Manuel d’exploitation Elasticsearch

Table des matières

1. Clients Beats 3
1.1 Filebeat 3
1.1.1 Installation de Filebeat 3
1.1.2 Input et output 3
1.1.3 Connexion à Kibana 4
1.1.4 Setup de Filebeat 4
1.2 Winlogbeat 5
1.2.1 Installation 5
1.2.2 Configuration 5
1.2.3 Automatisation de l'installation 7
2. Interface graphique de Kibana 8
2.1Créer une Visualisation de données 8
2.2 Créer un Dashboard 10
2.3 Créer une alerte 11

1. Clients Beats

Les outils “Beats” servent à transférer les données vers Elasticsearch. Il y a plusieurs types de Beats pour différents types de données, ou selon l’OS du client. Par exemple, WinlogBeat pour des logs d'événements de clients Windows ou Filebeat pour l’équivalent Linux

1.1 Filebeat

1.1.1 Installation de Filebeat

Filebeat obtient les données via les input que nous choisissons. Il va ensuite les transférer selon les output choisis, via Logstash qui va également les normaliser ou les filtrer.

Il faut donc installer Filebeat avec la commande :

```
apt install filebeat
```

Une fois installé, on a accès au ficher /etc/filebeat/filebeat.yml

C’est ici que nous pourrons gérer les chemins vers les logs que le Beat va transférer vers Logstash, et la connexion à Logstash et Kibana.

1.1.2 Input et output

Les Inputs permettent de choisir les logs qui seront envoyés via ce Beat. Ici, nous choisissons par exemple les logs d’un client, et d’un serveur zabbix. Il est possible grâce à l’id de choisir un nom, réutilisable par la suite sur l’interface graphique de Kibana pour filtrer les logs.

```
filebeat.inputs:
  # ================== ZABBIX ==================
  - type: filestream
    id: zabbix-server
    paths:
      - /var/log/zabbix/zabbix_server.log
    fields:
      service: zabbix
      log_type: zabbix_server
    fields_under_root: true

  - type: filestream
    id: zabbix-agent
    paths:
      - /var/log/zabbix/zabbix_agentd.log
    fields:
      service: zabbix
      log_type: zabbix_agent
    fields_under_root: true
```

L'output permet de renvoyer les logs vers Logstash. Il suffit de donner l'adresse IP du serveur en question, avec le port par défaut 5044.

```
# ================================== Output ==================================

output.logstash:
  hosts: ["172.22.100.11:5044"]
```

1.1.3 Connexion à Kibana

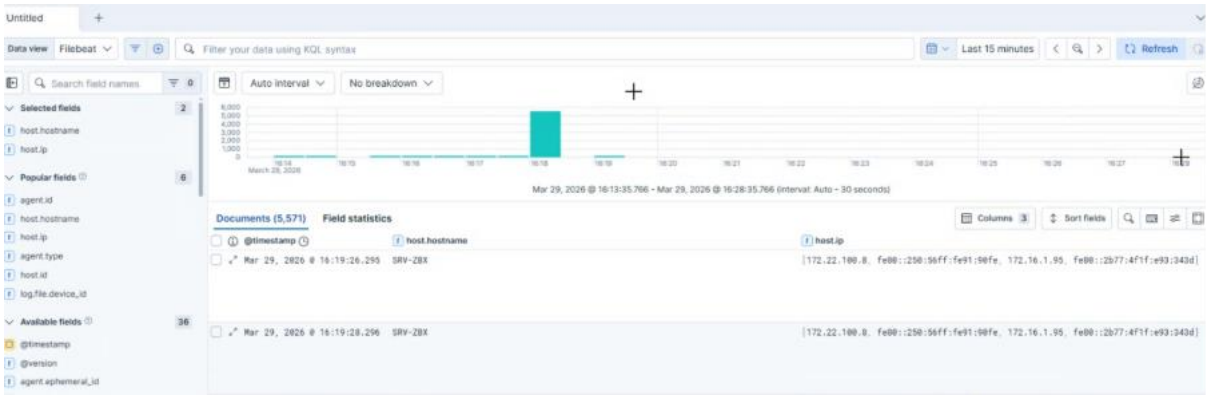
Il faut également définir l'hôte kibana, grâce à son adresse IP et avec le port par défaut 5601

```
# ================================== Kibana

setup.kibana:
  host: "https://172.22.100.11:5601"
```

1.1.4 Setup de Filebeat

Une fois la configuration de Filebeat terminée, il faut effectuer la commande filebeat setup afin de charger les dashboards, mettre en place l'index et finir la connexion entre filebeat et le reste de l'infrastructure.

Une fois cette commande terminée, on peut commencer à voir les logs arriver sur l'interface graphique de Kibana.



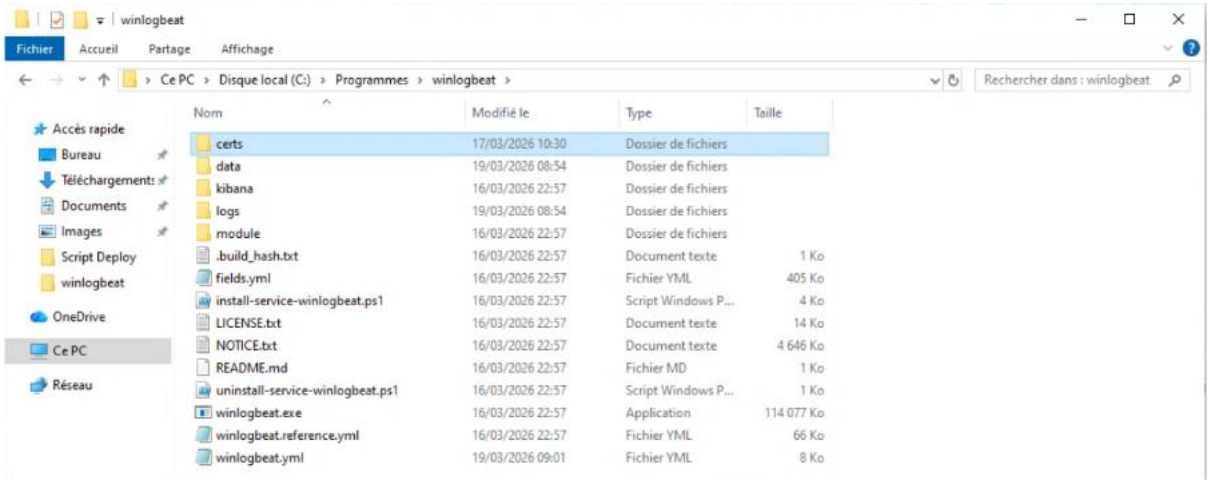
1.2 Winlogbeat

1.2.1 Installation

Winlogbeat fonctionne sur le même principe que Filebeat, mais sous Windows.

Pour l'installer, il faut aller sur : https://www.elastic.co/downloads/beats/winlogbeat

On peut ensuite extraire les fichiers dans C:\Programmes (C:\Program Files si le windows est en anglais), et renommer le dossier en Winlogbeat.



L'installation est donc finie et nous pouvons passer à la configuration.

1.2.2 Configuration

Dans ce dossier, on trouve le fichier winlogbeat qui sert de fichier de configuration de l'agent. C'est notamment ici que l'on va indiquer les informations concernant l'hôte Kibana :

```
# ================================== Kibana ===================================
setup.kibana:
  host: "https://172.22.100.11:5601"
  ssl:
    enabled: true
```

On y indique également les informations pour la cible des logs, donc dans notre cas Logstash.

```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["172.22.100.11:5044"]
```

De la même manière qu'avec Filebeat, on y choisit les logs que l'on enverra vers elasticsearch. Ici, les logs systèmes et de sécurité par exemple.

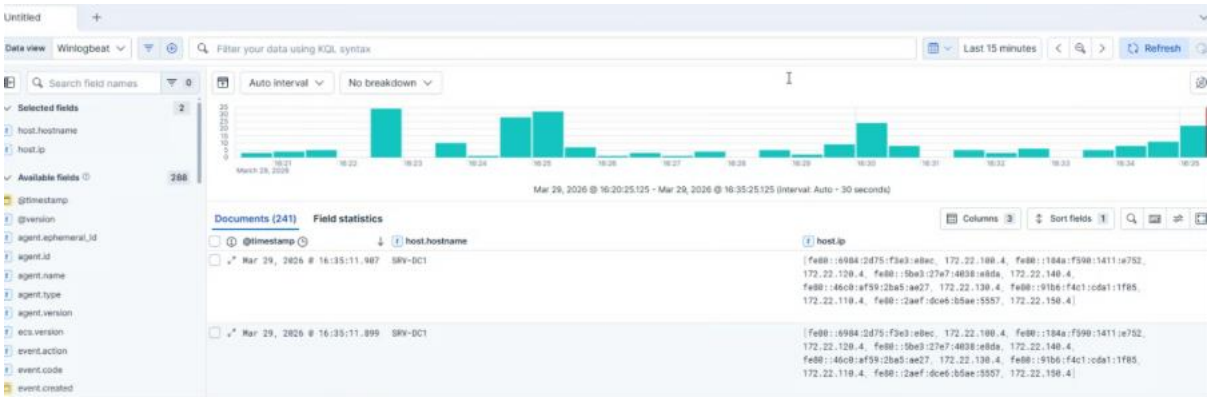
```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

  - name: Security

  - name: Microsoft-Windows-Sysmon/Operational

  - name: Windows PowerShell
    event_id: 400, 403, 600, 800

  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106

  - name: ForwardedEvents
    tags: [forwarded]
```

Une fois la configuration terminée, il faut lancer le script install-service-winlogbeat.ps1 afin d'installer le service Winlogbeat sur la machine Windows client.

Puis, il faut lancer le service avec la commande :

Start-Service winlogbeat

On peut alors observer les logs sur l'interface graphique Kibana



1.2.3 Automatisation de l'installation

Grâce à une GPO qui exécute un script, il est possible d'installer automatiquement winlogbeat sur tous les PC windows du domaine.

Le script permet de copier le dossier d'installation contenant une version configurée du winlogbeat.yml

```
robocopy $source $destination /E /Z /R:3 /W:5
```

Ici, cette ligne permet de copier le dossier et ses sous dossiers (/E), avec une barre de progression (/Z), en réessayant 3 fois maximum (/R:3) et en attendant 5 secondes entre chaque essai (/W:5)

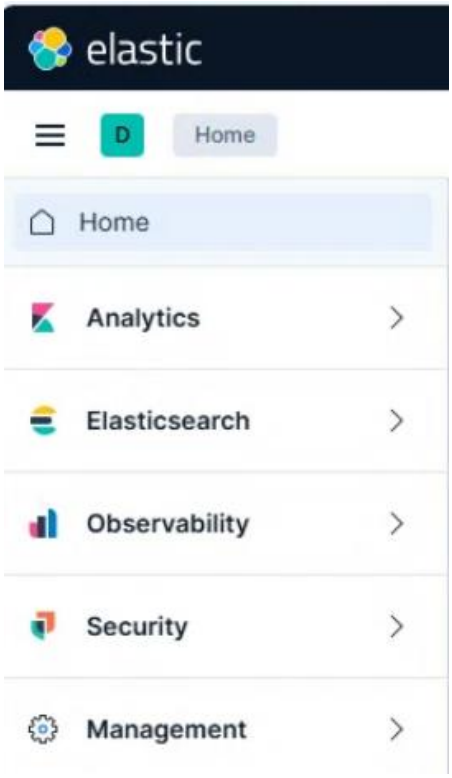
Ensuite, il ne reste qu'à installer et lancer le service, en utilisant le script comme avant.

```
# Installation du service si absent
$service = Get-Service -Name winlogbeat -ErrorAction SilentlyContinue
if (-not $service) {
    Write-Output "Installation du service Winlogbeat..."
    powershell.exe -ExecutionPolicy Bypass -File "$destination\install-service-winlogbeat.ps1"
    Start-Sleep 5
}
```

```
# Démarrage du service
if ($service.Status -ne "Running") {
    Write-Output "Demarrage du service Winlogbeat..."
    Start-Service -Name winlogbeat -ErrorAction Stop
    Start-Sleep 5
}
```

Ainsi, on obtient un client Winlogbeat fonctionnel sans avoir besoin de le faire manuellement.

2. Interface graphique de Kibana



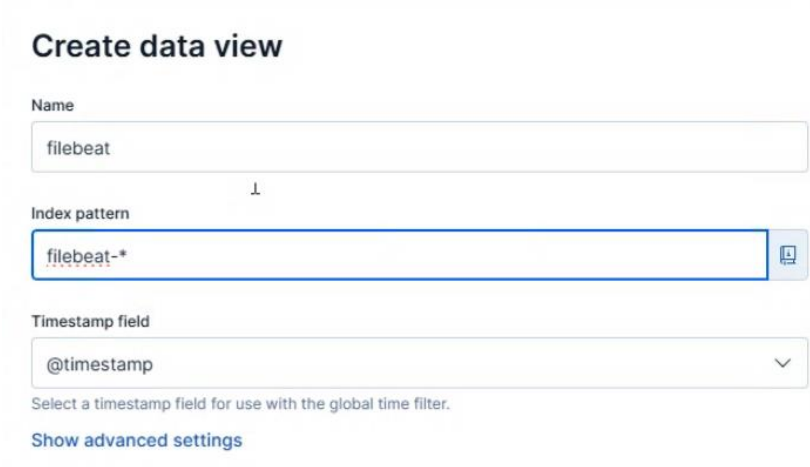
Une fois connecté sur l'interface graphique de Kibana, on peut voir ce menu. Analytics nous permettra de créer des visualisations des logs, sous forme de graphiques ou de tableaux. C'est ici que l'on exploite les données.

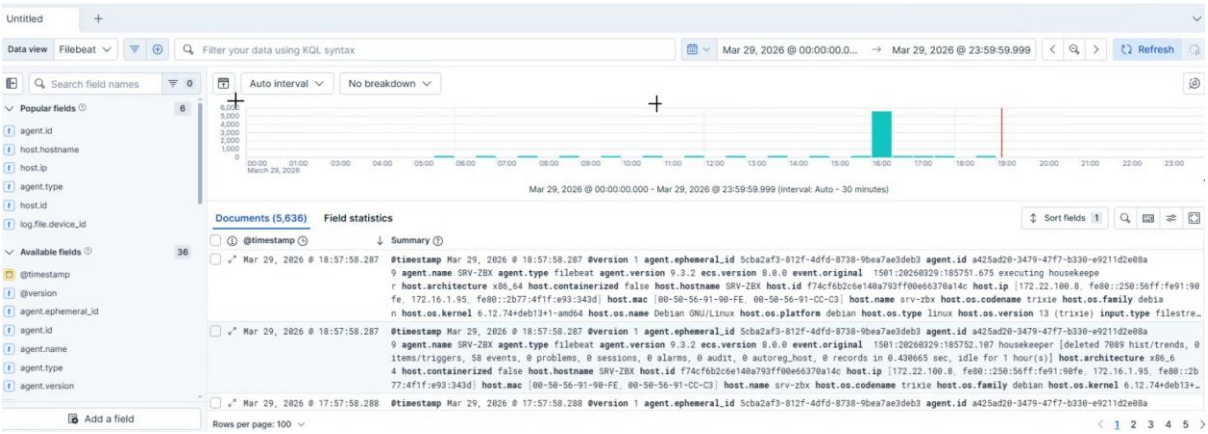
Elasticsearch permet de gérer les index, et est utilisé pour debug et administrer la partie elasticsearch.

Observability permet notamment de voir les Alertes, traquer les métriques importantes de certaines applications.

Security permet d'analyser les évènements de sécurité, notamment les détections d'intrusions. Management permet de configurer la stack ELK dans sa globalité, les utilisateurs et les rôles par exemple.

2.1 Créer une Visualisation de données



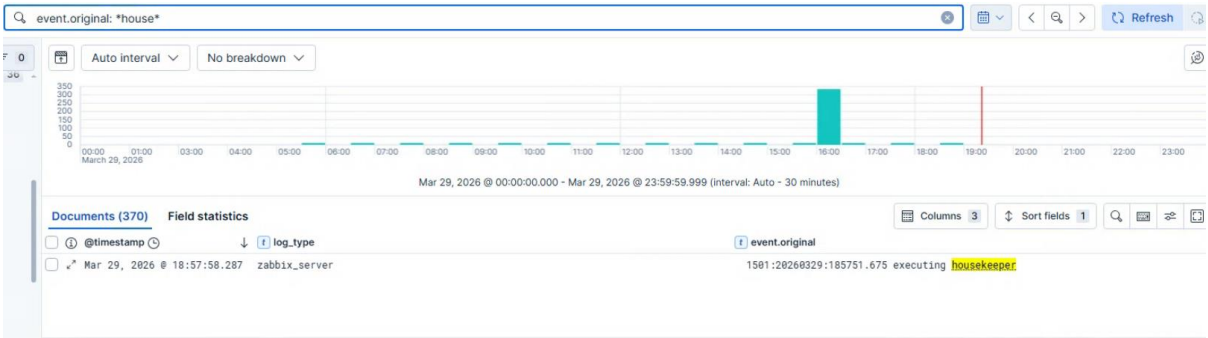


Chacun des champs nous permet de filtrer nos logs, pour par exemple n'afficher que ceux provenant d'une certaine IP avec ce filtre : host.ip: 172.22.100.8

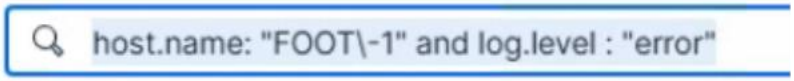
On peut également chercher dans le contenu du log en lui-même, avec ce filtre :

Event.original: *contenu*

Par exemple :



Un filtre un peu plus intéressant et plus compliqué serait celui-ci :

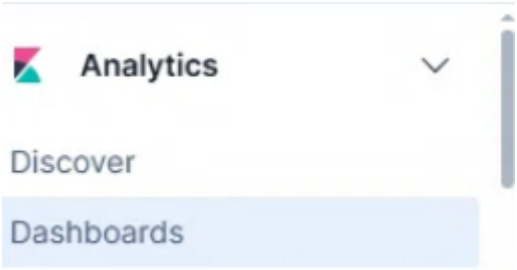


Il permet de vérifier les erreurs sur un pc en particulier, ce qui serait pratique notamment pour un service de support informatique. On notera que pour chercher le hostname “FOOT-1”, il faut mettre un antislash “\” devant le tiret “-” pour qu’il soit bien pris en compte comme un caractère.

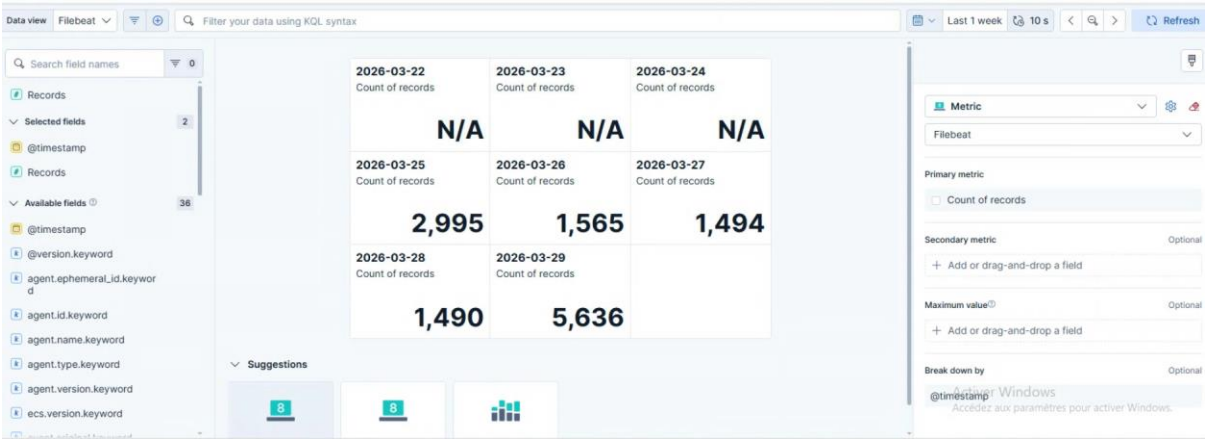
Note : les filtres sont effectués via le langage KQL (Kibana Query Language)

2.2 Créer un Dashboard

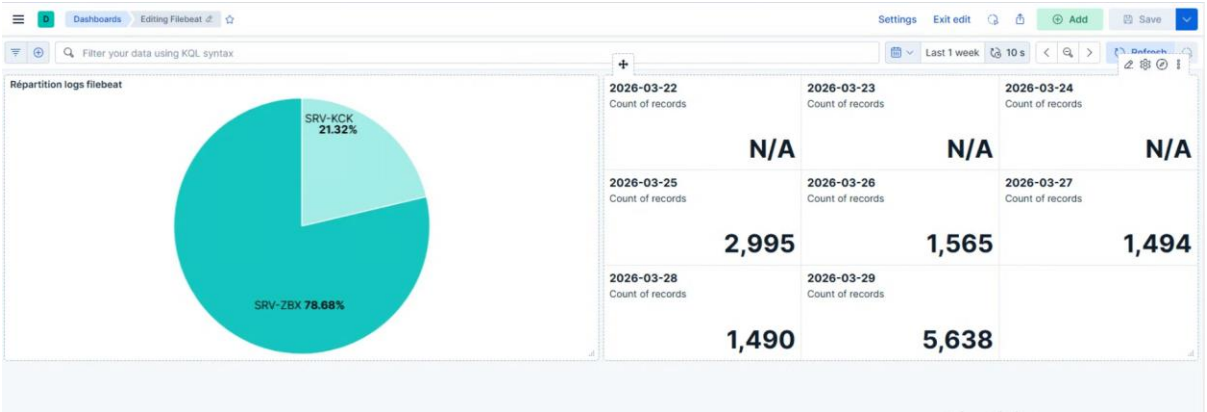
Un Dashboard permet de configurer et regrouper plusieurs visualisations de logs. Pour en créer un, il faut aller dans Analytics > Dashboards :



On peut ensuite cliquer sur Create Dashboard. On a ensuite la possibilité de créer plusieurs visualisations, qui seront ensuite visibles côte à côte. Par exemple, le cas de Filebeat, on peut créer une visualisation de la répartition des logs en fonction de la source, ou alors le nombre de logs par jour :



On obtient un résultat comme celui-ci :

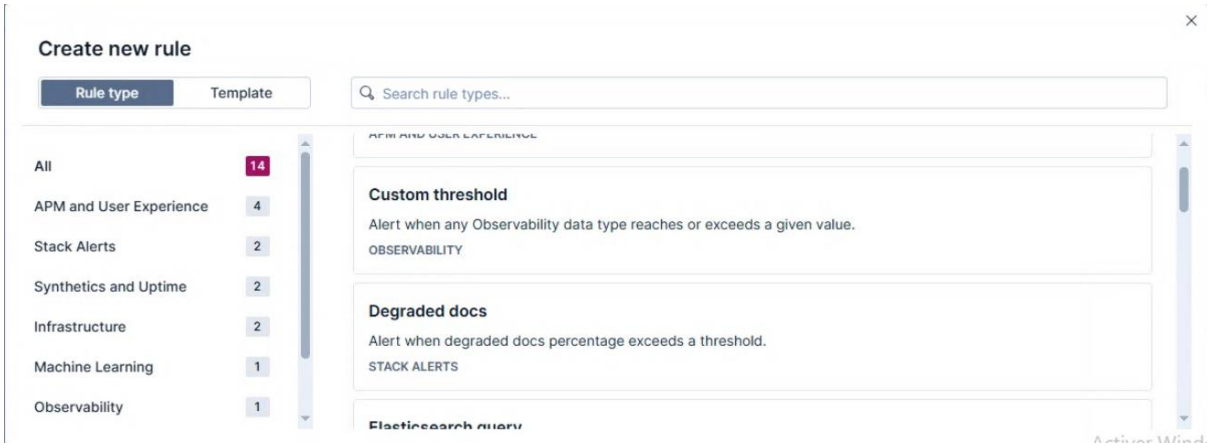


On peut ensuite sauvegarder, et il sera alors visible dans la liste des dashboards. Cela permet de visualiser rapidement des informations dont on a souvent besoin.

2.3 Créer une alerte

Il est également possible de créer une alerte, pour surveiller certaines erreurs, ou certains logs en particulier. Par exemple, on peut créer une alerte en cas de connexions Windows infructueuses trop nombreuses.

Pour cela, on va dans Observability > Alert, puis Manage Rules et Create Rules. On choisit ensuite un type de règle, ici “Custom Threshold” :



On peut ensuite définir la vue utilisée, un filtre, et des conditions d’alerte.

Dans le cas d’une alerte sur les connexions Windows infructueuses, on utilise la vue Winlogbeat, qui répertorie tous les logs provenant d’un client Winlogbeat, donc un client Windows. On utilise le filtre event.code: 4625, qui correspond à une connexion échouée. Ensuite, on indique que l’alerte se déclenche après plus de 10 connexions échouées dans la dernière minute.

De cette manière, on peut observer les alertes, ou l’historique d’exécution des alertes.

Une autre alerte du même type dont on peut avoir besoin dans le cadre de TrueNAS est une alerte sur les erreurs de connexions aux partages.