

La Fédération EGI: Operations, AAI et Cloud

Baptiste Grenier / EGI Operations team

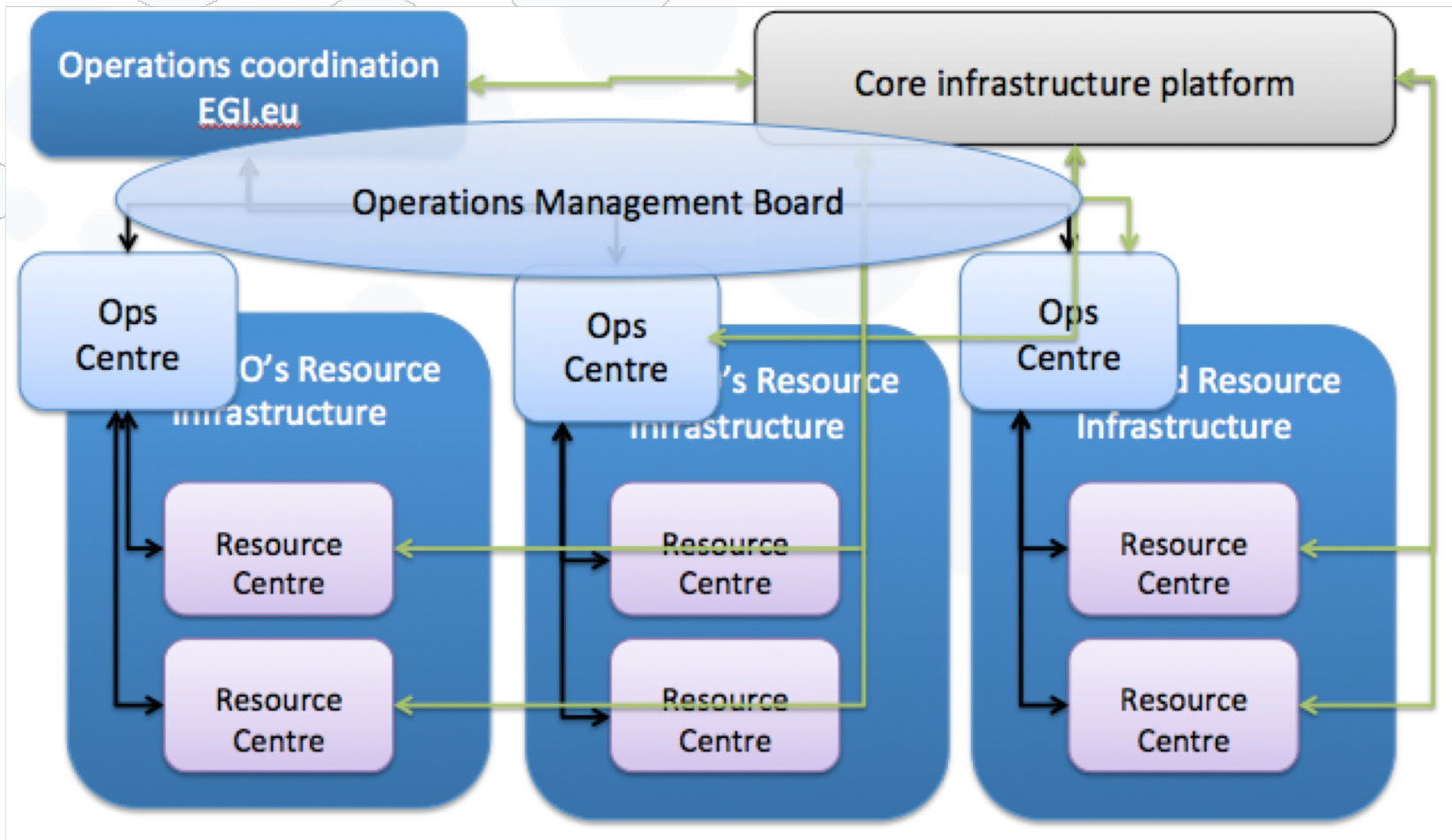
baptiste.grenier@egi.eu / operations@egi.eu



- EGI Operations
 - Organisation
 - OLA et SLA
 - Activités
 - Chiffres
- EGI Check-in
- EGI Federated Cloud

- Un ensemble d'équipes
 - Administrateur des sites nationaux et régionaux
 - Coordination des opérations (EGI F. Operations Team)
 - Expert sécurité (CSIRT, SVG)
 - Helpdesk, experts techniques et développeurs d'applications
 - Opérateurs des services centraux
 - Operations Portal, GGUS, GOCDB, ARGO, APEL, AppDB, Marketplace
 - Collaboration tools (RT, wiki, mailing list, discourse, DocDB,...)
 - User Community Support Team (UCST)
 - WLCG et autres infrastructures
- Management: Operations Management Board (OMB)

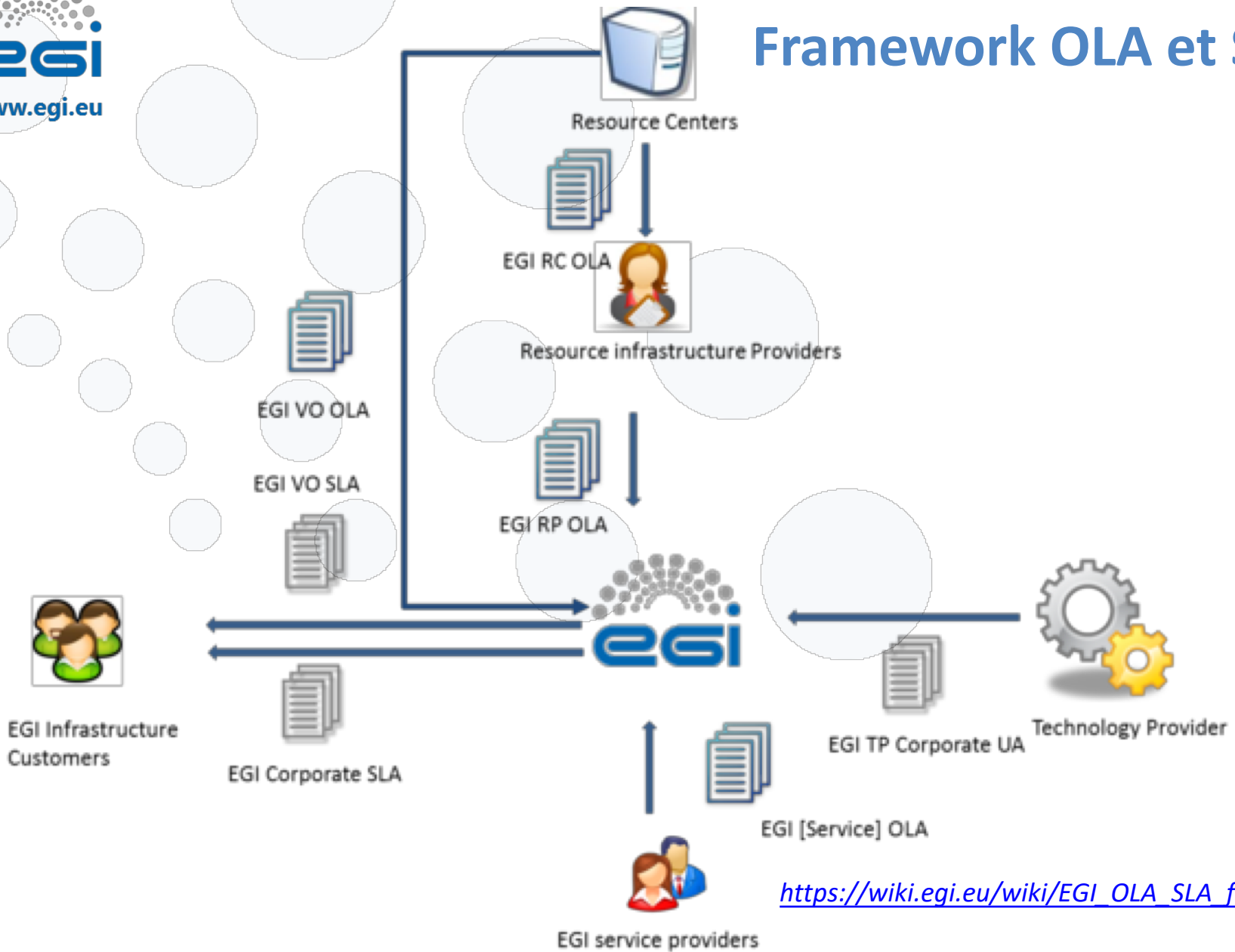
EGI Operations: organisation



- Fourniture **fiable** et **sure** de **services**
 - Pour les communautés d'utilisateurs
 - HTC, Cloud, Stockage, AAI, Applications on Demand
 - Formations (Outils, FitSM, ISO27001,...)
 - <https://www.esi.eu/services/>
 - Pour les participants de la fédération
 - Coordination
 - opérations, sécurité, communauté
 - technique, stratégique et communications
 - Formations: FitSM, ISO 27001
 - AAI
 - Marketplace, Accounting, GOCDDB, Collaboration Tools
 - <https://www.esi.eu/internal-services/>

- Définitions et maintenance des **Operational Level Agreements (OLA)** avec les **fournisseurs de services**
- Intégration et contrôle des **Service Level Agreements (SLA)** signées avec les **communautés d'utilisateurs**
 - Les **OLAs** agréés avec les **fournisseurs** doivent couvrir les besoins formulés dans les **SLAs** agréées avec les **utilisateurs**
- Supervision des objectifs des **OLAs** et **SLAs**

Framework OLA et SLA



https://wiki.egi.eu/wiki/EGI_OLA_SLA_framework

EGI Operations: répondre aux besoins

- **Validation** des **outils** logiciels
 - **Distribution** et **coordination** de leurs déploiements
- **Documentation**, mise en place des **procédures** et **politiques**
- **Supervision** des services (fonctionnement et sécurité)
- Suivi d'utilisation (**accounting**) pour comprendre les besoins actuels et évaluer les besoins futurs
- **Support** « service requests » et « incident response » (GGUS)
- **Collection** des **besoins** et **identification** des **fonctionnalités** et **services** manquants
 - Des participants **et** des utilisateurs
- Mise en place et participation à des Comités Techniques

• Instances de services gérées (GOCDDB)	3112
• Centres opérationnels coordonnés	34
• Middleware releases	13
– 128 mises à jour	
– 27 « Product Teams »	
• Alertes de sécurité publiées	29
• Tickets « service requests » mis a jours	6718

EGI Check-in

Solution AAI complète, moderne et flexible



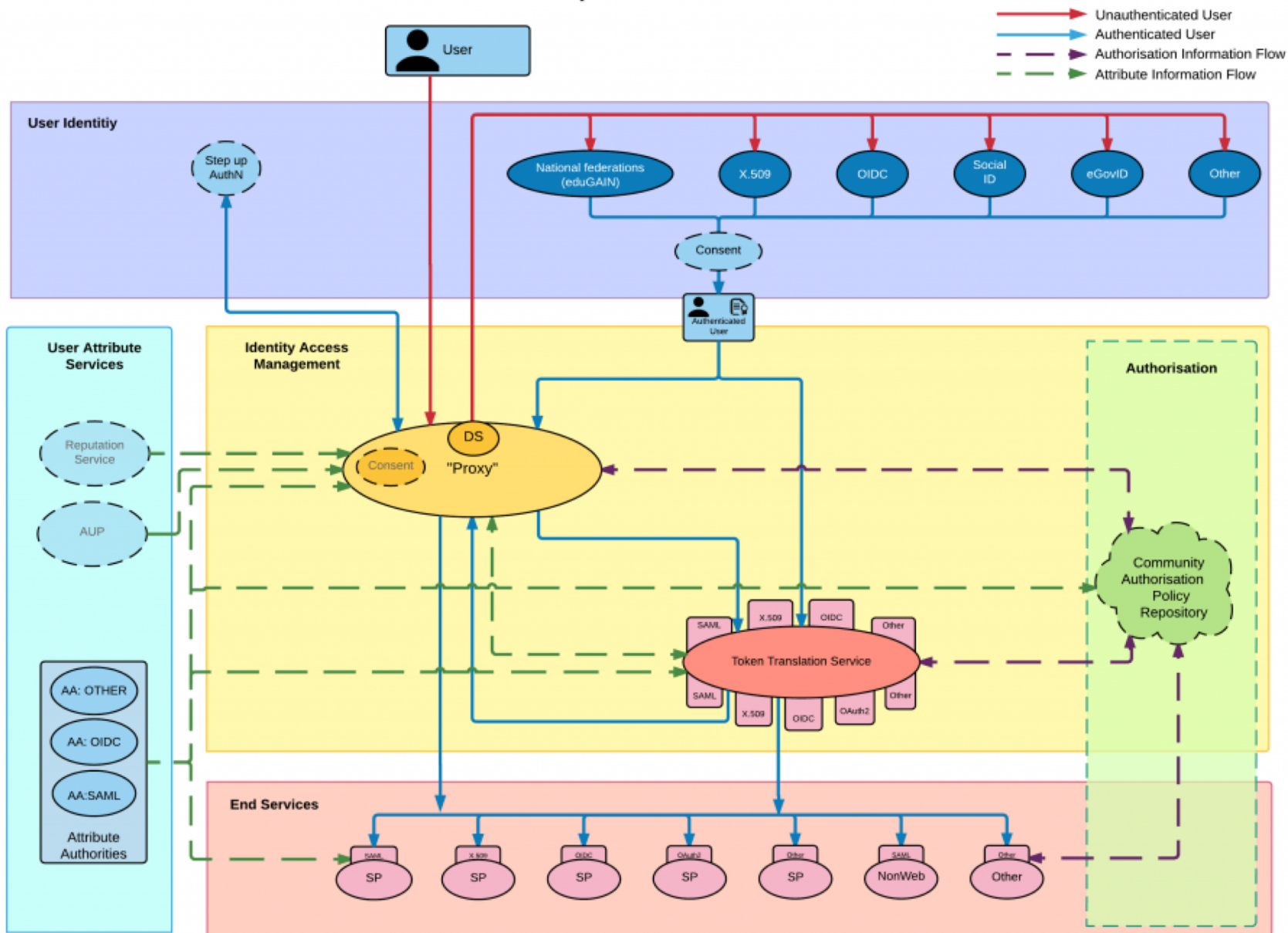
www.egi.eu

This work by EGI.eu is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).

- Identité unique et **SSO** pour services web et non web
 - Fédération de fournisseurs d'identité institutionnels eduGAIN
 - Comptes sociaux (ORCID, Google, Facebook, LinkedIn,...)
 - Autres fournisseurs (ELIXIR, DARIAH, B2ACCES, EGI,...)
 - Liaison d'identités
- Les services connectés à Check-in peuvent être mis a disposition de +2000 institutions avec peu d'effort
- Basé sur les technologies standard de fédération d'identité
 - SAML 2.0, OpenID Connect, Oauth 2.0, X509

- Implémentation de l'architecture proposée par AARC
 - Intégration des Service Providers (**SP**) avec **un** Identity Provider (**IdP**) agissant en **proxy** des autres **IdPs**
 - Permet d'**authentifier l'utilisateur**
 - Différents « **Level of Assurance** »
 - « **Attributes Authorities** » ajoutant des attributs utilisateur
 - Typiquement géré par les communautés
 - RCauth Online CA pour le support X509 simplifié
 - **Autorisation** basée sur les **attributs**
 - Gérée au niveau des ressources
 - Implémenté par de multiples infrastructures
 - GEANT, Elixir, Dariah, EUDAT, INDIGO, EGI...

AARC Blueprint Architecture



<https://aarc-project.eu/architecture>

- Pour **fournisseurs** de services et **Infrastructures de Recherche**
- Intégration avec de **multiples IdPs**
 - eduGAIN, Media Sociaux, X509, ...
 - Liaison de comptes
- Architecture **souple**
 - Installation et configuration partagée ou dédiée
 - Possibilité d'intégrer des composants existants
 - Fournisseurs d'identité (IdP)
 - SAML2.0, OpenID Connect, X509,...
 - Gestion des attributs/groupes (AA)
 - VOMS, PERUN, REST,...



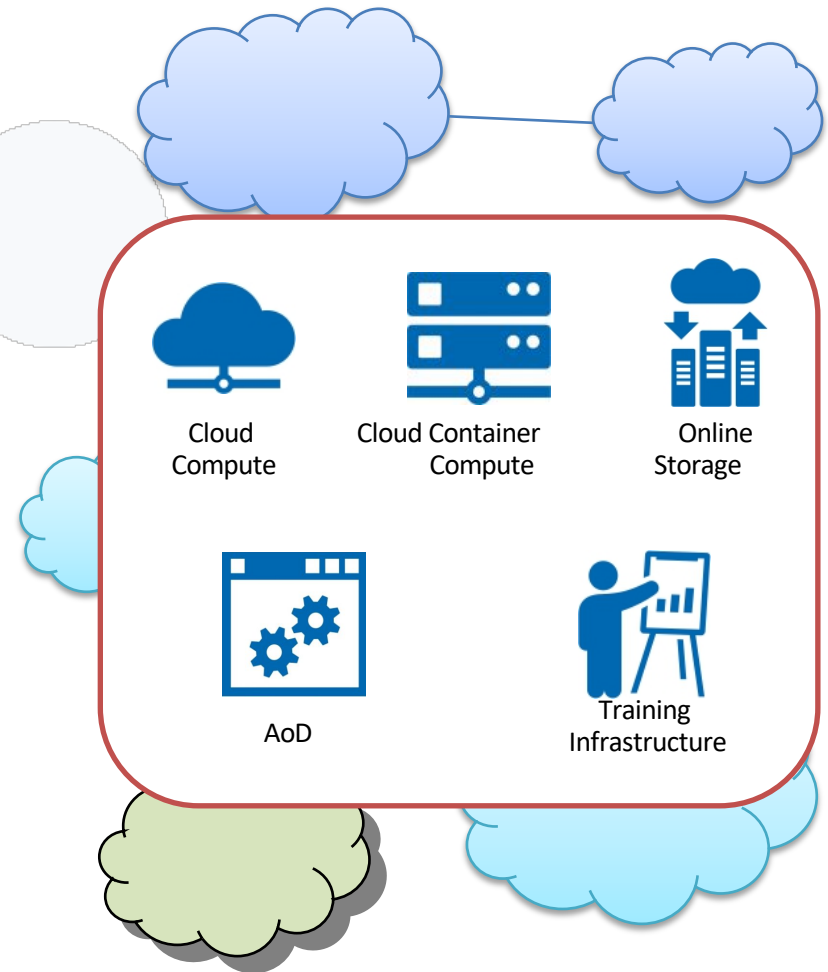
<https://www.egi.eu/services/check-in/>

EGI Federated Cloud

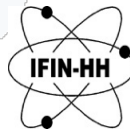
Fédération de fournisseurs de cloud
institutionnels



- Infrastructure as a Service (IaaS) multi-cloud
 - OpenStack, OpenNebula, Synnefo
 - SSO via Check-in
- Usage principaux constatés
 - Hébergement de « Science Gateways »
 - Outils de visualisation pour des analyses « data-intensive »



FedCloud: l'infrastructure



20 resource centres

- 15 OpenStack
- 4 OpenNebula
- 1 Synnefo

6 centres under integration

2 centres expressed interest on joining

« Infrastructure as a Service » pour la recherche

Pour les utilisateurs

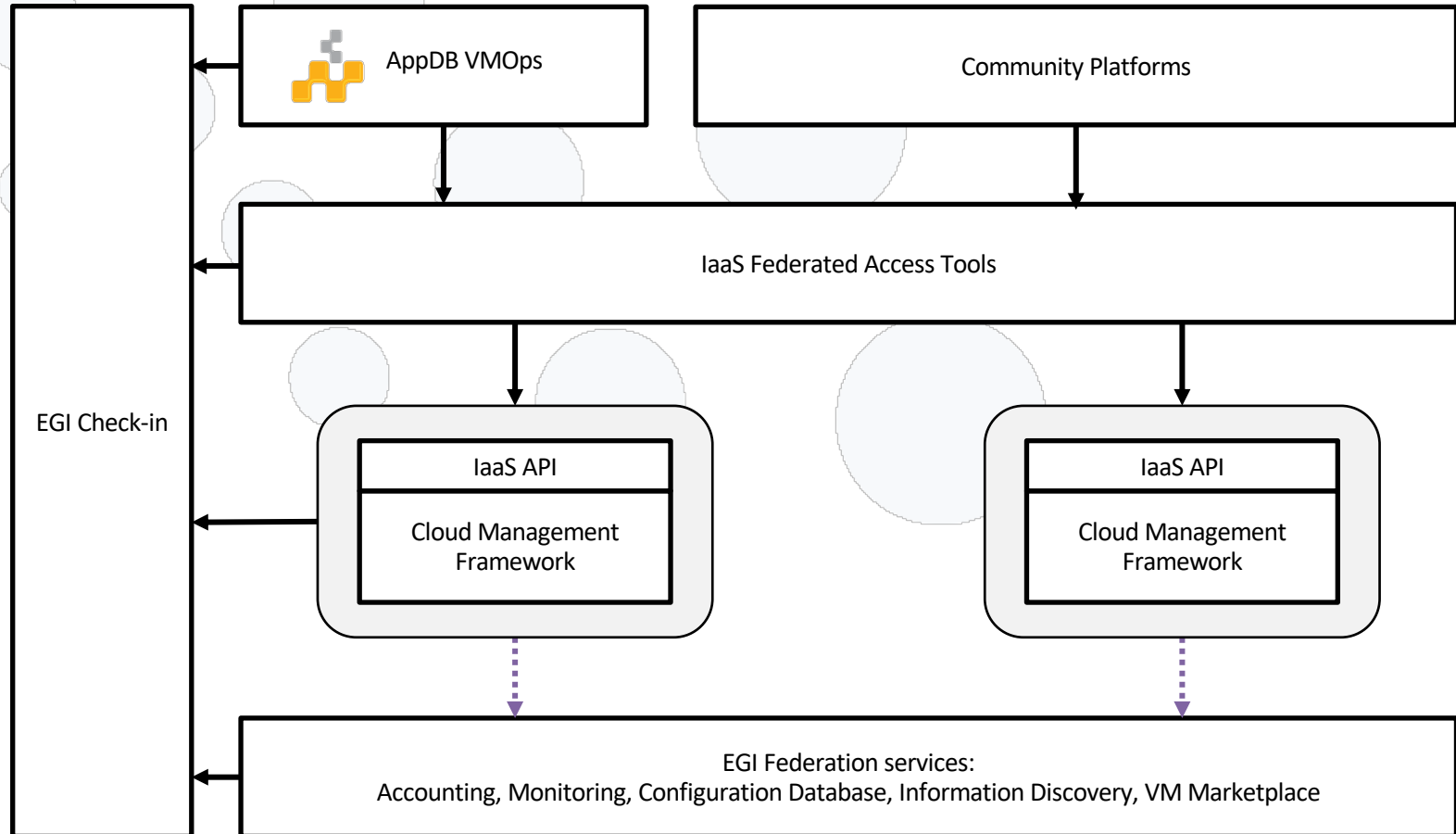
- SSO via Check-in
- Bibliothèque applicative
- Découverte de ressources
- Dashboard graphique
- Calcul a proximité des données

Pour les fournisseurs

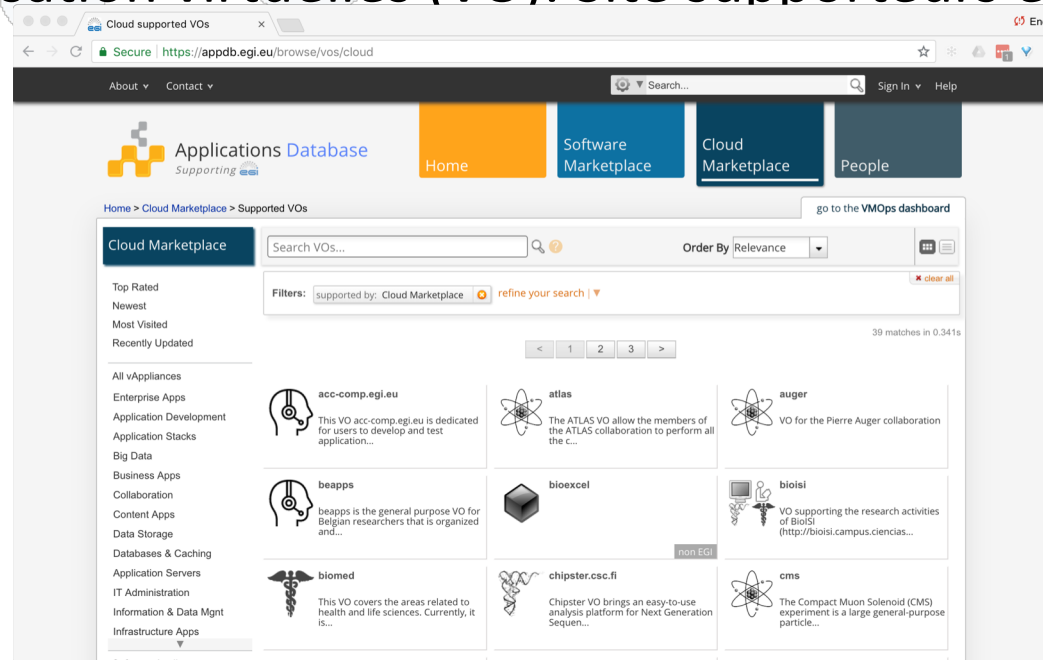
- Support des communautés internationales
- Déploiement simplifié des applications partagées
- Processus pour les opérations et la sécurité
- Supervision A/R
- Suivi d'utilisation

- **Les fournisseurs gardent le contrôle**
 - Accès basé sur les Organisations Virtuelles (**VO**)
 - Une VO est mappée sur un projet local
 - Utilisateurs avec des identifiants dédié à EGI
 - Fourniture de ressources encadrée par une **SLA**
 - Composants supplémentaires interagissant avec les **APIs**
 - **Retrouve** et **publie** des **informations** pour les autres services EGI
- **Pas d'impact majeur sur les opérations**
 - Fournir du support a travers les canaux EGI
 - Suivre les procédures opérationnelles et sécurité
 - Règles de l'art et besoins généraux
 - OCCl n'est plus requis (Infrastructure Manager, libcloud,...)

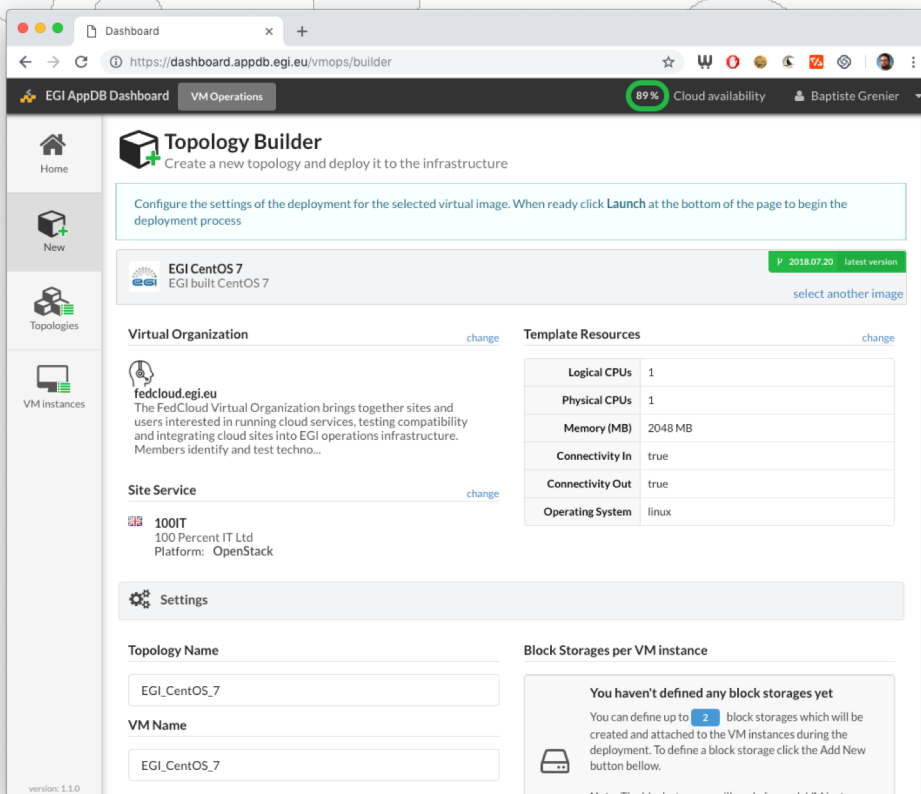
FedCloud: architecture



- Catalogue
 - Appliances Virtuelles (VA)
 - Fournisseurs: Sites, VAs et patrons/templates disponibles
 - Organisation virtuelles (VO): Site supporteurs et VA



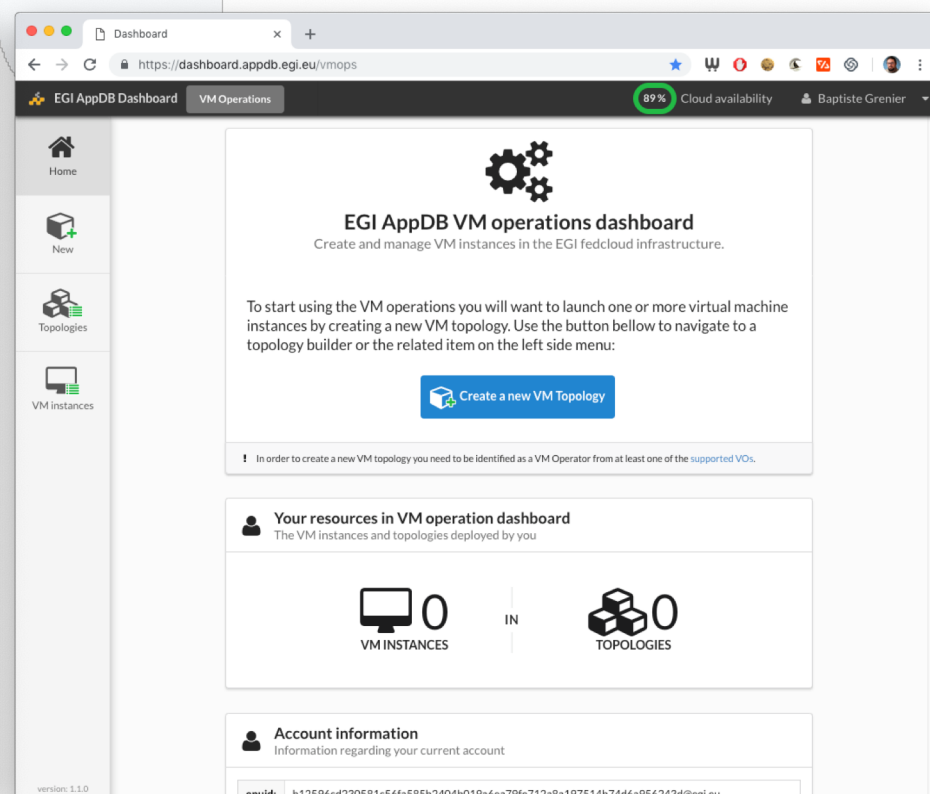
- Création graphique de topologies de déploiement – Découvertes des sites, patrons/templates et VA



The screenshot shows the 'Topology Builder' interface. At the top, it says 'Create a new topology and deploy it to the infrastructure'. Below this, there's a section for 'Configure the settings of the deployment for the selected virtual image'. The main content area is divided into several sections:

- Virtual Organization:** Shows 'fedcloud.egi.eu' with a description: 'The FedCloud Virtual Organization brings together sites and users interested in running cloud services, testing compatibility and integrating cloud sites into EGI operations infrastructure. Members identify and test techno...'
- Site Service:** Shows '100IT' with '100 Percent IT Ltd' and 'Platform: OpenStack'.
- Template Resources:** A table listing:

Logical CPUs	1
Physical CPUs	1
Memory (MB)	2048 MB
Connectivity In	true
Connectivity Out	true
Operating System	linux
- Settings:** Includes fields for 'Topology Name' (EGI_CentOS_7) and 'VM Name' (EGI_CentOS_7).
- Block Storages per VM instance:** A message states: 'You haven't defined any block storages yet. You can define up to 2 block storages which will be created and attached to the VM instances during the deployment. To define a block storage click the Add New button below.'



The screenshot shows the 'Overview' page of the 'EGI AppDB VM operations dashboard'. It features a large central card with the title 'EGI AppDB VM operations dashboard' and the subtitle 'Create and manage VM instances in the EGI fedcloud infrastructure.' Below this, a paragraph explains: 'To start using the VM operations you will want to launch one or more virtual machine instances by creating a new VM topology. Use the button below to navigate to a topology builder or the related item on the left side menu:'. A prominent blue button labeled 'Create a new VM Topology' is visible. Below the main card, there are sections for 'Your resources in VM operation dashboard' showing 'VM INSTANCES' and 'TOPOLOGIES' counts, and 'Account information' with a user ID.

- Exécuter des conteneurs sur des VMs Cloud Compute
- Différentes options
 - Single node: en utilisant la VM EGI Docker
 - Kubernetes: déployer un cluster Kubernetes sur un cluster de VMs
 - Le cluster peut être démarré avec Infrastructure Manager et Ansible
 - En cours: auto-scaling (EC3), intégration Check-in/Kubernetes
 - udocker: exécuter des conteneurs dans des jobs HTC (grille)
 - https://wiki.esi.eu/wiki/Federated_Cloud_Containers

- EGI Cloud Compute repose encore principalement sur
 - X509 et proxy VOMS pour l'accès aux ressources
 - Pour les utilisateurs sans certificats
 - Certificats robots (Science Gateways)
 - RCAuth Online CA pour obtenir un proxy personnel
- Mais déploiement en production d'un support natif OpenID Connect
 - 2 sites connectés (dont IPHC/IN2P3)
 - D'autres vont suivre
 - Plus besoin de certificats du tout!

Faites des retours sur la proposition: <http://go.egi.eu/egi-cloud-expansion>

- 3 modèles différents
 - Alliance IaaS – prérequis et intégration minimale / en option
 - Plateformes pour Applications – Déploiement TOSCA, k8s,...
 - Fédération « Software as a Service »
- Objectifs
 - Faciliter l'innovation
 - Permettre aux fournisseurs de faire partie du paysage EOSC plus simplement
 - Offrir un plus large choix de services

Thank you for your attention.

Questions?



www.egi.eu

This work by EGI.eu is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/).