Compléments pour l'administration et l'exploitation

SERVEUR FREERADIUS

XXX/XXX/DT – 12/12/2008

Légende : Le texte explicatif est **sous** l'image.
Texte normal : explication
Texte en italique : options à choisir, sélectionner ou valeur à rentrer dans un champ
… Texte en gras avec 3 points avant et après … : traitement de la machine qui dure quelques secondes ou quelques minutes ; patienter jusqu'à la fin du traitement.

Les attributs pour les équipements réseaux 3Com, Cisco, Nortel et Enterasys

Les attributs ci-dessous sont à insérer dans le même ordre qu'ils sont présentés (3Com, puis Cisco, puis …).

Equipement : 3Com
Nom attribut : **3Com-User-Access-Level**
Valeurs : **3** pour le profil *security*, **2** pour le profil *manager* et **1** pour le profil *monitor*.

Equipement : Cisco
Nom attribut : **cisco-avpair**
Valeurs : **shell:priv-lvl=15** pour les droits *root*, **shell:priv-lvl=7** ou **shell:priv-lvl=1** pour les droits restreints.

Equipement : Enterasys
Nom attribut : **Filter-ID**
Valeurs : **Enterasys:version=1:mgmt=su** pour les droits *root*, **Enterasys:version=1:mgmt=rw** pour les droits en lecture/écriture, **Enterasys:version=1:mgmt=ro** pour les droits en lecture seule.

Equipement : Nortel
Nom attribut : **Service-Type**
Valeur : **Administrative-User** pour les droits en administration.

Ajout d'un nouveau type d'attribut/prise en compte d'un nouveau type d'équipement

Aller dans le menu « gestion des groupes » puis « Ajouter un attribut de réponse à un groupe ». Suivre les instructions. Répéter cette opération pour tous les groupes concernés par ce nouveau type d'équipement.

Restauration d'une sauvegarde

Soit /adminradius/FichierSauvegarde_RADIUS2007_10_3_16_21_40 le fichier de sauvegarde. Taper la commande :
mysql radius –u root –p < /adminradius/FichierSauvegarde_RADIUS2007_10_3_16_21_40
Il sera demandé le mot de passe de l'utilisateur *root*.

Gestion du VPN de synchronisation

Taper la commande suivante pour savoir si le vpn est monté :
ps x | grep ssh
Sur le serveur principal : Si le VPN est monté, on doit pouvoir lire (entre autres) une ligne ressemblant à ceci (en gras les éléments indépendants des paramètres serveurs) :
1236 ? Ss 0:00 **ssh -N -f vpnssh@**172.16.69.40 **-L 30000:127.0.0.1:3306**
Sur le serveur secondaire : Si le VPN est monté, on doit pouvoir lire (entre autres) une ligne ressemblant à ceci (en gras les éléments indépendants des paramètres serveurs) :
1541 ? Ss 0:00 **sshd: vpnssh [priv]**

Pour couper le VPN (possible uniquement depuis le serveur principal), taper la commande suivante :
killall ssh
Cette commande coupe tous les processus ssh en cours, que ce soit le vpn ou les sessions de PMAD. On perd donc la main sur la machine, mais on peut se reconnecter en suivant.

Pour monter le VPN (à faire depuis le serveur principal), taper la commande suivante :

ssh -N -f vpnssh@192.168.0.44 -L 30000:127.0.0.1:3306
où 192.168.0.44 est l'adresse IP du serveur secondaire.

Changement du mot de passe d'un utilisateur du système

Ce qui suit ne doit pas être utilisé pour les comptes des utilisateurs RADIUS. Pour ces derniers, utiliser la console *netadmin.pl* .
Il ne devrait y avoir que *root*, *adminradius* et *vpnssh* de concernés au final. Pour changer le mot de passe, taper en tant qu'administrateur :
passwd LoginConcerné

Changement du mot de passe d'un utilisateur du SGBD

Se connecter à MySQL en tapant :
mysql –u root –p
Il est ensuite demandé d'indiquer le mot de passe du root.

Pour changer le mot de passe du root, taper les commandes suivantes en remplaçant *MotDePasseRoot* par le nouveau mot de passe :
*GRANT ALL PRIVILEGES on *.* to root@localhost IDENTIFIED BY "MotDePasseRoot" ;*
FLUSH PRIVILEGES ;
exit
Pour changer le mot de passe de l'utilisateur radiusXXX, taper les commandes suivantes en remplaçant *radiusXXXMdP* par le nouveau mot de passe :
GRANT INSERT on radius. to radiusXXX@localhost IDENTIFIED BY "radiusXXXMdP" ;*
GRANT SELECT on radius. to radiusXXX@localhost IDENTIFIED BY "radiusXXXMdP" ;*
GRANT DELETE on radius. to radiusXXX@localhost IDENTIFIED BY "radiusXXXMdP " ;*
GRANT UPDATE on radius. to radiusXXX@localhost IDENTIFIED BY "radiusXXXMdP " ;*
FLUSH PRIVILEGES ;
exit

Ces commandes sont à faire sur les 2 serveurs !
Attention, tout changement de mot de passe de *radiusXXX* implique que cela soit également changé dans le FreeRADIUS. Pour cela, aller dans le fichier */etc/freeradius/sql.conf* et y chercher une ligne ressemblant à :
*password = "*MonAncienMotDePasse*"*
Il faut aussi prendre en compte ce changement de mot de passe dans le fichier *AccesBD.txt* .

Changement des mots de passe RADIUS <-> MySQL

Le changement de mot de passe doit être réalisé dans plusieurs fichiers :
AccesBD.txt qui est utilisé par *netadmin.pl*.
/etc/freeradius/sql.conf qui est utilisé par FreeRADIUS pour se connecter à MySQL.
Dans le */etc/cron.weekly/maintfreeradius* qui est appellé pour les sauvegardes hebdomadaires.
Dans MySQL (voir ci-dessus).

Gestion du watchdog logiciel

Pour suspendre le watchdog logiciel	→ pour démarrer le watchdog logiciel
/etc/init.d/cron stop	→ */etc/init.d/cron start*
rmmod softdog	→ *modprobe softdog*

Dans le premier cas on joue sur le module sur le logiciel en espace utilisateur ➔ on désactive la vérification périodique de l'état du serveur. Cependant on inhibe toutes les tâches périodiques comme les synchronisations et les sauvegardes. Cette solution est donc à utiliser temporairement.
Dans le second cas, on joue sur le module noyau ➔ les contrôles se font toujours, mais si le logiciel en espace utilisateur veut déclencher le watchdog, il y a aura un message de son action, sans que rien n'arrive.

Mise à jour du système

Ouvrir le filtrage :
iptables –P INPUT ACCEPT

iptables –P OUTPUT ACCEPT
iptables –F
iptables –X

Mise à jour du système :
apt-get update
apt-get upgrade
Répondre aux éventuelles questions.

Réactiver le filtrage :
/etc/init.d/XXXXFirewall

Si le noyau a été mis à jour, redémarrer le serveur pour prise en compte.
Ces commandes sont à faire sur les 2 serveurs !

Ouvrir/fermer le filtrage

La configuration par défaut du firewall est chargée tous les jours à 1h00. Si l'on se coupe la PMAD, il suffit d'attendre le lendemain (sauf si on peut facilement accéder en local à la machine) pour que la configuration permettant la PMAD écrase la configuration courante. Cependant, toute modification du filtrage n'étant pas prise en compte dans le script de configuration du firewall n'aura pas une durée de vie supérieure à 24h.

Pour ouvrir le filtrage et désactiver le NAT :
iptables –P INPUT ACCEPT
iptables –P OUTPUT ACCEPT
iptables –F
iptables –X
iptables –Z
iptables –t nat –P PREROUTING
iptables –t nat –P POSTROUTING
iptables –t nat –P OUTPUT
iptables –t nat –F
iptables –t nat –X
iptables –t nat –Z

Pour activer le filtrage et les règles de NAT :
/etc/init.d/XXXXFirewall

Pour fermer le filtrage (attention, on perd irrémédiablement la PMAD. Il sera nécessaire d'intervenir en local pour ouvrir le filtrage) :
iptables –P INPUT DROP
iptables –P OUTPUT DROP
iptables –P FORWARD DROP
iptables –F
iptables –X

Gestion de la configuration IP et du routage

Voir le manuel des commandes *route* et *ifconfig*. Pour cela :
man route
man ifconfig

Gestion avec la console d'administration

La console d'administration permet d'effectuer tous les gestes de bases pour exploiter la solution :

- Gestion des utilisateurs FreeRADIUS
- Gestion des attributs RADIUS
- Gestion des nas
- Divers gestes d'administration comme réaliser les sauvegardes, les synchro des bases de données, consultation de journaux, activation du watchdog, …

Pour plusieurs tâches, il est nécessaire d'avoir les droits administrateurs système. Pour cette raison, la console d'administration ne sera accessible que par les administrateurs.
La console d'administration est un programme écrit en perl nommé *netadmin.pl* .
Ce programme a précédemment été copié dans le compte de l'administrateur adminradius, et il sera donc chargé en tapant :
`./netadmin.pl` si l'on se trouve dans le répertoire */home/adminradius* ,
`/home/adminradius/netadmin.pl` sinon.

Pour connaître les arguments possibles, taper :
```
./netadmin.pl –help
```

La console d'administration peut être utilisée en mode intéractif, en mode automatique ou encore dans un mode mixte.

Le mode intéractif :
Lancer l'outil comme expliqué précédemment. Apparaît alors le menu d'accueil et on utilise l'outil normalement, en se laissant guider.

Le mode automatique :
Ici, on connaît les variables que l'outil va nous demander. On peut donc lui donner en une seule fois toutes les variables et leurs valeurs pour éviter de devoir parcourir l'arborescence du menu et d'attendre que l'outil nous demande les variables les unes après les autres. Pour cela on va donner des arguments à la commande et pour indiquer à netadmin.pl de prendre en compte ces arguments, on va rajouter comme argument « -A ». Voici un exemple de déclaration d'un nas en mode automatique :
```
/adminradius/netadmin.pl -A -choix nas -sschoix add -nasname 192.168.0.10 -shortname
MonSwitch10 -type other -port 1 -secret granDSEcret -groupe utilisateur -description ''mon
commentaire''
```
Et nous est retourné :
```
[OK] Insertion effectuée.
```

Pour connaître les arguments possibles, taper :
```
./netadmin.pl –help
```

On voit donc que l'outil ne nous a rien demandé de plus et qu'il rend la main desuite. Ce mode est très utile si l'on veut utiliser les fonctionnalités de l'outil dans un script. Au lieu de recoder la fonctionnalité, on fait appel à l'outil en mode automatique. Ces scripts peuvent être utilisés pour des tâches automatisés régulières (comme la synchronisation des bases de données ou encore le watchdog) ou encore pour des opérations répétitives (pour rentrer un groupe de 100 nas, écrire un script qui va exécuter 100 fois la commande vue ci-dessus juste en adaptant les valeurs des arguments). On peut également récupérer le résultat de la commande pour ensuite réaliser un traitement :
```
# !/usr/bin/perl
print `/adminradius/netadmin.pl -A -choix nas -sschoix add -nasname 192.168.0.10 -shortname
MonSwitch10 -type other -port 1 -secret granDSEcret -groupe utilisateur -description ''mon
commentaire'' > FichierResultat.txt` ;
open (FICHIER, 'FichierResultat.txt') ;
        $resultat = <FICHIER> ;
        close (FICHIER) ;
if ($resultat =~ /[OK] .*/) {
… traitement suite à la réussite de la commande …
}
else {
… traitement suite à l'échec de la commande …
}
```

Les arguments peuvent être mis dans n'importe quel ordre ; il n'est pas nécessaire que l'ordre des arguments soit le même que l'ordre dans lequel les variables sont demandées en mode intéractif :
```
/adminradius/netadmin.pl –A –choix nas -sschoix add
```
est équivalent à
```
/adminradius/netadmin.pl –A -sschoix add –choix nas
```

Il n'est pas obligatoire de rentrer en entier le nom de l'argument. Il suffit de mettre suffisamment de lettre pour que cela ne soit pas ambigu :

```
/adminradius/netadmin.pl –A –choix nas -sschoix add
```

est équivalent à

```
/adminradius/netadmin.pl –A –ch nas -sscho add
```

En revanche, la commande suivante n'est pas valide :

```
/adminradius/netadmin.pl –A -s add –choix nas
```

car on ne sait pas si *–s* est mis pour *–secret*, *–shortname*, ou *–sschoix*. D'ailleurs le logiciel nous retourne :

```
Option s is ambiguous (secret, shortname, sschoix)
```

Les majuscules et minuscules pour le nom des variables n'a aucune importance.

Mettre 1 tiret ou 2 devant le nom de la variable n'a pas d'importance.

Le mode mixte :

Ce dernier mode est, comme son nom l'indique, un mix entre les modes intéractif et automatique.
Il existe plus exactement 2 modes mixtes : le mode mixte dérivé du mode automatique et le mode mixte dérivé du mode intéractif. Le mode mixte est le fait de mettre des arguments à la commande mais de ne pas tous les mettre. La différence entre les 2 sous-modes mixtes est le fait de mettre ou non l'option ''-A''.

Le mode mixte dérivé du mode automatique est comme le mode automatique classique mis à part que l'on ne renseigne pas tous les arguments. Il nous est alors demandé les valeurs pour les variables inconnues, et seulement pour celles-ci.
Le mode mixte dérivé du mode intéractif est comme le mode intéractif sauf qu'au lancement de *netadmin.pl*, nous avons tout de même donné des arguments :

```
/adminradius/netadmin.pl -choix nas --sschoix add -nasname 193.169.0.1
```

nous avons alors le menu d'accueil comme en mode intéractif : les arguments *–choix* et *–sschoix* ne sont pas pris en compte. Les autres arguments oui. Ainsi, si l'on va dans le menu d'ajout d'un nas ou encore dans le menu de suppression d'un nas (la variable *–nasname* est également utilisée dans ce menu), il ne sera pas demandé le nom du nas à ajouter/supprimer mais seulement les autres variables nécessaires au traitement de la demande.

En synthèse, si l'on met ''–A'' et que l'on ne met pas tous les arguments, le logiciel demande les valeurs des variables manquantes, mais il est indispensable de renseigner les arguments *–choix* et *–sschoix* sous peine de voir le logiciel rendre la main sans demander les autres arguments et en n'ayant fait aucun traitement. Soit on ne met pas le ''-A'' et l'on met quelques arguments qui fait qu'ils ne seront pas redemandés par la suite. Cependant, il est inutile dans ce dernier cas d'indiquer les variables *–choix* et *–sschoix* car elles ne sont pas prises en compte : on navigue manuellement dans l'arborescence comme en mode intéractif.

Contrôles réguliers

Les contrôles réguliers suivants permettent de toujours avoir un système cohérent.

La commande *last* permet de connaître les logins/date/@ip source/… des connexions au système réussie dans le mois. Pour plus d'information, voir *man last* .

La commande *lastb* permet de connaître les logins/date/… des connexions au système échouée dans le mois. Attention, ne sont répertoriée que les connexions échouées locales. Pour plus d'information, voir *man lastb* .

La commande *lastlog* permet de connaître la date de dernière connexion au système pour chaque login déclaré dans la machine. Pour plus d'information, voir *man lastlog* .

Les tentatives de connexions RADIUS réussies ou échouées peuvent être visualisées à travers la console d'administration, dans le menu *Administration* puis respectivement *Afficher les tentatives de connexions réussies* et *Afficher les tentatives de connexions erronnées*.

Pour voir le suivi des connexions (locales ou distantes) au système réussies ou échouée, il faut lire le fichier */var/log/auth.log*. Pour les connexions échouées, on peut voir si c'est le login qui est erroné ou si c'est le mot de passe, ainsi que diverses informations comme l'adresse IP source, le port source et le processus impacté.

Pour accéder aux logs complets du programme freeradius, lire le fichier */var/log/freeradius/radius.log* . Seules les connexions échouées tracées dans ce fichier sont remontées par la console d'admin.

L'ensemble des informations journalisée sont accessibles par le fichier */var/log/syslog* .

Pour accéder à l'ensemble des informations du système (espace disque dur, mémoire RAM utilisée, …), utiliser la console d'administration : *Administration* puis *Afficher l'état des serveurs* .

Il faut également vérifier les sauvegardes régulièrement. Pour cela, aller dans le répertoire */adminradius/* et y chercher la dernière sauvegarde ; c'est un fichier de la forme *FichierSauvegarde_RADIUSAAAA_MM_JJ_HH_mm_ss*. S'assurer que ce fichier n'est pas vide et qu'il date de moins d'une semaine.

Déchiffrer les logs

Dans la console d'administration, menu *Administration* → *Afficher l'état des serveurs* .

- L'*uptime* est le durée depuis laquelle la machine n'a pas redémarré matériellement. Vu qu'il y a un *watchdog* qui redémarre la machine dès qu'il y a un problème sur un des services (RADIUS, Syslog, SGBD, SSHD), si l'*uptime* est cassé, c'est peut-être le watchdog qui est entré en action. Voir à quelle heure s'est réalisé ce redémarrage. S'il est possible que cela soit suite à une action d'une personne, voir dans les logs s'il n'y a pas eu de connexion (et qui) un peu avant le redémarrage. Si ce n'est pas le cas, alors voir dans les logs des services les erreurs éventuelles qui auraient pu faire déclencher le *watchdog*.
- L'espace disque ne doit pas évoluer beaucoup sauf pour /var. En effet ce répertoire stocke les journaux systèmes. En conséquence s'assurer que l'on n'arrive pas à 100% auquel cas il faudra faire du nettoyage.
- L'utilisaton de la RAM et de la swap soit être assez basse en fonctionnement normal.
- *Active Internet connections (only servers)* indique les services en écoute. On ne doit pas avoir autre chose que ssh, mysql (sur *localhost*), syslog, radius, radius-acct et ntp. Tout autre service est peut-être un cheval de troie.
- *Active UNIX domain sockets (only servers)* indique les services en ecoute sur les socket UNIX. On doit juste avoir mysql et acpi.

Comment utiliser l'USB ?

Connecter la clef USB sur n'importe quel port. Au bout de quelques secondes on voit que la clef est détectée suite à une activité sur l'écran.
Monter la clef en tapant la commande :
mount /dev/sda1 /media/usbdisk
Les données sont accessibles depuis /media/usbdisk. Vous pouvez maintenant lire et écrire des données sur votre clef USB.
Pour démonter la clef (= "retirer le périphérique" sous MS Windows), taper la commande :
umount /media/usbdisk

Le montage de la clef est automatique en mode graphique, et le démontage se fait ensuite par accès à l'option "Démonter le volume" accessible par clic droit sur le lecteur.

Comment effacer l'écran de la console ?

On peut taper *clear* mais si cela efface l'écran courant, on peut malgré tout remonter dans le cache. Comme sous netadmin.pl il est parfois demandé de taper des mots de passe qui apparaissent en clair à l'écran, il est génant que qqcun puisse y accéder sans même avoir à se logguer.
La solution est alors soit de taper sur *Entrée*suffisamment de fois pour écraser le cache (beurk !), soit taper la commande (bien mieux) :
clear_console