Tendances Logicielles

PORTE 01

Tivoli

La mise en oeuvre d'une solution de gestion des identités et des accès: un long fleuve tranquille ?

Session 5

Bruno Mazeron - Ingénieur d'affaires

André Deville - Consultant sécurité avant-vente

1er et 2 octobre 2007

IBM

Agenda

- Gestion des Identités: une définition
- Les enjeux
- La démarche Projet
- Exemples concrets et conseils

Agenda

- Gestion des Identités: une définition
- Les enjeux
- La démarche Projet
- Exemples concrets et conseils

Gestion des identités: une définition

- Un ensemble de processus et d'infrastructure technologique permettant de gérer le cycle de vie de l'identité numérique des utilisateurs des systèmes d'information.

- 4 fonctions majeures:
  - Identification + Authentification : vérifier l'identité de l'utilisateur
  - Autorisation + Habilitations : contrôler l'accès des utilisateurs au SI
  - Administration: gérer les habilitations des utilisateurs et les propager à la totalité du SI
  - Audit: examiner et reporter : qui, où, quand et comment ?

Les processus de gestion des identités & accès

Processus Gestion identités

I - Création des identités

- 1 – Collecte des informations d'identité
- 2 – identifier les systèmes nécessaires à l'utilisateur
- 3 – Création des comptes
- 4 – Affectation des informations d'identité
- 5 – Création des droits d'accès

II - Maintien identités

- 1 – maintien des informations d'identité
- 2 – maintien des accès nécessaires

III - Suppression des identités

Processus Gestion accès

- 1 - Vérifier l'identité
- 2 – Authentifier l'utilisateur
- 3 – Déterminer le niveau d'autorisation utilisateur
- 4 – Donner l'accès aux systèmes

1 - Vérifier l'identité
1 – Authentifier l'utilisateur
1 – Déterminer le niveau d'autorisation utilisateur
1 – Donner l'accès aux systèmes

Gestionnaire d'identité

Identités

Service d' authentification

Service de « provisionning »

Accès

Service d' autorisation

Agenda

- Gestion des Identités: une définition
- Les enjeux
- La démarche Projet
- Exemples concrets et conseils

Les enjeux

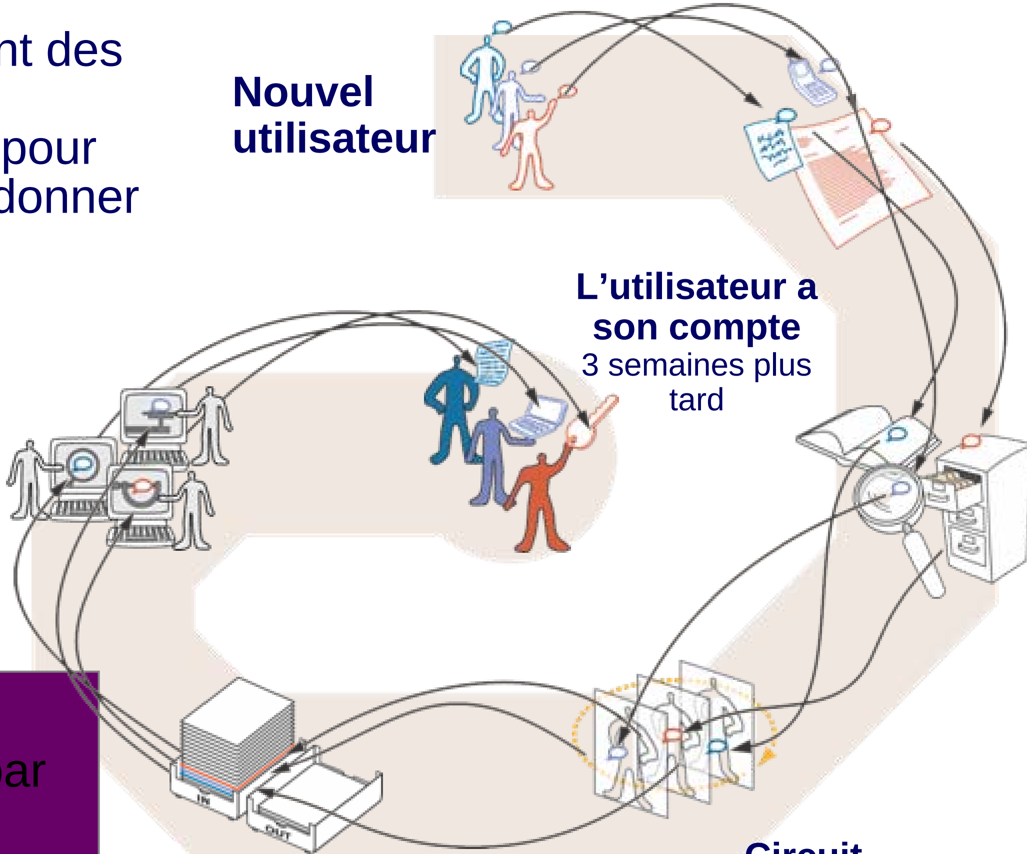
- Sécurité
  - Renforcement de la politique de sécurité
    - Gestion des comptes et mots de passe (SLO, SSO)
    - Gestion temps-réel des comptes orphelins/dormants
    - Gestion permanente des autorisations et profils basée sur les rôles-métiers des utilisateurs
    - Audit et traçabilité de toutes les opérations sur le SI

Les enjeux

- Productivité
  - Gain de temps et réduction des coûts
    - Propagation automatique des informations
    - Reporting automatisé et temps réel
    - Intégration simple de nouvelles applications
    - Rapidité des processus d'attribution des comptes
    - Auto-administration des mots de passe et profils
    - Satisfaction des utilisateurs SSO
  - Réduction des opérations « helpdesk »
    - 30% env. sur les coûts "hot line" & "call center" (chaque appel coute 20€)

Le constat: Un processus manuel et donc inefficace

Les entreprises utilisent des processus manuels et souvent inconsistants pour créer des comptes et donner acces aux ressources



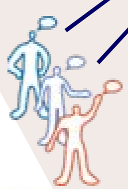
Durée d'activation: jusqu'à 3 semaines par utilisateur

Un administrateur peut gérer entre 300 et 500 utilisateurs.

Le processus idéal de création d'un utilisateur

- Un processus automatisé basé sur des autorisations par rôle et des politiques prédéfinies.
- Un workflow pré-établi et des procédures de réponse et d'escalade
- Une politique d'administration consistante

Nouvel utilisateur



Demande d'acces en ligne

Peut etre fait de façon automatique par les les RH lors de l'arrivée d'un nouvel employé

Vérification de la politique et des rôles

- Accès et habilitation établies à priori en fonction des rôles.
- Annuaire d'entreprise

Circuit d'approbation

- Approbation basée sur une politique et des rôles
- Workflow automatisé dirigeant la demande vers les bons aprouveurs assurant le suivi

Création automatisée des comptes

- Identifiant SSO et mots de passe généré automatiquement.
- Comptes créés automatiquement sur les ressources cibles.

Les utilisateurs disposent de leurs comptes

Heures et non semaines.

Durée d'activation: heures et non semaines

Capacité à faire face à des pics de charge sans monopoliser les ressources IT.

Les directions métiers peuvent facilement mettre en place les politiques d'accès

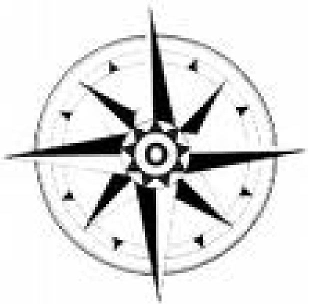
Les enjeux

- Conformité aux réglementations
  - Respect des règles à mettre en oeuvre
    - Sarbanes-Oxley – Contrôles d'audit améliorés, protection des investisseurs
    - Loi de sécurité Financière : Contrôle interne du reporting financier et communication financière
    - Bale II : Contrôle et gestion du risque
  - Fournir les outils permettant d’éditer les rapports utiles aux auditeurs

Agenda

- Gestion des Identités: une définition
- Les enjeux
- La démarche Projet
- Exemples concrets et conseils

Comment démarrer ? Dans quelle(s) direction(s) ?



Tivoli Identity Manager

Gestion des identités

- ✓Self service (demande d'accès, auto dépannage des mots de passe)
- ✓Gestion automatique des droits d'habilitation (Provisionning)
- ✓Workflow
- ✓Délégation d'administration
- ✓ …

Tivoli Access Manager for e-SSO

SSO d'entreprise

- ✓Quelles applications
- ✓Mode d'authentification
- ✓Génération des mots de passe
- ✓ Station partagée
- ✓ Auto dépannage Windows

Identity & Access Management

Tivoli Access Manager for e-Business

Tivoli Federated Identity Manager

Web SSO et contrôle d'accès

- ✓Quelles applications
- ✓Mode d'authentification
- ✓Internet | Externe
- ✓Fédération des identités

Annuaire LDAP

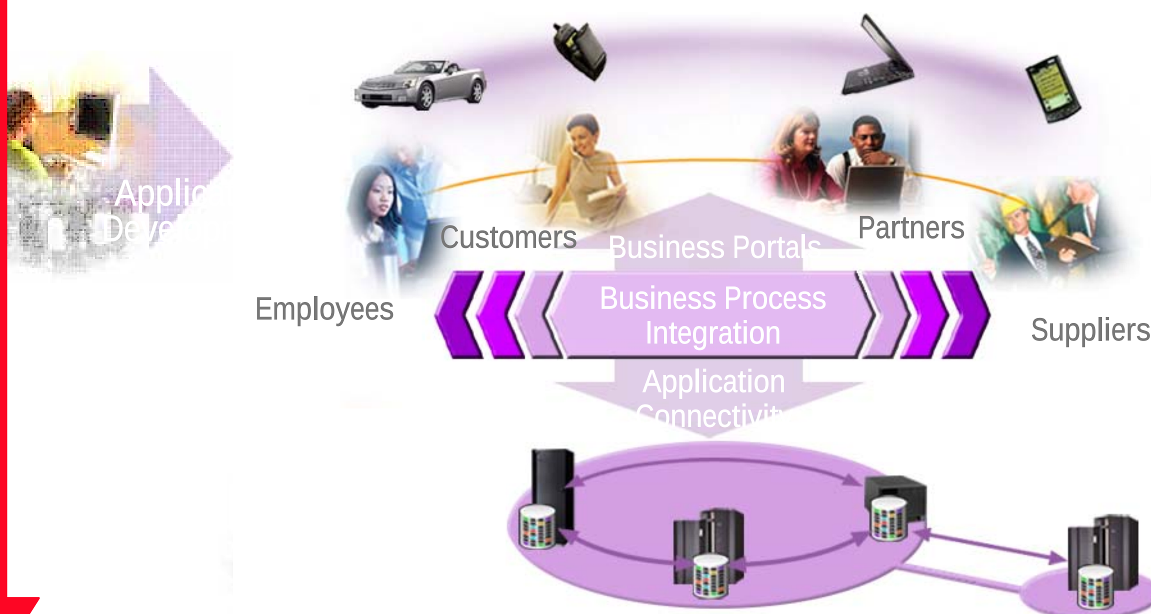
- ✓Authentification
- ✓Autorisation
- ✓ Synchronisation de données

Tivoli Directory Server

Tivoli Directory Integrator

Démarche – *recherche de ROI*

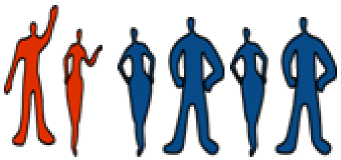
Déploiement "Top Down"
Couverture tactique, livrables restreints, ROI tardif, faible visibilité, coûts de déploiement supérieurs



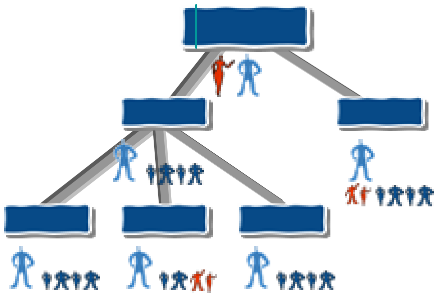
Applications
Applications
Applications
Applications
Infrastructure
Data
Operating Systems

Déploiement "Bottom Up" Large couverture, des livrables bien définis, ROI rapide, forte visibilité, fort impact

Périmètre : Identités et Organisations



- **Personnes**
  - ➢ Type de la population :statut employés, prestataire, stagiaire, partenaires, ..
  - ➢ Ces données existent-elles ? Si oui:
    - que contiennent ces données nom, prénom, matricule, téléphone, responsable, entités ou établissement de rattachement,..)
    - Fiabilité
    - Comment sont-elles mises à jour ?
    - Où et disponible sous quel format ?

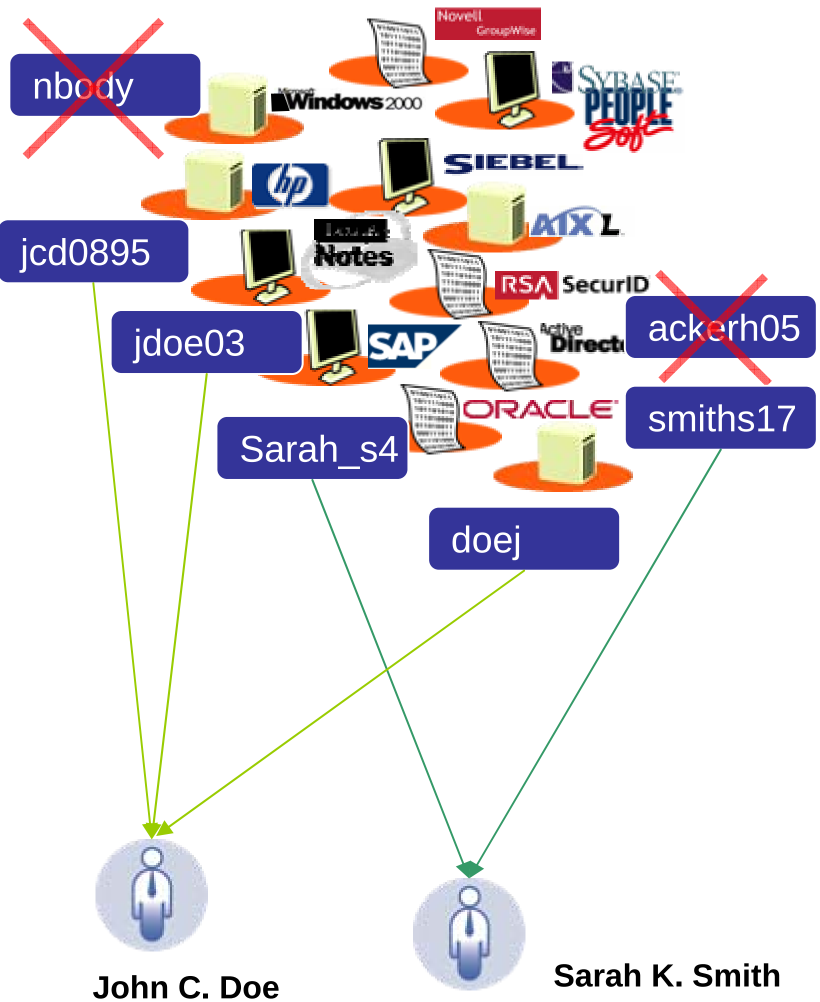


- **Notion de hiérarchie et organisation**
  - ➢ Commencer par quelles entités
  - ➢ Quels sont les processus de validation en cours ?
  - ➢ Connaît on les responsables des entités ou des personnes ?

- **Rôles métiers**
  - ➢ Utilisés pour décrire des règles d'habilitations
  - ➢ N'est pas forcément le type d'emploi stocké dans les bases RH
  - ➢ Ces données existent-elles ?

=> Il n'est pas nécessaire de faire dans un premier temps un cartographie fine

Périmètre des ressources :



- Définir les applications
  - pour être ‘SSO’isées
  - pour bénéficier de mise à jour automatique (provisioning de la gestion des identités)
- Prise en compte de ressource logique ?
- Où sont-elles ?
- Versions ?
- Politique de mots de passe et des identifiant
- Détection des comptes orphelins

Qui va utiliser IBM Tivoli Identity Manager ?

- Utilisateurs finaux pour

❑ Modifier des informations personnelles	Oui | Non
❑ Réinitialiser ses mots de passe	Oui | Non
❑ Faire des demandes d'accès	Oui | Non

- Gestionnaires
  - Approbation
  - Ordre de travail
  - Renseignement d'information complémentaire
  - Demande d'accès
  - Support Help Desk

- Administrateurs fonctionnels dans ITIM
  - Qui définit les nouveaux rôles ?
  - Qui définir les nouvelles entités ?
  - Qui définit les politiques d'habilitation ?
  - Qui définir les politiques de mots de passe ?
  - Générer et accéder aux rapports d'audit

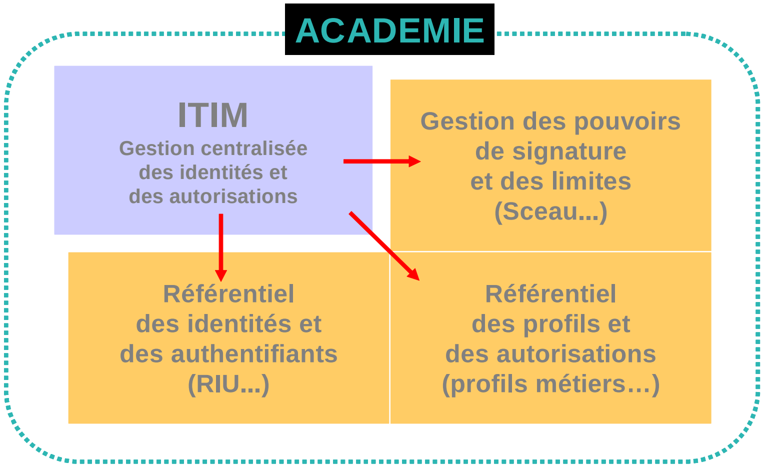
- Administrateurs techniques

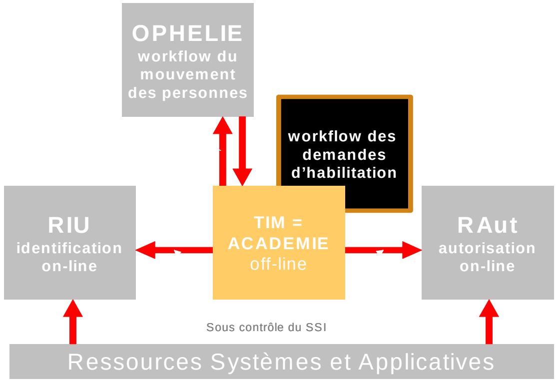
Agenda

- Gestion des Identités: une définition
- Les enjeux
- La démarche Projet
- Exemples concrets et conseils

Référence Groupe Bancaire

- Projet ACADEMIE (Administration Centrale des Administrations et des Demandes d'Identités Electroniques)
- Cible 17000 utilisateurs
- Modélisation AMOA
- Connecteurs : AIX, **Novell**, Oracle, Solaris, Sybase, DB2, **Windows NT et Windows 2000, Lotus Notes, RACF**.
- La priorité a été donnée aux environnements bureautiques (quick wins)
- Dans un second temps les applications spécifiques sont intégrées





Industrie

Projet UP (User Provisionning)

- 50 000 en production - Cible 80 000 utilisateurs
- Outil utilisé pour l'ensemble du groupe dans différents pays et continent.
- Connecteurs : Active Directory, Exchange, Radius, Unix, clé SSH,…
- Etapes par pays européens puis par continent
- Intégration avec outil de Help Desk
- Besoin de conformité SOX

Assurance

- 500 internes et 3000 externes
- Connecteurs : Active Directory, Exchange, bases RH, GED
- Projet de gestion des identités avec projet de carte à puce et identifiant unique avec SSO

- 2000 utilisateurs
- Projet de synchronisation de données (IBM Tivoli Directory Integrator) et annuaire LDAP (IBM Tivoli Directory Server) :
  - Détection des entrées/sorties des personnes depuis le référentiel RH
  - Synchronise de données dans l'annuaire LDAP utilisé par une application de type pages jaunes/blanches
  - Synchronisation des données dans l'annuaire Notes (email, téléphone) et Active Directory

Conseils et retour d’expérience

- Sponsor direction générale,
- Promouvoir le ROI sur le projet , en plus de la sécurité
- Créer une adhésion commune en faisant participer en amont du projet les futurs participants de la solution (notamment les RH)
- Communication interne (gestion du changement) et régulière
- Définir un schéma directeur avec plan projet et accompagnement
- Méthodologie et approche pragmatique

Un dernier conseil:

Think IBM !!

TEC - Technical Exploration Center - @ Paris

Accélérer le cycle de découverte des logiciels IBM

Les ressources hardware et software du TEC
à Noisy-Le Grand / Marne La Vallée
sont disponibles <u>gratuitement</u> :

« Les équipes Sales et TechSales de IBM Software, sont à votre disposition pour réserver des machines et des ateliers »

- EOTs - Exploration of Technology
  - Découvrir la valeur des logiciels IBM: Présentations, vidéos, démonstrations
- POTs – Proof of Technology, Ateliers/Workshops,
  - Démontrer les capacités des logiciels IBM
    - Présentations
    - Labs et hands-on …

une adresse E-mail à retenir:
TecParis@fr.ibm.com