos del ONTAP"](#).

Comandos para administrar el modo NDMP con ámbito SVM de ONTAP

Puede utilizar `vserver services ndmp` los comandos para gestionar NDMP en cada máquina virtual de almacenamiento (SVM, antes denominada Vserver).

Si desea...	Se usa este comando...
Active el servicio NDMP	<code>vserver services ndmp on</code>  El servicio NDMP siempre debe estar habilitado en todos los nodos de un clúster. Puede habilitar el servicio NDMP en un nodo mediante <code>system services ndmp on</code> el comando. De manera predeterminada, el servicio NDMP siempre está habilitado en un nodo.
Desactive el servicio NDMP	<code>vserver services ndmp off</code>
Mostrar la configuración de NDMP	<code>vserver services ndmp show</code>
Modifique la configuración de NDMP	<code>vserver services ndmp modify</code>
Muestra la versión NDMP predeterminada	<code>vserver services ndmp version</code>

Si desea...	Se usa este comando...
Mostrar todas las sesiones de NDMP	<code>vserver services ndmp status</code>
Mostrar información detallada acerca de todas las sesiones NDMP	<code>vserver services ndmp probe</code>
Terminar una sesión NDMP especificada	<code>vserver services ndmp kill</code>
Finalice todas las sesiones NDMP	<code>vserver services ndmp kill-all</code>
Genere la contraseña NDMP	<code>vserver services ndmp generate-password</code>
Mostrar el estado de la extensión NDMP	<code>vserver services ndmp extensions show</code> Este comando solo está disponible en el nivel de privilegios avanzado.
Modifique el estado de la extensión NDMP (enable o disable)	<code>vserver services ndmp extensions modify</code> Este comando solo está disponible en el nivel de privilegios avanzado.
Inicie el registro para la sesión NDMP especificada	<code>vserver services ndmp log start</code> Este comando solo está disponible en el nivel de privilegios avanzado.
Detenga el registro de la sesión NDMP especificada	<code>vserver services ndmp log stop</code> Este comando solo está disponible en el nivel de privilegios avanzado.

Obtenga más información sobre `vserver services ndmp` en el ["Referencia de comandos del ONTAP"](#).

Información relacionada

[Comandos para gestionar el modo NDMP con ámbito de la SVM](#)

[Qué hace la extensión Cluster Aware Backup](#)

[Qué es el modo NDMP con ámbito SVM](#)

["Administración del sistema"](#)

Obtenga información sobre la extensión Cluster Aware Backup para ONTAP NDMP

CAB (Backup para Cluster Aware) es una extensión del protocolo NDMP v4. Esta

extensión permite que el servidor NDMP establezca una conexión de datos en un nodo propietario de un volumen. Esto también permite a la aplicación de backup determinar si hay volúmenes y dispositivos de cinta ubicados en el mismo nodo de un clúster.

Para permitir que el servidor NDMP identifique el nodo propietario de un volumen y establezca una conexión de datos en dicho nodo, la aplicación de backup debe admitir la extensión CAB. La extensión CAB requiere que la aplicación de copia de seguridad informe al servidor NDMP del volumen que se va a realizar una copia de seguridad o restaurar antes de establecer la conexión de datos. Esto permite que el servidor NDMP determine el nodo que aloja el volumen y establezca la conexión de datos correctamente.

Con la extensión CAB que admite la aplicación de backup, el servidor NDMP proporciona información de afinidad acerca de los volúmenes y los dispositivos de cinta. Con esta información de afinidad, la aplicación de backup puede realizar un backup local en lugar de un backup triple si un volumen y un dispositivo de cinta están ubicados en el mismo nodo de un clúster.

Disponibilidad de volúmenes ONTAP y dispositivos de cinta para realizar copias de seguridad y restaurar en diferentes tipos de LIF

Puede configurar una aplicación de backup para establecer una conexión de control NDMP en cualquiera de los tipos de LIF de un clúster. En el modo NDMP de la máquina virtual de almacenamiento (SVM), puede determinar la disponibilidad de volúmenes y dispositivos de cinta para las operaciones de backup y restauración, en función de estos tipos de LIF y el estado de la extensión CAB.

En las siguientes tablas, se muestra la disponibilidad de volúmenes y dispositivos de cinta para los tipos de LIF de conexión de control NDMP y el estado de la extensión CAB:

La disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup no admite la extensión CAB

Tipo de LIF de conexión de control NDMP	Volúmenes disponibles para backup o restauración	Dispositivos de cinta disponibles para backup o restauración
LIF de gestión de nodos	Todos los volúmenes alojados por un nodo	Los dispositivos de cinta conectados al nodo que aloja el LIF de gestión del nodo
LIF de datos	Solo los volúmenes que pertenecen a la SVM alojada por un nodo que aloja la LIF de datos	Ninguno
LIF de gestión de clústeres	Todos los volúmenes alojados por un nodo que aloja el LIF de gestión de clústeres	Ninguno
LIF de interconexión de clústeres	Todos los volúmenes alojados por un nodo que aloja la LIF de interconexión de clústeres	Los dispositivos de cinta conectados al nodo que aloja la LIF de interconexión de clústeres

Disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup admite la extensión CAB

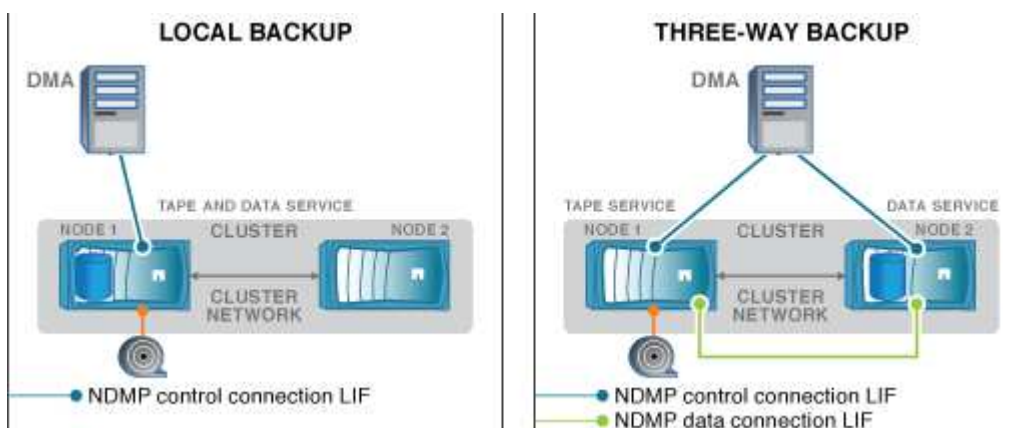
Tipo de LIF de conexión de control NDMP	Volúmenes disponibles para backup o restauración	Dispositivos de cinta disponibles para backup o restauración
LIF de gestión de nodos	Todos los volúmenes alojados por un nodo	Los dispositivos de cinta conectados al nodo que aloja el LIF de gestión del nodo
LIF de datos	Todos los volúmenes que pertenecen a la SVM que aloja la LIF de datos	Ninguno
LIF de gestión de clústeres	Todos los volúmenes del clúster	Todos los dispositivos de cinta del cluster
LIF de interconexión de clústeres	Todos los volúmenes del clúster	Todos los dispositivos de cinta del cluster

Obtenga información sobre la afinidad de ONTAP NDMP

Una vez que la aplicación de backup se detecta EN CABINA, el servidor NDMP proporciona información única sobre la ubicación de los volúmenes y los dispositivos de cinta. Mediante el uso de esta información de afinidad, la aplicación de backup puede realizar un backup local en lugar de un backup triple si un volumen y un dispositivo de cinta comparten la misma afinidad.

Si la conexión de control NDMP se establece en una LIF de gestión de nodos, LIF de gestión de clústeres, O mediante LIF de interconexión de clústeres, la aplicación de backup puede usar la información de afinidad para determinar si un volumen y un dispositivo de cinta están ubicados en el mismo nodo y, a continuación, realizar una operación de backup o restauración local o triple. Si la conexión del control NDMP se establece en una LIF de datos, la aplicación de backup siempre realiza un backup triple.

Backup NDMP local y backup NDMP triple



Mediante la información de afinidad con los volúmenes y los dispositivos de cinta, DMA (aplicación de backup)

realiza un backup NDMP local en el volumen y el dispositivo de cinta ubicados en el nodo 1 del clúster. Si el volumen se mueve del nodo 1 al nodo 2, cambia la información de afinidad sobre el volumen y el dispositivo de cinta. Por lo tanto, para un backup posterior, DMA realiza una operación de backup NDMP triple. De este modo se garantiza la continuidad de la política de backup del volumen independientemente del nodo al que se traslade el volumen.

Información relacionada

[Qué hace la extensión Cluster Aware Backup](#)

El servidor NDMP admite conexiones de control ONTAP seguras en modo de ámbito SVM

Se puede establecer una conexión de control segura entre la aplicación de administración de datos (DMA) y el servidor NDMP utilizando sockets seguros (SSL/TLS) como mecanismo de comunicación. Esta comunicación SSL se basa en los certificados del servidor. El servidor NDMP escucha en el puerto 30000 (asignado por IANA para el servicio "ndmps").

Tras establecer la conexión desde el cliente en este puerto, el protocolo de enlace SSL estándar se produce cuando el servidor presenta el certificado al cliente. Cuando el cliente acepta el certificado, se completa el apretón de manos SSL. Una vez completado este proceso, toda la comunicación entre el cliente y el servidor se cifra. El flujo de trabajo del protocolo NDMP sigue siendo exactamente igual que antes. La conexión NDMP segura sólo requiere autenticación de certificado del servidor. Un DMA puede optar por establecer una conexión mediante la conexión al servicio NDMP seguro o al servicio NDMP estándar.

De manera predeterminada, el servicio NDMP seguro está deshabilitado para una máquina virtual de almacenamiento (SVM). Puede habilitar o deshabilitar el servicio NDMP seguro en una SVM determinada mediante `vserver services ndmp modify -vserver vserver -is-secure-control -connection-enabled [true|false]` el comando.

Tipos de conexión de datos NDMP ONTAP

En el modo NDMP de la máquina virtual de almacenamiento (SVM), los tipos de conexión de datos NDMP admitidos dependen del tipo de LIF de conexión de control NDMP y el estado de la extensión CAB. Este tipo de conexión de datos NDMP indica si se puede ejecutar una operación de backup o restauración NDMP local o triple.

Puede realizar un backup o una operación de restauración NDMP triple a través de una red TCP o TCP/IPv6. En las siguientes tablas, se muestran los tipos de conexión de datos NDMP según el tipo de LIF de conexión de control NDMP y el estado de la extensión CAB.

Tipo de conexión de datos NDMP cuando la aplicación de backup admite una extensión CAB

Tipo de LIF de conexión de control NDMP	Tipo de conexión de datos NDMP
LIF de gestión de nodos	LOCAL, TCP Y TCP/IPV6
LIF de datos	TCP/TCP

Tipo de LIF de conexión de control NDMP	Tipo de conexión de datos NDMP
LIF de gestión de clústeres	LOCAL, TCP Y TCP/IPV6
LIF de interconexión de clústeres	LOCAL, TCP Y TCP/IPV6

Tipo de conexión de datos NDMP cuando la aplicación de backup no admite la extensión CAB

Tipo de LIF de conexión de control NDMP	Tipo de conexión de datos NDMP
LIF de gestión de nodos	LOCAL, TCP Y TCP/IPV6
LIF de datos	TCP/TCP
LIF de gestión de clústeres	TCP/TCP
LIF de interconexión de clústeres	LOCAL, TCP Y TCP/IPV6

Información relacionada

[Qué hace la extensión Cluster Aware Backup](#)

"Gestión de redes"

Autenticación de usuarios de ONTAP en el modo NDMP con ámbito SVM

En el modo NDMP de la máquina virtual de almacenamiento (SVM), la autenticación de usuario NDMP está integrada con el control de acceso basado en roles. En el contexto de la SVM, el usuario NDMP debe tener el rol `"vsadmin"` o `"vsadmin-backup"`. En un contexto de cluster, el usuario NDMP debe tener el rol `«'admin'»` o `«'backup'»`.

Además de estas funciones predefinidas, una cuenta de usuario asociada a una función personalizada también puede utilizarse para la autenticación NDMP siempre y cuando la función personalizada tenga la carpeta `«'vserver Services ndmp'»` en su directorio de comandos y el nivel de acceso de la carpeta no sea `«'none'»`. En este modo, debe generar una contraseña NDMP para una cuenta de usuario determinada, que se crea mediante el control de acceso basado en roles. Los usuarios de clúster con un rol de administrador o backup pueden acceder a una LIF de gestión de nodos, una LIF de gestión de clústeres o una LIF de interconexión de clústeres. Los usuarios de un rol de vsadmin o de vsadmin pueden acceder solo a la LIF de datos para esa SVM. Por lo tanto, según la función de un usuario, la disponibilidad de volúmenes y dispositivos de cinta para las operaciones de backup y restauración varía.

Este modo también admite la autenticación de usuario para usuarios NIS y LDAP. Por lo tanto, los usuarios NIS y LDAP pueden acceder a varias SVM con un ID de usuario y una contraseña comunes. Sin embargo, la autenticación NDMP no admite usuarios de Active Directory.

En este modo, una cuenta de usuario debe estar asociada a la aplicación SSH y al método de autenticación `«'Contraseña de usuario'»`.

Generar una contraseña específica de NDMP para los usuarios de ONTAP NDMP

En el modo NDMP de la máquina virtual de almacenamiento (SVM), debe generar una contraseña para un ID de usuario específico. La contraseña generada se basa en la contraseña de inicio de sesión real para el usuario NDMP. Si cambia la contraseña de inicio de sesión real, deberá generar de nuevo la contraseña específica de NDMP.

Pasos

1. Utilice `vserver services ndmp generate-password` el comando para generar una contraseña específica de NDMP.

Puede utilizar esta contraseña en cualquier operación NDMP actual o futura que requiera la introducción de la contraseña.



Desde el contexto de la máquina virtual de almacenamiento (SVM, antes denominada Vserver), puede generar contraseñas de NDMP para usuarios que solo pertenecen a esa SVM.

El ejemplo siguiente muestra cómo generar una contraseña específica de NDMP para un ID de usuario usuario1:

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. Si cambia la contraseña a su cuenta de sistema de almacenamiento normal, repita este procedimiento para obtener su nueva contraseña específica de NDMP.

Cómo se ven afectadas las operaciones de copia de seguridad y restauración en cinta durante la recuperación ante desastres en las configuraciones de ONTAP MetroCluster

Se pueden ejecutar operaciones de backup y restauración a cinta simultáneamente durante la recuperación ante desastres en una configuración de MetroCluster. Debe entender cómo se ven afectadas estas operaciones durante la recuperación de desastres.

Si las operaciones de backup y restauración de cinta se llevan a cabo en un volumen de anSVM en una relación de recuperación ante desastres, puede continuar con las operaciones de backup y restauración de cinta incrementales después de una conmutación de sitios y conmutación de estado.

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.