Garder la tête dans les nuages

Symposium GIA – Montréal

26 novembre 2015

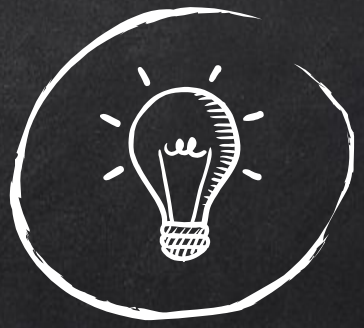
Facilité

Cloud =
Internet

Use cloud services
to solve cloud era problems
–Kim Cameron

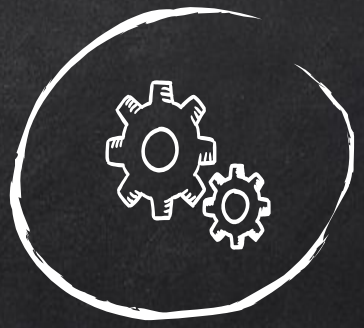
Application “Cloud Native”

- ✘ Pas d’installation
- ✘ Libre-service
- ✘ Protocoles standards/ouverts
- ✘ Facturation à l’utilisation
- ✘ Élasticité/Internet-scale
- ✘ API public disponible



Quelques Définitions ...

- ✘ Identification
- ✘ Authentification / AuthN
- ✘ Autorisation /AuthZ
- ✘ AuthN Multi-facteurs
- ✘ Approvisionnement / Provisioning
- ✘ Revalidation des accès / attestation / certification

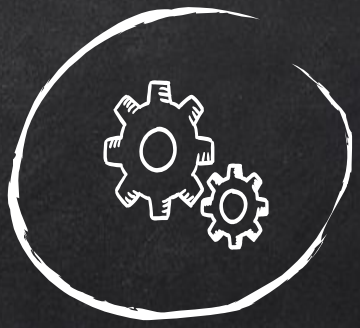


Les Modèles d'intégration AuthN

- ✘ Via des standards (SAML, oAuth, JWT, etc.)
- ✘ Voûtes à mot de passe (credential replay)
- ✘ Authentification Intégrée Windows (Kerberos)
- ✘ Libraries pour intégration rapide dans les applications

Les Modèles d'intégration AuthZ

- ✘ Autorisation "coarse grained" dans la GIA
- ✘ Autorisation fine dans les applications via RBAC
- ✘ Utilisation d'un PEP externe (ex.: WAF)



Intégration Approvisionnement et revalidation

- ✘ Aucune intégration (JIT provisioning)
- ✘ Synchronisation avec répertoire(s) interne
- ✘ Utilisation de protocoles standards SPML / SCIM
- ✘ API spécialisés
- ✘ Passerelle et des connecteurs
- ✘ Échange de fichiers

Authentification Multi-Facteurs
Les possibilités

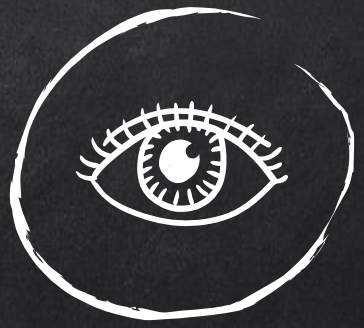
- ✘ Appels téléphonique avec OTP
- ✘ Reconnaissance de la voix
- ✘ OTP par SMS ou application mobile
- ✘ Autoriser des transactions spécifiques
- ✘ Validation du client (endpoint security)
- ✘ Lecteurs biométriques

Quand utiliser une GIA "cloud native"?

- ✘ Courts délais et/ou solution temporaire
- ✘ S'intégrer avec d'autres services cloud
- ✘ Mobilité des utilisateurs/accès via Internet
- ✘ Intégrations basées sur standards ouverts
- ✘ Développement d'applications Mobiles
- ✘ Développement avec nouveaux langages/framework
- ✘ Grosses variations de volumes transactionnels
- ✘ Préoccupations de sécurité mais peu de moyens
- ✘ Cas simples de gestion des accès et mots de passe

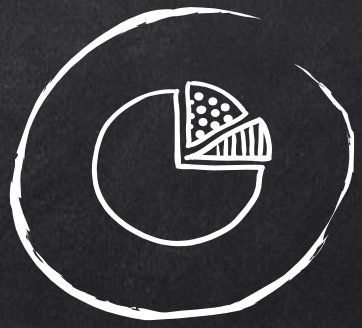
Quand **NE PAS** utiliser une GIA "cloud native"?

- ✘ Intégration avec des applications lourdes/desktop
- ✘ Intégration avec des systèmes legacy
- ✘ Besoins complexes de revalidation des accès
- ✘ Requis réglementaires ou politiques de conserver les données sur site
- ✘ Multi-domaines AD
- ✘ Aucune source autoritaire d'identité



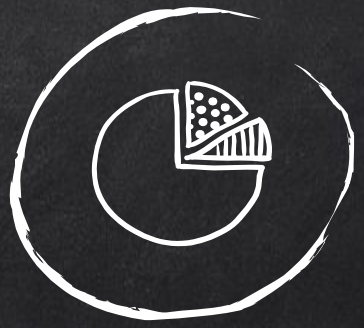
À surveiller

- ✘ Disponibilité d'une interface en français
- ✘ Utilisation des données par le fournisseur
- ✘ Pays où les données seront hébergées
- ✘ Sécurité/certifications/politiques de confidentialité
- ✘ Sauvegarde des données
- ✘ Éducation des utilisateurs contre la réutilisation des mots de passe et le hameçonage
- ✘ Budget



Les principaux joueurs

- ✘ Okta
- ✘ OneLogin
- ✘ Centrify
- ✘ Microsoft (Azure Active Directory)
- ✘ Sailpoint (IdentityNow)
- ✘ Ping Identity (PingOne)
- ✘ Salesforce



Les innovateurs

- ✘ Auth0 (pour son rule engine)
- ✘ Stormpath (pour son API)
- ✘ Gigya (GIA pour les clients/consumer IAM)
- ✘ Janrain
- ✘ Authentify
- ✘ DuoSecurity

QUESTIONS ?

Vincent Brousseau
Conseiller principal en architecture GIA, Groupe Facilité
vbrousseau@facilite.com

Facilité