

Servicios HTTP

Este tema está dividido en cuatro partes con pesos diferentes.

1. Configuración básica de un servidor Apache

Peso	4
Objetivos	<p>Instalar y configurar un servidor web. Esto incluye la monitorización de la carga y del rendimiento del servidor, el control de acceso, la configuración de los módulos interpretadores y la identificación de los clientes.</p> <p>Esto comprende también la configuración de las opciones del servidor para limitar el consumo de recursos, configurar los hosts virtuales y personalizar los archivos de control de acceso.</p>

a. Competencias principales

- ˘ Configuración de los archivos de registro de Apache y su contenido.
- ˘ Métodos y archivos de restricción de acceso.
- ˘ `mod_perl` y configuración PHP.
- ˘ Archivo y herramientas de autenticación de los clientes.
- ˘ Configuración del número máximo de peticiones, del número mínimo y máximo de procesos del servidor y de los clientes.
- ˘ Implementación de hosts virtuales Apache 2.4 (con o sin dirección dedicada).
- ˘ Uso de las declaraciones de redirección en los archivos de configuración Apache para personalizar el acceso a los archivos.

b. Elementos empleados

- ✓ Registros de acceso y de errores.
- ✓ `.htaccess`
- ✓ `httpd.conf`
- ✓ `mod_auth_basic`, `mod_authz_host` y `mod_access_compat`
- ✓ `htpasswd`
- ✓ `AuthUserFile`, `AuthGroupFile`
- ✓ `apachectl`, `apache2ctl`
- ✓ `httpd`, `apache2`

2. Configuración HTTPS de un servidor Apache

Peso	3
Objetivos	Configurar un servidor Apache para gestionar el protocolo HTTPS.

a. Competencias principales

- ✓ Archivos de configuración, herramientas y utilidades para SSL.
- ✓ Generación de una clave privada y de un CSR para una autoridad de certificación comercial.
- ✓ Generación de un certificado autofirmado.
- ✓ Instalación de la clave y del certificado, incluyendo las autoridades de certificación intermediarias.
- ✓ Configuración de los hosts virtuales con el módulo SNI.
- ✓ Conocimientos básicos de los problemas relativos al uso de SSL y de los hosts virtuales.
- ✓ Problemas de seguridad en el uso de SSL, desactivación de los protocolos y de

los algoritmos de cifrado no seguros.

b. Elementos empleados

- ✓ Archivos de configuración de Apache2.
- ✓ `/etc/ssl/` y `/etc/pki/`
- ✓ `openssl` y `CA.pl`
- ✓ `SSLEngine`, `SSLCertificateKeyFile` y `SSLCertificateFile`
- ✓ `SSLCACertificateFile` y `SSLCACertificatePath`
- ✓ `SSLProtocol`, `SSLCipherSuite`, `ServerTokens`, `ServerSignature` y `TraceEnable`

3. Servidor proxy y de caché Squid

Peso	2
Objetivos	Instalar y configurar un servidor proxy, incluyendo las reglas de acceso, la autenticación y el control del uso de los recursos.

a. Competencias principales

- ✓ Archivos, términos y herramientas de configuración de Squid 3.x.
- ✓ Métodos de restricción de acceso.
- ✓ Métodos de autenticación del usuario.
- ✓ Formato y contenido de las ACL en la configuración de Squid.

b. Elementos empleados

- ✓ `squid.conf`
- ✓ `acl`
- ✓ `http_access`

4. Nginx servidor HTTP y proxy inverso

Peso	2
Objetivos	Instalar y configurar un proxy inverso con Nginx. La configuración elemental de Nginx como servidor HTTP está incluida.

a. Competencias principales

- ✓ Nginx.
- ✓ Proxy inverso.
- ✓ Servidor web.

b. Elementos empleados

- ✓ `/etc/nginx/`
- ✓ `nginx`