netMET Network's METrology

Mise en œuvre pratique
Exploitations des données

CiRen formations

19-20 novembre 2001 - CINES, Montpellier

CiRen	*ciren@renater.fr*
netMET	*netmet@netmet-solutions.org*
Christine LIBOUBAN	*Christine.Libouban@cines.fr*
Alexandre SIMON	*Alexandre.Simon@ciril.fr*

netMET Network's METrology

CiRen formations

- un partenariat entre

  CINES et Renater

- Formation netMET - Network's METrology assurée par
  - Christine LIBOUBAN – CINES, Montpellier
    Christine.Libouban@cines.fr
  - Alexandre SIMON – CIRIL, Nancy
    Alexandre.Simon@ciril.fr
- Matériel (routeur Cisco 4000) prêté par AXIANS Opérateur de Solutions réseaux et télécoms
  - agence de Nancy

19-20 novembre 2001 Formation CiRen : Exploitation des données 2

netMET
Network's METrology

netMET Network's METrology

Une solution de métrologie développée par le

CRIL

Centre
Interuniversitaire des
Ressources
Informatiques de
Lorraine

netMET Network's METrology

Plan

- Les fichiers de logs
- L'arborescence des répertoires netMET
- netMET LookUp : Outil de recherches multi-critères
- Les binaires netMETxxx

netMET Network's METrology

Les fichiers de logs

- Fichier de logs général pour le(s) collecteur(s) netMET
  - sous `/var/log/netmet`
  - format à la "*cflowd*" : 3 types de messages
    - `[I]` : Information
    - `[W]` : Warning, avertissement non critique
    - `[E]` : Error, erreur critique... abandon du programme
  - les messages "classiques"
    - `[E] - initKNOWNprot_serv/getprotobyname() - src/accMETdata.c/271`
      - détection d'incohérence entre les fichiers `/etc/protocols` et `/etc/services`
    - `[W] - accMetFlow - protocol UNKNOWN : 130`
      - un paquet de protocole numéro 130 a été reçu par le collecteur, or ce protocole n'est pas déclaré dans `/etc/protocols`, il est donc considéré comme inconnu
        --> **le paquet n'est pas traité**

19-20 novembre 2001 Formation CiRen : Exploitation des données 5

Les messages classiques :

- `[E] - initKNOWNprot_serv/getprotobyname() -src/accMETdata.c/271`

Le processus d'accounting construit pour un couple {addrSRC - addrDST} une liste de services/protocoles avec les quantités octets échangées. Pour la reconnaissance des protocoles et services connus, le processus s'appuie sur les fichiers de configuration du système : `/etc/protocols` et `/etc/services`. Au démarrage, `netMETacc` "charge" ces fichiers et vérifie leur cohérence : un protocole utilisé dans `/etc/services` DOIT EXISTER dans `/etc/protocols`... si il existe une incohérence entre ces fichiers on obtient cette erreur.

- `[W] - accMetFlow - protocol UNKNOWN : 130`

Se reporter à "l'algorithme d'identification des services".

Ici, le collecteur a reçu un paquet transportant le protocole numéro `130` (champ protocole du paquet), mais comme il n'est pas pas déclaré dans `/etc/protocols`, il est considéré comme inconnu et le paquet n'est pas traité.

Certains protocoles sont et doivent rester inconnus (on ne peut pas être exhaustif pour le 255 protocoles du fichier `/etc/protocols`). Pour la prise en compte effective d'un protocole particulier, il faut donc renseigner le fichier `/etc/protocols`.

RQ: c'est exactement le même processus pour la détection des services, sauf qu'aucun message d'avertissement n'est envoyé à la détection d'un service dit "inconnu". Pour reconnaître un service donné (i.e. "port/protocole"), il faut renseigner le fichier `/etc/services`.

netMET Network's METrology

Les fichiers de logs

- Fichier de logs général pour le(s) collecteur(s) netMET
  - les messages "classiques"
    - `[W] - SHARED MEMORY seems to be TOO small at least one time, FLOWS could be lost !`
      et
      `[W] - SHARED MEMORY seems to be TOO small : [18/135 = 13.3%] flows lost`
      - la mémoire partagée entre les processus `netMETcll` et `netMETacc` a débordé, le processus `netMETacc` a été trop long à traiter les `MetFlows` envoyés par `netMETcll`
      - le premier message indique qu'il y a eu au moins 1 problème,
      - le second message apparaît à l'arrêt ou au redémarrage du collecteur pour quantifier les `MetFlows` réellement perdus
    - `[I] - Collector netMETcll restarted -[UDP=12198, FLOW_r=365940, FLOW_f=358273, FLOW_p=358273, 97.9% flows processed by netMETcll , 100.0% flows processed by netMETacc]`
      - quantification des paquets UDP et flows traités

19-20 novembre 2001 Formation CiRen : Exploitation des données 6

Les messages classiques :

- `[W] - SHARED MEMORY seems to be TOO small at least one time, FLOWS could be lost !`

et

`[W] - SHARED MEMORY seems to be TOO small : [18/135 = 13.3%] flows lost`

Les `MetFlows` passent du processus `netMETcll` au processus `netMETacc` via une mémoire partagée. Cette mémoire a une taille limitée et il se peut que `netMETcll` remplisse plus vite que `netMETacc` n'est capable de traiter… Ce problème traduit le fait que `netMETacc` est plus lent que `netMETcll` : ceci peut provenir essentiellement des 2 points suivants :

* puissance CPU trop faible

* pas assez de mémoire centrale, ce qui cause des overhead, et donc de l'indisponibilité CPU pour traiter les flows

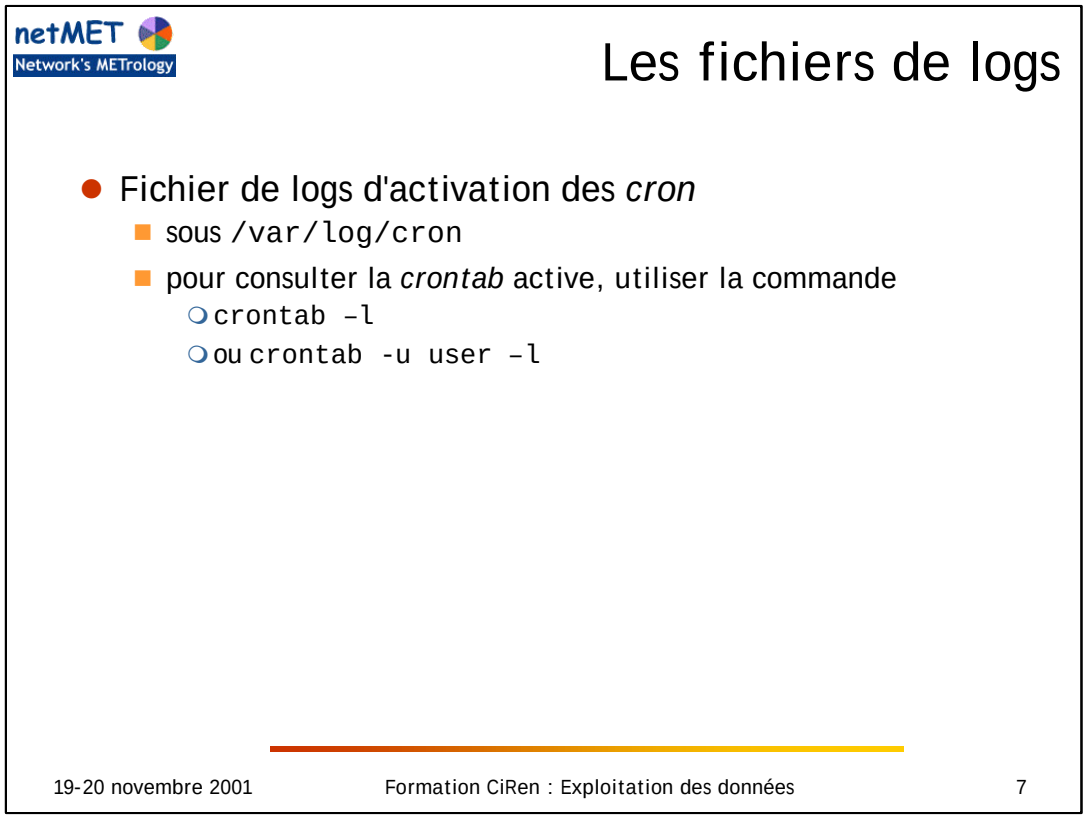
Le premier message apparaît lors du fonctionnement du collecteur : il détecte qu'un débordement a eu lieu, mais ce n'est pas une erreur JUSTE UN WARNING qui stipule que des flows pourront être perdus. Le second message apparaît à l'arrêt ou au redémarrage du collecteur pour quantifier exactement les `MetFlows` perdus entre `netMETcll` et `netMETacc`.

- `[I] - Collector netMETcll restarted -[UDP=12198, FLOW_r=365940, FLOW_f=358273, FLOW_p=358273, 97.9% flows processed by netMETcll , 100.0% flows processed by netMETacc]`

Toutes ces infos. sont disponibles à l'arrêt ou au redémarrage du collecteur.

* UDP=12198 : nombre de paquets UDP traités
* FLOW_r=365940 : nombre de flows reçus dans ces 12198 paquets UDP
* FLOW_f=358273 : nombre de flows réellement traités par netMETcll (après application des règles (IF_PROCESSED et IF_AGGREGATION) et passés au processus d'accounting netMETacc
* FLOW_p=358273 : nombre de flows réellement traités par netMETacc

Ici le pourcentage 97.9% est normale puisque le collecteur épure quelques flows (flows non désirés). Si des flows étaient perdus entre les 2 processus netMETcll et netMETacc, le 2ème pourcentage ne serait pas à 100%… Si ce pourcentage n'est pas à 100%, cela signifie que la machine n'a pas pu tout traiter (manque de puissance CPU ou manque de mémoire ?!?). Ce cas de figure s'accompagne d'un WARNING dans les logs… (i.e. le warning précédent)



Tous les scripts d'exploitation (génération des fichiers dump et génération des fichiers .html et .png) sont lancés à intervalles réguliers grâce à la *crontab* de l'utilisateur `netmet`.

Rq: le fait que ces scripts soient lancés par la *crontab* de `netmet`, implique qu'ils sont exécutés avec les droits du user `netmet` (et pas en `root` ou un autre utilisateur).

Les archives d'exécution de ces scripts se trouvent sous `/etc/log/cron`, au format :

```
netmet (11/12-14:31:01-11417) CMD (/home/netmet/netMet/scripts/STATScron-daily.pl
/home/netmet/netMet/etc/explt.conf)
netmet (11/12-14:32:00-11628) CMD (/home/netmet/netMet/scripts/METROcron-
daily_weekly_monthly.pl /home/netmet/netMet/etc/explt.conf --daily)
netmet (11/12-14:35:00-11636) CMD (/home/netmet/netMet/scripts/STATScron-5.pl
/home/netmet/netMet/etc/explt.conf)
```

*** La *crontab* de netmet : version simplifiée et lisible ***

```
MAILTO=administrateur-netmet@domaine.fr

# scripts/STATS : STATScron pour netMET-STATS
# scripts/STATS : Echantillons toutes les 5mn
# scripts/STATS : Parse et gen tous les jours toutes les 10mn
# scripts/STATS : Parse et gen tous les Lundi matin a 01h07mn pour la semaine
precedente
# scripts/STATS : Parse et gen tous les 1er du mois a 02h07mn pour le mois precedent

# scripts/METRO : METROcron pour netMET-METRO
# scripts/METRO : Echantillons toutes les 10mn
# scripts/METRO : Parse et gen tous les jours toutes les 10mn
# scripts/METRO : Parse et gen tous les Lundi matin a 01h37mn pour la semaine
precedente
# scripts/METRO : Parse et gen tous les 1er du mois a 03h07mn pour le mois precedent

# scripts/INDEX : INDEXcron pour netMET-STATS & netMET-METRO
# scripts/INDEX : Generation INDEX general tous les jours a 05h00

# scripts/SECURE : SECUREcron pour netMET-SECURE
# scripts/SECURE : Echantillons toutes les 10mn
# scripts/SECURE : Echantillons toutes les 10mn - pour une duree de 24h
# scripts/SECURE : Generation rapport scans
```

netMET Network's METrology

Les fichiers de logs

- Fichier de logs du serveur web *apache*
  - sous `/var/log/httpd/*`
  - mais plus particulièrement
    - `/var/log/httpd/netmet.access`
    - `/var/log/httpd/netmet.error`
    - `/var/log/httpd/suexec_log`
      !!! le nom `suexec_log` dépend de la compilation du binaire suexec (on peut aussi avoir `cgi.log`)
  - Pour l'administration/exploitation d'*apache*, se reporter à :
    - http://www.apache.org
    - http://httpd.apache.org/docs-project/
    - à venir sur netMET :
      - une documentation minimale pour démarrer avec *apache*

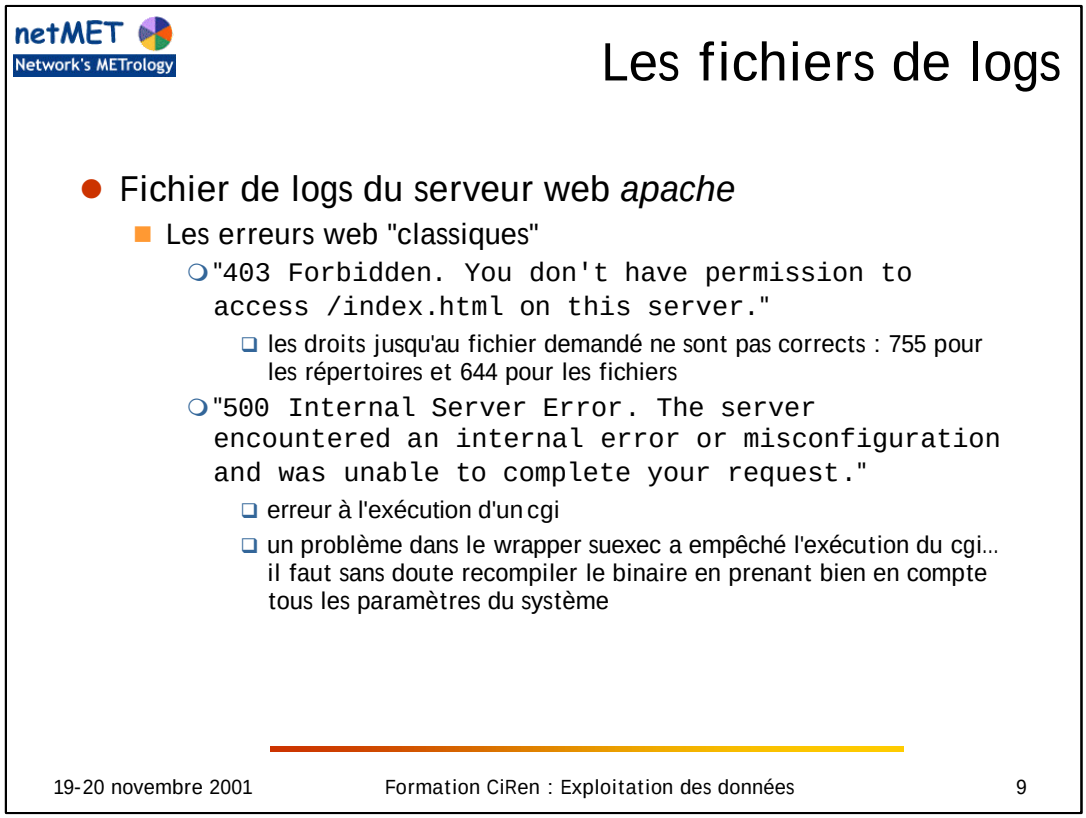
19-20 novembre 2001 Formation CiRen : Exploitation des données 8

Par défaut, les logs du serveur web *apache* se trouve sous `/etc/httpd/logs/` qui est un lien vers `/var/log/httpd/` ... pour des configurations non-standards, se reporter au fichier de configuration d'apache `httpd.conf` et consulter les variables :

- `ServerRoot`
- `ErrorLog`
- `CustomLog`

Les logs du wrapper suexec, se trouvent par défaut sous `/var/log/httpd/suexec_log` ou `/var/log/httpd/cgi.log` ... pour des configurations non-standards se reporter au fichier include des sources du binaire `suexec` : `suexec.h` et consulter la variable :

- `LOG_EXEC`



L'erreur 403 est vraiment classique (on peut y passer des heures avant de trouver la solution :-))… elle indique que le fichier n'a pas pu être accédé car les droits sur les répertoires et fichiers jusqu'à ce fichier n'étaient pas corrects. En effet, le serveur *apache* s'exécute généralement en user `httpd`, `apache` ou `nobody`, qui sont des users sans droits particuliers. Il faut donc que les répertoires soient en 755 (`rwx- r-x r-x`) et les fichiers en 644 (`rw- r-- r--`) pour que ces users puissent accéder à ce fichier. A faire: reprendre toute l'arborescence à partir de `/` et descendre jusqu'au fichier en vérifiant les droits.

L'erreur 500 peut apparaître lors de l'activation des cgi sur le serveur web virtuel de netMET. Le but ici n'est pas d'expliquer le fonctionnement du wrapper suexec, mais de donner quelques explications pour se sortir de cette situation (une documentation dédiée, pour *apache* sous netMET, devrait être disponible).

Le wrapper suexec permet au serveur web *apache*, qui par défaut fonctionne en user `httpd`, `apache` ou `nobody`, d'endosser les droits d'un autre user (ici le user `netmet`). C'est un mécanisme équivalent au `su` sur Unix. Seulement ici le suexec effectue un certain nombre de vérifications avant de permettre l'endossement entre autre :

- que le serveur web fonctionne avec un user particulier (`httpd`, `apache` ou `nobody`)
- que le UID et GID de l'utilisateur à endosser soient supérieurs à certaines valeurs
- que le cgi à exécuter se trouve sous une arborescence approuvée

Si ces paramètres sont mal configurés pour le wrapper suexec, cela entraînera des problèmes d'endossement et donc d'erreurs au niveau web. C'est paramètres s'éditent dans le fichier d'include `suexec.h`, après quoi il faut recompiler le binaire `suexec` et le réinstaller pour sa prise en compte. Les paramètres à éditer sont :

- `#define HTTPD_USER`
- `#define UID_MIN`
- `#define GID_MIN`
- `#define DOC_ROOT`
- `(#define LOG_EXEC)`

Le wrapper suexec se trouve par défaut sous `/usr/sbin/suexec` avec les droits 4711 (`-rws --x --x`). Pour sa reprise en compte, il faut arrêter/redémarrer le serveur web *apache* avec `/etc/rc.d/init.d/httpd restart` et vérifier cette prise en compte dans le fichier de log `/var/log/httpd/error_log` par la ligne :

```
[notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
```

netMET Network's METrology

Les fichiers de logs

- Informations fichier de collecte `zzaccounting.dmp`
  - pour consulter ces informations utiliser la commande
    - `netMETexp --accinfo zzaccounting.dmp`
  - permet de consulter/vérifier la cohérence d'un fichier de collecte
  - Exemple de sortie :

```
------------------------------------------------------------------------
Metrology from Tue-13/11/2001 14:00:17 to Tue-13/11/2001 14:02:16
--
Nb of differents hosts                                          : 15
Nb of differents bidirectionals communications                  : 28
Accounting info. memory size                                    : 1376
Average memory size of accounting info. by bidirectionals comm. : 49
Average Number      of [serv/prot]      by bidirectionals comm. : 2.43
------------------------------------------------------------------------
```

19-20 novembre 2001 Formation CiRen : Exploitation des données 10

Un fichier de collecte `zzaccounting.dmp` contient toutes les informations d'accounting pour une période horaire donnée. La commande `netMETexp --accinfo zzaccounting.dmp` permet de consulter ces informations de tranche horaires, mais fournit également quelques statistiques simplifiées sur les données contenues dans ce fichier, à savoir :

- l'heure de début et de fin de la collecte
- le nombre de machines différentes dans les couples @SRC-@DST (on construit une table unique des machines qui sont apparues dans les couples)
- le nombre de communications bidirectionnelles détectées, c'est également le nombre de couples @SRC-@DST
- la taille du fichier de collecte
- la taille moyenne des informations de métrologie pour un couple @SRC-@DST
- la taille moyenne de la liste [serv/prot](quantité) pour un couple @SRC-@DST

Remarque: grâce à l'information "taille moyenne des informations de métrologie pour un couple @SRC-@DST", on peut très facilement extrapoler la taille d'un fichier de collecte en fonction du nombre potentiel de couples différents @SRC-@DST :

taille fichier de collecte = (nb. de couples @SRC-@DST) x (taille moyenne des informations de métrologie pour un couple @SRC-@DST)

netMET Network's METrology

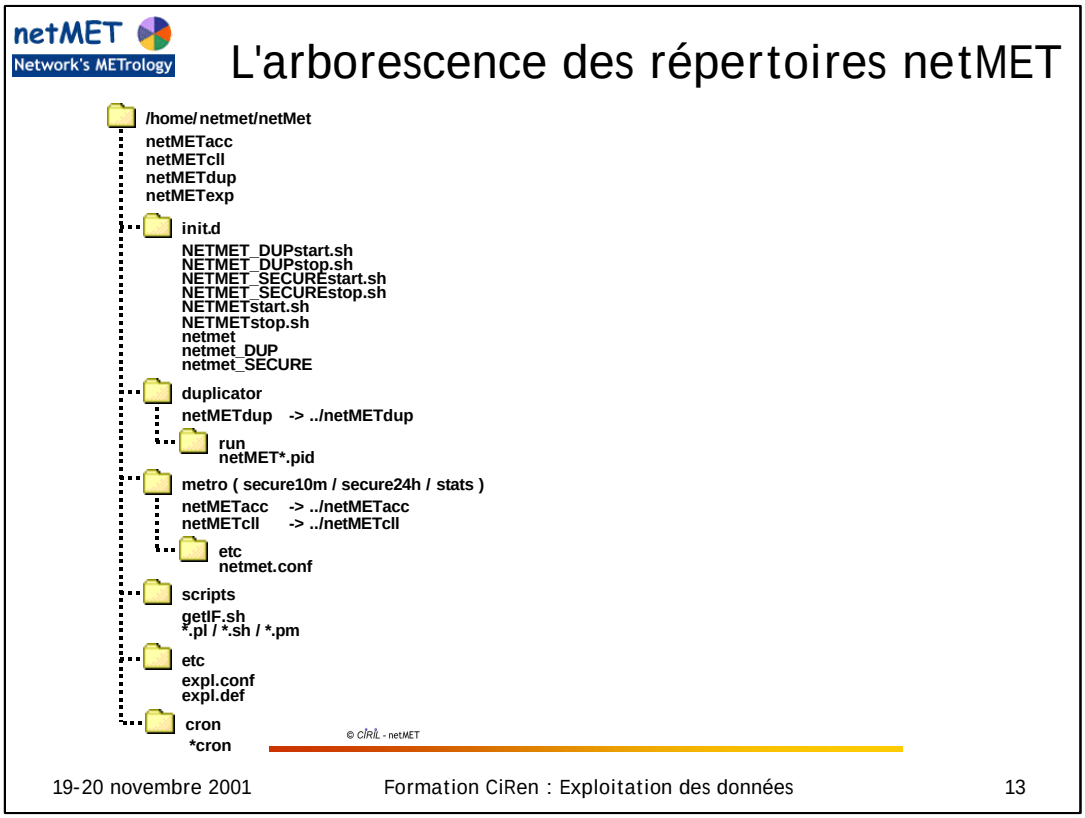
Plan

- Les fichiers de logs
- L'arborescence des répertoires netMET
- netMET LookUp : Outil de recherches multi-critères
- Les binaires netMETxxx

netMET Network's METrology

L'arborescence des répertoires netMET

- Pour netMET tout se passe sous `/home/netmet`
  - binaires et scripts
  - fichiers de configuration
  - données collectés et fichiers générés
- L'arborescence des répertoires est très cohérente/explicite, à tout moment on peut savoir
  - "où l'on est"
  - "d'où viennent les données manipulées"
  - "ce qu'est susceptible de faire un script/exécutable"



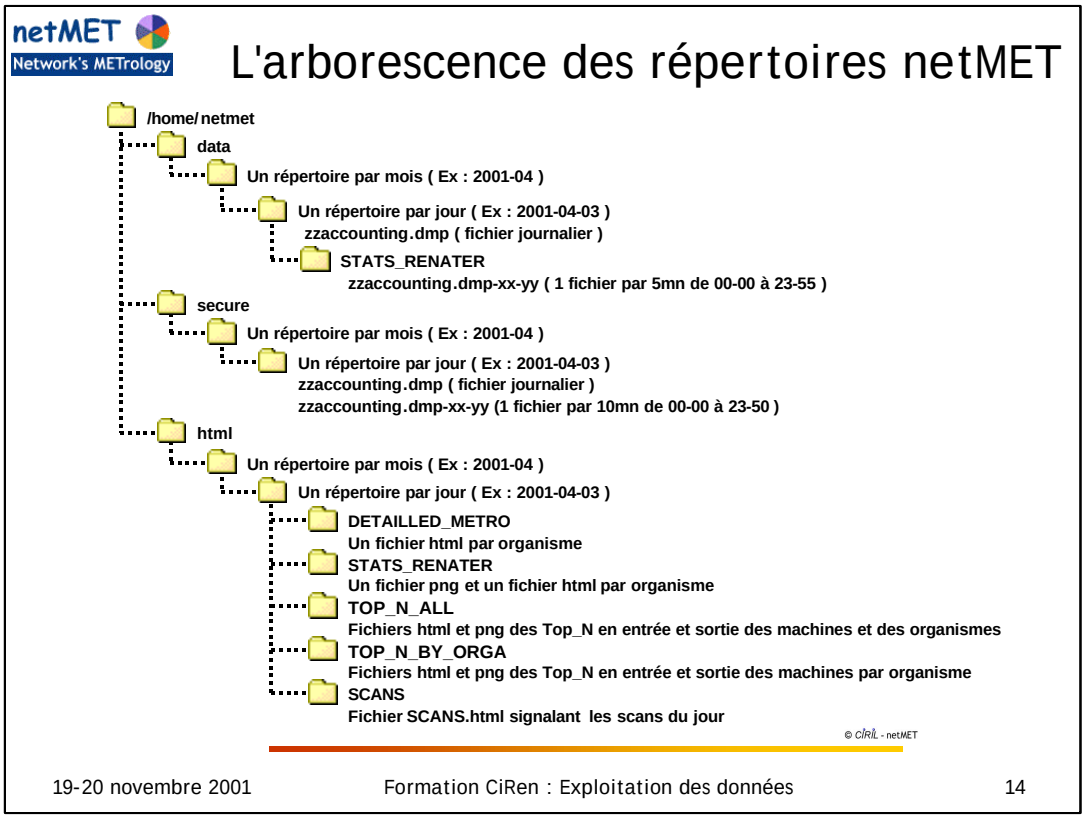
Toute la partie opérationnelle de netMET (les scripts, binaire et fichiers de configuration) se trouvent sous

- `/home/netmet/netMet`

On y trouve :

- les binaires de netMET (`netMETacc`, `netMETcll`, `netMETexp`, `netMETscn`, `netMETdup`)
- les scripts *perl* et *shell* : `scripts/*.pl  *.pm  *.sh`
- les scripts *cgi* : `scripts-cgi/*.pl`
- les 4 services avec les collecteurs et fichiers de configuration associés (`metro`, `stats`, `secure10m`, `secure24h`)
- les fichiers de configuration générale de l'exploitation : `etc/*`
- les fichiers *cron* utiliser pour générer la *crontab* en fonction des services démarrés : `cron/*`
- les scripts utilisés lors du processus init SysV : `init.d/*`

Rq: à ce sujet, il est rappelé de ne pas employer directement ces scripts, mais d'utiliser : `/etc/rc.d/init.d/netmet*` qui permettent de démarrer/arrêter les différents services.



Les répertoires `data`, `secure` et `html` contiennent toutes les données collectées (fichiers de collecte `zzaccounting.dmp`) et tous les fichiers générés (`*.html` `*.png`).

La structure se base sur une arborescence de répertoires d'`année-mois` et `année-mois-jour`. Le référencement et l'exploitation des données sont ainsi facilités :

- les structures et hiérarchies sont toujours les mêmes
- une base temporelle permet une meilleur exploitation de données : archives et nettoyage
- l'espace de nommage permet, au travers d'*apache*, de faire de l'authentification/permission pour des utilisateurs et/ou groupes sur des données particulières
  Par exemple : authentifier et permettre que certains utilisateurs n'accèdent
  * qu'aux informations d'un organisme donné
  * qu'uniquement aux TOP n généraux
  * …

  Pour cette configuration (authentification/permission) une documentation spécifique devrait être disponible d'ici peu.

L'arborescence des répertoires netMET

- Nettoyage des données
  - pour une exploitation à long terme, il faut :
    - conserver le répertoire `html` le plus longtemps possible
      - ces répertoires et fichiers peuvent être regénérés à la main (en utilisant les scripts d'exploitation) en fonction de la disponibilité des fichiers de collecte sous `data` et `secure` correspondants
    - conserver le répertoire `data` au moins 1 mois
      Rq: avec 18Go, il est possible de conserver plus d'une année de collecte!
      - pas de regénération possible!
    - le répertoire `secure` se nettoie automatiquement en ne conservant les fichiers de collecte que sur une durée déterminée (i.e. un nombre de jours)
      Rq: c'est le paramètre `NETMET_SECURE_RR` du fichier de configuration de l'exploitation `~/netMet/etc/explt.conf`
      - pas de regénération possible!

19-20 novembre 2001 Formation CiRen : Exploitation des données 15

Pour faire du ménage sous les répertoires `html`, `data` et `secure`, il suffit de supprimer (ou déplacer) tous les répertoires qui se trouvent sous ces arborescences. Attention, il faut néanmoins que certains répertoires ne soient pas supprimés car ils ne sont pas automatiquement regénérés, à savoir :

- `/home/netmet/html`
- `/home/netmet/html/Auth`
- `/home/netmet/html/images`
- `/home/netmet/html/netmet-cgi-bin`
- `/home/nemet/data`
- `/home/netmet/secure`

Il est recommandé (**en fonction des disponibilités d'espace disque et de la politique interne en terme de sécurité et d'archivage des logs**) de :

- conserver le plus longtemps possible les répertoires et fichiers `html`, de manière à publier les informations de métrologie sur de longues périodes et ainsi évaluer les tendances et évolutions des trafics du réseau
- conserver le plus longtemps possible les répertoires et fichiers `data`, de manière à pouvoir regénérer les informations de métrologie (top, stats, ...) en prenant en compte de nouveaux paramètres (nouveaux organismes, nouvelle exploitation, ...)
- conserver le plus longtemps possible les répertoires et fichiers `secure`, de manière à pouvoir traiter après coup des problèmes de sécurité. Remarquons que les répertoires et fichiers `secure` sont automatiquement nettoyés et seuls sont conservés un certain nombre de jours (i.e. on fait du tourniquet sur un nombre de jours maximum). Ce nombre de jours se configure dans le fichier de configuration de l'exploitation : `~/netMet/etc/explt.conf` avec le paramètre `NETMET_SECURE_RR`

Seuls les répertoires et fichiers sous `html` peuvent être regénérés après coup à la main, en fonction de la disponibilité des fichiers de collecte sous `data` et `secure`. Les scripts à utiliser sont les suivants :

```
INDEXgen-daily.pl
METROparse_gen-daily_weekly_monthly.pl
SECURE_SCANSparse_gen-daily.pl
STATSgen-daily_weekly_monthly.pl
STATSparse_gen-daily.pl
STATSparse_gen-weekly_monthly.pl
```

Ils peuvent être lancés "à la main", selon le format : "nom_du_script fichier_de_configuration période".

L'arborescence des répertoires netMET

- Index html général de netMET
  - cet index général est généré tous les matins à 5h00
  - on peut régénérer cet index à la main avec la commande
    - `~/netMet/scripts/INDEXgen-daily.pl ~/netMet/etc/explt.conf`
    - soit à la première installation
    - soit à la suite de modification/nettoyage dans le répertoire `html`
- Le logo de l'administration de netMET (en haut à gauche dans les pages html)
  - par défaut, c'est le logo de la Cellule Réseau StanNet
  - on peut modifier ce logo en remplaçant le fichier `~/html/images/admin-logo.gif` par son propre logo (conserver le nom du fichier `admin-logo.gif`)

netMET Network's METrology

Plan

- Les fichiers de logs
- L'arborescence des répertoires netMET
- netMET LookUp : Outil de recherches multi-critères
- Les binaires netMETxxx

netMET Network's METrology

netMET LookUp

- *netMET LookUp* : outil de recherche multi-critères
  - idées :
    - lancer des *grep* évolués dans les fichiers de collecte
    - répondre rapidement à « y a t-il un réel problème? »
  - applications :
    - choix d'un fichier de recherche (agrégé ou non, période)
    - choix machine source, destination, source et ou destination
    - choix service/protocole
    - choix quantité
    - ...
  - permet d'exprimer des requêtes quotidiennes simples (et parfois même compliquées) pour une première approche sécurité

19-20 novembre 2001 Formation CiRen : Exploitation des données 18

Idée de base :

- en consultant les informations de base (TOP et statistiques) j'étais intrigué par le comportement de certaines machines
- pour regarder ça de plus près, je me connectais en *telnet* sur la machine de production et à grands coups de "`netMETexp`" et "`grep`" je recherchais exactement ce qu'avait fait cette machine
- voyant que les "`grep`" étaient toujours les mêmes... l'idée du netMET LookUp avec son interface sur le web commençait à se préciser.

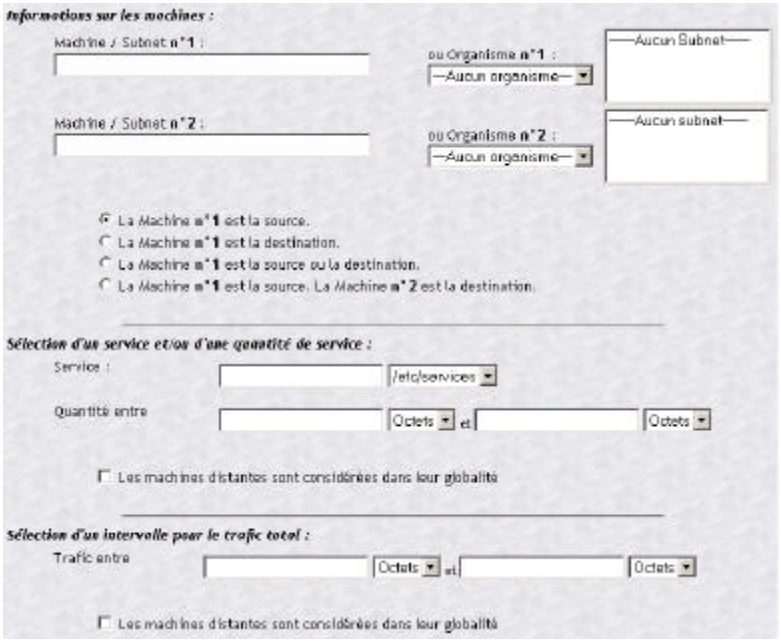
Aujourd'hui, netMET LookUp permet de répondre très facilement et assez rapidement aux questions classiques que l'on peut se poser en cas de problèmes avec une machine.

A lire :"netMET LookUp : Outil de recherche multicritères".

A voir : quelques requêtes réelles pour se rendre compte des possibilités de l'outil...

netMET Network's METrology

netMET LookUp



netMET Network's METrology

netMET LookUp

- A lire : la documentation
  "netMET LookUp : Outil de recherche multicritères"
- Mise en garde !!! : il faut bien comprendre le mécanisme du moteur de netMET LookUp
  - pour savoir ce qui est possible ou non avec cet outil
  - pour savoir interpréter les résultats fournis
  - pour ne pas lancer des requêtes "trop gourmandes"

netMET Network's METrology

Plan

- Les fichiers de logs
- L'arborescence des répertoires netMET
- netMET LookUp : Outil de recherches multi-critères
- Les binaires netMETxxx

netMET Network's METrology

Les binaires netMETxxx : netMETcll

```
Use of 'netMETcll' :
netMETcll -s --start [-p --printFLOWS [-w --withROUTERrules]] [ -a --accrecover __recoverFILE__ ]
netMETcll -r --restart
netMETcll -k --kill

netMETcll -v --version
netMETcll [-h --help]

Parameters         :
 -s --start [ -a --accrecover __recoverFILE__ ] :
      Start netMETcll and launch netMETacc.
      If option --accrecover is used, netMETcll launch netMETacc
      with recover file '__recoverFILE__'.
-p --printFLOWS [-w --withROUTERrules] :
      Combined with -s command, netMETcll prints on stdout NetFlows
      received from router(s).
      If -w option is used, NetFlows are printed after ROUTER's rules.
      Default prints NetFlows before ROUTER's rules.
 -r --restart      : REStart netMETcll and launch a new netMETacc.
 -k --kill         : Stop and quit netMETcll.
```

Les binaires netMETxxx : netMETacc

```
Use of 'netMETacc' :
netMETacc -d --dump
netMETacc -r --restart

netMETacc -v --version
netMETacc [-h --help]

Parameters         :
 -d --dump         :
      netMETacc dumps accounting information from memory to
      accounting file.
 -r --restart      :
      REStart a new netMETacc.
```

Les binaires netMETxxx : netMETdup

```
Use of 'netMETdup' :
netMETdup -l --listen IPaddr/port  -d --duplicate IPaddr/port -d ...
netMETdup -k --kill

netMETdup -v --version
netMETdup [-h --help]

Parameters         :
 -l --listen    IPaddr/port : netMETdup listen to UDP datagrams on
                              UDP 'port' associated to 'IPaddr'.
                              Only ONE listened port.
 -d --duplicate IPaddr/port : netMETdup duplicate UDP datagrams received
                              on listening port to host 'IPaddr' on UDP 'port'.
                              Duplication can be multiple.
 -k --kill                  : Stop and quit netMETdup.
```

netMET Network's METrology

Les binaires netMETxxx : netMETexp

```
Use of 'netMETexp' :
netMETexp -H --HOSTaccprint __zzaccounting_file__ [__..._]                          [-c --CUMULaccprint]
netMETexp -O --ORGAaccprint __zzaccounting_file__ [__..._] -f --ORGAfile __ORGAfile__ [-c --CUMULaccprint]
[-a --ALLtraffic]
netMETexp -M --MERGEfiles   __zzaccounting_file__ [__..._] -f --Mfile    __MERGEDfile__
netMETexp -V --VALIDhost    __zzaccounting_file__ [__..._] -f --ORGAfile __ORGAfile__
netMETexp -T --TESThost                                    -f --ORGAfile __ORGAfile__
netMETexp -p --PRINTdefs                                   -f --ORGAfile __ORGAfile__
netMETexp -i --accinfo      __zzaccounting_file__ [__..._]

netMETexp -v --version
netMETexp [-h --help]

Parameters         :
 -H --HOSTaccprint __zzaccounting_file__ :
      netMETexp prints on stdout HOST's accounting information from
      accounting file(s) __zzaccounting_file__ __..._ .
 -O --ORGAaccprint __zzaccounting_file__ :
      netMETexp prints on stdout ORGANISM's accounting information from
      accounting file(s) __zzaccounting_file__ __..._ .
 -M --MERGEfiles __zzaccounting_file__   :
      netMETexp reads accounting files __zzaccounting_file__ __..._ ,
      makes an accumulation of these files and merges the result into
      en MERGEDfile specified with option -f --Mfile.
```

netMET Network's METrology

Les binaires netMETxxx : netMETexp

```
Use of 'netMETexp' :
Parameters         :
-T --TESThost :
      netMETexp tests IP addresses passed on stdin and prints on stdout
      the attribution name or (null) if unknown respect to ORGAfile.
 -p --PRINTdefs :
      netMETexp prints on stdout in a formated form @IP attributions
      respect to ORGAfile.
 -f --ORGAfile __ORGAfile__              :
      netMETexp recognizes ORGANISMs into IP addresses with the __ORGAfile__
      correspondence file.
 -f --Mfile    __MERGEDfile__            :
      netMETexp merges result of the MERGE operation into __MERGEDfile__.
 -c --CUMULaccprint                      :
      Combined with -H or -O option, netMETexp prints on stdout accounting
      information in 'cumul' mode. Default is 'detailled' mode.
 -a --ALLtraffic                         :
      Combined with -O option, netMETexp prints on stdout accounting
      information for organisms from ORGAfile included traffics with
      undefined range of IP addresses. Default is 'defined' traffic.
 -i --accinfo  __zzaccounting_file__     :
      netMETacc prints on stdout some accounting statistics from
      accounting file(s) __zzaccounting_file__ __...__ .
```

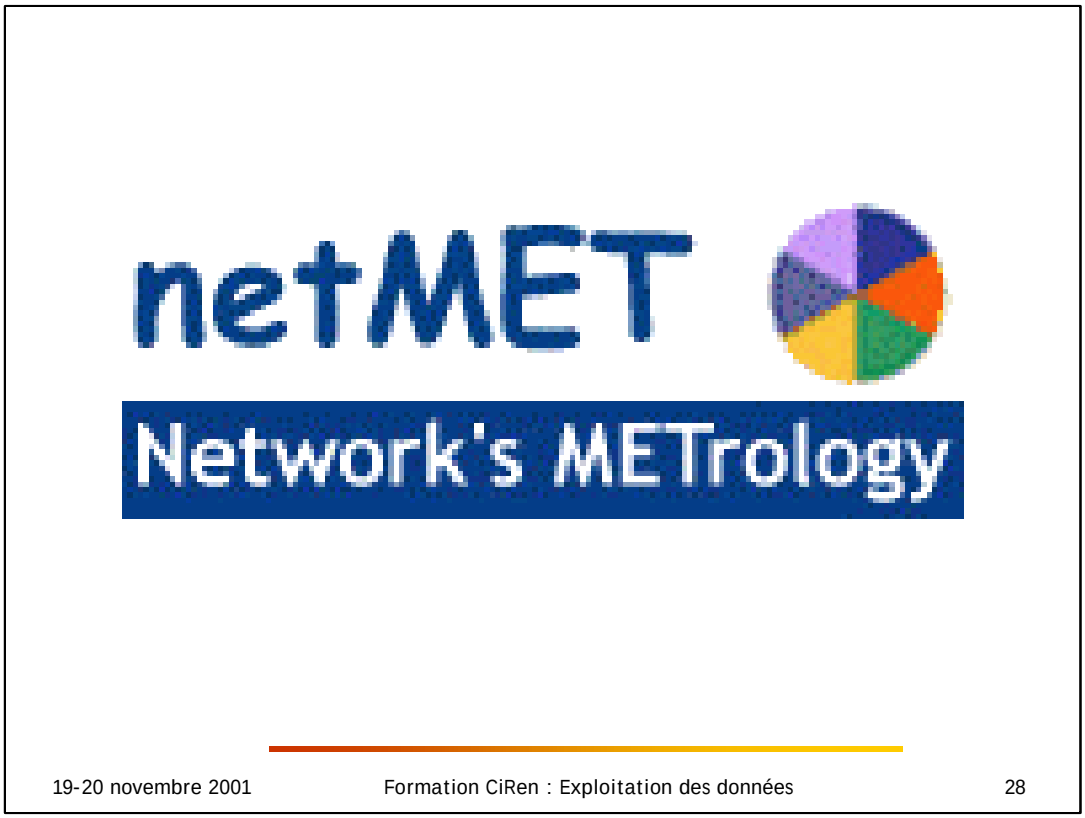
Les binaires netMETxxx : netMETscn

```
Use of 'netMETscn' :
netMETscn -H --Hscans __zzaccounting_file__ [__..._]
netMETscn -W --Wscans __zzaccounting_file__ [__..._]
netMETscn -c --ip2class

Parameters       :
 -H --Hscans     :
      netMETscn reads dump file __zzaccounting_file__ and prints on stdout
      scan informations with format :
        @IPsrc @SUBNETdst [serv/proto](nb scan) [serv/proto](nb scan) ...
        ...
      These are "height scans".

 -W --Wscans     :
      netMETscn reads dump file __zzaccounting_file__ and prints on stdout
      scan informations with format :
        @IPsrc @IPdst (nb of services scanned)
        ...
      These are "width scans".

 -c --ip2class     :
      netMETscn converts IP addresses passed on stdin and prints on stdout
      the conversion into IP classes format.
      Ex: 192.168.1.2 converst into 192.168.1.0
```


netMET
Network's METrology
19-20 novembre 2001
Formation CiRen : Exploitation des données
28