# Acessando um Servidor Linux Remotamente com OpenSSH

OpenSSH é um conjunto de ferramentas que permite acessar e gerenciar remotamente servidores Linux de forma segura. Neste tutorial, você aprenderá a instalar o OpenSSH, configurar um servidor SSH e acessar um servidor Linux remotamente através do terminal.

## Instalando o OpenSSH

## No Servidor (Linux)

**Atualize a lista de pacotes:**

```
sudo apt update
```

**Instale o servidor OpenSSH:**

```
sudo apt install openssh-server
```

**Verifique se o serviço SSH está ativo:**

```
sudo systemctl status ssh
```

Você deve ver uma saída indicando que o serviço está ativo e em execução.

## No Cliente (Linux/macOS)

**Atualize a lista de pacotes:**

```
sudo apt update
```

**Instale o cliente OpenSSH:**

```
sudo apt install openssh-client
```

## Configurando o Servidor SSH

O arquivo de configuração do servidor SSH está localizado em `/etc/ssh/sshd_config`. As configurações padrão são geralmente suficientes, mas você pode ajustar conforme necessário.

**Abra o arquivo de configuração:**

```
sudo nano /etc/ssh/sshd_config
```

**Configurações comuns:**

- **Porta de escuta:** Por padrão, o SSH usa a porta 22. Para aumentar a segurança, você pode alterar a porta.

```
Port 2222
```

- **Desativar login de root:** Para maior segurança, desative o login direto do usuário root.

```
PermitRootLogin no
```

- **Autenticação por senha:** Certifique-se de que a autenticação por senha está habilitada.

```
PasswordAuthentication yes
```

**Reinicie o serviço SSH para aplicar as alterações:**

```
sudo systemctl restart ssh
```

## Acessando o Servidor Remotamente

## Do Linux ou macOS

**Abra o terminal.**

**Conecte-se ao servidor SSH:**

```
ssh usuario@ip_do_servidor
```

- **usuario:** O nome de usuário no servidor.
- **ip_do_servidor:** O endereço IP ou nome de domínio do servidor.

## Do Windows (usando PuTTY)

1. **Baixe e instale o PuTTY:**Download PuTTY
2. **Abra o PuTTY.**
3. **Digite o endereço IP do servidor no campo "Host Name (or IP address)":**
4. **No campo "Port", insira a porta SSH (padrão é 22 ou a porta que você configurou):**
5. **Clique em "Open".**
6. **Uma janela de terminal se abrirá solicitando o nome de usuário e senha.**

## Configurações Adicionais de Segurança

## Usando Chaves SSH em vez de Senhas

**No cliente, gere um par de chaves SSH:**

```
ssh-keygen
```

Siga as instruções para salvar a chave em um local seguro.

**Copie a chave pública para o servidor:**

```
ssh-copy-id usuario@ip_do_servidor
```

**No servidor, verifique se a chave foi adicionada ao arquivo `~/.ssh/authorized_keys`.**

**Desabilite a autenticação por senha para aumentar a segurança:**

```
sudo nano /etc/ssh/sshd_config
```

Altere a linha:

```
PasswordAuthentication no
```

**Reinicie o serviço SSH:**

```
sudo systemctl restart ssh
```