	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

Sur un réseau, l'échange d'informations entre les machines est réalisé selon deux méthodes : soit classiquement par des partages réseaux via Samba ou NFS ; soit d'une manière plus universelle par le protocole FTP. Dans ce dernier cas, le transfert de fichiers a souvent pour objectif la mise à jour d'un site web.

Éléments d'informations sur le protocole FTP

Le protocole FTP (File Transfer Protocol) transfère des fichiers en s'inscrivant dans un modèle client/serveur avec TCP (TFTP utilise UDP et se réserve à des transferts spécifiques). Au-delà de sa définition, l'outil se révèle indispensable. La seule difficulté consiste à choisir le "bon" serveur FTP, c'est-à-dire le plus robuste, sécurisé et d'un maniement aisé. Retenez simplement les deux modes de fonctionnement de FTP :

- Le **mode actif** : le client détermine le port de connexion avant le transfert de données. Ce type de fonctionnement est peu courant car il impose une configuration supplémentaire derrière un pare-feu, voire problématique en cas de NAT.
- Le **mode passif** : le serveur détermine le port de connexion, ce qui laisse la possibilité au client de l'initialisation (port 21) et simplifie les règles d'un pare-feu.

Les transferts s'effectuent soit en mode ASCII pour les fichiers texte, soit en mode binaire pour tous les autres. Classiquement, un client FTP possède l'option permettant le choix automatique du mode de transfert.

a. Le choix des logiciels

Pour un serveur FTP et le système GNU/LINUX le choix est large : proftpd, pure-ftpd, twoftpd, wu-ftpd, vsftpd... S'il ne doit y avoir qu'une seule raison pour le choix, gardons celle de la sécurité. Pour cela, le logiciel serveur VsFTP (Very secure FTPd) porte en son nom son orientation.

À l'autre "bout" de la chaîne se trouve le client. Pour les utilisateurs :

- Sous Windows, **FileZilla** (<http://filezilla-project.org>).
- Sous Linux, le choix dépend de l'environnement graphique comme gftp sous GNOME, kftpGrabber sous KDE ; mais vous pouvez aussi choisir FileZilla...

Mise en place du serveur FTP

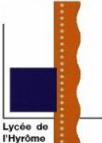
Vous allez mettre en place un serveur FTP sécurisé sur SRVDMZ suivant deux scénarios et avec deux types d'authentification.

a. Configuration du service dans le cadre d'une connexion anonyme

Cette pratique propose un accès FTP anonyme dans le cadre du serveur SRVDMZ pour des clients extérieurs à l'entreprise.

Installez le paquetage

```
sudo apt-get install vsftpd ccze.
```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

Vous installez aussi le très sympathique ccze qui a pour simple fonction de coloriser les logs de beaucoup de logiciels comme VsFTP évidemment, mais aussi Postfix, Apache, etc. Son utilisation se fait d'après le manuel par une redirection, mais cela est peu pratique dans le cas d'un long fichier comme syslog, préférez alors la pratique du tube.

Testez les deux formes de commande :

```
ccze </var/log/syslog
tail -f /var/log/syslog | ccze
```

L'installation de VsFTP ne provoque pas de question et il s'installe (à la différence d'un autre serveur FTP ProFTPD) en "standalone" (c'est-à-dire en service indépendant) et non avec le "super-démon" inetd. L'installation crée l'utilisateur ftp et le groupe nogroup.

Créez un fichier quelconque par touch /srv/ftp/test.txt, ce fichier ne dispose que des droits en lecture pour le groupe et le reste du monde (644). C'est là que seront entreposés les fichiers destinés au public.

Connectez-vous à partir du client (Linux) à partir d'une connexion dans la console et en anonymous avec un mot de passe vide (sortie par exit) :

```

eleve@ubuntu: ~
eleve@ubuntu:~$ ftp 192.168.4.10
Connected to 192.168.4.10.
220 (vsFTPd 2.3.5)
Name (192.168.4.10:eleve): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0          0 Sep 16 12:12 test.txt
226 Directory send OK.
ftp>

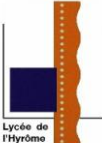
```

b. Configuration du service dans le cadre d'une connexion authentifiée

Cette pratique propose un accès FTP authentifié pour des clients soit de façon classique, soit par le service LDAP. Vous allez utiliser le service FTP sur le réseau interne supposé sûr. Chaque utilisateur local à la machine dispose de son répertoire FTP.

Modifier la configuration du serveur FTP. Les changements à apporter sur les directives du fichier /etc/vsftpd.conf sont indiqués en **gras** :

Configuration pour les utilisateurs locaux

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

```
# Démon en standalone et mutuellement exclusif avec listen_ipv6
listen=YES
# Plus d'accès anonyme cette fois, on doit mettre explicitement
# la directive à NO
anonymous_enable=NO

# Autorisation pour les utilisateurs locaux à YES
local_enable=YES
# Autorisation pour les utilisateurs locaux, évidemment à YES pour écrire
write_enabled=YES

# Masque appliqué pour l'écriture, droits à 644 (fichiers),
# 755 (répertoires)
local_umask=022

# Active l'affichage des fichiers .message à l'entrée dans les répertoires
dirmessage_enable=YES

# Activation du fichier de log
xferlog_enable=YES

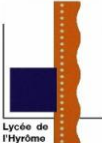
# Obliger les connexions par le port 20
connect_from_port_20=YES

# Message lors de la connexion
ftpd_banner=Bienvenue sur le service FTP du serveur SRVDMZ

# Restreindre l'utilisateur à son répertoire (préférable)
chroot_local_user=YES

# Liste des utilisateurs autorisés À NE PAS ÊTRE EN CHROOT
# si l'option précédente est activée (le CONTRAIRE sinon)
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list

# Spécifications liées à VsFTPD
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
rsa_cert_file=/etc/ssl/private/vsftpd.pem
```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

Relancez le service par `/etc/init.d/vsftpd restart`
 Créez le fichier `/etc/vsftpd.chroot_list`.

Créez un utilisateur nommé donald sur le serveur SRVDMZ (adduser donald) et relancez le service vsftpd.

Pour sécuriser le serveur vsftpd, retirez à l'utilisateur donald le droit d'écriture sur la racine de son répertoire en tapant :

```
sudo chmod u-w /home/donald.
```

Testez la connexion au serveur FTP depuis le client Lubuntu avec le compte donald.

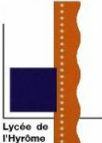
Sur le client Lubuntu, installez **filezilla** et testez une connexion à partir du client avec cet utilisateur et son mot de passe ; celui-ci doit se trouver « emprisonné » dans son répertoire personnel (`/home/donald` sur SRVDMZ).

Testez l'impossibilité de se connecter maintenant en anonymous.

Inscrivez l'utilisateur donald dans le fichier `/etc/vsftpd.chroot_list` sur le serveur FTP et vérifiez par une autre connexion FTP à partir du client que celui-ci a maintenant accès **à tout** le système de fichiers.

Cela ne veut pas dire que donald peut faire des modifications... mais il peut transférer et lire des fichiers, ce qui en soi pose des problèmes de sécurité importants. Dans le registre de la sécurité, ne pas oublier le fichier `/etc/ftpusers` qui contient les comptes locaux disponibles sur le serveur (comme le root) n'ayant pas le droit de se connecter au service FTP.

Revenir au fonctionnement sécurisé précédent et testez des transferts de fichiers.
 Visualiser les logs colorisés du serveur FTP.

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

Changement de DNS

Actuellement, le serveur SRVLAN sert de serveur DNS pour la zone virtualux.local. Il faut maintenant passer dans une optique d'entreprise avec un nom de domaine en .fr, soit virtualux.fr. Dans ce cadre on aura :

- SRVDMZ, serveur DNS pour la zone virtualux.fr.
- SRVLAN, serveur DNS en délégation pour la zone intra.virtualux.fr.

On supprime donc la zone virtualux.local au profit d'une délégation de zone en Intranet. Le fait d'utiliser un nom de domaine "normal", c'est-à-dire dans l'arborescence mondiale reconnue (.fr) sans être déposé peut poser problème à votre (et aux autres) serveur DNS qui s'intègre dans une hiérarchie, mais ici le serveur DNS principal se trouve pour l'instant "derrière" SRVLAN et la table de routage de votre système hôte ne comporte pas de route statique pour y parvenir.

a. Installation du nouveau service DNS

Installez BIND9 sur SRVDMZ comme indiqué dans le TP2 Installation du service DNS avec cette fois les zones suivantes :

Fichier `/etc/bind/named.conf.local` :

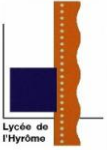
```
// Les zones
zone "virtualux.fr" IN {
    type master;
    file "db.virtualux.fr";
    allow-update { none; };
};

zone "4.168.192.in-addr.arpa" IN {
    type master;
    file "rev.virtualux.fr";
    allow-update { none; };
};
```

Créez le fichier pour la zone directe avec l'inscription d'un serveur en délégation pour la zone intra.virtualux.fr et de l'alias pour le serveur Web et FTP.

Fichier `/var/cache/bind/db.virtualux.fr`

```
; Fichier pour la résolution directe
$TTL 86400
@      IN SOA srvdmz.virtualux.fr. root.virtualux.fr. (
    2013091601
```

 Lycée de l'Hyrôme	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

```

1w
1d
4w
1w )
@      IN NS srvdmz.virtualux.fr.
intra.virtualux.fr.      IN NS srvlan.intra.virtualux.fr.
srvdmz      IN A 192.168.4.10
srvlan.intra.virtualux.fr. IN A 192.168.4.254
ftp      IN CNAME srvdmz
www      IN CNAME srvdmz

```

Vous notez la présence de l'enregistrement NS pour la zone intra.virtualux.fr et de l'enregistrement A nécessaire car le serveur de nom de la zone déléguée se trouve dans la même arborescence. Cet enregistrement est indispensable pour que le serveur puisse être contacté (on appelle cela le **mécanisme de la "glue"**). La présence des l'alias résout l'adresse de type ftp.virtualux.fr et www.virtualux.fr au lieu de srvdmz.virtualux.fr.

Créez ensuite le fichier pour la zone inverse :

Fichier `/var/cache/bind/rev.virtualux.fr`

```

; Fichier pour la résolution inverse
$TTL 86400
@      IN SOA srvdmz.virtualux.fr. root.virtualux.fr. (
2009061201
1w
1d
4w
1w )
@      IN NS srvdmz.virtualux.fr.
10     IN PTR srvdmz.virtualux.fr.

```

Attribuez ces deux fichiers de zones au groupe bind afin de les rendre accessibles au serveur bind par :

```

sudo chgrp bind /var/cache/bind/*
sudo chmod 664 /var/cache/bind/*

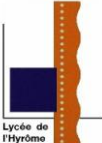
```

Vérifiez le fichier `/etc/hosts` qui ne doit contenir (laissez en plus les lignes pour IPv6) que la référence à la boucle locale et le nom de l'hôte positionné cette fois sur la zone virtualux.fr :

```

127.0.0.1 localhost
192.168.4.10 srvdmz.virtualux.fr srvdmz

```

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

Modifiez votre fichier `/etc/network/interfaces` pour qu'il contienne les lignes suivantes :

```
dns-search virtualux.fr
dns-domain virtualux.fr
dns-nameservers 192.168.4.10
```

La directive `dns-domain` fixe le domaine courant, `dns-search` fait ajouter le domaine `virtualux.fr` par défaut aux demandes avec un nom d'hôte non entièrement qualifié. Enfin, le serveur DNS indiqué par la directive `dns-nameserver` sera interrogé par défaut pour toute résolution de noms.

b. Test du nouveau serveur DNS

Redémarrer la carte réseau `eth0` avec les commandes `ifdown` et `ifup`.
Observer le fichier `/etc/resolv.conf` qui contient les serveurs DNS de votre machine

Lancer l'utilitaire de vérification `named-checkconf` (si c'est bon il ne retourne rien) qui vérifie par défaut le fichier `/etc/bind/named.conf` :

```
sudo named-checkconf
```

Lancer le deuxième utilitaire de vérification `named-checkzone` sur vos fichiers de zone :

```
cd /var/cache/bind/
sudo named-checkzone -d virtualux.fr db.virtualux.fr
```

Relancer le service `bind9` par :

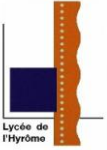
```
sudo /etc/init.d/bind9 restart
```

Avec les outils vus au TP2 vérifiez le bon fonctionnement de votre serveur DNS pour la résolution de la zone `virtualux.fr`.

Comme pour le TP2, de façon à réduire la charge de travail de votre DNS (et surtout des autres), nous allons faire en sorte qu'il interroge un serveur DNS "au-dessus de lui", qui peut être celui de votre FAI ou de votre réseau physique dans notre cas et non pas les serveurs racines.

Commenter les lignes ayant trait aux serveurs racines dans le fichier `/etc/bind/named.conf.default-zones` de façon à ce qu'il ne puisse plus les "importuner" :

```
// Référence aux serveurs racines
//zone "." {
// type hint;
// file "/etc/binc/db.root";
//};
```

 Lycée de l'Hyrôme	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

Modifier le fichier /etc/bind/named.conf.options :

```
options {
    directory "/var/cache/bind";
    forward only;
    forwarders { 172.16.0.1; };
    auth-nxdomain no;
    listen-on-v6 { any; }
};
```

Relancer votre serveur DNS.

c. Transformation du DNS sur SRVLAN

Modifiez sur SRVLAN le fichier de zones :

Fichier /etc/bind/named.conf.local

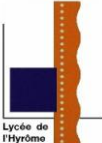
```
// Les zones
zone "intra.virtualux.fr" IN {
    type master;
    file "db.intra.virtualux.fr";
    allow-update { 127.0.0.1; };
};

zone "4.168.192.in-addr.arpa" IN {
    type master;
    file "rev.intra.virtualux.fr";
    allow-update { 192.168.4.254; };
};
```

Toujours sur SRVLAN, créez le fichier pour la zone directe, cette fois-ci adapté à la délégation de la zone :

Fichier /var/cache/bind/db.intra.virtualux.fr

```
; Fichier pour la résolution directe
$TTL 86400
@ IN SOA srvlan.intra.virtualux.fr. root.intra.virtualux.fr. (
    2009061201
    1w
    1d
    4w
    1w )
@ IN NS srvlan.intra.virtualux.fr.
srvlan IN A 192.168.4.254
```


 Lycée de l'Hyrôme	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

Créez ensuite le fichier pour la zone inverse :

Fichier `/var/cache/bind/rev.intra.virtualux.fr`

```
; Fichier pour la résolution inverse
$TTL 86400
@      IN SOA srvlan.intra.virtualux.fr. root.intra.virtualux.fr. (
        2009060101
        1w
        1d
        4w
        1w )
@      IN NS   srvlan.intra.virtualux.fr.
254    IN PTR  srvlan.intra.virtualux.fr.
```

Lancer l'utilitaire de vérification `named-checkconf` (si c'est bon il ne retourne rien) qui vérifie par défaut le fichier `/etc/bind/named.conf` :

```
sudo named-checkconf
```

Lancer le deuxième utilitaire de vérification `named-checkzone` sur vos fichiers de zone :

```
cd /var/cache/bind/
sudo named-checkzone -d intra.virtualux.fr db.intra.virtualux.fr
```

Changez le fichier `/etc/hosts` avec `srvlan.intra.virtualux.fr`

Modifier le fichier `/etc/network/interfaces` pour faire apparaitre :

```
dns-domain intra.virtualux.fr
dns-search intra.virtualux.fr
dns-nameservers 192.168.4.254
```

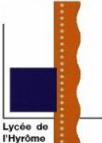
Redémarrer la carte réseau `eth1` avec les commandes `ifdown` et `ifup`.
Observer le fichier `/etc/resolv.conf` qui contient les serveurs DNS de votre machine
Pour que votre serveur DNS soit interrogé en premier, ajouter dans le fichier `/etc/resolvconf/resolv.conf.d/head` la ligne suivante :

```
nameserver 192.168.4.254
```

Redémarrer l'ensemble du réseau avec la commande :

```
sudo /etc/init.d/networking restart
```

Observer le fichier `/etc/resolv.conf` qui contient les serveurs DNS de votre machine

	Lycée de l'Hyrôme - Chemillé	
	Gestion d'un réseau local d'entreprise TP n° 4 Transfert de fichiers et délégation DNS	Réseaux informatiques
BTS IRIS		TP

Dernière manipulation sur SRVLAN :

Modifier le forwarders à 192.168.4.10 au lieu de 172.16.0.1 dans le fichier /etc/bind/named.conf.options
Remplacer virtualux.local par intra.virtualux.fr dans le fichier de configuration du DHCP /etc/dhcp/dhcpd.conf.

a. Tests de l'ensemble sur le client

Le plus simple passe ensuite par le redémarrage de l'ensemble des systèmes (entre autres pour vider le cache DNS). Le principe de résolution devient le suivant pour le client (faire les vérifications sur le client LUbuntu)

Une requête sur intra.virtualux.fr sera traitée par SRVLAN, tout le reste étant dévié sur SRVDMZ.
Une requête sur virtualux.fr sera traitée par SRVDMZ, tout le reste étant dévié sur le DNS externe.

Vérifiez cela à partir du client Ubuntu avec :
La commande dig SOA intra.virtualux.fr qui doit retourner le serveur srvdmz.virtualux.fr dans la section AUTHORITY.
La commande dig SOA virtualux.fr qui doit retourner le serveur srvdmz.virtualux.fr dans la section AUTHORITY.
La commande dig SOA google.fr qui doit retourner le serveur ns1.google.com dans la section AUTHORITY.
Tenter des résolutions pour vos machines.
Avec un navigateur sur le client tenter l'accès à votre serveur web et ftp avec l'URL adéquat.