MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE

Liberté
Égalité
Fraternité

UN OUTIL POUR DÉPLOYER DES SERVICES SUR KUBERNETES

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Le Pôle de Compétences Logiciels Libres

- Conception de solutions libres orientées serveurs à destination des établissements scolaire et des académies (EOLE²), du ministère (EOLE³)
- Veille technologique
- La distributions EOLE (Ubuntu)
- Tous les outils libres pouvant être utilisés dans le cadre de l'Éducation (ceux dans Apps)
- Toujours avec l'idée de faciliter la mise en œuvre
- Le suivi des alertes de sécurités et évolutions des outils
- Interaction avec des ministères (MTES, DINUM), et plus globalement à la communauté des Logiciels Libres
- Toutes les productions du pôle sont dans une logique de transparence (forge publique, code public, images publiques, dépôts publics)
- Portage MIM LIBRE (forge publication code MEN CADA)

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
L'équipe

Gilles Grandgérard

Scrum Master
- Joël Cuissinat

Intégrateurs Helm/Docker
- Daniel Dehennin
- Fabrice Barconnière
- Laurent Flori
- Klaas Tjebbes

Experts Dev
- Bruno Boiget
- Lionel Morin

Prestataires Marché EOLE

EOLE³
Rappel Logiciels Libres

4 règles

- La liberté de l'utiliser.
- La liberté d'en étudier le fonctionnement et de le modifier.
- La liberté d'en faire des copies et de le redistribuer.
- La liberté de l'améliorer et de diffuser ces améliorations.

Voir https://www.gnu.org/philosophy/free-sw.fr.html

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Évolutions techniques vers les conteneurs

- 2011 AmonEcole 2.3 LXC
- 2014 AmonEcole 2.4 LXC
- 2015 Docker
- 2016 mim-libre.fr : infra inter-ministérielle en prod (docker-compose)
- 2017 Docker Swarm
- 2018 Hackathon Docker Swarm -> Kubernetes 1.11
- 2018 Kubernetes dans OpenNebula / Hâpy
- 2019 Scribe 2.7 avec Conteneur
- 2020 Rancher / k8s
- 2022 EOLE³ -> **apps.education.fr**

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Choix techniques

- 2020, COVID → Continuité pédagogique → BétaApps
- Choix d'être agnostique (Kubernetes)
- Choix du packaging (Helm)
- Choix SSO obligatoire (Keycloak)

⇒ **EOLE³ est un catalogue de service**

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Cibles utilisées

- **Prestataires Kubernetes As Services**

  Kubernetes OVH

  Kubernetes SCALEWAY : hébergeur du Portail Apps

- **Cible Dev**

  K3D

- **Cible PHM**

  Rancher

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Apports des solutions EOLE

L'ADN du PCLL

- Facilité de distribution (Images Docker)
- Facilité de déploiement (Chart Helm)
- Facilité de configuration (EOLE³ Tools)
- Authenticité et qualification des sources
- Ouvert à toutes contributions
- Utilisable par tout le monde

EOLE³
Choix techniques

- Gérer beaucoup de services nécessite de mettre à jour beaucoup de ***values.yaml***
- « remplir tous les ***values.yaml*** à la main c'est laborieux »
  - ✓ Besoin d'industrialiser les opérations
  - ✓ Besoin d'assurer la cohérence inter Helm

EOLE³

Helm : Exemple avec Keycloak en mode cluster

```
helm repo add codecentric https://codecentric.github.io/helm-charts

cat > values.yaml <<EOF
extraEnv: |
  - name: JAVA_OPTS_APPEND
    value: >-
      -Djgroups.dns.query={{ include "keycloak.fullname" . }}-headless
replicas: 3
EOF

helm upgrade -i keycloak codecentric/keycloakx -f values.yaml
```

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Apps.education.fr est la première instance EOLE³

- LaBoite (portail) co construit avec la DINUM (Rizomo)
- Keycloak SSO avec Cluster obligatoire, Thème Apps, Plugin FranceConnect, Plugin de filtrage par nom de domaine, plugin de metrics, plugin Jgroup Kubernetes
- Blog
- Sondage
- Agenda / Radicale
- Mezig
- Codimd
- Front-next / lookup-server (services pour la fédération nextcloud en remplacement de globalscale)

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Autres services EOLE³ disponibles

- Minio pour le gérer l'espace de stockage
- Mongodb
- Nextcloud (dans le cas non Apps) et Collabora Online
- Screego
- Filepizza
- Discourse
- RocketChat
- Mastodon
- Gitea
- Drawio
- Mobilizon
- ExcaliDraw

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Partenaires

- Contributeurs
  - ✓ DINUM (Rizomo)
  - ✓ TOSIT (Association Entreprise Sncf, Société Générale, Carrefour, …)

  Usagers intéressés
  - ✓ Collectivités EOLE2 : Départements, Villes

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Différence EOLE³ / Apps

- Dans le cadre de Apps
  - ✓ Le périmètre des utilisateurs est limité au personnel de l'Éducation Nationale
  - ✓ Une seule fédération d'identité

- Dans le cadre de EOLE³
  - ✓ pas de contrainte sur les utilisateurs (modération)
  - ✓ possibilité de fédérer plusieurs fournisseurs (EN, FranceConnect/AgentConnect, Ldap, Ad, ...)

EOLE³ tools

Outil pour le déploiement EOLE³

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Qu'est-ce que c'est ?

C'est un outil *python3* de génération de configuration.

Comment cela fonctionne ?

Sur une machine de gestion indépendante du Kubernetes :

- ✓ À partir d'un fichier de configuration simple
- ✓ L'outil applique ces valeurs à des modèles de fichier (scripts, values, ...)
- ✓ Pour générer des ressources Kubernetes nécessaires aux services EOLE³

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Bénéfices

- Un endroit unique pour la configuration
- Permet de gérer les cas non gérables avec Helm
- Facilite l'ajout de services
- Reproductibilité des déploiements

Une session type

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Installer l'outil

Pour installer l'outil :

Installer le paquet python eole3

ou

Cloner le dépôt du projet

Documentation en ligne : https://wiki.eole.education/fr/tools

EOLE³
Installer l'outil

```
lolo@appseducation:~ $ eole3 --help
Usage: eole3 [OPTIONS] COMMAND [ARGS]...

Options:
  -c, --config PATH  Configuration value file
  --help             Show this message and exit.

Commands:
  build
  config  Show configuration merged from all the configuration files:
```

EOLE³
Créer le fichier minimum pour une installation

```
cat > socle.ini << EOF
[general]
domain=eole3.ac-test.fr
# Lets'encrypt est désactivé !
EOF
```

Pré requis minimum :
- Le nom DNS
- Un certificat SSL

EOLE³
Lancer la génération des fichiers

Cette opération va générer les fichiers sans modifier le cluster kubernetes.

```
eole3 --config socle.ini build socle
```

Les fichiers sont générés et vous pouvez les consulter

EOLE³
Installer grâce à la procédure générée

Vous devez copier votre certificat dans **./install/tls.key** et **./install/tls.crt**

```
cd install && bash deploy
```

Lorsque la procédure se termine, tous les services du cluster Kubernetes auront été installés.

EOLE³ en 10 minutes

(vidéo tronquée sur podeduc.apps.education.fr)

Hébergement des images Docker et des Helm

Ou

Chaîne de confiance des déploiements kubernetes

EOLE³
Problème

La communauté n'est pas consolidée comme les distributions GNU/Linux classiques

Les ressources peuvent être éparpillées

- ✓ quay.io (RedHat)
- ✓ gcr (Google)
- ✓ Docker hub (Docker Inc.)
- ✓ Dépôt Git (GitHub, …)

kubectl apply -f https://somewhere.example.net/something.yaml

est le nouveau

curl | sudo bash

Il est nécessaire de valider et auditer les images et charts Helm à chaque version

Créer un dépôt d'images de conteneur et de charts Helm

Reconstruire les images

Stocker toutes les images et charts dans ce dépôt

Signer et vérifier

EOLE³
Automatisation de la chaîne de production

Les images sont immutables et doivent être régénérées au besoin.

Exemple :
1. Une alerte de sécurité est levée sur l'image alpine
2. L'image est mise à jour
3. Les images qui en dépendent doivent être reconstruites
4. Les tests sont réappliqués

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Une communauté interministérielle

Tout le monde fait face à la même problématique

Une première journée BlueHats sur les Helm Charts

Plusieurs groupes de travail

- ✓ Partage des bonnes pratiques
- ✓ Création d'une communauté de mutualisation
- ✓ Un recensement du travail existant

Salon Tchap BlueHats - Helm Charts

LaBoite

- LaBoite un portail personnalisable
- Il est utilisé comme portail de Apps.Education.Fr
- Il peut être utilisé dans d'autres cas (Rizomo, Collectivités, Associations)

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Genèse de LaBoite

Le pôle de Compétences Logiciels Libres développe LaBoite :

Manque d'évolutions dans les portails existants, difficulté d'utilisation collaborative

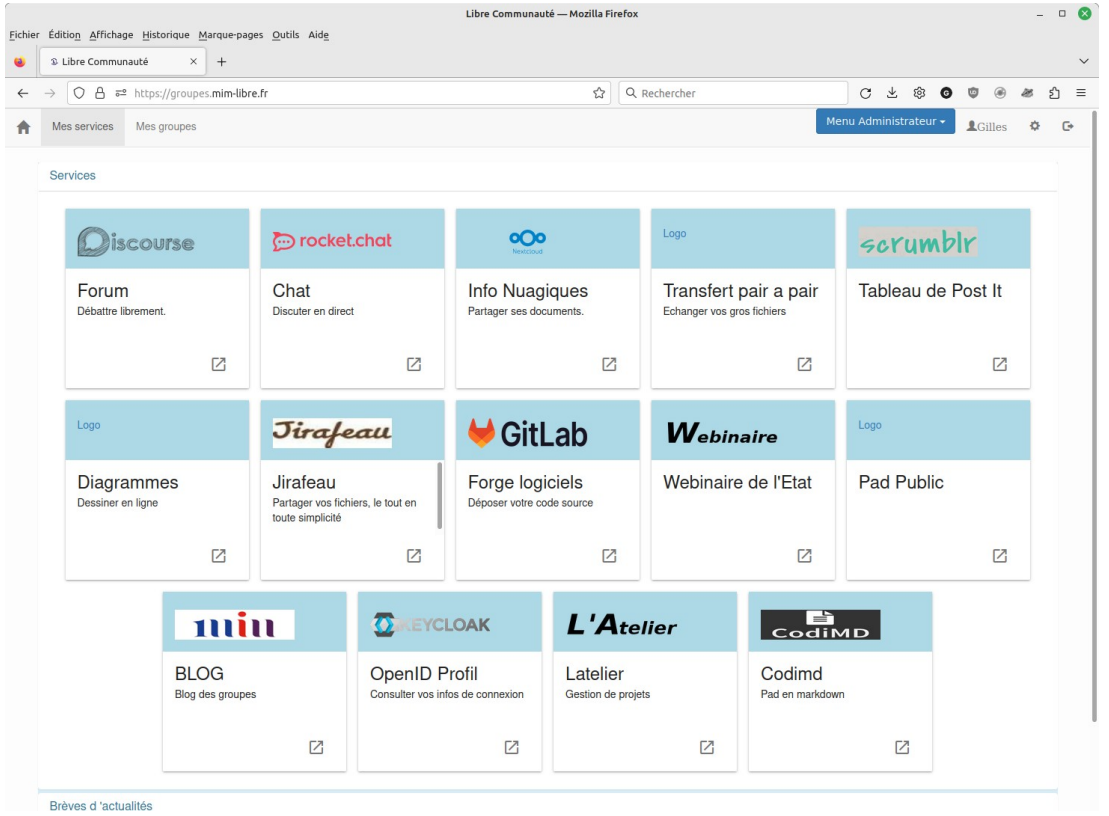
PCLL crée en 2016 le portail utilisé pour https://groupes.mim-Libre.fr

Au moment du confinement, utilisation LaBoite pour Apps Beta + services complémentaires

En RetEx, la notion de groupe devient l'élément central du portail

L'utilisateur contrôle son espace de travail dans le portail (on ne lui impose pas)

Le fonctionnement des groupes est pensé de manière globale



MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Le portail LaBoite

Un portail unique pour l'ensemble des utilisateurs qui permet :

Une authentification unique entre services (SSO)

La présentation des services

Un espace personnel

La gestion des structures

La création de groupes (ouverts, restreints, privés) et la configuration des outils tiers (Nextcloud, RocketChat, ...)

Une gestion des annonces (nouveautés, maintenance)

Gestion des marques pages (pour remplacer les raccourcis des navigateurs)

Gestion des mentions légales, CGU, contacts.

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Services complémentaires au portail

Le pôle de Compétences Logiciels Libres développe plusieurs applications complémentaires

La gestion de rendez-vous / événements : Agenda

La gestion des profils publics : Mezig

L'organisation de réunions / prise de rendez-vous : Sondage

La publication d'articles : Blog

EOLE³
Les structures

Une structure peut contenir d'autres structures

Chaque structure peut personnaliser ses services

L'administration est déléguée à des 'administrateurs de structure'

EOLE³
Personnalisation

Dans l'espace personnel

- Gestion des applications favorites
- Création des espaces de rangement thématique
- Utiliser un moteur de recherche interne (pour les groupes)

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Gestion des groupes

Grâce à la gestion des groupes, l'utilisateur dispose de services collaboratifs :

Gérer des événements de groupe

Gérer des sondages de groupe

Gérer des publications de groupe

Placer des marques-pages de groupe

Configurer automatiquement dans Nuage (Nextcloud) un partage de groupe

Configurer automatiquement un canal dans RocketChat

…

⇒ **LaBoite évite à l'usager de connaître en détail l'administration de chaque service**

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Un peu de technique

LaBoite est réalisé en MeteorJS, React
Son design est "*responsive*"
L'authentification s ‘appuie sur OpenID

LaBoite a été audité en terme de RGAA (Oct 2021) et de Sécurité (Jan 2023)

Le projet est hébergé sur la forge MIM Libre :
https://gitlab.mim-libre.fr/alphabet/laboite

Site de démo :
https://demo.eole3.dev

MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

EOLE³
Merci

- Documentation EOLE³ : https://wiki.eole.education/
- Hub EOLE³ : https://hub.eole.education/
- Forge MIM LIBRE : https://gitlab.mim-libre.fr
- Chat MIM LIBRE : https://chat.mim-libre.fr
- Inscription MIM LIBRE : https://groupes.mim-libre.fr
- Mastodon : https://mastodon.eole.education/@EOLE

- Listes de diffusion : https://pcll.ac-dijon.fr/listes
- Par messagerie instantanée: https://webchat.oftc.net canal #Eole
- Site de diffusion EOLE 2 : http://pcll.ac-dijon.fr/eole/
- Site de développement EOLE 2 : https://dev-eole.ac-dijon.fr
- Inscription EOLE 2 : https://pcll.ac-dijon.fr/inscription