IMPLANTACIÓN DE SISTEMAS OPERATIVOS

13 Mayo de 2025

Índice

1 Servicio de ficheros distribuidos,(DFS).

Definición: es un esquema de almacenamiento y gestión de datos que permite a los usuarios o a las aplicaciones acceder a archivos de datos como PDF, documentos de Word, imágenes, archivos de vídeo, archivos de audio, etc., desde un almacenamiento compartido en cualquiera de los múltiples servidores en red

Hay dos razones principales por las que una empresa usaría un sistema de archivos distribuidos (DFS):

- Para almacenar datos de forma permanente en soportes de almacenamiento secundario.
- Para compartir información de forma fácil, eficiente y segura entre usuarios y aplicaciones.

El DFS tiene dos componentes críticos:

- 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.

- 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.

1 Servicio de ficheros distribuidos,(DFS).

Características de los sistemas de archivos distribuidos (DFS)

- **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

Ventajas

Permite acceder a los mismos datos desde muchos lugares.
También hace que el intercambio de información en todas las geografías sea simple y extremadamente eficiente.

•**Resiliencia de los datos** – como los archivos residen en más de una ubicación, un fallo del servidor no será señal de desastre.

•**Eficiencia de la red** – las cargas de trabajo pesadas no ralentizarán el sistema porque DFS puede recopilar datos del siguiente nodo disponible.

•**Acceso a la información más reciente** – los cambios realizados en las carpetas o archivos compartidos son visibles y están disponibles al instante para todos los que utilizan el DFS.

•**Escalabilidad sencilla** – para hacer crecer el sistema basta con añadir más nodos – Alta fiabilidad - la pérdida de datos es mucho menos preocupante cuando los archivos se replican entre hosts.

2 Encriptación de datos

La **encriptación** es el proceso de transformar información legible (texto claro) en una forma ilegible (texto cifrado) para protegerla durante su almacenamiento o transmisión. El principal objetivo es garantizar la **confidencialidad**, asegurando que solo las personas autorizadas puedan acceder a los datos en su formato original

Importancia de la Encriptación en la Seguridad de la Información
La encriptación es esencial para la **protección de datos sensibles** en sistemas informáticos, redes de comunicación, y bases de datos, evitando accesos no autorizados y garantizando la integridad y privacidad de la información.

Tipos de Amenazas a la Seguridad de los Datos
- **Acceso no autorizado**: Ataques de hackers que intentan obtener acceso a datos privados.
- **Intercepción de datos**: Escucha de comunicaciones a través de redes inseguras.
- **Alteración de datos**: Manipulación o corrupción de la información almacenada o transmitida.

2 Encriptación de datos

Para encriptar utilizamos algoritmos:

Los **algoritmos criptográficos** son herramientas matemáticas que permiten estos procesos.

Algoritmos Simétricos y Asimétrico

- **Simétricos**: La misma clave se usa para encriptar y desencriptar los datos. Ejemplos: **AES, DES**.
- **Asimétricos**: Utilizan un par de claves, una pública para encriptar y una privada para desencriptar. Ejemplo: **RSA**.

Claves Criptográficas

- **Simétricas (privadas)**: Ambas partes usan la misma clave secreta.
- **Asimétricas (públicas)**: La clave pública se puede compartir, mientras que la clave privada debe mantenerse en secreto.

2 Encriptación de datos

Criptografía Simétrica

La principal **ventaja** es que es rápida y eficiente, pero la desventaja es la gestión de claves, ya que ambas partes deben tener la misma clave secreta.

Desventaja: El intercambio seguro de claves puede ser un desafío en redes no confiables.

Algoritmos de Encriptación Simétrica:

- **AES (Advanced Encryption Standard)**: El estándar actual, muy utilizado debido a su alta seguridad y eficiencia.
- **DES (Data Encryption Standard)**: Algoritmo más antiguo, ahora obsoleto debido a su vulnerabilidad a ataques de fuerza bruta.
- **RC4**: Un algoritmo de flujo de clave, ampliamente utilizado en protocolos como **SSL/TLS**, aunque también obsoleto debido a debilidades en su diseño.

2 Encriptación de datos

Criptografía Asimétrica

En la criptografía asimétrica, se utilizan dos claves: una pública para encriptar y una privada para desencriptar. Este sistema resuelve el problema de la distribución de claves de la criptografía simétrica.

Algoritmos de Encriptación Asimétrica

- **RSA**: Uno de los algoritmos más utilizados. Basado en la dificultad de factorizar grandes números primos.
- **ElGamal**: Utilizado en aplicaciones como PGP para la encriptación de correo electrónico.
- **ECC (Curvas Elípticas)**: Un enfoque más eficiente en cuanto a la seguridad por bit de clave, utilizado en muchas aplicaciones modernas.

Certificados Digitales y PKI (Infraestructura de Clave Pública)

Los **certificados digitales** aseguran que una clave pública pertenece realmente a una entidad. **PKI** es el sistema que gestiona, distribuye y revoca certificados y claves públicas.

Firma Digital

Utiliza criptografía asimétrica para garantizar la autenticidad de un mensaje. El remitente firma un mensaje con su clave privada, y el receptor verifica la firma usando la clave pública del remitente.

2 Encriptación de datos

Protocolos Criptográficos

SSL/TLS

- **SSL/TLS**: Protocolo que asegura las comunicaciones en la web mediante encriptación.
- Establece un canal seguro entre un servidor web y un cliente mediante un proceso de autenticación de certificados y establecimiento de claves compartidas.

IPsec

- **IPsec**: Protocolo que proporciona seguridad en la capa de red, cifrando los paquetes IP para proteger las comunicaciones en redes privadas virtuales (VPNs).

PGP/GPG

- **PGP (Pretty Good Privacy)** y **GPG (GNU Privacy Guard)** son protocolos de encriptación utilizados principalmente en correo electrónico. Garantizan la confidencialidad y la autenticidad de los mensajes.

VPN (Red Privada Virtual)

Una **VPN** usa criptografía para asegurar que las conexiones de red entre un usuario y un servidor remoto sean privadas, encriptando todos los datos que viajan por la red.

3 Compresión de datos

Definición: es el proceso de reducir el tamaño de un archivo o conjunto de datos con el fin de almacenar o transmitir dicha información de manera más eficiente. Este proceso busca reducir el uso de espacio de almacenamiento y aumentar la velocidad de transmisión, manteniendo la integridad de los datos.

Importancia de la Compresión de Datos

- **Eficiencia en el almacenamiento**: Permite almacenar más datos en el mismo espacio.
- **Optimización en la transmisión:** Reduce el tiempo necesario para enviar datos a través de redes, ideal para conexiones lentas.
- **Costos**: Disminuye los costos relacionados con el almacenamiento y el ancho de banda.
- **Respaldo y recuperación de datos**: Facilita la creación de copias de seguridad de manera más eficiente.

Tipos de Compresión de Datos

1. **Compresión sin pérdida (Lossless)**: La información original se puede recuperar exactamente sin pérdida de datos. Formatos y APP: .zip .tar.gz, código fuentes, compresión de BBDD

2. **Compresión con pérdida (Lossy)**: Algunos datos se descartan para reducir el tamaño del archivo, lo que puede resultar en una pérdida de calidad. Formatos y APP: JPEG MP3. Youtube o Netflix

3 Compresión de datos

Tipos de Compresión de Datos

1. **Compresión sin pérdida (Lossless)**: La información original se puede recuperar exactamente sin pérdida de datos. Formatos y APP: .zip .tar.gz, código fuentes, compresión de BBDD

2. **Compresión con pérdida (Lossy)**: Algunos datos se descartan para reducir el tamaño del archivo, lo que puede resultar en una pérdida de calidad. Formatos y APP: JPEG MP3. Youtube o Netflix

- **Ventaja**: Alta reducción en el tamaño de los archivos.

- **Desventaja**: La pérdida de calidad puede ser notable en algunos casos, dependiendo del nivel de compresión.