Instalación y configuración del servidor VSCAN

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

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.