Itinéraire d'un système de gestion d'identités numériques au sein d'un EPST

Antoine Gallavardin

Guillaume Perréal

Christophe Monrocq

irstea

Le 1er janvier, l'Inra et Irstea deviennent INRAE

Présentation

- Irstea
  - Institut national de recherche en sciences et technologies pour l'environnement et l'agriculture
  - 700 chercheurs, 250 doctorants, 290 personnes d'appui réparties sur 8 sites

Présentation

- Irstea
  - Institut national de recherche en sciences et technologies pour l'environnement et l'agriculture
  - 700 chercheurs, 250 doctorants, 290 personnes d'appui réparties sur 8 sites
- Une histoire riche en changements
  - Organisationnels
    - En 2012 : Changement de nom : Cemagref ⇒ Irstea
    - En 2020 : Fusion de l'Irstea et de l'Inra pour devenir l'Inrae

Présentation

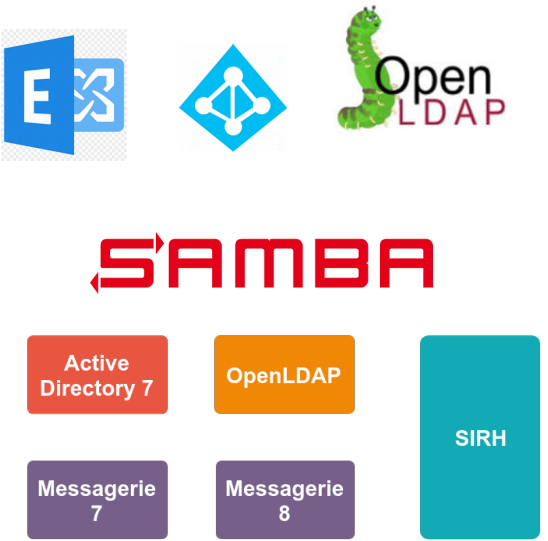
- Irstea
  - Institut national de recherche en sciences et technologies pour l'environnement et l'agriculture
  - 700 chercheurs, 250 doctorants, 290 personnes d'appui réparties sur 8 sites
- Une histoire riche en changements
  - Organisationnels
    - En 2012 : Changement de nom : Cemagref ⇒ Irstea
    - En 2020 : Fusion de l'Irstea et de l'Inra pour devenir l'Inrae
  - Techniques
    - En 2010 : Agrégation d'annuaires techniques
    - En 2015 : Externalisation de la messagerie chez RENATER
    - En 2016 : Changement de domaine Active Directory
    - En 2018 : Mise en production de SINAPS

Des problèmes réguliers ...

- Disparité des systèmes
  - 8 annuaires techniques différents
  - 2 outils de messagerie différents
  - Séparation entre
    - Outils de gestion RH
    - Outils d'infrastructure

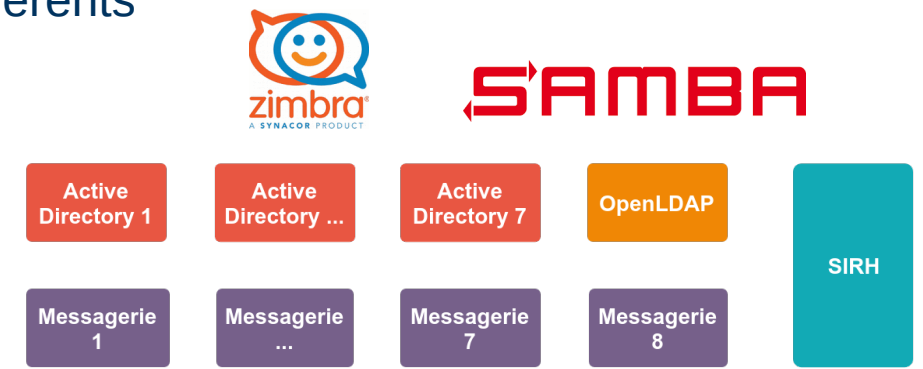
Des problèmes réguliers ...

- Disparité des systèmes
  - 8 annuaires techniques différents
  - 2 outils de messagerie différents
  - Séparation entre
    - Outils de gestion RH
    - Outils d'infrastructure
- Disparité des usages
  - Gestion des comptes
  - Procédure d'accueil



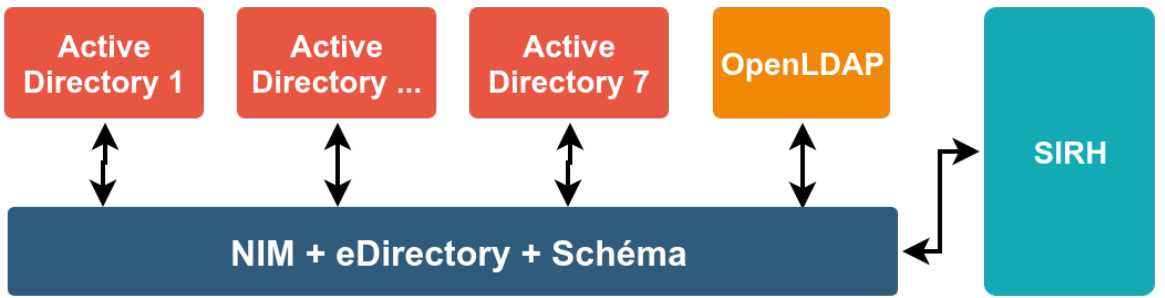
Des problèmes réguliers ...

- Disparité des systèmes
  - 8 annuaires techniques différents
  - 2 outils de messagerie différents
  - Séparation entre
    - Outils de gestion RH
    - Outils d'infrastructure
- Disparité des usages
  - Gestion des comptes
  - Procédure d'accueil
- Faible interconnexion avec le monde de l'ESR
  - Eduroam inexistant
  - Irstea non présent au sein de la Fédération



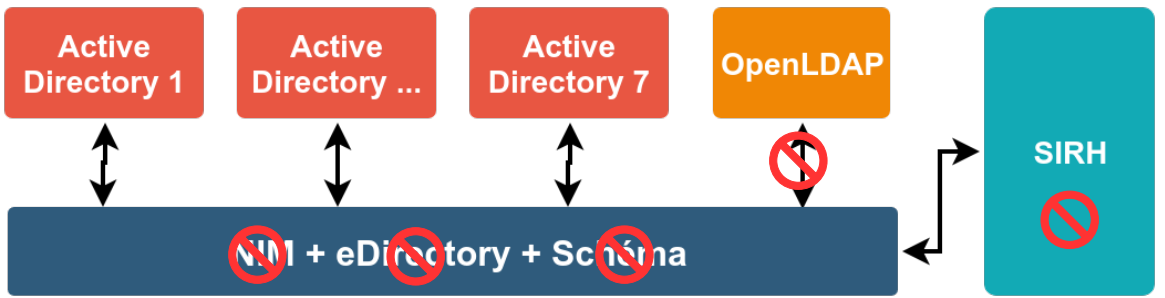
L’approche « cathédrale »

- Logiciel « multi rôles » : Novell Identity Manager
  - Une interface de gestion et de consultation : NIM
  - Un annuaire de stockage : eDirectory
  - Des clients de synchronisation
  - Une organisation de données spécifiques
  - Dans l’idéal :



L’approche « cathédrale »

- Logiciel « multi rôles » : Novell Identity Manager
  - Une interface de gestion et de consultation : NIM
  - Un annuaire de stockage : eDirectory
  - Des clients de synchronisation
  - Une organisation de données spécifiques
  - Dans l’idéal :



Retour d’expérience

© Gébé « L’an 01 »

Retour d’expérience

- Approche « Cathédrale » non pertinente
  - Trop monolithique
  - Administration complexe
  - Contraintes techniques

© Gébé « L’an 01 »

Retour d’expérience

- Approche « Cathédrale » non pertinente
  - Trop monolithique
  - Administration complexe
  - Contraintes techniques
- Maîtrise nécessaire
  - Briques techniques utilisées
  - Retour communautaire (SupAnn / outils)

© Gébé « L’an 01 »

Retour d’expérience

- Approche « Cathédrale » non pertinente
  - Trop monolithique
  - Administration complexe
  - Contraintes techniques
- Maîtrise nécessaire
  - Briques techniques utilisées
  - Retour communautaire (SupAnn / outils)
- Communication

  Le bon message aux bonnes personnes

© Gébé « L’an 01 »

Retour d'expérience

- Approche « Cathédrale » non pertinente
  - Trop monolithique
  - Administration complexe
  - Contraintes techniques
- Maîtrise nécessaire
  - Briques techniques utilisées
  - Retour communautaire (SupAnn / outils)
- Communication
  - Le bon message aux bonnes personnes
- Pilotage
  - « Release early, release often » (« Livrer tôt, livrer souvent »)
  - Découpage pertinent en fonction des acteurs et des besoins

© Gébé « L'an 01 »

L’approche « Bazar »

- Décomposition du processus global « identité numérique »

L’approche « Bazar »

- Décomposition du processus global « identité numérique »
  - Processus « Compte informatique » : Accès aux services numériques
    - Unification des différents annuaires OpenLDAP et AD
    - Formalisation des comptes et structures
    - Propagation des comptes et des méthodes d’authentification

L’approche « Bazar »

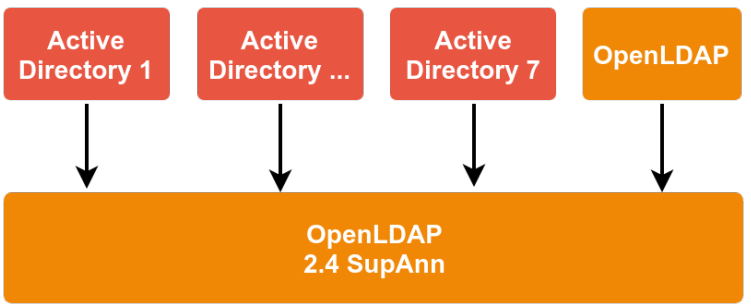
- Décomposition du processus global « identité numérique »
  - Processus « Compte informatique » : Accès aux services numériques
    - Unification des différents annuaires OpenLDAP et AD
    - Formalisation des comptes et structures
    - Propagation des comptes et des méthodes d’authentification
  - Processus « Identité » : Présentation des données RH
    - Formalisation d’une identité et d’une structure
    - Propagation des identités

L’approche « Bazar »

- Décomposition du processus global « identité numérique »
  - Processus « Compte informatique » : Accès aux services numériques
    - Unification des différents annuaires OpenLDAP et AD
    - Formalisation des comptes et structures
    - Propagation des comptes et des méthodes d’authentification
  - Processus « Identité » : Présentation des données RH
    - Formalisation d’une identité et d’une structure
    - Propagation des identités
  - Processus « Interconnexion »
    - Connexion des processus « Comptes informatiques » et « Identité »
    - Utilisation de SupAnn comme nomenclature « Pivot »

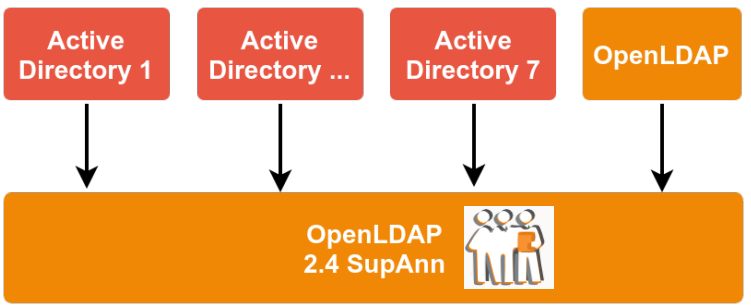
Processus « Compte informatique »

- Création d'un annuaire unique national
  - Agrégation des sources



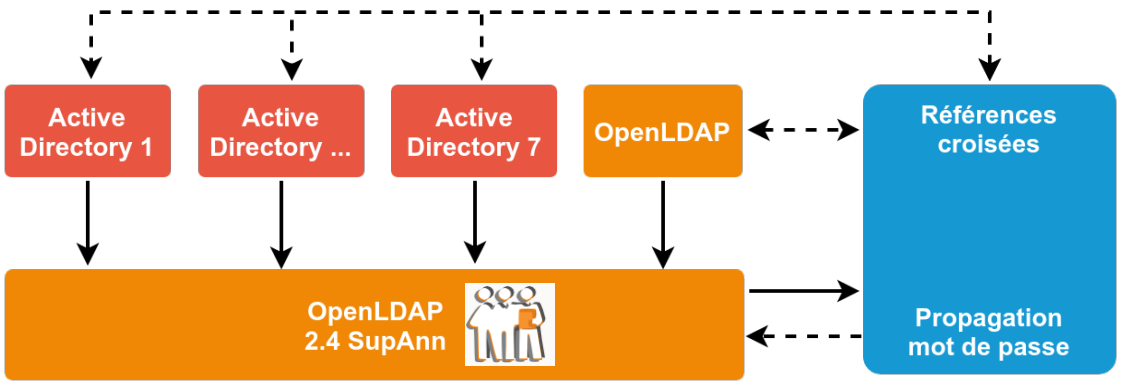
Processus « Compte informatique »

- Création d'un annuaire unique national
  - Agrégation des sources
  - Formalisation avec la norme SupAnn



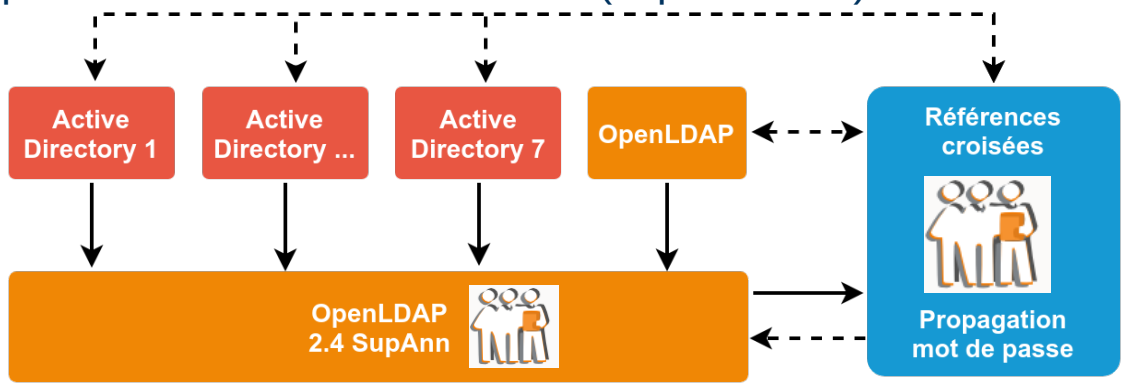
Processus « Compte informatique »

- Création d'un annuaire unique national
  - Agrégation des sources
  - Formalisation avec la norme SupAnn
- Diffusion et mise à jour
  - Interface de changement de mot de passe



Processus « Compte informatique »

- Création d'un annuaire unique national
  - Agrégation des sources
  - Formalisation avec la norme SupAnn
- Diffusion et mise à jour
  - Interface de changement de mot de passe
  - Annuaire SupAnn avec références croisées (supannRefId)



Processus « Identité »

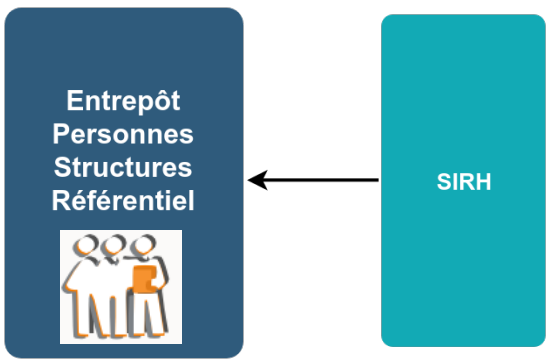
- Formalisation
  - Formalisation des structures et des identités

Processus « Identité »

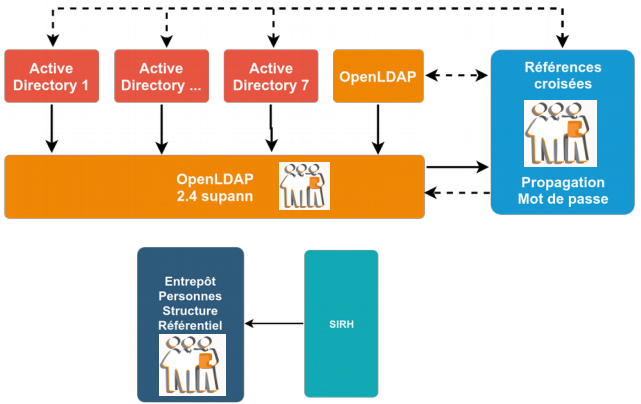
- Formalisation
  - Formalisation des structures et des identités
  - Adaptation des nomenclatures (SupAnn)

Processus « Identité »

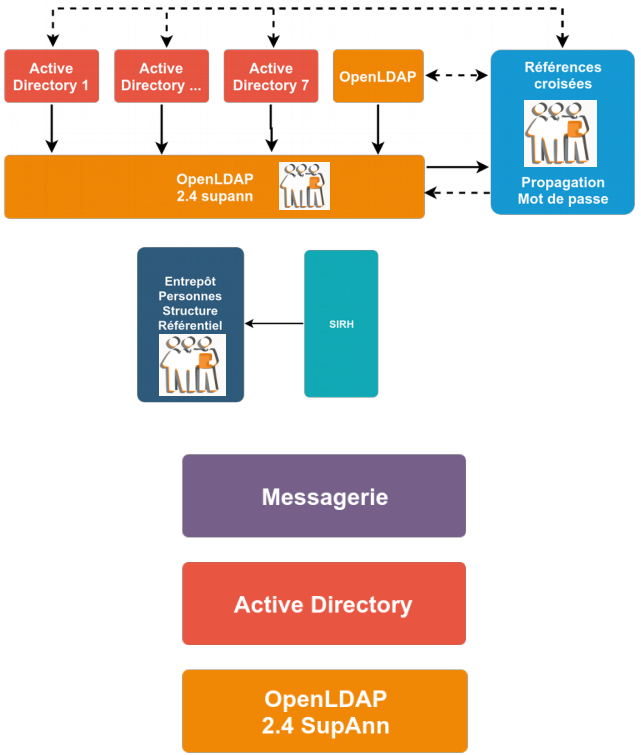
- Formalisation
  - Formalisation des structures et des identités
  - Adaptation des nomenclatures (SupAnn)
- Propagation
  - Propagation depuis le SIRH
  - Reprise des identités depuis le SIRH



Processus « Interconnexion »

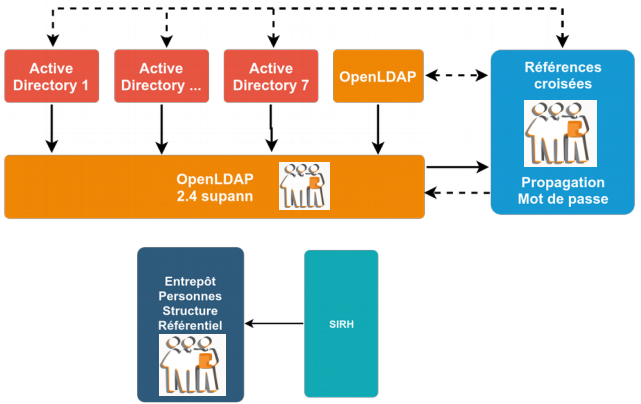


Processus « Interconnexion »

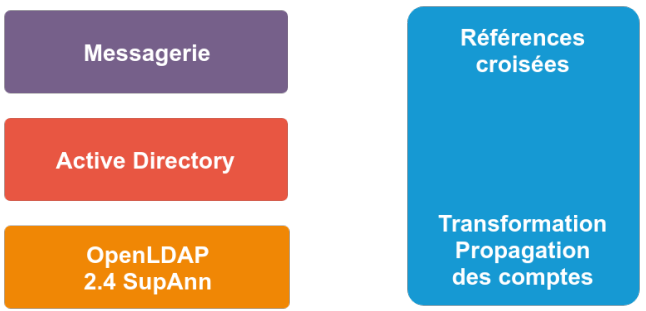


- Ajout messagerie

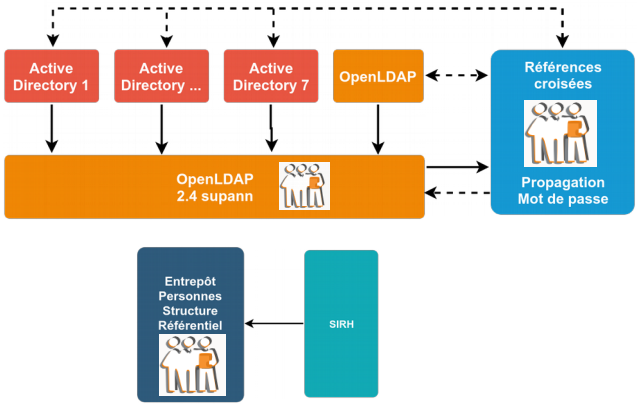
Processus « Interconnexion »



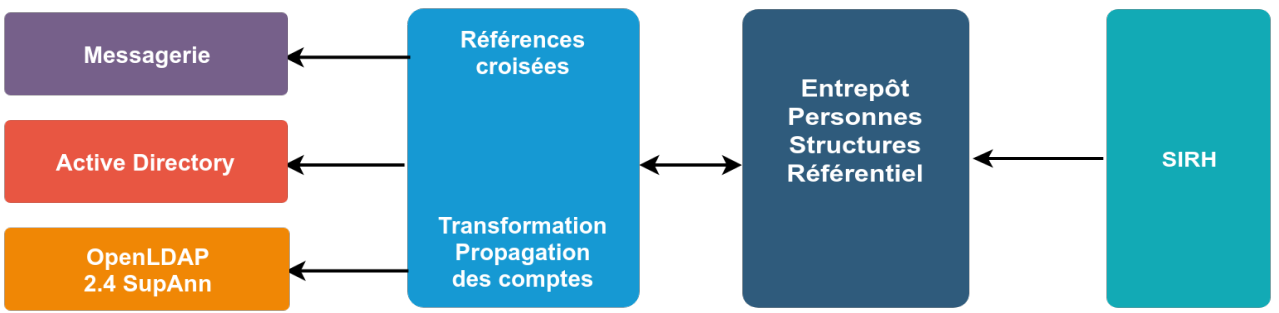
- Ajout messagerie
- Upgrade de la plate forme de propagation
  - Diffusion des mots de passe
  - Diffusion des comptes en fonction des besoins



Processus « Interconnexion »

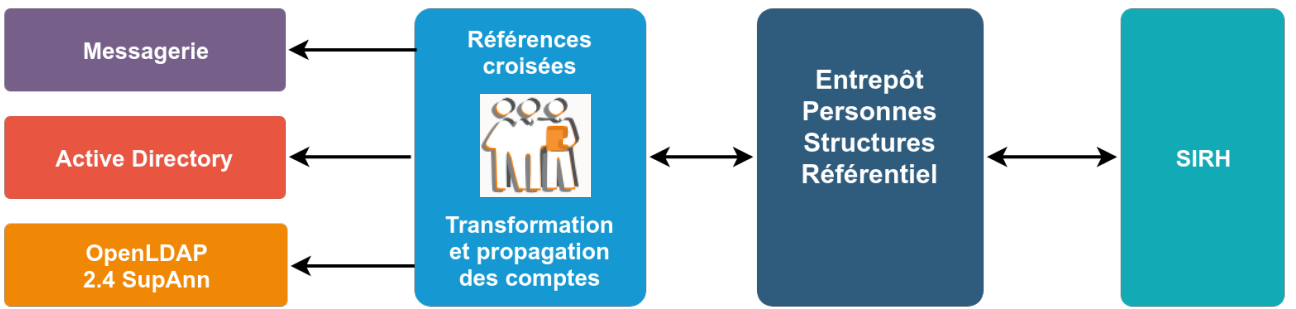


- Ajout messagerie
- Upgrade de la plate forme de propagation
  - Diffusion des mots de passe
  - Diffusion des comptes en fonction des besoins
- Réécriture des flux

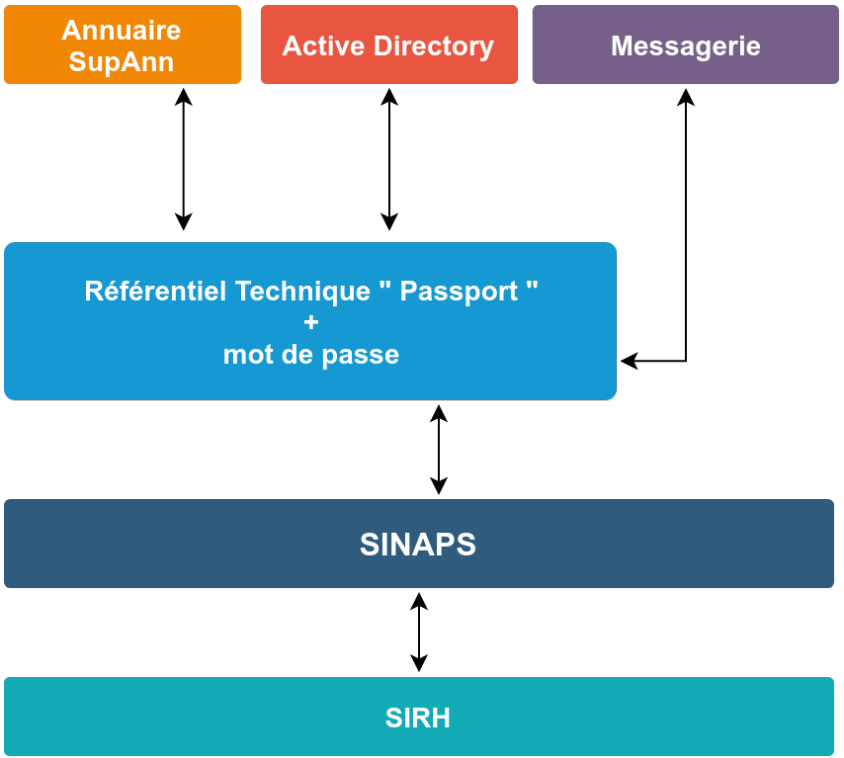


Avant ... et après !

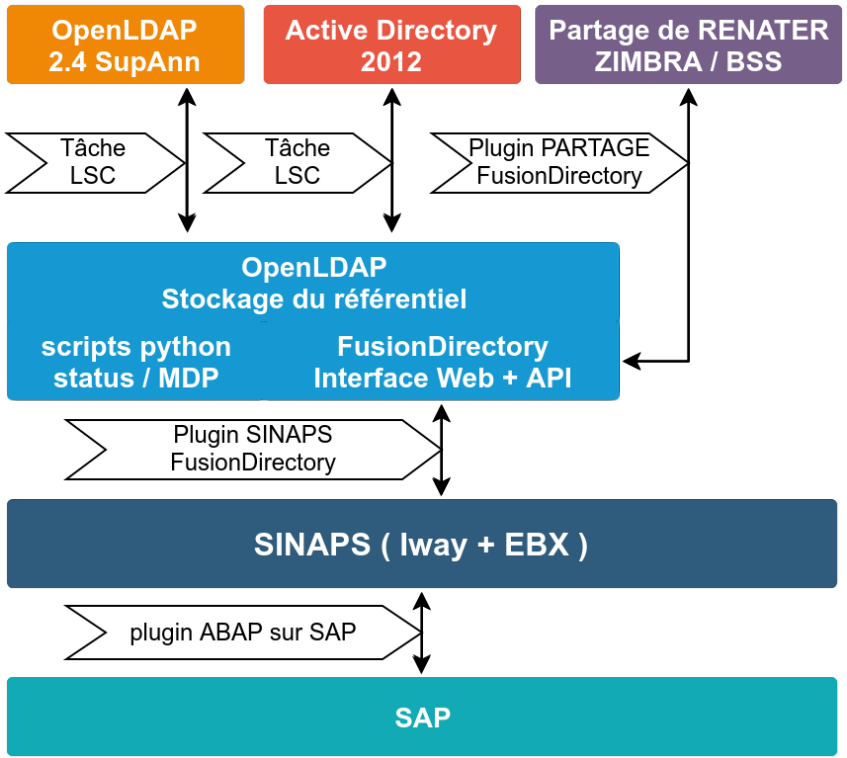
Avant ... et après !



Détails techniques



Détails techniques



- Partage :
  - https://www.renater.fr/fr/PARTAGE
  - Zimbra piloté par API : BSS
- LSC
  - https://lsc-project.org
  - Synchronisé des annuaires LDAP
  - Moteur de Javascript pour traitement d'informations
- SINAPS
  - Outils de l'AMUE
  - http://www.amue.fr/pilotage/logiciels/sinaps/
- FusionDirectory
  - https://www.fusiondirectory.org/enseignement-superieur-recherche/
- Développement effectués
  - Interne : script python (mot de passe)
  - Externe :
    - plugins FusionDirectory
    - Connecteur SAP <=> SINAPS

Pistes d’améliorations et futur

Pistes d’amélioration

- SINAPS
  - Cycle de vie
- Passport
  - Externe par parrainage
- Interaction SINAPS / Passport
  - Support SupAnn 2018 (cycle de vie)

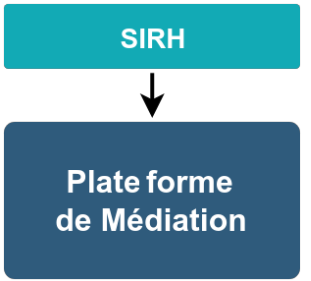
Pistes d'améliorations et futur

Pistes d'amélioration

- SINAPS
  - Cycle de vie
- Passport
  - Externe par parrainage
- Interaction SINAPS / Passport
  - Support SupAnn 2018 (cycle de vie)

Pour démarrer INRAE 2020

- Provisionnement des identités
  - Assuré par le système INRA



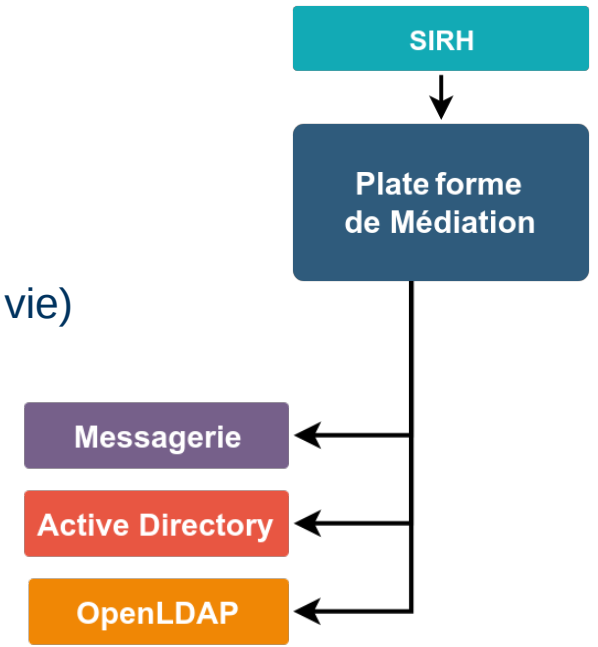
Pistes d'améliorations et futur

Pistes d'amélioration

- SINAPS
  - Cycle de vie
- Passport
  - Externe par parrainage
- Interaction SINAPS / Passport
  - Support SupAnn 2018 (cycle de vie)

Pour démarrer INRAE 2020

- Provisionnement des identités
  - Assuré par le système INRA
- Diffusion des comptes
  - Sur périmètre ex INRA
    - Conservation des outils INRA



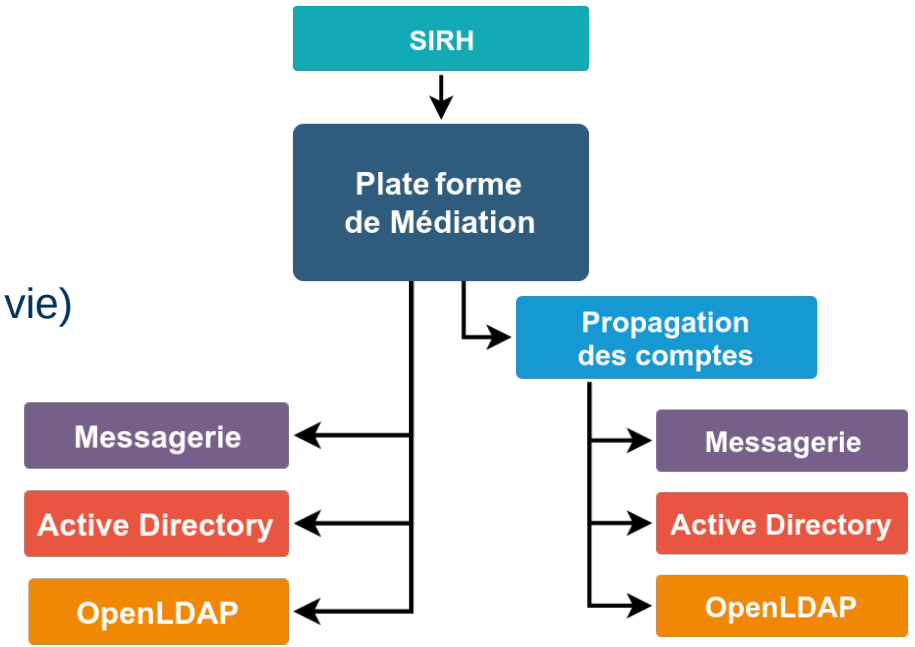
Pistes d'améliorations et futur

Pistes d'amélioration

- SINAPS
  - Cycle de vie
- Passport
  - Externe par parrainage
- Interaction SINAPS / Passport
  - Support SupAnn 2018 (cycle de vie)

Pour démarrer INRAE 2020

- Provisionnement des identités
  - Assuré par le système INRA
- Diffusion des comptes
  - Sur périmètre ex INRA
    - Conservation des outils INRA
  - Sur périmètre ex Irstea
    - Repris de la plate forme de propagation



Conclusion

Mise en place d'une Gestion des Identités

- Pilotage
  - « L'échec fait partie de la réussite »
  - Travail de longue haleine
  - Pas de trajectoire universelle
  - Périmètre de départ raisonnable
  - Identification des processus
  - Gouvernance par les besoins et par leur anticipation
  - Affichage de l'avancement (un peu de marketing) !
- Technique
  - Interopérabilité
  - Veille technologique

Remerciements / Questions

Remerciements

- DSI de l'Irstea
- Les nombreux relecteurs
- Le comité d'organisation JRES 2019

Questions !

- Je vous écoute !!