Apache : VirtualHosts et contrôle des accès

Formation : BTS SIO — Option SISR

1. Fonctionnement

Apache peut héberger plusieurs sites sur la même adresse IP. Le DNS conduit le client au serveur ; l'en-tête HTTP Host permet à Apache de sélectionner le VirtualHost demandé.

L'exemple comporte deux sites sur `192.36.3.20` : WordPress sur `www0.californie.cub.sioplc.fr` et une application de diagnostic sur `scanner0.californie.cub.sioplc.fr`.

2. Séparer les sites et leurs accès

Le scanner se trouve dans un sous-répertoire de la racine WordPress. Le VirtualHost WordPress doit donc interdire cet accès alternatif pour ne pas contourner la protection du scanner.

Fichier `/etc/apache2/sites-available/000-default.conf` :

```
<VirtualHost *:80>
    ServerName www0.californie.cub.sioplc.fr
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    <Directory /var/www/html/scanner>
        AllowOverride None
        Require all denied
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

```
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        ServerName www0.californie.cub.sioplc.fr

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

        <Directory /var/www/html/scanner>
                AllowOverride None
                Require all denied
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

VirtualHost WordPress et refus d'accès à son sous-répertoire scanner.

3. Créer le compte HTTP

```
sudo apt install apache2-utils
sudo htpasswd -c /etc/apache2/scanner0.htpasswd etudiant
sudo chown root:www-data /etc/apache2/scanner0.htpasswd
sudo chmod 640 /etc/apache2/scanner0.htpasswd
sudo a2enmod auth_basic authn_file authz_user authz_host
```

L'option `-c` est réservée à la première création du fichier ; elle écrase un fichier existant. Le mot de passe est saisi à l'invite, et le fichier d'empreintes reste hors de la racine Web.

4. Cumuler réseau autorisé et authentification

Fichier `/etc/apache2/sites-available/scanner0.conf` :

```
<VirtualHost *:80>
    ServerName scanner0.californie.cub.sioplc.fr
```

```
    DocumentRoot /var/www/html/scanner

    <Directory /var/www/html/scanner>
        Options -Indexes
        AllowOverride None
        DirectoryIndex index.php

        AuthType Basic
        AuthName "Scanner Californie - Acces administrateurs"
        AuthBasicProvider file
        AuthUserFile /etc/apache2/scanner0.htpasswd

        <RequireAll>
            Require ip 192.168.3.192/28
            Require valid-user
        </RequireAll>
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/scanner0-error.log
    CustomLog ${APACHE_LOG_DIR}/scanner0-access.log combined
</VirtualHost>
```

`RequireAll` impose les deux conditions : origine dans `192.168.3.192/28` et compte valide. `Options -Indexes` désactive la liste des fichiers ; `AllowOverride None` empêche un .htaccess de modifier ces règles.

```
<VirtualHost *:80>
    ServerName scanner0.californie.cub.sioplc.fr
    DocumentRoot /var/www/html/scanner

    <Directory /var/www/html/scanner>
        Options -Indexes
        AllowOverride None
        DirectoryIndex index.php

        AuthType Basic
        AuthName "Scanner Californie - Acces administrateurs"
        AuthBasicProvider file
        AuthUserFile /etc/apache2/scanner0.htpasswd

        <RequireAll>
            Require ip 192.168.3.192/28
            Require valid-user
        </RequireAll>
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/scanner0-error.log
    CustomLog ${APACHE_LOG_DIR}/scanner0-access.log combined
</VirtualHost>
```

Configuration finale du scanner avec RequireAll.

L'exemple a été réalisé en HTTP. L'authentification Basic ne chiffre pas les identifiants : utiliser HTTPS avant de réemployer ce mécanisme hors d'une maquette contrôlée.

5. Activer et vérifier

```
sudo a2ensite scanner0.conf
sudo apache2ctl configtest
# Seulement si le contrôle retourne Syntax OK :
sudo systemctl reload apache2
sudo apache2ctl -S
```

Les deux VirtualHosts doivent apparaître sur le port attendu. Une requête par IP sans Host correspondant peut atteindre le site par défaut.

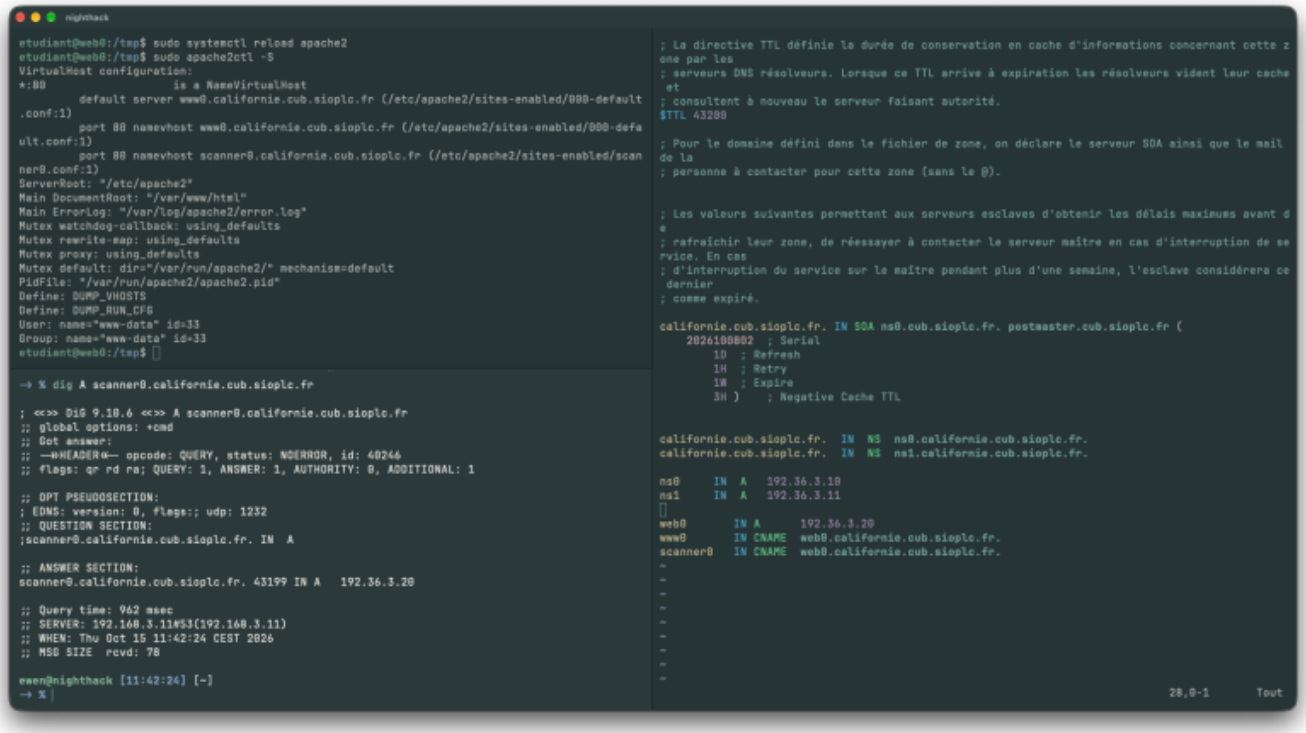
6. Associer les noms DNS

Sur le primaire de la zone, l'exemple utilise :

```
web0       IN A      192.36.3.20
www0       IN CNAME  web0.californie.cub.sioplc.fr.
scanner0   IN CNAME  web0.californie.cub.sioplc.fr.
```

Augmenter le numéro de série, valider la zone et la recharger sur son primaire. Ne pas modifier la copie transférée sur un secondaire. Le nom demandé dans l'en-tête HTTP reste celui du site, même lorsque le DNS retourne un CNAME.

```
dig A scanner0.californie.cub.sioplc.fr
```

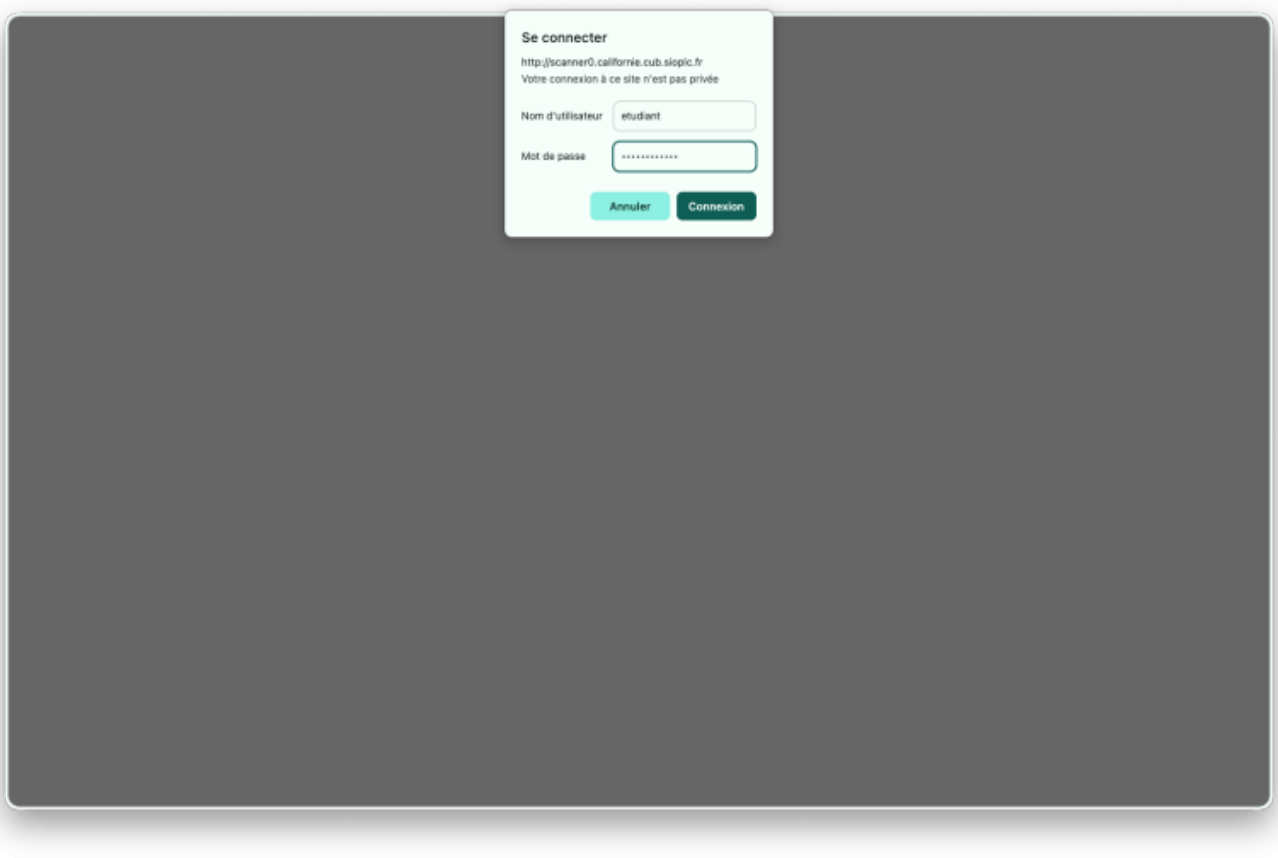


VirtualHosts et résolution vers 192.36.3.20.

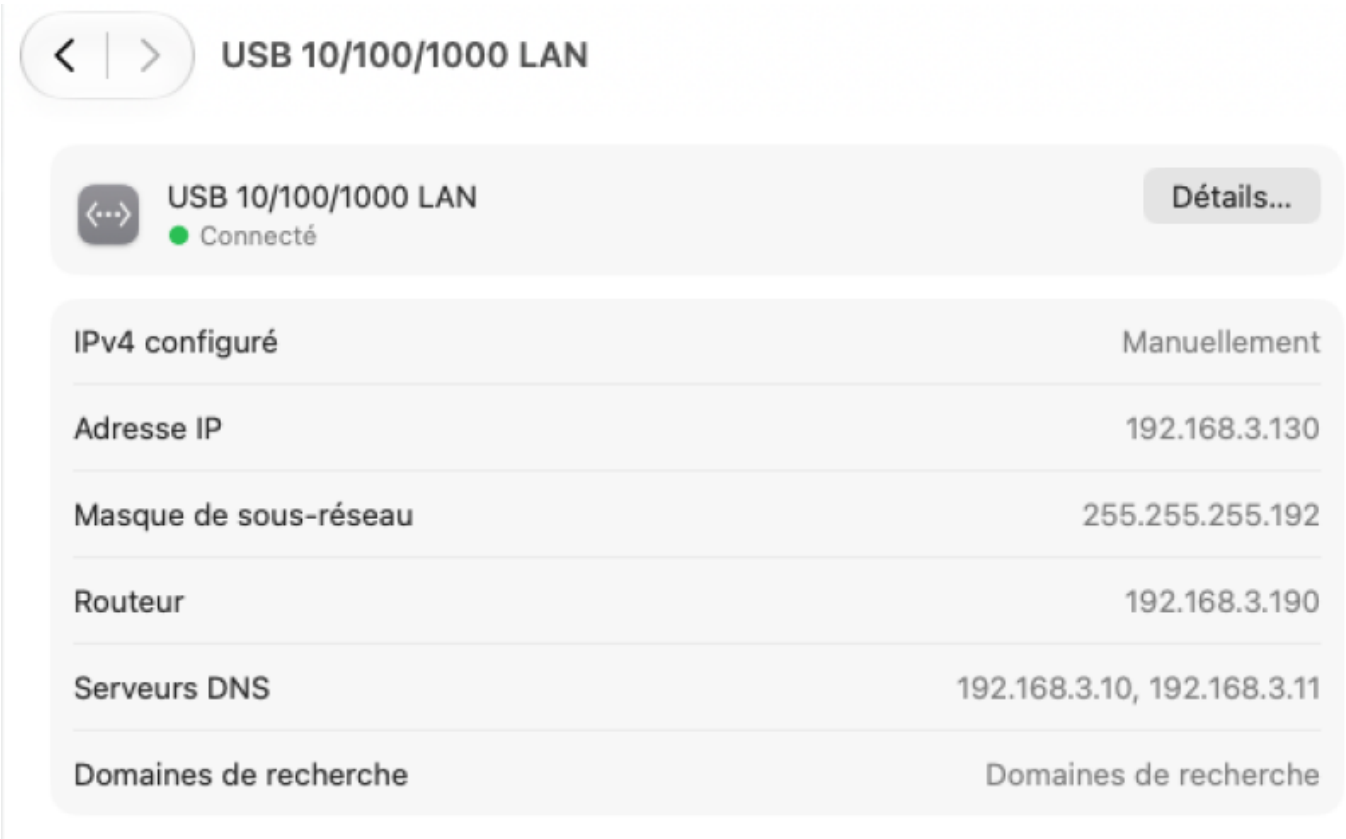
La sortie dig visible est antérieure au passage aux CNAME : elle valide l'adresse obtenue, pas le rechargement des nouveaux alias.

7. Résultats des essais

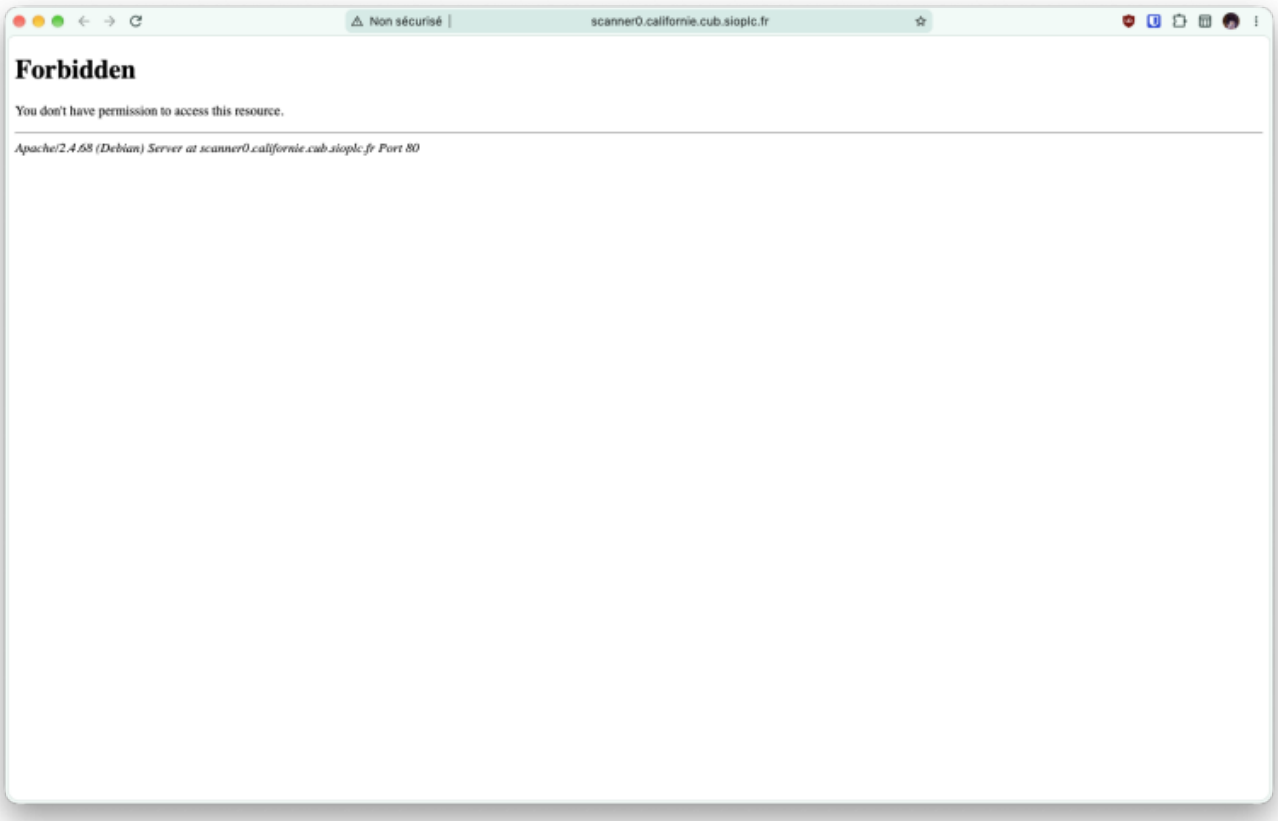
Contrôle	Observation consignée
Accès par le nom scanner0	Formulaire affiché
Accès depuis le VLAN Admin	Invite d'authentification ; accès avec le bon compte déclaré réussi
Accès depuis le VLAN client	HTTP 403 Forbidden



Demande d'authentification depuis le réseau Admin.



Poste client 192.168.3.130/26 utilisé pour le test de refus.



Refus HTTP 403 depuis le réseau client.

HTTP 403 signifie que le serveur a répondu et refusé l'accès. Ce résultat ne doit pas être interprété comme un simple problème de routage.

8. Limite de l'application de diagnostic

L'application pédagogique concatène une entrée utilisateur à une commande système :

```
exec("ping " . $_GET['ip'], $reponse, $retour);
```

Cette construction expose à une injection de commandes avec les droits du processus PHP. Le filtrage IP et l'authentification réduisent l'accès, mais ne corrigent pas le code. La correction applicative et le passage à HTTPS sont des améliorations proposées, pas des résultats déjà réalisés.

9. Références

- Apache — VirtualHosts
- TLS et certificats
- Publication et contrôle du NAT

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=services:apache

Last update: **2026/10/18 01:23**