

---

# Annuaire électronique

- Présentation
- Les Besoins
- Gérer un projet
- Sécurité
- État du marché

---

# Annuaire électronique

## Présentation



boutemy.com

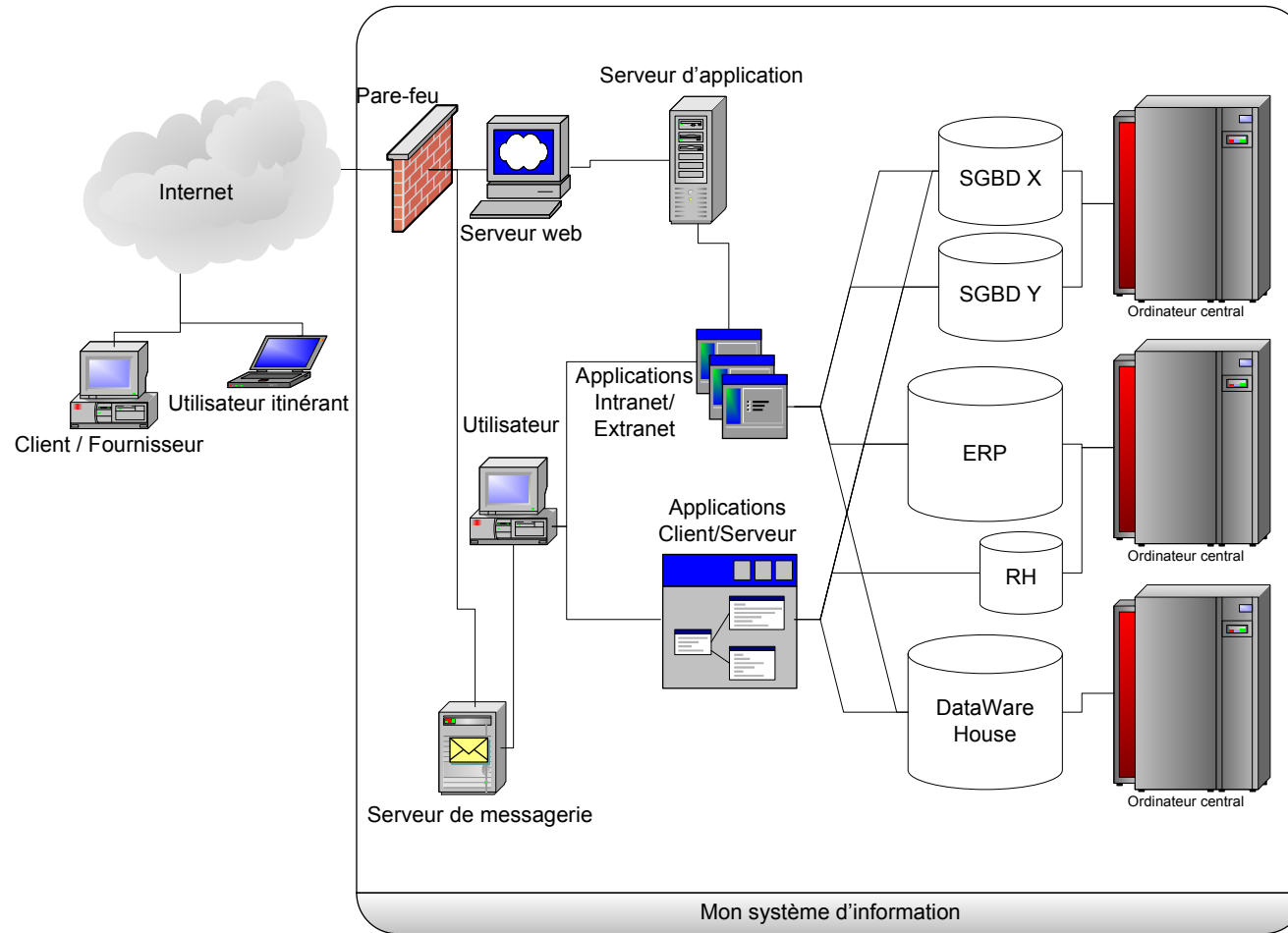


Annuaire LDAP - Sécurité

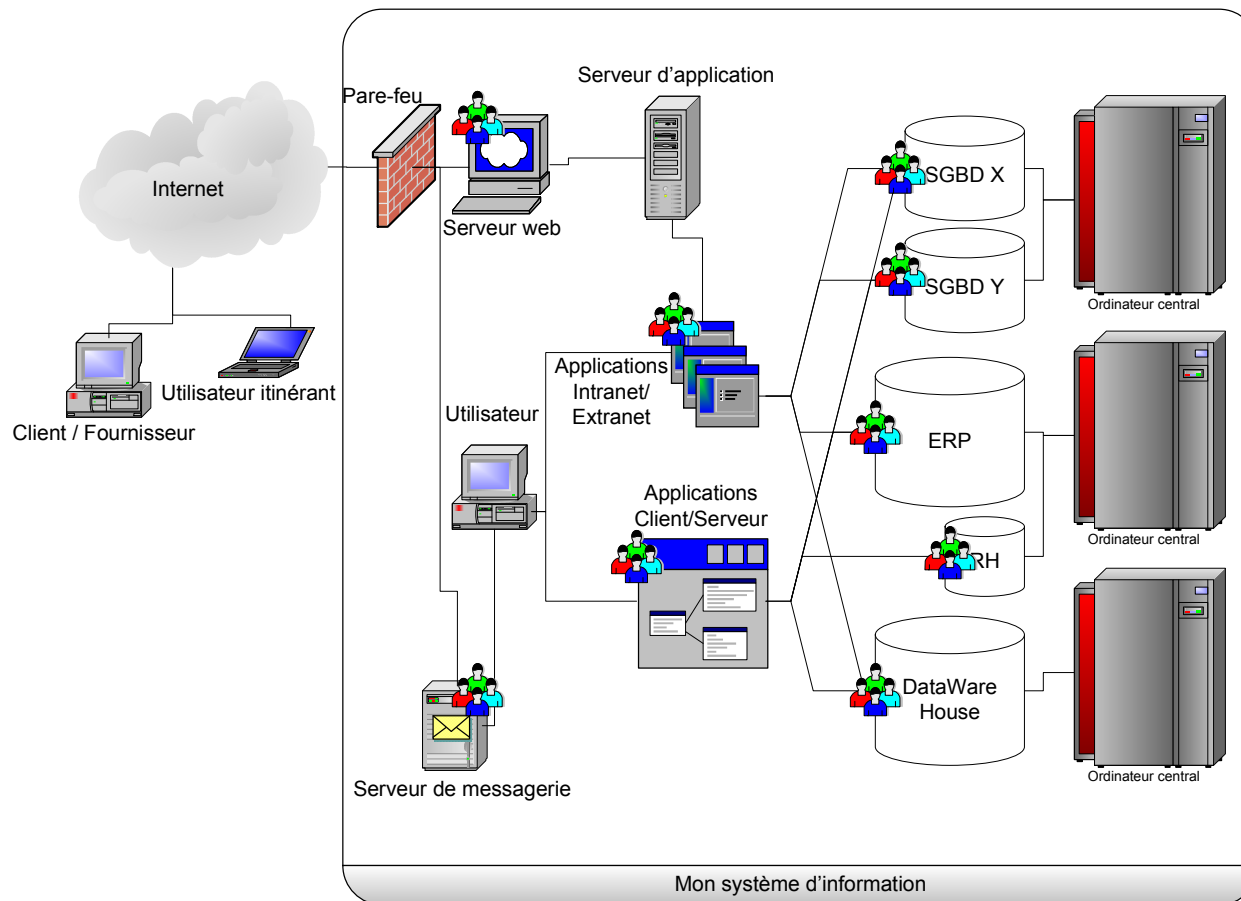
09/12/2003

2

# Aujourd'hui le système d'information



# Les annuaires dans ce SI



# Quelques constats

---

- Chaque application dispose d'un annuaire ou d'une base de données et d'une administration propre
- Chaque application dispose de sa propre gestion des utilisateurs
- Un besoin d'ouverture de ces applications à l'extérieur nécessite une gestion plus importante des utilisateurs et de leurs accès et d'implémenter un niveau de sécurité élevé.

**Un grand compte dispose au minimum de 25 annuaires utilisateurs différents !**

# La multiplication des annuaires induit

---

- Une perte de productivité des équipes d'administration : les administrateurs saisissent les mêmes données plusieurs fois avec un risque d'erreur non négligeable.
- Des failles de sécurité qui peuvent être très importantes : comment s'assurer qu'un utilisateur quittant l'entreprise ne restera pas déclaré dans un référentiel ?
- Des délais et des coûts supplémentaires lors du développement et du déploiement des applications et des services : chaque maîtrise d'œuvre doit concevoir, et alimenter un référentiel.
- Une complexité pour les utilisateurs qui doivent se souvenir de multiples couples identifiant / mot de passe.

# La solution : Un annuaire centralisé type LDAP

---

- LDAP = Lightweight Directory Access Protocol.
- Standard destiné à normaliser l'interface d'accès aux annuaires
- L'objectif de LDAP est de favoriser le partage et de simplifier la gestion des informations concernant des personnes, des ressources de l'entreprise, ainsi que les droits d'accès de ces personnes sur ces ressources
- LDAP centralise dans un seul annuaire toutes les configurations utilisateurs nécessaires aux différentes applications.

# Pourquoi choisir LDAP ?

---

- LDAP est un standard IETF (Internet Engineering Task Force) au même titre que FTP, TCP/IP, DNS, SMTP, HTTP... Protocole normalisé (RFC 1777 et 1778)
- LDAP simplifie la gestion des profils de personnes et de ressources
- LDAP favorise l'interopérabilité des Systèmes d'information à travers le partage de ces profils
- LDAP améliore la sécurité d'accès aux applications
- LDAP offre des accès en lecture/écriture
- LDAP permet des recherches puissantes sur des parties de l'arbre
- LDAP inclus un service d'authentification et de réplication
- LDAP s'appuie sur un modèle d'information bien-pensé et extensible

# Le ROI sur les projets annuaires

---

- Réduction des charges de recherche, de vérification, de saisie et de mise à jour des informations associées aux utilisateurs et à leurs droits d'accès par les administrateurs
- Réduction du temps consacré par le support à la réinitialisation des mots de passe des utilisateurs
- Diminution des coûts de déploiement et de développement informatique en s'appuyant sur un modèle d'habilitation commun des utilisateurs
- Des gains financiers en supprimant ou diminuant les annuaires « papier » (création et diffusion)

---

# Mairie de Vaulx-en-Velin

**Pourquoi mettre en œuvre un Annuaire ?**



# Le contexte

---

- Un parc qui a vite grossi (environ 50 micros supplémentaires par an sur 8 ans) soit 480 aujourd'hui.
- Une mise en réseau pratiquement systématique
- 15 serveurs
- Plus de 20 applications métiers
- Un effectif réduit de 4 (5) personnes
- Un besoin impératif de sécuriser les accès

# Les besoins exprimés par le SI

---

- Difficulté grandissante pour gérer l'administration des accès aux postes et aux applications.
- Avoir une vue générale de l'ensemble des utilisateurs potentiels et de leur droits d'accès (applications autorisées, plages horaires, etc. ... )
- Un public non conscient des risques de laisser son poste en libre service
- Vulnérabilité de la politique de sécurité du fait de la géographie des lieux
- Pouvoir ne donner qu'un seul nom d'utilisateur et un mot de passe par agent afin d'éviter le post-it sur l'écran
- Pouvoir changer plus facilement et plus régulièrement les mots de passe utilisateurs

# La cohérence du système d'information

---

- Les différentes sources de données dans l'établissement sans concordance ni concertation et jamais à jour
- Éditions papiers (annuaire téléphonique) tous les 3 ans
- Diffusion confidentielle de listes sur des formats différents (les numéros de portable - Excel; Annuaire téléphone Filemaker Pro; etc.)
- Les différentes listes de diffusion en messagerie en fonction de critères en gestion individuelle

# Interrogations

---

- Recherche d'une méthode de travail pour mettre en œuvre un annuaire fédérateur de toutes ces informations
- Trouver les arguments pour « vendre » le dispositif en interne
- Quels partenaires investir dans le projet
- Jusqu'où ne pas aller trop loin pour ne pas faire une « usine à gaz »
- Interfacer ces informations avec les applications et les droits d'accès
- Pouvoir faciliter la mise à jour automatique de la base (extractions)
- Trouver un outil travaillant sur des systèmes hétérogènes (Windows 2000 Unix et Linux)
- Diffuser une partie des informations avec un moteur de recherche sur l'intranet (à faire lui aussi)
- Donner la responsabilité d'une partie de la mise à jour à un service.
- Trouver une solution pas trop onéreuse (budgets réduits)

---

# Annuaire électroniques

Comment gérer un  
projet d'annuaire ?



# 1. Créer un groupe de travail

- Constituer un groupe d'utilisateurs, chargé de l'expression de besoin et de la validation des choix fonctionnels effectués.
  - Direction informatique
  - Service des Ressources Humaines
  - Le responsable de la sécurité
  - Les administrateurs du ST
  - Quelques responsables hiérarchiques

Un programme de sensibilisation



**La multiplicité des acteurs est la 1ère cause d'échec des projets d'annuaires !**

## 2. Les questions à vous poser ?

---

- Quelles sont les données qui vont être partagées à l'aide de l'annuaire ?
- D'où vont provenir ces données et qui en sont les propriétaires ?
- Comment décrire et organiser ces données dans un modèle commun à toutes les applications qui vont l'utiliser ?
- Qui va gérer ces données et comment ?
- Comment faire cohabiter les données partagées de l'annuaire et les applications existantes ?
- Quelles règles de sécurité faudra-t-il mettre en œuvre pour protéger l'accès à celle-ci ?

# 3. Organisation d'un projet annuaire

---

- Définition du modèle d'information
  - Phase 1 : Analyse des sources d'information
  - Phase 2 : Conception du schéma
- Définition du modèle de nommage
  - Phase 3 : organisation de la structure de l'arbre (DIT)
  - Phase 4 : Règles de nommage des entrées
- Définition du modèle fonctionnel
  - Phase 5 : Analyse des opérations LDAP et intégration des règles de fonctionnement
- Définition du modèle de sécurité
  - Phase 6 : Définition des contrôles d'accès
  - Phase 7 : Sécurisation du (des) serveur(s) LDAP
- Définition du modèle de duplication

# Le modèle d'information

---

- Il définit le type de données pouvant être stockées dans l'annuaire



1. Recenser toute la population de l'entreprise ayant un accès au SI (Employé, stagiaire, partenaire, intérimaires...)
2. Recenser les différents référentiels dans l'entreprise contenant cette population (annuaire LDAP, Base de données)
3. Faire l'inventaire des sources d'informations devant alimenter l'annuaire
4. Faire l'inventaire des applications devant utiliser l'annuaire

# Le modèle de nommage

- Le modèle de nommage définit comment sont organisées les entrées de l'annuaire et comment elles sont référencées
- L'organisation de ces objets se fait suivant une structure logique hiérarchique : le Directory Information Tree (DIT).

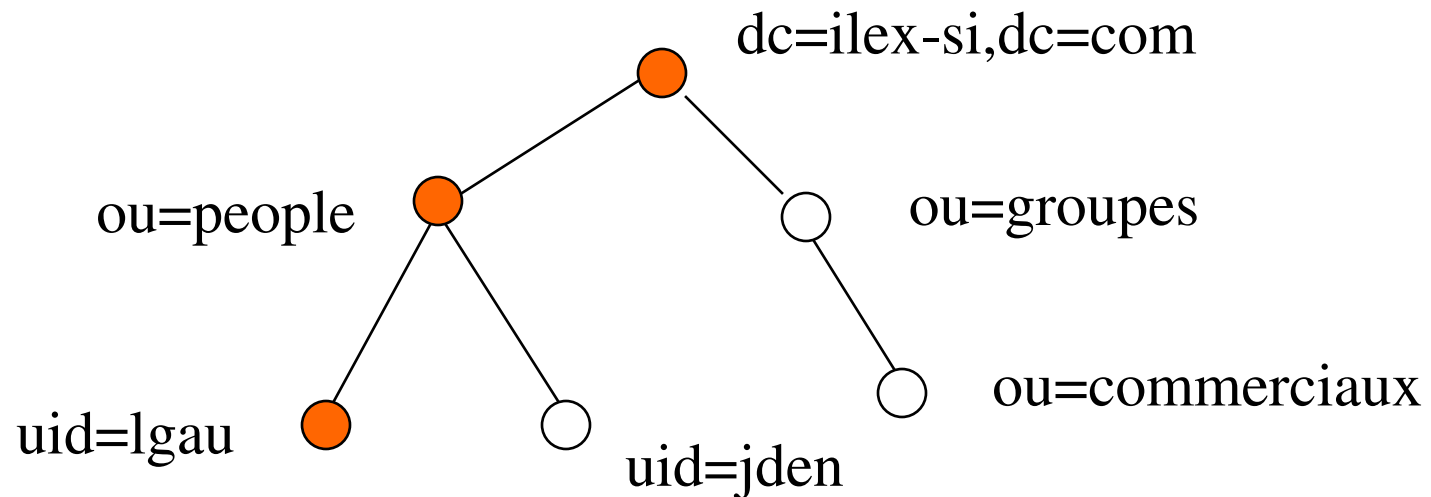


Dans cette phase, les paramètres qu'il faut prendre en compte sont :

- Le nombre d'entrées prévu et son évolution ?
- La nature (type d'objet) des entrées actuelles et futures ?
- Vaudra-t-il mieux centraliser les données ou les distribuer ?
- Seront-elles administrées de manière centrale ou faudra-t-il déléguer une partie
- La duplication est-elle prévue ?
- Quelles applications utiliseront l'annuaire et imposent-elles des contraintes particulières ?
- Quel attribut utiliser pour nommer les entrées et comment garantir son unicité de la gestion ?

# Modèle de nommage : Exemple

---



DN de l'entrée jden : uid=jden, ou=people, dc=ilex-si, dc=com

# Le modèle fonctionnel

---

- Le modèle fonctionnel décrit le moyen d'accéder aux données et les opérations qu'on peut leur appliquer.
- Le modèle définit :
  - Les opérations d'interrogation
  - Les opérations de comparaison
  - Les opérations de mise à jour
  - Les opérations d'authentification et de contrôle

# Le modèle fonctionnel



- Recenser les processus administratifs de création et de suppression de comptes sur ces ressources
- Identifier les différents profils (utilisateur, administrateur) disponibles sur chacune de ces ressources
- Identifier les différents paramètres à prendre en considération pour la création d'un compte utilisateur sur cette ressource en intranet ou en extranet (direction des HA, direction commerciale)
- Lister les différents cycles d'approbation (workflow) pour l'attribution d'un droit d'accès à chacune des ressources du système d'information (responsable hiérarchique et/ou administrateur système).
- Lister les règles en vigueur pour l'attribution d'un identifiant sur la ressource du système d'information, pour l'attribution d'une adresse email ...
- Définition des processus de mise à jour de chaque classe d'objet de l'annuaire.
- Ceci permet d'identifier les flux de données qui permettent de mettre à jour l'annuaire et de le synchroniser avec son environnement.

# Le modèle de sécurité

---

- Le modèle de sécurité décrit le moyen de protéger les données de l'annuaire des accès non autorisés
- La sécurité se fait à plusieurs niveaux :
  - Par l'authentification pour se connecter au service
  - Par un modèle de contrôle d'accès aux données
  - Par le chiffrement des transactions entre clients et serveurs et/ou entre serveurs.

---

# Annuaire électronique

Sécurité :

Les accès

La continuité de service

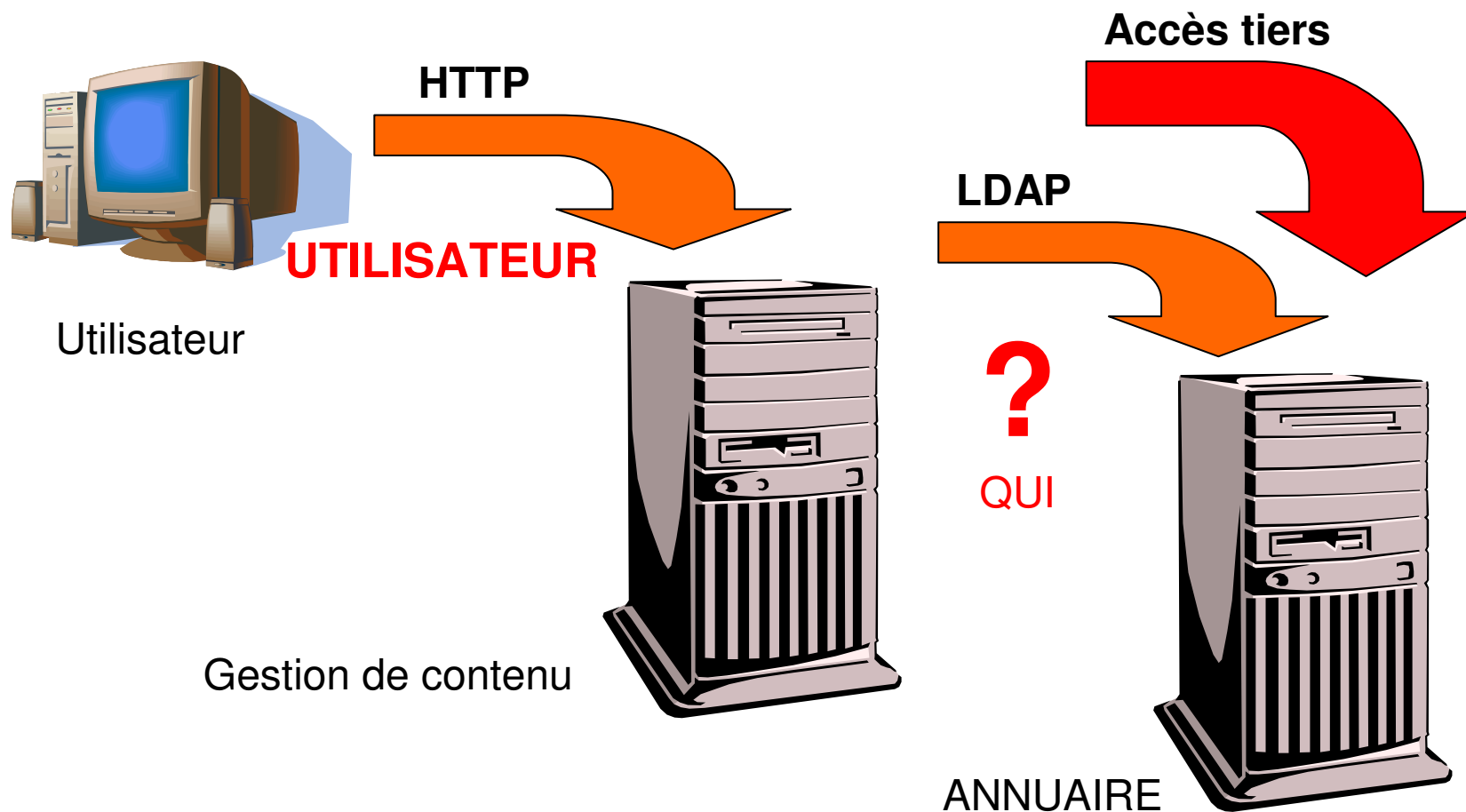


# Accès aux données

- Listes de contrôle d'accès
- Atome : un attribut dans un objet
- Quelle Interface Homme-Machine pour administrer ?

	Nom	Tél.	Mail
Util1	Jo	6598	jo@ldap.com
Util2	Bill	2506	bill@ldap.com
Util3	Kim	8943	kim@ldap.com

# Trous de sécurité ?



# Protection des données

---

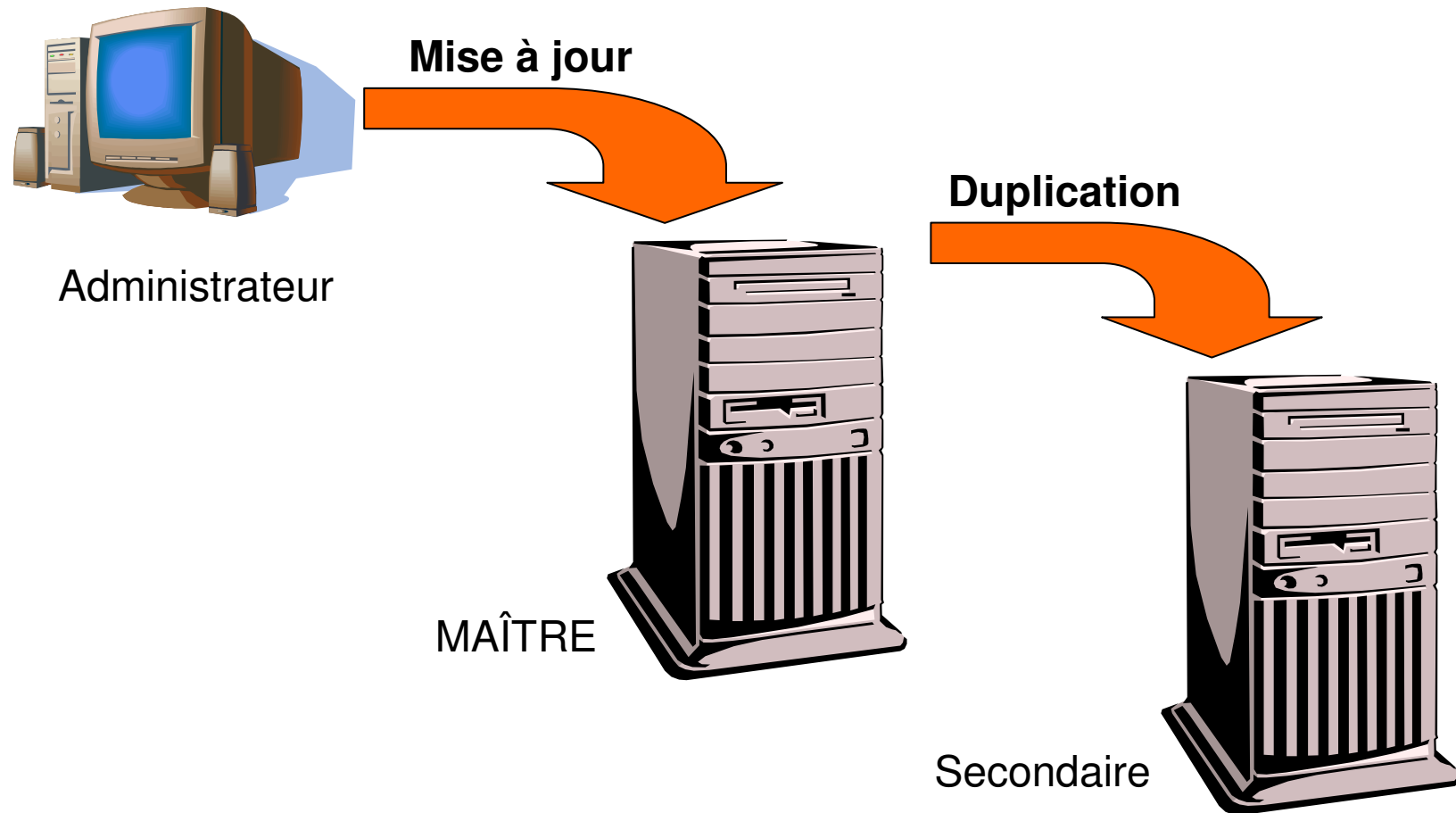
- Les applications ont leur propre sécurité
  - Protection **indépendante** de l'annuaire
- 
- **Un impératif !**

# Continuité de service

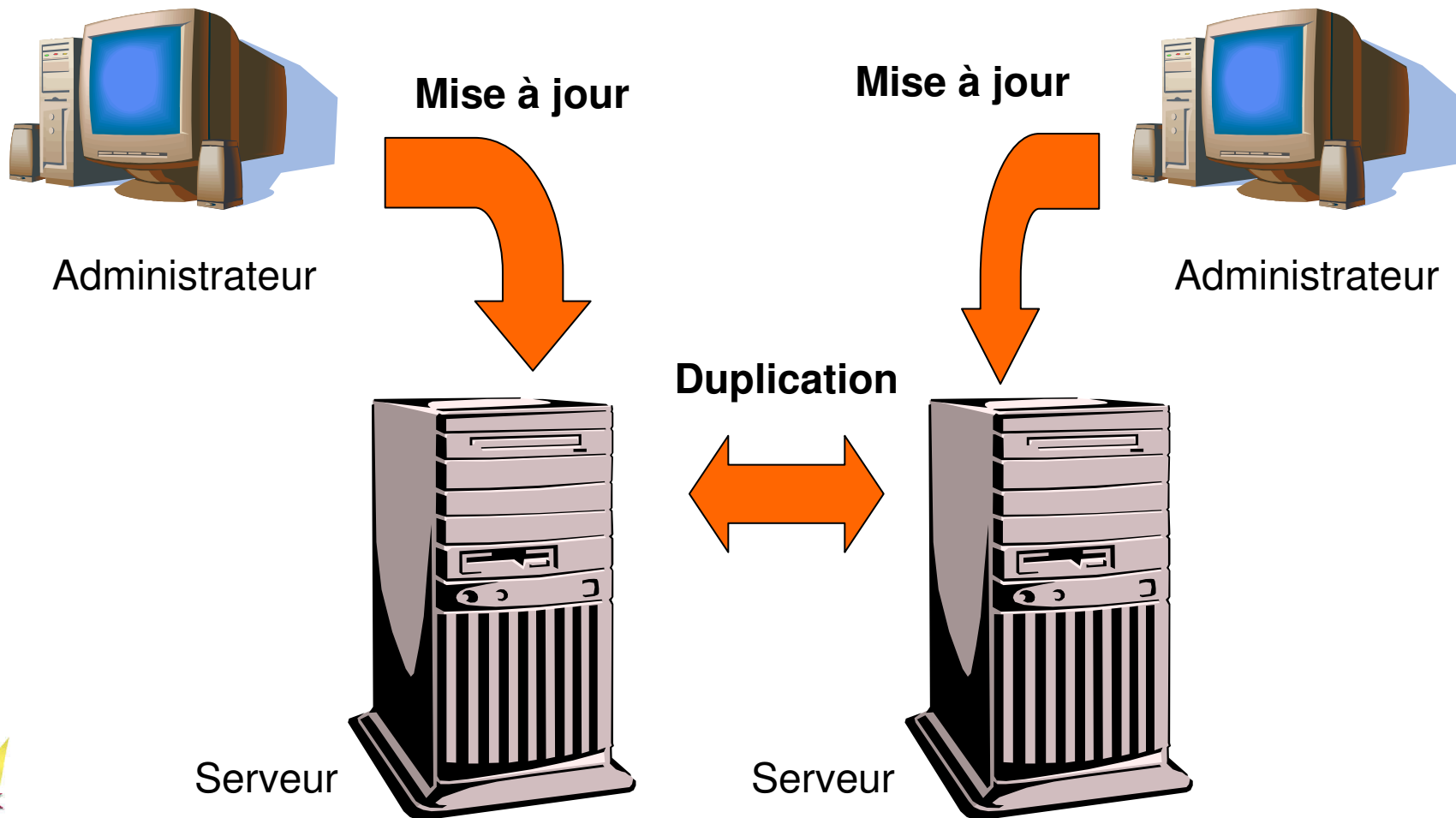
---

- L'indisponibilité de l'annuaire implique l'arrêt du Système d'Information
- Vous devez protéger votre SI
  - Les serveurs d'annuaire sont dupliqués
  - Les données de l'annuaire sont sauvegardées

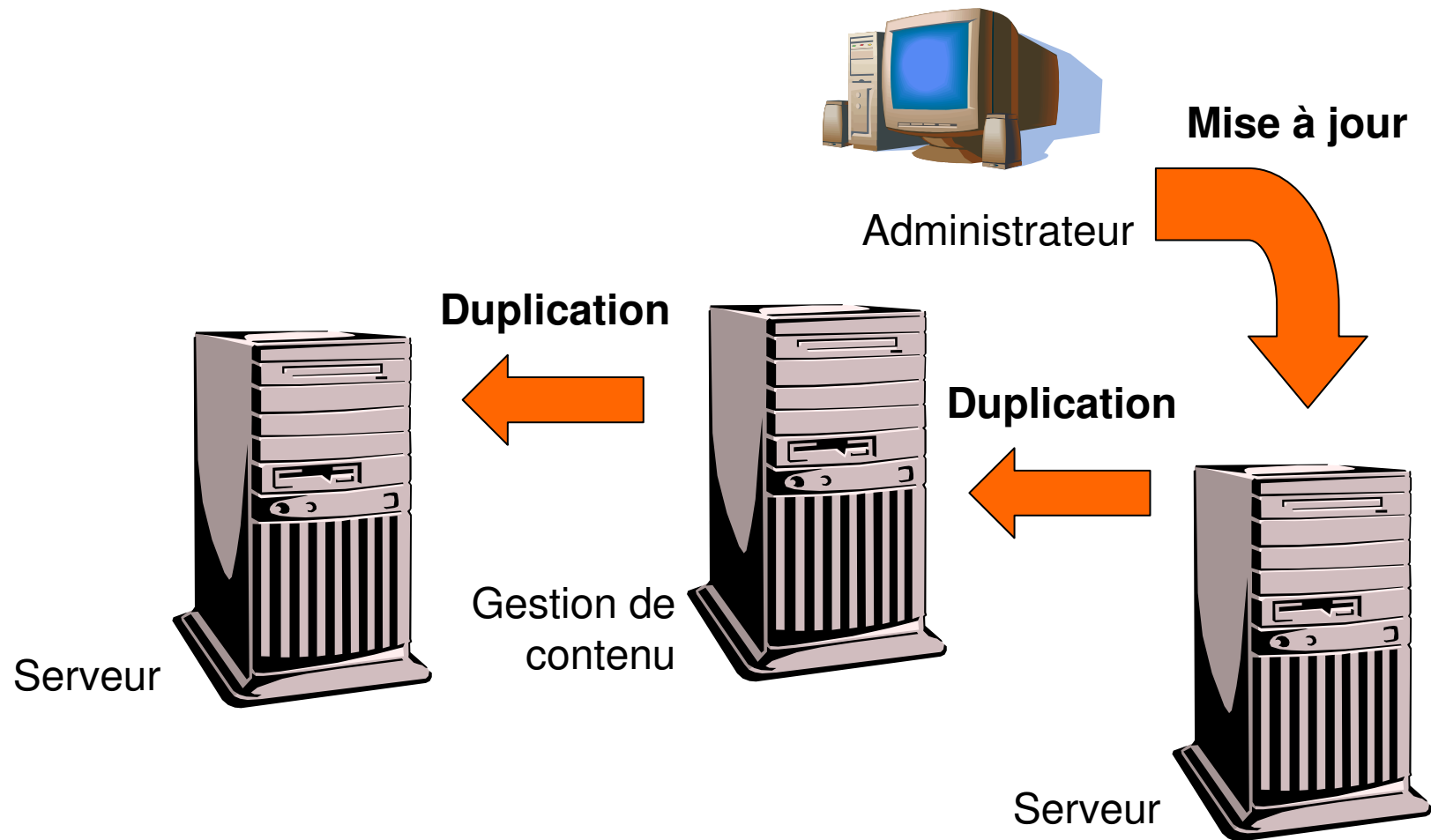
# Duplication *single master*



# Duplication *multi master*



# Duplication par une application



# Sauvegarde

---

- Serveurs en fonction 24h/24
- Services fondés sur des SGBD
- Nécessite
  - Journalisation
  - Sauvegarde base ouvertes
- Pas trivial, mais bien pris en compte par les outils du marché

# Restauration

---

- Disponible :
  - Une sauvegarde âgée (plusieurs heures ou jours)
  - Serveurs dupliqués
  - Données en provenance d'autres applications
- Quel jeu de données fait foi ?
- Des difficultés de mise en œuvre : temps, charge réseau, service en ligne...

# Conclusion

---

- **La sécurité doit être envisagée de façon globale**
- **La mise en œuvre demande de l'attention**

---

# Annuaire électronique

État du marché  
9 décembre 2003



boutemy.com



Annuaire LDAP - Sécurité

09/12/2003

36

# Les ténors

---

- Microsoft Active Directory
  - Intégré à Windows
  - 55% de parts de marché (du fait de son intégration ?)
  - Active Directory Application Mode (ADAM) : produit *stand alone*
- Novell eDirectory
  - 35% de parts de marché
  - AIX, HP-UX, Linux, Netware, Solaris, Windows

# Annuaire

---

- Computer Associates eTrust Directory
- CriticalPath Directory Server
- IBM Tivoli Directory Server
- Innosoft Distributed Directory Server
- Open LDAP
- Sun Java System Directory Server (Sun ONE Directory Server)
- Syntegra Aphelion Directory

# Méta annuaires

---

- CriticalPath Meta-Directory Server
- Sun Java System Meta-Directory
- MaXware Virtual Directory, MetaCenter
- Microsoft Identity Integration Server (MIIS)
- Radiant Logic Directory Application Integration
- Siemens DirX
- Syntegra Global Directory/Meta Edition

# Gestion de contenu

---

- Calendra Directory Manager
- Ilex Meibo
- MaXware Data Synchronization Engine
- Oblix NetPoint