Acerca de la protección antivirus de NetApp

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Acerca de la protección antivirus de NetApp

Obtenga más información sobre el análisis de virus de NetApp con ONTAP Vscan

VSCAN es una solución de análisis antivirus desarrollada por NetApp que permite a los clientes proteger sus datos para evitar que se vean comprometidos por virus u otro código malicioso. Combina el software antivirus proporcionado por los partners con las funciones de ONTAP para ofrecer a los clientes la flexibilidad que necesitan para gestionar los análisis de archivos.

Cómo funciona el análisis de virus

Los sistemas de almacenamiento descargan las operaciones de análisis en servidores externos que alojan software antivirus de otros proveedores.

Basado en el modo de análisis activo, ONTAP envía solicitudes de análisis cuando los clientes acceden a los archivos a través de SMB (en acceso) o acceden a archivos en ubicaciones específicas, en un horario o inmediatamente (bajo demanda).

- Puede utilizar *análisis en tiempo real* para comprobar si hay virus cuando los clientes abren, leen, renombran o cierran archivos en SMB. Las operaciones de archivos se suspenden hasta que el servidor externo informe del estado de análisis del archivo. Si el archivo ya se ha analizado, ONTAP permite la operación de archivo. De lo contrario, solicita un análisis desde el servidor.

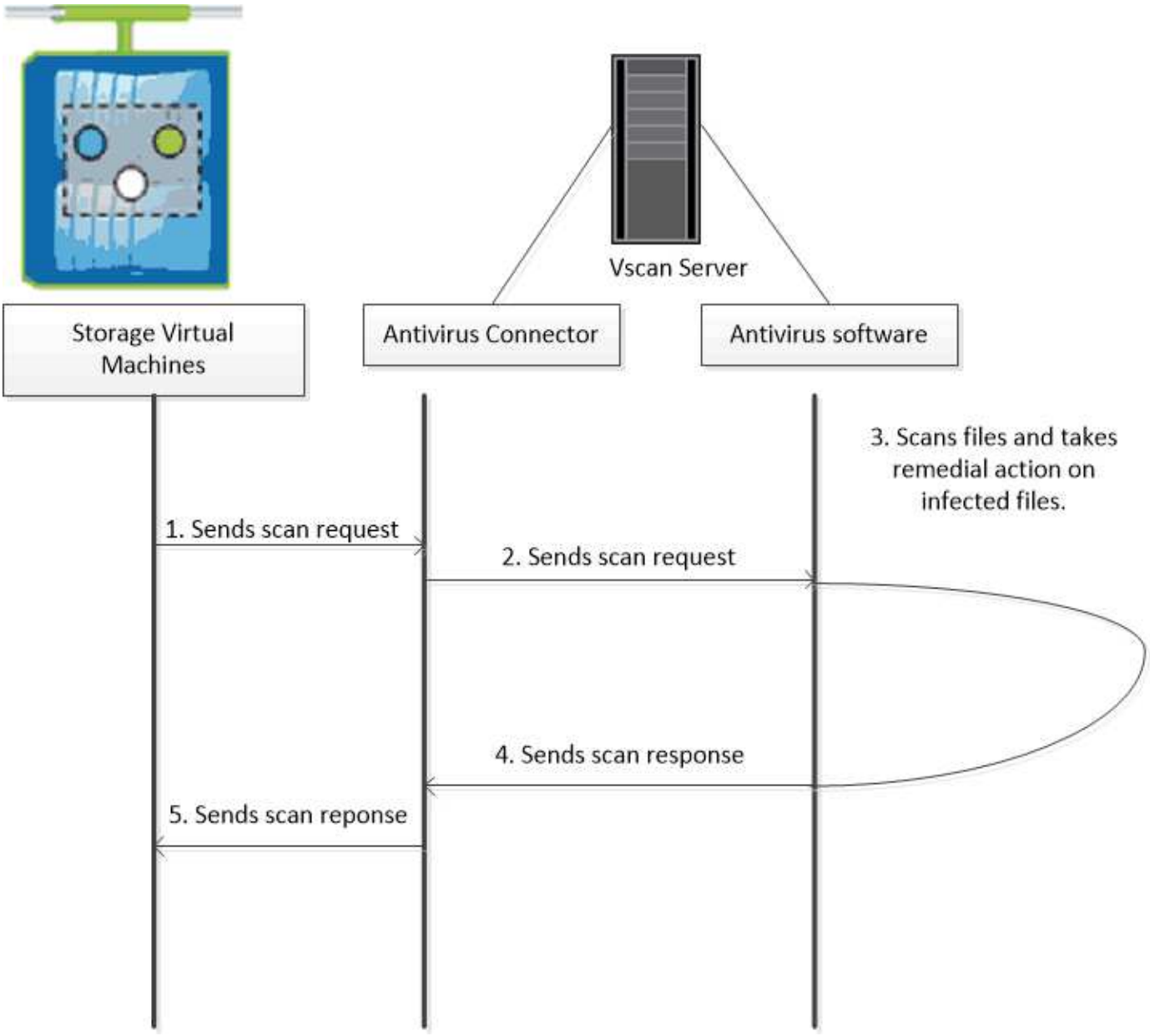
  El análisis en tiempo real no es compatible con NFS.

- Puede utilizar *análisis bajo demanda* para comprobar los archivos en busca de virus inmediatamente o en una programación. Recomendamos que los análisis bajo demanda se ejecuten solo en horas de menor actividad para evitar sobrecargar la infraestructura de antivirus existente, que normalmente está dimensionada para el análisis de acceso. El servidor externo actualiza el estado de escaneo de los archivos comprobados, de modo que la latencia de acceso a archivos se reduce con SMB. Si hubo modificaciones de archivos o actualizaciones de la versión de software, solicita un nuevo análisis de archivos desde el servidor externo.

  Puede utilizar el análisis bajo demanda para cualquier ruta del espacio de nombres de SVM, incluso para los volúmenes que solo se exportan mediante NFS.

Habitualmente, habilita los modos de análisis bajo acceso y bajo demanda en una SVM. En cualquiera de los dos modos, el software antivirus realiza una acción correctiva sobre los archivos infectados en función de la configuración del software.

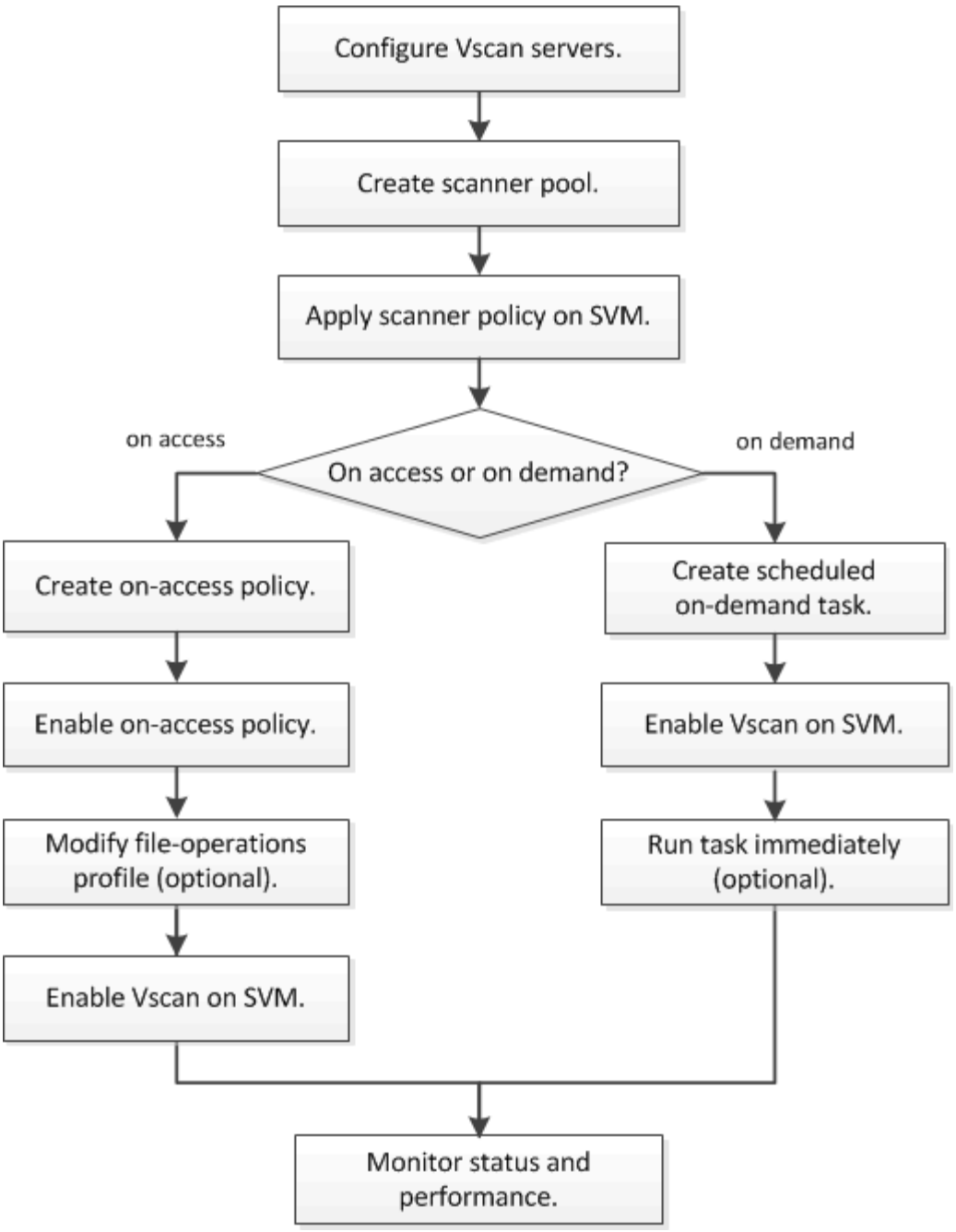
El conector antivirus ONTAP, proporcionado por NetApp e instalado en el servidor externo, gestiona la comunicación entre el sistema de almacenamiento y el software antivirus.



Flujo de trabajo de escaneo de virus con ONTAP Vscan

Debe crear un grupo de escáneres y aplicar una directiva de escáner antes de poder activar el análisis. Habitualmente, habilita los modos de análisis bajo acceso y bajo demanda en una SVM.

Debe haber completado la configuración de CIFS.



Para crear una tarea bajo demanda, debe haber al menos una política de acceso en curso activada. Puede ser la política predeterminada o un usuario creado en la política de acceso.

Siguientes pasos

- Cree un pool de escáneres en un único clúster
- Aplicar una política de escáner en un único clúster
- Crear una política de acceso

Arquitectura antivirus con ONTAP Vscan

La arquitectura antivirus de NetApp consiste en el software del servidor Vscan y la configuración asociada.

Software de servidor VSCAN

Debe instalar este software en el servidor Vscan.

- **Conector antivirus ONTAP**

  Se trata de un software proporcionado por NetApp que gestiona la comunicación de solicitudes de análisis y respuestas entre las SVM y el software antivirus. Puede ejecutarse en una máquina virtual, pero para obtener el mejor rendimiento, utilice una máquina física. Puede descargar este software desde el sitio de soporte de NetApp (requiere inicio de sesión).

- **Software antivirus**

  Este es un software proporcionado por los socios que analiza los archivos en busca de virus u otro código malicioso. Al configurar el software, se especifican las acciones correctivas que se van a realizar en los archivos infectados.

Configuración del software VSCAN

Debe configurar estos ajustes de software en el servidor Vscan.

- **Piscina del escáner**

  Esta configuración define los servidores Vscan y los usuarios con privilegios que se pueden conectar a SVM. También define un período de tiempo de espera de solicitud de exploración, tras el cual la solicitud de exploración se envía a un servidor Vscan alternativo si hay uno disponible.

  > Debe establecer el período de tiempo de espera en el software antivirus del servidor Vscan en cinco segundos menos que el período de tiempo de espera de solicitud de exploración del grupo de análisis. Esto evitará situaciones en las que el acceso al archivo se retrase o rechace por completo porque el período de tiempo de espera del software es mayor que el período de tiempo de espera de la solicitud de exploración.

- **Usuario privilegiado**

  Este ajuste es una cuenta de usuario de dominio que un servidor Vscan utiliza para conectarse a la SVM. La cuenta debe existir en la lista de usuarios con privilegios del grupo de escáneres.

- **Directiva del escáner**

  Esta configuración determina si un conjunto de escáneres está activo. Las políticas de escáner están definidas por el sistema, por lo que no puede crear políticas de escáner personalizadas. Solo estas tres políticas están disponibles:

  - `Primary` especifica que el conjunto de escáneres está activo.
  - `Secondary` Especifica que el grupo de escáneres está activo, sólo cuando no hay ningún servidor Vscan conectado en el grupo de escáneres principal.
  - `Idle` especifica que el conjunto de escáneres está inactivo.

- **Política de acceso**

  Esta configuración define el ámbito de una exploración en acceso. 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.

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 el acceso de ejecución:

- `scan-ro-volume` permite el análisis de volúmenes de solo lectura.
- `scan-execute-access` restringe el escaneo a archivos abiertos con acceso de ejecución.

> ⓘ "Ejecutar acceso" es diferente de "ejecutar permiso". Un cliente dado tendrá "acceso de ejecución" en un archivo ejecutable solo si el archivo fue abierto con "intención de ejecución".

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. En el modo de acceso puede elegir entre estas dos opciones mutuamente excluyentes:

- Obligatorio: Con esta opción, Vscan intenta entregar la solicitud de escaneo al servidor hasta que caduque el período de tiempo de espera. Si el servidor no acepta la solicitud de escaneo, se rechaza la solicitud de acceso del cliente.
- No Obligatorio: Con esta opción, Vscan siempre permite el acceso del cliente, independientemente de que haya o no un servidor Vscan disponible para la detección de virus.

- **Tarea a petición**

Esta configuración define el ámbito de una exploración bajo demanda. 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. Los archivos de los subdirectorios se analizan de forma predeterminada.

Utilice una programación cron para especificar cuándo se ejecuta la tarea. Puede utilizar `vserver vscan on-demand-task run` el comando para ejecutar la tarea inmediatamente. Obtenga más información sobre `vserver vscan on-demand-task run` en el "Referencia de comandos del ONTAP".

- **Perfil de operaciones de archivos Vscan (sólo escaneado en tiempo real)**

```
`vscan-fileop-profile`El parámetro para `vserver cifs share create` el
comando define qué operaciones de archivos SMB desencadenan el análisis
de virus. De forma predeterminada, el parámetro se establece en
`standard`, que es la mejor práctica de NetApp. Puede ajustar este
parámetro como sea necesario al crear o modificar un recurso compartido
de SMB:
```

- `no-scan` especifica que las exploraciones de virus nunca se activan para el recurso compartido.
- `standard` especifica que las operaciones de apertura, cierre y cambio de nombre activan los análisis de virus.
- `strict` especifica que las exploraciones de virus se activan mediante operaciones de apertura, lectura, cierre y cambio de nombre.

El `strict` perfil proporciona una seguridad mejorada para situaciones en las que varios clientes acceden a un archivo de forma simultánea. Si un cliente cierra un archivo después de escribir un virus en este y el mismo archivo permanece abierto en un segundo cliente, `strict` se asegura de que una operación de lectura en el segundo cliente active un análisis antes del cierre del archivo.

Debe tener cuidado de restringir el `strict` perfil a los recursos compartidos que contienen archivos que anticipa que se accederán simultáneamente. Dado que este perfil genera más solicitudes de análisis, puede afectar al rendimiento.

- `writes-only` especifica que las exploraciones de virus se activan sólo cuando se cierran los archivos modificados.

  Dado que `writes-only` genera menos solicitudes de escaneo, normalmente mejora el rendimiento.

Si utiliza este perfil, el escáner debe estar configurado para eliminar o poner en cuarentena los archivos infectados que no se pueden reparar, por lo que no se puede acceder a ellos. Si, por ejemplo, un cliente cierra un archivo tras escribir un virus y el archivo no se repara, elimina ni pone en cuarentena, se `without` infectará ningún cliente que acceda al archivo que escribe en él.

> Si una aplicación cliente realiza una operación de cambio de nombre, el archivo se cierra con el nuevo nombre y no se analiza. Si dichas operaciones suponen un problema de seguridad en su entorno, debe utilizar `standard` `strict` el perfil o.

Obtenga más información sobre `vserver cifs share create` en el "Referencia de comandos del ONTAP".

Conozca las soluciones de socios de ONTAP Vscan

NetApp colabora con Trellix, Symantec, Trend Micro, Sentinel One, Deep Instinct y OPSWAT para ofrecer soluciones antivirus y antimalware líderes en el sector que se basan en la tecnología Vscan de ONTAP. Estas soluciones le ayudan a analizar los archivos en busca de malware y corregir cualquier archivo afectado.

Tal y como se muestra en la siguiente tabla, los detalles de interoperabilidad de Trellix, Symantec y Trend Micro se conservan en la matriz de interoperabilidad de NetApp. Los detalles de interoperabilidad de Trellix, Symantec, Deep Instinct y OPSWAT también se pueden encontrar en los sitios web asociados. Los detalles de interoperabilidad de Sentinel One, Deep Instinct, OPSWAT y otros nuevos socios serán mantenidos por el socio en sus sitios web.

Como partner	Documentación de la solución	Detalles de interoperabilidad
Trellix (anteriormente McAfee)	"Documentación del producto Trellix"	• "Herramienta de matriz de interoperabilidad de NetApp" • "Plataformas compatibles con Endpoint Security Storage Protection (trellix.com)"

Como partner	Documentación de la solución	Detalles de interoperabilidad
Symantec	"Symantec Protection Engine 9.0.0"	• "Herramienta de matriz de interoperabilidad de NetApp" • "Matriz de compatibilidad para dispositivos asociados certificados con Symantec Protection Engine (SPE) para almacenamiento conectado a la red (NAS) 9.x.x."
Trend Micro	"Guía de inicio de Trend Micro ServerProtect for Storage 6,0"	"Herramienta de matriz de interoperabilidad de NetApp"
Sentinel One	• "SentinelOne Singularity Cloud Data Security" • "Compatibilidad con SentinelOne" Este vínculo requiere una conexión de usuario. Puede solicitar acceso desde Sentinel One.	N / A
Instinto profundo	Deep Instinct DSX para NAS • "Documentación e Interop" Este enlace requiere un inicio de sesión del usuario. Puede solicitar acceso desde Deep Instinct. • "Hoja de datos"	N / A
OPSWAT	Seguridad de almacenamiento OPSWAT MetaDefender • "Integración de la seguridad del almacenamiento de MetaDefender con NetApp" • "Página de socio de OPSWAT" • "Breve descripción de la solución de integración"	N / A