



**Nas Synology CS 407
et sûrement aussi les autres**

Création : OpenOffice.org Version 2.3

Collecteur : PHI

Création : 18/01/2008:

Version : 118

Modification : 24/03/2008

Fichier : E:\Mes documents\tuto NAS LB\astuces Syno.odt

Imprimer moi en reto/verso !!!!

Table des matières

1.Telnet.....	6
1.1.Installer telnet.....	6
1.2.De-installer telnet.....	6
2.SSH (version synology).....	7
2.1.Installer SSH.....	7
2.2.Dé-installer SSH.....	7
3.IPKG.....	7
3.1.Téléchargement du patch bootstrap sur votre PC.....	7
3.2.Téléchargement du patch bootstrap sur votre Syno.....	7
3.3.Installation.....	8
3.4.Installation d'un paquet.....	9
3.5.Mise à jour les paquets installés sur votre syno.....	10
3.6.Suppression d'un paquet.....	10
3.7.Quelques paquets intéressants.....	10
4.Les ports.....	11
5.Apache.....	13
5.1.Limiter l'accès a un répertoire.....	13
5.2.Ajouter les icônes Apache.....	13
5.3.Ajouter l'option Indexes.....	13
5.4.Et mes logs alors.....	14
5.4.1.Niveaux de LogLevel	14
5.4.2.Fichier httpd.conf-sys.....	15
5.4.2.1.Logformat.....	15
5.4.2.2.LogLevel.....	15
5.4.2.3.Log ERROR.....	15
5.4.2.4.Log ACCES	15
5.4.3.httpd-ssl.conf-sys	16
5.4.4.Fichier httpd.conf-user.....	16
5.4.4.1.Logformat.....	16
5.4.4.2.LogLevel.....	17
5.4.4.3.Log ERROR.....	17
5.4.4.4.Log ACCES	17
5.4.5.httpd-ssl.conf-user	17
5.5.Virtual Hosting	18
5.5.1.préparation (port 80 ouvert et 443 fermé).....	18
5.5.2.préparation (port 443 ouvert et 80 fermé).....	19
5.6.Relance du système apache.....	20
6.La rotation des logs (rédaction en cours).....	21
6.1.Le script.....	21

6.2.Le Cron.....	21
6.3.Autres paramétrages.....	22
7.MySQL.....	23
7.1.Mettre un mot de passe au compte ROOT.....	23
7.2.Créer un utilisateur.....	24
7.3.Accéder aux bases depuis un autre PC sans PHPmyAdmin.....	25
8.Installation.....	28
8.1.Twonkyvision.....	28
8.1.1.sur le NAS:.....	28
8.1.2.sur le PC	28
8.2.La grenouille du net.....	29
8.2.1.Installation de python.....	29
8.2.2.installation.....	29
8.2.3.Decompression de l'archive.....	29
8.2.4.Configuration.....	30
9.Limiter l'accès au syno (redaction en cours).....	32
9.1.Hosts.allows.....	32
9.2.Hosts.deny.....	32
10.Astuces.....	33
10.1.Photostation :.....	33
10.2.Certificat SSL.....	33
10.2.1.Préparation.....	33
10.2.2.génération de la clé d'autorité de certificat (CA).....	34
10.2.3.génération de la demande de signature de certificat (CSR).....	34
10.2.4.signature du certificat.....	34
10.2.5.Génération de la clé du serveur.....	34
10.2.6.Génération de la demande de signature de certificat.....	34
10.2.7.Signature du certificat	35
10.3.Wput.....	35
10.4.Downgrade du syno.....	37
11.Outils.....	39
11.1.Putty.....	39
11.2.Winscp.....	39
11.3.Filezilla.....	39

Documentation sur le NAS Synology CS407.

Toutes les infos ne sont pas de moi, c'est un condensé de mon expérience personnel et de choses glanées sur les forums de synology, de nas forum, et de sites traitant de linux.

Les tests ont été effectués sur un CS407 avec le firmware 571beta

ATTENTION

Aucune garantie de bonne fin

Sauvegardez vos données avant d'effectuer des manipulations critiques

En cas de doutes une question avant de commencer sur

www.nas-forum.com

pourra vous éviter bien des désagrément

1. Telnet

Source : site de synology.

Adresse : <http://www.synology.com/enu/support/download.php>

C'est l'une des première chose à faire pour qui veut bidouiller, et c'est vraiment très bien de la part de Synology de ne pas verrouiller l'accès au NAS

1.1. Installer telnet

Téléchargez le fichier « enabletelnet.zip » sur votre PC et dézippez l'archive.

Allez dans l'interface du syno faites une mise à jour en sélectionnant le fichier EnableTelnet.pat.

Maintenant vous pouvez vous connecter depuis votre PC sur le syno avec un logiciel d'émulation terminal comme Putty

1.2. De-installer telnet

Téléchargez le fichier « disabletelnet.zip » sur votre PC et dézippez l'archive

Allez dans l'interface du syno faites une mise à jour en sélectionnant le fichier DisableTelnet.pat.

Vous ne pouvez plus vous connecter sous telnet

2. SSH (version synology)

Source : site de synology.

Adresse : <http://www.synology.com/enu/support/download.php>

La version fournir par Synology ne permet pas les connexion SFTP. Il faudra la de-installer avant d'installer OpenSSH sur votre NAS

2.1. Installer SSH

Téléchargez le fichier « enableSSH.zip » sur votre PC et dézippez l'archive.

Allez dans l'interface du syno faite une mise à jour en sélectionnant le fichier EnableSSH.pat.

2.2. Dé-installer SSH

Téléchargez le fichier « disableSSH.zip » sur votre PC et dézippez l'archive

Allez dans l'interface du syno faite une mise a jour en sélectionnant le fichier DisableSSH.pat.

3. IPKG

Cette installation est pour le CS407 qui possède un processeur ARM, pour les autres types de processeurs utilisez le bootstap adéquate.

Source : nas-forum.com (ikeke).

Pré-requis : Telnet est installé sur votre syno

Téléchargement du bootstap soit directement sur le syno avec une commande wget, soit sur votre pc puis ensuite par ftp vous mettrez lz fichier dans le repertoire /root du syno.

3.1. Téléchargement du patch bootstrap sur votre PC

Vous trouverez le fichier a cette adresse

http://www.maartendamen.com/synoware/ds_armmarvell-bootstrap_1.0.xsh

puis export par FTP vers le syno dans le répertoire root.

3.2. Téléchargement du patch bootstrap sur votre Syno

Connectez vous avec putty en « root » mot passe est le mdp admin

puis entrez les commandes suivantes :

```
cd /root
```

```
wget http://www.maartendamen.com/synoware/ds_armmarvell-bootstrap_1.0.xsh
```

cela permet d'importer le fichier directement dans le repertoire root

le syno affiche cela en réponse

```
CS407> wget http://www.maartendamen.com/synoware/ds_armmarvell-bootstrap_1.0.xsh
--2008-03-03 08:48:22 -- http://www.maartendamen.com/synoware/ds_armmarvell-
bootstrap_1.0.xsh
Resolving www.maartendamen.com... 84.16.252.187
Connecting to www.maartendamen.com|84.16.252.187|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7796680 (7.4M) [text/plain]
Saving to: `ds_armmarvell-bootstrap_1.0.xsh'

100%[=====>] 7,796,680  839K/s  in 10s

2008-03-03 08:48:33 (738 KB/s) - `ds_armmarvell-bootstrap_1.0.xsh' saved [779668
0/7796680]
```

Le fichier se trouve dans le répertoire /root du syno.

3.3. Installation

entrez la commande suivante:

```
sh /root/ds_armmarvell-bootstrap_1.0.xsh
```

le syno va effectuer l'exécution et afficher les messages suivants :

```
DS-107+/DS-207+/CS-407/RS-407-bootstrap extracting archive... please wait
bootstrap
bootstrap/wget-ssl.ipk
bootstrap/bootstrap.ipk
bootstrap/openssl.ipk
bootstrap/ipkg.sh
bootstrap/ipkg.ipk
38218+1 records in
38218+1 records out
bootstrap/bootstrap.sh
Creating temporary ipkg repository... success
Installing DS-107+/DS-207+/CS-407/RS-407-bootstrap package...Unpacking bootstrap.ipk...Done.
Configuring bootstrap.ipk...
Adding /opt/lib to dynamic linker configuration...
Regenerating dynamic linker cache...
Modifying /etc/profile...
Modifying /etc/rc.local
Done.
success
Installing IPKG package... (Ignore missing md5sum warning)
Unpacking ipkg.ipk...Done.
Configuring ipkg.ipk.../ipkg.sh: ./ipkg.sh: 1170: md5sum: not found
Done.
Removing temporary ipkg repository...
Installing OpenSSL..Installing openssl (0.9.7m-3) to root...
Configuring openssl
Successfully terminated.
success
```



```
Installing wget-SSL...Installing wget-ssl (1.10.2-4) to root...
Configuring wget-ssl
Successfully terminated.
success
Setup complete...
If your network setup is correct, you should be able to do "ipkg update" to get the
full list of installable packages
```

Puis entrer la commande suivante qui permet de lancer l'éditeur VI et d'ouvrir le fichier ipkg.conf

```
vi /opt/etc/ipkg.conf
```

remplacez la ligne

```
src synoware http://www.maartendamen.com/synoware
```

par

```
src synoware http://ipkg.nslu2-linux.org/feeds/optware/syno-x07/cross/unstable
```

sauvegardez le fichier (: w) et quitter (: q)

Maintenant on met à jour la liste des packages disponibles en tapant

```
ipkg update
```

la commande affiche cela

```
CS407> ipkg update
Downloading http://ipkg.nslu2-linux.org/feeds/optware/syno-x07/cross/unstable/Packages
Updated list of available packages in /usr/lib/ipkg/lists/synoware
Successfully terminated.
```

on crée le répertoire init.d qui sera nécessaire pour certains packages:

```
mkdir /opt/etc/init.d
```

Maintenant vous pouvez charger/installer/exécuter des applications sur votre syno.

3.4. Installation d'un paquet

Pour les allergiques a VI je vous conseil l'installation de nano

```
ipkg install nano
```

C'est un éditeur de texte plus facile à utiliser.

```
CS407> ipkg install nano
Installing nano (2.0.7-1) to root...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/syno-x07/cross/unstable/nano_2.0.7-1_arm.ipk
Installing ncurses (5.6-3) to root...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/syno-x07/cross/unstable/ncurses_5.6-3_arm.ipk
Configuring nano
```

```
Configuring ncurses
update-alternatives: Linking //opt/bin/clear to /opt/bin/ncurses-clear
Successfully terminated.
CS407>
```

3.5. Mise à jour les paquets installés sur votre syno.

```
ipkg upgrade
```

ici aucune mise à jour a été trouvé

```
CS407> ipkg upgrade
Nothing to be done
Successfully terminated.
```

3.6. Suppression d'un paquet

Par exemple désinstaller nano

```
ipkg remove nano
```

3.7. Quelques paquets intéressants

Installation de python, openssh (si le patch ssh synology est installé pensé a le deinstaller avant), logrotate, et bien d'autres

La liste des paquets disponible se trouve là :

<http://ipkg.nslu2-linux.org/feeds/optware/syno-x07/cross/unstable/Packages>

3.8. Le fichier rc.local

L'installation d'IPKG rajoute automatiquement au fichier rc.local les lignes suivantes :

```
#!/bin/sh

# Optware setup
mkdir -p /opt
[ -e /volume1/opt ] && mount -o bind /volume1/opt /opt
[ -x /opt/etc/rc.optware ] && /opt/etc/rc.optware
[ -e /bin/killall ] || ln -s /bin/busybox /bin/killall
#
```

4. Les ports

Source : http://www.synology.com/enu/support/help-page.php?q_id=299

Liste des ports utilisés par le Nas, et ses outils.

Type	Port Number	Protocol
------	-------------	----------

Setup Utilities

Synology Assistant, DSAssistant	9999, 9998, 9997	UDP
---------------------------------	------------------	-----

Backup

Data Replicator, Data Replicator II	9999, 9998, 9997, 137, 138, 139, 445	TCP
Network Backup	873	TCP
Encrypted Network Backup	873, 22	TCP

Download

Download Redirector	9999, 9998, 9997, 5432	UDP/TCP
Download Management (Web Download Manager)	5000	TCP

The following ports are suggested to open for speeding up data transferring. 6890 ~ 6999 (for models with firmware earlier than v2.0.1-3.0401); 6881 ~ 6890 (for models with firmware v2.0.1-3.0401 and onward)

Web Application

HTTP	80, 5000	TCP
HTTPS	443, 5001	TCP
Photo Station, Web Station	80 (additional port can be added)	TCP
Audio Station, File Station	5000	TCP

File Transferring

FTP, FTP over SSL FTP over TLS	21 (command), 20 (Data in Active Mode), 55536-56559 (Data in Passive Mode)	TCP
AFP	548	TCP
CIFS	smbd: 139 (netbios-ssn), 445 (microsoft-ds)	TCP/UDP
	Nmbd: 137, 138	UDP

Listes des ports à ouvrir pour accéder à votre syno depuis l'Internet. Tous ces ports sont à ouvrir dans votre box internet et/ou votre routeur en fonction de vos besoins et du paramétrage de votre syno

- Si HTTPS est coché dans le syno
→ Ouvrir le port 5001 TCP pour accéder à l'interface syno

ex : httpS://.....dyndns.org:5001/

→ Ouvrir le port 443 TCP (service https) pour accéder au serveur WEB

ex : httpS://.....dyndns.org/photo

- Si HTTPS n'est pas coché dans le syno
 - Ouvrir le port 80 TCP (service http) pour accéder au serveur WEB
 - ex : http://.....dyndns.org/photo/
 - Ouvrir le port 5000 TCP pour accéder à l'interface syno
 - ex : http://.....dyndns.org:5000/
- Si le service FTP est activé :
 - Ouvrir le port 21 TCP.
 - ouvrir le port 20 TCP.
 - ouvrir les ports 55536 - 56559 TCP (mode passif)

5. Apache

5.1. Limiter l'accès a un répertoire

Source : (phi)

Synopsis : Limiter l'accès à un répertoire aux seules machines d'un réseau

Dans le fichier httpd.conf-user

```
<Directory "/var/services/web/test">
#
Options MultiViews
#
AllowOverride All
#
Order allow,deny
Allow from 192.168.1.
</Directory>
```

cela permet donc de limiter l'accès aux seuls machines ayant une IP comprise dans le masque 192.168.1. au répertoire test.

URL suivante 192.168.1.2/test/ affichera le contenu, mais l'URL suivante <http://mondomaine.com/test/> se soldera par un échec.

5.2. Ajouter les icônes Apache

Source : (phi)

Synopsis : le fichier httpd-autoindex.conf-user ou sys définit l'alias du répertoire contenant les icônes Apache, mais ce répertoire est inexistant dans le syno.

Dans le répertoire /usr/syno/apache créer un répertoire icons

puis récupérer le pack d'icônes apache à cette adresse et transférer le contenu dans le répertoire icons du syno.

<http://www.apache.org/icons/> sont les icônes officielles

5.3. Ajouter l'option Indexes

Source : (phi)

Synopsis : le répertoire ne contient pas de fichier index.

Vous avez créé un répertoire à accès limité pour vos développements HTML mais pour pouvoir voir le contenu du répertoire, si il n'y a pas de fichier index le syno vous répond désolé pas de fichier.

Pour palier à cela reprenons notre exemple du chapitre 5.1 :

```
<Directory "/var/services/web/test">
#
Options Indexes MultiViews
#
AllowOverride All
#
Order allow,deny
Allow from 192.168.1.
</Directory>
```

j'ai rajouté l'option Indexes à la directive Options.

Maintenant lorsque j'entre l'URL suivante dans mon navigateur 192.168.1.2/test/ si il n'y a pas de fichier index alors j'ai une jolie liste du contenu de mon répertoire avec des icônes

5.4. Et mes logs alors

Synopsis : je veux voir mes logs apache. Nous verrons dans le chapitre suivante comment automatiser la sauvegarde des log.

Source : nas-forum.com (Chéri², phi)

5.4.1. Niveaux de LogLevel

Voici les différents niveaux de compte-rendu d'apache

debug sera très bavard et générera rapidement de très gros fichiers.

Attention donc au niveau que vous allez choisir.

Nom	Types d'erreur
emerg	Urgence, serveur Web inutilisable
alert	Alertes, réaction immédiate requise
crit	Conditions critiques
error	Conditions d'erreur
warn	Conditions d'avertissement
notice	Conditions normales mais significatives
info	Informations
debug	Messages de débogage (tout est indiqué)

5.4.2. Fichier httpd.conf-sys

Ce fichier se trouve dans le répertoire /usr/syno/apache/conf

5.4.2.1. **Logformat**

Modification du format du log

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""  
combined
```

par

```
LogFormat "%h %l %u %t [%{SSL_PROTOCOL}x %{SSL_CIPHER}x]-[%r]-  
[%>s %b]-[%{Referer}i]-[%{User-Agent}i]" combined
```

5.4.2.2. **LogLevel**

Afin de ne pas avoir un fichier httpd-error-sys.log qui explose en taille je vous conseil de passer le niveau de log à info voir a notice

remplacez

```
LogLevel debug
```

par

```
LogLevel info
```

5.4.2.3. **Log ERROR**

Pour le log ERROR pas de problème, il faut supprimer le commentaire

```
#ErrorLog /var/log/httpd-sys.log
```

personnellement je l'ai remplacé par cela

```
ErrorLog /var/log/httpd-error-sys.log
```

puis remplacer la ligne

```
ErrorLog /dev/null
```

par

```
#ErrorLog /dev/null
```

Attention le fichier se remplit très vite et va devenir très gros, je tords le cou à ce problème un peu plus loin.

5.4.2.4. **Log ACCES**

Pour le log ACCES il faut supprimer le commentaire

```
#CustomLog /usr/syno/apache/logs/access_log combined
```

personnellement je l'ai remplacé par cela

```
CustomLog /var/log/httpd-access-sys.log combined
```

puis remplacer la ligne

```
CustomLog /dev/null common
```

par

```
# CustomLog /dev/null common
```

Mais si vous utilisez seulement les connexions en https sur le port 5001 ben y a comme un problème votre fichier httpd-access-sys.log ne se remplit pas donc si vraiment vous voulez tout tracer il faut aller modifier le fichier httpd-ssl.conf-sys se trouvant de le répertoire extra.

5.4.3. httpd-ssl.conf-sys

Ce fichier se trouve dans le répertoire /usr/syno/apache/conf/extra

Remplacer

```
CustomLog /dev/null \  
    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
```

par

```
#CustomLog /dev/null \  
#    "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
```

puis jouter la ligne à la suite

```
CustomLog /var/log/httpd-access-sys.log combined
```

5.4.4. Fichier httpd.conf-user

Ce fichier se trouve dans le répertoire /usr/syno/apache/conf

5.4.4.1. **Logformat**

Modification du format du log

```
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""  
combined
```

par

```
LogFormat "%h %l %u %t [%{SSL_PROTOCOL}x %{SSL_CIPHER}x-[%r]-  
[%>s %b]-[%{Referer}i]-[%{User-Agent}i]" combined
```


5.4.4.2. *LogLevel*

Afin de ne pas avoir un fichier httpd-error-user.log qui explose en place je vous conseil de passer le niveau de log à info voir à notice

remplacez

```
LogLevel debug
```

par

```
LogLevel info
```

5.4.4.3. *Log ERROR*

Pour le log ERROR pas de problème, il faut supprimer le commentaire

```
#ErrorLog /var/log/httpd-user.log
```

personnellement je l'ai remplacé par cela

```
ErrorLog /var/log/httpd-error-user.log
```

puis remplacer la ligne

```
ErrorLog /dev/null
```

par

```
#ErrorLog /dev/null
```

5.4.4.4. *Log ACCES*

Pour le log ACCES il faut supprimer le commentaire

```
#CustomLog /usr/syno/apache/logs/access_log combined
```

personnellement je l'ai remplacé par cela

```
CustomLog /var/log/httpd-access-user.log combined
```

puis remplacer la ligne

```
CustomLog /dev/null common
```

par

```
# CustomLog /dev/null common
```

5.4.5. httpd-ssl.conf-user

se trouvant de le répertoire /usr/syno/apache/conf/extra

Remplacer

```
CustomLog /dev/null \
```

```
"%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
```

par

```
#CustomLog /dev/null \  
# "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
```

puis jouter la ligne à la suite

```
CustomLog /var/log/httpd-access-user.log combined
```

5.5. Virtual Hosting

Synopsis: Je souhaite que mon syno réponde à deux (trois...) nom de domaine différent. j'ai un nom de domaine chez dyndns et chez no-ip.

Il y a deux versions, une avec le port 80 (http) seulement ouvert et l'autre avec seulement le port 443 (https)

Source : nas-forum.com (Ikeke)

5.5.1. préparation (port 80 ouvert et 443 fermé)

Création des répertoires devant recevoir les deux sites:

```
mkdir /volume1/web/no-ip  
mkdir /volume1/web/dyndns
```

Puis comme vous avez tous maintenant installé IPKG et nano ouvrez le fichier httpd.conf-user

```
nano /usr/syno/apache/conf/httpd.conf-user
```

rechercher

```
# Virtual hosts  
#Include conf/extra/httpd-vhosts.conf
```

et remplacez par

```
# Virtual hosts  
Include conf/extra/httpd-vhosts.conf-user
```

sauvegardez.

Donc lorsque apache user sera exécuté il cherchera le fichier httpd-vhosts.conf-user dans lequel nous allons mettre nos paramètres.

Toujours avec nano la commande

```
nano /usr/syno/apache/conf/extra/httpd-vhosts.conf-user
```

ouvre l'éditeur, puis

entrez le texte suivant (remplacez 192.168.1.2 pa l'IP local de votre syno)

```
NameVirtualHost 192.168.1.2:80

<VirtualHost 192.168.1.2:80 >
  DocumentRoot "/var/services/web/dyndns"
  <Directory "/var/services/web/dyndns">
    Options none
    Order allow,deny
    Allow from all
  </Directory>
  ServerName domaine-dyndns.com
</VirtualHost>

<VirtualHost 192.168.1.2:80 >
  DocumentRoot "/var/services/web/no-ip"
  <Directory "/var/services/web/no-ip">
    Options Indexes
    Order allow,deny
    Allow from all
  </Directory>
  ServerName domaine.no-ip.com
</VirtualHost>
```

savegardez et relancer apache user

```
/usr/syno/etc/rc.d/S97apache-user.sh restart
```

En fonction de vos besoin vous pouvez définir une adresse mel différente pour chacun des sites, définir des pages erreurs différentes...

5.5.2. préparation (port 443 ouvert et 80 fermé)

Création des répertoires devant recevoir les deux sites:

```
mkdir /volume1/web/no-ip
mkdir /volume1/web/dyndns
```

Puis comme vous avez tous maintenant installé IPKG et nano ouvrez le fichier httpd-ssl.conf-user

```
nano /usr/syno/apache/conf/extra/httpd-ssl.conf-user
```

recherchez le texte

```
<VirtualHost *:443>
```

et insérez la ligne suivante au dessus

```
NameVirtualHost *:443
```

puis à la fin du fichier entrez le texte suivant

```
<VirtualHost *:443>
  DocumentRoot "/var/services/web/dyndns"
  <Directory "/var/services/web/dyndns">
    Options none
    Order allow,deny
    Allow from all
  </Directory>
  ServerName domaine-dyndns.com
</VirtualHost>

<VirtualHost *:443 >
  DocumentRoot "/var/services/web/no-ip"
  <Directory "/var/services/web/no-ip">
    Options Indexes
    Order allow,deny
    Allow from all
  </Directory>
  ServerName domaine.no-ip.com
</VirtualHost>
```

sauvegardez et relancer apache user

```
/usr/syno/etc/rc.d/S97apache-user.sh restart
```

Si vous voulez tout ouvrir (80 et 443) appliquer les 2 chapitres

Nota : j'ai appliqué la deuxième solution mon routeur ne laissant passer que les ports 5001 et 443

5.6. Relance du système apache

Dans une fenêtre TELNET, pour apache root

```
/usr/syno/etc/rc.d/S97apache-sys.sh restart
```

puis pour apache user

```
/usr/syno/etc/rc.d/S97apache-user.sh restart
```

6. La rotation des logs (rédaction en cours)

Source : (phi)

Pré-requis : Bootstrap IPKG installé, Paquet Logrotate installé.

Je suppose que vous n'allez pas tous les jours sauvegarder vos logs, ou voir si le fichier ne devient pas monstrueusement gros.

En plus je pense que garder 1 an de log cela ne va pas le faire.

Donc nous allons installer logrotate afin que le système garde les logs sur une certaine durée et remplace les plus vieux.

Dans une fenêtre TELNET:

```
ipkg install logrotate
```

6.1. Le script

Allez dans le répertoire logrotate.d

```
cd /opt/etc/logrotate.d
```

ou si le répertoire n'existe pas

```
mkdir /opt/etc/logrotate.d
```

avec nano

```
nano /opt/etc/logrotate.d/apache.rotate
```

entrez le texte suivante

```
compress
/var/log/httpd-error-sys.log {
    rotate 10
    postrotate
        /sbin/killall -HUP httpd
    endscript
}
```

puis sauvegardez

ATTENTION EN COURS DE REDACTION et TEST

6.2. Le Cron

Ouvrir le fichier /etc/crontab avec nano

```
nano /etc/crontab
```

puis rajouter cette ligne

ATTENTION EN COURS DE REDACTION et TEST

6.3. Autres paramétrages

A venir

7. MySQL

Source : le site de Mysql et phi.

7.1. Mettre un mot de passe au compte ROOT

Par défaut le compte « ROOT » de MySQL ne comporte pas de mot de passe. Si PHPMyAdmin est installé nous allons sécuriser ce compte en lui mettant un mot de passe.

Lorsque vous êtes sur la page accueil de PHPMyAdmin cliquer  [Privilèges](#)

puis sélectionner « root » et cliquer sur 

<input checked="" type="checkbox"/>	root	localhost	Non	ALL PRIVILEGES	Oui	
-------------------------------------	------	-----------	-----	----------------	-----	---

entrer le mot de passe

Modifier le mot de passe

aucun mot de passe

Mot de passe: Entrer à nouveau:

Hachage du mot de passe: MySQL 4.1+
 compatible MySQL 4.0

cliquer sur exécuter

Lorsque vous retourner sur la page d'accueil PHPMyAdmin vous met un joli message d'erreur, pas de panique c'est normal.

Ouvrer le fichier « config.inc.php » ou « config.default.php » puis rechercher la ligne :

```
$cfg['Servers'][$i]['password'] = '';
```

ajouter votre mot de passe entre les cotes.

Maintenant le compte « root » possède son mot de passe.

Pour vérifier ouvrir une session telnet avec Putty puis

```
/usr/syno/mysql/bin/mysql -u root vous envoi un joli message d'erreur.
```

```
/usr/syno/mysql/bin/mysql -u root -p vous demande votre mdp
```

7.2. Créer un utilisateur

Source : phi

Si vous devez ouvrir votre serveur avec utilisation de Mysql au monde, créer un utilisateur avec des droits restreints qu'à la base sur laquelle il fera ses requêtes.

Ainsi si vous avez 4 sites qui tournent sur votre syno qui utilisent 4 bases différentes, créez 4 utilisateurs différents, un accès unique à une base.

Lorsque vous êtes sur la page accueil de PHPMyAdmin cliquez sur



Privilèges

Puis cliquez sur

puis remplissez

Information pour la connexion	
Nom d'utilisateur:	Entrez une valeur: <input type="text"/>
Serveur:	Tout serveur <input type="text"/>
Mot de passe:	Entrez une valeur: <input type="text"/>
Entrer à nouveau:	<input type="text"/>
Générer un mot de pas	<input type="button" value="Générer"/> <input type="button" value="Copier"/> <input type="text"/>

Nom d'utilisateur:
Serveur: localhost
Mot de passe:
Entrer à nouveau:

et c'est tout pour l'instant, cliquez sur le bouton exécuter en bas de la page.

La page concernant l'utilisateur s'ouvre, nous allons maintenant lui définir des droits seulement pour une base.

Ne cochez rien dans la zone paramètres globaux

ici sélectionnez la base sur laquelle l'utilisateur aura tous les droits

Privileges spécifiques à une base de données

Base de données Privileges "Grant" Privileges spécifiques à une table Action

aucune

Ajouter des privilèges sur cette base de données: Entrez une valeur: [valeur] [!]

Exécuter

Une nouvelle page s'ouvre

Privileges spécifiques à une base de données (Tout cocher / Tout décocher)

Veillez noter que les noms de privilèges sont exprimés en anglais

Données

- SELECT
- INSERT
- UPDATE
- DELETE

Structure

- CREATE
- ALTER
- INDEX
- DROP
- CREATE TEMPORARY TABLES
- CREATE VIEW
- SHOW VIEW
- CREATE ROUTINE
- ALTER ROUTINE
- EXECUTE

Administration

- GRANT
- LOCK TABLES
- REFERENCES

Exécuter

cliquez sur « tout cocher »

puis bouton exécuter

Vous avez donc un utilisateur qui a accès qu'à une seule base sur laquelle il a tous les droits.

C'est donc cette utilisateur que vous utiliserez dans vos scripts PHP pour la connexion a votre base.

7.3. Accéder aux bases depuis un autre PC sans PHPmyAdmin

Synopsis: Je veux créer un utilisateur itinérant ayant des droits administrateur sur tout.

Vous souhaitez faire des sauvegardes, ou l'administration depuis un Pc sur

votre réseau ou depuis internet, permettre l'accès à votre connecteur ODBC sur votre syno.

Créer un utilisateur avec des droits plus ou moins restreints. Cela dépendra de vos besoins et du niveau de sécurité que vous accordez à votre base.

Reprenons l'exemple de création d'un utilisateur :

C'est ici que vous permettrez la connexion à Mysql depuis un client.

Information pour la connexion

Nom d'utilisateur: Entrez une valeur: [dropdown] [input]

Serveur: Tout serveur [dropdown] [input]

Mot de passe: Entrez une valeur: [dropdown] [input]

Entrer à nouveau: [input]

Générer un mot de pas [Générer] [Copier] [input]

Pour le nom d'utilisateur je vous propose de ne pas utiliser admin, administrateur, root.

Pour serveur mettre %

puis le mot de passe, ici forcez vous à un mdp compliqué ou moins générer le mais surtout ne l'oubliez pas.

Ensuite

Privileges globaux (Tout cocher / Tout décocher)

Veuillez noter que les noms de privilèges sont exprimés en anglais

Données <ul style="list-style-type: none"><input type="checkbox"/> SELECT<input type="checkbox"/> INSERT<input type="checkbox"/> UPDATE<input type="checkbox"/> DELETE<input type="checkbox"/> FILE	Structure <ul style="list-style-type: none"><input type="checkbox"/> CREATE<input type="checkbox"/> ALTER<input type="checkbox"/> INDEX<input type="checkbox"/> DROP<input type="checkbox"/> CREATE TEMPORARY TABLES<input type="checkbox"/> CREATE VIEW<input type="checkbox"/> SHOW VIEW<input type="checkbox"/> CREATE ROUTINE<input type="checkbox"/> ALTER ROUTINE<input type="checkbox"/> EXECUTE	Administration <ul style="list-style-type: none"><input type="checkbox"/> GRANT<input type="checkbox"/> SUPER<input type="checkbox"/> PROCESS<input type="checkbox"/> RELOAD<input type="checkbox"/> SHUTDOWN<input type="checkbox"/> SHOW DATABASES<input type="checkbox"/> LOCK TABLES<input type="checkbox"/> REFERENCES<input type="checkbox"/> REPLICATION CLIENT<input type="checkbox"/> REPLICATION SLAVE<input type="checkbox"/> CREATE USER	Limites de ressources. <p><i>Note: Une valeur de 0 (zero) enlève la limite.</i></p> <p>MAX QUERIES PER HOUR [input]</p> <p>MAX UPDATES PER HOUR [input]</p> <p>MAX CONNECTIONS PER HOUR [input]</p> <p>MAX USER_CONNECTIONS [input]</p>
--	---	---	--

Exécuter

cliquez sur « tout cocher »

Vous venez de créer un utilisateur aillant tous les droits et pouvant se connecter depuis n'importe quel PC

Personnellement je trouve cela très dangereux surtout si vous avez des

chose importantes dans vos bases, on peut tout simplement vous kicker de votre base ou simplement créer un utilisateur silencieux.

C'est pour cela que je vous conseil de créer des utilisateurs en fonction de vos besoins réels en limitant leurs droits au strict nécessaire.

Outils Mysql pour l'administration depuis un poste extérieur pour win/osX/linux.

<http://dev.mysql.com/downloads/gui-tools/5.0.html>

8. Installation

8.1. Twonkyvision

Source : nas-forum.com, mes tests.

téléchargement ici :

<http://www.twonkyvision.de/Download/TwonkyMedia/TM4Technicians.html>

8.1.1. sur le NAS:

création d'un répertoire public dans volume1 et d'un répertoire twonkyvision dans public

avec telnet

```
mkdir /volume1/public/twookyvision
```

si le répertoire /volume1/public/twonkyvision n'existe pas l'utilitaire d'installation ne le crée pas. (enfin c'est comme cela que cela c'est passé chez moi)

Le fichier rc.local est modifié lors de l'installation de twonkyvision faire une copie de /etc/rc.local sur le PC local avec winscp ou avec Telnet

```
cp /etc/rc.local /volume1/public/rc.local.avant
```

8.1.2. sur le PC

extraction de l'archive

exécution de nassetup.exe

entrer IP du syno

entrer le mot de passe root

cliquer sur continue

à la fin du script exit

Sur le nas ouvrir etc/rc.local

y rajouter les lignes supprimées par l'installation de twonky du fichier sauvegardé sur le PC (important surtout si install IPKG)

puis dans un navigateur

<http://ipsyno:9000/configpage/index.html>

first step language -> français

bouton enregistrer les modifications

puis bouton redémarrer le serveur, ensuite gestion des partages.....

8.2. La grenouille du net.(A modifier)

Sources : phi

Synopsis : le syno étant en fonction, pourquoi ne pas l'utiliser pour faire remonter les infos de la ligne ADSL à la grenouille.com

téléchargement :

Pré-requis : IPKG, Python avoir un compte sur le site grenouille.com.

8.2.1. Installation de python

connexion au syno en root par une session telnet, puis

```
ipkg install python
```

8.2.2. installation

connexion au syno en root par une session telnet, puis se mettre a la racine

```
cd /
```

Telechargement de l'archive que j'ai préparé

```
wget http://pagesperso-orange.fr/cest-ici/pygmod.tar.gz
```

Le resultat

```
CS407> wget http://pagesperso-orange.fr/cest-ici/pygmod.tar.gz
--18:24:41-- http://pagesperso-orange.fr/cest-ici/pygmod.tar.gz
=> `pygmod.tar.gz'
Resolving pagesperso-orange.fr... 193.252.122.52
Connecting to pagesperso-orange.fr[193.252.122.52]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 92,643 (90K) [application/x-tar]

100%[=====>] 92,643 337.65K/s

18:24:43 (336.47 KB/s) - `pygmod.tar.gz' saved [92643/92643]

CS407>
```

8.2.3. Décompression de l'archive

```
tar zxvf pygmod.tar.gz
```

le fait d'etre à la racine met les fichiers dans les bons repertoires

```
CS407> tar zxvf pygmod.tar.gz
opt/etc/init.d/S99gre.sh
opt/etc/init.d
opt/etc
```

```

root/pyg/libs/fullconfigobj.pyc
root/pyg/libs/ping.py
root/pyg/libs/timeoutsocket.pyc
root/pyg/libs/fullconfigobj.py
root/pyg/libs/__init__.py
root/pyg/libs/__init__.pyc
root/pyg/libs/timeoutsocket.py
root/pyg/libs/ping.pyc
root/pyg/po/Makefile
root/pyg/po/pygrenouille.pot
root/pyg/po/pygettext.py
root/pyg/po/POTFILES.in
root/pyg/docs/versions.txt
root/pyg/docs/mod.txt
root/pyg/docs/grenouille.url
root/pyg/docs/gpl.txt
root/pyg/docs/install-linux-terminal.txt
root/pyg/contrib/linux2/trafic/trafic.py
root/pyg/contrib/linux2/trafic
root/pyg/contrib/linux2
root/pyg/contrib/template.asc
root/pyg/libs
root/pyg/logs
root/pyg/po
root/pyg/docs
root/pyg/contrib
root/pyg/lisezmoi
root/pyg/pygmod.py
root/pyg
CS407>

```

8.2.4. Configuration

Application des droits

```

chmod +x /root/pyg/pygmod.py
chmod +x /root/pyg/contrib/linux2/trafic/trafic.py
chmod +x /opt/etc/init.d/S99gre.sh

```

puis lancer **une première fois**

```
python /root/pyg/pygmod.py
```

pour remplir le fichier de configuration

```

CS407> python /root/pyg/pygmod.py
#####
# Demarrage de la grenouille
# Demarrage le 2008-03-16
# version 1.13b5 Mod synology
# Repertoire de travail : /root/pyg
#####
Starting pygrenouille v1.13 b5
platform: linux2
version de python: (2, 4, 5, 'final', 0)
version complete de python: 2.4.5 (#1, Mar 12 2008, 21:15:53)
[GCC 3.4.3 (CSL 2005Q1B) (Marvell 2006Q3)]
version de l'API: 1012

```

```
--- Pas de pygrenouille.conf ---  
pygrenouille.conf n'est pas accessible!
```

Vous devez creer le fichier de configuration de pyGrenouille
Ce wizard va vous aider a creer un fichier de configuration simple
Merci de repondre aux questions suivantes

utilisateur Grenouille? **Votre user grenouille**
Mot de passe? **Votre mot de passe grenouille**
Merci de confirmer votre Mot de passe? **Votre mot de passe grenouille**

```
Le fichier de configuration est ecrit.  
Vous pouvez maintenant lancer pyGrenouille.  
CS407>
```

renseignez le user et le mot de passe créer sur la grenouille.com

Maintenant soit

```
Reboot
```

ou

```
sh /opt/etc/init.d/S99gre.sh
```

ensuite sous telnet un

```
ps | grep -v grep | grep 'python'
```

pour voir si c'est bien démarré.

```
CS407> ps | grep -v grep | grep 'python'  
3046 root 17348 S /opt/bin/python /root/pyg/pygmod.py  
CS407>
```

Vous pouvez déplacer le fichier pygmod.tar.gz pour le sauvegarder dans vos archives.

Voilà c'est tout

- 1) la grenouille démarre en tache de fond
- 2) vos logs sur le résultats de connexion sont dans /root/pyg/logs/
- 3) le log de fonctionnement pygre.log est dans /var/log/

Mise a jour du 22 mars 2008

Le script de démarrage accepte maintenant les paramètres : start, stop, restart.

9. limiter l'accès au syno (redaction en cours)

Synopsis : je veux filtrer les accès a mon syno.

Source : nas-forum.com; ubuntu-fr.com; (phi)

9.1. Hosts.allows

A venir

9.2. Hosts.deny

A venir

10. Astuces

10.1. Photostation :

Source : nas-forum.com (phi)

Vous avez ce message d'erreur lorsque vous essayez de vous connecter à photostation

Warning: pg_connect() [function.pg-connect]: Unable to connect to PostgreSQL server: FATAL: could not open file "/volume1/@database/pgsql/global/1262": No such file or directory in /usr/syno/synoman/phpsrc/photo/include/database.php on line 15
Failed to connect

La base Postgres de photostation est corrompu.

Solution possible

- 1) arrêt de photostation par l'interface syno.
- 2) renommer le répertoire photo en oldphoto par exemple, ou le supprimer si tout est sauvegardé
- 3) reboote du syno
- 4) redémarrer photostation, le syno recréer un répertoire photo vide
- 5) y remettre quelques photos (une dizaine pour tester) - indexation
- 6) faire un test de connexion sur l'interface photostation.

10.2. Certificat SSL

Synopsis : installer un certificat SSL valide pour éviter lors l'accès sécurisé (https) à votre serveur la fenêtre d'avertissement.

source : nas-forum.com (pipobek);

http://www.synology.com/wiki/index.php/How_to_generate_custom_SSL_certificates

Pré-requis : SSL activé (firmware 0462 et au-delà.)

10.2.1. Préparation

Téléchargez le fichier openssl.cnf

<http://www.gateway-1.homedns.org/synology/openssl.cnf>

Avec FTP placer le dans le répertoire /volume1/public par exemple.

Relevez l'adresse MAC et le nom de votre serveur.

Ensuite toutes les opérations se passent sous telnet en root

Créez, s'il n'existe pas, le répertoire /usr/syno/ssl

```
mkdir /usr/syno/ssl
```

Copiez le fichier openssl.cnf dans le répertoire /usr/syno/ssl

```
cp /volume1/public/openssl.cnf /usr/syno/ssl/openssl.cnf
```

Faire une copie de sauvegarde du répertoire /usr/syno/etc/ssl/

```
cp -r /usr/syno/etc/ssl /volume1/save_ssl
```

Maintenant, il faut procéder à la création des clés et certificats.

Allez dans le répertoire usr/syno/ssl

```
cd /usr/syno/ssl
```

10.2.2. génération de la clé d'autorité de certificat (CA)

Cryptage sur 1024 bits (ne pas modifier)

```
openssl genrsa -out ca.key 1024
```

j'ai volontairement omis l'attribut « -des3 » qui sert à créer une phrase de passe.

10.2.3. génération de la demande de signature de certificat (CSR)

```
openssl req -new -key ca.key -out ca.csr
```

ATTENTION : des champs à renseigner vont vous être proposés, vous pouvez mettre n'importe quoi mais notez vos réponses.

Le seul point important est **Common Name** : à renseigner avec le nom du syno et l'adresse MAC de la manière suivante *nomdusyno adressemac* (séparés par un espace et sans les points), ex : CS407 01010101CA01

10.2.4. signature du certificat

```
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
```

10.2.5. Génération de la clé du serveur

```
openssl genrsa -out server.key 1024
```

j'ai volontairement omis l'attribut « -des3 » qui sert à créer une phrase de passe.

10.2.6. Génération de la demande de signature de certificat

```
openssl req -new -key server.key -out server.csr
```

ATTENTION : cette fois Common Name doit-être renseigné avec votre nom

de domaine, ex : www.titi.fr ou titi.dyndns.org. Mettre les mêmes réponses que précédemment.

Sachant que si vous en utilisez plusieurs, il faudra faire un choix réfléchi....

10.2.7. Signature du certificat

avec la clé d'autorité créée au 7.2.2

```
openssl x509 -req -days 365 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01
-out server.crt
```

Pour terminer, on fait en sorte qu'Apache ne demande pas systématiquement un mot de passe à chaque démarrage en créant une clé non sécurisé.

Cette clé doit être stockée en lieu sûr, car elle contient toutes les données de cryptage des transmissions

```
openssl rsa -in server.key -out server.key.insecure
mv server.key server.key.secure
mv server.key.insecure server.key
```

Il ne reste plus qu'à remplacer les fichiers et à rebooter le syno

```
mv /usr/syno/ssl/*.crt /usr/syno/etc/ssl/ssl.crt
mv /usr/syno/ssl/*.csr /usr/syno/etc/ssl/ssl.csr
mv /usr/syno/ssl/*.key /usr/syno/etc/ssl/ssl.key
reboot
```

10.3. Wput

Synopsis : je veux envoyer des fichiers d'un syno vers un serveur ftp.

Source : phi , <http://doc.ubuntu-fr.org/wput>, <http://wput.sourceforge.net/>.

Pré requis : `ipkg`

En premier lieu nous allons installer Wput grace à IPKG,
connexion au syno en root par une session telnet, puis

```
ipkg install wput
```

ce qui donne

```
CS407> ipkg install wput
Installing wput (0.6.1-1) to root...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/...0.6.1-1\_arm.ipk
Installing gnutls (1.6.3-1) to root...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/...1.6.3-1\_arm.ipk
Installing libtasn1 (0.3.10-1) to root...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/...3.10-1\_arm.ipk
Installing libgcrypt (1.2.4-1) to root...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/...1.2.4-1\_arm.ipk
Installing libgpg-error (1.4-1) to root...
```

```
Downloading http://ipkg.nslu2-linux.org/feeds/optware/...r\_1.4-1\_arm.ipk
Installing zlib (1.2.3-2) to root...
Downloading http://ipkg.nslu2-linux.org/feeds/optware/...1.2.3-2\_arm.ipk
Configuring gnutls
Configuring libgcrypt
Configuring libgpg-error
Configuring libtasn1
Configuring wput
Configuring zlib
Successfully terminated.
```

puis la ligne de commande suivante

```
wput -v /volume1/temp/toto ftp://user:pass@mondomaine/ >> /var/log/wput.log
```

à pour effet d'envoyer le fichier toto vers le serveur FTP mondomaine

Nota : le chemin sera reconstruit à l'identique , on retrouvera /volume1/temp du coté réception.

-v c'est pour que la commande vous parle, et >> /var/log/wput.log contiendra sa prose. Ou utilisation de -o''nom du fichier.log''. Je laisse a chacun le soin de lire la doc et d'adapter la commande à ses besoins

Donc on peut monter cela dans un script qui sera effectué lancé par cron

10.4. Downgrade du syno

Synopsis : je veux revenir à une version antérieure.

Source : nas-forum.com yansg, fredlime

Avertissement : Ce n'est pas quelque chose sans risque, alors si vous le pouvez avant toute chose sauvegardez vos données.

Le principe, c'est de faire croire au système de votre Syno qu'il fonctionne avec un Firmware inférieur à celui sur lequel vous voulez revenir.

En premier lieu les bonnes dates:

majorversion	minorversion	buildphase	buildnumber	bulldate
2	0	3	0590	2008/03/12
2	0	3	0571	2008/02/02
2	0	3	0569	2008/01/31
2	0	3	0524	2007/12/20
2	0	3	0518	2007/11/01

Nous allons prendre comme exemple mon vecu:

J'ai installé la version 0590 et cette version ne me convient pas, je voudrais réinstaller le version 0571.

Avec putty en root

```
nano /etc.defaults/VERSION
```

Voici les informations contenues dans le fichier

```
majorversion="2"  
minorversion="0"  
buildphase="3"  
buildnumber="0590"  
bulldate="2008/03/12"
```

donc il faut remplacer les valeurs

```
buildnumber="0590"  
bulldate="2008/03/12"
```

par

```
buildnumber="0524"  
bulldate="2007/12/20"
```

Cela va nous permettre de faire croire au contrôle de version que nous

sommes en 0524 et que nous voulons passer en 0571.

sauvegardons le fichier.

Sans rebooter la machine

Allez dans l'interface web du syno

système -> Mise à jour du progiciel

normalement il devrait s'afficher le numéro de version modifier.

Si ce n'est pas le cas rééditez le fichier /etc.defaults/VERSION

choisissez le fichier pat de la version 0571 et cliquez sur OK

et attendez jusqu'à la fin du reboot..... je sais cela paraît long, mais en final votre syno fini son boot et se remet à indexer les fichiers.

Comme cela est écrit sur le site de fredlime un cierge peut être...

11. Outils

11.1. Putty

<http://www.chiark.greenend.org.uk/~sgtatham/putty/>

<http://fr.wikipedia.org/wiki/PuTTY>

PuTTY est un client SSH, Telnet, Serial Link, rlogin, et TCP. Il était à l'origine disponible uniquement pour Windows, mais il est à présent porté sur diverses plate-formes Unix (et non-officiellement sur d'autres plate-formes). PuTTY est écrit et maintenu principalement par Simon Tatham.

Il est open source, sous une licence de type MIT.

11.2. Winscp

<http://winscp.net/eng/docs/lang:fr>

<http://fr.wikipedia.org/wiki/WinSCP>

WinSCP est un client SFTP graphique pour Windows. Il utilise SSH et est open source. Le protocole SCP est également supporté. Le but de ce programme est de permettre la copie sécurisée de fichiers entre un ordinateur local et un ordinateur distant.

il est publié sous licence GNU GPL et est hébergé sur SourceForge

11.3. Filezilla

<http://www.filezilla-project.org/>

<http://fr.wikipedia.org/wiki/Filezilla>

FileZilla est un client FTP, FTPS et SFTP ; développé sous la licence publique générale GNU. Il est multi-plateforme