Installation de la distribution *netMET (à partir de 4.0_5.6, mise à jour pour 4.3_5.7)*

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_aaaammjj*)

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_aaaammjj* où *aaaammjj* est la date de génération de l'archive distribuée.

Que signifient 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.

La version 4.0_5.6 est utilisée à l'Université de Lorraine sur une distribution «maison» développée par Alexandre Simon.
Elle est par ailleurs opérationnelle sur une Debian et le collecteur a été testé sur une distribution Ubuntu (9.04).

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

- l'interprète de commandes bash (http://www.gnu.org/software/bash)
- le compilateur C++ de Gnu (http://gcc.gnu.org)
- les générateurs flex (http://flex.sourceforge.net) et bison (http://www.gnu.org/software/bison)
- le GNU make (http://www.gnu.org/software/make)
- l'interprète Perl (http://www.perl.org)
- le serveur HTTP Apache : http://httpd.apache.org/
- l'outil RRDtool http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

Pour les codes C/C++ la bibliothèque net-snmp (http://www.net-snmp.org) est nécessaire.

Les modules Perl (http://www.perl.org) suivants sont nécessaires :

- CGI
- Date::Calc (n'est plus nécessaire à partir de l'exploitation 4.3)
- Encode
- English
- File::Basename (à partir de l'exploitation 4.3)
- File::Compare
- File::Copy
- File::Path
- File::Temp

- GD
- GD::Graph
- GD::Graph::area
- GD::Graph::bars
- GD::Graph::colour
- GD::Graph::lines
- GD::Graph::mixed
- GD::Graph::pie
- HTTP::Date
- IPC::Open2
- Mail::Send
- MIME::Lite
- MIME::Words
- NetAddr::IP (à partir de l'exploitation 4.3)
- Net::IP
- POSIX
- RRDs
- Socket
- Socket6
- Sys::Hostname
- Time::Local

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, lorsqu'ils ne sont pas absolus 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 de l'utilisateur **«netmet»**
2	**http://www.netmet-solutions.org**	Récupérer la distribution netMETdistrib-x.y_z.v_aaaammjj.tgz depuis le site officiel http://www.netmet-solutions.org
3	netmet> **tar zxvf netMETdistrib-x.y_z.v_aaaammjj.tgz**	Décompression de la distribution

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

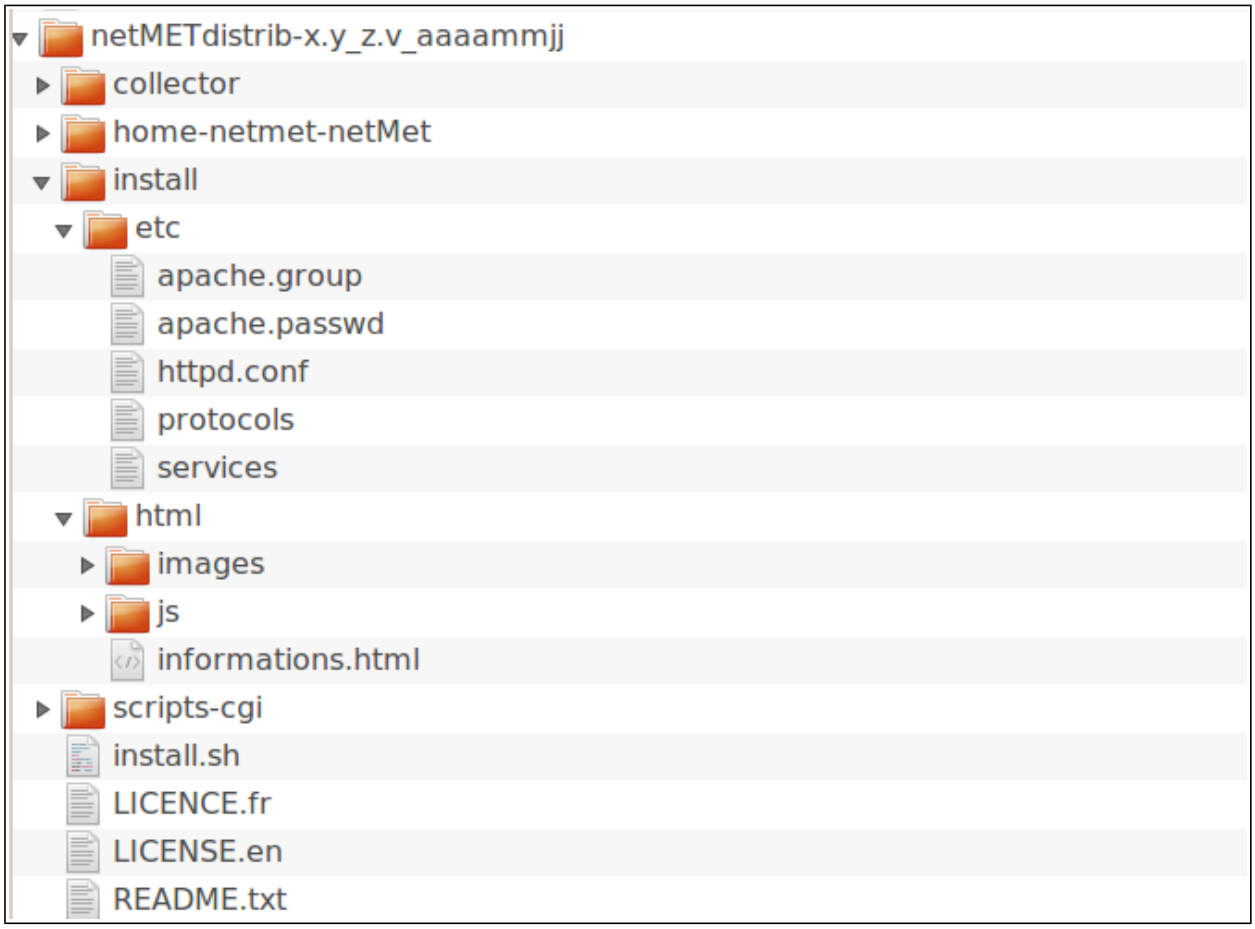

Figure 1 - Arborescence sous répertoire netMETdistrib-x.y_z.v_aaaammjj

2.2 Installation

L'installation de netMET se décline en trois étapes en étant connecté avec le compte «**root»** :

Etape	Commandes	Explications
1	root# **cd /home/netmet** root# **cd netMETdistrib-x.y_z.v_aaaammjj**	Positionnement dans le répertoire de travail
2	root# **./install.sh**	Installation de netMET - Si vous avez installé netMAT sur cette machine et que cette installation est à jour vous pouvez utiliser les exécutables du duplicateur et du collecteur de netMAT sous réserve que les droits d'accès soient correctement positionnés. Dans ce cas répondez «y» à la question «Is netMAT installed under /home/netmet and would you use the corresponding collector ? [y/n]». Vous devrez ensuite préciser le chemin d'accès à la distribution netMAT correspondante (/.../...//netMAT_dist_...aaaammjj) Si vous répondez «n», le duplicateur, le collecteur et les commandes associées seront compilés et placés dans le répertoire /home/netmet/netMet/bin. – Pour "l'installation Mode", répondre :

		- 12 : Si vous ne voulez faire que de la métrologie et les statistiques 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 :-) Si netMET était déjà installé sur cette machine (y compris une version 2.0_2.4 ou antérieure), le répertoire /home/netmet/netMet aura été sauvegardé et il vous sera demandé si vous souhaitez réutiliser les anciens paramètres de configuration et fichiers de configuration (de cron, des collecteurs, etc.). Dans l'affirmative il vous restera éventuellement à fixer les paramètres relatifs à l'IPv6. Si c'est la première installation de netMET ou si vous ne souhaitez pas réutiliser les anciens paramètres de configuration il sera demandé une adresse électronique pour l'envoi des rapports par le gestionnaire de tâches (cron). L'exécution du script se termine en vous indiquant ce qu'il vous reste à 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 :

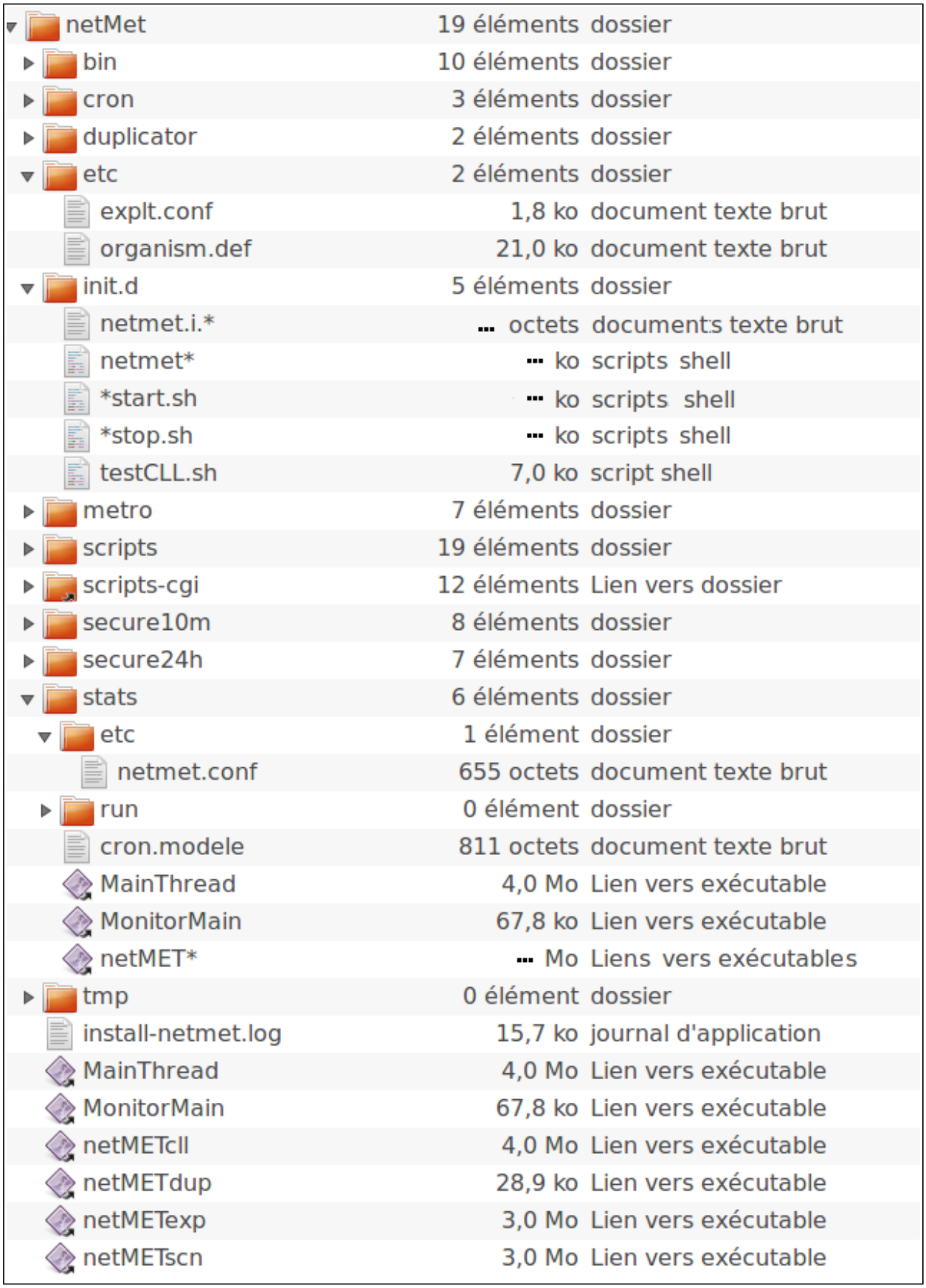

Figure 2 - Arborescence du répertoire netMet

3 Configuration de netMET

Si vous n'avez pas réutilisé les paramètres d'une installation précédente de netMET, la phase suivante est la mise à jour des différents fichiers de configuration utilisés par netMET.

Elle s'effectue en étant connecté en tant qu'utilisateur **netmet** et étant positionné dans le répertoire de travail /home/netmet/netMet.

3.1 Contexte

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 (noté metro sur la Figure 3) est au plus proche du routeur (mon_routeur) qui renvoie les NetFlow.

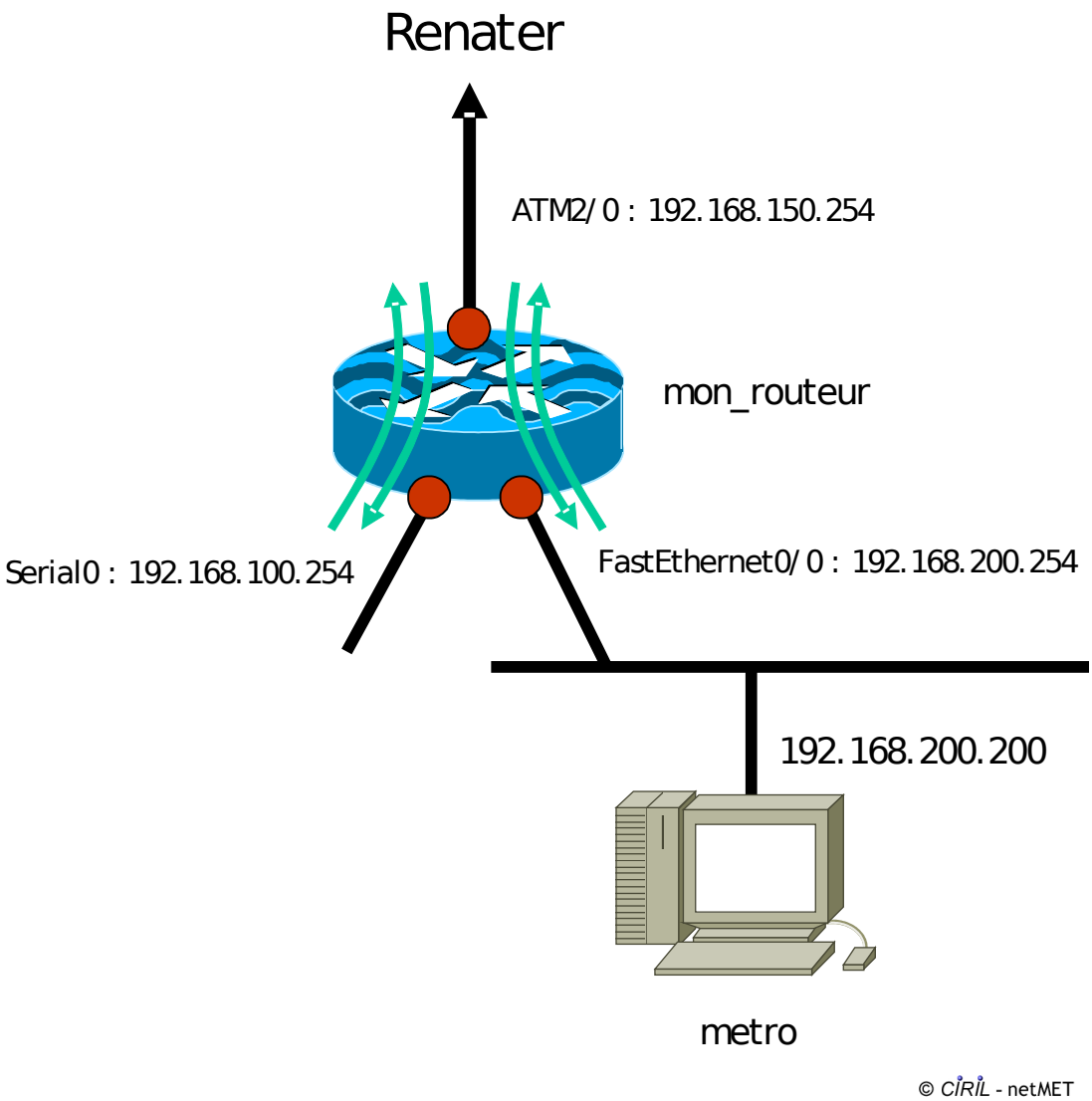

Figure 3 - Exemple de configuration d'interconnexion à Renater

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 écoutés par des collecteurs dont la

fonction est de traiter ces paquets selon certaines règles (cf. grammaire et fichier de configuration des collecteurs).
En standard le duplicateur écoute sur le port 8080 et renvoie vers les ports 8081, 8082 qui correspondent respectivement aux collecteurs dont les fonctionnalités sont :

- stats : collecte sur 5mn, agrégée
- secure10m : collecte sur 10mn, non agrégée

N.B. Depuis la version 4.0 les fonctionnalités metro et secure24h n'utilisent plus de collecteurs spécifiques.

<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>Dans les lignes comprises entre
----- DEBUT - CONFIGUREZ-MOI ----------
et
----- FIN - CONFIGUREZ-MOI ----------
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.
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 2 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 «stats»

<table>
<tr><th>Etape</th><th>Commandes</th><th colspan="2">Explications</th></tr>
<tr><td>1</td><td>root# cd /home/netmet/netMet</td><td colspan="2">Positionnement dans le répertoire de travail</td></tr>
<tr><td>2</td><td>netmet> vi stats/etc/netmet.conf</td><td colspan="2">Remplacer :</td></tr>
<tr><td></td><td></td><td>hhh.hhh.hhh.hhh</td><td>Adresse IP de la machine (192.168.200.200)</td></tr>
<tr><td></td><td></td><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>
<tr><td></td><td></td><td>IF_RENATER</td><td>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 sites.

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)</td></tr>
</table>

			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 " " **N.B.** Il peut y avoir plusieurs règles correspondant à plusieurs interfaces dans la clause.
		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*) **N.B.** Si la clause IF_PROCESSED comporte plusieurs règles correspondant à plusieurs interfaces la clause IF_AGGREGATION comportera elle aussi plusieurs règles, une par interface.

```
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 «secure10m»

Le fichier de configuration du collecteur «secure10m», /home/netmet/netMet/secure10m/etc/netmet.conf se configure presque de la même manière que celui du collecteur «stats» : le port d'écoute est différent (8082) et il n'y a pas de clause IF_AGGREGATION.

3.3.3 Configuration des fichiers communs aux 2 collecteurs

Etape	Commandes	Explications
1	netmet> **cd /home/netmet/netMet**	Positionnement dans le répertoire de travail

<table>
<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 :</td></tr>
<tr><td></td><td></td><td>NETMET_ADMIN_NET_NAME</td><td>Nom de votre réseau (qui apparaîtra dans les pages Web) (sans espace)</td></tr>
<tr><td></td><td></td><td>NETMET_ADMIN_MAIL</td><td>L'adresse à laquelle sont envoyés les rapports ; elle est renseignée par la commande install.sh.</td></tr>
<tr><td></td><td></td><td>NETMET_FEDERATE_NET_NAME</td><td>Nom du réseau fédérateur
ATTENTION : Même libellé que dans etc/organism.def (sans espace). La valeur par défaut est RENATER.</td></tr>
<tr><td></td><td></td><td>NETMET_FEDERATE_NET_ADDR
NETMET_FEDERATE_NET_V6_ADDR</td><td>Adresse d'agrégation réseau fédérateur IPv4 et IPv6 si nécessaire (cf. stats/etc/netmet.conf)</td></tr>
<tr><td></td><td></td><td>NETMET_EXPLT</td><td>Mots clefs à mettre ou à supprimer selon les fonctionnalités Web souhaitées :
TOP_N_ALL,
TOP_N_BY_ORGA,
DETAILLED_METRO,
STATS,
DETECT_SCANS
Il est possible d'enlever des fonctionnalités à la liste prédéfinie en fonction du choix (1,2,3) fait lors de l'installation, pas d'en ajouter.</td></tr>
<tr><td></td><td></td><td>NETMET_HOST_TOP_N</td><td>Nombre de machines dans le Top des machines</td></tr>
<tr><td></td><td></td><td>NETMET_ORGA_TOP_N</td><td>Nombre d'organismes dans le Top des organismes</td></tr>
<tr><td></td><td></td><td>NETMET_TOP_N_BY_ORGA</td><td>Nombre de machines dans les Top par organismes</td></tr>
</table>

		NETMET_TOP_N_PERIOD	Durée d'observation dans le top N des dernières minutes. (à partir de la version d'exploitation 4.3)
		NETMET_DETAILLED_TABLE_THRESHOLD	Seuil de précision pour l'affichage de la métrologie détaillée sous la forme d'une table (pourcentage : xx %)
		NETMET_DETAILLED_PIE_THRESHOLD	Seuil de précision pour l'affichage de la métrologie détaillée sous la forme d'un camembert (pourcentage : xx%)
		NETMET_SHOW_V4_V6	Lorsque ce paramètre est défini (i.e. la ligne est décommentée) le trafic IPv6 est compté séparément du trafic IPv4 dans les totaux.
		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	Durée 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 IPv4 virtuelle qui désigne le réseau fédérateur, c'est à dire l'adresse utilisée lors de la configuration des collecteurs. (NETMET_FEDERATE_NET_ADDR). De même xxxx:.../128 représente l'adresse IPv6 désignant le réseau fédérateur (NETMET_FEDERATE_NET_V6_ADDR). Si la collecte IPv6 est activée cette adresse doit être définie et la ligne décommentée.	

		Un exemple est donné dans la Figure 7
4	netmet> **vi cron/ARCHIVEScron**	Ce fichier contient entre autres les appels aux scripts de « nettoyage » des répertoires contenant les fichiers de collecte de la métrologie et du répertoire contenant les pages. Le nettoyage du répertoire contenant les fichiers de collecte de la métrologie et des statistiques est activé avec une durée de conservation de 10 mois par la commande **…/removeOldFiles.pl data .../etc/explt.conf 10** La durée de conservation peut être modifiée par l'utilisateur en fonction de son contexte. Le nettoyage du répertoire contenant les pages html figure en commentaire avec une durée de conservation de 24 mois : **#…/removeOldFiles.pl html .../etc/explt.conf 24** Il est bien entendu possible de décommenter la ligne et de changer la durée de conservation.
5	Facultatif netmet> **vi scripts/CONFmake.pl**	Ce script est appelé chaque jour pour archiver le fichier des organismes avec les collectes correspondantes et pour produire un nouveau fichier. Par défaut le nouveau fichier est une copie de l'ancien. L'utilisateur peut modifier ce script en fonction de son contexte.

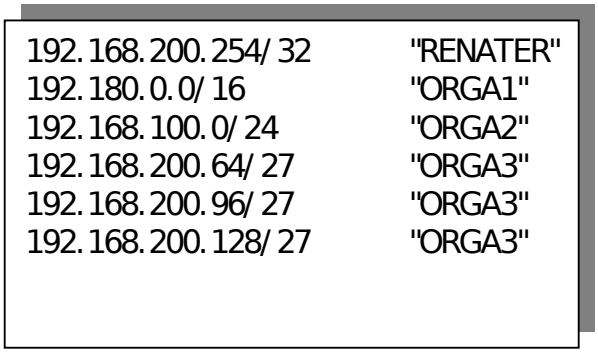

Figure 7 : Exemple de fichier organism.def

4 Configuration du système

4.1 Configuration du serveur Apache

Le répertoire install/etc de la distribution contient des exemples utiles à la configuration du serveur Apache.
Le fichier install/etc/httpd.conf une fois complété peut être inclus dans le fichier de configuration Apache du système, de préférence par une directive include.
Les fichiers install/etc/apache.passwd et install/etc/apache.group sont aussi donnés à titre d'exemple. Pour que les directives AuthUserFile et AuthGroupFile de httpd.conf soient correctes ces fichiers une fois complétés doivent être placés dans le répertoire /home/netmet/netMet/etc.

Les modifications à apporter au fichier /httpd.conf portent sur les directives :

- VirtualHost, ServerName : le nom « www.netmet-host.domain.fr » doit être remplacé par le nom ou l'adresse IP de la machine qui héberge ce serveur Apache.

- ServerAdmin : l'adresse électronique de l'administrateur du site

Le fichier install/etc/httpd.conf n'est donné qu'à titre d'exemple et chaque administrateur peut choisir une autre configuration, en particulier pour ce qui concerne l'authentification et les autorisations.
En revanche il est impératif que les règles de réécriture AliasMatch figurent dans la configuration.

```
# BEGIN - BEGIN - BEGIN - BEGIN - BEGIN - BEGIN - BEGIN
# Default configuration for netMET web server
# By            : Alexandre Simon (Alexandre.Simon@ciril.fr)
# Updated       : 2003/04/02
#
# conf. VIRTUAL HOST : www.netmet-host.domain.fr
# conf. DIRECTORY    : /home/netmet/html
# conf. DIRECTORY    : /home/netmet/html/cgi-bin

#NameVirtualHost netmet-host.domain.fr:80
<VirtualHost     netmet-host.domain.fr:80>
        Options                 FollowSymLinks IncludesNOEXEC ExecCGI Indexes
        User                    netmet
        Group                   users
#       SuexecUserGroup         netmet users    # a utiliser en Apache version 2.x
        DocumentRoot            /home/netmet/html
        ServerName              www.netmet-host.domain.fr
        ServerAdmin             moimeme@netmet-host.domain.fr
        ErrorLog                /var/log/httpd/netmet.error
        TransferLog             /var/log/httpd/netmet.access
        DirectoryIndex          index.cgi index.html
        AliasMatch      /netmet-cgi-bin/nmHOST-4.*-DETAILS(.*)\.cgi          /home/netmet/html/netmet-cgi-
bin/nmHOST-DETAILS$1.cgi
        AliasMatch      /netmet-cgi-bin/nmHOST-4.*-SERVICES(.*)\.cgi         /home/netmet/html/netmet-cgi-
bin/nmHOST-SERVICES$1.cgi
        AliasMatch      /netmet-cgi-bin/nmTOP_NforORGA4-.*\.cgi /home/netmet/html/netmet-cgi-
bin/nmTOP_NforORGA.cgi
        AddHandler      cgi-script      .cgi    .pl
</VirtualHost>

<Directory      "/home/netmet/html">
        Options                 FollowSymLinks          IncludesNOEXEC          ExecCGI Indexes
        AllowOverride           all
        Satisfy                 any
        AuthAuthoritative       on
        AuthUserFile            /home/netmet/netMet/etc/apache.passwd
        AuthGroupFile           /home/netmet/netMet/etc/apache.group
        AuthName                "netMET access's"
        AuthType                Basic
        require                 group netmet netmet-cgi
        order                   deny,allow
        deny from               all
#       allow from              host.domain.fr
</Directory>

<Directory      "/home/netmet/html/netmet-cgi-bin">
        Options                 IncludesNOEXEC ExecCGI
        AllowOverride           all
        Satisfy                 all
        AuthAuthoritative       on
        AuthUserFile            /home/netmet/netMet/etc/apache.passwd
        AuthGroupFile           /home/netmet/netMet/etc/apache.group
        AuthName                "netMET access's"
        AuthType                Basic
        require                 group netmet-cgi
        order                   deny,allow
        deny from               all
#       allow from              host.domain.fr
```

```
</Directory>

# Default configuration for netMET web server
# END - END - END - END - END - END – END
```

4.2 Personnalisation de votre serveur

Attention : pour cette partie, vous devez être connecté en tant qu'utilisateur **netmet**

Etape	Commandes	Explications
1	netmet> **cp votre_logo ~netmet/html/images/admin-logo.gif**	Remplacez le logo fourni par le votre dans le répertoire /home/netmet/html/images.
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 Répertoire init.d

Le répertoire init.d contient les fichiers nécessaires à la mise en œuvre du service netmet.
Si vous utilisez le système init de System V (/etc/rc.d) ou initng le script d'installation effectue les mises à jour nécessaires. Sinon vous devrez le faire en utilisant les fichiers contenus dans /home/netmet/netMet/init.d.

Noms	Fonctions
netmet.i.*	Ces fichiers correspondent aux différentes configurations possibles du service initng. En fonction du choix de l'utilisateur l'un d'entre eux est recopié dans /etc/initng/service/netmet.i lors de de l'installation de netmet.
netmetDUP netmet netmetSECURE	Démarrage/arrêt - du duplicateur - de la métrologie et des statistiques - de la sécurité selon la valeur du paramètre (start, stop, restart). Ces scripts sont copiés dans /etc/rcXXX.d si la commande update-rc.d est disponible.
NETMET_DUPstart NETMET_DUPstop	Lancement/arrêt de l'exécution du duplicateur. Ce script est utilisé par les scripts init.d/netmetDUP et init.d/netmet.i.1*

NETMETstart NETMETstop	Lancement/arrêt de l'exécution de la métrologie et des statistiques. Ce script est utilisé par init.d/netmet.
NETMET_SECUREstart NETMET_SECUREstop	Lancement/arrêt de l'exécution de la sécurité. Ce script est utilisé par le script init.d/netmetSECURE.
METRO_STATS_SECUREstart METRO_STATS_SECUREstop	Lancement/arrêt de l'exécution de la métrologie et des statistiques et/ou de la sécurité en fonction de la liste d'argumets (metro_stats secure). Ce script est utilisé par les scripts init.d/netmet.i.*.
testCLL.sh	Test du collecteur : init.d/testCLL.sh { stats | secure} start *nombre_de_flux* lance le collecteur avec la configuration stats/etc/netmet.conf ou secure10m/etc/netmet.conf selon le paramètre jusqu'à ce qu'au moins *nombre_de_flux* ait été collectés, affiche la trace des flux collectés sur la sortie standard et arrête la collecte. S'il est nécessaire d'arrêter la collecte avant que la limite soit atteinte il est possible d'utiliser : init.d/testCLL.sh { stats | secure} stop

5.2 Test du duplicateur et des collecteurs

Pour cette partie, vous pouvez être connecté en tant qu'utilisateur **netmet**

La suite de commandes suivante permet de vérifier la syntaxe des fichiers de configuration et de tester le bon fonctionnement des collecteurs.

Etape	Commandes	Explications
1	netmet# **cd ~/netMet**	Se placer dans le répertoire netMet
2	netmet# **bin/configurationFileCheck stats/etc/netmet.conf** netmet# **bin/configurationFileCheck secure10m/etc/netmet.conf**	Tester la correction des fichiers de configuration des collecteurs. La commande configurationFileCheck affiche la configuration sous forme synthétique et signale les éventuelles erreurs en indiquant le numéro des lignes erronées.
3	netmet# **bin/subnetFileCheck etc/organism.def**	Tester la correction du fichier descriptif des sous-réseaux. Ce n'est pas indispensable pour tester les collecteurs, mais c'est utile à l'exploitation complète.
4	netmet# **init.d/NETMET_DUPstart**	Démarrer le duplicateur, écoutant les NetFlow sur le port 8080 et les renvoyant sur les ports des collecteurs.

<table>
<tr><td>5</td><td>netmet# sudo grep duplicator /var/log/syslog.log</td><td>Lister le fichier de log (il faut éventuellement se connecter en tant que root)
Message de type :<table><tr><td>I</td><td>Information</td></tr><tr><td>W</td><td>Avertissement</td></tr><tr><td>E</td><td>Erreur</td></tr></table>Des messages d'informations indiquent les sockets ouverts, le port de lecture et les ports d'écriture.</td></tr>
<tr><td>6</td><td>netmet# init.d/testCLL.sh stats start 1</td><td>Test du collecteur « stats ». Si tout fonctionne la commande se termine dès que 1 flux a été collecté et en affiche la trace : l'adresse du routeur, les numéros des interfaces d'entrée et de sortie, l'IP de la source, le port, le protocole, l'IP de la destination, le port, le nombre d'octets du flux.
La trace se termine par l'affichage du nom du fichier de collecte.</td></tr>
<tr><td>7</td><td>netmet# netMETexp –H nom_du_fichier_de collecte</td><td>Visualiser le contenu du fichier de collecte dont le nom a été affiché lors de l'exécution de la commande précédente.
Les trois premières lignes contiennent :
- la date de début de collecte (Unix time)
...- la date de fin de collecte (Unix time)
- la durée de la collecte en secondes.
Les suivantes sont de la forme
@src @dst [port dest / protocole] (nb d'octets) …
Vous pouvez vérifier qu'il y a bien agrégation sur la source ou la destination.</td></tr>
<tr><td>8</td><td>netmet# rm nom_du_fichier_de collecte</td><td>Ne pas oublier de détruire le fichier de collecte. Ces fichiers peuvent être très volumineux.</td></tr>
<tr><td>9...</td><td>netmet# init.d/testCLL.sh secure start 1</td><td>Test du collecteur « secure ». Le fonctionnement est le même que pour le collecteur « stats » (sans agrégation des adresses du réseau fédérateur).</td></tr>
<tr><td>...</td><td>netmet# init.d/NETMET_DUPstop</td><td>Arrêter le duplicateur.</td></tr>
<tr><td>N.B.</td><td>netmet# init.d/testCLL.sh stats stop
ou
netmet# init.d/testCLL.sh secure stop</td><td>En cas de problème, si le collecteur ne s'arrête pas, la commande testCLL.sh s'utilise avec l'argument stop</td></tr>
</table>

5.3 Démarrage/arrêt des services netMET (init system V)

Pour cette partie, vous devez être connecté en tant qu'utilisateur **root**

Etap	Commandes	Explications

e		
1	root# **/etc/rc.d/init.d/netmetDUP start** root# **/etc/rc.d/init.d/netmetDUP stop**	Démarrer/arrêter le duplicateur.
2	root# **/etc/rc.d/init.d/netmet start** root# **/etc/rc.d/init.d/netmet stop**	Démarrer/arrêter les services « métrologie » et « statistiques » - Démarrer/arrêter le processus MainThread - Mettre à jour la « crontab »
2	root# **/etc/rc.d/init.d/netmetSECURE start** root# **/etc/rc.d/init.d/netmetSECURE stop**	Démarrer/arrêter le service « sécurité » - Démarrer/arrêter le processus MainThread - Mettre à jour la « crontab »

5.4 Démarrage/arrêt des services netMET (initng)

Pour cette partie, vous devez être connecté en tant qu'utilisateur **root**

Etape	Commandes	Explications
1	root# **ngc -u service/netmet** root# **ngc -d service/netmet**	Démarrage/arrêt de netmet : - Démarrer/arrêter le duplicateur (netMETdup) - Démarrer/arrêter les 2 processus MainThread - Mettre à jour la « crontab »
2	root# **ngc -s**	Vérifier l'état du service

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 et dans les répertoire metro, stats, secure10m, secure24h. Voici leurs noms et fonctions :

Noms	Fonctions
cron/ARCHIVEScron	Génère la page d'index des archives netMET. Le fichier contient aussi les appels aux scripts de « nettoyage » des répertoires (removeOldFiles.pl). Le nettoyage du répertoire contenant les fichiers de collecte de la métrologie et des statistiques est activé avec une durée de conservation de 10 mois. Le nettoyage du répertoire contenant les pages html figure en commentaire avec une durée de conservation de 24 mois. Ces options peuvent être modifiées par l'utilisateur (cf. 3.3.3). N.B. Le « nettoyage » des fichiers de collecte « secure » est effectué chaque jour conformément au paramètre NETMET_SECURE_RR du

	fichier de configuration de l'exploitation (31 jours par défaut).
cron/CONFcron	Sauvegarde quotidiennement le fichier des organismes avec les fichiers de collecte correspondants et regénère un nouveau fichier des organismes, par défaut identique au fichier sauvegardé. Le script appelé pour effectuer cette tâche (scripts/CONFmake.pl) peut être personnalisé.
cron/MAILcron	MAILTO=adresse électronique de l'administrateur netMET
metro/cron.modele	Génère les statistiques pour la métrologie - Statistiques journalières toutes les 10 mn - Statistiques hebdomadaires tous les lundis à 01h37 - Statistiques mensuelles le premier de chaque mois à 03h07
stats/cron.modele	Génère les statistiques pour Renater - Echantillonnage toutes les 5 mn - Statistiques journalières toutes les 10 mn - Statistiques hebdomadaires tous les Lundi à 01h07 - Statistiques mensuelles le premier de chaque mois à 02h07
secure10m/cron.modele	Génère les fichiers pour la sécurité - Echantillonnage toutes les 10 mn
secure24h/cron.modele	Génère les fichiers pour la sécurité - Rapport journalier à 01h01 sur les scans détectés la veille

6.2 Où sont les données et les résultats?

Les fichiers sont répartis dans 3 répertoires :

- data : pour la metrologie et les statistiques
- secure : pour la sécurité
- 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 10 minutes)
```

Figure 8 - Arborescence des données et résultats

7 Utilitaires (à partir de 4.3_5.7)

7.1 Le script fast_update.sh

Lorsque la nouvelle distribution diffère peu de la précédente, en particulier lorsqu'il n'est pas nécessaire de recompiler le collecteur et les commandes associées, le script fast_update.sh permet de migrer vers la nouvelle distribution en recopiant dans les répertoire /home/netmet/netMet et /home/netmet/html/netmet-cgi-bin les fichiers modifiés.
Attention, le numéro et la date de version affichées dans les pages générées ne sont pas modifiés.
De plus le service **netMet doit être arrêté** avant d'exécuter le script.

7.2 Le script nmHOST_DETAILS.pl

Situé dans le répertoire /home/netmet/netMet/scripts c'est la version « ligne de commande » du script activé en cliquant sur le lien Details des « Tops N » des machines.
La commande construit les 3 graphes correspondants pour l'adresse IP et la période en argument.
Ces graphes sont conservés dans le sous-répertoire GRAPHER du répertoire associé à la période dans /home/netmet/html.
De plus ils sont envoyés par courriel à l'adresse électronique fournie.

`~/netMet/scripts/nmHOST_DETAILS.pl` *`adresse_IP`* *`periode`* *`adresse_mail`*

La période est soit une journée au format `aaaa-mm-jj`, un mois sous la forme `aaaa-mm` ou une semaine spécifiée par son numéro dans l'année sous la forme `aaaa-Week#ww`.

L'intérêt de cette commande est de permettre d'obtenir les graphes de détail lorsque leur durée de construction n'est pas compatible avec le « time out » du serveur.

7.3 Le script nmTOP_NforORGA.cgi

Situé dans le répertoire /home/netmet/html/netmet-cgi-bin ce script activé en cliquant sur le lien « Top N des X dernières minutes » de la barre de navigation est aussi utilisable en ligne de commande.

`~/html/netmet-cgi-bin/nmTOP_NforORGA.cgi [period=X] [organism=nom] [lastdate=aaaa-mm-jj_xxhmn]`

Le paramètre `period` est la durée de la période d'observation.
Lorsque ce paramètre est absent c'est le champ NETMET_TOP_N_PERIOD du fichier de configuration qui est utilisé.
En l'absence de ce champ, la valeur par défaut est 15.

`organism` est le nom de l'organisme à prendre en compte.
Lorsque que ce nom est celui du réseau fédérateur (champ NETMET_FEDERATE_NET_NAME du fichier de configuration, RENATER dans nos exemples) le top concerne l'ensemble des organismes du réseau métropolitain observé.
La valeur par défaut de ce paramètre est le nom du réseau fédérateur.

`lastdate` est la date et l'heure de fin de la période d'observation. En l'absence de ce paramètre ce sont la date et l'heure courante qui sont retenues.

Exécuté via une ligne de commande ce script affiche sur la sortie standard une feuille de calcul au format csv contenant le trafic entrant et sortant des "N" (cf. paramètre NETMET_HOST_TOP_N du fichier de configuration de netMet) adresses IP les plus consommatrices de bande passante rattachées à l'organisme dont le nom est donné en paramètre sur la période spécifiée.
Lorsque c'est possible le nom des machines est affiché ainsi que l'organisme de rattachement lorsque celui ci n'est pas déterminé par les paramètres de la commande.

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

Documentation netMET		
par :	Annick FAUCOURT Cyril PROCH (maj) Sébastien MOROSI (maj) Karol PROCH (maj)	Karol.Proch@univ-lorraine.fr
crée le :	Mars 2001	
mise à jour le :	2003-01-19 2013-09-24 2014-02-11	