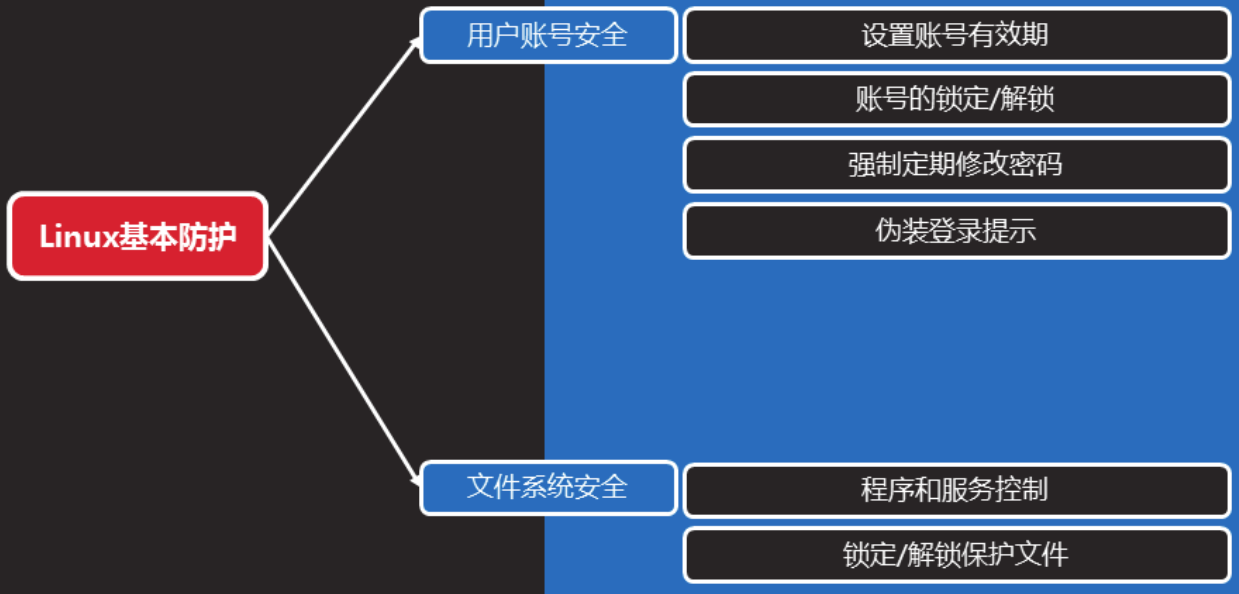
SECURITY DAY01

内容

上午	09:00 ~ 09:30	Linux基本防护
	09:30 ~ 10:20	
	10:30 ~ 11:20	用户切换与提权
	11:30 ~ 12:00	
下午	14:00 ~ 14:50	SSH访问控制
	15:00 ~ 15:50	SELinux安全防护
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑

Linux基本防护



用户账号安全

设置账号有效期

知识讲解

- 使用chage工具
  - -d 0，强制修改密码
  - -E yyyy-mm-dd，指定失效日期（-1取消）

```
[root@svr7 ~]# chage  -E  2017-12-31  zengye
[root@svr7 ~]# chage  -l  zengye
.. ..
Password inactive                       : never
Account expires                         : Dec 31, 2017
.. ..
```

账号的锁定/解锁

Tedu.cn 达内教育

知识讲解

- 使用passwd命令
  - -l 锁定、-u 解锁、-S 看状态

```
[root@svr7 ~]# passwd  -l  zengye
锁定用户 zengye 的密码 。
passwd: 操作成功
[root@svr7 ~]# passwd  -S  zengye
zengye LK 2017-07-13 0 99999 7 -1 (密码已被锁定。)
```

强制定期修改密码

Tedu.cn 达内教育

知识讲解

- 配置文件/etc/login.defs
  - 对新建的用户有效
- 主要控制属性
  - PASS_MAX_DAYS
  - PASS_MIN_DAYS
  - PASS_WARN_AGE

伪装登录提示

Tedu.cn 达内教育

知识讲解

- 配置文件/etc/issue、 /etc/issue.net
  - 分别适用于本地、远程登录
  - 默认会提示内核、系统等版本信息

```
Windows Server 2012 Enterprise R2
NT 6.2 Hybrid
svr1 login: root
Password:
Last login: Mon Jul 29 11:24:12 on tty1
[root@svr1 ~]#
```

Tedu.cn 达内教育

文件系统安全

程序和服务控制

Tedu.cn 达内教育

知识讲解

- 禁用非必要的系统服务
  - 使用systemctl、chkconfig工具

锁定/解锁保护文件

Tedu.cn 达内教育

知识讲解

- EXT3/EXT4的文件属性控制
  - chattr、lsattr
- +、-、=控制方式
  - 属性i：不可变（immutable）
  - 属性a：仅可追加（append only）

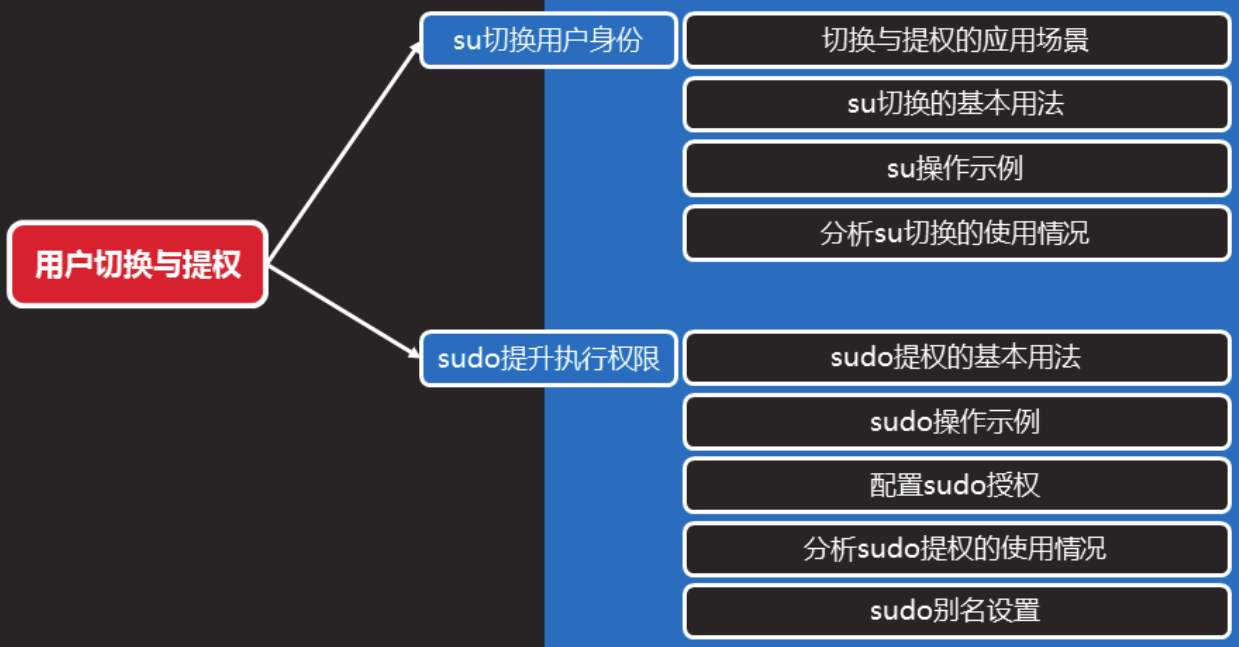
```
[root@svr7 ~]# chattr +i /etc/hosts
[root@svr7 ~]# echo "1.2.3.4 www.qq.com" >> /etc/hosts
bash: /etc/hosts: 权限不够
```

案例1：Linux基本防护措施

课堂练习

1. 使用户zhangsan在2017-12-31日失效
2. 临时锁定用户lisi的账户，验证效果后解除锁定
3. 锁定文件/etc/resolv.conf、/etc/hosts，以防止其内容被无意中修改
4. 修改tty终端提示，使得登录前看到的第一行文本为“Windows Server 2012 Enterprise R2”，第二行文本为“NT 6.2 Hybrid”

用户切换与提权



su切换用户身份

切换与提权的应用场景

知识讲解

- 切换用户身份，When？
  - SSH远程管理
  - 运维测试
- 提升执行权限，When？
  - 管理权限细分

su切换的基本用法

Tedu.cn 达内教育

知识讲解

- Substitute User，换人
  - 快速切换为指定的其他用户
  - 普通用户执行时，需验证目标用户的口令
  - root执行时，无需验证口令
- 命令格式
  - 用法1：su [-] [目标用户]
  - 用法2：su [-] -c "命令" [目标用户]

su操作示例

Tedu.cn 达内教育

知识讲解

- 从普通用户切换为root，并登录新Shell环境
  - 执行 su - ，或者 su - root
  - 不指名目标用户时，默认视为root

```
[zengye@svr7 ~]$ whoami
zengye
[zengye@svr7 ~]$ su  -
密码：                          //验证root用户的口令
[root@svr7 ~]# whoami
root
```

su操作示例（续1）

知识讲解

- root以指定的普通用户身份执行任务
  - 以用户tom的身份创建目录
  - 以用户tom的身份执行管理员操作会出错

```
[root@svr7 ~]# su - tom  -c "mkdir /home/tom/test  "

[root@svr7 ~]# su - nb -c "systemctl restart sshd"
Error creating textual authentication agent
```

分析su切换的使用情况

知识讲解

- 安全日志/var/log/secure
  - 记录su验证、Shell开启与关闭

```
[root@svr7 ~]# tail  /var/log/secure
.. ..
Jul 29 15:11:05 svr7 su: pam_unix(su-l:session): session opened
for user root by zengye(uid=500)
Jul 29 15:11:09 svr7 su: pam_unix(su-l:session): session closed for
user root
```

su切换登入成功

su会话断开成功

sudo提升执行权限

sudo提权的基本用法

知识讲解

- Super or another Do，超级执行
  - 管理员预先为用户设置执行许可
  - 被授权用户有权执行授权的命令，验证自己的口令
- 命令格式
  - 用法1：sudo 特权命令
  - 用法2：sudo [-u 目标用户] 特权命令

sudo操作示例

知识讲解

- 查看自己的sudo授权
  - sudo -l
- 以用户zengye的权限新建一个文件夹
  - sudo -u zengye mkdir /tmp/mydir

```
[root@svr7 ~]# sudo -u zengye mkdir /tmp/mdir
[root@svr7 ~]# ls -ld /tmp/mydir/
drwxr-xr-x. 2 zengye zengye 4096 7月  29 15:31 /tmp/mdir/
```

配置sudo授权

知识讲解

- 修改方法
  - 推荐：visudo
  - 其他：vim /etc/sudoers
- 授权记录格式
  - 用户 主机列表=命令列表

```
[root@svr7 ~]# grep ^root /etc/sudoers
root            ALL=(ALL)       ALL
```

可以是 %组名

目标身份，省略时表示root

配置sudo授权（续1）

Tedu.cn 达内教育

知识讲解

- 示例1
  - 允许mike以root权限执行/sbin/下的所有命令
  - 但是，禁止修改eth0网卡的参数

```
[root@svr7 ~]# visudo
.. ..
mike    localhost,svr1=/sbin/*, !/sbin/ifconfig  eth0
```

配置sudo授权（续2）

Tedu.cn 达内教育

知识讲解

- 示例2
  - wheel组的用户无需验证可执行所有命令

```
[root@svr7 ~]# visudo
.. ..
%wheel      ALL=(ALL)      NOPASSWD: ALL
```

分析sudo提权的使用情况

Tedu.cn 达内教育

知识讲解

- 修改全局配置，启用日志
  - Defaults logfile="/var/log/sudo"

```
[root@svr7 ~]# tail /var/log/sudo
.. ..
Jul 29 16:10:26 : mike : TTY=pts/0 ; PWD=/home/mike ; USER=root ;
   COMMAND=/bin/mkdir /opt/mydata
Jul 29 16:11:02 : mike : TTY=pts/0 ; PWD=/home/mike ; USER=root ;
   COMMAND=/bin/cp /etc/shadow /opt/mydata/
```

sudo别名设置

Tedu.cn 达内教育

知识讲解

- 主要用途
  - 提高可重用性、易读性
  - 简化配置、使记录更有条理

```
[root@svr7 ~]# visudo
.. ..
User_Alias  OPERATORS=jerry,tom,tsengyia
Host_Alias  MAILSERVERS=mail,smtp,pop,svr7
Cmnd_Alias  SOFTMGR=/bin/rpm,/usr/bin/yum
OPERATORS   MAILSERVERS=SOFTMGR
```

别名的名称必须全大写

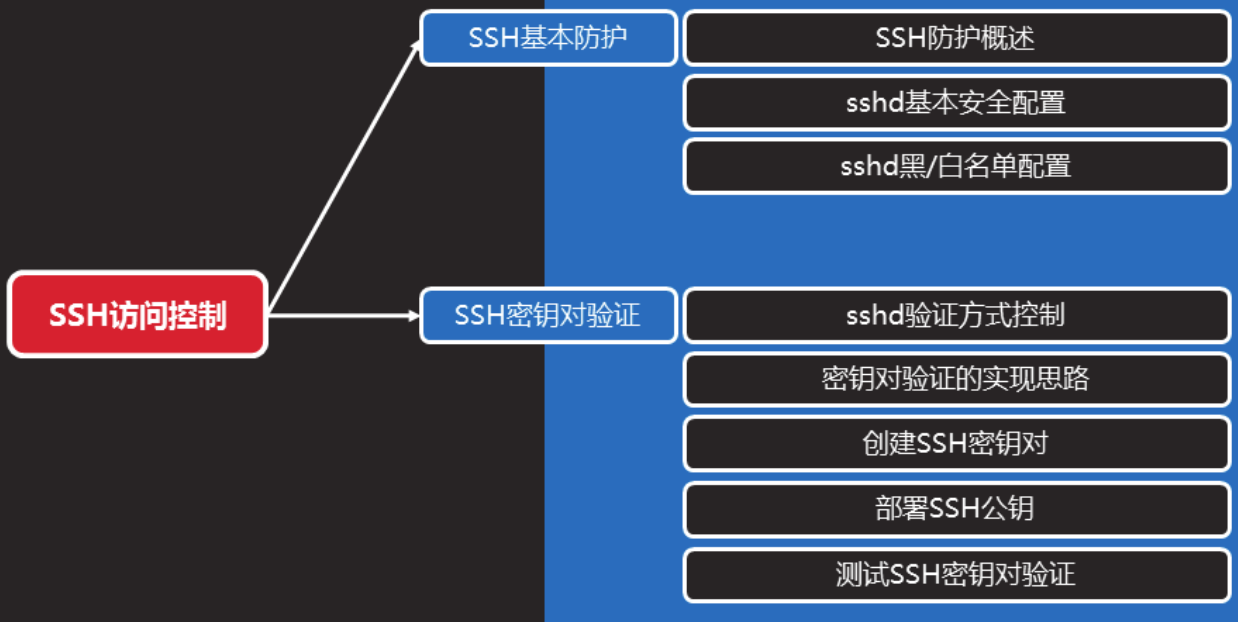
案例2：使用sudo分配管理权限

Tedu.cn 达内教育

课堂练习

1.使用su命令临时切换账户身份，并执行命令
2.允许softadm管理系统服务的权限
3.允许用户useradm管理本地账号（root除外）
4.允许wheel组成员以特权执行/usr/bin/下的命令
5.启用sudo日志以便跟踪

SSH访问控制



SSH基本防护

SSH防护概述

知识讲解

- 存在的安全隐患
  - 密码嗅探、键盘记录
  - 暴力枚举账号、猜解密码
- 常见的防护措施
  - 用户限制、黑白名单
  - 更改验证方式（密码-->密钥对）
  - 防火墙.. ..

sshd基本安全配置

知识讲解

- 配置文件 /etc/ssh/sshd_config
  - Port 3389 //改用非标准端口
  - Protocol 2 //启用SSH V2版协议
  - ListenAddress 192.168.168.174
  - PermitRootLogin no //禁止root登录

sshd基本安全配置（续1）

知识讲解

- 配置文件 /etc/ssh/sshd_config
  - UseDNS no //不解析客户机地址
  - LoginGraceTime 1m //登录限时
  - MaxAuthTries 3 //每连接最多认证次数

sshd黑/白名单配置

知识讲解

- 配置文件 /etc/ssh/sshd_config
  - DenyUsers USER1 USER2 ...
  - AllowUsers USER1@HOST USER2 ...
  - DenyGroups GROUP1 GROUP2 ...
  - AllowGroups GROUP1 GROUP2 ...

sshd黑/白名单配置（续1）

知识讲解

- 应用示例
  - 仅允许一部分用户（从指定地点）登入
  - 其他任何用户均禁止登入

```
[root@svr7 ~]# vim /etc/ssh/sshd_config
.. ..
AllowUsers zengye@192.168.0.*,192.168.4.110
AllowUsers tradm tom jerry

[root@svr7 ~]# service sshd reload
```

SSH密钥对验证

sshd验证方式控制

知识讲解

- 口令验证
  - 检查登录用户的口令是否一致
- 密钥验证
  - 检查客户端私钥与服务器上的公钥是否匹配

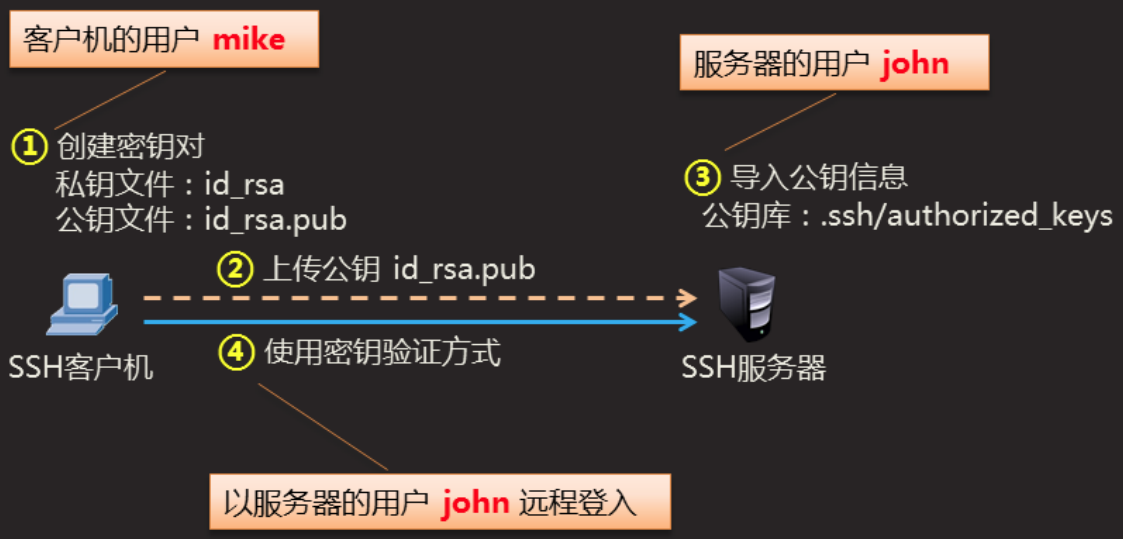
```
PasswordAuthentication   yes
.. ..
PubkeyAuthentication   yes
AuthorizedKeysFile   .ssh/authorized_keys
```

公钥库：存放授权客户机的公钥文本

密钥对验证的实现思路

Tedu.cn 达内教育

知识讲解



创建SSH密钥对

Tedu.cn 达内教育

知识讲解

- 使用工具 ssh-keygen
  - 可以手动指定加密算法（ -t rsa 或 -t dsa ）
  - 若不指定，默认采用RSA加密

```
[mike@svr7 ~]$ ssh-keygen
Enter passphrase (empty for no passphrase):          //设置私钥口令为空
Enter same passphrase again:
.. ..
[mike@svr7 ~]$ ls  -Al  /home/mike/.ssh/
-rw-------.  1  mike  mike  1743 7月  31 15:32  id_rsa          //私钥文件
-rw-r--r--.  1  mike  mike   391 7月  31 15:32  id_rsa.pub      //公钥文件
```

部署SSH公钥

Tedu.cn 达内教育

知识讲解

- 方法一，通过 ssh-copy-id 自动部署
  - 好处： ② ③ 一步到位
  - 局限性：要求SSH口令认证可用
- 方法二，通过FTP等方式上传、手动添加
  - 好处：灵活、适用范围广
  - 局限性：操作繁琐、易出错

```
[mike@svr7 ~]$ ssh-copy-id  john@192.168.4.7
john@192.168.4.7's password:
Now try .. ..  check in:
    .ssh/authorized_keys
.. ..
```

测试SSH密钥对验证

Tedu.cn 达内教育

知识讲解

- 客户端登录操作
  - 仅限密钥对创建人使用
  - 需验证私钥口令（如果有的话，否则免密码登录）

```
[mike@svr7 ~]$ ssh  john@192.168.4.7

[john@svr7 ~]$ whoami
john
```

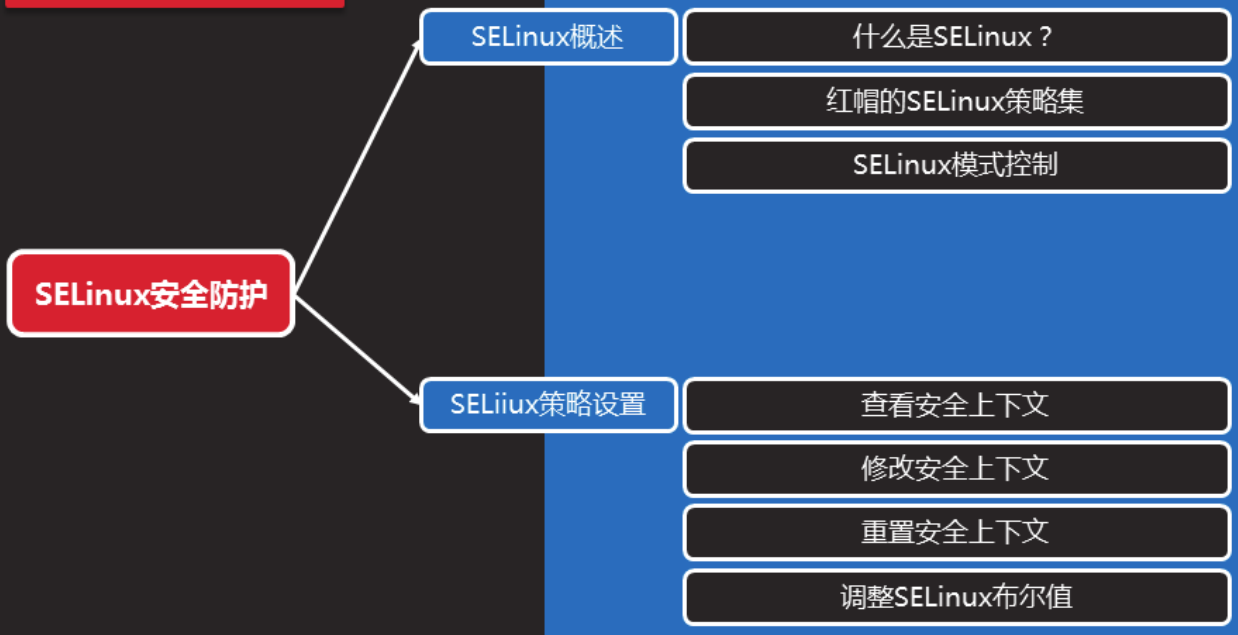
案例3：提高SSH服务安全

Tedu.cn 达内教育

课堂练习

1. 基本安全策略（禁止root、禁止空口令）
2. 为SSH访问配置“仅允许”策略
3. 分别实现密钥验证登入、免密码登入
4. 禁用密码验证

SELinux安全防护



Tedu.cn 达内教育

SELinux概述

Tedu.cn 达内教育

什么是SELinux？

知识讲解

- Security-Enhanced Linux
  - 一套强化Linux安全的扩展模块
  - 美国国家安全局主导开发
- SELinux的运作机制
  - 集成到Linux内核（2.6及以上）
  - 操作系统提供可定制的策略、管理工具

红帽的SELinux策略集

Tedu.cn 达内教育

知识讲解

- SELINUXTYPE=targeted
  - 推荐，仅保护最常见/关键的网络服务，其他不限制
  - 主要软件包：
    selinux-policy、selinux-policy-targeted、
    libselinux-utils、libselinux-utils、
    coreutils、policycoreutils

```
[root@svr7 ~]# sestatus
SELinux status:                 enabled
Current mode:                   enforcing
.. ..
Policy from config file:        targeted
```

SELinux模式控制

Tedu.cn 达内教育

知识讲解

- 方法一，修改kernel启动参数
  - 添加 selinux=0 以禁用
  - 添加 enforcing=0 设置SELinux为允许模式
- 方法二，修改文件/etc/selinux/config
  - 设置 SELINUX=disabled 以禁用
  - 设置 SELINUX=permissive 宽松/允许模式
  - 设置 SELINUX=enforcing 强制模式

SELinux开关控制（续1）

知识讲解

- 临时调整，setenforce 命令
  - 设为 1，对应强制模式
  - 设为 0，对应宽松模式

非Disabled状态下才可可用

```
[root@svr7 ~]# getenforce                //看当前状态
Permissive
[root@svr7 ~]# setenforce  1             //设为强制模式
[root@svr7 ~]# getenforce                //确认结果
Enforcing
```

SELinux策略设置

查看安全上下文

知识讲解

- Security Context，安全上下文
  - 为文件/目录/设备标记访问控制属性
- 属性构成
  - 用户:角色:访问类型:选项...

```
[root@svr7 ~]# ls  -Z  /bin/ls  /etc/fstab
-rwxr-xr-x. root root system_u:object_r:bin_t:s0   /bin/ls
-rw-r--r--. root root system_u:object_r:etc_t:s0   /etc/fstab

[root@svr7 ~]# ls  -dZ  /var/www/html
drwxr-xr-x. root root system_u:object_r:httpd_sys_content_t:s0
/var/www/html
```

修改安全上下文

知识讲解

- 使用 chcon 工具
  - -t，指定访问类型
  - -R，递归修改
- 一般操作规律
  - 移动的文件，原有的上下文属性不变
  - 复制的文件，自动继承目标位置的上下文

修改安全上下文（续1）

知识讲解

- 应用示例：
  - 有一个权限为644的文件，但是FTP无权下载
  - 分析故障原因，并解决此问题

管理员才有权访问

```
[root@svr7 ~]# ls  -Z  /var/ftp/rt.txt
-rw-r--r--. root root system_u:object_r:admin_home_t:s0

[root@svr7 ~]# chcon  -t  public_content_t  /var/ftp/rt.txt
[root@svr7 ~]# wget ftp://192.168.4.5/rt.txt
.. ..
2013-08-02 15:14:19 (94.4 MB/s) -  “rt.txt”  已保存 [45527]
                                          //成功下载
```

重置安全上下文

知识讲解

- 使用 restorecon 工具
  - 恢复为所在位置的默认上下文属性
  - -R，递归修改
- /.autorelabel 文件
  - 下次重启后全部重置

```
[root@svr7 ftp]# ls  -Z  rt.txt
-rw-r--r--. root root system_u:object_r:etc_t:s0       rt.txt
[root@svr7 ftp]# restorecon  rt.txt
[root@svr7 ftp]# ls  -Z  rt.txt
-rw-r--r--. root root system_u:object_r:admin_home_t:s0 rt.txt
```

调整SELinux布尔值

知识讲解

- 使用 getsebool 查看
  - -a，可列出所有布尔值
- 使用 setsebool 设置
  - -P，永久更改，重启后仍然有效

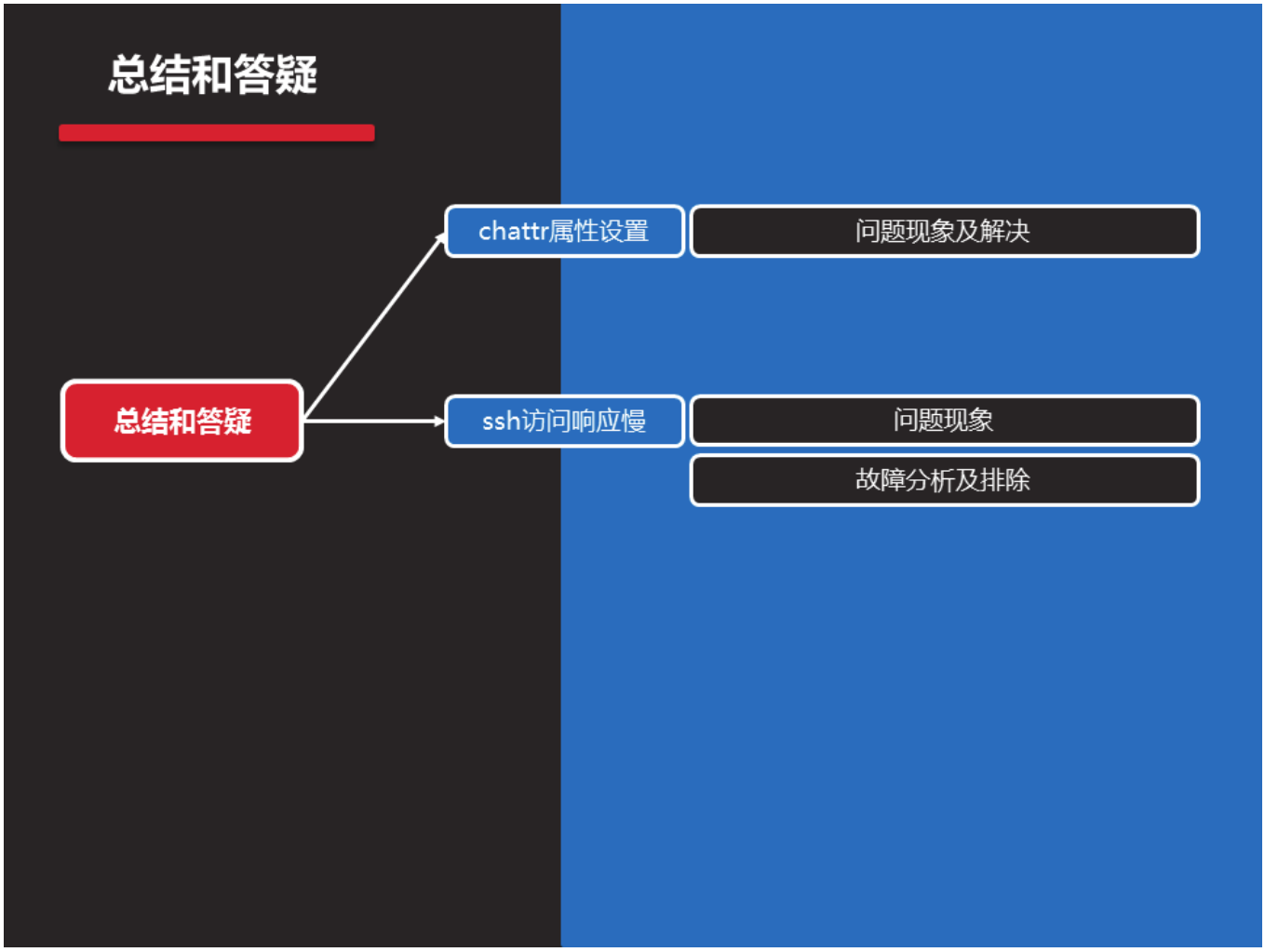
```
[root@svr7 ~]# getsebool   -a
.. ..
allow_httpd_anon_write --> off
allow_httpd_mod_auth_ntlm_winbind --> off
allow_httpd_mod_auth_pam --> off
.. ..
```

案例4：SELinux安全防护

课堂练习

1.将Linux服务器的SELinux设为enforcing强制模式

2.从/root目录下移动一个包文件到FTP下载目录，调整策略使其能够被下载


总结和答疑
总结和答疑
chattr属性设置
问题现象及解决
ssh访问响应慢
问题现象
故障分析及排除


Tedu.cn
达内教育
chattr属性设置

问题现象及解决

知识讲解

- 关于chattr的+a属性
  - 为一个文件设置 +a 属性以后，
  - 无法用vim编辑的方式向文件末尾添加新内容
- 故障分析及排除
  - 原因分析：使用vim修改文件会影响文件属性，这是+a不允许的
  - 解决办法：改用 >> 追加的方式添加新内容

ssh访问响应慢

问题现象

知识讲解

- 客户机设置DNS以后，使用ssh连接远程主机时
  - 在提示输密码之前要等待好久
  - 清空 /etc/resolv.conf 设置则没这个问题

故障分析及排除

知识讲解

- 原因分析
  - sshd服务端会尝试查找客户端的主机名
  - ssh客户端的GSS认证会尝试查找服务端的主机名
- 解决办法
  - 服务端启用 UseDNS no，或者添加hosts映射
  - 客户端启用 GSSAPIAuthentication no，或者添加hosts映射

故障分析及排除（续1）

Tedu.cn 达内教育

知识讲解

- 服务端

```
[root@svr7 ~]# vim  /etc/ssh/sshd_config
.. ..
UseDNS  no
```

- 客户端

```
[root@pc207 ~]# vim  /etc/ssh/ssh_config
.. ..
Host *
#       GSSAPIAuthentication yes                    //注释此行
```