服务器安全配置重要步骤

下面的安全设置主要包括：
1、修改服务器SSH端口号；
2、创建非root用户，设置管理员权限；
3、指定某一特定用户可切换到root用户，其他用户不可切换到root，且切换到root用户时必须要使用密码；
4、禁用root用户直接使用SSH方式登录；
5、（可选）根据自己选择，可设置密钥登录或者密码登录；
6、（可选）如果有固定IP，可以设置只有在指定IP才可以登录；
7、设置登录失败次数锁定

禁用root用户直接SSH登陆

要设置禁止root用户直接SSH登录，并强制通过指定普通用户跳转到root，请按以下步骤操作：

完整配置步骤

1. 创建管理员用户（如果还没有）

```
# 创建新用户（例如：newrtad，不建议使用admin等类似英语单词）
sudo adduser newrtad

# 设置密码（需要输入两次）
sudo passwd <建议英文大写小子字母+特殊字符+数字组合，长度至少不要低于8位>

# 将用户添加到sudo组（Ubuntu/Debian）
sudo usermod -aG sudo newrtad

# CentOS/RHEL系统使用wheel组
sudo usermod -aG wheel newrtad
```

2. 配置SSH禁止root登录

编辑SSH配置文件：

```
sudo nano /etc/ssh/sshd_config  #如果命令失败，则检查服务器中是否有nano工具，如果没有则安装一下，也可以使用vim
```

修改或添加以下配置：

```
# 修改SSH端口号(修改一个高位端口，然后测试使用新端口打开一个新的SSH窗口看能否正常链接，原端口先不要关，测试无问题后)
port 51289

# 禁止root直接登录
PermitRootLogin no

# 允许密码认证（如果使用密钥登录可设为no）
PasswordAuthentication yes

# 只允许指定用户登录（可选但推荐）
AllowUsers newrtad
```

```
nano保存及退出命令：
保存：Ctrl+O
退出：Ctrl+X
```

> **重要提醒**：
>
> - 修改SSH配置前**务必保留一个root会话不退出**
> - 测试新配置**成功后再关闭所有root会话**
> - 建议先在测试环境验证配置

3. 配置sudo权限（关键步骤）

确保普通用户可以切换到root：

```
# 编辑sudoers文件（安全操作）
sudo visudo
```

在文件末尾添加：

```
# 允许nertad用户无密码切换到root（可选，建议选下面需要输入密码的方式）
newrtad ALL=(ALL) NOPASSWD: ALL

# 或者要求输入密码（更安全）
newrtad ALL=(ALL) ALL
```

4. 重启SSH服务

```
# Ubuntu/Debian
sudo systemctl restart sshd

# CentOS/RHEL
sudo systemctl restart sshd
```

5. 测试配置（重要！）

不要关闭当前root会话，新开终端测试该用户是否能正常切换到root用户下：

```
# 1. 用newrtad用户登录
ssh newrtad@your_server_ip

# 2. 切换到root（两种方式）
# 方式1：使用sudo（推荐）
sudo su -

# 方式2：使用su（需要root密码）
su -
```

安全增强建议

1. 禁用密码认证，使用SSH密钥

```
# 在本地生成密钥（如果还没有）
ssh-keygen -t rsa -b 4096

# 复制公钥到服务器
ssh-copy-id admin@your_server_ip

# 修改SSH配置
sudo nano /etc/ssh/sshd_config
```

修改：

```
PasswordAuthentication no
PubkeyAuthentication yes
```

2. 限制SSH登录IP（可选）

```
sudo nano /etc/hosts.allow
```

添加：

```
sshd: 192.168.1.0/24, your_trusted_ip
```

3. 设置登录失败锁定

```
sudo nano /etc/pam.d/sshd
```

在文件开头添加：

```
auth required pam_tally2.so deny=3 unlock_time=600 onerr=fail
```

验证配置

```
# 1. 检查SSH配置语法
sudo sshd -t

# 2. 检查sudo权限
sudo -l -U newrtad

# 3. 检查SSH服务状态
sudo systemctl status sshd
```

故障排除

问题现象	解决方案
无法用newrtad登录	检查/etc/ssh/sshd_config中的AllowUsers
无法切换到root	检查/etc/sudoers中的权限配置
SSH连接被拒绝	检查防火墙：sudo ufw status
密码认证失败	确认PasswordAuthentication yes

最终安全配置示例

```
# /etc/ssh/sshd_config
Port 51289
PermitRootLogin no
PasswordAuthentication no
PubkeyAuthentication yes
AllowUsers newrtad
MaxAuthTries 3
LoginGraceTime 60
```

```
# /etc/sudoers
admin ALL=(ALL) PASSWD: ALL
Defaults:admin !requiretty
```

操作后测试清单

1. ✅ 用newrtad用户SSH登录成功
2. ✅ `sudo su -` 切换到root成功
3. ✅ root直接SSH登录被拒绝
4. ✅ 其他用户SSH登录被拒绝（如果设置了AllowUsers）
5. ✅ SSH密钥认证正常工作（如果配置了）

> **重要提醒**：
>
> - 修改SSH配置前**务必保留一个root会话不退出**
> - 测试新配置**成功后再关闭所有root会话**
> - 建议先在测试环境验证配置
> - 定期备份SSH配置：`sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.bak`

微信