

ENGINEER DAY07



云计算应用管理

NSD ENGINEER

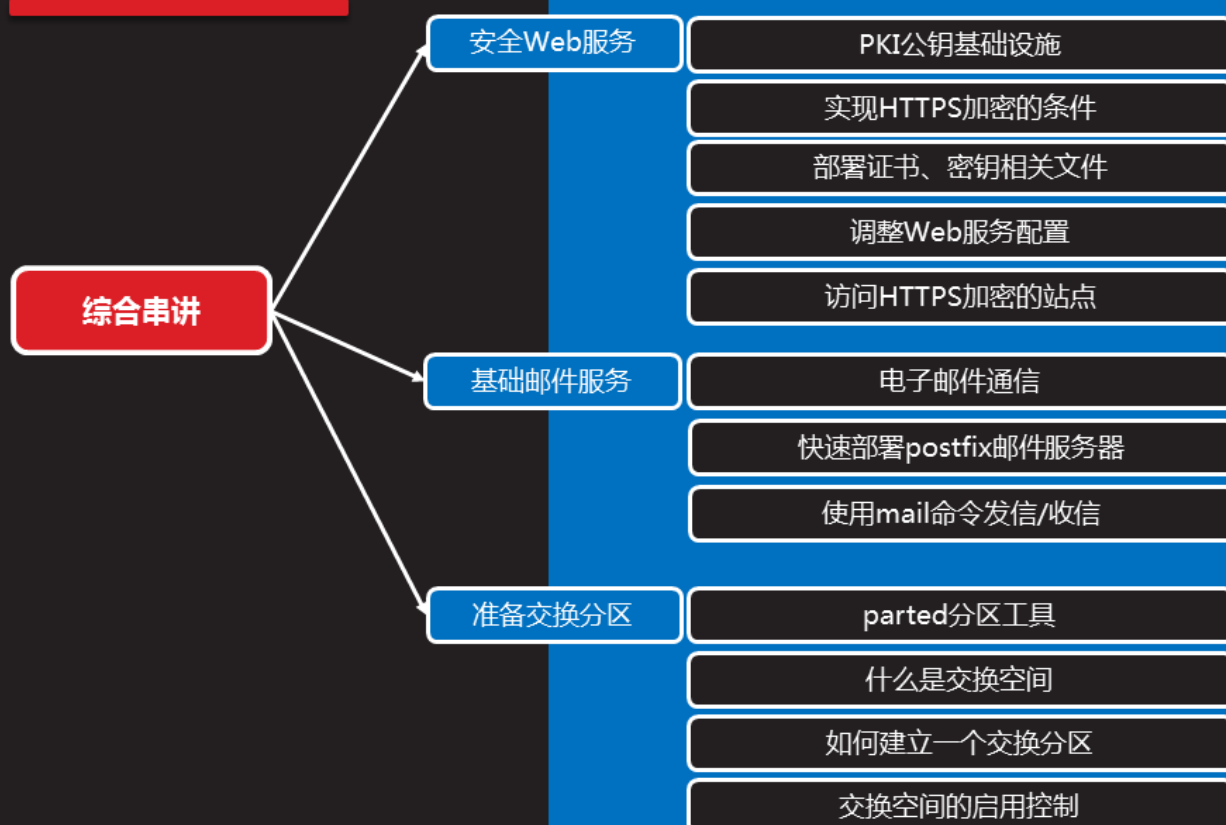
DAY07

内容

| | | |
|----|---------------|---------|
| 上午 | 09:00 ~ 09:30 | 作业讲解和回顾 |
| | 09:30 ~ 10:20 | 综合串讲 |
| | 10:30 ~ 11:20 | |
| | 11:30 ~ 12:00 | |
| 下午 | 14:00 ~ 14:50 | 综合练习 |
| | 15:00 ~ 15:50 | |
| | 16:10 ~ 17:00 | |
| | 17:10 ~ 18:00 | 总结和答疑 |



综合串讲



安全Web服务

PKI公钥基础设施

知识讲解

- **P**ublic **K**ey **I**nfrastructure , 公钥基础设施
 - 公钥：主要用来加密数据
 - 私钥：主要用来解密数据（与相应的公钥匹配）
 - 数字证书：证明拥有者的合法性/权威性（单位名称、有效期、公钥、颁发机构及签名、.....）
 - **C**ertificate **A**uthority , 数字证书授权中心：负责证书的申请/审核/颁发/鉴定/撤销等管理工作



实现HTTPS加密的条件

知识讲解

- HTTPS 加密Web通信 (TCP 443端口)
 - Secure Sockets Layer , 安全套接字层
 - Transport Layer Security , 安全传输层协议
- 实现条件
 - 启用 SSL 模块支持
 - 部署好加密素材：网站服务器的数字证书、网站服务器的私钥、根证书 (CA管理机构的证书)

```
[root@server0 ~]# yum -y install mod_ssl
[root@server0 ~]# ls /etc/httpd/conf.d/ssl.conf
/etc/httpd/conf.d/ssl.conf
```



部署证书、密钥相关文件

知识讲解

- 证书、密钥文件的部署路径
 - /etc/pki/tls/certs/证书文件.crt
 - /etc/pki/tls/private/私钥文件.key
- ```
[root@server0 ~]# cd /etc/pki/tls/certs/
[root@server0 certs]# wget http://classroom/pub/example-ca.crt
[root@server0 certs]# wget
http://classroom/pub/tls/certs/server0.crt
.. ..
[root@server0 certs]# cd /etc/pki/tls/private/
[root@server0 private]# wget
http://classroom/pub/tls/private/server0.key
.. ..
```



## 调整Web服务配置

- 配置要点

- 指定 SSL 虚拟站点的DNS名称、网页根目录
- 指定站点证书/根证书/站点密钥的位置

```
[root@server0 ~]# vim /etc/httpd/conf.d/ssl.conf
<VirtualHost _default_:443>
 DocumentRoot "/var/www/html"
 ServerName server0.example.com:443

 ..
 SSLCertificateFile /etc/pki/tls/certs/server0.crt
 SSLCertificateKeyFile /etc/pki/tls/private/server0key
 SSLCACertificateFile /etc/pki/tls/certs/example-ca.crt
</VirtualHost>
```

```
[root@server0 ~]# systemctl restart httpd
```

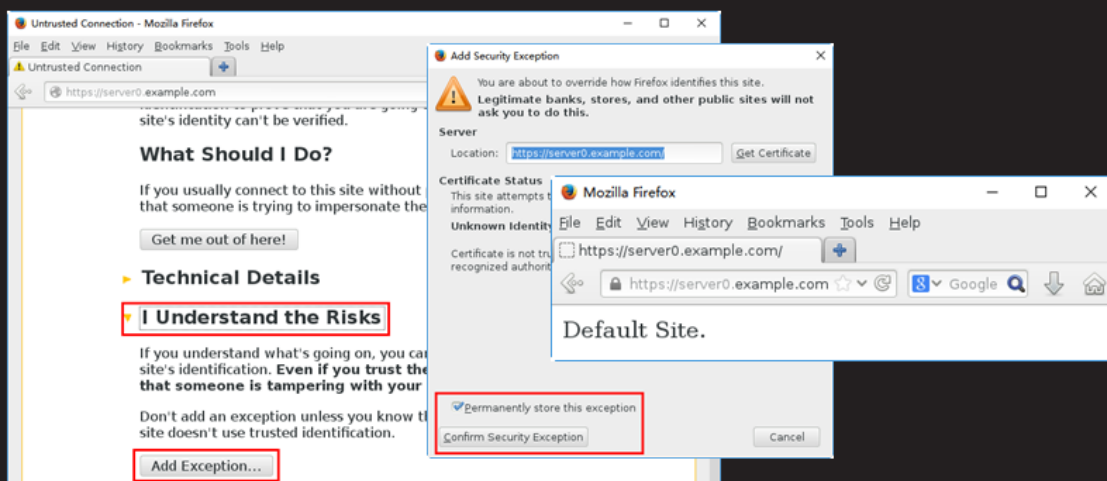
知识讲解



## 访问HTTPS加密的站点

- 对比 HTTP 与 HTTPS 访问效果
  - <http://server0.example.com/>
  - <https://server0.example.com/>

知识讲解



## 案例1：配置安全Web服务

为站点 <http://server0.example.com> 配置TLS加密

1) 一个已签名证书从以下地址获取

<http://classroom/pub/tls/certs/server0.crt>

2) 此证书的密钥从以下地址获取

<http://classroom/pub/tls/private/server0.key>

3) 此证书的签名授权信息从以下地址获取

<http://classroom/pub/example-ca.crt>

课堂  
练习



## 基础邮件服务

# 电子邮件通信

知识讲解

- 电子邮件服务器的基本功能
  - 为用户提供电子邮箱存储空间（用户名@邮件域名）
  - 处理用户发出的邮件 —— 传递给收件服务器
  - 处理用户收到的邮件 —— 投递到邮箱

管辖的邮箱区域（DNS后缀）：sina.com  
 邮箱账号：zhsan、lisi、.....  
 电子邮箱地址：zhsan@sina.com、lisi@sina.com



## 快速部署postfix邮件服务器

知识讲解

- 装包、配置、起服务
  - 默认的标准配置即可为本机提供发/收邮件服务
  - 若有必要，可扩大服务范围（邮件域）

```
[root@server0 ~]# vim /etc/postfix/main.cf
```

```
.. ..
```

```
inet_interfaces = all //监听接口
mydomain = example.com //邮件域
myhostname = example.com //本服务器主机名
```

```
[root@server0 ~]# systemctl restart postfix
```

```
[root@server0 ~]# netstat -antpu | grep :25
```

```
tcp 0 0 0.0.0.0:25 0.0.0.0:* LISTEN 3270/master
```



# 使用mail命令发信/收信

## 知识讲解

- mail 发信操作
  - mail -s '邮件标题' 收件人[@收件域]...
- mail 收信操作
  - mail [-u 用户名]

```
[root@server0 ~]# echo '1111' | mail -s 'mail1' root //发信
[root@server0 ~]# mail -u root //收信
Heirloom Mail version 12.5 7/5/10. Type ? for help.
"/var/mail/root": 1 message 1 new
>N 1 root Mon Nov 21 18:36 18/530 "mail"
& 1 //读取第1封邮件内容
...
& q //退出mail工具
Held 1 message in /var/mail/root
```



## 案例2：postfix基础邮件服务

## 课堂练习

1. 配置 server0 的 postfix 基础服务
  - 1) 监听本机的所有接口
  - 2) 将邮件域和邮件服务主机名都改为 example.com
2. 在 server0 上使用 mail 命令测试发信/收信操作
  - 1) 由 root 给本机用户 mike 发一封测试邮件
  - 2) 查收用户 mike 的邮箱，读取邮件内容，确保是从 root@example.com 发过来的





# 准备交换分区



## parted分区工具

- 使用fdisk操作>2.2TB的磁盘时
  - 超出容量的磁盘将会无法识别，导致分区失效
  - 如何处理大容量的磁盘？

知识讲解



## parted分区工具 (续1)

知识讲解

- 原因分析
  - 主要受限于 msdos 分区模式
  - 要支持大容量, 需改用 gpt 分区模式 (只有primary 分区, 可超过4个)
- 解决办法
  - 使用 gdisk 分区工具, 用法与 fdisk 类似
  - 使用 parted 分区工具 ——  
**mktable gpt 重建分区表**  
**mkpart primary 文件系统类型 起始位置 结束位置**



## 什么是交换空间

知识讲解

- 相当于虚拟内存,
  - 当物理内存不够用时, 使用磁盘空间来模拟内存
  - 在一定程度上缓解内存不足的问题
  - **交换分区**: 以空闲分区充当的交换空间
  - **交换文件**: 以文件模拟的设备充当的交换空间



# 如何建立一个交换分区

- 将提供的设备按 swap 类型进行格式化
  - mkswap 空闲分区或文件设备

知识讲解

```
[root@server0 ~]# mkswap /dev/vdb7 //格式化交换分区
Setting up swspace version 1, size = 524284 KiB
no label, UUID=26b95ed8-e648-4d30-bea3-de48494bbdfe
```

```
[root@server0 ~]# blkid /dev/vdb7 //查看块设备ID
/dev/vdb7: UUID="26b95ed8-e648-4d30-bea3-de48494bbdfe"
TYPE="swap"
```



# 交换空间的启用控制

- 手动管理操作
  - swapon 交换设备
  - swapon -s
  - swapoff 交换设备

知识讲解

```
[root@server0 ~]# swapon /dev/vdb7 //启用
[root@server0 ~]# swapon -s //查看
Filename Type Size Used Priority
/dev/vdb7 partition 524284 0 -1
```

```
[root@server0 ~]# swapoff /dev/vdb7 //停用
[root@server0 ~]# swapon -s //再次查看
[root@server0 ~]#
```



## 交换空间的启用控制（续1）

- 修改 /etc/fstab 配置文件

– 交换设备 swap swap defaults 0 0

```
[root@server0 ~]# vim /etc/fstab
```

```
.. ..
```

```
/dev/vdb7 swap swap defaults 0 0
```

```
[root@server0 ~]# swapon -a
```

//启动fstab可用交换设备

```
[root@server0 ~]# swapon -s
```

//查看

| Filename  | Type      | Size   | Used | Priority |
|-----------|-----------|--------|------|----------|
| /dev/vdb7 | partition | 524284 |      | -1       |

知识讲解



## 案例3：添加一个swap分区

为虚拟机 server0 添加一个交换分区

- 1) 此交换分区的大小为 512MiB
- 2) 当系统启动时，swap分区应该可以自动挂载
- 3) 不要移除或更改其他已经存在于你系统中的交换分区

课堂练习



## 综合练习



# Linux工程师测试

## 环境准备及说明

知识讲解

- 依次重置教学虚拟机 classroom、server

```
[root@room9pc13 ~]# rht-vmctl reset classroom
```

```
[root@room9pc13 ~]# rht-vmctl reset server
```

```
[root@room9pc13 ~]# rht-vmctl reset desktop
```

- !! 注意：所有练习操作在虚拟机 **server0**、**desktop** 上进行



## 案例4：Linux工程师 综合测试

课堂练习

**机试及评测**



# 总结和答疑

