TP d'administration Unix Solaris 9

Ronan.Keryell@enst-bretagne.fr
—
Département Informatique
École Nationale Supérieure des Télécommunications de Bretagne
—
Formation Continue

8–10 octobre 2003

Résumé

Ce TP propose quelques tâches d'administration sur Solaris agrémentant et mettant en application le cours disponible à : http://www.lit.enstb.org/~keryell/cours/ENSTBr/FC/Administration_Unix/.

Ce TP étant fait soit sur Sun, soit sur PC, certains points peuvent ne pas avoir d'objet.

Notre bac à sable est constitué des machines suivantes : angus, archimede, cramer, fresnel, huygens, leibniz, llyr, tantale dans le domaine enst-bretagne.fr et il s'agit en l'occurrence pour cette session de Sun Ultra/5.

1 Environnement utilisateur

1.1 Analyse

Examiner ses fichiers de configuration.

Examiner ses variables d'environnement. Tracer leur provenance.

Changer de fuseau horaire et même de langue pour se croire en vacances.

1.2 Construire un environnement configurable

Si on avait le temps...

Créer un environnement maximaliste pour les utilisateurs, pour bash et tcsh, qui prenne en compte tous les répertoires contenant des applications. On rendra le système configurable par un mécanisme de « SETUP ». Par exemple son .bashrc ou son .cshrc pourra contenir :

```
SETUP STANDARD
SETUP GNU
SETUP BSD
SETUP LATEX
SETUP JAVA2
```

SETUP tout court donnera à l'utilisateur curieux ce qui est disponible sur le système avec la liste des choix possibles et leur explication.

Conseils de réalisation possibles :

- créer un fichier `SETUP.csh` et `SETUP.sh` qui contiendront les définitions nécessaires à ce mécanisme. Chaque fichier de configuration utilisateur lira un de ces fichiers avant d'utiliser les `SETUP` ;
- il faudra éviter de rajouter plusieurs fois la même chose dans une variable (du style dans le `PATH`,...). Cela permettra de gérer simplement les religions en mettant par exemple `SETUP BSD` avant `SETUP STANDARD` pour les fans de BSD même si `/usr/ucb` est rajouté dans le `PATH` par ces 2 `SETUP` ;
- chaque `SETUP` *x* sera traduit par une lecture (et exécution) d'un fichier `SETUP.`*x* que l'on mettrait à terme par exemple dans `/usr/local/share/conf/SETUP/` ;
- on isolera les primitives portables au sens `sh` et `csh` utiles pour faire ce genre de mécanisme que l'on implémentera sous forme de fonction (`sh`) ou alias (`csh`) :
  - `SETUP_PREPEND_VAR` *variable valeur* rajoutera la *valeur* au début de la *variable* ;
  - `SETUP_APPEND_VAR` *variable valeur* rajoutera la *valeur* à la fin de la *variable* ;
  - `SETUP_PREPEND_PATHVAR` *variable valeur* et `SETUP_APPEND_PATHVAR` *variable valeur* auront le même effet si ce n'est que la *variable* sera interprétée comme une liste de valeurs séparées par des « `:` » et que la *valeur* ne sera rajoutée que si elle n'était pas déjà présente dans la variable. Typiquement pour gérer `PATH`, `MANPATH`, `LD_LIBRARY_PATH`,...
- pour faire des choses très spécifiques on définira aussi des gardes du style :
  - `SETUP_SH_ONLY_BEGIN` et `SETUP_SH_ONLY_END` chacun sur une ligne délimiteront une zone à n'exécuter que si on est sous un shell de style `sh` ;
  - `SETUP_CSH_ONLY_BEGIN` et `SETUP_CSH_ONLY_END` chacun sur une ligne délimiteront une zone à n'exécuter que si on est sous un shell de style `csh`.

2 Gestion du démarrage

Rajouter des messages vantant les mérites de son organisation lors du démarrage.

Faire un `shutdown` propre pour éteindre la machine.

Redémarrer la machine en mode `single-user`. Pourquoi est-ce que cela ne marche pas ?

Continuer en mode multi-utilisateur.

Afficher la configuration de l'`eeprom`.

Corriger et recommencer.

3 Installation de logiciels

Installer le système de gestion de paquets `pkg-get` et l'utiliser pour installer des logiciels de votre choix.

4 Utilisateurs et groupes

4.1 Création

Visualiser la liste des utilisateurs définis sur sa machine. En faire de même avec les groupes.

Pourquoi ne vous voyez-vous pas ?

Créer un nouvel utilisateur.

Créer un groupe de projet `cao` local à sa machine pour son projet et mettre tous les membres du projet dedans (groupe secondaire). Tester le fonctionnement de manière progressive :

- créer sous `root` le répertoire où travailleront tous les membres du projet :
  ```
  mkdir -p /projet/cao
  cd /projet/cao
  ls -al
  ```
- le groupe `cao` en devient le propriétaire :
  ```
  chgrp cao .
  ls -al
  ```
- essayer de créer un fichier en tant qu'utilisateur du groupe
  ```
  touch a
  ```
- donner en tant que `root` le droit d'écriture au groupe avec
  ```
  chmod g+w .
  ```
- tester en tant qu'utilisateur du groupe :
  ```
  touch a
  mkdir b
  ls -al
  ```
  est-il possible de travailler en équipe (que les autres du groupe puissent modifier ces fichiers) ?
- en tant que `root` donner la sémantique « BSD » au répertoire :
  ```
  chmod g+s .
  ```
- en tant qu'utilisateur du groupe :
  ```
  touch c
  mkdir d
  ls -al
  ```
  alors ?
- mettre un `umask` altruiste et recommencer :
  ```
  umask 2
  touch e
  mkdir f
  ls -al
  ```

4.2 Access Control Lists

Refaire la même chose en rajoutant des accès pour certains utilisateurs avec les ACL.

En particulier on utilisera la définition de valeurs par défaut pour que les répertoires et fichiers créés aient les bons droits automatiquement.

4.3 Tests de robustesse de mots de passe

Les plus bidouilleurs pourront essayer de craquer les mots de passe avec des outils *ad-hoc* (`crack`, *John the Ripper*...) afin d'éliminer les mots de passe trop faibles avant qu'un pirate ne le fasse, comme indiqué dans le cours/TP de sécurité[1].

5 Réseau

5.1 Configuration

Étudier la configuration réseau du système.

Regarder avec `traceroute` le trajet suivi par des paquets vers un site local et distant.

Supprimer la route par défaut et recommencer.

Quels sont les services qui tournent sur la machine ?

Quelles sont les connexions réseaux établies ? Et celles en attentes de connexion ?

5.2 Protocoles sécurisés ou non ?

Tracer verbeusement les paquets d'une connections `telnet` ou `rsh`.

Comparer à une connexion `ssh`.

6 NIS

Déclarer sa machine comme serveur NIS de conserve avec un collègue qui deviendra le client de votre serveur NIS.

Devenez le serveur esclave (secondaire) d'un serveur NIS d'un collègue.

Changez le mot de passe sur le client et comprendre comment cela se propage sur le serveur.

Regarder la liste des tables NIS distribuées dans le `/var/yp/Makefile` du serveur NIS.

Rajouter une nouvelle table `truc` qui exportera les valeurs de votre `/etc/truc`.

7 Sécurité

7.1 RBAC

Créer des rôles et des profils pour pouvoir mettre la date à jour et contrôler l'imprimante sans devoir être `root`.

7.2 Sécurisation

Récupérer les patches du jour et les installer.

Mettre en place une procédure qui télécharge les patches et, s'ils sont plus récents que ceux déjà installés, les installe.

Tester un trou de sécurité[2]. Essayer de mettre la pile non exécutable.

Effondrer la machine d'un collègue et essayer de se défendre.

[1] `http://www.lit.enstb.org/~keryell/cours/Mines/Securite`

[2] Diffi cile d'en trouver avec un système d'exploitation tout neuf !

8 Périphériques et disques

Étudier la configuration courante du système avec les commandes `dmesg`, `prtconf` et `sysdef`.

Sur PC Les hackers regarderont si la carte son du PC est utilisable et si ce n'est pas le cas la feront marcher...

Étudier le disque dur avec `format` et `fdisk` (*sur* PC).

Sur PC On devrait pouvoir étendre la partition Solaris actuelle mais il semble que certaines machines ont une partition PC NT-FS juste derrière rajoutée pour des TPs avec NT...

Étudier les montages actuels.

Sur PC Modifier `/etc/vfstab` pour avoir la partition de Windows98 dans `/windows`. Trouver le moyen pour la monter en évitant de rebooter.

Essayer de faire un crash système alors que vous êtes en train de créer et d'effacer plein de fichiers dans un répertoire de `var/tmp`) à supposer ne pas utiliser la journalisarion. Au reboot, aller voir dans `/usr/lost+found`. Rajouter la journalisation de tous les systèmes UFS et recommencer.

Faire une sauvegarde de son compte dans un fichier dans `/tmp` (pas dans son propre compte... Pourquoi ?). Quel devrait être les droits du fichier de sauvegarde pour assurer la protection des fichiers utilisateur ?

9 NFS

Étudier les montages NFS du TP.

Exporter une hiérarchie locale de votre machine aux autres machines du TP.

Exporter la partition Windows aux membres du TP et vérifier l'accès distant dans `/net/`*`machine`*`/windows`.

Mettre en place l'utilisation de l'automonteur avec les hiérarchies suivantes :

`/disk/`*`m`*`/`*`d`*`: contient le disque utilisateur *d* de la machine *m* ;

`/net`: permet d'avoir dans `/net/`*`m`* tous les fichiers exportés par la machine *m* ;

`/project/`*`p`*: accède au répertoire du projet *p* ;

`/users/`*`s`*`/`*`u`*: contient le répertoire maison de l'utilisateur *u* qui appartient au service *s*.

10 Média amovibles

Si vous avez un lecteur de CD-ROM, Lire un CD-ROM. Exporter le CD-ROM à toute la promotion.

Si vous avez un lecteur de disquette, formater une disquette au format PC et sauvegarder des données dessus. Les relire.

Trouver un moyen astucieux et rapide de dupliquer une disquette (par exemple la disquette de démarrage de Solaris).

11 Imprimantes

Étudier la configuration actuelle des imprimantes du TP.

Configurer d'autres imprimantes.

12 Installation

On pourra faire cette partie du TP en début de cours afin de recouvrir le temps d'installation par le temps de l'exposé et en utilisant une autre machine.

Tester une installation de type WebStart ou `suninstall` depuis le réseau (sur PC en préservant les partitions Windows NT et Windows98 pour gagner du temps en interrompant le démarrage de Solaris avec la touche <ESC>).

Tester une installation de type JumpStart automatique depuis le réseau.

13 La suite...

Logiquement il faudrait enchaîner avec le cours de sécurité :
`http://www.lit.enstb.org/~keryell/cours/Mines/Securite`