OKIOK

Solutions de sécurité d'entreprise
et d'affaires électroniques

La Gestion des Identités et des Accès

… à la façon OKIOK

Claude Vigeant Ing.

Sept 2015

Agenda

L'expérience OKIOK

Réflexions sur la GIA

L'approche OKIOK

- Focus sur la gouvernance des identités et des accès

L'offre OKIOK en GIA

- Leadership et accompagnement en GIA
- La conformité des identités en tant que service (ICAAS)
- RAC/M Identity – Un outil performant pour prendre le contrôle des identités et des accès

Démonstration

Questions ?

L'expérience OKIOK
30 ans d'innovations en solutions de GIA

Années 80

- Conception de la carte RAC/M pour gérer les accès aux ordinateurs personnels tournant sous DOS, Windows et OS/2

Années 90

- Conception de Branch Manager pour gérer les accès aux ordinateurs personnels de façon centralisées en appliquant le modèle RBAC
- Conception de Focal Point, une solution de logon unique (ESSO) – devenue SAM ESSO

Années 2000

- Conception de Global Trust, une solution de gestion des accès Web incluant la fédération d'identité avec SAML2 et l'approvisionnement automatisé sous SPML2 – devenue Siemens DirX Access

Années 2010

- Conception de RAC/M Identity, une solution de gouvernance des identités et des accès
- Lancement de l'offre « Identity Compliance As A Service » (ICAAS)

L'expérience OKIOK
15 ans de leadership de projets de GIA

- **Conception de l'Infrastructure de Corporative de Sécurité (ICS) de la Banque Nationale qui met en œuvre les concepts de sécurité en profondeur par l'utilisation de jetons, modèle de gestion basé sur les rôles (RBAC), signature unique et gestion des accès Web (Web SSO)**

  Ces principes et éléments technologiques ont donnés naissance à la solution Global Trust

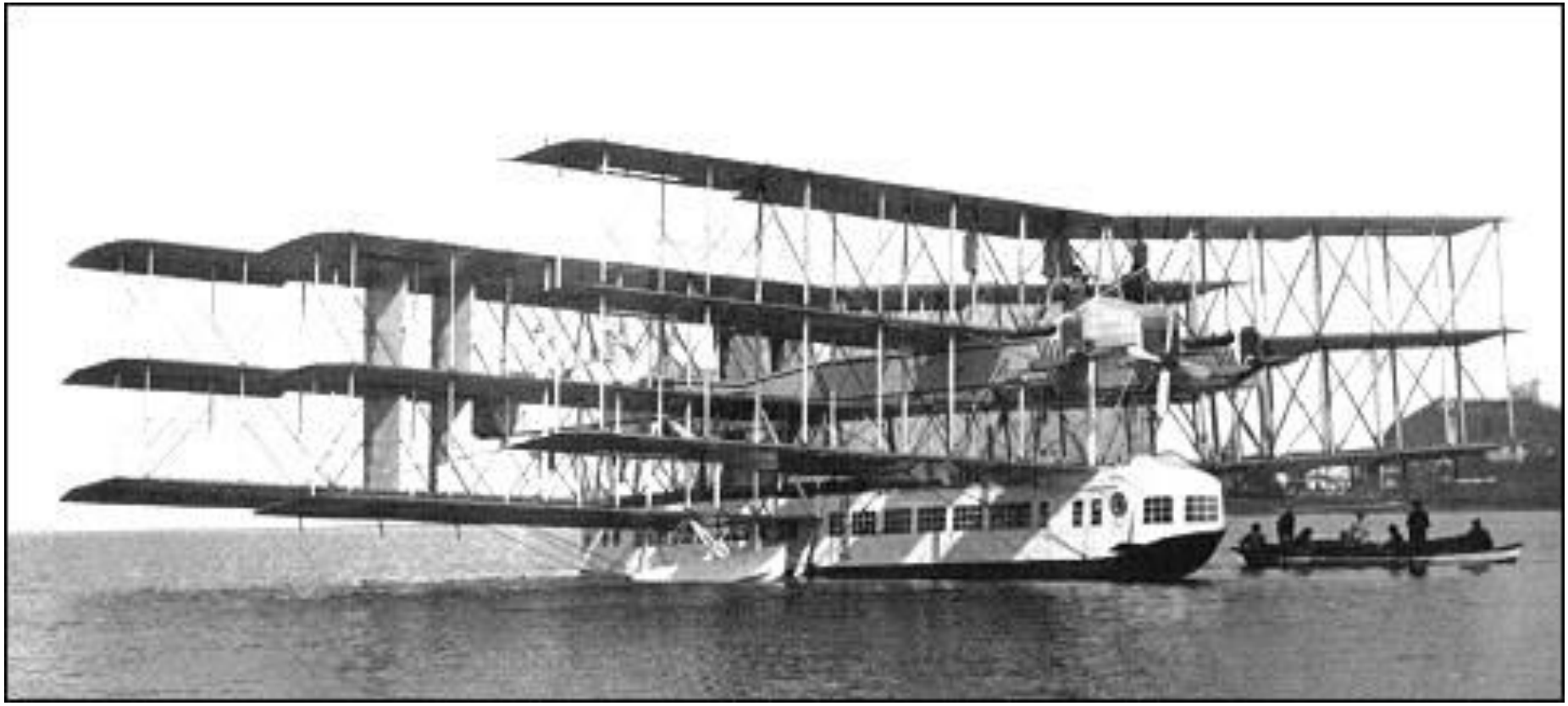
- **Prestation de services d'accompagnement en GIA chez plusieurs clients québécois et internationaux**

  Banque Laurentienne, Banque Nationale, Desjardins, Fonds FTQ, CUSM, AT&T, Banque KBC, Groupe Malakoff, CHU Ste-Justine, Hôpital Charles-Lemoyne, Atos

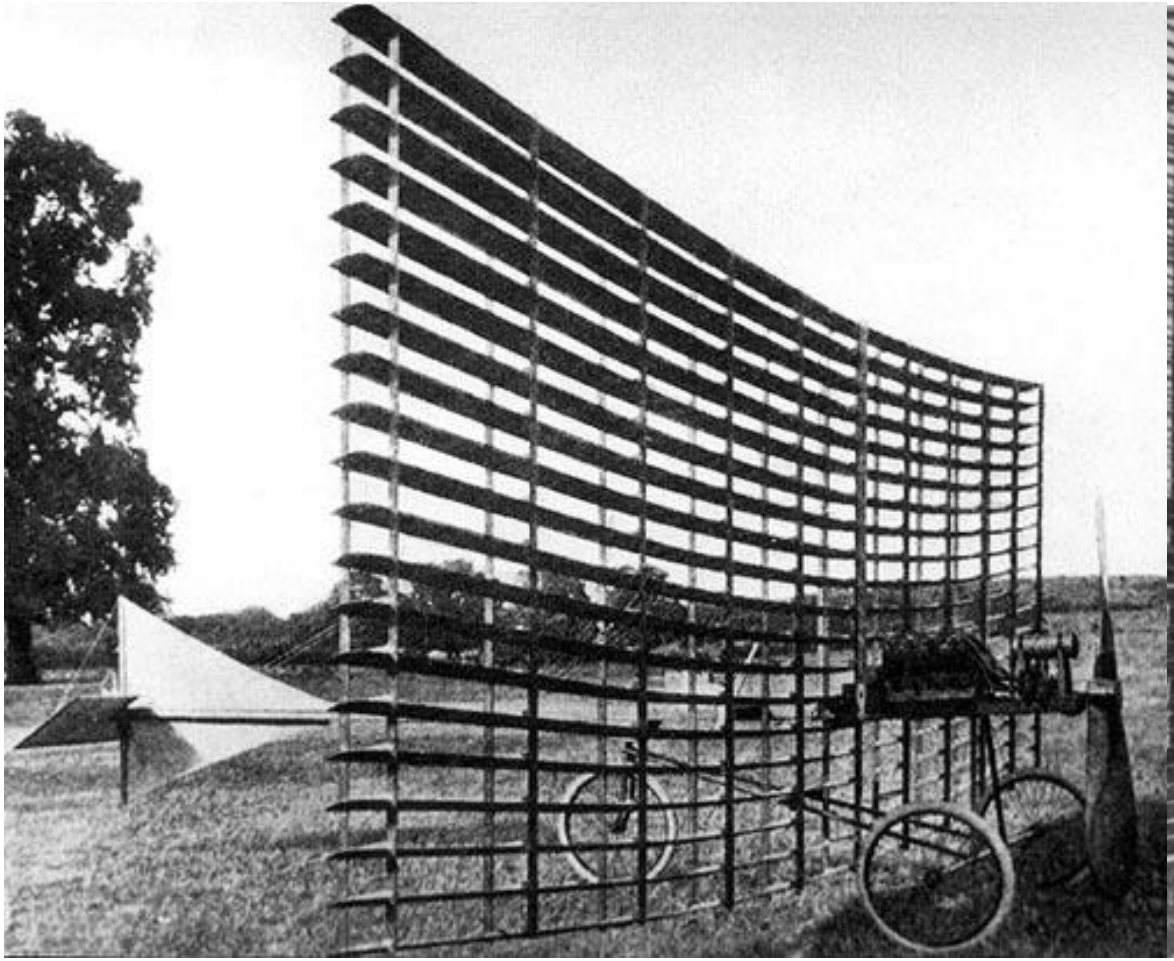
- **Prestation de GIA en mode service chez plusieurs clients québécois**
- **Lancement de l'offre ICAAS sur le marché local et international**
- **Leadership d'un projet majeur de GIA à portée Nord-Américaine pour un groupe multinational (en cours)**

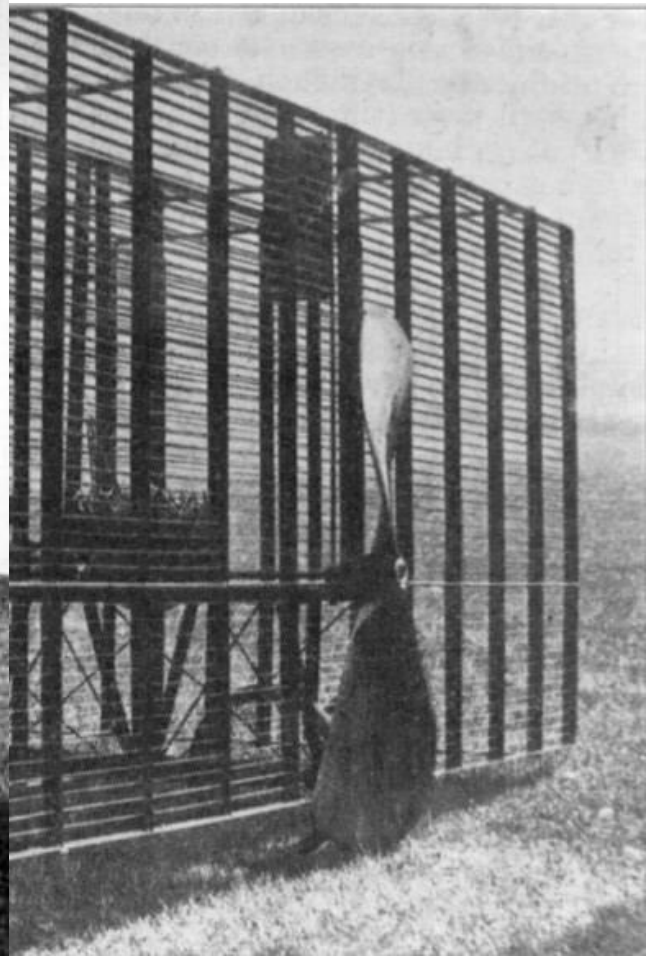
La majorité des projets de GIA échouent…

Souvent pour des raisons évidentes



Si une méthode ne fonctionne pas… pourquoi persister dans la même voie ?





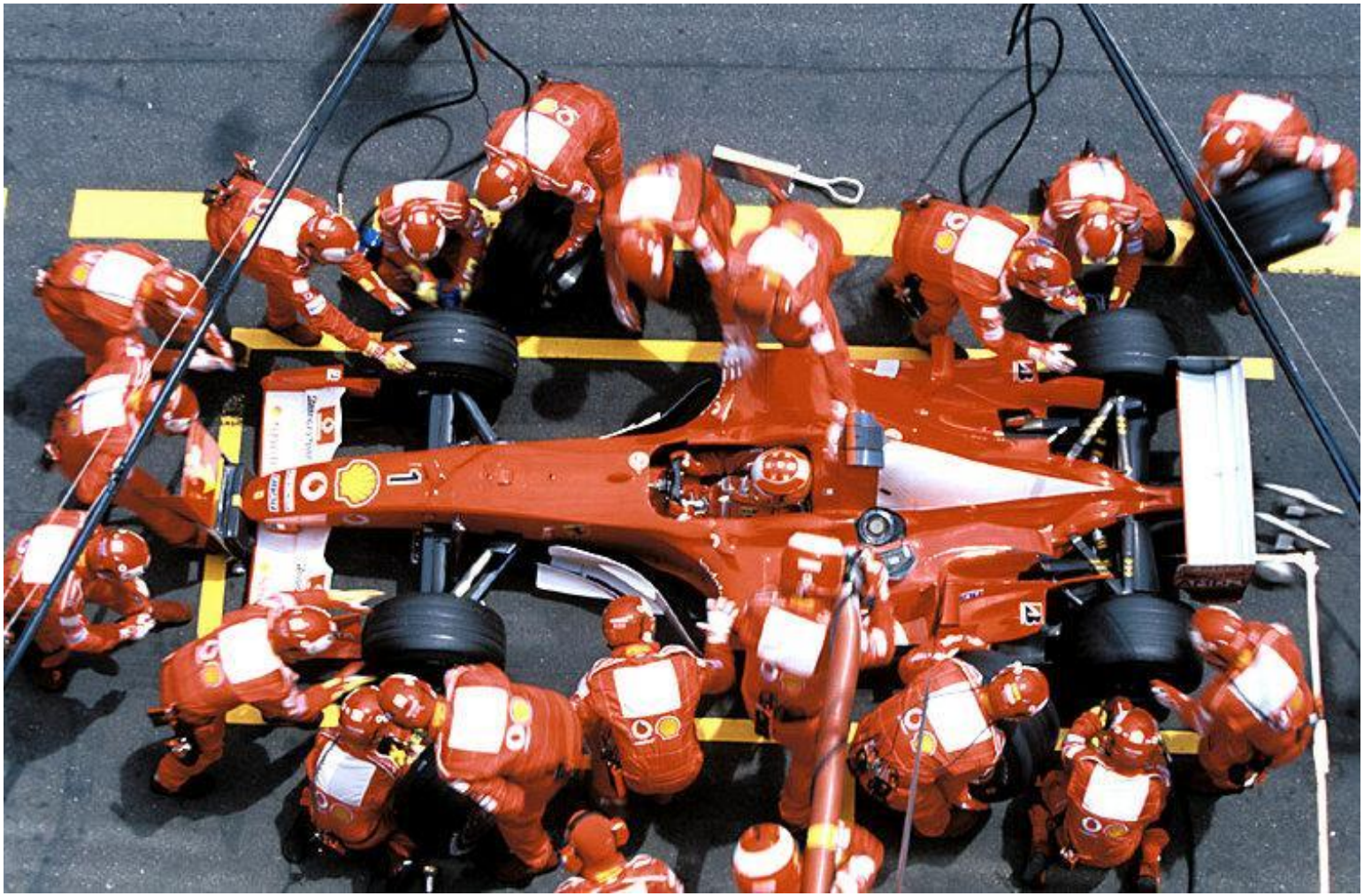
Pour réussir, il faut faire autrement

Traditionnellement, les projets de GIA visent l'automatisation de l'approvisionnement…

L’approche OKIOK…

Axer sur la gouvernance des accès – un but plus réaliste

L’approche OKIOK…
Créer des conditions gagnantes



L'offre OKIOK en GIA

EXPERTISE
SUR DEMANDE

Leadership et accompagnement de projets de GIA

ICAAS

Conformité des Identités et des Accès en mode service

RAC/M
IDENTITY

Solution RAC/M Identity

Leadership et accompagnement en GIA

L'approche OKIOK, agile et axée sur la réduction des risques

- **Définir des objectifs réalistes**
  - Prioriser la gouvernance des identités et des accès
- **Créer des conditions gagnantes**
  - Assurer d'avoir toute la latitude nécessaire
  - Établir la vision du projet
  - S'assurer du support du client
  - Appliquer notre modèle de gestion de projet proactive
  - Assurer l'expertise technique du plus haut calibre - manufacturier
  - Éliminer les éléments de risque hors de notre contrôle direct

Résultats

- **Succès à 100%**

Leadership et accompagnement en GIA

L'approche conventionnelle, souvent problématique

- **Objectifs irréalistes et/ou mal définis**
- **Lourdeur liée au cadre de gestion rigide**
- **Enjeux technologiques élevés**
- **Absence de leviers pour régler les problèmes techniques**
- **Expertise technique limitée**

Résultats

- **Délais**
- **Démobilisation**
- **Dépassement de coûts**
- **Insatisfaction**

Leadership et accompagnement en GIA

Prestation type en étapes et phases

Étape 1 – Analyse préliminaire

- **État de la nation**
- **Cible fonctionnelle et d'architecture**
- **Plan d'action**
  - Trois livrables
  - 12 à 15 semaines

Étape 2 - Réalisation

- **Phase 1 – fonctionnalité de base (Gouvernance)**
  - Mise en œuvre du référentiel
  - Revue initiale des accès
- **Phase 2 – fonctionnalité avancée**
  - Revue périodique des accès
  - Modélisation des accès en rôles
  - Libre service
- **Phase 3-**
  - Automatisation des retraits et de l'approvisionnement si requis

Leadership et accompagnement en GIA

Exemple d'un projet réel

Description

L'unité d'affaire nord-américaine d'une multinationale doit rehausser ses processus de GIA pour l'année de référence 2014 afin de passer avec succès les audits SSAE16

Environnements

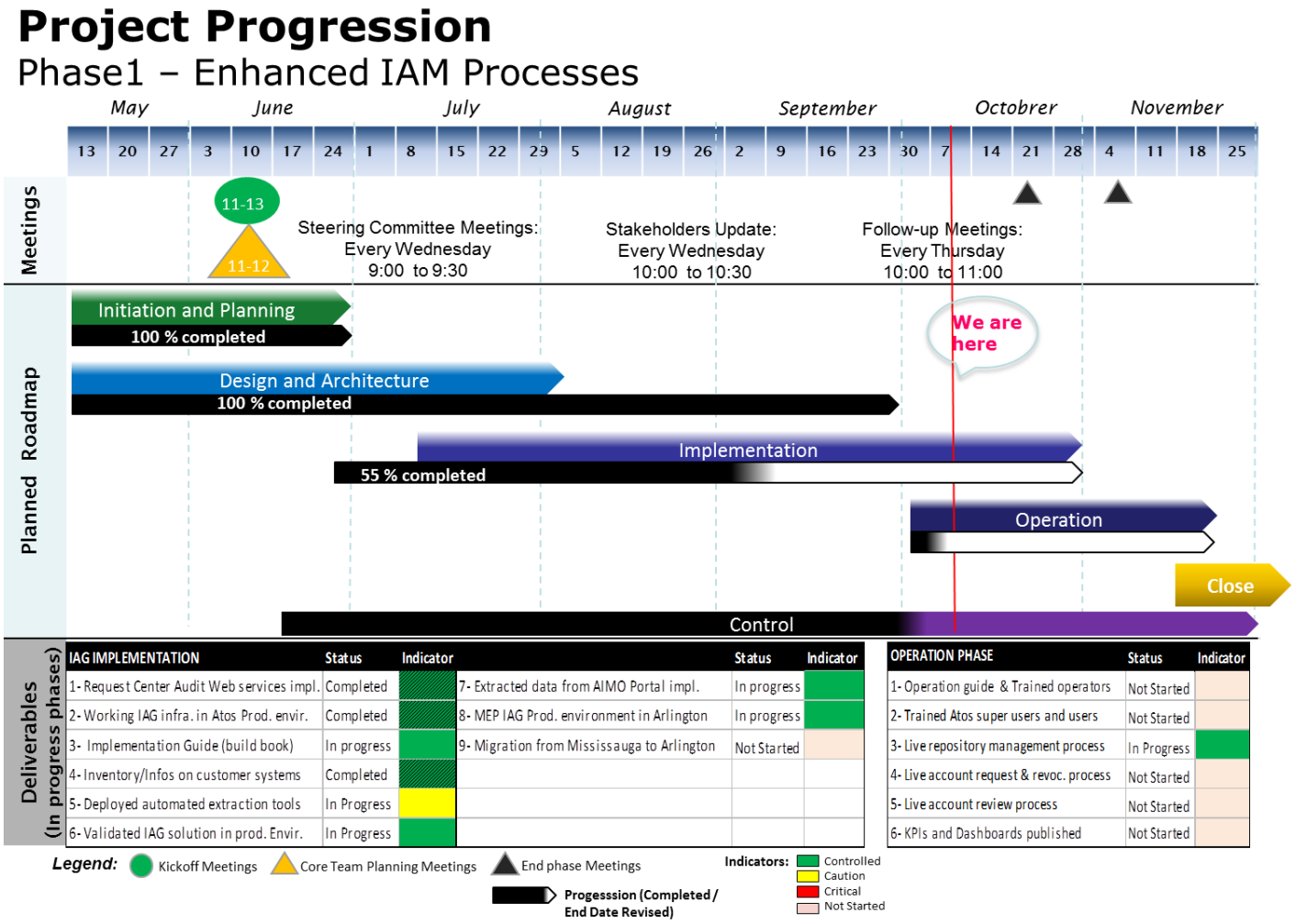
- 5 centres de données au Canada et USA
- Services et infrastructure distribués en Europe, Inde, Asie
- >20,000 serveurs Wintel, UNIX/Linux, centrales Z/OS, AS400
- 300 serveurs dans la portée de la phase 1

Déroulement

- Étape 1 – Janvier à avril 2013
- Étape 2 – Juin à décembre 2013 (phase 1) – livraison en 72 jrs ouvrables
  Janvier 2014 à Décembre 2015 (phase 2) - 20,000 serveurs

Leadership et accompagnement en GIA

Exemple réel d'un plan de projet



Conformité des Identités et des Accès en mode service (ICAAS)

Bien adapté aux PMEs

- Aucun investissement en capitalisation
- Capacité limitée d'exploiter une infrastructure
- Capital humain limité (expertise, compétences, disponibilité)
- Particulièrement utile pour la mise en conformité périodique requise par les cadres règlementaires

Avantages - résultats ultra-rapides

- Démarrage des campagnes de révision en moins d'une semaine
- Travaux complétés typiquement entre 5 et 10 semaines pour 20,000 comptes d'accès, 30 applications
- Coûts très avantageux

Conformité des Identités et des Accès en mode service (ICAAS)

Modalités

- Infrastructure hébergée chez OKIOK ou partenaire (RAC/M Identity)
- Données d'accès du client transportées et stockées de façon sécuritaire dans un centre de traitement sécurisé (utilisation de S-Filer)

Déroulement typique

- Rencontre de planification avec le client
- Déploiement des collecteurs (agents d'extraction)
- Traitement initiaux, construction du référentiel
- Production des premiers rapports
- Validation avec le client
- Représentant(s) du client valide les accès avec les lignes d'affaires
- Les ajustements sont apportés aux systèmes cibles
- Itérations jusqu'à ce que les critères de terminaison soient atteints
- Clôture et post-mortem du projet
- Durée typique de 5 à 10 semaines pour 20,000 comptes, 30 applications

Un exemple réel

Entreprise dans le domaine du transport

- 7,000 utilisateurs
- 8,000 identités
- 20,000 comptes d'accès
- 20 applications

Nature de la prestation

- Mise en conformité par révision systématique des accès par les gestionnaires de service
- 3 itérations – Collecte de données, production des rapports, validation

Temps total

- 5 semaines (25 jours ouvrables)

LA SOLUTION RAC/M IDENTITY

OKIOK

Solutions de sécurité d'entreprise
et d'affaires électroniques

www.okiok.com

Facilite et optimise la gestion des identités et des accès aux actifs de votre entreprise

Utilisateurs

Actifs TI et biens confiés

Entreprise

RAC/M Identity

La problématique

Impossible de savoir (et de démontrer)

- Qui a accès à quoi
- Quels comptes d'accès et quels privilèges sont requis
- Quels biens doivent être confiés (cartes d'accès, téléphones, etc.)
- Combien de licences de logiciels sont réellement requises
- Qui doit approuver les demandes d'accès
- Quels biens ont été confiés à une personne
- Que les accès accordés sont juste ce qui est requis
- Que les accès d'un utilisateur qui quitte ont été retirés
- Que les biens confiés ont été récupérés
- Que les accès attribués en exception ont été bien retirés au moment opportun

Les cadres normatifs tels que SOX, PCI, NERC, HIPAA, CobiT, SSAE16 et autres requièrent qu'une entreprise puisse démontrer qu'elle est en contrôle des accès aux actifs informationnels critiques.

Plusieurs défis…

Multitude de systèmes hétéroclites

Documentation défaillante ou inexistante

Organisation complexe et en mouvance

Modèles de gestion variés

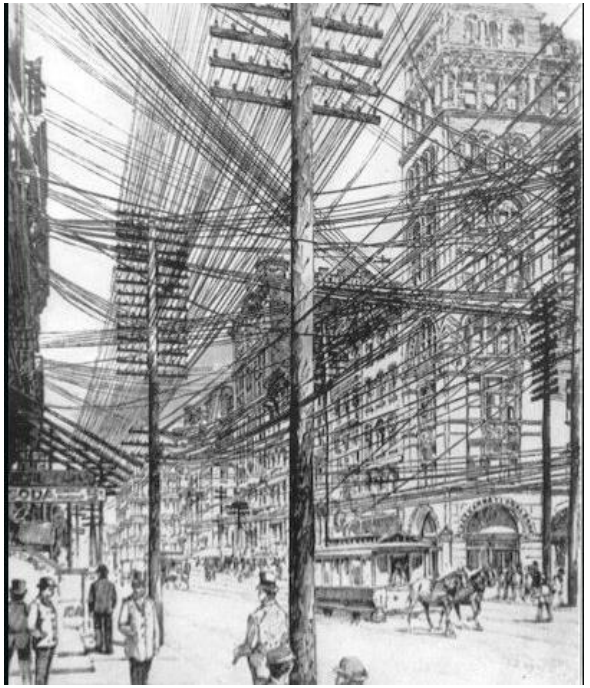
Lien d'emplois multiples et dynamiques

Incohérence des données d'accès

Écarts entre les processus RH et la réalité

Équipe de gestion des accès surchargée

Coupures budgétaires



Gestion proactive des accès logiques et des biens confiés

Personnes	Identités	Accès logiques	Biens confiés

Chantale St-Germain

Hôpital St-Jude

Chantale Saint-Germain
Médecin
Dépt.: Oncologie

Institut de Recherches

Chantal St-Germain
Chercheur
Dépt.: Recherche fondamentale

Grands principes

Constituer un référentiel

- Centraliser les informations d'accès pour offrir une vision complète et cohérente

Décentraliser les processus de GIA

- Habiliter les personnes qui connaissent les utilisateurs (principe d'AVI)
- Implanter un portail libre service

Automatiser les traitements

- Automatiser l'extraction et le traitement des données
- Initier les traitements sur les événements déclencheurs
  - Embauche / terminaison / mouvement
  - Requêtes en mode libre-service
  - Modifications au modèle d'accès

Arrimer aux systèmes connexes

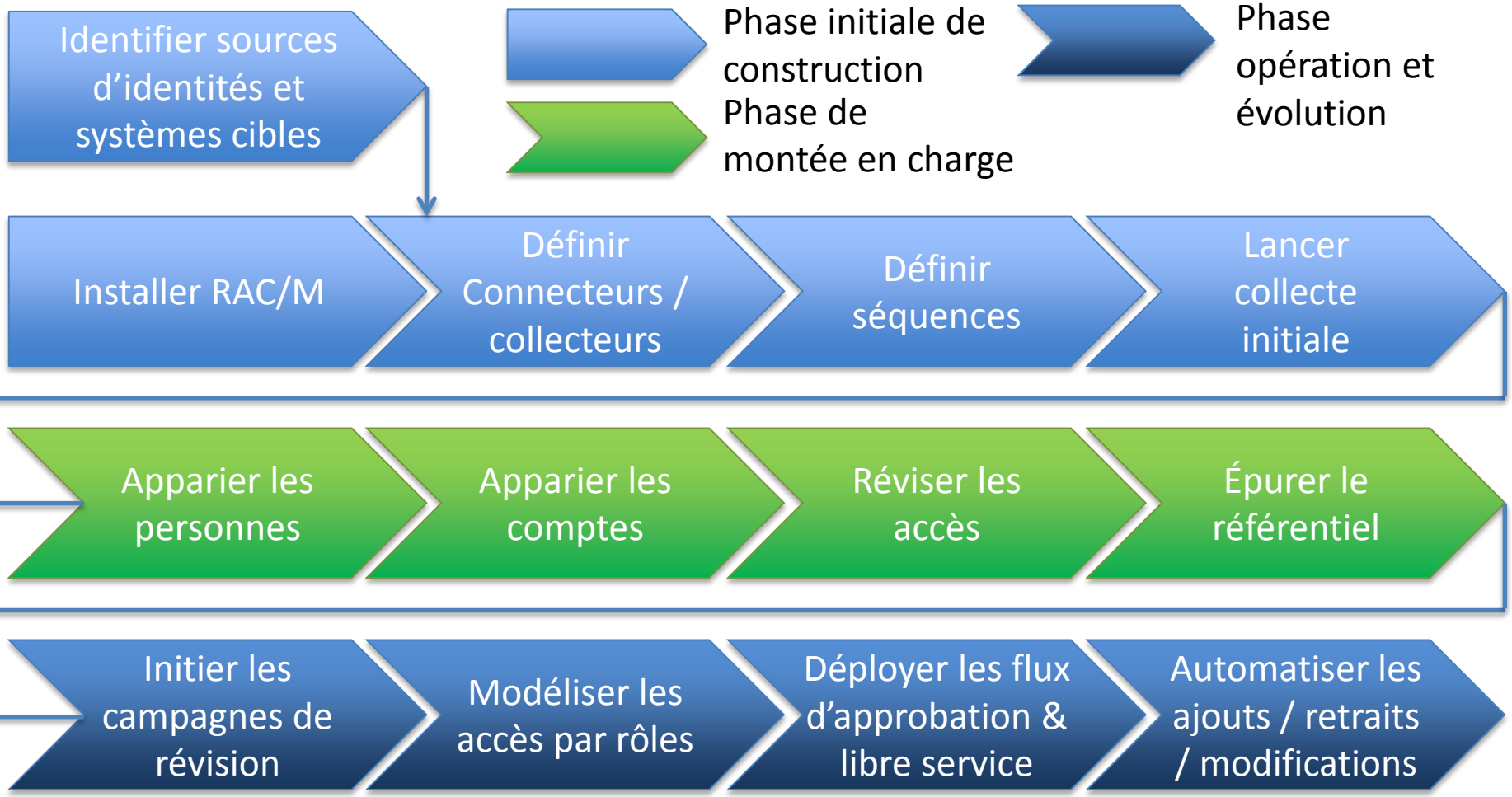
- Systèmes d'information
- Systèmes de gestion des accès
- Ex: Générateur / service d'IUN du MSSS

Fonctionnalités de RAC/M Identity

Analytique	**Déterminer** qui a accès à quoi et établir un modèle d'accès
Gouvernance	**Formaliser** les processus de requêtes et de révision
Opérations	**Implanter** le libre service et les flux de travail
Automatisation	**Ajouter**, **modifier** et **retirer** automatiquement les accès

RAC/M
IDENTITY

Planification des étapes



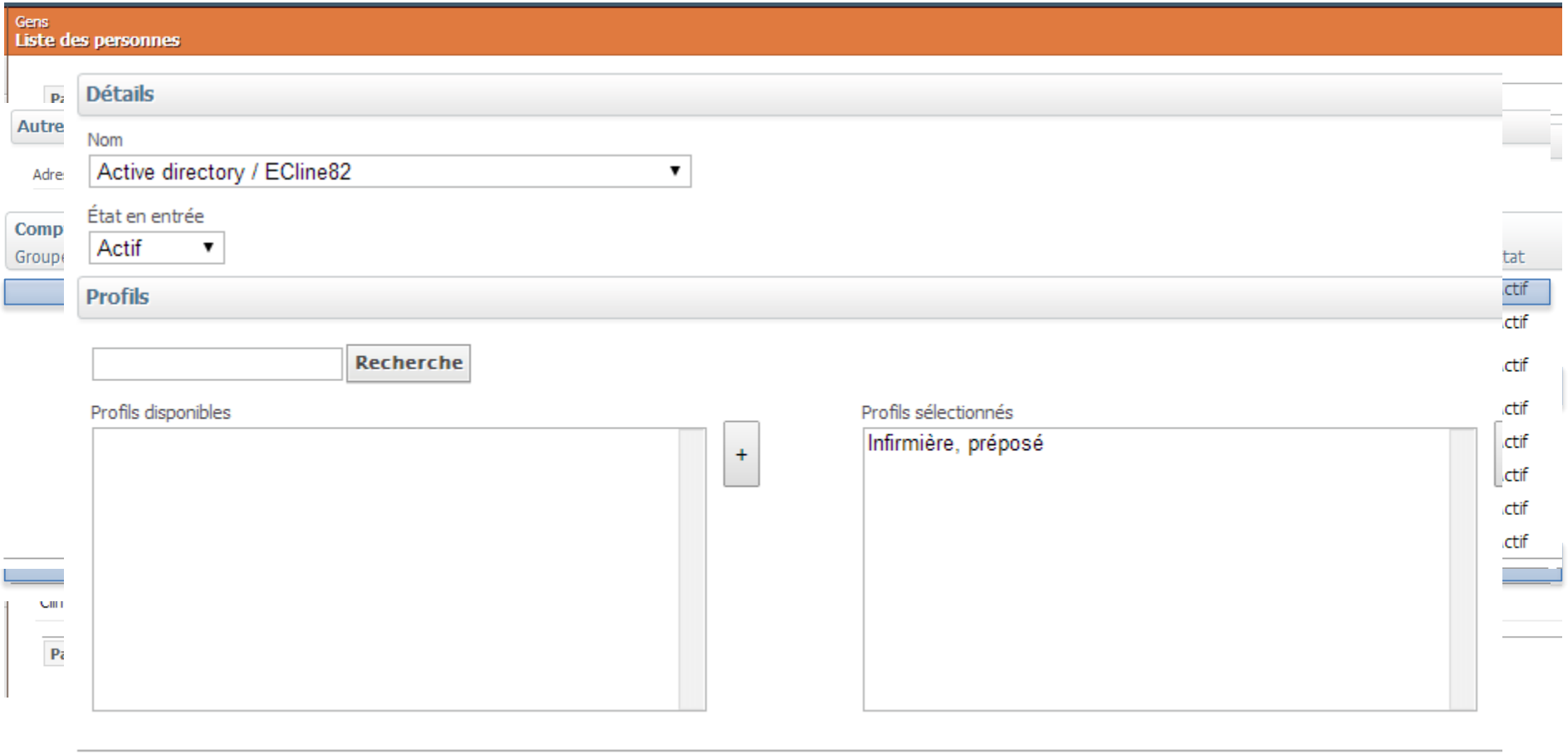
Construction du référentiel

Première étape du déploiement

- Comprend la phase de construction initiale et la montée en charge
- On doit viser à intégrer l'ensemble des sources d'identités dès le départ afin d'éviter l'accumulation de comptes « orphelins » c'est-à-dire qui ne peuvent être associés à des identités
- On intègre ensuite un petit nombre de systèmes cibles choisi parmi les plus importants ou critiques. AD fait habituellement partie des premiers systèmes à intégrer
- On procède ensuite à l'importation des identités et à la promotion des identités en personnes. Ceci n'est fait que la première fois qu'une nouvelle source d'identités est intégrée, si les identités ne peuvent être appariées aux personnes

Le référentiel en 3 clics

Personne -> Identités -> Applications -> Profils (groupes AD)



Plusieurs types de rapports

RAC/M IDENTITY

Access permission by jobs - Nurse

25/03/2014, 22:50:04

Abbott, Susan; Sainte-Marie's Hospital : Legal psychiatric care - Nurse (Actif) 383689

Application Name	*Profile*	*Type*
Active directory	Infirmière, préposé	Not in role
Active directory	Infirmière, préposé	Not in role
Lotus Notes	Utilisateurs de notes	Not in role
Medical Records Abstracting	Infirmière, préposé	Not in role
Medivisit	Utilisateurs	Not in role
Oacis	Infirmière, préposé, assistants	Not in role

Abbott, Troy; Saint-Gabriel's Hospital : Cardiovascular and Thoracic Surgery - Nurse (Actif) 384229

Application Name	*Profile*	*Type*
Active directory	Infirmière, préposé	Not in role
Active directory	Infirmière, préposé	Not in role
Lotus Notes	Utilisateurs de notes	Not in role
Medical Records Abstracting	Infirmière, préposé	Not in role
Medivisit	Utilisateurs	Not in role
Oacis	Infirmière, préposé, assistants	Not in role

Campagnes de revue des accès

RAC/M IDENTITY

DOLAN, Milton - Lacroix - Q1 2014 - Access Review Report (Full) Start Date: 02/08/2014 End Date: 02/28/2014

Milton.Dolan@LHC.com

Edgar Cline	Status : Actif	E-mail : Edgar.Cline@LHC.com	DAS ID :	
Application Groups	***Applications***	***Accounts***	***Profiles***	***Remove***
Administrative	Active directory	ECline82	Infirmière, préposé	☐
	Lotus Notes	Edgar.Cline@CHL.com	Utilisateurs de notes	☐
	Medical Records Abstracting	ECline82	Infirmière, préposé	☐
	Medivisit	ECline82	Utilisateurs	☐
	Oacis	ECline98	Infirmière, préposé, assistants	☐
	Gestion des actifs - Cartes de	Edgar Cline	Stationnement - Médecins	☐
			Stationnement - Administration	☐
	Gestion des actifs - Cartes	Edgar Cline	Accès général 234 Viger	☐
	Gestion des actifs - RFID	Edgar Cline	Puce RFID Auth base	☐

Roger ABCD	Status : Actif	E-mail : ok@bonjour.ca	DAS ID :	
Application Groups	***Applications***	***Accounts***	***Profiles***	***Remove***
	Unix file	143	uucp	☐
			Unix Access	☐
	Lotus Notes	Pour la forme	null	☐

Principe de forage des rôles

Personnes (identités)

Actifs

Les identités peuvent être filtrées par des critères arbitraires tels que:
Métier
Départements
Équipes, Groupes
Classe
Centre de coût
Site
Souscription
Inscription
Certification

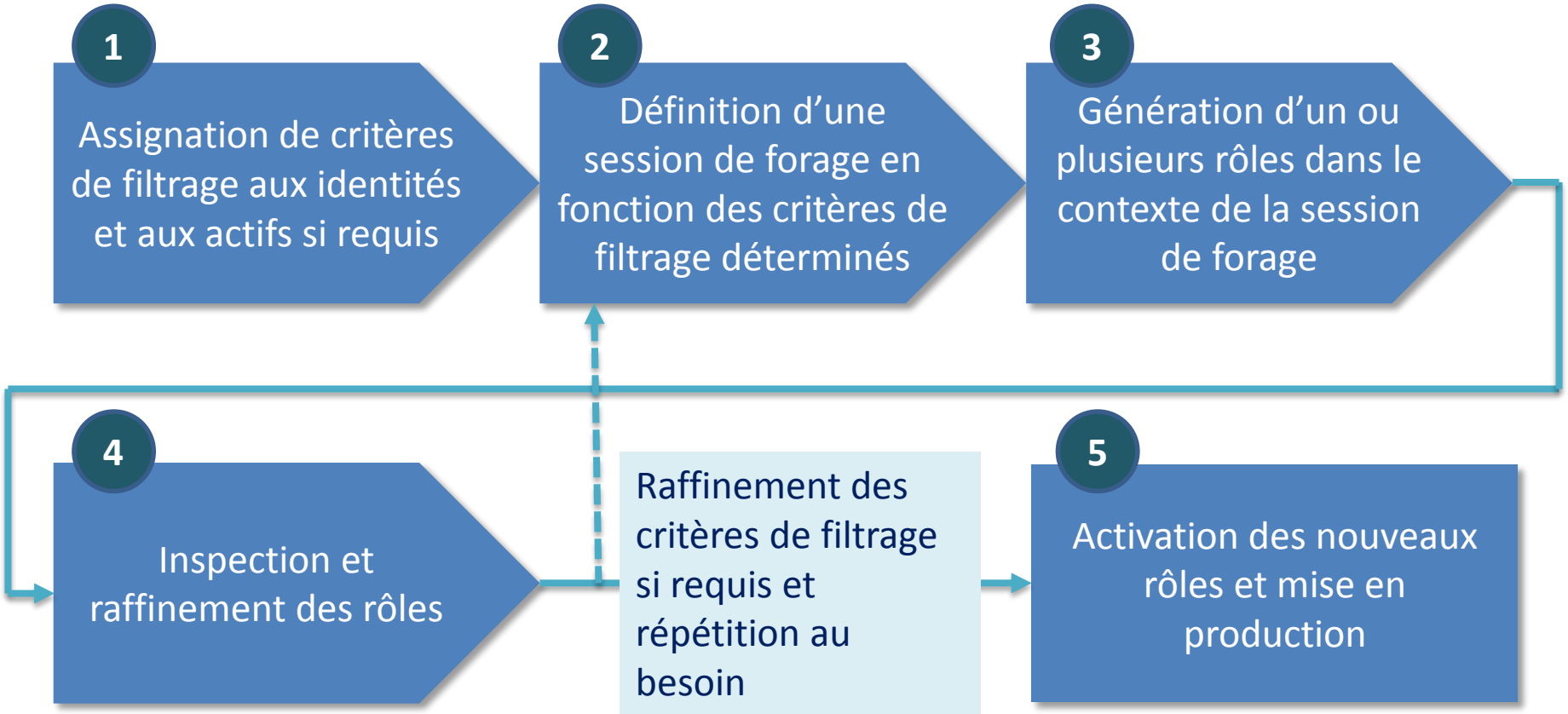
Qui accède à quoi

Le forage permet de déterminer quels accès sont détenus par un sous-ensemble de personnes

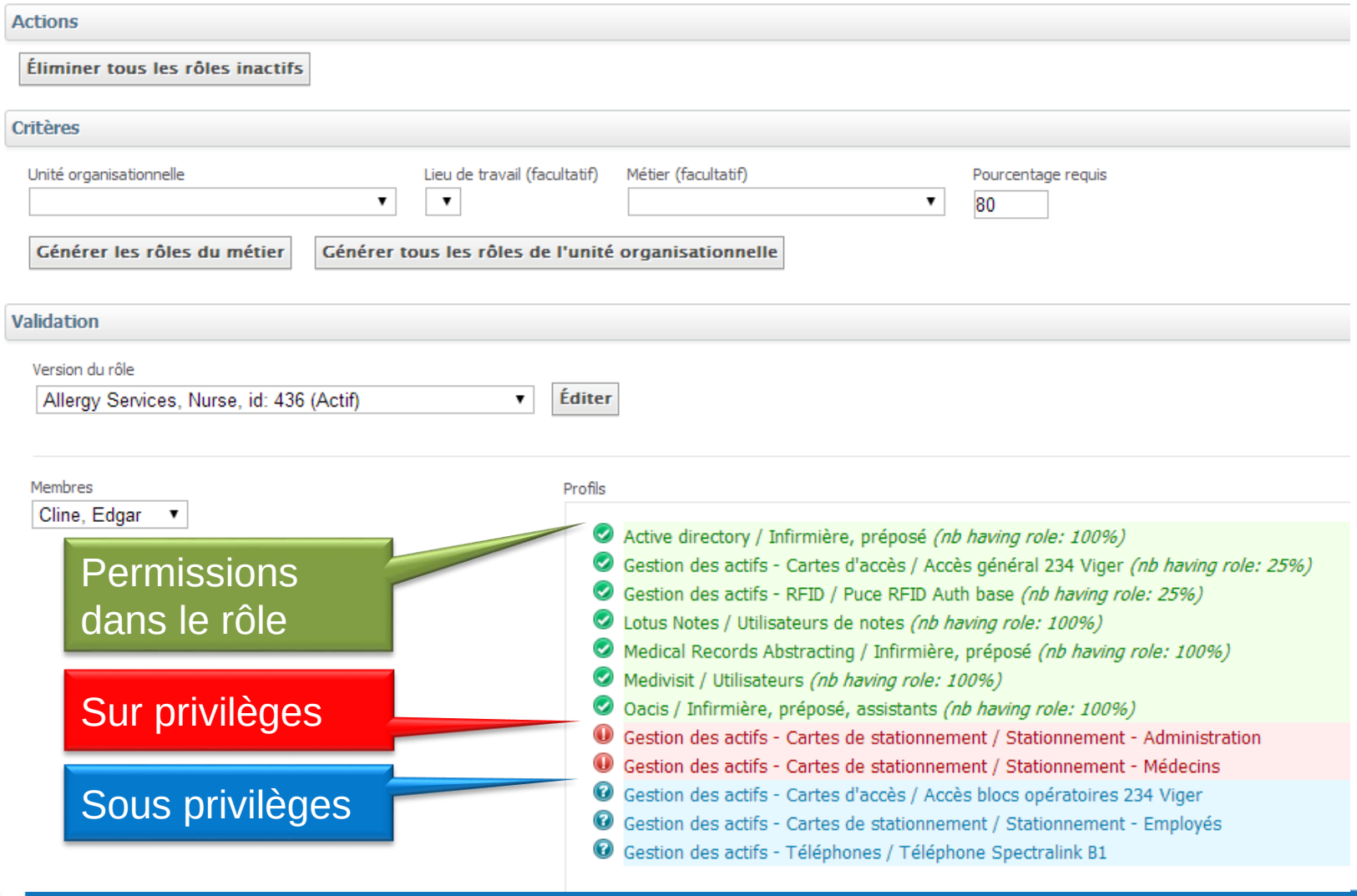
Les actifs peuvent être filtrés par des critères arbitraires tels que:

Type
Platforme
Application
Client
Site
Fournisseur
Etc.

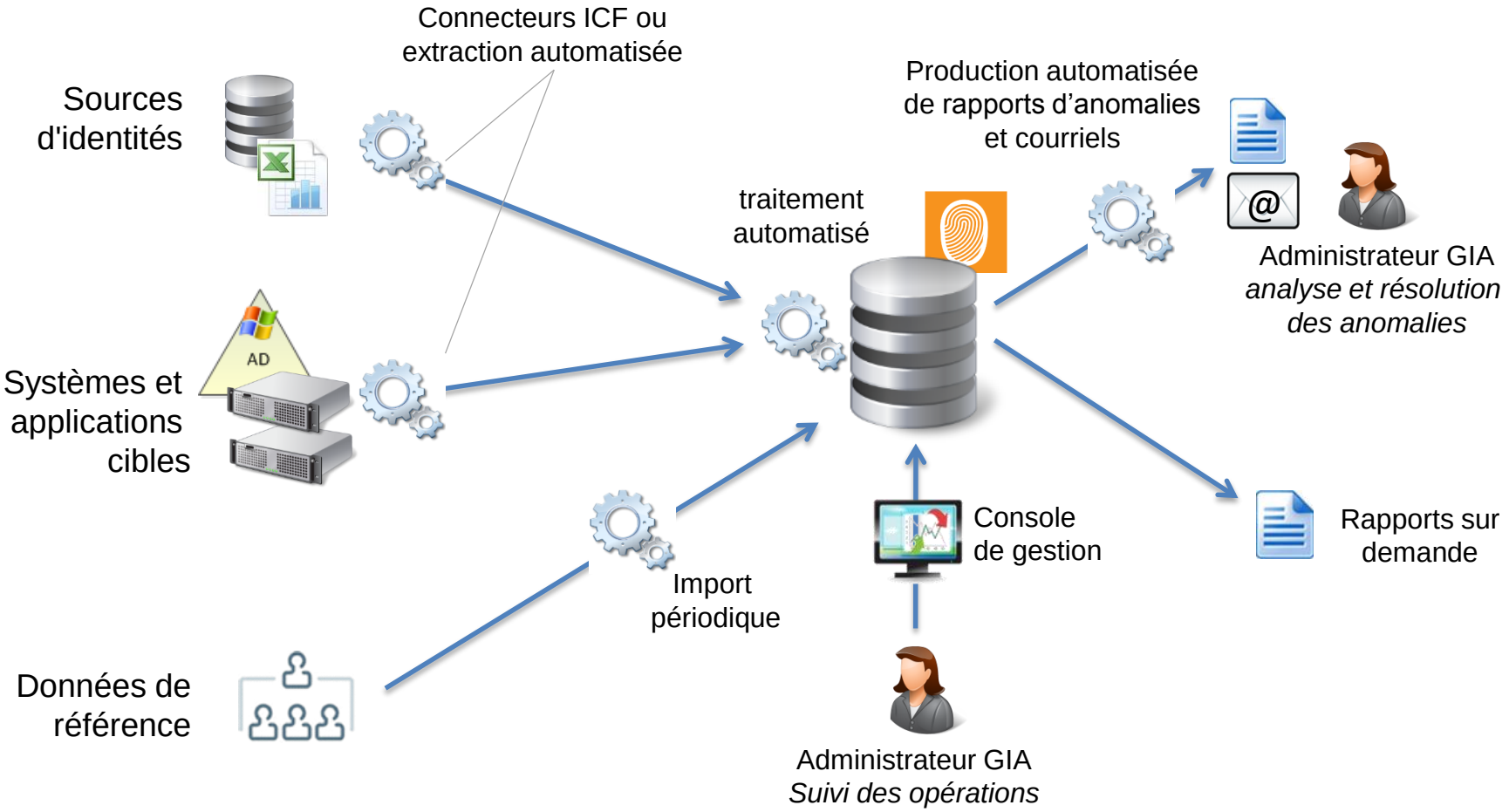
Démarche de forage



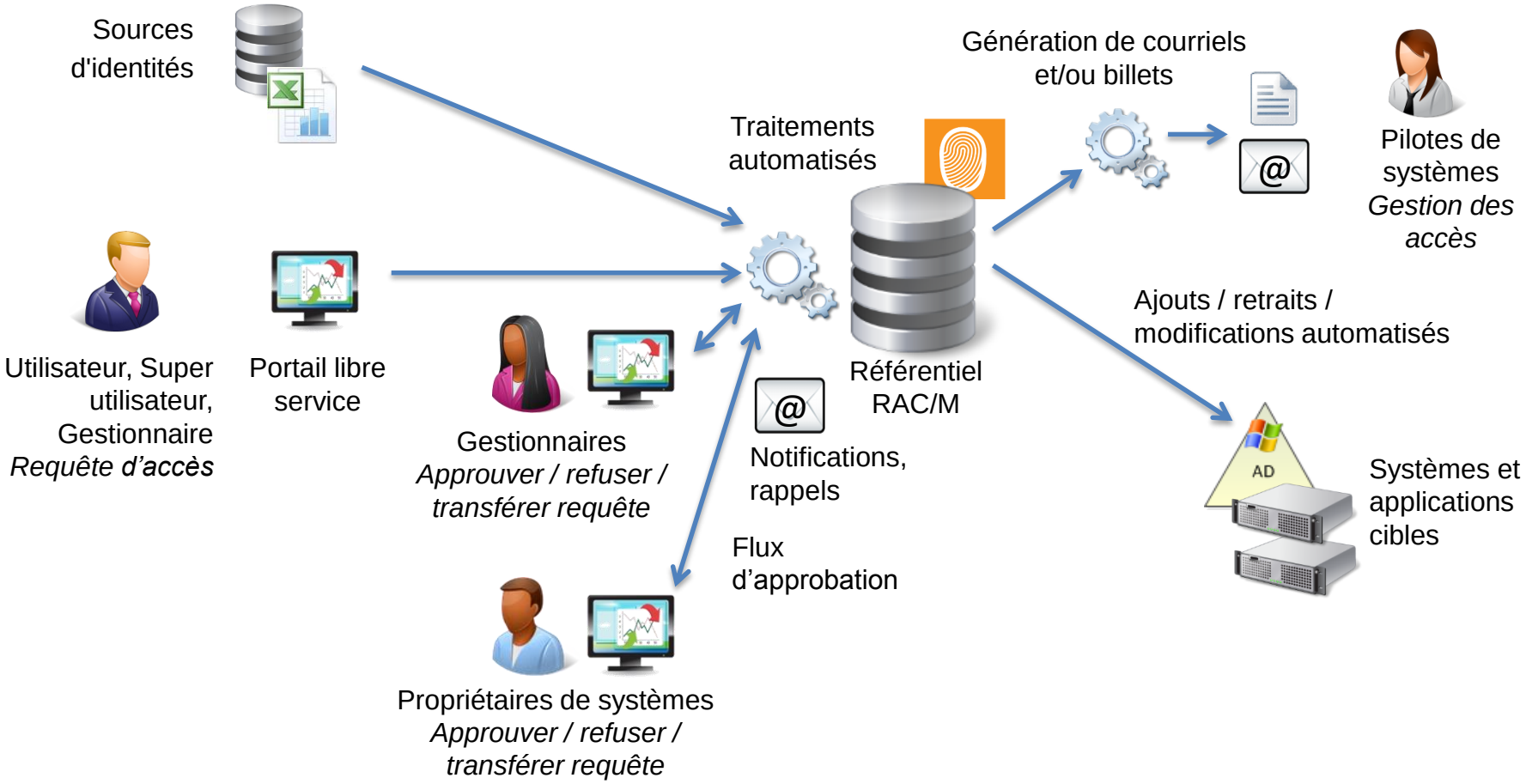
Analytique – Forage de Rôles



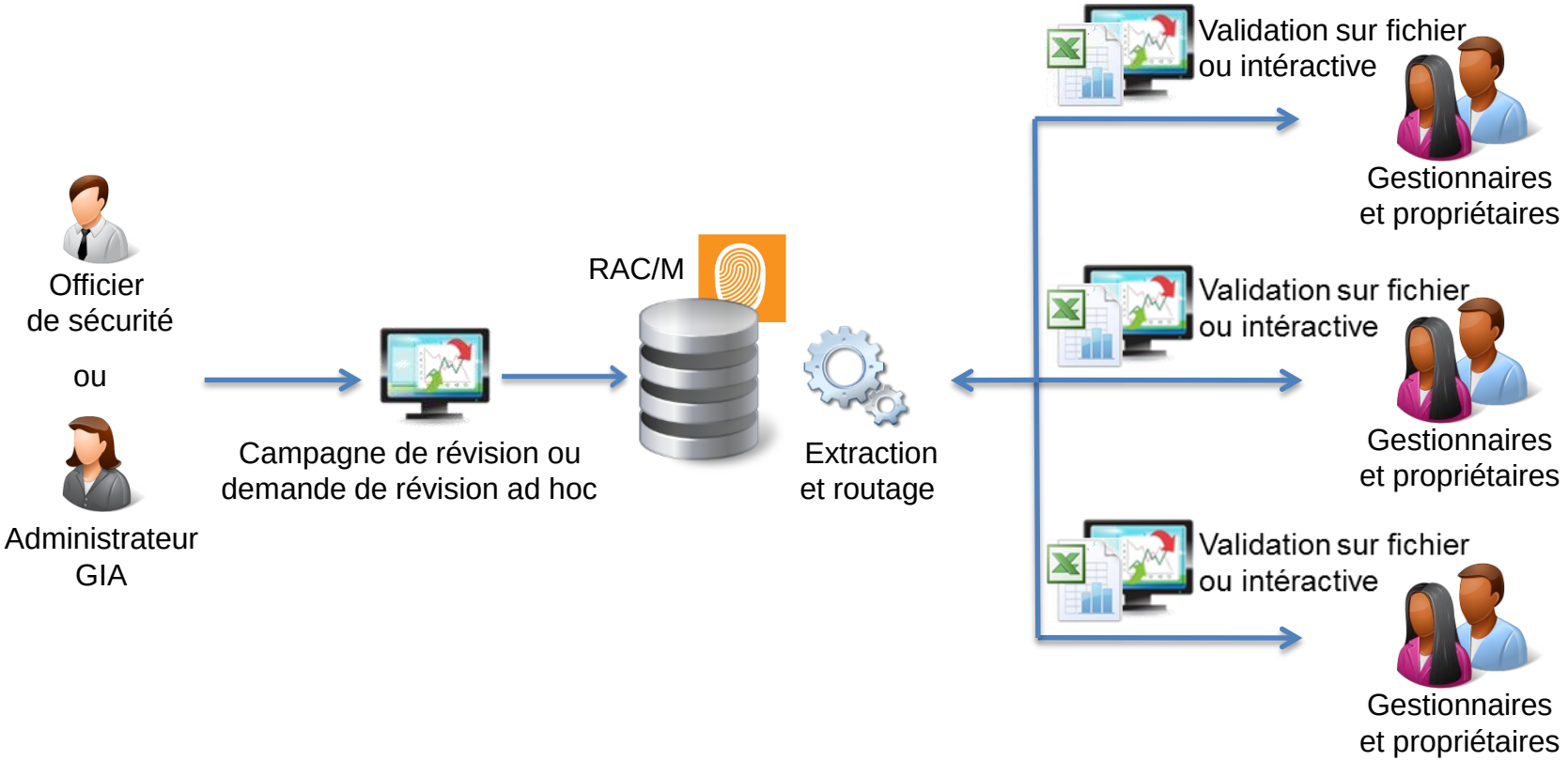
Processus de gestion du référentiel



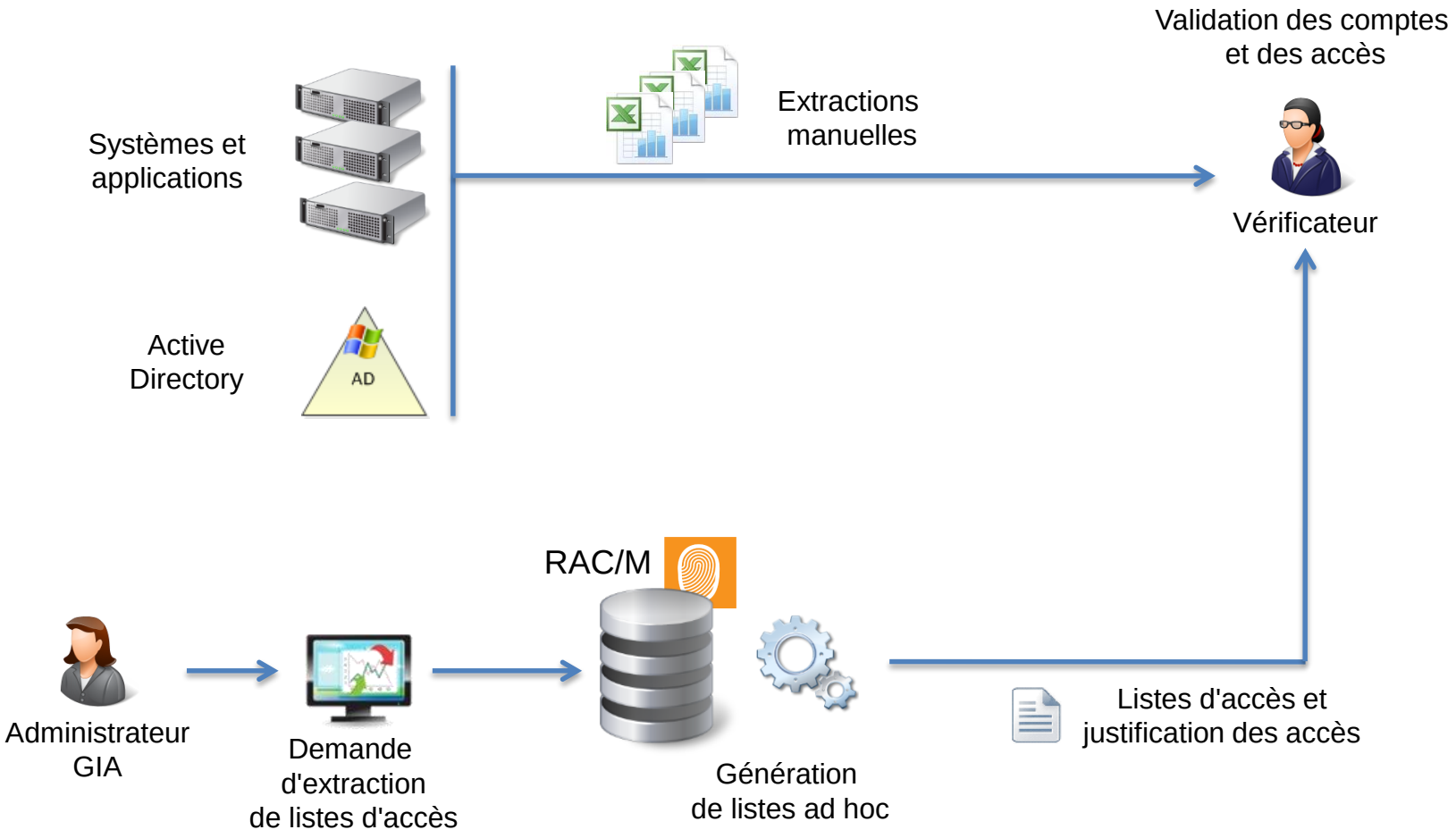
Processus de gestion des requêtes
Arrivées / départs / déplacements



Processus de revue périodique des accès



Processus d'audit



RAC/M Identity

Facilite la mise en conformité à l'échelle de l'entreprise

- Constitution d'un référentiel d'identités et d'accès et épuration initiale
- Mise en place de processus récurrents de validation et de révision périodiques des accès
- Optimisation des accès et des coûts en identifiant ceux qui sont requis et en éliminant les comptes et accès superflus

Optimise la gestion et de l'attribution des accès

- Modèle d'accès ascendant et descendant basé sur des rôles, des règles, des attributs constituant un contexte
- Libre-service et flux de travail pour l'approbation des requêtes
- Intégration aux processus d'affaires

Réduit le risque

- Identification et élimination des comptes et accès superflus
- Identification des comptes surprivilégiés
- Gestion serrée des exceptions

Bénéfices

Coûts d'acquisition, de déploiement and d'opération minimes

- Solution complète – inclus tous les éléments technologiques requis;
- Utilisation de règles pour éliminer la gestion laborieuse des rôles;
- Mécanismes d'intégration permettant d'éliminer les opérations manuelles;
- Flux d'approbation flexibles permettant le partage de charge, la délégation et l'escalade;

Évolue selon vos besoins d'affaires sans programmation

- Ajout / retrait d'applications et systèmes cibles;
- Évolution de la logique d'affaires et des blocs et séquences de traitement;
- Génération de rapports ad hoc;

Réduction des risques de sécurité

- Retrait rapide des accès non-requis lors des départs et mouvements;
- Suivi serré des droits attribués vs ce qui est requis;
- Réconciliation périodique entre les sources d'identités et les systèmes cibles;

Réduction dramatique des coûts, efforts et des délais pour la mise en conformité

- Application proactive des règles d'affaires et du modèle d'accès;
- Génération de listes et rapports sur les droits accordés ainsi que sur les écarts et exceptions;

RAC/M Identity
Spécifications fonctionnelles

Fonction analytiques

- Construction et maintien d'un référentiel d'identités et d'accès
- Traitement des sources d'identités, données complémentaires et systèmes cibles
- Appariement automatique et manuel des personnes aux identités et aux comptes d'accès
- Gestion des comptes génériques, homonymes et techniques
- Résolution des droits d'accès effectifs sous UNIX/Linux, Windows et Z/OS incluant les groupes imbriqués, globaux/locaux
- Résolution des droits d'accès aux objets et aux fichiers
- Forage & modélisation des rôles

Fonctions de gouvernance

- Formalisation des approbations
- Gestion et traitements des événements d'audit
- Séparation des tâches
- Gestion des campagnes de révision et certification des accès
- Rapports d'inventaire et exceptions
- Courriels de notification

Fonctions opérationnelles

- Portail libre service pour requêtes d'accès
- Gestion des queues de requêtes
- Notifications par courriel
- Génération de billets
- Création / modification / retrait des comptes et des accès

RAC/M Identity
Spécifications techniques

Mécanismes d'intégration

- Toutes formes de fichiers plats CSV, XLS, XLSX, LDIF, autres
- Services Web d'audit, de portail libre-service et d'approvisionnement (SPML)
- Connecteurs ICF (logiciel libre)

Technologie

- Java J2EE, conteneur Tomcat intégré
- Flux de travail JBOSS
- Serveur de BD
  - SQL Express intégré
  - MS SQL recommandé

Compatibilité

- SAP
- Logibec
- OACIS
- Active Directory
- Windows server (2003, 2008, 2012)
- HP UX 11.31
- AIX
- Linux (SUSE, RedHat)
- Z/OS
- RAC/F
- Top Secret
- ACF2
- Tous serveurs LDAP
- Toutes BD SQL
- Tous systèmes de billetterie - ex: C2, Omnitracker

Références intéressantes

http://www.puttyq.com/blog/2010/top-10-reasons-why-identity-management-projects-fail

http://evolvingidentity.blogspot.ca/2011/09/dirty-secret-of-identity-management_30.html

http://www.youtube.com/watch?v=iMhdksPFhCM

MERCI !

OKIOK

Solutions de sécurité d'entreprise
et d'affaires électroniques

www.okiok.com