

# Introduction à la gestion d'identité

Bruno Bonfils <[asyd@asyd.net](mailto:asyd@asyd.net)>

RMLL, 10 Juillet 2009

# La gestion d'identité

---

# La gestion d'identité

---

- ★ Gérer **toutes** les entités qui échangent des données avec le système d'information
- ★ Les internes
- ★ Les prestataires
- ★ Les partenaires

# Gérer une identité

---

# Gérer une identité

---

- ★ Gérer son cycle de vie et ses relations hiérarchiques avec les autres identités (*manager*)

# Gérer une identité

---

- ★ Gérer son cycle de vie et ses relations hiérarchiques avec les autres identités (*manager*)
- ★ Gérer sa propagation (*provisioning*)

# Gérer une identité

---

- ★ Gérer son cycle de vie et ses relations hiérarchiques avec les autres identités (*manager*)
- ★ Gérer sa propagation (*provisioning*)
- ★ Contrôler son utilisation (authentification et contrôle d'accès)

# Le cycle de vie d'une identité

---

# Le cycle de vie d'une identité

---

- ★ Création (ex. : signature d'un CDI)
  - ★ A quel moment créer le compte ?

# Le cycle de vie d'une identité

---

- ★ Création (ex. : signature d'un CDI)
  - ★ A quel moment créer le compte ?
- ★ Mobilité interne
  - ★ Changement de poste (période de chevauchement ?)

# Le cycle de vie d'une identité

---

- ★ Création (ex. : signature d'un CDI)
  - ★ A quel moment créer le compte ?
- ★ Mobilité interne
  - ★ Changement de poste (période de chevauchement ?)
- ★ **Départ**

# La propagation

## provisioning

---

# La propagation

## provisioning

---

- ★ Un système d'information est souvent composé de plusieurs référentiels
- ★ Active Directory pour les postes utilisateurs
- ★ Annuaire LDAP pour les serveurs UNIX
- ★ Base de données pour applications métiers

# La propagation

## provisioning

---

- ★ Un système d'information est souvent composé de plusieurs référentiels
- ★ Active Directory pour les postes utilisateurs
- ★ Annuaire LDAP pour les serveurs UNIX
- ★ Base de données pour applications métiers
- ★ **Maintien d'un dépôt maître**

# Son utilisation

---

# Son utilisation

---

- ★ Méthode d'authentications
  - ★ Faire appliquer une charte de sécurité
  - ★ Authentification forte (PKI, OTP)
    - ★ Une information que l'on possède
    - ★ Une information que l'on connaît

# Son utilisation

---

# Son utilisation

---

- ★ Le contrôle d'accès
  - ★ Qui peut accéder à quoi ? (et pourquoi)
  - ★ Gestion dans le temps des accès
  - ★ Audit / Conformité

# Son utilisation

---

- ★ Le contrôle d'accès
  - ★ Qui peut accéder à quoi ? (et pourquoi)
  - ★ Gestion dans le temps des accès
  - ★ Audit / Conformité
- ★ **Un accès : qui, quand (durée), comment, pourquoi ?**

# Les problématiques

---

# Les problématiques

---

- ★ La gestion de cycle de vie d'une identité est un processus complexe
- ★ aussi bien au niveau métier (liens avec les ressources humaines)
- ★ qu'au niveau technique

# Les problématiques

---

- ★ La gestion de cycle de vie d'une identité est un processus complexe
- ★ aussi bien au niveau métier (liens avec les ressources humaines)
- ★ qu'au niveau technique
- ★ Définir les processus est la première étape, et une des plus importante !

# La gestion d'identité dans le logiciel libre

---

# La gestion d'identité dans le logiciel libre

---

- ★ Annuaires

- ★ OpenLDAP, **OpenDS**, ApacheDS, PenRose (Virtual Directory)

# La gestion d'identité dans le logiciel libre

---

- ★ Annuaires

- ★ OpenLDAP, **OpenDS**, ApacheDS, PenRose (Virtual Directory)

- ★ SSO / Contrôle d'accès

- ★ **OpenSSO**, **LemonLDAP::NG**, Shibboleth, CAS

# La gestion d'identité dans le logiciel libre

---

- ★ Annuaires
  - ★ OpenLDAP, **OpenDS**, ApacheDS, PenRose (Virtual Directory)
- ★ SSO / Contrôle d'accès
  - ★ **OpenSSO**, **LemonLDAP::NG**, Shibboleth, CAS
- ★ PKI
  - ★ **EJBCA**

# La gestion d'identité dans le logiciel libre

---

- ★ Annuaires
  - ★ OpenLDAP, **OpenDS**, ApacheDS, PenRose (Virtual Directory)
- ★ SSO / Contrôle d'accès
  - ★ **OpenSSO**, **LemonLDAP::NG**, Shibboleth, CAS
- ★ PKI
  - ★ **EJBCA**
- ★ Provisioning / Synchronisation
  - ★ **OpenRegistry**, **LSC**

# Merci de votre attention

La suite dans quelques instants...

- LSC, Jonathan Clarke
- OpenDS, Ludovic Poitou
- EJBCA, Tomas Gustavsson
- OpenRegistry, Benn Oshrin
- OpenSSO, Fulup Ar Foll
- LemonLDAP::NG, Clément Oudot

Table ronde sur la gestion d'identité  
cette après midi à 15h40 !