Administration **Unix** (Part. 2)

Thierry Vaira

Esimed

v1.0 - 17 février 2017

esimed
École supérieure d'informatique de la Méditerranée

Sommaire

esimed
École supérieure d'informatique de la Méditerranée

Sommaire

esimed
École supérieure d'informatique de la Méditerranée

Protocoles utilisés

La plupart des systèmes d'exploitation utilisent actuellement le protocoles "**TCP/IP**" basés sur des réseaux de type **Ethernet** (du moins pour les réseaux locaux). Un protocole est un **ensemble de règles** gérant l'échange de données entre deux entités. Les protocoles interviennent à plusieurs niveaux dans une communication (cf. modèle à couches).

- Protocoles de niveau **réseau** : IP (*Internet Protocole*), ARP, RARP (*Adresse Resolution Protocol*, *Reverser ARP*), ICMP (*Internet Control Message Protocol*), ...
- Protocoles de niveau **transport** : TCP (*Transmission Control Protocol*) et UDP (*User Datagram Protocol*)
- Protocoles de niveau **application** : HTTP (*HyperText Transfert Protocol*), FTP, TFTP (*File Transfert Protocol*, *Trivial FTP*), SMTP (*Simple Mail Transfert Protocol*), NFS (Network File System), ...

esimed
École supérieure d'informatique de la Méditerranée

Les interfaces réseaux

Sous Linux, les périphériques de type cartes réseau sont accessibles par l'intermédiaire d'un fichier de périphérique nommé `/dev/ethX` où `X` est le numéro de la carte réseau, attribué par le système en fonction de l'ordre de détection de la carte.
Quelques commandes utiles :

- la commande `dmesg` qui affiche les messages systèmes depuis le démarrage du système
- la commande `lspci` qui liste les périphériques PCI (ne fonctionne donc qu'avec les cartes réseau PCI)
- la commande `ifconfig` qui configure et affiche les interfaces réseaux
- contrôler le service réseau : `[service] (start|stop|restart) networking` pour **Upstart** ou `systemctl (start|stop|restart) networking` pour **systemd**

Notions de bases

Les paramètres réseaux les plus souvent modifiés sont :

- Les **adresses IP et masques de sous réseau** des cartes
- L'**adresse de la passerelle par défaut**
- Le **nom d'hôte** de la machine
- La **résolution des noms** de machines

Les commandes configuration

- La commande `ifconfig` permet de stopper ou de démarrer le fonctionnement d'une carte réseau, de voir et de changer la configuration d'une carte.
- La commande `route` permet de modifier la table de routage et donc de configurer l'adresse de la passerelle par défaut (la route par défaut pour tous les paquets non destinés au réseau local).
- La commande `hostname` permet de manipuler le nom d'hôte.

Les fichiers de configuration

Les paramètres de configuration du système se trouvent (dans le cas de **Debian/Ubuntu** Linux) dans le répertoire `/etc/network`.

- En ce qui concerne la configuration des cartes réseau, il y a un fichier de configuration, qui porte le nom `/etc/network/interfaces`.
- Le nom d'hôte (et le nom de domaine DNS si besoin) par défaut se trouve dans le fichier `/etc/hostname`.
- La résolution des noms de machines peut utiliser deux bases de données pour convertir des adresses IP en nom de machine ou inversement : la base locale (fichier `/etc/hosts`) et la base distribuée DNS (`/etc/resolv.conf`).

Remarque : le fichier `/etc/resolv.conf` est mis à jour par le système (notamment en configuration DHCP), il faut alors éditer les fichiers `/etc/resolvconf/resolv.conf.d/head` ou `/etc/resolvconf/resolv.conf.d/tail`.

esimed
École supérieure d'informatique de la Méditerranée

Les outils de surveillance et diagnostic

- La commande `ping` permet de vérifier la présence active d'un autre système et affiche, si celui-ci répond, le **rtt** (*round-trip time*).
- L'outil `nmap` permet de trouver les services actifs ou filtrés (par un *firewall* par exemple) d'une machine.
- La commande `tcpdump` est très utile pour déterminer les informations transitant entre deux systèmes. On peut visualiser toutes les communications, ou filtrer par nom de machine, par protocole, ... Voir aussi : `wireshark/tshark`
- La commande `netstat` permet de visualiser les informations concernant le fonctionnement du réseau. Cette commande est très utile pour résoudre les problèmes.

esimed
École supérieure d'informatique de la Méditerranée

Sommaire

syslog

Le service `syslog` gère les messages générés par les processus systèmes (qui, par définition, n'interagissent pas avec la console).

- Ces processus envoient leurs messages au démon `syslogd` qui se charge de les transmettre vers une destination au choix de l'administrateur :
  - Dans un fichier journal (ou un périphérique),
  - Sur la ou les consoles d'un ou de plusieurs utilisateurs,
  - Sur la console système,
  - Au démon `syslogd` d'une autre machine.
- Les messages sont transmis dans un format standard.
- Les journaux sont stockés dans des fichiers dans le répertoire `/var/log`.

Configuration et utilisation de syslog

- On peut configurer la destination des messages transmis par `syslogd` à l'aide du fichier `/etc/syslog.conf`.
- Sous Ubuntu Linux, si le logiciel `rsyslog` est installé le fichier est `/etc/rsyslog.d/50-default.conf`
- Les processus systèmes et les programmes utilisent directement le service `syslog` mais, il est possible de l'utiliser dans des scripts ou manuellement avec la commande `logger`.
- Si vous voulez avoir `syslog` en parallèle avec `journald`, il suffit d'installer `syslog-ng`, puis de l'activer : `systemctl enable syslog-ng.service`.

systemd

`systemd` possède son propre mécanisme de journalisation, `syslog` n'est plus requis par défaut. La commande `journalctl` (pour l'utilisateur *root*) permet d'accéder au *log*.

- Tout le log : `journalctl` (l'option `-f` pour un affichage continu comme pour `tail`)
- Par service : `journalctl -u wicd`
- Par PID : `journalctl _PID=1`
- Par exécutable : `journalctl /usr/sbin/dhcpcd`
- Par jour : `journalctl -since="today"`
- Par niveau : `journalctl -p err`

La configuration du journal de `systemd` est réalisée avec le fichier `/etc/systemd/journald.conf`.

Des outils d'audit

- L'utilitaire `who` peut fournir des informations sur les utilisateurs connectés et la commande `w` affiche les utilisateurs connectés et ce qu'ils font.
- La commande `last` peut être utilisée pour déterminer toutes les connexions/déconnexions d'un utilisateur.
- La commande `uptime` nous renseigne depuis quand le système fonctionne et la charge de celui- ci.
- La commande `vmstat` permet de suivre en temps réel l'activité de la mémoire virtuelle, des zones de swap, des processus, ...
- La commande `free` affiche la somme totale de mémoire physique et des zones de swap, ainsi que leur utilisation.
- La commande `fuser` identifie les processus qui utilisent des fichiers et la commande `lsof` liste les fichiers ouverts.
- Voir aussi : `ps`, `pstree`, `pgrep`, `top`, `df`, `du`, `netstat`, ...

esimed
École supérieure d'informatique de la Méditerranée

Sommaire

Qu'est ce que le RAID ?

- Le RAID (*Redudant Array Of Independent Disks*) permet de combiner plusieurs disques en une seule partition dans le but d'augmenter soit la performance, soit la redondance des informations, soit les deux.
- Les différentes méthodes RAID les plus courantes sont nommées par **niveau** (*level*) :
  - le *disk striping* (volume segmenté) ou RAID level 0
  - le *mirroring* (volume en miroir) ou RAID level 1
  - le *disk striping with parity* (volume segmenté avec parité) ou RAID 5
- Il existe deux sortes de RAID :
  - Le RAID matériel (les contrôleurs de disques gèrent eux-mêmes le RAID)
  - Le RAID logiciel (il existe plusieurs solutions pour Linux, dont le pilote **MD**)

esimed
École supérieure d'informatique de la Méditerranée

Principe

Le principe de base est la distribution des données sur plusieurs disques d'un même ensemble (*disk array*), les disques étant regroupés en un seul volume logique. Les données sont découpées en blocs de taille fixe (*chunks*), puis ces blocs sont distribués sur les différents disques du volume logique suivant un algorithme déterminé par le niveau RAID.

- Level 0 : est utilisé pour améliorer la **performance** en distribuant la charge de lecture/écriture de façon équitable sur tous les disques de l'ensemble.
- Level 1 : est utilisé pour améliorer la **sécurité** en augmentant la redondance, les données étant écrites en plusieurs exemplaires sur plusieurs disques en même temps.
- Level 4 : est destiné à améliorer la sécurité en utilisant un disque pour le stockage de la parité. Ce niveau est très peu utilisé.
- Level 5 : offre un maximum de sécurité avec une bonne performance. Il utilise le principe du striping du Level 0 et la technique de la parité du Level 4, sauf que la parité est répartie sur l'ensemble des disques, éliminant le problème de performance du Level 4. C'est le niveau le plus utilisé.

Configuration

- La configuration d'un ensemble RAID (pilote **MD**) se fait à l'aide de la commande `mdadm`
- Les informations concernant les ensembles RAID en cours de fonctionnement sont accessibles avec le fichier `/proc/mdstat`
- Pour que les ensembles soient activés au démarrage il faut créer un fichier de configuration `/etc/mdadm/mdadm.conf`
- Pour que l'ensemble soit monté automatiquement au démarrage, il faut ajouter une ligne au fichier `/etc/fstab`

Sommaire

Zone de swap

La zone de *swap* est utilisée lorsque la mémoire physique (RAM) est remplie. Si le système a besoin de plus de ressources mémoires et que la mémoire physique est remplie, les pages de mémoire (page = bloc de taille fixe) inactives (non utilisées depuis un certain temps) sont déplacées dans la zone de *swap*.
Quelques règles de base pour la zone de *swap* :

- Elle soit stockée dans une partition dédiée,
- La partition dédiée à la zone de *swap* soit sur un disque (voire un contrôleur) différent de la partition système et des données les plus utilisées,
- Que sa taille soit au minimum la taille de la mémoire physique.

Configuration

- Les zones de *swap* en cours d'utilisation par le système peuvent être listées avec la commande `swapon -s`
- La création d'une partition sur un disque existant ou un nouveau disque peut se faire avec les outils `parted`, `fdisk` ou autre. Pour un fichier, on utilisera la commande `dd`.
- Il faut ensuite créer les structures de la zone de swap avec la commande `mkswap` et l'activer avec `swapon`
- L'arrêt de l'utilisation de la zone de swap se fera avec la commande `swapoff`.

ramdisk

- Un *ramdisk* est une zone de mémoire utilisée comme partition.
- Une fois montée, cette partition est utilisable comme n'importe quelle partie du système de fichiers.
- Pour créer un *ramdisk*, rien de plus simple : il suffit de le monter avec la commande `mount` et l'option `-t ramfs`

Sommaire

DHCP

- DHCP (*Dynamic Host Configuration Protocol*) permet d'automatiser la configuration TCP/IP des machines du réseau, quel que soit leur système d'exploitation.
- L'utilisation de DHCP simplifie l'administration système en regroupant en un seul point la configuration de tout un réseau (adresses dynamiques, semi-statiques, masque de sous-réseaux, DNS, passerelle par défaut, ...).
- Le service DHCP peut aussi servir à renvoyer la configuration des démarrages par réseau (serveur de *boot*, fichiers de démarrage réseau, ...).
- Il est nécessaire de configurer le serveur DHCP avec une adresse IP statique.

Configuration DHCP

- Il est nécessaire d'installer le paquet `isc-dhcp-server` car seuls les paquets clients DHCP sont installés par défaut.
- Il faut éditer le fichier de configuration `/etc/dhcp/dhcpd.conf`.

```
subnet 10.0.0.0 netmask 255.255.255.0
{
  option broadcast-address 10.0.0.255; # adresse de
      diffusion
  range 10.0.0.100 10.0.0.250; # plage d'adresses dynamiques
  option domain-name-servers 10.0.0.1, 10.0.0.254; #
      serveurs DNS
}
```

DNS

- Le service DNS (*Domain Name System*) est utilisé pour associer les adresses IP aux noms complets (**FQDN**, *Fully Qualified Domain Name*) des machines (et inversement).
- Le DNS est une base de données distribuée, chaque domaine et sous domaine (appelés **zones**) étant gérés par un serveur DNS différent (un serveur peut gérer plusieurs zones). De plus, les serveurs sont organisés entre eux de façon hiérarchique.
- Une **zone** est gérée par un et un seul serveur DNS principal, et peut être répliquée sur un ou plusieurs serveurs secondaires.
- Chaque serveur DNS contient, pour chaque zone qu'il gère, les fichiers de la base de données permettant de convertir un nom de machine en adresse IP et inversement, ainsi que les noms et adresses des autres serveurs DNS de la zone et des serveurs de mail.

esimed
École supérieure d'informatique de la Méditerranée

Configuration DNS

- Le serveur de nom fourni avec Ubuntu Linux est **BIND** (*Berkeley Internet Name Domain*).
- **BIND** est composé, entre autre, du démon `/usr/sbin/named` et de la commande `/usr/sbin/rndc`.
- Il lit sa configuration dans le fichier `/etc/bind/named.conf`, et stocke ses informations dans le répertoire `/var/cache/bind/`.

```
zone "xxx.esimed" {
    type master;
    file "/etc/bind/db.esimed.xxx";
};

zone "0.168.192.in-addr-arpa" {
    type master;
    file "/etc/bind/db.esimed.xxx.rev";
};
```

Fichiers de zone I

- Les fichiers de zones contiennent les enregistrements constituant les différents noms de machines et serveurs du domaine.
- Les différents types d'enregistrements les plus courants sont :
  - **A** : *Address*, un nom de machine associé à une adresse IP.
  - **CNAME** : *Canonical NAME*, un alias sur un nom de machine.
  - **MX** : *Mail eXchange*, noms des serveurs de mails du domaine.
  - **NS** : *Name Server*, noms des serveurs DNS.
  - **SOA** : *Start Of Authority*, informations à propos de cette zone.
  - et pour la résolution inverse **PTR** : *PoinTeR*, une adresse IP associée à un nom de machine.

Fichiers de zone II

```
$TTL 86400
@   IN  SOA ns.xxx.esimed. root.xxx.esimed. (
            12345 ; Version
            21600 ; Refresh secondaires
            3600 ; Attente après demande erronee
            604800 ; TTL max dans les caches des DNS secondaires
            86400 ; TTL min dans les caches
        )
    IN  NS  ns.xxx.esimed.
    IN  MX  10 mail.xxx.esimed.

@   IN  A   192.168.0.2
ns  IN  A   192.168.0.2
mail    IN  A   192.168.0.2
server  IN  A   192.168.0.2
client  IN  A   192.168.0.3
www   IN CNAME server
```

NFS

- **NFS** (*Network File System*) est un système de partage de fichiers qui utilise les protocoles TCP/IP, RPC et XDR.
- Les termes utilisés dans NFS sont :
  - **Serveur** NFS : Désigne le système qui possède physiquement les ressources (fichiers, répertoires) et les partages sur le réseau avec d'autres systèmes.
  - **Client** NFS : Désigne un système qui monte les ressources partagées sur le réseau (option `-t nfs` de la commande `mount`). Une fois montées, les ressources apparaissent comme si elles étaient locales.

Remarque : Malgré ses défauts d'origine, NFS reste le standard pour les partages de fichiers en réseaux hétérogènes. En effet, les autres systèmes de fichiers réseaux sont soit trop liés à un type de système d'exploitation (SMB, CIFS), soit propriétaires (NCP), soit trop lourd à mettre en oeuvre pour la plupart des réseau locaux de petites tailles (Coda).

Configuration NFS

- La configuration du service NFS, côté serveur, se limite à lister les ressources partagées et les droits de montage.
- La liste des ressources partagées peut être obtenue à l'aide de la commande `showmount`.
- Le fichier `/etc/exports` contient la liste des ressources partagées, une ligne par ressource.
- L'option `root_squash` : L'utilisateur *root* local des clients (UID 0, GID 0) est considéré comme un utilisateur anonyme par le serveur.

```
/export/home 192.168.0.0/16(rw,root_squash) admin.intra.net(rw,no_root_squash)
/usr/local machin.intra.net(ro) 192.168.0.10(rw)
```

esimed
École supérieure d'informatique de la Méditerranée

Sommaire

Concepts

- Un **annuaire** est une application **client-serveur** dont le rôle est de convertir les requêtes de nommage, comme les noms de machines, les noms d'utilisateurs, répertoires personnels. . . en leur identifiant ou localisation associés.
- L'annuaire centralise l'information d'un réseau d'une entreprise : le but étant de fournir toutes les informations utiles au fonctionnement du réseau à partir d'une seule et unique source.
- Les services de ce type d'annuaire les plus souvent rencontrés sont :
  - *Active Directory* : Annuaire hiérarchisé et distribué disponible pour l'environnement *Microsoft Windows*.
  - **LDAP** (*Lightweight Directory Access Protocol*) : Annuaire hiérarchisé et protocole de consultation d'annuaires (le protocole seul peut être utilisé avec d'autres annuaires comme *Active Directory*, *Novell* ou des bases de données).
- Pour chaque type d'information, on peut fixer l'ordre de recherche de l'information à l'aide du fichier `/etc/nsswitch.conf` sous Linux.

LDAP

- LDAP (*Lightweight Directory Access Protocol*) est un **système d'annuaire** basé sur **X500**.
- LDAP est aussi un **protocole** qui permet d'interroger des systèmes d'annuaires **X500** comme par exemple *Microsoft Active Directory*.
- Le standard **X500** définit comment un annuaire doit être organisé. Les annuaires **X500** sont organisés sous forme d'**arbre avec une racine et différents niveaux** pour chaque catégorie d'informations (des **branches** et des feuilles **feuilles**).

esimed
École supérieure d'informatique de la Méditerranée

Un annuaire simple

- Une **racine** portant le nom du domaine de la société, `mondomaine.com` : `dn: dc=mondomaine, dc=com`
- Des **branches** (**ou** : *Organizational Unit*) pour stocker :
  - les informations des utilisateurs, *People* :
    `dn: ou=People, dc=mondomaine, dc=com`
  - les informations des groupes, *Group* :
    `dn: ou=Group, dc=mondomaine, dc=com`
- Une **feuille** (**cn** : *Common Name*) pour un utilisateur LDAP qui fait office d'administreur, *admin* :
  `dn: cn=admin, dc=mondomaine, dc=com`

esimed
École supérieure d'informatique de la Méditerranée

Outils LDAP

- Il est nécessaire d'installer le paquet `ldap-utils` pour bénéficier des commandes de gestion LDAP : `ldapadd`, `ldapsearch`, ...
- La commande `slapcat` qui permet de visualiser l'annuaire LDAP et de générer des fichiers LDIF (*LDAP Data Interchange Format*).
- Le paquet `migrationtools` qui forunit des scripts PERL de transformation de fichiers de données en (`/etc/passwd`, `/etc/group`, ...) en fichiers LDIF.
- Il existe aussi un paquet nommé `ldapscripts` qui contient des outils pratiques pour la gestion de l'annuaire (`ldapadduser`, `ldapdeleteuser`, ...).

➠ Fichier de configuration : `/etc/ldap/ldap.conf`

esimed
École supérieure d'informatique de la Méditerranée

L'automonteur

L'automonteur est un système qui permet de monter les ressources locales (disques, CDROM, clés USB, ...) ou distantes (partages NFS) automatiquement et de façon transparente à l'utilisateur.

- Le système de fichiers `autofs` a pour fonction d'intercepter les requêtes d'accès aux répertoires (et à leur contenu) gérés par l'automonteur.
- A chaque accès, `autofs` envoie au démon `automount` une requête qui va monter le répertoire.
- L'automonteur s'utilise souvent avec LDAP, notamment pour les répertoires des utilisateurs, ce qui permet de centraliser les tables de montages pour simplifier l'administration.
- L'utilisation de l'automonteur avec LDAP implique de placer les tables de l'automonteur dans la base de données LDAP sur le serveur.

esimed
École supérieure d'informatique de la Méditerranée

Côté clients

Trois fichiers sont à configurer :

- `/etc/default/autofs`
- `/etc/autofs_ldap_auth.conf`
- `/etc/nsswitch.conf`

Sommaire

Samba

- Le logiciel **Samba** est utilisé pour le partage de fichiers et d'imprimantes à l'aide des protocoles **SMB** et **CIFS**.
- Ces protocoles étant ceux utilisés pour les systèmes d'exploitation *Microsoft*, l'installation de Samba sur une machine équipée de Linux permet :
  - d'intégrer celle-ci dans le "réseau Microsoft" de l'entreprise
  - de prendre la place d'un serveur *Microsoft Windows*
- On configure le service Samba à l'aide du fichier `/etc/samba/smb.conf`.

Configuration et commandes

- Le fichier `/etc/samba/smb.conf` est composé de deux parties :
  - Un partie globale, qui permet de configurer le fonctionnement du service.
  - Une partie partages, où sont listés les partages de répertoires et d'imprimantes et leurs paramètres.
- Quelques commandes : `smbclient`, `smbmount`, `smbstatus`, ...
- Ajouter manuellement des utilisateurs Samba : `smbpasswd`
- Vérifier la configuration de Samba en utilisant la commande : `testparm -s`