



Lycée Louis PERGAUD

TABLE DES MATIERES

Introduction	3
Serveur zabbix	4
Serveurs Syslog et ELk	5

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.

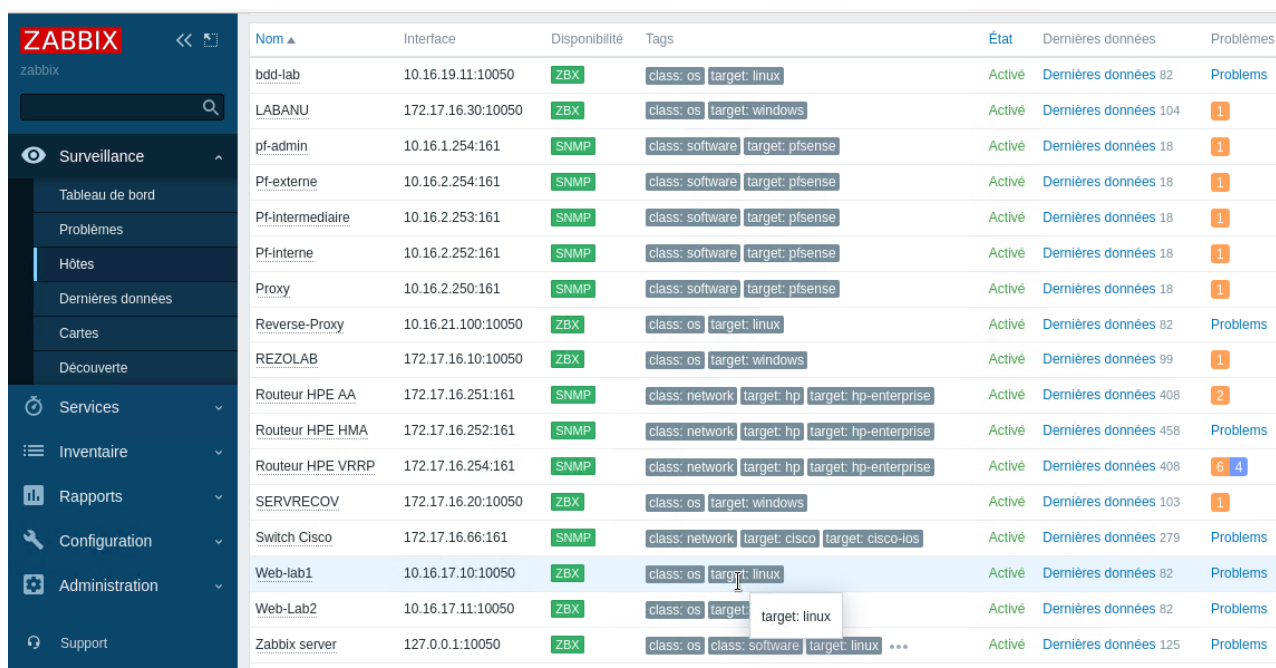
SERVEUR ZABBIX

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 :



Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes
bdd-lab	10.16.19.11:10050	ZBX	class: os target: linux	Activé	Dernières données 82	Problèmes
LABANU	172.17.16.30:10050	ZBX	class: os target: windows	Activé	Dernières données 104	1
pf-admin	10.16.1.254:161	SNMP	class: software target: pfsense	Activé	Dernières données 18	1
Pf-externe	10.16.2.254:161	SNMP	class: software target: pfsense	Activé	Dernières données 18	1
Pf-intermediaire	10.16.2.253:161	SNMP	class: software target: pfsense	Activé	Dernières données 18	1
Pf-interne	10.16.2.252:161	SNMP	class: software target: pfsense	Activé	Dernières données 18	1
Proxy	10.16.2.250:161	SNMP	class: software target: pfsense	Activé	Dernières données 18	1
Reverse-Proxy	10.16.21.100:10050	ZBX	class: os target: linux	Activé	Dernières données 82	Problèmes
REZOLAB	172.17.16.10:10050	ZBX	class: os target: windows	Activé	Dernières données 99	1
Routeur HPE AA	172.17.16.251:161	SNMP	class: network target: hp target: hp-enterprise	Activé	Dernières données 408	2
Routeur HPE HMA	172.17.16.252:161	SNMP	class: network target: hp target: hp-enterprise	Activé	Dernières données 458	Problèmes
Routeur HPE VRRP	172.17.16.254:161	SNMP	class: network target: hp target: hp-enterprise	Activé	Dernières données 408	6 4
SERVRECOV	172.17.16.20:10050	ZBX	class: os target: windows	Activé	Dernières données 103	1
Switch Cisco	172.17.16.66:161	SNMP	class: network target: cisco target: cisco-ios	Activé	Dernières données 279	Problèmes
Web-lab1	10.16.17.10:10050	ZBX	class: os target: linux	Activé	Dernières données 82	Problèmes
Web-Lab2	10.16.17.11:10050	ZBX	class: os target: linux	Activé	Dernières données 82	Problèmes
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Activé	Dernières données 125	Problèmes

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

SERVEURS SYSLOG ET ELK

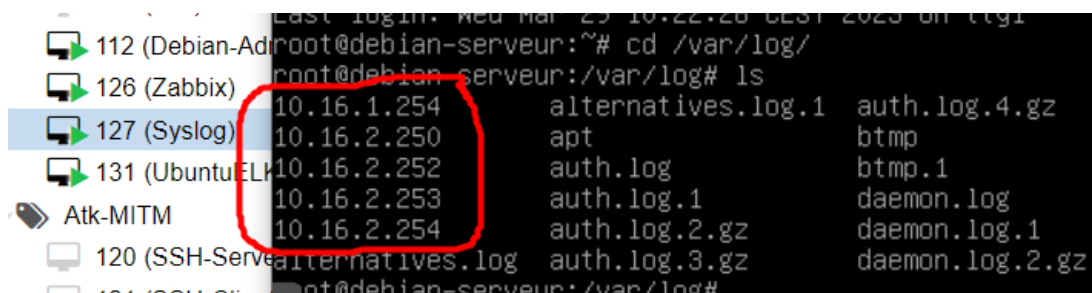
L'objectif de cette mission est la mise en place d'un serveur de collecteur de log ainsi que d'une solution d'analyse de log (ELK dans ce cas de figure).

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,,100000 0103,vtnet0,match,block,in,4,0x0,,64,42173,0,none,17,udp,166,10.1 6.2.252,10.16.2.1,514,5140,146
08:41:02.423	pfelk.firewall	[pfelk.firewall] <134>May 3 06:41:03 filterlog[9187]: 4,,100000 0103,vtnet0,match,block,in,4,0x0,,64,3503,0,none,17,udp,180,10.1 6.2.252,10.16.2.1,514,5140,160
08:41:02.424	pfelk.firewall	[pfelk.firewall] <134>May 3 06:41:03 filterlog[9187]: 4,,100000 0103,vtnet0,match,block,in,4,0x0,,64,36497,0,none,1,icmp,29,10.1 6.2.254,10.16.2.1,request,21082,120469

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