# 在 Linux 上保护 SSH 服务器连接的 8 种方法

[在 Linux 上保护 SSH 服务器连接的 8 种方法](https://www.linuxmi.com/secure-ssh-connections-linux.html)

SSH 是一种广泛使用的协议，用于安全地访问 Linux 服务器。大多数用户使用默认设置的 SSH 连接来连接到远程服务器。但是，不安全的默认配置也会带来各种安全风险。

具有开放 SSH 访问权限的服务器的 root 帐户可能存在风险。尤其是如果您使用的是公共 IP 地址，则破解 root 密码要容易得多。因此，有必要了解 SSH 安全性。

这是在 Linux 上保护 SSH 服务器连接的方法。

## 1.禁用root用户登录

为此，首先，禁用 root 用户的 SSH 访问并创建一个具有 root 权限的新用户。关闭 root 用户的服务器访问是一种防御策略，可以防止攻击者实现入侵系统的目标。例如，您可以创建一个名为**exampleroot**的用户，如下所示：

useradd -m exampleroot  
passwd exampleroot  
usermod -aG sudo exampleroot

以下是上述命令的简要说明：

* **useradd**创建一个新用户，并且**-m**参数在您创建的用户的**主**目录下创建一个文件夹。

* **passwd**命令用于为新用户分配密码。请记住，您分配给用户的密码应该很复杂且难以猜测。

* **usermod -aG sudo**将新创建的用户添加到管理员组。

在用户创建过程之后，需要对**sshd\_config**文件进行一些更改。**您可以在/etc/ssh/sshd\_config**找到此文件。使用任何文本编辑器打开文件并对其进行以下更改：

# Authentication:   
#LoginGraceTime 2m   
PermitRootLogin no   
AllowUsers exampleroot



**PermitRootLogin** 行将阻止 root 用户使用 SSH 获得远程访问。在**AllowUsers** 列表中包含 **exampleroot** 会向用户授予必要的权限。

最后，使用以下命令重启 SSH 服务：

linuxmi@linuxmi /home/linuxmi/www.linuxmi.com   
⚡ sudo systemctl restart ssh

如果失败并且您收到错误消息，请尝试以下命令。这可能因您使用的 Linux 发行版而异。

linuxmi@linuxmi /home/linuxmi/www.linuxmi.com  
 sudo systemctl restart sshd

## 2.更改默认端口

默认的 SSH 连接端口是 22。当然，所有的攻击者都知道这一点，因此需要更改默认端口号以确保 SSH 安全。尽管攻击者可以通过 Nmap 扫描轻松找到新的端口号，但这里的目标是让攻击者的工作更加困难。

要更改端口号，请打开**/etc/ssh/sshd\_config**并对文件进行以下更改：/

Include /etc/ssh/sshd\_config.d/\*.conf  
Port 22099



在这一步之后，使用**sudo systemctl restart ssh**再次重启 SSH 服务。现在您可以使用刚刚定义的端口访问您的服务器。如果您使用的是防火墙，则还必须在此处进行必要的规则更改。在运行**netstat -tlpn**命令时，您可以看到您的 SSH 端口号已更改。

## 3. 禁止使用空白密码的用户访问

在您的系统上可能有您不小心创建的没有密码的用户。要防止此类用户访问服务器，您可以将**sshd\_config**文件中的**PermitEmptyPasswords**行值设置为**no**。

PermitEmptyPasswords no

## 4.限制登录/访问尝试

默认情况下，您可以根据需要尝试多次输入密码来访问服务器。但是，攻击者可以利用此漏洞对服务器进行暴力破解。通过指定允许的密码尝试次数，您可以在尝试一定次数后自动终止SSH 连接。

为此，请更改**sshd\_config**文件中的**MaxAuthTries**值。

MaxAuthTries 3

## 5. 使用 SSH 版本 2

SSH 的第二个版本发布是因为第一个版本中存在许多漏洞。默认情况下，您可以通过将**Protocol**参数添加到**sshd\_config**文件来启用服务器使用第二个版本。这样，您未来的所有连接都将使用第二个版本的 SSH。

Include /etc/ssh/sshd\_config.d/\*.conf   
Protocol 2

## 

## 6.关闭TCP端口转发和X11转发

攻击者可以尝试通过 SSH 连接的端口转发来访问您的其他系统。**为了防止这种情况，您可以在sshd\_config**文件中关闭**AllowTcpForwarding**和**X11Forwarding**功能。

X11Forwarding no   
AllowTcpForwarding no

## 7. 使用 SSH 密钥连接

连接到服务器的最安全方法之一是使用 SSH 密钥。使用 SSH 密钥时，无需密码即可访问服务器。**另外，您可以通过更改sshd\_config**文件中与密码相关的参数来完全关闭对服务器的密码访问。

创建 SSH 密钥时，有两个密钥：**Public**和**Private**。公钥将上传到您要连接的服务器，而私钥则存储在您将用来建立连接的计算机上。

**在您的计算机上使用ssh-keygen**命令创建 SSH 密钥。不要将**密码短语**字段留空并记住您在此处输入的密码。如果将其留空，您将只能使用 SSH 密钥文件访问它。但是，如果您设置了密码，则可以防止拥有密钥文件的攻击者访问它。例如，您可以使用以下命令创建 SSH 密钥：

ssh-keygen

## 8. SSH 连接的 IP 限制

大多数情况下，防火墙使用自己的标准框架阻止访问，旨在保护服务器。但是，这并不总是足够的，您需要增加这种安全潜力。

为此，请打开**/etc/hosts.allow**文件。通过对该文件进行的添加，您可以限制 SSH 权限，允许特定 IP 块，或输入单个 IP 并使用拒绝命令阻止所有剩余的 IP 地址。

下面您将看到一些示例设置。完成这些之后，像往常一样重新启动 SSH 服务以保存更改。



## Linux 服务器安全的重要性

所有服务器管理员都应该考虑数据和数据安全问题。服务器安全是一个非常敏感的问题，因为攻击的主要焦点是 Web 服务器，它们几乎包含有关系统的所有信息。由于大多数服务器都在 Linux 基础架构上运行，因此熟悉 Linux 系统和服务器管理非常重要。

SSH 安全只是保护服务器的方法之一。可以通过停止、阻挡或减缓攻击来最大程度地减少您受到的伤害。除了提供 SSH 安全性之外，您还可以实施许多不同的方法来保护您的 Linux 服务器。