

PPE-2

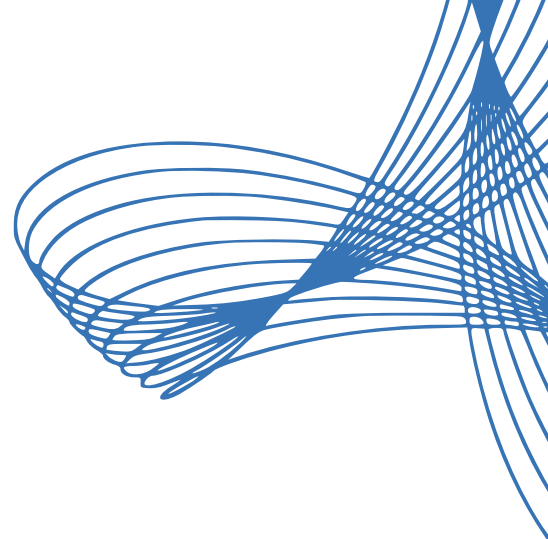
TRAÇABILITÉ ET SUPERVISION DE LA SANTÉ ET
DE LA SÉCURITÉ DU SYSTÈME D'INFORMATION

Pauline JIMENEZ
BTS SIO 26

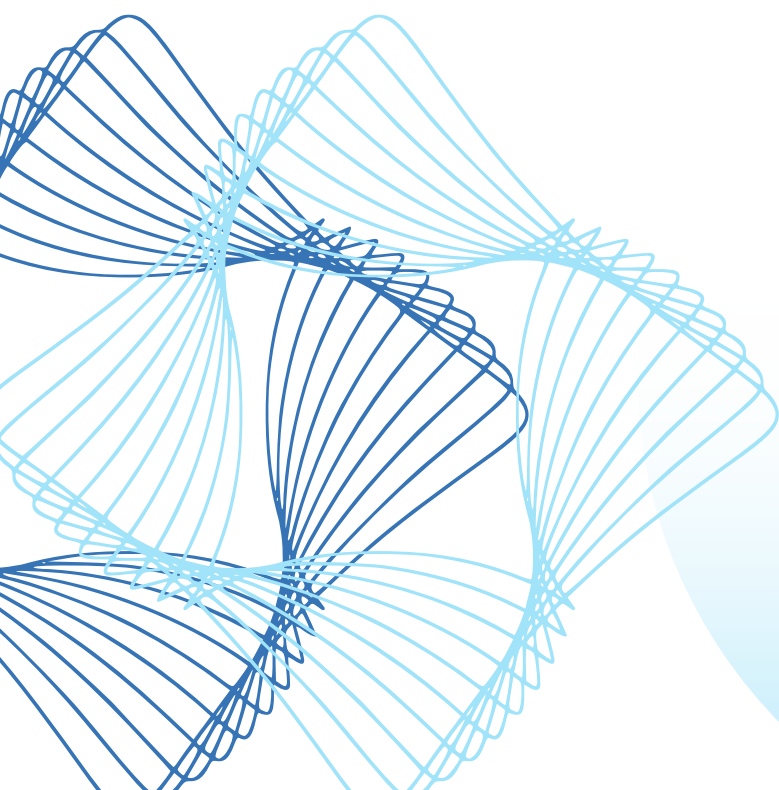
pauline.jimenez.etude@gmail.com

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

SOMMAIRE :



Situation initiale	page 01
Problématique	page 02
liste des équipements.....	page 03
Tâches à effectuer	page 04
Annexe	Page 05



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 :

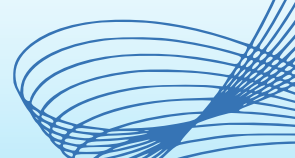
Comment déployer une supervision et une traçabilité adaptées à l'entreprise JIM ?

L'objectif :

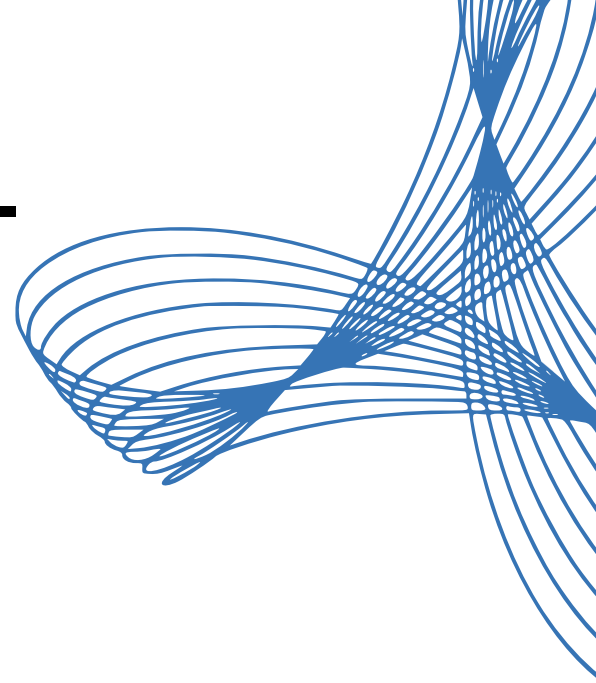
Moderniser la supervision des équipements réseaux et des serveurs avec un système d'alerte par mail

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.



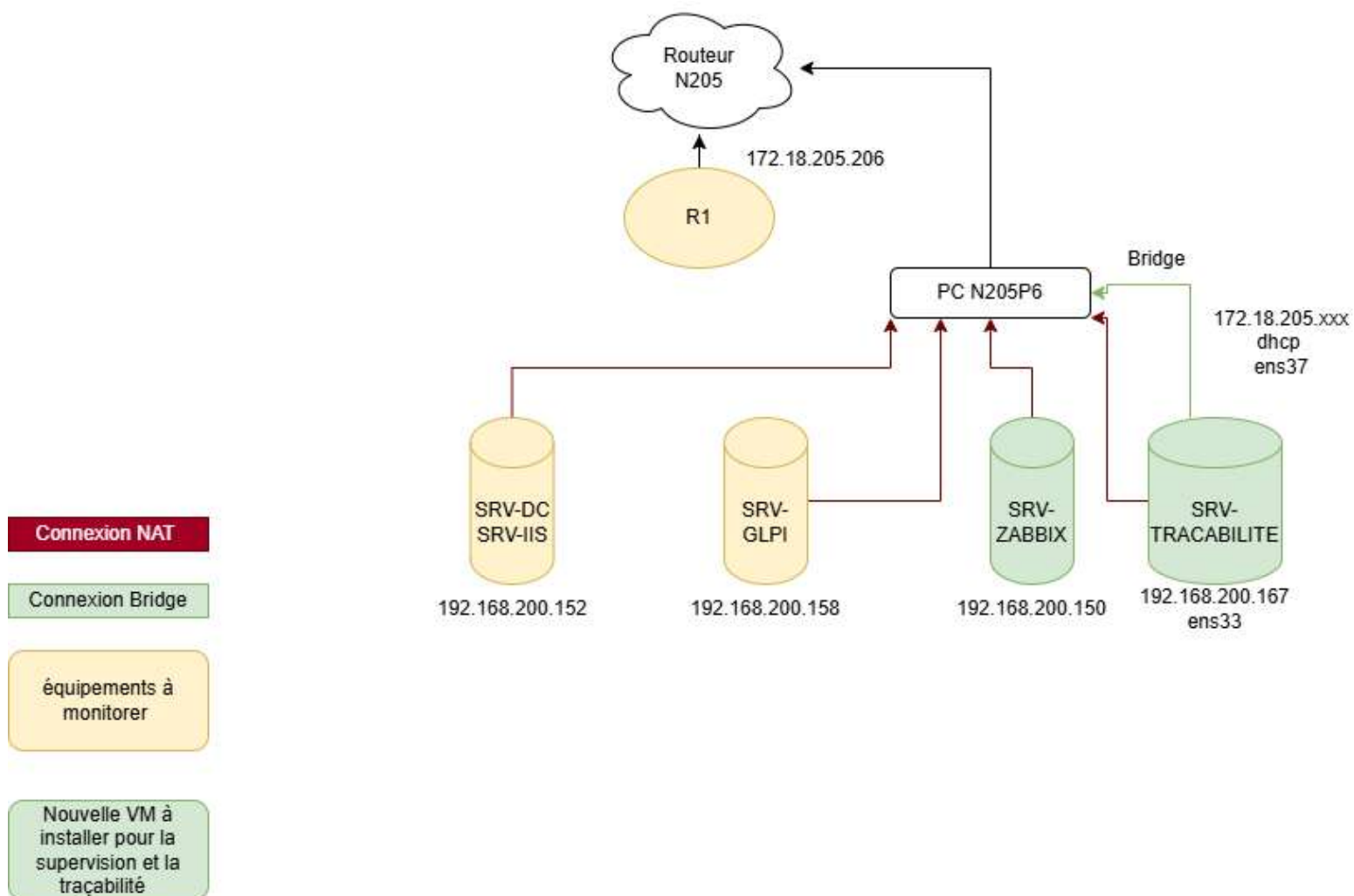
Matériel



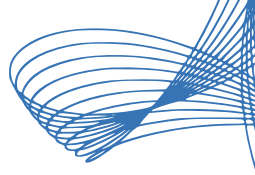
Pour ce projet nous aurons besoin :

- 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.

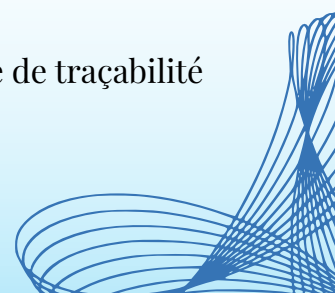
- Installation du serveur Zabbix : Déploiement sur une VM dédiée (IP: 192.168.200.150).
- Configuration du protocole SNMP : Activation du SNMP sur le routeur Cisco R1 pour remonter les statistiques de trafic et l'état des interfaces.
- Déploiement des agents Zabbix : Installation de l'agent sur les serveurs 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 :

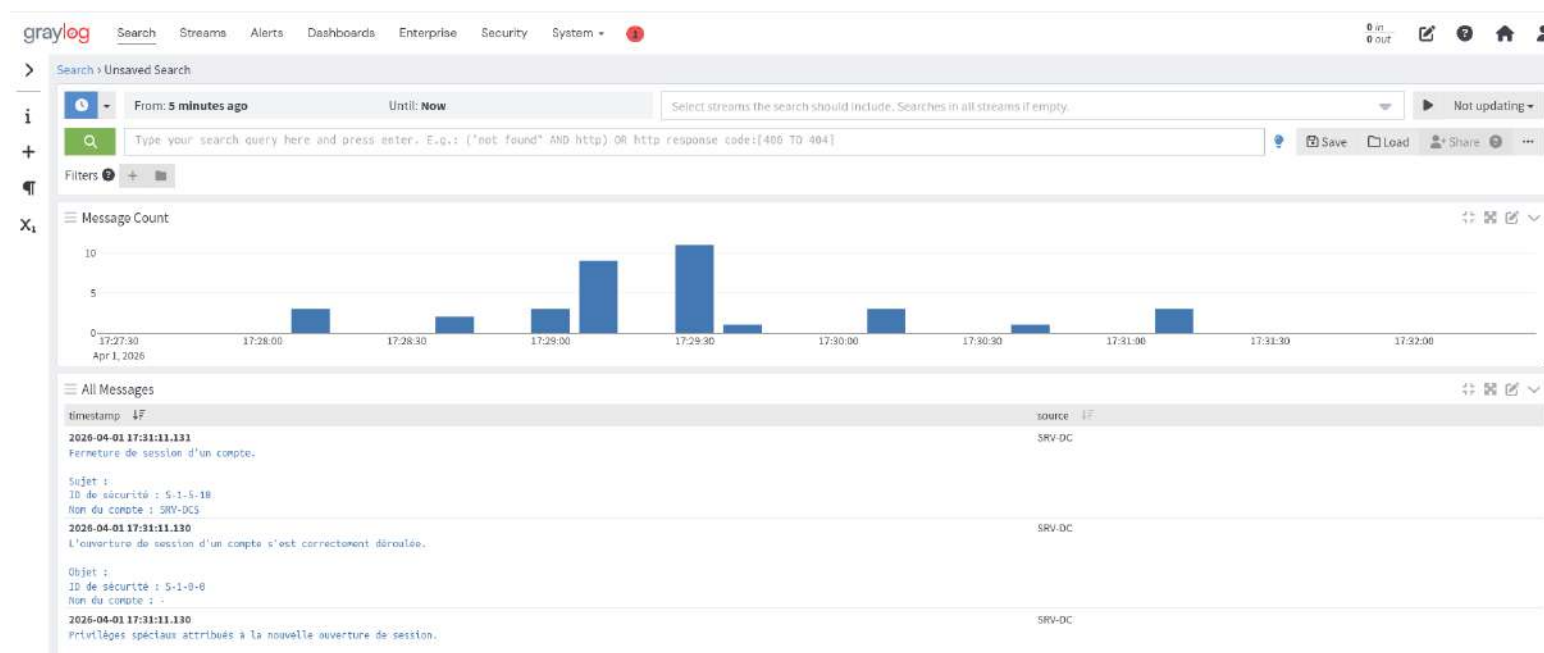
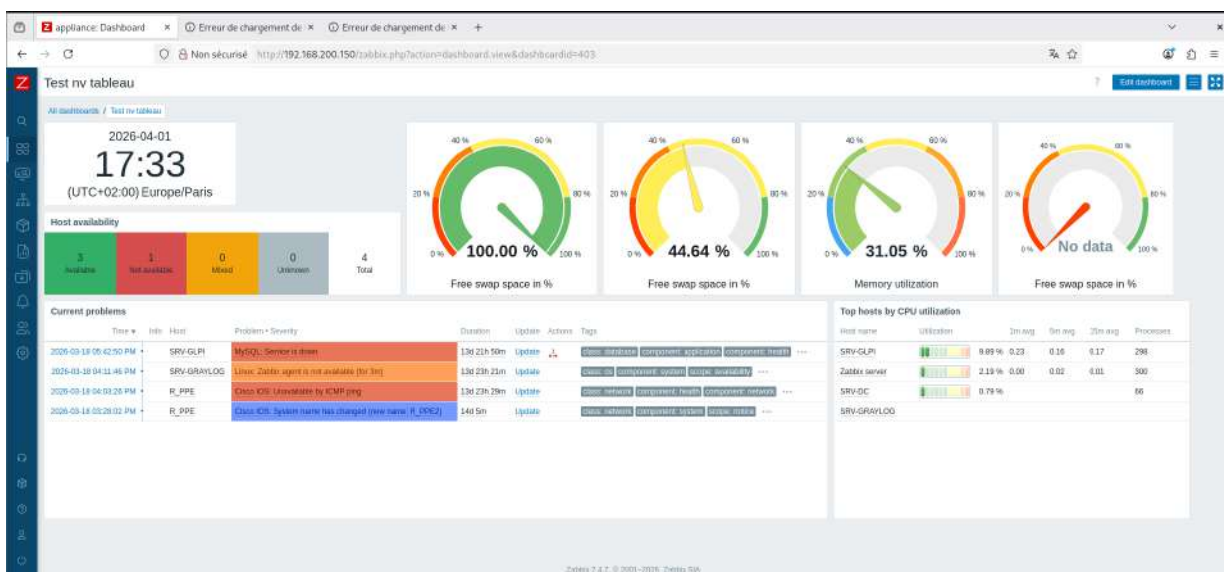
Les tests de connectivité sont tous ok : les serveurs communiquent entre eux avec le routeur
Le serveur Zabbix reçoit les métriques avec les agents et la communauté SNMP
Graylog reçoit bien tous les logs des serveurs et du routeur :

- 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 :

Config de base

conf t	line console 0	line vty 0 15
hostname R1	password test	password test
exit	login	login
banner motd "attention zone interdite"	enable password test	
Service password-encryption		

Création de l'interface Gio/o

```
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 équipement 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 :

```
GNU nano 0.4 /etc/zabbix/zabbix_agent2.conf
# If this parameter is not specified, active checks are disabled.
# Example for Zabbix proxy:
#   ServerActive=127.0.0.1:10051
# Example for Zabbix proxy group:
#   ServerActive=proxy1.example.com:proxy2.example.com:proxy3.example.com:proxy4.example.com:proxy5.example.com
# Example for multiple servers:
#   ServerActive=127.0.0.1:10051,zabbix.domain,[::1]:10051,[12fc::1]
# Example for high availability:
#   ServerActive=zabbix.cluster.node1;zabbix.cluster.node2;20051;zabbix.cluster.node3
# Example for high availability with two clusters and one server:
#   ServerActive=zabbix.cluster.node1;zabbix.cluster.node2;20051;zabbix.cluster2.node1;zabbix.cluster2.node2;zabbix.d
#
# Mandatory: no
# Default:
# ServerActive=

ServerActive=192.168.200.150

## Option: Hostname
# List of comma delimited unique, case sensitive hostnames.
# Required for active checks and must match hostnames as configured on the server.
# Value is acquired from HostnameFunction if undefined.
#
# Mandatory: no
# Default:
# Hostname=

Hostname=Zabbix server

## Option: HostnameTemplate
# Item used for generating Hostname if it is undefined. Ignored if Hostname is defined.
```

Configuration des agents zabbix sur Windows :

Aller chercher l'agent sur la plateforme zabbix

```
zabbix_agent2 - Win nodes
Fichier Edition Format Affichage Aide
# LogRemoteCommands=0

##### Passive checks related

## Option: Server
# List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix servers and Zabbix proxies.
# Incoming connections will be accepted only from the hosts listed here.
# If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated equally and '::/0' will allow any IPv4 or IPv6 address.
# '0.0.0.0/0' can be used to allow any IP address.
# Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::1,zabbix.domain
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=192.168.200.150
```

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

```
GNU nano 0.4 /etc/filebeat/filebeat.yml
##### Filebeat Configuration Example #####

# This file is an example configuration file highlighting only the most common
# options. The filebeat.reference.yml file from the same directory contains all the
# supported options with more comments. You can use it as a reference.
#
# You can find the full configuration reference here:
# https://www.elastic.co/guide/en/beats/filebeat/index.html
#
# For more available modules and options, please see the filebeat.reference.yml sample
# configuration file.

# ===== Filebeat Inputs =====

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input-specific configurations.

# Filestream is an input for collecting log messages from files.
- type: filestream

# Unique ID among all inputs, an ID is required.
id: my-filestream-id

# Change to true to enable this input configuration.
enabled: true

# Paths that should be crawled and fetched. Glob based paths.
paths:
  - /var/log/*.log
  - c:\programdata\elasticsearch\logs\

# Exclude lines. A list of regular expressions to match. It drops the lines that are
# matching any regular expression from the list.
# Line filtering happens after the parsers pipeline. If you would like to filter lines
# before parsers, use include_message_parser.
#exclude_lines: ['^DBG']
```

```
# ===== Outputs =====

# Configure what output to use when sending the data collected by the beat.

# ----- Elasticsearch Output -----
output.elasticsearch:
  # Array of hosts to connect to.
  # hosts: ["localhost:9200"]

  # Performance preset - one of "balanced", "throughput", "scale",
  # "latency", or "custom".
  # preset: balanced

  # Protocol - either 'http' (default) or 'https'.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

# ----- Logstash Output -----
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.200.167:5044"]
```

Configuration des agents Filebeat sur windows :

Commenter les deux
premiere ligne surlignée

Décommenter les deux
dernière lignes surlignée

```
winlogbeat - Bloc-notes
Fichier Edition Format Affichage Aide
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `:<pass>`.
#cloud.auth:

# ===== Outputs =====

# Configure what output to use when sending the data collected by the beat.

# ----- Elasticsearch Output -----
#output.elasticsearch:
# Array of hosts to connect to.
#hosts: ["localhost:9200"]

# Protocol - either `http` (default) or `https`.
#protocol: "https"

# Authentication credentials - either API key or username/password.
#api_key: "id:api_key"
#username: "elastic"
#password: "changeme"

# Pipeline to route events to security, sysmon, or powershell pipelines.
pipeline: "winlogbeat-%[agent.version]}-routing"

# ----- Logstash Output -----
#output.logstash:
# The Logstash hosts
#hosts: ["192.168.200.167:5044"]

# Optional SSL. By default is off.
# List of root certificates for HTTPS server verifications
#ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

# Certificate for SSL client authentication
#ssl.certificate: "/etc/pki/client/cert.pem"

# Client Certificate Key
#ssl.key: "/etc/pki/client/cert.key"

# ===== Processors =====
```

- Lancer un powershell en admin et lancer le .ps1 dans le dossier winlogbeat
- Aller dans les services windows et lancer le service winlogbeat