netMET Network's METrology

Exploiter & intégrer netMET

24-28 mars 2003 - CINES, Montpellier

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

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

- Introduction

- Les fichiers de netMET
- Exploiter les fichiers de netMET
- Apache : authentification et permissions pour netMET
- Les fichiers de log de netMET

- Conclusion

netMET Network's METrology

Introduction

- netMET est une solution 'out of the box'
  - netMET collecte & analyse les informations issues de la technologie NetFlow
  - netMET ne nécessite pas de développement annexe
    - Installez,
    - attendez les premiers résultats
  - netMET ne nécessite pas de logiciel 'tiers' pour fonctionner
- netMET reste néanmoins 'ouvert' et peut être étendu pour intégrer des besoins spécifiques

netMET Network's METrology

Introduction (suite)

- Une intégration netMET nécessite des connaissances plus approfondies sur l'exploitation des fichiers de collecte
- Une intégration netMET nécessite une utilisation adaptée du serveur HTTP Apache
- Une intégration netMET nécessite de savoir déchiffrer les fichiers 'logs'

netMET Network's METrology

Plan

- Introduction
- Les fichiers de netMET
- Exploiter les fichiers de netMET
- Apache : authentification et permissions pour netMET
- Les fichiers de log de netMET
- Conclusion

netMET Network's METrology

Les fichiers de netMET

- Deux types de fichiers
  - Données collectées : les fichiers de collecte, également appelés 'dumps'
  - Résultats de l'exploitation des fichiers de collecte : fichiers d'exploitation
- Trois répertoires distincts
  - `~netmet/data` et `~netmet/secure` : fichiers de collecte
  - `~netmet/html` : fichiers d'exploitation

netMET Network's METrology

Fichiers de collecte

- Fichiers dump (.dmp) répartis dans 2 répertoires
  - Agrégation du réseau fédérateur
  - Toute adresse Internet visible

```
/home/netmet
|
+---data
|   \---2003-02                          (Un répertoire par mois)
|       \---2003-02-18                   (Un répertoire par jour)
|           +---zzaccounting.dmp         (Fichier journalier)
|           \---STATS_FederNET
|               +---zzaccounting.dmp-xx-yy (1 fichier par 5 minutes)
|
\---secure
    \---2003-02                          (Un répertoire par mois)
        \---2003-02-18                   (Un répertoire par jour)
           +---zzaccounting.dmp          (1 fichier par jour)
           +---zzaccounting.dmp-xx-yy    (1 fichier par 5 minutes)
```

24-28 mars 2003 Formation CiRen - netMET : Exploiter & intégrer netMET 8

Format des fichiers

Les fichiers 'dump' ont un format binaire propriétaire à netMET. Ce format à pour objectif principal de diminuer l'espace utilisé pour stocker les informations collectées.

Répertoire data

Le répertoire data contient des fichiers de collecte dans les quels les flow concernant le réseau fédérateur sont agrégés.

Le répertoire data contient un ensemble de sous répertoires. Un répertoire par mois au format aaaa-mm (année-mois).

Chacun de ces sous répertoires contient un répertoire par jour du mois : aaaa-mm-jj. Dans ces répertoires, un fichier `zzaccounting.dmp` contenant toutes les informations de collectées avec une agrégation à la journée.

Un sous répertoire au nom du réseau fédérateur : STATS_FederNET (où FederNET est à remplacer par le nom du réseau fédérateur). Il contient un ensemble de fichiers nommés `zzaccounting.dmp-hh-mm` (ou hh = heure et mm = minute). Chaque fichier contient les données agrégées sur 5 minutes, soit 288 fichiers par jour.

Répertoire secure

Le répertoire data contient des fichiers de collecte dans les quels les MetFlow ne sont pas agrégés au regard du réseau fédérateur (toute adresse IP visible)

La sous arborescence est identique à celle du répertoire data : un répertoire par mois contenant un répertoire par jour. Chaque répertoire journalier contient alors un fichier `zzaccounting.dmp` avec une agrégation à la journée. 288 fichiers `zzaccounting.dmp-hh-mm` avec une agrégation de 5 minutes.

netMET Network's METrology

Fichiers d'exploitation

- Dans le répertoire ~netmet/html
  - Fichiers de l'interface
  - HTML, texte, images

```
/home/netmet
|
\---html
   +---2003-02                  (Un répertoire par mois)
       +---2003-02-18           (Un répertoire par jour)
           +---SCANS            (Fichiers html & txt par organisme + 1 global)
           +---DETAILLED_METRO  (1 fichier html par organisme)
           +---TOP_N_ALL        (Fichiers html & png)
           +---TOP_N_BY_ORGA    (Fichiers html & png)
           \---STATS_FederNET   (Fichiers html & png)
```

24-28 mars 2003 Formation CiRen - netMET : Exploiter & intégrer netMET 9

Les fichiers d'exploitation se trouvent dans le répertoire ~netmet/html. Ils sont le résultat de l'analyse des fichiers de collecte et peuvent avoir plusieurs formats :

- •html
- •text
- •png

Ces fichiers sont par nature utilisés pour afficher les informations aux utilisateurs, notamment via le serveur http.

Arborescence

L'arborescence du répertoire html est définie comme suit : un sous répertoire par mois contenant autant de répertoire que de jour dans le mois.

Chaque sous répertoire contient alors :

- •SCANS : rapport de scan global + rapport de scan par organisme (aux formats html et txt)
- •DETAILLED_METRO : métrologie détaillée au format html
- •TOP_N_ALL : top N pour l'ensemble des organismes (format html)
- •TOP_N_BY_ORGA : top N par organisme (format html)
- •STATS_FederNET : statistiques vers le réseau fédérateur (format html)

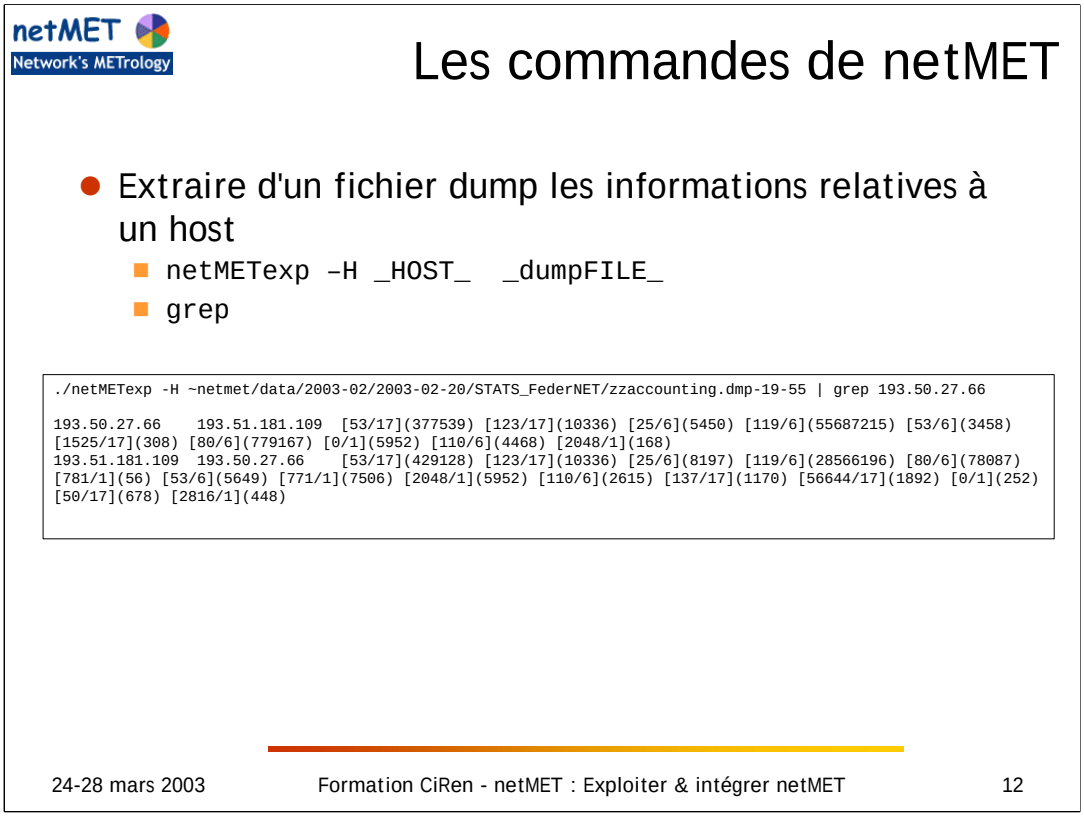
netMET Network's METrology

Plan

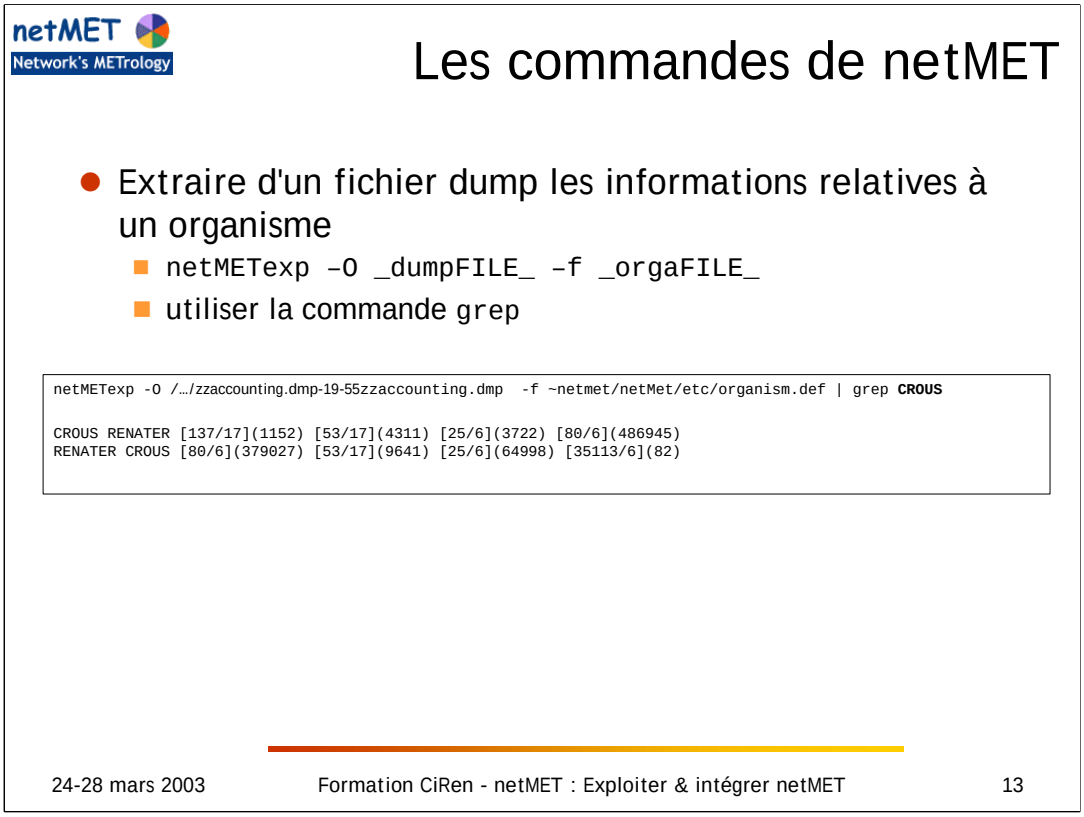
- Introduction
- Les fichiers de netMET
- Exploiter les fichiers de netMET
- Apache : authentification et permissions pour netMET
- Les fichiers de log de netMET
- Conclusion

Exploiter les fichiers de netMET

- L'exploitation de netMET se fait par le biais
  - des commandes netMET disponibles
  - de scripts Perl/cgi
  - et avec l'aide du démon 'cron'
- Ces outils sont disponibles en standard dans la distribution pour étendre les fonctionnalités de netMET en fonction de vos besoins



La commande `netMETexp` permet également de lister pour chaque machine (@IP) la quantité en octets de trafic pour chaque couple service/protocole. Encore un fois, combinée à la commande grep, vous pouvez extraire des fichiers dumps toutes les informations concernant une adresse IP particulière.



La commande `netMETexp` permet d'extraire des informations des fichiers 'dump' de netMET.

Cette commende permet notamment de lister pour chaque organisme la quantité en octets de trafic pour chaque couple service/protocole. Combinée à la commande grep, vous pouvez extraire d'un ou plusieurs fichiers toutes les informations relatives à un organisme.

Options de 'netMETexp' :

```
netMETexp -H --HOSTaccprint zzaccountingfile [...]                          [-c --
CUMULaccprint]
netMETexp -O --ORGAaccprint zzaccountingfile [...] -f --ORGAfile ORGAfile [-c --
CUMULaccprint] [-a --ALLtraffic]
netMETexp -M --MERGEfiles   zzaccountingfile [...] -f --Mfile    MERGEDfile
netMETexp -V --VALIDhost    zzaccountingfile [...] -f --ORGAfile ORGAfile
netMETexp -T --TESThost                                    -f --ORGAfile ORGAfile
netMETexp -p --PRINTdefs                                   -f --ORGAfile ORGAfile
netMETexp -i --accinfo      zzaccountingfile [...]
```

netMET Network's METrology

Les commandes de netMET

- Recherche de scans
  - `netMETscn –W` liste le nombre de ports utilisés pour les échanges entre chaque couple d'adresses IP

```
217.128.16.71   193.49.139.125  (1)
193.50.27.67    66.163.169.170  (1)
80.247.224.130  193.50.27.66    (1)
```

  - `netMETscn –H` liste pour chaque couple service/protocole le nombre d'échanges entre deux adresses IP

```
64.15.229.113   194.214.119.0   [80/6](1)
129.194.4.32    193.54.29.0     [53/17](1)
```

24-28 mars 2003 Formation CiRen - netMET : Exploiter & intégrer netMET 14

Utilisation de netMETscn:

```
netMETscn -H --Hscans zzaccountingfile [...]
netMETscn -W --Wscans zzaccountingfile [...]
netMETscn -c --ip2class
```

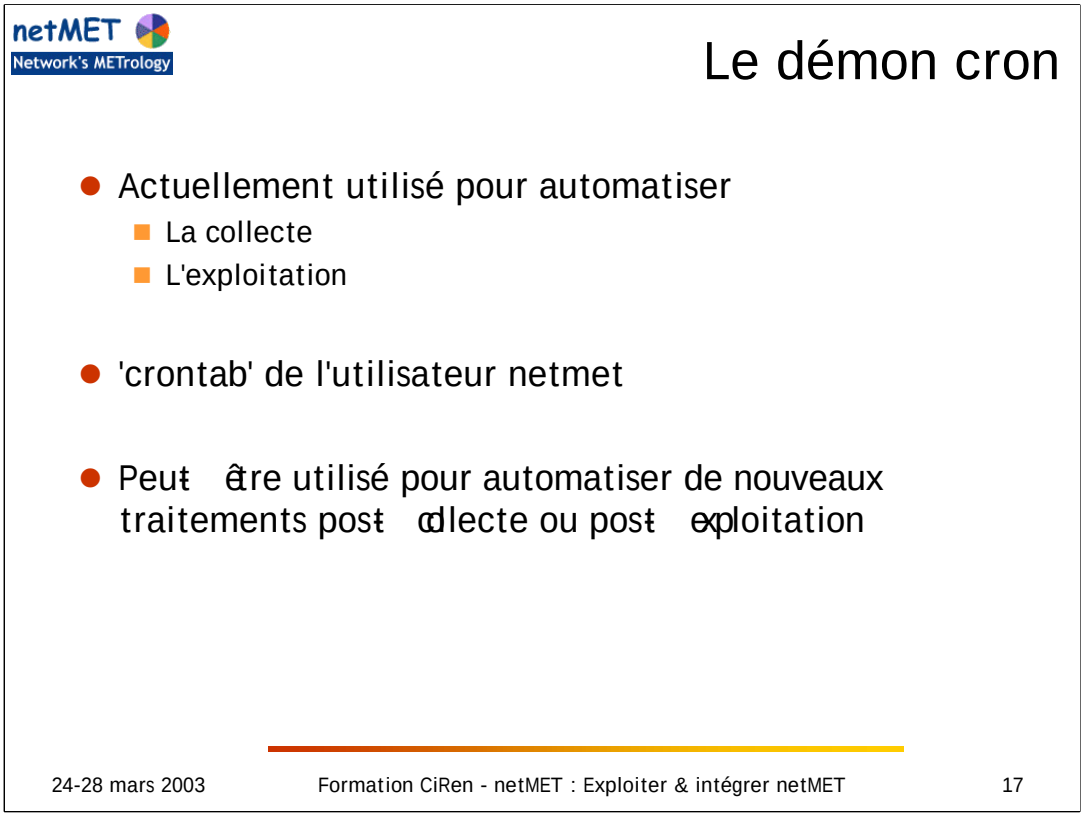
Les commandes de netMET

- Afficher en directe les flows reçus :
  - `netMETcll –s -p`

netMET Network's METrology

Bibliothèque Perl

- Une bibliothèque Perl (`netMETtk.pm`) a été développée de façon à regrouper les fonctions les plus couramment utilisées dans l'exploitation
- Cette bibliothèque peut être utilisée pour développer de nouveaux scripts
- Pour en comprendre son utilisation : regardez l'existant !



Fichier de logs d'activation des *cron* sous /var/log/cron

pour consulter la *crontab* active, utiliser la commande
`crontab -l` ou `crontab -u user -l`

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.
Remarque: 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

Plan

- Introduction
- Les fichiers de netMET
- Exploiter les fichiers de netMET
- Apache : Authentification et permissions pour netMET
- Les fichiers de log de netMET
- Conclusion

netMET Network's METrology

Apache

- Authentification apache pour
  - un accès login/passwd
  - accès par user/organisme
- `~netmet/html/` utilise un espace de nommage complet et cohérent
  - identification du type d'information (STATS, TOP_N, ...)
  - identification de l'organisme concerné
- `.htaccess` non utilisable car arborescence dynamique

netMET Network's METrology

Apache

- Solution proposée par Alexandre Simon et disponible dans les archives de la liste netMET
- Solution basée sur
  - le fichier de configuration générale d'apache : `/etc/httpd/conf/httpd.conf`
  - les fichiers d'authentification d'apache :
    - `~netmet/netMet/etc/apache.passwd`
    - `~netmet/netMet/etc/apache.group`

netMET Network's METrology

Apache

- La configuration par l'exemple
- Administrateurs netMET
  - groupe "admin"
  - utilisateurs "adm1"et "adm2"
- Membres de l'organisme CHATS
  - groupe "chats"
  - utilisateurs "chat1" et "chat2"
- Membres de l'organisme CHIENS
  - groupe "chiens"
  - utilisateurs " chien1" et " chien2"

24-28 mars 2003 Formation CiRen - netMET : Exploiter & intégrer netMET 21

Les organismes CHATS et CHIENS sont des organismes définis dans `~netmet/netMet/etc/organism.def`

Chaque utilisateur ne doit avoir accès qu'aux informations concernant sont organisme
Les administrateurs ont accès à tout

Apache – Authentification

- Réaliser l'authentification avec les fichiers
  - Fichier `~netmet/netMet/etc/apache.passwd`

```
adm1:passwdcripté
adm2:passwdcripté
chat1:passwdcripté
chat2:passwdcripté
chien1:passwdcripté
chien2:passwdcripté
```

  - Fichier `~netmet/netMet/etc/apache.group`

```
netmet: adm1 adm2 chat1 chat2 chien1 chien2
admin: adm1 adm2
chats: chat1 chat2
chiens: chien1 chien2
```

24-28 mars 2003 Formation CiRen - netMET : Exploiter & intégrer netMET 22

Les fichiers `~netmet/netMet/etc/apache.passwd` et `~netmet/netMet/etc/apache.group` doivent être créés au regard des groupes de personnes par organisme

Utilisation de htpasswd

netMET Network's METrology

Apache - Permissions

- Modifier le fichier `/etc/httpd/conf/httpd.conf`
  - Créer un 'VirtualHost' pour votre serveur netMET
  - utiliser les clauses 'LocationMatch' pour définir les permissions

```
<LocationMatch "/.*CHATS.*">
AuthUserFile /home/netmet/netMet/etc/apache.passwd
AuthGroupFile /home/netmet/netMet/etc/apache.group
AuthName "netMET's access"
AuthType Basic
require group admin chats
satisfy any
order deny,allow
allow from lepcquiadroitatout.domain.fr
deny from all
</LocationMatch>
```

Fichier /etc/httpd/conf/httpd.conf

```
<VirtualHost www.monserveur.domain.fr>
Options FollowSymLinks IncludesNOEXEC ExecCGI Indexes
User netmet
Group users
DocumentRoot /home/netmet/html
ServerName www.monserveur.domain.fr
ServerAdmin Moi@domain.fr
ErrorLog /var/log/httpd/netmet.error
TransferLog /var/log/httpd/netmet.access

<LocationMatch "/.*">
AuthUserFile /home/netmet/netMet/etc/apache.passwd
AuthUserFile /home/netmet/netMet/etc/apache.group
AuthName "netMET's access"
AuthType Basic
require group admin netmet
satisfy any
order deny,allow
allow from lepcquiadroitatout.domain.fr
deny from all
</LocationMatch>

<LocationMatch "/.*\.cgi$">
AuthUserFile /home/netmet/netMet/etc/apache.passwd
AuthUserFile /home/netmet/netMet/etc/apache.group
AuthName "netMET's access"
AuthType Basic
require group admin
satisfy all
order deny,allow
allow from lepcquiadroitatout.domain.fr
deny from all
</LocationMatch>

<LocationMatch "/.*CHATS.*">
AuthUserFile /home/netmet/netMet/etc/apache.passwd
AuthUserFile /home/netmet/netMet/etc/apache.group
AuthName "netMET's access"
AuthType Basic
require group admin chats
satisfy any
order deny,allow
allow from lepcquiadroitatout.domain.fr
deny from all
</LocationMatch>

<LocationMatch "/.*CHIENS.*">
AuthUserFile /home/netmet/netMet/etc/apache.passwd
AuthUserFile /home/netmet/netMet/etc/apache.group
AuthName "netMET's access"
AuthType Basic
require group admin chiens
satisfy any
order deny,allow
allow from lepcquiadroitatout.domain.fr
deny from all
</LocationMatch>

</VirtualHost>
```

netMET Network's METrology

Plan

- Introduction
- Les fichiers de netMET
- Exploiter les fichiers de netMET
- Apache : Authentification et permissions pour netMET
- Les fichiers de log de netMET
- Conclusion

netMET Network's METrology

Les fichiers de log de netMET

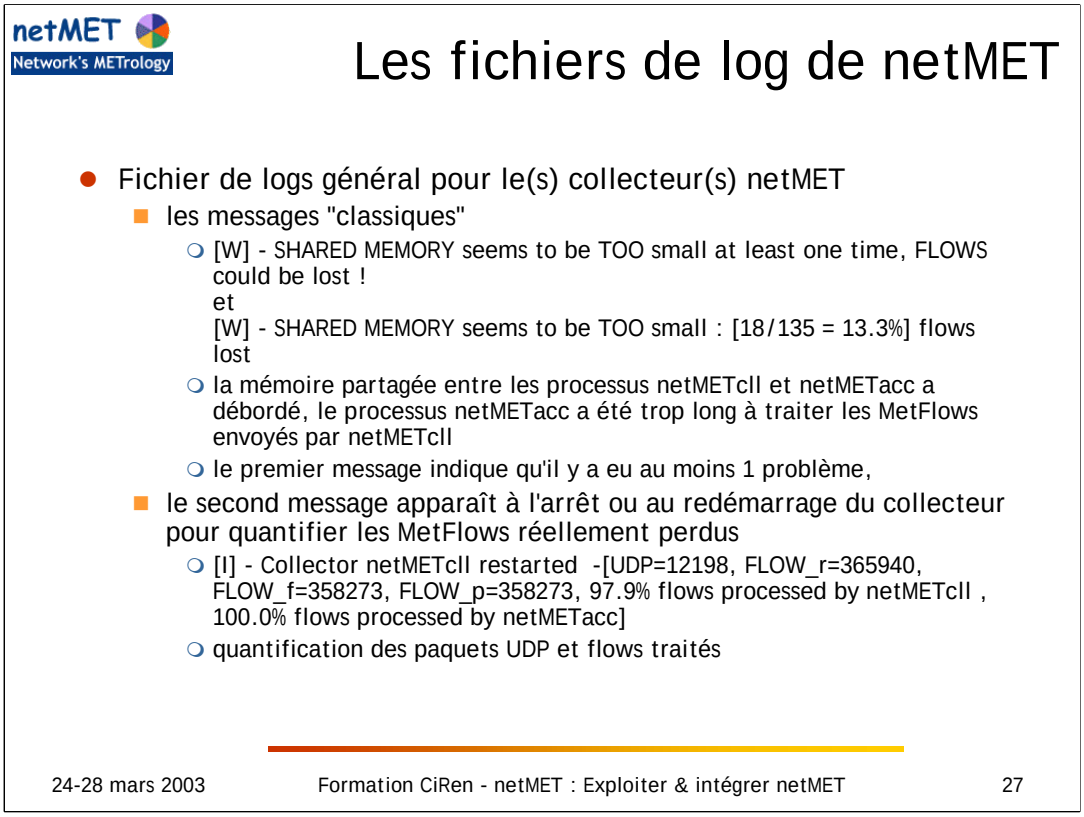
- Fichier de logs général pour le(s) collecteur(s) netMET
- sous `/var/log/netmet`
  - format à la "*cflowd*" : 3 types de messages
  - [I] : Information
  - [W] : Warning, avertissement non critique
  - [E] : Error, erreur critique… abandon du programme
  - les messages "classiques"
    - [E] - initKNOWNprot_serv/getprotobyname() -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**

24-28 mars 2003 Formation CiRen - netMET : Exploiter & intégrer netMET 26

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.



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

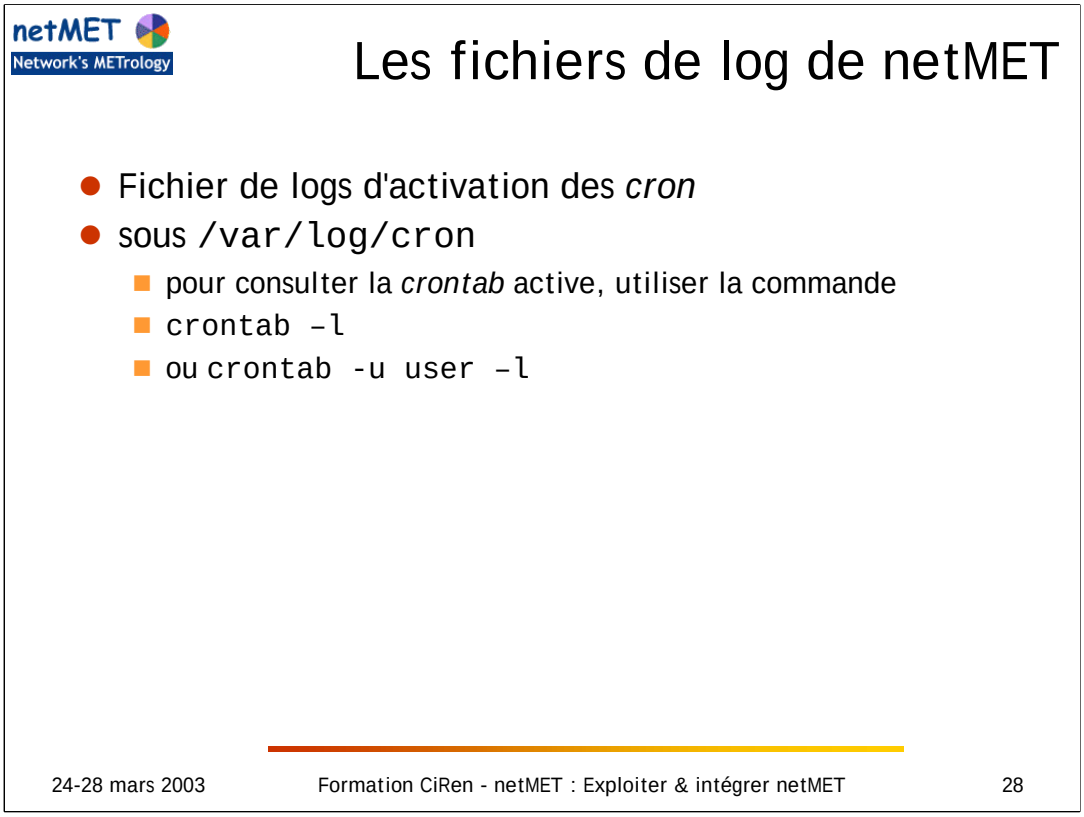
Le premier message apparaît lors du fonctionnement du collecteur : il détecte qu'un débordement a eu lieu, mais ce n'est pas une erreur JUSTE UN WARNING qui stipule que des flows pourront être perdus. Le second message apparaît à l'arrêt ou au redémarrage du collecteur pour quantifier exactement les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



Fichier de logs d'activation des *cron* sous /var/log/cron

pour consulter la *crontab* active, utiliser la commande
`crontab –l` ou `crontab -u user –l`

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.
Remarque: 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 log de netMET

- 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*

24-28 mars 2003 Formation CiRen - netMET : Exploiter & intégrer netMET 29

Fichier de logs du serveur web *apache*

sous /var/log/httpd/* mais plus particulièrement

•/var/log/httpd/netmet.access

•/var/log/httpd/netmet.error

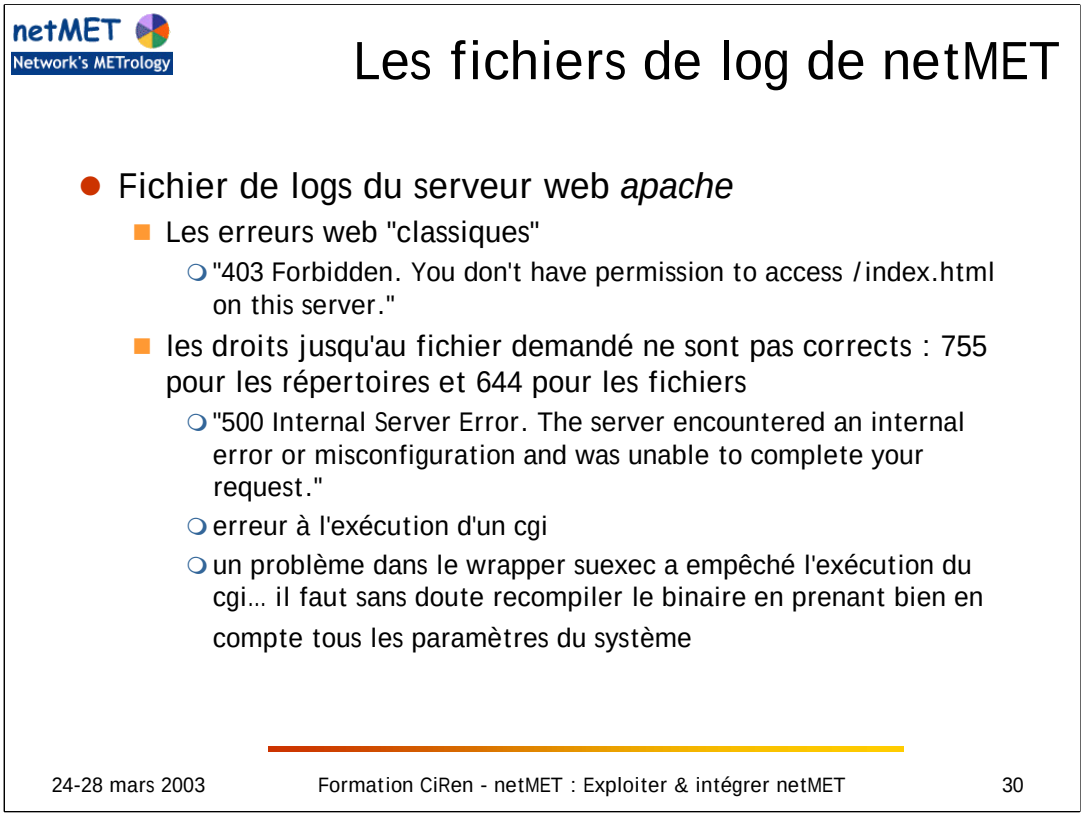
•/var/log/httpd/suexec_log
!!! Attention !!! le nom suexec_log dépend de la compilation du binaire suexec (on peut aussi avoir cgi.log)

Pour l'administration/exploitation d'*apache*, se reporter à :
http://www.apache.org et http://httpd.apache.org/docs-project/

à venir sur netMET : une documentation minimale pour démarrer avec *apache*

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



Fichier de logs du serveur web *apache*

Les erreurs web "classiques"

- "403 Forbidden. You don't have permission to access /index.html on this server."
  → les droits jusqu'au fichier demandé ne sont pas corrects : 755 pour les répertoires et 644 pour les fichiers
- "500 Internal Server Error. The server encountered an internal error or misconfiguration and was unable to complete your request."
  → erreur à l'exécution d'un cgi. Un problème dans le wrapper suexec a empêché l'exécution du cgi… il faut sans doute recompiler le binaire en prenant bien en compte tous les paramètres du système

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).

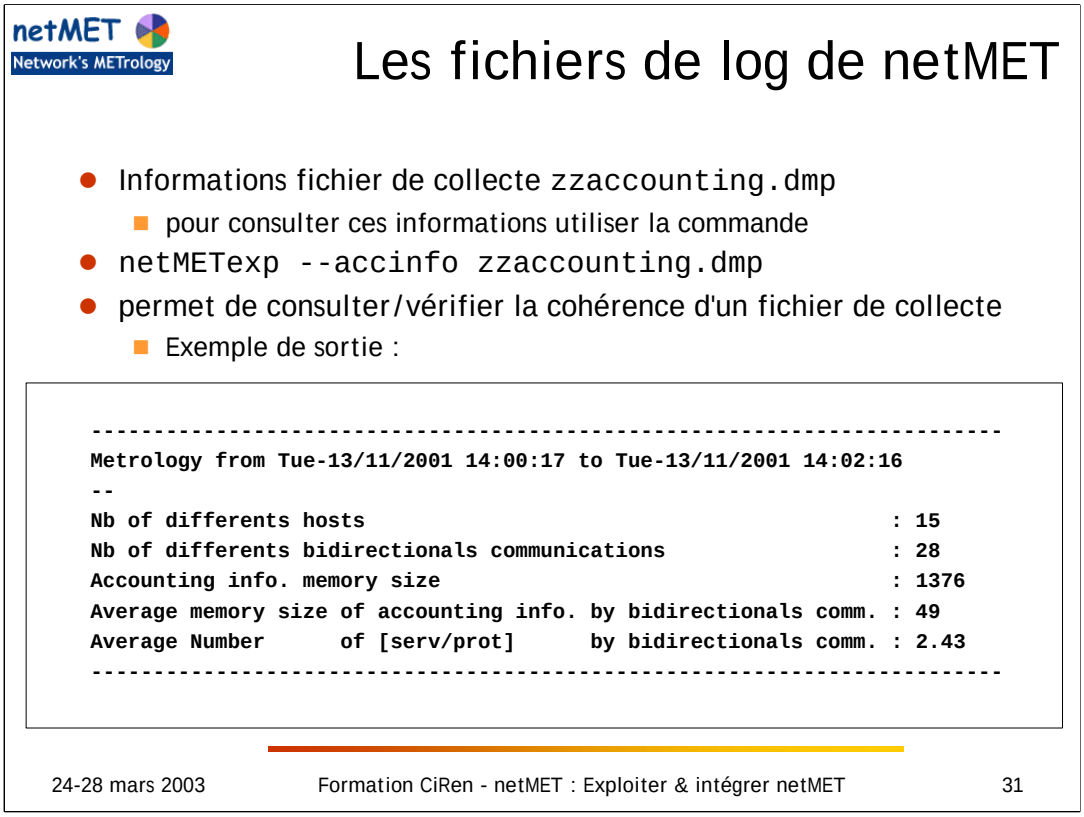
Le wrapper suexec permet au serveur web *apache*, qui par défaut fonctionne en user httpd, apache ou nobody, d'endosser les droits d'un autre user (ici le user netmet). C'est un mécanisme équivalent au su sur Unix. Seulement ici le suexec effectue un certain nombre de vérifications avant de permettre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



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
---------------------------------------------------------------------
```

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

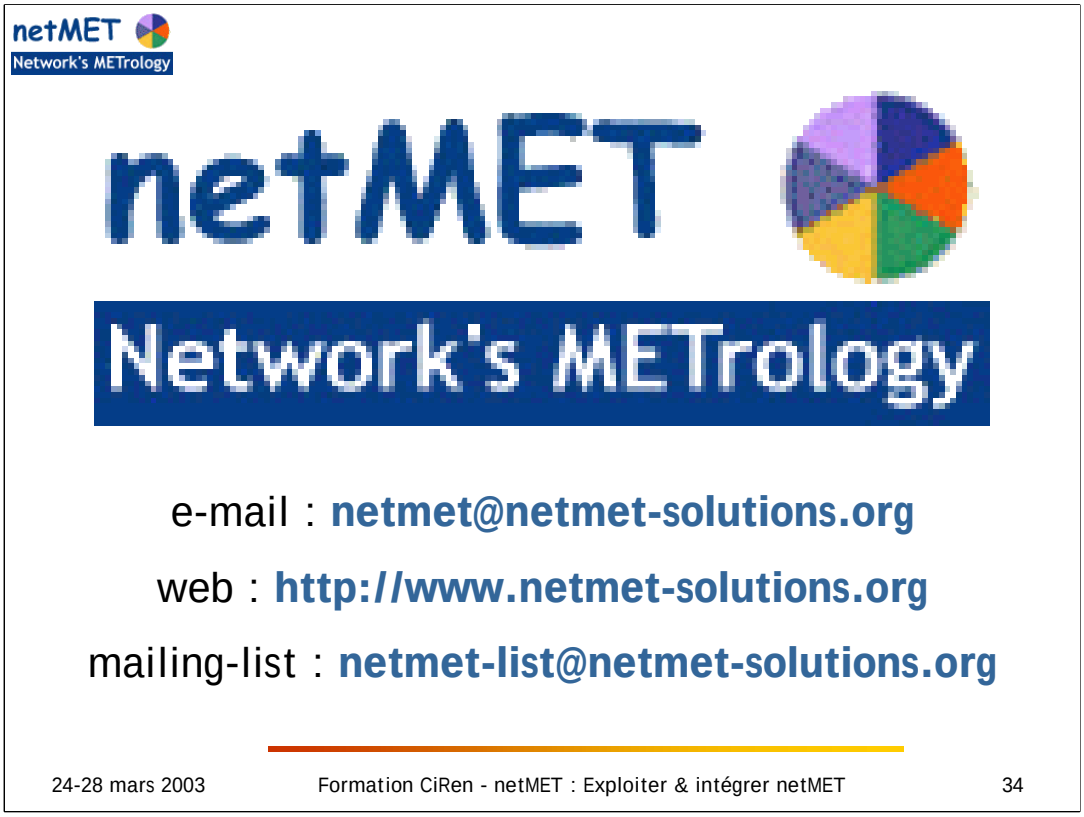
Plan

- Introduction
- Les fichiers de netMET
- Exploiter les fichiers de netMET
- Apache : Authentification et permissions pour netMET
- Les fichiers de log de netMET
- Conclusion

netMET Network's METrology

Conclusion

- netMET est une solution 'ouverte'
  - elle peut-être utilisée telle quel
  - elle peut-être étendue pour s'ajuster à vos besoins
- netMET fournit en standard des outils de bas niveau pour exploiter les fichiers de collecte
- L'accès aux informations peut être sécurisée via une utilisation adaptée du serveur HTTP Apache
- netMET est une solution qui est amenée à évoluer avec le temps


netMET
Network's METrology
netMET
Network's METrology
e-mail : netmet@netmet-solutions.org
web : http://www.netmet-solutions.org
mailing-list : netmet-list@netmet-solutions.org
24-28 mars 2003
Formation CiRen - netMET : Exploiter & intégrer netMET
34