



RÉPUBLIQUE DU SÉNÉGAL



Université numérique  
**CHEIKH HAMIDOU KANE**

**SIMAC**

*(Sciences Informatiques et Mathématiques de la Cybersécurité)*

Pôle Sciences Technologie et Numérique

**CYB**

🔗 Bienvenue dans votre cours de

**Administration des systèmes  
MS Windows Server**



Projet

**Surveillance et Gestion des Logs pour  
la Cybersécurité**

**Groupe**

**3**

**Membres**

**BASSENE Massina Sylvanus**

**GOMIS Laurence**

**NDIAYE Elhadji Fallou**

**SECK Fatou Samb**

**massinasylvanus.bassene@unchk.edu.sn**

**laurence.gomis@unchk.edu.sn**

**elhadjifallou.ndiaye1@unchk.edu.sn**

**fatousamb.seck@unchk.edu.sn**

**Professeur**

**M. DIEME**

**Année Académique: 2023-2024**



## Table des matières

Introduction.....	2
Étape 1 : Configuration de Windows Event Forwarding (WEF).....	3
Étape 2 : Déploiement d'un SIEM Open-Source (ELK Stack).....	8
Étape 3 : Détection des menaces avec Windows Defender ATP.....	11
Étape 4 : Automatisation des alertes avec PowerShell et SIEM.....	13
Étape 5 : Bonnes pratiques et optimisation.....	16
Conclusion.....	17

## ***Introduction***

Dans un contexte où les cybermenaces évoluent constamment, la gestion efficace des logs devient essentielle pour anticiper, détecter et répondre aux incidents de sécurité. Le projet "Surveillance et Gestion des Logs pour la Cybersécurité" vise à établir une infrastructure robuste pour la collecte, l'analyse et la surveillance des logs provenant de différents serveurs et systèmes. Cette approche centralisée permet de mieux visualiser les événements critiques, d'automatiser les alertes, et d'implémenter une stratégie Zero Trust grâce à des outils performants tels que ELK Stack et Microsoft Defender ATP. Ce projet couvre l'intégration de plusieurs solutions, permettant une protection proactive et une réponse rapide aux menaces potentielles.

## Étape 1 : Configuration de Windows Event Forwarding (WEF)

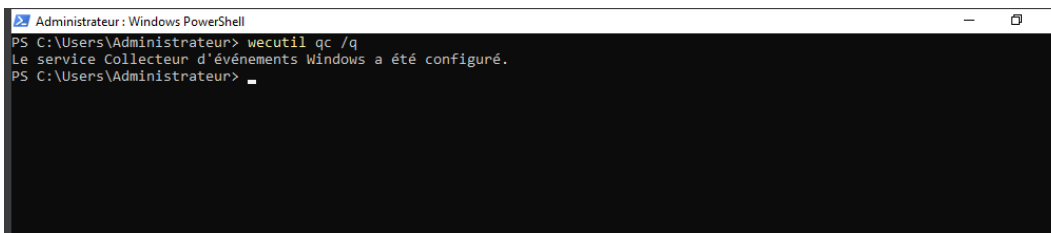
Windows Event Forwarding (WEF) permet de centraliser la collecte des logs provenant de serveurs Windows vers un serveur collecteur, facilitant ainsi leur gestion et leur analyse. Cette étape vise à configurer le service WEF pour rediriger les journaux de sécurité, de système et d'application vers un point central. Afin d'assurer une transmission sécurisée des logs, l'utilisation de certificats SSL est recommandée pour chiffrer les données en transit. En utilisant des Stratégies de Groupe (GPO), nous pouvons facilement gérer et appliquer les configurations de redirection sur l'ensemble des serveurs sources du réseau.

**Objectif :** Centraliser les logs des serveurs Windows.

### 1. Configurer le serveur collecteur :

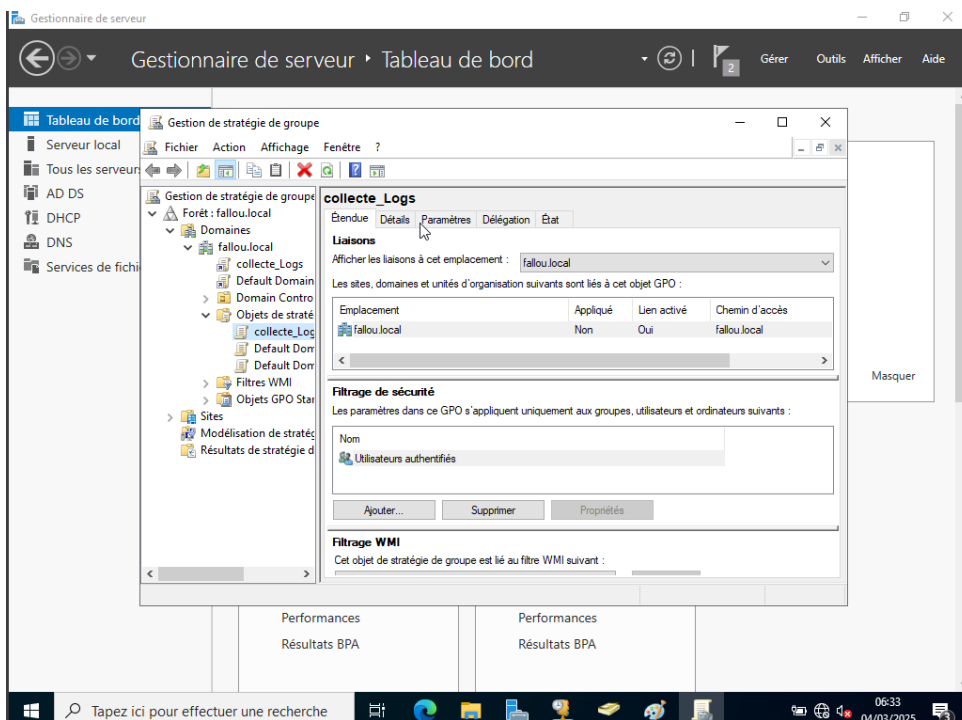
a. Sur un serveur Windows dédié :

# Activer le service "Windows Event Collector" : **wecutil qc /q**



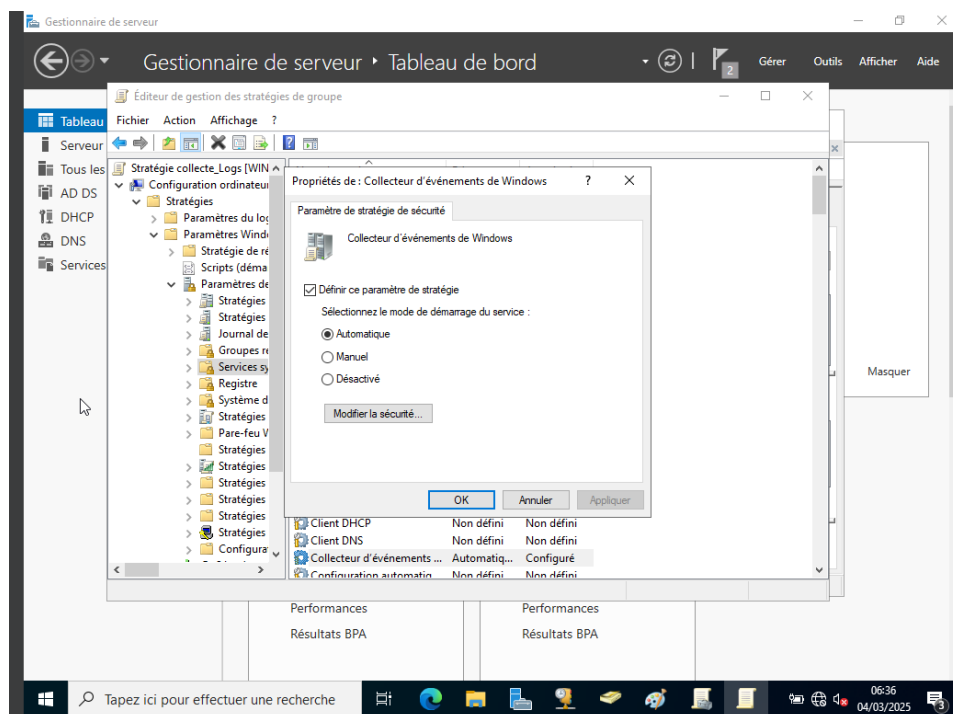
```
Administrateur : Windows PowerShell
PS C:\Users\Administrateur> wecutil qc /q
Le service Collecteur d'événements Windows a été configuré.
PS C:\Users\Administrateur> _
```

b. Créer un **Groupe de Collecte** via l'Éditeur de Stratégie de Groupe (ex : collecter les logs de sécurité, système, et application).  
Creation d'un GPO nommé "collecte logs"



## 2. Configurer les serveurs sources :

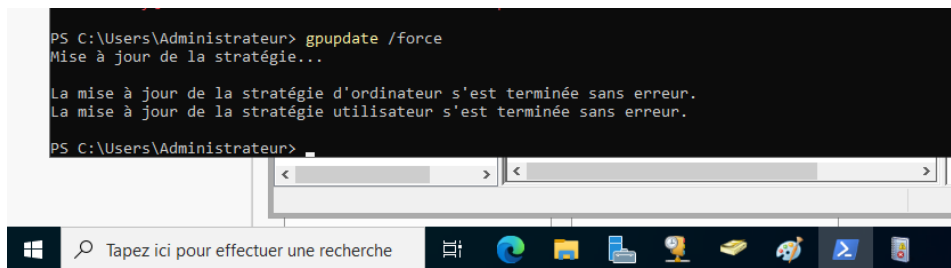
- a. Appliquer une **Stratégie de Groupe** pour rediriger les logs vers le collecteur :
  - i. **Chemin : Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Transfert d'événements**



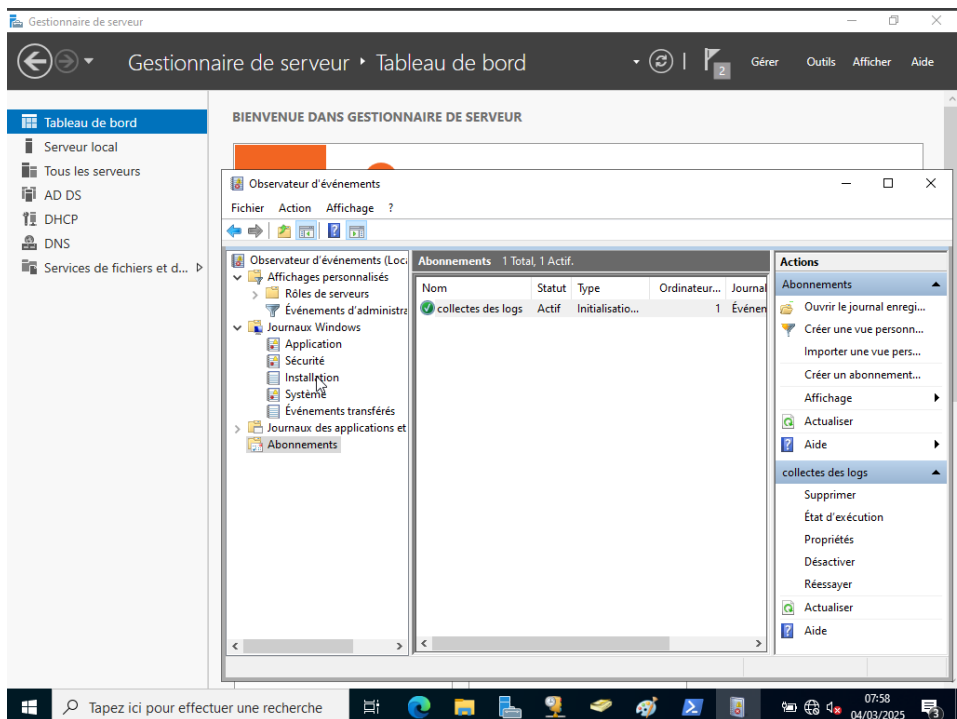
```
PS C:\Users\Administrateur> gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.

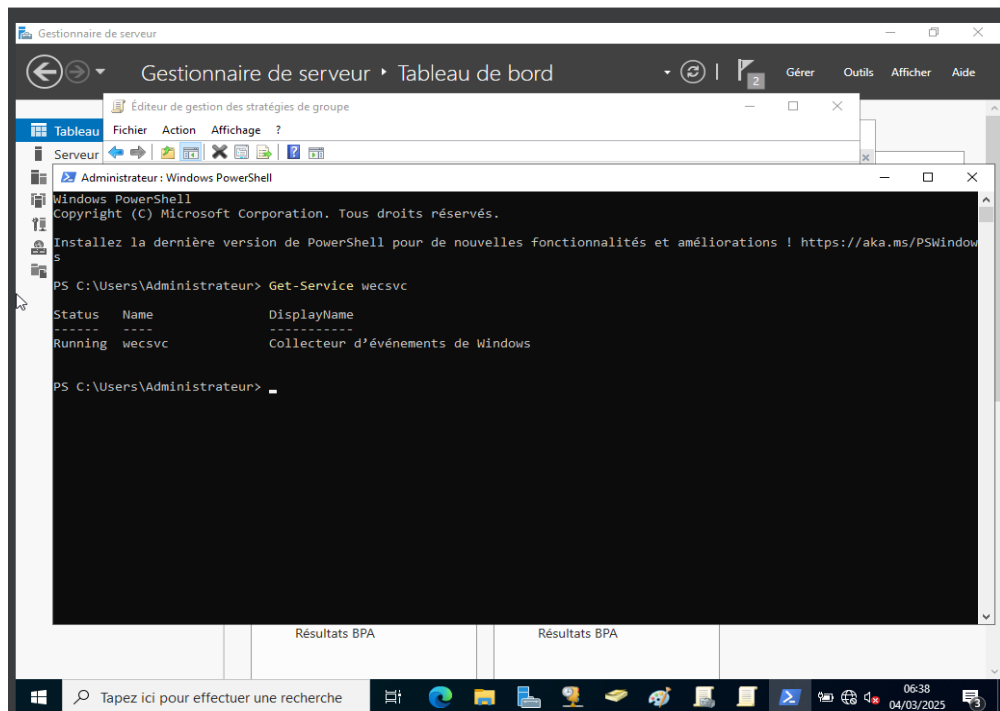
PS C:\Users\Administrateur>
```



ii. Définir l'adresse du collecteur et les canaux d'événements (ex : Security, System).



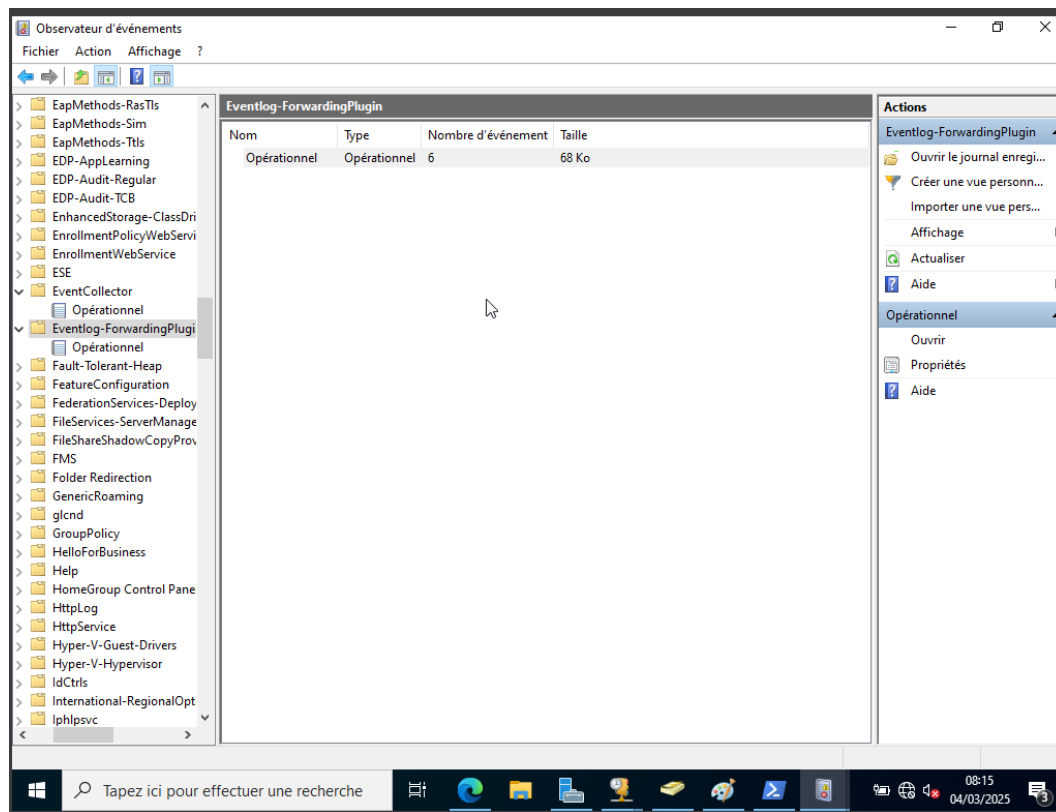
Vérifions si le service des collecte des événements de windows est en cours.



### 3. Vérifier la collecte :

- a. Sur le collecteur, utiliser l'**Observateur d'événements > Journaux des applications et des services > Microsoft > Windows > EventForwarding-Operational** pour vérifier les erreurs.





## Étape 2 : Déploiement d'un SIEM Open-Source (ELK Stack)

L'ELK Stack (Elasticsearch, Logstash, Kibana) est un outil open-source couramment utilisé pour l'analyse et la visualisation des logs en temps réel. Elasticsearch permet de stocker et d'indexer de grandes quantités de données, tandis que Logstash collecte et traite les logs avant de les envoyer à Elasticsearch. Kibana fournit des capacités de visualisation avancées qui permettent de créer des dashboards personnalisés pour suivre les événements de sécurité en temps réel. Ce déploiement de l'ELK Stack permet d'automatiser l'analyse des journaux des serveurs Windows et de détecter les comportements suspects à travers des filtres avancés et des requêtes sur les événements.

**Objectif :** Analyser et visualiser les logs.

### 1. Installer l'ELK Stack (Elasticsearch, Logstash, Kibana) :

#### a. Sur un serveur Linux (ex : Ubuntu) :

# Installer Java

**sudo apt install openjdk-11-jdk**

# Ajouter le dépôt Elastic :

- **wget -qO - <https://artifacts.elastic.co/GPG-KEY-elasticsearch> | sudo apt-key add -**
- **echo "deb <https://artifacts.elastic.co/packages/7.x/apt> stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list**

```
html root@rakib:/var/www# rm -rf magento
root@rakib:/var/www# cd sudo apt install apt-transport-https ca-certificates gnupg2 -y^C
root@rakib:/var/www# sudo apt install apt-transport-https ca-certificates gnupg2 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
ca-certificates is already the newest version (20210119-20.04.2).
apt-transport-https is already the newest version (2.0.6).
gnupg2 is already the newest version (2.2.19-3ubuntu2.1).
0 upgraded, 0 newly installed, 0 to remove and 28 not upgraded.
root@rakib:/var/www# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
root@rakib:/var/www# sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.li
st'
root@rakib:/var/www# apt update -y
Hit:1 https://deb.debian.org/debian bullseye InRelease
Hit:2 https://deb.debian.org/debian bullseye-updates InRelease
Hit:3 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Get:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease
Get:5 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages
Fetched 10.5 kB in 1s (10.5 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
28 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

# Installer Elasticsearch, Logstash, Kibana

**sudo apt update && sudo apt install elasticsearch logstash kibana**

```
Building dependency tree
Reading state information... Done
28 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@rakib:/var/www# apt install elasticsearch -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  elasticsearch
```

### 2. Configurer Logstash pour ingérer les logs Windows :

- a. Créer un fichier de configuration `/etc/logstash/conf.d/windows-logs.conf` :
 

```
input {
  beats {
    port => 5044
  }
}
filter {
  # Parsing des logs Windows (ex : EventID 4625 pour les échecs de connexion)
  grok { match => { "message" => "%{EVENTLOG}" } }
}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "windows-logs-%{+YYYY.MM.dd}"
  }
}
```

```
root@rakib:/var/www# sudo apt install apt-transport-https ca-certificates gnupg2 -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
ca-certificates is already the newest version (20210119-20.04.2).
apt-transport-https is already the newest version (2.0.6).
gnupg2 is already the newest version (2.2.19-3ubuntu2.1).
0 upgraded, 0 newly installed, 0 to remove and 28 not upgraded.
root@rakib:/var/www# wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
OK
root@rakib:/var/www# sudo sh -c 'echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" > /etc/apt/sources.list.d/elastic-7.x.li
st'
root@rakib:/var/www# apt update -y
Hit:1 http://mirrors.digitalocean.com/ubuntu focal InRelease
Get:2 http://mirrors.digitalocean.com/ubuntu focal-updates InRelease [114 kB]
Hit:3 https://repos.insights.digitalocean.com/apt/do-agent main InRelease
Get:4 https://artifacts.elastic.co/packages/7.x/apt stable InRelease [13.7 kB]
Hit:5 https://deb.nodesource.com/node_14.x focal InRelease
Hit:6 https://repos.droplet.digitalocean.com/apt/droplet-agent main InRelease
Get:7 http://mirrors.digitalocean.com/ubuntu focal-backports InRelease [108 kB]
Hit:8 https://dl.yarnpkg.com/debian stable InRelease
Hit:9 http://ppa.launchpad.net/ondrej/php/ubuntu focal InRelease
Get:10 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:11 https://artifacts.elastic.co/packages/7.x/apt stable/main amd64 Packages [89.7 kB]
```

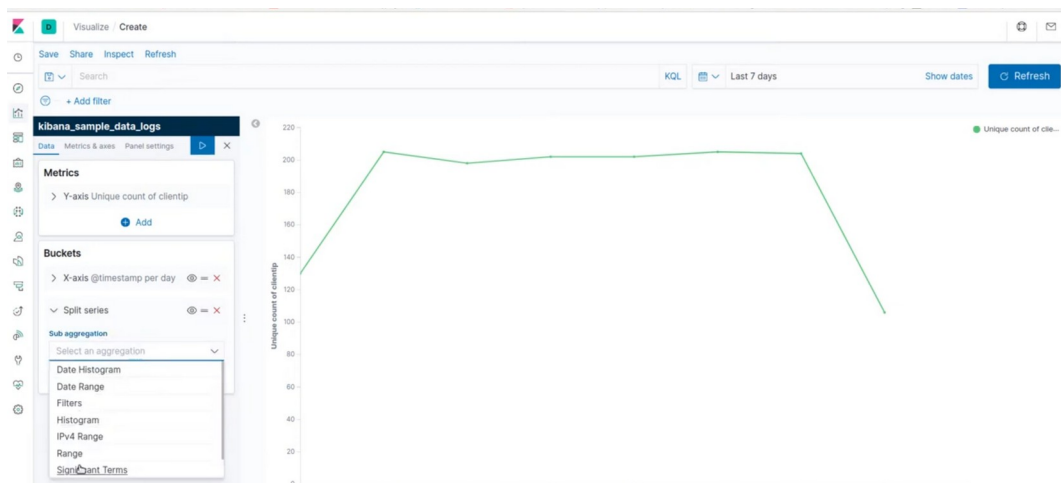
### 3. Installer Winlogbeat sur le collecteur WEF :

- a. Télécharger Winlogbeat et configurer `/etc/winlogbeat/winlogbeat.yml` :
 

```
output.logstash:
  hosts: ["IP_SIEM:5044"]
```

### 4. Démarrer les services et visualiser dans Kibana :

- a. Accéder à [http://IP\\_SIEM:5601](http://IP_SIEM:5601) pour créer des dashboards (ex : cartographie des tentatives de connexion suspectes).



## Étape 3 : Détection des menaces avec Windows Defender ATP

Windows Defender ATP (Advanced Threat Protection) offre une détection proactive des menaces en analysant les comportements des endpoints et en fournissant des alertes en temps réel sur les activités suspectes. L'intégration avec le SIEM permet de centraliser les alertes provenant de Defender ATP dans l'ELK Stack, garantissant une meilleure visibilité sur les menaces à travers toute l'infrastructure. Grâce à Microsoft Graph API, les alertes générées par Defender ATP peuvent être facilement exportées vers Elasticsearch pour enrichir l'analyse des journaux et renforcer la cybersécurité globale.

**Objectif :** Intégrer la détection avancée.

### 1. Activer Microsoft Defender pour point de terminaison :

- a. Via le **Centre de sécurité Microsoft 365** > Intégrer les appareils via une Stratégie de Groupe **Accéder au Centre de sécurité Microsoft 365**

### 2. Ouvrir le Centre de sécurité Microsoft 365

Accédez à [security.microsoft.com](https://security.microsoft.com).

### 3. Naviguer vers la gestion des points de terminaison

Allez dans **Paramètres** > **Points de terminaison** > **Intégration**.

#### Détails du dépannage

Si vous contactez votre administrateur, envoyez-lui ces informations.

[Copier les informations dans le presse-papiers](#)

**Request Id:** 2e326ac1-dccd-4e6c-a7d0-b4014bb81100

**Correlation Id:** 7696221e-5d41-4846-a6e2-e3d02563f503

**Timestamp:** 2025-03-16T01:02:16Z

**Message:** AADSTS500200: User account 'elhadjifalloundiaye92@gmail.com' is a personal Microsoft account. Personal Microsoft accounts are not supported for this application unless explicitly invited to an organization. Try signing out and signing back in with an organizational account.

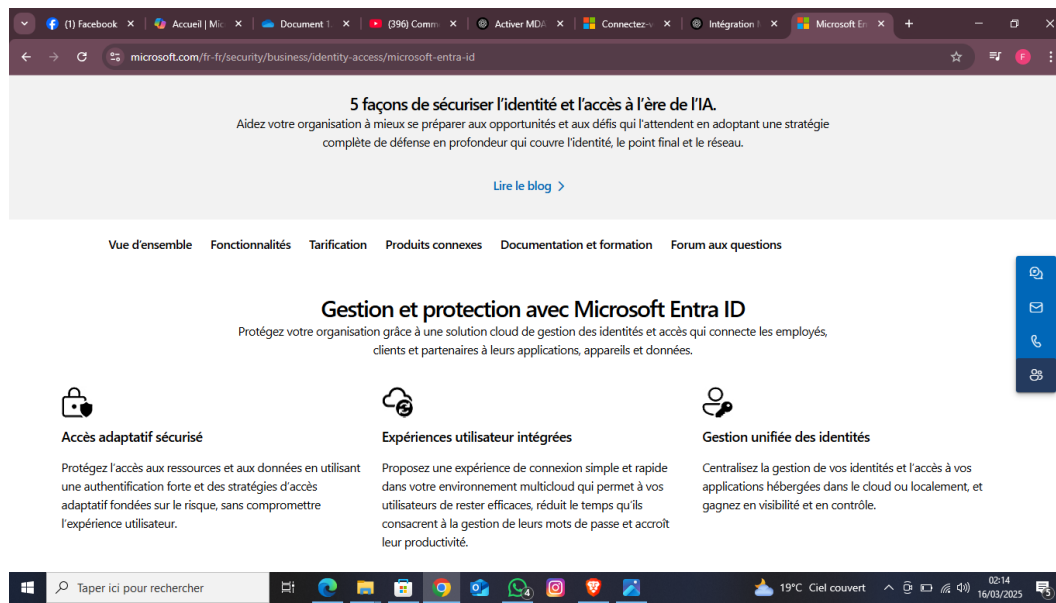
**Signaler les erreurs de connexion pour la révision :** [Activer les indicateurs](#)

Si vous prévoyez d'obtenir de l'aide pour ce problème, activez les indicateurs et essayez de reproduire l'erreur dans un délai de 20 minutes. Les événements avec indicateur rendent les diagnostics disponibles et sont portés à l'attention de l'administrateur.

### 4. Configurer l'intégration avec le SIEM :

- a. Utiliser l'API Microsoft Graph pour exporter les alertes vers Elasticsearch via un script PowerShell ou Logstash.
- b. Enregistrer une application dans Azure AD

- c. Tu dois créer une application pour accéder à l'API Microsoft Graph.
5. Va sur **Azure Portal** → **Enregistrements d'applications**
  6. Clique sur **Nouvelle inscription**
  7. Configure les **autorisations** :
    - a. API Microsoft Graph → **Alert.Read.All**
    - b. Accorde le **consentement admin**
  8. Génère un **Client ID**, **Secret**, et récupère le **Tenant ID**



## **Étape 4 : Automatisation des alertes avec PowerShell et SIEM**

L'automatisation des alertes de sécurité est essentielle pour garantir une réaction rapide en cas de menace. Grâce à des scripts PowerShell, il est possible de surveiller en continu les événements critiques, comme les tentatives de connexion échouées, et d'envoyer automatiquement des notifications aux administrateurs. L'intégration avec le SIEM permet de déclencher des alertes personnalisées, configurées pour identifier des patterns spécifiques, comme un nombre élevé de connexions échouées en un court laps de temps. Cette automatisation permet de réduire le temps de réponse et d'optimiser la gestion des incidents de sécurité.

**Objectif :** Créer des alertes en temps réel.

### **1. Script PowerShell pour surveillance d'événements critiques :**

**# Surveiller les événements de connexion échouée (EventID 4625)**

```
$Query = '@'
```

```
<QueryList>
```

```
<Query Id="0">
```

```
<Select Path="Security">*[System[(EventID=4625)]]</Select>
```

```
</Query>
```

```
</QueryList>
```

```
'@'
```

```
Get-WinEvent -FilterXml $Query -MaxEvents 10 | ForEach-Object {
```

```
# Envoyer une alerte par email
```

```
Send-MailMessage -To "admin@domain.com" -Subject "Alerte Sécurité" -Body "Échec de connexion détecté !"
```

}

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

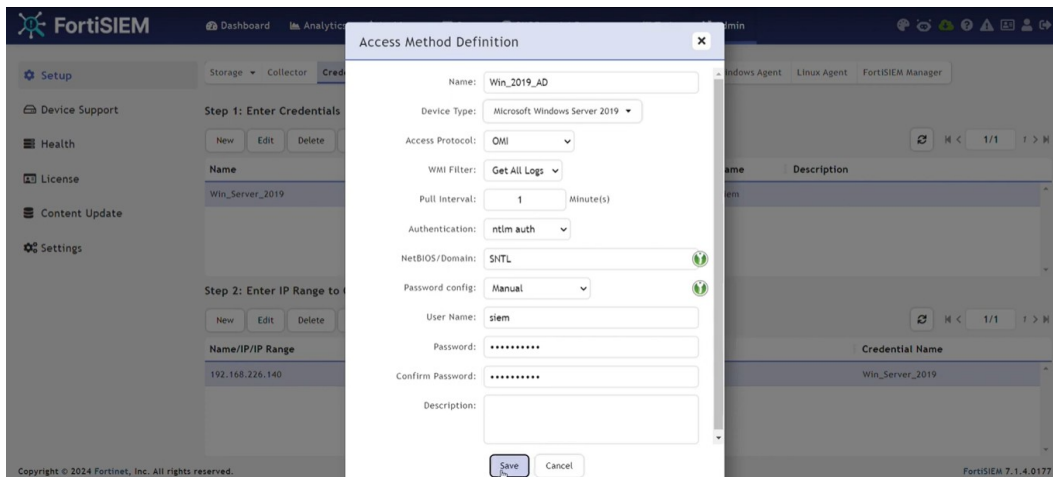
Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\Users\user> $tenantId = "TON_TENANT_ID"
>> $clientId = "TON_CLIENT_ID"
>> $clientSecret = "TON_CLIENT_SECRET"
>> $elasticsearchUrl = "http://localhost:9200/alerts/_doc/"
>>
>> # Obtenir un token d'accès
>> $body = @{
>>     grant_type = "client_credentials"
>>     client_id = $clientId
>>     client_secret = $clientSecret
>>     scope = "https://graph.microsoft.com/.default"
>> }
>>
>> $tokenResponse = Invoke-RestMethod -Method Post -Uri "https://login.microsoftonline.com/$tenantId/oauth2/v2.0/token"
>> -ContentType "application/x-www-form-urlencoded" -Body $body
>> $accessToken = $tokenResponse.access_token
>>
>> # Récupérer les alertes depuis Microsoft Graph
>> $graphUrl = "https://graph.microsoft.com/v1.0/security/alerts"
>> $headers = @{ Authorization = "Bearer $accessToken" }
>>
>> $alerts = Invoke-RestMethod -Method Get -Uri $graphUrl -Headers $headers
>>
>> # Envoyer les alertes à Elasticsearch
>> foreach ($alert in $alerts.value) {
>>     $jsonBody = $alert | ConvertTo-Json -Depth 10
>>     Invoke-RestMethod -Method Post -Uri $elasticsearchUrl -Headers @{ "Content-Type" = "application/json" } -Body $jsonBody
>> }
>>
```

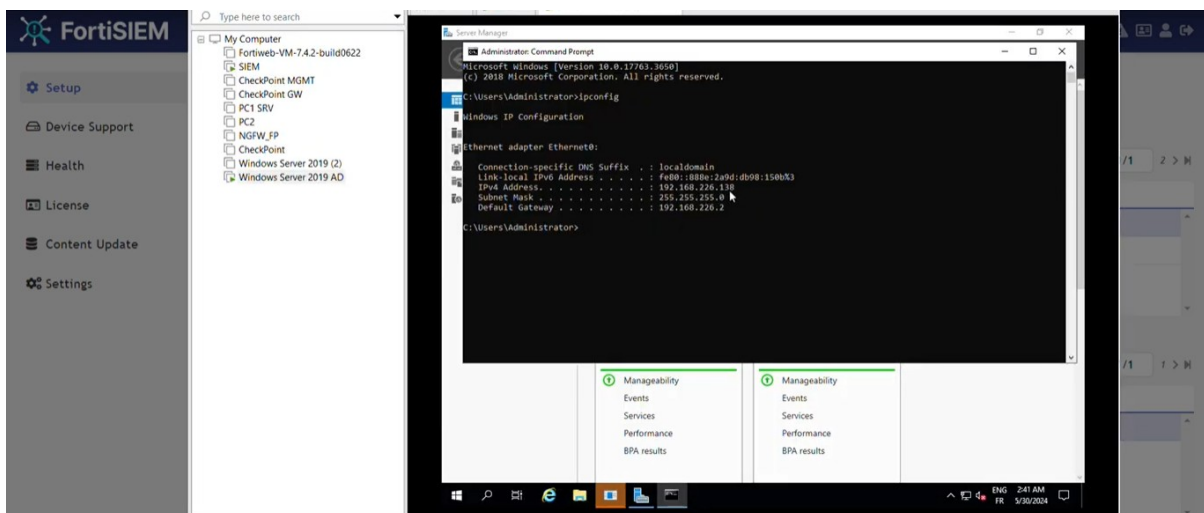
## 2. Alertes SIEM:

- a. Créer une règle pour déclencher une alerte en cas de **5 échecs de connexion en 1 minute** :  
*name: "Tentatives de connexion échouées"*  
*type: frequency*  
*index: windows-logs-\**  
*num\_events: 5*  
*timeframe:*  
*minutes: 1*  
*filter:*  
*- query:*  
*query\_string:*  
*query: "event\_id:4625"*  
*alert:*  
*- "email"*  
*email: "[admin@domain.com](mailto:admin@domain.com)"*

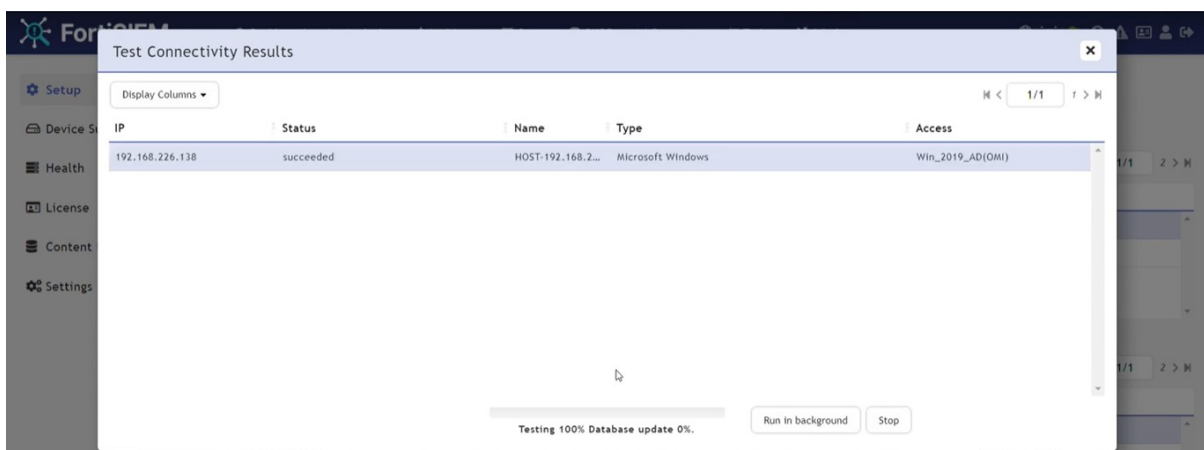




b. Config seim windows server



c. vérification



## ***Étape 5 : Bonnes pratiques et optimisation***

Pour garantir la sécurité et l'efficacité du système de gestion des logs, il est essentiel d'implémenter des bonnes pratiques telles que la sécurisation des communications via HTTPS, l'activation de l'authentification multifactorielle pour accéder à Kibana, et la limitation des accès via des rôles basés sur les utilisateurs dans Elasticsearch. Une stratégie de rétention doit également être définie pour optimiser le stockage, en tenant compte des contraintes réglementaires, telles que la conservation des logs pendant 30 jours avec un archivage sur des solutions de stockage froid. Enfin, des tests réguliers de détection, comme des simulations d'attaques par force brute avec Kali Linux, sont nécessaires pour valider l'efficacité des alertes et la performance du SIEM.

### **1. Sécuriser le SIEM :**

- a. Activer HTTPS et l'authentification pour Kibana.
- b. Restreindre l'accès aux logs via des rôles Elasticsearch.

### **2. Rétention et archivage :**

- a. Configurer une stratégie de rétention (ex : 30 jours dans Elasticsearch, archivage sur stockage froid).

### **3. Tests de détection :**

- a. Simuler des attaques (ex : Bruteforce avec Kali Linux) pour valider les alertes.

### **Résultat final :**

- Logs centralisés et analysés en temps réel.
- Alertes automatisées pour les activités suspectes.
- Détection proactive des menaces avec Defender ATP et ELK.

**Visualisation Kibana :** Exemple de dashboard pour suivre les événements de sécurité critiques.

## ***Conclusion***

Grâce à la mise en place d'un système centralisé de gestion des logs, l'infrastructure bénéficie désormais d'une meilleure visibilité sur les événements critiques et d'une réponse plus rapide aux incidents de sécurité. L'automatisation des alertes, couplée à une détection avancée via Windows Defender ATP et l'ELK Stack, permet une surveillance proactive des menaces. En appliquant des stratégies de rétention et en sécurisant l'accès aux logs, le projet garantit non seulement une meilleure gestion des données, mais aussi une conformité renforcée aux standards de cybersécurité. Ces améliorations assurent une posture de sécurité plus robuste et une gestion plus efficace des incidents futurs.