

Autenticació contra servers

Genera i utilitza diferents certificats digitals com a mitjà d'accés a un servidor remot.

Índex

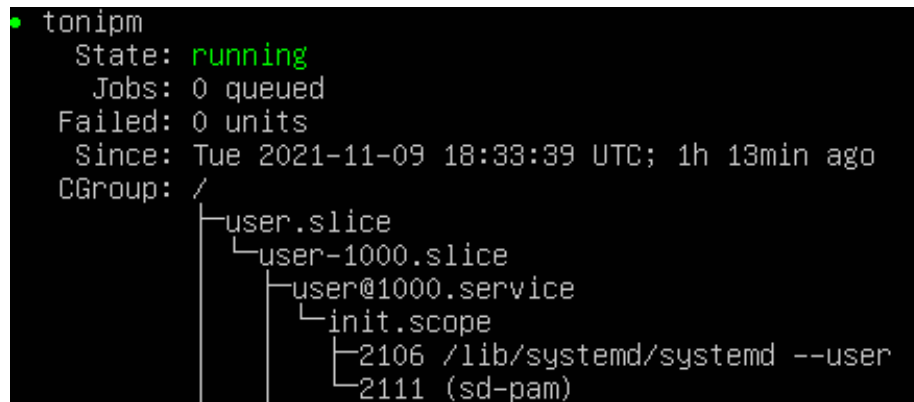
- Instal·la un servei ssh en un Ubuntu server virtual machine
- Utilitza una màquina client (pot ser virtual o real) per generar un parell de claus RSA o utilitza'n alguna que ja tinguis generada
- Instal·la la clau pública al servidor que té el servei ssh
- Configura el servei ssh per tal que només es pugui fer login mitjançant claus RSA
- Configura el client per tal que s'autentiqui automàticament mitjançant el fitxer config ## Instal·la un servei ssh en un Ubuntu server virtual machine

```
sudo apt-get install openssh-server
```

```
sudo systemctl enable ssh
```

```
sudo systemctl start ssh
```

```
systemctl status
```



```
• tonipm
  State: running
    Jobs: 0 queued
  Failed: 0 units
  Since: Tue 2021-11-09 18:33:39 UTC; 1h 13min ago
  CGroup: /
          └─user.slice
              └─user-1000.slice
                  └─user@1000.service
                      └─init.scope
                          └─2106 /lib/systemd/systemd --user
                              └─2111 (sd-pam)
```

Figure 1: alt_text

Utilitza una màquina client (pot ser virtual o real) per generar un parell de claus RSA o utilitza'n alguna que ja tinguis generada

```
ssh-keygen -t rsa -b 4096
```

SHA256:Xzpx65xJin6i0sMQAFntFxp0d/sv3pNzfy1SXIc6DyE

```
+ .ssh ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/tperaira/.ssh/id_rsa): server_auth
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in server_auth
Your public key has been saved in server_auth.pub
The key fingerprint is:
SHA256:Xzpx65xJin6i0sMQAFntFxp0d/sv3pNzfy1SXIc6DyE tperaira@Vodafone
The key's randomart image is:
+---[RSA 4096]-----+
|  .+.. .0.          |
|  . . . 0.          |
|    0  0. . . .    |
|    0 . E.....0   |
|    0S ..+0..      |
|    . . 0+.00      |
|    +  + .0+      |
|    . + .+0+=B=    |
|    ..+00.0*0X     |
+-----[SHA256]-----+
```

Figure 2: alt_text

Instal·la la clau pública al servidor que té el servei ssh

```
ssh-copy-id -i ~/.ssh/server_auth tonipm@192.168.2.169
```

```
+ .ssh ssh-copy-id -i ~/.ssh/server_auth tonipm@192.168.2.169
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/tperaira/.ssh/server_auth.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
tonipm@192.168.2.169's password:

Number of key(s) added: 1

Now try logging into the machine, with:  "ssh 'tonipm@192.168.2.169'"
and check to make sure that only the key(s) you wanted were added.
```

Figure 3: alt_text

```
ssh tonipm@192.168.2.169
```

Configura el servei ssh per tal que només es pugui fer login mitjançant claus RSA

Editarem línies de configuració del servidor SSH.

```
* .ssh ssh tonipm@192.168.2.169
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Tue 09 Nov 2021 06:57:05 PM UTC

System load:  0.0               Processes:            117
Usage of /:   32.8% of 19.56GB  Users logged in:     1
Memory usage: 5%               IPv4 address for enp0s3: 192.168.2.169
Swap usage:   0%

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation
```

Figure 4: alt_text

```
sudo vi /etc/ssh/sshd_config
```

Editem la línia:

```
PasswordAuthentication yes
```

La canviem per:

```
PasswordAuthentication no
```

Reiniciem el servei:

```
sudo systemctl restart ssh
```

Configura el client per tal que s'autentiqui automàticament mitjançant el fitxer config

```
vi ~/.ssh/config
```

```
Host konoha
```

```
    Hostname 192.168.2.169
```

```
    Port 2266
```

```
    User tonipm
```

```
    IdentityFile ~/.ssh/server_auth
```

Ara podem entrar simplement amb:

```
ssh konoha
```

```
Host github.com
    IdentityFile ~/.ssh/ciberseguiretat_montilivi_rsa
    HostName github.com

Host konoha
    Hostname 192.168.2.169
    Port 2266
    User tonipm
    IdentityFile ~/.ssh/server_auth
```

Figure 5: alt_text

```
+ .ssh ssh konoha
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue 09 Nov 2021 07:16:13 PM UTC

System load:  0.0               Processes:            118
Usage of /:   32.8% of 19.56GB   Users logged in:     1
Memory usage: 6%               IPv4 address for enp0s3: 192.168.2.169
Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation
```

Figure 6: alt_text