Installation de la distribution *netMET (à partir de 5.1_5.9)*

Table des matières

1 Introduction

La version 5.1_5.9 marque une évolution majeure de l'interface de netMET par rapport aux versions précédentes (jusqu'à la 4.5_5.8). En revanche les informations fournies par netMET restant les mêmes, la collecte n'est pas affectée et les fichiers de configuration des collecteurs sont donc inchangés ainsi que le fichier définissant les sous-réseaux (fichier des organismes).
Contrairement aux versions précédentes de netMET, l'exploitation de la collecte ne nécessite plus la génération de pages HTML statiques. Les données collectées sont « compilées » pour produire des fichiers Json visualisés grâce à des scripts Javascript.
De ce fait le passage d'une version 4.5_5.8 (ou antérieure) de netMET à la version 5.1_5.9 amène une discontinuité dans l'affichage des résultats : les diverses pages statistiques antérieures à la date du changement de version ne sont plus accessibles avec la nouvelle interface.
Si vous souhaitez une transition en « douceur » il vous faudra conserver un accès aux anciennes pages ou conserver deux versions de netMET pendant une période de transition.
La présente documentation est pour l'essentiel une réécriture de la documentation « historique » de netMET.

1.1 Un peu de vocabulaire

Cette documentation décrit 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.

Un « service netMET » est une instance du logiciel netMET produite par la commande d'installation. Contrairement aux versions antérieures de netMET, les versions d'exploitation à partir de la 5.1 permettent l'installation de plusieurs services netMET sur une même machine sous réserve de modifier les fichiers de configuration fournis.

1.2 Les prérequis

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

La version 5.1_5.9 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/)
- le «framework» Mojolicious (http://mojolicious.org/)

Il est souhaitable de maîtriser les commandes système de base et de savoir configurer Apache, les fichiers de configuration fournis par la distribution (pour Apache, pour la « crontab », pour l'« init » système, etc.) pouvant ne pas convenir à votre configuration.

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

- Encode
- English
- Fcntl
- File::Basename
- File::Compare
- File::Copy
- File::Find
- File::Path
- File::Temp
- GD
- GD::Graph
- GD::Graph::bars
- GD::Graph::colour
- HTTP::Date
- IPC::Open2
- JSON::XS
- Mail::Send
- MIME::Lite
- MIME::Words
- Mojo::Base
- Net::IP
- POSIX
- RRDs
- Socket
- Socket6
- Sys::Hostname
- Time::Local

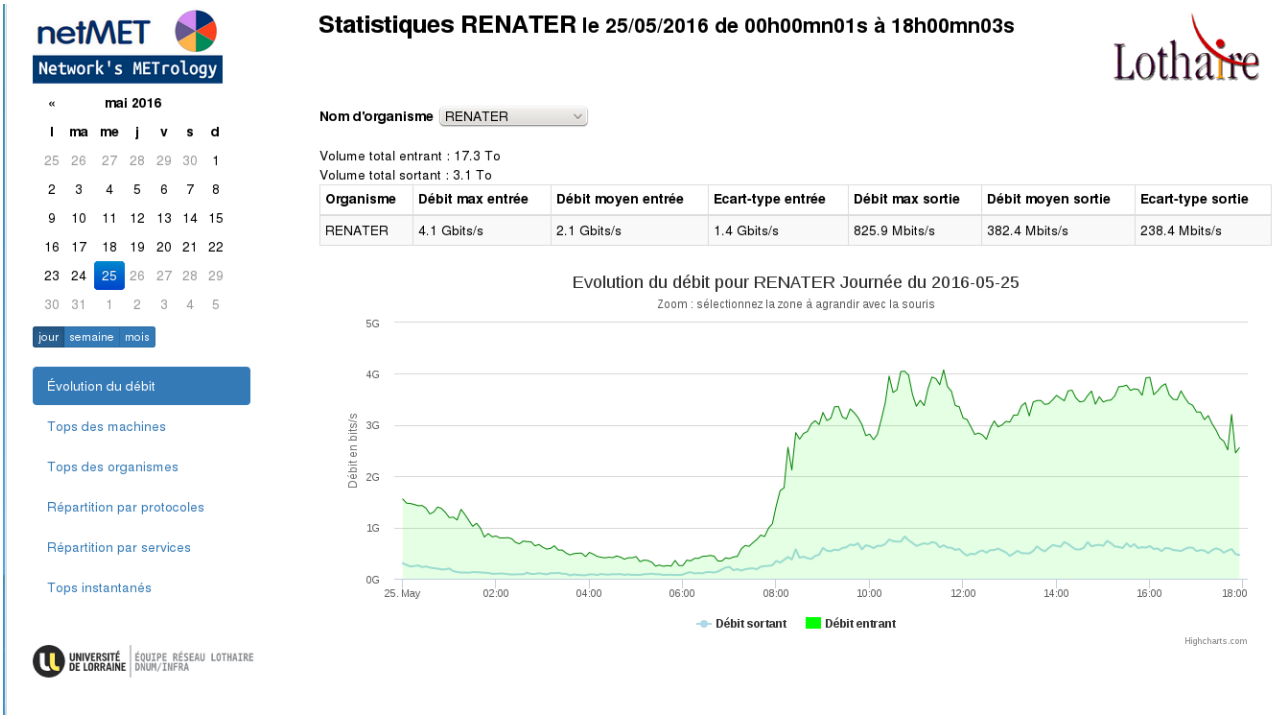
Les bibliothèques Javascript suivantes sont fournies dans la distribution :

- bootstrap
- bootstrap-datepicker
- highcharts
- jquery
- moment

ainsi que la bibliothèque de polices de caractères et de styles CSS font-awesome.

1.3 Une vue de l'interface

La nouvelle interface de netMET se présente sous cette forme :



2 Principe de fonctionnement

Les informations affichées par netMET concernent le trafic échangé entre un « réseau fédérateur » et un réseau « métropolitain » et sont obtenues par l'analyse des « netflows » envoyés à la machine de métrologie par le ou les routeurs assurant la connexion entre le réseau fédérateur et le réseau métropolitain.
Les netflows sont collectés, agrégés et conservés dans des fichiers de collecte selon des modalités paramétrables. Cette collecte est assurée par un duplicateur et deux collecteurs.
Les informations plus élaborées accessibles via une interface Web sont produites par des scripts d'exploitation de ces fichiers de collecte.

Prenons la configuration représentée par la figure 1 pour présenter le fonctionnement de netMET. Ce même exemple sera utilisé 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.
Le routeur **`mon_routeur`** renvoie les netflows à la machine de métrologie (notée `metro` dans cet exemple) d'adresse IP 192.168.200.200, de préférence située au plus proche du routeur.
Le duplicateur écoute sur le port où arrivent les paquets UDP contenant ces netflows, par défaut le **port 8080**, et les renvoie vers deux autres ports (par défaut les **ports 8081** et **8082**) écoutés par les deux collecteurs (nommés « `stats` » et « `secure` ») chargés de traiter ces paquets selon des règles décrites dans leurs fichiers de configuration.

Dans cet exemple seuls les netflows relatifs aux flux symbolisés par des flèches vertes sur la figure sont conservés, i.e. les netflows dont une seule des deux interfaces d'entrée ou de sortie est `ATM2/0`.

Le collecteur « `stats` » remplace dans les netflows conservés, l'adresse IP source ou destination correspondant à l'interface `ATM2/0` par l'adresse du réseau fédérateur 192.168.150.254. Le « monde extérieur » au réseau observé est ainsi considéré comme un tout, ce qui permet une agrégation des mesures.
Le collecteur « `secure` » conserve inchangées les adresses source et destination, permettant l'obtention d'informations plus détaillées sur le trafic observé.

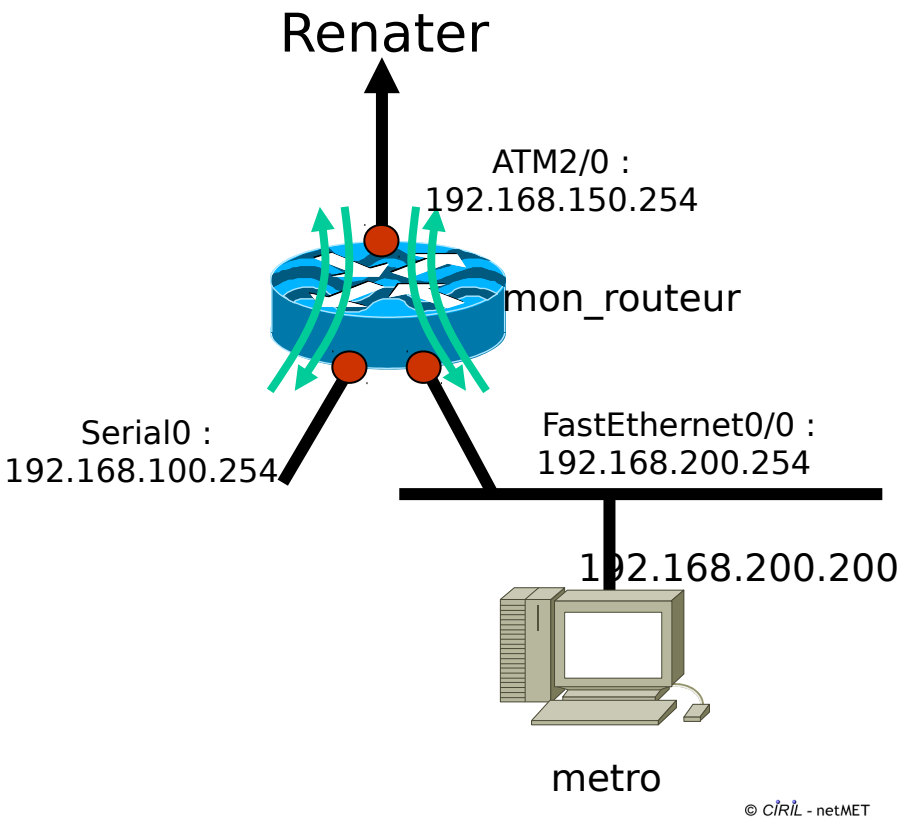


Figure1 - Exemple de configuration d'interconnexion à Renater

3 Installation de netMET

Contrairement aux versions antérieures il n'est plus indispensable de créer un utilisateur **«netmet»** ; netMET peut maintenant être installé à un emplacement quelconque par un utilisateur quelconque appartenant à un groupe quelconque.
Dans la la suite de ce documentation nous supposerons toutefois que le compte **«netmet»** appartenant au groupe **«netmet»** est utilisé pour installer, puis administrer la solution netMET.
Sauf indication contraire les commandes nécessaires à l'installation de netMET sont lancées en étant connecté avec l'utilisateur retenu (netmet dans notre exemple).

Par convention, lorsqu'ils ne sont pas absolus les chemins que nous indiquons sont relatifs au « home directory » de cet utilisateur netmet : **/home/netmet**.

3.1 Récupération de la distribution et extraction

Une fois la distribution netMET téléchargée depuis le site www.netmet-solutions.org dans un répertoire quelconque (`/home/netmet` par exemple) elle doit être décompressée :

```
netmet# tar xzvf  netMETdistrib-x.y_z.v_aaaammjj.tgz
```

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

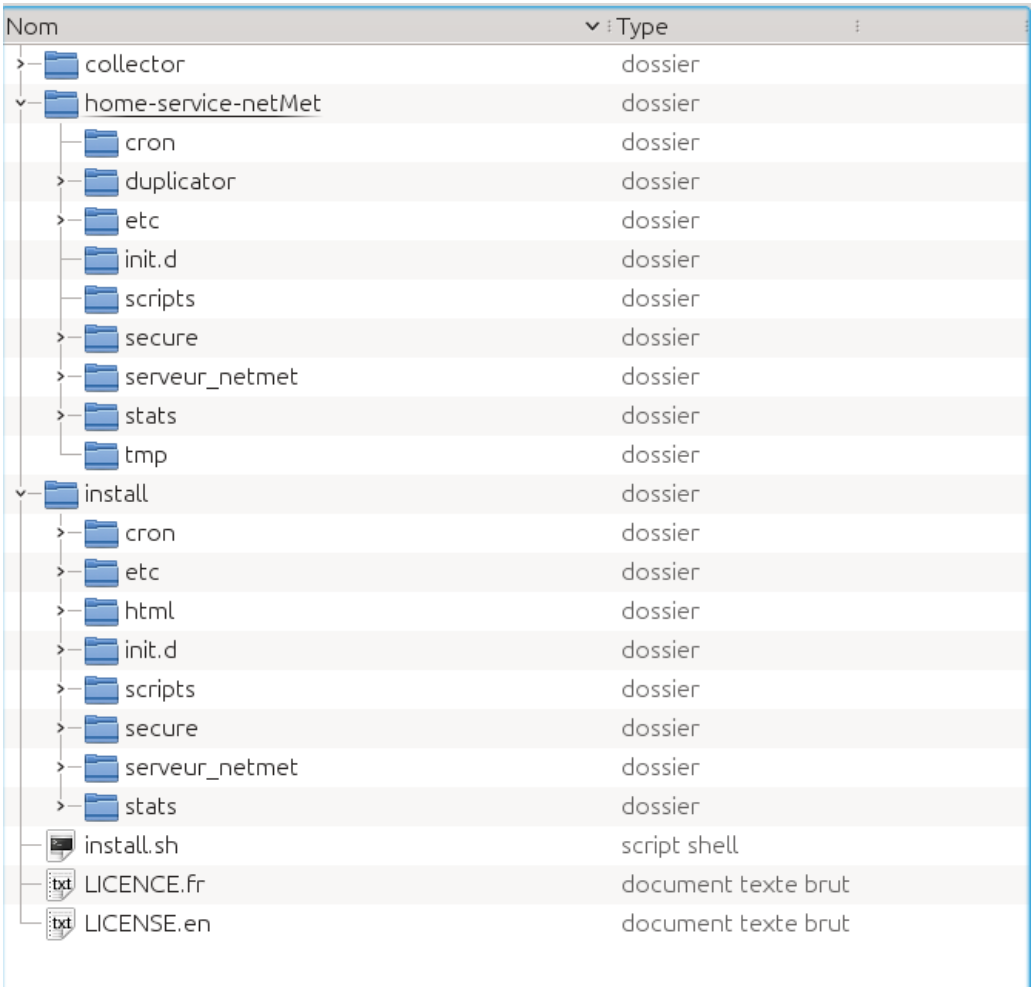


Figure 2 - Arborescence d'un répertoire netMETdistrib-x.y_z.v_aaaammjj

Le répertoire `collector` contient les fichiers sources C++ du duplicateur, du collecteur et des commandes associées à la collecte.
Le répertoire `home-service-netMet` est le modèle de l'arborescence du répertoire construit par la commande d'installation `install.sh`. Il contient des fichiers qui sont recopiés tels quels.
Le répertoire `install` a presque la même structure que `home-service-netMet` mais contient des fichiers modifiés lors de la procédure d'installation.
Enfin les fichiers `LICENCE.fr` et `LICENSE.en` contiennent les textes français et anglais de la licence couvrant le logiciel netMET (licence CeCILL).

3.2 Installation

Attention :

- Lors de l'installation, en particulier s'il s'agit d'une première installation, l'utilisateur est amené à saisir des paramètres de configuration. Il est donc indispensable de les préparer avant de lancer la commande.

L'installation s'effectue avec le script `install.sh` en étant situé dans le répertoire de la distribution, par exemple :

```
netmet#  cd /home/netmet/netMETdistrib-x.y_z.v_aaaammjj
netmet# ./install.sh /home/netmet   netMET_de_test
```

La première commande positionne le répertoire de travail dans le répertoire de la distribution préalablement dé-archivée.
La deuxième installe un service netMET dans le répertoire `/home/netmet` avec comme nom `netMET_de_test`.

Plusieurs cas de figure se présentent :

- C'est la première installation d'un service netMET sous ce nom dans le répertoire indiqué : vous allez devoir saisir les paramètres de configurations de netMET,
- un service netMET était déjà installé sur cette machine dans le même répertoire avec le même nom : l'ancien service sera sauvegardé et vous aurez la possibilité d'utiliser les paramètres de configuration de la version installée y compris dans le cas particulier où le répertoire d'installation est **/home/netmet,** le nom du service **netMet** et la version antérieure à la version 5.1. Les éventuelles paramètres manquants seront saisis par dialogue sur l'entrée standard.

Dans tous les cas l'exécution du script se termine en indiquant ce qu'il reste à faire.

3.2.1 Cas d'une première installation (pas de service netMET avec ce nom dans le répertoire indiqué)

La commande `install.sh` affiche la trace suivante sur la sortie standard (une partie de la trace a été supprimée pour alléger sa lecture) :

```
$ ./install.sh /home/netmet netMET_de_test
Checking PERL libraries ...
  Check library : Apache2::Const ... ok.
  Check library : Apache2::RequestIO ... ok.
  Check library : Apache2::RequestRec ... ok.
  Check library : CGI ... ok.
  Check library : Encode ... ok.
  Check library : English ... ok.
  Check library : Fcntl ... ok.
  Check library : File::Basename ... ok.
  Check library : File::Compare ... ok.
  Check library : File::Copy ... ok.
  Check library : File::Find ... ok.
  Check library : File::Path ... ok.
  Check library : File::Temp ... ok.
  Check library : GD ... ok.
  Check library : GD::Graph ... ok.
  Check library : GD::Graph::bars ... ok.
  Check library : GD::Graph::colour ... ok.
  Check library : HostDetails4Json ... ok.
  Check library : HTTP::Date ... ok.
  Check library : IPC::Open2 ... ok.
  Check library : JSON::XS ... ok.
  Check library : lib ... ok.
  Check library : Mail::Send ... ok.
  Check library : MIME::Lite ... ok.
  Check library : MIME::Words ... ok.
  Check library : Mojo::Base ... ok.
  Check library : Net::IP ... ok.
  Check library : netMETtk4Json ... ok.
  Check library : POSIX ... ok.
  Check library : RRDs ... ok.
  Check library : Running4Json ... ok.
  Check library : Socket ... ok.
  Check library : Socket6 ... ok.
  Check library : strict ... ok.
  Check library : Sys::Hostname ... ok.
  Check library : Time::Local ... ok.
  Check library : vars ... ok.
  Check library : XServUsers::ToolKit ... ok.
------------------------------------------------------------------------
Enter directory name for aggregated data collected (or return if /home/netmet/netMET_de_test/DATA) ?
®
Enter directory name for not aggregated (secure) data collected (or return if
/home/netmet/netMET_de_test/SECURE) ? ®
Enter directory name for resulting (json) files (or return if /home/netmet/netMET_de_test/HTML) ? ®
Enter directory name for computed data files (or return if
/home/netmet/netMET_de_test/COMPUTED_DATA) ? ®
Enter administrator email (for warning/error messages) ? monmail@chezmoi.fr
Enter netmet service URL ?netmet.monsite.fr
Enter federate net name (RENATER for example) ? RENATER
Enter federate net IPv4 address ? 192.168.150.254
Enter federate net IPv6 address or return if you don't collect IPv6 traffic ? ®
Enter netflows listen (IPv4) address (used by duplicator and collectors) ? 192.168.200.200
```

```
--------------------------------------------------------------------------------
Installing new netMET distribution under /home/netmet/netMET_de_test ...
Installing embedded netMET/netMAT collector ...for dir in ./src ./dependencies ; do \
          make -C $dir  all ; \
        done
… trace de la compilation des codes C++ (collecteur)
Embedded netMET/netMAT collector installation done.
--------------------------------------------------------------------------------
Directories cron
duplicator
etc
init.d
scripts
secure
serveur_netmet
stats
tmp created
--------------------------------------------------------------------------------
Checking data/secure/json directories...
  Check directory /home/netmet/netMET_de_test/HTML … /home/netmet/netMET_de_test/HTML created.
   /home/netmet/netMET_de_test/HTML/images created.
  Check directory /home/netmet/netMET_de_test/DATA … /home/netmet/netMET_de_test/DATA created.
  Check directory /home/netmet/netMET_de_test/SECURE … /home/netmet/netMET_de_test/SECURE created.
  Check directory /home/netmet/netMET_de_test/COMPUTED_DATA …
/home/netmet/netMET_de_test/COMPUTED_DATA created.
--------------------------------------------------------------------------------
Now you can edit configurations files :
   /home/netmet/netMET_de_test/stats/etc/netmet.conf
   /home/netmet/netMET_de_test/secure/etc/netmet.conf
   /home/netmet/netMET_de_test/etc/organism.def
You must probably update Apache configuration files (/etc/httpd/conf/httpd.conf
or /etc/apache/httpd.conf) :
        --> netMET directories, virtual host, ...
        --> AddHandler cgi-script .cgi
        --> DirectoryIndex index.cgi
Look a the file /home/netmet/netMET_de_test/etc/httpd.conf as an example of file to
include in an Apache configuration file.
--------------------------------------------------------------------------------

Complete the functions :
        netMETtk4Json::check_organism()
        netMETtk4Json::get_organisms_for_user()
        Auth_netMet::authorize_netmet()
if you need access control.
You can complete the function mkconfs() in /home/netmet/netMET_de_test/scripts/CONFmake.pl
for generating the "organism's" file (subnet's definitions).
--------------------------------------------------------------------------------
Use   /home/netmet/netMET_de_test/init.d/ngc-instal4netMET_de_test.sh   as  root  to  install  service
netMET_de_test for ngc
--------------------------------------------------------------------------------
********** netMET service netMET_de_test : installation completed. **********
```

La commande commence par vérifier la présence des bibliothèques Perl nécessaires.
En cas d'absence d'une ou plusieurs de ces bibliothèques la commande termine en affichant la liste des bibliothèques manquantes.
Sinon la commande se poursuit par la saisie des différents paramètres de configuration :

- les noms des différents répertoires où sont conservés les fichiers de collecte agrégés ou détaillés, les fichiers résultats au format Json et des fichiers de données pré-traitées ; l'utilisation de la touche Entrée (noté ® dans la trace ci-dessus) localise ces répertoires dans le répertoire du service avec des noms prédéfinis,
- l'adresse électronique de l'administrateur du service, c'est à cette adresse que seront envoyés les messages d'avertissement ou d'erreur,
- l'URL du service telle qu'elle figurera dans les fichiers de configuration d'Apache,
- le nom du réseau fédérateur,
- l'adresse IPv4 associée au réseau fédérateur (l'adresse IPv4 « d'agrégation » du réseau fédérateur),
- l'adresse IPv6 associée au réseau fédérateur (l'adresse IPv6 « d'agrégation » du réseau fédérateur) ; dans l'exemple aucune adresse IPv6 n'étant donnée le collecteur ignorera un éventuel trafic IPv6. Si une adresse IPv6 est saisie le dialogue se poursuit en demandant s'il faut distinguer dans la volumétrie le trafic IPv6 du trafic IPv4.

- L'adresse (IPv4) sur laquelle le duplicateur et les collecteurs reçoivent les netflows ; par défaut le duplicateur écoute les netflows sur le port 8080 et les duplique sur les ports 8081 et 8082 à destinations des collecteurs « stats » et « secure ».

Après vérification de ces paramètres (les différents noms de répertoires doivent être différents) le répertoire du service est créé (ici `/home/netmet/netMET_de_test`) et les différents fichiers source C++ du collecteur et des commandes associées sont compilés.

Une fois la compilation terminée les autres répertoires du service sont créés et initialisés.

La commande se termine en listant les opérations à effectuer pour rendre le service opérationnel.

Il reste à compléter
- les fichiers de configuration des collecteurs,
- le fichier d'« organismes »,
- le(s) fichier(s) de configuration d'Apache en s'inspirant du fichier cité,
- trois fonctions de modules Perl si les différents utilisateurs du service n'ont pas accès aux informations concernant tous les organismes,
- la fonction `mkconfs()` du module `scripts/CONFmake.pl` si le fichier descriptif des sous-réseaux (le fichier des « organismes ») doit être construit automatiquement.

Un script de mise en place du service est généré selon l'« init » du système :`initng`, `Sys V init`, `systemd`. (`initng` dans l'exemple ci-dessus)/

La figure 3 ci-dessous montre l'arborescence construite :
- le répertoire `bin` contient les exécutables issus de compilations C++, en particulier le code du collecteur et des commandes de traitement des données collectées,
- le répertoire `COMPUTED_DATA` destiné à contenir les données de collecte pré-traitées,
- le répertoire `cron` contient des modèles à charger dans la « crontab »,
- le répertoire `DATA` destiné à contenir les données collectées agrégées (flux dont la source ou la destination est remplacée par l'adresse du réseau fédérateur),
- le répertoire `duplicator` contient les informations relatives au duplicateur,
- le répertoire `etc` contient les fichiers de configuration de l'exploitation, en particulier `exploit.conf` qui regroupe les paramètres précédemment saisis, ainsi que le (modèle de) fichier des organismes (descriptif des sous-réseaux),
- le répertoire HTML destiné à contenir les fichiers générés par l'exploitation ainsi que les images utilisées dans l'interface,
- le répertoire `init.d` contenant les scripts d'initialisation, de démarrage et d'arrêt du service,
- le répertoire `scripts` contenant les divers scripts Perl de l'exploitation,
- le répertoire `secure` contient les informations nécessaires à la collecte sans agrégation des netflows, en particulier les liens vers les exécutables du collecteur (`MainThread` et `MonitorMain`), le fichier de configuration de cette collecte `etc/netmet.conf`, et le modèle des commandes à insérer dans la « crontab »,
- le répertoire `SECURE` destiné à contenir les données collectées non agrégées (i.e. les flux dont les adresses sources et destinations sont conservées telles quelles),
- le répertoire `serveur_netmet` contenant l'ensemble des fichiers nécessaires au serveur (scripts Perl, code et bibliothèques javascript, feuilles de style CSS…),
- le répertoire `stats` contient les informations relatives au collecteur des netflows avec agrégation, sa structure est analogue à celle de `secure`,
- le répertoire `tmp` utilisé pour des fichiers temporaires,
- enfin le fichier `history.log` qui permet de retrouver les différentes versions de netMET utilisées pour mettre à niveau le service au fur et à mesure des évolutions du logiciel.

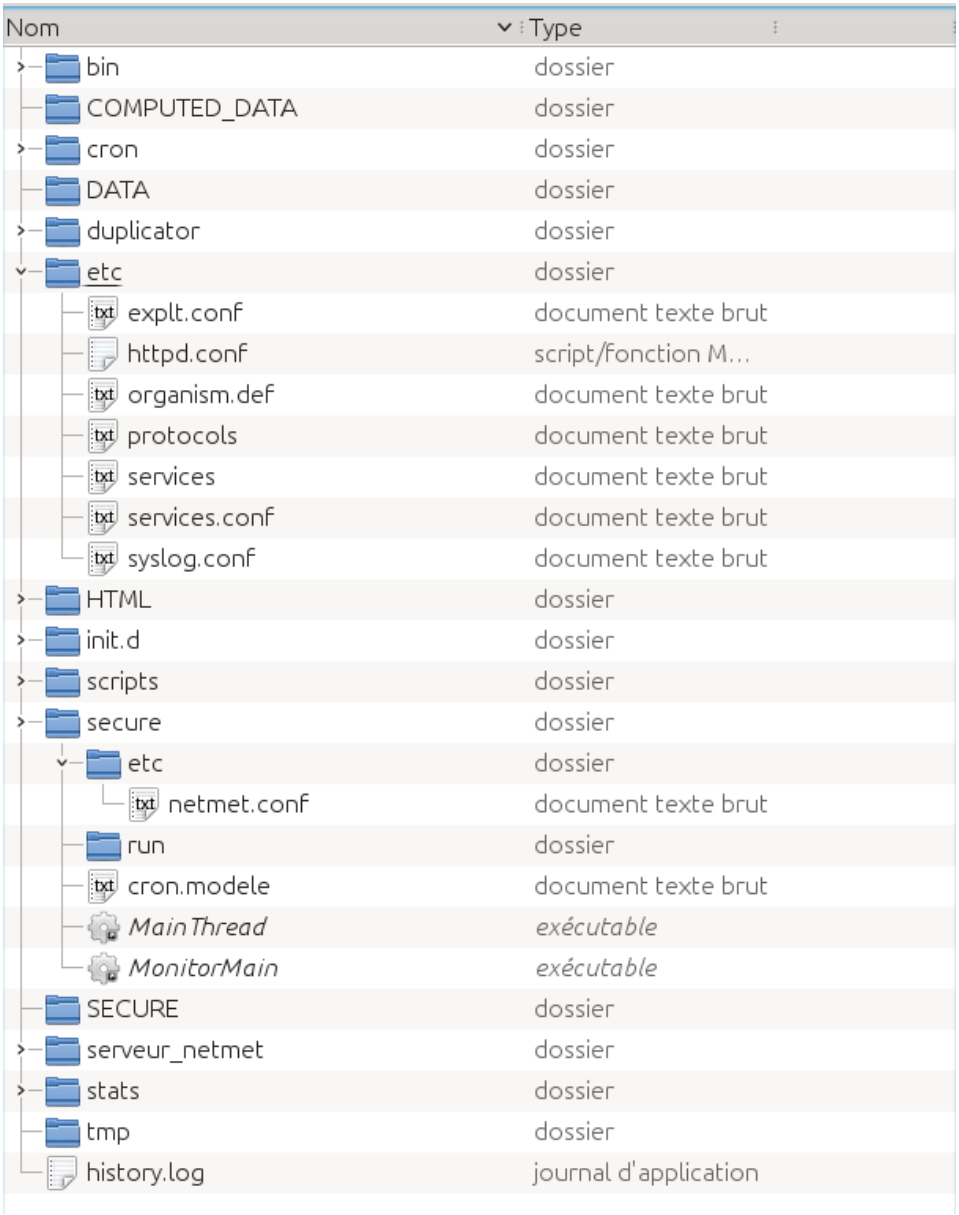


Figure 3 - Arborescence du répertoire du service netMET_de_test

3.2.2 Cas d'une mise à jour (il existe un service netMET de même nom et d'une version ≥ 5.1 dans le répertoire indiqué)

Dans le cas où il existe déjà un service netMET de même nom dans le même répertoire et dans une version d'exploitation supérieure ou égale à 5.1, le script demande s'il s'agit d'une mise à niveau. Dans l'affirmative (réponse « `y` ») les fichiers de configuration existants sont recopiés. Le script d'installation du service est toutefois reconstruit.

Attention :

- **il faut bien sûr arrêter le service avant de le mettre à jour,**
- **si vous avez ajouté des scripts d'exploitation et/ou modifié les fichiers contenant les modèles des commandes à insérer dans la « crontab » (`MAILcron`, `CONFcron`, `ARCHIVEScron`, `stats/crom.modele`, `secure/cron.modele`) vous devrez reporter ces modifications dans le répertoire du service recréé.**

```
$ ./install.sh /home/netmet/tmp netMETessai
Checking PERL libraries ...
  Check library : Apache2::Const ... ok.
  Check library : Apache2::RequestIO ... ok.
  Check library : Apache2::RequestRec ... ok.
```

```
  Check library : CGI ... ok.
  Check library : Encode ... ok.
  Check library : English ... ok.
  Check library : Fcntl ... ok.
  Check library : File::Basename ... ok.
  Check library : File::Compare ... ok.
  Check library : File::Copy ... ok.
  Check library : File::Find ... ok.
  Check library : File::Path ... ok.
  Check library : File::Temp ... ok.
  Check library : GD ... ok.
  Check library : GD::Graph ... ok.
  Check library : GD::Graph::bars ... ok.
  Check library : GD::Graph::colour ... ok.
  Check library : HostDetails4Json ... ok.
  Check library : HTTP::Date ... ok.
  Check library : IPC::Open2 ... ok.
  Check library : JSON::XS ... ok.
  Check library : lib ... ok.
  Check library : Mail::Send ... ok.
  Check library : MIME::Lite ... ok.
  Check library : MIME::Words ... ok.
  Check library : Mojo::Base ... ok.
  Check library : Net::IP ... ok.
  Check library : netMETtk4Json ... ok.
  Check library : POSIX ... ok.
  Check library : RRDs ... ok.
  Check library : Running4Json ... ok.
  Check library : Socket ... ok.
  Check library : Socket6 ... ok.
  Check library : strict ... ok.
  Check library : Sys::Hostname ... ok.
  Check library : Time::Local ... ok.
  Check library : vars ... ok.
  Check library : XServUsers::ToolKit ... ok.
------------------------------------------------------------------------------
Would you upgrade from previous service netMETessai (/home/netmet/tmp/netMETessai) ? [y/n] y
***     Warning     :     existing     directory     /home/netmet/tmp/netMETessai     is     renamed
/home/netmet/tmp/SAVEDnetMETessai20160517-1336
Upgrading new netMET service under /home/netmet/tmp/netMETessai ...
------------------------------------------------------------------------------
Installing embedded netMET/netMAT collector ...for dir in ./src ./dependencies ; do \
           make -C $dir  all ; \
        done
...
Embedded netMET/netMAT collector installation done.
------------------------------------------------------------------------------
Directories cron
duplicator
etc
init.d
scripts
secure
serveur_netmet
stats
tmp created
------------------------------------------------------------------------------
Checking data/secure/json directories...
  Check directory /home/netmet/tmp/HTML ...    Directory /home/netmet/tmp/HTML exist
          ***    Warning    :    existing    directory    /home/netmet/tmp/HTML/images    is    renamed
/home/netmet/tmp/HTML/images.old.20160517-1336 !
   /home/netmet/tmp/HTML/images created.
  Check directory /home/netmet/tmp/netMETessai/DATA …  /home/netmet/tmp/netMETessai/DATA created.
  Check directory /home/netmet/tmp/netMETessai/SECURE … /home/netmet/tmp/netMETessai/SECURE created.
  Check directory /home/netmet/tmp/COMPUTED_DATA … Directory /home/netmet/tmp/COMPUTED_DATA exist
------------------------------------------------------------------------------
Previous file etc/organism.def copied to /home/netmet/tmp/netMETessai/etc/organism.def.
Previous file html/images/admin-logo.gif copied to /home/netmet/tmp/HTML/images/admin-logo.gif.
Previous file stats/etc/netmet.conf copied to /home/netmet/tmp/netMETessai/stats/etc/netmet.conf.
Previous file secure/etc/netmet.conf copied to /home/netmet/tmp/netMETessai/secure/etc/netmet.conf.
Previous file etc/httpd.conf  copied to /home/netmet/tmp/netMETessai/etc/httpd.conf.
Previous    files    init.d/NETMET_DUPstart.sh    and    init.d/NETMET_DUPstop.sh        copied    to
/home/netmet/tmp/netMETessai/init.d.
------------------------------------------------------------------------------
Complete the functions :
        netMETtk4Json::check_organism()
```

```
        netMETtk4Json::get_organisms_for_user()
        Auth_netMet::authorize_netmet()
if you need access control.
You can complete the function mkconfs() in home/netmet/netMETessai/scripts/CONFmake.pl
for generating the "organism's" file (subnet's definitions).
-------------------------------------------------------------------------
Use    /home/netmet/tmp/netMETessai/init.d/ngc-instal4netMETessai.sh    as  root  to  install  service
netMETessai for ngc
-------------------------------------------------------------------------
********** netMET service netMETessai : installation completed. **********
```

Comme dans le cas précédent il reste à compléter les trois fonctions Perl `check_organisme()`, `get_organisms_for_user()` du module Perl `netMETtk4Json` et `authorize_netmet()` du module `Auth_netMet` si les différents utilisateurs du service ne doivent pas avoir accès à l'ensemble des informations et la fonction `mkconfs()` du module `scripts/CONFmake.pl` si le fichier descriptif des sous-réseaux (le fichier des « organismes ») doit être construit automatiquement.

3.2.3 Cas d'une mise à jour (il existe un service netMET de même nom et d'une version ≤ 5.1 dans le répertoire indiqué)

S'il existe un service netMET de même nom situé dans le répertoire indiqué dont la version est antérieure à 5.1 (les paramètres de la commande sont alors nécessairement **`/home/netmet`** et **`netMet`**), la commande demande s'il faut mettre à jour (« upgrader ») ce service. Dans l'affirmative seuls les paramètres de configuration manquants devront être saisis sur l'entrée standard lors de l'exécution de la commande : le nom du répertoire destiné à contenir les données de collecte pré-traitées et l'URL du service.

Attention :

- **là encore il faut arrêter le service avant de le mettre à jour,**
- **il n'y a pas continuité du service,** c'est-à-dire que les résultats passés n'apparaîtront pas dans la nouvelle interface, en effet si le format et l'emplacement des fichiers de collecte sont inchangés par rapport aux versions antérieures, le processus d'exploitation est totalement différent ; il est possible de reconstruire les résultats passés à partir des fichiers de collecte disponibles mais les scripts correspondant n'ont pas été développés,
- si vous avez modifié la configuration « standard » de l'installation de netMET ancienne formule, la mise à niveau risque de ne pas s'effectuer correctement. Les fichiers de configuration impactés par vos modifications devront être examinés et les scripts Perl que vous auriez pu développer sur la base de l'ancienne distribution en utilisant le module `netMETtk` devront être modifiés pour utiliser le nouveau module `netMETtk4Json`.

```
$ ./install.sh /home/netmet   netMet
Checking PERL libraries ...
  Check library : Apache2::Const ... ok.
  Check library : Apache2::RequestIO ... ok.
  Check library : Apache2::RequestRec ... ok.
  Check library : CGI ... ok.
  Check library : Encode ... ok.
  Check library : English ... ok.
  Check library : Fcntl ... ok.
  Check library : File::Basename ... ok.
  Check library : File::Compare ... ok.
  Check library : File::Copy ... ok.
  Check library : File::Find ... ok.
  Check library : File::Path ... ok.
  Check library : File::Temp ... ok.
  Check library : GD ... ok.
  Check library : GD::Graph ... ok.
  Check library : GD::Graph::bars ... ok.
  Check library : GD::Graph::colour ... ok.
  Check library : HostDetails4Json ... ok.
  Check library : HTTP::Date ... ok.
  Check library : IPC::Open2 ... ok.
  Check library : JSON::XS ... ok.
  Check library : lib ... ok.
  Check library : Mail::Send ... ok.
  Check library : MIME::Lite ... ok.
  Check library : MIME::Words ... ok.
```

```
  Check library : Mojo::Base ... ok.
  Check library : Net::IP ... ok.
  Check library : netMETtk4Json ... ok.
  Check library : POSIX ... ok.
  Check library : RRDs ... ok.
  Check library : Running4Json ... ok.
  Check library : Socket ... ok.
  Check library : Socket6 ... ok.
  Check library : strict ... ok.
  Check library : Sys::Hostname ... ok.
  Check library : Time::Local ... ok.
  Check library : vars ... ok.
  Check library : XServUsers::ToolKit ... ok.
-------------------------------------------------------------------------------
Would you upgrade from "old" (before 5.x version) netMet (/home/netmet/netMet) ? [y/n] y
Enter directory name for computed data files (or return if /home/netmet/netMet/COMPUTED_DATA) ?
/home/netmet/computed_data
Enter netmet service URL ? Mon-netmet.ciril.fr
*** Warning : existing directory /home/netmet/netMet is renamed /home/netmet/oldNetMet20160517-1757
Upgrading new netMET service under /home/netmet/netMet ...
-------------------------------------------------------------------------------
Installing embedded netMET/netMAT collector ...for dir in ./src ./dependencies ; do \
           make -C $dir  all ; \
        done
...
Embedded netMET/netMAT collector installation done.
-------------------------------------------------------------------------------
Directories cron
duplicator
etc
init.d
scripts
secure
serveur_netmet
stats
tmp created
-------------------------------------------------------------------------------
Checking data/secure/json directories...
  Check directory /home/netmet/html ...    Directory /home/netmet/html exist
           ***    Warning    :    existing    directory    /home/netmet/html/images    is    renamed
/home/netmet/html/images.old.20160517-1757 !
   /home/netmet/html/images created.
  Check directory /home/netmet/data …   Directory /home/netmet/data exist
  Check directory /home/netmet/secure … Directory /home/netmet/secure exist
  Check directory /home/netmet/computed_data …   /home/netmet/computed_data created.
-------------------------------------------------------------------------------
"old" file etc/organism.def copied to /home/netmet/netMet/etc/organism.def.
"old" file html/images/admin-logo.gif copied to /home/netmet/html/images/admin-logo.gif.
"old" netMet .data files moved from /home/netmet/data to /home/netmet/computed_data.
"old" file stats/etc/netmet.conf copied to /home/netmet/netMet/stats/etc/netmet.conf.
"old" file secure10m/etc/netmet.conf copied to /home/netmet/netMet/secure/etc/netmet.conf.
-------------------------------------------------------------------------------
You must probably update Apache configuration files (/etc/httpd/conf/httpd.conf
or /etc/apache/httpd.conf) :
        --> netMET directories, virtual host, ...
        --> AddHandler cgi-script .cgi
        --> DirectoryIndex index.cgi
Look a the file /home/netmet/netMet/etc/httpd.conf as an example of file to
include in an Apache configuration file.
-------------------------------------------------------------------------------
Complete the functions :
        netMETtk4Json::check_organism()
        netMETtk4Json::get_organisms_for_user()
        Auth_netMet::authorize_netmet()
if you need access control.
You can complete the function mkconfs() in /home/netmet/netMet/scripts/CONFmake.pl
for generating the "organism's" file (subnet's definitions).
-------------------------------------------------------------------------------
Use  /home/netmet/netMet/init.d/init-systemd-instal4netMet.sh  as root to install service netMet for
init Systemd
-------------------------------------------------------------------------------
********** netMET service netMet : installation completed. **********
```

Depuis la version 5.1 de l'exploitation netMET il n'y a plus de génération statique de pages HTML, la configuration Apache est donc différente de celle utilisée pour les versions antérieures.

Là encore les éventuels contrôles des droits d'accès des différents utilisateurs nécessitent la personnalisation des fonctions `check_organisme()` et `get_organisms_for_user()` du module Perl `netMETtl4Json` et de la fonction `authorize_netmet()` du module Perl `Auth_netMet` puisque par défaut toutes les fonctionnalités sont autorisées à tous les utilisateurs.
Il faut aussi compléter la fonction `mkconfs()` du module `scripts/CONFmake.pl` si le fichier descriptif des sous-réseaux (le fichier des « organismes ») doit être construit automatiquement.

4 Configuration de netMET

Nous nous plaçons dans le cas d'une première installation de netMET (cf. 3.2.1) dans le contexte présenté au paragraphe 2. Dans les autres cas de figure la procédure est simplifiée puisque tout ou partie de la configuration est déjà définie.

Elle s'effectue donc en étant connecté sous le même compte que celui utilisé pour installer le service (**netmet**) et en étant positionné dans le répertoire de ce service (**/home/netmet/netMET_de_test**).

4.1 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).

Le duplicateur est lancé par la commande `NETMET_DUPstart.sh` située dans le répertoire `init.d` d'installation du service, `/home/netmet/netMET_de_test/init.d` dans cet exemple. Il s'arrête en utilisant la commande `NETMET_DUPstop.sh` située dans ce même répertoire.

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
- secure : collecte sur 10mn, non agrégée

Il est possible de modifier ce comportement par exemple en changeant le port sur lequel le duplicateur écoute les netflows ou un ajoutant un destinataire à la liste par défaut. Il suffit de modifier la ligne 136 du script `NETMET_DUPstart.sh`, qui dans notre exemple contient :

```
dup="--listen 192.168.200.200/8080  -d 192.168.200.200/8081  -d 192.168.200.200/8082"
```

et précise à quelle adresse et sur quel port les netflows sont écoutés (option `–listen` ou `-l`) et vers quelles adresses/ports ils sont dupliqués (options `-d` ou `–duplicate`).

N.B. Il ne faut pas utiliser l'interface « loopback » (127.0.0.0).

Pour vérifier que des netflows arrivent bien sur le port écouté il suffit d'utiliser la commande `tcpdump` en étant connecté en « root » (en ajoutant éventuellement l'option `-i nom_de_l_interface` à cette commande) :

```
root# tcpdump -n dst port 8080
```

on obtient alors une trace comparable à :

```
root# tcpdump -n dst port 8080
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
14:59:17.415616 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1468
14:59:17.415633 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1468
14:59:17.415640 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1240
14:59:17.417468 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1468
14:59:17.417478 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1468
14:59:17.417485 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1240
14:59:17.419312 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1468
```

```
14:59:17.419326 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1468
14:59:17.419333 IP 192.168.200.254.63455 >192.168.200.200.8080: UDP, length 1240
^C
9 packets captured
9 packets received by filter
0 packets dropped by kernel
root#
```

4.2 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 sur le site www.netmat.org : http://www.netmat.org/Documentation/FichierDeConfigurationDuCollecteur
que nous vous conseillons de lire attentivement avant de commencer cette configuration.

4.2.1 Le collecteur «stats»

Après exécution de la commande `install.sh` (cf. paragraphe 3.2.1) le fichier de configuration `/home/netmet/netMET_de_test/stats/etc/netmet.conf` est partiellement rempli, il contient :

```
NETFLOW_LISTEN_ADDR_PORT {  192.168.200.200/8081 }

__ROUTER_IP_ADDR__
{
        SNMP_READ_COMMUNITY { "public" }

        IF_PROCESSED
        {
          "__IF_V4_RENATER__" <-> OTHER
#         "__IF_V6_RENATER__" <-> OTHER
        }

        IF_AGGREGATION
        {
          "__IF_V4__RENATER__" (192.168.150.254)
#         "__IF_V6__RENATER__" (__NETMET_FEDERATE_NET_V6_ADDR__)
        }
}
```

L'adresse d'écoute des netflows ayant été saisie lors de l'exécution de la commande `install.sh` la rubrique `NETFLOW_LISTEN_ADDR_PORT` est renseignée.

Il reste à remplacer `__ROUTER_IP_ADDR__` par l'adresse du routeur d'où proviennent les paquets de netflows à traiter, `192.168.200.254` (cf. figure 1) et à compléter les clauses `IF_PROCESSED` et `IF_AGGREGATION`.

4.2.1.1 Clause `IF_PROCESSED`

La clause `IF_PROCESSED` nous permet d'indiquer que le collecteur ne doit garder que les flux entre l'interface Renater notée `__IF_V4_RENATER__` et les interfaces de sites, et qu'il doit ignorer les flux inter sites. Comme nous n'avons pas saisi d'adresse IPv6 lors de l'installation la règle associée à l'interface Renater IPv6 est en commentaire.

L'interface IPv4 se trouve dans la description associée à la variable SNMP d'OID : `.iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr` que l'on obtient en utilisant la commande `listerIFs` du service netMET :

```
netmet # /home/netmet/netMET_de_test/bin/listerIFs  192.168.200.254  public
router : 192.168.200.254 - community : public
Routeur : 192.168.200.254
   ATM2/0 : 1
   Serial0 : 2
   FastEthernet0/0 : 3
```

```
   ATM2/0-atm layer : 4
   ATM2/0.0-atm subif : 5
   ATM2/0-aal5 layer : 6
   ATM2/0.0-aal5 layer : 7
   Null0 : 8
   ATM2/0.999-atm subif : 9
   ATM2/0.999-aal5 layer : 10
netmet #
```

Dans notre exemple l'interface Renater est spécifiée par le libellée `"ATM2/0.999-aal5 layer"` qui remplacera `"__IF_V4_RENATER__"` dans la règle.

N.B. Il peut y avoir plusieurs règles correspondant à plusieurs interfaces dans la clause.

4.2.1.2 Clause `IF_AGGREGATION`

La clause `IF_AGGREGATION` permet d'indiquer que le collecteur doit agréger à la volée les adresses IP provenant de l'interface «Renater» ou à destination de cette interface. Ces adresses seront remplacées par l'adresse d'agrégation spécifiée entre les parenthèses qui désigne le TROU NOIR Renater et qui a été saisie à l'exécution de la commande `install.sh`. Par convention nous avons donné lors de la saisie l'adresse de l'interface Renater (192.168.150.254), ainsi sommes nous sûr de son unicité.

Comme dans la clause «`IF_PROCESSED`» le texte `"__IF_V4_RENATER__"` doit être remplacé par le libellé `"ATM2/0.999-aal5 layer"`.

N.B. Si la clause `IF_PROCESSED` comporte plusieurs règles correspondant à plusieurs interfaces la clause `IF_AGGREGATION` doit comporter elle aussi plusieurs règles, une par interface.

4.2.1.3 Le fichier de configuration de la collecte « stats »

Une fois ces substitutions effectuées et les clauses en commentaires supprimées le fichier configuration contient (dans cet exemple) :

```
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)
        }
}
```

4.2.2 Le collecteur «secure»

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

```
NETFLOW_LISTEN_ADDR_PORT {  192.168.200.200/8082 }

192.168.200.254
{
        SNMP_READ_COMMUNITY { "public" }

        IF_PROCESSED
```

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

}
```

4.3 Configuration de l'exploitation

4.3.1 Le fichier `etc/explt.conf`

Le fichier `/home/netMET_de_test/etc/explt.conf` est complètement renseigné par la commande d'installation (les paramètres de la commande d'installation ou les éléments saisis lors de son exécution apparaissent en rouge) :

```
# ----------------------------------------------------
# PATH - PATH - PATH
#
NETMET_BIN_PATH                 /home/netmet/netMET_de_test/bin
NETMET_DUPLICATOR_BIN_PATH      /home/netmet/netMET_de_test/duplicator
NETMET_STATS_BIN_PATH           /home/netmet/netMET_de_test/stats

# obsoletes ----------------------------------------------------
NETMET_METRO_BIN_PATH           /home/netmet/netMET_de_test/metro
NETMET_SECURE10m_BIN_PATH       /home/netmet/netMET_de_test/secure10m
NETMET_SECURE24h_BIN_PATH       /home/netmet/netMET_de_test/secure24h
# ------------------------------------------------------------

NETMET_SCRIPT_PATH              /home/netmet/netMET_de_test/scripts
NETMET_ETC_PATH                 /home/netmet/netMET_de_test/etc

NETMET_DATA_PATH                /home/netmet/netMET_de_test/DATA
NETMET_SECURE_PATH              /home/netmet/netMET_de_test/SECURE
NETMET_HTML_PATH                /home/netmet/netMET_de_test/HTML
NETMET_TMP_PATH                 /home/netmet/netMET_de_test/tmp

# ----------------------------------------------------
# FILE - FILE - FILE
#
NETMET_ORGA_FILE                organism.def
NETMET_DUMP_FILE                zzaccounting.dmp

# ----------------------------------------------------
# VARIABLES - VARIABLES - VARIABLES
#
# inutilise en 5.x ------------------------------------------
NETMET_ADMIN_NET_NAME           __NETMET_ADMIN_NET_NAME__
# ------------------------------------------------------------

NETMET_FEDERATE_NET_NAME        RENATER
NETMET_FEDERATE_NET_ADDR        192.168.150.254
#NETMET_FEDERATE_NET_V6_ADDR    __NETMET_FEDERATE_NET_V6_ADDR__

# ----------------------------------------------------
# DESIGN - DESIGN - DESIGN

# Inutilisé en 5.x, conservé pour une réutilisation éventuelle de DETECT_SCANS
NETMET_EXPLT                    (TOP_N_ALL TOP_N_BY_ORGA DETAILLED_METRO STATS)
# DETECT_SCANS)

NETMET_HOST_TOP_N                       15
NETMET_ORGA_TOP_N                       10
NETMET_TOP_N_BY_ORGA                    10
NETMET_DETAILLED_TABLE_THRESHOLD        0.5     # 0.5% because of table length
NETMET_DETAILLED_PIE_THRESHOLD          3.0     # 3.0% because of graphics limitations
#NETMET_SHOW_V4_V6                      1       # to distinguish V4 and V6 trafic

NETMET_INFORMATIONS_URL                 /informations.html

# Scans detection thresholds - SECURE_SCANS -
NETMET_SCANS_THRESHOLD_B_A      800
```

```
NETMET_SCANS_THRESHOLD_C        176
NETMET_SCANS_PORT               500

# Store 31 days of SECURE DATA (Round Robin)
NETMET_SECURE_RR                31

NETMET_ADMIN_MAIL               monmail@chezmoi.fr
# ----------------------
# DEPUIS LA VERSION 4.3
NETMET_TOP_N_PERIOD             10
# ----------------------
# DEPUIS LA VERSION 5.1
NETMET_COMPUTED_DATA_PATH       /home/netmet/netMET_de_test/COMPUTED_DATA
# période en minutes entre deux collectes "STATS"
NETMET_DATA_DUMP_PERIOD         5
# période en minutes entre deux analyses des données "STATS" collectées
NETMET_DATA_PARSE_PERIOD        10
# période en minutes entre deux collectes "SECURE"
NETMET_SECURE_DUMP_PERIOD       10
NETMET_TODO_FILE                todo4data.txt
# remplace NETMET_SECURE10m_BIN_PATH et NETMET_SECURE24h_BIN_PATH
NETMET_SECURE_BIN_PATH          /home/netmet/netMET_de_test/secure
# nom du service et répertoire d'installation
NETMET_HOME                     /home/netmet
NETMET_SERVICE_NAME             netMET_de_test
NETMET_SERVICE_URL              netmet.monsite.fr
```

Pour personnaliser la fréquence des collectes et divers paramètres de l'exploitation consultez la documentation en ligne: http://www.netmet-solutions.org/DocumentationDepuisV5/FichiersDeConfiguration.

4.3.2 Le fichier des organismes

Le fichier des organisme (`/home/netmet/netMET_de_test/etc/organism.def` dans l'exemple) doit contenir les couples (SubnetIP, libellé de l'organisme) **SANS RECOUVREMENT** d'adresses IP.
Il est initialisé avec l'adresse IPv4 et le nom du réseau fédérateur et l'adresse IPv6 si elle est définie et contient en outre des exemples en commentaires :

```
192.168.150.254/32      "RENATER"
#nnn.nnn.nnn.nnn/mm     "ORGA_1"
#xxx.xxx.xxx.xxx/hh     "ORGA_2"
#yyy.yyy.yyy.yyy/tt     "ORGA_3"
#zzz.zzz.zzz.zzz/vv     "ORGA_3"
#__NETMET_FEDERATE_NET_V6_ADDR__/128       "RENATER"
```

Chaque ligne contient l'adresse du sous-réseau au format CIDR suivie par le nom qui lui est associé, par exemple :

```
192.168.150.254/32      "RENATER"
192.180.0.0/16     "ORGA_1"
192.168.100.0/24   "ORGA_2"
192.168.200.64/27  "ORGA_3"
192.168.200.96/27  "ORGA_3"
```

Le nom d'un sous-réseau doit être entre doubles-quotes et ne doit pas contenir d'espace.
La commande `bin/subnetFileCheck` du service netMET permet de vérifier la syntaxe et la cohérence de ce fichier.

4.3.3 Le fichier `cron/ARCHIVEScron`

Ce fichier chargé dans la « crontab » lors du démarrage du service netMET contient les appels aux scripts de « nettoyage » des répertoires contenant les fichiers de collecte de la métrologie, du répertoire contenant les données « pré-compilées » (`COMPUTED_DATA`) et du répertoire contenant les fichiers Json construits :

```
# scripts/ARCHIVES : ARCHIVEScron pour netMET et nettoyage des répertoires data et html
# scripts/ARCHIVES :

# scripts/removeOldFiles.pl : nettoyage des répertoires tous les 2 de chaque mois a 04h00 ou 04h30
#00 04 2 * *  /.../scripts/removeOldFiles.pl  /.../etc/explt.conf   html 24
#00 04 2 * *  /.../scripts/removeOldFiles.pl  /.../etc/explt.conf   computed 24
```

```
30 04 2 * *  /.../scripts/removeOldFiles.pl  /.../etc/explt.conf   data 10 > /dev/null  2>&1
# scripts/ARCHIVES : Generation ARCHIVES generales tous les jours a 05h00
00 05 * * *  /.../scripts/ARCHIVES4Json_gen-daily.pl /.../etc/explt.conf  > /dev/null 2>&1
```

N.B. Pour faciliter la lecture le nom du répertoire du service (`/home/netmet/netMET_de_test`) a été remplacé par `/.../`.

Le nettoyage du répertoire contenant les fichiers de collecte « stats » est lancé chaque début de mois avec une durée de conservation de 10 mois par la commande

```
30 04 2 * *  /.../removeOldFiles.pl    /.../etc/explt.conf  data 10 > /dev/null  2>&1
```

La durée de conservation peut être modifiée par l'utilisateur en fonction de son contexte.

Le nettoyage du répertoire contenant les fichiers Json et de celui contenant les données « pré-compilées » figure en commentaire avec une durée de conservation de 24 mois :

```
#00 04 2 * *  /.../removeOldFiles.pl    /.../etc/explt.conf  html 24
#00 04 2 * *  /.../removeOldFiles.pl    /.../etc/explt.conf  computed 24
```

Il est bien entendu possible de dé-commenter ces lignes et de changer la durée de conservation.

Ce fichier contient aussi l'appel du script `ARCHIVES4Json_gen-daily.pl` qui reconstruit le fichier Json descriptif de l'état des archives. Ce fichier est utilisé dans l'interface pour construire le calendrier permettant la navigation dans l'historique des données.

N.B. Le « nettoyage » des fichiers de collecte « secure » est effectué chaque jour, la durée de rétention est définie par le paramètre `NETMET_SECURE_RR` du fichier de configuration de l'exploitation (`/home/netmet/netMET_de_test/etc/explt.conf` dans l'exemple) et est de 31 jours par défaut.

4.3.4 Le fichier `cron/CONFcron`

Il définit la fréquence de génération et d'archivage du fichier des organismes.

```
PATH=/sbin:/bin:/usr/sbin:/usr/bin:/usr/local/cvs/bin

### scripts/CONFmake.pl tous les les jours a 1h00
00 01  * * * /.../scripts/CONFmake.pl /.../etc/explt.conf   >/dev/null  2>&1
```

Par défaut le nouveau fichier est une copie de l'ancien et l'ancien est archivé dans le répertoire des données collectées de la veille. L'utilisateur peut modifier ce script en fonction de son contexte.

4.3.5 Personnalisation du logo

Le logo affiché en haut à droite de la page netMET peut être personnalisé. Il suffit pour cela de copier votre logo dans le fichier `admin-logo.gif` situé dans le répertoire `images` du répertoire des fichiers Json résultats (`/home/netmet/netMET_de_test/HTML` dans notre exemple).

5 Configuration du système

5.1 Configuration du serveur Apache

Le fichier `/home/netmet/netMET_de_test/etc/httpd.conf` est un exemple utile à la configuration du serveur Apache. Il est généré par le script `install.sh` à partir d'un modèle dans lequel sont mis à jour le nom du site, l'adresse électronique de l'administrateur et le nom du service netMET avec les données saisies lors de l'exécution du script (les éléments saisis lors de l'exécution du script d'installation - cf. 3.2.1 - figurent en rouge dans le texte ci-dessous). Une fois personnalisé il peut être inclus dans le fichier de

configuration Apache du système, de préférence par une directive `include`. Ce fichier 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 clauses `RewriteEngine` et `RewriteRule` figurent dans la configuration.

```
## pour les autorisations (a titre d'exemple) ----
PerlModule apache::Auth_netMET_de_test
## ------------------------------------------------

<VirtualHost netmet.monsite.fr:80>
        ServerName              netmet.monsite.fr
        ServerAdmin             monmail@chezmoi.fr
        DocumentRoot            /home/netmet/netMET_de_test/serveur_netmet/STATIC
        ErrorLog                /var/log/apache/netMET_de_test.error
        TransferLog             /var/log/apache/netMET_de_test.access

        Options                 FollowSymLinks
        DirectoryIndex          index.html

        <Directory "/">
            Options               FollowSymLinks IncludesNOEXEC ExecCGI
            AllowOverride         all

##  pour les autorisations ..
            AuthName    "Accès authentifié au service netMET netMET_de_test ... "
            AuthType            Basic
            PerlSetVar          debug_netMET_de_test yes
            PerlAuthzHandler    apache::Auth_netMET_de_test::authz
## ------------------------------------------------

            order           deny,allow
            deny from       all
# INCLURE ICI LES (FICHIERS D') AUTORISATIONS ('Allow   from ... ')

        </Directory>

        RewriteEngine      on
        RewriteRule      ^/ws/(.*)    http://127.0.0.1:3000/$1 [QSA,P,L,E=RU:%1]

</VirtualHost>


<Directory "/home/netmet/netMET_de_test/serveur_netmet/STATIC">
        Options                 FollowSymLinks IncludesNOEXEC ExecCGI
        AllowOverride           all

##  pour les autorisations .
        AuthName        "Accès authentifié au service netMET netMET_de_test ... "
        AuthType          Basic
        PerlSetVar        debugAuth_netMET_de_test yes
        PerlAuthzHandler  apache::Auth_netMET_de_test::authz
## ------------------------------------------------

        order             deny,allow
        deny from         all
# INCLURE ICI LES (FICHIERS D') AUTORISATIONS ('Allow   from ... ')
```

```
</Directory>
```

6 Tests, arrêt et démarrage des services

6.1 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`), initng ou Systemd le script d'installation génère dans ce répertoire le script permettant d'effectuer les mises à jour nécessaires (respectivement `init-systemV-instal4`*`nom_du_service`*`.sh`, `ngc-instal4`*`nom_du_service`*`.sh`, et `init-systemd-instal4`*`nom_du_service`*`.sh`). Ce script doit être exécuté en étant connecté sous « root » ou avec une commande `sudo`.

Le répertoire `init.d` contient de plus :

- `NETMET_DUPstart.sh`, `NETMET_DUPstop.sh` : les scripts de lancement et d'arrêt du duplicateur,
- STATS_SECUREstart.sh, STATS_SECUREstop.sh : les scripts de lancement et d'arrêt des collecteurs et de l'exploitation,
- *`nom_du_service`*`.i` : le fichier de configuration de initng,
- *`nom_du_service`* : le fichier de configuration de l'init System V,
- *`nom_du_service`*`.service` : le fichier de configuration de l'init Systemd .

N.B. Un seul de ces trois derniers fichiers est utilisé dans une configuration donnée.

6.2 Test de la configuration

La suite de commandes ci-dessous permet de vérifier la syntaxe des fichiers de configuration et de tester le bon fonctionnement des collecteurs.
Nous nous plaçons dans le contexte de l'exemple 3.2.1 et supposons que l'utilisateur connecté avec le compte netmet positionne le répertoire de travail dans `/home/netmet/netMET_de_test` :

```
netmet#  cd /home/netmet/netMET_de_test
```

6.2.1 Test du duplicateur

Pour tester le duplicateur il faut d'abord s'assurer que le routeur est correctement configuré et envoie bien les netflows à la machine de métrologie. Pour cela il suffit d'utiliser la commande `tcpdump` (cf. 4.1).
Il est possible alors de démarrer le duplicateur :

```
netmet# init.d/NETMET_DUPstart
```

Pour s'assurer du démarrage du duplicateur il faut consulter le fichier « syslog.log », on doit y trouver une trace comparable à celle-ci (pour faciliter la lecture nous avons remplacé `/home/netmet/netMET_de_test/` par `/xxx/`) :

```
netmet# sudo tail /var/log/syslog.log
May 23 16:29:26 local@... /xxx/duplicator/netMETdup[2928]: [I] - Socket opened listener - 192.168.200.200/8080
May 23 16:29:26 local@... /xxx/netMET_de_test/duplicator/netMETdup[2928]: [I] - Socket opened duplicator - 0.0.0.0/33917
May 23 16:29:26 local@... /xxx/duplicator/netMETdup[2928]: [I] - netMETdup duplicate 192.168.200.200/8080 to 192.168.200.200/8081
May 23 16:29:26 local@... /xxx/duplicator/netMETdup[29282]: [I] - Socket opened duplicator - 0.0.0.0/33872
May 23 16:29:26 local@... /xxx/duplicator/netMETdup[2928]: [I] - netMETdup duplicate 192.168.200.200/8080 to 192.168.200.200/8082
May 23 16:29:26 local@... /xxx/duplicator/netMETdup[29282]: [I] - Duplicator netMETdup started
```

```
netmet#
```

Une fois le duplicateur lancé on peut s'assurer qu'il duplique effectivement sur les deux ports 8081 et 8082 en utilisant là encore la commande `tcpdump` :

```
netmet#  sudo tcpdump -c  3  -n  -i lo dst port 8081
Password:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
17:13:43.155833 IP 192.168.200.200.33917 > 192.168.200.200.8081: UDP, length 1469
17:13:43.155887 IP 192.168.200.200.33917 > 192.168.200.200.8081: UDP, length 1469
17:13:43.155952 IP 192.168.200.200.33917 > 192.168.200.200.8081: UDP, length 1277
3 packets captured
74 packets received by filter
42 packets dropped by kernel
netmet# sudo tcpdump -c  3  -n  -i lo dst port 8082
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 65535 bytes
17:13:56.976022 IP 192.168.200.200.33872 > 192.168.200.200.8082: UDP, length 1469
17:13:56.976068 IP 192.168.200.200.33872 > 192.168.200.200.8082: UDP, length 1469
17:13:56.976110 IP 192.168.200.200.33872 > 192.168.200.200.8082: UDP, length 1277
3 packets captured
4138 packets received by filter
4102 packets dropped by kernel
netmet#
```

Une fois ces contrôles effectués, il est possible d'arrêter le duplicateur :

```
netmet# init.d/NETMET_DUPstop.sh
```

et de s'assurer de son arrêt :

```
netmet# sudo grep duplicator /var/log/syslog.log
...
May  23  17:21:13  local@...  /xxx/duplicator/netMETdup[2928]:  [I]  -  Socket  closed  –
192.168.200.200/8080
May 23 17:21:13 local@... /xxx/duplicator/netMETdup[2928]: [I] - Socket closed - 0.0.0.0/33917
May 23 17:21:13 local@... /xxx/duplicator/netMETdup[2928]: [I] - Socket closed - 0.0.0.0/33872
May  23  17:21:13  local@...  /xxx/duplicator/netMETdup[2928]:  [I]  -  Duplicator  netMETdup  exited
[13067126]
...
netmet#
```

6.2.2 Test des fichiers de configuration des collecteurs

La commande `bin/configurationFileCheck` teste la correction du fichier de configuration de collecteur donné en argument :

```
netmet# bin/configurationFileCheck  stats/etc/netmet.conf
192.168.200.200/8081
192.168.200.254
public
(#d10 et =s10)
 ou (=d10 et #s10)

10 == 192.168.150.254

Data templates ...
Options templates ...
Samplers ...

netmet# bin/configurationFileCheck secure/etc/netmet.conf
```

```
192.168.200.200/8082
192.168.200.254
public
(#d10 et =s10)
 ou (=d10 et #s10)

# no aggregation rules
Data templates ...
Options templates ...
Samplers ...

netmet#
```

La commande affiche soit un message d'erreur soit une trace de la « compilation » des règles.
On retrouve

- le couple adresse/port d'écoute des netflows, ici 192.168.200.200/8081 pour la configuration du collecteur « stats » et 192.168.200.200/8082 pour le collecteur « secure »,
- l'adresse du routeur dont on collecte les netflows 192.168.200.254,
- la communauté SNMP (pour l'instant seul « public » est autorisé, toute autre valeur provoque une erreur de syntaxe),
- les règles `IF_PROCESSED` sous forme codée ; comme nous l'avons vu au paragraphe 4.2.1.1 l'interface `ATM2/0.999-aal5 layer` a pour numéro 10, l'unique règle de l'exemple

  `"ATM2/0.999-aal5 layer" ↔ OTHER`

  indique que sont conservés les flux dont la source est l'interface numéro 10 et la destination une interface différente de 10 (`#d10 et =s10`) ainsi que les flux dont la source est une interface différente de 10 et la destination l'interface 10 (`=d10 et #s10`) ; l'une ou l'autre de ces conditions doit être vérifiée pour qu'un flux soit collecté,
- le numéro de l'interface d'agrégation suivi de l'adresse d'agrégation ou le libellé `# no aggregation rules` en l'absence de règle d'agrégation.

Les 3 dernières lignes sont sans signification dans ce contexte.

6.2.3 Test du fichier des organismes

La commande `bin/subnetFileCheck` teste la correction du fichier décrivant les sous-réseaux. Elle regroupe les définitions qui peuvent l'être, comme le montre l'exemple ci-dessous :

```
netmet# cat etc/organism.def
192.168.150.254/32      "RENATER"
192.180.0.0/16     "ORGA_1"
192.168.100.0/24   "ORGA_2"
192.168.200.64/27  "ORGA_3"
192.168.200.96/27  "ORGA_3"
netmet# bin/subnetFileCheck -p etc/organism.def
Parsing etc/organism.def...
192.168.100.0/24 :   192.168.100.0      "ORGA_2"
192.168.150.254/32 : 192.168.150.254    "RENATER"
192.168.200.64/26 :  192.168.200.96     "ORGA_3"
192.180.0.0/16 :     192.180.0.0        "ORGA_1"
netmet#
```

Avec l'option `-p` la commande affiche chaque sous-réseau suivi de la première adresse de l'intervalle d'adresses et du nom associé.

Avec l'option `-i` la commande signale aussi les incohérences, par exemple :

```
netmet# cat etc/erreur.def
192.168.150.254/32      "RENATER"
192.180.0.0/16     "ORGA_1"
192.168.100.0/24   "ORGA_2"
```

```
192.168.200.64/27  "ORGA_3"
192.168.200.80/28  "ORGA_4"
netmet# bin/subnetFileCheck -p -i etc/erreur.def
Parsing etc/erreur.def...
192.168.100.0/24 :   192.168.100.0      "ORGA_2"
192.168.150.254/32 : 192.168.150.254    "RENATER"
192.168.200.64/27 :  192.168.200.64     "ORGA_3"
192.168.200.80/28 :  192.168.200.80     "ORGA_4"
192.180.0.0/16 :     192.180.0.0        "ORGA_1"
Parsing terminated (5 subnet definitions).
warning : 192.168.200.64/27 ORGA_3 contains 192.168.200.80/28 ORGA_4
WARNING : 1 naming problems ?
netmet#
```

N.B. Le fichier des organismes n'étant pas utilisé par les collecteurs il n'est pas indispensable de le vérifier pour tester les collecteurs mais sa vérification est indispensable avant de démarrer le service.

6.2.4 Test des collecteurs

La commande `scripts/testCollecteur.sh` permet de tester le collecteur dont le nom est fourni en argument (« stats » ou « secure »). Pour utiliser cette commande il faut que duplicateur s'exécute (cf. 6.2.1). La commande lance l'exécution du collecteur, lance l'exécution d'un des scripts provoquant le « vidage » des netflows collectés dans un fichier de collecte (`scripts/STATS4Json_cron4dump.pl` pour le collecteur stats ou `scripts/SECURE4Json_cron4dump.pl` pour le collecteur secure), puis arrête l'exécution du collecteur.
Une fois la commande `testCollecteur.sh` terminée il reste à vérifier qu'un fichier de collecte a bien été construit au « bon » endroit en utilisant la commande bin/netMETexp puis que le collecteur a bien été arrêté.

Une séquence de test du collecteur « stats » est par exemple :

```
netmet# cd /home/netmet/netMET_de_test
netmet# scripts/testCollector.sh  stats
C'est fini, il faut vérifier le contenu du fichier de collecte (avec bin/netMETexp ...)
netmet# ls DATA/2016-05/2016-05-25/
STATS_RENATER  todo4data.txt  zzaccounting.dmp
netmet# ls -l DATA/2016-05/2016-05-25/
total 856
drwx------ 2 netmet netmet   4096 mai   25 10:28 STATS_RENATER
-rw-r--r-- 1 netmet netmet     89 mai   25 10:28 todo4data.txt
-rw-r--r-- 1 netmet netmet 865402 mai   25 10:28 zzaccounting.dmp
netmet# ls -l DATA/2016-05/2016-05-25/STATS_RENATER/
total 848
-rw------- 1 netmet netmet 865402 mai   25 10:28 zzaccounting.dmp-10-23
netmet# bin/netMETexp -i DATA/2016-05/2016-05-25/STATS_RENATER/zzaccounting.dmp-10-23
------------------------------------------------------------------------
Metrology IPv4 from Wed-25/05/2016 10:27:51 to Wed-25/05/2016 10:28:01
--
Nb of differents hosts                                      : 17001
Nb of differents bidirectionals communications              : 20328
Accounting info. memory size                                : 1272016
Average memory size of accounting info. by bidirectionals comm. : 54
Average Number      of [serv/prot]      by bidirectionals comm. : 1.91
------------------------------------------------------------------------
------------------------------------------------------------------------
Metrology IPv6 from Wed-25/05/2016 10:27:51 to Wed-25/05/2016 10:28:01
--
Nb of differents hosts                                      : 0
Nb of differents bidirectionals communications              : 0
Accounting info. memory size                                : 96
Average memory size of accounting info. by bidirectionals comm. : -
Average Number      of [serv/prot]      by bidirectionals comm. : -
------------------------------------------------------------------------
netmet# bin/netMETexp -H DATA/2016-05/2016-05-25/STATS_RENATER/zzaccounting.dmp-10-23  | head -n 5
1464164871
1464164881
10
193.51.181.109  195.221.83.158  [1900/17](118)
```

```
193.51.181.109  147.99.214.5    [6000/6](40)
netmet# bin/netMETexp -H DATA/2016-05/2016-05-25/zzaccounting.dmp  | head -n 5
1464164871
1464164881
10
193.51.181.109  195.221.83.158  [1900/17](118)
193.51.181.109  147.99.214.5    [6000/6](40)
netmet# ps -u netmet
  PID TTY          TIME CMD
netmet#
```

Les commande `ls` montrent la structure du répertoire de collecte des flux « agrégés » (`/home/netmet/netMET_de_test/DATA` dans cet exemple) :

- à chaque mois est associé un répertoire dont le nom est de la forme *AAAA-MM*,
- à chaque jour est associé un répertoire dont le nom est de la forme *AAAA-MM-JJ*,
- chaque répertoire journalier contient le fichier de collecte de l'ensemble des flux de la journée (`zzaccounting.dmp`), un fichier temporaire des données à traiter utilisé par l'exploitation (`todo4data.txt`) et un répertoire `STATS_«`*`nom du réseau fédérateur`*`»` (ici `STATS_RENATER`).

Le répertoire `STATS_«nom du réseau fédérateur»` est destiné aux fichiers de collecte par tranches de N minutes (5 minutes par défaut).

La commande `bin/netMETexp` affiche avec l'option `-i` des informations de synthèse sur le contenu du fichier. Avec l'option `-H` elle affiche le contenu du fichier de collecte en commençant par l'affichage de la date (Unix time) de début de collecte, de celle du dernier « dump » et de la durée de collecte. Vient ensuite la liste (ici abrégée) des flux collectés :

adresse source adresse destination volume du trafic en octets pour chaque service

Le fonctionnement de la commande `netMETexp` est détaillé sur le site `www.netmat.org` (www.netmat.org/Documentation/CommandeNetMETexp).

On peut constater ici l'agrégation sur les adresses IP sources. Un extrait plus long mettra en évidence l'agrégation sur les adresses IP destinations.

Ici un seul vidage ayant été demandé, le fichier de collecte journalier est identique à celui de la tranche. Si un deuxième test du même collecteur est effectué, les flux de la nouvelle collecte seront placés dans un nouveau fichier associé à la tranche horaire puis ajoutés au fichier journalier.

Les test du collecteur « secure » s'effectue sur le même schéma :

```
netmet# scripts/testCollector.sh  secure
C'est fini, il faut vérifier le contenu du fichier de collecte (avec bin/netMETexp ...)
netmet# ls -l SECURE/2016-05/2016-05-25
total 2904
-rw------- 1 netmet netmet 2970130 mai   25 11:45 zzaccounting.dmp-11-35
netmet# bin/netMETexp -i SECURE/2016-05/2016-05-25/zzaccounting.dmp-11-35
------------------------------------------------------------------------
Metrology IPv4 from Wed-25/05/2016 11:45:25 to Wed-25/05/2016 11:45:35
--
Nb of differents hosts                                      : 38377
Nb of differents bidirectionals communications              : 102042
Accounting info. memory size                                : 5011024
Average memory size of accounting info. by bidirectionals comm. : 41
Average Number      of [serv/prot]      by bidirectionals comm. : 1.07
------------------------------------------------------------------------
------------------------------------------------------------------------
Metrology IPv6 from Wed-25/05/2016 11:45:25 to Wed-25/05/2016 11:45:35
--
Nb of differents hosts                                      : 0
Nb of differents bidirectionals communications              : 0
Accounting info. memory size                                : 96
Average memory size of accounting info. by bidirectionals comm. : -
Average Number      of [serv/prot]      by bidirectionals comm. : -
------------------------------------------------------------------------
netmet# bin/netMETexp -H SECURE/2016-05/2016-05-25/zzaccounting.dmp-11-35 | head -n 5
1464169525
1464169535
10
152.81.13.243   93.184.221.200  [443/6](40)
193.50.175.32   149.5.224.172   [80/6](104)
netmet# ps -u netmet
```

```
  PID TTY          TIME CMD
netmet#
```

Comme le répertoire de collecte des données « agrégées », le répertoire de collecte des flux non « agrégés » situés dans `/home/netmet/netMET_de_test/SECURE` dans l'exemple contient un répertoire *AAAA-MM* par mois, chaque répertoire mensuel contenant un répertoire journalier *AAAA-MM-JJ*. Le répertoire journalier contient les différentes tranches de collecte de la journée.
On remarque sur l'extrait qu'il n'y a pas d'agrégation d'adresse conformément au fonctionnement du collecteur « secure ».

N.B. Il est préférable de supprimer les répertoires créés par ces tests avant de démarrer le service netMET pour partir d'un état initial cohérent. Il faut aussi arrêter le duplicateur à l'issue des tests, la commande associée au service netMET effectue à la fois le lancement du duplicateur, des collecteurs et la mise en place de l'exploitation.

6.3 Démarrage/arrêt des services netMET

6.3.1 Démarrage « manuel » du service netMET

Il est possible de démarrer et d'arrêter netMET en utilisant les scripts du répertoire `init.d` du service netMET (dans notre exemple `~netmet/netMET_de_test/init.d`). Pour cela il suffit de démarrer le duplicateur puis les collecteurs et l'exploitation :

```
netmet# ~netmet/netMET_de_test/init.d/NETMET_DUPstart.sh
netmet# ~netmet/netMET_de_test/init.d/STATS_SECUREstart.sh
```

L'arrêt s'effectue de façon analogue :

```
netmet# ~netmet/netMET_de_test/init.d/STATS_SECUREstop.sh
netmet# ~netmet/netMET_de_test/init.d/NETMET_DUPstop.sh
```

Il est aussi possible d'effectuer l'ensemble avec une seule commande en étant toutefois connecté en tant que super-utilisateur :

```
root#~netmet/netMET_de_test/init.d/netMET_de_test start
```

L'arrêt s'effectue avec la même commande et l'argument `stop` :

```
root#~netmet/netMET_de_test/init.d/netMET_de_test stop
```

6.3.2 Avec l'init System V

Si votre système utilise l'init System V, lors de son exécution la commande `install.sh` a généré dans le répertoire `init.d` du service netMET une commande d'installation du service dans `/etc/init.d` nommée `init-systemV-instal4`*`nom_du_service`*`.sh` (`init-systemV-instal4netMET_de_test.sh` dans l'exemple). Il suffit alors d'exécuter cette commande en tant que super-utilisateur pour créer le service :

```
root#~netmet/netMET_de_test/init.d/init-systemV-instal4netMET_de_test.sh
```

Le service démarre alors avec

```
root#/etc/init.d/netMET_de_test start
```

et s'arrête avec

```
root#/etc/init.d/netMET_de_test stop
```

Il est aussi possible d'utiliser la commande `service` si elle est disponible sur votre système.

6.3.3 Avec initng

Dans ce cas la commande d'installation du service se nomme `ngc-instal4`*`nom_du_service`*`.sh` (`ngc-instal4netMET_de_test.sh` dans l'exemple). Le service s'installe en mode super-utilisateur avec

```
root#~netmet/netMET_de_test/init.d/ngc-instal4netMET_de_test.sh
```

Il démarre avec

```
root#ngc -u service/netMET_de_test
```

et s'arrête avec

```
root#ngc -d service/netMET_de_test
```

6.3.4 Avec systemd (non testé)

La commande d'installation se nomme alors `init-systemd-instal4`*`nom_du_service`*`.sh` (`init-systemd-instal4netMET_de_test.sh` dans l'exemple) et le service s'installe avec

```
root#~netmet/netMET_de_test/init.d/init-systemd-instal4netMET_de_test.sh
```

Il démarre avec la commande

```
root#systemctl start netMET_de_test.service
```

et s'arrête avec

```
root#systemctl stop netMET_de_test.service
```

7 Complément

7.1 Où sont les données et les résultats?

Le paragraphe 6.2.4 a déjà présenté la structure des répertoire de collecte.
L'emplacement des différents fichiers produits dépend des paramètres fournis lors de l'installation du service et conservés dans le fichier de configuration de l'exploitation (`etc/explt.conf`) avec les intitulés :

- `NETMET_DATA_PATH` : le répertoire des fichiers de collecte des flux agrégés (`~/netMET_de_test/DATA` dans l'exemple),
- `NETMET_SECURE_PATH` : le répertoire des fichiers de collecte des flux non agrégés (`~/netMET_de_test/SECURE` dans l'exemple),
- `NETMET_COMPUTED_DATA_PATH` : le répertoire des fichiers pré-traités (`.data`) (`~/netMET_de_test/COMPUTED_DATA` dans l'exemple),
- `NETMET_HTML_PATH` : le répertoire des fichiers Json (`~/netMET_de_test/HTML` dans l'exemple),

Dans chacun d'eux, l'arborescence est pratiquement la même, à savoir un répertoire par mois nommé *`année-mois`*, dans lequel on trouve un répertoire par jour nommé *`année-mois-jour`*.

Les répertoires « `HTML` » et « `COMPUTED_DATA` » comportent de plus des répertoire hebdomadaires nommés *`année`*`-Week#`*`numéro de semaine`*.

Puis nous avons des fichiers ou des sous-répertoires selon la problématique.

```
...

DATA
|--2016-05                          (Un répertoire par mois)
|  |--2016-05-01                    (Un répertoire par jour)
|  |  |--zzaccounting.dmp           (Fichier journalier)
|  |  |--todo4data.txt              (Fichier de travail, journée courante uniquement)
|  |  |--organism.def               (sauvegarde, sauf dans la journée courante)
|  |  |--STATS_réseau-fédérateur
|  |  |  |--zzaccounting.dmp-xx-yy  (1 fichier par 5 minutes)
|  |  |  |--...
|  |--...
|--...

...

SECURE
|--2016-05                        (Un répertoire par mois)
|  |--2016-05-01                     (Un répertoire par jour)
|  |  |  |--zzaccounting.dmp-xx-yy  (1 fichier par 10 minutes)
|  |  |  |--...
|  |--...
|--...

...

COMPUTED_DATA
|--2016-05                          (Un répertoire par mois)
|  |--2016-05-01                    (Un répertoire par jour)
|  |  |--STATS_réseau-fédérateur
|  |  |  |--réseau-fédérateur.data  (fichier « compilé » associé au réseau fédérateur)
|  |  |  |--XXX.data                (fichier « compilé » associé l'organisme XXX)
|  |  |  |--...
|  |--...
|  |--Month    (récapitulatif du mois entier, les fichiers sont analogues à ci-dessus)
|  |  |--STATS_réseau-fédérateur
|  |  |  |--réseau-fédérateur.data
|  |  |  |--XXX.data
|  |  |  |--...
|--...
|
|--2016-Week#17                     (Un répertoire par semaine)
|  |  |--STATS_réseau-fédérateur
|  |  |  |--réseau-fédérateur.data  (fichier « compilé » associé au réseau fédérateur)
|  |  |  |--XXX.data                (fichier « compilé » associé l'organisme XXX)
|  |  |  |--...
|--...

...

HTML
|--2016-05                                  (Un répertoire par mois)
|  |--2016-05-01                            (Un répertoire par jour)
|  |  |-- DETAILLED_METRO
|  |  |   |-- RENATER-DETAILLED_METRO.json  (trafic par services, protocoles)
|  |  |   |-- XXX-DETAILLED_METRO.json      (trafic par services, protocoles pour XXX)
|  |  |   | ...
|  |  |-- index.json                 (date de collecte, volume du trafic du jour)
|  |  |-- RENATER-data.json          (évolution du débit)
|  |  |-- XXX-data.json              (évolution du débit pour XXX, généré « à la volée »)
|  |  |-- ....json
|  |  |-- STATS_RENATER
|  |  |   `-- ALL-STATS_RENATER.json (statistiques : volumes moyen, débits moyens, etc.)
|  |  |-- TOP_N_ALL
|  |  |   |-- host-TOP_N_ALL.json    (top N des machines)
|  |  |   `-- orga-TOP_N_ALL.json    (top N des organismes)
|  |  `-- TOP_N_BY_ORGA
|  |     |-- XXX-TOP_N_BY_ORGA.json  (top N des machines pour l'organisme XXX)
|  |     |--...
|  |--...
|  |--Month  (récapitulatif du mois entier, les fichiers sont analogues à ci-dessus)
```

```
|   |--|-- DETAILLED_METRO
|   |  |   |-- RENATER-DETAILLED_METRO.json
|   |  |   |-- XXX-DETAILLED_METRO.json
|   |  |   |--...
|   |  |  |-- index.json
|   |  |-- RENATER-data.json
|   |  |-- STATS_RENATER
|   |  |   `-- ALL-STATS_RENATER.json
|   |  |-- TOP_N_ALL
|   |  |   |-- host-TOP_N_ALL.json
|   |  |   `-- orga-TOP_N_ALL.json
|   |  `-- TOP_N_BY_ORGA
|   |      |-- XXX-TOP_N_BY_ORGA.json
|   |      |--...
|--...
|--2016-Week#17     (un répertoire par semaine, les fichiers sont analogues à ci-dessus)
|--|-- DETAILLED_METRO
|   |   |-- RENATER-DETAILLED_METRO.json
|   |   |-- XXX-DETAILLED_METRO.json
|   |   |...
|   |-- index.json
|   |-- RENATER-data.json
|   |-- STATS_RENATER
|   |   `-- ALL-STATS_RENATER.json
|   |-- TOP_N_ALL
|   |   |-- host-TOP_N_ALL.json
|   |   `-- orga-TOP_N_ALL.json
|   `-- TOP_N_BY_ORGA
|       |-- XXX-TOP_N_BY_ORGA.json
|       |--...
|
|--...
|--LAST_TOP
|   |-- RENATER.json  (Fichier contenant le top N des X dernières minutes tous organismes)
|   |-- XXX.json      (Fichier contenant le top N des X dernières minutes de XXX)
|   |--…
|
```

Figure 4 - Arborescence des données et résultats

8 Utilitaires

8.1 Le script fast_update.sh (pas utilisable en 5.1_5.9)

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 mettant à jour les fichiers modifiés dans le répertoire du service existant.

Attention, le numéro et la date de version ne sont pas nécessairement modifiés.
De plus le service **netMet doit être arrêté** avant d'exécuter le script.

N.B. Ce script n'est pas disponible avec la version 5.1_5.9.

8.2 Le script nmHOST_DETAILS4Json.pl

Ce script situé dans le répertoire `scripts` du service netMET 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 arguments.
Ces graphes sont conservés dans le sous-répertoire GRAPHER du répertoire associé à la période dans le répertoire « html » (où se trouvent les fichiers Json générés).
De plus ils sont envoyés par courriel à l'adresse électronique fournie.

```
…/scripts/nmHOST_DETAILS4Json.pl  fichier_de_conf  adresse_IP date periode  adresse_mail
```

La date est au format `aaaa-mm-jj`, et la période est `jour`, `semaine` ou `mois` selon la durée souhaitée.

8.3 Le script TOPS4Json.pl

Situé dans le répertoire `scripts` du service netMET ce script utilisé pour produire les « tops » instantanés de l'interface Web est aussi utilisable en ligne de commande. La version initiale intégrée à l'ancienne distribution netMET a été développée par Emmanuel Reuter de l'IFSTTAR que je remercie.

Ce script affiche le trafic entrant et sortant des "N" adresses IP les plus consommatrices de bande passante rattachées à l'organisme dont le nom est donné en paramètre sur la période spécifiée (« N » est le paramètre `NETMET_HOST_TOP_N` du fichier de configuration du service netMET).

```
…/scripts/TOPS4Json.pl conf=fichier_de_conf [duree=X] [organisme=nom] [datefinale=aaaa-mm-jj_xxhmn] [format=format]
```

- Le paramètre `duree` est la durée en minutes 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.
- `organisme` 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. Attention, ce paramètre n'est pas utilisé dans la version actuelle, les tops de tous les organismes sont actuellement générés.
- `datefinale` 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 utilisées.
- Le paramètre `format` est `json` ou `csv`. Dans le premier cas les tops sont conservés au format `json` à raison d'un fichier par organisme placé dans le répertoire `LAST_TOP` du répertoire défini par le paramètre `NETMET_HTML_PATH` du fichier de configuration. Avec `csv` le script affiche le résultat sur la sortie standard dans une feuille de calcul au format `csv`. Lorsque c'est possible le nom des machines est affiché ainsi que l'organisme de rattachement.

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 2016-06-07 (nouveau netMET, version 5_1.5_9)	