

Práctica 2.4. Control de Acceso y Autenticación- Nginx y Apache

Alejandro Priego Izquierdo

PARTE 1. Control de acceso por IP

1. Recuerda : Las directivas de control de acceso en Apache son:

- Require all granted: El acceso es permitido incondicionalmente. Equivale a Deny All
- Require all denied: El acceso es denegado incondicionalmente. Equivale a Allow All.
- Require ip 10 172.20 192.168.2: El acceso es permitido si se hace desde el conjunto de direcciones especificadas. Equivale a Allow from 10.0.0.0/255.0.0.0 172.20.0.0/255.255.0.0 192.168.2.0/255.255.255.0
- Require host example.org: El acceso es permitido si se hace desde el dominio especificado. Equivale Allow from example.org
- Require local: El acceso es permitido desde localhost. Equivale a Allow from 127.0.0.1

2. ¿Qué significan los códigos 401 y 403 ?

El 401 significa que se ha rechazado la conexión por no tener las credenciales necesarias, mientras que el 403 indica que nadie puede acceder a este recurso.

3. Control de acceso por IP.

- a) Indica el servidor web que vas a utilizar (IP y nombre) y el cliente (IP y/o nombre).

Servidor:

192.168.131.2
172.16.220.132
priegodaw2.org

Cliente:

172.16.220.1

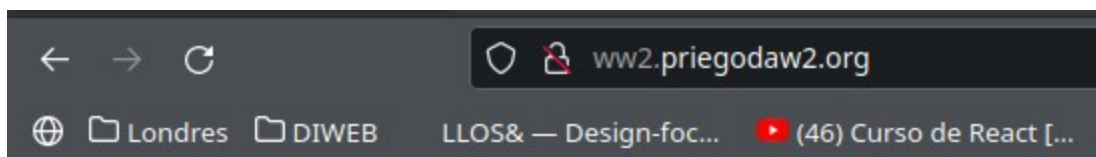
b) Configuración del site para que el cliente inicialmente tenga acceso y luego denegárselo. En lugar de modificar el fichero de configuración del site, vamos a usar un fichero .htaccess para denegar acceso al site desde la IP (de una de tus máquinas clientes).

- Captura el contenido del .htaccess

Nota: asegúrate que la directiva AllowOverride en el servidor está configurada correctamente

Permitir:

```
GNU nano 6.2 .htaccess
allow from all
```

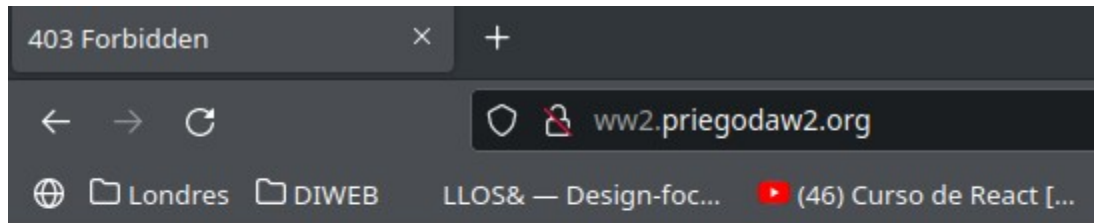


Esto es WW2 - APACHE

[Directorio 1](#) [Directorio 2](#) [Fichero 1](#) [Fichero 2](#)

Denegar:

```
GNU nano 6.2 .htaccess
deny from all
```



Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at ww2.priegodaw2.org Port 80

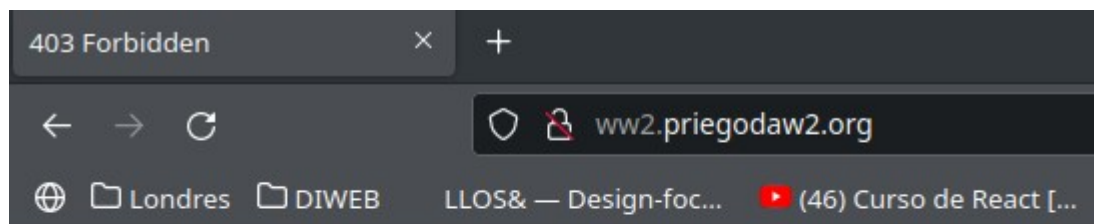
- Captura de esta parte en el fichero

```
<VirtualHost *:80>
    DocumentRoot /var/www/ww2/apache
    ServerName ww2.priegodaw2.org
    ErrorDocument 404 /error404.html
    <Directory /var/www/ww2/apache>
        Redirect "/iesgc" "https://www.iesgrancapitan.org/"
        Options -Indexes
        AllowOverride All
    </Directory>
    Alias "/test" "/var/www/ww2/apache/tmp/test"
    <Directory "/tmp/test">
        Options +Indexes
    </Directory>
    CustomLog /var/log/apache2/ww2priegodaw2-access.log combined
    ErrorLog /var/log/apache2/ww2priegodaw2-error.log
</VirtualHost>
```

c) Protege el acceso a los archivos .htaccess:

```
<VirtualHost *:80>
    DocumentRoot /var/www/ww2/apache
    ServerName ww2.priegodaw2.org
    ErrorDocument 404 /error404.html
    <Directory /var/www/ww2/apache>
        Redirect "/iesgc" "https://www.iesgrancapitan.org/"
        Options -Indexes
        AllowOverride All
        <FilesMatch "^\.ht">
            Require all denied
        </FilesMatch>
    </Directory>
    Alias "/test" "/var/www/ww2/apache/tmp/test"
    <Directory "/tmp/test">
        Options +Indexes
    </Directory>
    CustomLog /var/log/apache2/ww2priegodaw2-access.log combined
    ErrorLog /var/log/apache2/ww2priegodaw2-error.log
</VirtualHost>
```

d) ¿Qué código de error ha enviado Apache durante la ejecución? Muéstralo. ¿Qué significa?



Forbidden

You don't have permission to access this resource.

Apache/2.4.52 (Ubuntu) Server at ww2.priegodaw2.org Port 80

El código enviado es un 403, nadie tiene permiso para acceder aquí.

B. Procedimiento Apache

Las Directivas de Autenticación Digest son: AuthType, AuthName, AuthUserFile, AuthGroupFile y Require

1. Lee la práctica completa y activar los módulos necesarios

```
root@priegoDAWServer:/var/www/ww2/apache# a2enmod auth_digest
Considering dependency authn_core for auth_digest:
Module authn_core already enabled
Enabling module auth_digest.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@priegoDAWServer:/var/www/ww2/apache#
```

2. Indica en el siguiente código para qué sirve cada directiva (mete comentario en cada línea explicándolo):

```
AuthType Digest      // Esta indica el tipo de autenticación (negociación con usuario/contraseña)
AuthName "1ASIR"    // Nombre que aparecerá junto a la contraseña en algunos navegadores.
AuthUserFile /usr/local/apache/passwd/digest    // Fichero con usuarios/contraseñas
Require user pepe    // Usuario que puede acceder al recurso
```

3. ¿Que valores puede tomar la directiva Require para autenticación (no para control de acceso)? Explicarlas brevemente.

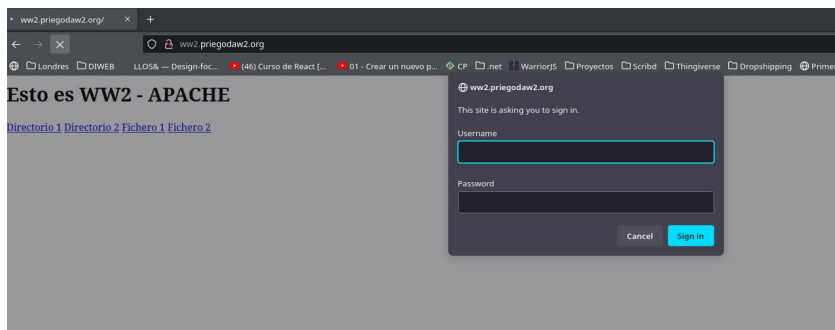
```
Require user userid [userid] ...
    Solo los usuarios nombrados pueden acceder
Require group group-name [group-name] ...
    Solo los usuarios en estos grupos pueden acceder
Require valid-user
    Todos los usuarios válidos pueden acceder
Require ip 10 172.20 192.168.2
    Solo los clientes en este rango de IP pueden acceder
Require forward-dns dynamic.example.org
    Solo los clientes a los cuales su IP resuelva a partir del dominio indicado
```

4. Controla el acceso a un determinado Directory de tu site mediante Autenticación Digest por usuario. Usa un fichero cuyo contenido sea nombre de cuentas de usuario . Crea dos usuario llamados tuapellido1 y tuapellido2 y permite que se pueda acceder sólo con tuapellido2.

```
root@priegoDAWServer:/var/www/ww2/apache# htpasswd -c ./htpasswd priego1
New password:
Re-type new password:
Adding password for user priego1
root@priegoDAWServer:/var/www/ww2/apache# htpasswd ./htpasswd priego2
New password:
Re-type new password:
Adding password for user priego2
root@priegoDAWServer:/var/www/ww2/apache# cat .htpasswd
priego1:$apr1$XKyEGpyg$yWqkcXGHXLmHSesZ64iX81
priego2:$apr1$T2fGmPLv$YWqE76RZYXBQ7ZPB0tLhC1
root@priegoDAWServer:/var/www/ww2/apache#
```

```
GNU nano 6.2
AuthType Digest
AuthName "Restringido"
AuthDigestDomain /var/www/ww2/apache/
AuthDigestProvider file
AuthUserFile /var/www/ww2/apache/.htpasswd
Require user priego2
```

5. Prueba a entrar con éxito con el usuario correcto y a fallar con el incorrecto Captura error en el fichero de log (ver pregunta 6)



```
apriego@priegoDAWServer:~$ cat /var/log/apache2/ww2priegodaw2-error.log
[Sun Feb 25 20:35:50.785525 2024] [authn_file:error] [pid 1536] (2)No such file or directory: [client 172.16.220.1:54752] AH01622: Could not open password file: /var/www/ww2/apache2/.htpasswd
[Sun Feb 25 20:40:25.134690 2024] [auth_digest:error] [pid 1596] [client 172.16.220.1:42128] AH01790: user 'priego1' in realm 'Secure' not found: /
[Sun Feb 25 20:40:29.858591 2024] [auth_digest:error] [pid 1596] [client 172.16.220.1:42128] AH01790: user 'priego1' in realm 'Secure' not found: /
[Sun Feb 25 20:40:35.009664 2024] [auth_digest:error] [pid 1598] [client 172.16.220.1:34792] AH01790: user 'priego2' in realm 'Secure' not found: /
```

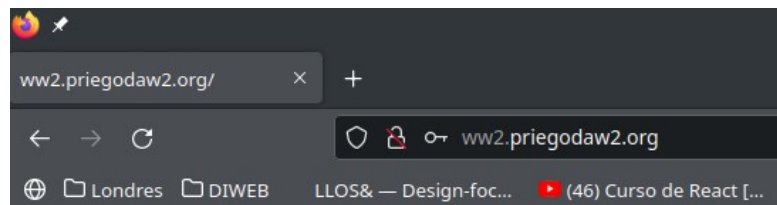
6. Autenticación de un grupo (llámalo grupo_tuapellido)

```
apriego@priegoDAWServer:/var/www/ww2/apache$ cat groups.txt
grupo_priego: priego1 priego3
```

```
<VirtualHost *:80>
    DocumentRoot /var/www/ww2/apache
    ServerName ww2.priegodaw2.org
    ErrorDocument 404 /error404.html
    <Directory /var/www/ww2/apache>
        Redirect "/iesgc" "https://www.iesgrancapitan.org/"
        Options -Indexes
        AllowOverride All
        <FilesMatch "^\.ht">
            Require all denied
        </FilesMatch>
        AuthType DIGEST
        AuthName "Secure"
        AuthUserFile "/var/www/ww2/apache/.htpasswd"
        AuthGroupFile "/var/www/ww2/apache/groups.txt"
        Require group grupo_priego
    </Directory>
    Alias "/test" "/var/www/ww2/apache/tmp/test"
    <Directory "/tmp/test">
        Options +Indexes
    </Directory>
    CustomLog /var/log/apache2/ww2priegodaw2-access.log combined
    ErrorLog /var/log/apache2/ww2priegodaw2-error.log
</VirtualHost>
```

7. ¿Qué código de error ha enviado Apache durante la ejecución? Muéstralo ¿Qué significa?

```
[Sun Feb 25 20:49:23.162315 2024] [auth_digest:error] [pid 1748] [client 172.16.220.1:33538] AH01790: user 'priego2' in realm 'Secure' not found: /
[Sun Feb 25 20:49:26.522084 2024] [auth_digest:error] [pid 1748] [client 172.16.220.1:33538] AH01790: user 'priego1' in realm 'Secure' not found: /
```



Esto es WW2 - APACHE

[Directorio 1](#) [Directorio 2](#) [Fichero 1](#) [Fichero 2](#)