Université de Bretagne Occidentale

Administration des systèmes d'exploitation

Gestion centralisée des postes de travail

Cours 2

Hai Nam TRAN
Université de Bretagne Occidentale – M1 Informatique

Devoir 2

- **Proposer une solution de gestion centralisée en utilisant NFS + NIS**
  - **Il y a 1 server et 100 clients (nommés client1 → client100)**
  - **Dans votre solution, préciser les détails ci-dessous**
    - Les configuration à effectuer côté server/client
      - Fichiers à configurer + les configurations à réaliser
      - Réseau, NFS, NIS
    - Où sauvegarder les dossiers et les applications partagés ?
    - Comment configurer le montage côté client ?
    - Comment configurer l'authentification côté server/client ?
    - Comment gérer le dossier "home" de chaque client ?

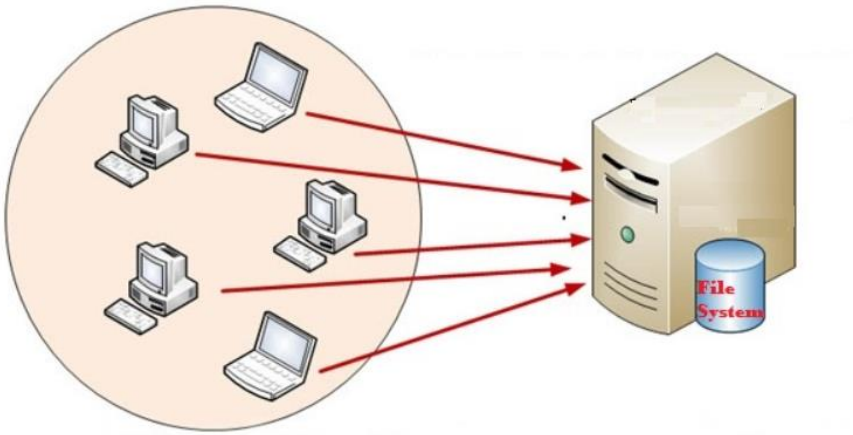
Devoir 2
Date limite : 03/02 23:59
Zone de dépôt : Moodle

Plan

- Introduction
- Configuration - Introduction aux scripts BASH
- Configuration réseau
- **Accès distant aux ressources de stockage**
- **Infrastructure d’annuaires**
  - **Notion d'annuaires informatiques**
  - **Network Information System (NIS)**
  - **Domain Name Server (DNS)**
  - **OpenLDAP, Active Directory**
  - **Sélection du service d'annuaires**

Montage de systèmes de fichiers distants

- **Il est possible de rendre accessible, sur une machine donnée, un système de fichiers géré par une autre machine (sur laquelle le matériel de stockage est installé)**
  - **Exemple : vador/vador-fs à l'UBO**
- **Le montage de fichiers distants permet**
  - **La mise en place de serveurs de fichiers et d'exécutables**
  - **De centraliser leur installation et leur administration**



Montage de systèmes de fichiers distants

- **Pour les OS Windows**
  - **ClFS (Common Internet File System) ou SMB (Server Message Block), est un protocole pour le partage de fichiers**
  - **Samba est un serveur SMB pour les système Linux**
- **Pour les OS UNIX**
  - **Le protocole le plus utilisé est NFS (Network File System), créé par Sun Microsystems**
  - **NFS s'appuie sur le modèle des RPC (Remote Procedure Call).**

Rappel : **RPC** (remote procedure call) est un protocole réseau permettant de faire des appels de procédures sur un ordinateur distant à l'aide d'un serveur d'applications

Montage de systèmes de fichiers distants

- **Opérations à effectuer (NFS)**
  - **Au niveau du serveur**
    - Autorisation de montage distant d'une sous-arborescence de répertoires (export ou partage), depuis une machine cliente
      - systemctl enable nfs-server
      - systemctl start nfs-server
      - systemctl : contrôle le système systemd et le service manager
    - L'arborescence exportée doit être accessible (montée) localement sur le serveur
    - Configurer /etc/exports. Le fichier /etc/exports permet de contrôler les systèmes de fichiers spécifiques qui sont exportés vers des hôtes distants, et de spécifier des options

```
<export> <host1>(<options>) <hostN>(<options>)...
```

      - http://www.linux-france.org/article/man-fr/man5/exports-5.html

Projet : **TP3, TP4**

Montage de systèmes de fichiers distants

- **Opérations à effectuer (NFS)**
  - **Au niveau du serveur**
    - /etc/export d'exemple

```
# fichier       /etc/exports d'exemple
/               maître(rw) confiance(rw,no_root_squash)
/projects       proj*.local.domain(rw)
/usr            *.local.domain(ro) @trusted(rw)
/home/joe       pc001(rw,all_squash,anonuid=150,anongid=100)
/pub            (ro,insecure,all_squash)
```

Montage de systèmes de fichiers distants

- **Options**
  - **secure** : requires that requests originate on an Internet port less than IPPORT_RESERVED (1024)
  - **rw** : allow both read and write requests
  - **ro** : allow only read requests
  - **async** : reply to requests before any changes made by that request have been committed to stable storage
  - **sync** : reply to requests only after the changes have been committed to stable storage
  - **no_subtree_check** : If a subdirectory of a filesystem is exported, but the whole filesystem isn't then whenever a NFS request arrives, the server must check not only that the accessed file is in the appropriate filesystem (which is easy) but also that it is in the exported tree (which is harder). This check is called the *subtree_check*
  - **root_squash** : map requests from uid/gid 0 to the anonymous uid/gid
  - **no_root_squash** : turn off root squashing

Montage de systèmes de fichiers distants

- **Opérations à effectuer (NFS)**
  - **Au niveau des clients**
    - Montage d'une arborescence exportée par un serveur
      - Commande mount

```
sudo mount serveur:/export/home /home/mount/serveur
```

      - Configurer /etc/fstab

```
serveur:/export/home /home/mount/serveur nfs hard,rw 0 0
```

    - Identification : nomserveur:/rep_racine
    - Type système de fichiers : nfs
    - Un fois monté, un système de fichiers distant est vu comme une partition locale dans l'arborescence de la machine cliente
  - **Résumé**

1. Start NFS Server

2. Configurer /etc/exports

3. Configurer /etc/fstab

Les démons NFS (et RPC)

- **NFS fonctionne grâce à plusieurs démons**
  - **rpc.nfsd (serveur) traite les requêtes d'accès aux fichiers des clients**
  - **rpc.mountd (serveur) traite les requêtes de montage des clients**
  - **rpc.lockd, rpc.statd (serveur, client) gère les verrous sur les fichiers**
  - **rpc.rquotad (serveur) gère les quotas**
  - **rpcbind (verseur) enregistre et communique les numéros de port RPC**

NFS : caractéristiques

- **NFS est transparent pour les applications grâce à la couche d'abstraction VFS (Virtual File System)**
  - **Accès identique aux fichiers locaux et distants**
  - **Abstraction du système de fichiers et de l'OS utilisés coté serveur**
  - **Le protocole NFS est dit « sans état » (stateless)**
- **Le serveur ne maintient pas d'informations qui décrivent l'état de ses clients**
  - **Le client est responsable de la gestion de son état vis-à-vis du système de fichiers**
  - **Les requêtes NFS sont indépendantes**

NFS : caractéristiques

- **Les communications par le réseau peuvent être non fiables (protocole User Datagram Protocol - UDP)**
  - **Les requêtes peuvent être retransmises en cas d'absence d'acquittement -> nécessité de garantir l'idempotence des requêtes**
  - **UDP est un protocole orienté « non connexion »**
    - Une machine A envoie des paquets à destination d'une machine B, ce flux est unidirectionnel
    - La transmission des données se fait sans prévenir le destinataire (machine B)
    - Le destinataire reçoit les données sans effectuer d'accusé de réception vers l'émetteur (machine A)
  - **TCP est orienté « connexion »**
    - Une machine A envoie des données vers une machine B, la machine B est prévenue de l'arrivée des données, et témoigne de la bonne réception de ces données par un accusé de réception

NFS : locks (verrous)

- **Une exclusion mutuelle est nécessaire lors de l'accès à certains fichiers**
- **Utilisation de verrous**
  - **La gestion des verrous est effectuée au niveau du serveur (protocole Network Lock Management - NLM)**
  - **Gestion des verrous en cas d'arrêt**
    - En cas d'arrêt temporaire du serveur, les clients doivent obtenir à nouveau leurs verrous : période de « grâce » après le démarrage du serveur où uniquement des verrous posés précédemment sont acceptés
    - En cas d'arrêt temporairement d'un client, ses verrous sont libérés au redémarrage de celui-ci
    - En cas d'arrêt permanent d'un client, ses verrous restent posés →intervention de l'administrateur ou redémarrage du serveur

NFS : problème de permissions

- **Origine du problème : les autorisations de montage d'un répertoire sont fondées sur l'identité de la machine cliente**
- **Après le montage, la machine cliente vérifie les permissions des utilisateurs selon sa propre politique**
  - **Nécessité de disposer des mêmes UID/GID pour tous les clients (et le serveur)**
  - **Les fichiers appartenant à root doivent être réattribués à un utilisateur anonyme nobody (fait par défaut)**

Auto-montage

- **Définition : montage à la demande d'une arborescence**
  - **Réduire le nombre de montages actifs mais non utilisés**
  - **Le montage a lieu lors de la première accès à l'arborescence**
  - **Le démontage est effectué après une période d'inactivité de l'arborescence**
- **Sous Linux, le montage à la volée (ou auto-montage) est apporté par le paquetage autofs**
  - **Le démon automount doit être démarré pour gérer les auto-montages.**
  - **Il est configuré par le fichier /etc/auto.master**
    - Indique les répertoires racines des points de montage et les fichiers qui définissent ces montages (appelés cartes)

NFS version 4

- **Évolution du service NFS version 3**
  - **Protocole avec état sur TCP**
  - **Permet de rassembler les différents protocoles utilisées par NFSv3 en un seul démon rpc.nfsd au lieu de 4 démons**
  - **Sémantique des verrous amélioré**
  - **Augmentation de la sécurité**
    - Processus d'authentification Kerberos supporté
    - Les autorisations d'accès ne sont plus uniquement fondées sur l'adresse IP des clients, mais sur les utilisateurs
    - Un nouveau démon (rpc.idmapd) établit une correspondance entre les noms NFSv4 (utilisateur@domaine) et les UID et GID locaux
- **Remarque : les apports de NFS v4 par rapport à la version précédente, résident plus dans la sécurisation que dans l'amélioration des performances**

Université de Bretagne Occidentale

Administration des systèmes d'exploitation

Gestion centralisée des postes de travail

Quiz 1

Hai Nam TRAN
Université de Bretagne Occidentale – M1 Informatique

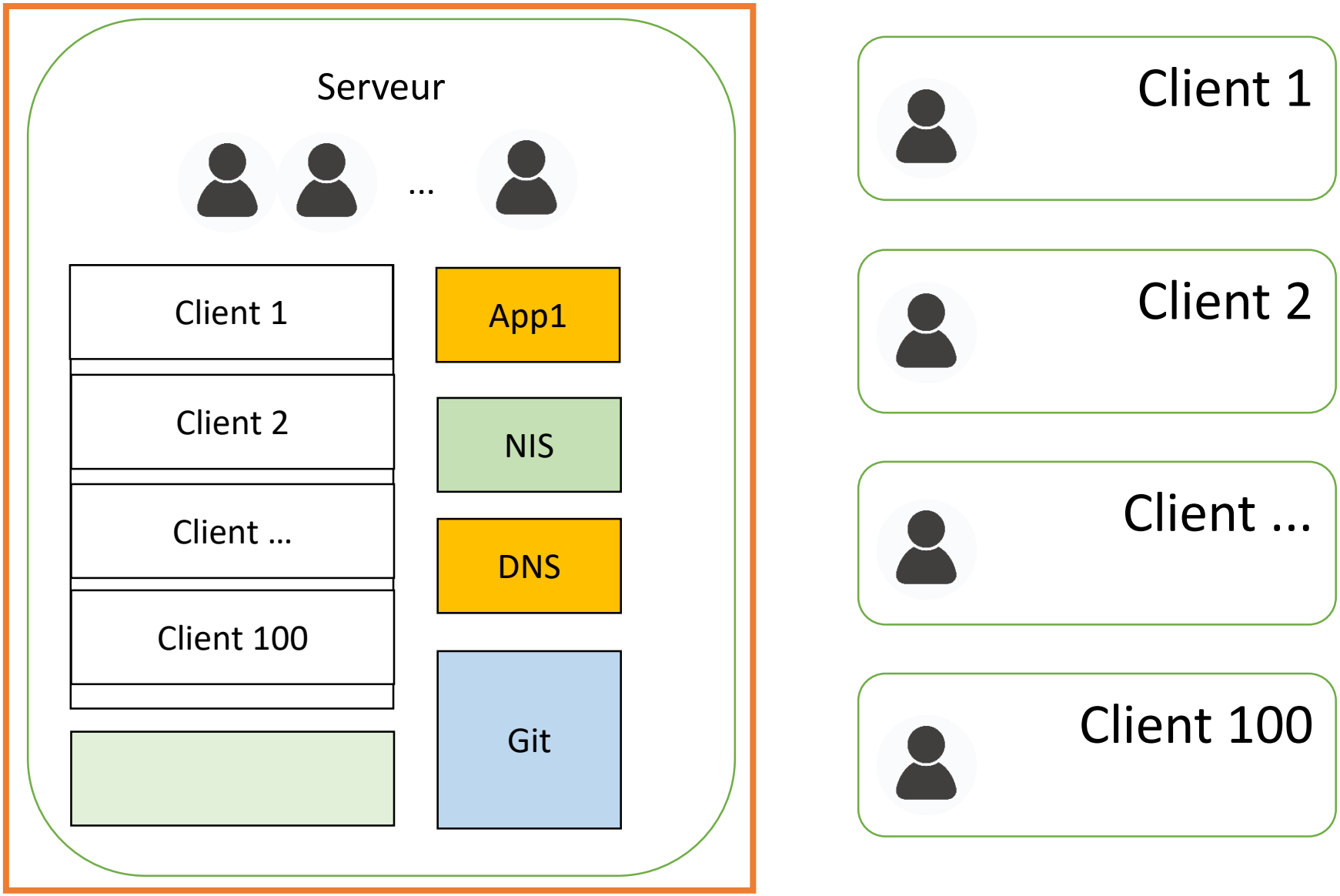
Quiz

- **Q1 : NFS est l'acronyme de**
  - A. Need For Speed
  - B. Network File System
  - C. Network File Service
  - D. Numération Formule Sanguine
- **Q2 : Quel est le nom du paquetage apportant le auto-montage**
  - A. automount
  - B. autofs
  - C. autonfs
  - D. getnfs
- **Q3 : Il y a combien version de NFS**
  - 1
  - 2
  - 3
  - 4

Quiz

- **Q4 : Sous Linux, quelle commande affiche la configuration des interfaces réseaux ?**
  - **A. ipconfig**
  - **B. netipcfg**
  - **C. ifconfig**
  - **D. networkedit**
- **Q5 : Pour afficher une ligne de texte dans le terminal, on utilise quelle commande ?**
  - **A. echo**
  - **B. display**
  - **C. write**
  - **D. printf**

Projet


Serveur
...
Client 1
Client 2
Client ...
Client 100
App1
NIS
DNS
Git
Client 1
Client 2
Client ...
Client 100

Projet

- **Comment les projets sont-ils notés**
  - **Scripts : 25%**
    - set_[abc] : 10%
    - verify_[abc] : 15%
  - **Presentation (TP6) : 25%**
  - **CR : 50%**
    - Descriptions de vos scripts, manuel d'utilisation
    - Réponses aux questions marquées "CR"

Examen (documents non autorisés)

- **Questions théoriques**
  - **Exemple : Donner la définition du terme « client légers ». Citer 3 intérêts et 3 inconvénients du modèle client-serveur.**
- **Questions pratiques**
  - **Exemple : Expliquer le plus précisément possible la configuration donnée dans les 2 fichiers ci-dessous :**

Machine serveur - Fichier: /etc/exports
/export/opt client(ro) /export/opt esclave(ro) /export/home client(rw,no_root_squash) /export/home esclave(rw,no_root_squash)
Machine client - Fichier: /etc/fstab
serveur:/export/home /home/serveur nfs hard,rw 0 0 serveur:/export/opt /opt nfs soft,ro 0 0

- **QCM**
  - **(1 point)**

Plan

- Introduction
- Configuration - Introduction aux scripts BASH
- Accès distant aux ressources de stockage
- Configuration réseau
- **Infrastructure d’annuaires**
  - **Notion d'annuaires informatiques**
  - **Network Information System (NIS)**
  - **Domain Name Server (DNS)**
  - **OpenLDAP, Active Directory**
  - **Sélection du service d'annuaires**
- **Outils de travail collaboratif**

Configuration des postes de travail : besoins

- **La configuration des systèmes d'exploitation s'appuie sur un ensemble de fichiers**
  - **Ces fichiers constituent de petites bases de données. Les enregistrements sont organisés sous forme de lignes de texte. Ils sont sélectionnés par un clef de recherche s'appliquant sur un champ dans la ligne**
- **Exemples sous Unix :**
  - **/etc/passwd**
  - **/etc/group**
  - **/etc/protocols**
  - **/etc/netgroup**
  - **/etc/services**

Maintenance des fichiers de configuration

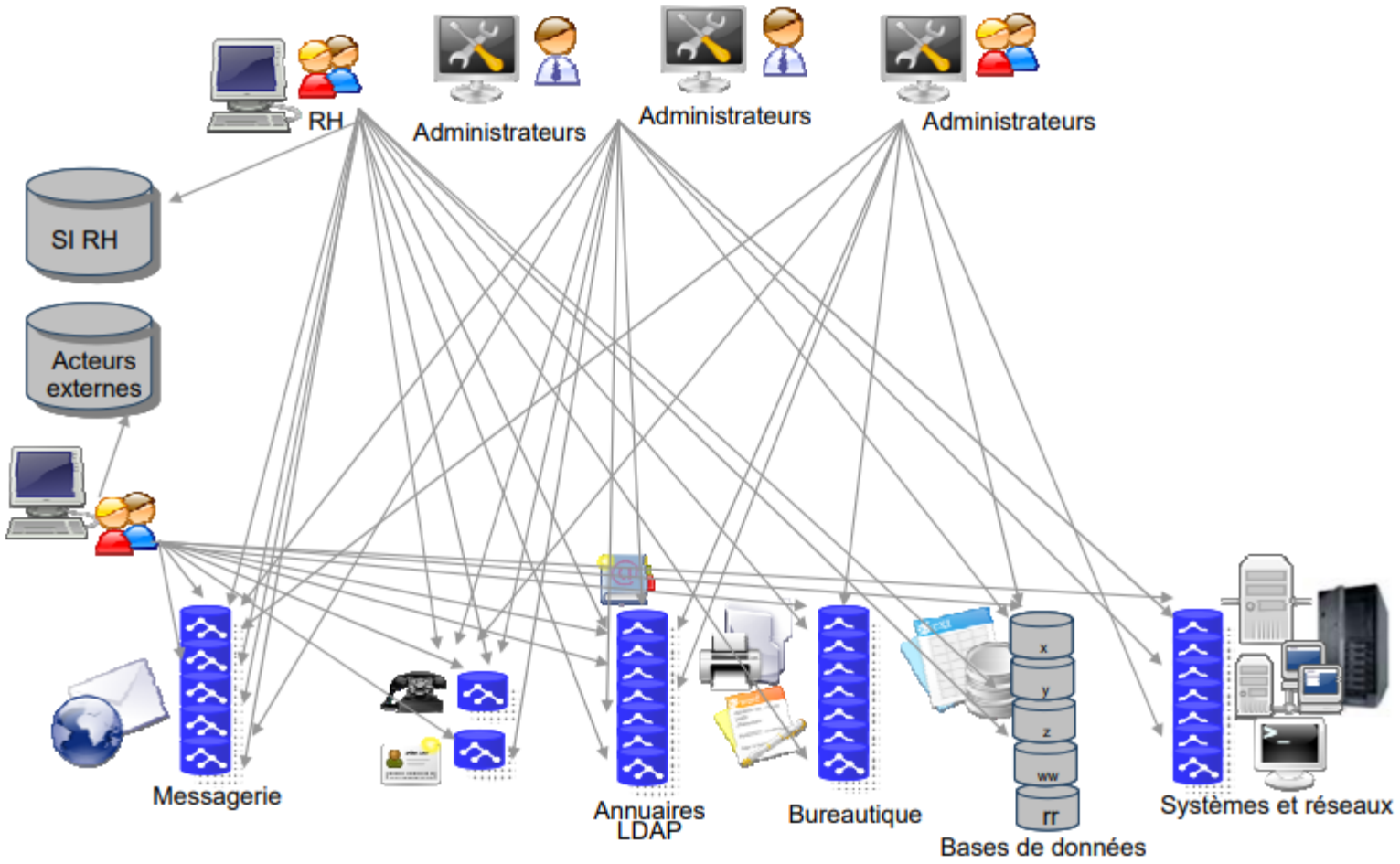
- **La configuration des systèmes d'exploitation s'appuie sur un ensemble de fichiers**
  - **La création de ces fichiers et leur maintenance constitue l'un des taches importantes de l'administrateur système**
  - **Au sein d'un site, pour une classe d'ordinateurs donnée, les configurations sont souvent identiques**
  - **Nécessité d'automatiser les opérations de maintenance de ces fichiers pour gagner du temps et garantir la cohérence des configurations**

Infrastructure d'annuaires

Exemple : gestion des identités

- **Gestion des identités et des droits d'accès (Identity and Access Management IAM)**
  - **Attribution des droits d'accès aux ressources d'un système informatique**
  - **Traçabilité des accès (exigences réglementaires)**
- **Gestion du « cycle de vie » des personnes dans l'entreprise : embauche, départ, promotion, rôle**
- **Éventuellement, la gestion fonctionnelle des identités peut être prise en charge par des « non informaticiens » (RH par exemple)**

Gestion « distribuée »

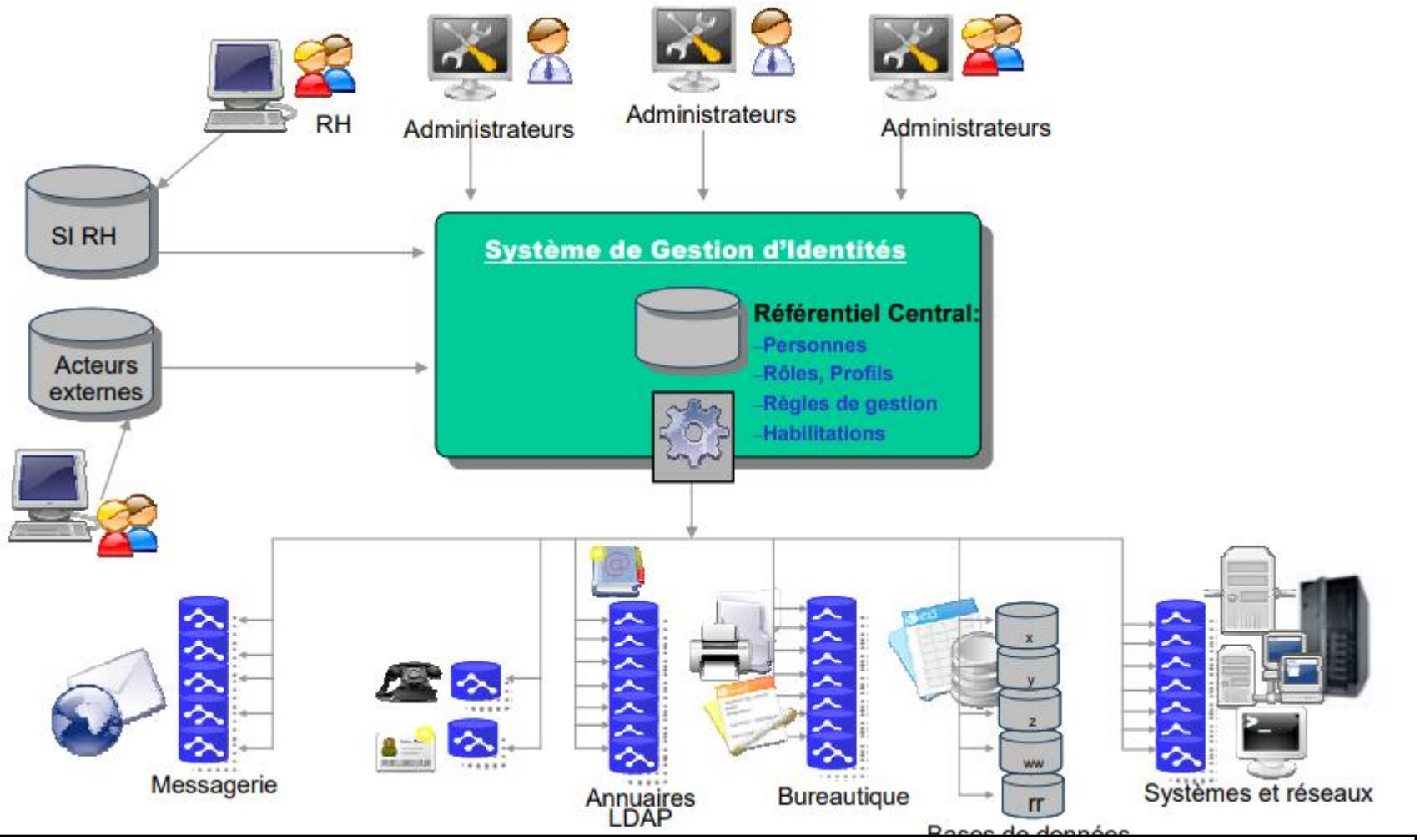


Gestion des identités, rapport Clusif, 2007

Gestion « distribuée »

- **Un nouvel employé doit être référencé :**
  - **Dans le système de gestion de la paie**
  - **Dans la base du service logistique (bureau, courrier)**
  - **Dans la base téléphonique**
  - **Dans le système bureautique (ordinateur, identifiant, mot de passe)**
  - **Dans le système de gestion des badges**
  - **Dans la base du restaurant d'entreprise**
  - **Dans les bases d'accès des applications**
  - **...**

Gestion « centralisée »



Gestion des identités, rapport Clusif, 2007

Gestion « centralisée »

- **Des économies d'échelle**
  - **La centralisation offre des possibilités de concentration et de mutualisation de ressources**
    - Ressources humaines (administrateurs, techniciens),
    - Matérielles (salles normées, climatisation, protection incendie, sécurité physique, éléments de redondance…)
- **Une information exhaustive et pertinente**
  - **Faciliter l'indexation des contenus et donc augmenter la pertinence des résultats de recherche**
- **Accessibilité et sécurité simplifiées (?)**
  - **La définition des politiques de sécurité (dont les droits d'accès) est simplifiée**
- **L'unicité de l'information**

Annuaires informatiques

- **Un annuaire informatique est un système de stockage de données, éventuellement hiérarchique**
  - **Enregistrement de données pérennes (c'est à dire relativement stables)**
  - **Optimisé pour les opérations d'accès en lecture, prédominantes par rapport à celles d'écriture**
- **Enregistrements constitués par des attributs, normalement de petites tailles**

Annuaires informatiques

- **Recherche dans l'annuaire à partir**
  - **d'une clef définissant la valeur des attributs**
  - **d'une position dans la hiérarchie de l'annuaire**
- **Publication à grande échelle d'un ensemble d'informations nécessaires pour le fonctionnement d'un système d'information**
- **La maintenance de cette base est centralisée en un lieu unique**
  - **Cohérence des informations diffusées**

Plan

- Introduction
- Configuration - Introduction aux scripts BASH
- Accès distant aux ressources de stockage
- Configuration réseau
- Infrastructure d’annuaires
  - Notion d'annuaires informatiques
  - **Network Information System (NIS)**
  - **Domain Name Server (DNS)**
  - **OpenLDAP, Active Directory**
  - **Sélection du service d'annuaires**
- **Outils de travail collaboratif**

Service NIS (Network Information System)

- **Service permettant la diffusion, sur un réseau de machines, d'une base de données d'informations de configuration. Il permet une centralisation des activités d'administration de ce réseau**
  - **Distribuer les informations contenues dans des fichiers de configuration contenant par exemple les comptes utilisateurs (/etc/passwd), etc. sur un réseau**
- **Créé par Sun Microsystems en 1986, sous le nom originel de “yellow pages”**

Filename
/etc/passwd
/etc/group
/etc/hosts
/etc/services
/etc/protocols
/etc/mail/aliases
/etc/rpc
/etc/printcap
/etc/termcap

Fichier : /etc/passwd

- **Passwd est un fichier de texte qui contient la liste des comptes sur le système**

```
account:passwd:UID:GID:GECOS:directory:shell
```

  - **account : Le nom que l'utilisateur utilisera pour se connecter, il ne devrait normalement pas contenir de majuscules**
  - **passwd : La représentation encryptée (optionnelle) du mot de passe**
  - **UID : L'ID numérique de l'utilisateur**
  - **GID : L'ID numérique du groupe principal de l'utilisateur**
  - **GECOS : Ce champ est optionnel et n'a qu'un rôle informatif. Il contient généralement le nom complet de l'utilisateur.**
  - **directory : Le répertoire de connexion de l'utilisateur**
  - **shell : Le programme à exécuter après la phase de connexion (par défaut /bin/sh)**

Fichier : /etc/passwd

```
[root@arch01 ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/usr/bin/nologin
daemon:x:2:2:daemon:/:/usr/bin/nologin
mail:x:8:12:mail:/var/spool/mail:/usr/bin/nologin
ftp:x:14:11:ftp:/srv/ftp:/usr/bin/nologin
http:x:33:33:http:/srv/http:/usr/bin/nologin
uuidd:x:68:68:uuidd:/:/usr/bin/nologin
dbus:x:81:81:dbus:/:/usr/bin/nologin
nobody:x:99:99:nobody:/:/usr/bin/nologin
systemd-journal-gateway:x:191:191:systemd-journal-gateway:/:/usr/bin/nologin
systemd-timesync:x:192:192:systemd-timesync:/:/usr/bin/nologin
systemd-network:x:193:193:systemd-network:/:/usr/bin/nologin
systemd-bus-proxy:x:194:194:systemd-bus-proxy:/:/usr/bin/nologin
systemd-resolve:x:195:195:systemd-resolve:/:/usr/bin/nologin
systemd-journal-upload:x:998:998:systemd Journal Upload:/:/sbin/nologin
systemd-journal-remote:x:999:999:systemd Journal Remote:/:/sbin/nologin
avahi:x:84:84:avahi:/:/bin/nologin
polkitd:x:102:102:Policy Kit Daemon:/:/usr/bin/nologin
mbo:x:1000:1000::/home/mbo:/bin/bash
git:x:997:997:git daemon user:/:/bin/bash
michael:x:1001:1001::/home/michael:/bin/bash
                                                    linux-audit.com
```

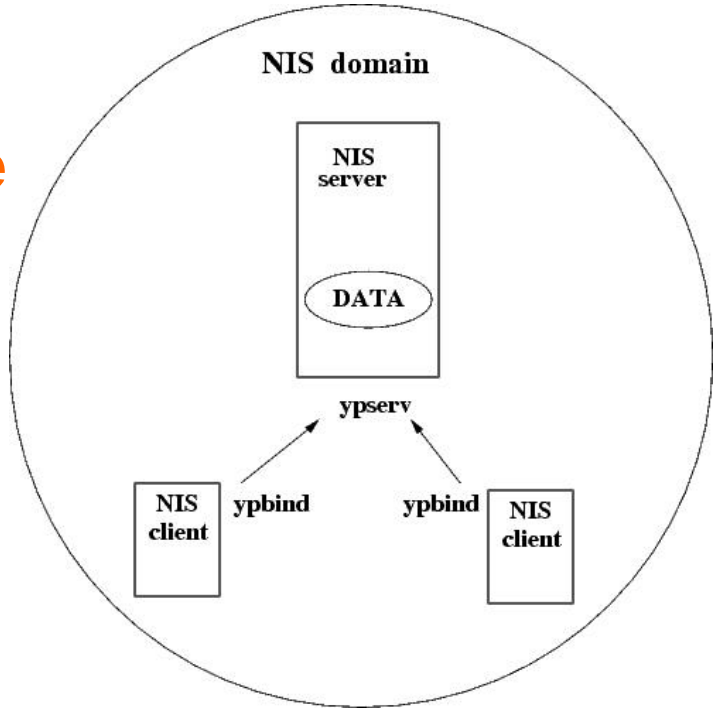
- **Pour la raison de sécurité, Linux a déplacé le mot de passe de l'utilisateur dans un fichier séparé /etc/shadow**

NIS : Maps

- **Les bases de données sont enregistrées dans des fichiers appelés “carte” (map)**
  - **Tout fichier organisé en lignes et champs peut être géré par NIS. Adapté aux systèmes Unix**
  - **Une carte est la représentation d'un fichier sous la forme d'une table indexée par une clef; celle-ci est construite à partir de l'un des champs du fichier**

NIS : Architecture logicielle

- Le service NIS fonctionne en mode client-serveur. Il est bâti sur les RPC (Remote Procedure Call)
- Les machines adhérant au service appartiennent à un domaine NIS
- Chaque domaine comprend :
  - un serveur maître
  - des serveurs esclaves (optionnels)
  - et des clients
- Les clients se lient (binding) aux serveurs selon leur disponibilité.



NIS : Configuration

- **Opérations à effectuer (NIS)**
  - **Au niveau du serveur**
    - Démarrer et activer ypserv
      - `systemctl enable ypserv`
      - `systemctl start ypserv`
    - Créer le sous-répertoire de domaine de /var/yp pour le domaine
      - `$ ./usr/lib64/yp/ypinit`
  - **Au niveau du client**
    - Démarrer et activer ypbind
      - `systemctl enable ypbind`
      - `systemctl start ypbind`
    - Configurer **/etc/nsswitch.conf**
      - Indiquer où le système d'exploitation doit rechercher l'information et dans quel ordre

Plus de détail dans la sujet de TP NIS

Fichier /etc/nsswitch.conf

- **Dans un système intégrant un ou plusieurs services d'annuaires, et des fichiers de configuration locaux :**
  - **Il est nécessaire d'indiquer où le système d'exploitation doit rechercher l'information et dans quel ordre**
- **Sun Microsystem a proposé avec Solaris 2 le service NSS, intégré dans la bibliothèque C, et configuré par le fichier /etc/nsswitch.conf**

Fichier /etc/nsswitch.conf - Exemple

```
passwd:      files nis
shadow:      files nis
group:       files nis
hosts:        dns [!UNAVAIL=return]  files
protocols:   files nis
rpc:         files
services:    nis[NOTFOUND=return] files
netgroup:    files nis
automount:   nis files
aliases:     files nisplus
```

NIS : Architecture logicielle

- **Avantages**
  - **Pas nécessaire de connaître le format de données interne de NIS**
  - **Multi plateforme**
  - **Convient aux petites, moyennes nombres d'utilisateurs**
- **Désavantage**
  - **Consommer le réseau**
  - **Si un serveur NIS esclave est en panne, la copie de l'esclave peut ne pas être mise à jour**
  - **Sécurité : tout le monde peut lire les cartes**