**DOSSIER D’ADMINISTRATION**

**« COLOG : Consolidation des Logs »**

REDACTION

|  |  |  |  |
| --- | --- | --- | --- |
| **Auteurs** | **Action** | **Version** | **Date** |
| A.DELLACHERIE |  | 1.0 | 17/01/2022 |
|  |  |  |  |

INTERVENANT

|  |  |  |  |
| --- | --- | --- | --- |
| **Approbateur** | **Rôle** | **Signature** | **Date** |
| Rynaud TADJER | Responsable Domaine Production |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

DIFFUSION

|  |  |  |  |
| --- | --- | --- | --- |
| **Destinataire** | **Rôle** | **Pour action** | **Pour info** |
| DOI Delivery Integration | Equipe d’intégration | Rédaction / Utilisation |  |
|  |  |  |  |
|  |  |  |  |

REFERENCE

|  |  |  |  |
| --- | --- | --- | --- |
| **Auteurs** | **Description document** | **Version** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Sommaire**

[1 Presentation et objectifs du dossier 2](#_Toc94792506)

[1.1.1 Architecture de l’application 3](#_Toc94792507)

[2 Les differents fichiers de config a maintenir de l’appli COLOG 3](#_Toc94792508)

[Administration OpenSearch 6](#_Toc94792509)

[Emplacement des Alarmes CloudWatch 6](#_Toc94792510)

[Emplacement des habilitations Cognito/OpenSearch 6](#_Toc94792511)

[Création des comptes Acces a l'environnement 6](#_Toc94792512)

[Affectation des Roles Amazone aux Comptes D'accès 6](#_Toc94792513)

[Emplacement des Tags Pour OpenSearch 6](#_Toc94792514)

[2.1.1 Configuration Logstash AWS 6](#_Toc94792515)

[Configuration des Templates d'index 7](#_Toc94792516)

[Configuration des Pipeline Logstash 7](#_Toc94792517)

[Exemple de Configuration agent filebeat 7](#_Toc94792518)

[Emplacement des Tags Pour Logstash AWS 7](#_Toc94792519)

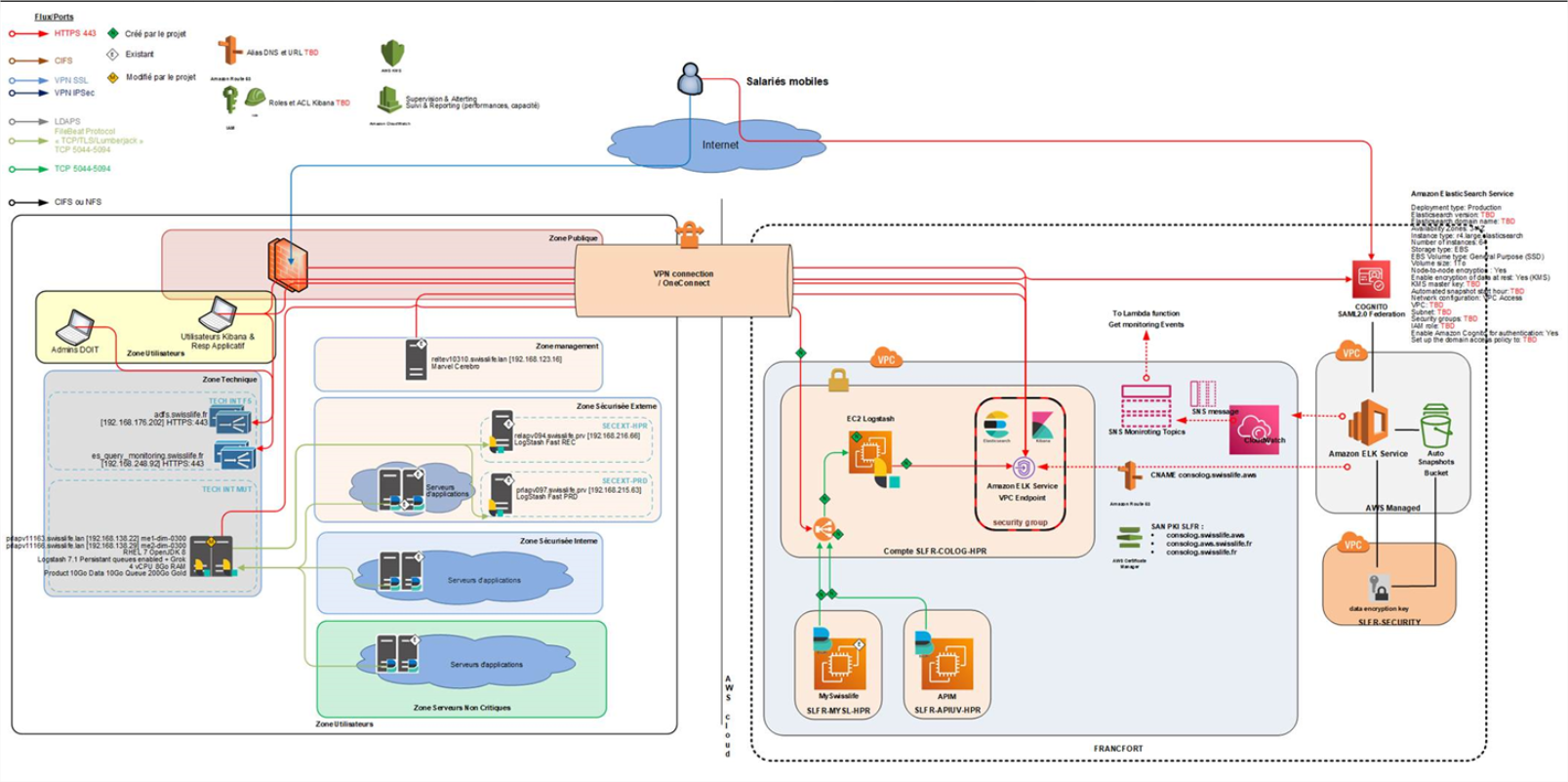
[3 Surveillance 10](#_Toc94792520)

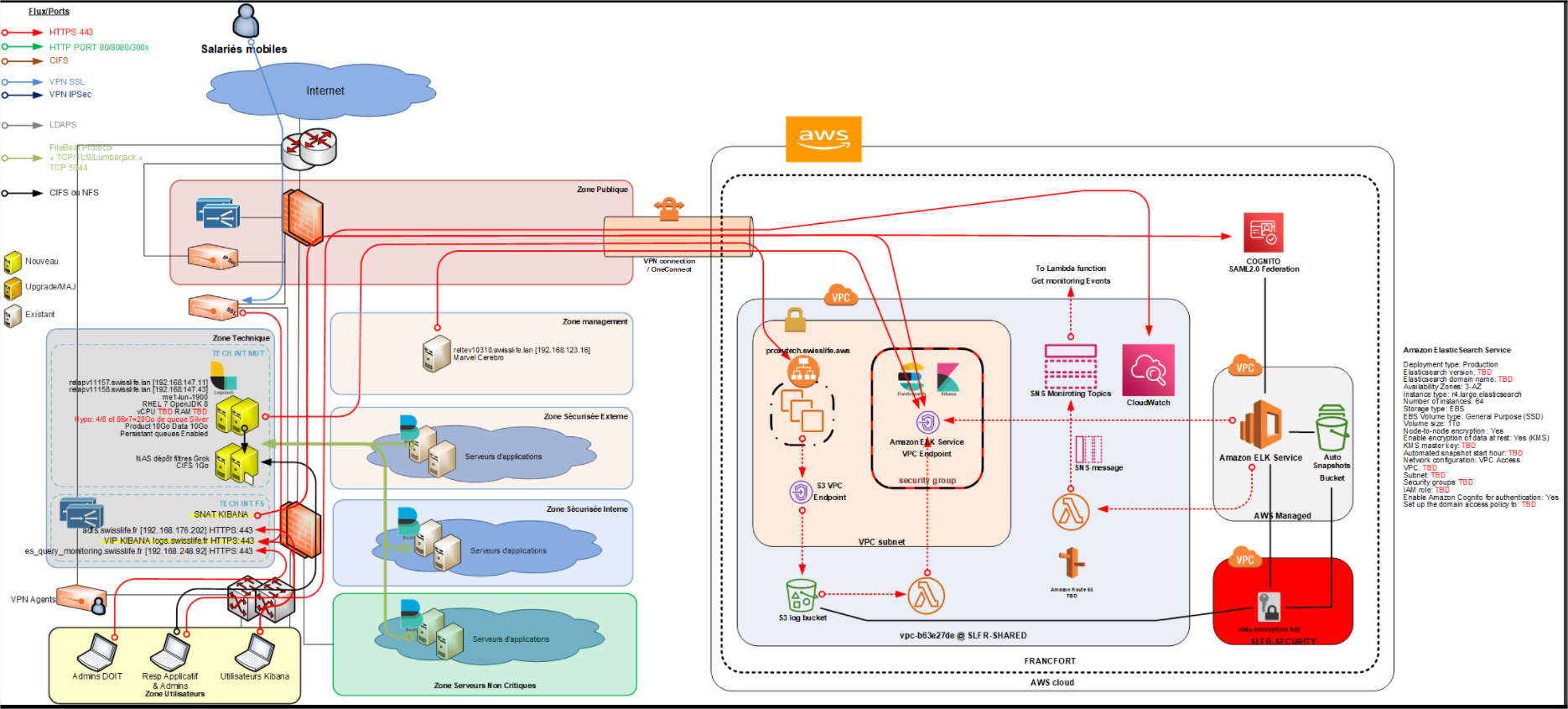
[3.1.1 Cloudwatch 10](#_Toc94792521)

# Presentation et objectifs du dossier

Ce document recense les tâches à dérouler en vue de vérifier le fonctionnement de l’application COLOG dans AWS

## Architecture de l’application





# Les differents fichiers de config a maintenir de l’appli COLOG

Les serveur logstash de production sont : **logstach.colog.swisslife.aws**



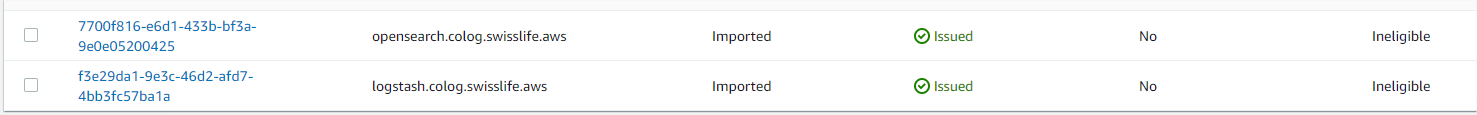
On peut être amener à ajouter de nouveaux ports pour des évolutions et/ou autres outils autres que Logstach, cognito…

Une image contenant texte

Description générée automatiquement

Partie Certificate Manager (ACM)

Mettre à jour ces certificats dans les fichiers de configuration serverless.xml d’Opensearch et Logstach



Cliquer sur chacun des 2 ci-dessus et faire la copie avec le bouton de la console :

Une image contenant texte

Description générée automatiquement

Mettre cette valeur dans le fichier C:\Users\adellacherie\reposhared\lxo01\_consolidationdeslogs\service-opensearch\module-opensearch-cluster\serverless.yml

Une image contenant texte

Description générée automatiquement

Renouveler l’opération pour la partie Logstach :

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

Si ajout de Template dans LogStach, il faudra créer un nouveau fichier de config et lui associé un port

Fb\_apigateway.conf 🡪 Port 5048

Fb\_apimanagement.conf 🡪 Port 5046

Etc….

Une image contenant texte

Description générée automatiquement

Tout ce qui est dans /conf\_files, ces fichiers sont récupérés par les EC2.

* Si on souhaite augmenter ou changer le type d’instance(s), il faut modifier un/des paramètre(s) dans le fichier serveless.yml

Une image contenant texte

Description générée automatiquement

* Version du LogStach : dans le fichier serverless.yml.

Une image contenant texte

Description générée automatiquement

Partie documentation réalisée sous Confluence par le responsable d’application :

## Administration OpenSearch

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/service-opensearch/

### Emplacement des Alarmes CloudWatch

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-opensearch](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch)/[module-opensearch-cluster](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch/module-opensearch-cluster)/[templates](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch/module-opensearch-cluster/templates)/cloudwatch-alarms.yml

### Emplacement des habilitations Cognito/OpenSearch

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-opensearch](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch)/[config](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch/config)/conf.hpr.yml

### Création des comptes Acces a l'environnement

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-opensearch](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch)/[module-opensearch-cluster](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch/module-opensearch-cluster)/[templates](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch/module-opensearch-cluster/templates)/opensearch.yml

* ADFS-Admin
* ADFS-DevOps
* ADFS-RunProd

### Affectation des Roles Amazone aux Comptes D'accès

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-opensearch](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch)/[module-opensearch-cluster](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch/module-opensearch-cluster)/[templates](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch/module-opensearch-cluster/templates)/roles.yml

### Emplacement des Tags Pour OpenSearch

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-opensearch](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch)/[module-opensearch-groups](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch/module-opensearch-groups)/serverless.yml

## Configuration Logstash AWS

### Configuration des Templates d'index

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-logstash](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash)/[conf\_files](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash/conf_files)/[config](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash/conf_files/config)/conf.d/

### Configuration des Pipeline Logstash

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-logstash](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash)/[conf\_files](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash/conf_files)/[config](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash/conf_files/config)/pipelines.yml

### Exemple de Configuration agent filebeat

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-logstash](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash)/exemplefilebeat.yml

### Emplacement des Tags Pour Logstash AWS

[LXO01\_ConsolidationDesLogs](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse)/[service-logstash](https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash)/serverless.yml

Lorsqu’il y a une modification d’un répertoire particulier suivi d’un push sur bitbucket, il y a automatiquement un plan de déploiement qui est lancé.

<https://jenkins-cicd-master-dev.swisslife.aws/>

Onglet :  (autres applications)

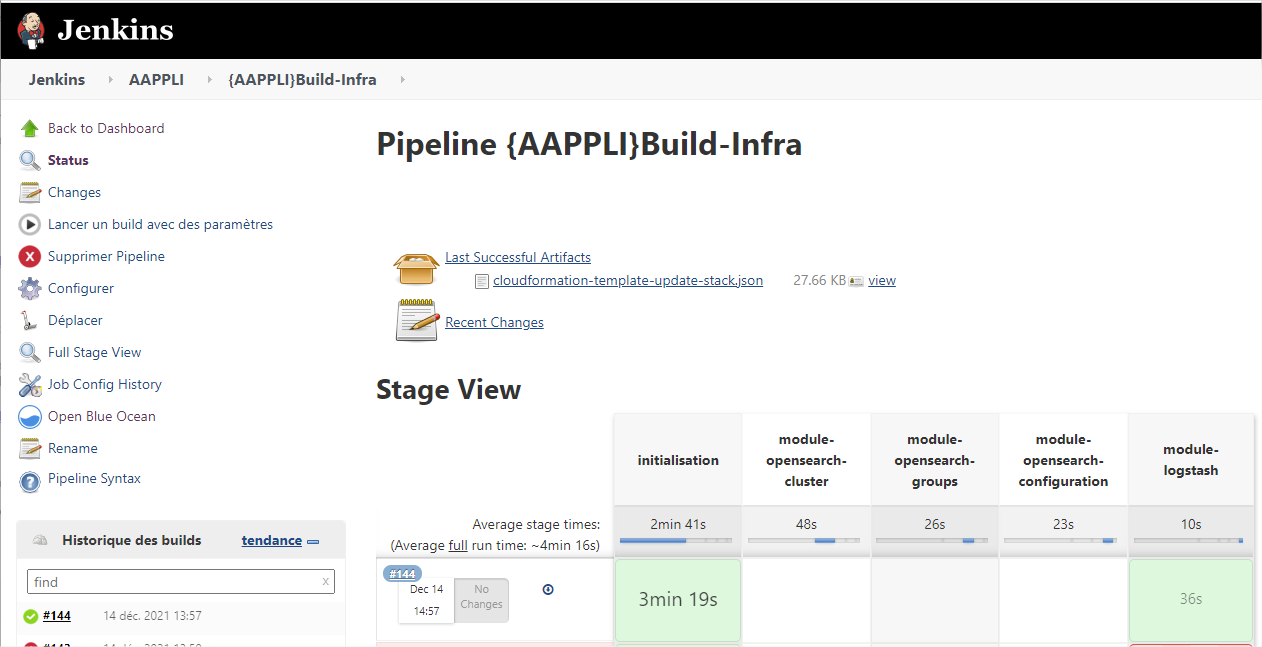


Une image contenant texte

Description générée automatiquement

Puis : On peut voir que selon le répertoire modifié, on met à jour que la partie nécessaire

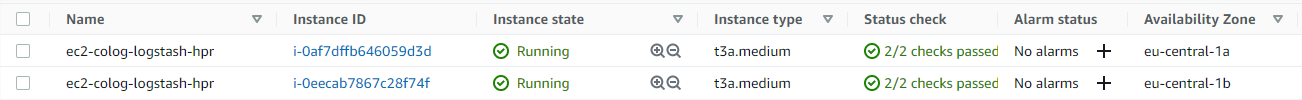
Le script est réalisé avec des boucles où : par contre si on monte l’EC2 on a pas le choix de remettre les habilitations COGNITO.



**Se Connecter à la console AWS**



Si les EC2 sont disponibles se connecter sur celui-ci



Clic sur ***Connect***

Une image contenant texte

Description générée automatiquement

**Et visualiser** **/var/log/awslogs.log ou /var/log/messages**

Faire les tests habituelles sur les service linux : verification des FS, de la mémoire disponible

Si une des 2 instances est arrêtée, faire un start instance

Une image contenant texte

Description générée automatiquement

Configuration de L’Auto Scaling groups

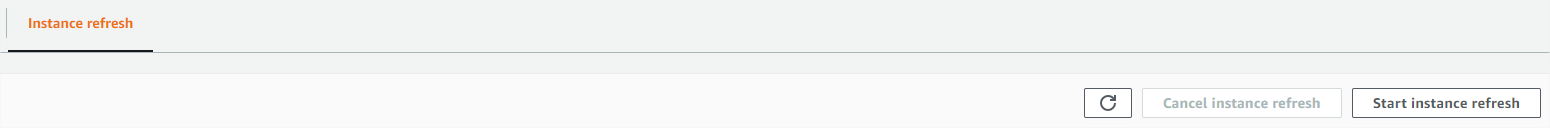
Une image contenant texte

Description générée automatiquement

Puis

Une image contenant texte

Description générée automatiquement



**Affiner le % et le refresh avant la validation cf ci-dessous** :

Une image contenant texte

Description générée automatiquement et valider par Start

Pourcentages à prévoir selon le nombre de machines.

# Surveillance

## Cloudwatch

To do : surveiller la partie LOGSTACH (via API ???) et faire du Scaling en fonction des métriques.

Contrôle et vérification des différentes étapes du build sur AWS :

Une image contenant texte

Description générée automatiquement

**PRINCIPE DE FONCTIONNEMENT DE LA STACK** :

**Si l’un des fichiers du ou des répertoires est modifié(s) et pushé** :

<https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash?at=refs%2Fheads%2Ffeature%2Fcicd>

ou

<https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-logstash?at=refs%2Fheads%2Ffeature%2Fcicd>

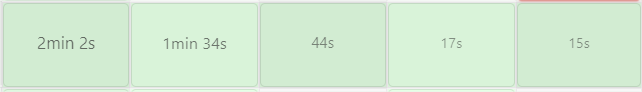
ou

<https://bitbucket.swisslife.fr/projects/AAPPLI/repos/lxo01_consolidationdeslogs/browse/service-opensearch?at=refs%2Fheads%2Ffeature%2Fcicd>

**Alors l’une ou les étapes sont montées** :

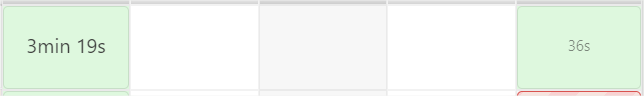
Une image contenant texte

Description générée automatiquement



Ou

Seulement une modification dans le module Logstach



Initialisation :



**Module-opensearch-cluster**

/var/lib/jenkins/workspace/{AAPPLI}Master/featurecicd/node\_modulesvar/lib/jenkins/workspace/{AAPPLI}Master/featurecicd/service-opensearch/module-opensearch-cluster

**module opensearch-groups**

/var/lib/jenkins/workspace/{AAPPLI}Master/featurecicd/service-opensearch/module-opensearch-groups

**module opensearch-configuration**(cognito)

cd service-opensearch/module-opensearch-configuration

**module logstash**

/var/lib/jenkins/workspace/{AAPPLI}Master/featurecicd/service-logstash

# DEPLOIEMENT de L’APPLICATION via Jenkins : COLOG

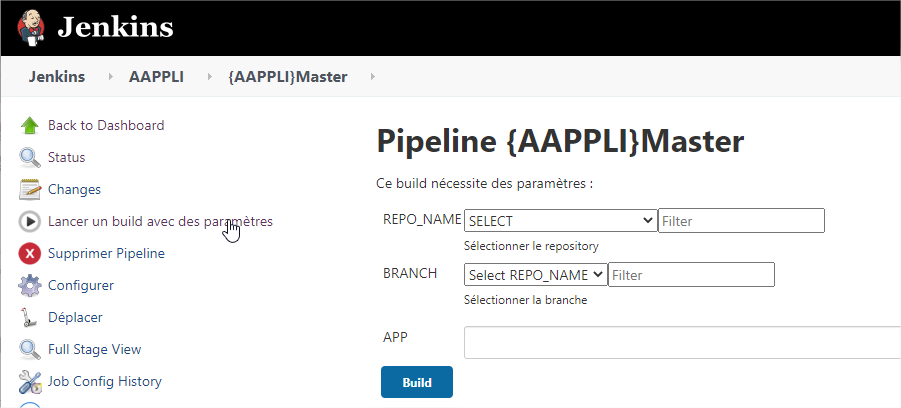
<https://jenkins-cicd-master-dev.swisslife.aws/login?from=%2F>

Nous avons ajouter dans le cadre de ce projet la possibilité de lancer un build avec le paramètre APP dans le but de builder une partie de la Stack ou toute la stack en forçant

Le but étant de pouvoir builder sans avoir à modifier un ou des fichiers faisant partie de la STACK donc de :

* Minimiser les risques d’erreur.
* Limiter de toucher a un ou des fichier(s) de configuration de la stack initiale.





* **module-opensearch-cluster**  : (APP = **ALL** ou **CLUSTER**)
* **module-opensearch-groups** : (APP = **ALL** / **GROUPS** et/ou **CONFIG**)
* **module-opensearch-configuration** : (APP = **ALL** ou **CONFIG**)
* **module-logstash** : (APP= **ALL** ou **LOGSTACH**)

Vous pouvez donc sélectionner une partie que vous souhaitez mettre à jour sachant que l’option APP peut être renseigné une minuscule ou majuscule.

Visualisé son, ses Build(s) : Une image contenant texte

Description générée automatiquement

Une image contenant table

Description générée automatiquement

**On peut voir dans le détail que le build ci-dessus : 179 a monté la partie groups et configuration**

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

