Elastic Beats

Nirah-Technology

Introduction

- **Définition** : Elastic Beats sont des agents légers qui envoient des données vers Elasticsearch ou Logstash.

- **But principal** : Collecter, expédier et surveiller les données de vos systèmes en temps réel.

- **Comparaison avec Logstash** :
    - **Logstash** : Traitement de données avec enrichissement complexe, transformations.
    - **Beats** : Collecte légère, souvent utilisée pour envoyer des données brutes à Elasticsearch ou Logstash.

Cas d'utilisation

- **Logs :** Collecte des logs système et application.
- **Réseaux :** Collecte de données réseau et de paquets (**packetbeat**).
- **Metrics :** Collecte des métriques de performance (**metricsbeat**).
- **Audit de sécurité :** Collecte d’informations de sécurité (**filebeat**).
- **Surveillance des containers et Kubernetes :** Collecte des logs et des métriques de containers (**dockerbeat**, **kubernetesbeat**).

Types de Beats

Elastic Beats sont des agents légers qui se concentrent sur des cas d'utilisation spécifiques :

- **Filebeat** : Collecte de fichiers journaux (**logs**).
- **Metricbeat** : Collecte des métriques système et d’application.
- **Packetbeat** : Collecte des données réseau.
- **Heartbeat** : Surveillance des services pour vérifier leur disponibilité.
- **Auditbeat** : Collecte d’événements de sécurité.
- **Winlogbeat** : Collecte des logs d’événements Windows

Architecture

- **Collecte des données** : Chaque Beat est un agent léger qui collecte des données spécifiques.
- **Transmission vers Elasticsearch ou Logstash** : Les Beats envoient les données collectées vers Elasticsearch pour l'indexation ou vers Logstash pour un traitement supplémentaire.
- **Visualisation** : Utilisation de Kibana pour visualiser les données collectées par les Beats

Configuration

- **Fichier de configuration** : Chaque Beat a un fichier de configuration principal (filebeat.yml, metricbeat.yml, etc.).

- **Paramètres essentiels** :
  - **output** : Définir Elasticsearch ou Logstash comme destination des données collectées.
  - **logging** : Configurer les journaux internes de Beats.
  - **modules** : Activer des modules préconfigurés pour une collecte spécifique (par exemple, les logs Nginx avec Filebeat).

Filebeat - Collecte des Logs

- **Description** : Filebeat est utilisé pour collecter des logs de fichiers et les envoyer vers Elasticsearch ou Logstash.
- **Cas d'utilisation** : Logs d'application, logs système, logs Apache, Nginx, etc.

Metricbeat - Collecte des Métriques

- **Description** : Metricbeat collecte des métriques système et des services d’application.
- **Cas d'utilisation** : Surveillance des serveurs, bases de données, containers Docker, etc.

Packetbeat - Analyse du Réseau

- **Description** : Packetbeat capture et analyse les paquets réseau pour fournir des informations sur les transactions réseau.

- **Cas d'utilisation** : Surveillance du trafic réseau, détection d'anomalies, analyse de latence.

Heartbeat - Surveillance de la Disponibilité des Services

- **Description** : Heartbeat envoie des pings vers des services afin de vérifier leur disponibilité.
- **Cas d'utilisation** : Surveillance de la disponibilité des serveurs, services web, applications.

Auditbeat - Collecte des Événements de Sécurité

- **Description** : Auditbeat collecte des événements de sécurité du système d'exploitation (audit de l'activité des utilisateurs, changements de fichiers).

- **Cas d'utilisation** : Surveillance de la sécurité des systèmes.

Winlogbeat - Collecte des Logs Windows

- **Description** : Winlogbeat collecte les logs d'événements Windows (sécurité, application, système).
- **Cas d'utilisation** : Surveillance des serveurs Windows, sécurité.