Universidad de Costa Rica

Ciudad Universitaria Rodrigo Facio

Escuela de Ciencias de la Computación e Informática

Redes de Comunicación de Datos CI-0121

Grupo 2

Proyecto de Investigación

Servicios de Red: Almacenamiento

Primer Avance

Profesor: Mag. José Antonio Brenes Carranza

Estudiantes:

Ricardo Alfaro Víquez - B70257

Allan Barrantes Chaves - B80986

Luis Eduardo Rojas Carrillo - B86875

Mario Vargas Campos - B67454

II Semestre 2020

Introducción

Al momento de la implementación de los servicios informáticos en los diferentes ámbitos de la cotidianidad económica y social, se ha buscado la mejor manera de transmitir información digital de vital importancia para el funcionamiento de empresas y organizaciones.

Una de las grandes virtudes de la invención de internet fue que brindó la capacidad de compartir información con personas de diferentes partes del mundo a partir de diferentes métodos y protocolos, generando de esta forma una mayor transmisión de conocimiento de manera masiva.

Sin embargo, incluso antes de la masificación de transmisiones de internet, ya se contaba con la habilidad de transmisión de información de manera interna o por medio de dispositivos de almacenamiento masivos. Esto requirió que se implementarán diversas arquitecturas y protocolos para mejorar la transmisión de información, entre ordenadores de una misma compañía que requerían del traspaso de datos y la alta disponibilidad de los datos.

Dadas estas necesidades de las empresas por el acceso efectivo y eficiente a su información, así como su respaldo, se desarrollaron los servicios de almacenamiento de red.

En las siguientes páginas de este documento se desarrolla una breve explicación sobre los principales servicios de red de almacenamiento tales como: FTP, Samba, NAS, SAN, NFS, además de los protocolos necesarios para el correcto funcionamiento de estos.

Objetivo General

Investigar acerca de servicios de red de almacenamiento tales como FTP, Samba, NAS, SAN, NFS.

Objetivos Específicos

-Examinar los servicios de red FTP, Samba, NAS ,SAN y NFS.

-Caracterizar los servicios de red FTP, Samba, NAS ,SAN y NFS.

-Diferenciar los servicios de red FTP, Samba, NAS ,SAN y NFS.

Metodología

Es un trabajo de investigación teórico en el cual se recolectó y analizó información sobre los conceptos especificados anteriormente, donde luego se resumieron los aspectos de mayor importancia. Dicho trabajo investigativo será complementado con una presentación de la información recolectada, utilizando filminas informativas que se expondrán ante la clase.

Marco Teórico

Protocolo FTP (File Transfer Protocol)

Descripción general

FTP es una de las formas más populares, o quizás la más popular, para mover archivos a través de internet.

De acuerdo a Greg Mooney (2020), ¿Cómo funciona? Este protocolo trabaja en un modelo de cliente/servidor como la mayoría de protocolos TCP/IP. Existirá un cliente FTP y un servidor FTP, el cliente será el encargado de conectarse al servidor para enviar o recibir archivos, y el servidor se encargará de almacenar o enviar los archivos según lo solicite el cliente. El FTP server continuamente recibe solicitudes de clientes, cada vez que esto pasa entonces se establece una sesión de control que solicita detalles de login al cliente y si la autenticación se logra entonces se establece la conexión.

El protocolo FTP tiene dos tipos de conexiones: conexión de control y conexión de datos. La conexión de control es la que se utiliza para enviar cualquier información de autenticación del cliente, comandos con detalles de conexión, comandos para recuperar o almacenar archivos. La conexión de datos es la que se realiza para enviar los archivos que se soliciten por parte del cliente, ya sea para almacenarlos en el servidor o para enviarlos hacia el cliente.

Configuración de servidores y clientes

Estructura de la "conversación" entre el cliente y el servidor

FTP usa mecanismos de comando/respuesta básicos. Lo que sucede es que el cliente se conectará al servidor que por lo general se da a través del puerto 21 según South River Technologies (2013). Una vez que el cliente se haya conectado, se recibirán respuestas por parte del servidor indicando algún mensaje (mensajes de éxito o error por ejemplo). El primer dígito se considera como el más significativo en los mensajes y por lo general siguen estas reglas:

- 1, 2, 3 éxito

- 4 ó 5 fallo

Lo anterior se vería por ejemplo si se recibe un mensaje 200 “éxito” o 550 “acceso denegado”.

Conexiones de datos

Las conexiones de datos se mantienen abiertas hasta que la transferencia haya sido completada, en caso de que el cliente sea el que esté enviando archivos entonces él mismo se encargará de cerrar la conexión una vez que haya finalizado, lo mismo ocurre en el caso de que sea el servidor el que esté enviando archivos.

Puertos

Puertos 20, 21 y modos pasivo/activo:

De acuerdo a South River Technologies (2013), cuando se desea iniciar una conexión entre un cliente y un servidor FTP, se realiza un procedimiento para los detalles de la conexión antes de que esta se realice. Existen detalles predeterminados con valores default para la conexión pero los clientes pocas veces se apoyan en esos valores. Con respecto a lo anterior es importante destacar los comandos PORT y PASV, los cuales deben ser ingresados por el cliente y significan lo siguiente:

- PORT y modo activo: el cliente indica el puerto y la dirección IP para realizar la conexión.
- PASV y modo pasivo: el cliente indica que la conexión es pasiva y esperará por un puerto y dirección IP que brinde el servidor FTP, en este caso el puerto más común es el 20.

Una vez que se brinde la dirección IP y el puerto entonces se hará un listen hasta que ambas partes estén conectadas y se pueda iniciar la transferencia de archivos.

¿Cuando usar pasivo o activo?

Esto será útil cuando se navega por firewalls. Entonces si hay un firewall delante de un servidor, el firewall bloquea el tráfico de datos que no provengan del puerto 21. Sin embargo, el servidor puede enviar datos de manera libre por el firewall. En caso de

que el cliente utilice el comando PASV entonces no se podría establecer una conexión porque el firewall bloquea cualquier puerto que no sea el 21, entonces es necesario que el cliente utilice el comando PORT para indicar los detalles de la conexión entre ambas partes.

¿Problemas actuales?

Una situación que se da es que por motivos de seguridad, ahora muchos clientes también tienen un firewall y esto puede causar que si el servidor va a brindar una respuesta al comando PORT del cliente para establecer una conexión, sea bloqueada. Para corregir el problema, muchos servidores FTP ahora incluyen una bloque de puertos pasivos que permiten establecer una conexión entre el cliente y el servidor aunque haya un firewall en ambos.

Seguridad

¿Es un protocolo seguro? No es un protocolo tan seguro por sí solo, ya que al funcionar de una manera tan simple puede ser configurado para que se pueda acceder sin una autenticación válida o modo anónimo y mucha información almacenada no se encuentra encriptada o se encuentra en texto plano, esto causa que la información pueda ser obtenida por hackers.

Para proveer una mayor seguridad se han creado métodos de encriptado como FTPS, SFTP y HTTPS.
Además, Mooney (2020) especifica detalles de esos tres métodos de encriptado que veremos a continuación:

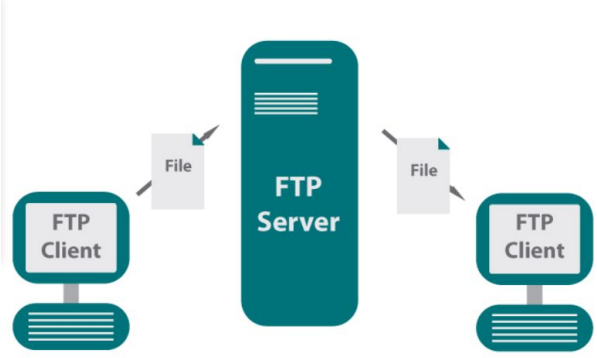
- FTPS: es el más rápido de los tres y más implementado, este método asegura el envío de los archivos mediante TLS (Transport Layer Security) que también es referido en muchas ocasiones como SSL (Secure Sockets Layer). De acuerdo a Cloudflare (2020), SSL es un protocolo de encriptamiento de internet que se encarga de encriptar la información que se envía a través de internet, por lo que cualquier persona que intente interceptar esa información solo verá caracteres que son casi imposibles de descifrar.

- SFTP: este protocolo se encarga de proveer administración y envío de archivos sobre un solo canal, además el autor Mooney menciona como posee algunas funciones adicionales como la habilidad de resumir transferencias que hayan sido interrumpidas y poder también remover archivos de una manera remota.

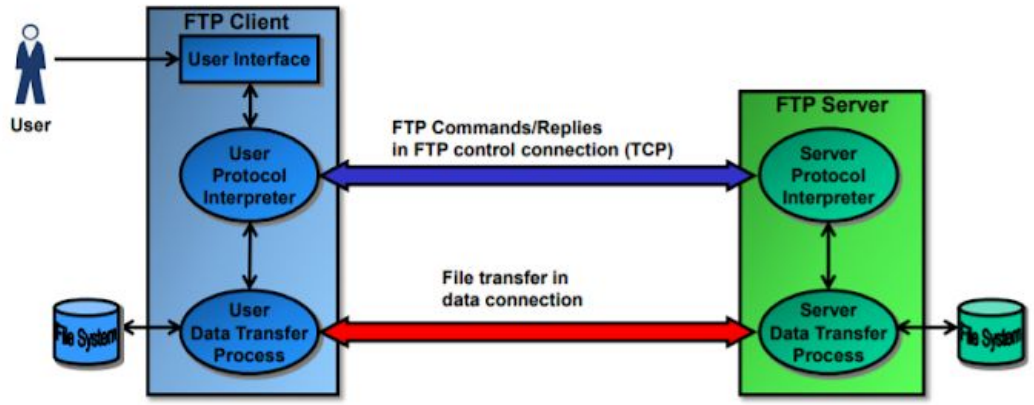
- HTTPS: es una versión con más seguridad de HTTP, usa de igual manera encriptación para transferir archivos por medio de TLS y así permite encriptar las comunicaciones.

¿Proveen mayor seguridad? “SSH, SSL, TLS y HTTPS aseguran una transmisión segura de datos. Sin embargo, en el escenario actual es importante considerar que los archivos aún se almacenan en “texto plano” y que los servidores FTP configurados en modo anónimo siguen siendo un punto de ataque para hackers.” (Mooney, 2020).

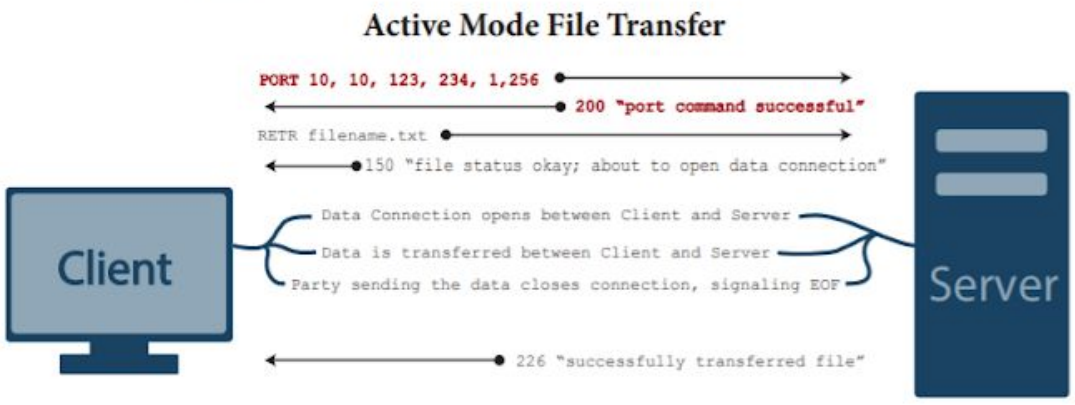
Diagramas, Imágenes, Arquitecturas



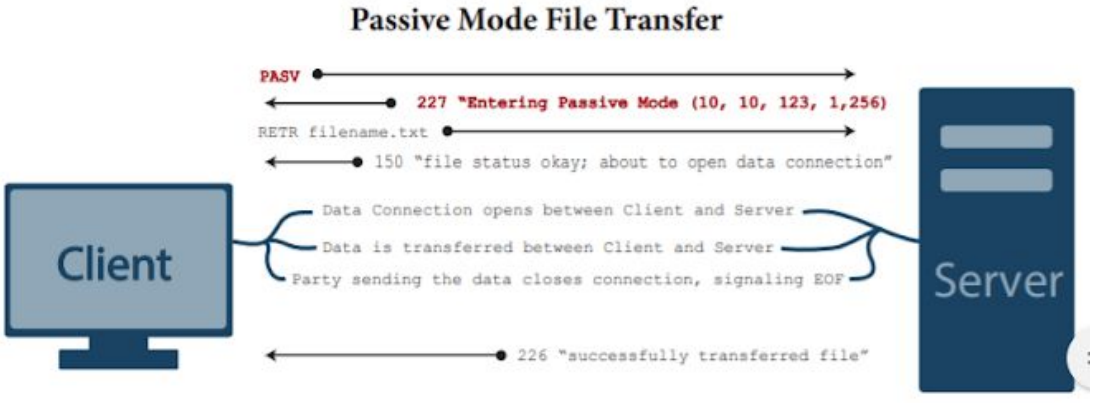
Esta imagen representa de manera gráfica y a grandes rasgos el comportamiento del protocolo FTP.



Esta imagen permite ver gráficamente lo que respecta a la conexión de control y conexión de datos.



Modo activo de FTP.



Modo pasivo de FTP

SAN (Storage Area Network)

Descripción general

Primero es importante definir que es SAN, de acuerdo al sitio web la organización SNIA (Storage Networking Industry Association),

> SAN es una red especializada y de alta velocidad que provee acceso de red a nivel de bloques a servidores con información. SANs están compuestas por hosts, switches, elementos y dispositivos de almacenamiento que están interconectados usando una variedad de tecnologías, topologías y protocolos. Las SANs además se pueden extender por múltiples sitios. (s.f)

De acuerdo a NetApp, “SANs son la arquitectura de almacenamiento de red más utilizadas por empresas para aplicaciones que necesitan una gran salida de datos y una latencia baja” (s.f). Las SANs se basan en un almacenamiento centralizado, por lo que las organizaciones que lo emplean pueden implementar metodologías consistentes y herramientas para la seguridad, protección de datos y recuperación ante fallos.

Generalidades de los componentes de SANs de acuerdo a VMware

- Switches: conectan varios elementos de la SAN, de manera particular pueden conectar hosts a arrays de almacenamiento.
- Conexiones - Host Bus Adapters (HBA) y procesadores de almacenamiento: Un host se conecta a un cable (fabric) a través de un HBA y los dispositivos de almacenamiento se conectan a los puertos de cables a través de los procesadores de almacenamiento. En la siguiente ilustración se puede ver de manera gráfica:

Componentes del host

Estos componentes consisten en los mismos servidores y los componentes que habilitan a los servidores a estar conectados de manera física a la SAN. Los HBA son uno de ellos.

Componentes del fabric

- Switches mencionados previamente.
- Data de routers permiten a los servidores acceder a dispositivos de disco o cinta en la SAN.
- Cables (Fabric) que son usualmente cables de fibra óptica que permiten conectar a todos los componentes de la SAN.

Componentes de almacenamiento

- Storage processors: proveen conexión a los servidores y a los discos físicos o medios de almacenamiento en la SAN.
- Storage devices: grupos de discos múltiples (disk arrays) y son el típico dispositivo de almacenamiento en SAN. Estos arrays utilizan tecnología RAID para brindar capacidad, desempeño y redundancia. Los sistemas que utilizan RAID, un grupo RAID equivale a un LUN.
- Tape storage devices: son parte de las capacidades de respaldo de datos/información y procesos en las SANs.

De acuerdo a la definición de NetApp sobre las SANs, el hecho de que sean de almacenamiento a nivel de bloques permiten que sea una arquitectura sumamente rápida que conecta los servidores con sus unidades de disco lógicas (LUNs). Un LUN es es un rango de bloques que se obtiene de una pila de almacenamiento compartido y presentado al servidor como un disco de almacenamiento lógico, y lo que hace el servidor es realizar particiones y darle formato a los bloques de información para que pueda almacenar información en el LUN de la misma manera en que lo haría en un disco de almacenamiento local.

Además, se destaca igualmente por parte de NetApp que las SANs están diseñadas para ser altamente resilientes ante fallos y pueden soportar una gran cantidad de fallos de dispositivos o componentes.

Puertos SAN

- WWPN (World Wide Port Name): identificador global único para un puerto que permite a ciertas aplicaciones acceder a él. Los switches FC se encargan de

identificar el WWPN de un dispositivo o host y le asignan una dirección de puerto del dispositivo local.

- Port_ID: dentro de la SAN, cada puerto tiene un ID único que funciona como la dirección FC a cada uno.

Protocolos utilizados en la comunicación SAN

- Fibre Channel Protocol (FCP): el protocolo de transporte de bloques más utilizado, utiliza protocolos de transporte por fibra óptica con comandos SCSI.
- Internet Small Computer System Interface (iSCSI): este protocolo es el segundo más utilizado. Encapsula comandos SCSI dentro de un frame de ethernet y luego utiliza un Ethernet IP para el transporte en la red. Permite que bloques de datos SCSI se transporten entre el iniciador iSCSI y el destinatario final de almacenamiento en redes TCP/IP. Este protocolo permite encriptar los paquetes de red y desencriptarlos una vez que lleguen al destino final.
- Fibre Channel over Ethernet (FCoE): es similar al iSCSI, ya que encapsula un frame de fibra óptica dentro de un datagrama de Ethernet, y luego de igual manera utiliza una red IP de ethernet para el transporte.
- Non-Volatile Memory Express over Fibre Channel (FC-NVMe): NVMe es un tipo de protocolo de interfaz utilizado para acceder almacenamiento flash por medio de un PCI Express (PCIe) bus. La diferencia de esta arquitectura con las tradicionales, es que estas pueden soportar miles de colas paralelas que tienen la habilidad de soportar miles de comandos concurrentes y en el caso tradicional se está limitado a un solo comando serial y cola simple.

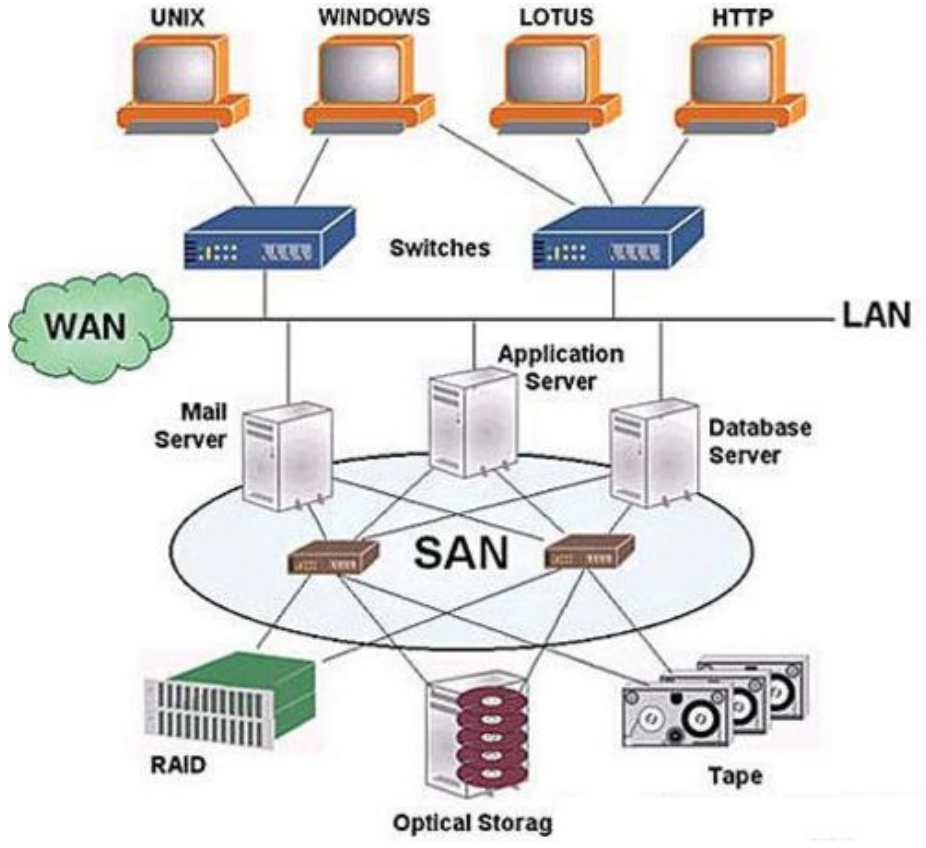
Seguridad

Para proveer seguridad en redes SAN se utilizan algunas técnicas mencionadas a continuación:

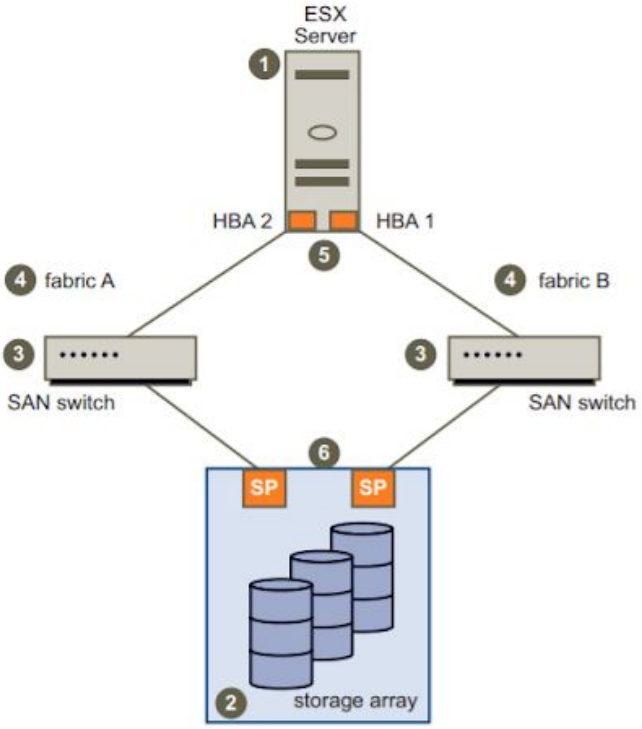
- Encriptar la información que se encuentra almacenada en infraestructura SAN o dispositivos de almacenamiento
- Aislamiento de organizaciones, departamentos, usuarios que utilicen una SAN virtual.
- Remover y resolver puntos específicos de vulnerabilidad a fallos y ataques.

Zoning: esto define el control de acceso dentro de una SAN, establece cuales HBAs se pueden conectar a SPs específicos. Pueden haber múltiples puertos hacia el mismo SP en diferentes zonas. Cuando una SAN utiliza zoning, los dispositivos que estén fuera de esa “zona” no son visibles para los que sí están dentro. Este método se utiliza para seguridad y aislamiento, dispositivos compartidos y arrays de almacenamiento múltiples.

Diagramas, Imágenes, Arquitecturas



Representación gráfica de SAN



Componentes de SAN (Switches, HBA, SPs)

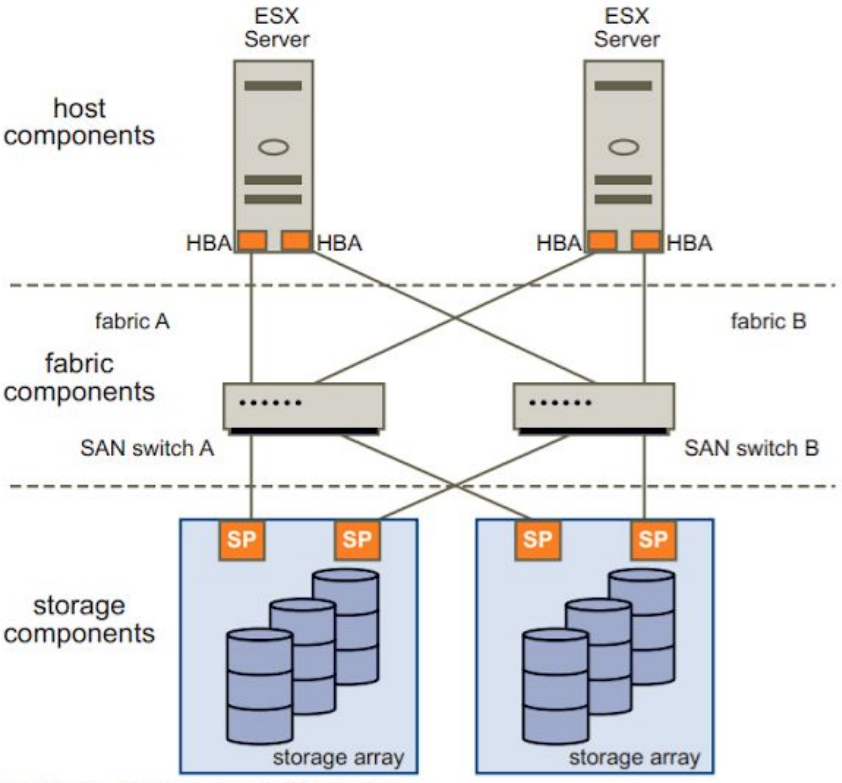


Figure 2. SAN Component Layers

Protocolo NFS (Network File System):

Descripción General

NFS es un protocolo de nivel de aplicación, según el Modelo OSI. El modelo OSI es un sistema de interconexión de sistemas abiertos de referencia para los protocolos de la red, creado en el año 1980 por la Organización Internacional de Normalización. Este protocolo es utilizado para poder compartir sistemas de archivos distribuidos en un entorno de red de computadoras del área local. Posibilita a todos los sistemas conectados a una misma red que accedan a los archivos compartidos como si se tratara de locales. (Oracle Corporation, 2010).

Para lograr que los diferentes dispositivos conectados a la misma red accedan a los datos almacenados en el servidor, este implementa procesos de dominio NFS para que los datos estén disponibles para los clientes o dispositivos. El administrador del servidor determina qué poner a disposición y se asegura de que pueda reconocer a los clientes aceptados. Desde el lado del cliente, la máquina solicita acceso a los datos exportados, normalmente emitiendo un comando de entrada. Si tiene éxito, la máquina cliente puede ver e interactuar con los sistemas de archivos dentro de los límites previamente establecidos. (Microsoft, 2018).

NFS asume un sistema de archivos que es jerárquico, con directorios menos el nivel inferior de archivos. Cada entrada en un directorio tiene un nombre predeterminado. Los sistemas pueden tener restricciones sobre la profundidad del árbol o los nombres utilizados, además de utilizar una sintaxis diferente para representar el nombre de la ruta a acceder. Cada cliente NFS también puede ser potencialmente un servidor remoto y los sistemas de archivos montados localmente se pueden mezclar libremente. (Red Hat Inc, 2005).

Configuración de servidores y clientes

Se supone que todos los procedimientos del protocolo NFS son sincrónicos. Cuando un procedimiento regresa al cliente, el cliente puede asumir que la operación se ha completado y cualquier dato asociado con la solicitud está ahora en almacenamiento estable.

Suponiendo un escenario de estilo Unix en el que un cliente necesita acceder a los datos almacenados en un servidor:

- El servidor implementa y ejecuta procesos de daemon (es un tipo especial de proceso informático no interactivo, es decir, que se ejecuta en segundo plano en vez de ser controlado directamente por el usuario) NFS, que se ejecutan de forma predeterminada como nfsd (sistema de archivos especial que proporciona acceso al servidor NFS de Linux), para que sus datos estén genéricamente disponibles para los clientes.
- El administrador del servidor determina qué datos poner a disposición, exportando los nombres y parámetros de los directorios, generalmente usando el archivo de configuración / etc / exports y el comando exportfs. Este comando especifica el directorio a compartir.
- La administración de seguridad del servidor asegura que pueda reconocer y aprobar clientes validados.
- La configuración de la red del servidor asegura que los clientes apropiados puedan comunicarse con ella a través de cualquier sistema de firewall.
- El equipo del cliente solicita acceso a los datos exportados, normalmente emitiendo un comando de montaje. El cliente le pregunta al servidor (rpcbind) qué puerto está usando el servidor NFS, el cliente se conecta al servidor NFS (nfsd), nfsd pasa la solicitud a mountd.
- Finalmente, los usuarios de la máquina cliente pueden ver e interactuar con los sistemas de archivos montados en el servidor dentro de los parámetros permitidos, ya que dependen de los permisos establecidos por el servidor. (Red Hat Inc, 2005).

Versiones NFS

- *NFSv1:* Esta versión no se utilizó en su totalidad, ya que esta se desarrolló para fine experimentales
- *NFSv2:* La versión dos trabaja solo sobre el Protocolo de datagramas de usuario (UDP) y está limitado a archivos de 32 bits. Sus diseñadores pretendían mantener el concepto del servidor sin estado.

- *NFSv3:* En esta versión se agregó a diferencia de la versión dos el soporte para archivos de 64 bits, soporte para escrituras asincrónicas en el servidor para mejorar el rendimiento de escritura. Además agregó soporte para TCP como transporte para NFS.
- *NFSv4:* incluye mejoras de rendimiento, exige una seguridad sólida, tiene como objetivo proporcionar soporte para aprovechar las implementaciones de servidores agrupados, incluida la capacidad de proporcionar acceso paralelo escalable a archivos distribuidos entre varios servidores, clonación y copia del lado del servidor, archivos dispersos y reserva de espacio. Una gran ventaja de NFSv4 sobre sus predecesores es que solo se usa un puerto UDP o TCP, 2049, por lo que no tiene interacción con portmapper, rpc.mountd , rpc.lockd y rpc.statd ya que no tiene necesidad de mapear los puertos para ejecutar el servicio, lo que simplifica el uso del protocolo a través de firewalls. (Red Hat Inc, 2005).

Puertos

El protocolo NFS utiliza actualmente el número de puerto UDP o TCP 2049. Este no es un puerto asignado oficialmente, ya que las versiones anteriores del protocolo utilizan la función portmapper de RPC para mapear los puertos.

Servicios y Protocolos

El protocolo de montaje de soporte permite al servidor distribuir privilegios de acceso a un conjunto restringido de clientes. Realiza funciones específicas del sistema operativo que permiten, por ejemplo, adjuntar árboles de directorios remotos a algún sistema de archivos local. El protocolo de montaje es independiente de NFS, pero está relacionado con él. El protocolo de montaje se mantiene separado del protocolo NFS para que sea fácil de conectar nuevos métodos de verificación y validación de acceso sin cambiar el protocolo del servidor NFS.

NFS se admite normalmente en UDP y TCP. Todas las versiones de NFS se basan en llamadas a procedimiento remoto (RPC). RPC es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre clientes y servidores. (Microsoft, 2018). Los

servicios RPC bajo Linux están controlados por el servicio portmap. El servicio Portmap asigna las solicitudes RPC a los servicios correctos. (Red Hat Inc, 2005).

Según microsoft para compartir o montar sistemas de archivos NFS, los siguientes servicios funcionan juntos, según la versión de NFS que se implemente, algunos de estos servicio son:

- *service nfs start:* inicia el servidor NFS y los procesos RPC apropiados para atender las solicitudes de sistemas de archivos NFS compartidos.
- *service nfslock start:* es un servicio obligatorio que inicia los procesos RPC apropiados para permitir que los clientes NFS bloqueen archivos en el servidor.
- *service portmap:* acepta reservas de puertos de los servicios RPC locales. Estos puertos se ponen a disposición (o se anuncian) para que los servicios RPC remotos correspondientes accedan a ellos. Portmap responde a las solicitudes de servicios RPC y establece conexiones con el servicio RPC solicitado. No se utiliza con NFSv4.

Los siguientes procesos RPC facilitan los servicios NFS según Oracle:

- *rpc.mountd:* este proceso recibe solicitudes de montaje de los clientes NFS y verifica que el sistema de archivos solicitado esté actualmente exportado. Este proceso lo inicia automáticamente el servicio nfs y no requiere configuración por parte del usuario. No se utiliza con NFSv4.
- *rpc.nfsd:* permite definir versiones explícitas de NFS y protocolos que el servidor anuncia. Funciona con el kernel de Linux para satisfacer las demandas dinámicas de los clientes NFS, como proporcionar subprocesos de servidor cada vez que se conecta un cliente NFS. Este proceso corresponde al servicio nfs.
- *rpc.lockd:* permite a los clientes NFS bloquear archivos en el servidor. Si no se inicia rpc.lockd, el bloqueo de archivos fallará. rpc.lockd implementa el protocolo Network Lock Manager (NLM). Este proceso corresponde al servicio nfslock. No se utiliza con NFSv4.

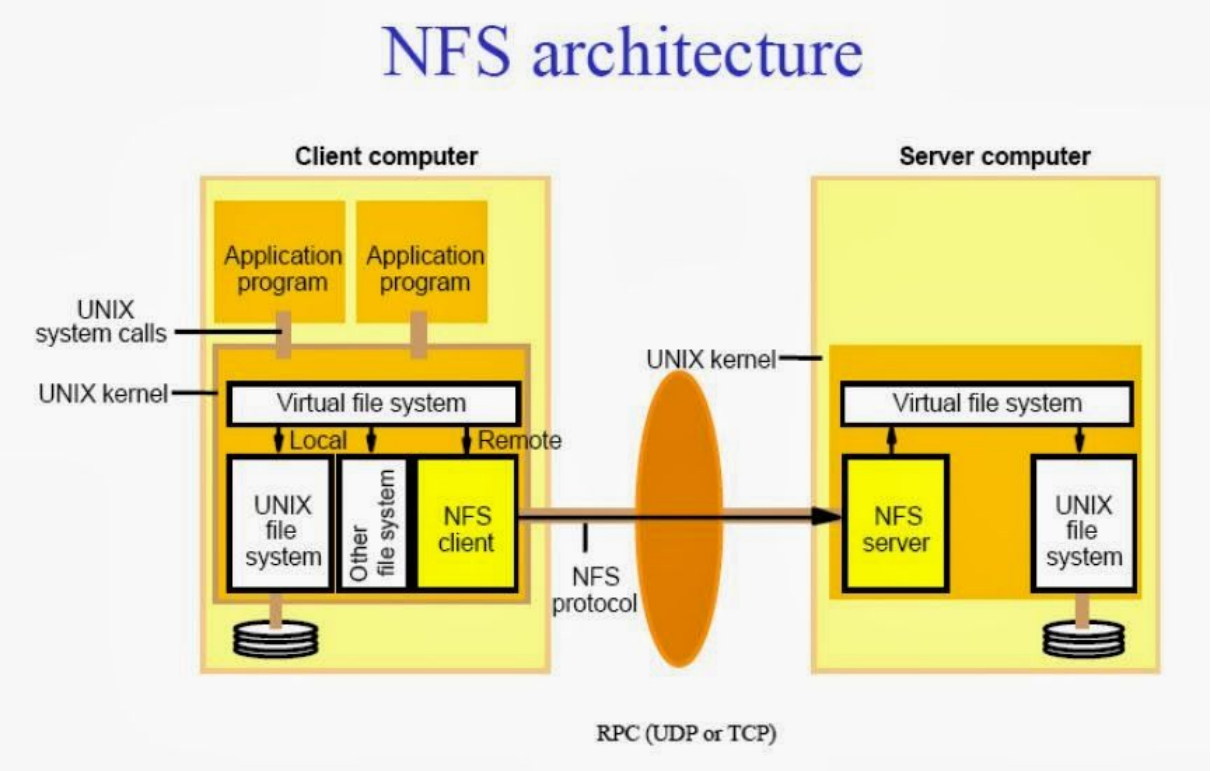
- *rpc.statd:* este proceso implementa el protocolo RPC Network Status Monitor (NSM) que notifica a los clientes NFS cuando se reinicia un servidor NFS sin haber sido desactivado correctamente. Este proceso lo inicia automáticamente el servicio nfslock y no requiere configuración por parte del usuario. No se utiliza con NFSv4.
- *rpc.rquotad:* este proceso proporciona información de cuotas de usuario para usuarios remotos. Este proceso lo inicia automáticamente el servicio nfs y no requiere configuración por parte del usuario.
- *rpc.idmapd:* este proceso proporciona llamadas ascendentes de cliente y servidor NFSv4 que se asignan entre nombres NFSv4 en el cable (que son cadenas en forma de usuario - dominio) y UID (User ID) y GID (Group ID) locales.

Seguridad

Para que nuestro sistema NFS sea seguro es importante tomar en consideración los siguientes aspectos:

- Utilizar cortafuegos para limitar el acceso a los puertos utilizados por los procesos del servicio NFS.
- Exportar sistemas de archivos de lectura siempre que sea posible.
- Evitar usar las versiones 2 y 3 de NFS, ya que no disponen de control de acceso para los usuarios en concreto. En estas, cuando un sistema de archivos es exportado, cualquier usuario en cualquier máquina remota conectada al servidor NFS puede acceder a los datos compartidos en él.
- Si no se utiliza la opción de exportación squash, cualquier usuario root en el equipo cliente puede convertirse en un usuario con acceso privilegiado. Conviene siempre tener activada alguna opción de squash.
- La versión más segura de NFS es la 4. (Red Hat Inc, 2005).

Diagramas, Imágenes, Arquitecturas



En el diagrama anterior, se observa un ejemplo del funcionamiento del protocolo NFS basado en el sistema operativo UNIX.

NAS (Network Attached Storage):

Descripción General

El servicio de almacenamiento conectado a la red (NAS por sus siglas en inglés) se refiere a una arquitectura de almacenamiento, a nivel de ficheros, en la cual uno o varios dispositivos de almacenamiento dedicados, están conectados a una red y permiten el acceso a los archivos a los usuarios autorizados que se encuentren dentro de la red.

En este sistema, se utilizan uno o varios dispositivos de almacenamiento (por ejemplo, discos duros), con la salvedad que pueden conectarse a una red, y esta permite que varios dispositivos accedan a los archivos almacenados simultáneamente, siempre y cuando cuenten con las credenciales necesarias. Puede decirse que funciona como una nube privada. (SNIA, 2020).

Seguridad

En cuanto a la seguridad, al funcionar como una red privada, aumenta la confiabilidad de que sus datos se encuentran en su propia infraestructura, además generalmente los sistemas NAS vienen con capas de seguridad como firewalls, protección DoS e incluso encriptación de los discos, sin embargo, si alguno de los ordenadores se viera comprometido, o la conexión a la red NAS mediante dispositivos remotos fuera interceptada, sería posible el robo o perdida de información. Se debe tomar en cuenta también la protección de los puertos y la protección ante *command injection*, así como la elección de contraseñas robustas, para evitar su obtención con métodos como *brute-force*. (Meyer, 2019).

Características, servicios y protocolos

Dentro de las características propias de este tipo de estructura para almacenamiento y transferencia de datos se pueden mencionar la facilidad de acceso a los archivos que existe desde diferentes sistemas operativos, la estable escalabilidad a la que puede ser sometida la estructura y los bajos costos de operación. (Deng, 2009).

Otra de las características importantes de los sistemas NAS es que permiten la interacción con sus ficheros tanto a sistemas Unix como Windows, pues utilizan protocolos estándar para la transferencia y acceso a los archivos, como lo son SMB/CIFS, NFS, FTP, TFTP o SFTP, por nombrar algunos. (Sánchez S, 2009)

Este tipo de implementaciones suelen conformarse de hardware y software especializado para satisfacer las demandas de la arquitectura, actualmente, compañías como Western Digital, ofrecen discos duros especializados en NAS. (Western Digital Corporation, 2019).

Los sistemas NAS son utilizados generalmente para propósitos moderados en términos de tamaño, su conexión se realiza generalmente a través de cableados LAN, donde el dispositivo NAS mantiene su dirección IP así como lo hacen los ordenadores conectados a este, de esta manera, los principales objetivos o clientes de este sistema son usuarios finales. (Ferrando, 2016).

Los sistemas de almacenamiento conectado a la red tienen en muchas ocasiones, su implementación en un sistema RAID, para manejar adecuadamente la

redundancia de datos, esto permite además un mejor acceso simultáneo a los datos y proteger la integridad de los mismos, sin embargo, por utilizar la red LAN para enviar paquetes utilizando el protocolo TCP/IP, los momentos de alto tráfico, o de respaldo de datos, pueden generar un gran consumo del ancho de banda y de poder de procesamiento.

Es importante mencionar que este último apartado se presenta como una gran desventaja, pues si bien los sistemas NAS son fácilmente escalables en almacenamiento, generalmente traen una configuración de procesador fija y no tienden a ser escalables.

En comparación con los sistemas SAN, la principal diferencia es que en una red SAN se hace un acceso directo a los archivos por bloques de disco, mientras que en la NAS se hace por medio de ficheros. Los sistemas SAN suelen utilizar fibra óptica para la transferencia de archivos mientras que la red NAS utiliza los cables de RJ45.

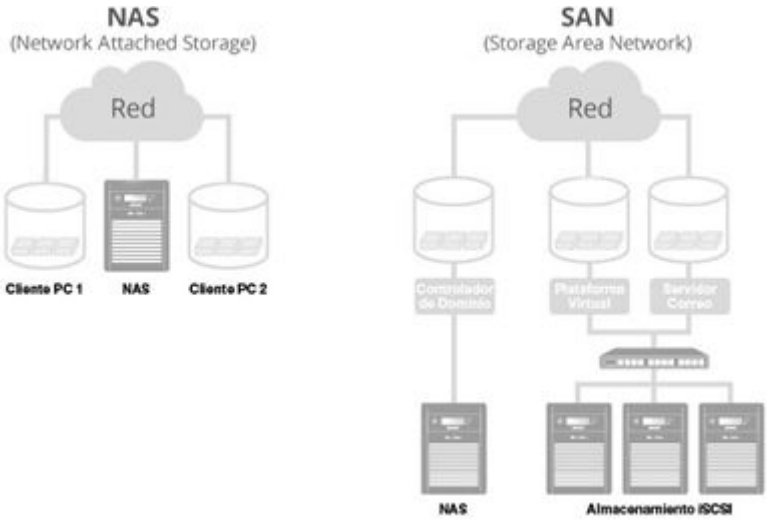
La principal desventaja que presentan las NAS respecto a las SAN, es que estas últimas están orientadas a la baja latencia y la casi nula perdida de datos, mientras que las primeras no pueden entregar esas garantías de manera tan eficiente. (Universidad Politécnica de Navarra, área de ingeniería telemática, 2016).

A principios de siglo, uno de los grandes retos que presentaban los sistemas NAS era el cuello de botella que se generaba en la red, pues se utilizaba la misma conexión para hacer consultas al sistema de ficheros como para las solicitudes del resto de la red de computadores.(IMEX Research,1997) Sin embargo, actualmente las implementaciones de NAS son mucho más complejas, se componen de una caja de NAS, la cual contiene un sistema de software dedicado especializado en el manejo de hardware específico, y además se conecta a un switch, lo que permite que se dé una mayor estabilidad y rendimiento en el servicio.(Red Hat Inc, s.f).

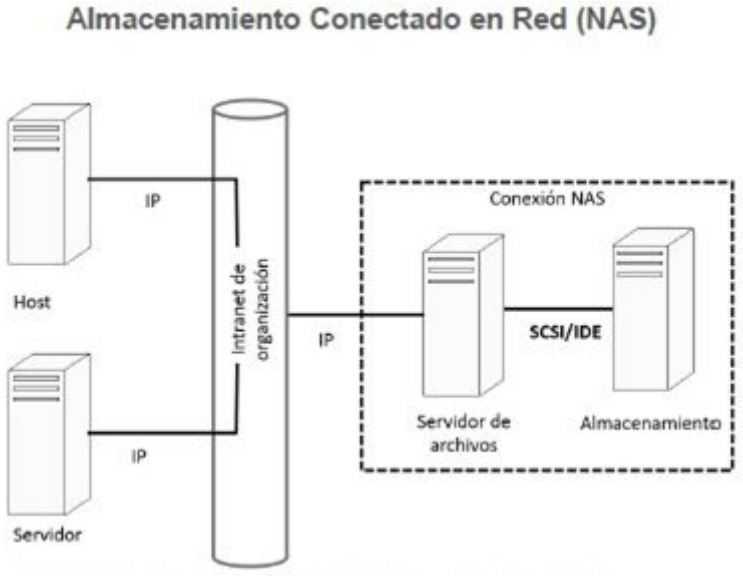
En la actualidad el servicio NAS se ofrece como una opción de alto rendimiento y bajo costo para empresas pequeñas y medianas, con diversidad de configuraciones y características ofrecidas por las empresas más importantes del mercado, por ejemplo Seagate o Red Hat. Se ofrecen también servicios híbridos de NAS en la nube, en la cual la empresa dueña de la nube se encarga de la configuración y la capacidad de procesamiento, y los clientes tienen total control de la seguridad y la ubicación del sistema. (SNIA, 2020).

Además, al funcionar sobre la red LAN y con protocolos TCP/IP, es posible conectarse a la red NAS desde un dispositivo remoto, utilizando las credenciales correctas, todo esto lo hace una opción muy atractiva para pequeñas o medianas empresas que quieran asegurar el acceso a sus datos (de gran utilidad para quienes realizan teletrabajo) y mejorar su rendimiento. (SNIA, 2020).

Diagramas, Imágenes, Arquitecturas



Diferencias entre arquitecturas de redes NAS y SAN. Fuente (Ferrando, 2016).



En la figura anterior se esquematiza el funcionamiento a nivel de red de los sistemas NAS. Donde se conectan mediante la red LAN y permiten el acceso a los ficheros a todos los dispositivos conectados a ella. Fuente (Vázquez-Moctezumas, 2015).

Protocolo Samba

Descripción General

Es una implementación de código abierto del protocolo SMB (Server Message Block) anteriormente llamado de dicha manera y renombrado recientemente como CIFS (Common Internet File System), creado en 1992 por The Samba Team. Es un protocolo de archivos compartidos de Microsoft Windows para sistemas UNIX, tales como GNU/Linux, Mac OS X o Unix. Estos sistemas tipo UNIX, actúan como servidores o como clientes de redes para Windows. (Gutmann, 2007).

Dentro de las características de Samba, es desempeñarse como una aplicación de servidor. Es sumamente poderosa y versátil ya que permite administrar colas de impresión, directorios compartidos, autenticar mediante su archivo de usuarios, etc. (Red Hat Inc, 2005).

Samba permite diversas funcionalidades, las cuales serán detalladas más adelante. Permite la validación de usuarios por medio del PDC (Controlador Principal de Dominio). Mediante este controlador, se permite un manejo de usuarios ya sea para aceptar o denegar el acceso a los recursos compartidos del sistema, además de cualquier máquina dentro de la red. En el sistema Linux se almacenan los datos tanto del usuario como sus contrasenńas, por lo que los usuarios inician sesión desde Windows. La seguridad de este manejo, se garantiza normalmente mediante una contraseña como tal. (Gutmann, 2007).

Configuración de servidores y clientes

Para configurar un servidor Samba, es necesario acceder al archivo de configuración. Este se encuentra en la ruta (/etc/samba/smb.conf). Este archivo permite que los usuarios puedan visualizar todos sus directorios principales como si fuera una partición de Samba compartida (Samba share). Esto además permite compartir todas las impresoras que se encuentran en la red, como si fuera un sistema de impresoras compartido por todas las computadoras. La red compartida, permite conectar cualquier impresora, y a partir de ello mediante una computadora Windows, enviar archivos que serán impresos posteriormente. (Red Hat Inc, 2005).

Puertos

Un gran porcentaje del tráfico de red generado por el protocolo SMB, se produce a través del protocolo TCP. Para servidores Windows NT4 y anteriores, todo el tráfico se produce mediante el puerto 139. A esto se le establece el nombre de servicio de red NetBIOS-SSN (Session service). Como parte de las funciones que se realizan a través de dicho puerto esta: Copia de archivos, listado de directorios y principalmente operaciones totalmente relacionadas con funcionalidades que pertenecen a las impresoras. A partir de Windows 2000, se implementa la operatividad mediante el puerto 445.

Otro protocolo que se implementa es el UDP. Principalmente permite búsquedas rápidas de difusión dentro de una red local. Además, existen diversas funcionalidades como: Búsqueda de servidores y estaciones de trabajo, mantener listas de exploración, y otras búsquedas dirigidas y de difusión para servidores, nombres de estaciones y dominios. NetBIOS Name Service trabaja mediante el puerto 137, sin embargo, existe un servicio llamado NetBIOS Datagram Service, el cual opera en el puerto 138.

Por lo tanto, para poder bloquear el tráfico compartido de archivos e impresoras, es necesario bloquear los puertos TCP 139 y 445 respectivamente. En el caso de los puertos UDP, para bloquear el tráfico sobre NetBIOS Name Service y NetBIOS Datagram Service, es necesario restringir el acceso en los puertos 137 y 138 respectivamente. (Potter, 2005).

Servicios y Protocolos

Samba es una implementación de diversos servicios y protocolos. A continuación se detallan cada uno de ellos:

- SMB (Server Message Block): Samba es una implementación de este protocolo. SMB es un protocolo de red, el cual permite una funcionalidad para compartir archivos e impresoras entre diversos nodos que se encuentran en una red de computadoras Windows.
- CIFS (Common Internet File System): Anteriormente conocido como SMB. Es un protocolo de sistema de archivos de red. Permite funcionalidades como el

acceso compartido a archivos e impresoras entre diversas máquinas mediante la red. (Visuality Systems, 2016).

- TCP/IP: Es una familia de protocolos bastante importante de red. En este conjunto de protocolos, se compone internet y por lo tanto permite la transmisión de datos entre diversas computadoras. Se divide en 4 capas: Capa de aplicación, transporte, internet y de acceso al medio.

  El protocolo TCP, permite establecer conexiones entre computadoras para el intercambio mediante un flujo de datos en la capa de transporte. Se garantiza una transmisión sin errores y además, los datos se reciben en el mismo orden en el que se enviaron. Este protocolo, proporciona soporte a otros protocolos como HTTP, SMTP, SSH y FTP. Una máquina, puede diferenciar distintas aplicaciones mediante puertos.

  El protocolo IP, es conocido como el protocolo de internet, y permite mediante la capa de red, una comunicación de datos digitales clasificados. El protocolo más común y popular es el IPv4, aunque existe igualmente el protocolo IPv6. El objetivo de este protocolo, es lograr una comunicación bidireccional entre el origen y el destino, de manera segura y confiable. Esto se realiza a través de distintas redes físicas las cuales son previamente enlazadas.
- NetBT o NBT (NetBIOS sobre TCP/IP): Es un servicio de red que se desempeña en la capa de sesión. Este servicio, asigna un nombre a la dirección IP para la resolución de nombres. Esto ocurre mediante WINS (Windows Internet Name Service), el cual es una implementación de NBSN (NetBIOS Name Service). WINS es para los nombres de NetBIOS el equivalente a DNS para los nombres de dominio. (Oracle Corporation, 2010).

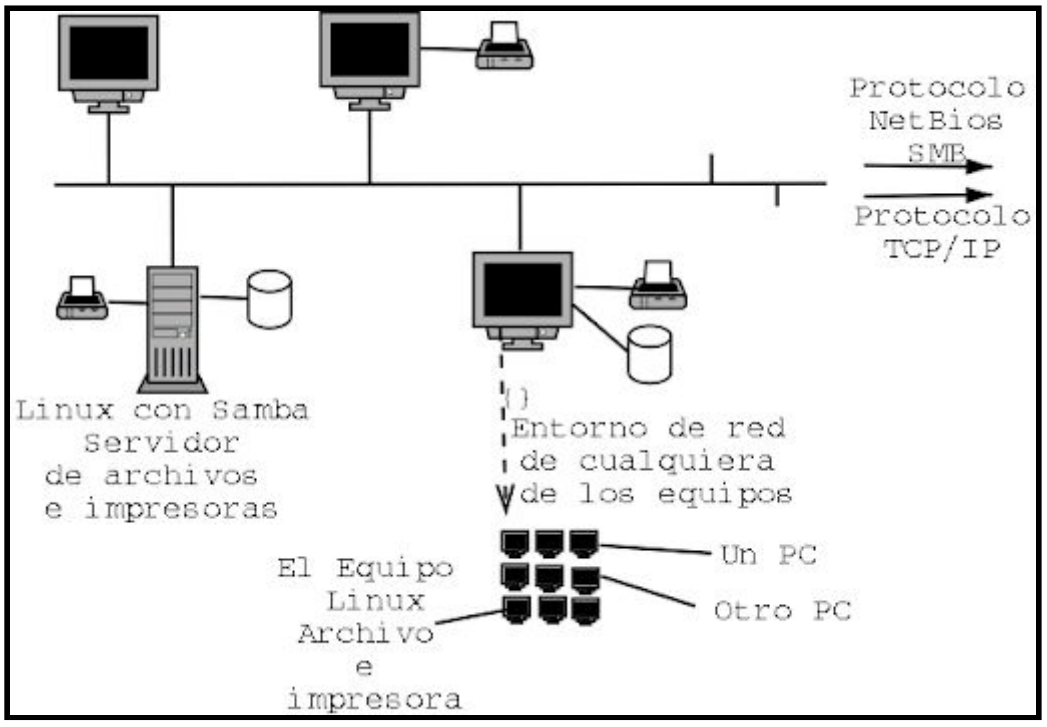
Seguridad

Como parte de la seguridad implementada por Samba, se tiene que cada vez que un usuario intente conectarse a un recurso no accesible para invitados, deba ingresar una contraseña previamente establecida para llevar a cabo la conexión de manera satisfactoria.

El servidor de Samba, almacena todos los datos tanto de los usuarios, como de sus contraseñas correspondientes. Estos datos, se encuentran ubicados en el archivo

/etc/samba/smbpasswd. Este último comando smbpasswd, permite un manejo en el servidor, ya sea para agregar nuevos usuarios, equipos, o ya sea modificarlos y por lo tanto realizar cambios. (Mikeliunas, 2020).

Diagramas, Imágenes, Arquitecturas



En el diagrama anterior, se observa el funcionamiento del protocolo Samba. Mediante una red de nodos de computadoras Windows o del sistema UNIX que funcionan como servidores, se comparten archivos e impresoras entre sí. Todo esto se da mediante el protocolo Samba, el cual es una implementación del protocolo SMB, además se observa NetBT, el cual es un servicio de red. Este servicio se forma a partir del protocolo NetBIOS sobre el protocolo TCP/IP, definidos anteriormente.

Conclusión

Los servicios de red de almacenamiento son indispensables hoy en día para el funcionamiento de muchos sistemas informáticos implementados en instalaciones laborales y personales, mediante las cuales es posible tener un acceso remoto y compartido generalmente a un conjunto de datos especificados por un servidor. Esto permite mantener un conjunto de datos en un solo equipo, sin tener que duplicar la información en todos los dispositivos o clientes que necesiten de esta. Además esto agiliza el traspaso de información, ya que es de manera inmediata y los clientes pueden acceder, con su debido permiso, instantáneamente cuando lo deseen.

El protocolo FTP es uno de los más utilizados e importantes para la transferencia de archivos. Su gran simplicidad al funcionar con un modelo de cliente/servidor lo hace más propenso a ataques maliciosos pero con los años se han implementado métodos para realizar transferencias cada vez más seguras de archivos entre clientes y servidores.

Con respecto al protocolo SAMBA, este es un sistema de tipo Unix muy versátil que actúa como servidor o cliente de redes para windows. Principalmente es capaz de administrar colas de impresión, directorios compartidos y además tiene la capacidad de administrar y autenticar las conexiones mediante su archivo de usuarios.

El sistema de almacenamiento NAS es una opción económicamente viable, de fácil instalación y mantenimiento, y con un buen rendimiento para empresas pequeñas o medianas que no poseen mucho tráfico de datos, que buscan mantener una estabilidad de acceso mediante una red privada a sus archivos, sin necesidad de invertir en una arquitectura complicada. Actualmente muchas empresas ofrecen servicios NAS basados en la nube, cuyo principal beneficio es la capacidad de procesamiento, sin embargo, NAS requiere un buen ancho de banda, pues utiliza ese medio (red de internet o LAN) para transferir sus datos.

Adicionalmente, el protocolo NFS es un protocolo de gran utilidad ya que permite compartir a los clientes acceso a un directorio especificado anteriormente por el equipo servidor. Además dependiendo de los permisos que se les otorguen, estos tienen la capacidad de escribir y leer en los datos incluidos en el directorio.

Por último, SAN es una red que permite el acceso a nivel de bloques de la información. Su gran resiliencia ante fallos y la gran capacidad que tiene en aspectos

como velocidad de transmisión de datos por componentes como la fibra óptica, hace que sea uno de los métodos más utilizados para la comunicación de datos entre diferentes hosts y servidores, así como en empresas grandes y pequeñas.

Referencias

[1] Deng, Y. (2009). Deconstructing Network Attached Storage Systems. Journal of Network and Computer Applications, 32(5), 1064-1072. https://www.researchgate.net/publication/220172709_Deconstructing_Network_Attached_Storage_systems

[2] Ferrando, J. (2016, 1 diciembre). COMPARATIVA SAN VS. NAS. Infordisa. https://www.infordisa.com/es/comparativa-san-vs-nas/#:%7E:text=Tanto%20SAN%20(Storage%20Area%20Network,operan%20en%20bloques%20de%20disco.

[3] Gutmann, J. (2007). SAMBA: Linux y Windows en Red. Septiembre 1, 2020, de Wayback Machine Sitio web: https://web.archive.org/web/20090123063455/http://estaciondetransito.com.ar/estaciondetransito/?p=18

[4] IMEX Research. (1997–2000). SAS, NAS, SAN Past, present, and future. http://www.imexresearch.com/pdfs/sasnassan.pdf

[5] Meyer, B. (2019, 1 noviembre). *Network Attached Storage*. CyberNews. https://cybernews.com/resources/nas-security-guide

[6] Microsoft Corporation. (2018). Network File System overview. Septiembre 1, 2020, de Microsoft Corporation Sitio web: https://docs.microsoft.com/en-us/windows-server/storage/nfs/nfs-overview

[7] Microsoft Corporation. (2018). How RPC Works. Septiembre 1, 2020, de Microsoft Corporation Sitio web: https://docs.microsoft.com/en-us/windows/win32/rpc/how-rpc-works

[8] Mikeliunas, S. (2020). Material Samba. Septiembre 18, 2020, de Mikeliunas, S. Sitio web: https://www.fing.edu.uy/tecnoinf/maldonado/cursos/adminf/materiales/ADI-samba.pdf

[9] Mooney, G. (2020). What is file transfer protocol (FTP)? Defrag This – Security and Network Monitoring Blog And Podcast. https://blog.ipswitch.com/what-is-file-transfer-protocol-ftp

[10] Nagle, D. F., Ganger, G. R., Butler, J., Goodson, G., & Sabol, C. (1999). Network Support for Network-Attached Storage. Proceedings of Hot Interconnects 1999,1-6. https://www.researchgate.net/publication/2458046_Network_Support_for_Network-Attached_Storage

[11] NetApp. (2019). What is a storage area network (SAN)? | SAN vs. NAS | NetApp: The Global Leader In Hybrid Cloud Data Services. https://www.netapp.com/us/info/what-is-storage-area-network.aspx

[12] Oracle Corporation. (2010). How the NFS Service Works. Septiembre 1, 2020, de Oracle Corporation Sitio web: https://docs.oracle.com/cd/E19683-01/806-4076/6jd6amr0j/index.html

[13] Oracle Corporation. (2010). NetBIOS over TCP/IP (NetBT) Name Resolution. Septiembre 19, 2020, de Oracle Corporation Sitio web: https://docs.oracle.com/cd/E19957-01/806-2749-10/z40005fe4710/index.html

[14] Potter, T.. (2005). Firewalling Samba. Septiembre 20, 2020, de Samba.org Sitio web: https://www.samba.org/~tpot/articles/firewall.html

[15] Red Hat Enterprise Linux 3: Manual de administración del sistema: Capítulo 24. (2005). Samba. Septiembre 18, 2020, de Massachusetts Institute of Technology Sitio web: http://web.mit.edu/rhel-doc/3/rhel-sag-es-3/s1-samba-configuring.html

[16] Red Hat Enterprise Linux 4: Manual de referencia: Capítulo 14. (2005). Samba. Septiembre 1, 2020, de Massachusetts Institute of Technology Sitio web: https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-samba.htm

[17] Red Hat Enterprise Linux 8: Manual de referencia: Capítulo 3. (2005). MOUNTING NFS SHARES. Septiembre 1, 2020, de Red Hat Enterprise Linux Sitio web: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/managing_file_systems/mounting-nfs-shares_managing-file-systems

[18] Red Hat Inc. (2020). ¿Qué es el almacenamiento conectado en red (NAS)? Red Hat. https://www.redhat.com/es/topics/data-storage/network-attached-storage

[19] Sánchez S, J. F. (2009, abril). *Sistemas de Almacenamiento SAN, NAS, DAS* [Diapositivas]. unitec.edu.ve. http://www.unitec.edu.ve/materiasenlinea/upload/T1022-10-1.pdf

[20] SNIA (Storage Networking Industry Association). (2020). What is NAS (Network Attached Storage) and why is NAS Important? | SNIA. snia.org. https://www.snia.org/education/what-is-nas.

[21] SNIA (s.f.). What is a storage area network (SAN)? | Advancing Storage and Information Technology. https://www.snia.org/education/storage_networking_primer/san/what_san

[22] South River Technologies. (2013). *FTP - The File Transfer Protocol*. https://southrivertech.com/wp-content/uploads/FTP_Explained1.pdf

[23] Universidad Politécnica de Navarra, área de ingeniería telemática. (2016, 16 febrero). SAN y NAS [Diapositivas]. www.tlm.unavarra.es/. https://www.tlm.unavarra.es/~daniel/docencia/rng/rng14_15/slides/Tema1-11-SANyNAS.pdf

[24] Visuality Systems. (2016). All About CIFS. Septiembre 20, 2020., de Visuality Systems Ltd. Sitio web: https://cifs.com.

[25] *What is SSL?* | *SSL definition*. (2020). Cloudflare. https://www.cloudflare.com/learning/ssl/what-is-ssl/

[26] Western Digital Corporation. (2019). WD RedTM [Especificaciones de producto]. media.flixcar.com. https://media.flixcar.com/f360cdn/Western_Digital-4160230904-esn_spec_data_sheet_2879-800002.pdf