



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

Disciplina: **Administração de serviços de rede**

Professor: **Ricardo Taveira**

Aluno: **Cícera Márcia da Fonseca Silva** (mat. 20222013020016)

**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.

Instalação OpenSSH:

```
Arquivo Editar Abas Ajuda
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 (3.184 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.deb ...
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:Xi1C0ZakqG1QFuAcLCgFIjmYQNs+FPK0hQ+YttUJM root@raspberrypi (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:GJHTUONKT3MrwB1NqE/trPOyYogg7d768fp7R6KgK8 root@raspberrypi (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:RE4Q6ljsVJFMU6z3YtKQnZ1DLmrh26eapsJmMNL0oYc root@raspberrypi (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.
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:~$
```

```

Arquivo Editar Abas Ajuda
pi@raspberrypi:~$ sudo apt install openssh-server
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
openssh-server is already the newest version (1:8.4p1-5+deb11u1).
0 pacotes atualizados, 0 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
pi@raspberrypi:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2023-08-31 00:27:55 CEST; 2min 57s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 5214 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 5215 (sshd)
      Tasks: 1 (limit: 3933)
         CPU: 56ms
    CGroup: /system.slice/ssh.service
            └─5215 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

ago 31 00:27:55 raspberrypi systemd[1]: Starting OpenBSD Secure Shell server...
ago 31 00:27:55 raspberrypi sshd[5215]: Server listening on 0.0.0.0 port 22.
ago 31 00:27:55 raspberrypi sshd[5215]: Server listening on :: port 22.
ago 31 00:27:55 raspberrypi systemd[1]: Started OpenBSD Secure Shell server.
pi@raspberrypi:~$ ssh <username>@<ip_address>
-bash: erro de sintaxe próximo ao token inesperado 'newline'
pi@raspberrypi:~$

```

Criação das chaves pública e privada:

```

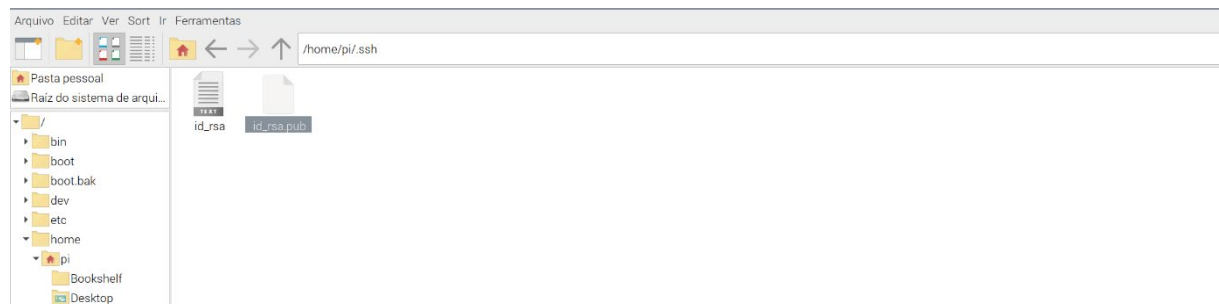
Arquivo Editar Abas Ajuda
pi@raspberrypi:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/pi/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/pi/.ssh/id_rsa
Your public key has been saved in /home/pi/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:CR87p0CfYJb0wZTL+DRVpDntB01PrbIo4e/886aQ0DM pi@raspberrypi
The key's randomart image is:
+---[RSA 3072]-----+
|      .00. 0+0. 0|
|      . 00..0 ..0.|
|      B000+ 0 ...|
|      +.=** +...|
|      .+SoE. 0   |
|      .+=.+.    |
|      .00       |
|      . . . . .|
|      .0.0=.    |
+---[SHA256]-----+
pi@raspberrypi:~$

```

## Comprovação da cópia da chave pública no Linux:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDttw14hsAueBBiw0SEu+aGD7TzgfX/-  
icPDTwrR9i7RmY8KkwNqh6nuKSjPxyGaWoxGPs1J1hblyYXsGf4cM26u7NUJk3XptkZ6d9+Uonk/-  
xXFj8SeRzPmi7ML2svRZgHtZ0GrUiYCFj6s7ESWfD7MNHx2xmvBoCYqh85BwCAU94P8Eru2TEz291D0MZp3ozQPZFKEvF2S1hjEAVLzVf5Sx+o4+mR0TatzM60Fn7wdc2y+Dm6xYZVe-  
wg9X4X0e30wjGCXx41LqZrC0Me7fSx1MX3Z4VgHjwUhzZFCcQhLY83m1nFeaTBeDgn06VukR5zuN9TX67hgASJEIilbRaDpImLmPdd+Coj8tJifRuHwEGFGXyLCTIMmm8WfDooq1uN8J-  
23Bg/uLcMrIwtoowFFXNa0AwNexEXLGFsh0+x/h9T1TH48uwZ0cB5GvbICDFJw6/P1dcK3WjhzZ4h5ieqD3x5xh0Rl0i/RxmCW6/bgqVhbRgA4Vvx4ME50A65ZawMU=  
pi@raspberrypi
```

## Evidenciar as chaves pública e privada no diretório:



## Teste de conexão usando as chaves pública e privada

```
Arquivo  Editar  Abas  Ajuda  
pi@raspberrypi:~$ cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys  
pi@raspberrypi:~$ ssh localhost  
The authenticity of host 'localhost (:::1)' can't be established.  
ECDSA key fingerprint is SHA256:GJHTUoNKT3MrwB1NqE/trPOYqYogg7d768fp7R6KgK8.  
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: Thu Aug 31 00:14:38 2023 from ::1  
pi@raspberrypi:~$
```