



## 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'éducation et de la formation
  - Acteurs des politiques publiques
  - Secteur Privé

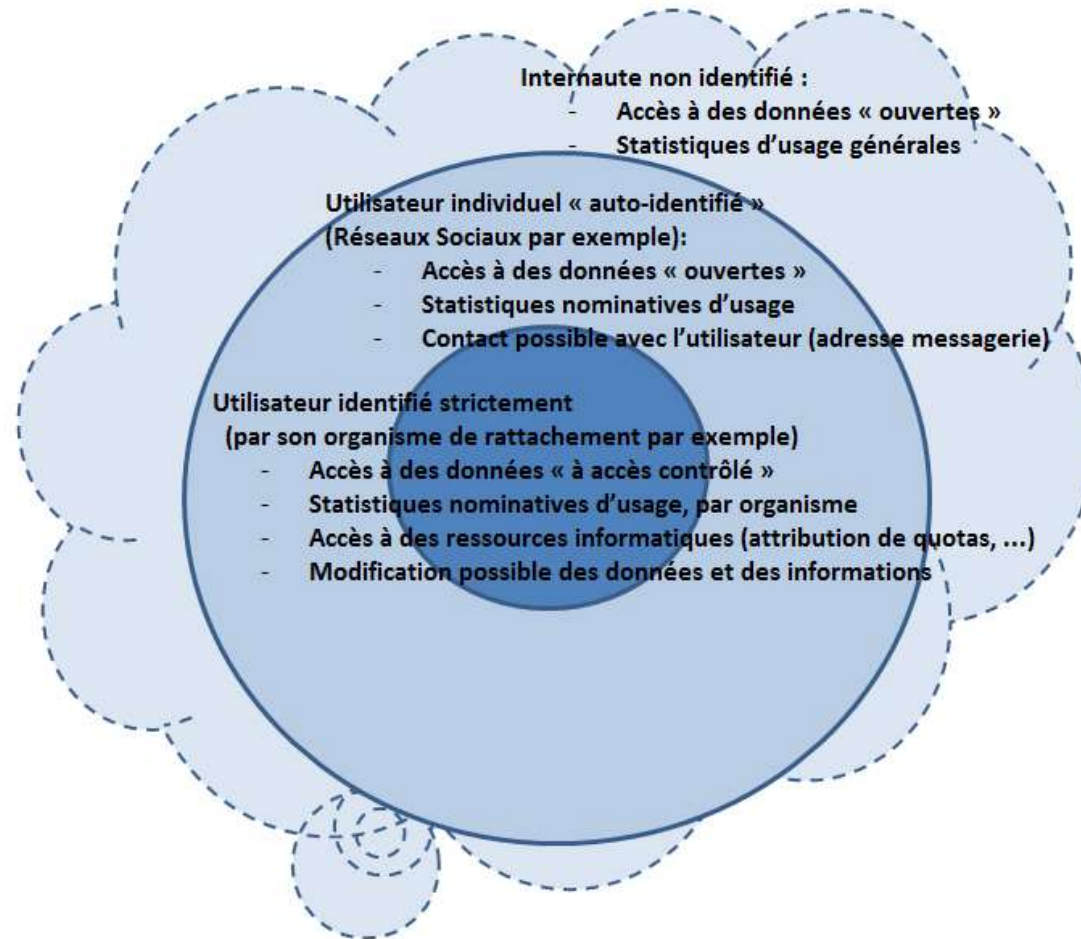


Les systèmes d'authentification (annuaire + autorisations) dépendent de chaque pôle, voire de chaque service

→ **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



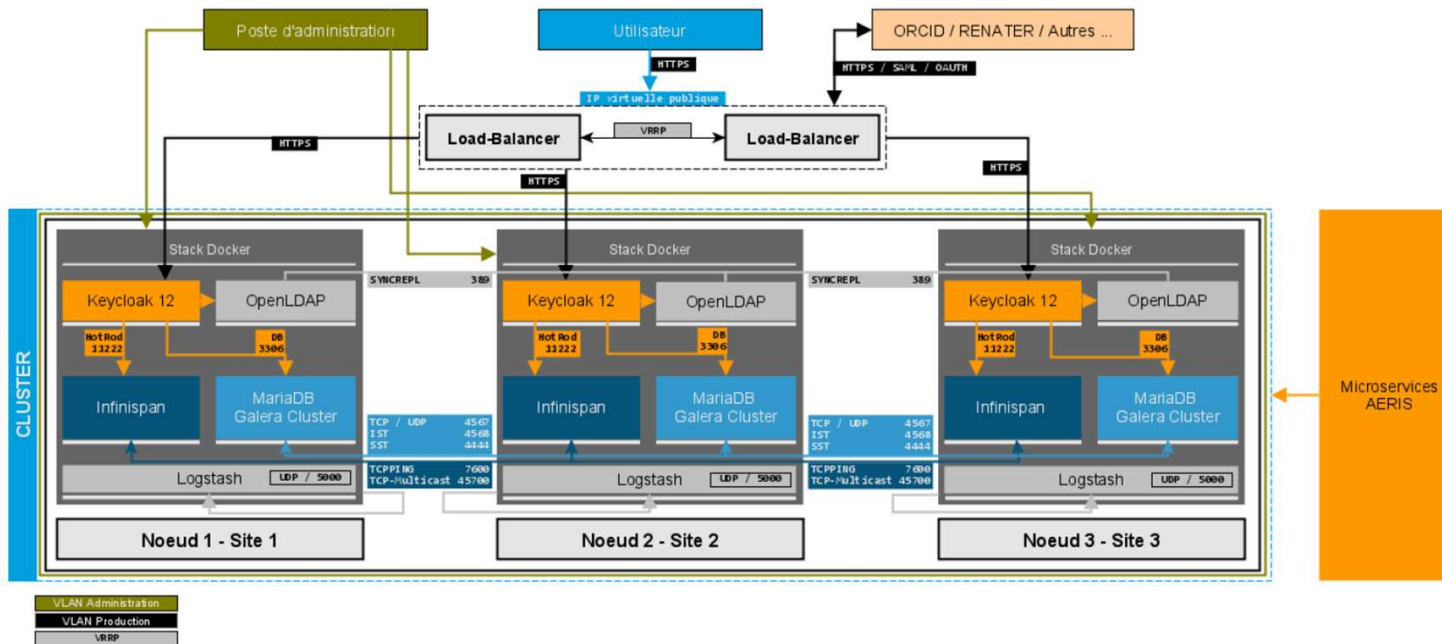
### Fonctionnalités – Authentification

- 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)

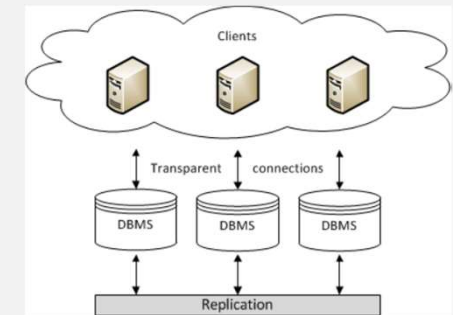
### Fonctionnalités – Autorisations

- 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



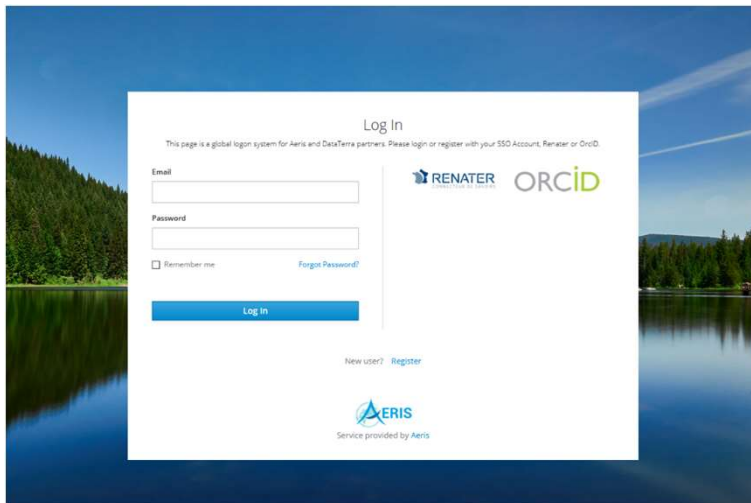
- **Réplication :**
- MariaDB Galera Cluster



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



# Authentication



## Fournisseurs d'identité :

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



# Utilisateurs – Création / Modification

AERIS-TEST

Configure

- Realm Settings
- Clients
- Client Scopes
- Roles
- Identity Providers
- User Federation
- Authentication

Manage

- Groups
- Users**
- Sessions
- Events
- Import
- Export

## Users

Lookup

ID	Username	Email	Last Name	First Name	Actions
bb27189b-6c2c-46e1-...	thibauld.chapotard	thibauld.chapotard@t...	CHAPOTARD	Thibauld	Edit Impersonate Delete



# Utilisateurs – Création / Modification

AERIS-TEST

Configure

- Realm Settings
- Clients
- Client Scopes
- Roles
- Identity Providers
- User Federation
- Authentication

Manage

- Groups
- Users**
- Sessions
- Events
- Import
- Export

Thibault.chapotard

Details | Attributes | Credentials | Role Mappings | Groups | Consents | Sessions

ID: bb27189b-6c2c-46e1-82f4-d443a63876d0

Created At: 9/23/19 10:56:09 AM

Username: thibault.chapotard

Email: thibault.chapotard@thales-services.fr

First Name: Thibault

Last Name: CHAPOTARD

User Enabled:

Email Verified:

Required User Actions: Select an action...

Impersonate user:

# Utilisateurs – Roles

## Gestion des rôles utilisateurs

- 2 niveaux : realm et client
- Possibilité de créer des rôles 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)

AERIS-TEST

Configure

- Realm Settings
- Clients
- Client Scopes
- Roles
- Identity Providers
- User Federation**
- Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import
- Export

User Federation > OMP LDAP

OMP LDAP

Settings Mappers

Required Settings

- Provider ID: c33eae0d-dd85-4d88-bb51-5f0fa7d3a261
- Enabled:  ON
- Console Display Name: OMP LDAP
- Priority: 0
- Import Users:  ON
- Edit Mode:
- Sync Registrations:  OFF
- \* Vendor: Active Directory
- \* Username LDAP attribute: cn
- \* RDN LDAP attribute: cn
- \* UUID LDAP attribute: objectGUID
- \* User Object Classes: person, organizationalPerson, user
- \* Connection URL: a Test connection
- \* Users DN: a
- \* Bind Type: simple



# Clients Keycloak

The screenshot displays the Keycloak administration console. On the left is a navigation sidebar with options like 'Configure', 'Clients', 'Client Scopes', 'Roles', 'Identity Providers', 'User Federation', 'Authentication', 'Groups', 'Users', 'Sessions', 'Events', 'Import', and 'Export'. The main area shows the 'Clients' list with a search bar and a table of client entries. A modal window is open for the client 'Catalogue-aeris-services', showing its configuration details:

- Client ID:** catalogue-aeris-services
- Name:** (empty)
- Description:** Client utilisé par tous les services/back-ends
- Enabled:** ON
- Consent Required:** OFF
- Login Theme:** (empty)
- Client Protocol:** openid-connect
- Access Type:** bearer-only
- Admin URL:** (empty)

Below these fields are expandable sections for 'Fine Grain OpenID Connect Configuration', 'OpenID Connect Compatibility Modes', 'Advanced Settings', and 'Authentication Flow Overrides'. A second modal window is open to the 'Roles' tab for the same client, displaying a table of roles:

Role Name	Composite	Description	Actions
GLORI_EMBARGO_DATA_ACCESS	False		Edit Delete
EPARADISE_DATA_ACCESS	False		Edit Delete
ECCAD_PROVIDER	False		Edit Delete
S2M_METADATA_EDITOR	False		Edit Delete
ICE-GENESIS_METADATA_EDITOR	True		Edit Delete
LIAISE_METADATA_EDITOR	False		Edit Delete
VEGA_METADATA_EDITOR	False		Edit Delete
SOFOG3D_EMBARGO_DATA_ACCESS	True		Edit Delete
YAK-AEROSIB_DATA_ACCESS	False		Edit Delete
YAK-AEROSIB_EMBARGO_DATA_ACCESS	False		Edit Delete
IAGOS_MEMBER	False		Edit Delete
WRCP_CORDEX_METADATA_EDITOR	False		Edit Delete
YAK-AEROSIB_METADATA_EDITOR	False		Edit Delete
CERDANYA_EMBARGO_DATA_ACCESS	False		Edit Delete
BIOMAIDO_METADATA_EDITOR	False		Edit Delete

# Gestions des autorisations – User Interface

The screenshot displays the 'Data Access Validation' interface. At the top, there is a navigation bar with 'PENDING REQUESTS', 'HISTORY', 'ADMINISTRATION', and the user name 'Guillaume Brissebrat'. Below this, the 'Administration' section contains a table of existing applications:

Application name	Role
IAGOS	IAGOS_DATA_ACCESS
YAK-AEROSIB	YAK-AEROSIB_DATA_ACCESS
YAK-AEROSIB_EMBARGO	YAK-AEROSIB_EMBARGO_DATA_ACCESS
SOF0G3D	SOF0G3D_DATA_ACCESS
SOF0G3D_EMBARGO	SOF0G3D_EMBARGO_DATA_ACCESS
SAETTA	SAETTA_DATA_ACCESS
P20A	P20A_DATA_ACCESS

Overlaid on this is the 'New application' form, which includes the following fields:

- Application name: **ACROSS** (Project name (application name by default))
- Keycloak client: **catalogue-aeris-services**
- Role: **ACROSS\_DATA\_ACCESS**
- PI EMAILS: **moderateur@example.org** (with an 'ADD' button)
- Contact email (sso-admin@aeris-data.fr by default)

Buttons for 'CANCEL' and 'SAVE' are located at the bottom right of the form.

## 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 Organisations Virtuelles EGI pour la gestion des communautés





**DATATERRA**



[contact@data-terra.org](mailto:contact@data-terra.org)

+33 (0)4 67 54 87 08

[www.data-terra.org](http://www.data-terra.org)