

Mise en oeuvre d'une plateforme

ElasticSearch - Logstash - Kibana

Date : 23 et 24 novembre 2017

Lieu : salle interactive du bâtiment 40 sur le campus du CNRS à Cronenbourg (23 rue du loess, 67200 Strasbourg)

Voici le programme de la formation "Mise en oeuvre d'une plateforme ELK (ElasticSearch - Logstash - Kibana) pour la centralisation des logs systèmes et réseaux" organisée par le groupe X/Stra avec e soutien financier et logistique du bureau de la formation permanente du CNRS.

Les inscriptions se font auprès du bureau de la formation permanente du CNRS :

<https://www.alsace.cnrs.fr/fpdel/Stage/Fiche/630>

Pour ceux qui n'auraient pas accès au site, vous pouvez utiliser le formulaire en pièce jointe (formats [doc](#) et [pdf](#)).

Fiche programme

Objectifs :

Comprendre le fonctionnement de la suite ELK. Être capable de déployer et opérer une plateforme ELK Être capable d'utiliser les fonctionnalités de la suite ELK

Prérequis :

Bases d'administration d'un système Linux.

Public :

Administrateur systèmes et réseaux.

Programme :

- Introduction
 - Présentation de l'écosystème
 - Historique du projet

- Concepts et composants
- Elasticsearch
 - Déploiement & configuration
 - Gestion des données
 - Recherche
- Logstash
 - Concepts de pipeline
 - Input
 - Filter
 - Output
- Kibana
 - Découverte des données et de l'interface
 - Gestion des requêtes
 - Définition de visualisations
 - Construction de tableaux de bord
- Beats
 - Principe et intérêt
 - Présentation et mise en oeuvre
 - Intégration avec Kibana
- Notions d'architecture
 - Architectures classiques
 - Ingest Node
 - MultiRégion
- Pour aller plus loin
 - Fluentd
 - Graylog
 - Gérer ses archives
 - Mise en place d'alerting
 - XPack, ESHadoop

From:
<https://xstra.unistra.fr/> - **Xstra**

Permanent link:
<https://xstra.unistra.fr/doku.php?id=forma:form-elk&rev=1508740355>

Last update: **2017/10/23 08:32**

