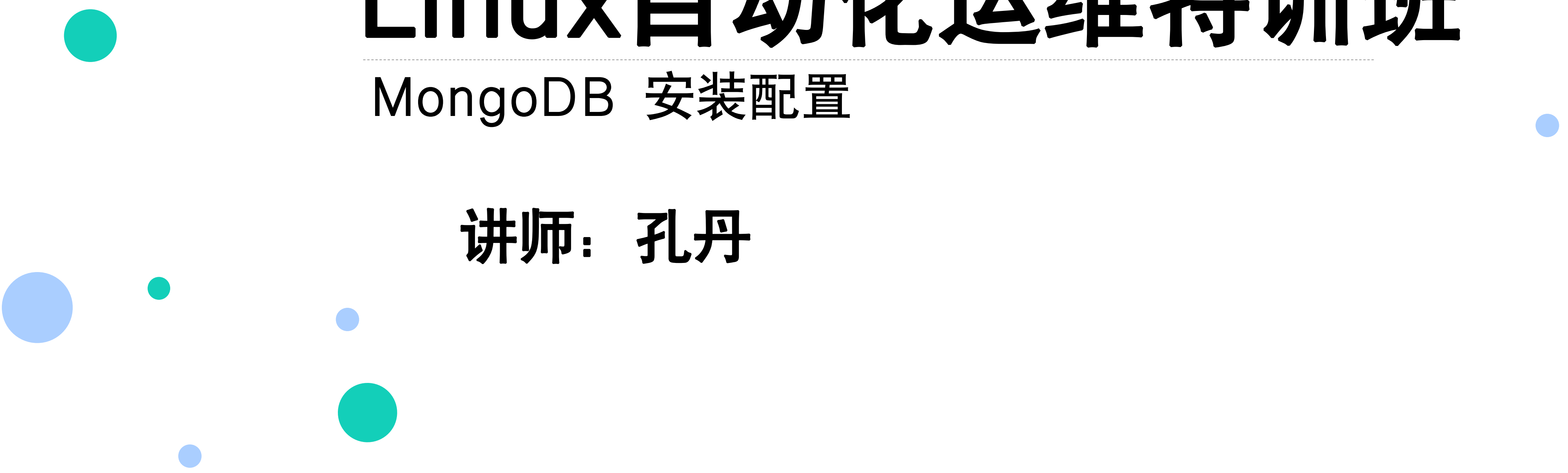




Linux自动化运维特训班

sshd服务实战

讲师：孔丹



大纲

- sshd简介
- 配置sshd服务
- 安全密钥验证
- 远程传输命令
- 安全文件传输协议sftp

sshd简介

- 传统的网络服务程序，如：ftp和telnet在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的非常人很容易就可以截获这些口令和数据。

演示tcpdump截获ftp用户名和密码。

```
tcpdump -i eth0 -nnX port 21
```

- SSH (Secure Shell) 是一种能够以安全的方式提供远程登录的协议，也是目前远程管理Linux系统的首选方式。
- 最初SSH是由芬兰的一家公司开发的。但是因为受版权和加密算法的限制，现在很多人都转而使用OpenSSH。OpenSSH是SSH的替代软件，而且是免费的，可以预计将来会有越来越多的人使用它而不是SSH。

配置sshd服务

- 想要使用SSH协议来远程管理Linux系统，则需要部署配置sshd服务程序。
- 提供两种安全验证的方法：
 - ✓ 基于口令的验证—用账户和密码来验证登录；
 - ✓ 基于密钥的验证—需要在本地生成密钥对，然后把密钥对中的公钥上传至服务器，并与服务器中的公钥进行比较；该方式相比较来说更安全。

配置sshd服务

□ sshd服务配置文件中包含的参数以及作用

参数	作用
Port 22	默认的sshd服务端口
ListenAddress 0.0.0.0	设定sshd服务器监听的IP地址
Protocol 2	SSH协议的版本号
HostKey /etc/ssh/ssh_host_key	SSH协议版本为1时，DES私钥存放的位置
HostKey /etc/ssh/ssh_host_rsa_key	SSH协议版本为2时，RSA私钥存放的位置
HostKey /etc/ssh/ssh_host_dsa_key	SSH协议版本为2时，DSA私钥存放的位置
PermitRootLogin yes	设定是否允许root管理员直接登录
StrictModes yes	当远程用户的私钥改变时直接拒绝连接
MaxAuthTries 6	最大密码尝试次数
MaxSessions 10	最大终端数
PasswordAuthentication yes	是否允许密码验证
PermitEmptyPasswords no	是否允许空密码登录（很不安全）

配置sshd服务

□ 客户端软件的连接方式:

ssh username@ip

ssh -X username@ip

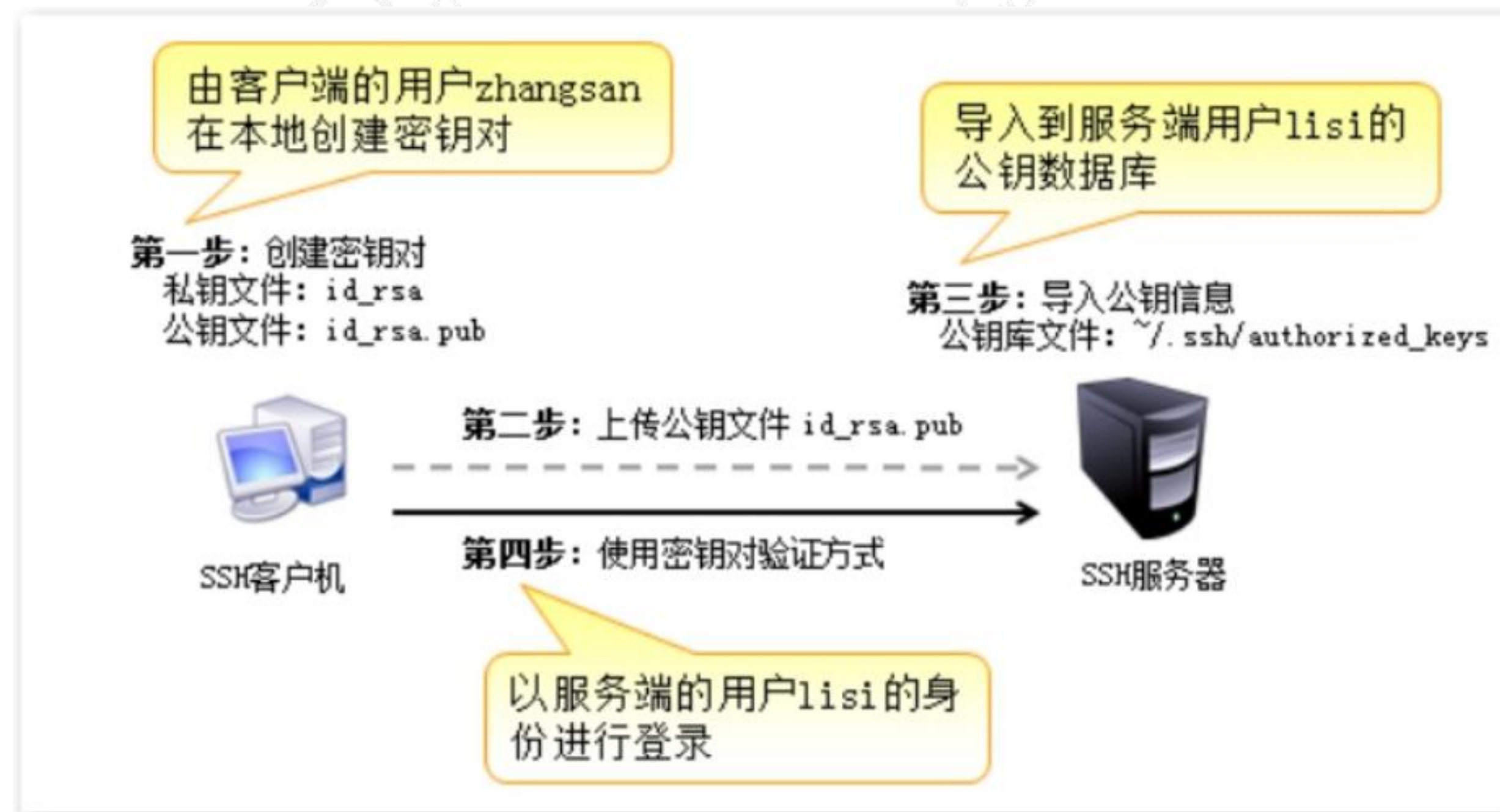
图形

##文本模式的连接

##可以在连接成功后开启

安全密钥验证

- 在生产环境中使用密码进行口令验证终归存在着被暴力破解或嗅探截获的风险。如果正确配置了密钥验证方式，那么sshd服务程序将更加安全。



安全密钥验证

- 第1步：在客户端主机中生成“密钥对”。

```
[root@kongd ~]# ssh-keygen -f ~/.ssh/id_rsa -P "" -q
```

- 第2步：把客户端主机中生成的公钥文件传送至远程主机。

```
[root@kongd ~]# ssh-copy-id -i ~/.ssh/id_rsa.pub  
root@192.168.95.15
```

- 第3步：对服务器进行设置，使其只允许密钥验证，拒绝传统的口令验证方式。

- 第4步：在客户端测试登录到服务器。

```
[root@kongd ~]# ssh 192.168.95.15 ip a
```


远程传输命令

- scp (secure copy) 是一个基于SSH协议在网络之间进行安全传输的命令，其格式：

scp [参数] 本地文件 远程帐户@远程IP地址:远程目录

scp命令中可用的参数及作用：

- v: 显示详细的连接进度
- P: 指定远程主机的sshd端口号
- r: 用于传送文件夹

安全文件传输协议sftp

□ sftp是Secure File Transfer Protocol的缩写，安全文件传送协议。可以为传输文件提供一种安全的网络的加密方法。sftp 与 ftp 有着几乎一样的语法和功能。SFTP 为 SSH的其中一部分，是一种传输档案至 Blogger 服务器的安全方式。

□ 常见命令参数

usage: sftp [-1246aCfpqrv] [-B buffer_size] [-b batchfile] [-c cipher]

 [-D sftp_server_path] [-F ssh_config] [-i

identity_file] [-l limit]

 [-o ssh_option] [-P port] [-R num_requests] [-S

program]

 [-s subsystem | sftp_server] host

sftp [user@]host[:file ...]

sftp [user@]host[:dir[/]]

sftp -b batchfile [user@]host

ssh的安全设定

- 1.是否允许用户通过登陆系统的密码做sshd的认证（不让其他用户去试密码）
- 2.设置是否允许root用户通过sshd服务的认证
- 3.黑名单与白名单

Allowusers westos ##设定用户白名单，白名单指默认不在名单中的用户不能使用sshd

Denyusers westos ##设定用户黑名单，黑名单指默认不在名单中的用户可以使用sshd

xshell基于密钥验证案例

□ 案例：使用xshell基于密钥验证

总结

- 1.sshd的验证方法。
- 2.基于密钥验证的配置。
- 3.sshd安全设置。

作业

- 1.在node1主机中建立用户westos，并设定其密码为westoslinux
- 2.配置node1中的sshd服务要求如下：
 - 1) 设定sshd服务只允许westos用户可以被访问使用
 - 2) 创建westos用户的key认证方式
 - 3) 设定westos用户只允许使用key认证方式，屏蔽其系统密码认证方式



谢谢观看

更多好课，请关注[万门大学APP](#)

