



Habilitar la protección ARP

ONTAP 9

NetApp
January 08, 2026

Tabla de contenidos

- Habilitar la protección ARP 1
 - Habilite la protección autónoma frente a ransomware de ONTAP 1
 - Habilitar ARP en volúmenes NAS FlexVol 2
 - Habilitar ARP en volúmenes NAS FlexGroup 5
 - Habilitar ARP en volúmenes SAN 7
 - Información relacionada 8
 - Habilita la protección autónoma frente a ransomware de ONTAP de forma predeterminada en nuevos volúmenes 8

Habilitar la protección ARP

Habilite la protección autónoma frente a ransomware de ONTAP

A partir de ONTAP 9.10,1, puede habilitar la protección autónoma frente a ransomware (ARP) en un volumen existente o crear un volumen nuevo y habilitar ARP desde el principio.

Si desea configurar su clúster ONTAP para que todos los volúmenes nuevos se habiliten de forma predeterminada en Protección autónoma contra ransomware (ARP), consulte esto "[Procedimiento ARP relacionado](#)".

Acerca de esta tarea

Para habilitar ARP, siga el procedimiento que corresponda a su entorno después de [usted se asegura de que su entorno cumpla con ciertos requisitos](#) :

- [NAS con volúmenes FlexVol](#)
- [NAS con volúmenes FlexGroup](#)
- [Volúmenes SAN](#)

Después de habilitar ARP, es posible que ARP entre en un período de transición dependiendo de su entorno y versión de ONTAP :

Tipo de volumen	Versión de ONTAP	Comportamiento tras la habilitación
NAS FlexGroup	ONTAP 9.18.1 y posteriores	ARP/IA se activa inmediatamente sin necesidad de periodo de aprendizaje.
	ONTAP 9.13.1 a 9.17.1	ARP inicia en modo de aprendizaje durante 30 días
NAS FlexVol	ONTAP 9.16.1 y versiones posteriores	ARP/IA se activa inmediatamente sin necesidad de periodo de aprendizaje.
	ONTAP 9.10.1 a 9.15.1	ARP inicia en modo de aprendizaje durante 30 días
Volúmenes SAN	ONTAP 9.17.1 y posteriores	ARP/AI se activa de inmediato, iniciando un período de evaluación para establecer un umbral de alerta adecuado antes de pasar de un umbral conservador inicial.

Antes de empezar

Antes de habilitar ARP, asegúrese de que su entorno tenga lo siguiente:

Requisitos específicos de NAS

- Una máquina virtual de almacenamiento (SVM) con el protocolo NFS o SMB (o ambos) habilitado.
- Carga de trabajo NAS con clientes configurados.
- Un activo "[ruta de unión](#)" para el volumen.

Requisitos específicos de SAN

- Una máquina virtual de almacenamiento (SVM) con protocolo iSCSI, FC o NVMe habilitado.

- Carga de trabajo SAN con clientes configurados.

Requisitos generales

- El ["licencia correcta"](#) para su versión de ONTAP .
- (Recomendado) Verificación multiadministrador (MAV) habilitada (ONTAP 9.13.1 y posterior). Ver ["Habilite la verificación multiadministradora"](#) .

Habilitar ARP en volúmenes NAS FlexVol

Puede habilitar ARP en volúmenes NAS FlexVol utilizando System Manager o la CLI de ONTAP . El proceso varía según la versión de ONTAP .

ONTAP 9.16.1 y versiones posteriores

A partir de ONTAP 9.16.1, ARP/AI se activa inmediatamente sin necesidad de un período de aprendizaje.

System Manager

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, selecciona **Estado** para cambiar de Deshabilitado a Activado.
3. Verifique el estado ARP del volumen en la casilla **Antiransomware**.

Para mostrar el estado ARP para todos los volúmenes: En el panel **Volúmenes**, seleccione **Mostrar/Ocultar** y asegúrese de que el estado **Anti-ransomware** esté marcado.

CLI

Habilitar ARP en un volumen existente:

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

Crea un nuevo volumen con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path  
</path_name>
```

Verificar el estado de ARP:

```
security anti-ransomware volume show
```

Obtenga más información sobre `security anti-ransomware volume show` en el ["Referencia de comandos del ONTAP"](#).

ONTAP 9.10.1 a 9.15.1

Para ONTAP 9.10.1 a 9.15.1, debe habilitar ARP inicialmente en ["modo de aprendizaje"](#) (o estado de "prueba en seco"). El sistema analiza la carga de trabajo para caracterizar el comportamiento normal. Comenzar en modo activo puede generar un exceso de informes de falsos positivos.

Se recomienda dejar que ARP se ejecute en modo de aprendizaje durante un mínimo de 30 días. A partir de ONTAP 9.13.1, ARP determina automáticamente el intervalo óptimo del periodo de aprendizaje y automatiza el cambio, que podría ocurrir antes de los 30 días.

System Manager

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, selecciona **Estado** para cambiar de

Deshabilitado a Activado.

3. Seleccione **Habilitado en modo de aprendizaje** en la casilla **Antiransomware**.



Puede "[Deshabilitar el aprendizaje automático a transiciones de modos activos en la máquina virtual de almacenamiento asociada](#)." Si desea controlar manualmente la transición del modo de aprendizaje al modo activo.



En los volúmenes existentes, los modos de aprendizaje y activos solo se aplican a los datos recién escritos, no a los datos ya existentes en el volumen. Los datos existentes no se analizan y analizan, ya que se asumen las características del tráfico de datos normal anterior según los nuevos datos una vez habilitado para ARP el volumen.

4. Verifique el estado ARP del volumen en la casilla **Antiransomware**.

Para mostrar el estado ARP para todos los volúmenes: En el panel **Volúmenes**, seleccione **Mostrar/Ocultar** y asegúrese de que el estado **Anti-ransomware** esté marcado.

CLI

Habilitar ARP en un volumen existente:

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver  
<svm_name>
```

Obtenga más información sobre `security anti-ransomware volume dry-run` en el "[Referencia de comandos del ONTAP](#)".

Crea un nuevo volumen con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path  
</path_name>
```

Desactivar el cambio automático (opcional):

Si actualizó a ONTAP 9.13.1 a través de ONTAP 9.15.1 y desea controlar manualmente el cambio del modo de aprendizaje al modo activo para todos los volúmenes asociados, puede hacerlo desde la SVM:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to  
-enabled false
```

Verificar el estado de ARP:

```
security anti-ransomware volume show
```

Habilitar ARP en volúmenes NAS FlexGroup

Puede habilitar ARP en volúmenes NAS FlexGroup mediante System Manager o la CLI de ONTAP . El proceso varía según su versión de ONTAP .

ONTAP 9.18.1 y posteriores

A partir de ONTAP 9.18.1, ARP/AI se activa inmediatamente para los volúmenes FlexGroup sin necesidad de un período de aprendizaje.

System Manager

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen de FlexGroup que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, seleccione **Estado** para cambiar de Deshabilitado a Activado.
3. Verifique el estado ARP del volumen en la casilla **Antiransomware**.

Para mostrar el estado ARP para todos los volúmenes: En el panel **Volúmenes**, seleccione **Mostrar/Ocultar** y asegúrese de que el estado **Anti-ransomware** esté marcado.

CLI

Habilitar ARP en un volumen FlexGroup existente:

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

Crea un nuevo volumen FlexGroup con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list  
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti  
-ransomware-state enabled -junction-path </path_name>
```

Verificar el estado de ARP:

```
security anti-ransomware volume show
```

ONTAP 9.13.1 a 9.17.1

Para ONTAP 9.13.1 a 9.17.1, los volúmenes FlexGroup comienzan en "modo de aprendizaje". El sistema analiza la carga de trabajo para caracterizar el comportamiento normal.

Se recomienda dejar que ARP se ejecute en modo de aprendizaje durante un mínimo de 30 días. ARP determina automáticamente el intervalo óptimo del período de aprendizaje y automatiza el cambio, que podría ocurrir antes de 30 días.

System Manager

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen de FlexGroup que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, seleccione **Estado** para cambiar de Deshabilitado a Activado.
3. Seleccione **Habilitado en modo de aprendizaje** en la casilla **Antiransomware**.



Puede "[Deshabilitar el aprendizaje automático a transiciones de modos activos](#)" Si desea controlar manualmente la transición del modo de aprendizaje al modo activo.

4. Verifique el estado ARP del volumen en la casilla **Antiransomware**.

CLI

Habilitar ARP en un volumen FlexGroup existente:

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver  
<svm_name>
```

Crea un nuevo volumen FlexGroup con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list  
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti  
-ransomware-state dry-run -junction-path </path_name>
```

Desactivar el cambio automático (opcional):

Si desea controlar manualmente el cambio del modo de aprendizaje al modo activo:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to  
-enabled false
```

Verificar el estado de ARP:

```
security anti-ransomware volume show
```

Habilitar ARP en volúmenes SAN

A partir de ONTAP 9.17.1, puede habilitar ARP en volúmenes SAN. La funcionalidad ARP/AI se habilita automáticamente e inmediatamente comienza a supervisar y proteger activamente los volúmenes SAN durante el proceso. "[período de evaluación](#)" al mismo tiempo que determina si las cargas de trabajo son adecuadas para ARP y establece un umbral de cifrado óptimo para la detección.

Puede habilitar ARP en volúmenes SAN utilizando System Manager o la CLI de ONTAP .

System Manager

Pasos

1. Seleccione **Almacenamiento > Volúmenes** y, a continuación, seleccione el volumen SAN que desea proteger.
2. En la pestaña **Seguridad** de la vista general **Volúmenes**, seleccione **Estado** para cambiar de Deshabilitado a Activado.
3. ARP/AI entra automáticamente en el período de evaluación.
4. Verifique el estado de ARP y el estado de evaluación en la casilla **Antiransomware**.

Para mostrar el estado ARP para todos los volúmenes: En el panel **Volúmenes**, seleccione **Mostrar/Ocultar** y asegúrese de que el estado **Anti-ransomware** esté marcado.

CLI

Habilitar ARP en un volumen SAN existente:

```
security anti-ransomware volume enable -volume <vol_name> -vserver  
<svm_name>
```

Crear un nuevo volumen SAN con ARP habilitado:

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate  
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

Verifique el estado y la evaluación del ARP:

```
security anti-ransomware volume show
```

Comprueba el `Block device detection status` campo para monitorear el progreso del período de evaluación.

Obtenga más información sobre `security anti-ransomware volume show` en el ["Referencia de comandos del ONTAP"](#).

Información relacionada

- ["Cambia al modo activo después de un periodo de aprendizaje"](#)

Habilita la protección autónoma frente a ransomware de ONTAP de forma predeterminada en nuevos volúmenes

A partir de ONTAP 9.10.1, puede configurar máquinas virtuales de almacenamiento (SVM) para que los nuevos volúmenes estén habilitados de forma predeterminada con

protección autónoma contra ransomware (ARP). Puede modificar esta configuración mediante System Manager o con la CLI.

Si desea configurar solo volúmenes individuales nuevos o existentes sin que ARP sea el valor predeterminado, consulte este ["Procedimiento ARP relacionado"](#).

Acerca de esta tarea

Por defecto, los nuevos volúmenes se crean con la funcionalidad ARP desactivada. Deberá habilitar la funcionalidad ARP y configurarla para que esté habilitada de forma predeterminada en los nuevos volúmenes creados en la SVM.

Los volúmenes existentes sin ARP habilitado no cambiarán automáticamente su estado de habilitación de ARP cuando cambie el valor predeterminado para la SVM. Los cambios en la configuración de SVM descritos en este procedimiento solo afectan a los volúmenes nuevos. Aprende cómo ["Habilite ARP para los volúmenes existentes"](#).

Después de habilitar ARP, es posible que ARP entre en un período de transición dependiendo de su entorno y versión de ONTAP :

Tipo de volumen	Versión de ONTAP	Comportamiento tras la habilitación
NAS FlexGroup	ONTAP 9.18.1 y posteriores	ARP/IA se activa inmediatamente sin necesidad de periodo de aprendizaje.
	ONTAP 9.13.1 a 9.17.1	ARP inicia en modo de aprendizaje durante 30 días
NAS FlexVol	ONTAP 9.16.1 y versiones posteriores	ARP/IA se activa inmediatamente sin necesidad de periodo de aprendizaje.
	ONTAP 9.10.1 a 9.15.1	ARP inicia en modo de aprendizaje durante 30 días
Volúmenes SAN	ONTAP 9.17.1 y posteriores	ARP/AI se activa de inmediato, iniciando un período de evaluación para establecer un umbral de alerta adecuado antes de pasar de un umbral conservador inicial.

Antes de empezar

Antes de habilitar ARP, asegúrese de que su entorno tenga lo siguiente:

Requisitos específicos de NAS

- Una máquina virtual de almacenamiento (SVM) con el protocolo NFS o SMB (o ambos) habilitado.
- Un activo ["ruta de unión"](#) para el volumen.

Requisitos específicos de SAN

- Una máquina virtual de almacenamiento (SVM) con protocolo iSCSI, FC o NVMe habilitado.

Requisitos generales

- El ["licencia correcta"](#) para su versión de ONTAP .
- (Recomendado) Verificación multiadministrador (MAV) habilitada (ONTAP 9.13.1+). Ver ["Habilite la verificación multiadministradora"](#) .

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para habilitar ARP de manera predeterminada en los volúmenes nuevos.

System Manager

1. Seleccione **Almacenamiento** o **Clúster** (según su entorno), seleccione **Máquinas virtuales de almacenamiento** y seleccione la máquina virtual de almacenamiento que contendrá los volúmenes que desea proteger con ARP.
2. Vaya a la pestaña **Configuración**. En **Seguridad**, localice la opción **Anti-ransomware** y seleccione .
3. Marque la casilla para habilitar el antiransomware (ARP). Marque la casilla adicional para habilitar ARP en todos los volúmenes elegibles de la máquina virtual de almacenamiento.
4. Para las versiones de ONTAP con un período de aprendizaje recomendado, seleccione **Cambiar automáticamente del modo de aprendizaje al modo activo después de un aprendizaje suficiente**. Esto permite que ARP determine el intervalo óptimo del periodo de aprendizaje y automatice el cambio al modo activo.

CLI

Modificar una SVM existente para habilitar ARP de forma predeterminada en los nuevos volúmenes.

Seleccionar `dry-run` si su versión de ARP requiere un [período de aprendizaje](#). De lo contrario, seleccione `enabled`.

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume  
-state <dry-run|enabled>
```

Cree una nueva SVM con ARP habilitado de forma predeterminada para los nuevos volúmenes.

Seleccionar `dry-run` si su versión de ARP requiere un [período de aprendizaje](#). De lo contrario, seleccione `enabled`.

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume  
-state <dry-run|enabled>
```

Modificar la SVM existente para deshabilitar la transición automática del aprendizaje al modo activo

Si actualizó a ONTAP 9.13.1 a través de ONTAP 9.15.1 y el estado predeterminado es `dry-run` (modo de aprendizaje), el aprendizaje adaptativo está habilitado para que el cambio a `enabled` El estado (modo activo) se realiza automáticamente. Puede desactivar este interruptor automático para controlar manualmente el cambio del modo de aprendizaje al modo activo para todos los volúmenes asociados:

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to  
-enabled false
```

Verifique el estado ARP

```
security anti-ransomware volume show
```

Información relacionada

- "Cambia al modo activo después de un periodo de aprendizaje"
- "Visualización de volumen de seguridad antiransomware"

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.