

STREAM SERIES

devnator

Acesso remoto SSH com senha ou
chaves de criptografia

SERGIO CABRAL



sergijocabral.com

Índice

1. Conexão com senha	2
2. Conexão com chaves de criptografia	3
3. Alternativas para clientes SSH	5
4. Demonstração em vídeo	6

Objetivo prático desta demonstração

Estabelecer uma conexão via SSH, ou usando senha, ou usando um par de chaves de criptografia.

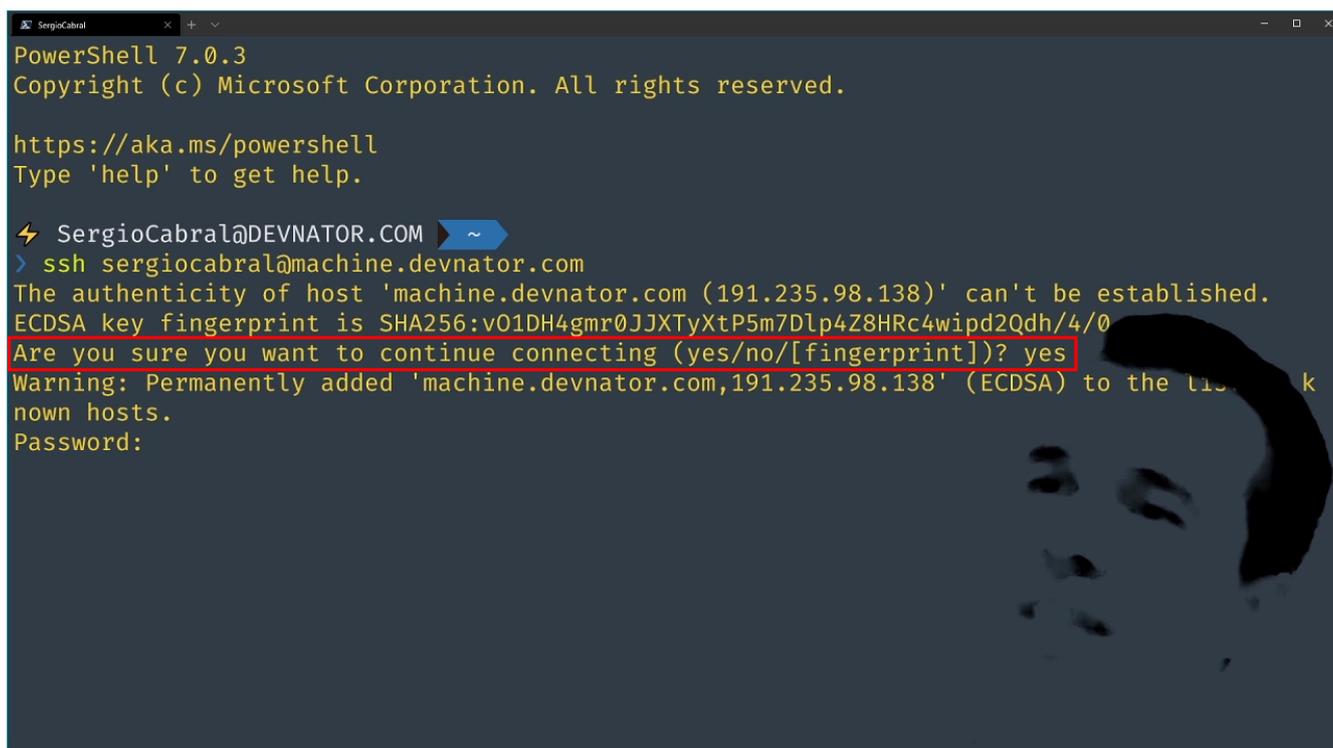
1. Conexão com senha

Para se conectar a um servidor com o cliente nativo do Windows 10, digite:

```
ssh nome-do-usuario@endereço-do-servidor
```

Existem outros clientes SSH famosos como indicado na seção [Alternativas para clientes SSH](#). Mas o cliente nativo do Windows 10 provavelmente já será o suficiente para o que você precisa fazer.

Quando é o primeiro acesso você precisa informar que confia na identidade do computador remoto respondendo **yes**, como indicado na *Figura 1*.



```
PowerShell 7.0.3
Copyright (c) Microsoft Corporation. All rights reserved.

https://aka.ms/powershell
Type 'help' to get help.

⚡ SergioCabral@DEVNATOR.COM ~
> ssh sergiocabral@machine.devnator.com
The authenticity of host 'machine.devnator.com (191.235.98.138)' can't be established.
ECDSA key fingerprint is SHA256:v01DH4gmr0JJXTyXtP5m7Dlp4Z8HRc4wipd2Qdh/4/0
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'machine.devnator.com,191.235.98.138' (ECDSA) to the list of known hosts.
Password:
```

Figura 1. Confirmação no primeiro acesso ao computador remoto



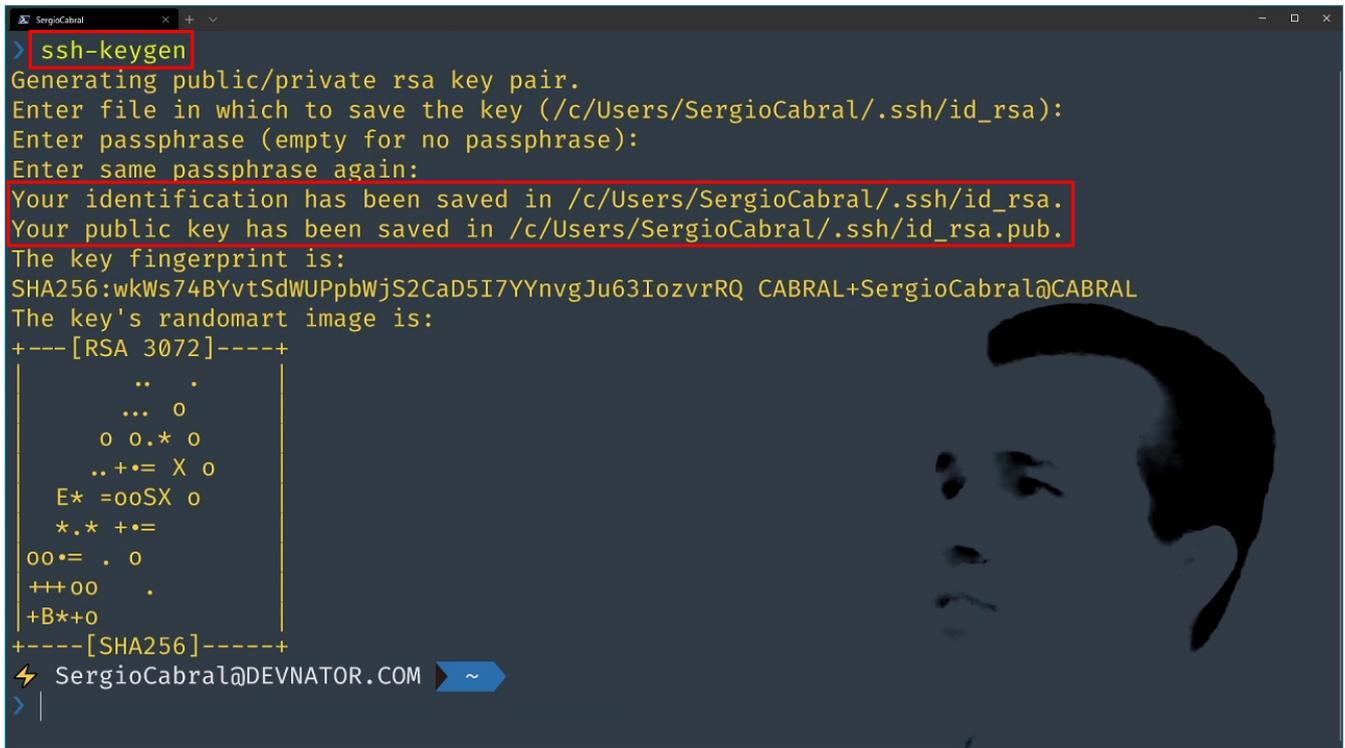
Ao fazer isso a chave de criptografia pública do computador remoto é armazenada no arquivo `~/.ssh/known_hosts` do computador local.

Se este arquivo for apagado ou tiver a linha que contém a chave pública do computador remoto removida, então a mensagem de confirmação voltará a ser exibida.

Na sequência você informa sua senha, e pronto. Conectado!

2. Conexão com chaves de criptografia

Outra forma de autenticação é fazer com que o computador de destino conheça o computador de origem. Neste caso criamos um par de chaves de criptografia no computador de origem com o comando `ssh-keygen`. Execute e pressione **Enter** até concluir, como mostrado na *Figura 2*.



```
SergioCabral
> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/c/Users/SergioCabral/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /c/Users/SergioCabral/.ssh/id_rsa.
Your public key has been saved in /c/Users/SergioCabral/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:wkWs74BYvtSdWUPpbWjS2CaD5I7YynvgJu63IozvrRQ CABRAL+SergioCabral@CABRAL
The key's randomart image is:
+---[RSA 3072]-----+
|
| .. .
| ... 0
|  0 0.* 0
| ..+*= X 0
| E* =ooSX 0
| *. * +=
| oo*= . 0
| +++oo .
| +B*+0
+-----[SHA256]-----+
⚡ SergioCabral@DEVNATOR.COM ~
> |
```

Figura 2. Execução padrão do comando "ssh-keygen"



Se você executar novamente o comando `ssh-keygen`, por padrão (ao pressionar **Enter** até o final) ele não sobrescreve as chaves geradas anteriormente. Mas se você especificar que deseja fazer isso vai perder qualquer acesso a serviços que dependiam daquelas chaves. É uma operação irreversível.

Como também indicado na *Figura 2*, um par de arquivos é gerados. Nos interessamos para esta demonstração no arquivo público `id_rsa.pub`. O arquivo privado `id_rsa` deve ser mantido seguro e nunca compartilhado.

```
SergioCabral
*. * +=
00*= . 0
+++00 .
+B*+0
+----[SHA256]-----+
SergioCabral@DEVNATOR.COM ~
> type /Users/SergioCabral/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCesxW56XDbbmvxkIv5wtRLVuZgiKchtaJ/Zj0/+RPrsY5DHzBhn
Hzi1egWvxlF8CP76shM40XXLFv19Uz5qbck0hoJvE06mG0DlZ1au3pS4nfbfDMrIUVyIDR5mgt+17fna0zLItVK6K
1BAYpVK7007HHXRT0EbmSsNgwpGA46Bb8LdLWNmyGEY00wY2FUCpJ0wrNzGzjOPMKI8aMT...BhNjqYGZun
t92yumz7mw+hZy2Fn4top2MfTRsrHJvqLTHqd4NcLpNdAXqGwcz9/YwBKID9U7iWXL+CA...M/8pEN
0kR4rggfsftk8eEz0kHLZ/hQz/6exY8zjeDaEt01dvHnbygnHo7DHQsBb5XfC6DEN0IFMhLMntHwWqIS...LDrj
DQaf+RqHELMWDEIhU56MShgpEI2j8mq5cHlhQsOUxAo03CVXZtQvNTYZ3MVpChl5PQ7ZXUggQqYii6dgc...Ng/
vgr06TEopihGN7mV0= CABRAL+SergioCabral@CABRAL
SergioCabral@DEVNATOR.COM ~
> ssh sergiocabral@machine.devnator.com
Password:
Linux devnator 4.19.0-10-cloud-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

Last login: Tue Sep 29 23:54:17 2020 from 177.79.120.44
sergiocabral@devnator:~$ mkdir .ssh
sergiocabral@devnator:~$ cd .ssh
sergiocabral@devnator:~/.ssh$ echo "" >> authorized_keys
```

Figura 3. Conteúdo do arquivo "id_rsa.pub"

Então, enviamos o conteúdo do arquivo `id_rsa.pub`, como exemplificado na *Figura 3*, para o computador de destino, o servidor. Esse conteúdo deve ser adicionado ao arquivo `~/.ssh/authorized_keys`. Caso não exista deve ser criado.

Como mostrado na *Figura 3*, o conteúdo da chave de criptografia pública é um texto curto que você pode copiar usando o mouse e a combinação de comandos `type` ou `cat` para exibir e `echo` para escrever.

Mas caso esteja sem mouse, talvez prefira copiar o arquivo diretamente com o comando `scp` e, então, fazer a adição da chave no arquivo `authorized_keys`:



Comando no computador de origem:

- `scp ~/.ssh/id_rsa.pub nome-do-usuario@endereço-do-servidor:~/.ssh`

Comando no computador de destino:

- `cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys`

A partir de agora tanto o seu computador conhece o servidor, como o servidor conhece o seu computador. Cada computador tem a chave pública do outro.

Faça uma nova tentativa de conexão e pronto. Conectado com o uso de chaves sem precisar informar dados de autenticação.

3. Alternativas para clientes SSH

Nome	Licença	Download
PuTTY	free; open-source	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
SuperPutty	free; open-source; baseado no PuTTY	https://github.com/jimradford/superputty
PuTTY Tray	free; open-source; baseado no PuTTY	https://puttytray.goeswhere.com/
KiTTY	free; open-source; baseado no PuTTY	http://www.9bis.net/kitty/
MobaXterm	free; versão Pro disponível para compra	http://mobaxterm.mobatek.net/
SmarTTY	free	http://smartty.sysprogs.com/
Dameware SSH client	free; versões disponíveis para compra	http://www.dameware.com/free-ssh-client-for-windows.aspx
mRemoteNG	free; open-source	http://www.mremoteng.org/
Terminals	free; open-source	https://terminals.codeplex.com/
Secure Shell App	free; Chrome Addon	https://chrome.google.com/webstore/detail/pnhechapfaindjhompbnflcldab bghjo

4. Demonstração em vídeo



The image shows a terminal window with a dark blue background. A large, semi-transparent watermark in the center reads "SSH com senha ou chave" in white, bold, sans-serif font. To the right of the watermark, there is a circular inset image of a man with short dark hair and a mustache, wearing black sunglasses. The terminal text is as follows:

```

SergioCabral
Password:
Linux devnator 4.19.10-10-cloud-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

Last login: Tue Sep 29 23:54:11 2020 from 177.79.120.44
sergiocabral@devnator:~$ mkdir .ssh
sergiocabral@devnator:~$ cd .ssh
sergiocabral@devnator:~/.ssh$ echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGCesxW56XDbbmvx
kIv5wtRLVuZgiKch...rsY5DHZBhnl...i1egWvxlf8CP76shM40XXLFv19Uz5qbck0hoJvE06mG0Dlz1a
u3pS4nfbfDMrIUvyIDR5mef+17...5K...AYpVK7007HHXRTtoEbmSsNgwpGA46Bb8LdLWNmyGEY00wY2FU
CpJ0wrNzG7...un...2yumz7mw+hZy2Fn4top2MfTRSrH...NcLpNdAXqGw
cz9/YwBK...8pEN...kR4rggfsftk8eEz0kHLZ/hQz/6...1dvHnbygn
Ho7DHQsBb...MhLMntHwWdTSW7gi/LDr...Qaf+RqHELMWDEIhU56MShgr...2j8mq5cHlhQs...Ao03CV
Xz...vNTYZ3mVpCh15P07...8P+bNg/vgrO6TEopihGN7mV0= CA...AL+SergioCabral@DEVNATOR"
>> authoriz...
sergiocabral@devnator:~$ exit
logout
Connection to machine.devnator.com closed.
⚡ SergioCabral@DEVNATOR.COM ~
> ssh sergiocabral@machine.devnator.com
Linux devnator 4.19.10-10-cloud-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

Last login: Tue Sep 29 23:55:29 2020 from 177.79.113.52
sergiocabral@devnator:~$
```

<https://youtu.be/64WqbNNJ0n4>

Hasta la vista.