Utilice la firma SMB para mejorar la seguridad de la red

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Utilice la firma SMB para mejorar la seguridad de la red

Obtenga más información sobre el uso de la firma SMB de ONTAP para mejorar la seguridad de la red

La firma SMB ayuda a garantizar que el tráfico de red entre el servidor SMB y el cliente no se vea comprometido; esto evita los ataques de repetición. De forma predeterminada, ONTAP admite la firma SMB cuando lo solicita el cliente. De manera opcional, el administrador de almacenamiento puede configurar el servidor SMB para que requiera la firma SMB.

Conozca cómo las políticas de firma afectan a la comunicación con servidores SMB de ONTAP

Además de la configuración de seguridad de firma SMB del servidor CIFS, dos políticas de firma SMB en clientes de Windows controlan la firma digital de las comunicaciones entre clientes y el servidor CIFS. Puede configurar el ajuste que cumpla con sus requisitos empresariales.

Las directivas SMB de cliente se controlan a través de la configuración de la directiva de seguridad local de Windows, que se configuran mediante Microsoft Management Console (MMC) o los GPO de Active Directory. Para obtener más información acerca de los problemas de firma SMB de cliente y de seguridad, consulte la documentación de Microsoft Windows.

A continuación, se muestran descripciones de las dos políticas de firma SMB en los clientes de Microsoft:

- `Microsoft network client: Digitally sign communications (if server agrees)`

  Esta configuración controla si la capacidad de firma SMB del cliente está habilitada. Está activado de forma predeterminada. Cuando se deshabilita esta configuración en el cliente, las comunicaciones del cliente con el servidor CIFS dependen de la configuración de firma SMB en el servidor CIFS.

- `Microsoft network client: Digitally sign communications (always)`

  Esta configuración controla si el cliente requiere la firma SMB para comunicarse con un servidor. Está desactivado de forma predeterminada. Cuando esta configuración está deshabilitada en el cliente, el comportamiento de la firma SMB se basa en la configuración de la política `Microsoft network client: Digitally sign communications (if server agrees)` y del servidor CIFS.

> ⓘ Si el entorno incluye clientes de Windows configurados para requerir la firma SMB, debe habilitar la firma SMB en el servidor CIFS. Si no lo hace, el servidor CIFS no puede proporcionar datos a estos sistemas.

Los resultados efectivos de la configuración de firma SMB del cliente y del servidor CIFS dependen de si las sesiones SMB utilizan SMB 1.0 o SMB 2.x y versiones posteriores.

En la tabla siguiente se resume el comportamiento efectivo de la firma SMB si la sesión utiliza SMB 1.0:

Cliente	No se requiere firma con ONTAP	Se requiere firma ONTAP
Firma desactivada y no requerida	No firmado	Firmado
Firma habilitada y no requerida	No firmado	Firmado
Firma desactivada y obligatoria	Firmado	Firmado
Firma habilitada y requerida	Firmado	Firmado

Es posible que los clientes Windows SMB 1 anteriores y algunos clientes SMB 1 distintos de Windows no puedan conectarse si la firma está deshabilitada en el cliente, pero es necesaria en el servidor CIFS.

En la tabla siguiente se resume el comportamiento efectivo de la firma SMB si la sesión utiliza SMB 2.x o SMB 3.0:

Para los clientes SMB 2.x y SMB 3.0, la firma SMB siempre está habilitada. No se puede deshabilitar.

Cliente	No se requiere firma con ONTAP	Se requiere firma ONTAP
No se requiere firma	No firmado	Firmado
Se requiere firma	Firmado	Firmado

En la tabla siguiente se resume el comportamiento de firma SMB de servidor y cliente de Microsoft predeterminado:

Protocolo	Algoritmo hash	Puede activar/desactivar	Se puede requerir o no se puede requerir	Valor predeterminado del cliente	Valor predeterminado del servidor	DC predeterminado
SMB 1,0	MD5	Sí	Sí	Habilitado (no es necesario)	Deshabilitado (no obligatorio)	Obligatorio
SMB 2.x	HMAC SHA-256	No	Sí	No es obligatorio	No es obligatorio	Obligatorio
SMB 3,0	AES-CMAC.	No	Sí	No es obligatorio	No es obligatorio	Obligatorio

Microsoft ya no recomienda utilizar `Digitally sign communications (if client agrees)` `Digitally sign communications (if server agrees)` la configuración de directiva de grupo o. Microsoft ya no recomienda utilizar `EnableSecuritySignature` la configuración del Registro. Estas opciones solo afectan al comportamiento de SMB 1 y se pueden reemplazar por la `Digitally sign communications (always)` configuración de directiva de grupo o la `RequireSecuritySignature` configuración del registro. También puede obtener más información en el blog de Microsoft.Conceptos básicos de The para la firma de SMB (cubriendo tanto SMB1 como SMB2)

Conozca el impacto en el rendimiento de la firma SMB de ONTAP

Cuando las sesiones SMB utilizan la firma SMB, todas las comunicaciones SMB a y desde clientes de Windows experimentan un impacto en el rendimiento, lo cual afecta tanto a los clientes como al servidor (es decir, los nodos del clúster que ejecuta la SVM que contiene el servidor SMB).

El impacto en el rendimiento muestra que el uso de CPU ha aumentado tanto en los clientes como en el servidor, aunque la cantidad de tráfico de red no cambia.

La magnitud del impacto en el rendimiento depende de la versión de ONTAP 9 que esté ejecutando. A partir de ONTAP 9.7, un nuevo algoritmo de descarga del cifrado puede permitir un mejor rendimiento en el tráfico de SMB firmado. La descarga de firma SMB se habilita de forma predeterminada cuando se habilita la firma SMB.

El rendimiento mejorado de la firma SMB requiere la funcionalidad de descarga de AES-ni. Consulte el Hardware Universe (HWU) para verificar que la descarga AES-ni es compatible con su plataforma.

Otras mejoras de rendimiento también son posibles si usted es capaz de utilizar SMB versión 3,11 que admite el algoritmo GCM mucho más rápido.

Según la red, la versión de ONTAP 9, la versión de SMB y la implementación de SVM, el impacto en el rendimiento de la firma SMB puede variar enormemente; puede verificarlo únicamente mediante pruebas en el entorno de red.

La mayoría de los clientes de Windows negocian la firma SMB de forma predeterminada si está habilitada en el servidor. Si necesita protección SMB para algunos de sus clientes Windows y la firma SMB está provocando problemas de rendimiento, puede deshabilitar la firma SMB en cualquiera de sus clientes Windows que no necesiten protección contra ataques de repetición. Para obtener información sobre cómo deshabilitar la firma SMB en clientes Windows, consulte la documentación de Microsoft Windows.

Recomendaciones de configuración de firma SMB de ONTAP

Puede configurar un comportamiento de firma SMB entre clientes SMB y el servidor CIFS para satisfacer sus requisitos de seguridad. La configuración que elija al configurar la firma SMB en el servidor CIFS depende de cuáles sean sus requisitos de seguridad.

Es posible configurar la firma SMB en el cliente o en el servidor CIFS. Tenga en cuenta las siguientes recomendaciones al configurar la firma SMB:

Si…	Recomendación…
Desea aumentar la seguridad de la comunicación entre el cliente y el servidor	Haga que se requiera la firma SMB en el cliente habilitando `Require Option (Sign always)` la configuración de seguridad en el cliente.
Es conveniente que todo el tráfico de SMB esté firmado a una determinada máquina virtual de almacenamiento (SVM)	Para requerir la firma SMB en el servidor CIFS, configure la configuración de seguridad para requerir la firma SMB.

Consulte la documentación de Microsoft para obtener más información acerca de la configuración de la seguridad del cliente de Windows.

Obtenga información sobre la configuración de firma SMB de ONTAP para varias LIFS de datos

Si habilita o deshabilita la firma SMB requerida en el servidor SMB, debe tener en cuenta las directrices para varias configuraciones de LIF de datos para una SVM.

Cuando configura un servidor SMB, puede haber varios LIF de datos configurados. Si es así, el servidor DNS contiene varias `A` entradas de registro para el servidor CIFS, todos utilizando el mismo nombre de host del servidor SMB, pero cada uno con una dirección IP exclusiva. Por ejemplo, un servidor SMB que tiene dos LIF de datos configuradas puede tener las siguientes `A` entradas de registro DNS:

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

El comportamiento normal es que, al cambiar la configuración de firma SMB necesaria, solo las nuevas conexiones de clientes se ven afectadas por el cambio en la configuración de firma SMB. Sin embargo, hay una excepción a este comportamiento. Existe un caso en el que un cliente tiene una conexión existente con un recurso compartido y éste crea una nueva conexión con el mismo recurso compartido después de cambiar la configuración, manteniendo la conexión original. En este caso, tanto la conexión SMB nueva como la existente adoptan los nuevos requisitos de firma SMB.

Observe el siguiente ejemplo:

1. CLIENT1 se conecta a un recurso compartido sin necesidad de firma SMB mediante la ruta de acceso `O:\`.
2. El administrador de almacenamiento modifica la configuración del servidor SMB para requerir la firma SMB.
3. CLIENT1 se conecta al mismo recurso compartido con la firma SMB necesaria mediante la ruta de acceso `S:\` (manteniendo la conexión mediante la ruta `O:\`).
4. El resultado es que se utiliza la firma SMB cuando se accede a los datos `O:\` en `S:\` las unidades y.

Configure la firma ONTAP para el tráfico SMB entrante

Puede aplicar el requisito de que los clientes firmen mensajes SMB habilitando la firma

SMB requerida. Si está habilitada, ONTAP solo acepta mensajes SMB si tienen firmas válidas. Si desea permitir la firma SMB, pero no la requiere, puede deshabilitar la firma SMB requerida.

Acerca de esta tarea

De manera predeterminada, la firma SMB requerida está deshabilitada. Es posible habilitar o deshabilitar la firma SMB requerida en cualquier momento.

La firma SMB no está deshabilitada de forma predeterminada en las siguientes circunstancias:

1. La firma SMB necesaria está habilitada y el clúster se revierte a una versión de ONTAP que no admite la firma SMB.
2. Posteriormente, el clúster se actualiza a una versión de ONTAP que admite la firma SMB.

   En estas circunstancias, la configuración de firma SMB configurada originalmente en una versión compatible de ONTAP se conserva mediante la reversión y la posterior actualización.

Cuando se configura una relación de recuperación ante desastres de una máquina virtual de almacenamiento (SVM), el valor que se selecciona para `-identity-preserve` la opción del `snapmirror create` comando determina los detalles de configuración que se replican en la SVM de destino.

Si establece `-identity-preserve` la opción en `true` (ID-preserve), la configuración de seguridad de firma SMB se replica en el destino.

Si establece `-identity-preserve` la opción en `false` (non-ID-preserve), la configuración de seguridad de firma SMB no se replica en el destino. En este caso, la configuración de seguridad del servidor CIFS en el destino se establece en los valores predeterminados. Si habilitó la firma SMB requerida en la SVM de origen, debe habilitar manualmente la firma SMB requerida en la SVM de destino.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea que la firma SMB sea…	Introduzca el comando…
Activado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
Deshabilitado	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. Compruebe que la firma SMB necesaria esté habilitada o deshabilitada; para ello, determine si el valor del `Is Signing Required` campo de la salida del siguiente comando está establecido en el valor deseado: `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

Ejemplo

En el siguiente ejemplo, se habilita la firma SMB requerida para SVM vs1:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

Los cambios en la configuración de cifrado surten efecto para las nuevas conexiones. Las conexiones existentes no se ven afectadas.

Información relacionada

- "snapmirror create"

Determinar si las sesiones SMB de ONTAP están firmadas

Puede ver información sobre las sesiones SMB conectadas en el servidor CIFS. Puede usar esta información para determinar si las sesiones SMB están firmadas. Esto puede resultar útil para determinar si las sesiones de cliente SMB se conectan con la configuración de seguridad deseada.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea mostrar información acerca de…	Introduzca el comando…
Todas las sesiones firmados en una máquina virtual de almacenamiento (SVM) específica	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
Detalles de una sesión firmada con un ID de sesión específico en la SVM	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

Ejemplos

El siguiente comando muestra información de sesión sobre las sesiones firmadas en la SVM vs1. El resultado de resumen predeterminado no muestra el campo de salida "'is Session Signed'":

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe          2          23s
```

El siguiente comando muestra información detallada de sesión, incluido si la sesión está firmada, en una sesión SMB con un ID de sesión de 2:

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                        Node: node1
                     Vserver: vs1
                  Session ID: 2
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                 Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

Información relacionada

Supervisar estadísticas de sesión firmada por SMB

Supervisar las estadísticas de sesión firmadas por SMB de ONTAP

Es posible supervisar las estadísticas de sesiones SMB y determinar qué sesiones establecidas se han firmado y cuáles no.

Acerca de esta tarea

`statistics`El comando en el nivel de privilegio avanzado proporciona `signed_sessions` el contador que se puede utilizar para supervisar el número de sesiones SMB firmadas. El `signed_sessions` contador está disponible con los siguientes objetos de estadísticas:

- `cifs` Permite supervisar la firma SMB para todas las sesiones de SMB.
- `smb1` Permite supervisar la firma SMB para sesiones SMB 1,0.
- `smb2` Permite supervisar la firma SMB para sesiones SMB 2.x y SMB 3,0.

  Las estadísticas de SMB 3,0 se incluyen en la salida del `smb2` objeto.

Si desea comparar el Núm. De sesiones firmadas con el Núm. Total de sesiones, puede comparar la salida del `signed_sessions` contador con la salida del `established_sessions` contador.

Debe iniciar una colección de ejemplos de estadísticas para poder ver los datos resultantes. Puede ver los datos de la muestra si no detiene la recopilación de datos. Al detener la recopilación de datos, se proporciona una muestra fija. No detener la recopilación de datos le ofrece la posibilidad de obtener datos actualizados que puede utilizar para compararlos con consultas anteriores. La comparación puede ayudarle a identificar tendencias.

Pasos

1. Establezca el nivel de privilegio en AVANZADO:
   `set -privilege advanced`
2. Iniciar una recopilación de datos:
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   Si no se especifica `-sample-id` el parámetro, el comando genera un identificador de muestra para usted y define esta muestra como la muestra predeterminada de la sesión CLI. El valor para `-sample-id` es una cadena de texto. Si ejecuta este comando durante la misma sesión de la CLI y no se especifica `-sample-id` el parámetro, el comando sobrescribe la muestra predeterminada anterior.

   Opcionalmente, puede especificar el nodo en el que se desea recoger estadísticas. Si no especifica el nodo, la muestra recopila estadísticas para todos los nodos del clúster.

   Obtenga más información sobre `statistics start` en el "Referencia de comandos del ONTAP".
3. Utilice `statistics stop` el comando para detener la recogida de datos para la muestra.

   Obtenga más información sobre `statistics stop` en el "Referencia de comandos del ONTAP" .
4. Ver estadísticas de firma SMB:

Si desea ver información acerca de…	Introduzca…
Sesiones firmadas	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	Sesiones firmadas y sesiones establecidas
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

Si desea mostrar información de un solo nodo, especifique el `-node` parámetro opcional.

Obtenga más información sobre `statistics show` en el "Referencia de comandos del ONTAP".

5. Vuelva al nivel de privilegio de administrador:
`set -privilege admin`

Ejemplos

El siguiente ejemplo muestra cómo se pueden supervisar las estadísticas de firma de SMB 2.x y SMB 3.0 en vs1 de la máquina virtual de almacenamiento (SVM).

El siguiente comando cambia al nivel de privilegio avanzado:

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

El siguiente comando inicia la recogida de datos de una nueva muestra:

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

El siguiente comando detiene la recogida de datos de la muestra:

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

El siguiente comando muestra sesiones SMB firmadas y sesiones SMB establecidas por nodo a partir de la muestra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

En el siguiente comando, se muestran las sesiones SMB firmadas para el nodo 2 en la muestra:

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

El siguiente comando vuelve a pasar al nivel de privilegios de administrador:

```
cluster1::*> set -privilege admin
```

Información relacionada

- Determinar si se han firmado las sesiones SMB
- "Información general sobre la gestión y el control del rendimiento"

Información de copyright

Información de la marca comercial