

## TP16 : X-Pack

### ***Installation de X-Pack***

Installer une nouvelle distribution des produits ELK (seulement Elastic et Kibana)

Installer le plugin X-Pack pour ELK, pour kibana

Dans l'arborescence ELK, lancer ***bin/x-pack/setup-password auto*** pour générer des mots de passe pour les utilisateurs elastic, kibana et logstash

Visualiser dans l'interface Kibana les apports du plugin x-pack

### ***Tutorial Machine-Learning***

#### 1. Importation de données exemples :

Récupérer et décompresser *server-metrics.tar.gz*

Vérifier puis utiliser le script *upload\_server-metrics.sh* pour charger les données

Visualiser les données importées via Kibana

#### 2. Création d'un job d'analyse

S'authentifier avec l'utilisateur ***elastic***

Créer un nouveau job dans Kibana s'appuyant sur l'index pattern ***server-metrics-\****

Choisir « Single Metric » puis :

- Aggrégation : Somme
- Champ : Total
- Bucket span : 10mn

Sélectionner une période de temps entre le 23 Mars 2017 et 22 Avril 2017 en utilisant le bouton « *Use full server-metrics data* »

Donner un nom au job

#### 3. Visualiser les résultats

Utiliser les onglets : Job management, Anomaly Explorer, Single Metric Viewer pour visualiser les résultats et en particulier les anomalies.