PROMÉO
BEAUVAIS

PPE-2

TRAÇABILITÉ ET SUPERVISION DE LA SANTÉ ET DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

Pauline JIMENEZ
BTS SIO 26

pauline.jimenez.etude@gmail.com

https://pjimenez.promeo-capnumerique.fr/?page_id=177

SOMMAIRE :

Situation initiale

L’entreprise JIM n’a pas réussi à tenir à jour son système de supervision. Elle ne reçoit plus les alertes concernant ses VM mais aussi de ses équipements réseaux.

L’entreprise souhaiterait à la suite de cet évènement avoir des informations plus précises concernant la santé, la traçabilité et la sécurité de chacun de ses équipements pour pallier les attaques et aux incidents qu’elle pourrait connaître.

Problématique

La problématique est donc la suivante :

Comment déployer une supervision et une traçabilité adaptées à l’entreprise JIM ?

L’objectif :

Moderniser la supervision des équipements réseaux et des serveurs avec un système d’alerte par mail

Installer un serveur pour la traçabilité du système d’information en ayant une vue quotidienne des logs

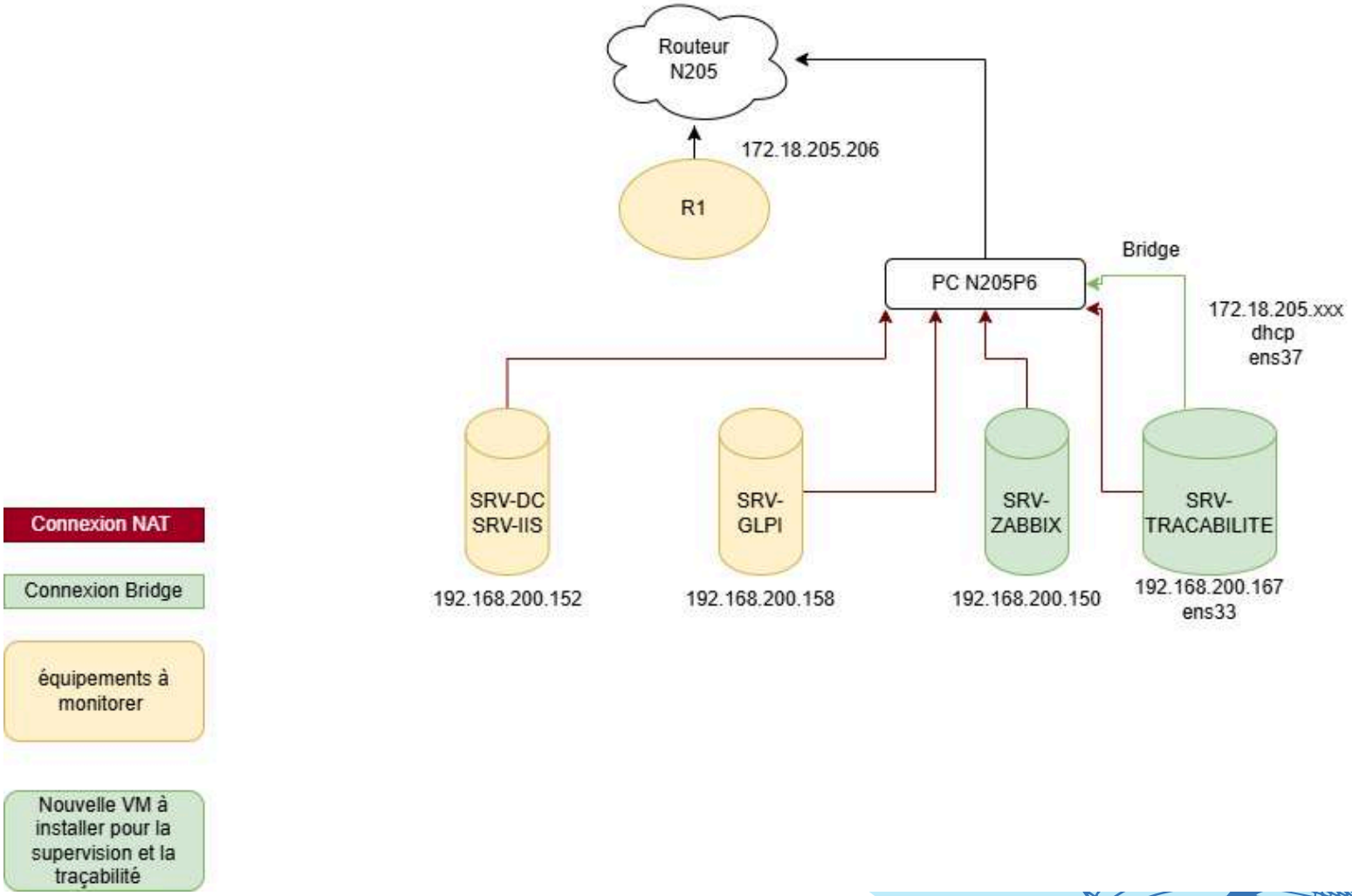
Mettre en place des audits pour assurer la sécurité de l’entreprise.

Matériel

Pour ce projet nous aurons besoin :

- 1 routeur Cisco
- 1 VM Serveur AD, DNS, IIS
- 1 VM Serveur GLPI
- 1 VM serveur Zabbix + serveur de messagerie
- 1 VM serveur Graylog

Schéma :



Solution

Pour répondre au besoin de l'entreprise JIM, la solution repose sur trois piliers : la supervision active, la centralisation des logs et la sécurisation des accès.

- Installation du serveur Zabbix : Déploiement sur une VM dédiée (IP: 192.168.200.150).
- Configuration du protocole SNMP : Activation du SNMP sur le routeur Cisco R1 pour remonter les statistiques de trafic et l'état des interfaces.
- Déploiement des agents Zabbix : Installation de l'agent sur les serveurs SRV-DC, SRV-IIS et SRV-GLPI pour surveiller l'utilisation du CPU, de la RAM et de l'espace disque.
- Système d'alerte : Configuration d'un serveur de messagerie (SMTP) pour l'envoi automatique de mails en cas d'incident (ex: serveur injoignable, service IIS arrêté).

Pour assurer la traçabilité demandée, nous centralisons les journaux d'événements :

- Mise en place de Graylog : Installation sur la VM "SRV-TRACABILITE" (IP: 192.168.200.167).
- Collecte des logs (Filebeat) : Installation de l'agent Filebeat sur les serveurs critiques pour envoyer les logs Windows et IIS vers Graylog en temps réel.
- Logs Réseau : Configuration du routeur Cisco pour envoyer ses messages Syslog vers le serveur Graylog.
- Tableaux de bord : Création de vues quotidiennes pour visualiser les tentatives de connexion échouées et les erreurs système.

Conformément à l'objectif d'audit, plusieurs mesures de durcissement ont été appliquées :

- Sécurisation du Routeur : Chiffrement des mots de passe, configuration d'une bannière d'avertissement et sécurisation des lignes virtuelles (VTY).
- Contrôle d'accès : Utilisation du serveur Graylog pour centraliser la journalisation sur les serveurs et équipements réseaux
- Analyse des vulnérabilités : Mise en place de rapports réguliers via l'interface de traçabilité pour identifier les comportements anormaux

Conclusion

Test :

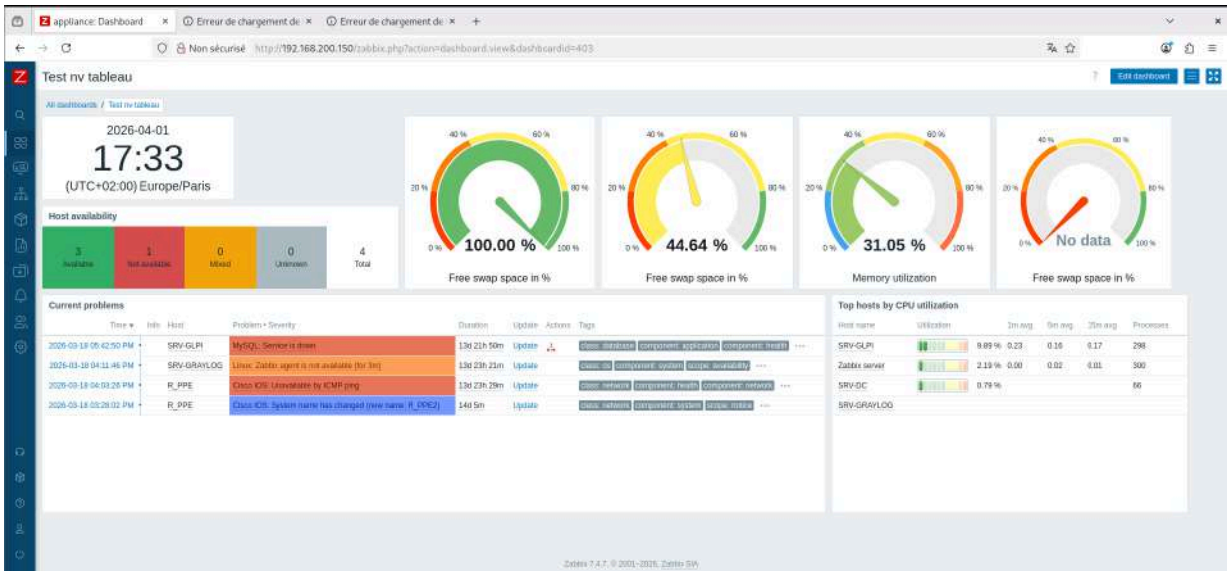
Les tests de connectivité sont tous ok : les serveurs communiquent entre eux avec le routeur
Le serveur Zabbix reçoit les métriques avec les agents et la communauté SNMP
Graylog reçoit bien tous les logs des serveurs et du routeur :

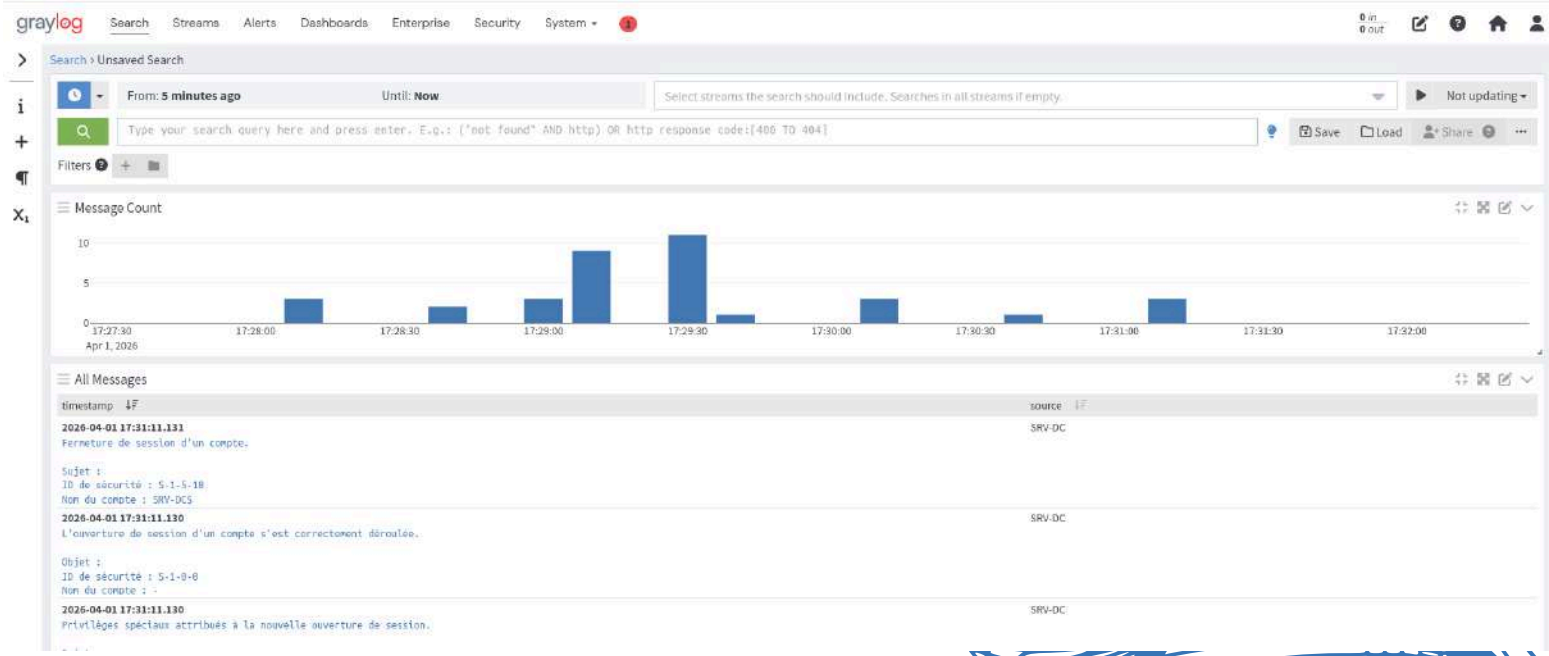
- Tentative de fausse connexion sur les serveurs et le routeur

Zabbix envoie bien les alertes sur le tableau de bord et par mail grâce au serveur Mail :

- Arrêt volontaire du service Web (IIS) sur le serveur SRV-IIS (192.168.200.152)
- Eteindre un serveur par exemple ou en changeant le déclencheur de valeur

Depuis l'intervention dans l'entreprise JIM peut désormais être alertée de tout problème au niveau de leur infrastructure système et réseaux.





Annexe

Configuration du Routeur :

Confiig de base

conf t
hostname R1
exit
banner motd “attention zone interdite”
Service password-encryption

line console 0
password test
login
enable password test

line vty 0 15
password test
login

Création de l’interface Gio/0

ip address 172.18.205.206 255.255.255.0
no shutdown

Administration du serveur de logs :

conf t
Logging host 192.168.200.167

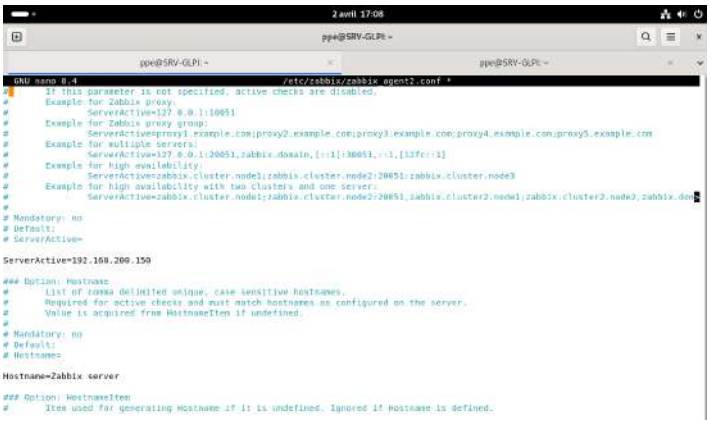
configuration du protocole SNMP :

snmp-server community ppe.jim RO
snmp-server enable traps

```
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 172.18.205.206 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
logging host 192.168.200.167
!
!
snmp-server community ppe.jim RO
snmp-server enable traps entity-sensor threshold
!
control-plane
!
!
banner motd ^CAttention equipement surveill
banner motd ^C
!
line con 0
 password promeo
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password promeo
 login
 transport input all
line vty 5 15
 password promeo
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Annexe

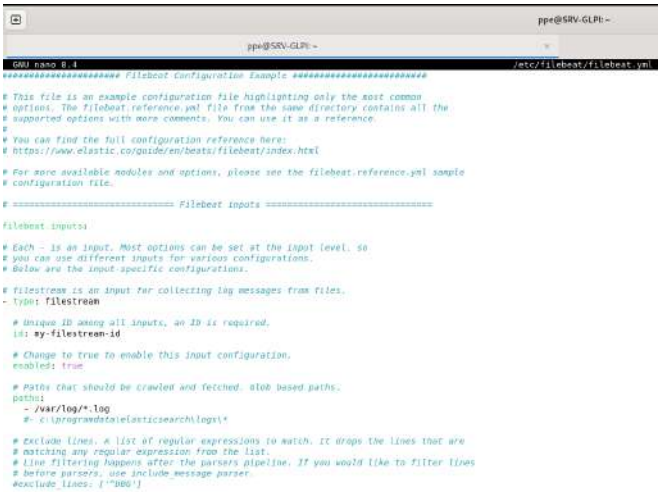
Configuration des agents zabbix sur linux :



Configuration des agents zabbix sur Windows :

Aller chercher l'agent sur la plateforme zabbix

Configuration des agents Filebeat sur linux



- Télécharger le paquet depuis elastic
- Modifier le fichier /etc/filebeat/filebeat.yml

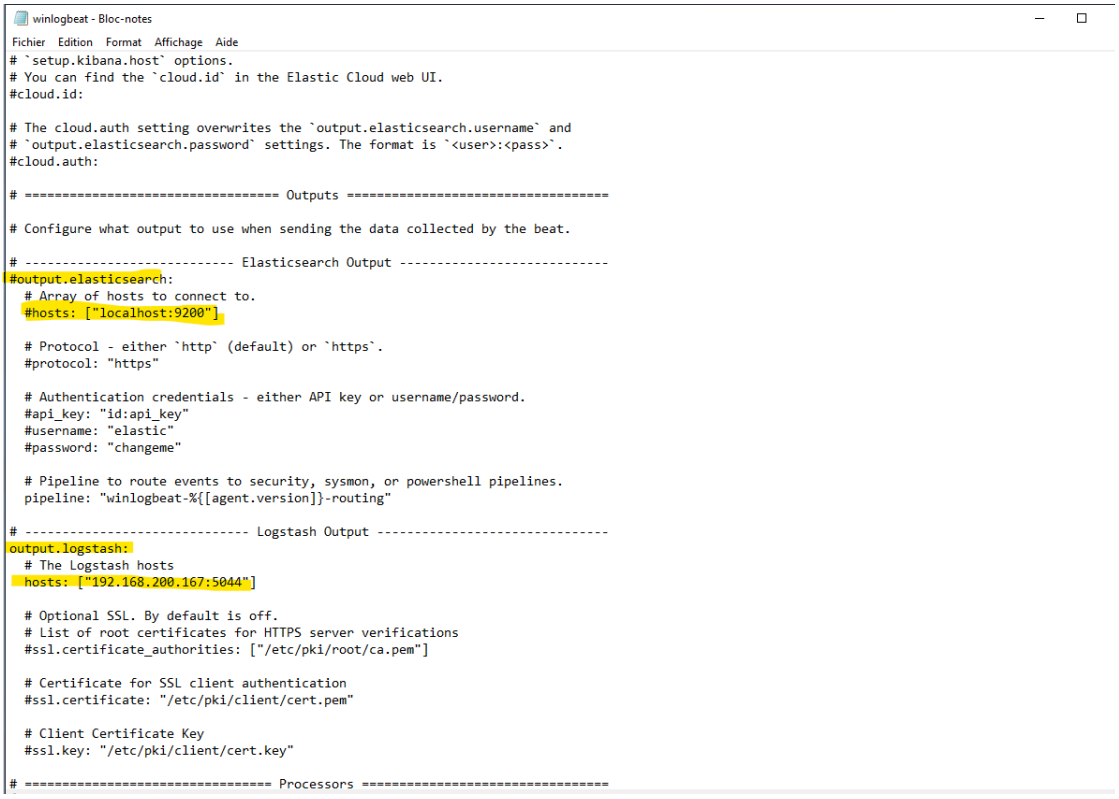
passer la valeur enabled à "true"

- commenter les lignes : Output.elasticsearch et hosts ["localhost:9200"
- décommenter les lignes : output.logstash et hosts: ["localhost:5044"]
- Remplacer la valeur localhost par l'ip du serveur Graylog

Configuration des agents Filebeat sur windows :

Commenter les deux premiere ligne surlignée

Décommenter les deux dernière lignes surlignée



- Lancer un powershell en admin et lancer le .ps1 dans le dossier winlogbeat

- Aller dans les services windows et lancer le service winlogbeat