**Qué es SSH?**

Secure Shell (SSH) es un protocolo de conexión cifrada que permite inicios de sesión seguros a través de conexiones no seguras. SSH permite conectarse a un shell de terminal desde una ubicación remota mediante una conexión de red.

Se pueden usar dos métodos para autenticar una conexión SSH: **nombre de usuario y contraseña** o un **par de claves SSH**.

Aunque SSH proporciona una conexión cifrada, el uso de contraseñas con conexiones SSH deja a la máquina virtual vulnerable ante ataques por fuerza bruta de contraseñas. Un método más seguro y preferible para conectarse a una máquina virtual Linux con SSH es un par de claves pública- privada, lo que se conoce también como claves SSH.

Con un par de claves SSH, puede iniciar sesión en máquinas virtuales de Azure basadas en Linux sin contraseña. Este método es más seguro si solo se planea iniciar sesión en la máquina virtual desde varios equipos. Si necesita poder acceder a la máquina virtual Linux desde varias ubicaciones, es posible que una combinación de nombre de usuario y contraseña sea un enfoque mejor.

Un par de claves SSH consta de dos partes: una clave pública y una clave privada.

* La clave pública se coloca en la máquina virtual Linux o en cualquier otro servicio que se quiera usar con una criptografía de clave pública. Se puede compartir con cualquiera.
* La **clave privada** es la que se presenta para verificar la identidad en la máquina virtual Linux al crear una conexión SSH. Considere que es información confidencial y protéjala como si fuera una contraseña o cualquier otro dato privado.

Puede usar el mismo par único de claves pública y privada para acceder a varios servicios y máquinas virtuales de Azure.

**Creación del par de claves SSH**

En Windows 10, Linux y macOS, puede usar el comando ssh-keygen integrado para generar los archivos de clave pública y privada SSH.

Windows 10 incluye un cliente SSH con **Fall Creators Update**. Las versiones anteriores de Windows requieren software adicional para el uso de SSH. Como alternativa, puede instalar el subsistema de Linux para Windows y obtener la misma función.

Usaremos Azure Cloud Shell, que almacena las claves generadas en Azure en la cuenta de almacenamiento privado. Si lo prefiere, también puede escribir estos comandos directamente en el shell local. Si adopta este método, deberá ajustar las instrucciones que aparecen a lo largo de este módulo para reflejar una sesión local.

Aquí está el comando mínimo necesario a fin de generar el par de claves para una máquina virtual de Azure. Esto crea un par de claves pública y privada de RSA con el protocolo SSH 2 (SSH 2). La longitud mínima es de 2048 bits, pero para este módulo de aprendizaje usaremos 4096.

1. En Cloud Shell, ejecute el comando siguiente.

BashCopiar

ssh-keygen -m PEM -t rsa -b 4096

1. Presione Entrar para aceptar la ubicación predeterminada. El comando crea dos archivos: id\_rsa e id\_rsa.pub, en el directorio ~/.ssh. Si los archivos existen, se sobrescriben.
2. Escriba una frase de contraseña que pueda recordar. Necesitará esta frase de contraseña cuando use la clave SSH para acceder a la máquina virtual.

Se pueden usar varias opciones para especificar el nombre de archivo o una frase de contraseña a fin de evitar las solicitudes.

**Frase de contraseña de clave privada**

También se puede especificar una frase de contraseña al generar la clave privada. Es una contraseña que debe escribir al usar la clave. Esta frase de contraseña se usa para acceder al archivo de claves SSH privado y no es la contraseña de la cuenta de usuario.

Cuando agrega una frase de contraseña a la clave SSH, cifra la clave privada mediante AES de 128 bits para que la clave privada no se pueda usar sin la frase de contraseña para descifrarla.

Se recomienda encarecidamente agregar una frase de contraseña. Si un atacante robara su clave privada y esta no tuviera una frase de contraseña, podría usarla para iniciar sesión en los servidores que tuvieran la clave pública correspondiente. Si una frase de contraseña protege una clave privada, ese atacante no la puede usar. Esto proporciona una capa adicional de seguridad para la infraestructura en Azure.

**Usar el par de claves SSH con una máquina virtual Linux de Azure**

Cuando se haya generado el par de claves, podrá usarlo con una máquina virtual Linux en Azure. La clave pública se puede especificar durante la creación de máquinas virtuales o se puede agregar después de que se haya creado la máquina virtual.

Puede ver el contenido del archivo en Cloud Shell si ejecuta el comando siguiente.

BashCopiar

cat ~/.ssh/id\_rsa.pub

Tendrá un aspecto similar a la salida siguiente:

ResultadosCopiar

ssh-rsa XXXXXXXXXXc2EAAAADAXABAAABAXC5Am7+fGZ+5zXBGgXS6GUvmsXCLGc7tX7/rViXk3+eShZzaXnt75gUmT1I2f75zFn2hlAIDGKWf4g12KWcZxy81TniUOTjUsVlwPymXUXxESL/UfJKfbdstBhTOdy5EG9rYWA0K43SJmwPhH28BpoLfXXXXXGX/ilsXXXXXKgRLiJ2W19MzXHp8z3Lxw7r9wx3HaVlP4XiFv9U4hGcp8RMI1MP1nNesFlOBpG4pV2bJRBTXNXeY4l6F8WZ3C4kuf8XxOo08mXaTpvZ3T1841altmNTZCcPkXuMrBjYSJbA8npoXAXNwiivyoe3X2KMXXXXXdXXXXXXXXXXCXXXXX/ azureuser@myserver

Copie este valor para poder usarlo en el ejercicio siguiente.

**Uso de la clave SSH al crear una máquina virtual Linux**

Para aplicar la clave SSH al crear una nueva máquina virtual Linux, será preciso copiar el contenido de la clave pública y especificarlo en Azure Portal, *o* especificar el archivo de clave pública para el comando de CLI de Azure o de Azure PowerShell. Usaremos este método al crear nuestra máquina virtual Linux.

**Adición de la clave SSH a una máquina virtual Linux existente**

Si ya ha creado una máquina virtual, puede instalar la clave pública en la máquina virtual Linux con el comando ssh-copy-id. Cuando se haya autorizado la clave SSH, se concederá acceso al servidor sin contraseña, aunque se le seguirá pidiendo la frase de contraseña en la clave si la tiene establecida.

Por ejemplo, si tuviéramos una máquina virtual Linux denominada *myserver* con un usuario *azureuser*, podríamos ejecutar el comando siguiente para instalar el archivo de clave pública y autorizar al usuario con la clave.

BashCopiar

ssh-copy-id -i ~/.ssh/id\_rsa.pub azureuser@myserver

Ahora que tenemos la clave pública, vamos a cambiar a Azure Portal y crear una máquina virtual Linux.