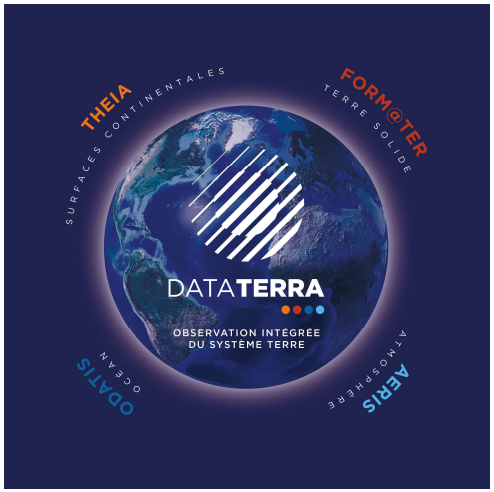


Solution AAI de DataTerra

Karim Ramage (IPSL/CNRS), Directeur Technique Adjoint Data Terra

Guillaume Brissebrat *(IPSL/CNRS), directeur technique pôle de données* ***AERIS***
GT tâche SSO du projet Equipex+ Gaia Data

Contexte : IR Data Terra

- L'IR Data Terra est composée de :
  - **4 pôles de données** : AERIS, ForM@Ter, ODATIS, THEIA (+ PNDB d'ici 2025)
  - 1 service DINAMIS de réception de données satellite haute résolution
  - **30 Centres de Données et de Services** (CDS) et Infrastructures de données spatiales (IDS)

- L'ensemble de ces Centres de Données et Services proposent l'accès à plus de **500 produits** et **plusieurs dizaines de Services** d'accès aux données

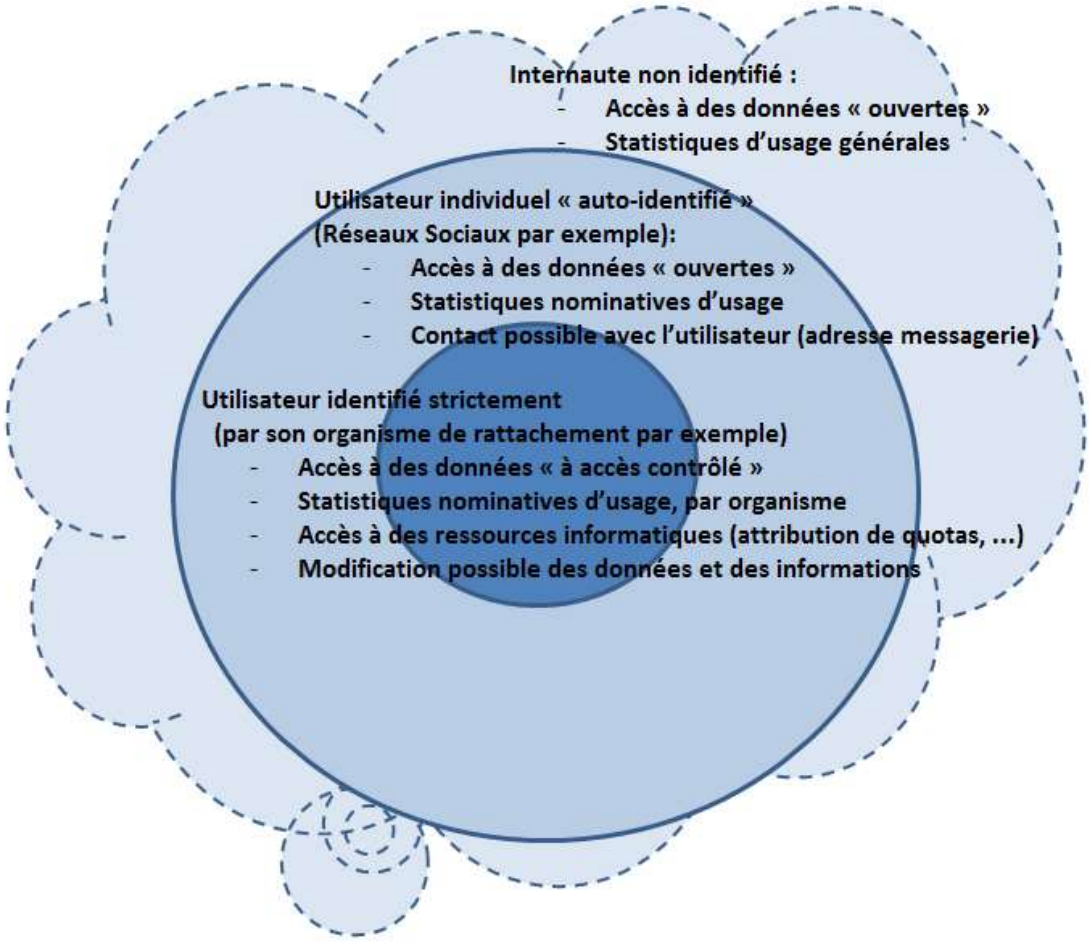
Contexte : Les Services et Users

- Les services d'accès et d'exploitation des données comprennent :
  - Des interfaces en ligne de découverte et de téléchargement des données
  - Des interfaces de visualisation des données
  - L'accès à des ressources informatiques pour permettre l'exploitation et le traitement des données
- Les utilisateurs (producteurs et utilisateurs de données) des pôles de Data Terra sont :
  - Communauté scientifique française
  - Partenaires scientifiques européen et internationaux
  - Secteur de l'education et de la formation
  - Acteurs des politiques publiques
  - Secteur Privé

Les systèmes d'authentification (annuaire + autorisations) dépendent de chaque pôle, voire de chaque service

➔ **Besoin d'harmoniser et unifier** le système pour **permettre le Single Sign On** sur l'ensemble des services, tout en respectant la **variété des contraintes d'accès** aux jeux de données et ressources

Différents niveaux d'authentification



Tâche 2.2 Gaia Data : AAI Data Terra

- **Spécifications du besoin :**
- Etude Thales Service 2019 pour AERIS étendue en 2021 pour Data Terra
- Recommandations du GT SSO Data Terra
  - Annuaire commun
  - Mécanisme d'authentification unique
  - Mécanisme d'autorisation centralisée
- Besoins fonctionnels particuliers :
  - Workflow de création de compte
  - Gestion des autorisations fines
  - Gestion des métadonnées spécifiques
- Besoin techniques :
  - Compatibilité protocoles SAML2 et OIDC
  - Migration HTTPS (OAuth 2.0)
  - Compatible authentification PAM (SSH, FTP, …)

Solutions proposées

Nom	License	Ancienneté	Dernière activité	Contributeurs
OpenAM	CDDL	14 ans	3 ans	72
OpenIAM Identity Server CE	GPL3	7 ans	2 ans	29
Keycloak	Apache_2	6 ans	21h	432
Apache Syncope	Apache_2	9 ans	3 jours	50
CAS	Apache_2	9 ans	9 h	106
GLUU	MIT	5 ans	18h	96
WSO2 Identity Server	Apache_2	10 ans	7h	281

Tâche 2.2 Gaia Data : AAI Data Terra

- Porté et intégré par RedHat
- Support
- Nombreux connecteurs
- Gestion de workflow intégré
- Déploiement en cluster
  - Géo réplication
  - Synchronisation
- Personnalisation
  - Connecteurs / Workflows / Thèmes

Solutions proposées

Nom	License	Ancienneté	Dernière activité	Contributeurs
OpenAM	CDDL	14 ans	3 ans	72
OpenIAM Identity Server CE	GPL3	7 ans	2 ans	29
Keycloak	Apache_2	6 ans	21h	432
Apache Syncope	Apache_2	9 ans	3 jours	50
CAS	Apache_2	9 ans	9 h	106
GLUU	MIT	5 ans	18h	96
WSO2 Identity Server	Apache_2	10 ans	7h	281

DATA TERRA

KEYCLOAK

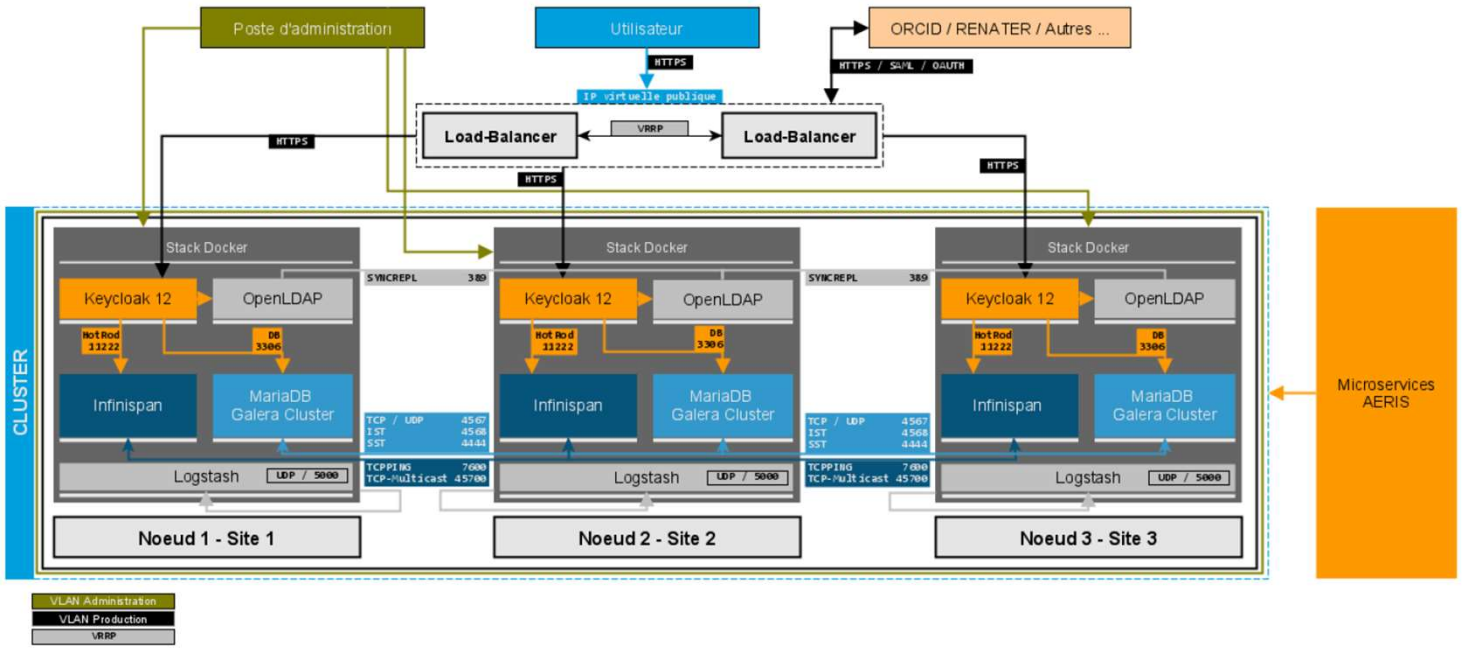
Fonctionnalités – Authentification

- Authentification de type Single Sign On (SSO)
- Plusieurs protocoles disponibles (OIDC, OAuth 2.0, SAML)
- Possibilité de déléguer l'authentification à un fournisseur externe compatible OIDC / SAML
  - Renater (Shibboleth), ORCid (OIDC),
  - Préconfiguration de fournisseurs externes tels que GitHub, Google, Facebook, Twitter, ...
- Synchronisation avec des LDAP (Active Directory server) externes
- Authentification forte (TOTP/HOTP)
- Personnalisation des workflows d'authentification (SPI)

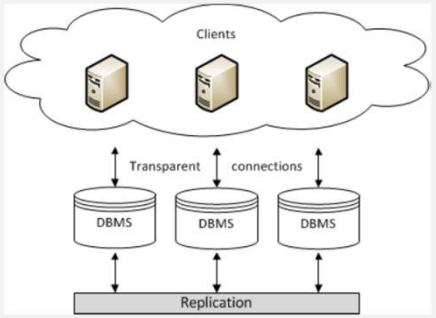
Fonctionnalités – Autorisations

- Gestion poussée des autorisations (Protection API et Permissive Tickets JWT)
- La gestion des autorisations peut se faire sur :
  - Attribut
  - Rôle
  - Utilisateur
  - Contexte
  - Règle (JavaScript)
  - Temps
  - Personnalisé (code applicatif JAVA)
- Sur des type de ressources (URLs), ou des scopes (OAuth 2.0)
- S'applique également sur le Keycloak lui même pour la gestion des Realms et des applications
- Cloisonnement possible par pôle avec les Realms

Architecture Cible SSO Data Terra

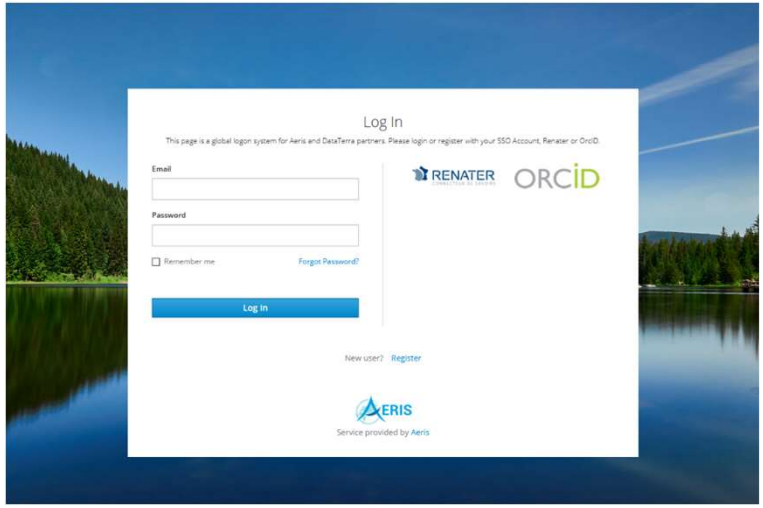


- **Réplication :**
- MariaDB Galera Cluster



- Données de cache : Infinispan - Jboss Data Grid (JDG)
- **Load Balancer** (HTTPD / Wildfly / NGINX / HA Proxy) --> Sticky Sessions
- (Keycloak Gatekeeper)

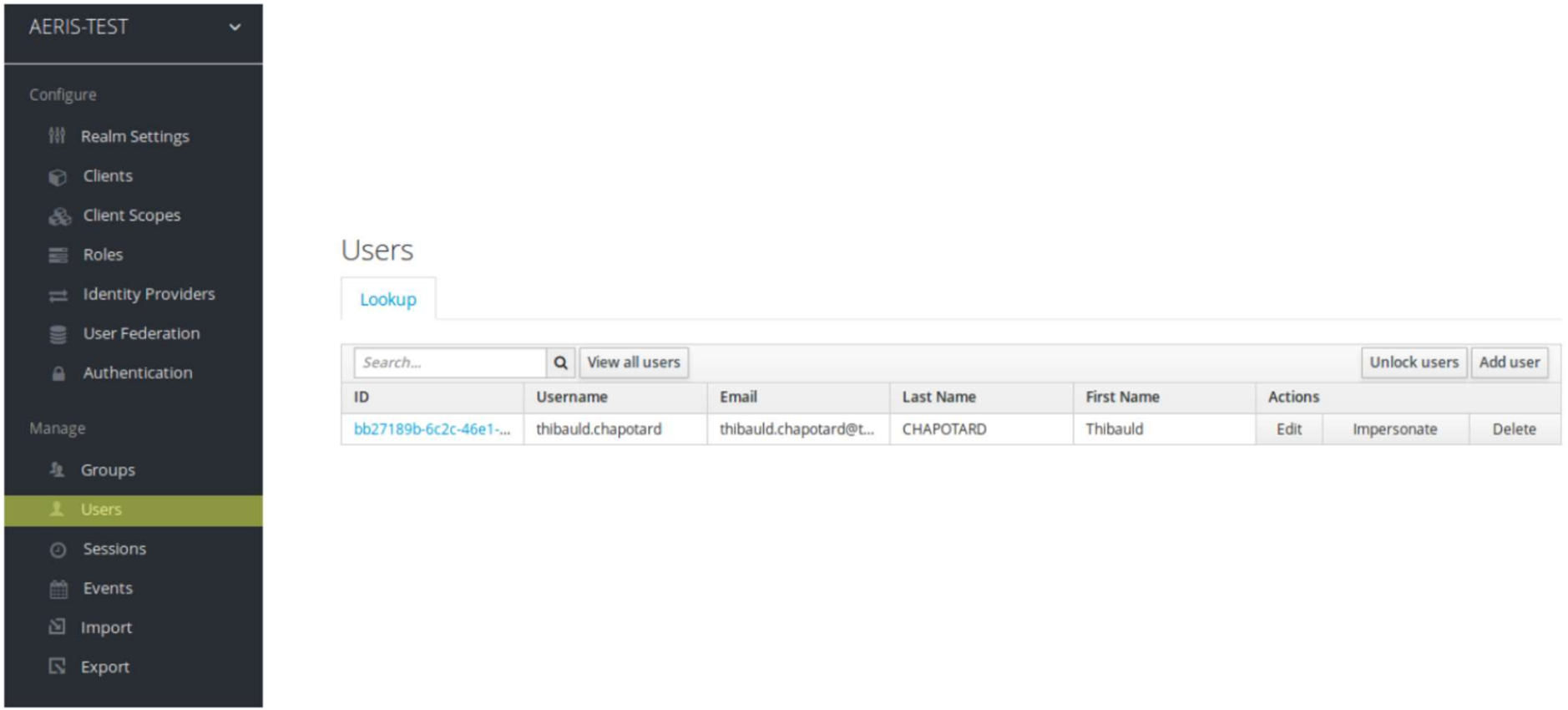
Authentification



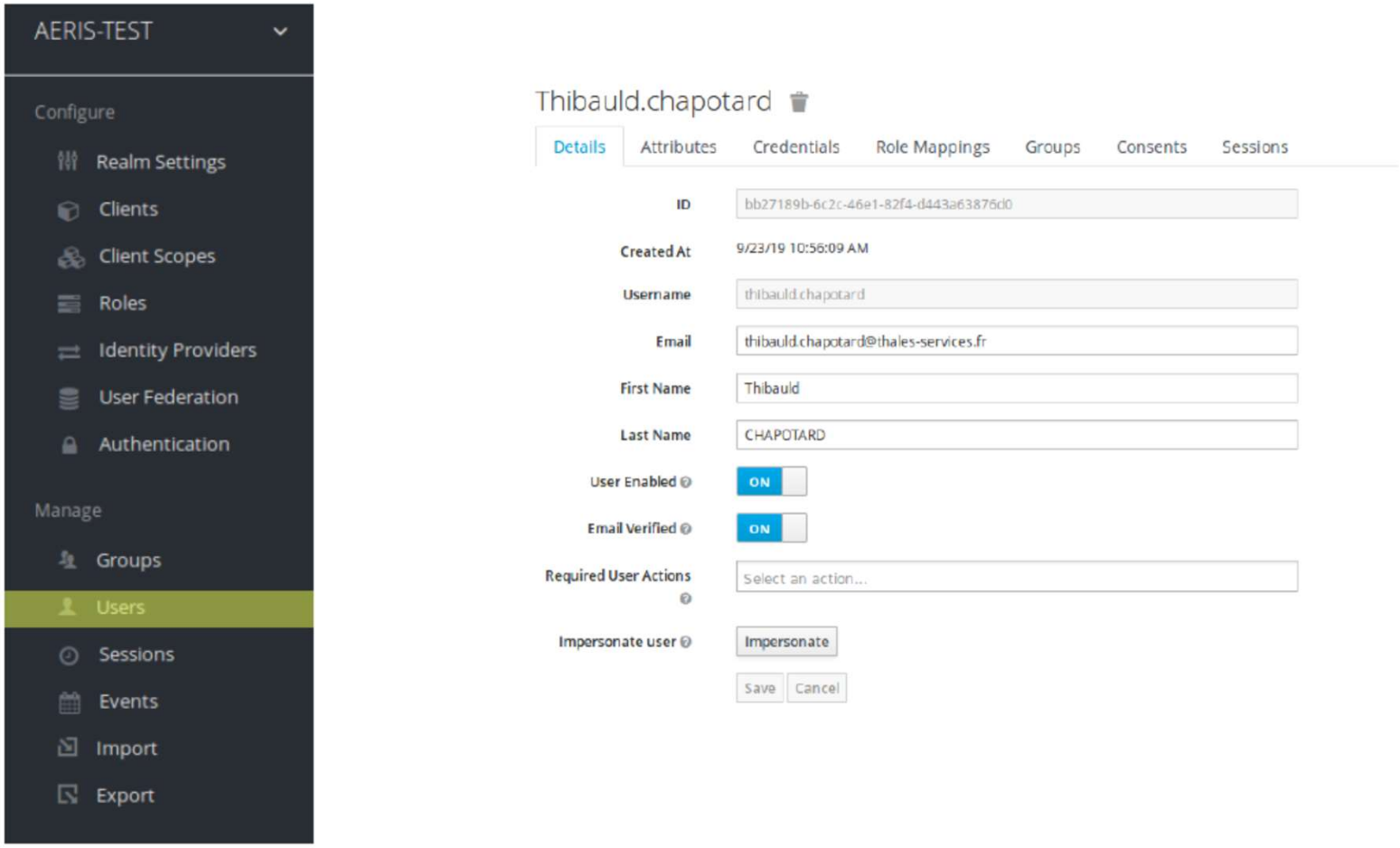
Fournisseurs d'identité :

- OrcID
- Fédération EduGain
- Comptes locaux
  - Keycloak
  - Imports LDAP

Utilisateurs – Création / Modification



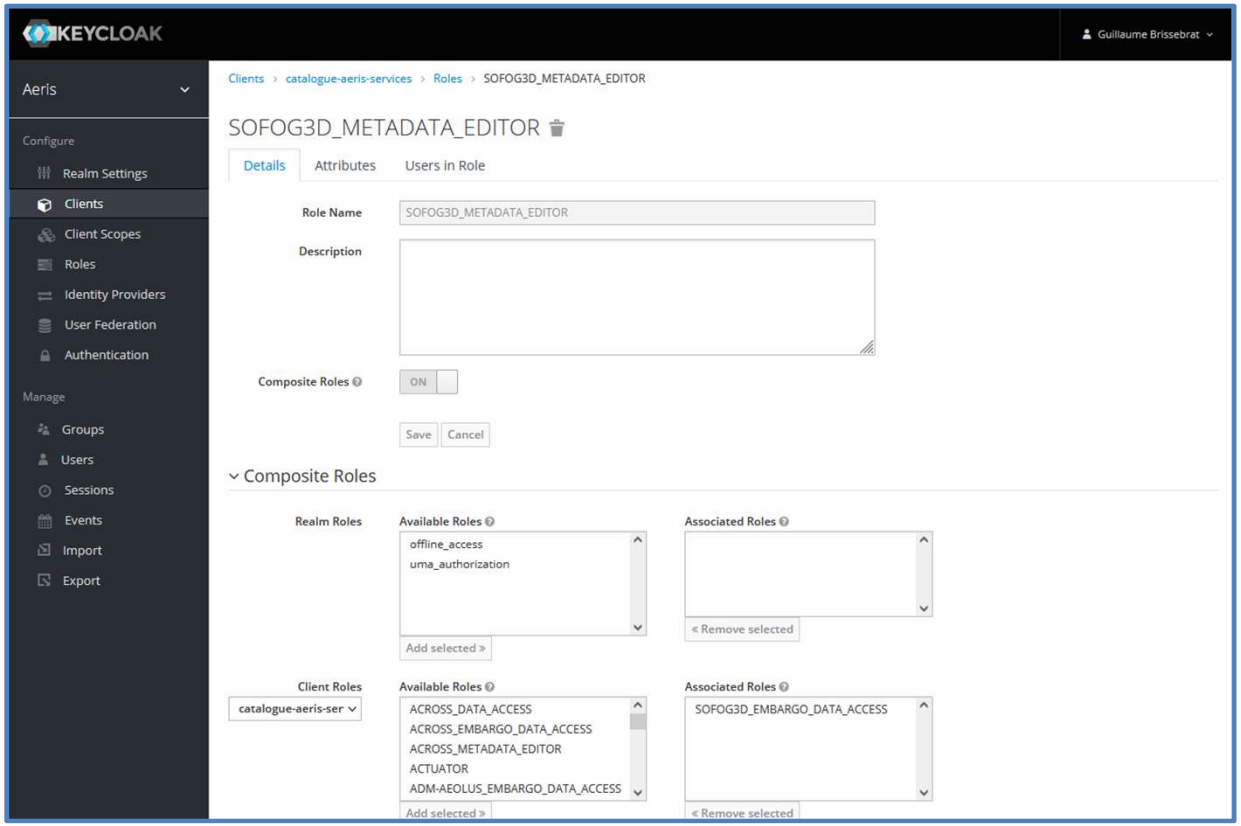
Utilisateurs – Création / Modification



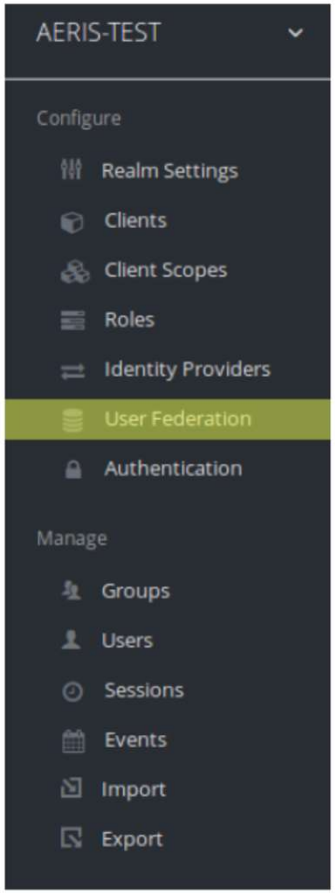
Utilisateurs – Roles

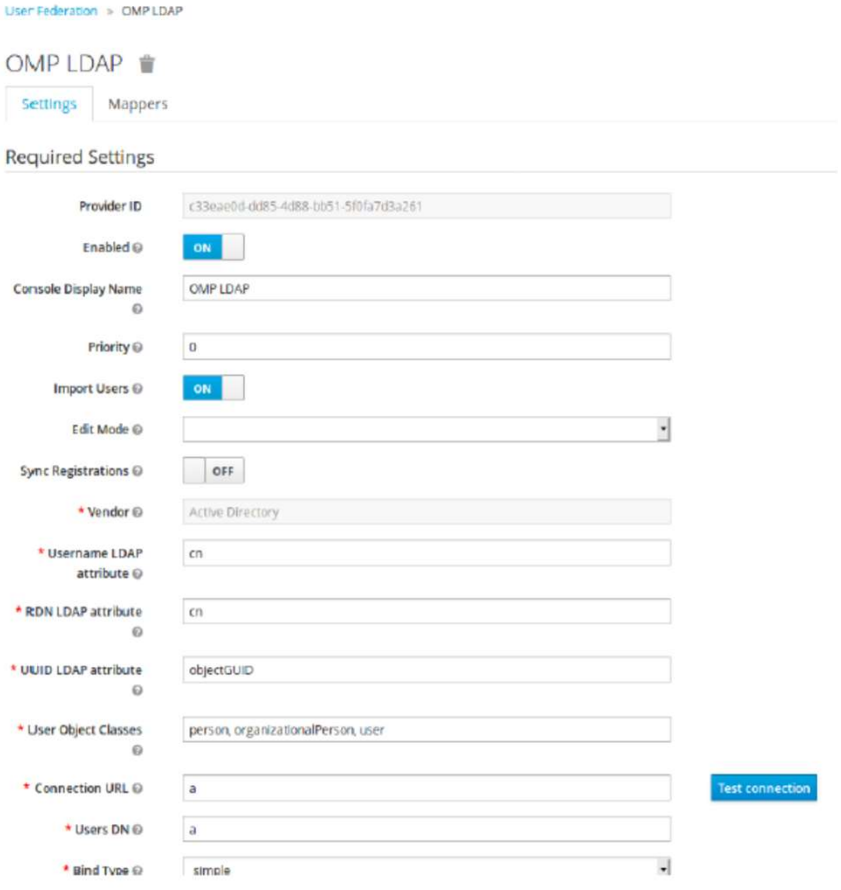
Gestion des rôles utilisateurs

- 2 niveaux : realm et client
- Possibilité de créer des roles composite
  - Permet d'agréger des rôles des 2 niveaux et de tous les clients (du realm)
  - Si on ajoute un rôle composite à un utilisateur, il aura tous les rôles associés

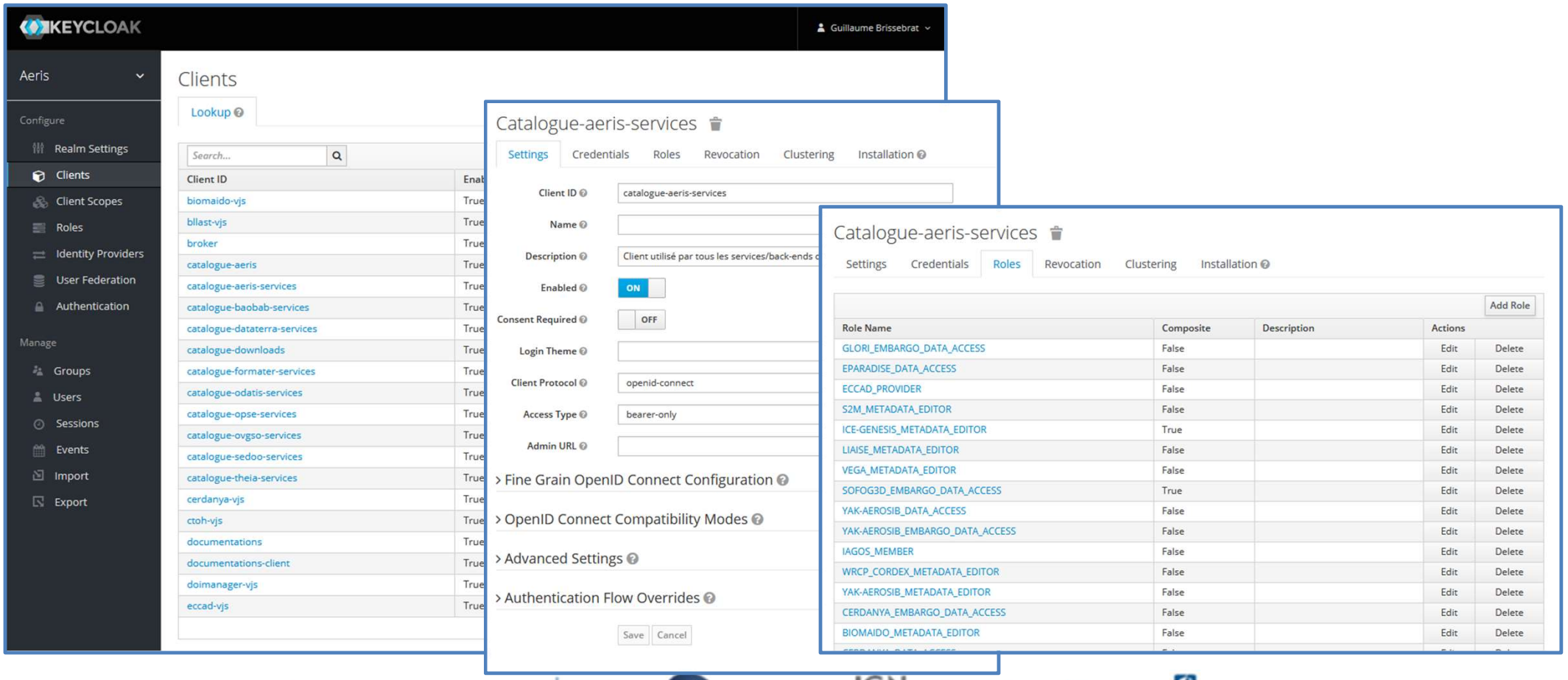


Utilisateurs – Synchro LDAP (in/out)

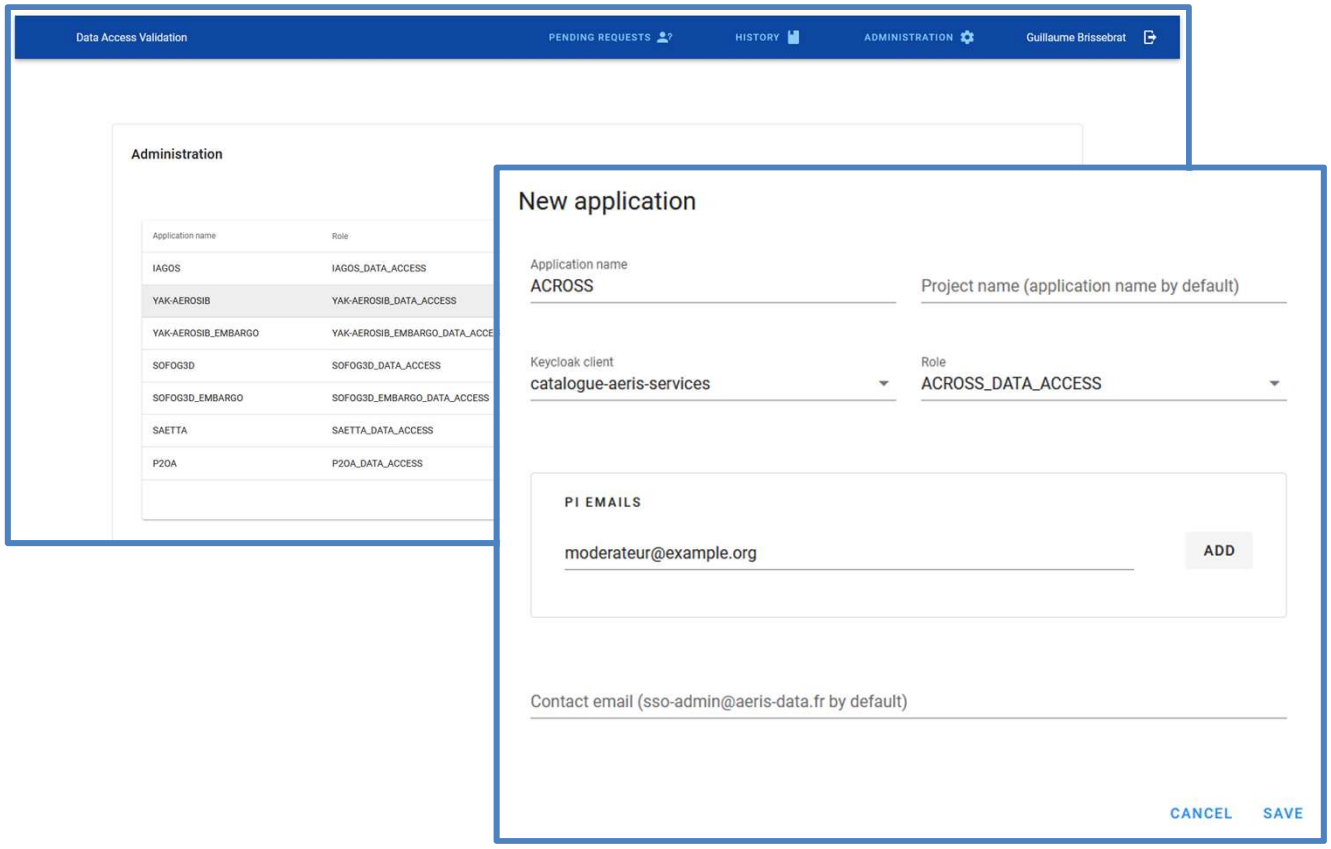




Clients Keycloak



Gestions des autorisations – User Interface



Délégation de la gestion des autorisations

- Accès à un jeu de données géré par le PI
- Interface spécifique développée par AERIS
- Utilisation de l'API Keycloak
- Workflow de validation:
  - Demande d'accès par le user transmise au PI
  - Validation par le PI
  - Ajout des droits d'accès au compte utilisateur (keycloak) via l'API

Conclusion et travaux en cours

- Solution Keycloak déployée à l'IPSL pour Data Terra
  - Realms en production pour AERIS et Formater
  - Realms de tests pour Theia, Odatis, PNDB
- Intégration de la solution Keycloak dans le système AAI du GeoDataHub CNES

- Travaux Gaia Data
  - Inventaire des annuaires utilisateurs des pôles
  - Inventaire des workflows de gestion des comptes des applications des pôles de Data Terra, ClimERI et PNDB
  - Spécifications et développement d'une application « user friendly » pour la gestion des autorisations :
    - Délégation de la gestion vers les pôles, les responsables applicatifs, les producteurs de données
  - Inventaire des attributs utilisateurs à intégrer dans les profils keycloak (ex. : nationalité)
  - Prise en compte des exigences RGPD dans la gestion du compte (attributs et cycle de vie)
  - Connexion des applications des pôles de Data Terra et des services de Gaia Data au SSO
- S'inspirer des Orgnisations Virtuelles EGI pour la gestion des communautés

contact@data-terra.org
+33 (0)4 67 54 87 08

www.data-terra.org