MESONET
le mésocentre des mésocentres

Authentification, gestion des comptes et projets

Atelier EOSC, 26/01/2023

Michel Jouvin, IJCLab
Pierre-Antoine Bouttier, Dir. Adj UAR GRICAD

Les objectifs de MesoNET

MESONET
Le mésocentre des mésocentres

1. **Mettre en place une infrastructure nationale distribuée de type mésocentre…**
2. **…ainsi qu'une fédération de stockage…**
3. **…à destination de l'ensemble de l'ESR français.**
4. **A moyen terme, créer une Infrastructure de Recherche (IR)**

Les actions

MESONET
Le mésocentre des mésocentres

PORTAIL

SUPPORT MUTUALISÉ

OPEN SCIENCE / OPEN DATA

MACHINE CODE FORMATION – TRL 9

- Partition OpenStack
- Partition CPU
- Partition GPU

ARCHITECTURES SPECIALISÉES

- ARM - TRL 7-8
- VECTORIELLE - TRL 8-9
- QUANTIQUE - TRL 2-4

FÉDÉRATION DE STOCKAGE

Mise à Niveau & sécurité

Services aux utilisateurs

Enseignants, étudiants, industriels, chercheurs

MESONET
Le mésocentre des mésocentres

Chercheurs :

- Accès facile (uniforme) et gratuit (processus d'attribution)
- Machines à l'état de l'art, architectures spécialisées, formation, support, outils logiciels
- Disponibilités des données entre les centres MesoNET, les centres nationaux et d'autres plateformes communautaires

Enseignants, Étudiants :

- Machines hors ZRR (Zone à restriction d'accès) & Cloud
- Accès & Création de contenus pédagogiques
- Accès réservé en mode classe et libre en mode projet

Industriels :

- Accès payant
- Offre de services en lien avec le *Competence Center* Français (EuroHPC)

Le triptyque services/rôles/auth.

MESONET
Le mésocentre des mésocentres

Un utilisateur de MesoNET aura accès :

- Au portail web de gestions des comptes, des projets et ressources associées
- Aux ressources dédiées sur le site vitrine du projet
- À la documentation, au support
- Aux machines de calcul
- À la fédération de stockage

Un utilisateur pourra avoir différents droits :

- Selon son statut (étudiants, industriel, contractuel, permanent)
- Selon l'usage (e.g. fédération de stockage, différentes plateformes de calcul)
- Selon son rôle (e.g. resp. de projet, ASR, support, collaborateur externe)

MesoNET doit répondre à ces contraintes…

- …en découplant l'authentification des différents services (sites web, apps web, CLI)

Une gestion d'authentification dédiée

MESONET
Le mésocentre des mésocentres

MesoNet : créer une fédération de ressources avec un accès unifié aux différentes ressources

- Nécessité d'une authentification et autorisation globale/cohérente, utilisable par tous les services
- Choix d'une approche de type fédération d'identité pour permettre une intégration de l'authentification avec les crédentiels locaux/habituels d'un utilisateur

RENATER FER/eduGAIN : la principale infrastructure de fédération d'identité disponible

- Problème : basé sur la technologie SAML, son intégration est au mieux difficile, voire impossible dans les applications/services (surtout ceux ne reposant pas sur http)
- Ne traite que l'authentification, pas l'autorisation

Choix : mettre en place service d'authentification de MesoNet utilisant la technologie OpenID Connect/OAuth2 pour dialoguer avec les applications

- OIDC/OAuth2 est devenu la « lingua franca » de l'authentification et de l'autorisation dans les infrastructures distribuées
- Intégration facile dans les applications web, possible dans les outils mode ligne
- Basé sur un « broker d'identités » qui permet d'identifier l'utilisateur via plusieurs sources/protocoles dont SAML : l'utilisateur reste le même pour les applications

Solution retenue : Indigo IAM

OpenID Connect (OIDC) / OAut2

MESONET
Le mésocentre des mésocentres

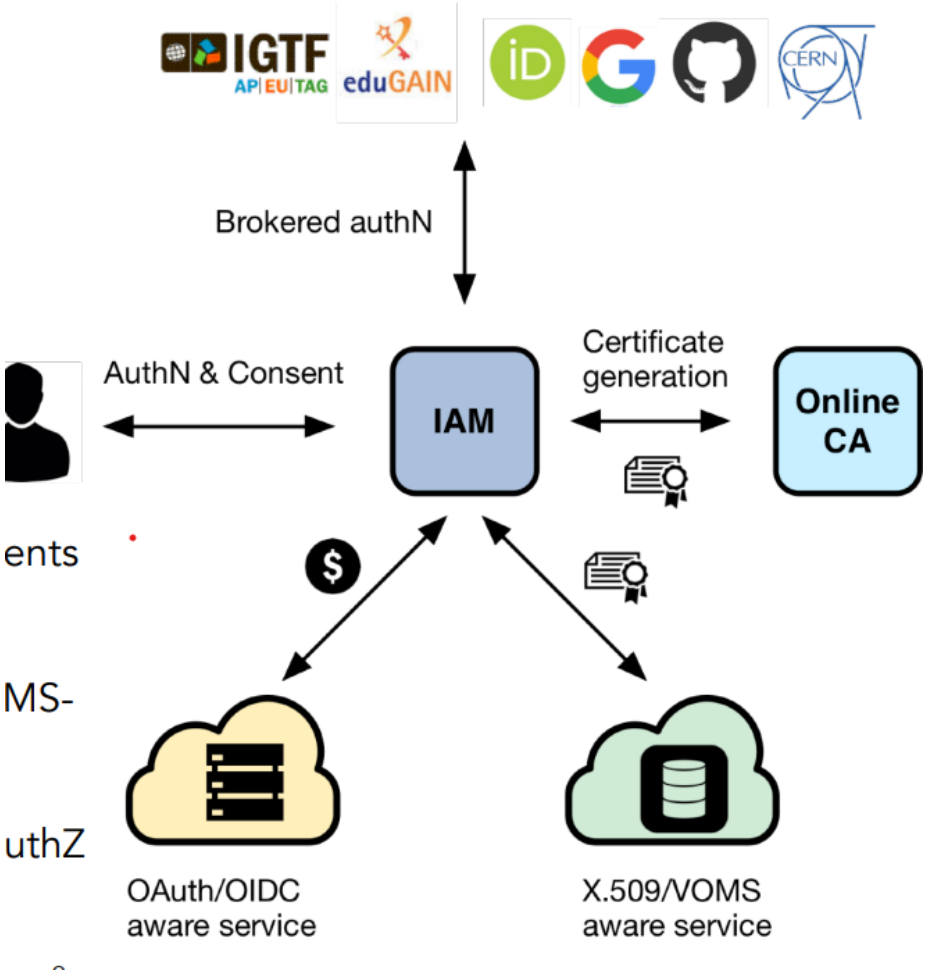
- OAuth2 : développé par les Google, Facebook & co pour échanger les informations d'authorisation
  - Permettre la cooperation entre applications tout en maintenant la coherence des authorisations
  - S'appuie sur la technologie des Jason Web Tokens (JWT)
- OIDC : extension de OAuth2 pour traiter les problématiques d'authentification
  - Devenu un standard de fait et plus vraiment d'utilisation de OAuth2 sans OIDC
  - Utilise aussi les JWT (même format de token)
  - OIDC permet la redirection de l'identification de l'utilisateur vers un provider externe
    - Exemple : utilisation d'un login GitHub ou social networks pour s'authentifier sur un autre service
    - th2 allows an application to act on behalf of a user without forwarding his credentials
  - Lingua franca de l'authz/authn dans l'internet/web
- Pour plus de details : https://indico.cern.ch/event/1185598/

Federated IAM: INDIGO IAM

MESONET
Le mésocentre des mésocentres

- IAM : Identity and Access Management
  - Multiples services IAM basés sur OIDC ont émergé : Keycloak (Red Hat), EGI Checkin, CILogon OIDC service…
- INDIGO IAM : service IAM développé par le projet européen INDIGO
  - Clouds et fédération de clouds (2014-2018)
  - Support de plusieurs protocoles d'authentification : SAML, OIDC, X509, user/password
  - Identity brokering: un utilisateur reste le même quelque soit la source d'identité qu'il utilise, s'il en a plusieurs
  - Gestion de groupes : utilisateurs peuvent être répartis dans des groupes, appartenances passées dans le token pour permettre de baser dessus les décisions d'autorisation
  - Définition de « scopes » pour permettre des autorisations à grain fin, par exemple (droit de lecture d'un répertoire particulier)
  - Parle OIDC/OAuth2 avec les applications (OIDC clients), aussi support de X509/VOMS
  - Gestion du cycle de vie des comptes : validation des demandes, signatures régulières d'AUP…

Indigo IAM Workflow



Adoption INDIGO IAM et alternatives

MESONET
Le mésocentre des mésocentres

- Adopté depuis 2 ans par WLCG comme base de l'authentification pour l'infrastructure distribuée (mondiale) des expériences LHC
  - Garantit un passage à l'échelle majeur et une pérennité
- Plusieurs projets ont adopté INDIGO IAM depuis 1 an
  - UK IRIS: INDIGO IAM utilisé pour l'authz/authn de diverses communautés nationales ou internationales (dont SKA)
  - Italie: utilisé pour l'authentification du cloud INFN, utilisé par de nombreuses communautés
  - France: MesoNET
  - Astronomie multi-messager : projet GRANDMA (MMA lié aux ondes gravitationnelles)
  - ESCAPE
- Des alternatives disponibles… qui peuvent interopérer
  - EGI Check-In : service similaire, intégré avec CoManage pour la gestion de la VO
  - Keycloak (Red-Hat) : solution utilisée dans de nombreux sites mais peut dans un contexte de fédération

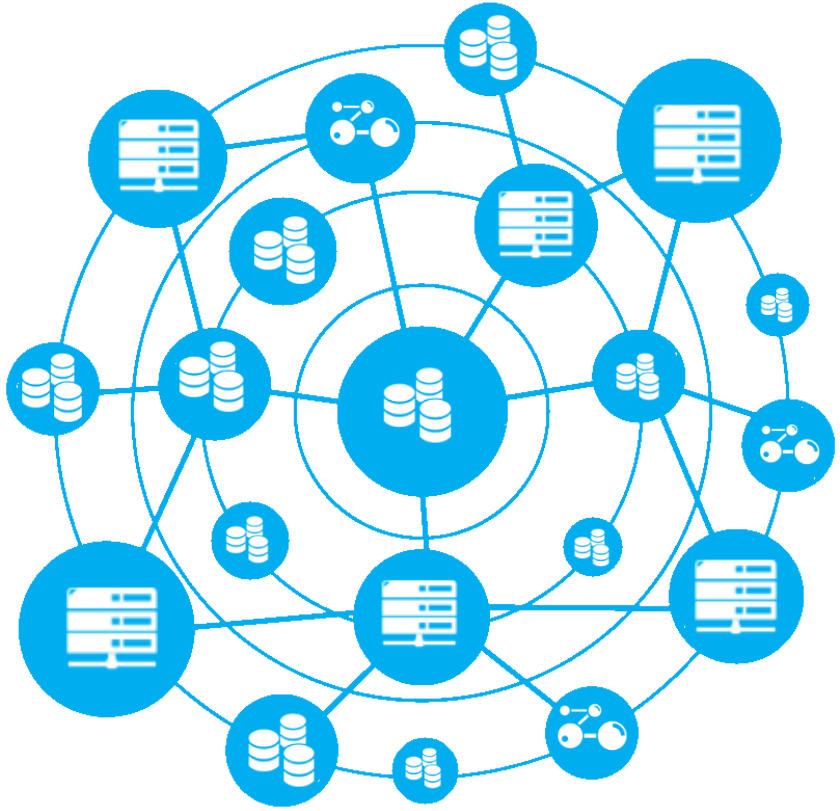
INDIGO IAM : intégration des services

MESONET Le mésocentre des mésocentres

- Services (OIDC clients) doivent être enregistrés dans le IIAM (OIDC issuer)
  - Permet d'établir le trust qui est fournit par les certificats et CAs dans le monde X509
- OIDC a été conçu pour permettre une intégration simple des services
- OIDC has been designed with a focus on easy integration with web applications
  - Très simple dans les frameworks/serveurs/services Web
  - Apache : il suffit de charger le module mod_auth_oidc et d'ajouter une clause Require
  - Extraction/traitement des informations d'autorisation contenues dans le ticket est la responsabilité des services/applications
- Application non web : nécessité d'utiliser un outil qui permet de récupérer le ticket
  - Ticket est une chaine de caractère cryptée qui sera passée à l'application
  - Plusieurs agents disponibles : oidc-agent, Hashicorp Vault/htgettoken, mytoken…)
- Batch systems : plusieurs supportent l'authentification par token (HTCondor, SLURM)
- Services de stockage : supporté par les endpoints S3 et les principaux services basés sur http
  - Particulièrement les services du monde ESCAPE : EOS, dCache, Rucio

MESONET

le mésocentre des mésocentres



https://mesonet.fr

contact@mesonet.fr