



Cifre datos de volúmenes con NVE

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

- Cifre datos de volúmenes con NVE 1
 - Cifre datos de volúmenes con la información general de NVE 1
 - Habilite el cifrado a nivel de agregado con la licencia ve. 1
 - Habilite el cifrado en un nuevo volumen 3
 - Habilite el cifrado en un volumen existente 4
 - Configure el cifrado de volúmenes NetApp en un volumen raíz de SVM 8
 - Habilite el cifrado de volumen raíz del nodo 9

Cifre datos de volúmenes con NVE

Cifre datos de volúmenes con la información general de NVE

A partir de ONTAP 9.7, el cifrado de volúmenes y agregados se habilita de forma predeterminada cuando se dispone de la licencia ve y la gestión de claves interna o externa. Para ONTAP 9.6 y versiones anteriores, es posible habilitar el cifrado en un volumen nuevo o en uno existente. Debe haber instalado la licencia ve y haber habilitado la gestión de claves para poder habilitar el cifrado de volúmenes. NVE es conforme a la normativa FIPS-140-2 de nivel 1.

Habilite el cifrado a nivel de agregado con la licencia ve

A partir de ONTAP 9.7, los agregados y volúmenes recién creados se cifran de forma predeterminada cuando tenga el "[LICENCIA VE](#)" o la gestión de claves externas o incorporadas. A partir de ONTAP 9.6, puede utilizar el cifrado a nivel de agregado para asignar claves al agregado que contiene para los volúmenes que se van a cifrar.

Acerca de esta tarea

Debe utilizar el cifrado a nivel de agregado si tiene pensado realizar deduplicación en línea o en segundo plano a nivel de agregado. De lo contrario, NVE no admite la deduplicación a nivel de agregado.

Un agregado habilitado para el cifrado a nivel de agregado se denomina agregado NAE (para el cifrado de agregados de NetApp). Todos los volúmenes de un agregado de NAE deben estar cifrados con NAE o NVE. Con el cifrado a nivel de agregado, los volúmenes que cree en el agregado se cifran de forma predeterminada con el cifrado NAE. Puede anular el valor predeterminado para utilizar el cifrado NVE en su lugar.

No se admiten volúmenes de texto sin formato en los agregados de la NAE.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Pasos

1. Habilite o deshabilite el cifrado de nivel de agregado:

Para...	Se usa este comando...
Cree un agregado de NAE con ONTAP 9.7 o posterior	<pre>storage aggregate create -aggregate aggregate_name -node node_name</pre>
Cree un agregado de NAE con ONTAP 9.6	<pre>storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</pre>

Convertir un agregado que no sea NAE en un agregado de NAE	<code>storage aggregate modify -aggregate <i>aggregate_name</i> -node <i>node_name</i> -encrypt-with -aggr-key true</code>
Convertir un agregado de NAE en un agregado que no sea NAE	<code>storage aggregate modify -aggregate <i>aggregate_name</i> -node <i>node_name</i> -encrypt-with -aggr-key false</code>

Para obtener una sintaxis de comando completa, consulte las páginas man.

El siguiente comando habilita el cifrado a nivel de agregado para `aggr1`:

- ONTAP 9.7 o posterior:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 o anterior:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. Compruebe que el agregado está habilitado para el cifrado:

```
storage aggregate show -fields encrypt-with-aggr-key
```

Para obtener una sintaxis de comando completa, consulte la página man.

El siguiente comando lo verifica `aggr1` está habilitado para el cifrado:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate          encrypt-aggr-key
-----
aggr0_vsim4        false
aggr1               true
2 entries were displayed.
```

Después de terminar

Ejecute el `volume create` comando para crear los volúmenes cifrados.

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor al cifrar un volumen.

Habilite el cifrado en un nuevo volumen

Puede utilizar el `volume create` comando para habilitar el cifrado en un volumen nuevo.

Acerca de esta tarea

Puede cifrar volúmenes con el cifrado de volúmenes de NetApp (NVE) y, para comenzar con ONTAP 9.6, el cifrado de agregados de NetApp (NAE). Para obtener más información sobre NAE y NVE, consulte [información general de cifrado de volúmenes](#).

El procedimiento para habilitar el cifrado en un nuevo volumen en ONTAP varía en función de la versión de ONTAP que esté usando y su configuración específica:


- A partir de ONTAP 9.4, si se habilita `cc-mode` Cuando se configura el gestor de claves incorporado, los volúmenes que se crean con el `volume create` el comando se cifra automáticamente, tanto si se especifica como si no `-encrypt true`.
- En ONTAP 9.6 y versiones anteriores, es necesario utilizar `-encrypt true` con `volume create` comandos para habilitar el cifrado (siempre que no se haya habilitar `cc-mode`).
- Si desea crear un volumen NAE en ONTAP 9.6, debe habilitar NAE en el nivel de agregado. Consulte [Habilite el cifrado a nivel de agregado con la licencia ve](#) para obtener más detalles sobre esta tarea.
- A partir de ONTAP 9.7, los volúmenes recién creados se cifran de forma predeterminada cuando el "LICENCIA VE" o la gestión de claves externas o incorporadas. De forma predeterminada, los nuevos volúmenes que se crean en un agregado de NAE serán del tipo NAE en lugar de NVE.
 - Si añade, en ONTAP 9.7 y versiones posteriores `-encrypt true` para la `volume create` Comando para crear un volumen en un agregado de NAE, el volumen tendrá el cifrado NVE en lugar de NAE. Todos los volúmenes de un agregado de NAE deben estar cifrados con NVE o NAE.



No se admiten los volúmenes de texto sin formato en los agregados de NAE.

Pasos

1. Cree un volumen nuevo y especifique si el cifrado está habilitado en el volumen. Si el nuevo volumen se encuentra en un agregado de NAE, de forma predeterminada el volumen será un volumen de NAE:

Para crear...	Se usa este comando...
Un volumen NAE	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</pre>
Un volumen de NVE	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true</pre> <div><p>En ONTAP 9.6 y versiones anteriores en las que NAE no es compatible, <code>-encrypt true</code> Especifica que el volumen se debe cifrar con NVE. En ONTAP 9.7 y posteriores, donde se crean volúmenes en agregados de NAE, <code>-encrypt true</code> Reemplaza el tipo de cifrado predeterminado de NAE para crear un volumen NVE en su lugar.</p></div>

Un volumen de texto sin formato	<code>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false</code>
---------------------------------	---

Para obtener la sintaxis completa del comando, consulte la página de referencia de comandos de LINK:[https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html\[volume create#\]](https://docs.netapp.com/us-en/ontap-cli-9141/volume-create.html[volume create#]).

2. Compruebe que los volúmenes estén habilitados para el cifrado:

```
volume show -is-encrypted true
```

Para obtener una sintaxis completa del comando, consulte "[referencia de comandos](#)".

Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP "inserta automáticamente" una clave de cifrado en el servidor cuando se cifra un volumen.

= :allow-uri-read:

Habilite el cifrado en un volumen existente

Puede utilizar cualquiera de los dos `volume move start` o `la volume encryption conversion start` comando para habilitar el cifrado en un volumen existente.

Acerca de esta tarea

- A partir de ONTAP 9.3, puede utilizar la `volume encryption conversion start` comando para habilitar el cifrado de un volumen existente «in situ», sin necesidad de mover el volumen a otra ubicación. Como alternativa, puede utilizar el `volume move start` comando.
- Para ONTAP 9.2 y versiones anteriores, solo puede utilizar el `volume move start` comando para habilitar el cifrado mediante el movimiento de un volumen existente.

Habilite el cifrado en un volumen existente con el comando `volume Encryption conversion start`

A partir de ONTAP 9.3, puede utilizar la `volume encryption conversion start` comando para habilitar el cifrado de un volumen existente «in situ», sin necesidad de mover el volumen a otra ubicación.

Después de iniciar una operación de conversión, debe completarse. Si se encuentra con un problema de rendimiento durante la operación, puede ejecutar el `volume encryption conversion pause` para pausar la operación y el `volume encryption conversion resume` comando para reanudar la operación.



No puede utilizar `volume encryption conversion start` Para convertir un volumen de SnapLock.

Pasos

1. Habilitar el cifrado en un volumen existente:

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando habilita el cifrado en el volumen existente `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

El sistema crea una clave de cifrado para el volumen. Los datos del volumen se cifran.

2. Compruebe el estado de la operación de conversión:

```
volume encryption conversion show
```

Para obtener información sobre la sintaxis de toda el comando, consulte la página `man` del comando.

El siguiente comando muestra el estado de la operación de conversión:

```
cluster1::> volume encryption conversion show
```

Vserver	Volume	Start Time	Status
-----	-----	-----	-----
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. Cuando finalice la operación de conversión, compruebe que el volumen esté habilitado para el cifrado:

```
volume show -is-encrypted true
```

Para obtener información sobre la sintaxis de toda el comando, consulte la página `man` del comando.

El siguiente comando muestra los volúmenes cifrados en `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor al cifrar un volumen.

Habilite el cifrado en un volumen existente con el comando `volume Move start`

Puede utilizar el `volume move start` comando para habilitar el cifrado mediante el movimiento de un volumen existente. Debe usar `volume move start` En ONTAP 9.2 y anteriores. Se puede usar el mismo agregado o uno diferente.

Acerca de esta tarea

- A partir de ONTAP 9.8, se puede utilizar `volume move start` Para habilitar el cifrado en un volumen de

SnapLock o FlexGroup.

- A partir de ONTAP 9.4, si activa "cc-mode" cuando configura el Administrador de claves incorporado, los volúmenes que crea con el `volume move start` el comando se cifra automáticamente. No es necesario que especifique `-encrypt-destination true`.
- A partir de ONTAP 9.6, puede utilizar el cifrado a nivel de agregado con el fin de asignar claves al agregado que contiene para mover los volúmenes. Un volumen cifrado con una clave única se denomina *NVE volume* (lo que significa que utiliza cifrado de volúmenes de NetApp). Un volumen cifrado con una clave de nivel de agregado se denomina *NAE volume* (para el cifrado de agregados de NetApp). No se admiten los volúmenes de texto sin formato en los agregados de NAE.
- A partir de ONTAP 9.14.1, se puede cifrar un volumen raíz de SVM con NVE. Para obtener más información, consulte [Configure el cifrado de volúmenes NetApp en un volumen raíz de SVM](#).

Antes de empezar

Debe ser un administrador de clústeres para realizar esta tarea o un administrador de SVM a quien el administrador de clúster haya delegado esta autoridad.

"Delegar la autoridad para ejecutar el comando `volume move`"

Pasos

1. Mueva un volumen existente y especifique si el cifrado está habilitado en el volumen:

Para convertir...	Se usa este comando...
Un volumen de texto sin formato a un volumen NVE	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true</code>
Un volumen NVE o un volumen sin texto en un volumen NAE (suponiendo que se habilite el cifrado a nivel de agregado en el destino)	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true</code>
Un volumen NAE a un volumen NVE	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false</code>
Volumen NAE a un volumen de texto sin formato	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false</code>
Un volumen NVE a un volumen de texto sin texto	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false</code>

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando convierte un volumen de texto sin formato denominado `vol1` Para un volumen NVE:


```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr2 -encrypt-destination true
```

Si asumimos que el cifrado a nivel de agregado está habilitado en el destino, el siguiente comando convierte un volumen NVE o de texto sin formato denominado `vol1` A un volumen de NAE:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr2 -encrypt-with-aggr-key true
```

El siguiente comando convierte un volumen NAE llamado `vol2` Para un volumen NVE:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-with-aggr-key false
```

El siguiente comando convierte un volumen NAE llamado `vol2` a un volumen de texto sin formato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

El siguiente comando convierte un volumen de NVE llamado `vol2` a un volumen de texto sin formato:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-destination false
```

2. Vea el tipo de cifrado de volúmenes de clúster:

```
volume show -fields encryption-type none|volume|aggregate
```

La `encryption-type` Campo está disponible en ONTAP 9.6 y versiones posteriores.

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando muestra el tipo de cifrado de volúmenes en `cluster2`:

```
cluster2::> volume show -fields encryption-type  
  
vserver  volume  encryption-type  
-----  -  
vs1      vol1     none  
vs2      vol2     volume  
vs3      vol3     aggregate
```

3. Compruebe que los volúmenes estén habilitados para el cifrado:

```
volume show -is-encrypted true
```

Para obtener información sobre la sintaxis de toda el comando, consulte la página man del comando.

El siguiente comando muestra los volúmenes cifrados en `cluster2`:

```
cluster2::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

Resultado

Si utiliza un servidor KMIP para almacenar las claves de cifrado de un nodo, ONTAP inserta automáticamente una clave de cifrado en el servidor cuando se cifra un volumen.

Configure el cifrado de volúmenes NetApp en un volumen raíz de SVM

A partir de ONTAP 9.14.1, puede habilitar el cifrado de volúmenes de NetApp (NVE) en un volumen raíz de una máquina virtual de almacenamiento (SVM). Con NVE, el volumen raíz se cifra con una clave única, lo que permite una mayor seguridad en la SVM.

Acerca de esta tarea

NVE en un volumen raíz de SVM solo se puede habilitar una vez que se creó la SVM.

Antes de empezar

- El volumen raíz de SVM no debe estar en un agregado cifrado con el cifrado de agregados de NetApp (NAE).
- Debe haber habilitado el cifrado con el administrador de claves incorporado o un gestor de claves externo.
- Debe ejecutar ONTAP 9.14.1 o una versión posterior.
- Para migrar una SVM que contiene un volumen raíz cifrado con NVE, debe convertir el volumen raíz de la SVM en un volumen de texto sin formato una vez finalizada la migración y, luego, volver a cifrar el volumen raíz de la SVM.
 - Si el agregado de destino de la migración de SVM utiliza NAE, el volumen raíz hereda NAE de manera predeterminada.
- Si la SVM está en una relación de recuperación ante desastres de SVM:
 - La configuración de cifrado en una SVM reflejada no se copia en el destino. Si habilita NVE en el origen o destino, debe habilitar por separado NVE en el volumen raíz de la SVM reflejada.
 - Si todos los agregados del clúster de destino utilizan NAE, el volumen raíz de SVM utilizará NAE.

Pasos

Puede habilitar NVE en un volumen raíz de SVM con la interfaz de línea de comandos de ONTAP o System Manager.

CLI

Puede habilitar NVE en el volumen raíz de la SVM sin movimiento o mediante el movimiento del volumen entre agregados.

Cifre el volumen raíz en su lugar

1. Convierta el volumen raíz en un volumen de cifrado:

```
volume encryption conversion start -vserver svm_name -volume volume
```

2. Confirme que el cifrado se ha realizado correctamente. La `volume show -encryption-type volume` Muestra una lista de todos los volúmenes con NVE.

Cifre el volumen raíz de la SVM al moverlo


1. Inicie un movimiento de volumen:

```
volume move start -vserver svm_name -volume volume -destination-aggregate aggregate -encrypt-with-aggr-key false -encrypt-destination true
```

Para obtener más información acerca de `volume move`, consulte [Mover un volumen](#).

2. Confirme el `volume move` la operación se ha realizado correctamente con el `volume move show` comando. La `volume show -encryption-type volume` Muestra una lista de todos los volúmenes con NVE.

System Manager

1. Navegue hasta **Almacenamiento > Volúmenes**.
2. Junto al nombre del volumen raíz de la SVM que desea cifrar, seleccione  Luego **Editar**.
3. En el encabezado **Almacenamiento y optimización**, seleccione **Activar cifrado**.
4. Seleccione **Guardar**.

Habilite el cifrado de volumen raíz del nodo

A partir de ONTAP 9.8, puede usar el cifrado de volúmenes de NetApp para proteger el volumen raíz del nodo.



Acerca de esta tarea

Este procedimiento se aplica al volumen raíz del nodo. No se aplica a los volúmenes raíz de SVM. Los volúmenes raíz de SVM se pueden proteger mediante cifrado a nivel de agregado y [A partir de ONTAP 9.14.1, NVE](#).

Una vez que se inicia el cifrado del volumen raíz, se debe completar. No puede pausar la operación. Una vez completado el cifrado, no puede asignar una nueva clave al volumen raíz y no puede ejecutar una operación de purga segura.

Antes de empezar

- Su sistema debe utilizar una configuración de alta disponibilidad.
- Se debe crear el volumen raíz del nodo.
- El sistema debe tener un administrador de claves incorporado o un servidor de gestión de claves externo mediante el protocolo de interoperabilidad de gestión de claves (KMIP).

Pasos

1. Cifre el volumen raíz:

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. Compruebe el estado de la operación de conversión:

```
volume encryption conversion show
```

3. Una vez completada la operación de conversión, compruebe que el volumen esté cifrado:

```
volume show -fields
```

El siguiente ejemplo muestra el resultado de un volumen cifrado.

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver      volume is-encrypted
-----
xyz          vol0    true
```

Información de copyright

Copyright © 2024 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.