在 Ubuntu 中配置 SSH 的完整指南

作者： Chris Patrick Carias Stas 译者： LCTT Donkey | 2022-10-25 10:21

> 如今 SSH 已成为了登录远程服务器的默认方式。

SSH 的全称是 “ 安全的 Shell(Secure Shell) ”，它功能强大、效率高，这个主流的网络协议用于在两个远程终端之间建立连接。让我们不要忘记它名称的“安全”部分，SSH 会加密所有的通信流量，以防止如劫持、窃听等攻击，同时提供不同的身份认证方式和无数个配置选项。

在这份新手指南中，你会学到：

- SSH 的基本概念
- 设置 SSH 服务器（在你想要远程登录的系统上）
- 从客户端（你的电脑）通过 SSH 连接远程服务器

SSH 的基本概念

在学习配置过程前，让我们先了解一下 SSH 的全部基础概念。

SSH 协议基于 客户端-服务器(server-client) （CS）架构。 “ 服务器(Server) ” 允许 “ 客户端(Client) ” 通过通信通道进行连接。该信道是经过加密的，信息交换通过 SSH 公私钥进行管理。

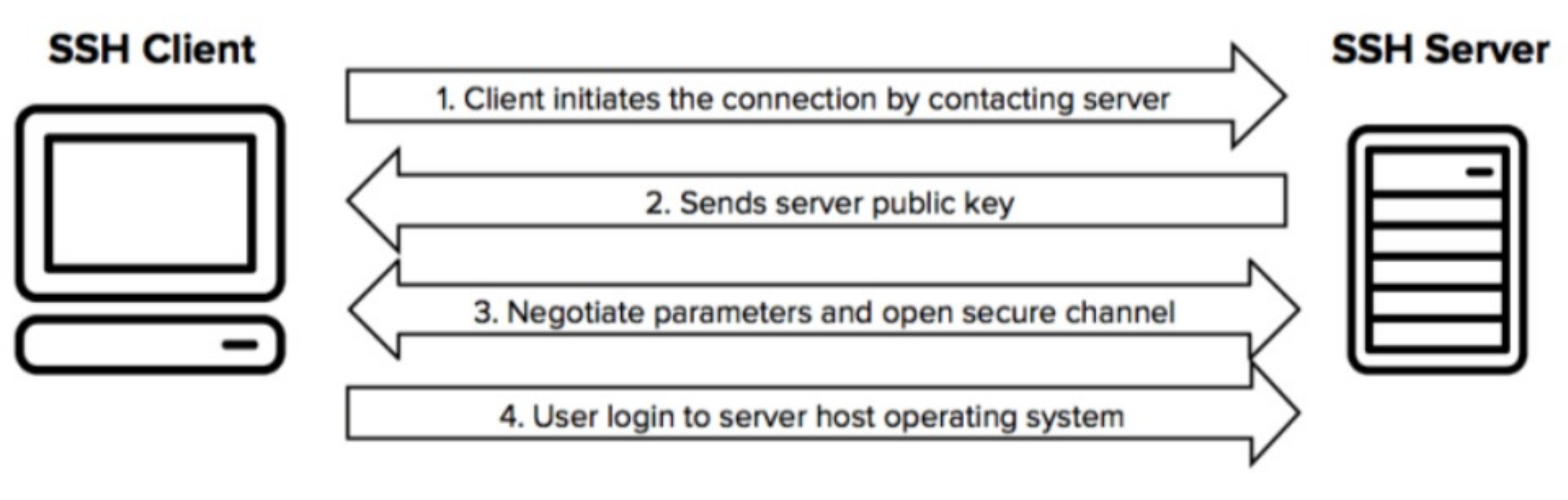


Image credit: SSH

OpenSSH 是在 Linux、BSD 和 Windows 系统上提供 SSH 功能的最流行的开源工具之一。

想要成功配置 SSH，你需要：

- 在作为服务器的机器上部署 SSH 服务器组件，它由 `openssh-server` 包提供。
- 在你远程访问服务器的客户端机器上部署 SSH 客户端组件，它由 `openssh-client` 包提供，大多数 Linux 和 BSD 发行版都已经预装好了。

区分服务器和客户端是十分重要的事情。或许你不想要你的 PC 作为 SSH 服务器，除非你有充分理由希望其他人通过 SSH 连接你的系统。

通常来说，你有一个专用的服务器系统。例如，一个 运行 Ubuntu 的树莓派 。你可以 启用树莓派的 SSH 服务 ，这样你可以在你 PC 中的终端中，通过 SSH 控制并管理该设备。

有了这些信息，让我们看看如何在 Ubuntu 上设置 SSH 服务器。

在 Ubuntu 服务器中配置 SSH

设置 SSH 并不复杂，只需要以下几步。

前提

- 一个在服务器端拥有 `sudo` 权限的用户
- 可以下载所需包的互联网连接
- 在你的网络中至少有另一个系统。可以是局域网中的另一台电脑，远程服务器或者计算机中托管的虚拟机。

再次强调，在你想要通过 SSH 远程登录的系统上安装 SSH 服务。

第一步：安装所需包

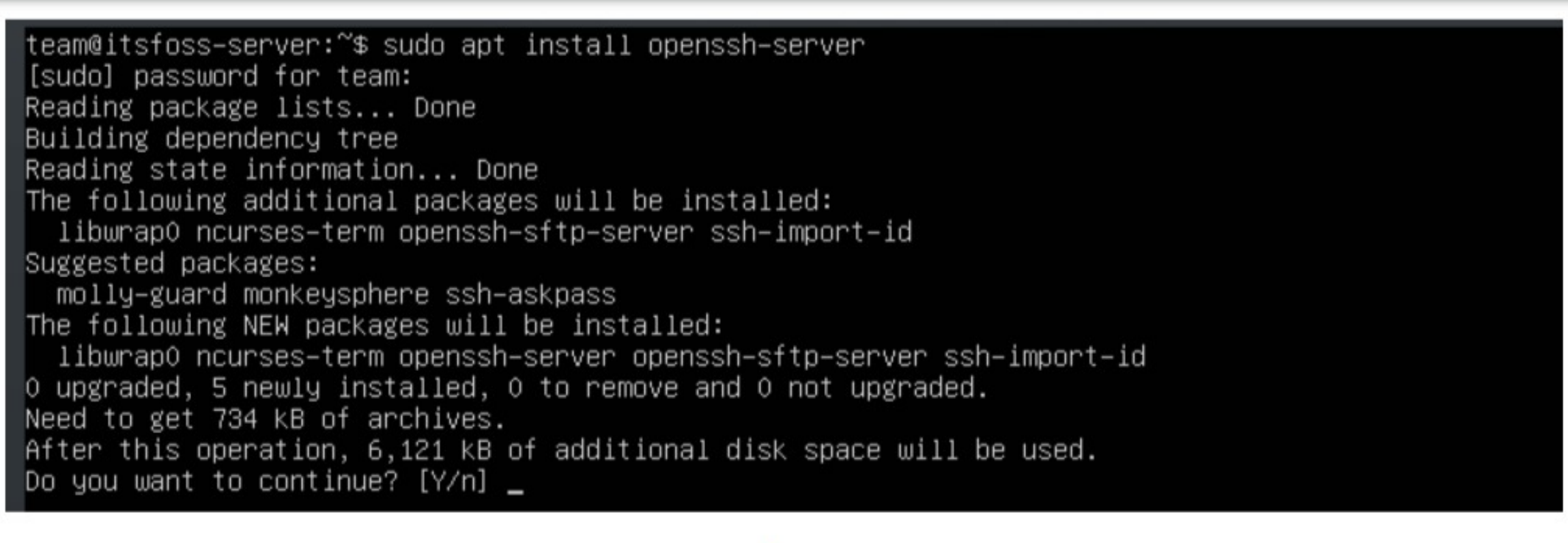
让我们从打开终端输入一些必要命令开始。

注意，在安装新的包或者软件前，要 更新你的 Ubuntu 系统 ，以确保运行的是最新版本的程序。

```
sudo apt update && sudo apt upgrade
```

你要运行 SSH 服务器的包由 OpensSSH 的 `openssh-server` 组件提供：

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



```
team@itsfoss-server:~$ sudo apt install openssh-server
[sudo] password for team:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libwrap0 ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  libwrap0 ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.
Need to get 734 kB of archives.
After this operation, 6,121 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

第二步：检查服务器状态

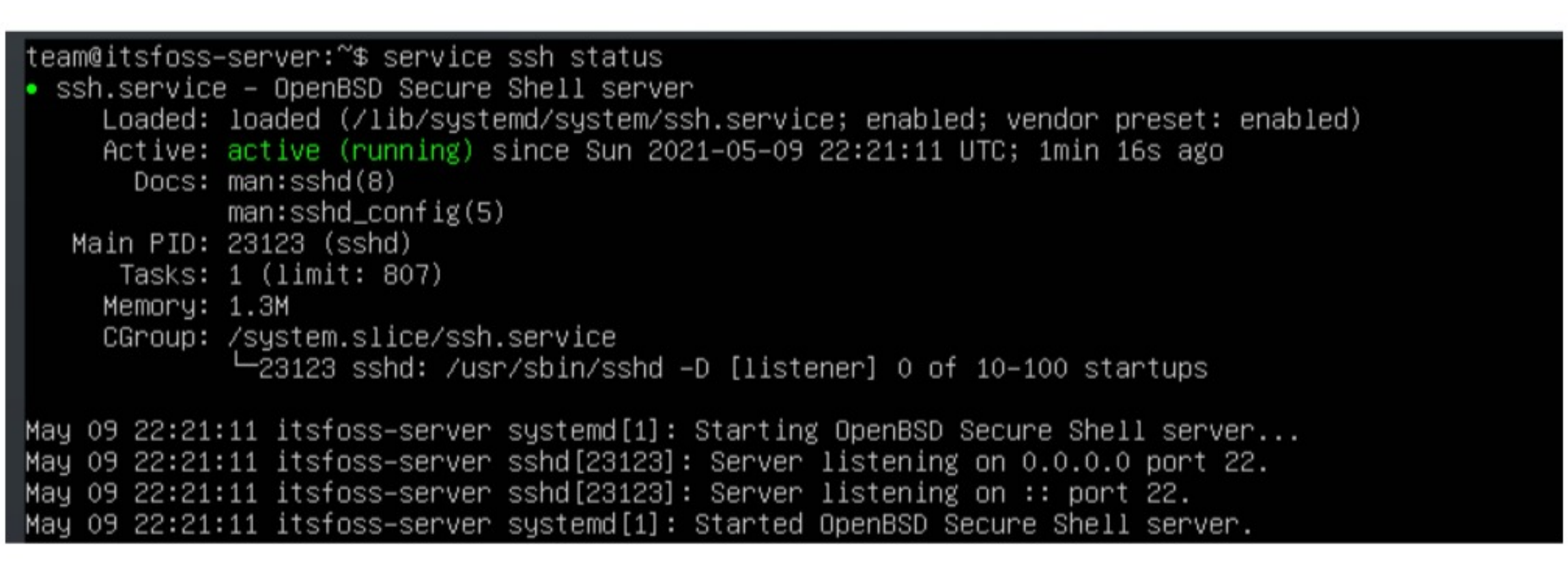
当你下载并安装完包后，SSH 服务器应该已经运行了，但是为了确保万无一失我们需要检查一下：

```
service ssh status
```

你还可以使用 `systemctl` 命令：

```
sudo systemctl status ssh
```

你应该会看到这样的结果，其中 `active` 是高亮的。输入 `q` 退出该页面。



```
team@itsfoss-server:~$ service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Sun 2021-05-09 22:21:11 UTC; 1min 16s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 23123 (sshd)
      Tasks: 1 (limit: 807)
     Memory: 1.3M
     CGroup: /system.slice/ssh.service
             └─23123 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

May 09 22:21:11 itsfoss-server systemd[1]: Starting OpenBSD Secure Shell server...
May 09 22:21:11 itsfoss-server sshd[23123]: Server listening on 0.0.0.0 port 22.
May 09 22:21:11 itsfoss-server sshd[23123]: Server listening on :: port 22.
May 09 22:21:11 itsfoss-server systemd[1]: Started OpenBSD Secure Shell server.
```

如果你的结果中 SSH 服务没有运行，使用这个命令运行它：

```
sudo systemctl enable --now ssh
```

第三步：允许 SSH 通过防火墙

Ubuntu 带有名为 UFW （ 简单的防火墙(Uncomplicated Firewall) ）的防火墙，这是管理网络规则的 `iptables` 的一个接口。如果启动了防火墙，它可能会阻止你连接服务器。

想要配置 UFW 允许你的接入，你需要运行如下命令：

```
sudo ufw allow ssh
```

UFW 的运行状态可以通过运行 `sudo ufw status` 来检查。

现在，我们的 SSH 服务器已经开始运行了，在等待来自客户端的连接。

连接远程服务器

你本地的 Linux 系统已经安装了 SSH 客户端。如果没有，你可以在 Ubuntu 中使用如下命令安装：

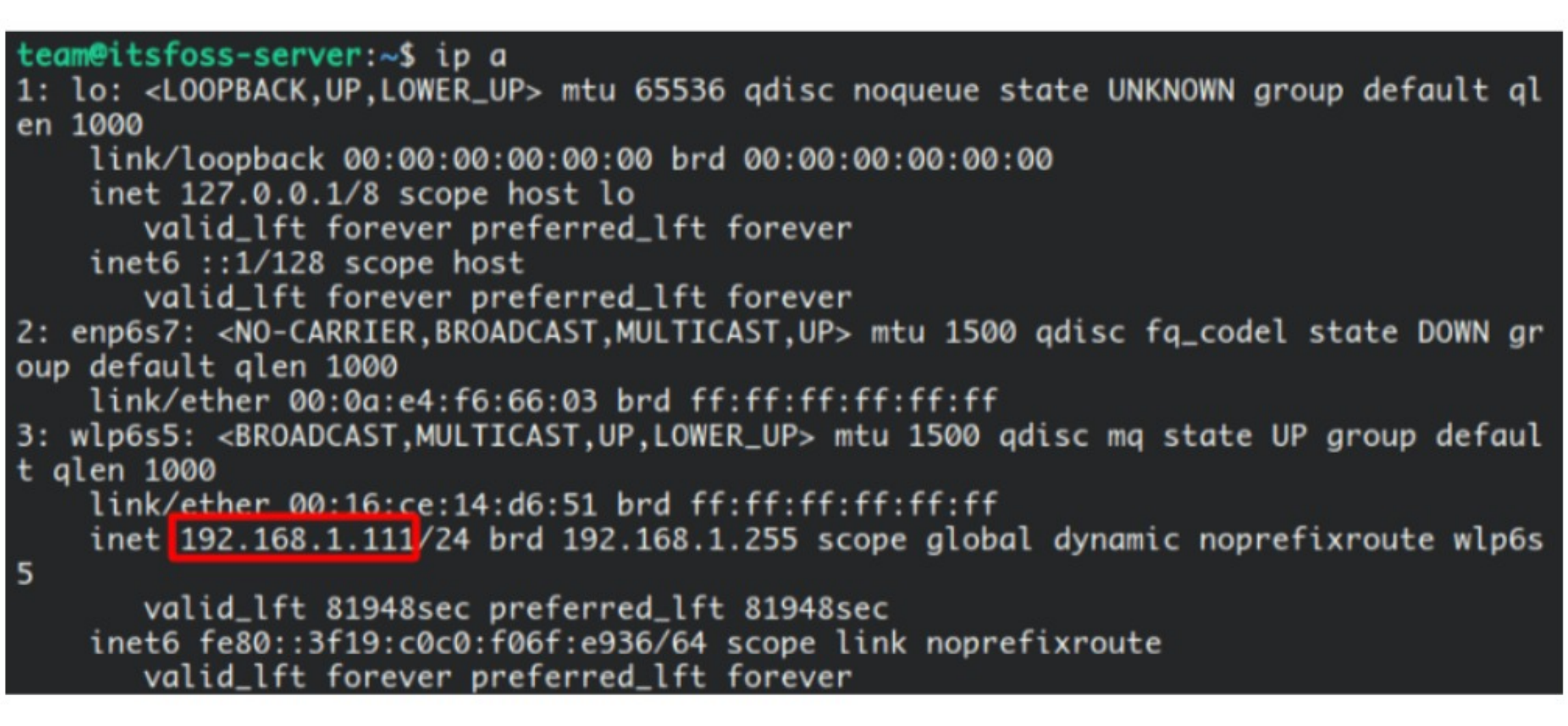
```
sudo apt install openssh-client
```

要连接你的 Ubuntu 系统，你需要知道它的 IP 地址，然后使用 `ssh` 命令，就像这样：

```
ssh username@address
```

将 **用户名** （ `username` ）改为你的系统上的实际用户名，并将 **地址** （ `address` ）改为你服务器的 IP 地址。

如果你 不知道 IP 地址 ，可以在服务器的终端输入 `ip a` 查看结果。应该会看到这样的结果：



```
team@itsfoss-server:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default ql
en 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp6s7: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN gr
oup default qlen 1000
    link/ether 00:0a:e4:f6:66:03 brd ff:ff:ff:ff:ff:ff
3: wlp6s5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group defaul
t qlen 1000
    link/ether 00:16:ce:14:d6:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.111/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp6s
5
       valid_lft 81948sec preferred_lft 81948sec
    inet6 fe80::3f19:c0c0:f06f:e936/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Using “ip a” to find the IP address

可以看到我的 IP 地址是 `192.168.1.111` 。让我们使用 `username@address` 格式进行连接。

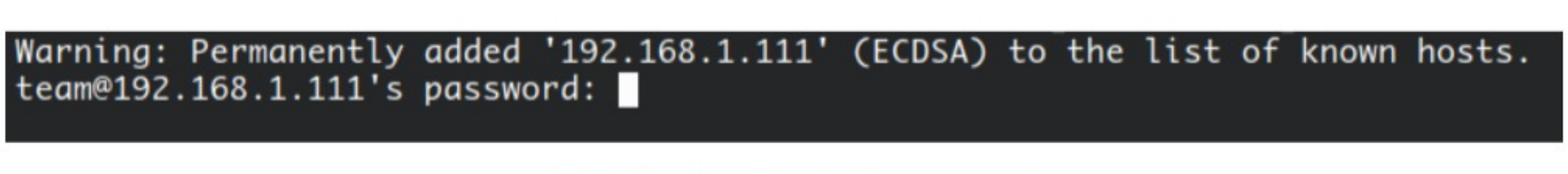
```
ssh team@192.168.1.111
```

这是你第一次连接到该 SSH 服务器，它会请求添加主机。输入 `yes` 并回车即可。

```
team@itsfoss:~$ ssh team@192.168.1.111
The authenticity of host '192.168.1.111 (192.168.1.111)' can't be established.
ECDSA key fingerprint is SHA256:lfLBuAFRhr68VwU7epRbF+oQKyfiUBwTihor/87Bvak.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

First time connecting to the server

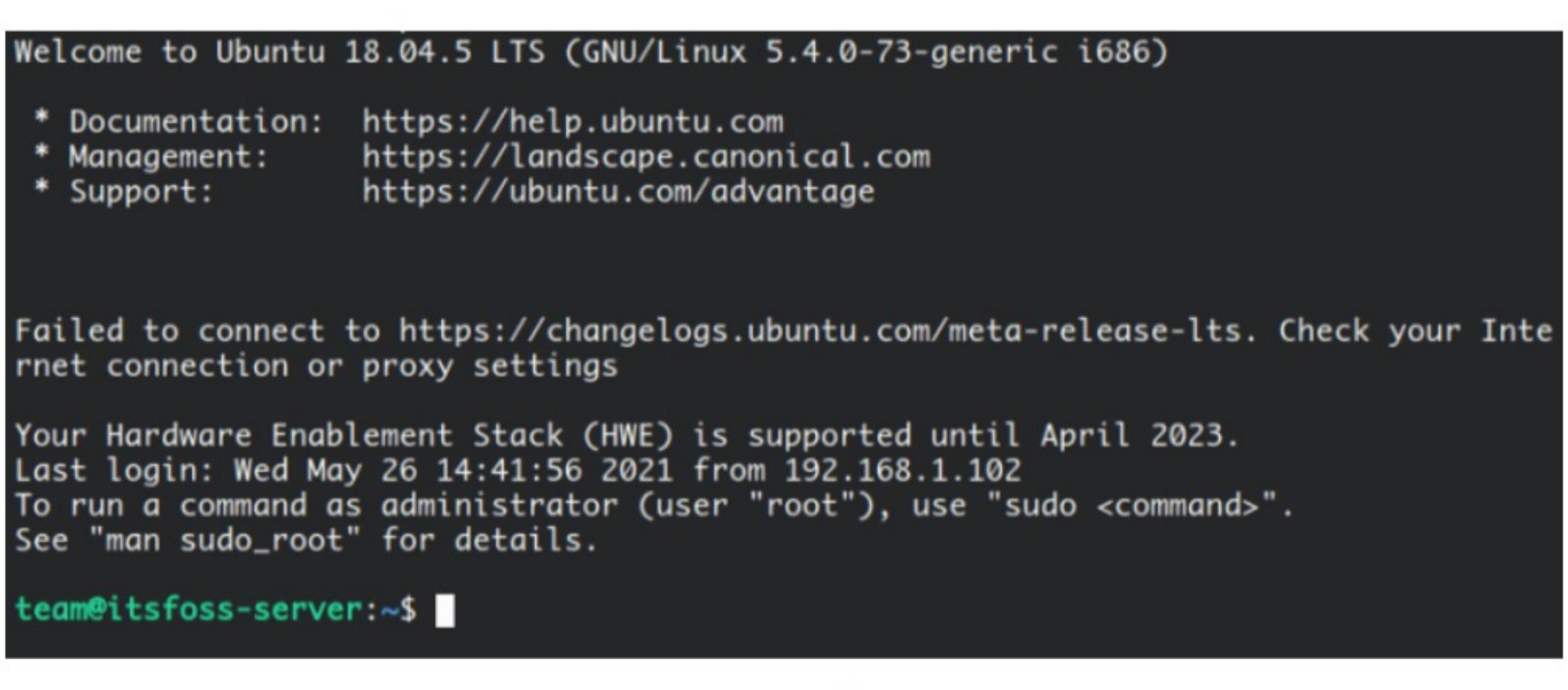
SSH 会立即告诉你该主机已经被永久添加了，并要求你输入指定用户的密码，输入密码并再次按回车即可。



```
Warning: Permanently added '192.168.1.111' (ECDSA) to the list of known hosts.
team@192.168.1.111's password:
```

Host added, now type in the password

瞧，你远程登录了你的 Ubuntu 系统！



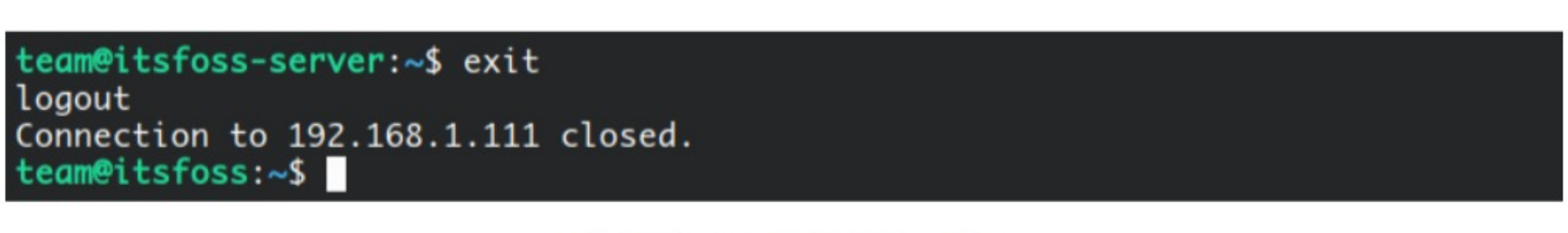
```
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-73-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Inte
rnet connection or proxy settings

Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Wed May 26 14:41:56 2021 from 192.168.1.102
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

team@itsfoss-server:~$
```

Connected!

现在，你可以在远程服务器的终端里和寻常一样工作了。

关闭 SSH 连接

你只需要输入 `exit` 即可关闭连接，它会立马关闭不需要确认。



```
team@itsfoss-server:~$ exit
logout
Connection to 192.168.1.111 closed.
team@itsfoss:~$
```

Closing the connection with “exit”

在 Ubuntu 中关闭并禁止 SSH

如果你想要停止 SSH 服务，需要运行该命令：

```
sudo systemctl stop ssh
```

该命令会关闭 SSH 服务，直到重启它或者系统重启。想要重启它，输入：

```
sudo systemctl start ssh
```

现在，如果你想要禁止 SSH 跟随系统启动，使用该命令：

```
sudo systemctl disable ssh
```

该命令不会停止当前的 SSH 会话，只会在启动的时候生效。如果你想要它跟随系统启动，输入：

```
sudo systemctl enable ssh
```

其他 SSH 客户端

从 Linux 到 macOS，大多数 *nix 系统中都有 `ssh` 工具，但这并不是唯一的选项，这里有几个可以在其他操作系统中使用的客户端：

- PuTTY 是一个自由开源的 Windows 系统上的 SSH 客户端。它功能强大并且简单易用。如果你从 Windows 系统上连接你的 Ubuntu 服务器，PuTTY 是最好的选择。（LCTT 译注：切记从官方网站下载。）
- 对安卓用户来说， JuiceSSH 是十分优秀的工具。如果你在旅途中需要一个移动客户端来连接你的 Ubuntu 系统，我强烈建议你试试 JuiceSSH。它已经出现了将近 10 年，并且可以免费使用。
- 最后是 Termius ，它可用于 Linux、Windows、macOS、iOS 和安卓。它有一个免费版本和几个付费选项。如果你运行大量服务器并进行共享连接的团队合作，那么 Termius 对你来说是一个不错的选择。

总结

在这份指导中，你可以在 Ubuntu 系统中设置 SSH 作为服务器，允许来自你电脑的远程安全的连接，便于你通过命令行开展工作。

此，我推荐以下文章：

- Linux SSH 入门教程
- 利用 SSH 配置文件管理多个 SSH 连接
- 向 SSH 服务器添加公钥以进行无密码身份验证
- 保护你的 SSH 服务器的 SSH 加固技巧

远程工作快乐！