Chap7 : Serveur Debian DS2 et DS1: délégation DNS

Sommaire

1 – Serveurs Web virtuels :

- Depuis la VM DS2, j'ajoute l'alias IP sur enp0s3 dans le fichier /etc/network/interfaces.

```
  GNU nano 7.2                                                  /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.4.10
netmask 255.255.255.0
network 192.168.4.0
broadcast 192.168.4.255
gateway 192.168.4.254
dns-search sio-exupery.fr
dns-domain sio-exupery.fr
dns-nameservers 192.168.4.10

auto enp0s3:0
iface enp0s3:0 inet static
address 192.168.4.9
netmask 255.255.255.0
network 192.168.4.0
broadcast 192.168.4.255


# This is an autoconfigured IPv6 interface
#iface enp0s3 inet6 auto
```

- J'active l'alias (ifup enp0s3:0), je vérifie avec la commande ip a, puis je lance un ping sur la nouvelle adresse pour m'assurer que tout fonctionne correctement.

```
root@DS2: ~#ifup enp0s3:0
root@DS2: ~#ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f8:03:ea brd ff:ff:ff:ff:ff:ff
    inet 192.168.4.10/24 brd 192.168.4.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet 192.168.4.9/24 brd 192.168.4.255 scope global secondary enp0s3:0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef8:3ea/64 scope link
       valid_lft forever preferred_lft forever
root@DS2: ~#
```

```
root@DS2: ~#ping -c 2 192.168.4.9
PING 192.168.4.9 (192.168.4.9) 56(84) bytes of data.
64 bytes from 192.168.4.9: icmp_seq=1 ttl=64 time=0.032 ms
64 bytes from 192.168.4.9: icmp_seq=2 ttl=64 time=0.041 ms

--- 192.168.4.9 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1020ms
rtt min/avg/max/mdev = 0.032/0.036/0.041/0.004 ms
root@DS2: ~#_
```

- Je crée les deux répertoires nécessaires pour les deux hébergements virtuels. Le premier correspond à l'accès sécurisé, et le deuxième à l'accès normal.

```
root@DS2: ~#mkdir /var/www/html/secu /var/www/html/web
root@DS2: ~#
```

- Je copie, dans ces deux répertoires, le fichier HTML de test index.html précédemment utilisé, puis je personnalise la page d'accueil des répertoires secu et web en y indiquant respectivement « Site secu en construction » et « Site web en construction ».

```
root@DS2: ~#cp /var/www/html/index.html /var/www/html/secu
root@DS2: ~#cp /var/www/html/index.html /var/www/html/web
root@DS2: ~#
```

```
 GNU nano 7.2                                  /var/www/html/secu/index.html

<html>
<head>
<title>SIO Saint-Ex</title>
</head>

<body> bgcolor="#EEEEEE">
<h1>BTS SIO</h1>
<p>Site secu_en construction</p>

</body>
</html>
```

```
 GNU nano 7.2                                  /var/www/html/web/index.html

<html>
<head>
<title>SIO Saint-Ex</title>
</head>

<body> bgcolor="#EEEEEE">
<h1>BTS SIO</h1>
<p>Site web en construction</p>

</body>
</html>
```

- Je crée les répertoires pour les fichiers de logs.

```
root@DS2: ~#mkdir /var/www/html/secu/logs /var/www/html/web/logs
root@DS2: ~#
```

- Je consulte le fichier du virtualhost par défaut 000-default.conf, situé dans /etc/apache2/sites-available/.

```
  GNU nano 7.2                                  /etc/apache2/sites-available/000-default.conf
<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 www.example.com

        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

        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>
```

- Je supprime le fichier `/etc/apache2/sites-enabled/000-default.conf, qui est le lien vers le fichier du virtualhost par défaut situé à `/etc/apache2/sites-available/000-default.conf.

```
root@DS2: ~#ls -l /etc/apache2/sites-enabled
total 0
lrwxrwxrwx 1 root root 35 26 févr. 09:52 000-default.conf -> ../sites-available/000-default.conf
root@DS2: ~#rm /etc/apache2/sites-enabled/000-default.conf
root@DS2: ~#
```

- Je copie le fichier du virtualhost par défaut et je nomme la copie sites-sio.conf.

```
root@DS2: ~#cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/sites-sio.conf
root@DS2: ~#
```

- Afin de créer les Virtualhosts correspondant aux différents sites, je modifie le fichier /etc/apache2/sites-available/sites-sio.conf avec les conteneurs déclarés par la directive VirtualHost, dans lesquels figurent les éléments de configuration spécifiques à chaque hôte virtuel.

```
  GNU nano 7.2                                    /etc/apache2/sites-available/sites-sio.conf
<VirtualHost 192.168.4.9>
        ServerName secu.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/secu
        ErrorLog /var/www/html/secu/logs/error.log
        CustomLog /var/www/html/secu/logs/access.log combined
</VirtualHost>

<VirtualHost *:80>
        ServerName www.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/web
        ErrorLog /var/www/html/web/logs/error.log
        CustomLog /var/www/html/web/logs/access.log combined
</VirtualHost>
```

- J’active les fichiers des virtualhost crée avec la commande a2ensite.

```
root@DS2: ~#a2ensite sites-sio.conf
Enabling site sites-sio.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@DS2: ~#systemctl reload apache2
root@DS2: ~#_
```

- J'ajoute dans le fichier /var/cache/bind/db.sio-exupery.fr la ligne correspondant à l’enregistrement « secu ».

```
  GNU nano 7.2                                    /var/cache/bind/db.sio-exupery.fr

; Fichier pour la résolution directe
$TTL 86400
@       IN SOA DS2.sio-exupery.fr. root.sio-exupery.fr (
               2019020701
               1w
               1d
               4w
               1w )
@                           IN NS DS2.sio-exupery.fr.
intra.sio-exupery.fr        IN NS DS1.intra.sio-exupery.fr.
DS2.sio-exupery.fr.         IN A  192.168.4.10
DS1.intra.sio-exupery.fr.   IN A  192.168.4.254
ftp                         IN    CNAME DS2
www                         IN    CNAME DS2
secu                        IN A  192.168.4.9_
```

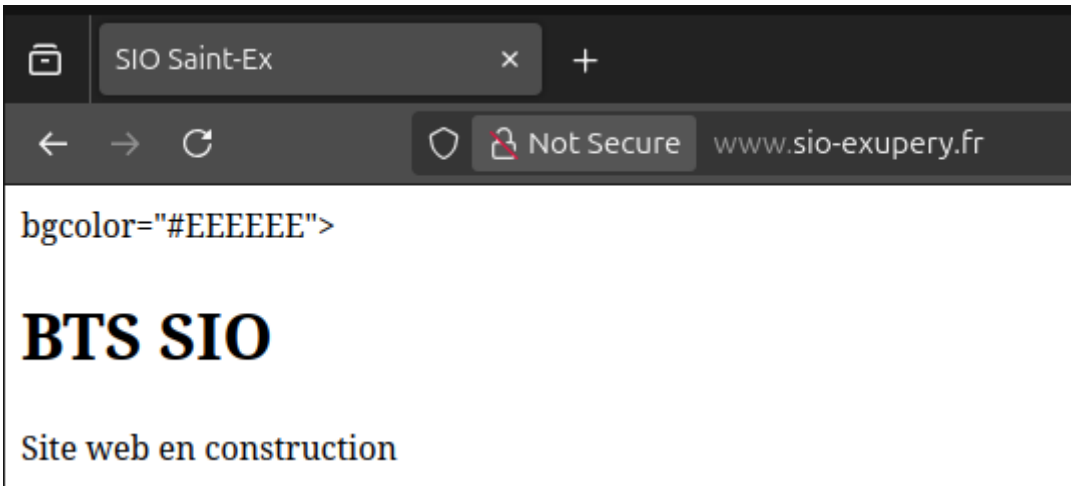
- Je relance le service DNS sur DS2.

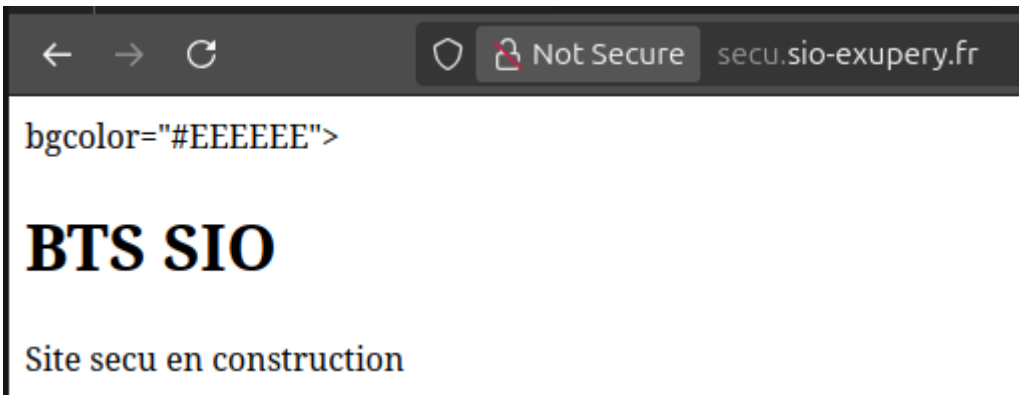
```
root@DS2: ~#systemctl restart bind9
root@DS2: ~#
```

- Je vérifie par un ping que la réponse est correcte sur secu.sio-exupery.fr.

```
root@DS2: ~#ping secu.sio-exupery.fr
PING secu.sio-exupery.fr (192.168.4.9) 56(84) bytes of data.
64 bytes from 192.168.4.9 (192.168.4.9): icmp_seq=1 ttl=64 time=0.036 ms
64 bytes from 192.168.4.9 (192.168.4.9): icmp_seq=2 ttl=64 time=0.045 ms
64 bytes from 192.168.4.9 (192.168.4.9): icmp_seq=3 ttl=64 time=0.046 ms
```

- Je teste depuis le navigateur d'UD1 les URL www.sio-exupery.fr et secu.sio-exupery.fr.





- Je crée les deux répertoires projet1 et projet2 avec les sous-répertoires repweb.

```
root@DS2: ~#mkdir -p /var/www/html/projet1/repweb/logs /var/www/html/projet2/repweb/logs
root@DS2: ~#_
```

- Je crée le répertoire logs pour l'hôte virtuel associé au site WordPress.

```
root@DS2: ~#mkdir /var/www/html/sitewordpress/wordpress/logs
root@DS2: ~#_
```

- J'affiche les 5 répertoires correspondant aux 5 virtualhosts.

```
root@DS2: ~#ls -l /var/www/html/
total 44
-rw-r--r-- 1 root root   140 28 févr. 15:57 index.html
-rw-r--r-- 1 root root 10701 26 févr. 09:52 index.sauv
-rw-r--r-- 1 root root   367 28 févr. 16:23 pagepdo.php
-rw-r--r-- 1 root root    21 28 févr. 16:00 pagephptest.php
drwxr-xr-x 3 root root  4096 26 mars  09:36 projet1
drwxr-xr-x 3 root root  4096 26 mars  09:36 projet2
drwxr-xr-x 3 root root  4096 26 mars  09:11 secu
drwxr-xr-x 3 root root  4096  5 mars  09:00 sitewordpress
drwxr-xr-x 3 root root  4096 26 mars  09:11 web
root@DS2: ~#_
```

- Je modifie le fichier des hôtes virtuels /etc/apache2/sites-available/sites-sio.conf.

```
  GNU nano 7.2                                    /etc/apache2/sites-available/sites-sio.conf
<VirtualHost 192.168.4.9:80>
        ServerName secu.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/secu
        ErrorLog /var/www/html/secu/logs/error.log
        CustomLog /var/www/html/secu/logs/access.log combined
</VirtualHost>

<VirtualHost 192.168.4.10:80>
        ServerName www.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/web
        ErrorLog /var/www/html/web/logs/error.log
        CustomLog /var/www/html/web/logs/access.log combined
</VirtualHost>

<VirtualHost 192.168.4.10:80>
        ServerName projet1.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/projet1/repweb
        ErrorLog /var/www/html/projet1/repweb/logs/error.log
        CustomLog /var/www/html/projet1/repweb/logs/access.log combined
</VirtualHost>

<VirtualHost 192.168.4.10:80>
        ServerName projet2.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/projet2/repweb
        ErrorLog /var/www/html/projet2/repweb/logs/error.log
        CustomLog /var/www/html/projet2/repweb/logs/access.log combined
</VirtualHost>
<VirtualHost 192.168.4.10:80>
        ServerName blog.sio-exupery.fr
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/sitewordpress/wordpress
        ErrorLog /var/www/html/sitewordpress/wordpress/logs/error.log
        CustomLog /var/www/html/sitewordpress/wordpress/logs/access.log combined
</VirtualHost>_
```

- Je recharge la configuration d'apache2.

```
root@DS2: ~#systemctl reload apache2
root@DS2: ~#_
```

- J'ajoute dans le fichier de zone /var/cache/bind/db.sio-exupery.fr les trois alias nécessaires.

```
 GNU nano 7.2                                          /var/cache/bind/db.sio-exupery.fr

; Fichier pour la résolution directe
$TTL 86400
@       IN SOA DS2.sio-exupery.fr. root.sio-exupery.fr (
               2019020701
               1w
               1d
               4w
               1w )
@                               IN NS DS2.sio-exupery.fr.
intra.sio-exupery.fr            IN NS DS1.intra.sio-exupery.fr.
DS2.sio-exupery.fr.             IN A  192.168.4.10
DS1.intra.sio-exupery.fr.       IN A  192.168.4.254
ftp                             IN    CNAME DS2
www                             IN    CNAME DS2
secu                            IN A  192.168.4.9
projet1                         IN    CNAME DS2
projet2                         IN    CNAME DS2
blog                            IN    CNAME DS2_
```

- Je relance le service DNS sur DS2.

```
root@DS2: ~#systemctl restart bind9
root@DS2: ~#
```

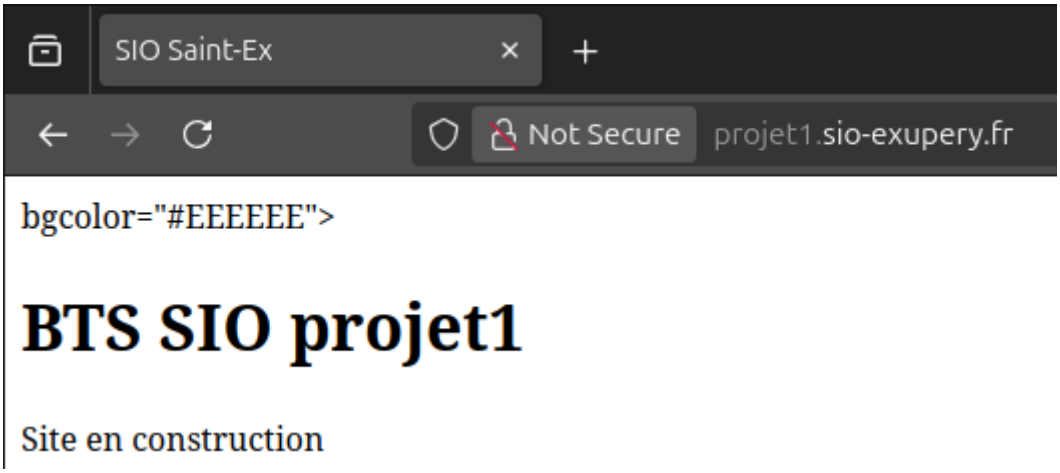
- Je copie la page index.html, utilisée précédemment, dans /var/www/html/projet1/repweb ainsi que dans /var/www/html/projet2/repweb, puis je modifie les deux pages en y ajoutant « projet1 » pour l'une et « projet2 » pour l'autre.

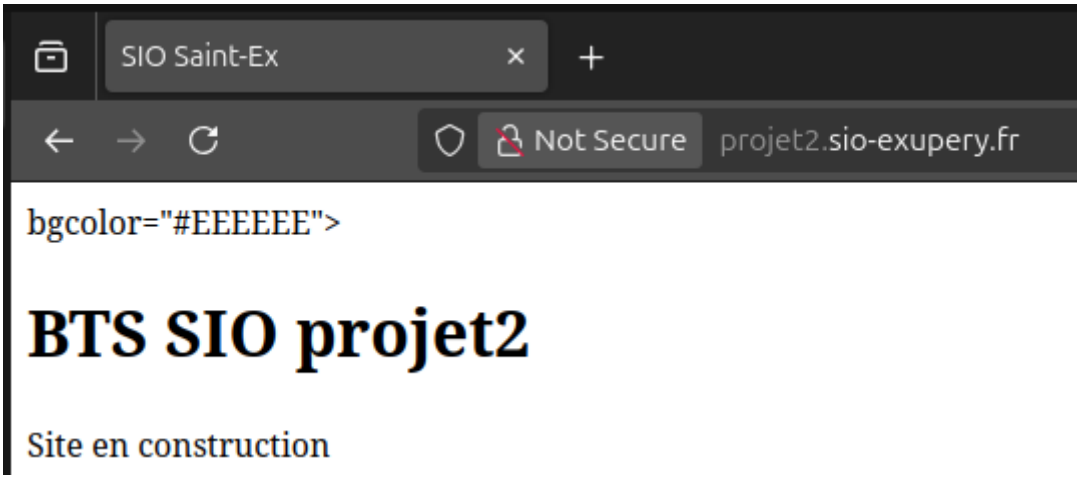
```
root@DS2: ~#cp /var/www/html/index.html /var/www/html/projet1/repweb
root@DS2: ~#cp /var/www/html/index.html /var/www/html/projet2/repweb
root@DS2: ~#
```

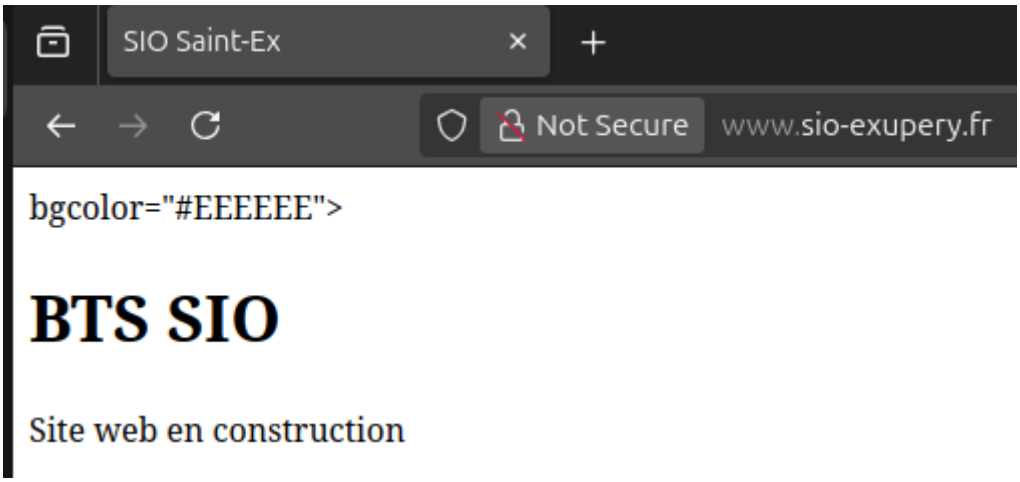
```
 GNU nano 7.2                                    /var/www/html/projet1/repweb/index.html

<html>
<head>
<title>SIO Saint-Ex</title>
</head>

<body> bgcolor="#EEEEEE">
<h1>BTS SIO projet1</h1>
<p>Site en construction</p>

</body>
</html>
```

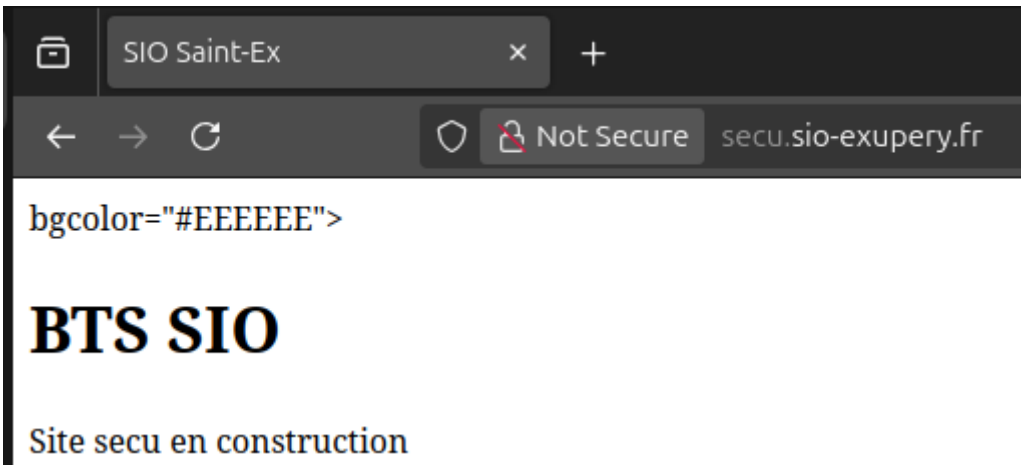
```
 GNU nano 7.2                                  /var/www/html/projet2/repweb/index.html *

<html>
<head>
<title>SIO Saint-Ex</title>
</head>

<body> bgcolor="#EEEEEE">
<h1>BTS SIO projet2</h1>
<p>Site en construction</p>

</body>
</html>
```

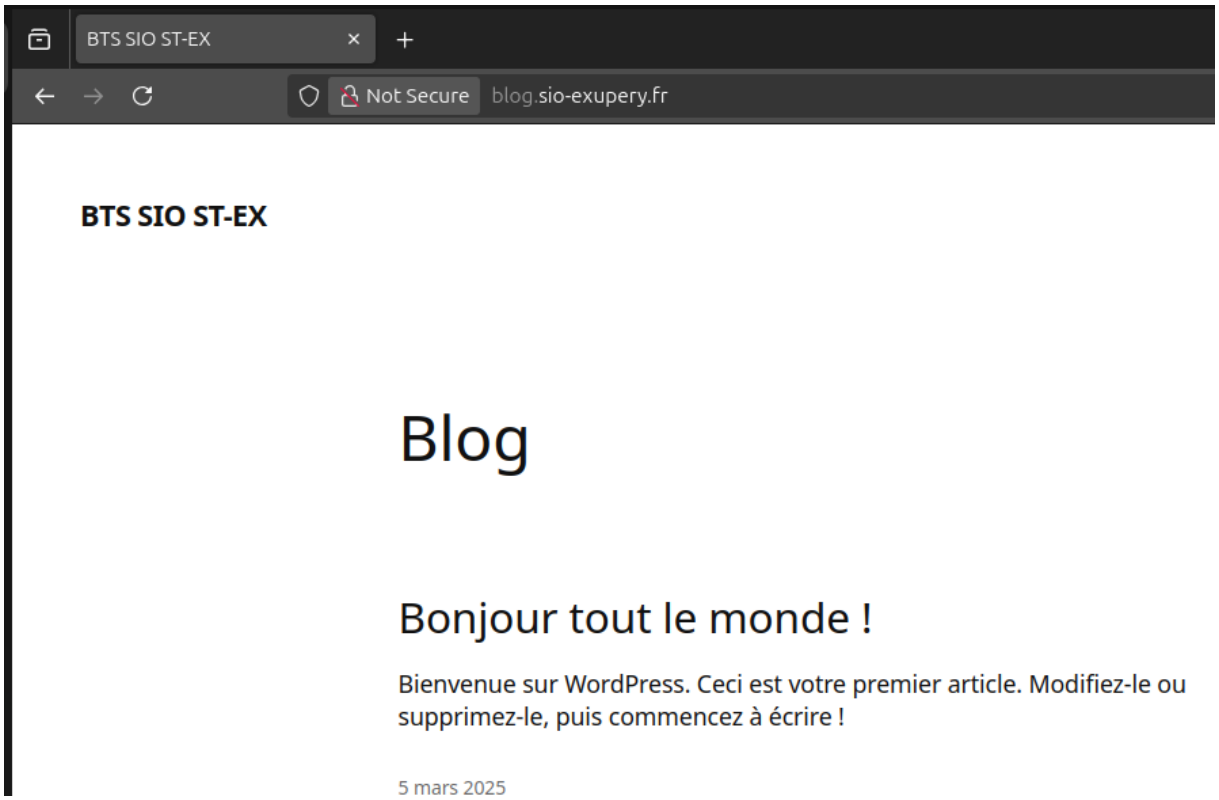
- Je vérifie, à partir du navigateur du client UD1, la bonne conformité des réponses en testant notamment les URL indiquées.





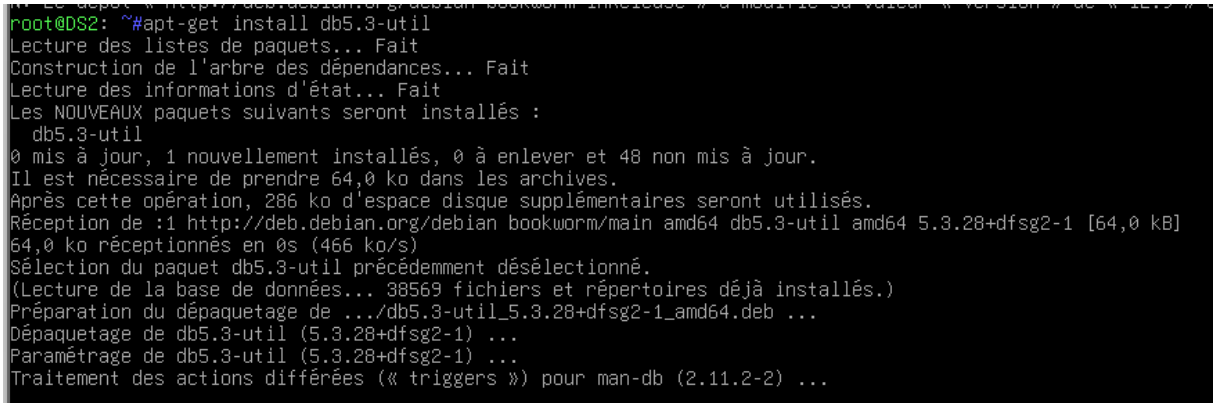

SIO Saint-Ex
Not Secure
www.sio-exupery.fr
bgcolor="#EEEEEE">
BTS SIO
Site web en construction


SIO Saint-Ex
Not Secure
secu.sio-exupery.fr
bgcolor="#EEEEEE">
BTS SIO
Site secu en construction


BTS SIO ST-EX
Not Secure
blog.sio-exupery.fr
BTS SIO ST-EX
Blog
Bonjour tout le monde !
Bienvenue sur WordPress. Ceci est votre premier article. Modifiez-le ou supprimez-le, puis commencez à écrire !
5 mars 2025

2 – Coupler VsFTPd avec Apache :

- J'installe les utilitaires Berkeley avec la commande apt-get install db5.3-util.



- Je donne les droits à l'utilisateur et au groupe www-data sur le répertoire html qui contient les sites Web.

- Je crée les répertoires /etc/vsftpd/ pour stocker les données de configuration de vsftpd, et /etc/vsftpd/users.conf/ pour les fichiers de configuration de chaque utilisateur FTP, simultanément.

- J'indique, dans un fichier texte nommé users.txt, les couples login/mot de passe correspondant aux utilisateurs FTP virtuels.

- Dans la mesure où ce fichier contient les noms d'utilisateurs et mots de passe associés, je dois changer les droits d'accès à ce fichier.

```
root@DS2: ~#chmod 600 /etc/vsftpd/users.txt
root@DS2: ~#ls -l /etc/vsftpd/users.txt
-rw------- 1 root root 34 28 mars  16:30 /etc/vsftpd/users.txt
root@DS2: ~#
```

- Je convertis, à l'aide de db5.3-util, ce fichier en base de données, puis je change les droits d'accès pour garantir sa sécurité.

```
root@DS2: ~#db5.3_load -T -t hash -f /etc/vsftpd/users.txt /etc/vsftpd/users.db
root@DS2: ~#chmod 600 /etc/vsftpd/users.db
root@DS2: ~#_
```

- Je remplace tout le contenu du fichier /etc/pam.d/vsftpd par les seules lignes spécifiées.

```
  GNU nano 7.2                                                    /etc/pam.d/vsftpd

auth    required        pam_userdb.so db=/etc/vsftpd/users
account required        pam_userdb.so db=/etc/vsftpd/users_
```

- Je modifie ou ajoute les directives figurant en gras dans le fichier de configuration de VsFTPd (/etc/vsftpd.conf).

```
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#anon_root=/var/ftp
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Active les utilisateurs virtuels
guest_enable=YES

# Fait correspondre tous les utilisateurs virtuels à l'utilisateur www-data
guest_username=www-data
# Utilisation de l'utilisateur non privilégié
nopriv_user=www-data

# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
anon_upload_enable=NO
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
anon_mkdir_write_enable=NO
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# If enabled, vsftpd will display directory listings with the time
```

```
# chroot)
chroot_local_user=YES
chroot_list_enable=YES
# (default follows)
chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# Customization
#
# Some of vsftpd's settings don't fit the filesystem layout by
# default.
#
# This option should be the name of a directory which is empty.  Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require filesystem
# access.
secure_chroot_dir=/var/run/vsftpd/empty
#
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO

#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES

# Permet d'utiliser les configurations individuelles pour chaque utilisateur
user_config_dir=/etc/vsftpd/users.conf
```

- Je crée, pour chaque utilisateur, son fichier de configuration dans le répertoire /etc/vsftpd/users.conf/.

```
  GNU nano 7.2                                    /etc/vsftpd/users.conf/webmaster1
anon_world_readable_only=NO
local_root=/var/www/html/projet1
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES
anon_other_write_enable=YES
```

```
  GNU nano 7.2                                    /etc/vsftpd/users.conf/webmaster2

anon_world_readable_only=NO
local_root=/var/www/html/projet2
write_enable=YES
anon_upload_enable=YES
anon_mkdir_write_enable=YES
anon_other_write_enable=YES
```

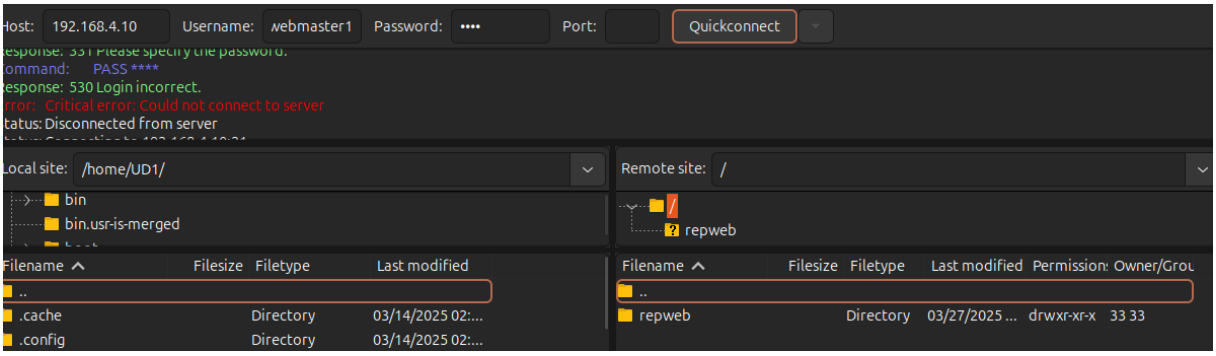
- Je relance le service Vsftpd sur le serveur DS2.

```
root@DS2: ~#systemctl restart vsftpd
root@DS2: ~#_
```

- En tant que root sur DS2, je retire à l'utilisateur www-data le droit d'écriture sur la racine des répertoires /var/www/html/projet1 et /var/www/html/projet2.

```
root@DS2: ~#chmod u-w /var/www/html/projet1
root@DS2: ~#chmod u-w /var/www/html/projet2
root@DS2: ~#ls -ld /var/www/html/projet*
dr-xr-xr-x 3 www-data www-data 4096 26 mars  09:36 /var/www/html/projet1
dr-xr-xr-x 3 www-data www-data 4096 26 mars  09:36 /var/www/html/projet2
root@DS2: ~#
```

- Je teste depuis UD1 une connexion FTP au répertoire Projet1 en utilisant le client FileZilla, et je vérifie que l'utilisateur virtuel webmaster1 est bien « chrooté » dans le répertoire Projet1.



- Je transfère une page web dans le répertoire /var/www/html/projet1/repweb, puis je vérifie les droits sur ce fichier pour m'assurer qu'il appartient à l'utilisateur www-data.

```
root@DS2: ~#ls -l /var/www/html/projet1/repweb
total 8
-rw------- 1 www-data www-data    0  2 avril 09:29 fichier.txt
-rw-r--r-- 1 www-data www-data  148 27 mars  10:40 index.html
drwxr-xr-x 2 www-data www-data 4096 27 mars  10:35 logs
root@DS2: ~#_
```