Usando chave do ssh

O que é chave do ssh e por quê usá-la?

A chave de ssh é uma credencial que permite o detentor da chave acessar um servidor ssh. Ela consiste na verdade em um par de chaves: uma privada e outra pública. A chave privada deve ser guardada com segurança e, idealmente, não compartilhada. A pública deve ser colocada no servidor ssh de destino para a autenticação.

A chave ssh é uma alternativa à senha. Ela é mais segura pois não necessita transferir a senha ao servidor, possui tamanho maior e mais complexo do que qualquer senha que o usuário possa ter e permite acesso mais fácil ao servidor, sem ter precisar lembrar de senhas.

Como criar uma chave ssh e transferir para o servidor

Host Linux

Criar um par de chaves

Para criar um par de chaves com as opções padrões, basta rodar o comando `ssh-keygen` e responder as perguntas interativamente. Supondo *username* como o seu nome de usuário **local** e *hostname* como o host name de sua máquina:

```
> ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/<username>/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/<username>/.ssh/id_rsa
Your public key has been saved in /home/<username>/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:rwnGdXmwaCQvlAfoNsbfQz8jmKkmgwlrzHzH4rPkcBI @<hostname>
The key's randomart image is:
+---[RSA 3072]----+
|     ..          |
|    .  o         |
|   o  + o .      |
|    *. =.. +     |
| E o o.*S.+ .    |
|. .  .=++o+.     |
|=* o..+  o.o     |
|+=O+o+ . o       |
|. oB=   o        |
+----[SHA256]-----+
```

Pode-se alterar o nome e o caminho das chaves e, opcionalmente, adicionar uma senha associada à

chave. A senha será perguntada ao usuário tentar logar no servidor com a chave pública, a fim de aumentar a segurança. Recomenda-se utilizar a pasta e os nomes padrões para facilitar o próximo passo.

Adicionar a chave pública ao servidor

No exemplo será usado o servidor `sites.ime.usp.br` como o servidor ssh. Além disso, *server_username* é o nome do usuário no **servidor**.

```
> ssh-copy-id -i <pub_key_file> -p <port_num>
<server_username>@sites.ime.usp.br
/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
<server_username>@sites.ime.usp.br's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh
'<server_username>@sites.ime.usp.br'"
and check to make sure that only the key(s) you wanted were added.
```

A flag `-p <port_num>` é opcional e especifica a porta do servidor caso não seja a padrão 22. A `-i <pub_key_file>` especifica o caminho da chave pública (nome colocado ao criar com o `ssh-keygen` com o final `.pub`), sendo opcional caso tenha usado o caminho padrão na criação das chaves.

O comando pergunta interativamente a senha do servidor ssh do seu usuário para copiar a chave.

Acessando o servidor

Com as chaves criadas e a pública copiada, o usuário pode acessar o servidor com o comando `ssh -i <pub_key_file> -p <port_num> '<server_username>@sites.ime.usp.br'`. Assim como no comando anterior, as flags `-i <pub_key_file>` e `-p <port_num>` são opcionais. A senha da chave, caso tenha sido criada, será perguntada interativamente.

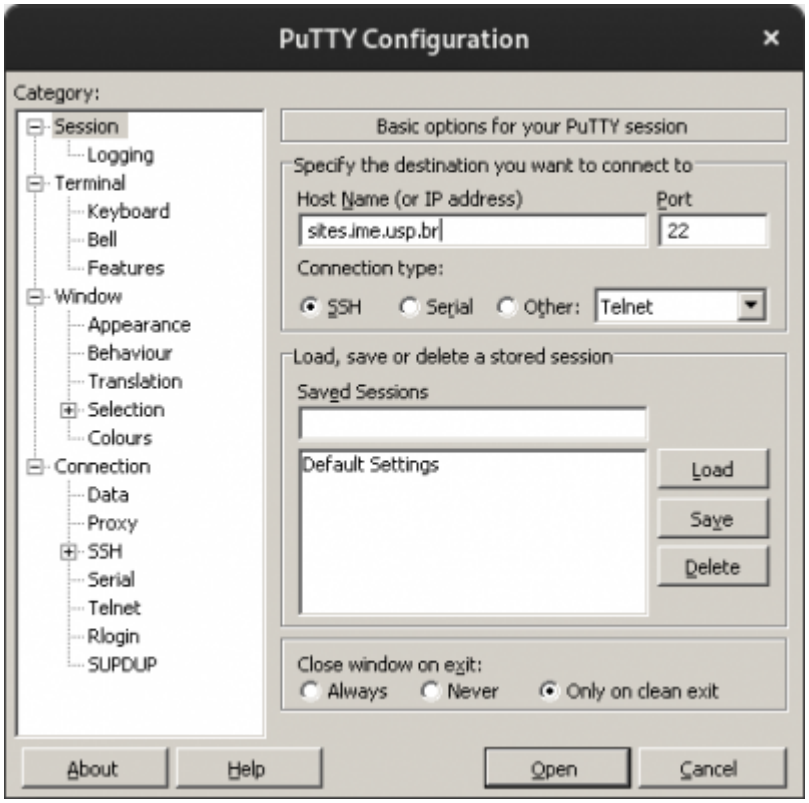
Host Windows

Instale o PuTTY

Acesse o link https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html e baixe o instalador do *PuTTY*. Execute o instalador.

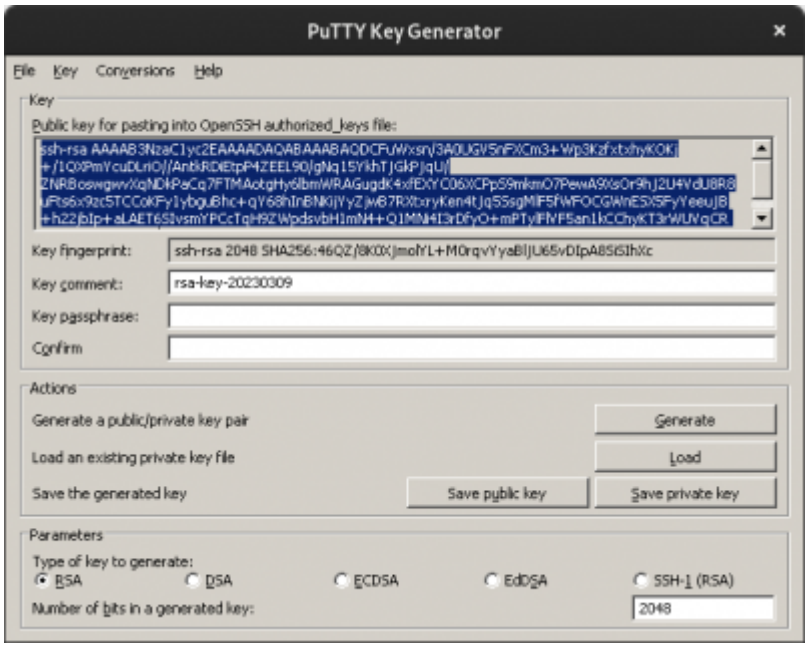
Logue no sites.ime.usp.br

Abra o programa **PuTTY** e insira `sites.ime.usp.br` no campo `Host Name` e clique em `Open`. Logue e deixe a janela aberta para os próximos passos.



Criando as chaves

Execute o programa **PuTTYgen**, crie as chaves clicando no botão `Generate` e copie a chave pública.



Adicionar a chave pública no servidor

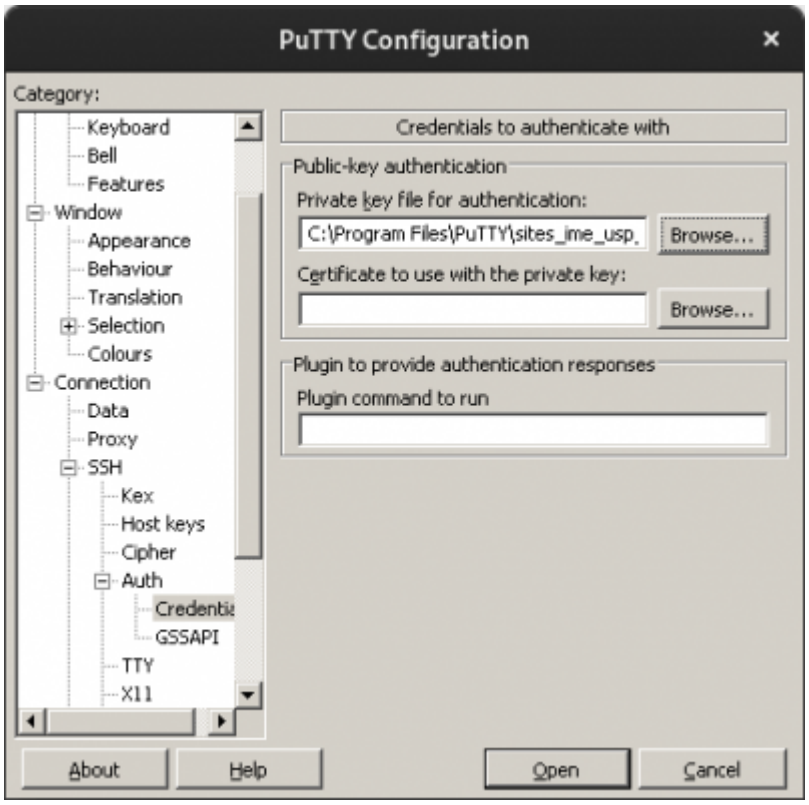
No servidor logado no **PuTTY** edite, com seu editor de texto favorito, o arquivo `${HOME}/.ssh/authorized_keys` para acrescentar a chave copiada no passo anterior e feche a sessão.

Salvar a chave privada

Clique no botão **Save private key** no **PuTTYgen** e salve em um lugar apropriado.

Adicionar chave privada ao PuTTY

No **PuTTY**, vá em `Connection > SSH > Auth > Credentials` e adicione o arquivo salvo no passo anterior em `Private key file for authentication`.



Com isso você consiguirá logar no `sites.ime.usp.br` usando a chave do ssh através do programa **PuTTY**.