Sparks.

Programme de formation

Elastic Stack (Elasticsearch, Logstash, Kibana et Beats)

Objectifs

Avec cette formation, prenez en main la suite Elastic Stack pour collecter, analyser et visualiser vos données de manière efficace. Couplez Elasticsearch, Logstash, Kibana et le nouveau venu Beats grâce à notre formation, qui vous permettra de maîtriser ces quatre logiciels de façon à produire une analyse de log performante et complète. Formez-vous aux bonnes pratiques et découvrez finalement les différents outils qui viennent étendre Elastic Stack.

Pré requis

Connaissances de base d'un système Unix

Durée

2 jours

Public

Administrateurs, Architectes, Developpeurs

Plan de formation

Introduction - Découvrez la suite Elastic Stack
Ecosystème autour d'Elasticsearch
Elasticsearch, Logstash, Kibana et Beats : rôles et concepts clés
Gérer les versions
Architectures
Principes et fonctionnement
Cas d'utilisation

Elasticsearch - Maîtrisez le moteur d'indexation, de recherche et d'analyse de données
Présentation générale
Installation d' Elasticsearch : serveur, cluster...
Configuration
Plugins
Indexation et recherche
Analyse de données
Mappings et configuration de l'analyse
Requêtes Elasticsearch
Filtres
Agrégations
Réplication et partitionnement

Logstash - Analysez, filtrez et découpez des logs pour les transformer en documents formatés pour Elasticsearch
Concepts fondamentaux : input, output, filtre, codecs...
Inputs : file, redis, rabbitMQ...
Filtres : grok ; date, mutate...
Outputs : file, elasticsearch, redis...
Threading et haute-disponibilité

Kibana - Visualisez les données stockées dans Elasticsearch
Installer et configurer Kibana
Découverte des données et production de requêtes
Agrégations et construction de visualisations
Panels
Créer des vues
Mettre en place un tableau de bord

Beats - Découvrez le nouveau venu de la pile ELK
PacketBeat : moniteur réseau
TopBeat : moniteur des « tops »
FileBeat : moniteur temps-réel des fichiers
WinlogBeat : moniteur temps-réel des eventlog Windows
LibBeat : une bibliothèque de fonctions spécialisée

Monitoring et analyse - Formez-vous aux

bonnes pratiques pour la suite Elastic Stack
Exemples d'utilisation
Supervision système
Supervision JVM/JMX
Log as a Service
Analyse métier, Business Intelligence

Pour aller plus loin - Maîtrisez les fonctionnalités avancées d'Elastic Stack
X-Pack, une extension pour Elastic Stack
Elasticsearch pour Apache Hadoop
Elastic Cloud, ElasticSearch as a Service
Fonctionnalités graphiques avec Graph
Modules avancés pour l'administration : tuning, supervision, sauvegarde, sécurité...