Projet Exploratoire - Semestre 6

Debray Matthieu Desquiens Cyprien Thibeuf Antoine

30 Mars 2017

Plan

Introduction

Objectifs

- Elaboration d'un tableau de bord grâce à la collecte de trace d'activités
- Afin de superviser l'avancement des travaux pratiques

Analyse des besoins

- Un moteur de recherche couplé à une interface d'exploitation des données
- Des outils de collecte et de gestions des fichiers de logs

Gamme Elastic

- Contrainte du sujet mais choix pertinent
- Logiciels libres avec documentation exemplaire
- Quatre choix : Elastic Search, Kibana, Filebeat et Logstash

Déroulement du projet

I

- Mise en place du poste de Monitoring

II

- Installation et configuration Elastic Search & Kibana
- Découverte d'une interface d'administration graphique

III

- Rédaction des scripts et automatisation
- Association d'outils de collecte et de gestion des fichiers de logs

IV

- Elaboration du tableau de bord
- Remarques

Mise en place du poste de Monitoring

Pré-requis

- Système d'exploitation retenu : Debian
- Accès SSH
- Performances en mémoire vive

Java

- Nécessite la dernière version

Serveur Web

- Installation Apache et un navigateur web

Accès distant

- Configuration côté serveur et côté client

Suite Elastic

Procédure d'installation

- Plusieurs formats disponibles
- Installation des divers logiciels similaire et simple
- Un terminal par logiciel
- Choix d'une archive (TAR) dans notre cas

Exemple

- Récupérer le fichier ou dossier au format voulu
- Extraire l'archive (dans notre cas)
- Se rendre dans le dossier contenant le script
- L'executer tel quel

Elastic Search

Prise en main

- Utilisation en tant qu'user
- Rêquetes avec la commande curl sur le port 9200

Notions

- Cluster
- Noeud
- Index
- Documents

Configuration

- Accès publique

Kibana

Configuration

- Association avec Elastic Search
- Accès publique

Notion

- Index Pattern

Elastic Search Head

Complément

- Pas d'interface d'administration de base
- Anciennement plugin
- Ecoute sur le port 9100

Configuration

- Installation d'un serveur à part
- Modification à apporter dans Elastic Search

Récupération des traces

Définition des besoins

- Un script pour une vérification d'une étape
- Résultat envoyés vers des fichiers de logs automatiquement créés
- Syntaxe précise
- Utilisation du dossier partagé entre l'hôte et la machine virtuelle

Rédaction des scripts

- Langage bash
- Utilisation de structures conditionnelles et de variables

Automatisation

- Service cron
- Choix des intervalles

Association de Filebeat et Logstash

Principe

- Un outil installé sur chaque poste pour collecter les fichiers
- Les envoyer à un autre outil qui se charge de les transformer pour les envoyer au moteur de recherche

Configuration

- Paramètres Input & Output
- Debug en live

Déploiement

- Tests réussis sur plusieurs postes en 4A10

Gestion côté serveur

Configuration

- Vérification dans le moteur de recherche
- Définition de l'Index Pattern

Construction du tableau de bord

- Recherche dans Kibana
- Affiné avec divers champs
- Problèmes de tri avec les colonnes de type texte

Remarques

Problèmes

- Alteration de l'objectif initial
- Fonctionnalités de Kibana restreintes

Améliorations

- Gestion du temps
- Mapping dans le moteur de recherche

Conclusion

Résultat final

- Base sur laquelle Mr Peter pourra se pencher

Futur du projet

- Gamme Elastic riche et variée (Heartbeat, X-Pack)

Apport Personnel

- Technologies intéressantes
- Confiance en la documentation

Remerciements

- Mr Peter
- Mr Beaufils
- Legrand Florian et Zohari Fatemeh