POC ENVOLE

INTRODUCTION

Envole est une solution qui propose un ensemble d'applicatifs web fédérés autour d'un annaire afin de gérer l'identité ainsi qu'un SSO afin de gérer l'authentification.

Il s'appuit sur la distrution EOLE pour déployer ses différents composants.

Envole rencontre depuis des années des problèmatiques :

- Elle doit se baser sur une version précise d'EOLE 2.5 ou 2.6 ou 2.7 ou 2.8 ou 2.9 qui ont chacune leur contrainte de version php
- Les différentes applications Envole ont leur propre contrainte de version php.
- Ce qui oblige de limiter les possibilités de montée de version de l'application dans une version x d'eole car cette dernière ne fournit pas la version minimum de php requise
- Ou qui empéche le passage d'une application de fonctionner dans une version x d'eole car cette dernière propose une version trop résente de php pour l'application

Ce document va chercher à évaluer la possibilité de conteneriser les applications Envole, afin qu'elles puissent fonctionner le moins possible en contrainte avec la version d'Eole

ARCHITECTURE

EOLEBASE

La présente étude part du principe qu'Envole ne serait plus installé sur une instance Scribe mais sur une installation EoleBase d'Eole

Avantages

- Décharger le serveur Scribe et lui laisser ses fonctions principales. C'est à dire
  - Contrôleur de Domaine
  - SSO
  - Annuaire
  - Imap (et SMTP ?)
- Faire évoluer plus facilement le serveur Envole vers des versions plus récente d'Eole avec moins de contrainte tout en assurant une mise à jour de sécurité plus régulière

Inconvéhients

- L'adminstrateur devra configurer le lien SSO et Annaire qui eux restent sur le scribe.
- Il devra donc fixer certains secrets sur le Scribe (notamment le compte reader/writer annuaire sur le scibe)
- Connaitre et renseigner les hosts/ports des service SSO et Annuaire
- Avoir un second nom de domaine pour l'accès aux applications Envole

PAQUET DEBIAN

Contrairement à la précédente logique Envole, il n'y aurait qu'un seul paquet Debian pour Envole. Il n'installerait pas les sources des applications, mais uniquement

- le dictionnaire eole de configuration
- les templates de configuration
- le dossier de définitions de l'ensemble des conteneurs possible pour Envole
- un script qui viendrait monter ou non les conteneurs souhaités par l'administateur

POC

Afin de s'assurer de la faisabilité d'un tel changement, un POC a été initié, dans le cadre des éléments précédents cités. La première question fut de savoir quelle technologie de conteneurisation serait à utiliser PODMAN ou DOCKER, et dans leur logique de composer PODMAN-COMPOSE ou DOCKER-COMPOSER.

PODMAN VS DOCKER SUR EOLE

PODMAN

Eole a intégré à partir de la 2.9 dans sa distribution podman. Ce qui de prime abord devrait-être la technologie à utiliser, sauf que

- Ubuntu 22.04 ne dispose pas de paquet pour podman-compose
- Pour installer podman-compose, il est nécessaire de l'installer via pip
- De plus la version de podman disponible sur Ubuntu 22.04 est une version 3.4 qui n'est pas compatible avec la version de podman-compose
- Il est nécessaire d'installer la dernière version 4.4 de Podman PPA pour faire fonctionner l'ensemble
- Par la suite il est possible de créer un composer d'image docker comme on pourrait le faire avec docker-compose. Podman est juste plus stricte dans sa synthaxe et certaines commandes ne sont pas tout à fait indentique
- Mais il apparait qu'un reconfigure rendra totalement inopérant le réseau des conteneurs. Pour le rendre de nouveau opérant, il est nécessaire de le détruire pour le reconstruire.

DOCKER

Eole n'a pas intégré nativement docker. Mais il est tout à fait possible de l'installer par ses propres moyens sauf que

- Tout comme Podman Ubuntu ne propose pas de paquet suffisament à jour de docker-ce et docker-compose
- Il est nécessaire de les installer via la mise en place d'un PPA
- Par la suite docker se comporte bien mieux que podman. Il est plus souple d'usage, moins verbeux
- Mais tout comme podman, un reconfigure vient rendre totalement inopérant le reseau des conteneurs. Il est nécessaire de réinitialiser docker-ce pour rétablir le reseau.

CONCLUSION

Quoi qu'il arrive, une intégration compléte que cela soit avec Podman ou avec Docker, demandera un travail d'intégration d'Eole

- afin de disposer des dernières versions possibles de l'un ou de l'autre
- que l'un ou l'autre ne détruit pas le réseau associé au composer de conteneur

Ma préférence va malgrés tout sur Docker, il est plus souple moins verbeux et me semble plus fiable à long terme. Il serait possible de maitenir les deux solutions en parrallèle avec un effort supplémentaire d'intégration et de maintenance.

POC

SOURCES

Les sources du POC sont disponible ici
https://forge.cadoles.com/Envole/envole

Elles sont pour l'instant hébergé à Cadoles pour des raisons de simplicité de mise en oeuvre, mais à terme elles seront bien stockées chez Eole

REPOSITORY

Certaines images sont hébergées elles aussi sur un repository public de Cadoles. Là aussi pour des raisons de simplicité de mise en oevre, mais à terme Eole devra fournir un repository propre aux images Envole.

Les images en questions sont celles des applications maintenues par Envole, en l'occurence pour l'instant uniquement Ninegate. Mais à terme pourra aussi y figurer des images d'applications tiers sur lesquelles nous aurions besion d'altérer légèrement le comportement.

INSTALLATION DU POC

1- Instancier un eolebase 2.9

2- Installer eole-web

```
apt-get install eole-web
Genconfig
Services > Activer l'interface web de l'EAD = non
Services > Activer le serveur de bases de données MySQL = non
Services > Activer l’interface d’administration du module (EAD3) = non
Applications Web > Nom de domaine des applications web = mondomaine.fr
save & quit
Reconfigure
```

3- Installer docker & docker-compose

```
apt install git make apt-transport-https ca-certificates curl gnupg-agent
software-properties-common
mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | gpg --dearmor -o
/etc/apt/keyrings/docker.gpg
echo \
"deb [arch=$(dpkg --print-architecture) signed-
by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu \
$(lsb_release -cs) stable" | tee /etc/apt/sources.list.d/docker.list >
/dev/null
apt update
apt-get install docker-ce docker-ce-cli containerd.io docker-compose-plugin
docker-compose
```

4- Installer Envole

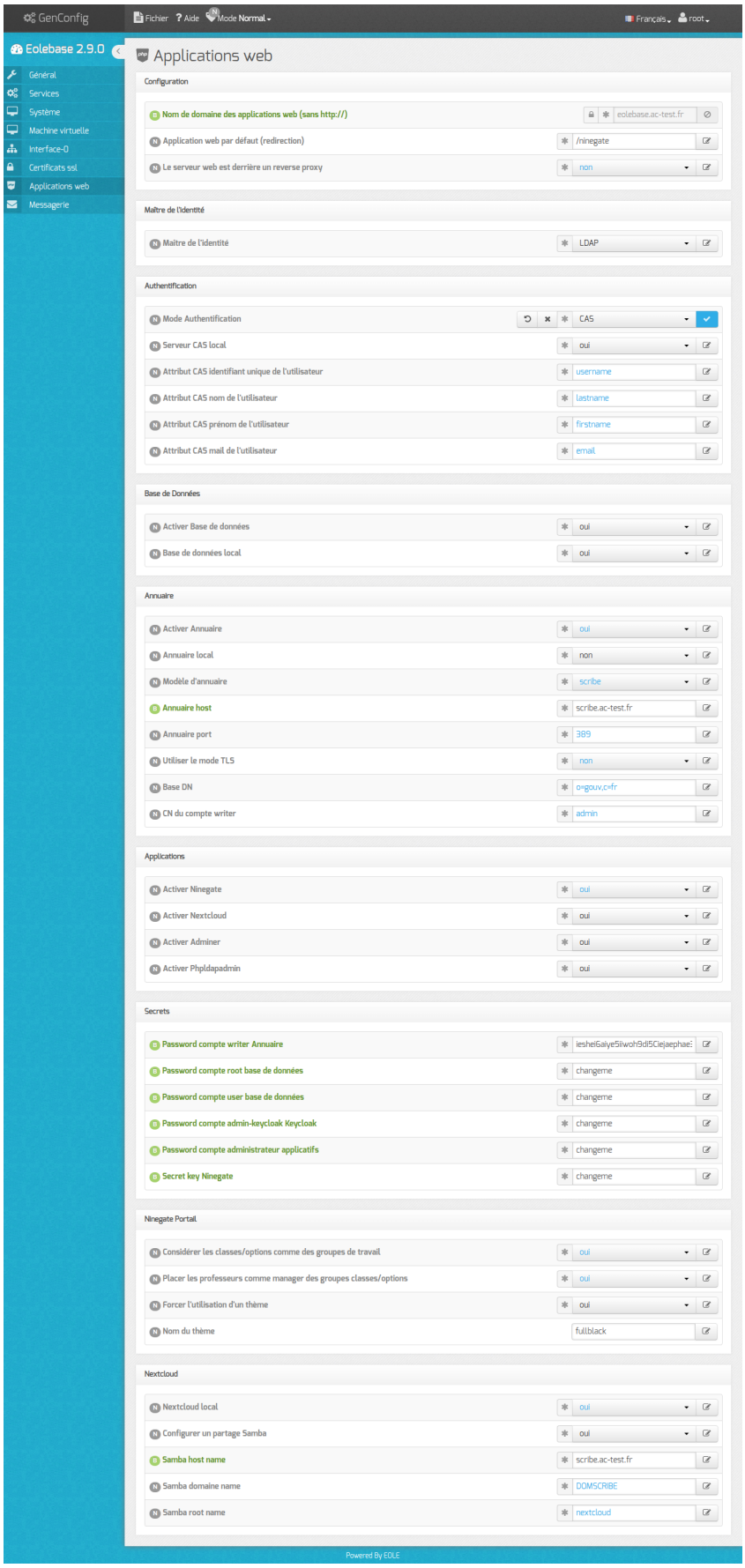
```
cd /root
mkdir git
cd /root/git
git clone https://forge.cadoles.com/Envole/envole.git
cd /root/git/envole
make install
```

5- Configurer Envole

Le dictionnaire d'Envole dans genconfig est initalisé pour que l'on y indique un scribe distant.

6- Reconfigure

COMPLÉMENT SUR VARIABLES GENCONFIG



Maître de l'identité

- SQL = c'est un cas bien particulier qui devrait pas vous concerner. C'est le cas où c'est Ninegate qui gére les utilisateurs et les groupes et qui va pousser ces informations dans un annuaire qui doit-être forcement local
- LDAP = c'est le cas classique d'un établissement scolaire. Ninegate synchronisera les utilisateurs et les groupes en fonction d'un annuaire distant. Cela pourrait-être aussi le cas d'usage d'un PIA qui a son propre annuaire. Tout dépendra du modèle d'annuaire déclaré dans le genconfig
- SSO = c'est le cas où il n'y a pas de synchronisation annuaire, mais que les applications se basent sur les attributs SSO pour autocreate et autoupdate les utilisateurs qui se connectent

Mode d'Authentification

Il n'y a que Ninegate qui pour l'instant peut faire varier son mode d'authentification
A l'avenir on pourrait implémeter d'autre méthode d'authenfication, l'OPENID ou le SAML par exemple.

- SQL = l'authentification se fait par le mécanisme interne à l'application. Pas de SSO dans ce cas.
- LDAP = l'authentification se fait via un bind sur l'annuaire. Pas de SSO dans ce cas.
- CAS = l'authentification se fait via le protocole CAS. Déclarer un serveur CAS dans ce cas est obligatoire. C'est le cas classique d'Envole à l'heure actuelle

Server CAS local

Si oui un conteneur Keycloak sera instancié qui sera préparamétré pour utiliser le procotole CAS en lien avec l'annuaire soit local soit distant déclaré dans le genconfig

ATTENTION = une foi instancié le serveur Keycloak ne prendra pas en compte des changement de paramétrage lié à l'annuaire

Base de Données

Si désactivé, l'ensemble des applications nécessitant une base de données ne pourront être activée.

Si distant, Envole ne fera pas le travail de créer les utilisateurs de base de données ainsi que les bases de données applicatives en elles-même. Cela sera à la charge d'un administrateur de réaliser ces tâches.

ATTENTION = une foi instancié les changement de login/password d'accès à la BDD ne seront pas appliqués

Annuaire

Le cas d'un annuaire local n'est utile que si le maître de l'authenfication est local.

ATTENTION = une foi instancié les changement de login/password d'accès à la BDD ne seront pas appliqués

Secrets

L'ensemble des secrets nécessaires. Comme indiqué plus haut un grand nombre d'entre eux ne peuvent être modifié après instanciation du service associé au secret : BDD / Annuaire / Keycloak

Nextcloud

Possiblité d'indiqué un partage Samba pour générer automatiquement un partage externe dans Nextcloud

CONCLUSION

Ce POC démontre qu'un modèle conteneriser d'Envole est tout à fait possible. Mais

Ce que le POC à montrer comme problème

- Des versions trop anciennes que cela soit sur Podman ou Docker
- Un problème de variable d'environnement via Podman qui n'accepte pas de surcouche de variables
- Des problèmatiques de réseau après reconfigure à résoudre par EOLE
- Sur scribe29 : Nextcloud et Roundcube sont préinstallés. Si demain on souhaite mettre Envole sur scribe il faudra enlever cette dépendance.

Ce que ne fait pas le POC

- Changer les secrets après instanciation
- Changer la configuration Keycloak après instanciation

Ce que le POC n'a pas du tout aborder

- Comment migrer de la version actuelle d'Envole vers ce modèle
- Comment gérer la mise à jour des conteneurs (monté de version des applications)
- Comment intégrer les scripts de synchronisation annuaire sur les applications qui n'ont pas de mécanisme interne (poshprofil)
- Comment intégrer la sonde statistique
- Comment envoyer du mail (service scribe imap/smtp CASsifié sur le scribe et très complexe à utiliser à distance)