# Les alertes Splunk



## 1. Sur quoi ce base les alertes

### 1.1 Le fonctionnement de splunk

Splunk permet de voir et d'analyser un fichier sur une machine extérieure depuis le bastion, à sa connexion aux autres machines. Il faut cependant préciser l'index (ou il doit regarder en premier), exemple: **index=portail_digital**. Il faudra ensuite indiquer le chemin absolue (D:\\...) avec l'attribut **source="***le_chemin_de_votre_fichier***"**.

### 1.2 Les erreurs dans les logs

La plus part du temps les erreurs de logs se manifestent (si bien configuré) par 1 statut: Error

```
2025-06-01 09:03:16.9111|Error|
2025-06-01 09:03:16.9901|Error|
```

**Cependant il faudra nuancer les Erreurs coté utilisateurs et les Erreurs cotés batch:**

```
2025-05-08 08:10:22.1774|Error|- Erreur pour le numPers
```

Ici une erreur coté utilisateur

2025-06-03 20:00:12,271 ERROR Batch.EnvoiNotifications.Program: Fin du batch - Erreur lors de l'execution du batch. D\xE9tail de l'erreur : An error occurred while sending the request.- The underlying connection was closed:

Ici une erreur coté batch

## 2. Les spécificités des alertes

Chaque batch nécessite une attention particulière: dans la forme les erreurs ce manifeste de manière similaire, dans le fond parfois il faut s'adapter au batch.

### 2.1 Les erreurs classiques

On retrouve la mise en place d'un relevé d'erreurs classique avec simplement le mot Error comme sujet de recherche `index=portail_digital source="D:\\..." Error`

### 2.2 Les erreurs spécifiques

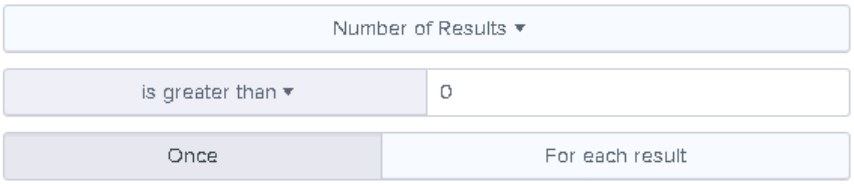
Pour les logs de batchs qui s'effectuent dans un fichier de logs ou plusieurs programme ce mélange on va sélectionner le mot d'echec du batch ainsi que le nom de programme du batch (on le trouve aux heures ou il s'exécute): `index=portail_digital source="D:\\..." Error "Midiway.Portal.Api.Adherent.Prestations.AbonnementPrestationsController"`

### 2.3 Les exclus

Parfois il faut exclure des mots de la requête Splunk qu'on sait qu'on ne retrouvera pas lors de l'erreur d'exécution d'un batch: du coup on va prendre les lignes ou il y a Error mais pas avec "adhérent" ou autre personnification ("numPers", ...). Pour cela on va utiliser NOT qui permet d'exclure un mot ou groupe de mot de la requête. Exemple: `index=portail_digital source="D:\\..." "Error" NOT "adhérent"`

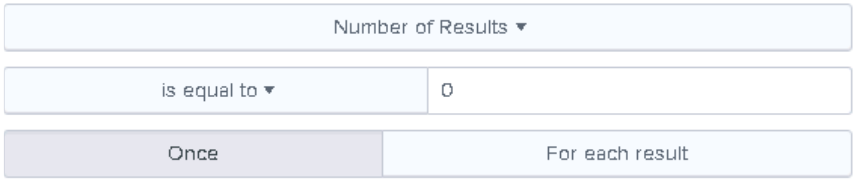
### 2.4 Les riens

Ils sont rares, mais parfois les batchs ne donnent pas de logs quand ils sont en erreur, c'est à dire que quand ils réussissent pas le lancement rien ne s'affiche. On peut donc mettre en place une alerte simple de lecture sauf que dans le paramétrage de l'alerte on change la case:




"Is greater than"

**Par la case:**



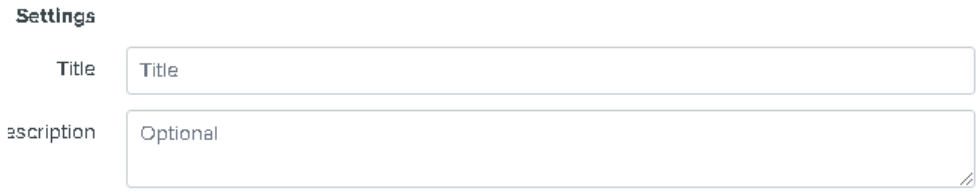

"Is equal to"

Cela permet lorsque la requête ne lit aucun résultat (si le fichier est vide ou s'il n'a pas été crée) d'envoyer une alerte.

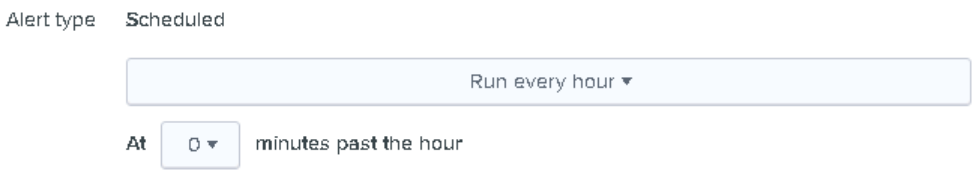
# 3. La création d'une alerte

Passons maintenant à la création d'une alerte dans Splunk.

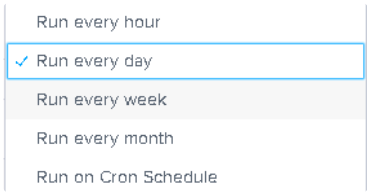
### 3.1 Le titre et la description




### 3.2 La date d'exécution




On a le choix entre: toutes les heures à une minute qu'on définis; chaque jour à une heure qu'on définis; chaque semaine à un jour définis et une heure définis; chaque mois à un jour définis et une heure définis; *le Run on Cron Schedule fait l'objet de l'annexe 1*



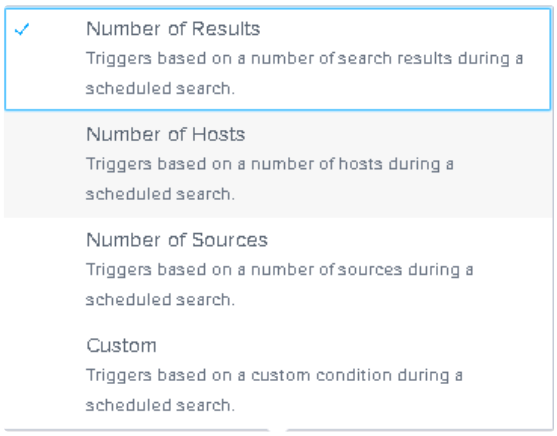

La fonction Expires (ci-dessous), est le temps maximal que Splunk garde la requête pour la rejouer si elle ne s'est pas exécuter en cas d'embouteillages dans la liste d'attente. Cela est à configurer celons vos besoins.


### 3.3 La condition


Cela correspond à la condition la requête va s'exécuter, par exemple ici celons le nombre de résultat qui est supérieur à 0 *(le 0 est modifiable en cliquant dessus)*, alors déclenché l'alerte 1 fois pour tout les résultat de la requête.

### 3.3.1 When

Cela représente la condition de lancement du début, on peut le comparer au mot celons.




> Pour les alertes sur les batchs j'ai utilisé le Nomber of Results car il permet une précision supérieur à 0 sur les résultats de recherche.

### 3.3.2 Triger Once ou Trigger For each result

Imaginons que le résultat de la requête est de 15: Triger once permet de déclencher une fois l'alerte pour les 15 résultat et renverras les 15 lignes 1 fois (pratique pour l'envoie de mail et de .pdf car cela évite le spam sur la boite de réception ).

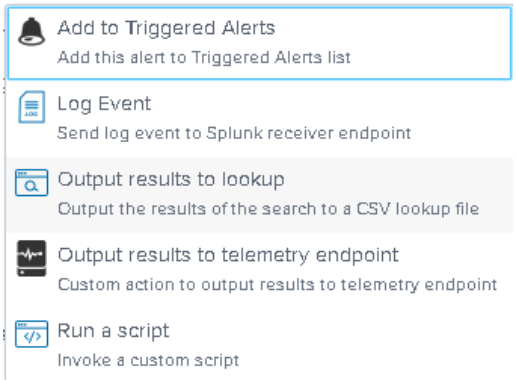
Trigger For each result vas déclencher l'alerte pour chaque ligne de la requête (ici 15 fois l'alerte s'affichera).

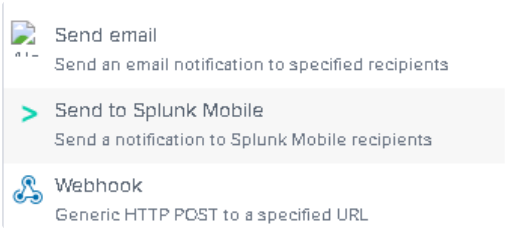
### 3.3.3 Throttle

C'est une fonction qui va permettre de limiter la fréquence d'exécution d'une alerte (même si les conditions d'exécution sont remplies), elle est souvent utilisée pour "calmer" une recherche en For each Results. On peut choisir le temps d'attente avant une nouvelle exécution de l'alerte en secondes ou minutes ou heures ou jours.


### 3.4 L'action

Cela correspond à ce que va déclencher votre alerte si elle obtient le résultat attendu. On peut voir différentes options:






Chaque options est paramétrable.

> Comme je me suis focalisé sur l'envoie de mail, l'annexe 2 explique sa configuration.

## 4. Les alertes mises en place

Pour voir les alertes déployées, il faut ce rendre sur le git: https://itgit.emea.cegedim.grp/it-security/splunk-cis/-/blob/CIS-Files/SHD_ALL_CIS-PoleDigital-extranet/local/savedsearches.conf

> Les alertes déployées sont sous code git, ce qui rends les requêtes beaucoup plus flexible au niveau du paramétrage.

Sur le git on retrouve aussi les fichiers .csv (https://itgit.emea.cegedim.grp/it-security/splunk-cis/-/tree/CIS-Files/SHD_ALL_CIS-PoleDigital-extranet/lookups) qui servent à mes inputloookup pour faire des stats sur les erreurs à l'intérieur des logs (voir dashboard Splunk: https://splunk-et1.cegedim.com/en-US/app/SHD_ALL_CIS-PoleDigital-extranet/erreurs_logs)

## Annexe 1: Le Run on Cron Schedule

Ce processus lors de la customisation de la date d'éxecution de l'alerte permet un paramètrage plus approfondis: par exemple on peut configuré une alerte du lundi au vendredi à 03h30 (on peut configuré à la minute près).


Le champ ce paramètre comme cela:

*  *  *  *  *

minutes  heures  jours(du mois)  mois  jours( de la semaine)

Les différents séparateurs:

* = toutes les valeurs

, = liste de valeurs (ex tout les lundis, mardis, mercredis: * * * * 1,2,3)

– = c’est une plage (ex de lundi à vendredi: * * * * 1-5)

/ = incrément (ex toutes les 5 minutes: */5 * * * * )

(ex toutes les 2 heures: 0 */2 * * * )

On peut aussi combiner les différents opérateurs, exemple:

Aux 10, 20, 30, 40, 50 minutes de chaque heures: 10-50/10 * * * *

Toutes les 2 heures, entre 8h et 18h, du lundi au vendredi: 0 8-18/2 * * 1-5

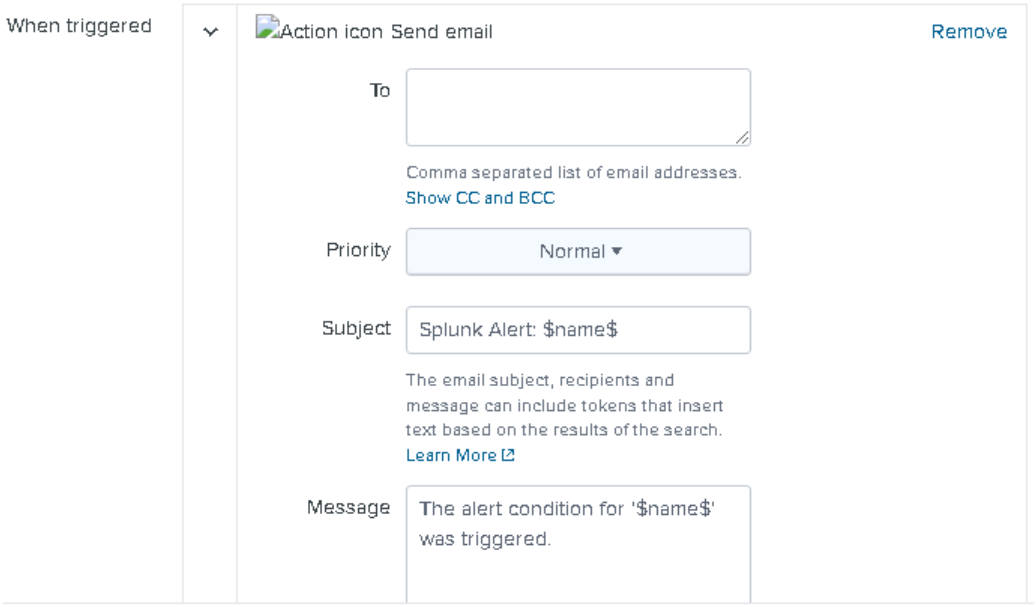
Pour essayer le cron rentré lors d’une requête on peut aller sur **crontab.guru**, on rentre ensuite le cron est une “traduction” sera disponible.

On peut aussi choisir depuis quand on veut que l’alerte s'exécute pour avoir des résultat antérieur.

## Annexe 2: L’envoie par mail

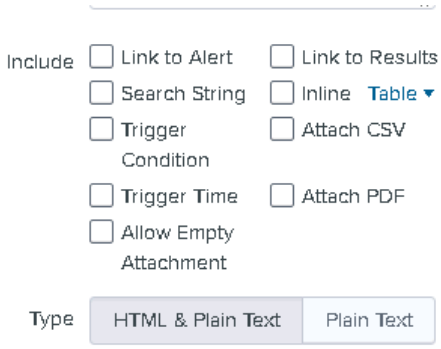
L’envoie par mail est une action à exécuter en cas de déclenchement d’une alerte. L’option se distingue en 2 parties distinctes: 1 le corps du mail et 2 les options rattachées au mail.

### 1. Le corps du mail




Rien de plus classique: on choisit le destinataire en premier, on choisit ensuite la “priorité” du mail (entre: lowest, low, normal, high, highest). On choisit ensuite le subject (objet) et on rentre ensuite le message que l’on veut afficher lorsqu’on reçoit le mail. A noté que ces différents champs texte peuvent prendre en compte des variables pour simplifier la configuration.

### 2. Les options du mail




**Include permet d'ajouter du contenu à votre mail:**

Link to Alert = ajoute un lien vers l'alerte dans Splunk (vers sa configuration pas son résultat)

Link to Results = ajoute un lien vers le résultat de la requête

Search String = ajoute la requête de déclenchement de l'alerte

Inline =

- Table = résultat directement dans le corps de l'email sous forme de tableau
- Raw = résultat directement dans le corps de l'email sans formatage, sans tableau
- CSV = format CSV

Trigger Condition = affiche la condition d'exécution de l'alerte dans le mail

Attache CSV = affiche le résultat de l'alerte dans un fichier .csv

Trigger Time = ajoute la date exacte de l'exécution de l'alerte

Attach PDF = affiche le résultat de l'alerte dans un fichier .pdf

Allow Empty Attachement = même si l'alerte n'a aucun résultat cela va quand même envoyer le mail, et si une PJ est inclue habituellement, elle sera générée mais sera vide.

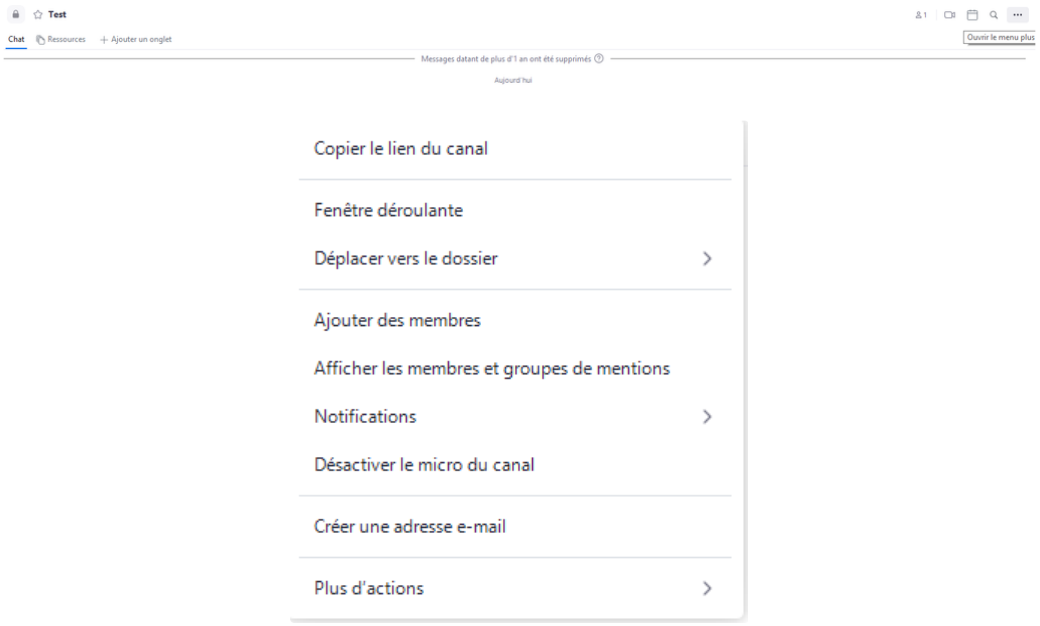
**Type ce distingue en 2 options :**

- HTML & Plain Text:
  - Cela permet d'avoir une version HTML (si possible) du mail et une version texte. A sélectionné si il y a un envoie de liens, des tableaux ou encore des fichiers pour une compatibilité maximale.
- Plain Text:
  - Cela permet d'avoir uniquement une version texte du mail avec aucune spécificités (pas de gras rien). Très limités, je recommande d'utiliser cette option pour du monitoring très simple (pas de PJ, pas de couleur, ...).

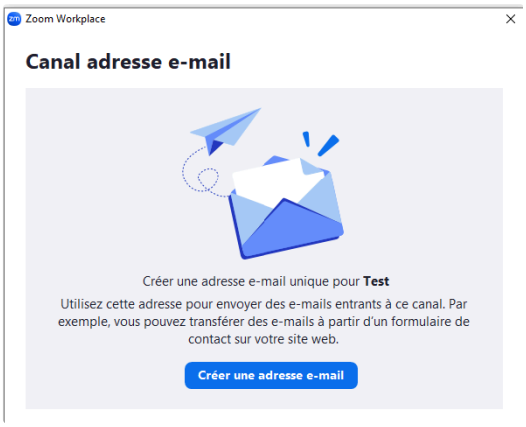
## Annexe 3: L'attribution d'un mail à un canal zoom

Un canal zoom peut obtenir une adresse mail, on peut ensuite ce servir de celle-ci pour recevoir les alertes sans avoir besoin d'aller consulter sa boite mail en permanence. Pour ce faire on se rends sur le canal zoom visé:

On clisk sur les ...



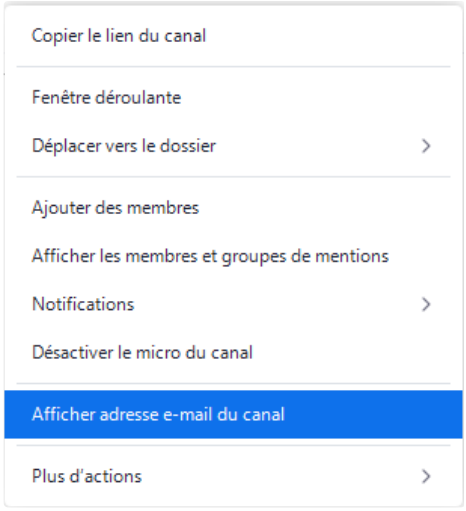

Puis sur “Créer une adresse mail”




On confirme

Et ensuite on peut copier l’adresse mail pour ainsi la rentrée dans l’alerte lors du paramétrage de mails.


Pour afficher l’adresse mail du canal après la création de celle-ci, il suffit juste de suivre la procédure depuis le début et à la place de “Créer une adresse mail” cela affichera “Afficher adresse mail du canal”.


Copier le lien du canal
Fenêtre déroulante
Déplacer vers le dossier
Ajouter des membres
Afficher les membres et groupes de mentions
Notifications
Désactiver le micro du canal
Afficher adresse e-mail du canal
Plus d'actions