

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ  
CAMPUS FORTALEZA  
TELEMÁTICA

30/08/2023

Disciplina: Administração de serviços de rede (01.302.25)

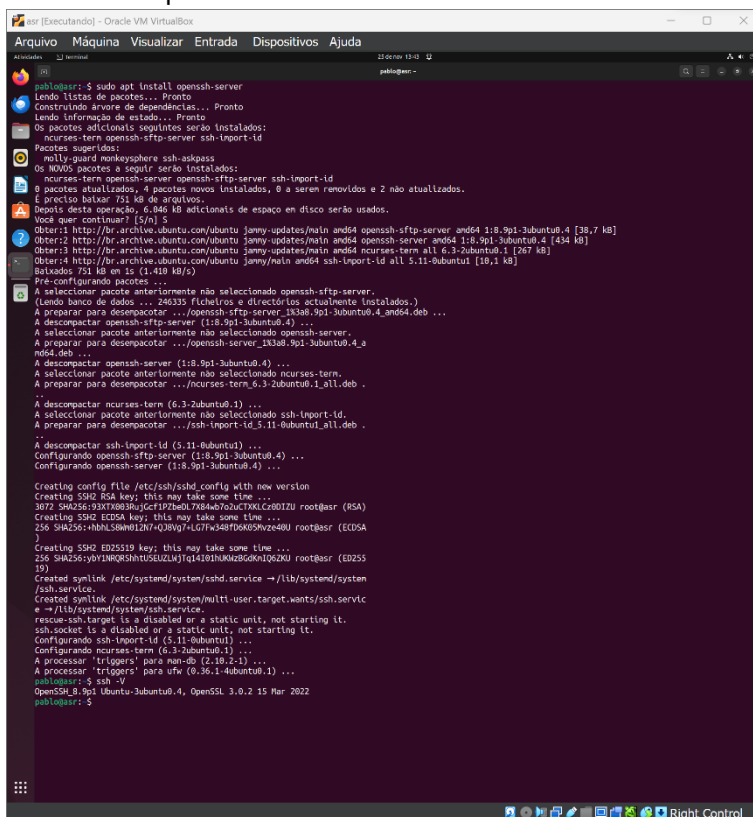
Professor: Ricardo Duarte Taveira

Aluno: Pablo Busatto (mat. 20221013020042)

### Avaliação 3 – OpenSSH

1. Instalar o OpenSSH. Gerar chaves pública e privada. Copiar a chave pública no Linux. Mostrar a chave copiada no diretório do Linux. Testar a conexão usando as chaves pública e privada. Fazer um registro em PDF de cada etapa.

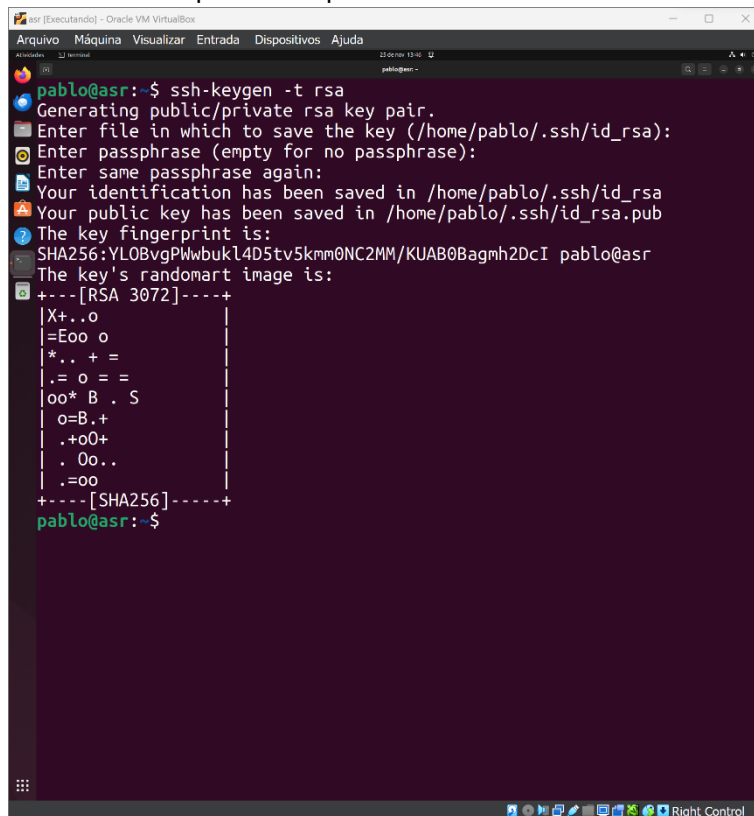
#### a. Instalar o OpenSSH.



```
pablo@pbr:~$ sudo apt install openssh-server
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
Os pacotes adicionais seguintes serão instalados:
ncurses-termin openssh-sftp-server ssh-import-id
Pacotes sugeridos:
  multi-guard nkeysphere ssh-keypass
Os NOVOS pacotes a seguir serão instalados:
ncurses-termin openssh-sftp-server ssh-import-id
e pacotes atualizados, 4 pacotes novos instalados, 0 a serem removidos e 2 não atualizados.
É preciso baixar 751 kB de arquivos.
Depois desta operação, 6.046 kB adicionais de espaço em disco serão usados.
Você quer continuar? [5/n] 5
Obter:1 http://br.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0.4 [38,7 kB]
Obter:2 http://br.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-server amd64 1:8.9p1-3ubuntu0.4 [434 kB]
Obter:3 http://br.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-termin all 6.3-2ubuntu1 [507 kB]
Obter:4 http://br.archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10,1 kB]
Baixados 751 kB em 1s (1.419 kB/s)
Pre-configurando pacotes ...
A selecionar pacote anteriormente não selecionado openssh-sftp-server.
Lendo banco de dados ... 246325 ficheiros e directorios actualmente instalados.
A preparar para descompactar .../openssh-sftp-server_1:8.9p1-3ubuntu0.4_amd64.deb ...
A descompactar openssh-sftp-server (1:8.9p1-3ubuntu0.4) ...
A selecionar pacote anteriormente não selecionado openssh-server.
A preparar para descompactar .../openssh-server_1:8.9p1-3ubuntu0.4_amd64.deb ...
A descompactar openssh-server (1:8.9p1-3ubuntu0.4) ...
A selecionar pacote anteriormente não selecionado ncurses-termin.
A preparar para descompactar .../ncurses-termin_6.3-2ubuntu1_all.deb ...
A descompactar ncurses-termin (6.3-2ubuntu1) ...
A selecionar pacote anteriormente não selecionado ssh-import-id.
A preparar para descompactar .../ssh-import-id_5.11-0ubuntu1_all.deb ...
A descompactar ssh-import-id (5.11-0ubuntu1) ...
Configurando openssh-sftp-server (1:8.9p1-3ubuntu0.4) ...
Configurando openssh-server (1:8.9p1-3ubuntu0.4) ...
Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:93XTW8b9jCp1F7B0L7W84b7e9uCTXK0Cz80IZU root@pbr (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:nbHL5bW6L2N7-QJ8Vq7+LGF7a548TD6K9Shvze40U root@pbr (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:y0r1WNg3h1ntUSLZLk7q14193hukz6d6n1q2XU root@pbr (ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
ssh.socket is a disabled or a static unit, not starting it.
Configurando ssh-import-id (5.11-0ubuntu1) ...
Configurando ncurses-termin (6.3-2ubuntu1) ...
A processar 'triggers' para man-db (2.10.2-1) ...
A processar 'triggers' para ufw (0.36-1-0ubuntu1) ...
pablo@pbr:~$ ssh -V
OpenSSH_8.9p1-3ubuntu0.4, OpenSSL 3.0.2 15 Mar 2022
pablo@pbr:~$
```

Figura 1. Instalação do OpenSSH.

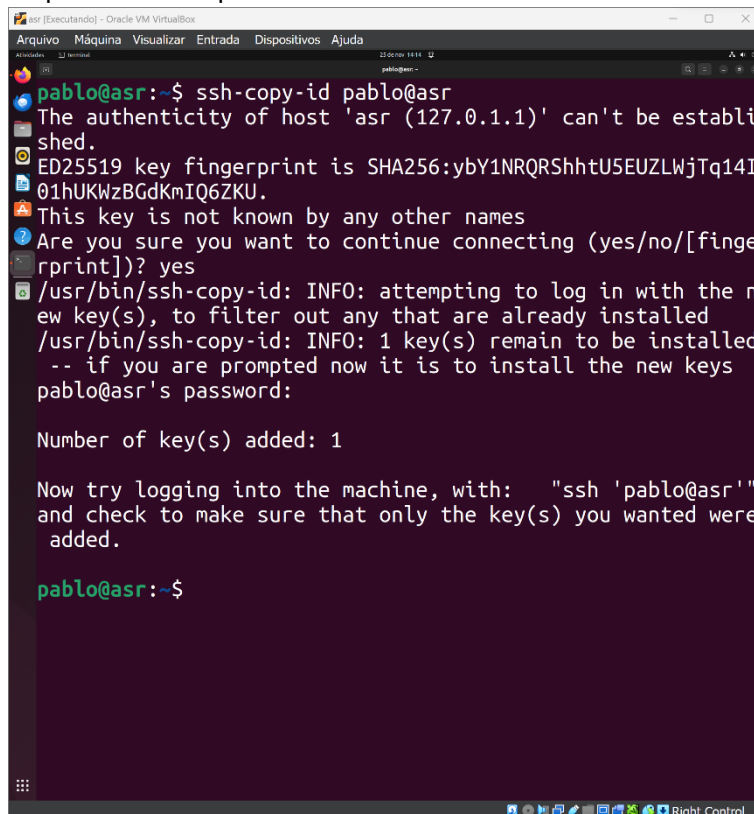
b. Gerar chaves pública e privada.



```
pablo@asr:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/pablo/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/pablo/.ssh/id_rsa
Your public key has been saved in /home/pablo/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:YLOBvgPWwbukl4D5tv5kmm0NC2MM/KUAB0B9gmh2DcI pablo@asr
The key's randomart image is:
+---[RSA 3072]-----+
|X+..o|
|=Eoo o|
|*.. + =|
|, o = =|
|oo* B . S|
|o=B.+|
|. +o0+|
|. 0o..|
|. =oo|
+---[SHA256]-----+
pablo@asr:~$
```

Figura 2. Geração das chaves pública e privada.

c. Copiar a chave pública no Linux.



```
pablo@asr:~$ ssh-copy-id pablo@asr
The authenticity of host 'asr (127.0.1.1)' can't be established.
ED25519 key fingerprint is SHA256:yby1NRQRShhtU5EUZLWjTq14I
01hUKWzBGdKmIQ6ZKU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/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
pablo@asr's password:

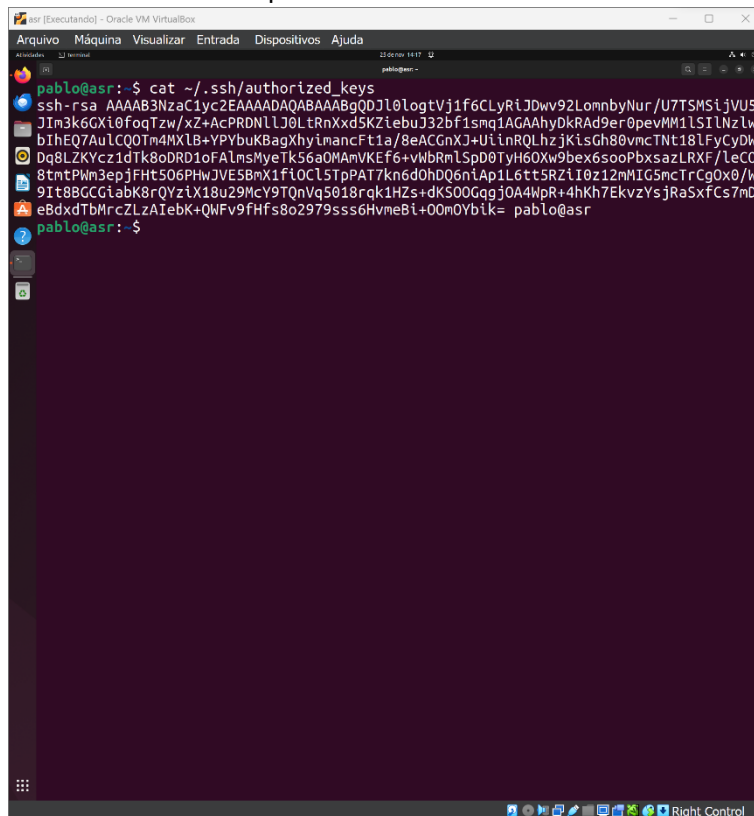
Number of key(s) added: 1

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

pablo@asr:~$
```

Figura 3. Cópia da chave pública no Linux.

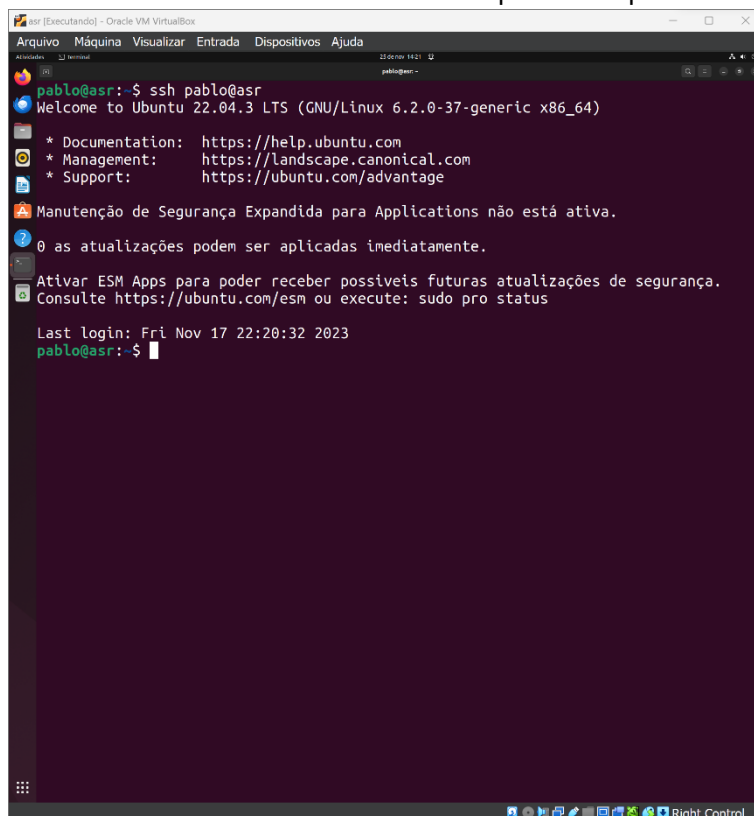
d. Mostrar a chave copiada no diretório do Linux.



```
pablo@asr:~$ cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDJl0lgtVj1f6CLyRiJDwv92LomnbyNur/U7TSMsiJVU5
JIm3k6CXi0foqTzw/xZ+AcPRDNLJ0LrRnXxd5KZiebuJ32bf1smq1AGAAhyDkRAd9er0pevMM1LSILNzlw
bIHEQ7AulCQ0Tm4MXlB+YPYbuKBAGXhyimancFt1a/8eACGnXJ+UinRQLhzjKisGh80vmcTnt18lFyCyDW
Dq8LZYcz1dTk8oDRD1oFAlmsMyeTk56a0MAMVKEf6+vwBRmLSpD0TyH60Xw9bex6sooPbxsazLRXF/leCO
8tntPwm3epjFHT506PHwJVE5BmX1fi0CL5TpPAI7kn6d0hDQ6nIap1L6tt5RziI0z12mMIG5mcTrCg0x0/W
9It8BGCgiabK8rQYziX18u29McY9TQnVq5018rqk1HZs+dKS00Gggj0A4WpR+4hKh7EkvzYsjRaSxfCs7mD
eBdxdTbMrcZLzAiebK+QWfv9fHfs8o2979sss6HvmeBi+00m0YbIk= pablo@asr
pablo@asr:~$
```

Figura 4. Exibindo a chave copiada no diretório do Linux.

e. Testar a conexão usando as chaves pública e privada.



```
pablo@asr:~$ ssh pablo@asr
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-37-generic x86_64)

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

Manutenção de Segurança Expandida para Applications não está ativa.
0 as atualizações podem ser aplicadas imediatamente.
Ativar ESM Apps para poder receber possíveis futuras atualizações de segurança.
Consulte https://ubuntu.com/esm ou execute: sudo pro status

Last login: Fri Nov 17 22:20:32 2023
pablo@asr:~$
```

Figura 5. Testando a conexão SSH. A conferência de chaves foi automática, por ter sido copiada para o Linux.