# Configurar el análisis en tiempo real

ONTAP 9

NetApp
April 16, 2024

# Tabla de contenidos

# Configurar el análisis en tiempo real

## Crear una política de acceso

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 ajustar la `scan-mandatory` Opción de desactivar para especificar que se permite el acceso al archivo cuando no hay servidores Vscan disponibles para el análisis 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 `paths-to-exclude`, `file-ext-to-exclude`, o. `max-file-size` los parámetros no se consideran para la adquisición, incluso si el `scan-mandatory` la opción está activada. (Compruebe esto "resolución de problemas" sección para los problemas de conectividad relacionados con el `scan-mandatory` opcional.)
- 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 "Arquitectura de antivirus" Sección para obtener detalles 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 como `.vhd` y.. `.tmp` debido a que 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.
- Se necesita una política de acceso para un análisis bajo demanda. Para evitar la búsqueda en acceso, debe establecer `-scan-files-with-no-ext` hasta false y. `-file-ext-to-exclude` a * 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.
   - La `-file-ext-to-exclude` el ajuste anula la `-file-ext-to-include` ajuste.
   - Configurado `-scan-files-with-no-ext` true para analizar archivos sin extensiones. El siguiente comando crea una política de acceso llamada `Policy1` en 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: `vserver vscan on-access-policy show -instance` *`data_SVM|cluster_admin_SVM`* `-policy-name` *`name`*

   Para obtener una lista completa de las opciones, consulte la página de manual del comando.

   El siguiente comando muestra los detalles de `Policy1` 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
   ```

# Activar una política de acceso

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 `Policy1` en 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`*

   Para obtener una lista completa de las opciones, consulte la página de manual del comando.

   El siguiente comando muestra los detalles de `Policy1` 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
   ```

# Modifique el perfil de operaciones de archivos Vscan para un recurso compartido de SMB

El perfil *Vscan file-operations* para un recurso compartido SMB define las operaciones en el recurso compartido que pueden activar el análisis. De manera 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 "Arquitectura de antivirus" Sección para obtener detalles 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`

   Para obtener una lista completa de las opciones, consulte la página de manual del comando.

   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 para gestionar políticas en 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 | `vserver vscan on-access-policy create` |
| Modifique una política de acceso | `vserver vscan on-access-policy modify` |
| Activar una política de acceso | `vserver vscan on-access-policy enable` |
| Deshabilitar una política de acceso | `vserver vscan on-access-policy disable` |
| Eliminar una política de acceso | `vserver vscan on-access-policy delete` |

| | |
|---|---|
| Consulte el resumen y los detalles de una política de acceso | `vserver vscan on-access-policy show` |
| Agregar a la lista de rutas de acceso que se van a excluir | `vserver vscan on-access-policy paths-to-exclude add` |
| Eliminar de la lista de rutas de acceso que se van a excluir | `vserver vscan on-access-policy paths-to-exclude remove` |
| Consulte la lista de rutas de acceso que desea excluir | `vserver vscan on-access-policy paths-to-exclude show` |
| Agregar a la lista de extensiones de archivo que se van a excluir | `vserver vscan on-access-policy file-ext-to-exclude add` |
| Eliminar de la lista de extensiones de archivo que se van a excluir | `vserver vscan on-access-policy file-ext-to-exclude remove` |
| Consulte la lista de extensiones de archivo que se van a excluir | `vserver vscan on-access-policy file-ext-to-exclude show` |
| Agregar a la lista de extensiones de archivo que se incluirán | `vserver vscan on-access-policy file-ext-to-include add` |
| Eliminar de la lista de extensiones de archivo que se van a incluir | `vserver vscan on-access-policy file-ext-to-include remove` |
| Consulte la lista de extensiones de archivo que se incluirán | `vserver vscan on-access-policy file-ext-to-include show` |

Para obtener más información sobre estos comandos, consulte las páginas man.