MISSION 2 - Mise en place d'une plateforme ELK sécurisée

SIO2 - BLOC 2 SISR

PETKOVIC Téo
SIO2

Compte rendu de mission — Mise en place d’une plateforme ELK sécurisée

Infrastructure GSB72

Sommaire

1. Contexte de la mission

La mission consiste à mettre en place une plateforme centralisée de collecte et d'analyse des journaux sur l'infrastructure GSB72 à l'aide de la stack ELK.

L'infrastructure est composée de plusieurs firewalls OPNsense, de serveurs Linux, de services internes et de services exposés. Avant la mise en place d'ELK, les journaux étaient consultés directement sur chaque équipement, ce qui compliquait la recherche d'incidents et la supervision globale.

La plateforme ELK permet de regrouper les journaux dans un point central afin de les analyser depuis Kibana.

Équipements concernés par la mission :

- 8 pare-feu OPNsense ;
- serveurs Linux ;
- serveurs de supervision ;
- serveurs applicatifs ;
- futurs serveurs Windows.

2. Objectif de la mise en place ELK

L'objectif principal est de centraliser les journaux de l'infrastructure afin de faciliter l'exploitation et le diagnostic.

Sans centralisation, chaque équipement conserve ses journaux localement. En cas d'incident, l'administrateur doit donc se connecter sur plusieurs machines pour retrouver les événements importants.

Avec ELK, les journaux sont envoyés vers Logstash, stockés dans Elasticsearch et consultables depuis Kibana.

Objectifs de la mission :

- centraliser les journaux OPNsense ;
- centraliser les journaux Linux ;
- préparer l'intégration des serveurs Windows ;
- séparer les sources de données dans des index distincts ;
- faciliter les recherches dans Kibana ;
- préparer la création de tableaux de bord et d'alertes.

Exemple de fonctionnement attendu :

```
Pare-feu OPNsense  -> Logstash -> Elasticsearch -> Kibana
Serveurs Linux     -> Logstash -> Elasticsearch -> Kibana
Serveurs Windows   -> Agent    -> Elasticsearch -> Kibana
```

3. Principe de fonctionnement de la stack ELK

ELK est composé de trois éléments principaux : Elasticsearch, Logstash et Kibana.

Composant	Rôle
Elasticsearch	Stocke, indexe et permet la recherche dans les journaux.

Logstash	Reçoit les journaux, les traite et les envoie vers Elasticsearch.
Kibana	Permet de visualiser les journaux et de créer des dashboards.

Le principe est le suivant :

```
Equipement source
     ↓
Logstash
     ↓
Elasticsearch
     ↓
Kibana
```

Dans cette mission, Logstash est utilisé comme point d'entrée des journaux pour les pare-feu OPNsense et les serveurs Linux. Les sources sont séparées par ports et par pipelines afin d'éviter le mélange des événements.

4. Pré-requis pour la plateforme ELK

Pour que la plateforme fonctionne correctement, plusieurs pré-requis doivent être respectés :

- le serveur ELK doit être joignable depuis les équipements sources ;
- les règles firewall doivent autoriser les flux de journalisation ;
- les pare-feu doivent envoyer leurs journaux vers Logstash ;
- rsyslog doit être actif sur les serveurs Linux ;
- Elasticsearch, Logstash et Kibana doivent être démarrés ;
- les index doivent être créés automatiquement dans Elasticsearch.

Le serveur ELK utilisé pour la mission possède l'adresse suivante :

Équipement	Adresse IP	Rôle
Serveur ELK	172.20.3.50	Réception, stockage et visualisation des journaux
Kibana	172.20.3.50:5601	Interface web d'administration et d'analyse
Logstash OPNsense	172.20.3.50:5514	Réception des journaux pare-feu
Logstash Linux	172.20.3.50:5515	Réception des journaux Linux

5. Table d'adressage ELK et équipements concernés

Les équipements importants pour la centralisation des journaux sont les suivants :

Nom	Adresse IP	Rôle
ELK_SERVER_IP	172.20.3.50	Serveur ELK
DEBIAN_ADMIN	172.20.2.100	Machine d'administration
ZABBIX_SERVER	172.20.3.60	Serveur Zabbix
WAZUH_SERVER_IP	172.20.3.100	Serveur Wazuh
PF-Admin	172.20.3.253 / 172.20.2.253 / autres interfaces	Firewall d'administration
PF-Externe	172.19.4.253 / 172.20.1.240	Firewall externe
PF-Intermédiaire	172.19.2.253 / 172.19.3.250 / 172.20.1.242	Firewall intermédiaire
PF-Interne	172.19.1.249 / 172.20.1.244 / VLAN	Firewall interne

	utilisateurs et serveurs	

Les alias utilisés dans OPNsense permettent de simplifier les règles firewall. Les alias principaux liés à ELK sont :

Alias	Contenu	Utilisation
ELK_SERVER_IP	172.20.3.50	Destination des journaux et accès Kibana
KIBANA_PORT	5601	Accès interface Kibana
SYSLOG_PORT	5514, 5515	Ports Logstash pour OPNsense et Linux
DEBIAN_ADMIN	172.20.2.100	Poste autorisé à accéder à Kibana
ZABBIX_SERVER	172.20.3.60	Serveur de supervision
WAZUH_SERVER_IP	172.20.3.100	Serveur Wazuh

6. Architecture de collecte des journaux

L'architecture retenue repose sur deux flux principaux : un flux pour les pare-feu OPNsense et un flux pour les serveurs Linux.

```
OPNsense x8
    ↓ UDP/5514
Logstash pipeline opnsense
    ↓
Index opnsense-YYYY.MM.dd

Serveurs Linux
    ↓ UDP/5515
Logstash pipeline linux
    ↓
Index linux-YYYY.MM.dd
```

Cette séparation permet d'avoir une meilleure lisibilité dans Kibana. Les journaux des pare-feu ne sont pas mélangés avec les journaux des serveurs Linux.

7. Configuration des pipelines Logstash

Logstash utilise plusieurs pipelines afin de traiter séparément les différentes sources de journaux.

Pipeline	Port	Protocole	Source	Index Elasticsearch
opnsense	5514	UDP/TCP	Pare-feu OPNsense	opnsense-YYYY.MM.dd
linux	5515	UDP/TCP	Serveurs Linux	linux-YYYY.MM.dd
windows	prévu	Agent / Beats	Serveurs Windows	windows-YYYY.MM.dd

Le fichier pipelines.yml permet de séparer les pipelines :

```
- pipeline.id: opnsense
  path.config: "/usr/share/logstash/pipeline/opnsense.conf"

- pipeline.id: linux
  path.config: "/usr/share/logstash/pipeline/linux.conf"
```

Grâce à cette séparation, chaque source utilise son propre port et son propre index.

8. Configuration des pare-feu OPNsense

Les pare-feu OPNsense sont configurés pour envoyer leurs journaux au serveur ELK.

Chemin de configuration dans OPNsense :

```
System > Settings > Logging > Targets
```

Paramètres appliqués :

Paramètre	Valeur
Transport	UDP IPv4
Destination	172.20.3.50
Port	5514
Type de journaux	filterlog, system
Destination Logstash	pipeline opnsense

Les huit pare-feu OPNsense envoient donc leurs journaux vers Logstash sur le port 5514.

Le champ host.hostname permet ensuite de distinguer les différents pare-feu dans Kibana.

9. Configuration des serveurs Linux

Les serveurs Linux sont configurés avec rsyslog afin d'envoyer leurs journaux vers Logstash.

Fichier de configuration :

```
/etc/rsyslog.d/90-elk.conf
```

Contenu du fichier :

```
*.* @172.20.3.50:5515
```

Après modification, le service rsyslog doit être redémarré :

```
sudo systemctl restart rsyslog
```

Un test peut être réalisé avec la commande suivante :

```
logger "TEST_LINUX_TO_ELK"
```

Les journaux Linux sont reçus par Logstash sur le port 5515 puis stockés dans l'index linux-YYYY.MM.dd.

10. Configuration des serveurs Windows

Les serveurs Windows peuvent être intégrés à la plateforme ELK à l'aide d'un agent adapté, comme Elastic Agent ou Winlogbeat.

L'objectif est de récupérer les journaux de sécurité Windows, les connexions utilisateurs, les erreurs système et les événements liés à Active Directory.

Source Windows	Collecteur	Index prévu
Contrôleur de domaine	Elastic Agent ou Winlogbeat	windows-YYYY.MM.dd
Serveurs applicatifs Windows	Elastic Agent ou Winlogbeat	windows-YYYY.MM.dd
Journaux sécurité	Event Logs Windows	windows-YYYY.MM.dd

Cette intégration permet de compléter la supervision en ajoutant les événements Windows aux journaux déjà collectés depuis OPNsense et Linux.

11. Règles firewall nécessaires pour ELK

Les règles firewall sont nécessaires pour autoriser uniquement les flux utiles à la plateforme ELK. Les règles principales se trouvent sur PF-Admin, car le serveur ELK se situe dans le réseau de supervision 172.20.3.0/24.

11.1 Règles générales nécessaires

Flux	Source	Destination	Port	Protocole	Rôle
Accès Kibana	DEBIAN_ADMIN	ELK_SERVER_IP	5601	TCP	Administration de Kibana
Journaux OPNsense	Pare-feu OPNsense	ELK_SERVER_IP	5514	UDP/TCP	Envoi des logs firewall vers Logstash
Journaux Linux	Serveurs Linux	ELK_SERVER_IP	5515	UDP/TCP	Envoi des logs Linux vers Logstash
DNS sortant ELK	ELK_SERVER_IP	DNS_LIST	53	TCP/UDP	Résolution DNS du serveur ELK
Web sortant ELK	ELK_SERVER_IP	Any	80/443	TCP/UDP	Mises à jour et accès web
NTP	ELK_SERVER_IP	Firewall NTP relay	123	UDP	Synchronisation horaire

11.2 Règles configurées sur PF-Admin

Description de la règle	Interface	Source	Destination	Port	Protocole	Rôle
Allow DEBIAN_ADMIN access to KIBANA WEB	LAN	DEBIAN_ADMIN	ELK_SERVER_IP	KIBANA_PORT (5601)	TCP	Autorise l'administration de Kibana depuis le poste d'administration
Allow ELK_SERVER LOGSTACH	OPT2, OPT3, OPT4, WAN	Any	ELK_SERVER_IP	SYSLOG_PORT (5514, 5515)	TCP/UDP	Autorise la remontée des logs OPNsense et Linux vers Logstash
Allow WAZUH/ZABBIX/ELK/DEBIAN-ADMIN Access NTP relay	LAN, OPT1	DEBIAN_ADMIN, ELK_SERVER_IP, WAZUH_SERVER_IP, ZABBIX_SERVER	This firewall	123	UDP	Autorise la synchronisation horaire
Allow access to HTTP/HTTPS for ZABBIX_SERVER/WAZUH/ELK	OPT1	ELK_SERVER_IP, WAZUH_SERVER_IP, ZABBIX_SERVER	Any	WEB_PORTS (80, 443)	TCP/UDP	Autorise les accès web sortants nécessaires
Allow access to DNS for ZABBIX_SERVER/WAZUH/ELK	OPT1	ELK_SERVER_IP, WAZUH_SERVER_IP, ZABBIX_SERVER	DNS_LIST	53	TCP/UDP	Autorise la résolution DNS

11.3 Logique des règles firewall

La règle Allow ELK_SERVER LOGSTACH autorise les réseaux situés derrière PF-Admin à envoyer leurs journaux vers le serveur ELK. Cette règle utilise l'alias SYSLOG_PORT qui contient les ports 5514 et 5515.

Le poste d'administration n'a pas besoin d'accéder directement à Elasticsearch. L'administration quotidienne se fait via Kibana sur le port 5601.

Elasticsearch reste accessible uniquement par les conteneurs internes de la stack ELK, ce qui réduit l'exposition réseau.

12. Organisation des index Elasticsearch

Les index Elasticsearch sont organisés par type de source et par date.

Source	Index	Exemple
OPNsense	opnsense-YYYY.MM.dd	opnsense-2026.05.21
Linux	linux-YYYY.MM.dd	linux-2026.05.21
Windows	windows-YYYY.MM.dd	windows-2026.05.21

Cette organisation permet une rotation naturelle des journaux et facilite les recherches par période.

Dans Kibana, les Data Views utilisées sont :

- opnsense-* pour les pare-feu ;
- linux-* pour les serveurs Linux ;
- windows-* pour les serveurs Windows.

13. Logique d'exploitation dans Kibana

Kibana permet d'exploiter les journaux stockés dans Elasticsearch.

Les administrateurs peuvent utiliser Discover pour rechercher les événements et les dashboards pour visualiser l'état général de l'infrastructure.

Champs utiles pour l'analyse :

Champ	Utilisation
@timestamp	Date et heure de l'événement
host.hostname	Nom de l'équipement source
host.ip	Adresse IP source
event.module	Type de source : opnsense, linux, windows
message	Message principal du journal
event.original	Message syslog brut

Exemples de filtres Kibana :

```
host.hostname : "zabbix"
event.module : "opnsense"
message : *TEST*
host.hostname : "pf-admin.gsb72.local"
```

14. Vérifications à effectuer

Après la configuration, plusieurs vérifications sont nécessaires.

14.1 Vérifier les index Elasticsearch

```
curl -k -u elastic:'motdepasse' https://localhost:9200/_cat/indices?v
```

Les index attendus sont :

- opnsense-YYYY.MM.dd ;
- linux-YYYY.MM.dd ;
- windows-YYYY.MM.dd lorsque Windows sera intégré.

14.2 Vérifier les pipelines Logstash

```
docker logs elk-logstash --tail 100
```

Les pipelines attendus sont :

- pipeline.id = opnsense ;
- pipeline.id = linux.

14.3 Vérifier un envoi Linux

```
logger "TEST_LINUX_TO_ELK"
```

Le message doit apparaître dans Kibana dans la Data View linux-*.

14.4 Vérifier un envoi OPNsense

Depuis un pare-feu OPNsense, il suffit de générer une activité réseau ou d'appliquer une règle afin de produire un événement filterlog.

Le message doit apparaître dans Kibana dans la Data View opnsense-*.

14.5 Vérifier l'état Elasticsearch

```
curl -k -u elastic:'motdepasse' https://localhost:9200/_cluster/health?pretty
```

L'état attendu est green ou yellow. L'état yellow est acceptable dans un environnement mono-nœud Elasticsearch, car les réplicas ne peuvent pas être placés sur un second nœud.

15. Résultat attendu

Après la mise en place de la plateforme ELK, le résultat attendu est le suivant :

- les 8 pare-feu OPNsense envoient leurs journaux vers Logstash ;
- les serveurs Linux envoient leurs journaux via rsyslog ;
- les journaux OPNsense sont stockés dans opnsense-* ;
- les journaux Linux sont stockés dans linux-* ;
- Kibana permet de rechercher les événements ;
- les règles firewall limitent les accès aux flux nécessaires ;
- la plateforme est prête pour l'intégration des serveurs Windows.

La mission est validée lorsque les événements apparaissent correctement dans Kibana et que les sources sont séparées par index.

16. Conclusion

La mise en place de la plateforme ELK permet d'apporter une centralisation des journaux à l'infrastructure GSB72.

Les pare-feu OPNsense, les serveurs Linux et les futurs serveurs Windows peuvent être supervisés depuis une interface unique. Les pipelines Logstash permettent de séparer proprement les flux afin de faciliter les recherches et les analyses.

Les règles firewall mises en place permettent de limiter les communications aux flux nécessaires : accès Kibana depuis le poste d'administration, remontée des journaux vers Logstash, accès DNS/Web/NTP nécessaires au fonctionnement du serveur ELK.

La plateforme constitue donc une base solide pour la supervision, l'analyse d'incidents et l'ajout futur de dashboards et d'alertes.

La mission ELK est validée lorsque :

- les sources de journaux sont configurées ;
- les flux firewall sont autorisés ;
- les index sont créés automatiquement ;
- les événements sont visibles dans Kibana ;
- les sources sont séparées par type d'équipement.