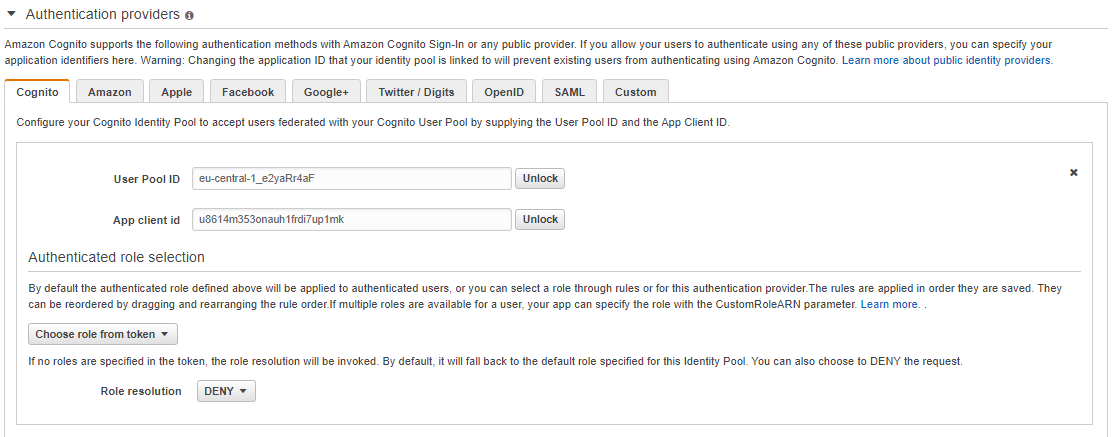
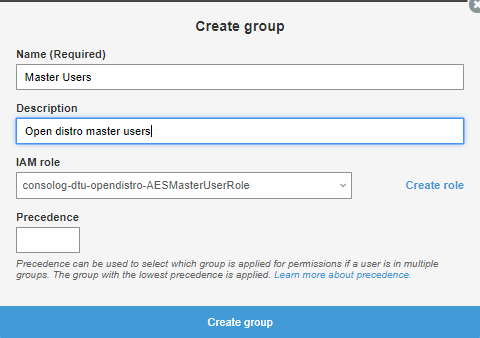
Procédure de déploiement AES

# Configuration Cognito

## Configuration Authentication Provider

1. Navigue vers le console d’AWS Cognito
2. Sélectionnez « Manage User Pools »
3. Sélectionnez « consolog-AES-UserPool-${ENV} »
4. Sélectionnez « App Clients » et notez le « App Client ID »
5. Sélectionnez « Federated Identities » (haut de page)
6. Sélectionnez le « consolog-AES-IdentityPool-${ENV} »
7. Clic sur « Edit Identity Pool » haut du page à droite
8. Éclater le panneau « Authentication Providers » et vérifiez que le User Pool ID et App Client ID sont bien saisie
9. Dans le menu déroulant choisissez « Choose Role from Token »
10. Role Resolution : « Deny »   
    
11. Enregistrer les modifications

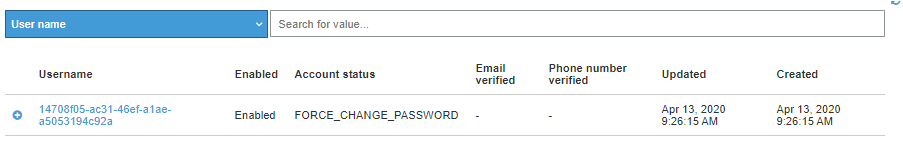
## Configuration Groupe Admin

1. Navigue vers le console d’AWS Cognito
2. Sélectionnez « Manage User Pools »
3. Sélectionnez « consolog-${ENV}-AESUserPool »
4. Sélectionnez « Users and Groups »
5. Sélectionnez l’onglet « Groups » puis « Create Group »
6. Name : Master\_Users
7. IAM Role : Sélectionnez le Master Role dans la liste déroulant (consolog-${ENV}-opendistro-MasterUsers)  
   
8. Clic sur « Create Group »

## Configuration Groupe Accès Restreint

1. Navigue vers le console d’AWS Cognito
2. Sélectionnez « Manage User Pools »
3. Sélectionnez « consolog-${ENV}-AESUserPool »
4. Sélectionnez « Users and Groups »
5. Sélectionnez l’onglet « Groups » puis « Create Group »
6. Name : LIMITED\_GROUP\_NAME
7. IAM Role : Sélectionnez le Role IAM Limité dans la liste déroulant (consolog-AESLimitedUserRole-${ENV})
8. Clic sur « Create Group »

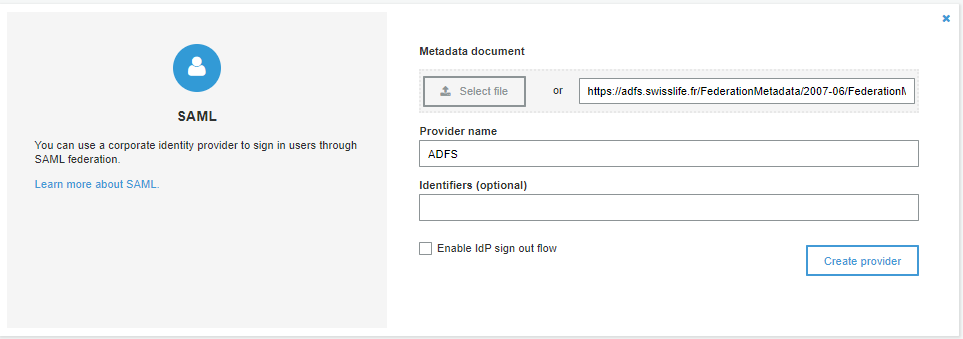
## Ajouter un utilisateur dans un groupe Cognito

1. Navigue vers le console d’AWS Cognito
2. Sélectionnez « Manage User Pools »
3. Sélectionnez « consolog-${ENV}-AESUserPool »
4. Sélectionnez « Users and Groups »
5. Sélectionnez l’onglet « Groups » puis clic sur le nom du groupe à modifier
6. Clic « Add Users »
7. Trouvez l’utilisateur dans la liste (Ou chercher un utilisateur par nom de l’utilisateur)
8. Ajouter l’utilisateur en cliquant sur l’icône +  
   

## Supprimer un utilisateur d’un groupe

1. Navigue vers le console d’AWS Cognito
2. Sélectionnez « Manage User Pools »
3. Sélectionnez « consolog-AES-UserPool-${ENV} »
4. Sélectionnez « Users and Groups »
5. Sélectionnez l’onglet « Groups » puis clic sur le nom du groupe à modifier
6. Trouvez l’utilisateur à supprimer dans le tableau des utilisateurs
7. Supprimer l’utilisateur en cliquant sur l’icône X dans la colonne « Remove »

# Configuration ADFS

1. Navigue vers le console d’AWS Cognito
2. Sélectionnez « Manage User Pools »
3. Sélectionnez « consolog-AES-UserPool-${ENV} »
4. Selectionnez « Identity Providers »
5. Selectionnez « SAML »
6. Metadata URL : <https://adfs.swisslife.fr/FederationMetadata/2007-06/FederationMetadata.xml>
7. Provider Name : ADFS  
   
8. Clic « Create Provider »
9. Selectionnez « App Client Settings »
10. Cochez « ADFS »
11. Decochez « Cognito User Pool »
12. « Save Changes »

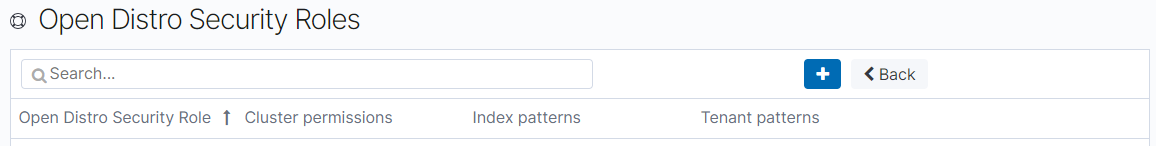
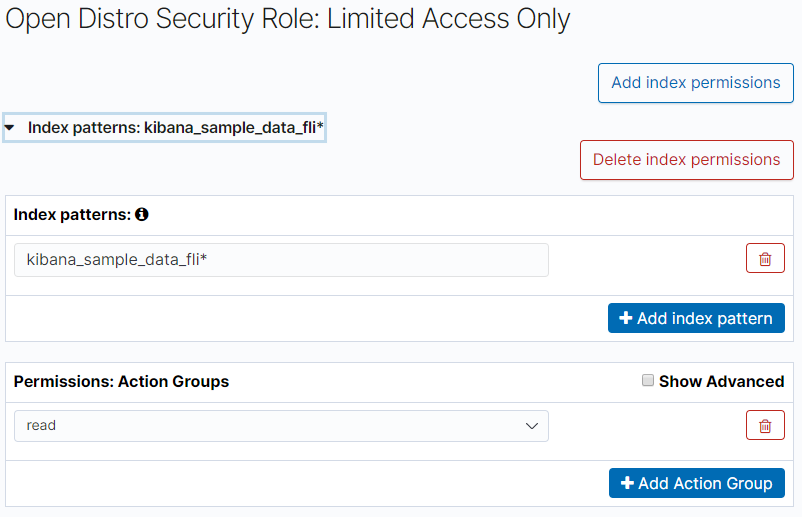
# Configuration Kibana / Cognito

## Création d’un Tenant pour l’index

Open Distro n’utilise pas des dossiers pour regrouper les objets. Pour organiser les objets associés à un index il faut utiliser un tenant. Ce tenant permet également de limiter l’accès des utilisateurs aux objets.

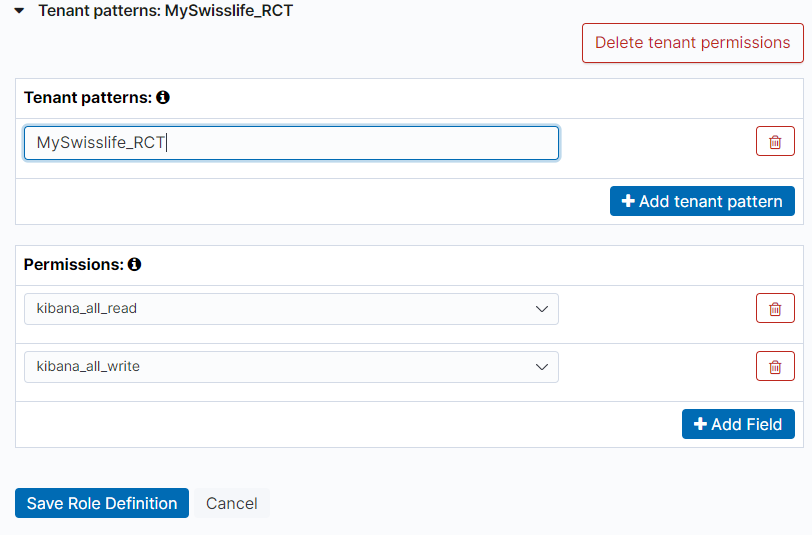
1. Naviguer vers Kibana
2. Connectez-vous comme Administrateur
3. Sélectionnez « Security » dans le menu à gauche
4. Sélectionnez « Tenants » puis ajoute un nouveau Tenant ()
5. Name : le nom du tenant
6. Submit

## Création d’une Rôle sur Kibana

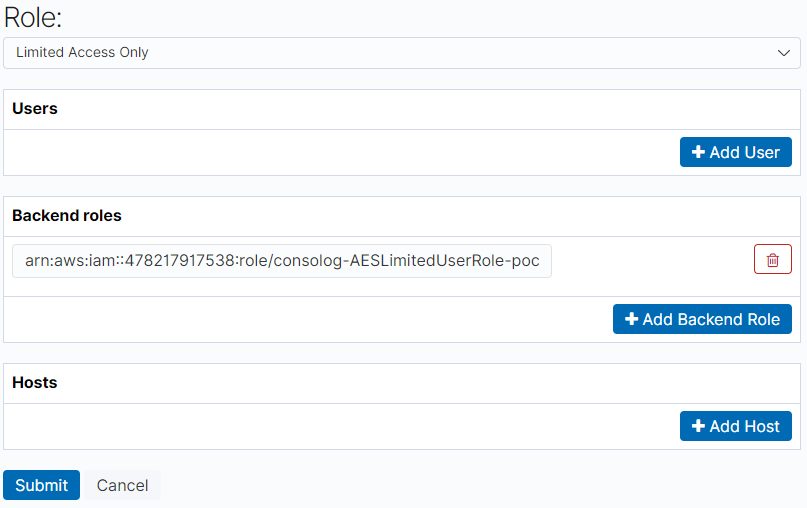
1. Naviguer vers Kibana
2. Connectez-vous comme Administrateur
3. Sélectionnez « Security » dans le menu à gauche
4. Sélectionnez « Roles » puis « Add a new Role » ()  
   
5. Name : Nom du Role
6. Sélectionnez : « Index Permissions »
7. Clic : Add Index Permissions
8. Spécifier une paterne d’indexe à utiliser
9. Clic « Add Action Group »
10. Sélectionnez les droits à attribuer (Read)  
    
11. Clic « Save Role Definition »

## Association d’un Tenant à un Rôle Kibana

Pour autoriser un groupe d’utilisateurs d’enregistrer leurs objets sur un tenant il faut leur donner les droits associé sur la configuration du rôle.

1. Naviguer vers Kibana
2. Connectez-vous comme Administrateur
3. Sélectionnez « Security » dans le menu à gauche
4. Sélectionnez « Roles » puis le rôle a modifier
5. Sélectionnez l’onglet « Tenant Permissions »
6. Dans la section Tenant Permissions clic « Add Tenant Permissions »
7. « Add tenant pattern »
8. Saisie du nom du Tenant a utiliser
9. Dans Permissions clic « Add Field »
10. Sélectionnez « kibana\_all\_read »
11. « Add Field »
12. Sélectionnez « kibana\_all\_write »
13. « Save Role Definition   
    

## Association d’une Role Kibana a une Role IAM

1. Naviguer vers Kibana
2. Connectez-vous comme Administrateur
3. Sélectionnez « Security » dans le menu à gauche
4. Sélectionnez « Role Mappings » puis « Add a new Role Mapping » ()
5. Selectionnez le Role Kibana dans la liste déroulante
6. Clic : Add Backend Role
7. Saisie de l’ARN du rôle IAM à utiliser  
   
8. Submit

## Associer une Role IAM aux role kibana\_users

Chaque nouveau Role IAM doit avoir le droit d’usage sur Kibana.

1. Naviguer vers Kibana
2. Connectez-vous comme Administrateur
3. Sélectionnez « Security » dans le menu à gauche
4. Sélectionnez « Role Mappings » puis « Add a new Role Mapping » ()
5. Selectionnez le kibana\_user dans la liste déroulante
6. Clic : Add Backend Role
7. Saisie l’ARN du rôle IAM à utiliser
8. Submit

## Autoriser un compte Ligne de commande

1. Naviguer vers Kibana
2. Connectez-vous comme Administrateur
3. Sélectionnez « Security » dans le menu à gauche
4. Sélectionnez « Roles » puis « Add a new Role » ()
5. Name : Nom du role
6. Index Permissions -> Add Index Permissions
7. Index Pattern : \*
8. Action groups : Unlimited
9. Save Role Definition
10. Sélectionnez « Security » dans le menu à gauche
11. Sélectionnez « Role Mappings » puis « Add a new Role Mapping » ()
12. Role : Selectionnez le role
13. Users : Saisissez l’ARN de l’utilisateur logstash
14. Submit

# Ajout / Mise à jour d’un template ElasticSearch

1. Naviguer vers Kibana
2. Connectez-vous comme Administrateur
3. Sélectionnez « Dev Tools » dans le menu à gauche
4. Saisie du commande exécuter :  
   PUT /\_template/template\_${NOM\_APPLICATION}\_${ENV}  
   {  
    Body  
   }
5. Exécuter la requête en cliquant sur la flèche ()

# Procédure d’ajout d’une groupe d’utilisateurs

1. Création d’un groupe dans IAM
2. Configuration Groupe Accès Restreint
3. Création d’une Rôle sur Kibana
4. Association d’une Role Kibana a une Role IAM
5. Associer une Role IAM aux role kibana\_users
6. Ajouter un utilisateur dans un groupe Cognito