LPIC2 2021 Sesión 10 (2021-03-04)

Documentación relacionada:

- Manual Certificacion LPIC-2.pdf, pag XX
- Material Practicas LPIC-2/LPIC-202/
- Presentaciones/2020/202/
- gdrive://

Clase

Web Services

- DOC: Material Practicas LPIC-2/LPIC-202/2-Web Services/Apache/Resumen Apache.txt
- DOC: Material Practicas LPIC-2/LPIC-202/2-Web Services/Apache/1-Servidor Web Apache Basico.pdf
- DOC: Material Practicas LPIC-2/LPIC-202/2-Web Services/Apache/4-Laboratorio Servidor Web Apache RHE7.pdf
- Manual Certificacion LPIC-2.pdf, pag. 289
- centos trabajando con apache como debian: https://medium.com/@danielmayurilevano/c%C3%B3mo-configurar-hosts-virtuales-de-apache-en-centos-7-5a348a612286

apache: directivas básicas

- DOC: Material Practicas LPIC-2/LPIC-202/2-Web Services/Apache/1-Servidor Web Apache Basico.pdf
- **ServerRoot**: configuración
- **Listen 80**: donde queremos que escuche (varios si queremos)
  - **Listen <IP>:<puerto>**
- **Include conf.modules.d/*.conf**: módulos
- **User apache**
  - sin shell!
- **Group apache**
- **ServerAdmin <mail>**
- **ServerName <URL>:<puerto>**
- contenedores:
  - **Directory**: afecta a un directorio
  - **Files**: afecta a ficheros
  - **Location**: URIs
- **AddDefaultCharset UTF-8**

```
<VirtualHost 192.168.2.5:80>
  ServerAdmin admin@server1.curso.esp
  DocumentRoot /var/www/html/intranet
  ServerName intranet.192.168.2.5.nip.io
  ServerAlias intranet
  DirectoryIndex index.html index.php
  <Location /administrador>
    Order Deny,Allow
    deny from all
    allow from 192.168.2.1
```

```
  </Location>
  <Location /prohibido>
    Order Deny,Allow
    deny from all
    allow from 192.168.0.9
  </Location>
   <Location /permitido>
    Order Deny,Allow
    deny from all
    allow from 192.168.2.1
  </Location>
  ErrorLog logs/intranet-error_log
  CustomLog logs/intranet-access_log common
</VirtualHost>
```

- Location
  - actua sobre las URI
- Directory
  - actua sobre los directorios
- módulo: mod_auth_basic
  - podríamos hacerlo con los 2 contenedores:
    - Directory: /var/www/html/intranet/privado
    - Location: /privado

```
<VirtualHost 192.168.2.5:80>
  ServerAdmin admin@server1.curso.esp
  DocumentRoot /var/www/html/intranet
  ServerName intranet.192.168.2.5.nip.io
  ServerAlias intranet
  DirectoryIndex index.html index.php
  <Location /administrador>
    Order Deny,Allow
    deny from all
    allow from 192.168.2.1
  </Location>
  <Directory /var/www/html/intranet/privado>
    Options -FollowSymLinks -Indexes
  </Directory>
  ErrorLog logs/intranet-error_log
  CustomLog logs/intranet-access_log common
</VirtualHost>
```

- Directivas
  - Timeout
  - KeepAlive
  - MaxKeepAliveRequests
  - KeepAliveTimeout
  - Listen
  - Options
- Directiva **Options**: La directiva Options indica varias posibles opciones de comportamiento y estas pueden ser aplicadas a un directorio concreto. Un claro ejemplo de aplicación de estas directiva se puede observar en el siguiente cuadro:
  - All: todas las opciones salvo MultiViews
  - ExecCGI: Se permite la ejecución de scripts CGI.
  - FollowSymLinks: el servidor seguirá los enlaces simbólicos. Tener esta opción activa aumenta el rendimiento ya que el servidor no comprueba si un fichero o directorio es un enlace simbólico y es más rápido, pero en algunos casos puede presentar problemas de inseguridad.

    - Includes: Se permiten incluir Server-side.
    - Indexes: Si una URL solicita un directorio y no existe DirectoryIndex (v.g., index.html) en ese directorio, el servidor devolverá una lista del contenido del directorio.
    - MultiViews: Se permite mostrar contenido negociado en función de diversos valores.
    - SymLinksIfOwnerMatch: Se sigue un enlace simbólico sólo si los propietarios del enlace y del destino coinciden.
- Directiva **AllowOverride**: La directiva AllowOverride controla qué directivas se pueden situar el los ficheros .htaccess y estas pueden ser aplicadas igualmente a un directorio concreto:
    - AuthConfig: Permitir el uso de directivas de autorización (AuthDBMGroupFile, AuthDBMUserFile, AuthGroupFile, AuthName, AuthType, AuthUserFile, Require, etc).
    - FileInfo: Permitir el uso de directivas de control de tipo de documentos (DefaultType, ErrorDocument, ForceType, LanguagePriority, SetHandler, SetInputFilter, SetOutputFilter, etc).
    - Indexes: Permitir el uso de directivas que controlan los índices de directorios (AddDescription, AddIcon, AddIconByEncoding,AddIconByType, DefaultIcon, DirectoryIndex, FancyIndexing, HeaderName, IndexIgnore, IndexOptions, ReadmeName, etc).
    - Limit: Permitir el uso de directivas de acceso de hosts (Allow, Deny y Order).
    - Options: Permitir el uso de las opciones antes vistas en la directiva Options

```
<VirtualHost 192.168.2.5:80>
  ServerAdmin admin@server1.curso.esp
  DocumentRoot /var/www/html/intranet
  ServerName intranet.192.168.2.5.nip.io
  ServerAlias intranet
  DirectoryIndex index.html index.php
  <Location /administrador>
    Order Deny,Allow
    deny from all
    allow from 192.168.2.1
  </Location>
  <Directory /var/www/html/intranet/privado>
    Options -FollowSymLinks -Indexes
    AllowOverride AuthConfig
    Order allow,deny
    Allow from all
  </Directory>
  ErrorLog logs/intranet-error_log
  CustomLog logs/intranet-access_log common
</VirtualHost>
```

.htaccess

```
AuthName "Solo usuarios autorizados"
AuthType Basic
require valid-user
AuthUserFile /var/www/claves
```

```
touch /var/www/claves
chmod 600 /var/www/claves
chown apache:apache /var/www/claves
htpasswd /var/www/claves jueves4
# para borrar, htpasswd -D /var/www/claves <usuario>
```

- **mod_digest** deprecado, para Apache 2.2

SSL

```
cd /etc/httpd/conf
# generamos la key
openssl genrsa -out intranet.key 2048

# generamos el certificado
openssl req -new -key intranet.key -out intranet.csr

# lo enviamos a firmar a la una CA ;)
openssl x509 -req -days 365 -in intranet.csr -signkey intranet.key -out
intranet.crt
```

```
# copiamos la configuración :80 y cambiamos por :443, añadiendo el certificado
creado
<VirtualHost 192.168.2.5:443>
  ServerAdmin admin@server1.curso.esp
  DocumentRoot /var/www/html/intranet
  ServerName intranet.192.168.2.5.nip.io
  ServerAlias intranet
  SSlEngine On
  SSLCertificateFile /etc/httpd/conf/intranet.crt
  SSLCertificateKeyFile /etc/httpd/conf/intranet.key
  DirectoryIndex index.html index.php
  <Location /administrador>
    Order Deny,Allow
    deny from all
    allow from 192.168.2.1
  </Location>
  <Directory /var/www/html/intranet/privado>
    Options -FollowSymLinks -Indexes
    AllowOverride AuthConfig
    Order allow,deny
    Allow from all
  </Directory>
  ErrorLog logs/intranet-error_log
  CustomLog logs/intranet-access_log common
</VirtualHost>
```

```
<VirtualHost 192.168.2.5:80>
  ServerAdmin admin@server1.curso.esp
  DocumentRoot /var/www/html/intranet
  ServerName intranet.192.168.2.5.nip.io
  Redirect / https://intranet.192.168.2.5.nip.io
  ServerAlias intranet
  ErrorLog logs/intranet-error_log
  CustomLog logs/intranet-access_log common
</VirtualHost>
```

- Digital Ocean
- Cloudflare: versión gratuita, enmascara servidor, prevención DDoS
- Modulos
    - **/etc/httpd/conf.modules.d**
    - LoadModule
    - desactivar modulos no usados

rsync

- DOC: Material Practicas LPIC-2/LPIC-202/2-Web Services/Apache/Laboratorio Servidor Web Apache.pdf pag. 11
- montarlo como servidor
    - a través **xnitd**, muy viejuno
- `rsync -e ssh -avvz <path_origen> <ip_destino>:<path_destino>`
    - **--delete**: espejo

ldap

```
NameVirtualHost 192.168.0.150:80

<VirtualHost 192.168.0.150:80>
ServerAdmin berto@srweb1.curso.esp
ServerName aplicaciones.curso.esp
ServerAlias aplicaciones
<Location />
    Options None
    Order deny,allow
   deny  from all
</Location>

<Location /hello>
#Utilizamos el modulo de Apache mod_authnz_ldap
  Options Includes
AuthBasicProvider ldap
AuthType Basic
AuthzLDAPAuthoritative off
AuthName "Solo Usuarios Active Directory"
AuthLDAPURL
"ldap://192.168.0.254:389/ou=Informatica,DC=miempresa,DC=com?sAMAccountName"
AuthLDAPBindDN "cn=Administrador,cn=users,dc=miempresa,dc=com"
AuthLDAPBindPassword 000000
require valid-user
Options None
   Order allow,deny
   allow  from all
</Location>

<Location /jkstatus>
    Options None
    Order allow,deny
    allow  from all
</Location>

ErrorLog logs/aplicaciones2-error_log
CustomLog logs/aplicaciones2-access_log combined
JkMountCopy on

</VirtualHost>
```

- **IPAServer.zip**, VMWare Player, LDAP

proxy : squid

- DOC: Material Practicas LPIC-2/LPIC-202/2-Web Services/Squid/Laboratorio Squid.pdf
- DOC: pag. 309
- http/https
- filtrado
- squid transparente
    - users → router (tráfico http(s)) → squid
        - protocolo WWCP
- algoritmos de caché
    - LRU
    - LFUDA
- `yum install squid -y`
- **/etc/squid/squid.conf**
    - ojo con los espacios en el fichero de configuración
    - **http_port**: transparent (se muestra en destino la IP de la máquina y no el squid)
    - **cache_dir**: <MB> <directorios> <ficheros>
- **/var/log/squid/access.log**
- **/var/log/squid/squid.out**
- `systemctl restart squid`

restricciones

- regular expression
    - **/etc/squid/expreg-denegada**
    - añadir al fichero de configuración:
        - `acl <nombre> url_regexp «/etc/squid/expreg-denegada`
        - `http_access deny <nombre>` (antes de permitir otras cosas)
- restricciones, excepto algunas
    - **/etc/squid/inocentes**
    - añadir al fichero de configuración:
        - `acl denegados url_regexp »/etc/squid/expreg-denegada`
        - `acl inocentes url_regexp «/etc/squid/inocentes`
        - `http_access deny denegados !inocentes` (antes de permitir otras cosas)
- destino de dominio: **dstdomain**
- validación contra LDAP
    - en los logs aparece el nombre de usuario
- **time**:
    - limitaciones horarias
- listas
    - **blackweb-master**
- **sarg**: generación de informes a partir de los logs de squid

From:
https://matebcn.eu/ - **miguel angel torres egea**

Permanent link:
https://matebcn.eu/info:cursos:pue:lpic2-2021:s10

Last update: **09/03/2021 18:03**