**Splunk**

Serveurs :

S00vl9978211 : Machine de Dev.

s00vl9982387 : Machine de Préprod.

URL DEV : <https://10.244.162.83:10080/fr-FR/account/logout>

URL PREPROD: [https:// 10.244.28.120:10080/fr-FR/account/logout](https://10.244.162.83:10080/fr-FR/account/logout)

Login/MdP : admin/azerty

**Expression de l’affichage**

**index="sauron\_test" |eventstats first(resultat) as test1 by source | eval test=if(test1="Listener is not running","Listener KO","") | eventstats first(test) as result by source | table result,application,site,hostname,\_time,source | search result="Listener KO" | rename result as "Status" | dedup source**

**index="sauron\_test"** =>appel de l’index

**|eventstats first(resultat) as test1 by source** => aggregation du premier résultat de l’index qu’on nomme test1 et qu’on filtre par source.

**| eval test=if(test1="Listener is not running","Listener KO","")** => On créée une variable “test” on test si il est “Listener is not running” alors “Listener KO” ou NULL.

**| eventstats first(test) as result by source** => Je reprends ma variable “test” que je classe par source que je nomme « result ».

**| table result,application,site,hostname,\_time,source** => J’affiche “result, application…”

**| search result="Listener KO"** => Je ne prends que “Listener KO”

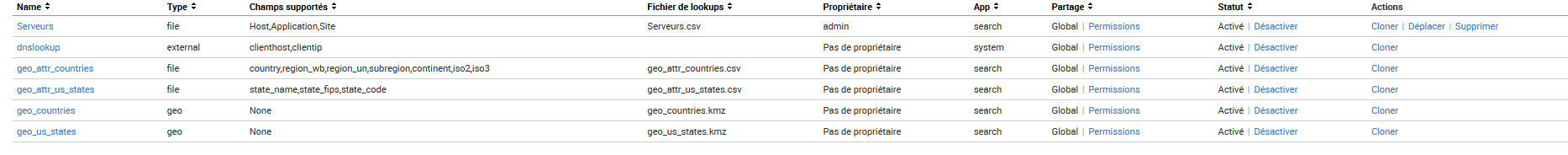
**| rename result as "Status"** => Renomme mon result “Status”

**| dedup source** => Ne prendre qu’un seul résultat (disctinct)

**Regex (regular expression de la log pour Splunk)**

**Date:\s+(?P<date>[^\,]+),\sSujet :\s+(?P<sujet>[^\,]+),\sResultat :\s+(?P<resultat>[^\,]+),\sHostname :\s+(?P<hostname>[^\,]+), Site :\s+(?P<site>[^\,]+), Application :\s+(?P<application>[^\,]+)**

Lookup :





Définition :



## Mise en forme des tableaux.

# SVMON

To display global report in terms of GB.

svmon -G -O unit=GB

To list top 10 processes utilizing the memory.

svmon -P -O summary=basic,unit=auto -t 10

To list top 10 users utilizing the memory.

svmon -U -O summary=basic,unit=auto -t 10

Affichage :

source="/apps/sauron/log/atlaslog/\*.log.\*" host="s00vl9978211" index="sauron\_test" sourcetype="Sauron:atlaslog" "Fin de job" | stats values(RC) as CODE by source | where CODE!=0

Ajout d’un CSV pour les références machine Application SITE.

Paramètres => Lookup (import d’un fichier csv) => Définition du lookup => Lookup automatique remplir les champs. (Host=Host ; Application=Application ; Site=Site)

1 CSV à entrer autant de fois qu’il y a de lookup par source.

**Vérification d’une base en dataguard.**

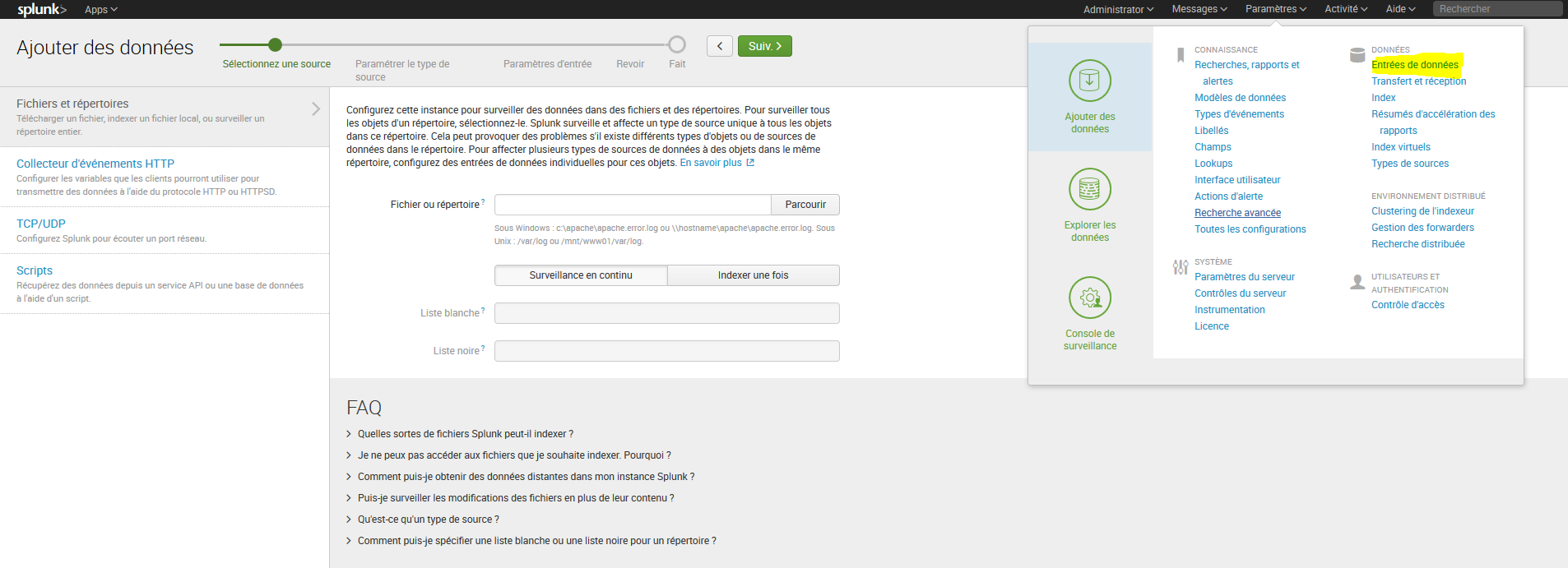
[PRIMARY] sys@P10716AP1 SQL> SELECT DATABASE\_ROLE, DB\_UNIQUE\_NAME INSTANCE, OPEN\_MODE, PROTECTION\_MODE, PROTECTION\_LEVEL, SWITCHOVER\_STATUS FROM V$DATABASE;

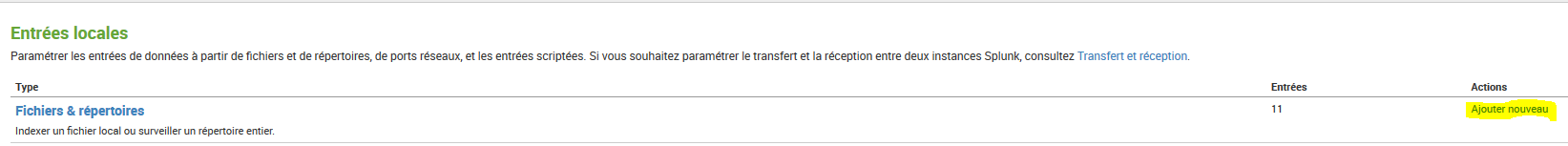
DATABASE\_ROLE INSTANCE OPEN\_MODE PROTECTION\_MODE PROTECTION\_LEVEL SWITCHOVER\_STATUS

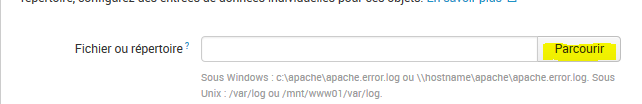
---------------- ------------------------------ -------------------- -------------------- -------------------- --------------------

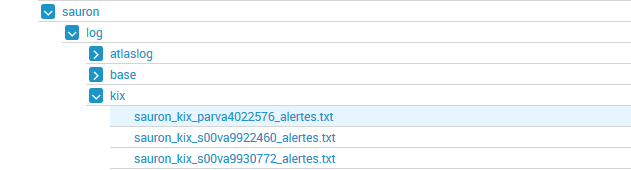
PRIMARY P10716AP1 READ WRITE MAXIMUM PERFORMANCE MAXIMUM PERFORMANCE TO STANDBY

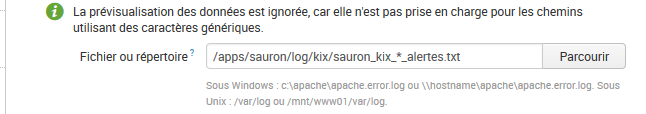
## Ajout d’une nouvelle donnée :

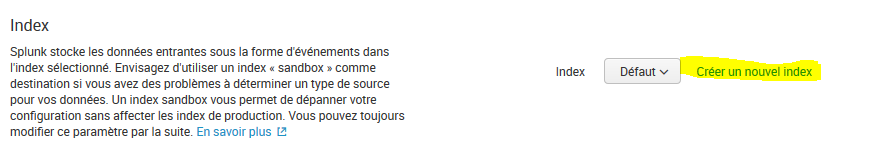


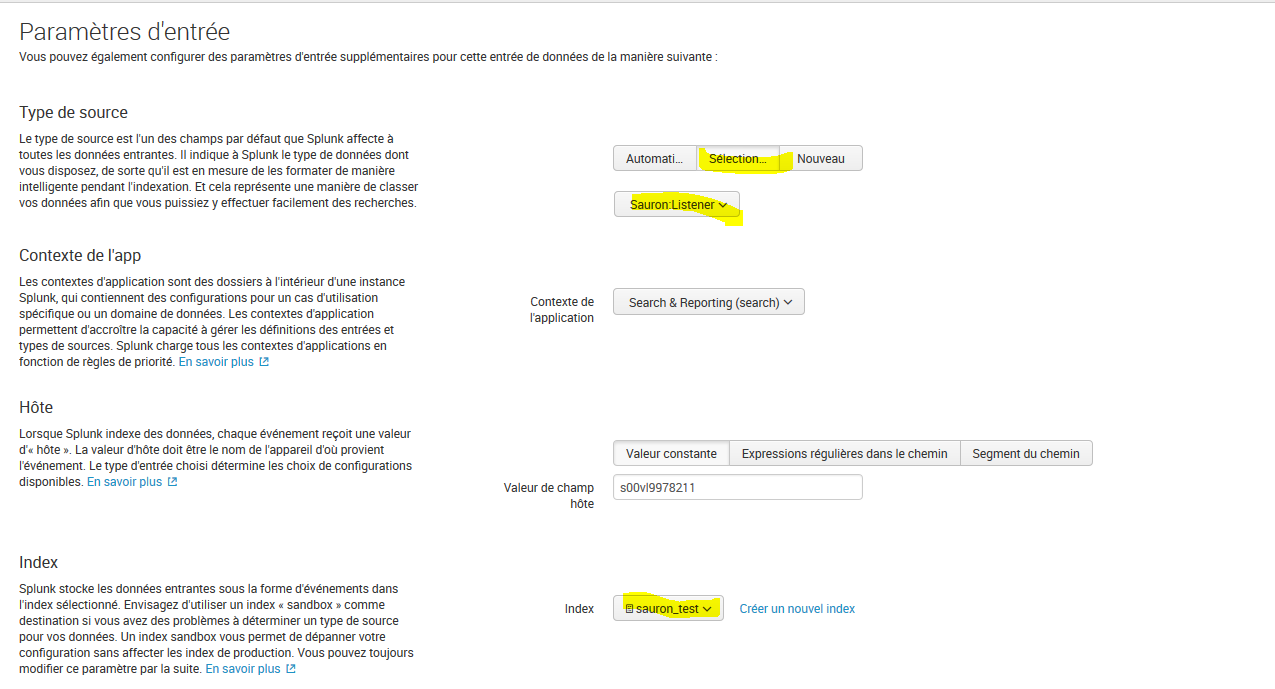












### recherche

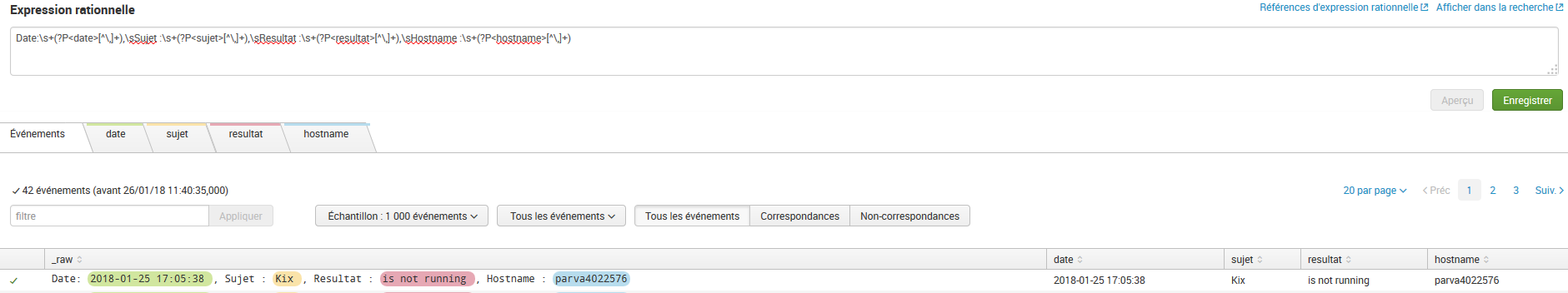
**source="/apps/sauron/log/kix/sauron\_kix\_\*\_alertes.txt" host="s00vl9978211" index="sauron\_primaire" sourcetype="sauron:alertes\_all" source="\*"**





Regex

**Date:\s+(?P<date>[^\,]+),\sSujet :\s+(?P<sujet>[^\,]+),\sResultat :\s+(?P<resultat>[^\,]+),\sHostname :\s+(?P<hostname>[^\,]+)**



**Terminer**

## Arrêt reliance status de splunk

root@s00va9930772:/apps/splunkforwarder/bin$ ./splunk status

splunkd is running (PID: 18088186).

splunk helpers are running (PIDs: 57147638).

**Stop**

/usr/bin/stopsrc -s splunkd

**Start**

/usr/bin/startsrc -s splunkd

## Autres méthode

|  |
| --- |
| **mkssys -G splunk -s splunkd -p /apps/splunkforwarder/bin -u** **splunk -a \_internal\_exec\_splunkd -S -n 2 -f 9** 0513-071 The splunkd Subsystem has been added.  **./splunk enable boot-start** 0513-071 The splunkd Subsystem has been added. SRC subsystem group installed. SRC subsystem group is configured to run at boot. |

## Configuration forwarder :

### Sur le serveur splunk

root@s00vl9982387:/apps/splunk/bin$ ./splunk enable listen 9997

Splunk username: admin

Password:

Listening for Splunk data on TCP port 9997.

### Sur le serveur qui doit forward

root@s00va9930772:/apps/splunkforwarder/bin$ ./splunk add forward-server 10.244.28.120:9997

Splunk username: admin

# Deploiement

#### Déployer le script par site (attention au hostname)

#### Donner les droits au script

#### Créer le dossier log

#### Mettre sous crontab

#### Modifier le fichier inputs.conf de splunk dans /apps/splunkforwarder/etc/apps/bigdata\_em\_sauron\_uf/local

#### Faire un arrêt relance du forwarder.

# Props et transforms

root@s00vl9982387:/apps/splunk/etc/system/local$ vi transforms.conf

[setnull]

REGEX=.

DEST\_KEY=queue

FORMAT=nullQueue

[setparsing]

REGEX=Fin de job

DEST\_KEY=queue

FORMAT=indexQueue

root@s00vl9982387:/apps/splunk/etc/system/local$ vi props.conf

[Sauron:Fs]

DATETIME\_CONFIG =

NO\_BINARY\_CHECK = true

category = Personnaliser

pulldown\_type = 1

[Sauron:Cft]

DATETIME\_CONFIG =

NO\_BINARY\_CHECK = true

category = Personnaliser

pulldown\_type = 1

[Sauron:Atlaslog]

TRANSFORMS-set=setnull,setparsing