PR0203: Copia de seguridad mediante SSH

Aspectos generales

Objetivos de la práctica

En esta práctica veremos otra utilidad de SSH, que es la posibilidad de crear copias de seguridad remotas.

Recursos

1. Box Ubuntu 22.04
2. How to change hostname on Ubuntu 22.04
3. How to make Windows resolve local hosts by their name

Entorno de trabajo

Esta práctica la realizaremos en un Ubuntu Server 22.04 LTS, para utilizar todos el mismo entorno usarás el box denominado `generic/ubuntu2204`.

¿Qué tenemos que saber antes?

Hasta ahora hemos visto varias posibilidades con SSH: conexión a un equipo remoto y transferencia segura de ficheros (SCP).

En esta práctica veremos otra posibilidad diferente que consiste en utilizar SSH para tunelizar con una conexión segura las copias de seguridad en nuestro sistema. Para ello vamos a combinar SSH con el comando `rsync`, que permite sincronizar diferentes carpetas.

RSync es una utilidad diseñada para realizar copias de datos incrementales minimizando la cantidad de información que ha de transmitirse. El truco de `rsync` consiste en utilizar un checksum rotatorio. Los archivos se dividen en bloques, y se utiliza una función resumen (por ejemplo, SHA1) y se utiliza un chequeo rotatorio para determinar los bloques que han cambiado. `RSync` solo envía los bloques que se han modificado (su función resumen es diferente).

Uso básico de `rsync`

El uso más básico de `rsync` es utilizarlo para realizar copias de seguridad locales en el propio equipo, en una carpeta diferente. La sintaxis de este comando es:

```
rsync modificadores fuente destino
```

Donde fuente y destino son dos directorios. Al indicar el directorio tenemos dos posibilidades:

- Si finaliza con el carácter / estamos indicando que lo que queremos copiar es el contenido del directorio, no el propio directorio.
- Si el directorio no finaliza con el carácter / estamos copiando el directorio completo.
-

Básicamente, esto se traduce en que si no ponemos la barra al final creará un directorio con el nombre del que copiemos en el directorio destino y dentro de él colocará los ficheros. Si ponemos la barra al final, solo copiará los ficheros.

Algunos de los modificadores que admite son:

- `--recursive`: incluye los subdirectorios
- `--links`: copia los enlaces como enlaces
- `--perms`: conserva los permisos
- `--times`: preserva la fecha de modificación
- `--group`: preserva el grupo
- `--owner`: preserva el usuario
- `-a:` incluye todos los modificadores anteriores
- `-v:` modo verbose, hará que se muestre más información por pantalla
- `--delete`: borra los ficheros que se encuentren en el segundo directorio y no en el primero.
- `-z:` comprime los datos
- `-P:` muestra el progreso
- `-c:` utiliza checksums para verificar que los archivos no han cambiado. El comportamiento por defecto es fijarse en si ha cambiado la fecha o el tamaño.
- `-u:` solo se fija en las fechas.
- `--size`-only: solo se fija en el tamaño.
- `-l:` copia todos los ficheros.

En la siguiente imagen tienes un ejemplo de ejecución de rsync.

Copias remotas con `rsync`

El comando rsync tiene varias posibilidades para crear copias remotas, pero en esta práctica nos interesan las **copias tunelizadas mediante SSH**. Para esto necesitamos que el equipo que vaya a alojar la copia de seguridad tenga instalado el servidor SSH, tal y como hemos visto en otras prácticas. Como ya hemos visto otras veces, por cuestiones de seguridad es conveniente configurar SSH para que únicamente admita conexiones mediante pares de claves pública/privada.

Una vez configurado el servidor SSH tenemos que realizar los siguientes pasos en el equipo que va a alojar las copias de seguridad:

- Crear un directorio donde alojar las copias de seguridad
- Crear el usuario que utilizaremos. Lo ideal es crear un usuario que se utilizará exclusivamente para realizar las copias de seguridad en lugar de utilizar un usuario ya creado en el sistema.
- Asignar los permisos que necesite el directorio y modificar su propietario para que sea el que hemos creado en el paso anterior.

Ya solo queda realizar las copias de seguridad desde el equipo cliente. La sintaxis de rsync para ese caso es:

```
rsync -av --delete origen [-e ssh] nombre_usuario@ip_destino:destino
```

El modificador `-e ssh` es opcional. También se podría indicar una ruta remota en el origen utilizando la misma sintaxis.

Ejercicios

Ejercicio 1

Suponemos que nuestro usuario en Ubuntu Server quiere hacer una copia de seguridad local diaria de los datos contenidos en su directorio personal.

Realiza y documenta los pasos necesarios para conseguir este objetivo utilizando cron y `rsync`. Puedes tomar las decisiones que consideres necesarias (p.e. directorios, ...) , pero tomando la precaución de documentarlas

Ejercicio 2

Vamos a realizar ahora una copia de seguridad remota. Utilizarás el Ubuntu Server para alojar la copia de seguridad y la máquina virtual con Linux Mint como origen de la copia de seguridad.

Tienes que realizar todos los pasos necesarios para mantener en el servidor una copia de seguridad del contenido del directorio `Documentos` del usuario del cliente.

Debes tener en cuenta lo siguiente:

- Debes documentar los pasos más importantes y las decisiones que tomes.
- En el servidor vas a crear un usuario específico como operador de copias de seguridad.
- Es tu decisión la carpeta del servidor donde alojarás las copias de seguridad, pero debes asegurarte de tener los permisos correctamente configurados para que únicamente el operador de copias de seguridad pueda acceder a ellos.
- También debes configurar SSH en el servidor con las siguientes características:
    - No debe permitir el acceso remoto al usuario root
    - Solamente puede acceder el usuario operador de las copias de seguridad
    - El acceso debe ser transparente para el usuario, es decir, no debe solicitar la contraseña al acceder por SSH
- Para comprobar que funciona debes programar la copia de seguridad para que se realice cada 2 minutos.
- Comprueba que funciona. Crea un fichero en el directorio Documents y espera un par de minutos. Luego verifica que dicho fichero se ha actualizado en el directorio de la copia de seguridad.