



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

Disciplina: **Administração de serviços de rede**

Professor: **Ricardo Taveira**

Aluno: **Pablo Busatto Figueiredo** (mat. 20221013020042)

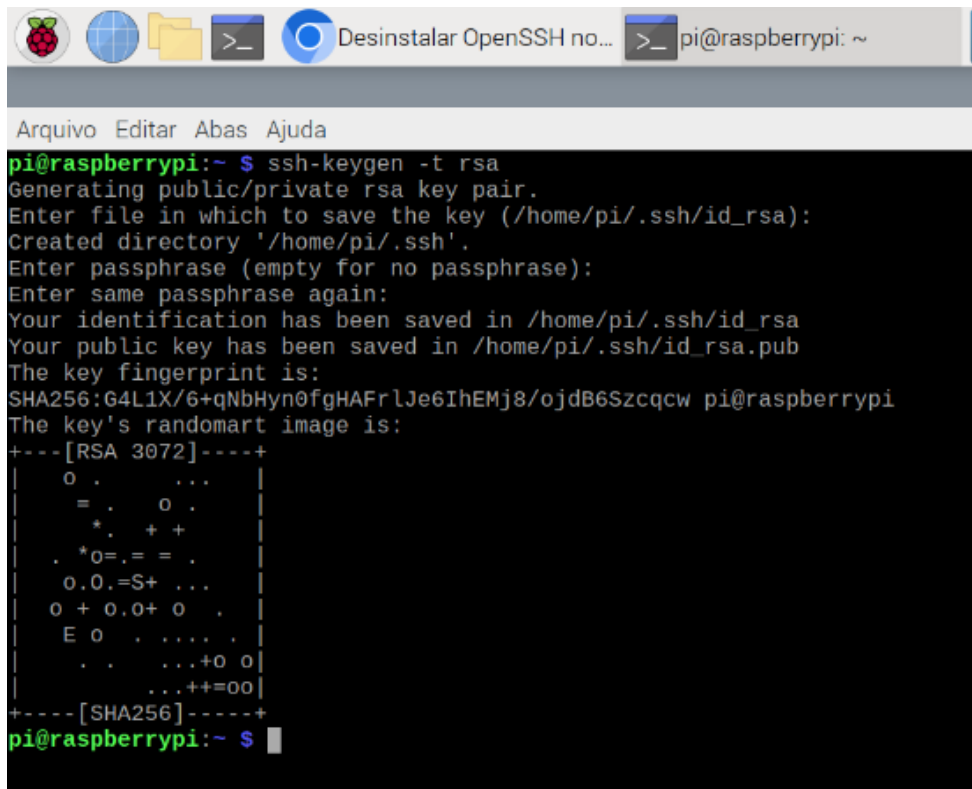
Avaliação 3 – OpenSSH

Instalar o Open-SSH. 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.

Instalar o Open-SSH:

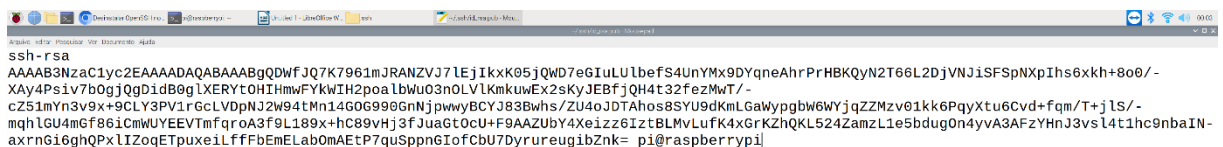
```
pi@raspberrypi:~$ sudo apt install openssh-server
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
The following additional packages will be installed:
  ncurses-term openssh-sftp-server runit-helper
Pacotes sugeridos:
  molly-guard monkeysphere ssh-askpass ufw
Os NOVOS pacotes a seguir serão instalados:
  ncurses-term openssh-server openssh-sftp-server runit-helper
0 pacotes atualizados, 4 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
E preciso baixar 924 kB de arquivos.
Depois desta operação, 6.057 kB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n] S
Obter:1 http://deb.debian.org/debian bullseye/main arm64 ncurses-term all 6.2+20201114-2+deb11u1 [505 kB]
Obter:2 http://deb.debian.org/debian bullseye/main arm64 openssh-sftp-server arm64 1:8.4p1-5+deb11u1 [49,6 kB]
Obter:3 http://deb.debian.org/debian bullseye/main arm64 runit-helper all 2.10.3 [7.808 B]
Obter:4 http://deb.debian.org/debian bullseye/main arm64 openssh-server arm64 1:8.4p1-5+deb11u1 [361 kB]
Baixados 924 kB em 0s (3.806 kB/s)
Pré-configurando pacotes ...
A seleccionar pacote anteriormente não seleccionado ncurses-term.
(Lendo banco de dados ... 124732 ficheiros e directórios actualmente instalados.
)
A preparar para desempacotar .../ncurses-term_6.2+20201114-2+deb11u1_all.deb ...
A descompactar ncurses-term (6.2+20201114-2+deb11u1) ...
A seleccionar pacote anteriormente não seleccionado openssh-sftp-server.
A preparar para desempacotar .../openssh-sftp-server_1%3a8.4p1-5+deb11u1_arm64.d
eb ...
A descompactar openssh-sftp-server (1:8.4p1-5+deb11u1) ...
A seleccionar pacote anteriormente não seleccionado runit-helper.
A preparar para desempacotar .../runit-helper_2.10.3_all.deb ...
A descompactar runit-helper (2.10.3) ...
A seleccionar pacote anteriormente não seleccionado openssh-server.
A preparar para desempacotar .../openssh-server_1%3a8.4p1-5+deb11u1_arm64.deb ..
)
A descompactar openssh-server (1:8.4p1-5+deb11u1) ...
Configurando runit-helper (2.10.3) ...
Configurando openssh-sftp-server (1:8.4p1-5+deb11u1) ...
Configurando openssh-server (1:8.4p1-5+deb11u1) ...
Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
3072 SHA256:5h0Y6EX5G2j3iQkXzzJmB3yZb4Y2Kx179agCHVgtjTY root@raspberrypi (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:KNdH6BoP3BhcxTIHp-zpDyBon0aokYsIPQNVQ/xDW30 root@raspberrypi (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:Wp1J+VTS1UwMqtqRIPq+QF7ntsxxu4UBe2Cg0iQmVQ root@raspberrypi (ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.servi
ce.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/s
ystemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Configurando ncurses-term (6.2+20201114-2+deb11u1) ...
A processar 'triggers' para man-db (2.9.4-2) ...
pi@raspberrypi:~$
```

Gerar chaves pública e privada:



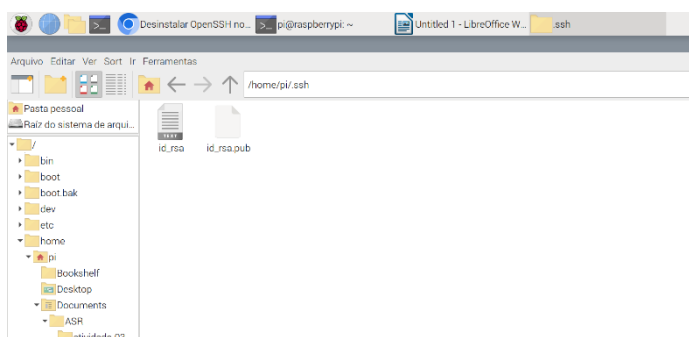
```
pi@raspberrypi:~ $ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/pi/.ssh/id_rsa):
Created directory '/home/pi/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/pi/.ssh/id_rsa
Your public key has been saved in /home/pi/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:G4L1X/6+qNbHyn0fgHAFrlJe6IhEMj8/ojdB6Szcqcw pi@raspberrypi
The key's randomart image is:
+---[RSA 3072]---+
|  o . . . . .
|  = . o .
|  * . + +
|  . * 0 = . = .
|  o . 0 = S + . . .
|  o + o . 0 + o .
|  E o . . . . .
|  . . . . . + o o |
|  . . . . . + = o o |
+---[SHA256]---+
pi@raspberrypi:~ $
```

Copiar a chave pública no Linux:

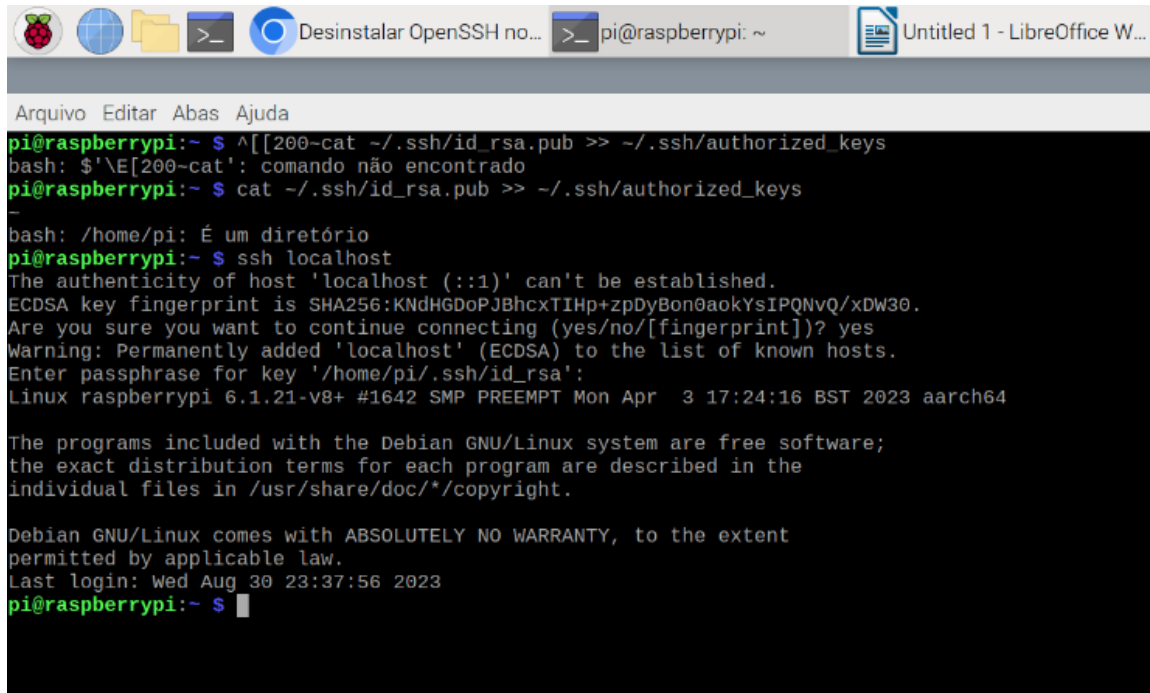


```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQGDwFJQ7K7961mJRANZVJ7lEjIkxK05jQWD7e6IuLulbefS4UnYMx9DYqneAhrPrHBKQyN2T66L2DjVNJiSFSpNXpIhs6xkh+8o0/-
Xy4Pslv7b0gj0gb1d80glXERYtOHIHmWfYkWIH2poalbWu03nOLVlKmkwEx2sKyJEBfjQH4t32fezMwT/-
cZ5lmYn3v9x+9CLY3PVlrGcLVDPNj2W94tMn14G06990GnNjpwWYBCYJ83Bwhs/ZU4oJDTAhos8SVU9dKmlGaWypgbW6WYjQZMZv01kk6PqyXtu6Cvd+fqm/T+jlS/-
mqhLGU4mGf86iCmUYEEVtmfqr0A3f9L189x+hC89vHj3fJuaGt0CU+F9AAZUbY4XeiZZ6IztBLMvLufK4xGrKZhQKL524ZamZL1e5bdug0n4yvA3AFzYHnJ3vs14t1hc9nbaIN-
axrn6i6ghQPxlIZoqETpuxeilFFbEmELab0MAEtP7quSppngIofCbU7DyrureugibZnk= pi@raspberrypi
```

Mostrar a chave copiada no diretório do Linux:



Testar a conexão usando as chaves pública e privada:



The image shows a terminal window on a Raspberry Pi. The window has a title bar with icons for a Raspberry Pi, a globe, a folder, a terminal, and a window titled "Desinstalar OpenSSH no...". The terminal prompt is "pi@raspberrypi: ~". The user enters the command "cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys". The terminal output shows the command being executed and the file being updated. The user then enters "ssh localhost". The terminal output shows the SSH connection attempt, including the authenticity of the host, the ECDSA key fingerprint, and the warning that the host has been permanently added to the list of known hosts. The user is prompted to enter a passphrase for the key, but no input is shown. The terminal output also shows the Linux version and the Debian GNU/Linux system information.

```
Arquivo  Editar  Abas  Ajuda
pi@raspberrypi:~ $ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
bash: $'\E[200~cat': comando não encontrado
pi@raspberrypi:~ $ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
bash: /home/pi: É um diretório
pi@raspberrypi:~ $ ssh localhost
The authenticity of host 'localhost (:::1)' can't be established.
ECDSA key fingerprint is SHA256:KNdHGDoPJ8hcxTIHp+zpDyBon0aokYsIPQNVQ/xDW30.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
Enter passphrase for key '/home/pi/.ssh/id_rsa':
Linux raspberrypi 6.1.21-v8+ #1642 SMP PREEMPT Mon Apr  3 17:24:16 BST 2023 aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Aug 30 23:37:56 2023
pi@raspberrypi:~ $
```