ACTIVIDAD 6.3 - CONTROL DE ACCESOS

1. INTRODUCCIÓN

El **control de acceso hace referencia a todos los medios que proporcionan una forma de controlar el acceso a un recurso**. Conviene diferenciar este concepto de la autenticación y la autorización.

- **Autenticación** es cualquier proceso por el cual se verifica que uno es quien dice ser.
- **Autorización** es cualquier proceso en el cuál a un usuario se le permite estar donde quiere estar, o tener la información que quiere tener.

2. DIRECTIVA REQUIRE

El control de accesos se basa en la directiva ***Require***, que depende del módulo ***authz_core*** y ***authz_host***.

Comprueba que ambos módulos están activos con:

```
ls /etc/apache2/mods-enabled/
```

`Require all granted`

Se permite el acceso siempre.

`Require all denied`

El acceso no se permite nunca.

`Require user userid [userid]` …

El acceso solo se permite a los usuarios especificados en la lista.

`Require valid-user`

El acceso se permite a todos los usuarios del sistema.

`Require group group-name [group-name]`…

El acceso solo se permite a los usuarios pertenecientes a los grupos especificados en la lista.

`Require ip address1 [address2]`…

El acceso solo se permite a las direcciones IP especificadas. Las IP pueden ser completas, completas con máscara (indicando una red) o parciales, en cuyo caso especifican un rango. Por ejemplo, 192.168.1 indicaría todos los hosts desde el 192.168.1.0 hasta el 192.168.1.255.

`Require host domain1-name [domain2-name]`…

El acceso solo se permite a los hosts cuyo nombre coincide con alguno de la lista. Se busca coincidencia total o parcial, empezando por el final del nombre del host. Por ejemplo, si se define **`Require host iesabastos.org`**, se permitirá el acceso a los hosts cuyo nombre acabe en ***iesbastos.org***, como por ejemplo ***daw.iesabastos.org*** o simplemente ***iesabastos.org***

`Require method http-method [http-method] ...`

El acceso solo se permite a los métodos HTTP especificados: GET, POST, OPTIONS… HEAD se trata como equivalente a GET. TRACE no se contempla.

La directiva ***Require*** se puede negar para que tenga el efecto contrario (denegar explícitamente el acceso) usando la opción ***not***. Por ejemplo:

- **`Require not user daw-user:`** no permite el acceso al usuario *daw-user*.
- **`Require not ip 192.168.1.25:`** no permite el acceso a la dirección IP 192.168.1.25.
- **`Require not host iesbastos.org:`** no permite el acceso a los hosts pertenecientes al dominio *iesabastos.org*.

Estas directivas se usarían combinadas con un contenedor tipo ***<Directory>*** o ***<File>*** para especificar los permisos de acceso a ese directorio o fichero. Por ejemplo, la siguiente directiva daría todos los permisos de acceso al directorio **/var/www**:

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

Es importante entender que la directiva ***Require*** puede producir tres resultados:

- **Positivo**: cuando se cumple un ***Require*** sin ***not.***
- **Negativo**: cuando se cumple un ***Require*** con ***not***.
- **Neutro**: en cualquier otro caso.

Por tanto, una directiva ***Require*** (sin not) puede dar positivo o neutro, mientras una directiva ***Require not*** puede dar negativo o neutro.

Sólo un resultado positivo autoriza el acceso.

2.1 Contenedores de autorización

Además existen contenedores de autorización que permiten combinar requerimientos de forma compleja y arbitraria, para cumplir cualesquiera que sean las políticas de acceso.

<RequireAll> ... </RequiereAll>

Permite el acceso si se cumplen todas las directivas y ninguna es negativa. Si todas las directivas contenidas son neutras, el resultado es neutro. Falla en cualquier otro caso

El siguiente ejemplo permite el acceso a todas las IP menos la 10.223.12.134 y a los hosts de youtube.com

```
<RequireAll>
    Require all granted
    Require not ip 10.223.12.134
    Require not host youtube.com
</RequireAll>
```

<RequireAny> ... </RequiereAny>

Permite el acceso si al menos una directiva es positiva. Si todas las directivas contenidas son neutras, el resultado es neutro. En cualquier otro caso, el resultado es negativo. No se permite el uso de ***Require not*** dentro de un contenedor ***RequireAny***.

El siguiente ejemplo permite el acceso al directorio /www/apuntes tanto a los hosts de youtube.com como a los que están en la red 192.168.0.0/24

```
<Directory "/www/apuntes">
    <RequireAny>
        Require host youtube.com
        Require ip 192.168.0.0
    </RequireAny>
</Directory>
```

<RequireNone> ... </RequiereNone>

Permite el acceso solo si ninguna directiva es positiva. En cualquier otro caso el resultado es neutro. No se permite el uso de ***Require not*** dentro de un contenedor ***RequireNone***.

Cuando se especifican varias directivas en una sección sin indicar un contenedor el comportamiento es idéntico a si estuvieran contenidas en un contenedor ***RequireAny***.

2.1.1 Ejemplo 1

```
<Directory "/www/mydocs">
      <RequireAll>
            Require all granted
            <RequireNone>
                  Require ip 192.168.205
                  Require host phishers.example.com moreidiots.example
                  Require host .ke
            </RequireNone>
      </RequireAll>
</Directory>
```

Todo el mundo podrá acceder al directorio excepto aquellos que se conecten desde la red 192.168.205.0 o los hosts phisers.example.com, moreidiots.example y los terminados en .ke

2.1.2 Ejemplo 2

```
<Directory "/www/mydocs">
      <RequireAny>
            <RequireAll>
                  Require user root
                  Require ip 123.123.123.123
            </RequireAll>
            <RequireAll>
                  <RequireAny>
                        Require group sysadmins
                        Require group useraccounts
                        Require user anthony
                  </RequireAny>
                  <RequireNone>
                        Require group restrictedadmin
                        Require host bad.host.com
                  </RequireNone>
            </RequireAll>
      </RequireAny>
</Directory>
```

Se obtendrá acceso al directorio en alguno de estos casos:

- Si accede el usuario root desde la IP 123.123.123.123
- Si accede un usuario del grupo sysadmins y no pertenece al grupo restrictedadmin ni se conecta desde el host bad.host.com
- Si accede un usuario del grupo useraccounts y no pertenece al grupo restrictedadmin ni se

conecta desde el host bad.host.com

- Si accede el usuario anthony y no pertenece al grupo restrictedadmin ni se conecta desde el host bad.host.com

3. EJERCICIOS

1. Dada la siguiente configuración, contesta:
   a. ¿Podemos acceder al directorio desde la IP 12.3.4.5?
   b. ¿Y desde la IP 127.159.235.255?
   c. ¿Y desde la IP 192.168.1.152?

```
<Directory /var/www/>
    <RequireAny>
        Require ip 192.168.1.0/24
        Require ip 127
    </RequireAny>
</Directory>
```

2. ¿Qué directivas serían necesarias para permitir el acceso al directorio ***/var/www*** a todo el mundo excepto a aquellos que se conecte desde el host www.example.com?
3. ¿Qué directivas serían necesarias para permitir el acceso a todas las IP de la red 192.168.0.0 excepto a la IP 192.168.5.5?
4. Modifica el archivo **000-default.conf** para que nadie pueda acceder al directorio **/var/www**. Compruébalo. Vuelve a dejarlo como estaba (acceso para todos)
5. Consigue tu IP pública y modifica el archivo **000-default.conf** para que pueda acceder al directorio **/var/www** todo el mundo excepto tu IP. Compruébalo usando otro dispositivo
6. Modifica el archivo **000-default.conf** para que solo se pueda acceder al directorio **/var/www** con tu IP. Compruébalo usando otro dispositivo
7. Vuelve a dejarlo como estaba (acceso para todos)