Servidor de Archivos

Tema 5

Prof. Ing. Angel Brito Segura

1. Introducción

Los servidores de archivos son una instancia de un servidor central de una red de computadoras que permite a los clientes conectados acceder a un conjunto de archivos o parte del mismo. El término abarca tanto el hardware como el software que se necesita para implementar dicho servidor. Si los usuarios obtienen los correspondientes permisos, pueden abrir las carpetas y archivos guardados en el servidor, así como consultarlos, modificarlos, eliminarlos o subir sus propios documentos.

Este tipo de servidores proporciona a los usuarios un lugar de almacenamiento centralizado para sus propios archivos, disponible para todos los clientes autorizados. El administrador del servidor establece unas directrices estrictas para determinar qué usuarios tienen derechos de acceso y a qué datos.

Para poder contar con un servidor de archivos se debe contar con suficiente espacio de disco duro para almacenar los archivos y programas deseados (incluidos el sistema operativo y el software necesarios para el uso del cliente). Además, el servidor necesita suficiente memoria RAM y capacidad de procesamiento para gestionar el acceso a los archivos y programas por parte de los diferentes usuarios de forma rápida y sin errores. El acceso al servidor de archivos por Internet generalmente se realiza a través del Protocolo de Transferencia de Archivos (FTP) o su variante cifrada SFTP. Alternativamente, también se utilizan los protocolos seguros SCP (Secure Copy o copia segura) y WebDAV, basado en HTTP.

2. Protocolos

Los protocolos de red especiales son responsables de la comunicación entre el servidor y los clientes: mientras que el protocolo ***SMB (Server Message Block)***, desarrollado por IBM, se usa en redes locales con dispositivos Windows y macOS, los ordenadores con distribuciones de Linux utilizan, en la mayoría de los casos, el protocolo NFS (Network File System). De ser necesario, desde Linux es posible conectarse con un servidor SMB a través de ***Samba***.

2.1. SFTP

Definido en el RFC 913, es el único protocolo seguro de transferencia de archivos que protege contra ataques en cualquier punto del proceso de transferencia de datos, lo que lo convierte en el protocolo preferido.

Durante la transferencia de archivos, todos los datos se dividen en paquetes y se envían a través de una única conexión segura. La información confidencial se cifrará y se volverá ilegible cuando se transfiera entre el cliente y el servidor. Solo el destinatario con la clave de descifrado requerida podrá ver el contenido original. Esto evita cualquier acceso no autorizado durante la transferencia de archivos.

Mientrsa que el protocolo de transferencia de archivos (FTP) tiene dos canales diferentes para intercambiar datos: el canal de comando y el canal de datos, el protocolo SFTP tiene solo un canal cifrado donde los datos se intercambian en paquetes formateados cifrados y al ser un subsistema de SSH admite todos los métodos de autenticación de este protocolo. Para conectarse a un servidor SFTP, se necesita un cliente de SFTP, ya sea con interfaz gráfica de usuario como FileZilla, WinSCP o Cyberduck, o bien, a través de la línea de comandos con el comando `sftp`.

```
$ sftp [-oPort=<puerto>] <nombre-usuario>@<IP-servidor>
```

Código fuente 1: Conexión con servidor SFTP

FTP	FTP/SSL	SFTP
Plain FTP	FTP over TLS/SSL	SSH File Transfer Protocol
• Transfer not encrypted • Clear-text password sent over the network • Typically runs over TCP port 21 • Defined by RFC 959 and 1123 • Extended by RFC 3659	• Often called 'FTPS' • Often called 'Secure FTP' • Plain FTP over TLS/SSL channel • Password is encrypted • Transfer is encrypted • Typically runs over TCP port 21 or 990 • Defined by RFC 959 and 1123 • Extended by RFC 2228, 3659 and 4217	• Has nothing common with original FTP • Often called 'Secure FTP' • Password is encrypted • Transfer is encrypted • Typically runs over TCP port 22 • RFC never finished

Figura 1: Comparativo entre FTP, FTPS y SFTP

2.2. Comandos básicos

Para verificar qué directorio de trabajo local y qué directorio remoto estás usando, se cuenta con los siguientes comandos:

```
sftp> lpwd
```

Código fuente 2: Directorio de trabajo local

```
sftp> pwd
```

Código fuente 3: Directorio de trabajo remoto

Para transferir un archivo desde un servidor remoto a la máquina local, se utiliza el siguiente comando:

```
sftp> get <ruta-absoluta-servidor-remoto>/<nombre-archivo>
```

Código fuente 4: Descarga de archivo

Para transferir varios archivos, se utiliza el siguiente comando:

```
sftp> mget <ruta-absoluta-servidor-remoto>/*.<extensión>
```

Código fuente 5: Descarga de varios archivos

Para transferir un archivo desde la máquina local a un servidor remoto, se utiliza el siguiente comando:

```
sftp> put <ruta-absoluta-local>/<nombre-archivo>
```

Código fuente 6: Subida de archivo

Para transferir varios archivos, se utiliza el siguiente comando:

```
sftp> mput <ruta-absoluta-local>/*.<extensión>
```

Código fuente 7: Subida de varios archivos

Para salir de la sesión SFTP, se utiliza el siguiente comando:

```
sftp> exit
```

Código fuente 8: Salir de la sesión

2.3. NFS

El protocolo ***NFS (Network File System)*** es un protocolo de red que permite a los sistemas operativos Unix compartir archivos y directorios en una red. NFS fue desarrollado por Sun Microsystems en 1984 y es un protocolo abierto que permite a los usuarios acceder a archivos en un servidor remoto como si estuvieran en su propio sistema local.

El protocolo NFS se basa en el modelo cliente-servidor, donde el servidor es responsable de almacenar los archivos y proporcionar acceso a los clientes. Los clientes pueden montar los sistemas de archivos remotos en sus sistemas locales y acceder a los archivos como si estuvieran almacenados en su propio sistema.

El protocolo NFS consta de dos componentes principales: el servidor NFS y el cliente NFS. El servidor NFS es responsable de almacenar los archivos y proporcionar acceso a los clientes, mientras que el cliente NFS es responsable de montar los sistemas de archivos remotos y acceder a los archivos.

El protocolo NFS utiliza el protocolo RPC (Remote Procedure Call) para permitir que los clientes realicen llamadas a procedimientos remotos en el servidor. El servidor NFS escucha en el puerto 2049 y utiliza el protocolo TCP o UDP para la comunicación.

Para montar un sistema de archivos remoto en un sistema local, se utiliza el comando `mount` con la opción `-t` para especificar el tipo de sistema de archivos con la dirección IP del servidor NFS y el directorio remoto como se muestra en el siguiente comando:

```
$ sudo mount -t nfs <IP-servidor>:/<directorio-remoto> <directorio-local>
```

Código fuente 9: Montaje de sistema de archivos remoto

Para desmontar un sistema de archivos remoto, se utiliza el comando `umount` seguido del directorio local.

```
$ sudo umount <directorio-local>
```

Código fuente 10: Desmontaje de sistema de archivos remoto

2.4. Samba

Implementación del protocolo SMB/CIFS que permite a los sistemas operativos Unix compartir archivos e impresoras con sistemas Windows. Samba es un software de código abierto que permite a los sistemas Unix actuar como servidores de archivos y proporcionar acceso a los clientes de Windows.

Samba consta de dos componentes principales: el servidor Samba y el cliente Samba. El servidor Samba es responsable de almacenar los archivos y proporcionar acceso a los clientes de Windows, mientras que el cliente Samba es responsable de acceder a los archivos compartidos en un servidor Samba.

El servidor Samba escucha en el puerto 139 y utiliza el protocolo TCP/IP para la comunicación. Samba utiliza el protocolo SMB/CIFS para permitir a los clientes de Windows acceder a los archivos compartidos en un servidor Samba.

Para instalar Samba en un sistema Linux, se utiliza el gestor de paquetes de la distribución. Para configurarlo, se debe editar el archivo de configuración `smb.conf` ubicado en el directorio `/etc/samba/`. En este archivo se definen los recursos compartidos, los permisos de acceso y las opciones de configuración del servidor Samba.

Para acceder a un recurso compartido en un servidor Samba desde un cliente de Windows, se debe abrir el explorador de archivos y escribir la dirección IP del servidor Samba en la barra de direcciones. Se mostrarán los recursos compartidos disponibles en el servidor Samba y se podrá acceder a ellos con las credenciales de usuario correspondientes.

3. Distribuidos

Un sistema de archivos distribuido (DFS) es un sistema de archivos que permite a los usuarios acceder y compartir archivos y directorios en una red de computadoras. Este tipo de servidores se utilizan en entornos donde los usuarios necesitan acceder a los mismos archivos y directorios desde diferentes ubicaciones geográficas.

Estos servidores son esquemas de almacenamiento y gestión de datos que permite a los usuarios o a las aplicaciones acceder a archivos desde un almacenamiento compartido en cualquiera de los múltiples

servidores en red. Sus datos compartidos y almacenados en un clúster de servidores permiten a muchos usuarios compartir recursos de almacenamiento y archivos de datos en múltiples equipos.

Como subsistema del sistema operativo del equipo, mediante DFS se gestiona, organiza, almacena, protege, recupera y comparte los archivos de datos. Las aplicaciones o los usuarios pueden almacenar o acceder a los archivos de datos en el sistema como lo harían con un archivo local. Desde sus ordenadores o teléfonos inteligentes, los usuarios pueden ver todas las carpetas compartidas de DFS como una ruta única que se ramifica en una estructura arbolada a los archivos almacenados en varios servidores.

El DFS tiene dos componentes críticos:

1. **Transparencia de la ubicación**: esto significa que los usuarios verán un único espacio de nombres para todos los archivos de datos, independientemente del ordenador que utilicen para acceder o almacenar los archivos. Los usuarios no podrán saber dónde se almacenó el archivo por primera vez y podrán mover archivos dentro de las carpetas según sea necesario sin tener que cambiar el nombre de la ruta.
2. **Redundancia**: mediante una característica de replicación de archivos, DFS extiende copias de un archivo a través de los nodos del clúster, lo que significa que los datos permanecen altamente disponibles, incluso en caso de fallo del servidor.

3.1. Funcionamiento

Mediante DFS, los terminales y servidores se conectan en red para crear un sistema de archivos paralelo con un clúster de nodos de almacenamiento. El sistema se agrupa bajo un único espacio de nombres y un grupo de almacenamiento y puede permitir el acceso rápido a los datos a través de varios hosts, o servidores, simultáneamente.

Los datos en sí pueden residir en diversos dispositivos o sistemas de almacenamiento, desde unidades de disco duro (HDD) hasta unidades de estado sólido (SSD) y la cloud pública. Independientemente de dónde se almacenen los datos, DFS se puede configurar como un espacio de nombres autónomo (o independiente), con solo un servidor host o un espacio de nombres basado en dominios con varios servidores host.

Cuando un usuario hace clic en un nombre de archivo para acceder a esos datos, el DFS comprueba varios servidores, dependiendo de dónde se encuentre el usuario, y luego sirve la primera copia disponible del archivo en ese grupo de servidores. Esto evita que cualquiera de los servidores se atasque demasiado cuando muchos usuarios acceden a los archivos y también mantiene los datos disponibles a pesar de que el servidor funcione mal o falle.

A través de la función de replicación de archivos DFS, cualquier cambio realizado en un archivo se copia en todas las instancias de ese archivo en los nodos del servidor.

3.2. Características

Hay muchas soluciones DFS diseñadas para ayudar a las empresas a gestionar, organizar y acceder a sus archivos de datos, pero la mayoría de esas soluciones incluyen las siguientes características:

- ***Transparencia de acceso***: los usuarios acceden a los archivos como si estuvieran almacenados localmente en sus propios terminales
- ***Transparencia de la ubicación***: las máquinas host no necesitan saber dónde se encuentran los datos del archivo porque el DFS lo gestiona
- ***Bloqueo de archivos***: el sistema bloquea los archivos en uso en todas las ubicaciones para evitar que dos usuarios de diferentes ubicaciones hagan cambios en el mismo archivo al mismo tiempo
- ***Cifrado de datos en tránsito***: DFS protege los datos cifrándolos a medida que se mueven por el sistema
- ***Compatibilidad con varios protocolos***: los hosts pueden acceder a los archivos mediante una variedad de protocolos, como Server Message Block (SMB), Network File System (NFS) y Portable Operating System Interface (POSIX), por nombrar solo algunos

Referencias

[1] B. A. Forouzan, *Data Communications and Networking*. McGraw-Hill, 2003.

[2] D. E. Comer, *Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture*. Pretince Hall, 2000.

[3] C. Hunt, *TCP/IP Network Administration*. O'Reilly Media, 2002.

[4] J. Edwards y R. Bramante, *Networking Self-Teaching Guide OSI, TCP/IP, LANs, MANs, WANs, Implementation, Management, and Maintenance*. Wiley, 2009.

[5] M. Burgess, *Principles of Network and System Administration*. Wiley, 2004.

[6] K. R. Fall y W. R. Stevens, *TCP/IP Illustrated, Volume 1: The Protocols*. Pearson, 2012.

[7] K. Siyan y T. Parker, *TCP/IP Unleashed*. Sams Publishing, 2002.

[8] C. M. Kozierok, *The TCP/IP Guide*. Charles M. Kozierok, 2005.

[9] IONOS. «File server: definición y aspectos básicos.» (2023), dirección: https://www.ionos.mx/digitalguide/servidores/know-how/file-server/. (accedido: 05.02.2025).

[10] D. A. «Qué es y cómo utilizar SFTP (Protocolo de transferencia de archivos SSH).» (2024), dirección: https://www.hostinger.com/mx/tutoriales/como-usar-sftp. (accedido: 05.02.2025).