Protección antivirus con Vscan

ONTAP 9

NetApp
August 31, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/antivirus/index.html on August 31, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Protección antivirus con Vscan

Información general de la configuración de antivirus

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.

VSCAN realiza análisis de virus cuando los clientes acceden a los archivos a través de SMB. Puede configurar Vscan para que escanee bajo demanda o según una programación. Puede interactuar con Vscan mediante la interfaz de línea de comandos (CLI) de ONTAP o las interfaces de programación de aplicaciones (API) de ONTAP.

Información relacionada

"Soluciones de partners de VSCAN"

Acerca de la protección antivirus de NetApp

Acerca de la detección de virus de NetApp

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.

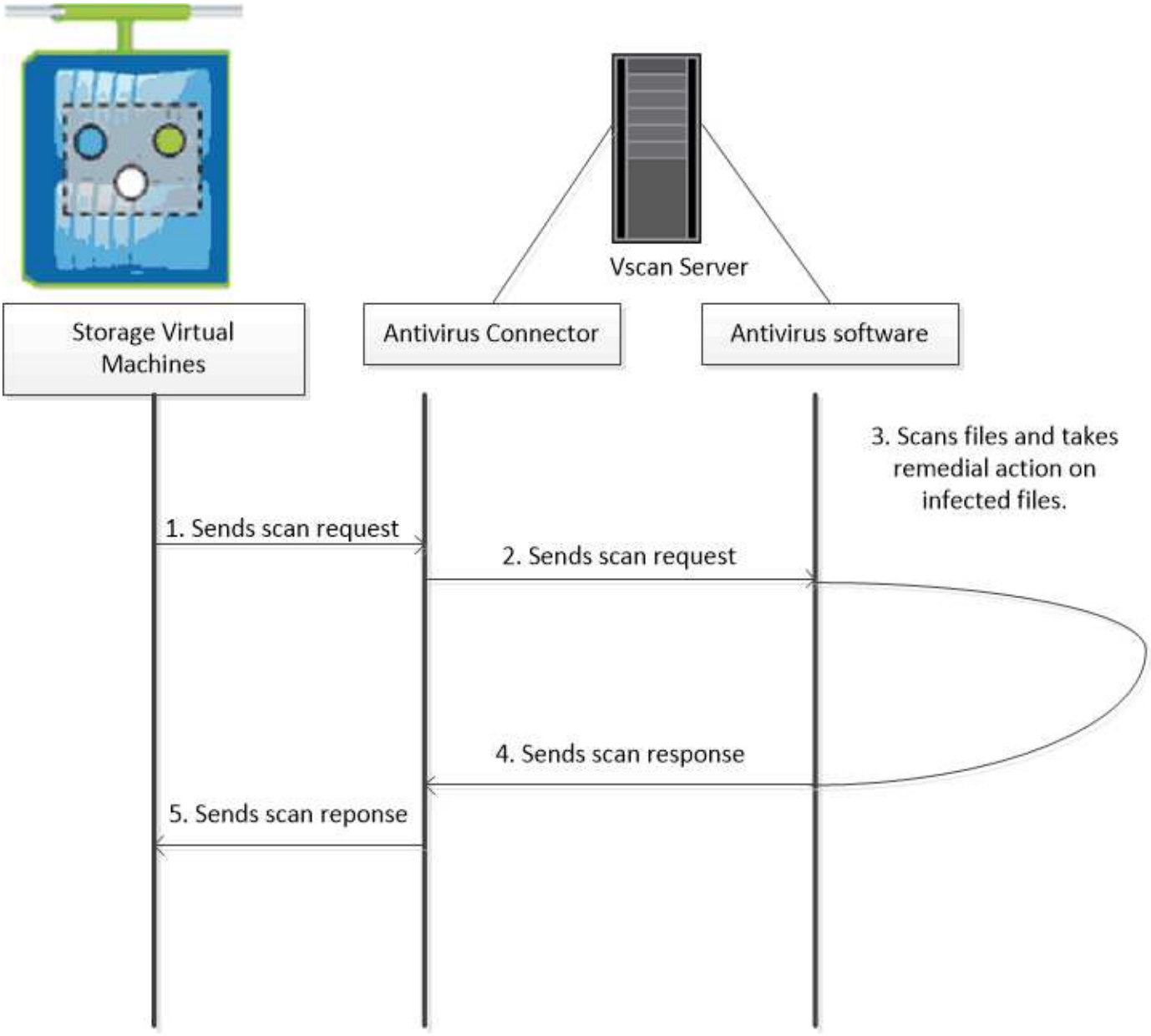
  El análisis en tiempo real no es compatible con NFS.

- 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.

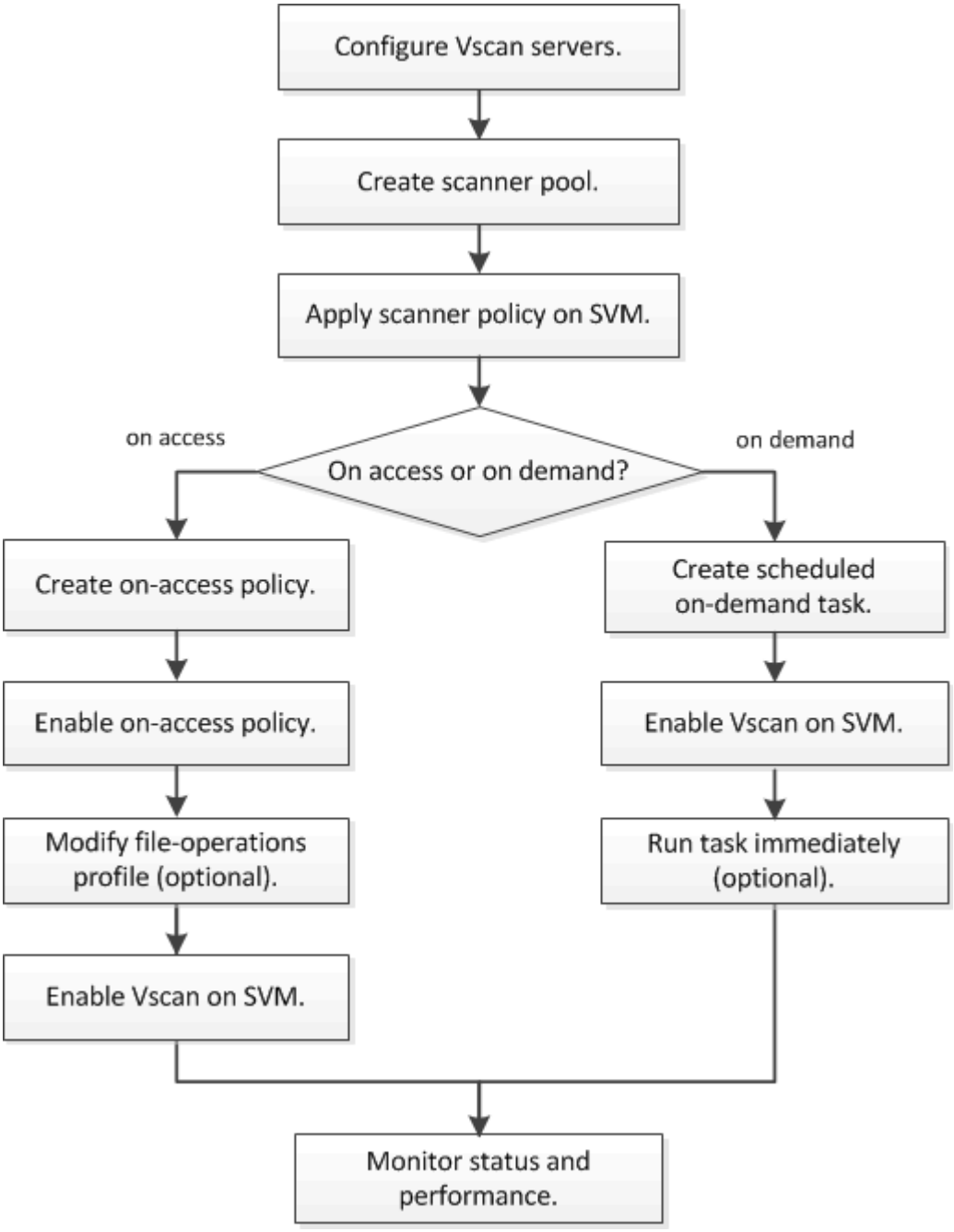
El conector antivirus ONTAP, proporcionado por NetApp e instalado en el servidor externo, gestiona la comunicación entre el sistema de almacenamiento y el software antivirus.



Flujo de trabajo de detección de virus

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.



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 de antivirus

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 grupo 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 grupo 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 analizar 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 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. 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 el `vserver vscan on-demand-task run` comando para ejecutar la tarea de inmediato.

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

La `vscan-fileop-profile` parámetro para `vserver cifs share create` El comando define qué operaciones de archivos SMB desencadenan el análisis de virus. De manera 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.

  La `strict` profile proporciona una seguridad mejorada para situaciones en las que varios clientes acceden a un archivo simultáneamente. Si un cliente cierra un archivo después de escribir un virus y el mismo archivo permanece abierto en un segundo cliente, `strict` garantiza que una operación de lectura del segundo cliente active un análisis antes de cerrar el archivo.

  Debe tener cuidado de restringir el `strict` se accederá simultáneamente a los recursos compartidos que contengan archivos que prevé. 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.

  Desde `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, ningún cliente que acceda al archivo `without` escribir a él será infectado.

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

Soluciones de partners de VSCAN

NetApp colabora con Trellix, Symantec, Trend Micro y Sentinel One para ofrecer soluciones antivirus y antimalware líderes del 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. También puede encontrar información sobre la interoperabilidad de Trellix y Symantec en los sitios web asociados. Los detalles de interoperabilidad de Sentinel One 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)"
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." • "Matriz de compatibilidad para dispositivos de partners certificados con Symantec Protection Engine (SPE) para almacenamiento conectado a la red (NAS) 8.x (broadcom.com)"

Como partner	Documentación de la solución	Detalles de interoperabilidad
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 enlace requiere una conexión de usuario. Puede solicitar acceso desde Sentinel One.	Instinto profundo

Instalación y configuración del servidor VSCAN

Instalación y configuración del servidor VSCAN

Configure uno o más servidores Vscan para asegurarse de que los archivos de su sistema se analicen en busca de virus. Siga las instrucciones proporcionadas por su proveedor para instalar y configurar el software antivirus en el servidor.

Siga las instrucciones del archivo README proporcionado por NetApp para instalar y configurar el conector antivirus de ONTAP. También puede seguir las instrucciones de la "Instale la página Conector antivirus de ONTAP".

> Para la recuperación ante desastres y las configuraciones de MetroCluster, debe configurar servidores Vscan independientes para los clústeres de ONTAP principal/local y secundario/asociado.

Requisitos del software antivirus

- Para obtener información acerca de los requisitos de software antivirus, consulte la documentación del proveedor.
- Para obtener información acerca de los proveedores, software y versiones compatibles con Vscan, consulte "Soluciones de partners de VSCAN" página.

Requisitos del conector antivirus de ONTAP

- Puede descargar el conector antivirus de ONTAP desde la página **Descarga de software** del sitio de soporte de NetApp. "Descargas de NetApp: Software"
- Para obtener información sobre las versiones de Windows compatibles con el conector antivirus de ONTAP y los requisitos de interoperabilidad, consulte "Soluciones de partners de VSCAN".

> Puede instalar diferentes versiones de servidores Windows para diferentes servidores Vscan en un clúster.

- .NET 3.0 o posterior debe estar instalado en el servidor Windows.

- Debe estar habilitado SMB 2.0 en el servidor de Windows.

Instale el conector antivirus de ONTAP

Instale el conector antivirus ONTAP en el servidor Vscan para permitir la comunicación entre el sistema que ejecuta ONTAP y el servidor Vscan. Cuando el conector antivirus ONTAP está instalado, el software antivirus puede comunicarse con una o más máquinas virtuales de almacenamiento (SVM).

Acerca de esta tarea

- Consulte "Soluciones de partners de VSCAN" Para obtener información sobre los protocolos compatibles, las versiones del software del proveedor de antivirus, las versiones de ONTAP, los requisitos de interoperabilidad y los servidores Windows.
- Se debe instalar .NET 4.5.1 o posterior.
- El conector antivirus ONTAP puede ejecutarse en una máquina virtual. Sin embargo, para obtener el mejor rendimiento, NetApp recomienda utilizar una máquina virtual dedicada para el análisis antivirus.
- SMB 2,0 debe estar habilitado en el servidor Windows en el que está instalando y ejecutando el conector antivirus de ONTAP.

Antes de empezar

- Descargue el archivo de instalación del conector antivirus de ONTAP desde el sitio de soporte y guárdelo en un directorio del disco duro.
- Compruebe que cumple los requisitos para instalar el conector antivirus de ONTAP.
- Compruebe que dispone de privilegios de administrador para instalar Antivirus Connector.

Pasos

1. Inicie el asistente de instalación de Antivirus Connector ejecutando el archivo de configuración adecuado.
2. Seleccione *Siguiente*. Se abre el cuadro de diálogo Carpeta de destino.
3. Seleccione *Next* para instalar el conector antivirus en la carpeta que aparece en la lista o seleccione *Change* para instalarlo en una carpeta diferente.
4. Se abre el cuadro de diálogo Credenciales de servicio de Windows del conector AV de ONTAP.
5. Ingrese sus credenciales de servicio de Windows o seleccione **Agregar** para seleccionar un usuario. Para un sistema ONTAP, este usuario debe ser un usuario de dominio válido y debe existir en la configuración del pool de análisis de la SVM.
6. Seleccione **Siguiente**. Se abre el cuadro de diálogo Preparado para instalar el programa.
7. Seleccione **Instalar** para comenzar la instalación o seleccione **Atrás** si desea realizar cambios en la configuración. Se abre un cuadro de estado y traza el progreso de la instalación, seguido del cuadro de diálogo InstallShield Wizard Completed.
8. Active la casilla de comprobación Configure ONTAP LIF si desea continuar con la configuración de la gestión de ONTAP o de las LIF de datos. Debe configurar al menos una LIF de datos o de gestión de ONTAP para poder utilizar este servidor Vscan.
9. Seleccione la casilla de verificación Mostrar el **registro de Windows Installer** si desea ver los registros de instalación.
10. Seleccione **Finish** para finalizar la instalación y cerrar el asistente InstallShield. El icono de configuración de LIF de ONTAP* se guarda en el escritorio para configurar las LIF de ONTAP.

11. Agregue una SVM al conector antivirus. Puede añadir un SVM al conector antivirus añadiendo una LIF de gestión ONTAP, pollada para recuperar la lista de LIF de datos, o bien configurando directamente el LIF o LIF con datos. También debe proporcionar la información de sondeo y las credenciales de la cuenta de administrador de ONTAP si se configuró la LIF de gestión de ONTAP.
    - Compruebe que la LIF de gestión o la dirección IP de la SVM estén habilitadas para `management-https`. Esto no es necesario cuando solo está configurando LIF de datos.
    - Compruebe que ha creado una cuenta de usuario para la aplicación HTTP y que ha asignado un rol que tiene (al menos de sólo lectura) acceso al `/api/network/ip/interfaces` API DE REST. Para obtener más información sobre la creación de un usuario, consulte "seguridad rol de inicio de sesión crear" y.. "seguridad de inicio de sesión creado" Páginas manuales de ONTAP.

> También puede usar el usuario de dominio como cuenta añadiendo una SVM de túnel de autenticación para una SVM administrativa. Para obtener más información, consulte "creación de dominio de conexión de seguridad-túnel" El comando man de ONTAP o utilice el `/api/security/acccounts` y.. `/api/security/roles` API REST para configurar la cuenta y el rol de administrador.

Pasos

1. Haga clic con el botón derecho del ratón en el icono de configuración de LIF de ONTAP*, que se guardó en su escritorio cuando completó la instalación del conector antivirus y, a continuación, seleccione * Ejecutar como administrador *.
2. En el cuadro de diálogo Configure ONTAP LIF, seleccione el tipo de configuración preferido y, a continuación, realice las siguientes acciones:

Para crear este tipo de LIF…	Realice estos pasos…
LIF de datos	a. Establezca la función en los datos. b. Establezca el protocolo de datos en «cifs». c. Establezca la «política de cortafuegos» en «datos». d. Establezca la «política de servicio» en «archivos de datos predeterminados».
LIF de gestión	a. Establecer “Rol* en “Datos” b. Establezca el protocolo de datos en ninguno. c. Establezca la política de firewall en «gestión» d. Establezca la política de servicio en la gestión predeterminada.

Más información acerca de "Crear una LIF".

Después de crear una LIF, introduzca la dirección IP o la LIF de gestión o la dirección IP de la SVM que desea añadir. También puede introducir la LIF de gestión del clúster. Si especifica la LIF de gestión de clúster, todas las SVM dentro de ese clúster que sirven SMB pueden utilizar el servidor Vscan.

Cuando se requiere autenticación Kerberos para los servidores Vscan, cada LIF de datos de SVM debe tener un nombre DNS único, y debe registrarlo como nombre principal de servidor (SPN) con Windows Active Directory. Cuando no hay un nombre DNS único disponible para cada LIF de datos o registrado como SPN, el servidor Vscan utiliza el mecanismo NT LAN Manager para la autenticación. Si agrega o modifica los nombres DNS y los SPN después de conectar el servidor Vscan, debe reiniciar el servicio Antivirus Connector en el servidor Vscan para aplicar los cambios.

3. Para configurar una LIF de gestión, introduzca la duración del sondeo en segundos. La duración del sondeo es la frecuencia con la que el Antivirus Connector comprueba si hay cambios en las SVM o en la configuración LIF del clúster. El intervalo de sondeo predeterminado es de 60 segundos.
4. Introduzca el nombre de cuenta de administrador de ONTAP y la contraseña para configurar una LIF de gestión.
5. Haga clic en **Test** para comprobar la conectividad y verificar la autenticación. La autenticación solo se verifica para una configuración de LIF de gestión.
6. Haga clic en **Update** para agregar la LIF a la lista de LIF a la que sondear o para conectarse.
7. Haga clic en **Guardar** para guardar la conexión al registro.
8. Haga clic en **Exportar** si desea exportar la lista de conexiones a un archivo de importación o exportación de registro. Esto resulta útil si varios servidores Vscan utilizan el mismo conjunto de LIF de datos o gestión.

Consulte "Configure la página Conector de antivirus de ONTAP" para opciones de configuración.

Configure el conector antivirus de ONTAP

Configure el conector antivirus de ONTAP para especificar una o varias máquinas virtuales de almacenamiento (SVM) a las que desee conectarse. Para ello, introduzca la LIF de gestión de ONTAP, la información de encuestas y las credenciales de la cuenta de administrador de ONTAP, o solo la LIF de datos. También es posible modificar los detalles de una conexión de SVM o quitarla. De forma predeterminada, el conector antivirus de ONTAP utiliza las API DE REST para recuperar la lista de LIF de datos si está configurada la LIF de gestión de ONTAP.

Modifique los detalles de una conexión de SVM

Para actualizar los detalles de una conexión de máquina virtual de almacenamiento (SVM), que se añadió al conector antivirus, modifique el LIF de gestión de ONTAP y la información de sondeo. No se pueden actualizar los LIF de datos después de que se hayan añadido. Para actualizar las LIF de datos, primero debe eliminarlas y volver a añadirlas con la nueva dirección IP o LIF.

Antes de empezar

Compruebe que ha creado una cuenta de usuario para la aplicación HTTP y que ha asignado un rol que tiene (al menos de sólo lectura) acceso al `/api/network/ip/interfaces` API DE REST. Para obtener más información sobre la creación de un usuario, consulte "seguridad rol de inicio de sesión crear" y la "seguridad de inicio de sesión creado" comandos. También puede usar el usuario de dominio como cuenta añadiendo una SVM de túnel de autenticación para una SVM administrativa. Para obtener más información, consulte "creación de dominio de conexión de seguridad-túnel" Página del comando man de ONTAP.

Pasos

1. Haga clic con el botón derecho en el icono de configuración de LIF de ONTAP*, que se guardó en su escritorio cuando completó la instalación del conector antivirus y, a continuación, seleccione * Ejecutar como administrador *. Se abre el cuadro de diálogo Configurar LIF de ONTAP.
2. Seleccione la dirección IP de SVM y, a continuación, haga clic en **Actualizar**.
3. Actualice la información, según sea necesario.
4. Haga clic en **Guardar** para actualizar los detalles de conexión en el registro.
5. Haga clic en **Exportar** si desea exportar la lista de conexiones a una importación de registro o a un archivo de exportación de registro. Esto resulta útil si varios servidores Vscan utilizan el mismo conjunto de LIF de datos o gestión.

Elimine una conexión SVM del conector antivirus

Si ya no requiere una conexión de SVM, puede quitarla.

Pasos

1. Haga clic con el botón derecho en el icono de configuración de LIF de ONTAP*, que se guardó en su escritorio cuando completó la instalación del conector antivirus y, a continuación, seleccione * Ejecutar como administrador *. Se abre el cuadro de diálogo Configurar LIF de ONTAP.
2. Seleccione una o más direcciones IP de SVM y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Guardar** para actualizar los detalles de conexión en el registro.
4. Haga clic en **Exportar** si desea exportar la lista de conexiones a un archivo de importación o exportación de registro. Esto resulta útil si varios servidores Vscan utilizan el mismo conjunto de LIF de datos o gestión.

Solucionar problemas

Antes de empezar

Al crear valores de registro en este procedimiento, utilice el panel lateral derecho.

Puede activar o desactivar los registros de Antivirus Connector con fines de diagnóstico. Por defecto, estos logs están desactivados. Para mejorar el rendimiento, debe mantener los registros del conector antivirus desactivados y solo habilitarlos para eventos críticos.

Pasos

1. Seleccione **Inicio**, escriba “regedit” en el cuadro de búsqueda y, a continuación, seleccione `regedit.exe` En la lista Programas.
2. En **Editor del Registro**, busque la siguiente subclave para el Conector de Antivirus de ONTAP: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. Cree valores de registro proporcionando el tipo, el nombre y los valores mostrados en la siguiente tabla:

Tipo	Nombre	Valores
Cadena	Tracepath	c:\avshim.log

   Este valor de registro puede ser cualquier otra ruta válida.

4. Cree otro valor de registro proporcionando el tipo, el nombre, los valores y la información de registro que se muestra en la siguiente tabla:

Tipo	Nombre	Registro crítico	Registro intermedio	Registro detallado
DWORD	Nivel de tracción	1	2 o 3	4

Esto activa los registros de Antivirus Connector que se guardan en el valor de ruta proporcionado en TracePath en el paso 3.

5. Desactive los registros de Antivirus Connector eliminando los valores de registro que creó en los pasos 3 y 4.
6. Crear otro valor de registro de tipo “MULTI_SZ” con el nombre “LogRotation” (sin comillas). En LogRotation, Proporcione “LogFileSize:1” como una entrada para el tamaño de rotación (donde 1 representa 1MB) y en la siguiente línea, proporcione “logFileCount:5” como un entrada para el límite de rotación (5 es el límite).

> Estos valores son opcionales. Si no se proporcionan, los valores predeterminados de los archivos 20MB y 10 se utilizan para el tamaño de rotación y el límite de rotación respectivamente. Los valores enteros proporcionados no proporcionan valores decimales ni de fracción. Si proporciona valores superiores a los predeterminados, se utilizan los valores predeterminados en su lugar.

7. Para desactivar la rotación de log configurada por el usuario, elimine los valores de registro que creó en el Paso 6.

Banner personalizable

Un banner personalizado le permite colocar una declaración legalmente vinculante y una exención de responsabilidad de acceso al sistema en la ventana *Configurar ONTAP LIF API*.

Paso

1. Modifique el banner predeterminado actualizando el contenido del `banner.txt` en el directorio de instalación y, a continuación, guarde los cambios. Debe volver a abrir la ventana Configure ONTAP LIF API para ver los cambios que se reflejan en el banner.

Active el modo Ordenanza ampliada (EO)

Puede activar y desactivar el modo de ordenanza extendida (EO) para un funcionamiento seguro.

Pasos

1. Seleccione **Inicio**, escriba “regedit” en el cuadro de búsqueda y, a continuación, seleccione `regedit.exe` En la lista Programas.
2. En el **Editor del Registro**, busque la siguiente subclave para el conector antivirus de ONTAP: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. En el panel de la derecha, cree un nuevo valor de registro del tipo “DWORD” con el nombre “EO_Mode” (sin comillas) y el valor “1” (sin comillas) para habilitar el modo EO o el valor “0” (sin comillas) para desactivar el modo EO.

> De forma predeterminada, si el `EO_Mode` La entrada del registro está ausente, el modo EO está desactivado. Cuando habilita el modo EO, debe configurar tanto el servidor de syslog externo como la autenticación de certificados mutuos.

Configure el servidor de syslog externo

Antes de empezar

Tenga en cuenta que cuando cree valores de registro en este procedimiento, utilice el panel lateral derecho.

Pasos

1. Seleccione **Inicio**, escriba “regedit” en el cuadro de búsqueda y, a continuación, seleccione `regedit.exe` En la lista Programas.
2. En **Editor del Registro**, cree la siguiente subclave para el conector antivirus de ONTAP para la configuración syslog: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. Cree un valor de registro proporcionando el tipo, el nombre y el valor como se muestra en la siguiente tabla:

Tipo	Nombre	Valor
DWORD	syslog_enabled	1 o 0

   Tenga en cuenta que un valor «1» activa el syslog y un valor «0» lo desactiva.

4. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

Tipo	Nombre
REG_SZ	Host_syslog

   Proporcione la dirección IP o el nombre de dominio del host de syslog para el campo Value.

5. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

Tipo	Nombre
REG_SZ	Puerto_syslog

   Proporcione el número de puerto en el que se ejecuta el servidor de syslog en el campo Value.

6. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

Tipo	Nombre
REG_SZ	Protocolo_syslog

   Introduzca el protocolo que se está utilizando en el servidor de syslog, «tcp» o «udp», en el campo Valor.

7. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

Tipo	Nombre	CRIT_LOG	AVISO_LOG	INFORMACIÓN_LOG	LOG_DEBUG

DWORD	Nivel_syslog	2	5	6	7

8. Cree otro valor de registro proporcionando la información que se muestra en la siguiente tabla:

Tipo	Nombre	Valor
DWORD	syslog_tls	1 o 0

Tenga en cuenta que un valor «1» habilita syslog con Transport Layer Security (TLS) y un valor «0» deshabilita syslog con TLS.

Asegúrese de que un servidor syslog externo configurado se ejecute sin problemas

- Si la clave está ausente o tiene un valor nulo:
  - El protocolo por defecto es «tcp».
  - El puerto de forma predeterminada es «514» para «tcp/udp» normal y, de forma predeterminada, «6514» para TLS.
  - El nivel syslog se establece de forma predeterminada en 5 (LOG_NOTE).
- Para confirmar que syslog está habilitado, se debe verificar que el `syslog_enabled` el valor es «1». Cuando la `syslog_enabled` El valor es 1. Debe poder iniciar sesión en el servidor remoto configurado tanto si el modo EO está activado como si no.
- Si el modo EO está establecido en “1” y cambia el `syslog_enabled` valor de «1» a «0», se aplica lo siguiente:
  - No es posible iniciar el servicio si syslog no está habilitado en modo EO.
  - Si el sistema se está ejecutando en un estado estable, aparece una advertencia que indica que syslog no se puede desactivar en el modo EO y syslog se establece forzosamente en “1”, que puede ver en el registro. Si esto ocurre, primero debe deshabilitar el modo EO y, a continuación, desactivar syslog.
- Si el servidor syslog no puede ejecutarse correctamente cuando el modo EO y syslog están habilitados, el servicio se detiene. Esto puede ocurrir por uno de los siguientes motivos:
  - Se configuró un syslog_host no válido o no.
  - Se ha configurado un protocolo no válido aparte de UDP o TCP.
  - Un número de puerto no es válido.
- Para una configuración TCP o TLS sobre TCP, si el servidor no está escuchando en el puerto IP, la conexión falla y el servicio se cierra.

Configure la autenticación de certificado mutuo X,509

La autenticación mutua basada en certificado X,509 es posible para la comunicación de capa de sockets seguros (SSL) entre el conector antivirus y ONTAP en la ruta de administración. Si el modo EO está activado y no se encuentra el certificado, el conector AV finaliza. Realice el siguiente procedimiento en el conector antivirus:

Pasos

1. El conector antivirus busca el certificado de cliente del conector antivirus y el certificado de la entidad de certificación (CA) para el servidor NetApp en la ruta del directorio desde donde el conector antivirus ejecuta el directorio de instalación. Copie los certificados en esta ruta de acceso de directorio fija.

2. Incruste el certificado de cliente y su clave privada en el formato PKCS12 y asígnele el nombre “AV_CLIENT.P12”.
3. Asegúrese de que el certificado de CA (junto con cualquier autoridad de firma intermedia hasta la CA raíz) utilizado para firmar el certificado para el servidor NetApp tenga el formato de correo mejorado de privacidad (PEM) y el nombre «ontap_ca.pem». Colóquelo en el directorio de instalación de Antivirus Connector. En el sistema NetApp ONTAP, instale el certificado de CA (junto con cualquier autoridad de firma intermedia hasta la CA raíz) que se utiliza para firmar el certificado de cliente para el conector antivirus en ONTAP como certificado de tipo client-ca.

Configurar grupos de escáneres

Descripción general de la configuración de los pools de escáner

Un grupo de escáneres define los servidores Vscan y los usuarios con privilegios que pueden conectarse a las SVM. Una directiva de escáner determina si un grupo de escáneres está activo.

Si utiliza una política de exportación en un servidor SMB, debe agregar cada servidor Vscan a la política de exportación.

Cree un pool de escáneres en un único clúster

Un grupo de escáneres define los servidores Vscan y los usuarios con privilegios que pueden conectarse a las SVM. Puede crear un pool de escáner para una SVM individual o para todas las SVM de un clúster.

Lo que necesitará

- Los SVM y los servidores Vscan deben estar en el mismo dominio o en dominios de confianza.
- Para los pools de análisis definidos para una SVM individual, debe haber configurado el conector antivirus de ONTAP con la LIF de gestión de SVM o la LIF de datos de SVM.
- Para los pools de análisis definidos para todas las SVM de un clúster, debe haber configurado el conector antivirus de ONTAP con la LIF de gestión de clúster.
- La lista de usuarios con privilegios debe incluir la cuenta de usuario de dominio que el servidor Vscan utiliza para conectarse a la SVM.
- Una vez configurado el grupo de escáneres, compruebe el estado de conexión a los servidores.

Pasos

1. Crear un grupo de escáneres:

```
vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
-pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
privileged_users
```

   - Especifique una SVM de datos para un pool definido para una SVM individual y especifique una SVM de administrador de clúster para un pool definido para todas las SVM de un clúster.
   - Especifique una dirección IP o FQDN para cada nombre de host del servidor Vscan.
   - Especifique el dominio y el nombre de usuario de cada usuario con privilegios. Para obtener una lista

completa de las opciones, consulte la página de manual del comando.

El siguiente comando crea un grupo de escáneres denominado `SP` en la `vs1` SVM:

```
cluster1::> vserver vscan scanner-pool create -vserver vs1 -scanner-pool
SP -hostnames 1.1.1.1,vmwin204-27.fsct.nb -privileged-users
cifs\u1,cifs\u2
```

2. Compruebe que se ha creado el grupo de escáneres:

`vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

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

El siguiente comando muestra los detalles de `SP` grupo de escáneres:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: idle
                             Current Status: off
          Cluster on Which Policy Is Applied: -
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
```

También puede utilizar el `vserver vscan scanner-pool show` Comando para ver todos los pools de análisis de una SVM. Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

Crear grupos de escáneres en configuraciones de MetroCluster

Debe crear pools de análisis primarios y secundarios en cada clúster en una configuración de MetroCluster que corresponda a las SVM primarias y secundarias en el clúster.

Lo que necesitará

- Los SVM y los servidores Vscan deben estar en el mismo dominio o en dominios de confianza.
- Para los pools de análisis definidos para una SVM individual, debe haber configurado el conector antivirus de ONTAP con la LIF de gestión de SVM o la LIF de datos de SVM.

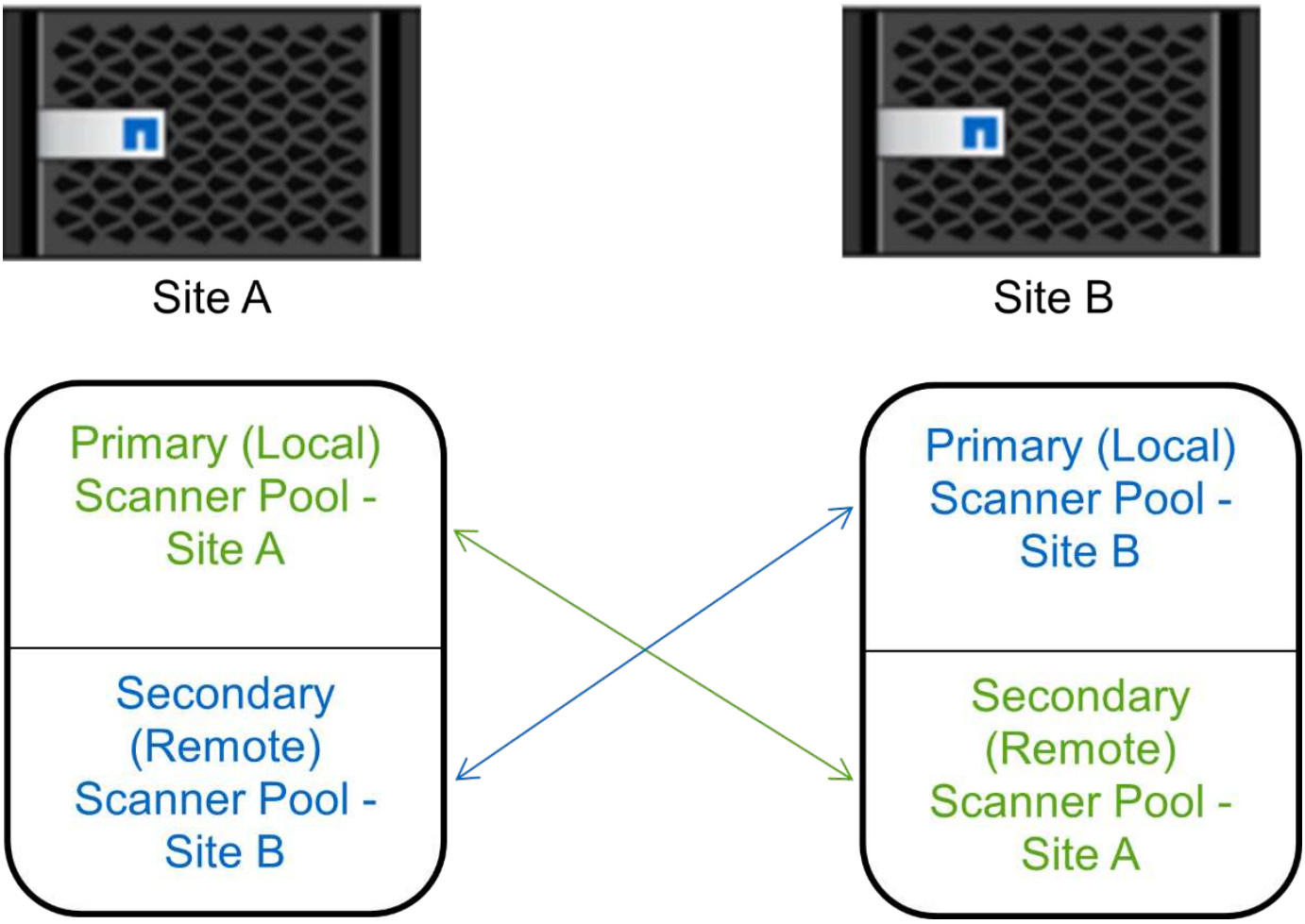
- Para los pools de análisis definidos para todas las SVM de un clúster, debe haber configurado el conector antivirus de ONTAP con la LIF de gestión de clúster.
- La lista de usuarios con privilegios debe incluir la cuenta de usuario de dominio que el servidor Vscan utiliza para conectarse a la SVM.
- Una vez configurado el grupo de escáneres, compruebe el estado de conexión a los servidores.

Acerca de esta tarea

Las configuraciones de MetroCluster protegen los datos mediante la implementación de dos clústeres reflejados físicamente independientes. Cada clúster replica de forma síncrona los datos y la configuración de SVM del otro. Una SVM primaria en el clúster local proporciona datos cuando el clúster está en línea. Una SVM secundaria en el clúster local proporciona datos cuando el clúster remoto está sin conexión.

Esto significa que debe crear pools de análisis primarios y secundarios en cada clúster en una configuración de MetroCluster; el pool secundario se activa cuando el clúster comienza a suministrar datos a partir de la SVM secundaria. Para la recuperación ante desastres, la configuración es similar a MetroCluster.

En esta figura se muestra una configuración MetroCluster/DR típica.



Pasos

1. Crear un grupo de escáneres:

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

- Especifique una SVM de datos para un pool definido para una SVM individual y especifique una SVM de administrador de clúster para un pool definido para todas las SVM de un clúster.
- Especifique una dirección IP o FQDN para cada nombre de host del servidor Vscan.
- Especifique el dominio y el nombre de usuario de cada usuario con privilegios.

  Debe crear todos los pools de escáner desde el clúster que contiene la SVM principal.

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

  Los siguientes comandos crean pools de análisis principales y secundarios en cada clúster en una configuración de MetroCluster:

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Compruebe que se han creado los grupos de escáneres:

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

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

   El siguiente comando muestra los detalles del grupo de escáneres `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                              Applied Policy: idle
                              Current Status: off
         Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

También puede utilizar el `vserver vscan scanner-pool show` Comando para ver todos los pools de análisis de una SVM. Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

Aplicar una política de escáner en un único clúster

Una directiva de escáner determina si un grupo de escáneres está activo. Debe activar un grupo de escáneres para que los servidores Vscan que define puedan conectarse a una SVM.

Acerca de esta tarea

- Sólo puede aplicar una directiva de escáner a un grupo de escáneres.
- Si ha creado un pool de escáner para todas las SVM de un clúster, debe aplicar una política de escáner en cada SVM de forma individual.

Pasos

1. Aplicar una política de escáner:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Una directiva de escáner puede tener uno de los siguientes valores:

   - `Primary` especifica que el grupo de escáneres está activo.
   - `Secondary` Especifica que el grupo de escáneres está activo sólo si no hay ninguno de los servidores Vscan del grupo de escáneres primario conectado.
   - `Idle` especifica que el grupo de escáneres está inactivo.

     En el siguiente ejemplo se muestra el nombre del grupo de escáneres `SP` en la `vs1` SVM está activa:

```
cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
-scanner-pool SP  -scanner-policy primary
```

2. Compruebe que el grupo de escáneres está activo:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

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

   El siguiente comando muestra los detalles de `SP` grupo de escáneres:

```
cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
SP

                                    Vserver: vs1
                               Scanner Pool: SP
                             Applied Policy: primary
                             Current Status: on
         Cluster on Which Policy Is Applied: cluster1
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                   List of Privileged Users: cifs\u1, cifs\u2
```

   Puede utilizar el `vserver vscan scanner-pool show-active` Comando para ver los pools de análisis activos en una SVM. Para obtener la sintaxis completa del comando, consulte la página de manual del comando.

Aplicar directivas de escáner en las configuraciones de MetroCluster

Una directiva de escáner determina si un grupo de escáneres está activo. Debe aplicar una política de escáner a los pools de análisis principal y secundario de cada clúster de una configuración de MetroCluster.

Acerca de esta tarea

- Sólo puede aplicar una directiva de escáner a un grupo de escáneres.
- Si ha creado un pool de escáner para todas las SVM de un clúster, debe aplicar una política de escáner en cada SVM de forma individual.
- Para la recuperación ante desastres y las configuraciones de MetroCluster, debe aplicar una directiva de escáner a cada grupo de escáneres del clúster local y del clúster remoto.
- En la política que cree para el clúster local, debe especificar el clúster local en el `cluster` parámetro. En la política que crea para el clúster remoto, debe especificar el clúster remoto en la `cluster` parámetro. A continuación, el clúster remoto puede hacerse cargo de las operaciones de detección de virus en caso de

desastre.

Pasos

1. Aplicar una política de escáner:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Una directiva de escáner puede tener uno de los siguientes valores:

   - `Primary` especifica que el grupo de escáneres está activo.
   - `Secondary` Especifica que el grupo de escáneres está activo sólo si no hay ninguno de los servidores Vscan del grupo de escáneres primario conectado.
   - `Idle` especifica que el grupo de escáneres está inactivo.

     Debe aplicar todas las políticas de análisis del clúster que contiene la SVM principal.

     Los siguientes comandos aplican políticas de análisis a los pools de análisis principal y secundario de cada clúster en una configuración de MetroCluster:

   ```
   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
   cluster1

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

   cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
   -scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
   cluster2
   ```

2. Compruebe que el grupo de escáneres está activo:

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

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

   El siguiente comando muestra los detalles del grupo de escáneres `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                               Scanner Pool: pool1_for_site1
                             Applied Policy: primary
                             Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                   Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

Puede utilizar el `vserver vscan scanner-pool show-active` Comando para ver los pools de análisis activos en una SVM. Para obtener una sintaxis de comando completa, consulte la página de manual del comando.

Comandos para administrar grupos de escáneres

Puede modificar y eliminar grupos de escáneres y administrar usuarios con privilegios y servidores Vscan para un grupo de escáneres. También puede ver información resumida sobre el conjunto de escáneres.

Si desea…	Introduzca el siguiente comando…
Modificar un grupo de escáneres	`vserver vscan scanner-pool modify`
Eliminar un grupo de escáneres	`vserver vscan scanner-pool delete`
Agregar usuarios con privilegios a un grupo de escáneres	`vserver vscan scanner-pool privileged-users add`
Eliminar usuarios con privilegios de un grupo de escáneres	`vserver vscan scanner-pool privileged-users remove`
Agregue servidores Vscan a un grupo de escáneres	`vserver vscan scanner-pool servers add`
Eliminar servidores Vscan de un grupo de escáneres	`vserver vscan scanner-pool servers remove`
Ver resumen y detalles de un grupo de escáneres	`vserver vscan scanner-pool show`
Ver usuarios con privilegios para un grupo de escáneres	`vserver vscan scanner-pool privileged-users show`

Vea los servidores Vscan de todos los grupos de escáneres	`vserver vscan scanner-pool servers show`

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

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.

Configurar el análisis bajo demanda

Configurar la descripción general del análisis bajo demanda

Puede utilizar el análisis bajo demanda para comprobar los archivos en busca de virus de forma inmediata o programada.

Puede que desee ejecutar análisis sólo en horas de menor actividad, por ejemplo, o puede que desee analizar archivos muy grandes que se excluyeron de un análisis en tiempo real. Puede utilizar una programación cron para especificar cuándo se ejecuta la tarea.

Acerca de este tema

- Puede asignar una programación al crear una tarea.
- Solo se puede programar una tarea a la vez en un SVM.
- El análisis bajo demanda no admite el análisis de enlaces simbólicos o archivos de flujo.

El análisis bajo demanda no admite el análisis de enlaces simbólicos o archivos de flujo.

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.

Crear una tarea bajo demanda

Una tarea a petición define el alcance de la exploración de virus a petición. Puede especificar el tamaño máximo de los archivos que se van a analizar, las extensiones y rutas de acceso de los archivos que se van a incluir en el análisis, así como las extensiones y rutas de acceso de los archivos que se van a excluir del análisis. Los archivos de los subdirectorios se analizan de forma predeterminada.

Acerca de esta tarea

- Puede haber un máximo de diez (10) tareas bajo demanda para cada SVM, pero solo una puede estar activa.
- Una tarea a petición crea un informe, que contiene información sobre las estadísticas relacionadas con las exploraciones. Se puede acceder a este informe con un comando o descargando el archivo de informe creado por la tarea en la ubicación definida.

Antes de empezar

- Debe tener se ha creado una política de acceso. La política puede ser una predeterminada o creada por el usuario. Sin la política de acceso, no puede activar el análisis.

Pasos

1. Crear una tarea bajo demanda:

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
-no-ext true|false -directory-recursion true|false
```

- 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.

  Para obtener una lista completa de opciones, consulte "referencia de comandos".

  El siguiente comando crea una tarea bajo demanda denominada `Task1` En el `VS1`SVM:

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

> Puede utilizar el `job show` comando para ver el estado del trabajo. Puede utilizar el `job pause` y.. `job resume` comandos para pausar y reiniciar el trabajo o el `job stop` comando para finalizar el trabajo.

2. Compruebe que la tarea bajo demanda se ha creado:

   ```
   vserver vscan on-demand-task show -instance data_SVM -task-name task_name
   ```

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

   El siguiente comando muestra los detalles de `Task1` tarea:

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

Después de terminar

Debe habilitar el análisis en la SVM antes de que se ejecute la tarea programada.

Programar una tarea bajo demanda

Puede crear una tarea sin asignar una programación y utilizar el `vserver vscan on-demand-task schedule` comando para asignar una programación o agregar una programación al crear la tarea.

Acerca de esta tarea

La programación asignada con `vserver vscan on-demand-task schedule` el comando anula una programación que ya se ha asignado con el `vserver vscan on-demand-task create` comando.

Pasos

1. Programar una tarea bajo demanda:

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   El siguiente comando programa una tarea en tiempo de acceso denominada `Task2` en la `vs2` SVM:

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

Para ver el estado del trabajo, utilice `job show` comando. La `job pause` y.. `job resume` comandos, pausar y reiniciar respectivamente el trabajo; el `job stop` el comando finaliza el trabajo.

2. Compruebe que la tarea bajo demanda se ha programado:

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

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

   El siguiente comando muestra los detalles de `Task 2` tarea:

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                           Vserver: vs2
                         Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
             Report Directory Path: /report
                      Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
            File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
```

Después de terminar

Debe habilitar el análisis en la SVM antes de que se ejecute la tarea programada.

Ejecute una tarea bajo demanda de inmediato

Puede ejecutar una tarea bajo demanda inmediatamente, independientemente de que haya asignado una programación.

Antes de empezar

Debe haber habilitado el análisis en la SVM.

Paso

1. Ejecute una tarea bajo demanda de inmediato:

   `vserver vscan on-demand-task run -vserver` *`data_SVM`* `-task-name` *`task_name`*

   El siguiente comando ejecuta una tarea en tiempo de acceso llamada `Task1` en la `vs1` SVM:

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

> Puede utilizar el `job show` comando para ver el estado del trabajo. Puede utilizar el `job pause` y.. `job resume` comandos para pausar y reiniciar el trabajo o el `job stop` comando para finalizar el trabajo.

Comandos para gestionar tareas bajo demanda

Puede modificar, eliminar o desprogramar una tarea bajo demanda. Puede ver un resumen y detalles de la tarea, así como administrar informes para la tarea.

Si desea…	Introduzca el siguiente comando…
Crear una tarea bajo demanda	`vserver vscan on-demand-task create`
Modifique una tarea bajo demanda	`vserver vscan on-demand-task modify`
Eliminar una tarea bajo demanda	`vserver vscan on-demand-task delete`
Ejecute una tarea bajo demanda	`vserver vscan on-demand-task run`
Programar una tarea bajo demanda	`vserver vscan on-demand-task schedule`
Desprogramar una tarea bajo demanda	`vserver vscan on-demand-task unschedule`
Vea el resumen y los detalles de una tarea bajo demanda	`vserver vscan on-demand-task show`
Ver informes bajo demanda	`vserver vscan on-demand-task report show`
Eliminar informes bajo demanda	`vserver vscan on-demand-task report delete`

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

Prácticas recomendadas para configurar la funcionalidad antivirus externa en ONTAP

Tenga en cuenta las siguientes recomendaciones para configurar la funcionalidad de configuración en ONTAP.

- Restringir a los usuarios con privilegios a las operaciones de exploración de virus. Los usuarios normales no deben utilizar credenciales de usuario con privilegios. Esta restricción se puede lograr desactivando los derechos de inicio de sesión para los usuarios con privilegios en Active Directory.
- No es necesario que los usuarios con privilegios formen parte de ningún grupo de usuarios que tenga un gran número de derechos en el dominio, como el grupo de administradores o el grupo de operadores de copia de seguridad. Sólo el sistema de almacenamiento debe validar los usuarios con privilegios para que puedan crear conexiones de servidor Vscan y acceder a archivos para análisis de virus.
- Utilice los equipos que ejecutan servidores Vscan solo para fines de detección de virus. Para desalentar el uso general, desactive los servicios de terminal de Windows y otras disposiciones de acceso remoto en estas máquinas, y otorgue el derecho de instalar nuevo software en estas máquinas solo a los administradores.
- Dedicar los servidores Vscan a la detección de virus y no los utilice para otras operaciones, como las copias de seguridad. Puede decidir ejecutar el servidor Vscan como una máquina virtual (VM). Si ejecuta el servidor Vscan como equipo virtual, asegúrese de que los recursos asignados a la máquina virtual no se comparten y son suficientes para realizar análisis de virus.
- Proporcione una capacidad adecuada de CPU, memoria y disco al servidor Vscan para evitar la asignación excesiva de recursos. La mayoría de los servidores Vscan están diseñados para usar varios servidores principales de CPU y para distribuir la carga entre las CPU.
- NetApp recomienda utilizar una red dedicada con una VLAN privada para la conexión desde la SVM al servidor Vscan para que el tráfico de análisis no se vea afectado por otro tráfico de red del cliente. Cree una tarjeta de interfaz de red (NIC) separada dedicada a la VLAN antivirus en el servidor Vscan y a las LIF de datos del SVM. Este paso simplifica la administración y la solución de problemas en caso de que surjan problemas de red. El tráfico antivirus debe segregarse mediante una red privada. El servidor antivirus debe configurarse para comunicarse con el controlador de dominio (DC) y ONTAP de una de las siguientes maneras:
  - El DC debe comunicarse con los servidores antivirus a través de la red privada que se utiliza para segregar el tráfico.
  - El servidor antivirus y DC deben comunicarse a través de una red diferente (no la red privada mencionada anteriormente), que no es la misma que la red de cliente CIFS.
  - Para habilitar la autenticación de Kerberos para la comunicación antivirus, cree una entrada DNS para las LIF privadas y un nombre principal de servicio en el DC correspondiente a la entrada de DNS creada para la LIF privada. Utilice este nombre cuando agregue una LIF al conector antivirus. El DNS debe ser capaz de devolver un nombre único para cada LIF privado conectado al conector antivirus.

Si la LIF para el tráfico de Vscan está configurada en un puerto distinto al de la LIF para el tráfico de cliente, la LIF Vscan puede conmutar por error a otro nodo si se produce un fallo de puerto. El cambio hace que el servidor Vscan no sea accesible desde el nuevo nodo y las notificaciones de escaneo para las operaciones de archivo en el nodo fallan. Compruebe que se puede acceder al servidor Vscan a través de al menos una LIF en un nodo para que pueda procesar solicitudes de análisis de operaciones de archivo realizadas en ese nodo.

- Conecte el sistema de almacenamiento de NetApp y el servidor Vscan utilizando al menos una red 1GbE.
- Para un entorno con varios servidores Vscan, conecte todos los servidores que tengan conexiones de red similares de alto rendimiento. La conexión de los servidores Vscan mejora el rendimiento al permitir el uso compartido de la carga.
- Para sitios remotos y sucursales, NetApp recomienda usar un servidor Vscan local en lugar de un servidor Vscan remoto porque el primero es un candidato perfecto para alta latencia. Si el costo es un factor, use un ordenador portátil o PC para una protección antivirus moderada. Puede programar análisis periódicos completos del sistema de archivos compartiendo los volúmenes o qtrees y analizándolos desde cualquier sistema del sitio remoto.
- Utilice varios servidores Vscan para analizar los datos de la SVM con fines de equilibrio de carga y redundancia. La cantidad de carga de trabajo CIFS y el tráfico antivirus resultante varían según la máquina virtual de almacenamiento. Supervisar la latencia de detección de virus y CIFS en la controladora de almacenamiento. Supervise la tendencia de los resultados a lo largo del tiempo. Si la latencia de CIFS y la latencia de análisis de virus aumentan debido a la CPU o las colas de aplicaciones en los servidores Vscan más allá de los umbrales de tendencias, es posible que los clientes CIFS experimenten largos tiempos de espera. Agregar servidores Vscan adicionales para distribuir la carga.
- Instale la última versión del conector antivirus de ONTAP.
- Mantenga actualizados los motores y definiciones antivirus. Consulte a los socios para obtener recomendaciones sobre la frecuencia con la que debe actualizar.
- En un entorno multi-tenancy, un pool de escáner (pool de servidores Vscan) se puede compartir con varias SVM siempre que los servidores Vscan y las SVM formen parte del mismo dominio o dominio de confianza.
- La política de software antivirus para los archivos infectados debe establecerse en “eliminar” o “cuarentena”, que es el valor predeterminado establecido por la mayoría de los proveedores de antivirus. Si vscan-fileop-profile se establece en “WRITE_ONLY”, y si se encuentra un archivo infectado, el archivo permanece en el recurso compartido y se puede abrir porque abrir un archivo no desencadena una exploración. El análisis antivirus solo se activa después de cerrar el archivo.
- La `scan-engine timeout` el valor debe ser menor que el `scanner-pool request-timeout` valor. Si se establece con un valor mayor, el acceso a los archivos podría retrasarse y podría agotarse el tiempo de espera en algún momento. Para evitarlo, configure la `scan-engine timeout` a 5 segundos menos que el `scanner-pool request-timeout` valor. Consulte la documentación del proveedor del motor de escaneo para obtener instrucciones sobre cómo cambiar el `scan-engine timeout` configuración. La `scanner-pool timeout` se puede cambiar utilizando el siguiente comando en modo avanzado y proporcionando el valor adecuado para el `request-timeout` parámetro: `vserver vscan scanner-pool modify`.
- En un entorno con un tamaño adecuado para cargas de trabajo de análisis de acceso y que requiera el uso de análisis bajo demanda, NetApp recomienda programar el trabajo de análisis bajo demanda en horas de menor actividad para evitar cargas adicionales en la infraestructura antivirus existente.

Obtenga más información sobre las prácticas recomendadas específicas para los partners en "Soluciones de partners de VSCAN".

Habilite la detección de virus en un SVM

Es necesario habilitar el análisis de virus en una SVM para que se pueda ejecutar un análisis bajo demanda o en tiempo real.

Pasos

1. Habilitar la detección de virus en una SVM:

   `vserver vscan enable -vserver data_SVM`

   > Puede utilizar el `vserver vscan disable` comando para desactivar la detección de virus, si es necesario.

   El siguiente comando habilita el análisis de virus en `vs1` SVM:

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. Compruebe que la detección de virus está habilitada en la SVM:

   `vserver vscan show -vserver data_SVM`

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

   El siguiente comando muestra el estado de Vscan del `vs1` SVM:

   ```
   cluster1::> vserver vscan show -vserver vs1

                               Vserver: vs1
                          Vscan Status: on
   ```

Restablece el estado de los archivos capturados

En ocasiones, es posible que desee restablecer el estado de análisis de los archivos analizados correctamente en una SVM mediante el `vserver vscan reset` comando para descartar la información almacenada en caché para los archivos. Es posible que desee utilizar este comando para reiniciar el procesamiento de análisis de virus en caso de un análisis mal configurado, por ejemplo.

Acerca de esta tarea

Después de ejecutar el `vserver vscan reset` comando, todos los archivos elegibles se analizarán la próxima vez que se acceda a ellos.

> Este comando puede afectar negativamente al rendimiento, dependiendo del número y el tamaño de los archivos que se van a volver a analizar.

Antes de empezar

Se requieren privilegios avanzados para esta tarea.

Pasos

1. Cambie al nivel de privilegio avanzado:

   `set -privilege advanced`

2. Restablecer el estado de los archivos capturados:

   `vserver vscan reset -vserver data_SVM`

   El siguiente comando restablece el estado de los archivos capturados en `vs1` SVM:

```
cluster1::> vserver vscan reset -vserver vs1
```

Ver la información del registro de eventos de Vscan

Puede utilizar el `vserver vscan show-events` Comando para ver información de registro de eventos sobre archivos infectados, actualizaciones en servidores Vscan y similares. Puede ver información sobre eventos del clúster o de los nodos, SVM o servidores Vscan.

Antes de empezar

Se necesitan privilegios avanzados para ver el registro de eventos Vscan.

Pasos

1. Cambie al nivel de privilegio avanzado:

   `set -privilege advanced`

2. Ver información del registro de eventos de Vscan:

   `vserver vscan show-events`

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

   El siguiente comando muestra información del registro de eventos para el clúster `cluster1`:

```
cluster1::*> vserver vscan show-events

Vserver     Node            Server          Event Type        Event Time
----------- --------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected     9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated   9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

Supervise y solucione problemas de conectividad

Posibles problemas de conectividad relacionados con la opción de adquisición obligatoria

Puede utilizar el `vserver vscan connection-status show` Comandos para ver información acerca de las conexiones del servidor Vscan que puede resultar útil para solucionar problemas de conectividad.

De forma predeterminada, la `scan-mandatory` La opción para el análisis en tiempo real deniega el acceso a archivos cuando no hay disponible una conexión de servidor Vscan para el análisis. Aunque esta opción ofrece importantes funciones de seguridad, puede dar lugar a problemas en algunas situaciones.

- Antes de habilitar el acceso de cliente, debe asegurarse de que al menos un servidor Vscan esté conectado a una SVM en cada nodo que tenga una LIF. Si necesita conectar servidores a las SVM después de habilitar el acceso de cliente, debe desactivar el `scan-mandatory` Opción en la SVM para asegurarse de que no se deniega el acceso al archivo porque no hay una conexión de servidor Vscan disponible. Puede volver a activar la opción después de haber conectado el servidor.
- Si un LIF de destino aloja todas las conexiones del servidor Vscan para una SVM, la conexión entre el servidor y la SVM se perderá si se migra el LIF. Para asegurarse de que no se deniega el acceso a los archivos porque no hay una conexión de servidor Vscan disponible, debe desactivar el `scan-mandatory` Opción antes de migrar la LIF. Puede volver a activar la opción después de migrar el LIF.

Cada SVM debe tener al menos dos servidores Vscan asignados. Se recomienda conectar los servidores Vscan al sistema de almacenamiento a través de una red diferente a la utilizada para el acceso de los clientes.

Comandos para ver el estado de conexión del servidor Vscan

Puede utilizar el `vserver vscan connection-status show` Comandos para ver información resumida y detallada acerca del estado de conexión del servidor Vscan.

Si desea…	Introduzca el siguiente comando…
Ver un resumen de las conexiones del servidor Vscan	`vserver vscan connection-status show`
Ver detalles de las conexiones del servidor Vscan	`vserver vscan connection-status show-all`
Ver detalles de los servidores Vscan conectados	`vserver vscan connection-status show-connected`
Ver detalles de los servidores Vscan disponibles que no están conectados	`vserver vscan connection-status show-not-connected`

Para obtener más información sobre estos comandos, consulte "Páginas manuales de ONTAP".

Solucionar problemas de detección de virus

Para los problemas comunes de detección de virus, existen posibles causas y formas de resolverlos. La detección de virus también se conoce como Vscan.

Problema	Cómo resolverlo
Los servidores Vscan no se pueden conectar El sistema de almacenamiento Clustered ONTAP de NetApp.	Compruebe si la configuración del grupo de escáner especifica la dirección IP del servidor Vscan. Compruebe también si los usuarios con privilegios permitidos en la lista de grupos de escáneres están activos. Para comprobar el conjunto de escáneres, ejecute el `vserver vscan scanner-pool show` comando en el símbolo del sistema de almacenamiento. Si los servidores Vscan siguen sin poder conectarse, es posible que haya un problema con la red.
Los clientes observan una alta latencia.	Probablemente sea el momento de agregar más servidores Vscan al grupo de escáneres.
Se activan demasiadas adquisiciones.	Modifique el valor de `vscan-fileop-profile` parámetro que permite restringir el número de operaciones de archivos supervisadas para el análisis de virus.
Algunos archivos no se están escaneando.	Compruebe la política de acceso. Es posible que la ruta de acceso de estos archivos se haya agregado a la lista de exclusión de ruta de acceso o que su tamaño supere el valor configurado para las exclusiones. Para comprobar la política de acceso, ejecute `vserver vscan on-access-policy show` comando en el símbolo del sistema de almacenamiento.
Se ha denegado el acceso al archivo.	Compruebe si el valor *scan-mandatory* está especificado en la configuración de la política. Esta opción deniega el acceso a los datos si no hay servidores Vscan conectados. Modifique la configuración según sea necesario.

Supervise el estado y las actividades de rendimiento

Puede supervisar los aspectos críticos del módulo Vscan, como el estado de conexión del servidor Vscan, El estado de los servidores Vscan y el número de archivos que se han analizado. Esta información ayuda Diagnostique problemas relacionados con el servidor Vscan.

Ver información de conexión del servidor Vscan

Puede ver el estado de conexión de los servidores Vscan para gestionar las conexiones que ya están en uso y las conexiones disponibles para su uso. Varios comandos muestran información Acerca del estado de conexión de los servidores Vscan.

Comando…	Información mostrada…
`vserver vscan connection-status show`	Resumen del estado de conexión
`vserver vscan connection-status show-all`	Información detallada sobre el estado de la conexión
`vserver vscan connection-status show-not-connected`	Estado de las conexiones disponibles pero no conectadas
`vserver vscan connection-status show-connected`	Información sobre el servidor Vscan conectado

Para obtener más información sobre estos comandos, consulte "Referencia de comandos de la ONTAP".

Ver estadísticas del servidor Vscan

Puede ver estadísticas específicas del servidor Vscan para supervisar el rendimiento y diagnosticar problemas relacionados con detección de virus. Debe recopilar una muestra de datos para poder utilizar el `statistics show` comando a. Mostrar las estadísticas del servidor Vscan. Para completar una muestra de datos, realice el siguiente paso:

Paso

1. Ejecute el `statistics start` y la `optional statistics` comando stop.

Ver estadísticas de las solicitudes y latencias del servidor Vscan

Puede usar ONTAP `offbox_vscan` Contadores por SVM para supervisar la tasa de Vscan Las solicitudes de servidor que se envían y reciben por segundo y las latencias de los servidores en todas las secuencias virtuales servidores. Para ver estas estadísticas, realice el siguiente paso:

Paso

1. Ejecute el resultado de estadísticas `object offbox_vscan –instance SVM` con el siguientes contadores:

Contador…	Información mostrada…
`scan_request_dispatched_rate`	Número de solicitudes de detección de virus enviadas desde ONTAP a los servidores Vscan por segundo
`scan_noti_received_rate`	Número de solicitudes de detección de virus recibidas por ONTAP desde los servidores Vscan por segundo

`dispatch_latency`	Latencia dentro de ONTAP para identificar un servidor Vscan disponible y enviar la solicitud a ese servidor Vscan
`scan_latency`	Latencia de ida y vuelta desde ONTAP al servidor Vscan, incluido el tiempo para que se ejecute el análisis

Ejemplo de estadísticas generadas a partir de un contador de vscan del buzón de ONTAP

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

Vea estadísticas de solicitudes y latencias de servidores Vscan individuales

Puede usar ONTAP `offbox_vscan_server` Contadores en un servidor Vscan por SVM, por cada servidor Vscan externo, Y por nodo para supervisar la tasa de solicitudes de servidor Vscan enviadas y la latencia del servidor activada Cada servidor Vscan individualmente. Para recopilar esta información, realice el siguiente paso:

Paso

1. Ejecute el `statistics show –object offbox_vscan –instance SVM:servername:nodename` comando con los siguientes contadores:

Contador…	Información mostrada…
`scan_request_dispatched_rate`	Número de solicitudes de detección de virus enviadas desde ONTAP
`scan_latency`	Latencia de ida y vuelta desde ONTAP al servidor Vscan, incluido el tiempo para que se ejecute el análisis A los servidores Vscan por segundo

Ejemplo de estadísticas generadas a partir de un contador ONTAP offbox_vscan_server

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-------------------------------------------------------------------
```

Ver estadísticas para el uso del servidor Vscan

También puede utilizar ONTAP `offbox_vscan_server` Contadores para recopilar la utilización del servidor Vscan estadísticas. Estas estadísticas se realizan para cada SVM, cada servidor Vscan externo, y por nodo. Ellos Incluya el uso de CPU en el servidor Vscan, la profundidad de cola para las operaciones de escaneo en el servidor Vscan (actual y máximo), memoria usada y red usada. Estas estadísticas son reenviadas por el conector antivirus a los contadores de estadísticas dentro de ONTAP. Ellos se basan en datos sondeados cada 20 segundos y deben recopilarse varias veces para obtener precisión; de lo contrario, los valores que se muestran en las estadísticas solo reflejan el último sondeo. La utilización de CPU y las colas son particularmente importante para monitorear y analizar. Un valor alto para una cola promedio puede indicar que el El servidor VSCAN tiene un cuello de botella. Para recopilar estadísticas de uso para el servidor Vscan en un servidor Vscan por SVM, por servidor Vscan externo y por nodo base, complete el siguiente paso:

Paso

1. Recopilar estadísticas de utilización del servidor Vscan

   Ejecute el `statistics show –object offbox_vscan_server –instance SVM:servername:nodename` comando con lo siguiente `offbox_vscan_server` contadores:

Contador…	Información mostrada…
`scanner_stats_pct_cpu_used`	Uso de CPU en el servidor Vscan
`scanner_stats_pct_input_queue_avg`	Cola media de solicitudes de exploración en el servidor Vscan
`scanner_stats_pct_input_queue_hiwaterma rk`	Cola pico de solicitudes de exploración en el servidor Vscan
`scanner_stats_pct_mem_used`	Memoria utilizada en el servidor Vscan
`scanner_stats_pct_network_used`	Red utilizada en el servidor Vscan

Ejemplo de estadísticas de utilización para el servidor Vscan

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

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.