Administración de Sistemas y Redes

Server Message Block

Grupo: Ignacio Comin, Federico Greco, Rocio Penalva.

¿Qué es?

SMB (Server Message Block) es un protocolo de red de nivel de aplicación que opera sobre la capa de sesión del modelo OSI y está diseñado para proporcionar acceso compartido a archivos, impresoras, puertos serie y otros recursos dentro de una red. SMB permite a los nodos de una red (clientes) acceder a recursos alojados en otros nodos (servidores) como si fueran locales, facilitando así la interoperabilidad y la administración centralizada en redes corporativas o domésticas.

El protocolo SMB define un conjunto de comandos que permiten a las aplicaciones cliente realizar operaciones como lectura, escritura, creación, eliminación y modificación de archivos o directorios remotos, así como la administración de sesiones, autenticación de usuarios y control de acceso. También permite la interacción con servicios del servidor mediante la invocación remota de funciones (por ejemplo, en impresoras compartidas o procesos de comunicación entre sistemas).

SMB utiliza un modelo cliente-servidor y puede ejecutarse directamente sobre TCP/IP (puerto 445) o sobre NetBIOS (puertos 137–139). A partir de SMB 2.0, introducido con Windows Vista. Posteriormente, SMB 3.0, incluido con Windows 8 y Windows Server 2012, introdujo características avanzadas como cifrado de extremo a extremo, multicanal (uso simultáneo de múltiples conexiones TCP para mejorar el rendimiento y la tolerancia a fallos).

En entornos Windows, SMB está profundamente integrado con Active Directory y otros mecanismos de autenticación de Windows, lo que permite aplicar políticas de acceso y auditoría detalladas. Esta integración garantiza que solo los usuarios autenticados y autorizados puedan acceder a los recursos compartidos.

Originalmente desarrollado por IBM en 1983, SMB ha pasado por múltiples revisiones. Su adopción masiva comenzó con OS/2 LAN Manager y LAN Server, y más adelante fue incorporado en los sistemas operativos de Microsoft, siendo uno de los pilares de su infraestructura de red. Gracias a su compatibilidad hacia atrás, las versiones más recientes de SMB pueden interactuar con implementaciones más antiguas, facilitando la interoperabilidad entre distintos sistemas y versiones de Windows.

Historia

La primera vez que SMB salió al público fue en 1983, y ha habido varias adaptaciones del estándar de red, que se han registrado en las distintas versiones de protocolo, desde SMB 1.0 hasta la versión actual SMB 3.1.1, que Microsoft lanzó junto con Windows 10.

SMB 1.0 (CIFS)

SMB 1.0 es la versión original heredada de CIFS. En esta versión el cliente y servidor negocian dialectos y usan un encabezado NetBIOS de 4 bytes (longitud) antes del paquete SMB clásico. El encabezado SMB1 incluye campos como el “command” (byte), el estado, banderas de sesión, identificadores de árbol (TreeID) y de sesión (SessionID), etc. SMB1 soporta más de 100 comandos diferentes; por ejemplo, comandos para crear/leer archivos, consultas de información, locks, mail slots, etc. Las operaciones de archivo (read/write) estaban limitadas a tamaños relativamente pequeños (p. ej. ~64 KB).

En seguridad, SMB1 ofrecía autenticación a nivel de recurso compartido (contraseñas LAN Manager) o a nivel de usuario (NTLM v1/v2). Debido a su antigüedad y debilidades criptográficas, SMB1 tiene vulnerabilidades graves.

Casos de uso: SMB1 era usado históricamente para compartir directorios, impresoras y recursos de red en redes Windows antiguas. Hoy en día se evita salvo compatibilidad. Se usaba también para funciones como exploración de red (browsing) y mailslots.

Compatibilidad: Cualquier cliente SMB antiguo solo habla SMB1 y no puede usar SMB2/3. Esto obliga a habilitar SMB1 en servidores legacy si se requiere compatibilidad. Sin embargo, dejar SMB1 habilitado es un riesgo de seguridad. En resumen, SMB1 está obsoleto.

SMB 2.0 y 2.1

SMB 2.0 y 2.1 llegaron con Windows Vista/Server 2008 (SMB 2.0) y Windows 7/Server 2008 R2 (SMB 2.1). Estas versiones rediseñaron el protocolo para mejorar rendimiento y escalabilidad. Se redujo drásticamente el número de comandos y se agruparon muchas operaciones, disminuyendo el overhead. El encabezado SMB2 ocupa 64 bytes fijos. En SMB2 no se utilizan sobrecargas de NetBIOS; el protocolo se envía directamente sobre TCP 445.

Entre las mejoras de SMB 2.0 destacan: compounding (empaquetar múltiples operaciones en una sola petición de red) y lecturas/escrituras mayores, lo que aprovecha redes rápidas. Se añadieron handlares duraderos (durable handles) para permitir reconexiones tras cortes breves. También se mejoró la firma de mensajes, pasando de MD5 (SMB1) a HMAC-SHA256. Esto significa que las respuestas tienen mayor integridad sin degradar tanto la performance.

SMB 2.1 (Windows 7/2008R2) introdujo ajustes adicionales: por ejemplo, mejor soporte para BranchCache en entornos de oficina remota y optimizaciones de rendimiento (como tamaños de MTU ajustables). En esencia, SMB 2.1 mantiene las mismas bases que SMB 2.0 pero con refinamientos menores.

Casos de uso: SMB 2.x es la base para compartir archivos en casi todas las versiones de Windows desde Vista en adelante. Proporciona mejor experiencia en redes modernas, y fue requisito para muchas funcionalidades empresariales (clustering, discos duros virtuales vía SMB, etc.). Dado que SMB2.x carece de cifrado, se suele usar en redes internas seguras o junto con IPSec cuando se requiere confidencialidad.

SMB 3.0, 3.02, 3.1.1

SMB 3.0 (Windows 8/Server 2012) amplió SMB 2.x con muchas características de alto rendimiento y resiliencia. Introdujo funcionalidades clave para entornos de servidor: SMB Multichannel (agrupa múltiples rutas de red para aumentar ancho de banda y tolerancia a fallos) y SMB Direct (soporte RDMA para baja latencia y CPU reducida). Permitió conmutación por error transparente en clusters: los clientes se reconectan a otro nodo sin interrumpir procesos críticos. Se añadió escalabilidad horizontal: varios nodos de cluster pueden servir simultáneamente un recurso compartido SMB (mediante CSV v2). Se habilitaron nuevos contadores de rendimiento y cmdlets PowerShell específicos para gestión SMB. Además, SMB3.0 incorpora cifrado de extremo a extremo de forma nativa: usa AES-CCM (AES-128 en modo CTR+CMAC) para proteger los datos en tránsito sin requerir IPsec.

En SMB 3.0 también aparece la negociación segura de dialectos, que detecta intentos de downgrade malicioso durante el Handshake y aborta la conexión. Esta característica (basada en firmas de las primeras respuestas) evita ataques Man-in-the-Middle contra la negociación del protocolo. Además, SMB3.0 introdujo directory leasing (concesiones de directorio) para mejorar el rendimiento en entornos WAN, reduciendo los viajes de ida y vuelta para operaciones de directorio. En conjunto, SMB 3.0 ofrece un gran salto en desempeño y seguridad para almacenamiento empresarial.

SMB 3.02 (Windows 8.1/Server 2012 R2) añadió mejoras sobre SMB3.0. Destacan un balanceo de carga mejorado en clusters de escalabilidad horizontal: los clientes se dirigen al nodo con mejor acceso al volumen subyacente, reduciendo tráfico innecesario. Se optimizó la copia remota de archivos en WAN (mejor uso de CopyFile Chunking). Se mejoraron las pequeñas operaciones de I/O en SMB Direct para redes de 40–56 Gbps. Se

introdujo un límite de ancho de banda por categoría (tráfico de VM, migración en vivo, etc.) configurable con PowerShell. En resumen, SMB3.02 perfecciona el rendimiento y escalabilidad.

SMB 3.1.1 (Windows 10/Server 2016) agregó nuevas protecciones criptográficas. Introduce la integridad previa a la autenticación (“preauthentication integrity”), que es obligatoria. Esto permite detectar ataques que intenten manipular o degradar el protocolo durante los mensajes de Negotiate y Session Setup. Con hashing criptográfico de estas fases, cliente y servidor derivan las claves a prueba de manipulación. SMB3.1.1 también refina los algoritmos de cifrado y firma: En la práctica, SMB 3.1.1 ofrece el más alto nivel de seguridad del protocolo, protegiendo la negociación y permitiendo cifrar con suites avanzadas.

Casos de uso: Las versiones 3.x se emplean en entornos de alto rendimiento y disponibilidad. Por ejemplo, Hyper-V puede almacenar sus VHD y estados en recursos SMB 3.x compartidos, y SQL Server puede alojar bases de datos sobre SMB 3.x. SMB 3.0 en adelante es ideal para almacenamiento en clúster, volúmenes compartidos CSV y soluciones de almacenamiento definido por software. SMB 3.x con directory leasing y cifrado reduce latencias y protege datos contra espionaje en redes WAN.

Versión SMB	Soportada desde:	Nuevas Funciones
CIFS	Windows NT 4.0	Comunicación a través de la interfaz NetBIOS.
SMB 1.0	Windows 2000	Conexión directa a través de TCP.
SMB 2.0	Windows vista, Windows Server 2008, Samba 3.5	Varias mejoras de rendimiento, firma de mensajes mejorada, función de cache para las propiedades de archivo.
SMB 2.1	Windows 7, Windows Server 2008 R2	mecanismos de bloqueo.
SMB 3.0	Windows 8, Windows Server 2012, Samba 4.0	conexiones multicanal, cifrado de extremo a extremo, acceso a almacenamiento remoto.

SMB 3.0.2	Windows 8.1,Windows Server 2012 R2	
SMB 3.1.1	Windows 10, Windows Server 2016, Samba 4.3	Prueba de integridad, cifrado AES-128 con Galois/Counter Mode (GCM)

¿Cómo funciona?

El protocolo Server Message Block (SMB) permite a un cliente establecer comunicación con otros nodos dentro de una red para acceder a recursos compartidos. Para que esta interacción sea posible, ambos extremos de la comunicación deben contar con una implementación compatible del protocolo SMB: el cliente como emisor de solicitudes y el servidor como receptor y procesador de las mismas, mediante un servicio SMB activo.

Antes de que pueda producirse cualquier operación de intercambio de datos, es necesario que se establezca una conexión lógica entre el cliente y el servidor. Este proceso se inicia mediante un intercambio de mensajes de negociación y autenticación, donde ambas partes acuerdan la versión del protocolo SMB a utilizar y los parámetros de sesión.

En redes basadas en TCP/IP, SMB se transporta generalmente sobre el protocolo TCP, utilizando el puerto 445. La conexión TCP subyacente se establece mediante el procedimiento estándar conocido como three-way handshake (triple apretón de manos), el cual garantiza una conexión fiable y orientada a la conexión antes de comenzar la transferencia de datos. Este proceso inicial consta del envío de un paquete SYN por parte del cliente, seguido de una respuesta SYN-ACK del servidor y, finalmente, un ACK del cliente para completar el establecimiento de la conexión.

Una vez establecida la conexión TCP, el protocolo SMB se encarga de gestionar la transmisión estructurada de mensajes, incluyendo solicitudes y respuestas, de acuerdo con su propio conjunto de comandos. El flujo de datos está sujeto a las garantías de fiabilidad, control de flujo y corrección de errores que proporciona TCP, lo que asegura una transferencia íntegra de la información entre los extremos.

¿Dónde se emplea e implementa?

Entre las implementaciones más famosas de SMB están las siguientes:

Samba: el proyecto de software Samba es probablemente el ejemplo más conocido de implementación SMB fuera de Windows. En 1991, el programador Andrew Tridgell comenzó a desarrollar software libre para permitir la comunicación mediante Server Message Block en sistemas Unix/Linux.

ConnectedNAS: el software ConnectedNAS de Connected Way es a la vez servidor y cliente SMB para dispositivos Android. Los usuarios de la aplicación de pago pueden intercambiar datos entre el dispositivo móvil u otros dispositivos SMB con facilidad, ya en el ámbito personal o en la empresa. Por motivos de seguridad, ConnectedNAS solo es compatible con SMB a partir de la versión 2.

Almacenamiento de archivos para visualización (Hyper-V™ a través de SMB) . En Hyper-V se pueden almacenar archivos de máquinas virtuales, como los archivos de configuración, disco duro virtual (VHD) e instantáneas, en recursos de archivos compartidos a través del protocolo SMB 3.0. Esto puede usarse tanto para los servidores de archivos independientes como para los servidores de archivos agrupados que usan Hyper-V con el almacenamiento de archivos compartidos del clúster.

Microsoft SQL Server a través de SMB. En SQL Server se pueden almacenar archivos de base de datos de usuarios en recursos compartidos de archivos SMB. Actualmente, se admite el uso de SQL Server a través de SMB con SQL Server 2008 R2 para servidores SQL independientes. Las próximas versiones de SQL Server agrega compatibilidad con servidores SQL Server en clúster y bases de datos del sistema.

Vulnerabilidades

En general, el SMB se considera seguro y se utiliza ampliamente tanto en redes corporativas como domésticas. Sin embargo, como cualquier sistema de seguridad, no es a prueba de balas y puede ser vulnerable a las nuevas amenazas que vayan surgiendo.

EternalBlue: descubierto por la Agencia de Seguridad Nacional de EE. UU. (NSA) y filtrado por el grupo de hackers, Shadow Brokers en 2017, este fallo en SMBv1 permite a los atacantes ejecutar el código malicioso de forma remota sin que los usuarios se den cuenta, haciéndo así con el control de los ordenadores infectados.

EternalRomance: también publicado por los Shadow Brokers, esta vulnerabilidad permite a los atacantes tomar el control remoto de sistemas Windows enviando paquetes especialmente diseñados a ordenadores sin parches.

SMBGhost y SMBleed: que afectan al último SMBv3, estas dos vulnerabilidades muy perjudiciales se pueden explotar para ejecutar código remoto y extraer memoria sensible del núcleo, lo que puede dar a los atacantes el control total del sistema cuando se combinan.

Incidentes destacados

Ransomware WannaCry (2017): aprovechando la vulnerabilidad de EternalBlue SMBv1, este ataque cifró los archivos de los usuarios y exigió el pago de un rescate en bitcoin, afectando finalmente a unos 200 000 ordenadores en 150 países.

Petya (2016): propagado inicialmente a través de correos electrónicos de phishing, las variantes posteriores explotaban la vulnerabilidad de SMB EternalBlue para cifrar archivos a cambio de un rescate y utilizaban el protocolo para desplazarse lateralmente desde las máquinas infectadas a otras máquinas de la misma red.

NotPetya (2017): diseñado para causar el máximo daño en lugar de simplemente extorsionar dinero, NotPetya cifró y destruyó datos, haciendo casi imposible su recuperación incluso si se pagaba el rescate.

Tipos de ataques dirigidos al protocolo SMB

Además del ransomware, los ciberdelincuentes también pueden dirigirse al protocolo SMB mediante otros tipos de ataques.

Tipos de ataques dirigidos al protocolo SMB

Ataques de fuerza bruta

Aquí es donde los hackers prueban sistemáticamente varias combinaciones de nombres de usuario y contraseñas utilizando herramientas automatizadas para acceder a los recursos SMB compartidos. Si tienen éxito, estos ataques de fuerza bruta pueden provocar el robo de datos y modificaciones no autorizadas.

Ataques de intermediario (MitM)

Los ataques de intermediario consisten en que un atacante intercepta y altera las comunicaciones entre dos partes sin que estas lo sepan. En el contexto de SMB, los atacantes pueden situarse entre el cliente y el servidor SMB. Esto puede dar lugar al robo de credenciales, al acceso no autorizado a documentos privados, al secuestro de sesiones o a la manipulación de intercambios de datos.

Ataques DDoS

Un ataque DDoS (denegación de servicio distribuida) inunda tus servicios SMB con una oleada masiva de solicitudes falsas, lo que dificulta el acceso a los archivos y recursos compartidos. Los objetivos de estos ataques pueden variar mucho, como causar interrupciones operativas, inducir tiempos de inactividad o servir de cortina de humo para otras actividades maliciosas.

¿Es seguro entonces?

SMB 1.0: No existe cifrado nativo de datos; se usaba IPsec si se necesitaba confidencialidad. Debido a sus vulnerabilidades, SMB1 debe desactivarse si no es indispensable.

SMB 2.x: Es mucho más fuerte que en SMB1. Aún no introduce cifrado de datos en tránsito. Se mejoró la política de seguridad predeterminada: por ejemplo, en Windows modernos SMB2/3 requiere firma en dominios.

SMB 3.0/3.02: Permite cifrado de datos por recurso compartido. SMB Encryption: una característica nativa que cifra todo el tráfico SMB entre cliente y servidor con AES en el modo elegido. En SMB3.0/3.02 el cifrado brinda integridad. A diferencia de IPSec, el cifrado SMB puede habilitarse por recurso compartido o globalmente y protege los datos contra escucha en redes no confiables.

SMB 3.1.1: Mantiene cifrado/firmas fuertes y agrega protecciones. La integridad previa (preauthentication integrity) impide ataques MITM durante el arranque de sesión; se basa en hashing de los mensajes Negotiate y Session Setup. Microsoft recomienda deshabilitar SMB1 y forzar el uso de SMB3.1.1 en links críticos para evitar degradación de seguridad.

Bibliografías:

https://www.ionos.com/es-us/digitalguide/servidores/know-how/server-message-block-smb/#c591582

https://surfshark.com/es/blog/que-es-smb

https://www.techtarget.com/searchnetworking/definition/Server-Message-Block-Protocol

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/fd2a8346-9414-40e2-81b1-ed294f9768ea

https://learn.microsoft.com/es-es/windows-server/storage/file-server/configure-smb-over-quic-client-access-control

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/ecd51ae2-478c-455b-8669-254b74208d3b

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/14b32996-29ca-4d5a-b888-a159af29e705

https://learn.microsoft.com/es-es/windows-server/storage/file-server/smb-security-hardening