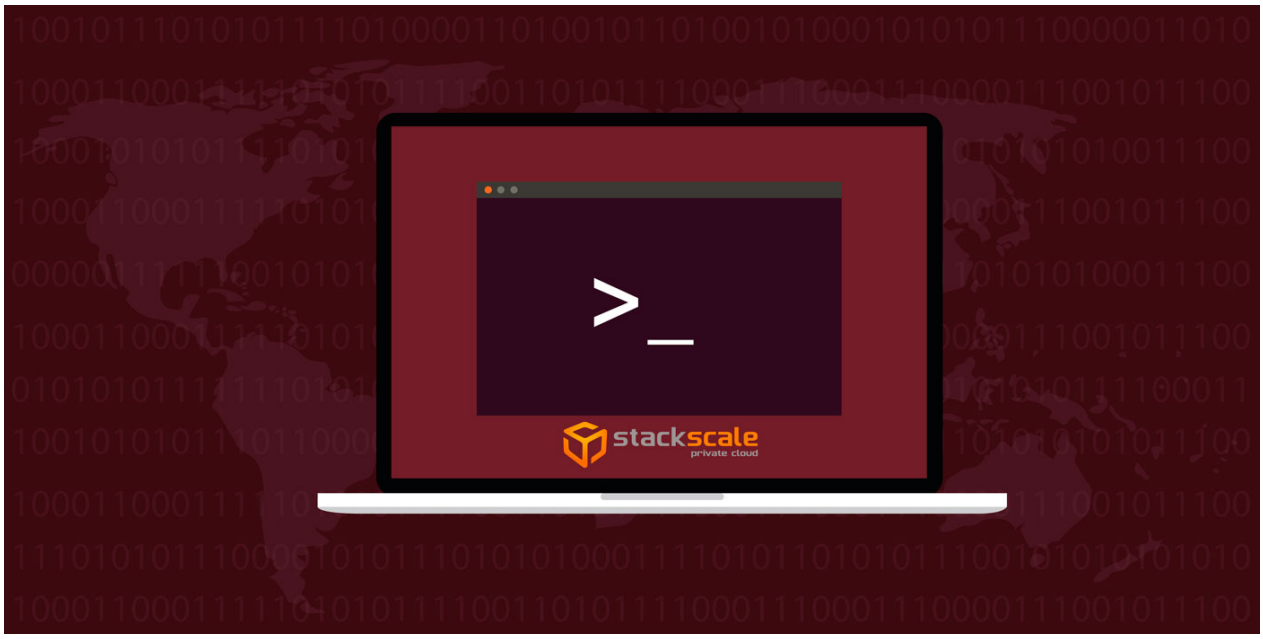
Aprende a configurar las llaves SSH en un servidor Linux

01/Jul/2016 - Sistemas



No siempre estamos delante de un servidor para poder conectarnos, sino que lo más habitual es tener que hacerlo de forma remota. Dependiendo del tipo de sistema operativo, las opciones pueden variar. En el caso de Linux, el protocolo SSH es el más utilizado. Lo que hoy os explicaremos será la forma de mejorar aún más la seguridad a la hora de utilizar SSH para conectarnos a nuestra máquina.

¿Qué es la llave SSH?

de un usuario y una contraseña. El problema de este sistema, es que la contraseña podría ser captorada por cualquier atacante, poniendo en riesgo la información que él se guarda. Mientras que esto puede ocurrir con el uso de contraseñas, el uso de llaves SSH es casi imposible de descifrar.

Consiste en la generación de un par de claves que proporciona dos largas cadenas de caracteres, una pública y otra privada. La clave pública es instalada en cualquier servidor, y luego desbloquearla mediante la conexión con un cliente que hace uso de la clave privada. Cuando se da el caso de que las dos claves coinciden, el sistema permite el acceso sin necesidad de tener que utilizar ninguna contraseña.

Si aún queremos mejorar la seguridad, siempre podemos aumentar la protección de la clave privada con el uso de una contraseña. Recomendamos siempre la creación de contraseñas seguras.

Pasos para crear las llaves SSH

Veamos los pasos que debemos seguir para conseguir nuestras llaves SSH

1.- Crear el par de claves RSA

Lo primero de todo, será crear el par de claves en la máquina cliente, que lo más probable es que sea el equipo que sueles utilizar. Para ello, ejecutaremos en la línea de comandos la siguiente instrucción.

```
ssh-keygen -t rsa
```

2.- Almacenar las claves y la contraseña

Una vez que hayamos ejecutado la instrucción para la generación de las claves, nos realizarán algunas preguntas.

```
Enter file in which to save the key (/home/demo/.ssh/id_rsa):
```

La primera pregunta que nos harán será la ruta donde queremos almacenar la clave. Si no escribimos nada y pulsamos la tecla intro, se almacenará en la ruta que aparece entre paréntesis.

```
Enter passphrase (empty for no passphrase):
```

La segunda pregunta hará referencia a la posibilidad de incluir una contraseña. Siempre lo podemos dejar en blanco pero si optamos por indicar una, estaremos mejorando aún más la seguridad, ya que aunque algún hacker consiguiera la clave, no podrían hacer uso de ella mientras que no dieran con la contraseña. El único inconveniente, es que cada vez que se hiera uso de ella, habría que escribirla.

Si todo hay ido de forma correcta, deberíamos ver en pantalla algo parecido a esto:

```
Enter file in which to save the key (/home/demo/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/demo/.ssh/id_rsa.
Your public key has been saved in /home/demo/.ssh/id_rsa.pub.
The key fingerprint is:
4a:dd:0a:c6:35:4e:3f:ed:27:38:8c:74:44:4d:93:67 demo@a
The key's randomart image is:
+--[ RSA 2048]----+
|          .oo.   |
|         .  o.E  |
|        + .  o   |
|     . = = .     |
|      = S = .    |
|     o + = +     |
|      . o + o .  |
|           . o   |
|                 |
+-----------------+
```

La clave pública estará localizada en "*/home/demo/.ssh/id_rsa.pub*", mientras que la clave privada estará localizada en "*/home/demo/.ssh/id_rsa*".

3.- Copiar la clave pública

Una vez que el par de claves están generadas, es hora de colocar la clave pública en el servidor virtual, donde nosotros lo queremos utilizar.

Podemos copiar la clave pública dentro del fichero "*autorized_keys*" en el servidor virtual con la instrucción "*ssh-coppy-id*". Habrá que indicar la dirección IP de la máquina para que el copiado se lleve a cabo de forma correcta.

```
ssh-copy-id user@123.45.69.56
```

Otra alternativa, es pegar la llave utilizando SSH.

```
cat ~/.ssh/id_rsa.pub | ssh user@123.45.56.78 "mkdir -p ~/.ssh && cat >>
~/.ssh/authorized_keys"
```

Independientemente del comando que utilices para ello, deberías ver algo parecido a esto:

```
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '12.34.56.78' (RSA) to the list of known hosts.
user@12.34.56.78's password:
Now try logging into the machine, with "ssh 'user@12.34.56.78'", and check in:
  ~/.ssh/authorized_keys
to make sure we haven't added extra keys that you weren't expecting.
```

4.- Desactivar el acceso para el usuario root

Este último paso es opcional y lo que buscamos con él es mejorar aún más la seguridad. Una vez que hayamos copiado las claves SSH en el servidor y que nos hayamos asegurado de que podemos acceder, podemos restringir el acceso vía SSH al usuario root, permitiendo el acceso únicamente mediante las claves SSH que hemos generado.

Para ello, abriremos el archivo de configuración de SSH.

```
sudo nano /etc/ssh/sshd_config
```

Dentro de este archivo, busque la línea donde aparezca "*PermitRootLogin*". Modifique esta línea para asegurarnos de que sólo se pueda acceder con el uso de las claves SSH generadas.

```
PermitRootLogin without-password
```

Por último, recarga SSH para que los cambios tomen efecto.

```
reload ssh
```

Una vez que hayamos completado todos los pasos explicados en esta entrada, dispondremos de una máquina virtual más segura donde acceder a ella sólo será posible si disponemos de las claves SSH generadas.

Si te ha gustado, compártelo en redes sociales

Categorías

- Cloud Elástico
- Curiosidades
- Entrevistas
- Eventos
- General
- Internet
- Sistemas

¿Quiénes somos?
Nuestros Centros de Datos
Nuestra red
Contactar

Ventajas
Casos de éxito
Blog
Trabaja con nosotros

Cloud Privado
Almacenamiento en red
Infraestructura para ISPs
Servicios gestionados

Solicita una oferta rápida y conoce Stackcale

Solicitar más información

Copyright 2013-2018 Stackscale España - Nervia Digital S.L.