# Gestion des accès/RBAC Grafana

**Démo Equipe Monitoring du 13/09/2022**

# Principe du POC

- On connecte 3 Grafana à Keycloak.
- On crée des utilisateurs avec des rôles Keycloak différents.
- On vérifie dans Grafana quel utilisateur a quel rôle.
- On vérifie les fonctionnalités disponibles dans Grafana selon les rôles.

# Comptes utilisateurs

| | grafana-PF1136-1 | grafana-PF1136-2 | grafana-PF1136-3 |
|---|---|---|---|
| **pf1136-user-1** | grafana-admin | grafana-viewer | pas de rôle (pas d’accès) |
| **pf1136-user-2** | grafana-viewer | pas de rôle (pas d’accès) | grafana-viewer |
| **pf1136-user-3** | grafana-editor | pas de rôle (pas d’accès) | grafana-bad-role (pas d’accès) |

# Configuration Keycloak

Différentes étapes à réaliser dans Keycloak :

- création de clients ;
- création de rôles dans chaque client ;
- créations de mappers dans chaque client ;
- création d’utilisateurs de test ;
- modification *role mapping* pour chaque utilisateur.

# Tests d’accès à Grafana

Deux types de tests réalisés :

- accès refusé par Keycloak
  - en utilisant la fonctionnalité *authorisation*
  - en utilisant l’extension de Keycloak `keycloak-restrict-client-auth`
- accès refusé par Grafana
  - en ne donnant aucun rôle Grafana à l’utilisateur connecté

# Tests d’accès à Grafana : refus par Keycloak

Fonctionnalité *authorisation* :

- Keycloak vérifie les permissions sur une ressource (policies : user, group, role…) et détermine si l’accès est autorisé ou non ;
- Keycloak indique à Grafana si l’accès est autorisé ou non dans les informations qu’il lui envoie ;
- Grafana (version communautaire) ignore cette information.

Extension Keycloak sventorben/keycloak-restrict-client-auth :

- permet de restreindre l’autorisation des utilisateurs sur les clients ;
- nécessite d’ajouter un fichier à Keycloak puis de lancer un script pour le reconfigurer.

# Tests d’accès à Grafana : refus par Grafana

On met `role_attribute_strict=true` dans la configuration de Grafana.

Si l’utilisateur n’a pas de rôle défini dans Keycloak, il n’a pas de rôle dans Grafana.


Donc l’utilisateur se connecte à Grafana mais n’a aucun droit.

# Tests sur les rôles dans Grafana

Le paramètre `role_attribute_path` de Grafana permet de faire une correspondance entre les rôles dans Keycloak et les rôles dans Grafana.

```
role_attribute_path = contains(roles[*], 'grafana-admin') && 'Admin'
   || contains(roles[*], 'grafana-editor') && 'Editor'
   || contains(roles[*], 'grafana-viewer') && 'Viewer'
   || 'Reject'
```

| compte | rôle Keycloak | rôle Grafana | Grafana de démo |
|---|---|---|---|
| **pf1136-user-1** | grafana-admin | Admin | Grafana 1 |
| **pf1136-user-3** | grafana-editor | Editor | Grafana 1 |
| **pf1136-user-2** | grafana-viewer | Viewer | Grafana 1 Grafana 3 |
| **pf1136-user-3** | grafana-bad-role | Viewer avec `role_attribute_strict=false`<br>Rejeté avec `role_attribute_strict=true` | Grafana 3 |
| **pf1136-user-2** | aucun | Viewer avec `role_attribute_strict=false`<br>Rejeté avec `role_attribute_strict=true` | Grafana 2 |
| **nominatif** | aucun | Viewer avec `role_attribute_strict=false`<br>Rejeté avec `role_attribute_strict=true` | Grafana 1 |

# Fonctionnalités de Grafana selon les rôles

Voir le tableau récapitulatif Grafana selon les rôles.

# Conclusion

- Refus d’accès à un Grafana : fonctionnel mais utilisation non instinctive, la solution est plus un moyen de contournement.
- Attribution d’un rôle dans Grafana : fonctionnelle.
- Test seulement sur la fin de la chaîne d’authentification :

habilitations myportal -> profilApplicatifs signon -> rôles keycloak -> Admin/Editor/Viewer grafana