Unidad 1: Introducción al módulo

- ¿Cómo crearemos nuestras máquinas virtuales en AWS Academy?

Aprenderemos a crear servidores virtuales en AWS, conocidos como EC2. Aunque la creación es siempre igual, independientemente del sistema operativo que instalemos, el acceso posterior será diferente en función de que nos conectemos en modo comando o en modo gráfico. Crearemos una máquina Linux a la que accederemos en modo comando por SSH y un servidor Windows al que accederemos en modo gráfico con RDP.

- ¿Cómo nos conectaremos por SSH a nuestras máquinas virtuales en AWS Academy?

Para conectarnos a una máquina de forma remota y segura en modo comando, la opción más recomendable es SSH. SSH o Secure Shell es un protocolo de red criptográfico para operar servicios de red de forma segura a través de una red no protegida. Las aplicaciones típicas incluyen línea de comandos remota, inicio de sesión y ejecución de comandos remota, pero cualquier servicio de red puede protegerse con SSH.

Autenticación

Los dos métodos de autenticación de usuario SSH más comunes que se utilizan son las contraseñas (cifrado simétrico) y las claves SSH (cifrado asimétrico o de clave pública). Los clientes envían contraseñas cifradas al servidor de forma segura. Sin embargo, las contraseñas son un método de autenticación arriesgado porque su solidez depende de que el usuario sepa qué hace que una contraseña sea segura.

- Cifrados simétricos o de clave privada:

Este tipo de cifrado utiliza la misma clave para cifrar y para descifrar la información. Por este motivo, la clave debe ser secreta y sólo conocida por el emisor y el receptor del mensaje.

- Cifrados asimétricos o de clave pública:

En este tipo de cifrados cada usuario utiliza un par de claves: una clave pública y una clave privada. Un mensaje cifrado con la clave pública sólo se puede descifrar con su correspondiente clave privada y viceversa.

La clave pública es accesible a cualquier persona que quiera consultarla, no hace falta que sea transmitida por un canal seguro.
La clave privada sólo la debe conocer su dueño.

Funcionamiento

El emisor cifra un mensaje con la clave pública del receptor. El receptor recibe el mensaje y es el único que podrá descifrarlo porque es el único que posee la clave cifrada asociada.

Aplicaciones diferentes de SSH

Gestión de servidores a los que no se puede acceder localmente

Transferencia segura de archivos

Creación de copias de seguridad

Conexión entre dos ordenadores con encriptación de extremo a extremo

Mantenimiento remoto desde otros ordenadores

Prácticas

P1.1. Linux Server en AWSAcademy

P1.2 Windows Server en AWSAcademy

P1.3. Conceder acceso a un segundo administrador

P1.4 Introducción a git y GitHub

P1.5. Git Trabajando con ramas y uniones

P1.6 Introducción a Markdown

By **jaotalvaro**
cheatography.com/jaotalvaro/

Not published yet.
Last updated 18th September, 2023.