

Identity Excellence Day

Projet de refonte IAM @ UNIGE

Division du Système et des Technologies de l'Information et de la
Communication (DiSTIC)



**UNIVERSITÉ
DE GENÈVE**

Ordre du jour

- Contexte UNIGE
- Situation initiale
- Notre projet
- Situation actuelle
- Facteurs de succès
- Prochaines étapes

Contexte UNIGE

Division du Système et des Technologies de l'Information et de la
Communication (DiSTIC)



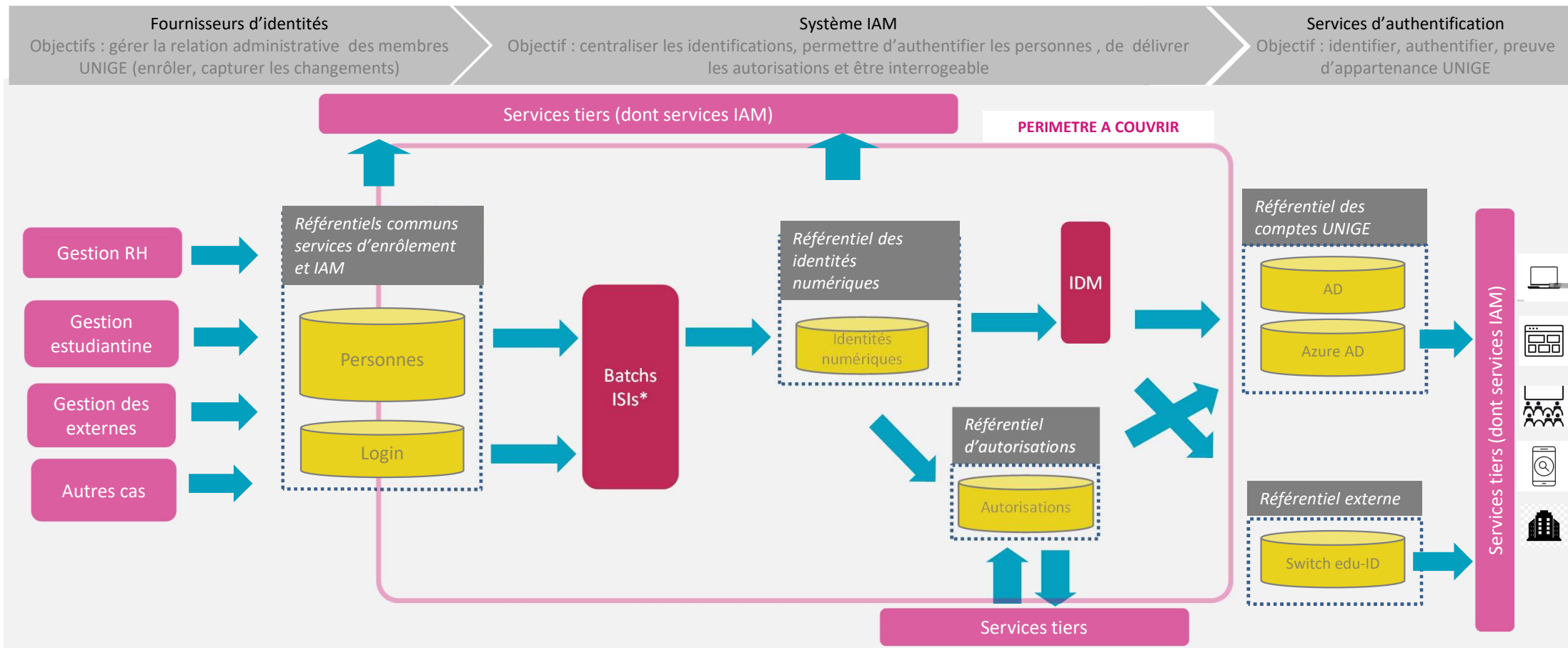
**UNIVERSITÉ
DE GENÈVE**

L'UNIGE

- 58^{ème} au classement Shangaï 2025 des meilleures universités mondiales
- 27'000 étudiants répartis dans 9 facultés, centres et instituts
- 12'400 collaborateurs
- 2'200 étudiants et collaborateurs
- Un éco-système IAM au service d'une variété des profils

Situation initiale

Systeme IAM avant migration



ISIs* : Infrastructure des Systèmes d'Identifications

Division du Système et des Technologies de Communication (DiSTIC)

- Composants IAM critiques
- Applications qui interagissent avec le système IAM
- Flux de données
- Référentiels IAM



UNIVERSITÉ
DE GENÈVE

Solution initiale - Composants IAM critiques

Batches ISIs*

- Scripts monolithiques
- Complexes
- Processus métiers intégrés aux scripts
- Evolutivité contraignante voir impossible

IDM

- Identity Manager de NetIQ (Novel)
- Solution non documentée
- Plus de support

ISIs* : Infrastructure des Systèmes d'Identifications

Gouvernance et organisation

- Considéré comme sujet technique
- Pas de sponsor hors IT, faible appétence pour le sujet
- Turn-over / départ des équipes
- Perte de maîtrise du cadre et de certaines règles
- Fonctionnement de l'équipe IAM en silo

Notre projet

Objectifs

En matière technologique ...

- Traiter obsolescence
- Interconnecter, y compris avec les solutions Cloud
- Maîtriser de la solution
- Ne pas impacter les services d'authentification (AD, IdP, MFA)

... et gouvernance

- Définir les rôles et responsabilités
- Impliquer toutes les parties prenantes
- Maîtriser des processus IAM
- Documenter
- Systématiser les revues de droits

Contraintes

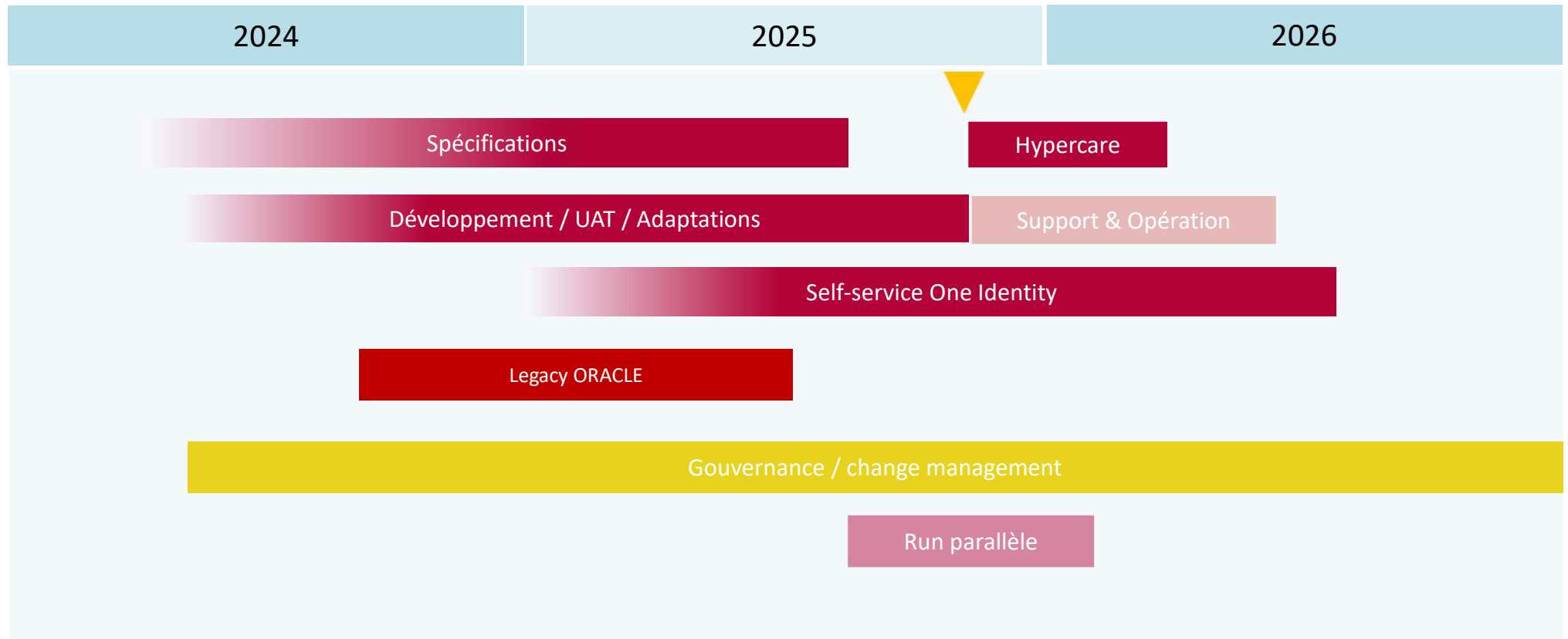
Technique

- Un SI administratif historique très imbriqué
- En pleine refonte
- Parties prenantes déjà fortement occupées
- Lancement en mode «*big bang*»
- Service essentiel

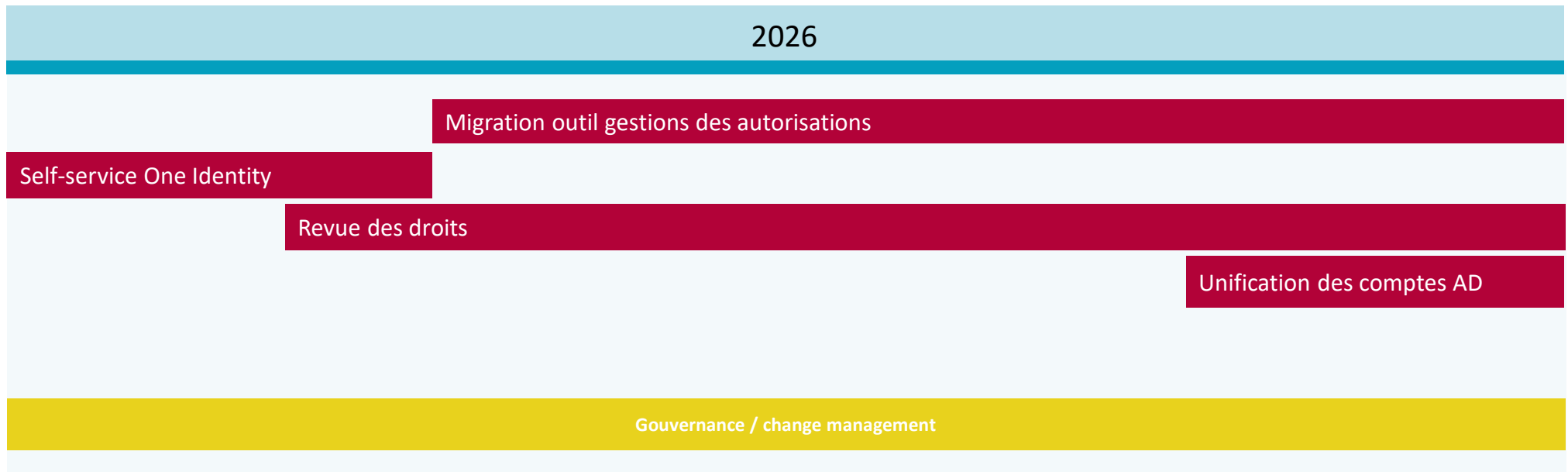
Activité

- Pas d'interruption de service
- Veiller aux inscriptions
- Tenir compte des périodes d'examens
- Être attentif à la présence des personnes essentielles au support (hypercare)

Planification phase 1 : mise en production

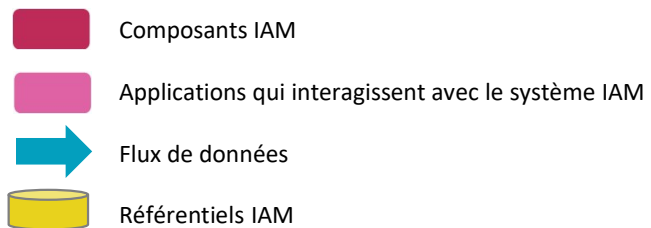
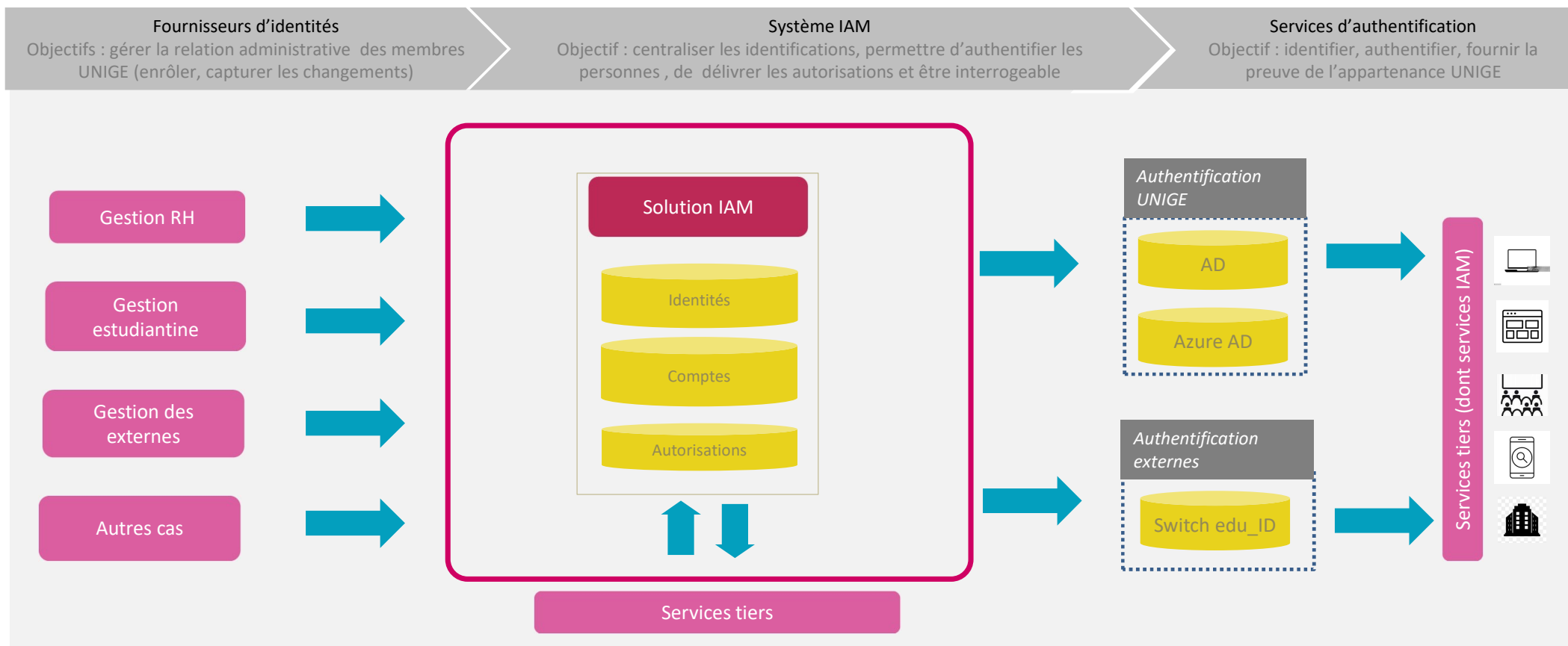


Planification phase 2



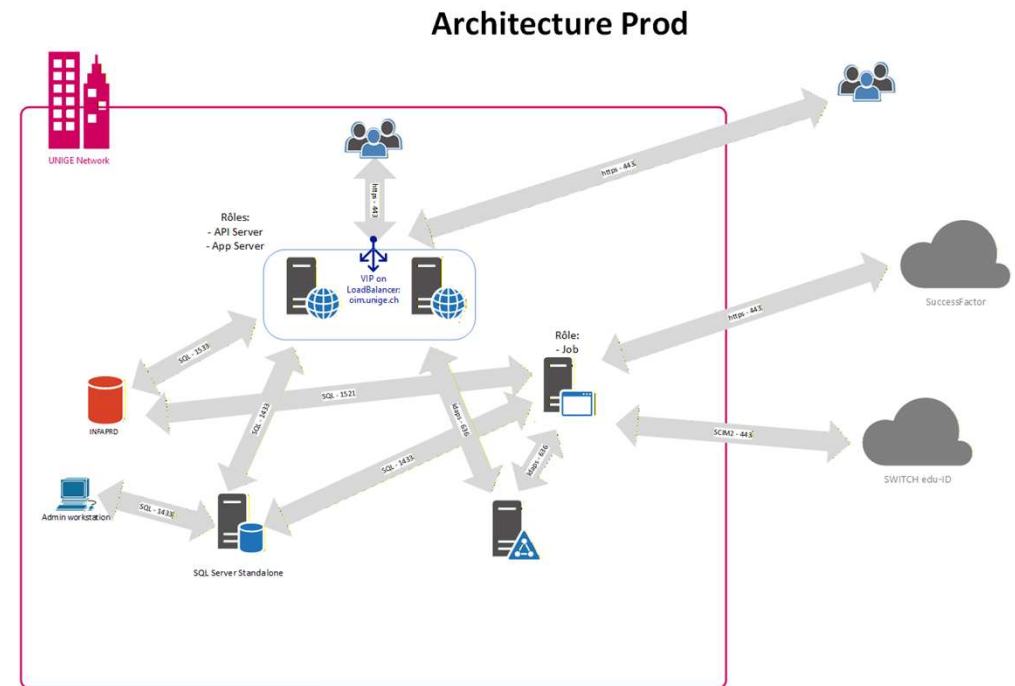
Situation actuelle

Système IAM cible

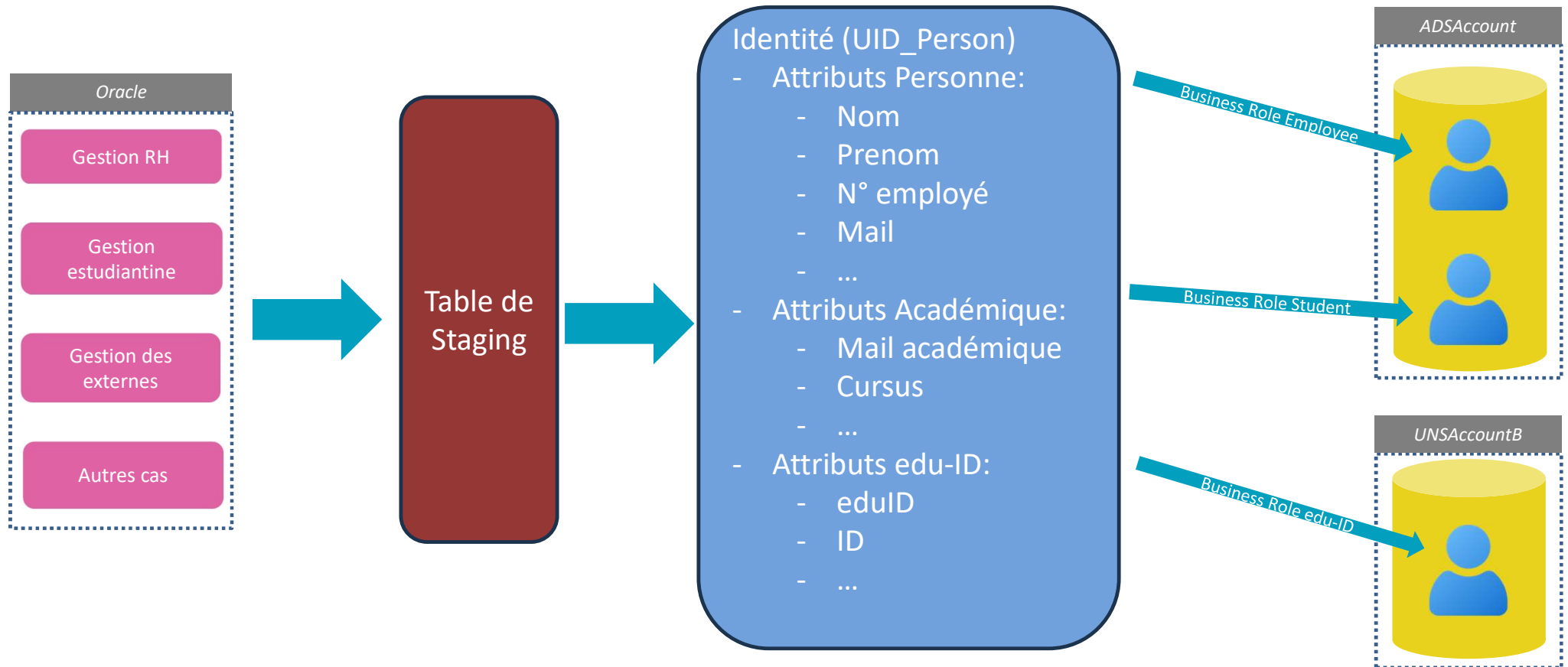


Architecture technique - One Identity Manager

- 3 environnements:
 - Dev (1 serveur + BDD)
 - Test (3 serveurs + BDD)
 - Prod (3 serveurs + BDD)
- Les environnements de test et de production ont les mêmes caractéristiques techniques à savoir:
 - 2 serveurs web
 - 1 serveur applicatif (job server)
 - 1 serveur de base de données



One Identity Manager – Modèle d'identité



Gouvernance et organisation

- Sujet assimilé à la politique de cyber-sécurité
- Implication des parties prenantes et partages des règles
- Montée en maturité, appétence accrue de la part des responsables d'équipe et de ressources
- Clarification des rôles et responsabilités

Résultats

- Phase 1 quasi-terminée
 - Nouvelle solution livrée
 - Montée en compétence en cours
 - Documentation technique rédigée au fil de l'eau
- Solution évolutive
- Complexité réduite induit réactivité, détection erreur de données
- Vision globale partagée par l'équipe IAM
- Difficultés résiduelles
 - Temps de prise en main
 - Corrections mineures dues au manque de spécification
 - Transfert de charge entre équipes

Mot de l'intégrateur ...

Facteurs de succès

- **Projet soutenu**
 - Fort sponsoring STIC
 - Promotion de la discipline IAM via nouvelles politiques
- **RH**
 - Equipe IAM volontaire, impliquée et compétente
- **Intégrateur**
 - Expertise, disponibilité et engagement
 - Force de conseils adaptés du fait de l'expérience
- **Prise de décisions rapides (choix techniques)**
- **Parties prenantes ouvertes au changement**
- **Solution adaptée à notre contexte**

Prochaines étapes

- Prochaines étapes
 - Livraison du portail
 - Migration de la gestion des autorisations : politiques, reporting, revues
 - Intégration de la gestion des comptes non nominatif (techniques, administrateurs...)
 - Interfaçage avec Zoom
- A plus long terme
 - Evolution du cadre de gouvernance
 - Unification des comptes AD (Employé - Etudiant)

Vos questions ?

Merci de votre attention