Configuración del cliente SSH para certificados

Cómo configurar una computadora cliente para usar certificados SSH para la autenticación de computadora anfitriona y cliente.

Autenticación de host:

ssh reconocerá los certificados de cualquier computadora host cuyo certificado esté firmado por una autoridad identificada en el archivo /etc/ssh/ssh_known_hosts.

Para configurar esto necesitas la siguiente línea en /etc/ssh/ssh_config:

```
GlobalKnownHostsFile /etc/ssh/ssh_known_hosts
```

Luego, debes agregar una línea como la que se muestra a continuación a /ets/ssh/ssh_known_hosts:

```
cat <<EOF | sudo tee -a /etc/ssh/ssh_known_hosts
@cert-authority * ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDTcMC1gp\
Ey/r0E/nolRkiOH/ppenhnbj1BFHKRi/RdxttVWSHoMg9ilKADdz6nItm2HuEZ04\
tfIIbEs9yH4VdnWbfAbgfkZBHzY4rueXuo7xlnAWx14JMFuCT2WaVRmi6Sf8eUDP\
BB3sGjE2yPWSaQUDp6kMx1V8whES0jiW7CLDOSlU6fW0T6lLgaRZ9h49Rh3jcV3I\
5ZZg1ogD0YNKgjdgnzHuFeGAZCB5fI5L+ndC8KXTKmC7shYN1adSIoWS3XgQiUHm\
ajpwFEIYOBE6/xI8QFU/F44j5EjFvfPq1k9zPEvi0SKV68Rl8JZ0X/SontVRQ/To\
gvYvftDWt32jACdv3vUk+QDpyyym+R7SCOKX/STlT3FDk/yrHMHQBzYO1KKhnVFv\
KzzZs0umsqDSGrYSLialPUJ+ZuXDTSelov+P5s200ZBAPjxYD6YIGiBsPKgHssVQ\
7GUlz1mxgOObQNVQjbrgdGwpdnYpY4YlsogtybI1QIbDtU/fIRPHHeWWBOW+iZ1w\
9/XHnSyP0EFyzk+bYz21lRxJHLBsfWehshM3Mwqs+A3cmwzUyGQCeT8XV+mKe7y1\
VAiqVVQQjhjHCoU+N4XkdM8pUzR0NkC33amlV68e1EDSD0XAtLZCUrJfil18X9/R\
hWkiDVElMOPwmsp3nJ9jU3UQRQ7Yf97V3oLw== pbz@ogopogo.biz_hostca_bzhosts
EOF
```

La autoridad anterior actualmente autentica los siguientes hosts:

autoridad: pbz@ogopogo.biz (tag bzhosts)

- mamey.ogopogo.biz
- repo.ogopogo.biz
- guanabana.bernatchez.net
- relay.bernatchez.net
- relay.ogopogo.biz
- repo.bernatchez.net

Autenticación del cliente:

Genere un par de claves privada/pública con este comando:

```
/usr/bin/ssh-keygen -b 4096 -t rsa -C computadora_propósito -f computadora_propósito
```

Sustituye «computadora» por el nombre del equipo cliente y «propósito» por algo que indique para qué se usará la clave. Algo así:

```
ssh-keygen -b 4096 -t rsa -C pedrolaptop_usario-remoto -f pedrolaptop_usario-remoto
```

Envíe un correo electrónico a la autoridad firmante solicitando un certificado firmado. Adjunte la clave pública generada anteriormente al correo.

La autoridad certificadora adjuntará un certificado que le otorga acceso en un correo electrónico de respuesta. Guarde ese certificado en el mismo directorio donde almacena la clave privada.

Cuando cargue la clave privada en su agente SSH, el certificado también se cargará.

Ejemplo:

```
ssh-add pedrolaptop_usario-remoto
```

Deberás responder con la contraseña correcta para tu clave y obtendrás algo como lo siguiente:

> Enter passphrase for pedrolaptop_usario-remoto:
>
> Identity added: pedrolaptop_usario-remoto (pedrolaptop_usario-remoto) Certificate added: pedrolaptop_usario-remoto-cert.pub (pedrolaptop_usario-remoto)

ASUNTO:

En Ubuntu, la utilidad ssh-add no carga los archivos de certificado. Esto no ocurre cuando ssh-agent es el agente real, sino cuando el agente es el implementado por gnome-keyring.

La solución es dejar de usar el componente ssh de gnome-keyring.

Dado que el proceso de inicialización inicia un agente ssh real y luego lanza gnome-keyring-ssh.desktop, que bloquea AUTH_SOCKET para tomar el control, volvemos al agente ssh original deshabilitando gnome-keyring-ssh.desktop.

Deshabilita gnome-keyring-ssh.desktop:

```
cd /etc/xdg/autostart/
sudo emacs gnome-keyring-ssh.desktop
```

Agregue la siguiente línea al archivo y guárdelo

```
X-GNOME-Autostart-enabled=false
```

Luego reinicie la computadora