Les prérequis *netMET*

1 Introduction

Cette documentation doit permettre de répondre aux questions suivantes : "je veux mettre en place netMET"

- quel type et quelles caractéristiques matérielles de machine faut-il ?
- avec quel système d'exploitation netMET fonctionne-t-il ?
- faut-il des services particuliers sur la machine ?
- faut-il des packages logiciels particuliers et si oui, avec quelles versions ?

2 Caractéristiques matérielles d'un serveur netMET

2.1 Généralités

Pour dimensionner un serveur netMET, il faut prendre en compte essentiellement 3 paramètres:

- la puissance CPU
- la mémoire centrale
- l'espace disque

Ces paramètres sont à dimensionner en fonction :

- de la taille du(es) lien(s) mesuré(s)
- du nombre de machines sur le réseau mesuré
- machines effectives (réelles)
- machines potentielles (somme des classes A, B et C)
- le nombre de flows à traiter
- les services souhaités
- métrologie + statistiques simples
- sécurité

Alors... que choisir ???

En fait il n'y a pas de recette miracle, on ne peut pas donner de références de puissance CPU ou taille de mémoire en fonction des paramètres cités ci-dessus. Et réalité, il n'y a aujourd'hui que des expériences acquises et les points de répères de chacun.

Etudions 2 exemples.

2.2 Exemples

Machine pour métrologie et statistiques simples :
Cette configuration dépend peu de la "taille" du réseau car les flows sont agrégés par le collecteur (metro et stats). Il faut donc une machine moyenne :

- PII monopro 200MHz à PIII monopro 500MHz
- 128 à 512 Mo de RAM
- 8Go à 18Go de disque

Machine pour métrologie et statistiques simples et sécurité :
Cette configuration dépend énormément de la "taille" du réseau mesuré car les flows ne sont pas agrégés par le collecteur (secure10m et secure24h). Il faut donc une machine performante :

- PIII monopro 700MHz à PIII bi-pro 1GHz
- 512Mo à 1Go de RAM
- 10Go à +++Go de disque

D'une manière générale, nous pouvons faire quelques remarques :

- les bi-processeurs sont vraiment adaptés à netMET (processus concurrents et démarrage des cron à intervalles réguliers)
- la mémoire centrale est vraiment très importante car toute la collecte se passe en mémoire (en particulier pour les processus sur 24h)
- la disponibilité d'espace disque implique directement la disponibilité d'archives sur de longues périodes
- la recompilation du noyau Linux est également un point important car cela entraine des performances accrues et une meilleur stabilité du serveur.

Pour l'évaluation de l'espace disque, voici quelques chiffres (en moyenne) des tailles de fichiers générés par les différents collecteurs et scripts d'exploitation. Ces chiffres sont tirés de notre serveur de production, qui mesure le réseau régional Lothaire dont voici les caractéristiques (novembre 2001):

- interconnexion Lothaire-Renater = 62Mb/s
- entre 15 000 et 20 000 machines effectives (pour 125 000 potentielles)
- entre 30 et 35 millions de flows par jour

Occupation de l'espace disque :

- html (.html et images) = 1 - 1.5 Mo par période (i.e. une période = journée, semaine ou mois)
- collecteur metro
- journée = 6.5 Mo
- semaine = 45 Mo
- mois = 200 Mo
- stats journée = 31 Mo
- semaine = 220 Mo
- mois = 950 Mo
- secure24h
- journée = 50 - 60 Mo
- secure10m
- journée = 100 - 120 Mo

2.3 Conclusion :

Avec 18Go pour les services "metro" et "stats" --> archives sur plus d'1 an
Avec 2.5Go pour les services "secure24h" et "secure10m" --> archives sur 15 jours

Aujourd'hui, le dimensionnement d'un serveur de production et les conseils associés se font plus par expérience, j'ai dans l'idée de :

- faire une enquête auprès des utilisateurs actuels pour connaître leurs configurations (réseau : routeur, nb de flow, machine Linux : version, CPU, mémoire, services activés, ...)
- de publier ces infos. sur le web de netMET
- et permettre ainsi à chacun de voir selon son contexte si sa machine de production est bien dimensionnée

3 Système Linux

La distribution netMET n'est disponible aujourd'hui que pour Linux (compilation des binaires). netMET n'est théoriquement lié à aucune distribution Linux particulière mais les distributions Redhat et Mandrake ont largement été validées et sont de ce fait préconisées pour l'installation. La distribution Debian est en cours de validation. La distribution netMET, une fois installée et configurée, demande peu de maintenance. netMET est d'ailleurs aujourd'hui reconnu pour être facilement installable et très cohérent en exploitation grâce à son déploiement (cohérence des noms de scripts, activation des crons, reprise sur fichier après arrêt, ressources et fichiers de configurations bien localisés) et à sa création d'arborescences hiérarchisées.

Pour une première mise en oeuvre, nous conseillons donc d'utiliser une distribution Linux :

RedHat ou Mandrake en version >= 7.2
Les versions du noyau Linux 2.2 et 2.4 ne posent à priori pas de problème particulier.

Lors de l'installation de ce serveur, nous conseillons :

- d'effectuer l'installation en mode expert : pour avoir le plus de choix possibles
- de partitionner soi-même le(s) disque(s) dur(s)
- de prendre un modèle "machine de type développement" : cela pause moins de problèmes pour les bibliothèques, langage perl, ...
- de choisir manuellement les RPM à installer : choisir et minimiser les packages à installer
- et, si possible, une fois la machine installée de recompiler le noyau pour retirer toutes les options multimédia (netMET ne cause pas encore dans le biniou :-)) et limiter les modules chargés lors de l'exécution du noyau :
    - retirer tous les modules multimédia et autres qui sont inutiles
    - compiler les drivers importants (carte réseau, contrôleur HD, carte SCSI, ...) en dur dans le noyau (pas en module)
- de limiter le nombre de comptes sur ce serveur : 2 suffisent
    - user root
    - user netmet
- de sécuriser au maximum la machine :
- fermer tous les services inutilisés dans /etc/inetd.conf
- protéger le serveur au niveau accès réseau (avec ACL ???) : seules certaines machines peuvent accéder au serveur (et pas tout l'Internet!!! merci!!!)

Pour le dimensionnement des partitions, on pourra se baser sur l'exemple suivant :

Partition	Taille
/	100-200 Mo
/var	200-300 Mo
/tmp	100-200 Mo
/usr	1.5-2.5 Go
/home	100-200 Go
/home/netmet	Le max dispo !

Pour le compte netmet, il est possible de décliner les partitions plus finement :

Partition	Commentaire	Taille
/home/netmet	distribution netMET (scripts, conf, ...).	>50 Mo
/home/netmet/htm	toutes les pages HTML et images publiées	1 mois = 50-100 Mo
/home/netmet/data	les fichiers de collecte pour métrologie générale et statistiques Renater	ça dépend !
/home/netmet/secure	tous les fichiers de collecte pour la sécurité	ça dépend !. Mais netMET nettoie périodiquement et automatiquement ces répertoires de sécurité

4 Les services requis

4.1 Obligatoires

Les services directement liés à netMET sont :

- le serveur web Apache (http://www.apache.org) : démon httpd. La version 1.3 fonctionne bien. La dernière version 2.0 a été testée sur un nombre restreint de sites et pose pas de problème particulier
  - support des CGI perl (exécution de scripts dans les formulaires HTML)
  - support du wrapper suexec pour l'endossement des droits d'exécution (sorte de *su* pour apache)
- le logueur de message type syslog : démon syslogd. Pas de version particulière. En standard sur tous les systèmes. Utilisé pour les logs des collecteurs
- un démon d'envoi de mail : démon sendmail, postfix, ... Pas de version particulière. Utilisé pour l'envoi des messages d'erreurs ou warning dans les cron
- le système de démarrage de commandes synchrones : démon cron. Pas de version particulière. En standard sur tous les systèmes. Utilisé pour le dump des collecteurs et le démarrage des scripts d'exploitation à intervalles réguliers

4.2 Optionels

Certains autres services sont optionnels, mais apportent un plus pour l'administration du serveur et pour netMET :

- services de connexion à distance : démons telnetd et ftp. Les versions en standard sur les distributions Linux fonctionnent bien (à surveiller tout de même les vulnérabilités liées à ces services). Pour l'activation de ces services se reporter au fichier de conf. : /etc/inetd.conf (ou /etc/xinetd.conf …)
- services de synchronisation d'horloge : démons ntp et xntp. Pas de version particulière. Utilisé pour la mise à jour automatique de l'horloge système du serveur (intéressant pour être sûr que le serveur est toujours bien à l'heure)
- cache local pour requêtes DNS : démon bind. Pas de version particulière (à surveiller tout de même les vulnérabilités liées à ce service). Utilisé pour limiter les requêtes DNS sortantes du serveur (les adresses IP à résoudre sont presque toujours les mêmes... autant avoir un système de cache qui accèlere ces résolutions). Serveur DNS à configurer en cache ou en serveur DNS secondaire (je préfère la solution cache qui est moins lourde)

A propos de l'accès local ou distant, certaines distributions Linux propose un accès X11 en local ou XDMCP distant. NOUS DECONSEILLONS FORTEMENT CETTE CONFIGURATION car les serveurs X11 ou XDMCP sont assez consommateurs de ressources, il est donc préférable de travailler en mode console ou telnet simple pour ne pas surcharger le serveur avec des process inutiles.

5 Les logiciels, bibliothèques et RPM requis

5.1 Perl

Le langage perl est utilisé dans tous les scripts d'exploitation. Il est donc obligatoire pour que netMET puisse fonctionner. Référence : http://www.perl.org

Les versions 5.005_03, 5.6 et 5.8 fonctionnent bien.

Beaucoup de distribution Linux propose perl en standard. Pour netMET il faut que certaines bibliothèques soient installées. Les bibliothèques perl se trouvent sur le site du CPAN : http://www.cpan.org/modules/ ou en RPM correspondants sur la distribution Linux.

5.2 RRDtool

RRDtool est utilisé par l'exploitation depuis la version 2.0. Il est donc nécessaire d'installer RRD dans une version 1.0.38 ou supérieure.

Référence: http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/

Lors de l'installation de RRDtool, pensez à installer le module perl RRD associé

5.3 Libraries

Certaines bibliothèques et RPM systèmes (RPM correspondants sur la distribution Linux utilisée, ou http://rpmfind.net/) sont requis pour que netMET s'installe et fonctionne correctement. A ce niveau, nous ne pouvons que conseiller un niveau de version minimum (ou maximum dans certains cas) des bibliothèques à installer :

Bibliothèque	Version Conseillée	
freetype	>=	1.3.1-8
freetype-devel	>=	1.3.1-8
gd	>=	1.8.1-4
gd-devel	>=	1.8.1-4
gd-utils	>=	1.8.1-4
libjpeg	>=	6b-15
libjpeg-devel	>=	6b-15
libpng	>=	1.0.8-2
libpng-devel	>=	1.0.8-2
ucd-snmp *	==	4.1.1-4 4.1.2-8 (RedHat 7.2)
ucd-snmp-devel *	==	4.1.1-4 4.1.2-8 (RedHat 7.2)
ucd-snmp-utils *	==	4.1.1-4 4.1.2-8 (RedHat 7.2)
xpm	>=	3.4k-10
xpm-devel	>=	3.4k-10
zlib	>=	1.1.3-11
zlib-devel	>=	1.1.3-11

(*)La version de ucd-snmp est la seule qu'il faut à priori respecter pour que netMET fonctionne bien. En effet, le collecteur utilise cette bibliothèque qui dans les nouvelles versions pose certains problèmes. L'installation de cette version est IMPERATIVE.
Vous pouvez trouver la version 4.1.2-8 de ucd-snmp pour RedHat 7.2 à l'adresse suivante : http://fr2.rpmfind.net/linux/RPM/redhat/7.0/i386/ucd-snmp-4.1.2-8.i386.html

5.4 Modules Perl

Un certain nombre de modules perl sont nécessaires pour que netMET fonctionne.

Certains de ces modules (les moins courants) sont livrés avec la distribution de netMET. Ils sont situés dans le répertoire *netMet-distribution-x.y/install/PERL.*

Modules perl fournis:

- File-Temp-0.12
- GD-1.41
- GDGraph-1.39
- GDGraph3d-0.56
- GDTextUtil-0.85

Liste des modules perl requis :

- POSIX
- Socket
- Time::Local
- HTTP::Date
- File::Path
- File::Temp
- GD
- GD::Graph
- RRDs (à installer lors de l'installation de RRDtool)

6 Autres points... :-)

6.1 Où connecter le serveur?

Pour des raisons évidentes de performances et pour limiter les pertes de datagrammes UDP NetFlow entre le routeur et la machine de collecte, il est conseillé de mettre en place la machine de collecte "au plus près du routeur". La configuration idéale étant la suivante :

- un nombre minimum de matériels réseau intermédiaires entre le routeur et la machine de collecte
- un débit de 100Mb/s Full duplex entre le routeur et la machine de collecte
- penser à ouvrir les ACL (ou équivalents) entre le routeur et la machine de collecte pour le port UDP d'exportation vers la machine de collecte

6.2 SNMP

Au démarrage d'un collecteur, celui-ci utilise le protocole SNMP pour récupérer des informations de configuration sur le routeur. Il faut donc autoriser la machine de collecte à faire des requêtes SNMP sur le routeur et penser entre autres à :

- ouvrir les ACL (ou équivalents) en SNMP entre la machine de collecte et le routeur
- ouvrir les ACL locaux au routeur pour autoriser la machine de collecte à faire des requêtes SNMP sur ce routeur
- activer le serveur SNMP sur le routeur
- bien noter le nom de la communauté read SNMP (ce paramètre doit être connu pour configurer les collecteurs) - par défaut cette communauté a le nom "public" -

Remarque: netMET n'a besoin que de l'accès SNMP en read et PAS EN WRITE.

6.3 DNS

Le serveur netMET sur lequel fonctionnera l'exploitation -et surtout le serveur web apache- doit être déclaré dans le DNS de 2 façons :

- une entrée simple : @IP <-> ma-machine.domaine.fr
- une entrée de type CNAME : www.ma-machine.domaine.fr <-> ma-machine.domaine.fr

Cette déclaration DNS est utilisée dans la configuration d'apache, notamment pour la mise en place d'un serveur web virtuel sur le CNAME déclaré.

Documentation netMET		
par :	Alexandre SIMON Sébastien Morosi (maj)	Alexandre.Simon@ciril.fr Sebastien.Morosi@ciril.fr
crée le :	Novenbre 2001	
mise à jour le :	2003-03-18	