SSH PUTTY et WINSCP

Création : OpenOffice.org Version 2.3

Auteur : TOF — Création : 18/01/2008:

Version : 25 — Modification : 20/03/2008

Fichier : E:\Mes documents\tuto NAS LB\tuto ssh.odt

Imprimer moi en reto/verso !!!!

Table des matières

Tuto récupérer sur le site www.nas-forum.com
Auteur : Tof

1. Utilisation PuTTY openSSH WinSCP

Cet HowTo couvre:

* l'utilisation simple de PuTTY en remplacement de la console Telnet de Windows et comme client SSH.

* l'installation pour un usage simple du shell sécurisé OpenSSH.

* des exemples d'utilisation de la suite PuTTY, notamment le transfert de port avec une carte de bouclage et Plink.

* l'installation et l'utilisation de WinSCP.

Pré-requis : activation de l'accès Telnet et installation du BootStrap.

Remarques:

Les logiciels utilisées sont libres (et gratuits) sauf Windows (cher et obscur).

Cet HowTo est essentiellement destiné aux utilisateurs de windows, bien que PuTTY soit porté sur d'autre plate-forme.

D'autres outils spécifiques existent pour les autres systèmes, mais le rédacteur initial n'est pas compétent et suggère qu'il y aurait matière à d'autres page pour aider les débutants, sous Mac ou Linux par exemple.

2. PuTTY en client telnet

PuTTY est un bon client libre (et gratuit) telnet et SHH (entre autres). Télécharger l'installeur et l'exécuter. L'installeur installera tous les outils du site qui pourraient vous servir prochainement.

Une fois installé, démarrer PuTTY: Démarrer->Programme->PuTTY->PuTTY

Dans la fenêtre de démarrage PuTTY configuration, se placer sur la branche (à gauche) session et à droite renseigner:

* l'hôte à atteindre (HostBame): Adresse IP ou nom de réseau du syno

* cocher le Protocole Telnet. Le port est changé en conséquence: 23, à modifier si le port standard Telnet 23 a été changé

cliquer Open pour vous connecter

Vous obtiendrez une fenêtre entièrement redimensionnable et des fonctions de copier/coller très confortables.

* pour copier un texte de la console, le sélectionner avec la souris. C'est

tout, ce texte est disponible dans le presse-papiers. Placez vous dans un éditeur de texte par exemple, et collez (^V) vous le verrez apparaître

* pour coller un texte dans la console, copiez (^C) le auparavant à partir de votre éditeur de texte par exemple et clic droit quelque part au-dessus de la console, vous verrez apparaître le texte à droite du prompt de commande.

Un Crtl+D (^D) suffit pour fermer la session proprement.

Toujours à partir de la fenêtre de démarrage PuTTY configuration, vous pouvez, après avoir fait vos réglages, indiquer dans Saved Sessions un nom (Telnet Syno par exemple) et cliquer sur Save. Vos réglages seront sauvegardés dans la fenêtre du dessous. Vous pourrez après

* sélectionner la session sauvegardée et cliquer sur Open pour la réouvrir

* double-cliquer sur le session pour l'ouvrir directement

* sélectionner la session sauvegardée et cliquer sur Load pour éditer les réglages (ne pas oublier de les re-sauvegarder ou de les enregistrer sous un autre nom).

Bien entendu, vous pouvez utiliser PuTTY pour vous connecter sur un serveur autre que Telnet, comme par exemple un serveur Pop avec le port 110, un serveur smtp avec le port 25, etc. Mais c'est un autre sujet.

3. Installation du serveur SSH

OpenSSh est un Démon riche en fonctionnalités, multi-plateformes, libre (et gratuit). Sa caractéristique initiale est l'utilisation du protocole SSH SSH pour chiffrer l'authentification à la connexion et les transferts entre un client et un serveur.

Installation du package OpenSSh pour un Syno. Dans une session PuTTY/Telnet, exécuter les commandes suivantes:

ipkg update #Mise à jour de la liste des packages

ipkg install openssh #Cela peut prendre un certain temps pour générer les clés

Exemple d'installation:

DiskStation> ipkg install openssh

Installing openssh (4.3p2-6) to root...

Downloading http://ipkg.nslu2-linux.org/feeds/optware/...6_SelonSyno.ipk

Installing zlib (1.2.3-1) to root...

Downloading http://ipkg.nslu2-linux.org/feeds/optware/...1_SelonSyno.ipk

Configuring openssh

Generating RSA Key...

Generating public/private rsa1 key pair.

Your identification has been saved in /opt/etc/openssh/ssh_host_key.

Your public key has been saved in /opt/etc/openssh/ssh_host_key.pub.

The key fingerprint is:

c0:mega_shok.gif:8a:f6:71:e3:5f:ab:e9:34:2a:a7:5b:f7:49:66

Generating RSA Key...

Generating public/private rsa key pair.

Your identification has been saved in /opt/etc/openssh/ssh_host_rsa_key.

Your public key has been saved in /opt/etc/openssh/ssh_host_rsa_key.pub.

The key fingerprint is:

5c:49:8a:a4:e9:27:4b:13:86:00:ec:74:a0:a1:c4:88

Generating DSA Key...

Generating public/private dsa key pair.

Your identification has been saved in /opt/etc/openssh/ssh_host_dsa_key.

Your public key has been saved in /opt/etc/openssh/ssh_host_dsa_key.pub.

The key fingerprint is:

c4:e4:00:ff:db:1a:43:25:c4:7c:15:f5:c7:2f:84:d0

Fixing permissions on the /tmp directory...

killall: sshd: no process killed

Configuring zlib

Successfully terminated.

DiskStation>

Une fois installé, vous pouvez vérifier que le démon est actif:

ps | grep sshd

le résultat doit ressembler à:

524 root 36 S /opt/sbin/sshd

C'est fini.

Pour utilisation avancée de SSH, en cas d'ouverture sur l'internet ou de fonctions de tunneling SSH, référez vous à Utilisation de OpenSSh pour l'accès distant.

Un fois installé, vous n'aurez, sauf besoins particuliers de configuration du serveur

SSH, plus besoin de telnet. Il est même conseillé d'arrêter ce service ou de le désactiver (voir Activation de telnet) ou tout du moins de bien vérifier que le port telnet 23 ne soit pas ouvert sur l'extérieur.

Pour affiner éventuellement la configuration du serveur SSH, éditez le fichier /opt/etc/openssh/sshd_config. Plus d'informations dans la doc SSHD_CONFIG

3.1. PuTTY en client SSH

L'utilisation de base de PuTTY ayant déjà été abordée dans la partie PuTTY en client telnet, il ne sera abordé ici que la configuration pour se connecter à un serveur SSH

Plus d'informations, en anglais, dans la doc PuTTY

3.1.1. Authentification par mot de passe

Remarques préliminaires:

* cette méthode n'est pas la plus sûre, elle dépend de la difficulté du mot de passe enregistré (cette difficulté ne portant souvent que son nom sans l'être réellement).

Il faut savoir qu'il existe des logiciels scanners ou robots qui peuvent tester toute une série de chiffres, ainsi que les mots contenus dans un dictionnaire. Ces dictionnaires sont disponibles en plusieurs langues selon la nationnalité de l'administrateur du serveur à attaquer...

Ce type d'attaque, appelée force brute, n'est bien souvent qu'une question de temps avant de réussir.

* Ou bien plus simple et couramment pratiqué:

renseignez vous sur les noms et la date anniversaire de l'administrateur (non qualifié), de son épouse, de ses enfant ou de son chien et essayer les en mot de passe. Vous risquez d'être surpris.

Cela s'appelle, pour info, du Social Engineering.

* Ne pas oublier que sous l'apparence du gentil syno se cache un redoutable Linux(entre de mauvaises mains).

* La remarque précédente est à pondérer selon le degré d'ouverture du syno.

Les précautions ne seront pas les mêmes si vous êtes seul avec votre Pc et votre syno en réseau (l'hypothèse étant faite que votre chien ne connaît pas l'informatique), sans port ouvert sur le routeur

ou bien si vous gérez un serveur dans une faculté (beaucoup de ressources intellectuelles et comiques disponibles)

ou pire si le port SSH est ouvert sur le net, laissant tout le loisir aux méchants pirates de la planète de s'amuser, dès fois que...

Maintenant que vous êtes informés,

ouvrez PuttY: Démarrer->Programme->PuTTY->PuTTY.

Dans la fenêtre configuration, dans les sections:

* Session: c'est le port 22 à utiliser (si le port standard n'a pas été changé)

* Connexion

o Data: dans le champs Auto-login username saisir le compte, existant sur le syno, sous lequel vous voulez vous connecter

enregistrer si besoin vos réglages.

Le mot de passe vous sera demandé à la connexion.

Pour une aide sur les mots de passe, consulter Mot de passe root.

A cette étape, en SSH, le mot de passe root est : synopass

3.1.2. Authentification clé privé

Se référer à: Configuration du serveur OpenSSH pour un accès par clé publique.

3.1.3. Première connexion à un serveur SSH

Quand vous vous connectez la première fois à un serveur SSH, Putty peut vous avertir que la signature de l'hôte (votre Syno) n'est pas en cache. C'est normal pour une première connexion et parce que vous connaissez la clé du serveur et/ou que vous faites confiance, vous pouvez cliquer sur Oui pour continuer et mettre dans le cache cette clé de serveur.

Si à l'avenir cet avertissement re-surgissait pour ce serveur, c'est que quelqu'un aurait modifié les clés du serveur, un pirate par exemple... ou une maladresse du root. Mode prudence à activer alors. Réfléchissez attentivement sur le pourquoi de la chose avant d'accepter une nouvelle mise en cache (prévenir l'administrateur du serveur au besoin).]

3.2. Utilisation de l'agent d'authentification Pageant

Pageant est un agent d'authentification SSH. Il garde en mémoire votre clé privée décodée. vous pouvez ainsi l'utiliser aussi souvent dans votre session windows que vous en avez besoin, sans pour autant spécifier votre mot de passe pour la décoder à chaque fois. Pageant fonctionne en partenariat avec PuTTY, Winscp et d'autres programmes qui, si Pageant est actif, rechercherons une clé adéquate déjà décodée dans sa mémoire.

Vous pouvez démarrez Pageant au démarrage de windows (raccourci à placer dans menu programmes/démarrage), voire installer une commande pour appeler Pageant avec les clés nécessaires.

Ouvrez Pageant: Démarrer->Programme->PuTTY->Pageant . Une icône sera alors visible dans la barre système.

Un clic droit sur son icône vous permettra:

* d'ajouter une clés privée Add key. Le mot de passe pour la décoder sera demandé. Vous pouvez ajouter plusieurs clés, le choix sera fait automatiquement selon le besoin.

* de voir les clés chargées en mémoire View keys

* de décharger une clé en mémoire View keys+sélection+Remove Key quand elle devenue inutile pour la session windows en cours.

Les clés ne seront plus utilisables lorsque vous quitterez Pageant ou votre session windows.

Plus d'informations, en anglais, dans la doc Pageant

4. Utilisation de Plink

Plink est un utilitaire disponible dans la suite PuTTY qui vous permet d'automatiser (scripter) une session SSH et/ou de programmer des transferts de ports.

dans les exemples suivants, l'authentification s'effectue par clés privée/publique, la clé publique étant déjà inscrite sur le serveur syno, la clé privée déjà décodée sur le poste client (avec Pageant par exemple). Les serveur syno est nommé sur le réseau DiskStation, mais vous pouvez biensûr utiliser une adresse IP ou un autre nom programmé.

Hypothèses sont faites que:

* vous vous connectez (uniquement pour l'administration du syno, hein?user posted image

* vous êtes dans le répertoire où sont installés les programmes PuTTY

* le répertoire où sont installés les programmes PuTTY est dans la variable d'environnement de windows.

pour modifier la variable d'environnement windows:

* clic droit sur poste de travail, propriétés/avancé, variables d'environnement

* dans variables utilisateur, modifier PATH et ajouter: ;C:\Program Files\putty (si le répertoire d'installation est par défaut)

ouvrez une console système (Démarrer/Exécuter/cmd), déplacez vous si besoin dans le répertoire des programmes PuTTY.

exemples:

plink root@diskstation -ssh

vous avez votre système syno dans votre console windows

vous forcez le protocole ssh (facultatif normalement, mais facilite la relecture d'un script)

plink root@diskstation -ssh echo "Bonjour planete"

vous affichez Bonjour planète dans votre console windows

vous pouvez biensûr utiliser d'autres commandes du syno ou lancer un script sur celui-ci

plink root@diskstation -ssh -i fichier.ppk echo "Bonjour planete"

vous exécutez la commande avec une authentification par la clé privée fichier.ppk (indiquer aussi son chemin d'accès)

si vous avez déjà décodé cette clé avec Pageant, il ne vous sera donc pas demandé de mot de passe

plink root@diskstation -ssh -L 10.0.0.1:139:Diskstation:139

vous transférez le port 139 de votre carte de bouclage (carte réseau loopbak virtuelle) sur le port Samba/smb de votre syno

vous obtenez donc le partage réseau des dossiers partagés de votre syno à travers SSH, c'est un tunnel SSH

notamment utile si vous devez traverser un réseau hostile comme l'internet

Plus d'informations, en anglais, dans la doc Plink

Autres exemple:

plink root@diskstation -ssh -L 10.0.0.1:25:SeveurSmtp:25 -L 10.0.0.1:110:ServeurPop:110 -L 10.0.0.1:3389:ServeurTSE:3389

vous accédez à distance, en toute sécurité, dans un réseau où se trouve le syno, au serveurs privé smtp, pop ou TSE

cet accès peut se faire sans trop se préoccuper de blinder certains services

notamment sans ouvrir le smtp sur le net et donc devoir le protéger du relayage

Dans Utilisation de OpenSSh pour l'accès distant, l'auteur indique avoir configuré le port 445 pour accéder à son imprimante partagée. Se référer donc à cette article si nécessaire. Ici, pour un accès simple à des dossiers réseau sur un serveur windows, nul besoin de se préoccuper de ce port.

5. Installation d'une carte de bouclage

Schéma d'installation sur un windows Xp

(la démarche devrait être similaire sur un autre windows NT, pour les systèmes win9x l'essai n'a pas été fait).

Panneau de configuration -> Ajout de matériel -> Assistant

suivant -> Oui, j'ai déjà connecté le matériel -> suivant

sélectionner Ajouter un nouveau périphérique matériel -> suivant

installer le matériel que je sélectionne manuellement dans la liste -> suivant

carte réseau -> suivant

fabricant: Microsoft / carte réseau: carte de bouclage Microsoft -> suivant -> suivant -> terminer -> terminer

Paramètres/Connexions réseau

sélectionner la nouvelle connexion au réseau local2 (carte de bouclage microsoft)

clic droit, renommer: LoopBack par exemple, valider

clic droit, propriétés

décocher Client pour les réseaux microsoft

décocher Partage de fichiers et d'imprimantes pour les réseaux microsoft

sélectionner Protocole internet (TCP/IP) -> Propretés

cocher Utiliser l'adresse IP suivante

saisir dans le champs Adresse IP: 10.0.0.1

saisir dans le masque de sous-réseau: 255.0.0.0

clic sur Avancé

sélectionner l'onglet Wins

cocher Désactiver NetBIOS avec TCP/IP -> Ok -> Ok -> Fermer

Votre nouvel adaptateur réseau est prêt pour servir à transférer des ports en SSH, avec des partages Samba/SMB. port139 pour les dossiers réseaux et port 445 pour les imprimantes réseaux).

Vous pouvez ajoutez similairement d'autres cartes de bouclage avec d'autres adresses IP pour atteindre simultanément d'autres serveurs SSH. Vous devriez même (pas essayé) vous servir de cette carte de bouclage pour établir un pont entre 2 réseaux privés via un tunnel SSH par l'internet. Attention, ce pont est susceptible de compromettre la sécurité des réseaux privés (si maillon faible) et l'opération est désespérée sous windows 2000.

6. Installation de WinSCP et paramètrage

Allez sur le site WinSCP. Pour une installation simple, utiliser le Multilanguage installation package. L'exécuter pour l'installer.

Dans les options d'installations par défaut:

* inutile d'installer PuTTY et Pageant dans l'hypothèse où vous avez déjà installé ces programmes (voir 1ère section)

* préférer l'interface Norton Commander pour avoir dans 2 fenêtres, le répertoire distant et local, comme un client ftp habituel

* les reste des options peuvent rester par défaut

6.1. Démarrer WinSCP:

* Dans Préférences/boutons Préférences:

Intégration: normalement, lors de l'installation, PuTTY a été détecté et sa localisation est indiquée ici. Vérifier et/ou modifier si besoin.

Enregistrement: cocher Fichier INI (WinSCP3.ini) pour enregistrer la configuration dans un fichier et pouvoir ainsi transférer simplement la configuration sur un autre Pc en copiant ce fichier WinSCP3.ini (situé dans le répertoire d'installation du programme).

clic sur ok pour quitter cette fenêtre.

Pour configurer une session, sélectionner la branche session:

* remplir Nom d'hôte avec l'adresse IP ou le nom du syno

* le numéro de port est 22 en standard, sauf si celui du serveur SSH a été changé

* saisir dans Nom d'utilisateur le login sous lequel la session doit être ouverte

o saisir le mot de passe si la connexion se fait par login/pass et si vous n'avez pas peur de le laisser stocké sur le Pc. Sinon il vous sera demandé de le saisir à la connexion.

o laisser vide dans la cas d'une authentification par clé

* si besoin, indiquer la localisation de votre clé privée dans le champs Fichier de clé privée

* sélectionner le protocole sftp

* cliquer sur le bouton Sauver pour enregistrer cette configuration et saisir un nom qui vous permettra de reconnaître cette configuration, par exemple MonSyno.

Sur le même principe que PuTTY, vous pouvez après avoir sélectionné la branche Session/Sessions sauvées:

* sélectionner la session sauvegardée et cliquer sur Connecter pour la réouvrir
* double-cliquer sur le session pour l'ouvrir directement
* sélectionner la session sauvegardée et cliquer sur Charger pour éditer les réglages

(ne pas oublier de les re-sauvegarder ou de les enregistrer sous un autre nom).

Ouvrir une session en cliquant sur Connecter.

Remarque:

si vous vous authentifiez par clé, et si vous avez décodé votre clé privé auparavant avec Pageant (voir section ci-dessus), vous serez automatiquement connecté, sinon, il vous sera demandé de saisir le mot de passe pour décoder votre clé privée.

Une fois connecté, vous aurez une interface style client graphique ftp, appelant peu de commentaires. A noter:

* Ctrl+P (^P): permet l'ouverture directe de PuTTY pour ouvrir un terminal sur le serveur.
* pour afficher l'arborescence distante: Options/Panneau Distant/Arborescence à sélectionner
* pour afficher l'arborescence locale: Options/Panneau Local/Arborescence à sélectionner
* pour voir la file d'attente des transferts: Options/Liste/Montrer

Vous pourrez aussi découvrir des fonctionnalités de synchronisation dans le menu Commandes

6.2. Utilisation de WinSCP couplé avec votre éditeur de texte préféré

Quand vous double-cliquez sur un fichier distant, WinSCP va l'ouvrir dans un éditeur de texte intégré, rudimentaire. Si vous utilisez habituellement un éditeur de texte avancé, il est facilement possible de le coupler avec WinSCP. Pour cela, ouvrir la fenêtre des options: Options/Préférences:

1. sélectionner la branche Editeurs
2. cliquer sur Ajouter
3. cocher éditeur externe, le localiser avec le bouton Naviguer
4. par défaut, il servira pour l'édition de tous les fichier (masque *.*)

5. si l'éditeur choisi ne gère pas plusieurs documents (comme notepad par exemple), s'arrêter là.

6. si l'éditeur à des capacités MDI (Multiple Document Interface), il gère donc plusieurs documents/onglets. Cocher la case l'éditeur gère plusieurs fichiers dans une fenêtre

7. valider par OK

8. sélectionner la nouvelle ligne de l'éditeur ajouté, et Monter cette ligne en tête de liste

9. valider par OK

Votre éditeur sera maintenant utilisé par défaut pour l'édition d'un fichier distant, lors d'un double-clic sur celui-ci par exemple. Il sera d'abord chargé dans un répertoire temporaire de votre Pc, puis chargé dans votre éditeur.

Lors de sa sauvegarde, il sera automatique rechargé dans le répertoire distant. Lors de ce premier rechargement, un nouveau mot de passe pourra vous être demandé pour lancer un deuxième processus sftp sur le syno. Il ne vous sera plus redemandé tant que durera votre session WinSCP. Si vous avez auparavant décodé votre clé dans Pageant, le deuxième processus sftp sera lancé automatiquement, sans demande de mot de passe.

Ecrit par Tof