



Configurar el análisis en tiempo real

ONTAP 9

NetApp
February 13, 2026

Tabla de contenidos

- Configurar el análisis en tiempo real 1
 - Crear políticas de acceso a ONTAP Vscan 1
 - Habilitar políticas de acceso en ONTAP Vscan 3
 - Modificar el perfil de operaciones de archivos de ONTAP Vscan para recursos compartidos SMB 4
 - Comandos de ONTAP Vscan para administrar políticas de acceso 5

Configurar el análisis en tiempo real

Crear políticas de acceso a ONTAP Vscan

Una directiva en tiempo real define el ámbito de un análisis en tiempo real. Puede crear una política de acceso para una SVM individual o para todas las SVM de un clúster. Si creó una política de acceso para todas las SVM de un clúster, debe habilitar la política en cada SVM de forma individual.

Acerca de esta tarea

- Puede especificar el tamaño máximo de archivo que se va a escanear, las extensiones de archivo y las rutas que se van a incluir en el escaneo, y las extensiones de archivo y las rutas de acceso que se van a excluir del escaneo.
- Puede configurar `scan-mandatory` la opción como OFF para especificar que se permita el acceso a archivos cuando no haya servidores Vscan disponibles para detección de virus.
- De forma predeterminada, ONTAP crea una política de acceso llamada «default_cifs» y la habilita para todas las SVM de un clúster.
- Cualquier archivo que califique para la exclusión de exploración basada en los `paths-to-exclude` `file-ext-to-exclude` `max-file-size` parámetros , , o no se tiene en cuenta para la exploración, incluso si la `scan-mandatory` opción está establecida en Activado. (Consulte esta ["resolución de problemas"](#) sección para ver los problemas de conectividad relacionados con la `scan-mandatory` opción.)
- De forma predeterminada, solo se analizan los volúmenes de lectura/escritura. Puede especificar filtros que permitan el análisis de volúmenes de sólo lectura o que restrinjan el análisis de archivos abiertos con acceso de ejecución.
- La detección de virus no se realiza en un recurso compartido de SMB para el cual el parámetro continuamente disponible se establece en Yes.
- Consulte la ["Arquitectura de antivirus"](#) sección para obtener más información sobre *Vscan file-operations profile*.
- Puede crear un máximo de diez (10) políticas de acceso por SVM. Sin embargo, solo puede habilitar una política de acceso a la vez.
 - Puede excluir un máximo de cien (100) rutas y extensiones de archivos del análisis de virus en una política de acceso.
- Algunas recomendaciones de exclusión de archivos:
 - Considere la posibilidad de excluir archivos grandes (se puede especificar el tamaño de archivo) del análisis de virus porque pueden provocar una respuesta lenta o tiempos de espera de solicitudes de análisis para los usuarios de CIFS. El tamaño de archivo predeterminado para la exclusión es 2GB.
 - Considere la posibilidad de excluir extensiones de archivo `.vhd` como y `.tmp` porque los archivos con estas extensiones pueden no ser adecuados para escanear.
 - Considere la posibilidad de excluir las rutas de archivos, como el directorio en cuarentena o las rutas en las que sólo se almacenan los discos duros virtuales o las bases de datos.
 - Verifique que todas las exclusiones están especificadas en la misma política, porque sólo se puede activar una política a la vez. NetApp recomienda tener el mismo conjunto de exclusiones especificado en el motor antivirus.
 - A partir de ONTAP 9.14.1, puedes usar comodines para especificar rutas de acceso y extensiones de

archivo para excluir.

- Se necesita una política de acceso para un [análisis bajo demanda](#). Para evitar la búsqueda en acceso, debe establecer `-scan-files-with-no-ext` en `false` y `-file-ext-to-exclude` en `*` para excluir todas las extensiones.

Pasos

1. Cree una política de acceso:

```
vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
-policy-name policy_name -protocol CIFS -max-file-size
max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
-file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
-exclude paths_of_files_to_exclude -scan-mandatory on|off
```

- Especifique una SVM de datos para una política definida para una SVM individual, una SVM de administrador de clúster para una política definida para todas las SVM de un clúster.
- `-file-ext-to-exclude` El ajuste anula el `-file-ext-to-include` ajuste.
- Establecer `-scan-files-with-no-ext` como verdadero para escanear archivos sin extensiones. El siguiente comando crea una política de acceso llamada en Policy1 la vs1 SVM:

```
cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
-name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
-file-ext-to-include "mp*", "tx*" -file-ext-to-exclude "mp3", "txt" -scan
-files-with-no-ext false -paths-to-exclude "\\vol\ a b\\", "\\vol\ a, b\\"
```

2. Compruebe que se ha creado la política de acceso continuo: `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

Obtenga más información sobre `vserver vscan on-access-policy` en el ["Referencia de comandos del ONTAP"](#).

El siguiente comando muestra los detalles de Policy1 la política:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```
                Vserver: vs1
                Policy: Policy1
                Policy Status: off
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

Habilitar políticas de acceso en ONTAP Vscan

Una directiva en tiempo real define el ámbito de un análisis en tiempo real. Debe habilitar una política de acceso en una SVM antes de que se puedan analizar los archivos.

Si creó una política de acceso para todas las SVM de un clúster, debe habilitar la política en cada SVM de forma individual. Solo puede habilitar una política de acceso en una SVM a la vez.

Pasos

1. Activar una política de acceso:

```
vserver vscan on-access-policy enable -vserver data_SVM -policy-name
policy_name
```

El siguiente comando habilita una política de acceso llamada en Policy1 la vs1 SVM:

```
cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
-name Policy1
```

2. Compruebe que la política de acceso está activada:

```
vserver vscan on-access-policy show -instance data_SVM -policy-name
policy_name
```

Obtenga más información sobre `vserver vscan on-access-policy show` en el ["Referencia de comandos del ONTAP"](#).

El siguiente comando muestra los detalles de Policy1 la política de acceso:

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1
```

```
                Vserver: vs1
                Policy: Policy1
                Policy Status: on
                Policy Config Owner: vserver
                File-Access Protocol: CIFS
                Filters: scan-ro-volume
                Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
                File Paths Not to Scan: \vol\ a b\, \vol\ a,b\
                File Extensions Not to Scan: mp3, txt
                File Extensions to Scan: mp*, tx*
                Scan Files with No Extension: false
```

Modificar el perfil de operaciones de archivos de ONTAP Vscan para recursos compartidos SMB

El perfil *Vscan file-operations* para un recurso compartido SMB define las operaciones en el recurso compartido que pueden activar el análisis. De forma predeterminada, el parámetro se establece en `standard`. Es posible ajustar el parámetro según sea necesario al crear o modificar un recurso compartido de SMB.

Consulte la ["Arquitectura de antivirus"](#) sección para obtener más información sobre *Vscan file-operations profile*.



La detección de virus no se realiza en un recurso compartido de SMB que tenga el `continuously-available` parámetro establecido en `Yes`.

Paso

1. Modifique el valor del perfil de operaciones de archivo Vscan para un recurso compartido de SMB:

```
vserver cifs share modify -vserver data_SVM -share-name share -path share_path
-vscan-fileop-profile no-scan|standard|strict|writes-only
```

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

El siguiente comando cambia el perfil de operaciones del archivo Vscan para un recurso compartido de SMB a `strict`:

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name
SALES_SHARE -path /sales -vscan-fileop-profile strict
```

Comandos de ONTAP Vscan para administrar políticas de acceso

Puede modificar, deshabilitar o eliminar una política de acceso. Puede ver un resumen y detalles de la política.

Si desea...	Introduzca el siguiente comando...
Crear una política de acceso	<code>vserver vscan on-access-policy create</code>
Modifique una política de acceso	<code>vserver vscan on-access-policy modify</code>
Activar una política de acceso	<code>vserver vscan on-access-policy enable</code>
Deshabilitar una política de acceso	<code>vserver vscan on-access-policy disable</code>
Eliminar una política de acceso	<code>vserver vscan on-access-policy delete</code>
Consulte el resumen y los detalles de una política de acceso	<code>vserver vscan on-access-policy show</code>
Agregar a la lista de rutas de acceso que se van a excluir	<code>vserver vscan on-access-policy paths-to-exclude add</code>
Eliminar de la lista de rutas de acceso que se van a excluir	<code>vserver vscan on-access-policy paths-to-exclude remove</code>
Consulte la lista de rutas de acceso que desea excluir	<code>vserver vscan on-access-policy paths-to-exclude show</code>
Agregar a la lista de extensiones de archivo que se van a excluir	<code>vserver vscan on-access-policy file-ext-to-exclude add</code>
Eliminar de la lista de extensiones de archivo que se van a excluir	<code>vserver vscan on-access-policy file-ext-to-exclude remove</code>
Consulte la lista de extensiones de archivo que se van a excluir	<code>vserver vscan on-access-policy file-ext-to-exclude show</code>
Agregar a la lista de extensiones de archivo que se incluirán	<code>vserver vscan on-access-policy file-ext-to-include add</code>
Eliminar de la lista de extensiones de archivo que se van a incluir	<code>vserver vscan on-access-policy file-ext-to-include remove</code>

Consulte la lista de extensiones de archivo que se incluirán

```
vserver vscan on-access-policy file-  
ext-to-include show
```

Obtenga más información sobre los comandos descritos en este procedimiento en el ["Referencia de comandos del ONTAP"](#).

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.