

Configuraci3 del control d'acc3s en Apache 2.4



Índex

1. Introducció.....	3
2. Objectius.....	3
3. Desenvolupament.....	3
3.1 Creació de directoris i arxius.....	3
3.2 Protecció per IP.....	3
Això impedirà l'accés a qualsevol altra IP que no siga la especificada.....	3
3.2 Protecció amb Usuari i Contrassenya.....	4
3.3 Configuració en el DocumentRoot.....	4
4. Validar.....	5

1. Introducció

Aquest document descriu el procés de configuració del control d'accés en Apache 2.4 per protegir directoris d'una aplicació web mitjançant restriccions per adreça IP i autenticació bàsica.

2. Objectius

- Comprendre el funcionament de les directives d'Apache per al control d'accés.
- Configurar l'accés restringit a un directori segons l'adreça IP.
- Protegir un directori mitjançant usuari i contrasenya.
- Implementar la configuració utilitzant un fitxer `.htaccess`.

3. Desenvolupament

3.1 Creació de directoris i arxius

En la aplicació desplegada anteriorment anem a desplegar dos directoris:

1. Crearem la carpeta `web/`.
2. `restringit`, sols será accessible des de la nostra IP.
3. `privat`, que sols será accessible amb l'usuari `gabi` i contrasenya `gabi`.
4. La configuració estarà en un fitxer `.htaccess` en el `DocumentRoot`.

Dins de cada directori crearem dos arxius `.htaccess` i `index.html`. I en el últim arxiu mencionat tindrà un missatge que es mostrarà cada vegada que accedim a aquest.

3.2 Protecció per IP

Per restringir l'accés al directori restringit segons l'adreça IP, crearem un fitxer `.htaccess` dins del directori restringit amb el següent contingut:

```
Require ip 10.2.216.14
```

Això impedirà l'accés a qualsevol altra IP que no siga la especificada.

3.2 Protecci33 amb Usuari i Contrassenya

Per protegir el directori **privat**, configurarem autenticaci33 b3sica amb **.htaccess**. Creem el fitxer **.htaccess** dins del directori privat amb el següent contingut:

```
AuthType Basic
AuthName "Acc3s restringit"
AuthUserFile /etc/apache2/.htpasswd
Require valid-user
```

I executem el següent comandament:

```
htpasswd -c /etc/apache2/.htpasswd gabi
```

3.3 Configuraci33 en el DocumentRoot

Obrim el fitxer **/etc/apache2/apache2.conf** i ens assegurem que la configuraci33 per al **DocumentRoot** contingui aquest contingut:

```
<Directory /var/www/html>
    AllowOverride All
    Require all granted
</Directory>
```

Aix33 permet que els fitxers **.htaccess** dins del **DocumentRoot** puguin sobreescriure la configuraci33 per defecte.

Tamb33 podem habilitar els m3duls necessaris per assegurar el correcte funcionament d'aquestes restriccions:

```
sudo a2enmod auth_basic
sudo a2enmod authn_file
```

I reiniciem el servei d'Apache per assegurar la c3rrega de les configuracions:

```
sudo systemctl restart apache2
```

Amb aquesta configuraci33, qualsevol directori dins del **DocumentRoot** pot ser protegit seguint els m3todes explicats pr3viament.

4. Validar

1. Accedir al directori restringit des d'una IP diferent i verificar que l'accés està denegat.

Anant a `localhost:8081/restringit` i tenint la IP correcta ens apareixerà correctament açó:

No sé per que no va si tots els passos son correctes i estic en una màquina virtual

2. Intentar accedir a privat i verificar que es requereix usuari i contrassenya.

Anant a `localhost:8081/privat` i ficant les credencials correctament

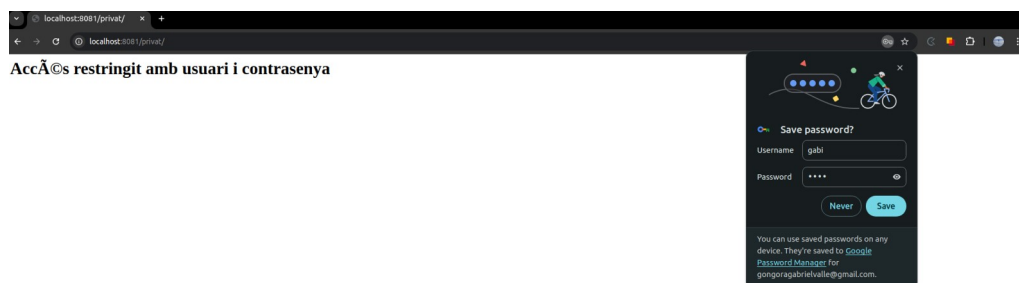
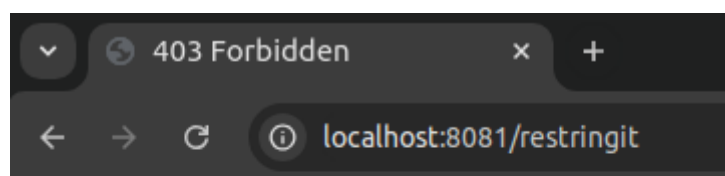


Figura 1: Accés a privat

3. Intentar accedir amb credencials incorrectes.

`localhost:8081/restringit` amb una IP diferent:



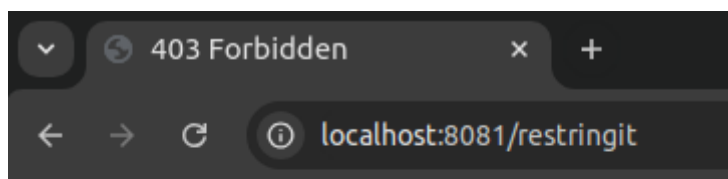
Forbidden

You don't have permission to access this resource.

Apache/2.4.62 (Debian) Server at localhost Port 8081

Figura 2: Permís denegat al tindre una IP diferent

localhost:8081/restringit



Forbidden

You don't have permission to access this resource.

Apache/2.4.62 (Debian) Server at localhost Port 8081

Figura 3: Permís denegat al tindre una IP diferent