

# SSH VIA CHAVE PUBLICA PRIVADA

#Criação da chave publica no computador que irá realizar o acesso;

```
samuelb@OFBNB037588: ~/s X + v
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.90.1-microsoft-standard-WSL2 x86_64)

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

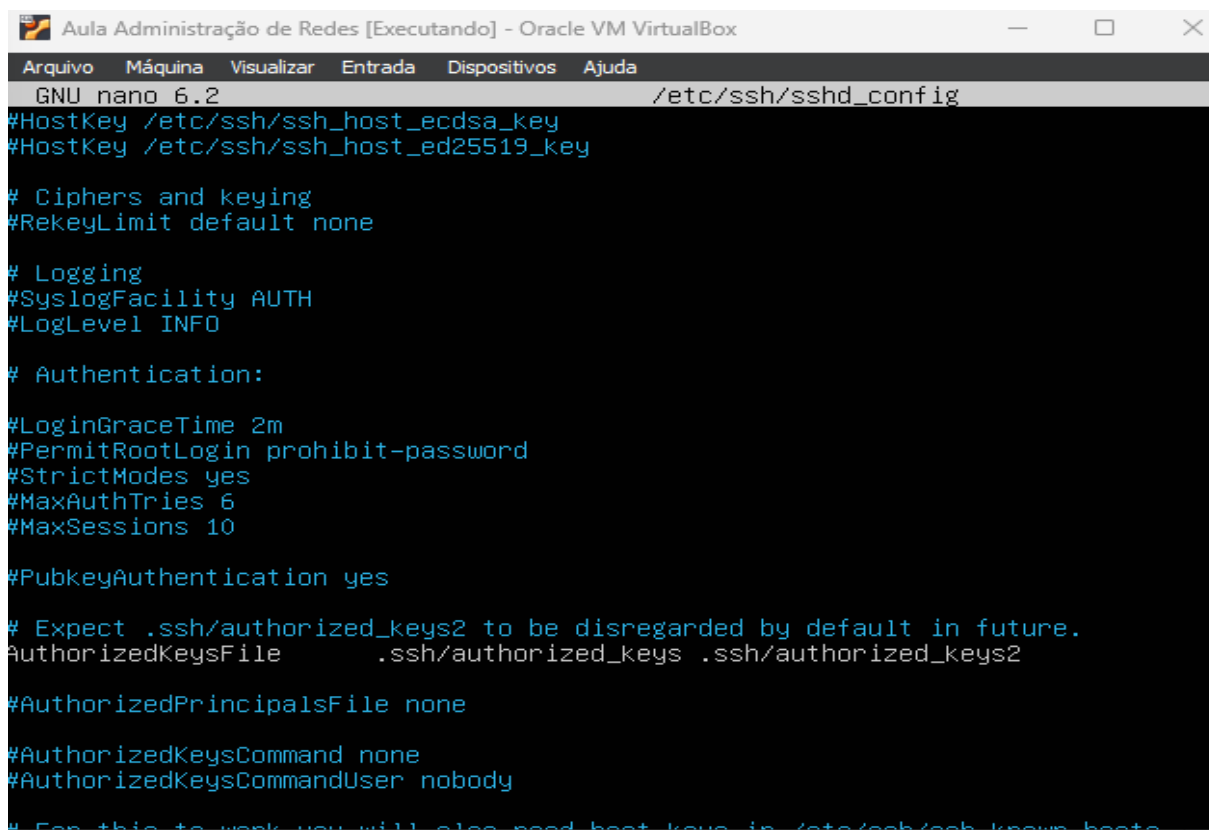
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

This message is shown once a day. To disable it please create the
/home/samuelb/.hushlogin file.
samuelb@OFBNB037588:~$
samuelb@OFBNB037588:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/samuelb/.ssh/id_rsa): /home/samuelb/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/samuelb/.ssh/id_rsa
Your public key has been saved in /home/samuelb/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:8TnpBd6dstG1HzeztcXze42nE8S60xeMj1dFbriHf4 samuelb@OFBNB037588
The key's randomart image is:
+--[RSA 3072]--+
|
|..+..+..+
|+E+ o+o=
|.So*.*+0o
|..o+..X
|..+0+
|..+*0
|..=
+--[SHA256]--+
samuelb@OFBNB037588:~$ /home/samuelb/.ssh/id_rsa
-bash: /home/samuelb/.ssh/id_rsa: Permission denied
samuelb@OFBNB037588:~$ /home/samuelb/.ssh/
-bash: /home/samuelb/.ssh/: Is a directory
samuelb@OFBNB037588:~$ ls
ubuntu-22.04.3-desktop-amd64.iso
ubuntu-22.04.3-desktop-amd64.iso?_ga=2.71452116.634195427.1692474393-1458567805.1692474393
samuelb@OFBNB037588:~$ /home/samuelb/.ssh
```

#Envio da chave publica para servidor e adição da chave na pasta de autorização

```
administrator@ifceasr: ~/.ssh X + v
./ .bash_logout .lessshst .sudo_as_admin_succ
../ .bashrc .profile
.bash_history .cache/ .ssh/
administrator@ifceasr:~$ cat id_rsa.pub > /home/administrator/.
./ .bash_logout .lessshst .sudo_as_admin_succ
../ .bashrc .profile
.bash_history .cache/ .ssh/
administrator@ifceasr:~$ cat id_rsa.pub > /home/administrator/.ssh/
authorized_keys known_hosts known_hosts.old
administrator@ifceasr:~$ cat id_rsa.pub > /home/administrator/.ssh/authorized_keys
administrator@ifceasr:~$ /home/administrator/.ssh/authorized_keys
-bash: /home/administrator/.ssh/authorized_keys: Permission denied
administrator@ifceasr:~$ cat authorized_keys
cat: authorized_keys: No such file or directory
administrator@ifceasr:~$ ls
id_rsa.pub
administrator@ifceasr:~$ /home/administrator/.ssh/
-bash: /home/administrator/.ssh/: Is a directory
administrator@ifceasr:~$ cd /home/administrator/.ssh/
administrator@ifceasr:~/.ssh$ ls
authorized_keys known_hosts known_hosts.old
administrator@ifceasr:~/.ssh$ cd /home/administrator/.ssh/authorized_keys
-bash: cd: /home/administrator/.ssh/authorized_keys: Not a directory
administrator@ifceasr:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCgY/T9yWALsaIIC5/sY+XgU6VqIh99vtGEDC/26q2g3mEfM8Na+8zNH6t50y0d
SulanC7eiUHDi4wCLYwrZP0qn0BneGaVFf01aT+ysMt5vLX35/ChIwnOCJgXs/bNycT5m5gIL9eJdEZwcTltPu2+SDZy+SSSQnu
vqc07VEP3BThEX4f7kTGk9wMhZrkZ4N/gF0gGEypEgV7rovW14biguFODL+NxLHMvy5ML9rGpCKNzPcdYbyuk+8xalBoo/pwmi+
3Wh64VsI/nplVwYnUue+JDyPPLVWUE81UTsivx8HbAu1kkwTic0bJZeIHYqzeP7deFXEWbrVwOzR0wNLMrv1SITR3m+B9k1Zfo5
IzkHiqt1HpzhcoYgQPWZCcak8GbZXxEJjHap9YjLCMRviEM4x44/bLF2hw+DyOZQC8GyxR8= samuelb@OFBNB037588
administrator@ifceasr:~/.ssh$ |
```

## #Modificação documento para acesso do ssh via chave



A screenshot of a terminal window titled "Aula Administração de Redes [Executando] - Oracle VM VirtualBox". The terminal shows the GNU nano 6.2 editor editing the file /etc/ssh/sshd\_config. The configuration includes settings for HostKey, Ciphers and keying, Logging, Authentication, and AuthorizedKeysFile. The file is currently open in nano editor, showing the following content:

```
GNU nano 6.2 /etc/ssh/sshd_config
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

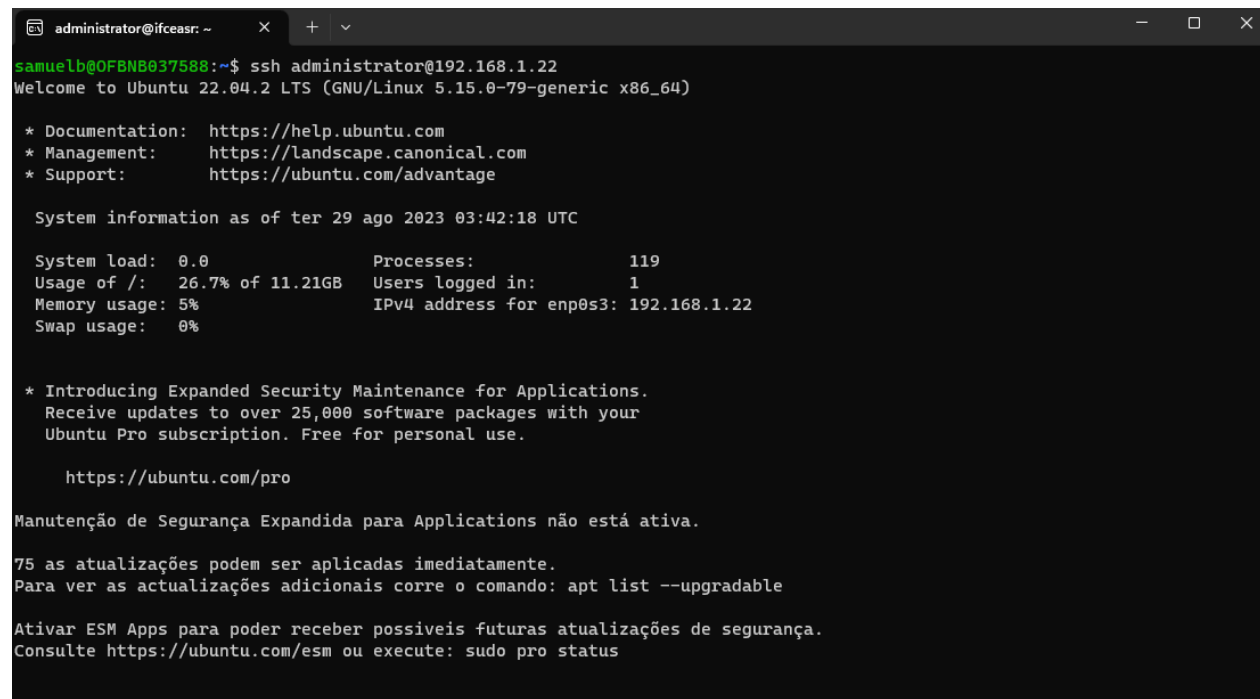
# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
```

## #Acesso via chave publica



A screenshot of a terminal window showing an SSH session. The user 'samuelb@OFBNB037588' is connected to 'administrator@192.168.1.22'. The terminal displays the Ubuntu 22.04.2 LTS welcome message and system information. The user has executed the command 'ssh administrator@192.168.1.22'.

```
administrator@ifceasr: ~
samuelb@OFBNB037588:~$ ssh administrator@192.168.1.22
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-79-generic x86_64)

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

System information as of ter 29 ago 2023 03:42:18 UTC

System load:  0.0               Processes:    119
Usage of /:   26.7% of 11.21GB  Users logged in: 1
Memory usage: 5%               IPv4 address for enp0s3: 192.168.1.22
Swap usage:  0%

 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.

   https://ubuntu.com/pro

Manutenção de Segurança Expandida para Applications não está ativa.

75 as atualizações podem ser aplicadas imediatamente.
Para ver as atualizações adicionais corre o comando: apt list --upgradable

Ativar ESM Apps para poder receber possiveis futuras atualizações de segurança.
Consulte https://ubuntu.com/esm ou execute: sudo pro status
```