Installation de la distribution *netMET*

1 Introduction

1.1 Un peu de vocabulaire

Cette documentation décrit pas à pas les étapes à suivre pour installer et configurer la solution netMET.

Une distribution netMET est toujours identifiée par un ensemble de chiffres : **x.y_z.v** (*netMETdistrib-x.y_z.v*)

En effet, dans la distribution netMET, une distinction est faite entre la version du module d'exploitation (x.y) et la version du collecteur (z.v). Ainsi, une distribution du logiciel complet aura pour nom, netMETdistrib-x.y_z.v.

Que signifie les différentes orthographes de netmet

- netMET : désigne le logiciel
- netmet : désigne le compte dont /home/netmet est le home directory
- netMet : désigne le répertoire de travail, qui est généré après l'installation de netMET

1.2 Les prérequis

Le serveur sur lequel vous allez installer netMET doit être un serveur Linux.

Les distributions Redhat et Mandrake ont été validées par de nombreux utilisateurs. D'autres distributions peuvent être utilisées, mais nécessiteront peut être certaines adaptations. Dans tous les cas, nous vous conseillons d'installer tous les outils et librairies nécessaires à la compilation.

Les logiciels suivants doivent impérativement être ajoutés avant l'installation de netMET:

- Perl http://www.perl.com
- RRDtool http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
- Server HTTP Apache : http://httpd.apache.org/

De plus, un certain nombre de modules Perl doivent être installés (POSIX, Socket, Time::Local, HTTP::Date, File::Path, File::Temp, GD, GD::Graph, RRDs)

Le document "***Les prérequis de netMET***" détaille l'ensemble des prérequis et vous conseille sur les choix de votre future plateforme de métrologie.

Un utilisateur **'netmet'** doit être créé. Cet utilisateur sera utilisé pour installer, puis administrer la solution netMET. Le compte **'netmet'** peut appartenir à un groupe quelconque ('netmet' ou 'users' ou '....'). Dans cette documentation, le compte **'netmet'** appartient au groupe **'users'**.

Par convention, tous les chemins que nous indiquons sont relatifs au home directory de cet utilisateur netmet : **/home/netmet**

2 Installation de netMET

2.1 Récupération de la distribution et extraction

Les étapes ci-dessous décrivent la façon de récupérer et de décompresser la distribution netMET.

Etape	Commandes	Explications
1	netmet> **cd /home/netmet**	Positionnement dans le home directory du user "**netmet**"
2	**http://www.netmet-solutions.org** netmet> **wget http://<login>:<passwd>@www.netmet-solutions.org/<path_de_la_distribution>**	Récupérer la distribution netMETdistrib-x.y_z.v.tgz depuis le site officiel http://www.netmet-solutions.org avec le login et passwd que vous avez reçus suite à votre inscription et à l'acceptation de la Licence et des conditions d'accès. - soit avec un navigateur Internet quelconque (page téléchargement) - soit avec la commande wget
3	netmet> **tar zxvf netMETdistrib-x.y_z.v.tgz**	Décompression de la distribution

La décompression de la distribution netMETdistrib-x.y_z.v créé l'arborescence suivante :

```
/home/netmet
|
\---netMETdistrib-2.0beta_2.4.2
    |   home-netmet-netMet-2.0beta_2.4.2.tgz
    |   install.sh
    |   LICENCE
    |
    \---install
        +---etc
        |       apache.group
        |       apache.passwd
        |       httpd.conf
        |       protocols
        |       services
        |       syslog.conf
        |
        +--html
        |   |   informations.html
        |   |
        |   +---images
        |   |       *.gif
        |   |
        |   \---js
        |
        \--PERL
           \-- *.tar.gz    (Modules PERL fournis avec la distribution)
```

Figure 1 - Arborescence sous répertoire netMETdistrib-x.y_z.v

2.2 Installation

L'installation de netMET se décline en trois étapes, à réaliser sous le compte "**root**" :

Etape	Commandes	Explications
1	root# **cd /home/netmet/netMETdistrib-x.y**	Positionnement dans le répertoire de travail
2	root# **./install.sh**	Installation de netMET - Répondre Yes à chaque question. - Pour "l'installation Mode", répondre : - 12 : Si vous ne voulez faire que de la métrologie et les stats Renater - 13 : Si vous ne voulez faire que de la sécurité - 123 : Si vous voulez faire les deux, ou si vous avez encore des interrogations sur ce que vous voulez faire :-)
3	root# **more install-netmet.log**	Lister le fichier de log, pour voir ce qui s'est passé et ce qu'il reste à faire.

L'installation crée un répertoire netMet avec l'arborescence suivante :

```
netMet
|   LICENCE
|   netMETacc, netMETexp
|   netMETcll, netMETscn
|
+---cron
|       *cron
|
+---duplicator
|       netMETdup -> ../netMETdup
|
+---etc
|       explt.conf
|       organism.def
|       apache.group
|       apache.passwd
|
+---init.d
|       netmet
|       netmetDUP
|       netmetSECURE
|       *.sh
|
+---metro (secure10m / secure24h / stats)
|   |   netMETacc
|   |   netMETcll
|   |   netMETexp
|   |   netMETscn
|   |
|   \---etc
|
+---scripts
|       *.pl / *.sh / *.pm / *.js
|       getIF.sh
|
+---scripts-cgi
\       *.cgi
```

Figure 2 - Arborescence du répertoire netMet

3 Configuration de netMET

3.1 Contexte

Comme cela vous est indiqué dans le fichier install-netmet.log, la phase suivante est la configuration des différents fichiers de configuration utilisés par netMET.

Prenons un exemple pour détailler les étapes de la configuration à mettre en place. Nous avons un routeur avec 2 interfaces. Par exemple, l'une série (Serial0), l'autre FastEthernet (FE0/0) vers les sites et une interface ATM (ATM2/0) vers Renater.

Comme nous l'avons conseillé, la machine de métrologie (metro) est au plus proche du routeur (mon_routeur) qui renvoie les NetFlow.

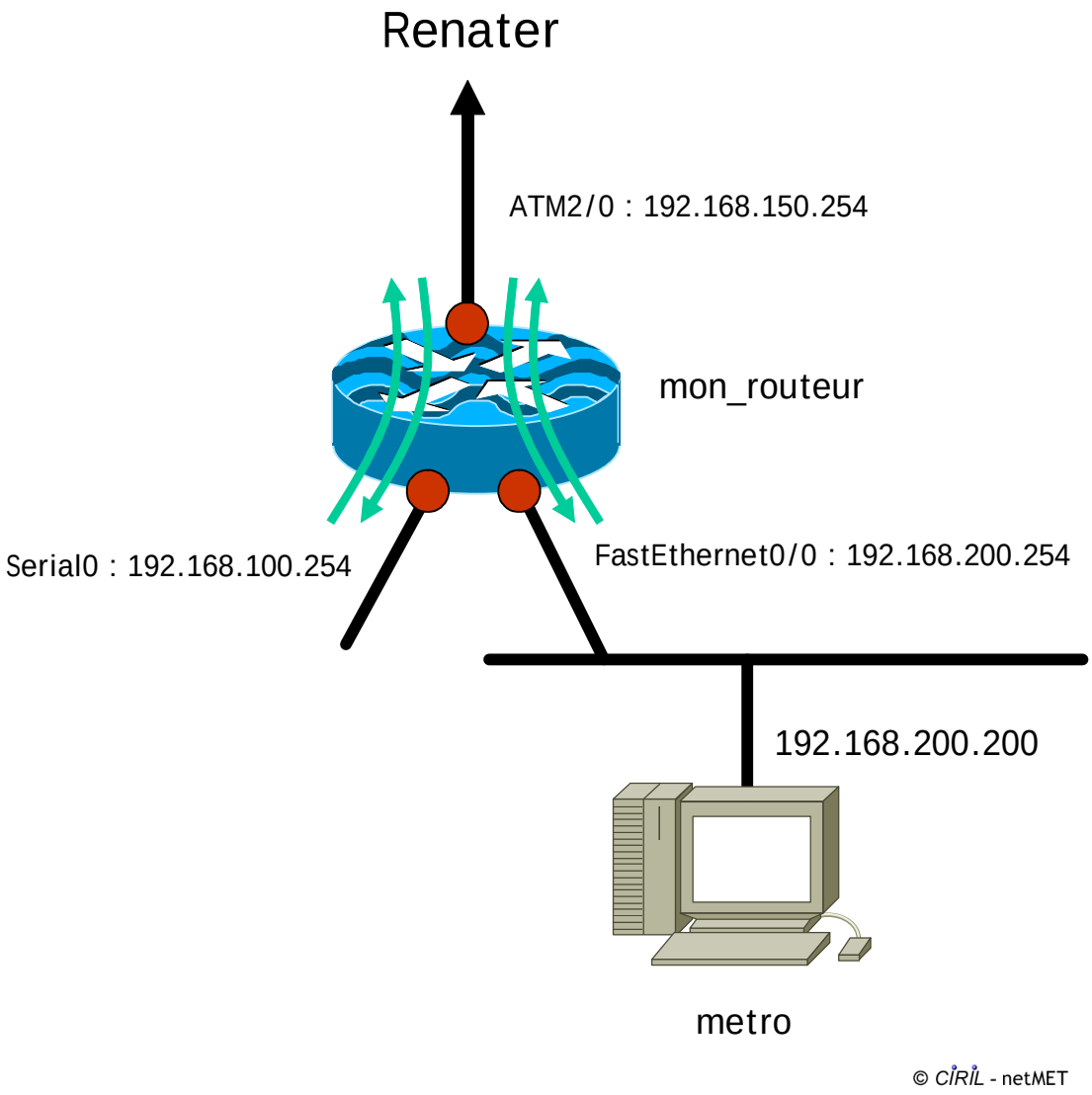

Figure 3 - Exemple de configuration d'interconnexion à Renater

Attention : Pour cette 3ème partie, nous repassons en user "netmet" et nous nous positionnons dans le répertoire de travail /home/netmet/netMet.

3.2 Configuration du duplicateur

Le duplicateur a pour fonction d'écouter sur le port où arrivent les paquets UDP NetFlow en provenance d'un routeur ou d'une autre machine, et de les renvoyer vers d'autres ports où écoutent des collecteurs dont la fonction est de traiter ces paquets selon certaines règles (grammaire et fichier de configuration des collecteurs).
En standard le duplicateur écoute sur le port 8080 et renvoie vers les ports 8081, 8082, 8083, 8084 qui correspondent respectivement aux collecteurs dont les fonctionnalités sont :

- metro : collecte sur 24h, agrégée
- stats : collecte sur 5mn, agrégée
- secure10m : collecte sur 10mn, non agrégée
- secure24h : collecte sur 24h, non agrégée

<table>
<tr><th>Etape</th><th>Commandes</th><th>Explications</th></tr>
<tr><td>1</td><td>netmet> cd /home/netmet/netMet</td><td>Positionnement dans le répertoire de travail</td></tr>
<tr><td>2</td><td>netmet> vi init.d/NETMET_DUPstart.sh</td><td>Remplacer les xxx.xxx.xxx.xxx dans :
<table><tr><td>-listen
xxx.xxx.xxx.xxx</td><td>Par l'adresse IP de la carte réseau sur laquelle les paquets UDP NetFlow vont arriver (si votre machine n'a qu'une carte, c'est simplement l'adresse IP de votre machine) (192.168.200.200)</td></tr><tr><td>-d
xxx.xxx.xxx.xxx/port</td><td>Même adresse IP que çi-dessus, car nos collecteurs tournent sur la même machine que le duplicateur.
Et par défaut, nous utilisons les ports 8081,8082,8083 et 8084.
Remarque : Si vous souhaitez ne pas utiliser tel ou tel collecteur, supprimer le paramètre -d correspondant.</td></tr></table>
ATTENTION : ne pas utiliser l'interface loopback (127.0.0.0) comme adresse IP d'écoute ou de duplication</td></tr>
<tr><td>3</td><td>root# /usr/sbin/tcpdump -n 'dst port 8080'</td><td>Permet de vérifier que le routeur envoie bien des trames sur le port 8080 et sur quelle adresse IP.
(cf Figure 4)

ATTENTION : Il faut être connecté en root pour exécuter cette commande</td></tr>
</table>

```
root@metro [21] ~/netMet # /usr/sbin/tcpdump -n 'dst port 8080'
tcpdump: listening on eth0
15:51:54.974840 192.168.200.254.1031 > 192.168.200.200.8080: udp 1468
15:51:54.975445 192.168.200.254.1031 > 192.168.200.200.8080: udp 1468
15:51:54.976683 192.168.200.254.1031 > 192.168.200.200.8080: udp 1468
15:51:54.977124 192.168.200.254.1031 > 192.168.200.200.8080: udp 1468
15:51:54.977997 192.168.200.254.1031 > 192.168.200.200.8080: udp 1468

^C
27 packets received by filter
0 packets dropped by kernel
```


Figure 4 : Résultat de la commande tcpdump

3.3 Configuration des 4 collecteurs

La configuration des collecteurs consiste essentiellement en la configuration du fichier "netmet.conf", que l'on trouve dans le répertoire "etc" de chaque collecteur.
Nous n'allons pas entrer dans les détails, car il existe une documentation spécifique sur ce sujet ("Collecteur & fichier de configuration netmet.conf") que nous vous conseillons de lire attentivement avant de commencer cette configuration.

3.3.1 Le collecteur "metro"

<table>
<tr><th>Etape</th><th>Commandes</th><th>Explications</th></tr>
<tr><td>1</td><td>root# cd /home/netmet/netMet</td><td>Positionnement dans le répertoire de travail</td></tr>
<tr><td>2</td><td>netmet> vi metro/etc/netmet.conf</td><td>Remplacer :
<table><tr><td>hhh.hhh.hhh.hhh</td><td>Adresse IP de la machine (192.168.200.200)</td></tr><tr><td>pppp</td><td>Numéro de port d'écoute du collecteur (par défaut : 8081)</td></tr><tr><td>ggg.ggg.ggg.ggg</td><td>Adresse IP de l'interface du routeur d'où les paquets NetFlow proviennent et que le collecteur souhaite traiter (192.168.200.254)</td></tr></table></td></tr>
</table>

		IF_RENATER	**Clause IF_PROCESSED :** Clause qui nous permet d'indiquer que le collecteur ne doit garder que les NetFlow entre l'interface Renater et les interface de site, et qu'il doit ignorer les flows inter-site. L'interface est spécifée par la description, que l'on a dans la variable SNMP d'OID : (.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.ifIndex) Utiliser la commande **~netmet/netMet/scripts/getIF.sh mon_routeur** pour avoir la description de l'interface Renater (cf Figure 5 et "Collecteur & fichier de configuration netmet.conf") Dans notre cas l'interface Renater est spécifiée par le libellée : *"ATM2/0.999-aal5 layer"* **ATTENTION** : NE PAS OUBLIER LES " "
		IF_RENATER (rrr.rrr.rrr.rrr)	**Clause IF_AGGREGATION :** Clause qui permet d'indiquer que le collecteur doit agréger à la volée les adresses IP provenant de l'interface "Renater". Ces adresses seront remplacées par l'adresse d'agrégation spécifiée entre les parenthèses. Description de l'interface Renater telle que nous l'avons donnée dans la clause "IF_PROCESSED" (*"ATM2/0.999-aal5 layer"*) Adresse IP d'agrégation (Adresse IP Virtuelle) qui désigne le TROU NOIR Renater. Par convention nous utilisons l'adresse de l'interface Renater, ainsi sommes nous sûr de son unicité. Cette adresse correspond à la description donnée ci-dessus (*192.168.150.254*)

```
netmet@metro [007] ~/netMet/scripts> getIF.sh mon_routeur.domain.fr
RFC1213-MIB
interfaces.ifTable.ifEntry.ifDescr.1 = ATM2/0
interfaces.ifTable.ifEntry.ifDescr.2 = Serial0
interfaces.ifTable.ifEntry.ifDescr.3 = FastEthernet0/0
interfaces.ifTable.ifEntry.ifDescr.4 = ATM2/0-atm layer
interfaces.ifTable.ifEntry.ifDescr.5 = ATM2/0.0-atm subif
interfaces.ifTable.ifEntry.ifDescr.6 = ATM2/0-aal5 layer
interfaces.ifTable.ifEntry.ifDescr.7 = ATM2/0.0-aal5 layer
interfaces.ifTable.ifEntry.ifDescr.8 = Null0
interfaces.ifTable.ifEntry.ifDescr.9 = ATM2/0.999-atm subif
interfaces.ifTable.ifEntry.ifDescr.10 = ATM2/0.999-aal5 layer
```


Figure 5 : Choix de la "bonne" interface : le script getIF.sh

```
NETFLOW_LISTEN_ADDR_PORT { 192.168.200.200/8081 }

192.168.200.254
{
        SNMP_READ_COMMUNITY { "public" }

        IF_PROCESSED
        { "ATM2/0.999-aal5 layer" <-> OTHER }

        IF_AGGREGATION
        { "ATM2/0.999-aal5 layer" (192.168.150.254) }
}
```


Figure 6 : Exemple de fichier netmet.conf

3.3.2 Le collecteur "stats"

Etape	Commandes	Explications
1	netmet> **cd /home/netmet/netMet**	Positionnement dans le répertoire de travail
2	netmet> **cp metro/etc/netmet.conf stats/etc/netmet.conf**	Copier le fichier netmet.conf du collecteur "metro"
3	netmet> **vi stats/etc/netmet.conf**	Remplacer le numéro de port 8081 par 8082

3.3.3 Le collecteur "secure10m"

Etape	Commandes	Explications
1	netmet> **cd /home/netmet/netMet**	Positionnement dans le répertoire de travail
2	netmet> **cp metro/etc/netmet.conf secure10m/etc/netmet.conf**	Copier le fichier netmet.conf du collecteur "metro"
3	netmet> **vi secure10m/etc/netmet.conf**	Remplacer le numéro de port 8081 par 8083 Supprimer la clause AGGREGATION (car dans le cas de la sécurité on veut conserver toutes les adresses IP)

3.3.4 Le collecteur "secure24h"

Etape	Commandes	Explications
1	netmet> **cd /home/netmet/netMet**	Positionnement dans le répertoire de travail
2	netmet> **cp metro/etc/netmet.conf secure24h/etc/netmet.conf**	Copier le netmet.conf du collecteur "metro"
3	netmet> **vi secure24h/etc/netmet.conf**	Remplacer le numéro de port 8081 par 8084 Supprimer la clause AGGREGATION (car dans le cas de la sécurité on veut conserver toutes les adresses IP)

3.3.5 Configuration des fichiers communs aux 4 collecteurs

<table>
<tr><th>Etape</th><th>Commandes</th><th colspan="2">Explications</th></tr>
<tr><td>1</td><td>netmet> cd /home/netmet/netMet</td><td colspan="2">Positionnement dans le répertoire de travail</td></tr>
<tr><td>2</td><td>netmet> vi etc/explt.conf</td><td colspan="2">Dans le paragraphe VARIABLES - VARIABLES - VARIABLES, initialisez par vos valeurs ou libellés les variables suivantes :
<table><tr><td>NETMET_ADMIN_NET_NAME</td><td>Nom de votre réseau (qui apparaîtra dans les pages Web) (sans espace)</td></tr><tr><td>NETMET_FEDERATE_NET_NAME</td><td>Nom réseau fédérateur
ATTENTION : Même libellé que dans etc/organism.def (sans espace)</td></tr><tr><td>NETMET_FEDERATE_NET_ADDR</td><td>Adresse d'agrégation réseau fédérateur (cf. metro/etc/netmet.conf)</td></tr><tr><td>NETMET_EXPLT</td><td>Mots clefs à mettre ou à supprimer selon les fonctionnalités Web souhaitées</td></tr></table></td></tr>
</table>

			TOP_N_ALL, TOP_N_BY_ORGA, DETAILLED_METRO, STATS, DETECT_SCANS
		NETMET_HOST_TOP_N	Nombre de machines dans le Top des machines
		NETMET_ORGA_TOP_N	Nombre d'organismes dans le Top des organismes
		NETMET_TOP_N_BY_ORGA	Nombre de machines dans les Top par organismes
		NETMET_DETAILLED_TABLE_THRESHOLD	Seuil de précision pour l'affichage de la métrologie détaillé sous la forme d'une table (pourcentage : xx%)
		NETMET_DETAILLED_PIE_THRESHOLD	Seuil de précision pour l'affichage de la métrologie détaillé sous la forme d'un camembert (pourcentage : xx%)
		NETMET_INFORMATIONS_URL	URL de la page d'information
		NETMET_SCANS_THRESHOLD_C	Seuil de détection de scans sur un réseau de classe C
		NETMET_SCANS_THRESHOLD_B_A	Seuil de détection de scans sur un réseau de classe B ou A
		NETMET_SCANS_PORT	Seuil de détection de scans "en largeur" sur une machine
		NETMET_SECURE_RR	Délai de conservation des fichiers de sécurité
3	netmet> **vi etc/organism.def**	Fichier qui contient les couples (SubnetIP, libellé de l'organisme) **SANS RECOUVREMENT** d'adresses IP - Le subnetIP est saisie sous la forme adresse-réseau/masque.(CIDR) - Le libellé de l'organisme doit être entre "" et sans espace **Remarque** : rrr.rrr.rrr.rrr correspond à l'adresse IP virtuelle qui désigne le réseau fédérateur, c'est à dire l'adresse utilisée lors de la configuration des collecteurs. (NETMET_FEDERATE_NET_ADDR) Un exemple est donné dans la Figure 7		

```
192.168.200.254/32      "RENATER"
192.180.0.0/16          "ORGA1"
192.168.100.0/24        "ORGA2"
192.168.200.64/27       "ORGA3"
192.168.200.96/27       "ORGA3"
192.168.200.128/27      "ORGA3"
```


Figure 7 : Exemple de fichier organism.def

4 Configuration du système

Attention : Pour cette 4ème partie, il faut être connecté en root

4.1 Configuration du démon SYSLOG

Etape	Commandes	Explications
1	root# **vi /etc/syslog.conf**	Invalider les lignes concernant les logs "user", sauf la dernière qui a été ajoutée par netMET, et qui indique que le renvoi des logs se fait dans le fichier /var/log/netmet
2	root# **/etc/rc.d/init.d/syslog restart**	Redémarrage du démon syslog

4.2 Configuration du serveur Apache

Un "technical tips" sur la configuration d'Apache est disponible sur le site http://www.netmet-solutions.org .

Nous donnons ici la configuration Apache de base nécessaire pour mettre en œuvre netMET.

<table>
<tr><th>Etape</th><th>Commandes</th><th>Explications</th></tr>
<tr><td>1</td><td>root# vi /etc/httpd/conf/httpd.conf</td><td>Activer les cgi en décommentant si nécessaire la ligne "AddHandler cgi-script .cgi"

A la fin de ce fichier, on trouve la configuration du site virtuel : netMET

Partie générale
<table>
<tr><td>Satisfy</td><td>Définit la politique de sécurité :
any (par défaut) = Machine autorisée OU Authentification</td></tr>
<tr><td>AuthUserFile</td><td>Indique le path du fichier qui contient la liste des comptes Apache, utilisés pour l'authentification lors de l'accès au serveur virtuel (liste de login:passwd)

Par défaut, notre user est : netmet (passwd : nm)</td></tr>
<tr><td>AuthGroupFile</td><td>Indique le path du fichier qui contient les groupes Apache, utilisés pour l'authentification lors de l'accès au serveur virtuel (liste de group:users)</td></tr>
</table>
</td></tr>
</table>

	Par défaut, nos groupes sont : **netmet** et **netmet-cgi** (avec le user : netmet)
require	groupes ou users autorisés à consulter le site netMET. Par défaut, on autorise le group **netmet**
order	Ordre de consultation. Par défaut : **deny,allow**
deny from	Interdit pour : **all** (par défaut)
allow from	Autorisé pour : liste d'adresses IP, de subnets, ou de domaines

Partie CGI (Par défaut FERME car partie considérée comme critique)

Satisfy	Définit la politique de sécurité : **all** (par défaut) = Machine autorisée ET Authentification
AuthUserFile	Indique le path du fichier qui contient la liste des comptes Apache, utilisés pour l'authentification dans l'accès des scripts du serveur virtuel.
AuthGroupFile	Indique le path du fichier qui contient les groupes Apache, utilisés pour l'authentification dans l'accès des scripts du serveur virtuel.
require	Groups ou users autorisés à exécuter les cgi Par défaut, on autorise le group **netmet-cgi**
order	Ordre de consultation Par défaut : **deny,allow**
deny from	Interdit pour : **all** (par défaut)
allow from	Autorisé pour : liste d'adresses IP, ou de subnet, ou de domaine

Partie Serveur Virtuel

VirtualHost	

			Nom ou adresse IP de la machine qui héberge ce serveur Apache. (important si plusieurs cartes réseaux)
		User	Nom unix du compte netmet (Par défaut : **netmet**)
		Group	Nom du groupe unix auquel appartient le compte netmet (Par défaut : **users**)
		DocumentRoot	Répertoire du site. Par défaut : **/home/netmet/html**
		ServerName	Nom de votre serveur netMET
		ServerAdmin	Email de l'administrateur de site
2	root# **vi ~netmet/netMet/etc/apache.passwd**	Mettre les users autorisés à parcourir le site et/ou à exécuter les scripts Par défaut, nous avons l'utilisateur netmet qui est créé (passwd = nm)	
3	root# **vi ~netmet/netMet/etc/apache.group**	Mettre les groupes "Apache" autorisés à parcourir le site et/ou à exécuter les scripts. Par défaut, nous avons le group : netmet et nmcgi qui contiennent l'utilisateur netmet	
4	root# **/etc/rc.d/init.d/httpd restart**	Relancer le serveur Apache	
5	root# **tail /var/log/httpd/error_log**	Vérifier que le serveur a bien redémarré, ainsi que le suexec, qui doit endosser les droits (netmet, users) afin de pouvoir exécuter correctement les cgi.	

4.3 Personnalisation de votre serveur

Attention : pour cette partie, vous devez repasser en user "**netmet**"

Etape	Commandes	Explications
1	netmet> **cp votre_logo ~netmet/html/images/admin-logo.gif**	Copier votre logo dans le fichier netMET
2	**~netmet/html/informations.html**	Vous avez la possibilité de personnaliser la page "informations" de netMET. Cette page est statique et peut-être remaniée en fonction de vos besoins.
3	**http://mon_site_netMET**	Vérifier que le serveur est accessible

5 Arrêt et démarrage des services

5.1 Démarrage du duplicateur

Etape	Commandes	Explications
1	root# **/etc/rc.d/init.d/netmetDUP start**	Démarrer le duplicateur, écoutant les NetFlow sur le port 8080 et les renvoyant sur les ports des collecteurs.
2	root# **vi /var/log/netmet**	Lister le fichier de log Message de type : I Infos W Warning E Erreur

5.2 Test sur le collecteur METRO

Ce test permet de vérifier que la duplication et que la collecte se passent bien, et donc le paramétrage des fichiers netmet.conf, et l'accès snmp sur le routeur.

Etape	Commandes	Explications
1	netmet> **cd ~netmet/netMet/metro**	Positionnement dans le répertoire metro
2	netmet> **netMETcll --start**	Activer le collecteur " **metro** ".
3	netmet> **tail /var/log/netmet** netmet> **ps -aux**	**VERIFICATION** - via le fichier de log, qui permet de les messages d'erreur du collecteur - via les processus (netMETcll, netMETacc)
4	netmet> **netMETcll --kill**	Stopper la métrologie, et vérifier que le fichier zzaccounting.dmp est supérieur à 18 octets
5	netmet> **netMETexp -H zzaccounting.dmp**	Visualiser le contenu du fichier zzaccounting.dmp ----> @src @dst [port srt / protocole] (nb d'octets), ...
6	root# **cp ~netmet/netMETdistrib-x.y/install/etc/protocols /etc/protocols**	S'il manque des protocoles, faites une mise à jour avec le fichier fournit dans la distribution, ou en récupérant la dernière mouture sur le site officiel de netMET. Attention : Il faut être **root**
7	root# **cp ~netmet/netMETdistrib-x.y/install/etc/services /etc/services**	S'il manque des services, faites une mise à jour avec le fichier fournit dans la distribution, ou en récupérant la dernière mouture sur le site officiel de netMET.

		Attention : Il faut être **root**

5.3 Démarrage des services netMET

Etape	Commandes	Explications
1	root# **/etc/rc.d/init.d/netmet start**	Démarrer les services de métrologie (métro et stats) - Démarre les processus netMETcll, et netMETacc - Ajoute dans la crontab l'exploitation "Métrologie"
2	root# **/etc/rc.d/init.d/netmetSECURE start**	Démarrer les services de sécurité (secure10m et secure24h) - Démarre les processus netMETcll, et netMETacc - Ajoute dans la crontab l'exploitation "Securité"

5.4 Arrêt des services netMET

Etape	Commandes	Explications
1	root# **/etc/rc.d/init.d/netmet stop**	Arrêt de la métrologie - Arrêt des processus netMETcll et netMETacc - Suppression de la crontab l'exploitation "Métrologie"
2	root# **/etc/rc.d/init.d/netmetSECURE stop**	Arrêt de la sécurité - Arrêt des processus netMETcll et netMETacc - Suppression de la crontab l'exploitation "Securité"

6 Complément

6.1 Remarque sur les fichiers utilisés dans la crontab

Les fichiers utilisées pour la configuration du cron se trouvent dans le répertoire /home/netmet/netMet/cron. Voici leur nom et fonction :

Noms	Fonctions
ARCHIVEScron	Genère la page d'index des archives netMET
METROcron	Génère les stats pour la métrologie - Echantillonnage toutes les 10 mn - Stats journalière toutes les 10 mn - Stats hebdomadaires tous les Lundi à 01h37 - Stats mensuels tous les 1er jour du mois à 03h07
STATScron	Génère les stats pour Renater - Echantillonnage toutes les 5 mn - Stats journalières toutes les 10 mn - Stats hebdomadaires tous les Lundi à 01h07 - Stats mensuels tous les 1er jour du mois à 02h07
SECUREcron	Génère les fichiers pour la sécurité - Echantillonnage toutes les 10 mn (pour secure10m) - Echantillonnage toutes les 10 mn sur 24h (pour secure24h) - Rapport journalier sur les scans détectés à 00h07

Ces fichiers n'ont à priori pas besoin d'être modifiés.

6.2 Où sont les données et les résultats?

Les fichiers sont répartis dans 3 répertoires :

- data : pour la métrologie metro et stats
- secure : pour la sécurité secure10m et secure24h
- html : pour le web

Dans chacun d'eux, l'arborescence est pratiquement la même, à savoir un répertoire par mois noté année-mois, dans lequel on trouve un répertoire par jour noté année-mois-jour. Puis nous avons des fichiers ou des sous-répertoires selon la problématique.

```
/home/netmet
|
+---data
|   \---2003-02                              (Un répertoire par mois)
|       \---2003-02-18                       (Un répertoire par jour)
|           +---zzaccounting.dmp             (Fichier journalier)
|           \---STATS_FederNET
|               +---zzaccounting.dmp-xx-yy   (1 fichier par 5 minutes)
|
+---html
|   +---2003-02                    (Un répertoire par mois)
|       +---2003-02-18             (Un répertoire par jour)
|           +---SCANS              (Fichiers html & txt par organisme + 1 global)
|           +---DETAILLED_METRO    (1 fichier html par organisme)
|           +---TOP_N_ALL          (Fichiers html & png)
|           +---TOP_N_BY_ORGA      (Fichiers html & png)
|           \---STATS_FederNET     (Fichiers html & png)
\---secure
    \---2003-02                (Un répertoire par mois)
        \---2003-02-18        (Un répertoire par jour)
           +---zzaccounting.dmp         (1 fichier par jour)
            +---zzaccounting.dmp-xx-yy  (1 fichier par 5 minutes)
```

Figure 8 - Arborescence des données et résultats

Et voilà, il n'y a plus qu'à ..... Bon courage :-)

Documentation netMET		
par :	Annick FAUCOURT Cyril PROCH (maj) Sébastien Morosi (maj)	Annick.Faucourt@ciril.fr Sebastien.Morosi@ciril.fr
crée le :	Mars 2001	
mise à jour le :	2003-01-19	