STREAM SERIES

devnator

Acesso remoto SSH com senha ou chaves de criptografia

SERGIO CABRAL

sergiocabral.com

Índice

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@endere□o-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*.

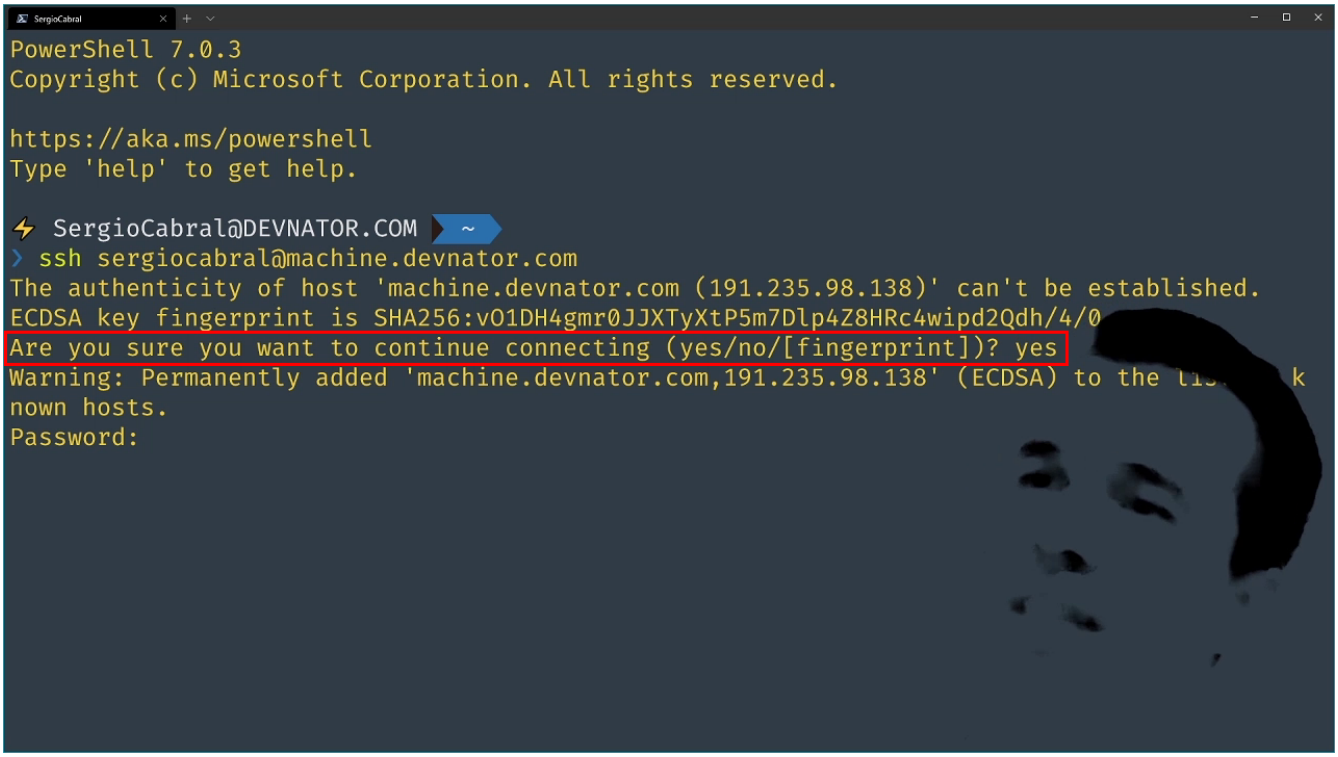


Figura 1. Confirmação no primeiro acesso ao computador remoto

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

Se este arquivo for apagado ou tiver a linha que contem 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 pressionar `Enter` até concluir, como mostrado na *Figura 2*.

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 sobreescreve 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.

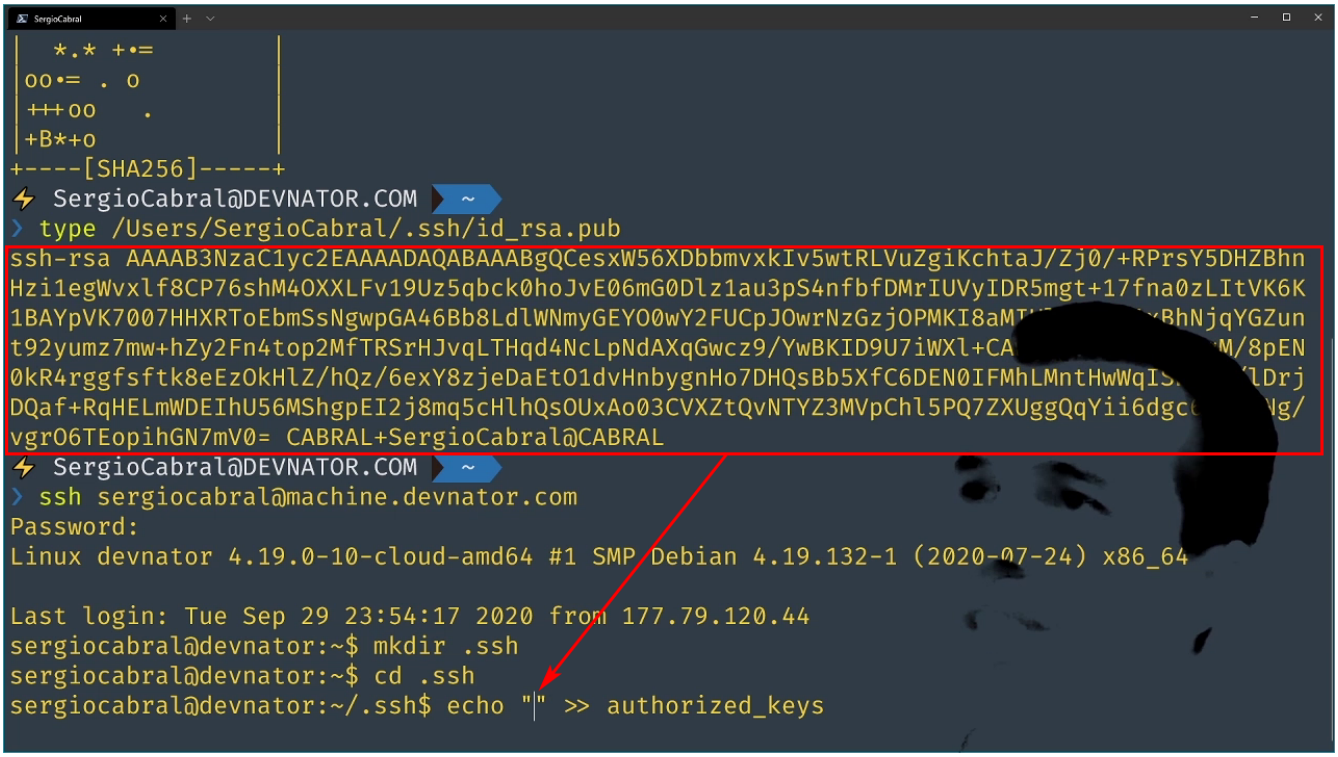


Figura 3. Conteúdo do arquivo "id_rsa.pub"

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 orígem:

- `scp ~/.ssh/id_rsa.pub nome-do-usuario@endere□o-do-servidor:~/.ssh`

Comando no computador de destino:

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

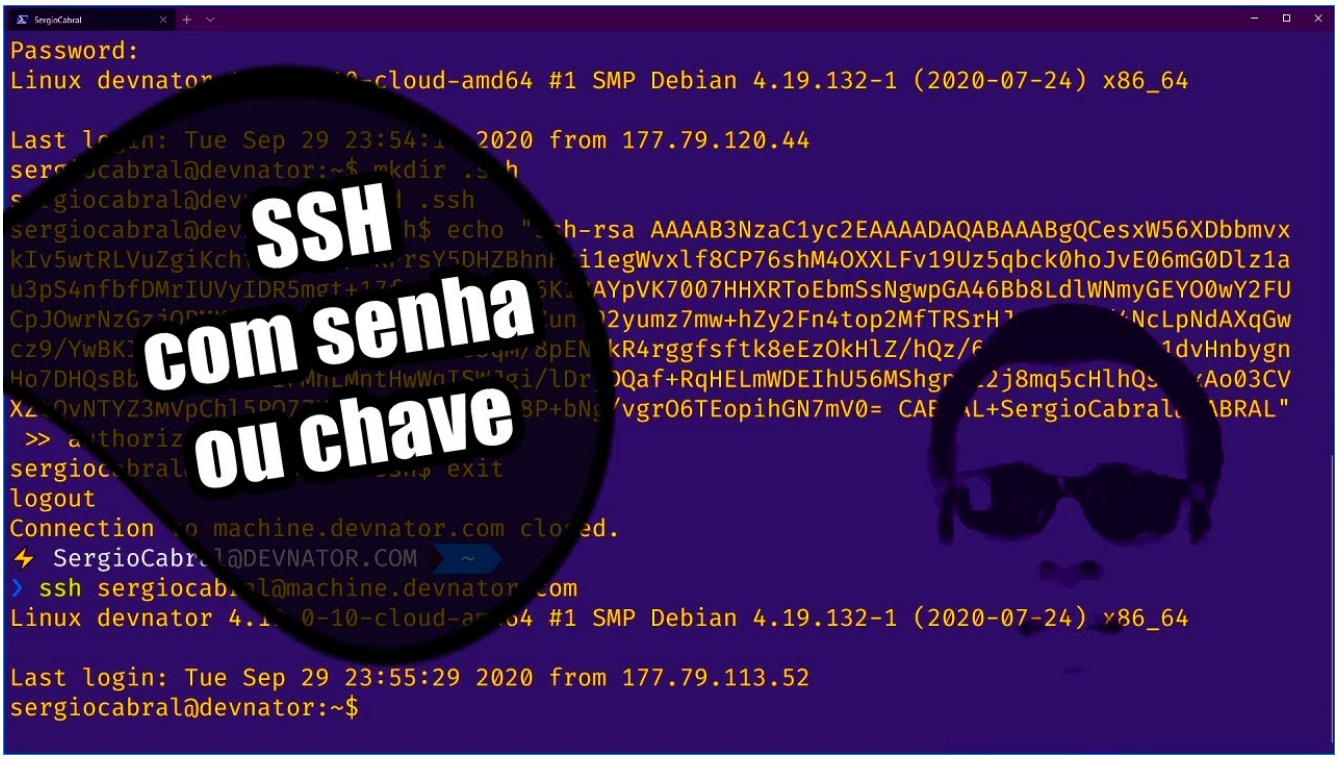
A partir de agora tanto o seu computador conhece o servidor, como o servidor conhece o seu computador. Cada computador tem a chave pública do outro.

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/pnhechapfaindjhompbnflcldabbghjo

4. Demonstração em vídeo



https://youtu.be/64WqbNNJ0n4

Hasta la vista.