COMPTE RENDU

Zabbix, Syslog et pfELK

Par Alexandre BEROT-ARMAND

BTS SIO 2

Lycée Louis PERGAUD

TABLE DES MATIERES

INTRODUCTION

Ce compte rendu est rédigé après la réalisation de 3 missions différentes avec comme but de mettre en place un serveur de supervision Zabbix ainsi qu'un serveur Syslog et un serveur ELK pour réunir, traiter et visualiser les différents logs générés par les machines du système.

Les différentes missions ne seront pas présentées en détails. Seuls les objectifs et les preuves de réalisation seront exposés.

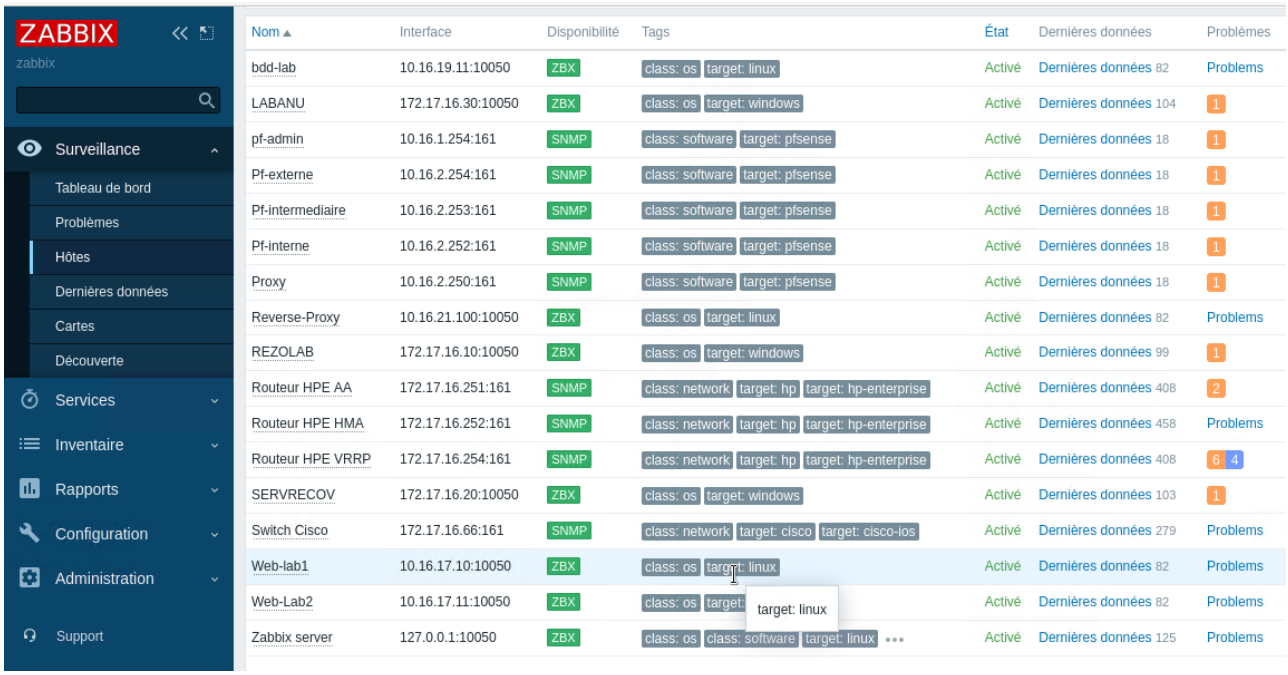
SERVEUR ZABBIX

L'objectif de la mission Zabbix est d'installer la solution de monitoring Zabbix et de superviser toutes les machines du système en dehors des machines clients donc :

- Les serveurs LABANU, REZOLAB et ServRecov,
- Les deux serveurs Web et le serveur de base de données,
- Le reverse proxy, le proxy et le serveur Zabbix,
- Les deux routeurs HPE (et le VRRP),
- Le switch Cisco,
- Les 4 pfSense.

Pour cela, il a fallu configurer des règles sécurisées dans les pare-feux pour autoriser les flux des clients et du serveur Zabbix. Puis j'ai installé et configuré les clients Zabbix sur les machines Windows et Linux, activé le SNMP dans les pare-feux ainsi que dans les deux HPE et le Cisco.

Finalement, le serveur mis en place est fonctionnel et nous avons un monitoring des machines du SI accessible depuis la Debian Admin :



Note : Les problèmes remontés ne sont que des faux positifs.

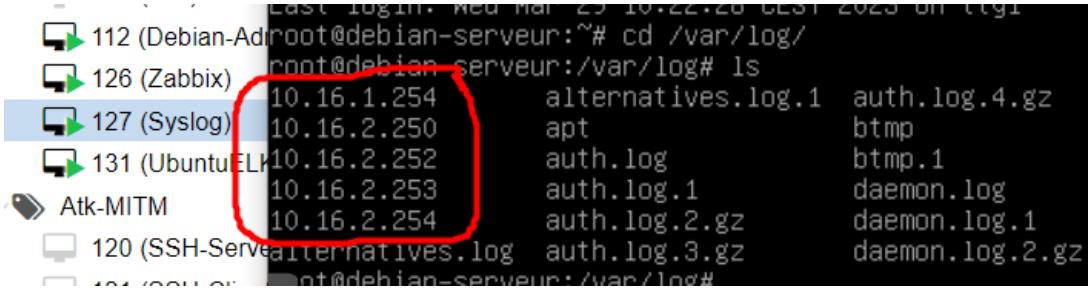
SERVEURS SYSLOG ET ELK

L'objectif de cette mission est la mise en place d'un serveur de collecteur de log ainsi que d'une solution d'analyse de log (ELK dans ce cas de figure).

Serveur SYSLOG

Le but d'un serveur de collecteur de log est la centralisation des journaux d'évènements des machines du système sur la même machine. Cette centralisation simplifie grandement l'utilisation et la conservation des logs.
Nous avons limité la remontée sur le serveur SYSLOG aux logs des pare-feux par manque de temps mais il aurait fallu remonter les logs des serveurs aussi.

Preuve :



On peut voir que la remontée des logs se fait.

Serveur ELK

Le serveur ELK est un serveur avec la suite logiciel ELK (ElasticSearch, Logstash et Kibana) qui permet de recevoir, analyser et virtualiser les données des logs pour permettre un traitement et une lecture plus claire des logs.

Preuve :

May 3, 2023	event.dataset	Message
08:41:02.423	pfelk.firewall	[pfelk.firewall] <134>May 3 06:41:03 filterlog[9187]: 4,,,1000000103,vtnet0,match,block,in,4,0x0,,64,42173,0,none,17,udp,166,10.16.2.252,10.16.2.1,514,5140,146
08:41:02.423	pfelk.firewall	[pfelk.firewall] <134>May 3 06:41:03 filterlog[9187]: 4,,,1000000103,vtnet0,match,block,in,4,0x0,,64,3503,0,none,17,udp,180,10.16.2.252,10.16.2.1,514,5140,160
08:41:02.424	pfelk.firewall	[pfelk.firewall] <134>May 3 06:41:03 filterlog[9187]: 4,,,1000000103,vtnet0,match,block,in,4,0x0,,64,36497,0,none,1,icmp,29,10.16.2.254,10.16.2.1,request,21082,120469

On peut ainsi voir qu'il y a une remontée de logs sur ELK ainsi qu'un traitement.