I-GENERALITES SUR KEYCLOAK

1. **Historique**

La première version de production de keycloak a eu lieu en septembre 2014, le développement ayant commencé environ un an plus tôt par Red Hat.

1. **Qu’est-ce que Keycloak ?**

Keycloak est un outil de gestion des identités et des accès, il facilite la sécurisation des applications et des services avec peu ou pas de code. De plus, Keycloak est un outil open source actuellement sous licence Apache Licence 2.0 et actuellement à la version 15.0.2 (2021-10-09). Il s’agit d’un projet en Amont pour Red Hat SSO (Red Hat Single Sign-on), c’est une initiative de Red Hat qui vise à offrir une Authentification Unique et qui permet de sécuriser des applications web en fournissant des fonctionnalités web Single Sign-on (SSO) basées sur des normes populaires telles que SAML 2.0, OpenID Connect et OAuth 2.0.

1. **Caractéristiques de Keycloak**
2. **Distributions de Keycloak**

Actuellement Keycloak a trois distributions principales disponible sur :

* **Serveur**

L’application autonome est téléchargeable à partir de la page Keycloak sous la forme d’une archive tar ou zip avec tous les scripts, documents et ressources nécessaires pour fonctionner normalement. Pour l’instant, il existe deux versions principales de cette distribution : l’une est alimentée par le serveur WildFly tandis que l’autre est alimentée par Quarkus.

* **Image Docker**

Distribution appropriée pour Docker, Podman, Kubernetes et OpenShift. Il existe deux images Docker officielles pour Keycloak : l’une est conservée dans Quay Container Registry-**quay.io/keycloak/keycloak**, la seconde est conservée dans Docker Hub-**jboss/keycloak**. Les deux sont téléchargeables avec la commande « docker pull ».

* **Operateur**

Distributions pour kubernetes et OpenShift basée sur Operator SDK.

1. **Composants**

Keycloak est compose de deux composants principaux à savoir :

* Un serveur Keycloak
* Un adapteur d’application

1. **Spécificités**

* **Prise en charge de plusieurs protocoles**

Pour l'instant, Keycloak prend en charge trois protocoles différents, à savoir - OpenID Connect, OAuth 2.0 et SAML 2.0.

* **Authentification unique**

Keycloak a un support complet pour Single Sign-On et Single Sign-Out.

* **Console d'administration**

Keycloak propose une interface graphique Web où l’on peut « cliquer » sur toutes les configurations requises par une instance pour fonctionner comme on le souhaitez.

* **Identité et accès de l'utilisateur**

Keycloak peut être utilisé comme un gestionnaire d'accès et d'identité d'utilisateur autonome en nous permettant de créer une base de données d'utilisateurs avec des rôles et des groupes personnalisés. Ces informations peuvent également être utilisées pour authentifier les utilisateurs au sein de notre application et en sécuriser certaines parties en fonction de rôles prédéfinis.

* **Fournisseurs d'identité sociale**

De plus, Keycloak permet d'utiliser des fournisseurs d'identité sociale. Il prend en charge Google, Twitter, Facebook, Stack Overflow mais, en fin de compte, l’on doit tous les configurer manuellement à partir du panneau d'administration. La liste complète des fournisseurs d'identité sociale pris en charge et leur manuel de configuration se trouvent dans la documentation de Keycloak.

* **Personnalisation des pages**

Keycloak permet de personnaliser toutes les pages qu'il affiche pour des utilisateurs. Ces pages sont au format « .ftl » de sorte que l’on puisse utiliser des HTML  balises et des CSS styles classiques pour adapter la page au style de votre application et à la marque de votre entreprise. L’on peut également mettre du JavaScript personnalisés dans le cadre de la personnalisation des pages afin que les possibilités soient illimitées.

1. **Pourquoi utiliser Keycloak ?**

Tout d’abord, Keycload est **gratuit** ce qui est un atout considérable car généralement la plupart des outils dotes des fonctionnalités telles que Autho ou Okta sont payants.

Deuxièmement, Keycloak prend en charge les protocoles standard suivants : **OAuth 2.0, OpenID Connect et SAML 2.0.** Cette prise en charge signifie que tout outil ou application prenant en charge l’intégration avec les protocoles ci-dessous peut-être connecte à Keycloak (par exemple, des applications d’entreprise telles que Red Hat Ansible Tower ou SAP Business Intelligence Platform). Par ailleurs, le fait de prendre en charge ces trois protocoles d’authentification différents donnent la possibilité de couvrir de nombreuses applications avec des exigences de sécurité différentes avec un seul outil.

De plus, Keycloak peux être utiliser avec des bases de données utilisateurs existantes telles que LDAP, Active Directory, car dispose d’un mécanisme de synchronisation avec de tels fournisseurs d’identité.

De plus, il prend en charge les fournisseurs d’identité sociale comme Google ou Facebook et fournit une interface graphique Web qui facilite les modifications de configuration.