Configure ssh certificate based authentication

298 Manu Chacko June 20, 2022 Security Features, Technical, Tweaks & Configuration
24595

Configure Certificate-Based SSH User Authentication

Support for certificate authentication of users and hosts using the new OpenSSH certificate format was introduced in Red Hat Enterprise Linux 6.5, in the openssh-5.3p1-94.el6 package. If required, to ensure the latest OpenSSH package is installed, enter the following command as root :

```
root@server:~#
```

1. Setting Up Certificate Authority Infrastructure

- *Generate the CA key (cert_ca) for signing user ssh keys with the following command :*

Copy the keys to /etc/ssh/

```
cert_ca* /etc/ssh/
```

2. Add CA public key (cert_ca.pub) as Trusted Key in the ssh server machines

Restart SSH service

3. Generate SSH key for the user

4. Sign user ssh public key by CA with the following command :

you should sign with user(username) you want to login to the server

machine. For example, If you want to login as user " TED " to the server, You should sign the with the user " TED ". Example : ssh-keygen -s cert_ca -I user_ted -n ted -V +52w id_rsa.pub

Copy the ssh keys to the client machine .ssh directory

```
@client1
```

Once you copied the ssh keys to the client machine, the user will be able to login into the server with ssh certificate authentication without any password.

```
admin@client1
```

You can also issue short-lived certificates for giving temporary ssh access

Follow the first three steps in the article.

you can generate short-lived certificates for a day or a week or for some minutes while Sign user SSH public key by CA with the following command: You can specify the validity interval (-V)while signing the certificate. We have issued a certificate that is valid for 60 minutes from the generated time. We can specify the Validity after **-V** option.

you should sign with the user(username) you want to log in to the server machine. For example, If you want to login as user " TED " to the server, You should sign the with the user " TED ". Example : ssh-keygen -s cert_ca -I user_ted -n ted -V +60m id_rsa.pub

Copy the ssh keys to the client machine .ssh directory

```
@client1
```

Once you copied the ssh keys to the client machine, the user will be able to login into the server with ssh certificate authentication without any password till 60 minutes from the certificated generated time. The certificate will expire after 60 minutes, so the user will not be able to ssh to that server with that certificate after 60 minutes.

```
admin@client1
```