21 octobre 2025 - PARIS

Entra ID Governance en action
Témoignage d’une migration d’IGA réussie

Jean-Sébastien DUCHÊNE

AGENDA DE LA CONFÉRENCE

- Aperçu des situations en entreprise
- L'IGA Nouvelle Génération
- Les erreurs à ne pas faire pour démarrer le projet
- L'approche projet gagnante
- Quel déploiement/migration faire ?
- Focus sur trois retours d'expériences
- Les orientations à venir
- Conclusion

Jean-Sébastien DUCHÊNE

Directeur Technique @EXAKIS-NELITE

Microsoft® Most Valuable Professional Security

Blogguer (windowstouch.fr), Ecrire, Partager, etc.

Expertise : Identité, Modern Workplace, Cloud et Sécurité

@microsofttouch

linkedin.com/in/jeansebastienduchene

Aperçu des situations en entreprise

Aperçu des situations en entreprise

Sur les identités et les applications

Legacy

- Des applications héritées (Legacy)
- Protocoles d'authentification non modernes (NTLM, Kerberos, Radius, etc.)
- Les référentiels d'utilisateurs utilisent parfois Active Directory (meilleur des cas) ou sont dédiés et non interconnectés
- Architecture non imaginée pour embrasser la mobilité hors de l'entreprise.

Ceci engendre **fragmentation**, non-conformité réglementaire, **incompatibilité** avec l'approche **ZeroTrust**, **coût de maintenance**, **risque de sécurité**, etc.

Cloud

- Des protocoles d'authentification modernes et standardisés (SAML, OpenID, etc.)
- Un standard de provisionnement (SCIM) (*pas systématique*)
- Un référentiel unique avec la gestion du cycle de vie et du provisionnement intégré.
- Support native du travail hybride

Approche **centralisée**, sécurité renforcée (**ZeroTrust**), **coût de maintenance réduit**

Hybride (et orientation vers le Cloud)

- Des transformations qui prennent du temps.
- Des niveaux de maturité disparates
- Des approches différentes pour gérer les identités et la sécurité de ces deux mondes

Les conséquences sont importantes : **non homogénéité** des processus, **fragmentation** des identités et de la traçabilité, **risque de sécurité**, **coût de maintenance élevé**

Aperçu des situations en entreprise

Sur la gestion et gouvernance des identités

1

MANUEL

Les processus sont gérés à la main par des techniciens :

- Erreurs fréquentes
- Inconsistance des pratiques
- Traçabilité inexistante
- Lenteur des processus
- Chute de la productivité
- Sécurité faible
- Non-conformité réglementaire
- Peu fiable à grande échelle
- Coûts cachés et risques (perte des ressources, connaissances, etc.)

2

SCRIPTS

Les processus sont gérés par des scripts :

- Maintenance lourde (TMA)
- Dépendances sur des compétences internes
- Absence de standardisation
- Traçabilité limitée
- Sécurité faible
- Souvent non fiable
- Non-conformité réglementaire
- Peu fiable à grande échelle

3

FRAMEWORKS EXISTANTS

Les processus sont gérés automatiquement via l'utilisation d'un Framework et de personnalisation:

- Complexité de personnalisation (TMA)
- Faible agilité métier
- Maintenance et évolutivité limitée
- Courbe d'apprentissage très élevée
- Sécurité et conformité non garantie
- Interopérabilité limitée avec les applications Cloud
- Coûts cachés de développement et maintenance

4

SOLUTIONS HÉRITÉS

Les processus sont gérés automatiquement l'utilisation d'un outil (MIM, etc.) :

- Rigidité et obsolescence technologique
- Workflows peu agiles
- Expériences utilisateur limitées
- Sécurité et conformité non natives
- Maintenance élevée
- Mise à l'échelle limitée

L’IGA Nouvelle Génération

Architecture

- Cloud-native
- API-first
- Microservices

Sécurité et Conformité

- Approche Zero Trust (Revue des accès, Réconciliation, etc.)
- Journalisation complète
- RGPD natif

Provisionnement

SCIM

Expérience utilisateur

- Interface utilisateur fluide
- Orientée Self-Service
- Campagne de certification/validation

Rôles & Habilitations

Dynamiques, contextuels et basés sur les attributs

Gestion des identités étendues

Employés, partenaires, freelances, clients, identités machines, IAs (agents...), etc.

Les erreurs à ne pas faire pour démarrer le projet

Les erreurs à ne pas faire pour démarrer le projet

Pas de cadrage **fonctionnel** des processus en amont

Cibler un outil plutôt que ses besoins

Adresser tous les cas d'usages dont les plus « rares »

Faire un projet en cycle en V

L’approche projet

L’approche gagnante

1 Cadrage fonctionnel

Cadrage des besoins fonctionnelle en matière de gestion et de gouvernance des identités (IAM/IAG).

2 Présentation des Outils

Présentation des différentes solutions Entra

3 Cadrage Du MVP

Cadrage de la solution minimale (MVP) attendue pour démontrer les capacités

4 MVP

Mise en œuvre des fonctionnalités de Microsoft Entra permettant de découvrir les cas d’usages et fonctionnalités définis dans le cadrage.

5 Restitution du MVP

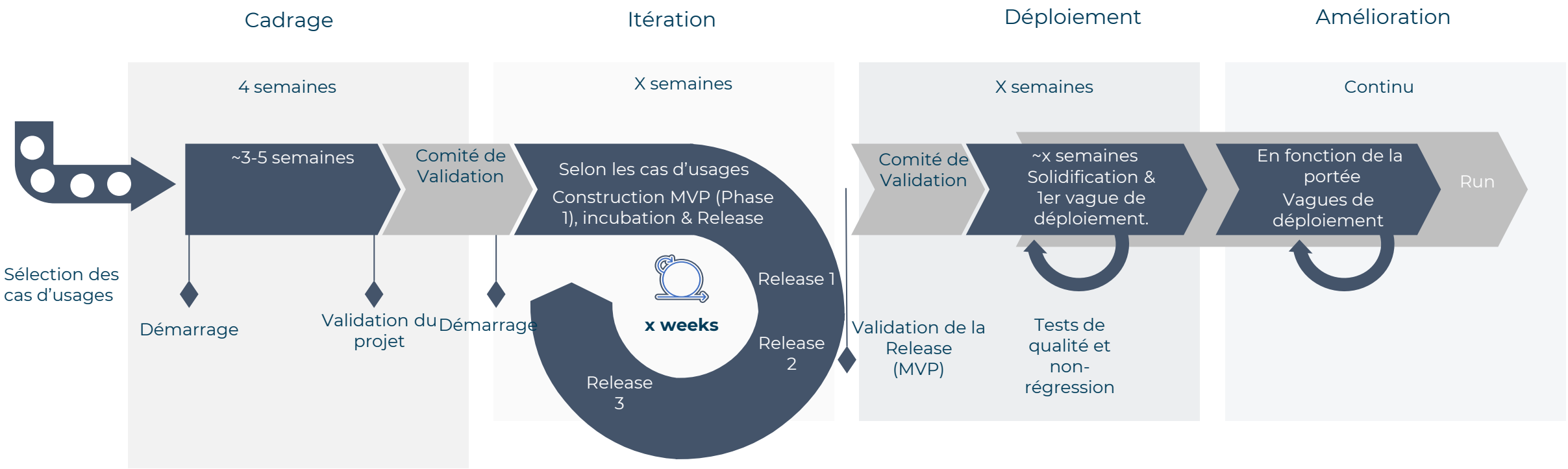
Analyse et présentation des différents composants mis en place pour couvrir les besoins fonctionnels exprimés pendant le cadrage

6 Améliorations itératives du MVP

Une fois le MVP validé, ajustement de la solution pour un passage en production

Cadrage accéléré

L'approche gagnante



Quelle déploiement/migration faire ?

Big Bang

+
- Transition immédiate et cohérence globale
- Simplification du processus (pas de double maintenance)

−
- Projet qui peut ne jamais atteindre sa cible
- Risque élevé & forte pression projet
- Resistance au changement

Approche à haut rendement mais haut risque

Par Business Unit

+
- Transition ciblée, adaptée et ajustable
- Apprentissage progressif
- Réduction des risques

−
- Allongement du projet
- Complexité de coordination
- Coexistence temporaire à gérer

Idéale pour des organisations complexes afin de maitriser, limiter le risque

Par User Story

+
- Alignement fort avec le métier
- Agilité et flexibilité
- Meilleure adoption des utilisateurs
- Réduction des risques
- Mesure rapide du ROI

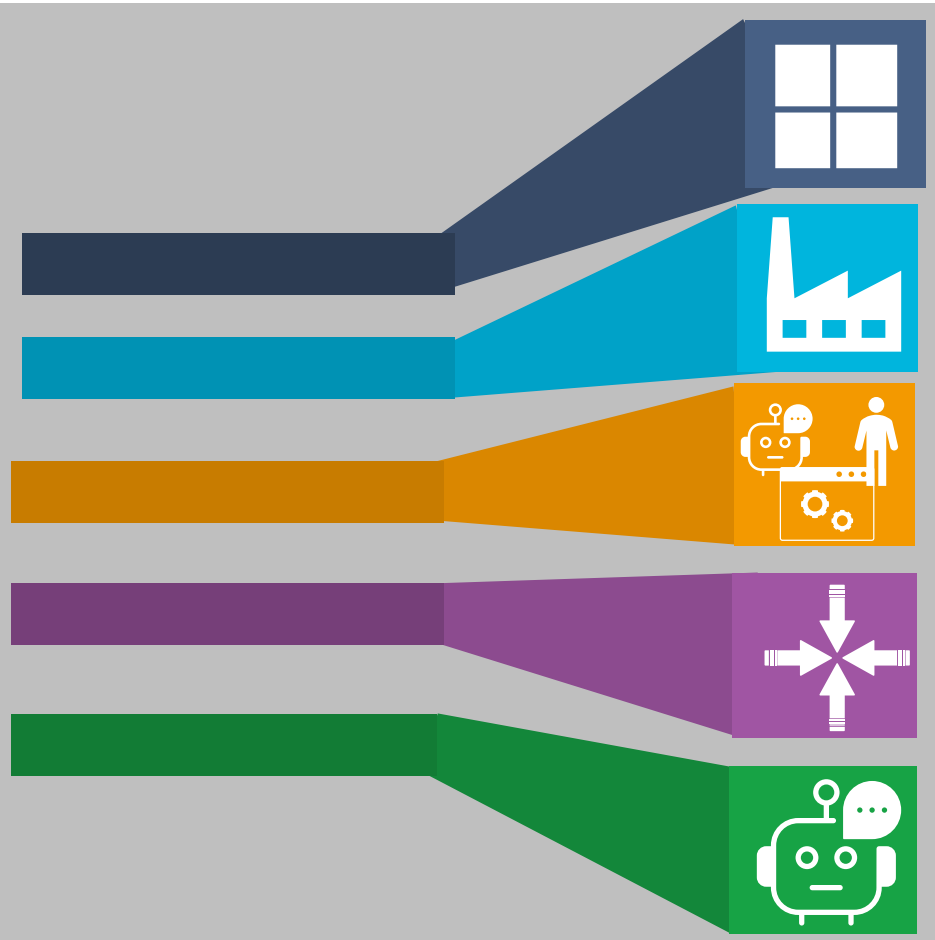
−
- Complexité de gouvernance
- Multiplication des tests et validations
- Coexistence temporaire à gérer
- Durée du projet difficile à estimer

Approche centrée sur la valeur métier apportant une agilité en limitant les risques

Focus sur trois retours d’expériences

Orientations & Conclusion

Orientations à venir



Microsoft a une **feuille de route ambitieuse** (réconciliation, etc.) et de faire d'Entra la source d'autorité (User SOA, Group SOA, etc.)

Des projets qui vont tendre vers « **l'Identity Factory** » avec une équipe et une démarche itérative sans approche projet (réponse **aux besoins métiers**)

L'identité utilisateur **n'est plus la seule identité** à gérer. Il faut gérer les identités **machines**, **applicatives**, **IA**, **Agents**, etc.

Convergence des **marchés IAM / IGA / CIEM / ZTNA** à prévoir. Microsoft a déjà donné la direction avec **Entra Suite**

L'**Intelligence Artificielle** s'intègre dans les solutions de gestion d'identité avec **des agents** afin de répondre à des besoins (revue des accès, etc.)

Conclusion

1

Etudiez et Cadrez !

Avant de démarrer, posez tous vos cas d'usages fonctionnels et contraintes
Réfléchissez à comment vous souhaiteriez les modéliser

2

Choisissez la bonne méthode de construction et de déploiement

Utilisez la méthode Agile et éventuellement construisez une Identity Factory
Déployez/Migrez par petits pas (User Stories)

3

Choix de la solution

Ne choisissez pas l'outil en fonction de ses capacités mais bien de vos besoins
Ne bloquez pas une approche pour un cas d'usages à la marge
Prenez en compte les ressources disponibles sur le marché
Privilégiez l'approche Plateforme et pensez à demain !

4

Orientez vous vers le futur

Pensez à l'arrivée de nouveaux types d'identité (Agents IA, Identités Machine, etc.) ou du multicloud
Imaginez que vos processus de gestion d'identité vont être boostés par l'IA

21 octobre 2025 - PARIS

IDENTITY DAYS

@IdentityDays
#identitydays2025