

云计算应用管理

NSD ENGINEER

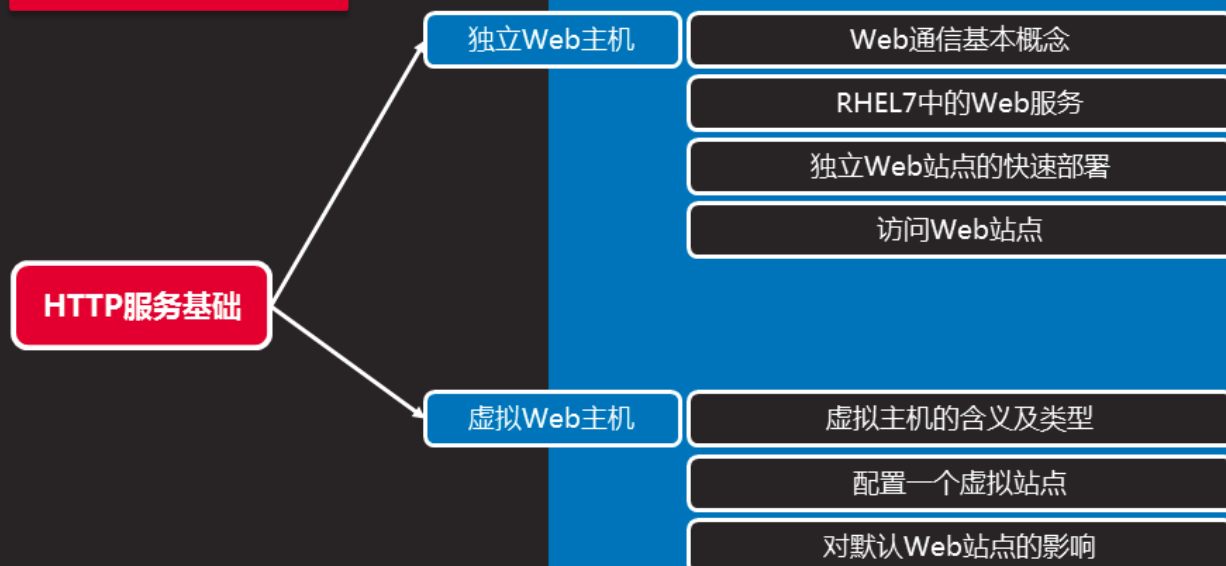
DAY06

内容

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



HTTP服务基础



独立Web主机

Web通信基本概念

知识讲解

- 基于 B/S (Browser/Server) 架构的网页服务
 - 服务端提供网页
 - 浏览器下载并显示网页
- Hyper Text Markup Language , 超文本标记语言
- Hyper Text Transfer Protocol , 超文本传输协议



RHEL7中的Web服务

知识讲解

- 软件包：httpd
- 系统服务：httpd
- 提供的默认配置
 - Listen：监听地址:端口（80）
 - ServerName：本站点注册的DNS名称（空缺）
 - DocumentRoot：网页根目录（/var/www/html）
 - DirectoryIndex：起始页/首页文件名（index.html）



独立Web站点的快速部署

知识讲解

1. 装包（httpd）
2. 配置（部署首页 index.html）
3. 起服务（httpd）

```
[root@server0 ~]# yum -y install httpd
.. ..
[root@server0 ~]# cd /var/www/html/
[root@server0 ~]# wget
http://classroom/pub/materials/station.html -O index.html
.. ..
[root@server0 ~]# systemctl restart httpd
```



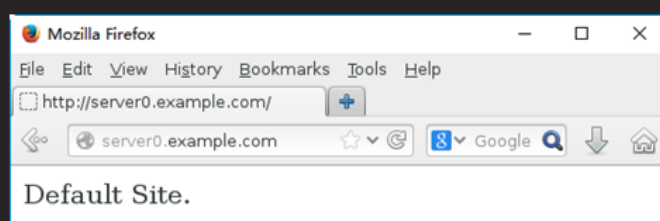
访问Web站点

知识讲解

- 为浏览器程序提供 URL 网址
 - Uniform Resource Locator , 统一资源定位器
 - 协议名://服务器地址[:端口号]/目录/文件名

```
[root@server0 ~]# elinks -dump http://server0.example.com/  
Default Site.
```

```
[root@server0 ~]# firefox http://server0.example.com/  
.. ..
```



案例1：独立Web站点的快速部署

课堂练习

1. 为 <http://server0.example.com> 配置Web站点
 - 1) 从 <http://classroom/pub/materials/station.html> 下载一个主页文件，将其重命名为 index.html
 - 2) 将此文件拷贝到站点的 DocumentRoot 目录下，不要对文件 index.html 的内容作任何修改
2. 访问此Web站点
 - 1) 使用 elinks 浏览上述Web站点
 - 2) 使用 firefox 浏览上述Web站点



虚拟Web主机

虚拟主机的含义及类型

- 虚拟Web主机
 - 由同一台服务器提供多个不同的Web站点
- 区分方式
 - 基于域名的虚拟主机
 - 基于端口的虚拟主机
 - 基于IP地址的虚拟主机

知识讲解

`http://server0.example.com/`
`http://www0.example.com/`
`http://webapp0.example.com/`
.. ..



配置一个虚拟站点

知识讲解

- 配置文件路径
 - /etc/httpd/conf/httpd.conf
 - /etc/httpd/conf.d/*.conf
- 为每个虚拟站点添加配置

```
<VirtualHost IP地址:端口>
    ServerName 此站点的DNS名称
    DocumentRoot 此站点的网页根目录
</VirtualHost>

.. ..
```



配置一个虚拟站点（续1）

知识讲解

- 注意事项
 - 为每个站点提前准备好网页目录
- ```
[root@server0 ~]# cd /var/www/virtual/
[root@server0 virtual]# wget
http://classroom/pub/materials/www.html -O index.html

[root@server0 virtual]# vim /etc/httpd/conf.d/01-www0.conf
<VirtualHost *:80>
 ServerName www0.example.com
 DocumentRoot /var/www/virtual
</VirtualHost>

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



## 对默认Web站点的影响

知识讲解

- 一旦启用虚拟Web主机以后
  - 外部的 DocumentRoot、ServerName 会被忽略
  - 第1个虚拟站点被视为默认站点，若客户机请求的URL 不属于任何已知站点，则由第1个站点响应

```
[root@server0 ~]# vim /etc/httpd/conf.d/00-default.conf
<VirtualHost *:80>
 ServerName server0.example.com
 DocumentRoot /var/www/html
</VirtualHost>
```

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

当独立Web服务器升级为虚拟主机服务器后，  
需要为原Web站点建一个虚拟站点



## 案例2：虚拟Web主机的部署

课堂练习

1. 在虚拟机 server0 上扩展Web站点，创建一个新的虚拟主机 <http://www0.example.com>

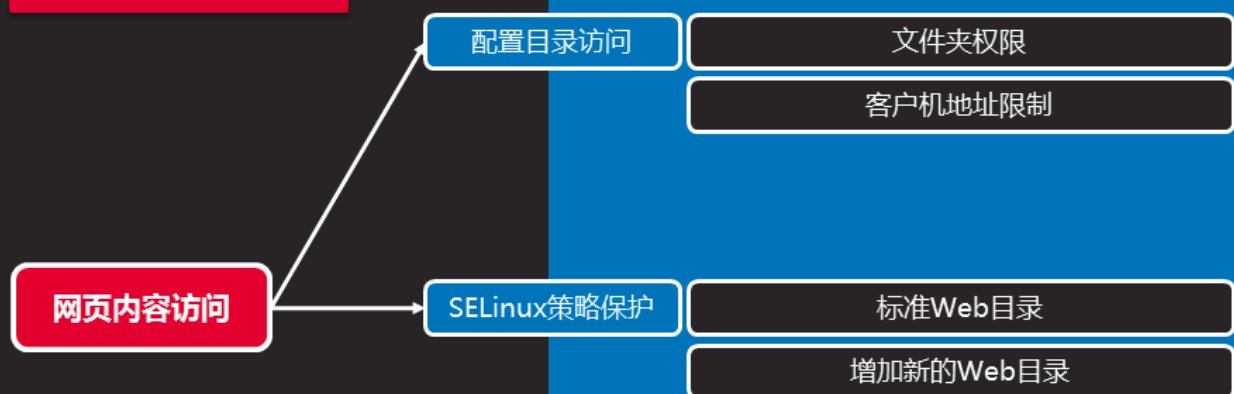
- 1) 设置 DocumentRoot 为 /var/www/virtual
- 2) 从 <http://classroom/pub/materials/www.html> 下载主页文件，并重命名为 index.html
- 3) 不要对文件 index.html 的内容作任何修改，将其放到此虚拟主机的 DocumentRoot 目录下
- 4) 确保 fleyd 用户能在 /var/www/virtual 目录建文件

2. 确保站点 <http://server0.example.com> 仍然可用





## 网页内容访问



## 配置目录访问

## 文件夹权限

知识讲解

- 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

```
[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

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）

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3：配置网页内容访问

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：

课堂练习

- 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

- 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4：使用自定Web根目录

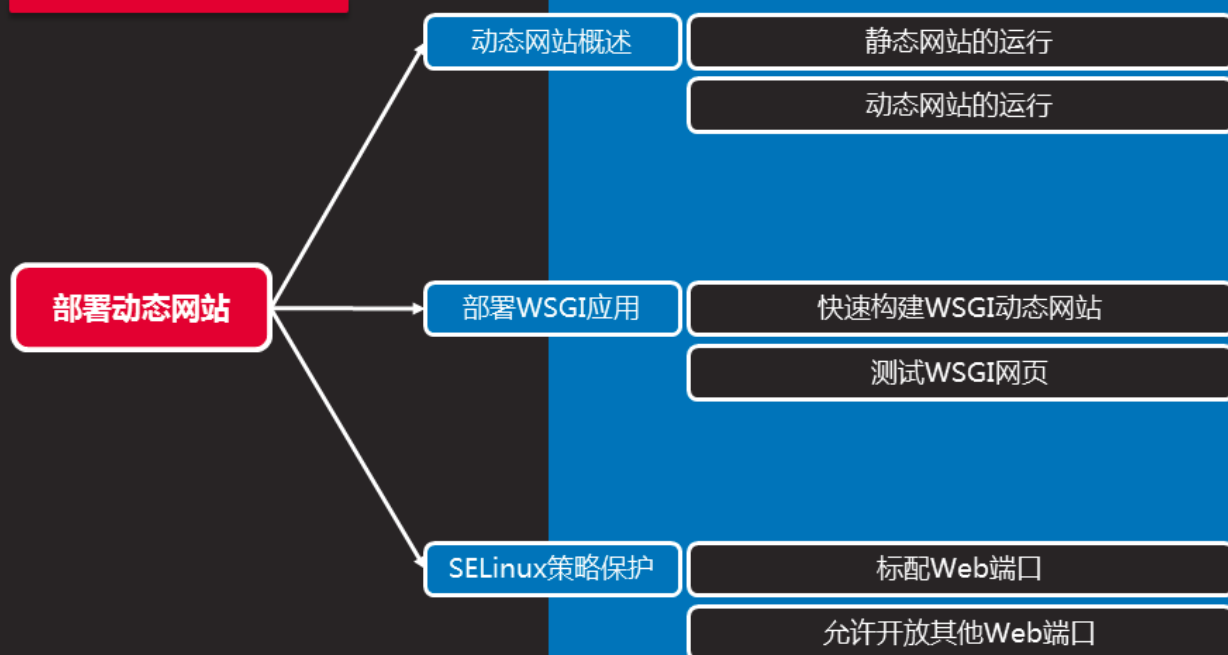
调整 Web 站点 <http://server0.example.com> 的网页目录，要求如下：

课堂练习

- 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



## 动态网站概述

## 静态网站的运行

知识讲解

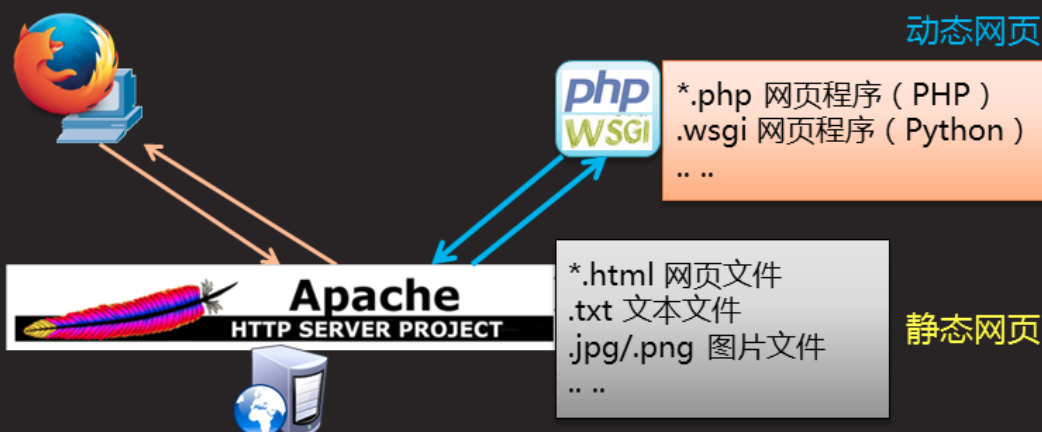
- 服务端的原始网页 = 浏览器访问到的网页
  - 由Web服务软件处理所有请求
  - 文本 ( txt/html ) 、 图片 ( jpg/png ) 等静态资源



## 动态网站的运行

知识讲解

- 服务端的原始网页  $\neq$  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.....



# 部署WSGI环境

## 快速构建WSGI动态网站

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）

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>
```

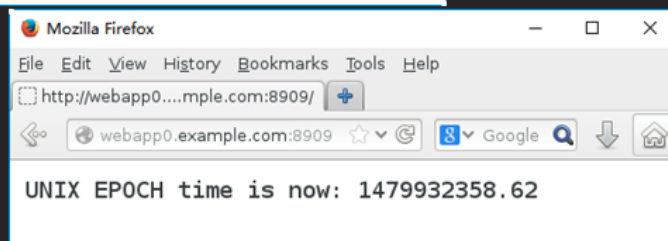
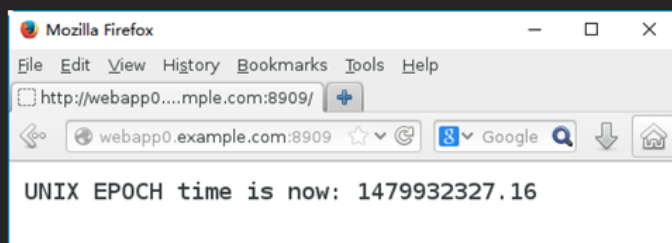
```
[root@server0 ~]# systemctl restart httpd
```



## 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



## 案例5：部署并测试WSGI站点

为站点 [webapp0.example.com](http://webapp0.example.com) 配置提供动态Web内容，要求如下：

课堂练习

- 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



## SELinux策略保护

## 标配Web端口

- 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

知识讲解



## 允许开放其他Web端口

- 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
.. ..
```

知识讲解



## 总结和答疑



# httpd启动失败

## 问题现象

知识讲解

- 调整了 httpd 配置以后，服务启动不成功
  - 报错1 : Job for httpd.service failed.
  - 报错2 : httpd -t 查语法提示 Syntax error on line xx

```
[root@server0 ~]# systemctl restart httpd
Job for httpd.service failed. See 'systemctl status httpd.service'
and 'journalctl -xn' for details.
```

```
[root@server0 ~]# httpd -t
AH00526: Syntax error on line 18 of /etc/httpd/conf.d/ssl.conf:
Invalid command 'SSPassPhraseDialog', perhaps misspelled or
defined by a module not included in the server configuration
```



## 故障分析及排除

知识讲解

- 原因分析
  - 报错1 : 配置文件有误，或者存在SELinux限制
  - 报错2 : 配置语句拼写错误，或者缺少必要的模块包
- 解决办法
  - 问题1 : httpd -t 查语法；结合 setenforce 排除
  - 问题2 : 根据提示定位文件并修复错误；安装必要的模块软件包



# SELinux策略故障

## 问题现象

- 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](#)

知识讲解

```
[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

