Tedu.cn
达内教育

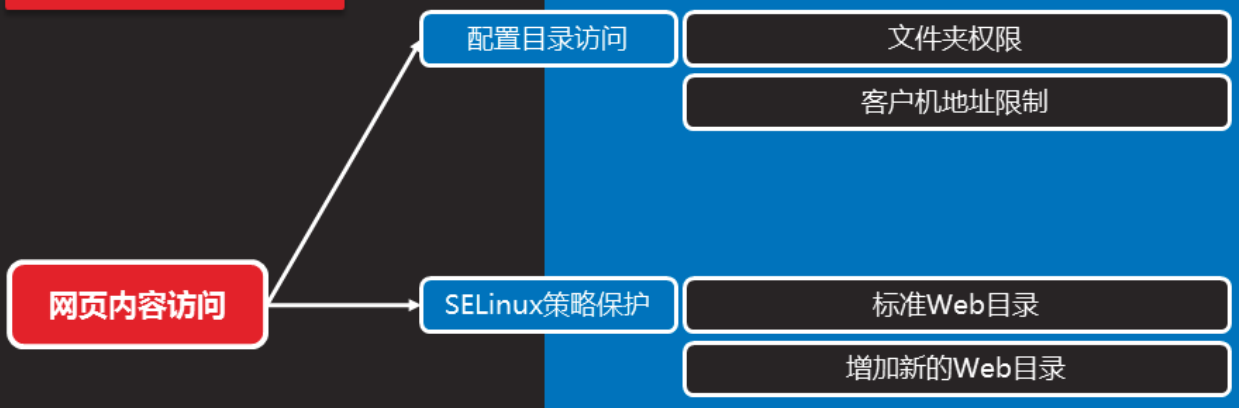
云计算应用管理

NSD ENGINEER DAY05

内容

上午	09:00 ~ 09:30	作业讲解和回顾
	09:30 ~ 10:20	网页内容访问
	10:30 ~ 11:20	
	11:30 ~ 12:00	部署动态网站
下午	14:00 ~ 14:50	
	15:00 ~ 15:50	安全Web服务
	16:10 ~ 17:00	
	17:10 ~ 18:00	总结和答疑

网页内容访问



Tedu.cn 达内教育

配置目录访问

Tedu.cn 达内教育

文件夹权限

- 针对 DocumentRoot 网页目录的权限控制
  - httpd 运行身份（用户/组）：apache
  - 能提取哪些网页资源

知识讲解

```
[root@server0 ~]# vim  /etc/httpd/conf/httpd.conf
User  apache
Group  apache
.. ..
[root@server0 ~]# ls  -ld  /var/www/*
.. ..
drwxr-xr-x. 2 root  root 23 Nov 23 23:21  /var/www/html
drwxr-xr-x. 2 root  root  6  Nov 23 23:50  /var/www/virtual
```

客户机地址限制

Tedu.cn 达内教育

知识讲解

- 使用 <Directory> 配置区段
  - 每个文件夹自动继承其父目录的ACL访问权限
  - 除非针对子目录有明确设置

```
<Directory  目录的绝对路径>
    .. ..
    Require  all  denied|granted
    Require  ip  IP或网段地址 .. ..
</Directory>
```

客户机地址限制（续1）

Tedu.cn 达内教育

知识讲解

- 禁止任何客户机访问

```
<Directory  />
    Require  all  denied
</Directory>
```

- 允许任何客户机访问

```
<Directory  "/var/www/html">
    Require  all  granted
</Directory>
```

- 仅允许部分客户机访问

```
<Directory  "/var/www/html/private">
    Require  ip  127.0.0.1  ::1  172.25.0.11
</Directory>
```

案例1：配置网页内容访问

课堂练习

在 Web 网站 http://server0.example.com 的 DocumentRoot 目录下创建一个名为 private 的子目录，要求如下：

1）从 http://classroom/pub/materials/private.html 下载一个文件副本到这个目录，重命名为 index.html

2）不要对文件 index.html 的内容作任何修改

3）从 server0 上，任何人都可以浏览 private 的内容，但是从其他系统不能访问这个目录的内容

SELinux策略保护

标准Web目录

知识讲解

- 使用 semanage 工具可查看

```
[root@server0 ~]# semanage fcontext -l | grep httpd_sys_content
/srv/([^/]*/)?www(/.*)?                    .. ..
/var/www(/.*)?                             .. ..
.. ..
```

- 新建标准Web目录时的初始化

```
[root@server0 ~]# mkdir -p /srv/vhost1/www
[root@server0 ~]# restorecon -R /srv/vhost1/www/
[root@server0 ~]# ls -Zd /srv/vhost1/www/
drwxr-xr-x. root root
unconfined_u:object_r:httpd_sys_content_t:s0 /srv/vhost1/www/
```

增加新的Web目录

知识讲解

- 方式1：参照标准目录，重设新目录的属性
  - chcon [-R] --reference=模板目录 新目录
- 方式2：将新目录增加到预设的标准Web目录范围
  - semanage fcontext -a -t httpd_sys_content_t '新目录(/.*)?'

```
[root@server0 ~]# semanage fcontext -a -t httpd_sys_content_t
'/webroot(/.*)?'

[root@server0 ~]# mkdir -p /webroot/
[root@server0 ~]# restorecon -R /webroot/
```

案例2：使用自定Web根目录

课堂练习

调整 Web 站点 http://server0.example.com 的网页目录，要求如下：

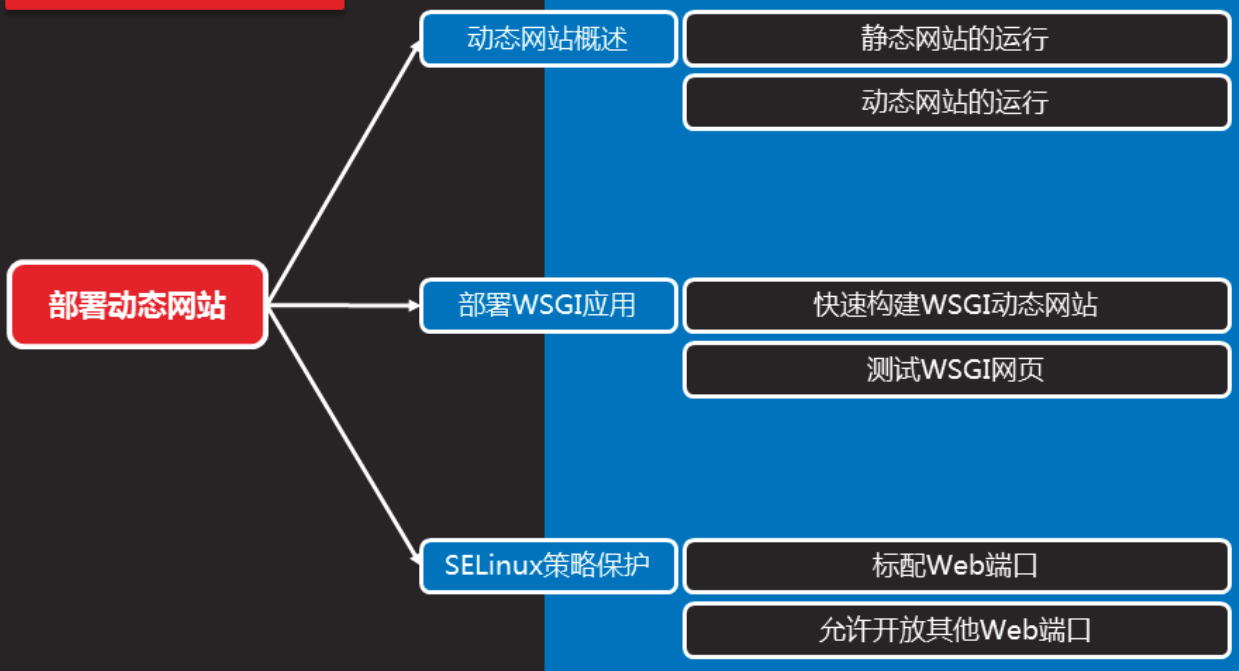
1）新建目录 /webroot，作为此站点新的网页目录

2）从 http://classroom/pub/materials/station.html 下载一个文件副本到这个目录，重命名为 index.html

3）不要对文件 index.html 的内容作任何修改

4）确保站点 http://server0.example.com 仍然可访问

部署动态网站



Tedu.cn 达内教育

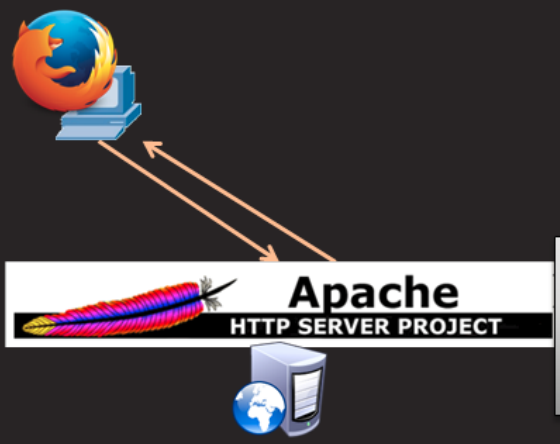
动态网站概述

Tedu.cn 达内教育

静态网站的运行

- 服务端的原始网页 = 浏览器访问到的网页
  - 由Web服务软件处理所有请求
  - 文本（txt/html）、图片（jpg/png）等静态资源

知识讲解



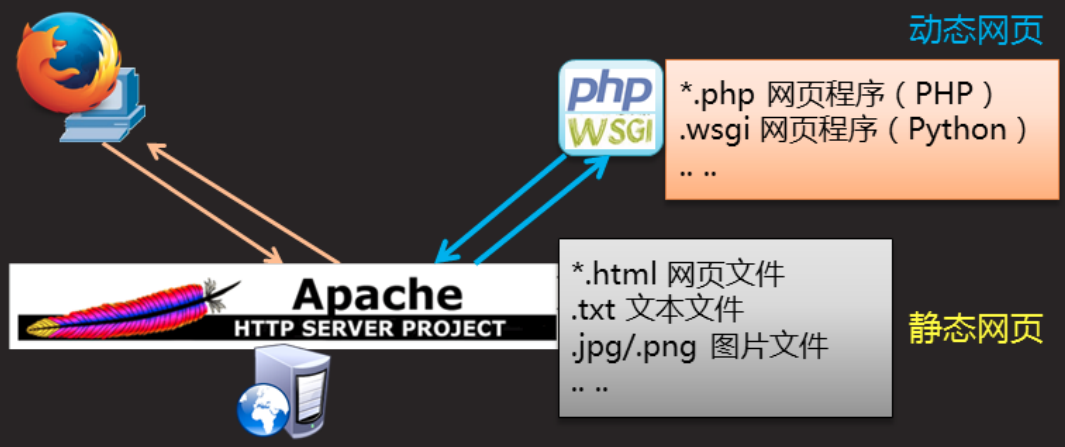
*.html 网页文件
.txt 文本文件
.jpg/.png 图片文件
.. ..

静态网页

动态网站的运行

- 服务端的原始网页 ≠ 浏览器访问到的网页
  - 由Web服务软件接受请求，动态程序转后端模块处理
  - PHP网页、Python网页、JSP网页.....

知识讲解



部署WSGI环境

快速构建WSGI动态网站

Tedu.cn 达内教育

知识讲解

1. 装包（httpd、mod_wsgi）
2. 配置（部署测试页 webinfo.wsgi 、调整首页跳转）
3. 起服务（httpd）

```
[root@server0 ~]# yum  -y  install  httpd  mod_wsgi
.. ..
[root@server0 ~]# cd  /var/www/webapp0/
[root@server0 webapp0]# wget
http://classroom/pub/materials/webinfo.wsgi
```

快速构建WSGI动态网站（续1）

Tedu.cn 达内教育

知识讲解

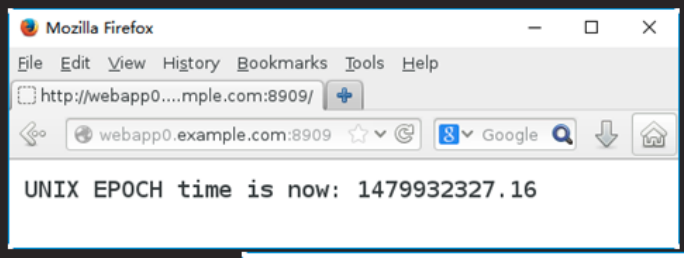
- 新建一个动态站点（虚拟主机）
  - 站点名称为 webapp0.example.com
  - 监听端口为 8909

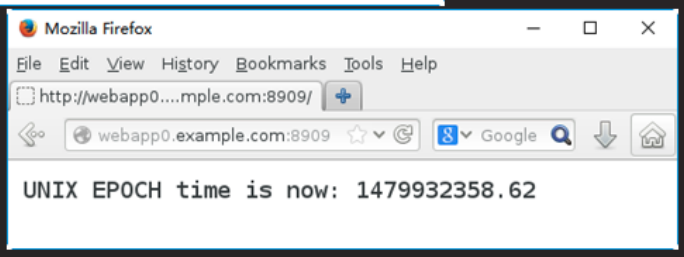
```
[root@server0 ~]# vim  /etc/httpd/conf.d/02-webapp0.conf
Listen 8909
<VirtualHost *:8909>
        ServerName  webapp0.example.com
        DocumentRoot  /var/www/webapp0
        WSGIScriptAlias      /    /var/www/webapp0/webinfo.wsgi
</VirtualHost>

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

测试WSGI网页

- 每次访问此动态站点，页面内容会变化

知识讲解





SELinux策略保护

标配Web端口

知识讲解

- 使用 semanage 工具可查看

```
[root@server0 ~]# semanage  port  -l  |  grep  http_port
http_port_t     tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
.. ..
```

- 当尝试监听非标配端口时，SELinux会阻止
  - 导致 httpd 服务启动失败
  - 查看 /var/log/messages 文件中会有记录

允许开放其他Web端口

知识讲解

- 使用 semanage 工具调整
  - 向现有的服务端口范围中增加新的端口
  - 此操作需足够内存/交换空间支持

```
[root@server0 ~]# semanage  port  -a  -t  http_port_t  -p tcp  8909
.. ..
[root@server0 ~]# semanage  port  -l  |  grep  http_port    //确认结果
http_port_t     tcp      8909,80, 81, 443, 488, 8008, 8009, 8443, 9000
.. ..
```

案例3：部署并测试WSGI站点

课堂练习

为站点 webapp0.example.com 配置提供动态Web内容，要求如下：

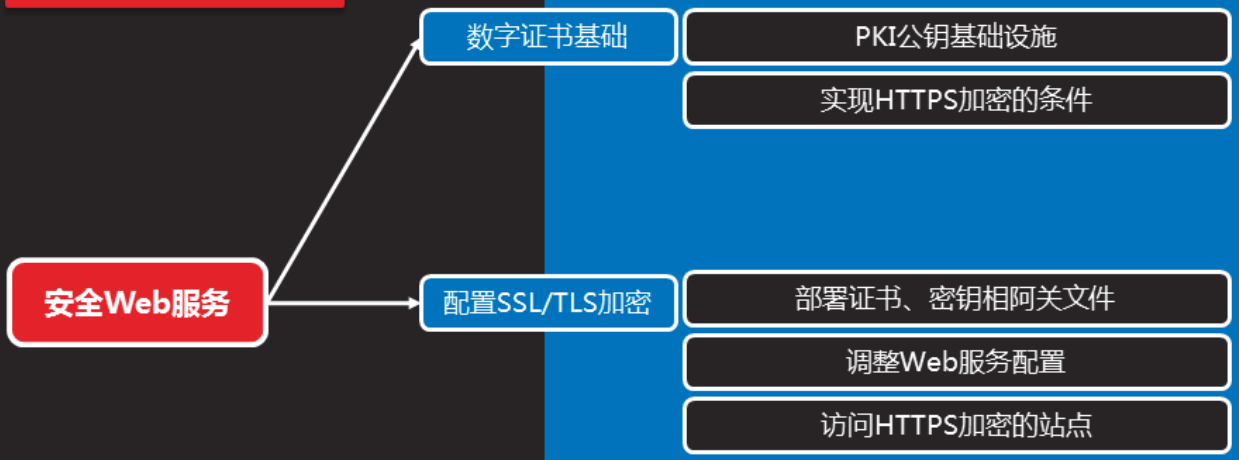
1）此虚拟主机侦听在端口8909

2）测试网页从以下地址下载，不要作任何更改
http://classroom/pub/materials/webinfo.wsgi

3）从浏览器访问 http://webapp0.example.com:8909 可接收到动态生成的 Web 页面

4）此站点必须能被 example.com 域内的所有系统访问

安全Web服务



Tedu.cn 达内教育

数字证书基础

Tedu.cn 达内教育

PKI公钥基础设施

知识讲解

- Public Key Infrastructure，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、……）
  - Certificate Authority，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
```

配置SSL/TLS加密

部署证书、密钥相关文件

Tedu.cn 达内教育

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

Tedu.cn 达内教育

知识讲解

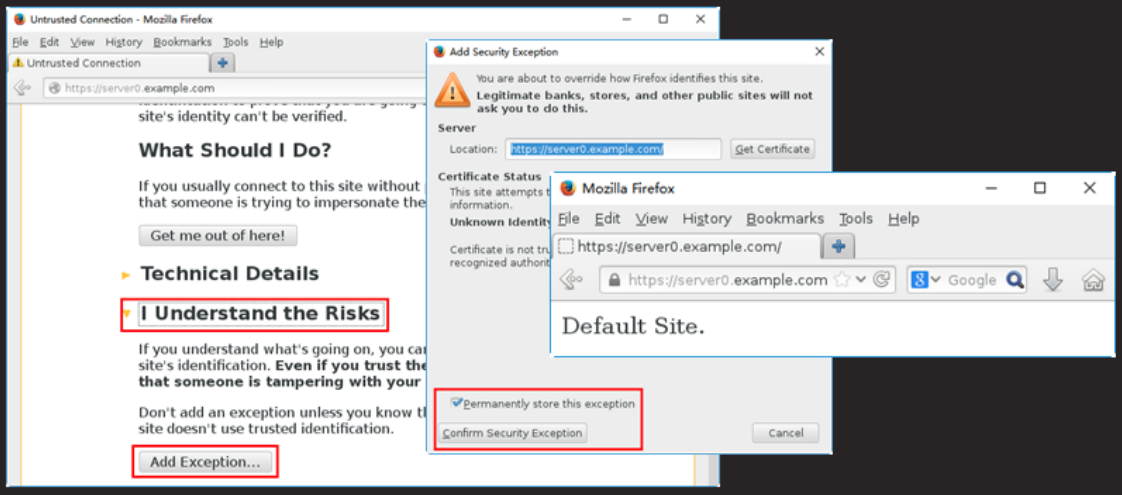
- 配置要点
  - 指定 SSL 虚拟站点的DNS名称、网页根目录
  - 指定站点证书/根证书/站点密钥的位置

```
[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
```

访问HTTPS加密的站点

知识讲解

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



案例4：配置安全Web服务

课堂练习

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

总结和答疑

Tedu.cn
达内教育

SELinux策略故障

问题现象

知识讲解

- 配置动态Web站点时，从浏览器访问失败
  - 问题1：访问其他虚拟站点正常，当访问此动态站点时失败，提示：ELinks: Connection refused
  - 问题2：执行 semanage port -a .. .. 操作添加Web端口失败，提示：Killed

```
[root@desktop0 ~]# elinks  -dump
http://webapp0.example.com:8909/
ELinks: Connection refused
```

故障分析及排除

知识讲解

- 原因分析
  - 问题1：httpd成功运行，但并没有启用8909端口
  - 问题2：内存不足，而且交换空间也不足
- 解决办法
  - 问题1：确认添加 Listen 8909 配置行
  - 问题2：添加一个交换分区（1GB左右）再重试