

Formation DevOps

Penser à bien valider sa présence sur : <http://quest.ajc-formation.fr:8000> (matin et après-midi).

Code wifi : 7894561230

Algo et Objet

Prof. : ASSOUS Steeve

Code : 3404

Conception d'algo :

ANALYSE -> CONCEPTION -> PROGRAMMATION -> TEST

En POO :

Objet contient 3 concepts fondamentaux :

- **polymorphisme**
- **encapsulation**
- **héritage**

Objets de bases :

- données en entrée et résultats intermédiaires
- règle opératoire
- ici on parle du nom commun objet (différent de POO)

Un objet contient :

- un **identificateur** (nom)
- un **type** (entier, numérique, caractère ...)
- une **valeur**

Types simples

Ce sont les **caractères**, **textes** (ou **chaînes de caractères**), **logiques**, **bouléens**, **indicateurs** et les **nombres**.

Types composés

Ce sont les **fiichiers** et les **tableaux**.

Actions de base

Elles sont :

- affectation : attribuer une valeur à un objet
- affectation particulière : initialisation, incrémentation/décrémentation

Ex :

```
// Debut
```

```
// DECLARATION  
variable : type
```

```
// INITIALISATION  
variable = 0
```

```
// CORPS DU PROGRAMMES  
instruction 1  
instruction 2  
...
```

Autres actions de base

- lecture : à partir du clavier / fichier
- écriture : écran / sur un support externe
- concaténer : associer variable avec texte

Choix ou Structures Conditionnelles

On a le choix entre plusieurs actions :

- structures conditionnelles pures

ex: SI condition

ALORS

action 1

FIN SI

- structures conditionnelles alternatives

ex: SI condition

ALORS

action 1

SINON

action 2

FIN SI

- structures conditionnelles alternatives imbriquées

ex: SI condition

ALORS

action 1

SINON

SI cond

ALORS

action 2

SINON

action 3

FIN SI

FIN SI

Répétition

Sert à repeter n fois une action :

- TANT QUE
- REPETER ... JUSQU'A : effectue l'action une fois avant de vérifier la condition
- POUR

Tableaux à une dimension

Ils peuvent être préremplis.

L'indexation commence à 0.

Un tableau de N case aura pour indice i de 0 à N-1.

Tableaux à deux dimensions

Lorsqu'un traitement utilise plusieurs tableaux à une dimension, on utilisera un tableau à deux dimensions.

On définit $T(i,j)$ avec i lignes et j colonnes.

Pour lire un tableau à 2 dimensions on doit imbriquer deux boucles l'une dans l'autre :

ex: POUR ligne DE 0 A N-1

POUR colonne DE 0 A M-1

AFF ligne, colonne, $T(\text{ligne}, \text{colonne})$

FIN POUR

FIN POUR

Les Concepts de l'Approche par Objets

3 concepts nécessaires à la POO :

- encapsulage
- héritage
- polymorphisme

Classe

Une classe est un modèle qui décrit une abstraction.

Permet de recenser une série d'éléments communs décrivant un concept précis.

Elles décrivent les propriétés des objets.

Analogie avec plan d'un pavillon, avec chaque pavillon qui peut avoir une couleur différente (plan = classe, pavillon = objet).

Elles sont de 2 types :

- propriétés contenant de l'information :
 - o modifiés au travers de la méthode
 - o ces propriétés sont les "attributs"
- propriétés actives
 - o fournissent un service et peuvent modifier l'état d'un Objet
 - o ses propriétés sont les "méthodes"

ex: classe compte

propriétés (attributs) : solde, decouvertAutorise, dateOuverture

propriétés actives (méthode) : `crediter()`, `debiter()`, `obtenirSolde()`, `calculAgiros()`

Il est possible de conférer un type à un attribut ou à un argument d'une methode.

Un type désigne un ensemble de valeurs que peut prendre un attribut ou un argument : entier, chaîne, booléen, réel...

Une classe peut également servir de type.

Objet

C'est une matérialisation de la classe (concrétisation).

L'acte de concrétiser une classe s'appelle le mécanisme d'instanciation.

On dit qu'on instancie une classe ou que l'on crée un Objet.

Objet = instance de Classe.

ex: MaVoiture:Automobile

```
marque = "Peugeot"
```

```
modèle = "607"
```

puissance = 10

```
couleur = "rouge"
```

Encapsulation

Pour chaque attribut et ou méthode d'une classe, on précisera son niveau de visibilité.

C'est l'idée de masquer le fonctionnement exacte du mécanisme bien que je puisse utiliser ce mécanisme (idée de la grosse boîte noire)

public | + | élément visible par tous

| | | |
|---------|---|---|
| protégé | # | élément visible par les sous-classes de la classe |
|---------|---|---|

privé | - | élément visible seulement par la classe

| | | |
|-----------|---|--|
| paquetage | ~ | élément encapsulé visible uniquement dans les classes du paquetage |
|-----------|---|--|

ex:

Personne | | => classe

```
-nom : chaine      | |
```

```
-prenom : chaine      | | => attributs
```

```
-dateNaissance : Date | |
```

```
+calculeAge() : entier
```

```
+getNom() : entier | ==> methode
```

```
+setDateNaissance(dateNaissance : Date) | |
```

+getNom() est un accesseur en lecture/getter

+getDateNaissance est un accesseur en ecriture/mutateur/setter

Propriétés de Classes

Un attribut de classe est partagée avec sa valeur par l'ensemble des instances.
Une méthode de classe est une méthode qui est directement liée à la classe elle-même.
Au sein d'une telle méthode, seuls les attributs dits "de classe" sont accessibles.
Un attribut de classe est un attribut transverse partagé par toutes les instances (ex: TVA pour des produits en ventes, si ils ont la même TVA).

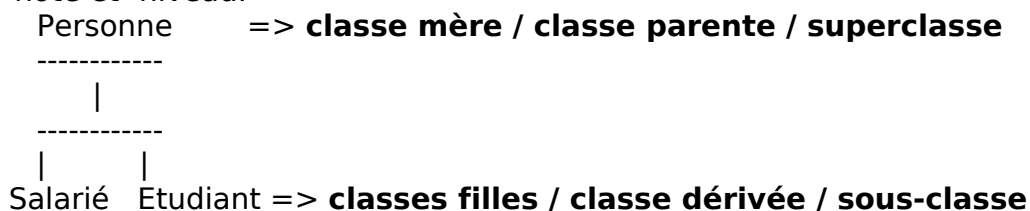
ex: reprenant la classe Personne. l'attribut -majorite : int = 18. On la met en valeur en la soulignant.

ex: en reprenant la classe Perssone, une méthode de classe +changeMajorite(nouvelMajorite : entier)

Généralisation/Spécialisation

La généralisation/spécialisation est une association particulière.
Elle ne porte pas sur les instances mais sur les classes.
Elle exprime que les instances d'une classe (classe fille) sont également des instances d'une autre classe (classe mère).
La généralisation a pour but de factoriser des attributs et des méthodes communs à plusieurs classes.

ex: on peut créer une classe spécialisé de personne : Salarié avec -salaire. Une autre Etudiant avec -note et -niveau.



Plus on remonte : généralisation. Plus on descent spécialisation.

On peut créer des classes stériles qui ne peuvent avoir d'enfants.

Héritage

Les instances d'une sous-classe sont aussi instance de ses surclasses.
Ces dernières sont donc également décrites par les attributs et méthodes introduites dans les surclasses.

Par conséquent, une sous-classe hérite des attributs et des méthodes de sa sur-classe.
Elle n'hérite que attributs et méthodes publiques (ou protégés : #) mais pas les publiques.

Cet héritage provient de la relation Généralisation/Spécialisation.

Polymorphisme

Le polymorphisme s'inscrit dans une logique de Généralisation/Spécialisation.

Le polymorphisme est le mécanisme qui consiste à appeler la méthode en fonction du type de l'objet instancié et non pas du type de l'objet réellement déclaré.

ex:

```
Salarié sal1;
sal1.affiche(); => va chercher la méthode affiche() de la classe Salarié
```

```
Personne p1;
p1.affiche(); => va chercher la méthode affiche() de la classe Personne
```

```
Personne TPers[3];
tPers[0] <- p1;    => possible car p1 est une Personne
tPers[1] <- sal1;  => possible car sal1 est une Personne
tPers[0].affiche(); => va chercher la méthode affiche() de la classe Personne
```

tPers[1].affiche(); => va chercher la méthode affiche() de la classe Salarié car on appelle le type de l'objet instancié (Salarié) par réellement déclaré (Personne)

Classe abstraite

Une classe “concrète” est une classe instanciable car elle décrit un modèle complet, tous les attributs et toutes les méthodes sont totalement décrits.

Une classe abstraite provient de la “Généralisation”.

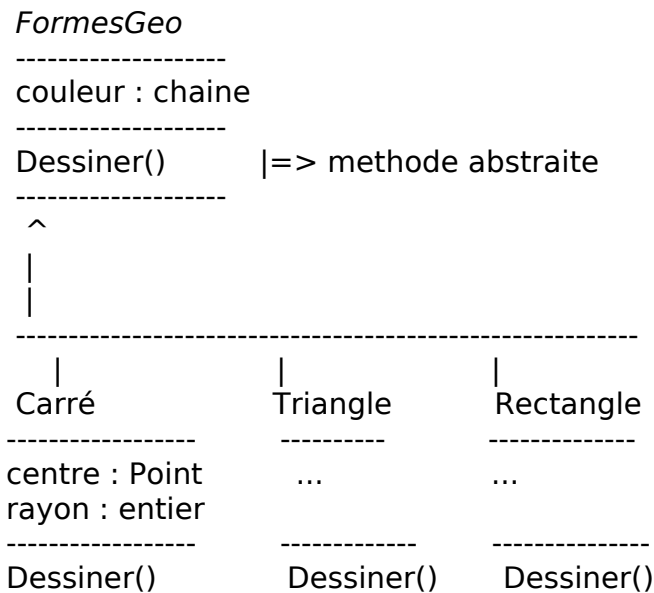
Il s'agit d'une factorisation de propriétés communes.

Une classe abstraite ne peut avoir d'instances directes.

Les méthodes d'une classe abstraite peuvent être décrites de façon limitée à la signature de méthodes.

On parle de “Méthode Abstraites”.

ex:



Traditionnelement, on indique une classe abstraite en l'écrivant en italique.

Ici la classe FormesGeo est abstraite (correspond à rien), mais permet de factoriser l'attribut couleur.

Forcer à avoir une methode abstraite (donc vide) force a avoir la méthode Dessiner() défini dans les sous-classe.

On garanti le **polymorphisme**.

On impose un “schéma”.

Si la sous-classe est elle aussi abstraite il n'est pas nécessaire de définir les méthode abstraite de la surclasse.

Interface

Une interface est une classe abstraite ne contenant que des signatures de méthode publiques.

Une interface est réalisée par une classe.

On dit qu'une classe implémente une interface.

Une interface est employée pour décrire les fonctionnalités d'une classe ou d'un composant.

C'est un élément fondamental de la conception objet.

On indique formellement qu'une classe implémente une interface avec une flèche en pointillées ou le formalisme lollipop Classe Interface ---O)--- Classe

Ligne de Commande

Prof. : ASSOUS Steeve

Code : 2518

Sommaire

- Présentation de Linux/Unix
- Système de fichiers : l'arborescence
- Manipulation de fichiers
- Edition de fichiers texte : VI
- Redirections et Filtres
- Recherche de Fichiers via "find"
- Recherche de motifs "grep"
- Gestion des processus

Présentation

Définition

C'est un OS

Programme ou ensemble de programmes et d'API, interface matériel et applications.

Disponible pour de simple micro (PC, MAC, Atarie...) jusqu' au gros syst_me (IBM Z Series) et même dans des PDA

Unix ? Linux ? Telle est la question.

Historique de UNIX

- 1969 : Bell Laboratoire; Ken Thompson travaille sur MULTICS; Bell Lab abandonne le projet K. Thomspon renomme UNICS et dev. sur DEC PDP-7
- 1974 : refonte du syst. en langage C; Unix gagne la fav. des univ.
- 1978 : V7 annoncée
- 1979 : cout des licences incite Berkley à continuer ses travaux. Création de BSD; le Darpa utilise BSD Unix
- 1983 : AT&T met en vente la version commercile de Unix Syst. V
- 1984 : Wenix 1er Unix sur PC
- 1991 : Apparation des premiers clones Unix comme Linux et FreeBSD
- 1992 : Sun sort Solaris

D'où vient Linux ?

- 1985 : création de la FSF par R. Stallman
 - Copyleft et GPL avec 4 libertés fondamentales :
 - exec. le programme pour tout usage commercial ou non et par n'importe quel type de personne ou d'organisation
 - étudier le fonctionnement du pregramme et l'adapter
 - redistribuer des copies gratuitement ou non
 - améliorer le programme et publier les améliorations
- 1991 : création de Linux par Linus Torvald

Caractéristiques

Unix/Linux est un OS :

- multi-taches
- multi-utilisateurs
- multiplateformes
- stable

Les composants de base d'un Unix/Linux sont les noyau (kernel) et les outils (shell et commandes).

L'OS a pour principales tâches les points suivants :

- gestion de la mémoire
- accès aux périphériques
- accès disque/ système de fichiers
- gestion des programmes (processus)
- sécurité / accès aux données
- collecte d'information système : statistiques

LAMP pour les serveurs : Linux (OS) Apache (serveur Web) MySQL (SGBDR) PHP (langage de programmation serveur).

Quelle distribution ?

Le choix d'une distribution dépend de :

- du coût
- de la suite logicielle
- de la compatibilité matérielle
- des outils d'administration
- mais aussi les préférences de chacun

Les distributions "grands publics"

- Fedora (distribué par Red Hat)
- Open Suse
- Mandriva (anciennement Mandrake)
- Ubuntu

Les distributions "pro."

- Red Hat
- Suse
- Debian
- Slackware

Les distributions "mobiles"

- Knoppix
- Mandriva Flash
- Fedora Live CD

Les distributions "spécialisées"

- Tomsrbt
- µLinux

Connexion : consoles et terminaux

Chaque utilisateur sera doté d'un login et d'un MdP

- root
- règle de mot de passe

La connexion peut se faire via différentes manières

- console virtuelle
 - Texte
 - Graphique
- émulateur de terminaux
- client ssh

Prompt (Invite shell)

Le shell

- interprétation en ligne des commandes
- il traduit les requêtes en actions

Prompt : PS1

- il s'agit de l'invite présente au moment de la saisie d'une commande
- cette invite diffère suivant les environnements et suivant les utilisateurs

ajc1@DebServ:~\$

- ajc1 : username
- DebServ : hostname
- ~ : repertoire de connexion (ici HOME)

La Documentation

- man
- info
- option --help
- internet :
 - www.linux.org
 - www.tldp.org
 - www.redhat.fr
- groupe de discussion

Deconnexion

Trois manières de se déconnecter d'un terminal texte :

- exit
- logout
- ...

Quelques commandes

Info utilisateur

- who
- whoami
- passwd

Affichage

- clear
- echo

Temps

- date
- cal

Système de Fichiers : Arborescence

Organisation

Un syst. de fichiers (FileSystem) définit comment sont gérés les fichiers par l'OS

Présenté de façon arborescente, le FS est une hiérarchie de répertoires ayant pour racine unique "/"

Organisation logique et indépendante du stockage physique des données.
Complètement transparente pour l'utilisateur.

Diff. rep. :

- bin : contient les commandes
- boot : gere le demarage du système
- cdrom : pour monter le cdrom
- dev : contient les périphériques
- etc : contient les fichiers de config
- home : repertoire des utilisateurs

- lib : contient les librairies
- lost+found : garde les fichiers non correctement fermés en cas de crash
- root : rep. du root
- sbin : commande admin
- tmp : fichiers temporaire
- mnt : montage fichiers
- proc : syst. de fichiers virtuel représentant l'état actuel du syst.
- sys : syst. de fichier vituels représentant l'état des différents peripheriques.
- var : fichiers dont la taille vaire au cours de la vie du systeme
- ...

“Tout est Fichier” : nomenclature

Unix fait la distinction entre min et maj.

La plupart des caracs. (chiffres, lettres, maj. min. certains signes, caractères accentués) sont acceptés, y compris l'espace (déconseillé)

Adressage Absolut/Relatif

Absolu : chemin identifié à partir de la racine

Relatif : chemin défini à partir du répertoire courant

Rep. :

- courant : .
- parent : ..
- personnel : appelé aussi répertoire HOME
→ définit le rep. de connexion, l'espace personnel de l'utilisateur (/home/nomUser)

Manipulation de Fichiers/Répertoires

Commandes permettant de manipuler les fichiers

- pwd : print working directory
- cd : change directory
- ls : liste le contenu du repertoire
→ ls -r : recursif
→ ls -l : affiche sur une seule colonne
- file : renvoie le type de fichier

Répertoire

- mkdir
- rmdir

Fichiers

- touch
- cp
- rm
- mv
- cat
→ cat > nomFichier : permet d'ecrire dans le fichier (attention efface ce qui est écrit)
→ cat >> nomFichier : écrit à la fin du fichier
- more
- head/tail : affiche les 10 premières/dernières lignes du fichier
→ head/tail -x : affiche les x premières/dernières lignes
- cut : affiche une partie des lignes du/des fichier(s) en argument
→ La selection peut se faire par champ ou par caractères
→ cut -d: (délimiteur ici :) -f3 (champ ici 3)
→ cut -c1-8 (caractères de 1 a 8)
- wc : comptabilise le nombre de lignes, mots, caractères

ex :

more /etc/passwd : affiche tous les utilisateurs inscrits

ajc1:x:1151:1003::/home/ajc1:/bin/bash

nomUser:PrésencePassword:uid:gid:NomGECOS:RepertoireDeCMX:PossibilitéDeSeConnecter

drwxr-xr-x 4 ajc1 unix 4096 oct 5 12:13 dos

- d : type (d : directory, - : fichier ordinaire, l : lien symbolique, b: block, c : caractere)
- rwxr-xr-x : permission User|Group|Other
- 4 : nombre de lien physique
- ajc1 : user propriétaire
- unix : groupe propriétaire
- 4096
- oct 5 12:13 : horodatage
- dos : nom

ls -l | cut -c1-10,41- : liste les fichiers avec détails | en ne gardant que les 10 premiers caractères puis les caractères à partir du 41e.

wc fichHello : affiche le nombre de lignes, mots et caractères dans fichHello

2 5 27 fichHello : 2 lignes, 5 mots, 27 caractères

wc -l /etc/passwd : affiche le nombre de ligne dans /etc/passwd, correspond au nombres d'utilisateurs déclarés.

Permission

rwX :

- r : readable
- w : writable
- x : executable

Pour un fichier normal :

- r : contenu peut être lu, chargé en mémoire, visualisé, copié
- w : le contenu du fichier peut être modifié, on peut écrire dedans. La suppression n'est pas forcément liée à ce droit (voir droit rep.)
- x : le fichier peut être exécuté depuis la ligne de commande, s'il s'agit soit d'un programme binaire (compilé), soit d'un script

Pour un repertoire

- r :
- w : droit de suppression
- x : droit d'accès

chmod : modifie les permissions

- chmod u+x : ajoute le droit d'exécuter à l'utilisateur
- chmod g-w : retire au groupe le droit de lire
- chmod og+x : ajoute au autres et au groupe le droit d'exécuter
- chmod u=rwx : donne à l'utilisateur le droit de lire, écrire et exécuter
- chmod a-x : retire à tout le monde le droit d'exécuter

chmod peut aussi être utiliser avec une notation octale :

- r : 4
- w : 2
- x : 1

vi

Editeur WYSIWYG

Grand classique des editeurs de texte en entreprise

vi : mode de fonctionnement

Jongler entre les différents modes :

- insertion : i, I, a, A, o, O
- commande : echap

- ligne : ':'

Pour sauvegarder ':wq'

Mode commande

- nG : emmène à la ligne n (identique :n)

vi : Correction

- x : efface le caractère sous le curseur
- X : efface le caractère devant le curseur
- re : remplace le caractère sous le curseur par le 'e'
- dw : efface le mot depuis le curseur jusqu'à la fin du mot
- d\$: (ou D) efface tous les caractères jusqu'à la fin de la ligne
- dd : efface la ligne active
- ndd : efface les n-lignes
- y/Y : copie la ligne
- nY : copie n-lignes
- p/P ; copie en dessous/au dessus de la ligne contenant le curseur

vi : mode ligne

- :w : enregistre
- :1,10w Nom_fich : enregistre les 10 premières lignes
- :r Nom_Fich : insère le fichier Nom_fich à partir de la ligne courante
- :! commande : exécute la commande puis retourne à l'éditeur
- :r ! commande : exécute la commande et inscrit le résultat dans l'éditeur
- :f Nom_fic : affiche en bas de l'écran le nom du fichier, nb de ligne et position actuel

vi : recherche et substitution

Recherche :

- on distingue deux façons de rechercher des chaînes dans vi
 - / : recherche de haut en bas
 - ? : recherche de bas en haut

Substitution :

- :[1ere ligne, dernière ligne]s/Modèle/Remplacement/[gil]
 - :1,5/bin/sbin/
 - :5,30s/bach/ksh/g
 - 1,\$s/fonction/function/gi
 - \$ (ou %) jusqu'à la fin du fichier
 - g : toutes les occurrences
 - i : insensible à la casse
 - I : sensible à la casse

vi : options

Options de l'éditeur

- :set all : liste l'ensemble des options disponibles
- :set number/nonumber : affiche/cache les numéros de lignes
- :set autoindent/noautoindent : l'indentation est conservée lors d'un retour de ligne
- :set showmode/noshowmode : vi affiche une ligne d'état (montre le mode actuel)
- :set tabstop=x : définit le nombre de caractères pour une tabulation
- :set showmatch/noshowmatch : montre la parenthèse d'ouverture lors de la fermeture de cette dernière
- ab DF DUPONT Franck : crée une abbréviation
- map x 10dd : mappage des touches

Pour conserver les options il faut créer un fichier spécifique avec les options (.exrc).
Commentaires avec "

Redirections et filtres

Tout processus lancé est associé à 3 descripteurs (input, output, error)

ex: ls

- entrée standard : dossier courant
- sortie standard : écran

mkdir rep

- entrée standard : rep
- sortie standard : écran

cat > f1

- entrée standard saisie redirigée en sortie vers f1

'>' est un opérateur de redirection de même que '>>' (mais lui redirige à la fin du fichier).

Opérateurs de filtre (pipe)

- | : permet de lier des commandes. La 2eme commande est liée au résultat de la 1ere.

Find : prototype

Permet de rechercher des fichiers

Find : critères de recherche

au niveau du nom :

- -name | iname motif
- ex: \$find . -name 'nom'

au niveau du temps :

- -mtime [+ -] n (n jours) : modif de contenu
 - -atime [+ -] n : accéder
 - -ctime [+ -] n : modif de contenu et/ou de caractéristiques
- ex: \$find . -atime -1

au niveau des caractéristiques :

- -size [+ -] taille [bck]
 - -user utilisateur
 - -group groupe
 - -type d|f|l|b|c : dossier|files|link|
 - -perm droits
- ex : \$ find / -user 'as1'

Combiner des critères

- et logique : -a ou -and
- ou logique : -o ou -or
- negation : -not ou !

Exécution des commandes

- -print : affiche le nom des occurrences trouvés
- -exec : exécute la commande spécifiée
- -ok : reprend l'option -exec mais avec une demande de confirmation
- -ls : affichage des résultats

ex:

- find . \(\(-name 'D*' -type d \) -o \(-name 'rep*' -type d \) \) -print
- find . -name '*.sh' -exec cat {} \; : applique cat à chaque résultat du find.

grep

grep : prototype

Extraire des lignes d'un fichier selon divers critères.

Pour cela on dispose de trois commandes grep, egrep et fgrep qui lisent les données soit

depuis un fichier d'entrée soit depuis le canal d'entrée standard.

grep [-options] motif [arguments]

Quelques options :

- v : affiche toutes les lignes qui ne correspondent pas au motif
- c : ne retourne pas les lignes mais leur nombres
- i : ne tient pas compte de la casse
- n : indique le numéro de ligne pour chaque ligne trouvée
- l : affiche le nom du fichier

grep : Expressions régulières

Quelques métacaractères

- ^ : début de ligne
- . : un caractère quelconque
- \$: fin de ligne
- x* : zéro ou plus d'occurrences du caractère x
- x+ : une ou plus occurrences du caractères x
- x? : 0 ou une occurrence unique de x
- [aX0] : classe de caractères permis
- [.-.] : plage de caractères permis
- [^...] : plage de caractères interdits
- \{n,m\} : facteur d'occurrences
- \ : caractère d'échappement
- () : définit un groupe
- | : ou

ex:

- grep '^unix' /etc/passwd : commence par unix
- grep '[^0-9]\$' /etc/passwd : ne se termine pas par un chiffre
- grep '^t(it|oto|ata)' nomFichier : commence par titi toto tata
- grep '^0[1-9](\[0-9\]\{2\})\{4\}' : recherche un numéro de téléphone 0x.yy.yy.yy.yy avec x

1-9 et y 0-9*

Gestion des processus

Un processus représente à la fois un programme en cours d'exécution et tout son environnement d'exécution (mémoire, état, ..)

Définit par :

- un numéro de processus unique PID
- un numéro de processus parent PPID
- un numéro d'utilisateur et un numéro de groupe
- un répertoire de travail

Daemons

La commande ps affiche les processus en cours (ou pstree).

- liste les processus du syst.
- liste les processus de façon hiérarchique

Quelques options :

- a : tous les utilisateurs
- u : nom des utilisateurs et date
- x : non rattaché à un terminal
- l : informations détaillées

Quelques colonnes :

- UID
- PID
- PPID

- C : facteur de priorité (plus la valeur est grande plus la priorité est basse)

-

Signaux et commande "kill"

Le signal est l'un des moyens de communications entre les processus.

Lorsqu'on envoie un signal à un processus, celui-ci doit l'intercepter et réagir en fonction de celui-ci.

Certain signaux peuvent être ignorés, d'autres non.

Suivant les UNIX; on dispose d'un nombre plus ou moins important de signaux.

L'option -l permet d'obtenir la liste des signaux.

Liste signaux :

- 1 SIGHUP : hang up, est envoyé par le père à tous ses enfants
- 5 SIGTRAP :
- 2 SIGINT : interruption du processus demandé (CTL+C)
- 3 SIGQUIT : idem SIGINT mais génération d'un core dump (fichier débogage)
- 9 SIGKILL : signal ne pouvant être ignoré, force le processus à finir brutalement
- 15 SIGTERM : signal envoyé par défaut par la commande kill. Demande au processus de se terminer normalement

Manipulation processus

Lancer un processus :

- en avant-plan : on attend la fin de la commande avant de récupérer la main.
- en arrière-plan : la commande se lance mais on ne perd pas la main. On utilise l'esperluette &.
- persistant : commande "nohup"
- priorité : nice/renice

Arrêter un processus :

- Ctrl + C : signal SIGINT
- Ctrl + \ : signal SIGQUIT
- Ctrl + Z : signal SIGSTOP

Contrôler les processus

- commande "jobs" : affiche la liste des processus lancés en arrière plan
- commande "bg" : relance un processus suspendu en arrière plan
- commande "fg" : lance un processus en avant-plan

Shell

Prof. : ASSOUS Steeve

Code : 4826

Sommaire :

Qu'est-ce-que le shell ?

Le shell est un interpréteur de commandes :

- initialise l'environnement
- génère le prompt
- assigne les variables
- effectue les substitutions de variables et commandes
- interprète les métacaractères
- génère les noms de fichiers
- gère les redirections et filtres
- gère l'historique des commandes
- complétion de noms de fichiers
- création d'alias

Différents types de shell :

- Ksh : Korn Shell
- Sh : Bourne shell
- Csh
- Bash : Bourn again shell

Que se passe-t-il lors de la connexion ?

Envoie de l'invite de connexion

- saisie des informations de connexion

Effectue la connexion

- validation du login
- place l'utilisateur dans son repertoire de connexion
- lance l'interpréteur de commandes

Etapes de l'interpréteur de commandes

- exécute le fichier `"/etc/profile"`
- exécute le fichier `"~/profile"`
- exécute le fichier `".bashrc"` (fichier bash utilisé)
- interpréteur de commande

umask fonctionne à l'inverse du chmode :

| | Repertoire | Fichier |
|---|------------|---------|
| 0 | rwX | rw- |
| 1 | rw- | rw- |
| 2 | r-X | r-- |
| 3 | r-- | r-- |
| 4 | -wX | -w- |
| 5 | -w- | -w- |
| 6 | --X | --- |
| 7 | --- | --- |

Substitution de variables

Une variable

- est un nom associé à une valeur
- **n'est valable que dans le shell où elle a été défini**
- doit commencer par une lettre, et ne contenir que des lettres, chiffres et underscore

Affectation `var = "toto"`

Affichage `echo = $var`

Notion d'Alias : "alias"

un alias est une substitution d'une commande par un raccourci

L'alias est prioritaire sur les fonctions, commandes

On peut rendre un alias permanent en le rajoutant au `.bashrc`.

On le supprime avec : `unalias [-a] name [name ...]`

Liste des variables : "set"

Permet d'afficher les noms et valeurs de toutes les variables du shell en zone de données et dans l'environnement.

`unset nomvariable`

- réinitialise le contenu d'une variable

`unset`

- réinitialise toutes les variables.

Variables d'environnement : "env"

Permet de lister les variables de l'environnement

Certaines variables décrivent des informations liées au système

- HOME
- PATH : définit les chemins à scruter lors de l'exécution des commandes
- PS1 : prompt primaire
- PS2 : prompt secondaire
- TERM : le type de terminal
- PWD : le dernier repertoire de travail
- LOGNAME : le nom de l'utilisateur logué

Export de variables

Par défaut une variable a une portée locale et n'est donc accessible uniquement dans le shell où elle a été défini.

La commande "export" permet de promouvoir les variables en tant que variables d'environnement et les rend accessibles dans l'environnement utilisateur

- export nomVariable

Rendre un fichier executable

Creer un script

- vi nomScript.sh ...

Le rendre executable

- chmod 755 nomScript.sh

Execution

- ./nomScript.sh

Pour rendre le chemin disponible dans le PATH, il faut le rajouter, par exemple dans .bashrc ou .profile.

Ne pas oublier de faire l'export.

Substitution de commande

Deux façons :

1. jour=\$(date)
2. jour=`date`

Metacaractères

- # : commentaire
- \$: substitution de variable
- & : lancer en arrière-plan
- && : enchainement conditionnel
- || : enchainement conditionnel
- | : filtre
- > : redirige la sortie standard
- 2> : redirige la sortie erreur
- ' : délimite une chaîne de caractères. Les caractères spéciaux sauf \ et ` perdent leur signification
- " : délimite une chaîne de caractères. Les caractères spéciaux sauf \, \$ et ` perdent leur signification
- `cmd` : Execution et substitution de commandes
- \$(cmd) : Execution et substitution de commandes
- \ : caractère d'échappement
- >> : redirection de la sortie standard avec ajout.

Passage d'argument

Les paramètres positionnels

◇ Le nom du fichier et les paramètres de la ligne de commande sont stockés et peuvent être récupérés au sein d'un shell script

- \$0 : nom de domaine (du script)
- \$1-9 : les neufs premiers paramètres du script
- \$# : nombre total de paramètres
- \$* : Liste des arguments
- @\$:

Variables spéciales

- ◇ \$? : code retour de la dernière commande exécutée (0 réussi, 1 échec)
- ◇ \$\$: PID du shell actif
- ◇ \$! : PID du dernier processus lancé en arrière plan
- ◇ \$- : options du shell

exit x : permet de sortir avec un code retour de x (0-255)

- ◇ théoriquement :
 - 0 : si tout se passe bien
 - 1 : si erreur dans la commande
 - 2 : si commande fausse
 - **Attention ! Il y a de nombreux contres exemples.**

Commande “shift”

Syntaxe :
shift [n]

- But :
- ◇ décale de n arguments vers la gauche
 - ◇ n prend 1 par défaut
 - ◇ met à jour la variable \$#

Saisie à l'écran “read”

Permet la saisie de chaîne de caractère à partir du clavier.

- Options :
- -p : read -p “Saisir un nom” nom, affiche une phrase
 - -e : echo -e “Nom Saisi \n” \$echo

Double expansion : “eval”

“eval” construit une commande en concaténant ses arguments.
Le shell lit et exécute cette commande.

| Commande | Affichage |
|---------------|-----------|
| var = 10 | 10 |
| x=var | var |
| y=\\$\$x | \$var |
| echo \$y | \$var |
| eval echo \$y | 10 |

Opérations sur les entiers : “expr”

Permet l'arithmétique entière sur les valeurs : + - / % *

Code retour

- Chaque commande génère un code retour
- 0 pour vrai, autre pour faux

Formulation de conditions

On distingue plusieurs manières de formuler des conditions.

- 2 syntaxes :
- test expression
 - [expression]

Ces conditions peuvent porter sur :

- les fichiers
- les chaînes de caractères
- les entiers

Opérations sur les fichiers

- Syntaxe :
- test -option nomfichier

- [-option nomfichier]

Quelques options

- -f : fichier normal
- -d : un repertoire
- -c : fichier en mode caractère
- -b : fichier en mode bloc
- -p : tube nommée
- -w : accès ecriture
- -r : accès lecture

Opérations sur les entiers

Syntaxe :

- test var -option argument
- [var -option argument]

Quelques options :

- -eq : égal
- -ne : not equal
- -lt : less than
- -gt : greater than
- -le : less or equal
- -ge : greater or equal

Opérations sur les chaines

test -z "variable"

- zero, retour OK si la variable est vide (test -z "\$a")

test -n "variable"

- non-zero, retour OK si la variable n'est pas vide (test -z "\$a")

test "variable" = "chaine"

- OK si les deux chaines sont identiques

["variable" != "chaine"]

- OK si les deux chaines sont différentes

Combiner les critères

On peut combiner les critères via :

- -a : and
- -o : or
- ! : not
- (...) : groupement des combinaisons. Les parenthèses doivent être verrouillées \(\...\)

ex:

```
test -d "rep1" -a -w "rep1"
```

Intruction "if"

```
if <commandes_condition>
```

```
then
```

```
<commandes executées si condition réalisée>
```

```
else
```

```
<commendes executées si condition pas réalisée>
```

```
fi
```

On peut aussi préciser le elif en fait un else if.

Si la dernière condition n'est pas réalisée on en teste une nouvelle.

Choix multiples “case”

La commande case esac permet de vérifier le contenu d'une variable ou d'un résultat de manière multiple

```
case var in
    Modele1) commandes ;;
    Modele2) commandes ;;
    *) action_defaut ;;
esac
```

Le modèle est soit un simple texte, soit composé de caractères spéciaux.

Chaque bloc de commandes lié au modèle doit se terminer par deux points virgules

Dès que le modèle est vérifié, le bloc de commandes correspondant est exécuté

L'étoile en dernière position (chaîne variable) est l'action par défaut si aucun critère n'est vérifié

Formation des “case”

Quelques caractères

- * : chaîne variable (même vide)
- ? : un seul caractère
- [...] : plage de caractères
- [!...] : négation de la plage de caractères
- | : ou logique

```
ex :
1)
xyz)
x??)
*x)
[cp]*
*[^0-9]
```

Structures itératives

while, until, for

Boucle While

La commande while permet une boucle conditionnelle “tant que”

Tant que la condition est réalisée, le bloc de commande est exécutée:

On sort si la condition n'est plus valable

ex:

```
1: while condition
do
    commande
done

ou

2: while
    bloc d'instruction formant la condition
do
    commande
done

3: cpt=1
while [ $cpt -le 10 ]
do
    echo " cpt : $cpt "
```

```
((cpt=$cpt+1))
```

```
done > fichier # redirige le flux vers un fichier
```

Boucle until

La commande until permet une boucle conditionnelle "jusqu'a"

Dès que la condition est réalisée, on sort de la bloucle

```
ex 1:  until condition
        do
            commandes
        done
```

```
ex 2:  until
        bloc d'instructions formant la condition
        do
            commandes
        done
```

```
ex 3:  cpt=1
        until [ $cpt -ge 11 ]
        do
            echo "cpt : $cpt"
            ((cpt++))
        done > fichier
```

Boucle for

La boucle for ne se base pas sur une quelqconque incrémentation de valeur mais sur une liste de valeurs, de fichiers...

```
ex1:  for var in liste
        do
            commandes
        done
```

```
ex 2:  for var in 1 2 cinq 7 11 # passe de valeur en valeur
        do
            echo "var : $var"
        done
        echo "Fin"
```

```
ex 3:  for var in $* # passe par les valeurs saisies en arguments
        do
            echo "var : $var"
        done
        echo "Fin"
```

```
ex 4:  for var in $(seq 1 5) # passe par les valeurs 1 2 3 4 et 5 (seulement valeurs entière)
        do
            echo "var : $var"
        done
        echo "Fin"
```

```
ex 5:  for var in * # prend tous les éléments du repertoire dans lequel on execute le script
        do
            echo "elm : $var"
        done
        echo "Fin"
```

```
ex 6: for var in `grep "^unix" /etc/passwd|cut -d: -f1` # prend tous les noms d'utilisateurs qui
commence par unix
do
    echo "user : $var"
done
echo "Fin"
```

Sortie anticipée "break"

La commande break permet d'interrompre une boucle

Dans ce cas le script continue après la commande done

Elle peut prendre un argument numérique indiquant le nombre de boucles à sauter, dans le cadre de boucles imbriquées (rapidement illisible).

Remonter en début de boucle : "continue"

La commande continue permet de relancer une boucle et d'effectuer un nouveau passage.

Elle peut prendre un argument numérique indiquant le nombre de boucles à relancer (on remonte de n boucles).

Le script redémarre à la commande do.

```
ex 1: while #1
do
    while #2
    do

        continue # remonte à la boucle #2 si continue 2 alors remonte à la boucle

    done

    continue # remonte au début de la boucle 1

done
```

Code retour "Exit"

Syntaxe :
exit [n]

Stoppe l'exécution du programme et positionne le code retour à n

Si aucun argument n'est spécifié, la valeur de retour est celle de la dernière instruction exécutée avant la commande "exit"

Les valeurs autorisées pour n sont comprises entre 0 et 255

Capture des signaux "Trap"

La commande trap permet d'effectuer 3 opérations sur les signaux

```
trap 'cmds' nosig nosig nosig
    capture des signaux et exécution des commandes "cmds" à la réception d'un signal
trap " nosig nosig nosig
    ignore les signaux, n'effectue aucune opération à la réception d'un signal
trap nosig nosig
    réinitialise les signaux, rétablissement des actions par défaut
```

La commande trap peut être placée n'importe où dans un shell script.

Dependant, un placement judicieux permet d'effectuer des traitements évolués.

Ex: si une partie du programme ne doit pas être interrompue, on peut positionner un trap qui

ignorera tous les signaux avant cette partie du code

```
trap ' ' 15 # interception du signal 15
```

```
code
```

```
...
```

```
trap 15 # rétablissement du signal 15
```


Role et Comportement du Consultant

Prof. Khaida Armand

Code :

Red Hat System Administration

Prof. : Brayer Marc

Code : 2529

Adresse du cloud : <http://91.121.52.156/owncloud/index.php/login>

ID : cgi

MdP : silenus

Pourquoi Red Hat

- Orientation entreprise avec un support.

Linux ?

- Kernel
- application

On parle de GNU/Linux.

- projet (open source)
- Richard Stallmann
 - ◇ Recompiler sur x86
 - ◇ Le premier c'est Linus Torvald (Linux)

Les distributions principales :

- Red Hat (entreprise)
- Debian (entreprise)
- SUSE (entreprise)
- Slackware (la 1ere)
- Arch Linux

Particularité de Red Hat : Oracle et son support.

On commencera par une CentOS (dérivée Red Hat) pour une histoire d'accès au dépôt.

Administration système

- système fichier
- users, permissions
- log, audit
- installation package
- configuration réseau
- openSSH
- virtualisation KVM

CentOS

- Community Enterprise Operating System
- principalement destinée aux serveurs
- tous ses paquets, à l'exception du logo, sont identiques. Interopérables.

De Fedora à CentOS

- Red Hat : stable, éprouvée, commerciale, support
 - ◇ CentOS : gratuit, support, communautaire
 - ◇ Fedora : user friendly
 - ◇ Scientific Linux

Pourquoi CentOS ?

- compatibilité avec Red Hat
- nombreux logiciels packagés rpm (rarement deb)
- installation automatique via kickstart sont plus simple que chez Debian

Architecture matérielle

- linux existe pour au moins trois architectures matérielles courantes
 - ◇ x86 ou i386/i686
 - ◇ x86_64
 - ◇ ppc : power pc anciens ordinateurs d'Apple

Linux est un noyau

- le noyau est une interface entre des programmes et des périphériques physiques
- l'accès à ces périphériques se fait par l'intermédiaire d'appels systèmes qui sont identiques quelle que soit la machine
- cette encapsulation du matériel libère les développeurs de logiciels de la gestion complexe des périphériques : c'est l'OS qui s'en charge
- ainsi, si l'OS existe sur plusieurs architectures, l'interface d'utilisation et de programmation sera la même sur toutes.
- on dira alors que le système d'exploitation offre une machine virtuelle à l'utilisateur et aux programmes qu'il exécute
- tous les systèmes d'exploitations sont basés sur ce principe

Espaces noyau vs utilisateur

- linux est un OS monolithique, écrit comme un ensemble de procédures qui peuvent s'appeler mutuellement
- pour l'utilisateur, il se présente comme un, seul gros fichier. Cependant il contient un ensemble de composants réalisant chacun une tâche bien précise
- Cette construction monolithique induit un aspect important
 - ◇ notion d'espace noyau : kernel space
 - ◇ notion d'espace utilisateur : userspace

Tâches réalisées par le noyau linux

- gestion processus, ordonnancement, scheduler
- gestion de la mémoire
- système de fichiers virtuel
- service réseau
- communications inter-processus

Installation Linux

- ISO
- PXE : par réseau (kickstart chez CentOS)
- netinstall : iso avec le minimum et le reste par le réseau

Systèmes de fichiers

- /bin : commande usuelle
- /boot : démarrage
 - ◇ Grub, bootloader
 - ◇ vmlinuz : noyaux
- /dev : périphérique
 - ◇ HD, souris, terminal...
- /etc : fichiers de configuration
- /home : répertoires utilisateurs
- /lib et /lib64 : bibliothèques systèmes partagées
- /proc : état temps réel du kernel
- /sbin : commande admin (par défaut root)

- /usr : tout ce qui concerne l'utilisateur
- /var : log, spool (printer), mail, site web

Réseau

Les fichiers de configuration sont dans /etc/sysconfig/network-scripts/

On peut voir l'état réseau avec `ip -a addr`.

On a plusieurs commandes :

- nmtui : avec UI
- nmcli
 - ◇ Elles sont appelées au network manager

Le fichier de config porte le nom ifcfg-nomCarteRéseau

Certifications

- LPI : peu utile
- Red Hat : 5h de TP, difficile à avoir.
 - ◇ RHCSA
 - ◇ RHCSE

On modifie le fichier pour mettre une ip fixe.

On relance la config en restart les services associés

- `systemctl restart NetworkManager`
- `systemctl stop`
- `systemctl start`
- `systemctl status`

On peut aussi faire :

- `ifdown NomCarte` puis `ifup NomCarte`

Hostname

/etc/hostname

ex: `www.marc.org`
`www=hostname`
`marc: =fqdn`

full qualified domain name

/etc/hosts/resolutionlocal
 permet de modifier le nom de domaine

Firewalld

`firewalld --> linux --> Netfilter --> kernel`
`systemctl stop firewalld`

Firewalld est une sous couche de netfilter
 iptables (pour écrire les règles dans netfilter)
 systemctl permet (arrêter démarrer visualiser les services)

Commande ip

Remplace la commande ifconfig dans les nouvelles releases de Linux.
`ip addr ~ ifconfig`

Pour installer ifconfig voir package net-tools.

Fichier de configuration

Généralement les fichiers de configuration se terminant par 'd' signifie 'daemon'.
Ils concernent le service.

RFC

Request For Comments
Série de documentations.

Port

De 1 à 1023 : réservé
Liste des services et des ports associés dans /etc/services

SSH

secure shell
openssh | client-serveur

ex: ssh root@hostname
ssh ibrahim@ultimatecoach

Le serveur écoute sur le port ssh (normalement le 22) tandis que le client ouvre un port aléatoire supérieur à 1023.

Il communique via le protocole TCP.

OpenSSH

Deux modes de connection
1. par password
2. par échange de clef

L'échange de clef se fait avec une clef publique/clef privé.

ex: PGP (private good privacy) écrit par P. Zimmerman

Chaque personne crée une clef publique et une privée.
La clef publique est envoyée sur le serveur que l'on veut joindre.
On chiffrera avec la clef privé et on pourra déchiffrer avec la clef publique.

ssh-keygen

option : -t [rsa | dsa] : les deux algorithmes classiques de création de clef
On peut mettre une passphrase (fortement conseillé)
Les clefs sont dans ~/.ssh/ (id_rsa et id_rsa.pub)

ssh-copy-id

Permet de copier la clef publique sur un serveur distant

Autres commandes SSH

scp : pour la copie
scp fichierAEnvoyer userdestination@host:/chemin/où/j'envoie/fichier
sftp : pour faire du ftp sécurisé
get fichier [/ou/placer/le/fichier]: download fichier
put fichier [/ou/placer/le/fichier]: upload fichier

Sur windows il existe winscp pour faire l'équivalent de scp.
Il existe aussi FileZilla (sftp)

Système de package

Tous les distributions Linux utilisent un système de package.

Un package est un binaire.

Ils sont stockés dans des dépôts (serveurs), chez les FAI, centre Universitaire...

Sur CentOS/Red Hat on utilise la commande yum.

Les dépôts sont définis dans /etc/yum.repos.d/*.repo

YUM

- update : liste des packages à mettre à jours
- upgrade : mise-à-jour des packages
- install nomPackage : installe un package ainsi que ces dépendances (ex: librairies)
- search nomPackage :

RPM

“Vrai” commande pour les packages.

Red Hat Package Manager

Permet d'installer les packages “à la main”.

Elle n'installe pas les dépendances.

Users, groups, permissions

Les fichiers

- passwd
 - ◇ root:x:0:0:root:/root:/bin/bash
 - ◇ login:PWD:UID:GID:info:\$HOME:shell
 - ◇ on peut créer à la main un utilisateur mais il faudra utiliser la commande “passwd” pour générer le mot de passe
 - ◇ on privilégiera “adduser” ou “useradd”

Les commandes

- useradd : ajoute un utilisateur. Il est nécessaire d'avoir un /home, gid et un uid.
- userdel : supprime un utilisateur
- usermod : modifie un compte utilisateur
- groupadd : ajoute un groupe
- groupdel : supprime un groupe
- groupmod : modifie un groupe
- id : montre les informations de l'utilisateur
- groups : montre les groupes auquel l'utilisateur appartient

Permissions

- sur les répertoires
 - ◇ r-x : lire (ls -l)
- chmod : modifie les permissions
 - ◇ octale ou avec les lettres
 - ◇ x=1, w=2, r=4
- En plus des permissions classiques, il y a des permissions spéciales : suid
 - ◇ place un ‘s’ sur la partie propriétaire à la place du ‘x’ du propriétaire
 - rws-----
 - on utilise chmod 4xxx (s'ajoute aux autres droit)
 - il donne un droit de root temporaire
 - ◇ autre permission speciale : sGID : rwxrws
 - on place cela parfois sur les répertoires pour que tous les fichiers créés héritent du groupe du repertoire
 - chmod 2xxx
 - ◇ dernier droit spécifique : sticky bit
 - chmod 1xxx
 - tous les droits sur un répertoire sauf que seul les propriétaires peuvent supprimer leurs fichiers

Changement de groupe ou propriétaire

- sur les fichiers et répertoires
 - ◇ chown : changement de propriétaire
 - ◇ chgrp : changement de groupe
 - ◇ ne peut être effectuée que par le root

Log

- Sont situés dans /var/log
 - ◇ le service en charge des logs est Rsyslog
 - son fichier de config est /etc/rsyslog.conf
- sont organisés dans des fichiers ex: /var/log/messages
 - ◇ pour choisir ce que l'on inclut (voir rsyslog.conf) : catégorie.sévérité (ex : mail.info)
 - ◇ si on a la commande none c'est que l'on exclut un élément (ex: *.info.none : on n'exclut tous les messages d'information de toutes les catégories).

DNS

- résolution DNS (Domain Name Service)
 - ◇ permet de lier les FQDN (Full Qualified Domain Name) ex: valentin.org vers l'IP
 - ◇ on interroge un dns lorsque l'on veut joindre un site web.
 - ◇ il y a plusieurs serveurs dns :
 - ceux qui contiennent les .org, .edu, .fr, .gov ...
 - ce sont les DNS:TLD
 - c'est "un peu" les racines d'internet
 - ils sont liés aux serveurs racines (13 serveurs à la NASA)
 - puis il y a les marc.edu, bill.org, aumbox.net
 - c'est les DNS du serveur personnel.
 - lorsque l'on veut se connecter à un site (ex: test.bill.org quand on est mcp.marc.edu), les étapes sont :
 1. cache de la machine
 2. si non, interroge mon serveur DNS (celui configuré, domaine ou FAI... etc) et notamment le cache du serveur DNS
 3. si non, envoie aux serveurs racines qui envoie au DNS:TLD de l'extension du nom de domaine correspondante (ici .org) qui nous renvoie vers la machine bill.org
 4. on interroge la machine bill.org qui nous renvoie test.bill.org
 5. la prochaine fois, on aura le site en cache.
 - ◇ il est nécessaire d'indiquer sur /etc/resolv.conf quelle est l'adresse ip du dns

Pour mettre en place un dns on utilise bind

- changer fichier de conf (named.conf)
- indiquer les zones et placer les fichiers correspondant dans /var/named/
- relancer named.service
- modifier le fichier de connection /etc/syslog/network-scripts/ifcfg-ens33
- relancer network-manager
- modifier /etc/resolv.conf pour indiquer le nouveau dns

Dans la zone dns il y a différent nom de propriétés

- A : adresse
- NS : nom de serveur
- CNAME : alias (canonical name)
- MX : serveur mail
- PTR : pointeur reverse

Zone DNS inversée

- se termine toujours .in-addr.arpa
- on met le champ d'IP à l'envers exemple pour 10.0.0.x on note 0.0.10
 - ◇ 0.0.10.in-addr.arpa
- Dans le fichier on renseigne les PTR en indiquant les morceaux d'adresses à considérer mais inversées ! (ex 10.0.10.11 -> 11.10)

Planificateur de taches : CRON

C'est un service, déjà installé dans le système.

Il existe une commande pour éditer la table de planification : "crontab".

- Il lance un vi avec un fichier à modifier

Si on a besoins de lancer une seule fois une tache on utilise la commande "at"

- at hh:mm puis la commande que l'on veut

Processus (gestion)

Sous unix tout est processus.

Designé par un pid (Processus ID).

Les commandes :

- ps : affiche les processus. Avec l'option aux on voit tous les processus.
- top : monitoring, affiche une page des processus mise-à-jour régulièrement.
- kill : permet d'envoyer un signal à un processus
 - ◇ avec -l on affiche les différents signaux.
 - ◇ kill PID : arrete normalement le processus PID avec signal 15 (SIGTERM)
 - arrete les processus enfants avant d'arreter le processus pere
 - equivalent Ctrl+C
 - ◇ kill -9 PID : tue le processus père sans tuer les processus enfants. Ceux ci deviennent des "zombies" et consomment de la mémoire.
 - ◇ kill -19 PID : SIGSTOP, met le processus en pause.
 - equivalent Ctrl+Z
 - ◇ killzll -HUP nomProcess : odonne au processus de relire son fichier de configuration, ce qui evite de le relancer.
 - "bg" on peut mettre en arrière plan avec la commande
 - "fb" on met au avant-plan

Firewall

"netfilter" appartient au noyau (kernel).

Il est donc plus difficile à arreter qu'un "simple service".

"iptables" est la commande pour écrire dans netfilter.

"firewalld" est une surcouche de "netfilter" pour l'utiliser plus simplement.

"firewall-cmd" est une commande qui permet de créer des règles de firewall.

Par contre "firewalld" est lié à "network-manager".

Si on arrête "network-manager", on perd "firewalld".

netfilter gère des hooks.

Qui sont des moments où on entre/sort des hook.

Processus locaux

NF_IP_PRE_ROUTING
PREROUTING



NF_IP_LOCAL_IN
INPUT



NF_IP_FORWARD
FORWARD



NF_IP_LOCAL_OUT
OUTPUT

NF_IP_POST_ROUTING
POSTROUTING



netfilter travaille avec des tables.
Chacunes ont différentes chaînes.

Il existe 3 tables :

- filter
 - ◇ INPUT
 - ◇ OUTPUT
 - ◇ FORWARD
- NAT
 - ◇ PREROUTING
 - ◇ OUTPUT
 - ◇ POSTROUTING
- mangle
 - ◇ PREROUTING
 - ◇ INPUT
 - ◇ FORWARD
 - ◇ OUTPUT
 - ◇ POSTROUTING

Les règles s'écrivent avec la commande "iptables".

Grace à cette commande, les règles sont écrites dans le Kernel.

Ces règles ne sont que temporaires et ne seront plus exécutées après avoir relancé la machine.

Sauf si on écrit un script avec ces règles.

Commandes iptables

Toujours en premier, on purge le firewall :

- iptables -t filter -F : on bloque toutes les tables pré-définies.
- iptables -t filter -X : on bloque toutes les tables utilisateurs.

Puis on bloque tout

- iptables -t filter -P INPUT DROP
- iptables -t filter -P OUTPUT DROP
- iptables -t filter -P FORWARD DROP

On ouvre les communications pour le réseau interne

- iptables -t filter -A OUTPUT -o eth0 -s 192.168.0.0/24 -d 192.168.0.0/24 -j ACCEPT
- iptables -t filter -A INPUT -i eth0 -s 192.168.0.0/24 -d 192.168.0.0/24 -j ACCEPT
 - ◇ eth0 correspond à la carte réseau liée au réseau interne.
 - ◇ 192.168.0.0/24 : autorise toutes les IP 192.168.x.x (car masque 24 bits)

On ouvre enfin la communications sur l'extérieur en restreignant aux services web (ici le http)

- iptables -t filter -A OUTPUT -o eth1 -s 10.0.0.0/8 -p tcp --dport 80 -j ACCEPT
- iptables -t filter -A INPUT -i eth1 -d 10.0.0.0/8 -p tcp --sport 80 -j ACCEPT

Si on test le nmap sur la machine "internet", on voit que le port 80 est ouvert.

Par contre il est possible de sonder les ports ouverts via un port d'entrée (ici 80) : nmap

10.0.0.66 -p 80

Conntrack

On peut lutter contre ça avec le suivi de connexion (conntrack).

Cela consiste à n'autoriser que les connexions qui sont déjà acceptées et à jeter toutes les nouvelles demandes connexions.

Pour l'utiliser on doit charger un module conntrack : "modprobe ip_conntrack"

- la commande "modprobe" permet de charger un module dans le noyau.

la commande pour iptables est :

- iptables -t filter -A OUTPUT -o eth1 -s 10.0.0.1 -d 0.0.0.0/0 -p all -m state --state ! INVALID -j ACCEPT
- iptables -t filter -A INPUT -i eth1 -s 0.0.0.0/0 -d 10.0.0.1 -p all -m state --state RELATED,ESTABLISHED -j ACCEPT
 - ◇ pour charger un module déjà dans le noyau dans netfilter on utilise la commande "-m nomModule" (ici "-m state")
 - ◇ "--state" : indique les états qui vont être utilisés pour nos règles
 - ◇ "! INVALID" : comme vu plus haut, le module de suivi de connexion gère 4 états, NEW, ESTABLISHED, RELATED et INVALID. Ce paramètre indique que l'on accepte uniquement les

connexions qui ne sont pas invalides, donc qui sont "NEW, ESTABLISHED, RELATED". Ceci est uniquement une manière plus rapide d'écrire qu'il faut que les connexions appartiennent à ces états.

IP Masquerading

On veut que la machine locale (paradise) puisse se connecter au web (sur pirate) par la machine interface (phoenix).

Cela s'appelle IP masquerading.

On cache son adresse IP.

On utilise le NAT pour cela.

C'est une table qui fait du pre- et post-routing.

On aura besoin de plusieurs modules :

- iptable_nat (pour le NAT)
- ip_nat_ftp (seulement si on veut se connecter à FTP)
- ip_nat_irc (seulement si on veut se connecter à IRC)

Cela se passe dans la table FORWARD.

Les règles sont :

- d'abord on supprime toutes les règles de NAT.
 - ◇ iptables -t nat -F
 - ◇ iptables -t nat -X
- puis on mets des règles par défaut
 - ◇ iptables -t filter -P FORWARD DROP
 - ◇ iptables -t nat -P PREROUTING ACCEPT
 - ◇ iptables -t nat -P POSTROUTING ACCEPT
 - ◇ iptables -t nat -P OUTPUT ACCEPT
- enfin on écrit les règles
 - ◇ iptables -t filter -A FORWARD -i eth0 -o eth1 -s 192.168.0.0/24 -d 0.0.0.0/0 -m state --state ! INVALID -j ACCEPT
 - ◇ iptables -t filter -A FORWARD -i eth1 -o eth0 -s 0.0.0.0/0 -d 192.168.0.0/24 -m state --state ESTABLISHED,RELATED -j ACCEPT
- il nous faut maintenant mettre en place le masquerading
 - ◇ iptables -t nat -A POSTROUTING -o eth1 -s 192.168.0.0/24 -j MASQUERADE
 - Masquerade indique que l'on masque les adresse en 192.168.0.0/24 lorsqu'elles veulent sortir du reseau.
 - ◇ on modifie la connection de la machine du reseau local (paradise) en indiquant une gateway dans /etc/sysconfig/network-scripts/ifcfg-nomCarteReseau
 - GATEWAY=192.168.0.1 (l'ip de Phoenix)
- Pour finir il faut activer l'ip forward manuellement dans le proc
 - ◇ echo 1 > /proc/sys/net/ipv4/ip_forward*

Dans le cas où l'on souhaite héberger un site sur le réseau local qui puisse être atteignable via internet, on fait une redirection de port (ici le 80).

On créera une autre carte réseau pour faire une DMZ où il y aura tous les PCs qui accède à internet sans qu'internet puisse y accéder.

Initialisation du système

Avant on avait System V.

System V

Le démarrage se déroule ainsi :

- tout d'abord le BIOS se lance, il initialise le matériel.
- puis il y a un bootloader qui charge (en mémoire) le MBR (Master Boot Record). Sur Linux c'est **GRUB**.
 - ce dernier charge le Kernel.
 - il lance INIT qui va lire le fichier /etc/inittab où sont inscrits tous les processus.

/etc/inittab

Il existe 6 niveaux dans le fichier :

- 0 : arrêt machine
- 1 : pour rentrer en mode mono-utilisateur, réservé à root
- 2 : mode multi-utilisateur, sans NTFS
- 3 : mode multi-utilisateur avec tous les services réseaux
- 5 : démarrage du serveur graphique X11 et plus
- 6 : redémarrage de la machine (la commande init 6 ou reboot lance le niveau 6)

Normalement le niveau par défaut est le x (id:x:initdefault)

Il charge d'abord l'ensemble des services importants (clavier, login, ...).

Puis il ira charger le niveau de démarrage (par ex. le 3).

Pour démarrer un service, on faisait : /etc/init.d/nomService restart/start/stop

/etc/init.d/script shell démarrage ou arrêt du service.

Systemd

Maintenant on utilise Systemd

Il s'occupe de :

- utilitaires :
 - systemctl
 - journalctl
 - notify
 - analyse
 - cgl
 - cgtop
 - logictl
 - nspawn
- cibles
 - ◇ bootmode
 - ◇ shutdown
 - ◇ basic
 - ◇ reboot
- démons
 - ◇ logind
 - ◇ journald
 - ◇ Systemd
 - ◇ user session
- coeur
 - ◇ manager
 - ◇ Systemd
 - ◇ namespace
 - ◇ log
 - ◇ cgroup
 - ◇ dbus
 - ◇ login
 -
 - ◇ unité
 -
- bibliothèques
 - ◇ dbus-1
 - ◇ libpam
 - ◇ libcap
 - ◇ libcryptsetup
 - ◇ tcpwrapper
 - ◇ lbaudit
 - ◇ libnotify
- noyau

- ◇ cgroups
- ◇ autofs
- ◇ kdbus

C'est tentaculaire et donc en cas de problème avec Systemd le système part en sucette.

Systemd : system daemon se charge donc de démarrer les services

Il diffère de l'init de system V en :

- Utilisant des sockets (80/tcp par ex) et des bus pour démarrer et gérer les services. Il est ainsi plus facile de paralléliser des services interdépendants
- pas de scripts shell, mais des fichiers de démarrages simples
- utilisant les cgroups pour suivre les processus des services en plus des PID. Cela permet de maintenir la trace des démons même s'ils se dupliquent
- permettant sauvegardes et restaurations de l'état du système
- parallélisant mieux, avec donc un temps de démarrage bien plus court
- permet de monter ou démonter les points de montages

Systemd utilise comme sysinit le principe d'exécution

- 0
- 1
- 3
- 2,4
- 5
- 6

Systemd est un gestionnaire de services qui remplace sysinit depuis Red Hat 7 :

- il démarre comme premier processus lancé par le noyau
- assure l'initialisation des services
- gère les démons linux : démarre, stoppe, désactive, active
- il démarre les services en parallèle
- il suit les services avec les groupes de contrôle (gestion des ressources)
- gère la journalisation et peut transmettre les journaux à syslog
- la configuration des noms d'hotes, des montages de fs
- les sessions utilisateurs et gère les ressources des utilisateurs avec les cgroups
- gère les machines virtuelles et conteneurs avec les cgroups et libvirt

Systemd se base sur une notions d'unités.

Ces units ont un type et un nom :

- type service : gestion démons
- type target :
- type mount : gestion des systèmes de fichiers
- type snapshot : permet de sauvegarder et restaurer l'état des services

Quelques commandes :

- lister les services
 - ◇ #systemctl list-units -t service
- activer un service au démarrage
 - ◇ #systemctl enable NetworkManager.service
- désactiver un service au démarrage
 - ◇ #systemctl disable NetworkManager.service

Gestion des cibles (target)

Une target est un runlevel

- changer de niveau de cible temporairement
 - ◇ #Systemd isolate rescue.target*
- obtenir le niveau de fonctionnement par défaut
 - ◇ #systemctl get-default
- Modifier le niveau de fonctionnement par défaut
 - ◇ #systemctl set-default graphical.target

Gestion d'un service avec Systemd

Les fichiers de configurations

- /lib/systemd/system
 - ◇ contient tous les services à démarrer
- /etc/systemd/system
 - ◇ contient la configuration de systemd
- /etc/systemd/user
 - ◇ endroit des services à ajouter par l'admin

Créer un service Systemd

- #cat /usr/lib/systemd/system/notre_service.service
 - ◇ [Unit]
 - Description=Notre service echo daemon
 - After=network.target

```
[Service]
Type=oneshot
ExecStart=/usr/sbin/srv_ludo
ExecStop=/no,/kill -KILL $MAINPID
KillMode=process
```

```
[Install]
WantedBy=multi-user.target
◇ #systemctl enable notre_service.service
```


Installation et Configuration de Microsoft Windows Server 2012

Savoir se Présenter, les Nouvelles Compétences Acquises

PowerShell

L'Ingenieurie DevOps sur Amazon Web Services

Puppet

Tips

Divers

Cours DevOps

- <https://ibmcloud.developpez.com/cours/devops-pour-nuls/>
- <https://www.developpez.net/forums/d1557231/general-developpement/alm/cours-devops-nuls/>

Shell

- `\n` : retour à la ligne
- `\t` : tabulation horizontale
- `\v` : tabulation verticales
- `dirname $HOME/Exos/C2_3.sh` : renvoie le chemin (repertoire sans nom de fichier)
- `basename $HOME/Exos/C2_3.sh` : renvoie le nom du fichier

Linux

- <https://linux.goffinet.org/06-03-processus-linux/>

Red Hat System

- site avec informations pour linux
 - ◇ <http://jean-luc.massat.perso.luminy.univ-amu.fr/ens/admunix/cours-linux/Welcome.html>
- DNS
 - ◇ <https://www.lecoindesdocs.fr/2016/07/21/installation-et-configuration-dun-serveur-dns-bind-centos-7-2/>
 - ◇ ocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-centos-7

Firewall et netfilter

- <http://olivieraj.free.fr/>

Systemd

- <http://lea-linux.org/documentations/Systemd>