

I] Installation de Splunk Enterprise sous Windows (usage perso)

0- on n'est pas obligé d'avoir une bête de course pour installer Splunk Enterprise pour découverte / démo en utilisation mono-utilisateur :

<https://docs.splunk.com/Documentation/Splunk/8.1.0/Capacity/Referencehardware>

Malgré tout :

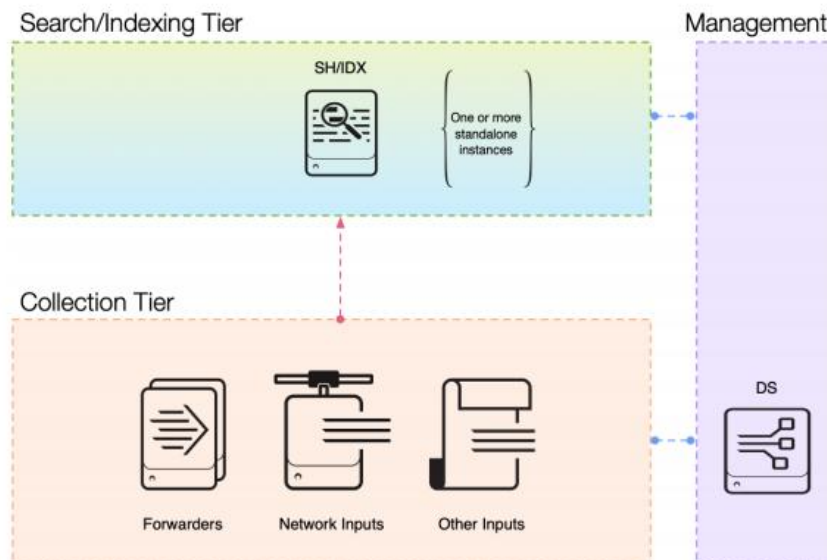
Reference host specification for single-instance deployments

This represents the minimum basic instance specifications for a production grade Splunk Enterprise deployment. A single-instance represents an S1 architecture in SVA:

- An x86 64-bit chip architecture
- 12 physical CPU cores, or 24 vCPU at 2Ghz or greater speed per core.
- 12GB RAM.
- For storage, see [What storage type should I use for a role?](#)
- A 1Gb Ethernet NIC, optional 2nd NIC for a management network .
- A 64-bit Linux or Windows distribution. See [Supported Operating Systems](#) in the *Installation Manual*.

SVA = Splunk Validated Architecture : <https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf>

Single Server Deployment (S1)



Spécifications de l'appareil

Nom de l'appareil	DESKTOP-N9FH26V
Processeur	Intel(R) Core(TM) i7-4800MQ CPU @ 2.70GHz 2.70 GHz
Mémoire RAM installée	32,0 Go
ID de périphérique	D84EC0CC-153B-4CD2- B382-58835B102CA5
ID de produit	00331-60000-00000-AA870
Type du système	Système d'exploitation 64 bits, processeur x64
Styllet et fonction tactile	La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran

Renommer ce PC

Spécifications de Windows

Édition	Windows 10 Professionnel N
Version	1909
Installé le	15/02/2020
Version du système d'exploitation	18363.1198

1- on télécharge le msi sur le site SPLUNK (demande création de compte – parfois pas possible avec mails exotiques – Peu de spams)


[https://www.splunk.com/en_us/download/splunk-enterprise.html?utm_campaign=bing_emea_tier1_en_search_brand&utm_source=bing&utm_medium=cpc&utm_term=%2Bsplunk%20%2Bdownload&utm_content=Splunk Enterprise Demo&bt=71193491264909](https://www.splunk.com/en_us/download/splunk-enterprise.html?utm_campaign=bing_emea_tier1_en_search_brand&utm_source=bing&utm_medium=cpc&utm_term=%2Bsplunk%20%2Bdownload&utm_content=Splunk+Enterprise+Demo&bt=71193491264909)





Splunk Enterprise 8.1.0

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

 Windows

 Linux

 Mac OS

64-bit


Windows 10

Windows Server 2016, 2019

.msi

286.79 MB

Download Now




[Release Notes](#) | [System Requirements](#) | [Older Releases](#) | [All Other Downloads](#)

Voir pour les requirements :

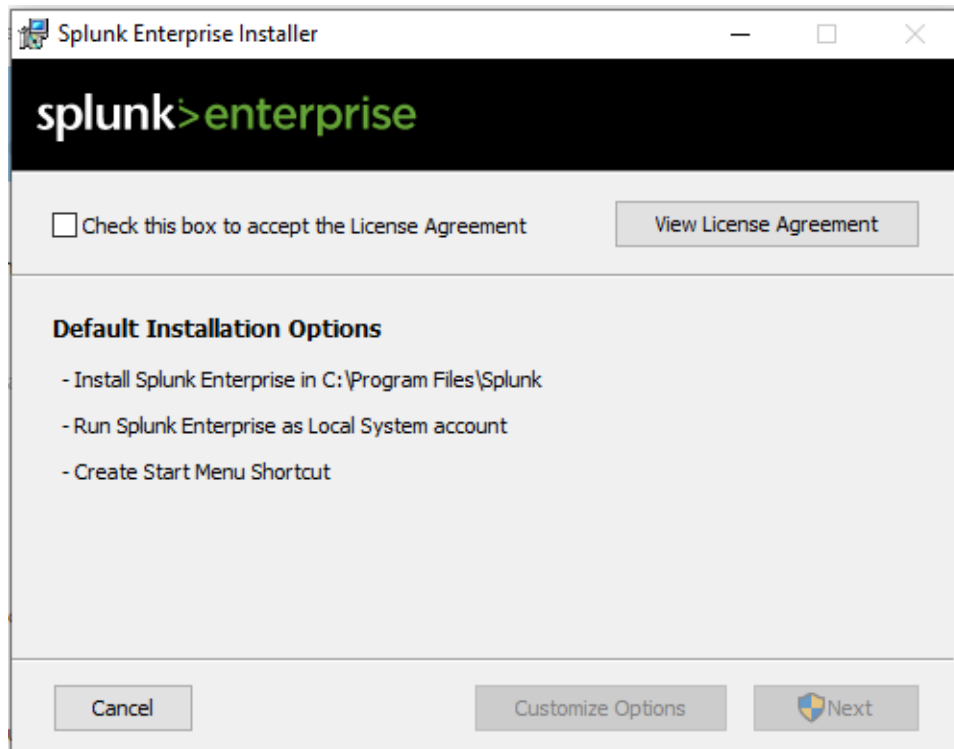
https://docs.splunk.com/Documentation/Splunk/latest/Installation/Systemrequirements#Recommended_hardware

Et possibilité d'installer VMs (attention baisse de perf) ou images Docker

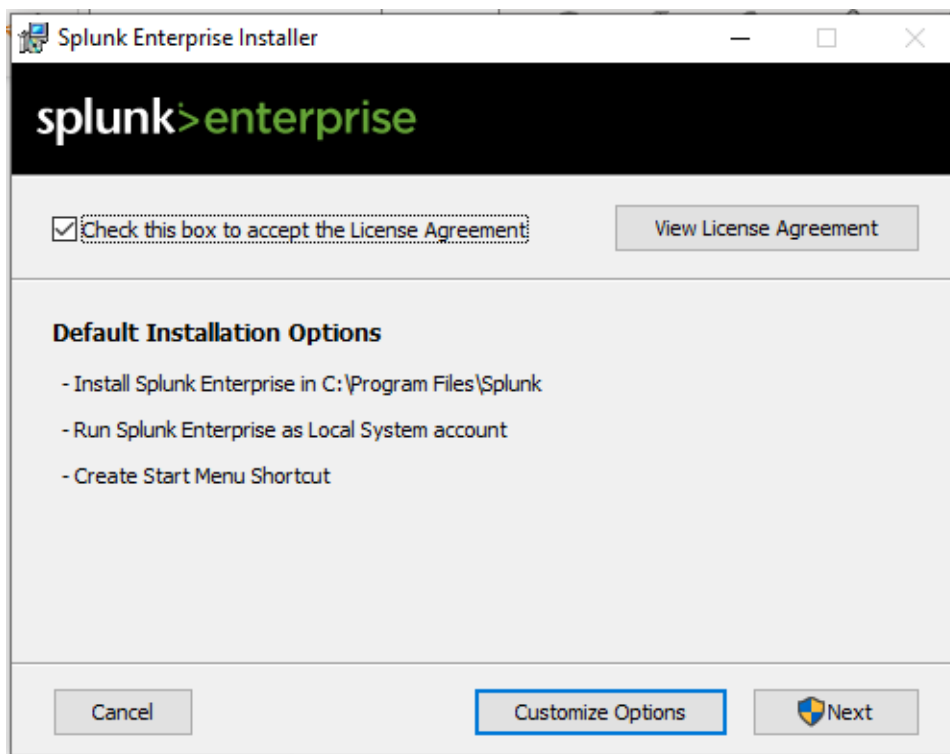
(<https://hub.docker.com/r/splunk/splunk/>.)

Aujourd'hui (1)			
 splunk-8.1.0-457c09e87251-x64-release	20/11/2020 08:49	Package Windows In...	293 668 Ko

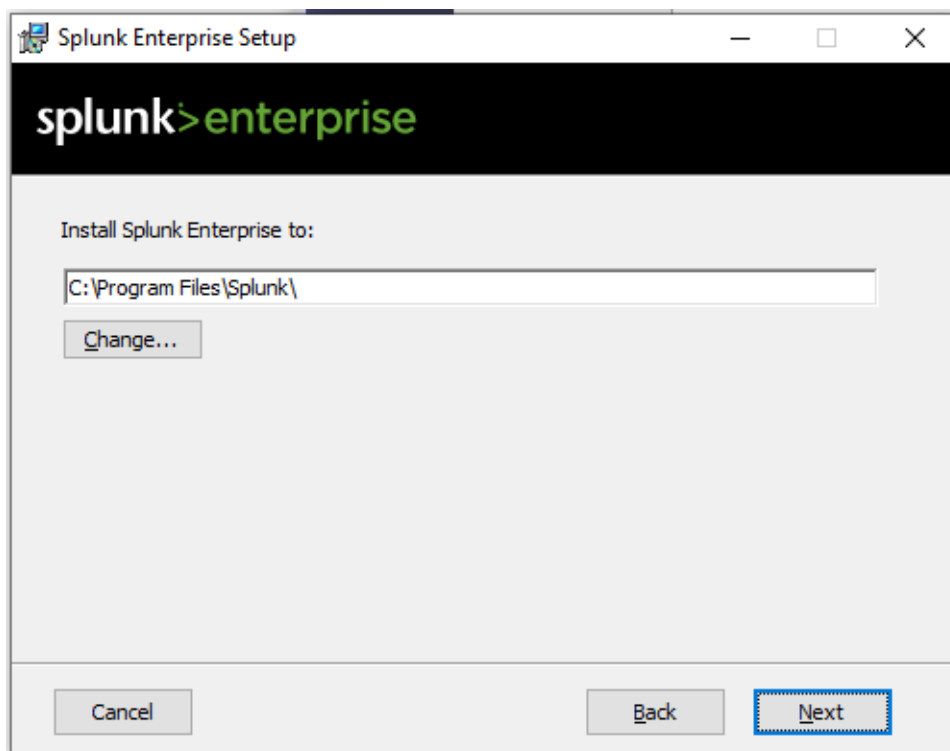
Traditionnellement, on fait clic, clic, clic et ça a l'air de marcher ... mais on n'a rien compris.



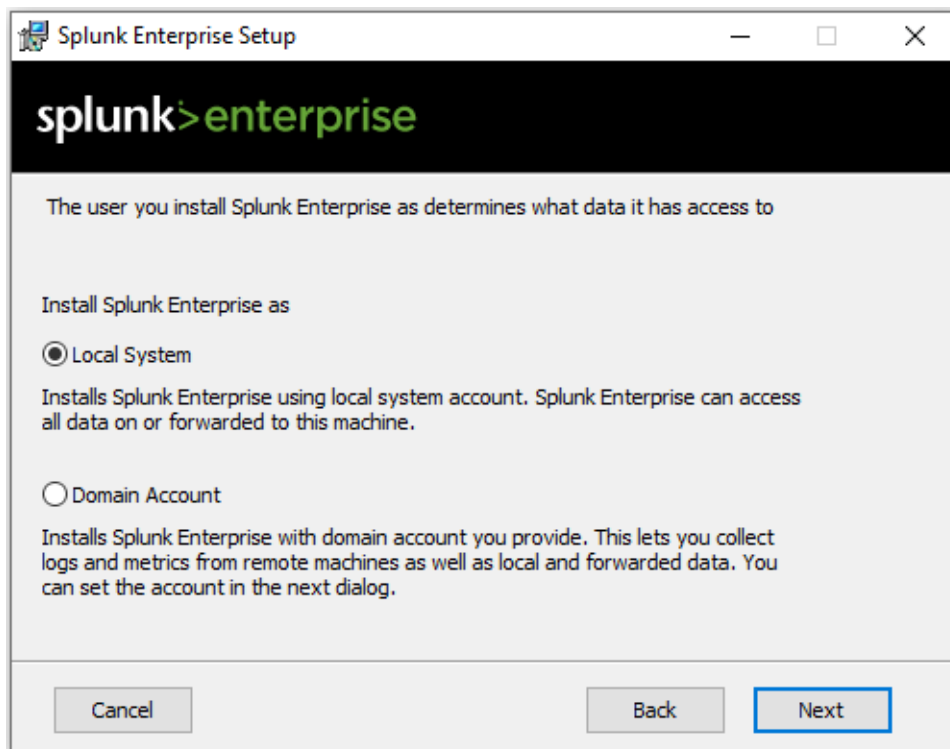
Je ne sais pas à quoi on s'engage en acceptant la licence, mais ça ne fait pas de mal de la transmettre au service juridique de votre structure. Quoi qu'il en soit, l'acceptation est obligatoire.



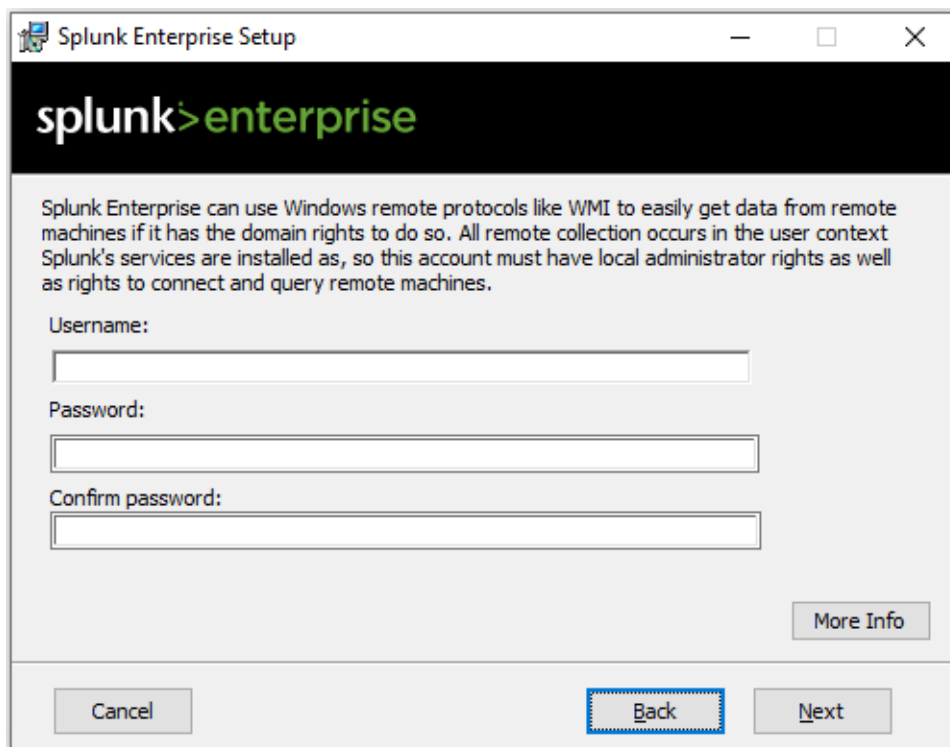
Il est indispensable de passer par “Customize Options” pour un minimum de maîtrise.



Chemin d'installation selon vos contraintes personnelles ou d'entreprise.



Choix du compte d'installation (souvent local ... car les données des autres serveurs du domaine peuvent être récupérés par d'autres moyens). On se pose la question de déterminer le niveau de droits de ce compte (on en reparlera quand on abordera les Apps)



Splunk Enterprise Setup

splunk>enterprise

Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.

Username:

Password:

Confirm password:

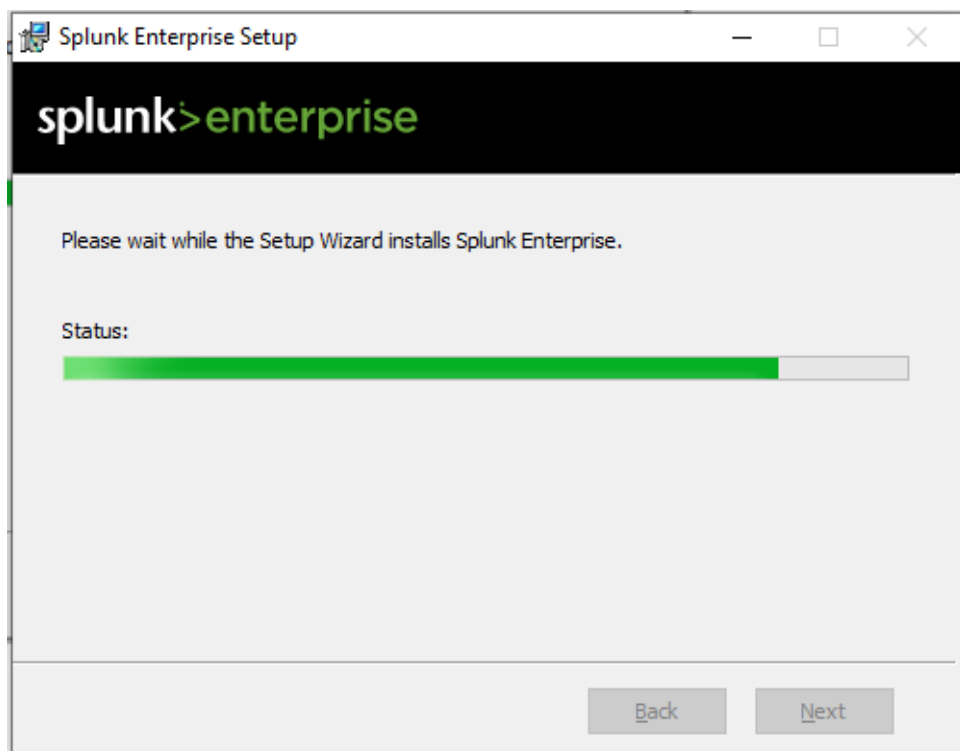
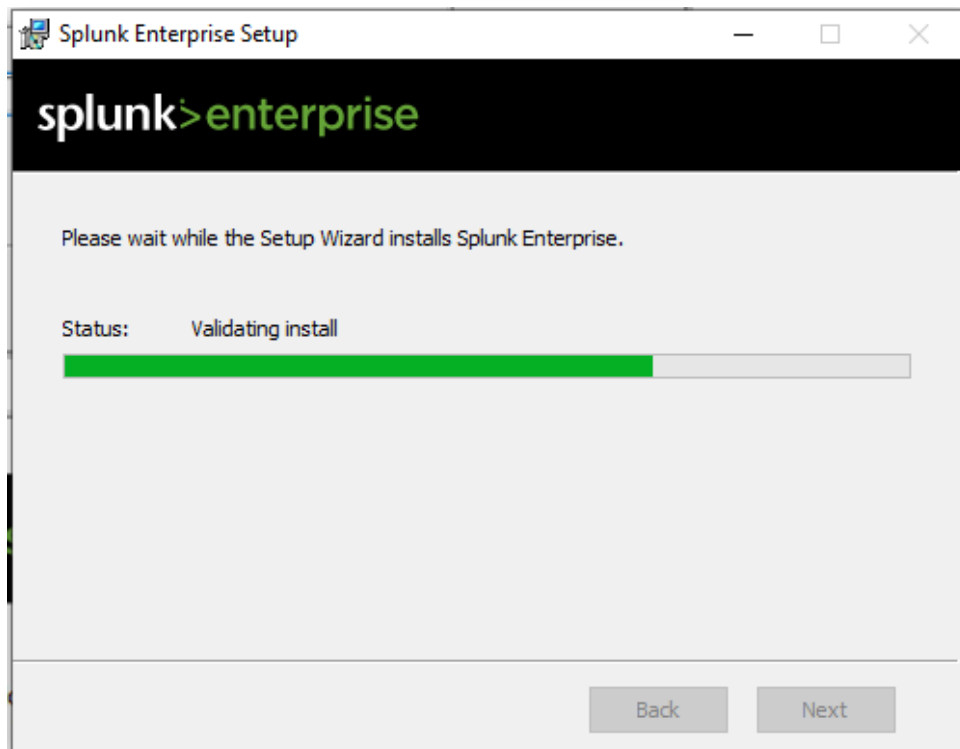
Vos informations de connexion au Keepass avant de les oublier (même s'il existe une procédure un peu tordue pour faire un reset password)

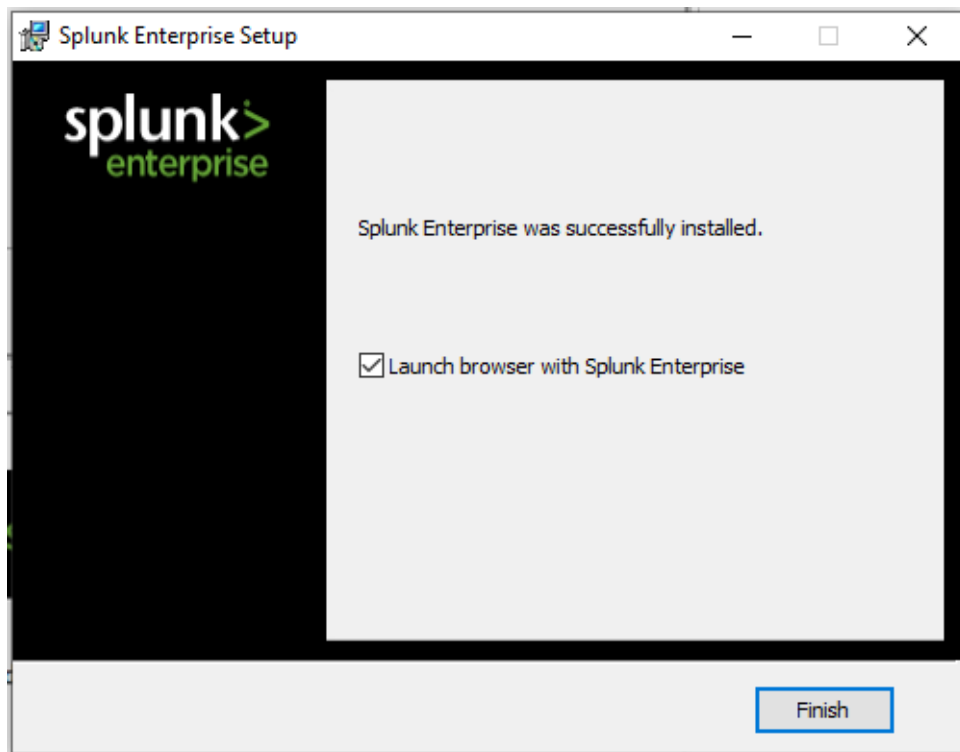
Splunk Enterprise Setup

splunk>enterprise

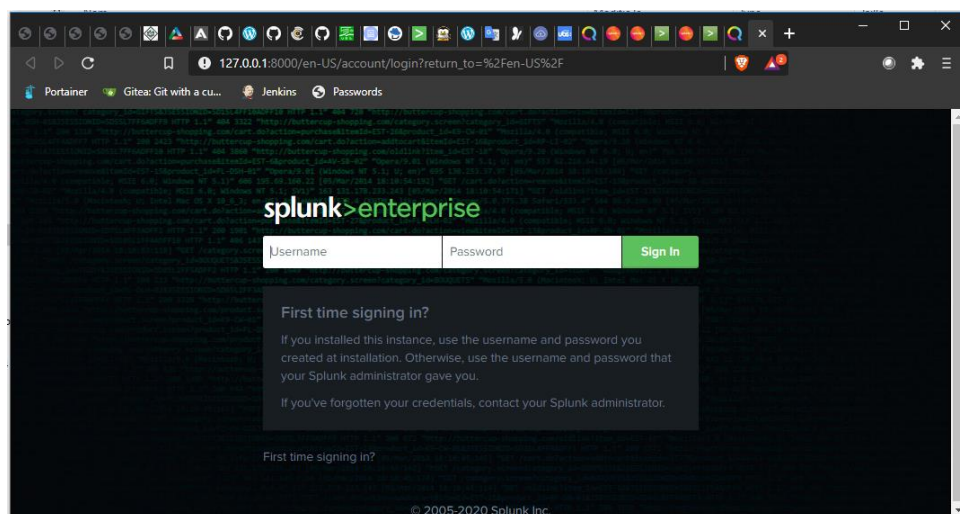
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

☒ Create Start Menu Shortcut

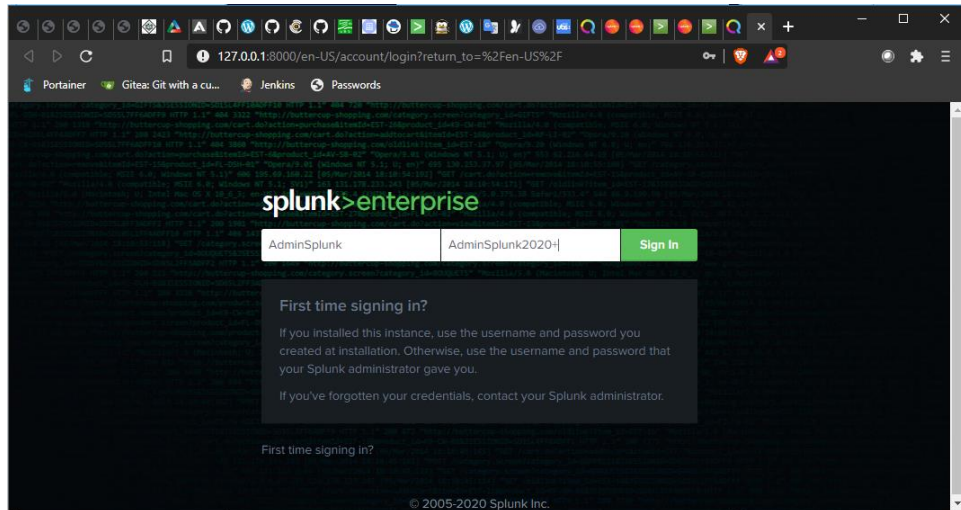




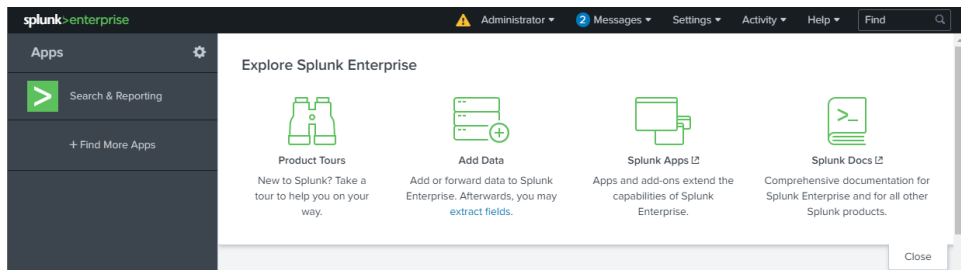
Installation visiblement Ok



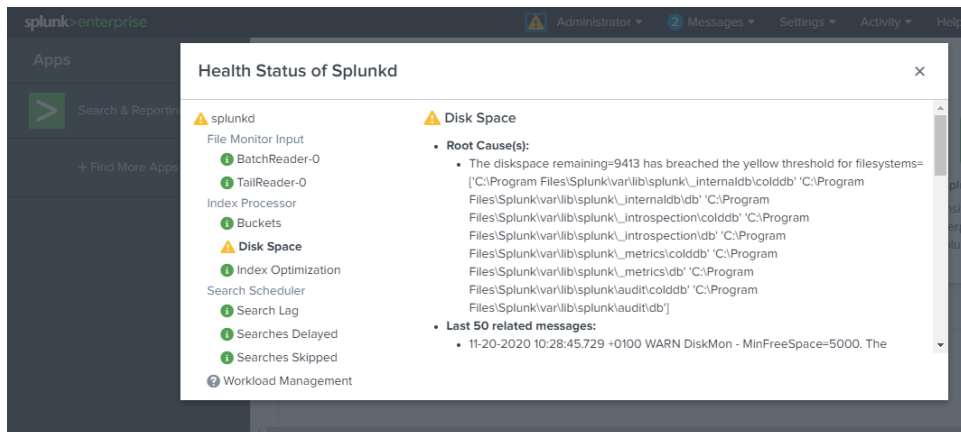
L'interface web s'ouvre automatiquement (localhost, port 8000, http)



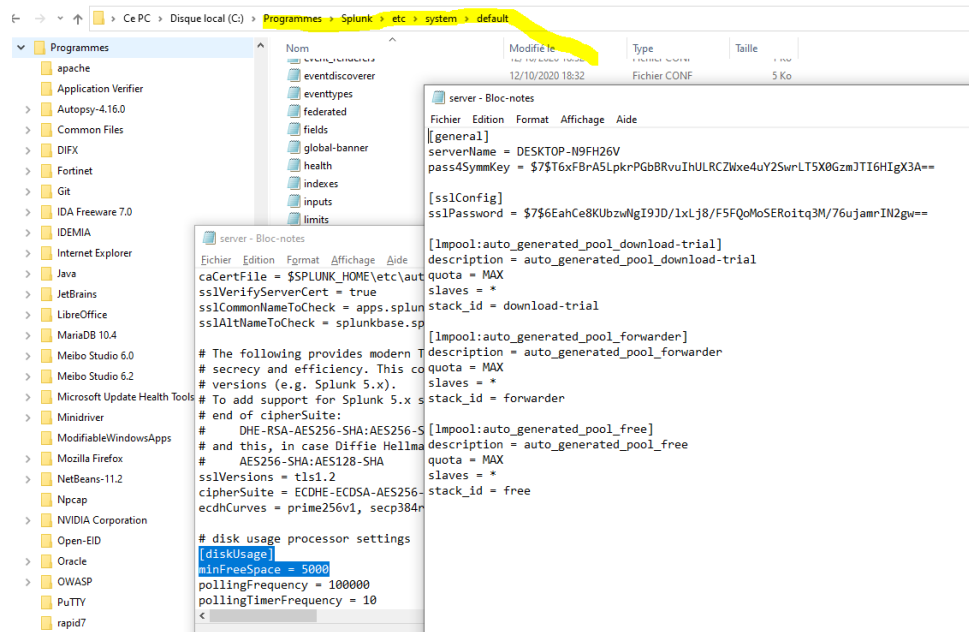
Première connexion



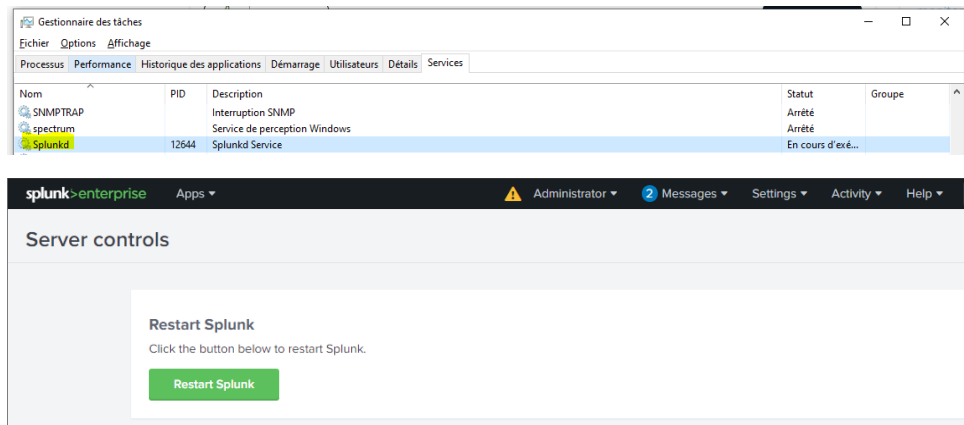
Fonctionnement ok ... ou presque (Warning !)



Je dispose de 9 Go de libre sur mon disque soit, moins de 2 fois l'espace disque minimum suffisant.



Tout est configurable dans des fichiers default / local !!!!



Le redémarrage suite augmentation de l'espace disque s'avère nécessaire. Opération faisable par redémarrage du service ou via GUI ou cmd

```
Administrator: Invite de commandes

c:\Program Files\Splunk\bin>splunk restart
Splunkd: Stopped

Splunk> Take the sh out of IT.

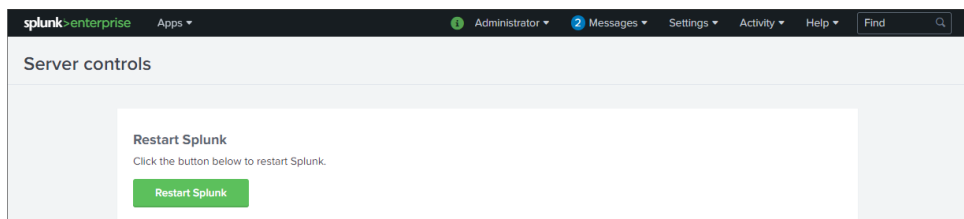
Checking prerequisites...
  Checking http port [8000]: open
  Checking mgmt port [8089]: open
  Checking appserver port [127.0.0.1:8065]: open
  Checking kvstore port [8191]: open
  Checking configuration... Done.
  Checking critical directories... Done
  Checking indexes...
    (skipping validation of index paths because not running as LocalSystem)
  Validated: _audit _internal _introspection _metrics _metrics_rollup _telemetry
  _thefishbucket history main summary
  Done
  Checking filesystem compatibility... Done
  Checking conf files for problems...
  Done
  Checking default conf files for edits...
  Validating installed files against hashes from 'c:\Program Files\Splunk\splunk-8.1.0-f
57c09e87251-windows-64-manifest'
  All installed files intact.
  Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...

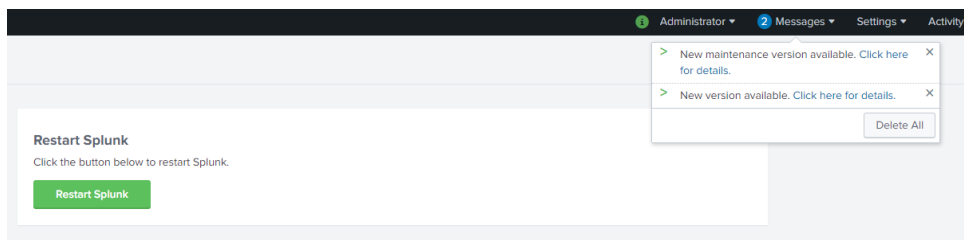
Splunkd: Starting (pid 8800)
Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://DESKTOP-N9FH26V:8000
```



Le warning a disparu. En revanche, nous avons 2 messages



Après vérification, il n'y a pas de nouvelle version :

splunk-8.1.0-f57c09e87251-x64-release

splunk>enterprise Apps ▾

Licensing

This server is acting as a standalone license server [Change to slave](#)

Trial license group

[Change license group](#)

This server is configured to use licenses from the **Trial license group**

[Add license](#) [Usage report](#)

Alerts

Licensing alerts notify you of excessive indexing warnings and licensing misconfigurations. [Learn more](#)

Current

- No licensing alerts

Permanent

- No licensing violations

Local server information

Indexer name	DESKTOP-N9FH26V
License expiration	Jan 19, 2021, 9:51:43 AM
Licensed daily volume	500 MB
Volume used today	0 MB (0% of quota)
Warning count	0
Debug information	All license details All indexer details

Politique de licence : 500 Mo/j pendant 2 mois. Nous avons droit à 5 dépassements de licence sur 30 jours glissants.

splunk>enterprise Apps ▾

Installed licenses

[Licensing](#) » Installed licenses

Installed licenses on: DESKTOP-N9FH26V (3)

1. Splunk Enterprise Download Trial

creation_time	2019-10-14 09:00:00+02:00
expiration_time	2021-01-19 09:51:43+01:00
features	<ul style="list-style-type: none"> Acceleration AdvancedSearchCommands AdvancedXML Alerting AllowDuplicateKeys ArchiveToHdfs Auth ConditionalLicensingEnforcement CustomRoles

hash	3D2E4634883A0648384BEEDCA226FC78EC2598B547553C90830CA3A93C305886
is_unlimited	False
label	Splunk Enterprise Download Trial
max_violations	5
payload	None
quota_bytes	524288000.0
sourcetypes	
stack_name	download-trial
status	VALID
type	download-trial
window_period	30

En cas de dépassement licence, il vous faudra demander une licence de déblocage au service commercial SPLUNK

splunk-enterprise

Apps

Administrator

Messages

Settings

Activity

Help

Find

Users

New User

1 Users

filter

Q

10 per page

Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last Login	Status
admins splunk	Edit	Splunk	Administrator	changeme@example.com		launcher	system	admin	11/20/2020, 11:50:07 AM	✓ Active

Première règle de sécu, je crée un compte pour un nouvel utilisateur (moi-même) et je mets le compte adminSplunk au coffre. Il est indispensable d'assurer une traçabilité des actions depuis la plateforme.

Create User

Name

Laurent

Full name

Laurent Marot

Email address

laurent@laurentmarot.fr

Set password

.....

Confirm password

.....

Password must contain at least ?

✓ 8 characters

Cancel

Save

Create User ×

Time zone ? (GMT+01:00) Brussels, Copenhagen, Madrid, Paris ▼

Default app ? launcher (Home) ▼

Assign roles ?

Available item(s) add all >

- admin
- can_delete
- power
- splunk-system-role
- user

Selected item(s) < remove all

- admin
- user

Create a role for this user ☐

Require password change ☒

Cancel Save

Je lui donne tous les droits (role admin – nous reviendrons sur cette notion de rôle).

Il va de cela que dans la vraie vie on activerait le “Require password change on first login”

splunk-enterprise Apps ▼ Administrator ▼ Messages ▼ Settings ▼ Activity ▼ Help ▼ Find

Users New User

2 Users 10 per page ▼

Name	Actions	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last Login	Status
admins plunk	Edit ▼	Splunk	Administrator	changeme@example.com		launcher	system	admin	11/20/2020, 11:50:07 AM	✓ Active
laurent	Edit ▼	Splunk	Laurent Marot	laurent@laurentmarot.fr	Europe/Brussels	launcher	system	admin, user		✓ Active

On s’aperçoit qu’il existe plusieurs “Authentication System”. Heureusement, en entreprise cela permet de s’interfacer avec le LDAP.

J’ai renseigné une adresse email mais pas de Gateway SMTP, ce qui devient rapidement indispensable pour tester les notifications d’alertes par messagerie.

Deuxième action de sécurité : on active HTTPS ... au cas où on accède au travers du réseau

splunk>enterprise Apps Administrator

General settings

Server settings > General settings

Splunk server name: DESKTOP-N9FH26V

Installation path: C:\Program Files\Splunk

Management port: 8089
Port that Splunk Web uses to communicate with the splunkd process. This port is also used for distributed search.

SSO Trusted IP
The IP address to accept trusted logins from. Only set this if you are using single sign-on (SSO) with a proxy server for authentication.

Splunk Web

Run Splunk Web: ☒ Yes ☐ No

Enable SSL (HTTPS) in Splunk Web: ☒ Yes ☐ No

Web port: 8000

App server ports: 8065
Port number(s) for the python-based application server to listen on. Use comma-separated list to specify more than one port number.

Session timeout: 1h
Set the Splunk Web session timeout. Use the same notation as relative time modifiers, for example 3h, 100s, 6d.

Index settings

Default host name: DESKTOP-N9FH26V
Sets the host field value for all events coming from this server.

Path to indexes: C:\Program Files\Splunk\var\lib\splunk

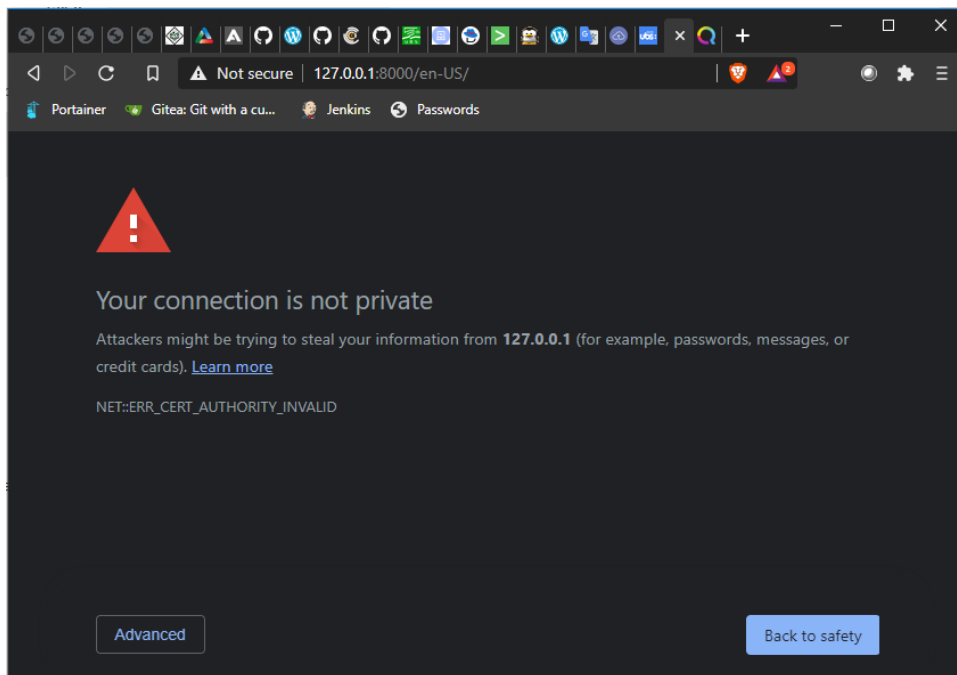
Administrator 1 Messages Settings Activity He

⚠ Splunk must be restarted for changes to take effect. [Click here to restart from Server controls](#)

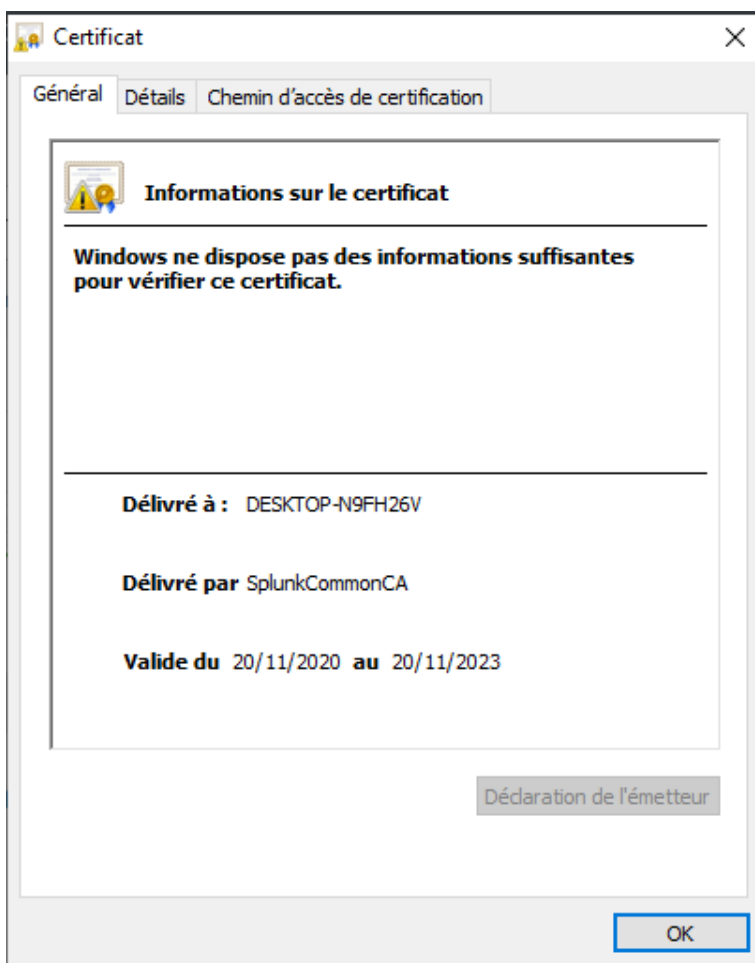
11/20/2020, 1:47:35 PM

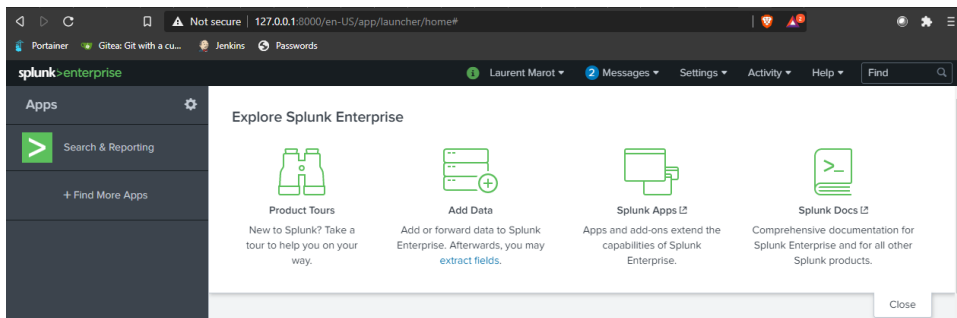
Delete All

Et on doit alors redémarrer.



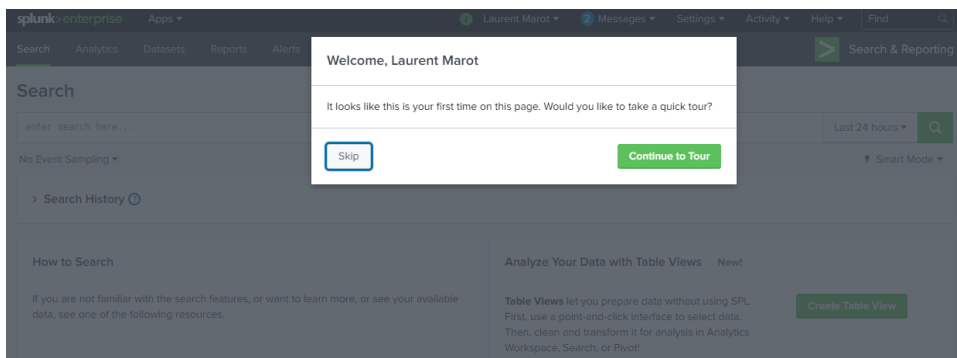
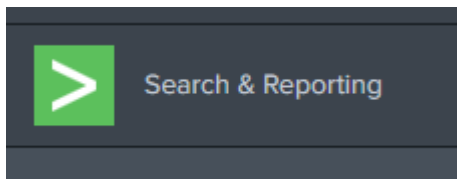
Forcément, certificat signé par CA non reconnue, ça couine un peu ... mais au moins le flux est chiffré. Et si on arrive à se connecter avec son compte c'est que c'est certainement la bonne machine.



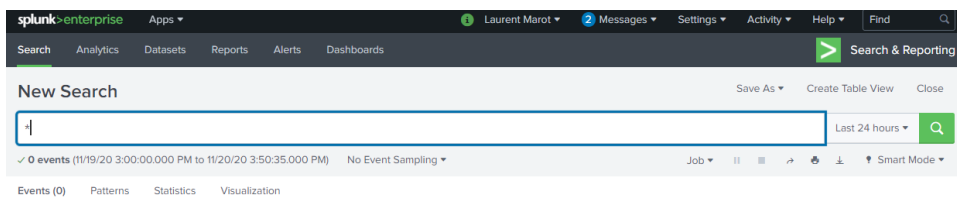


Je suis connecté avec mon nouveau compte.

Voyons ce que la bête a dans le ventre ...



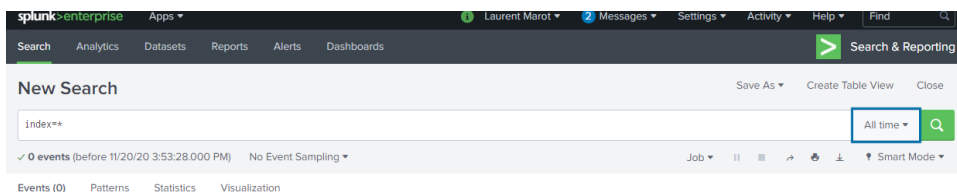
N'hésitez pas à parcourir le "Quick Tour"



Lançons notre première recherche : *. Magnifique : 0 résultat !

Notons que :

- 1- on peut passer en langue française
- 2- la recherche porte sur les 24 dernières heures
- 3- le mode de recherche est "Smart Mode"



index=* sur "All Times" => pas mieux !

Attention, sur les mots clefs (par exemple “index”) la solution est sensible à la casse.

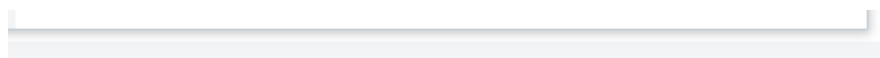
The screenshot shows the Splunk Search interface. The search bar contains 'index=*'. A warning message states: 'The search you ran returned a number of fields that exceeded the current indexed field extraction limit of 200. To ensure that all fields are extracted for search, set limits.conf: [kv] / indexed_kv_limit to a number that is higher than the number of fields contained in the files that you index.' The results show 150,760 events. The interface includes tabs for Events, Patterns, Statistics, and Visualization. A timeline visualization is shown at the bottom with a '1 hour per column' scale.

index=***** sur “All Times” => 150 760 enregistrements (et un warning bizarre) !

The screenshot shows the Splunk Search interface with the search 'index=*audit'. It returns 9,307 events. The interface includes tabs for Events, Patterns, Statistics, and Visualization. A timeline visualization is shown at the bottom. Below the timeline, there is a table of events with columns for Time and Event. The first event is from 11/20/20 at 4:05:12.148 PM, showing an audit trail for a search job. The second event is from 11/20/20 at 4:05:10.208 PM, showing a completed search for 'Sum maryDirector_1605884681.20'.

index=**_audit** => 9,307 events (before 11/20/20 4:05:12.000 PM)

Donc, il semblerait que l’on ait des index... par défaut (Vous vous souvenez de la fonction d’indexation ?)



Affirm' ... 11 index dont certains sont préfixés par un **_**

_internal	Edit	Delete	Disable	Events	system	9 MB	488.28 GB	133K	6 hours ago	a few seconds ago	\$SPLUNK_D B_internaldb	N/A
_audit	Edit	Delete	Disable	Events	system	2 MB	488.28 GB	9.43K	6 hours ago	a few seconds ago	\$SPLUNK_D B_auditdb	N/A

Pour la petite histoire, Splunk, pour des besoins d’audit de son propre fonctionnement indexe ses logs d’activité et d’erreurs dans l’index “_audit”

> _telemetry		_metrics.dat	20/11/2020 14:04	Fichier DAT	1 Ko
> audit		_telemetry.dat	20/11/2020 14:14	Fichier DAT	1 Ko

Et ces index se retrouvent au niveau du système de fichiers. On regardera en détail plus tard.

La gestion de ces index est très importante en termes de performance et en termes de sécurité.

Un exemple de ce qu'il ne faut pas faire : ne pas être vigilant sur l'index qui va accueillir nos données.

Imaginons vouloir alimenter notre outil avec des logs trouvés par hasard ...

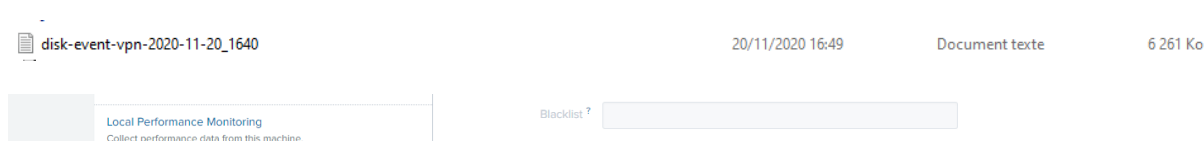


Add Data



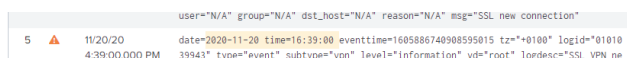
La partie haute de l'écran est nouvelle, je ne sais pas à quoi elle sert. Des exemples j'imagine... il y a de la ressource pléthorique sur Splunk.

Ne nous soucions pas trop des options. Indexons ce fichier :



Splunk arrive à trouver la date toute seul (souvenez-vous : un enregistrement \Leftrightarrow 1 bloc de données avec un timestamp. Attention on a souvent du multilignes dans les logs applicatives).

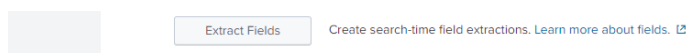
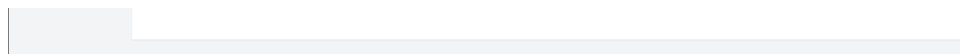
Choisissons, à tort, le source-type à "syslog" dans un premier temps :



Splunk n'apprécie pas le format de date mais ce n'est pas très grave dans notre cas.



On se dit que l'on jettera un œil à "How do index work ?" quand on aura le temps, et on ne le fera ... jamais.



Voilà, on peut ajouter la ligne “Expert Splunk” sur son CV.

On peut lancer notre première recherche.

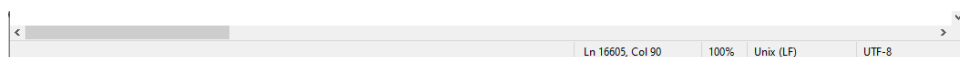


INTERESTING FIELDS
a action 18
a date 9

host = DESKTOP-N9FH26V | source = C:\Users\forge\Downloads\disk-event-vpn-2020-11-20_1640.log | sourcetype = syslog

> 11/20/20 date=2020-11-20 time=16:40:26 eventtime=1605886826849148063 tz="+0100" logid="0101039949" type="event" subtype="v

On nous annonce 16 605 évènements.



Ln 16605, Col 90 100% Unix (LF) UTF-8

Seems to be correct ... Notepad me dit la même chose. N'oubliez jamais de contrôler la cohérence de ce que vous annonce l'outil !



main Edit Delete Disable Events system 5 MB 488.28 GB 16.6K 9 days ago 38 minutes ago \$SPLUNK_D B\defaultdb \db

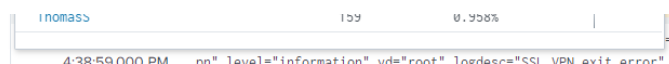
J'ai aussi une cohérence avec ce que m'indiquent les index (si je survole le 16,6k avec la souris, je retrouve bien mes 16 605 enregistrements) ... en particulier l'index “main”.

En revanche, lorsque je fais des tests ... je n'alimente JAMAIS l'index “main” qui risque autrement de devenir un index poubelle (accessible à tous). J'aurais dû créer un index dédié avec un nom signifiant !

Mais revenons à nos moutons ... la touche “back” de votre navigateur est très pratique pour revenir sur l'historique de vos actions.

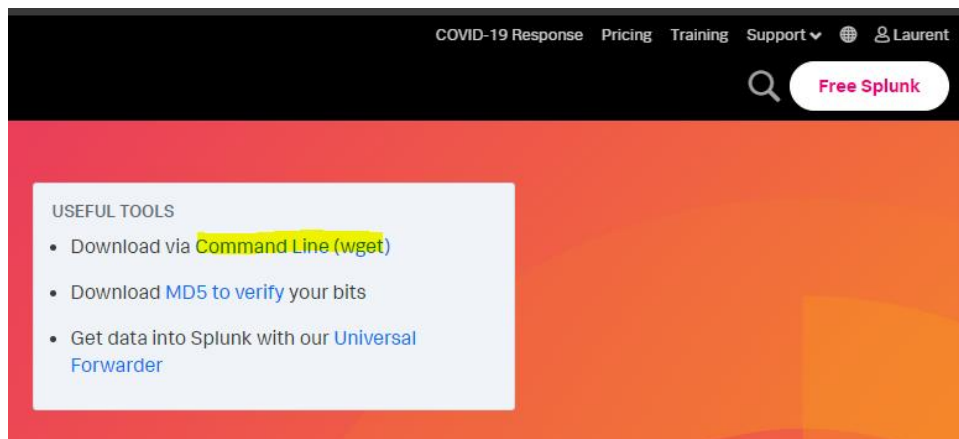
Le parsing “automatique” de nos logs, malgré un source-type hasardeux, semble s'être bien déroulé.

On va donc pouvoir utiliser les pires aspects de ce genre d'outil pour attribuer nos notes, non plus au hasard cette année mais selon la convention que celui qui se connecte le plus souvent est celui qui travaille le plus, donc est le plus méritant :



4:38:59.000 PM nn" level="information" vd="root" logdesc="SSI VPN exit error" s

II] Installation de Splunk Enterprise Linux



```
wget -O splunk-8.1.0.1-24fd52428b5a-Linux-x86_64.tgz  
'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=8.1.0.1&product=splunk&filename=splunk-8.1.0.1-24fd52428b5a-Linux-x86_64.tgz&wget=true'
```

Root ??? Really ???

```
root@keycloak:/home/laurent# mkdir /opt/splunk  
root@keycloak:/home/laurent# wget -O splunk-8.1.0.1-24fd52428b5a-Linux-x86_64.tgz  
z 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64  
&platform=linux&version=8.1.0.1&product=splunk&filename=splunk-8.1.0.1-24fd52428  
b5a-Linux-x86_64.tgz&wget=true'  
--2020-11-22 21:31:37-- https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=8.1.0.1&product=splunk&filename=splunk-8.1.0.1-24fd52428b5a-Linux-x86_64.tgz&wget=true  
Résolution de www.splunk.com (www.splunk.com)... 95.100.252.147, 95.100.252.137  
Connexion à www.splunk.com (www.splunk.com)|95.100.252.147|:443... connecté.  
requête HTTP transmise, en attente de la réponse... 302 Moved Temporarily  
Emplacement : https://download.splunk.com/products/splunk/releases/8.1.0.1/linux/splunk-8.1.0.1-24fd52428b5a-Linux-x86_64.tgz [suivant]  
--2020-11-22 21:31:38-- https://download.splunk.com/products/splunk/releases/8.1.0.1/linux/splunk-8.1.0.1-24fd52428b5a-Linux-x86_64.tgz  
Résolution de download.splunk.com (download.splunk.com)... 143.204.192.26, 143.204.192.66, 143.204.192.77, ...  
Connexion à download.splunk.com (download.splunk.com)|143.204.192.26|:443... connecté.  
requête HTTP transmise, en attente de la réponse... 200 OK  
Taille : 508221657 (485M) [application/x-gzip]  
Sauvegarde en : « splunk-8.1.0.1-24fd52428b5a-Linux-x86_64.tgz »  
  
splunk-8.1. 39%[=====>] 191,51M 5,48MB/s tps 60s
```

```
root@keycloak:/opt# tar -xvf splunk-8.1.0.1-24fd52428b5a-Linux-x86_64.tgz
```

```
root@keycloak:/opt/splunk/bin# ./splunk start
```

SPLUNK GENERAL TERMS

Last updated: February 13, 2020

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware corporation, with its principal place of business at 270 Brannan Street, San Francisco, California 94107, U.S.A ("Splunk" or "we" or "us" or "our") and you ("Customer" or "you" or "your") apply to the purchase of licenses and subscriptions for Splunk's Offerings. By clicking on the appropriate button, or by downloading, installing, accessing or using the Offerings, you agree to these General Terms. If you are entering into these General Terms on behalf of Customer, you represent that you have the authority to bind Customer. If you do not agree to these General Terms, or if you are not authorized to accept the General Terms on behalf of the Customer, do not download, install, access, or use any of the Offerings.

```
Do you agree with this license? [y/n]: y
```

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.

Create credentials for the administrator account.

Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin

Password must contain at least:

* 8 total printable ASCII character(s).

Please enter a new password:

Please confirm new password:

Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.

Generating RSA private key, 2048 bit long modulus

.....+++++

.....+++++

e is 65537 (0x10001)

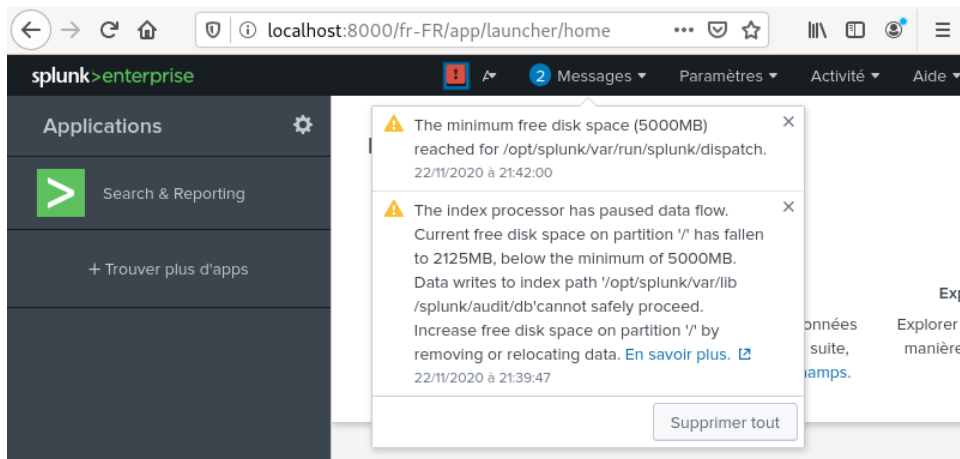
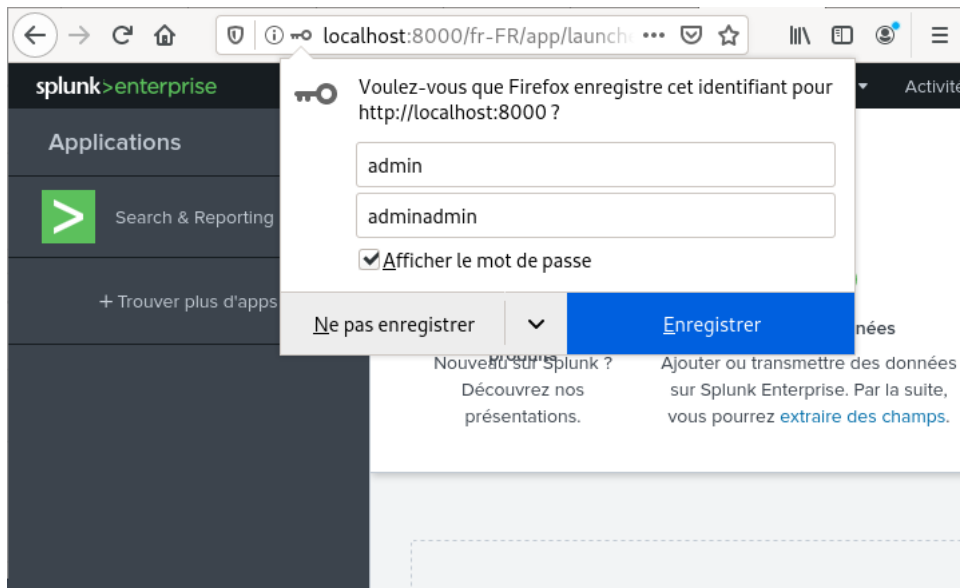
writing RSA key

If you get stuck, we're here to help.

Look for answers here: <http://docs.splunk.com>

The Splunk web interface is at <http://keycloak:8000>


```
root@keycloak:/opt/splunk/bin#
```



II] Installation d'une APP orientée "sécurité"

De base SPLUNK Enterprise n'est pas une solution de SIEM à proprement parler. La solution SIEM s'appelle "Enterprise sécurité" et est distribuée de manière payante. Et il faut justifier de la certification "Architecte SPLUNK" pour l'utiliser.

Malgré tout si on veut une petite appli didactique sympa orientée sécurité, nous avons "Splunk Security Essential "



Splunk Security Essentials

Install

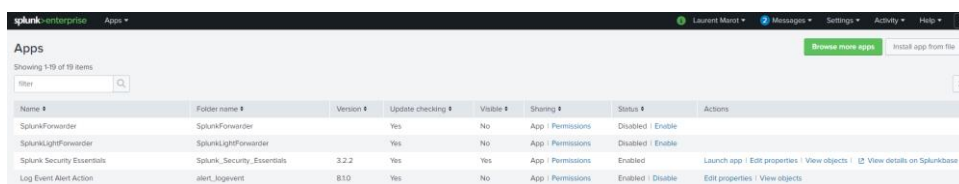
Splunk Security Essentials is the free Splunk app that makes security easier, with four key pillars: to help you find the best content (including from ES, ESCU, UBA and Phantom), learn how it works, deploy it successfully, and measure your success.

And the docs site: <https://docs.splunksecurityessentials.com/>

FIND THE BEST CONTENT
The #1 goal of... [More](#)

Category: Security, Fraud & Compliance | Author: Splunk Inc. | Downloads: 81827 | Released: 4 years ago | Last Updated: 4 days ago | [View on Splunkbase](#)

Découvrons au travers de cet exemple ce qu'est une APP Splunk.



Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
SplunkForwarder	SplunkForwarder		Yes	No	App Permissions	Disabled Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App Permissions	Disabled Enable	
Splunk Security Essentials	Splunk_Security_Essentials	3.2.2	Yes	Yes	App Permissions	Enabled	Launch app Edit properties View objects View details on Splunkbase
Log Event Alert Action	Alert_LogEvent	8.10	Yes	No	App Permissions	Enabled Disable	Edit properties View objects

A la base, une APP c'est une petite tgz de fichier de scripting/coding/configuration qui vous permet de construire automatiquement tout un tas de recherches, alertes, rapports sur une source de logs particulière. Le code embarqué dans votre APP s'exécute avec les droits de votre utilisateurs SPLUNK alors méfiance.

Installing App...

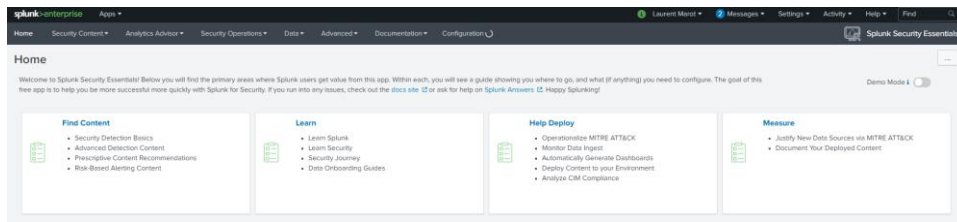
Splunk Security Essentials is being downloaded and installed.

Restart Required

You must restart Splunk Enterprise to complete installation of Splunk Security Essentials.

Restart Later
Restart Now

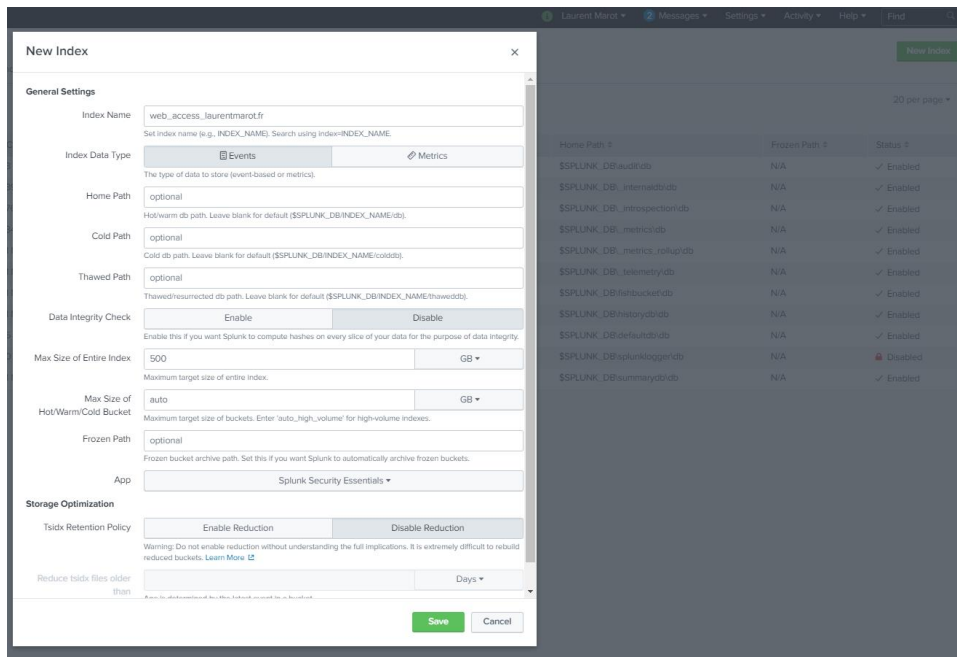
Larguez vos COD et vos World of Tanks, avec ça vous avez de quoi jouer pendant toutes vos vacances de Noël.



III] Playing with data

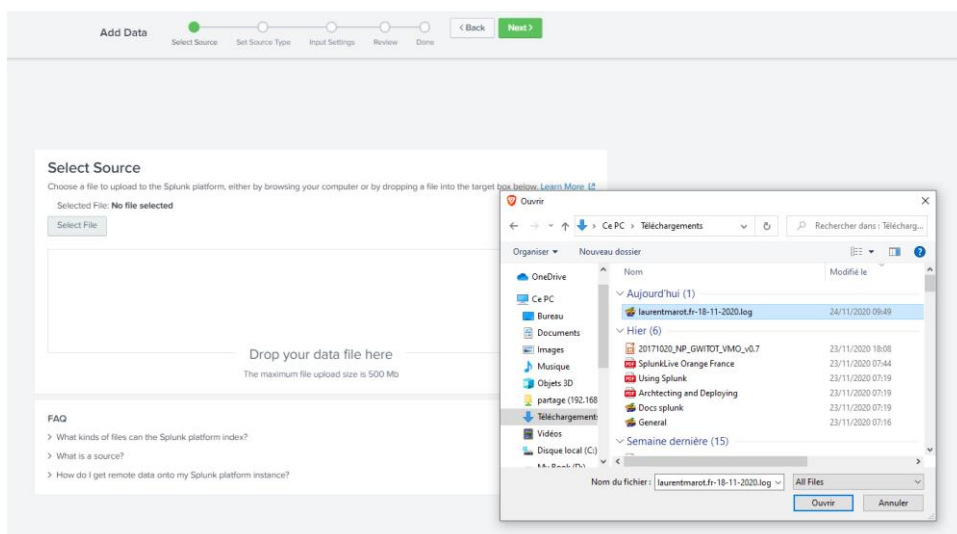
1 – acces web

Créons un index dédié :



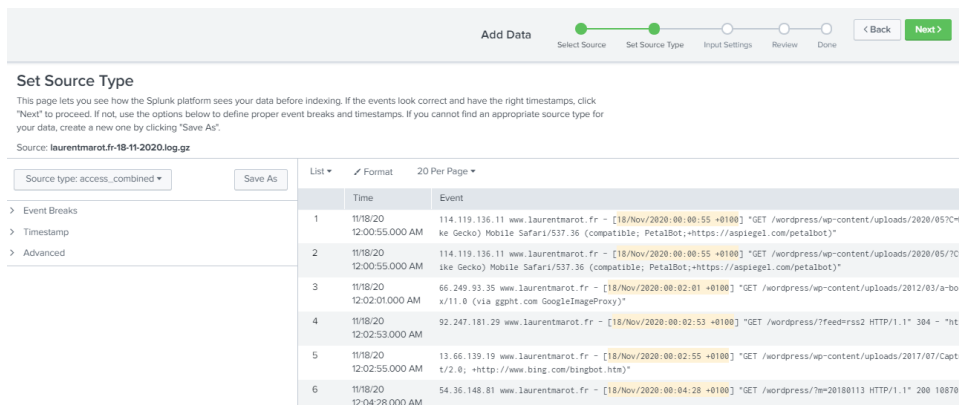
Attention d'avoir bien à l'esprit une convention de nommage explicite.

Et alimentons manuellement (dans un premier temps ... ou simplement parce que les contraintes d'hébergement ne permettent pas de faire autrement).



Procédure habituelle d'upload de fichiers (pour le coup logs Apache)

Comme le fichier est une archive gz, vous n'obtiendrez pas la visualisation des lignes de logs dans la première fenêtre du wizzard.



Set Source Type

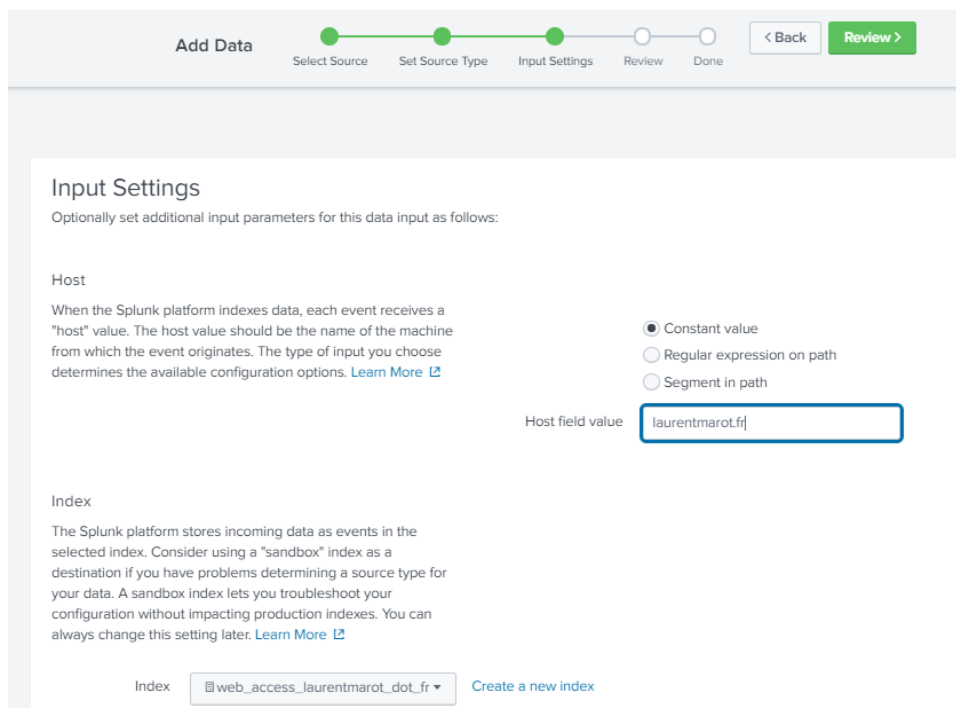
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **laurentmarot.fr-18-11-2020.log.gz**

Source type: **access_combined** Save As

Time	Event
11/18/20 12:00:55.000 AM	114.119.136.11 www.laurentmarot.fr - [18/Nov/2020:00:00:55 +0100] "GET /wordpress/wp-content/uploads/2020/05/7C4M ke Gecko) Mobile Safari/537.36 (compatible; PetalBot;https://aspiegel.com/petalbot)"
11/18/20 12:00:55.000 AM	114.119.136.11 www.laurentmarot.fr - [18/Nov/2020:00:00:55 +0100] "GET /wordpress/wp-content/uploads/2020/05/7C4M ke Gecko) Mobile Safari/537.36 (compatible; PetalBot;https://aspiegel.com/petalbot)"
11/18/20 12:02:01.000 AM	66.249.93.35 www.laurentmarot.fr - [18/Nov/2020:00:02:01 +0100] "GET /wordpress/wp-content/uploads/2012/03/a-bord x/11.0 (via ggpht.com GoogleImageProxy)"
11/18/20 12:02:53.000 AM	92.247.181.29 www.laurentmarot.fr - [18/Nov/2020:00:02:53 +0100] "GET /wordpress/?feedrss2 HTTP/1.1" 304 - "http
11/18/20 12:02:55.000 AM	13.66.139.19 www.laurentmarot.fr - [18/Nov/2020:00:02:55 +0100] "GET /wordpress/wp-content/uploads/2017/07/Captur t/2.0; +http://www.bing.com/bingbot.htm)"
11/18/20 12:04:28.000 AM	54.36.148.81 www.laurentmarot.fr - [18/Nov/2020:00:04:28 +0100] "GET /wordpress/?m=20180113 HTTP/1.1" 200 10870 "

Le moteur Splunk détecte automatiquement que c'est bien un source-type "access_combined".



Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

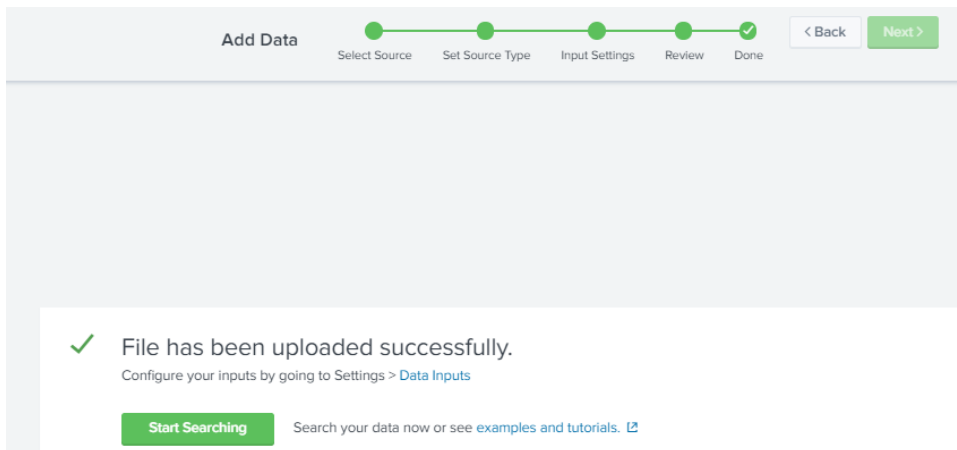
Host field value:

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index: [Create a new index](#)

N'oubliez pas de sélectionner le bon index (et éventuellement changer le "host field value").



Tutto va bene !

Nous pouvons commencer nos opérations de recherche

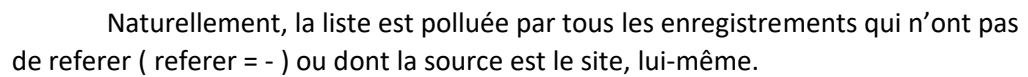
The screenshot shows the Splunk Search interface. The top navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'New Search' section shows a search query: `source="laurentmarot.fr-18-11-2020.log.gz" host="laurentmarot.fr" index="web_access_laurentmarot_dot_fr" sourcetype="access_combined"`. Below the query, it indicates '2,298 events (before 11/24/20 10:02:30.000 AM)' and 'No Event Sampling'. The 'Events (2,298)' tab is selected, showing a timeline visualization and a list of events. The list of events is displayed in a table format with columns for 'Time' and 'Event'. The table shows several log entries with details like IP addresses, hostnames, and HTTP methods. On the left side, there are sections for 'SELECTED FIELDS' and 'INTERESTING FIELDS'.

i	Time	Event
>	11/18/20 11:56:32.000 PM	216.244.66.229 www.laurentmarot.fr - [18/Nov/2020:23:56:32 +0100] "GET /robots.txt HTTP/1.1" 404 196 host = laurentmarot.fr source = laurentmarot.fr-18-11-2020.log.gz sourcetype = access_combined
>	11/18/20 11:55:28.000 PM	116.203.130.107 www.laurentmarot.fr - [18/Nov/2020:23:55:28 +0100] "GET /wordpress/?feed=rss2 HTTP/1.1" 200 196 host = laurentmarot.fr source = laurentmarot.fr-18-11-2020.log.gz sourcetype = access_combined
>	11/18/20 11:55:13.000 PM	114.119.131.195 www.laurentmarot.fr - [18/Nov/2020:23:55:13 +0100] "GET /wordpress/wp-content/upload 37.36 (compatible; PetalBot;+https://aspiegel.com/petalbot)" host = laurentmarot.fr source = laurentmarot.fr-18-11-2020.log.gz sourcetype = access_combined
>	11/18/20 11:55:12.000 PM	114.119.131.195 www.laurentmarot.fr - [18/Nov/2020:23:55:12 +0100] "GET /wordpress/wp-content/upload 7.36 (compatible; PetalBot;+https://aspiegel.com/petalbot)" host = laurentmarot.fr source = laurentmarot.fr-18-11-2020.log.gz sourcetype = access_combined
>	11/18/20 11:54:01.000 PM	92.247.181.29 www.laurentmarot.fr - [18/Nov/2020:23:54:01 +0100] "GET /wordpress/?feed=rss2 HTTP/1.1" 200 196 host = laurentmarot.fr source = laurentmarot.fr-18-11-2020.log.gz sourcetype = access_combined

Les champs significatifs sont reconnus(clientip, method, referer, ...). Nous voilà parés pour faire un peu d’analytique et un peu de sécu.

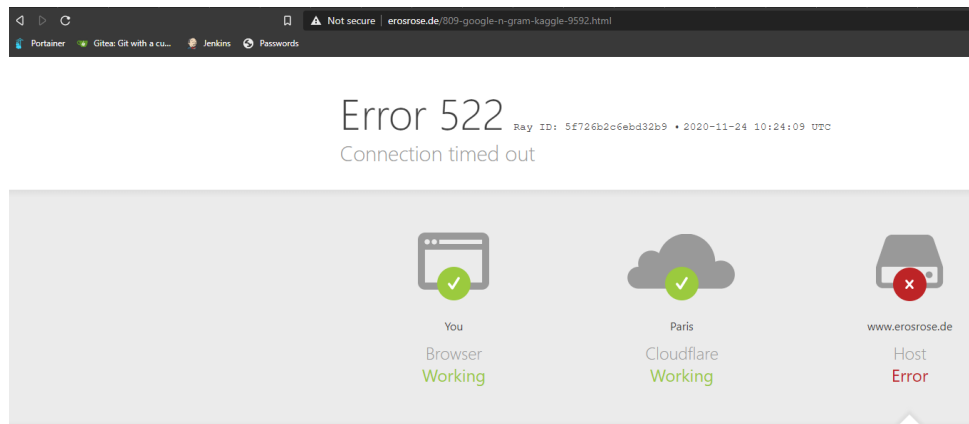
Intéressons-nous au champs “status”


```
source="laurentmarot.fr-18-11-2020.log.gz" host="laurentmarot.fr"
index="web_access_laurentmarot_dot_fr" sourcetype="access_combined" | top
limit=20 referer
```

[illegible]

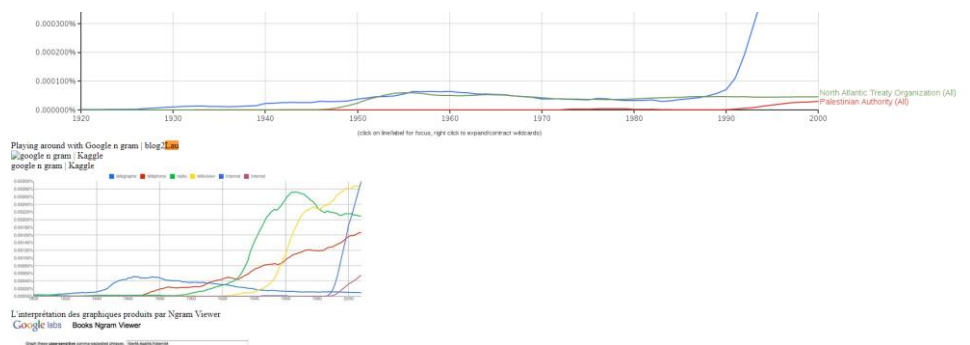
Un truc m'inquiète :





Le site semble down, je vois donc voir la version en cache.

<https://webcache.googleusercontent.com/search?q=cache:aYDa98shNkwJ:www.erosrose.de/809-google-n-gram-kaggle-9592.html+&cd=1&hl=fr&ct=clnk&gl=fr>



Pas grand-chose non plus sur webarchive, j'abandonne



Je ne me souvenais pas d'avoir fait un post sur Google n gramm

<http://www.laurentmarot.fr/wordpress/?s=google+n+gram&x=23&y=14>

Pour faire un peu de bruit sur le site, nous allons jouer avec WPScan

```
File Actions Edit View Help
Last Updated: 2016-12-30T16:46:00.000Z
Found By: Urls In Homepage (Passive Detection)
Version: 2016.1230 (100% confidence)
Found By: Query Parameter (Passive Detection)
- http://www.laurentmarot.fr/wordpress/wp-content/plugins/footnotes-for-wordpress/footnote-voodoo.css?ver=2016.1230
- http://www.laurentmarot.fr/wordpress/wp-content/plugins/footnotes-for-wordpress/footnote-voodoo.js?ver=2016.1230
Confirmed By: Readme - Stable Tag (Aggressive Detection)
- http://www.laurentmarot.fr/wordpress/wp-content/plugins/footnotes-for-wordpress/readme.txt

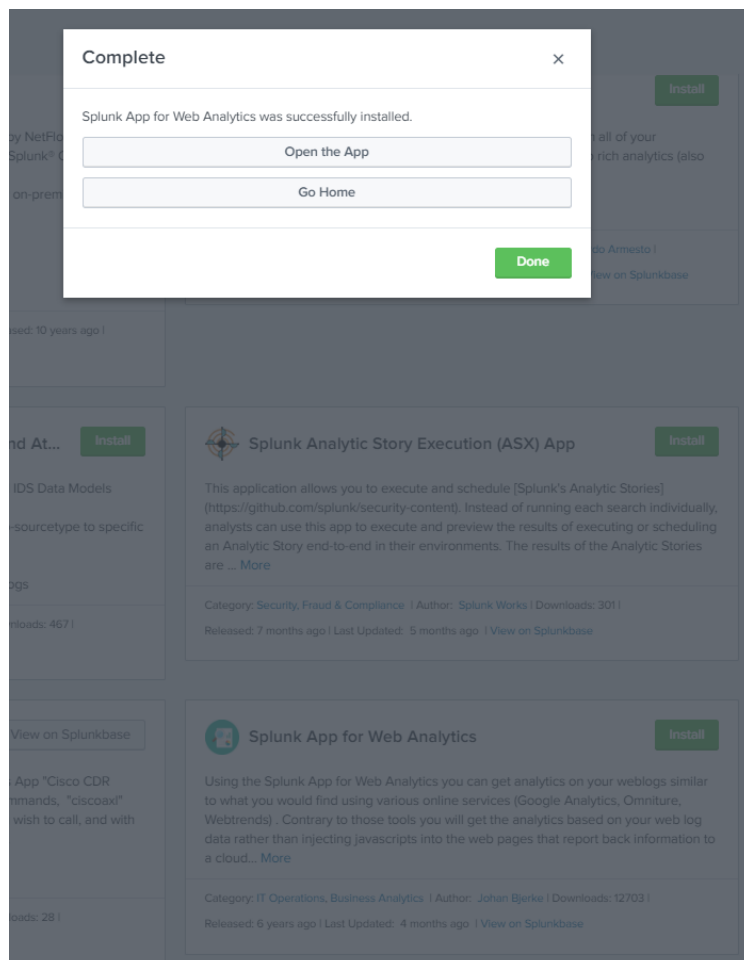
[-] wp-lightbox-2
Location: http://www.laurentmarot.fr/wordpress/wp-content/plugins/wp-lightbox-2/
Last Updated: 2020-11-09T21:17:00.000Z
[!] The version is out of date, the latest version is 3.0.6.4
Found By: Urls In Homepage (Passive Detection)
Version: 3.0.6.3 (50% confidence)
Found By: Readme - ChangeLog Section (Aggressive Detection)
- http://www.laurentmarot.fr/wordpress/wp-content/plugins/wp-lightbox-2/readme.txt

[-] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 (21 / 21) 100.00% Time: 00:00:00
[!] No Config Backups Found.

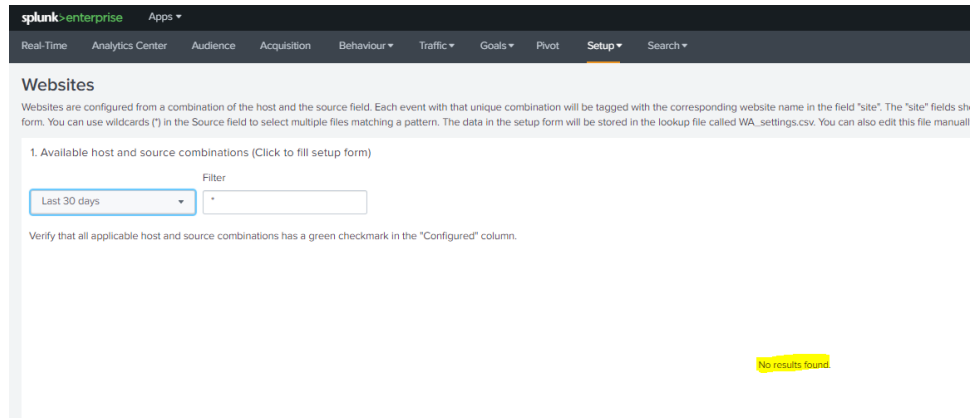
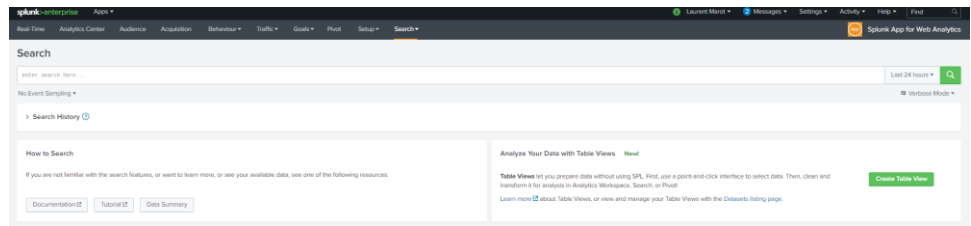
[!] No WPvulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up

[-] Finished: Tue Nov 24 05:41:44 2020
[-] Requests Done: 50
[-] Cached Requests: 6
[-] Data Sent: 14.647 KB
[-] Data Received: 250.533 KB
[-] Memory used: 189.609 MB
[-] Elapsed time: 00:00:06
kali@kali:~$
```

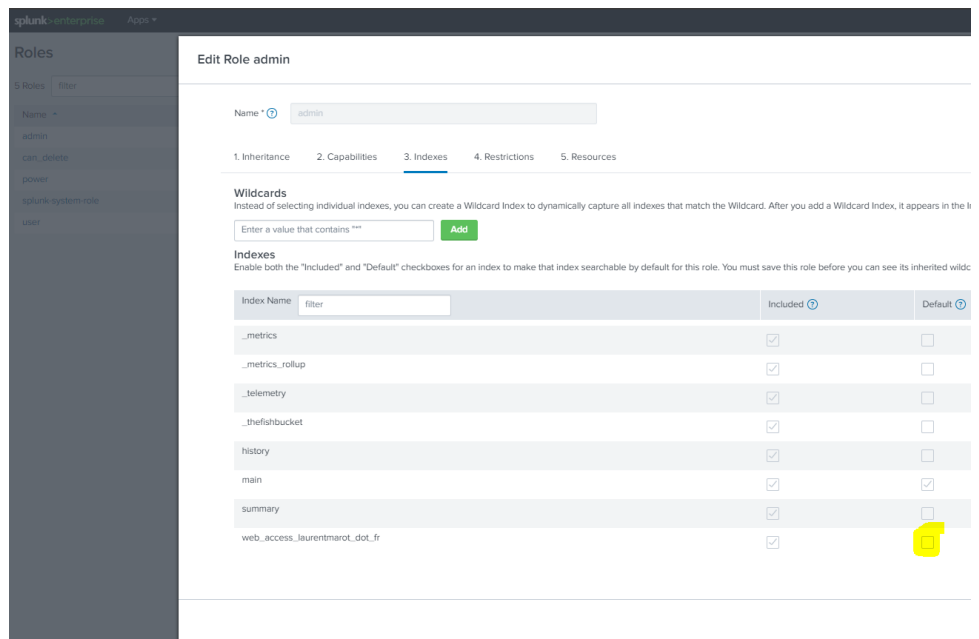
Les quelques requêtes faites précédemment montrent qu'avec un peu d'habitude et de patience on peut faire parler nos logs et savoir tout ce qui s'est passé sur notre serveur web. On peut ainsi créer manuellement toutes nos alertes et tableaux de bord. Pour procéder de manière plus performante, il existe un certain nombre d'applications qui vont faire le job à notre place.



Un peu de configuration...



Très inquiétante information ? Non, juste un problème de droits pas défaut sur un index nouvellement créé.



Bongo, notre index créé pour stocker les logs d'accès de notre serveur web n'est pas interrogeable par défaut, il faut donner explicitement son nom.

Pour vous en assurer, faites les requêtes suivantes :

status=404

Search Analytics Datasets Reports Alerts Dashboards

New Search

status=404

✓ 0 events (before 11/24/20 12:34:53.000 PM) No Event Sampling ▼

Events (0) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

Vs

status=404 index="web_access_laurentmarot_dot_fr"

Search Analytics Datasets Reports Alerts Dashboards

New Search

status=404 index="web_access_laurentmarot_dot_fr"

✓ 88 events (before 11/24/20 12:35:04.000 PM) No Event Sampling ▼

Pour que l'exemple soit probant, attention de placer le sélecteur de temps sur "All Times"

Et donc, après avoir donné les droits d'accès sur l'index, cela fonctionne mieux :

Websites

Websites are configured from a combination of the host and the source field. Each event with that unique combination will be tagged with the corresponding website name in the field "site". The "site" field should match your domain name, i.e. "www.mydomain.com". Click the tables below to prefill the setup form. You can use wildcards (*) in the Source field to select multiple files matching a pattern. The data in the setup form will be stored in the lookup file called `lookups/settings.csv`. You can also edit this file manually.

1. Available host and source combinations (Click to fill setup form)

Filter

Last 30 days

Verify that all applicable host and source combinations has a green checkmark in the "Configured" column.

key	host	source	Site in logs	Site in lookup	Events	Configured	Reason
	laurentmarot.fr	laurentmarot.fr-10-11-2020.log.gz			1	✓	

2. Add or edit website configuration

key Site (www.mydomain.com) Host (Accepts wildcard *) Source (Accepts wildcard *)

Save config Clear form Delete config

3. Configured websites (Click to edit from the form)

Sauvons la config

Websites

Websites are configured from a combination of the host and the source field. Each event with that unique combination will be tagged with the corresponding website name in the field. You can use wildcards (*) in the Source field to select multiple files matching a pattern. The data in the setup form will be stored in the lookup file called WA_settings.csv. You can

1. Available host and source combinations (Click to fill setup form)

Filter

Last 30 days

*

Verify that all applicable host and source combinations has a green checkmark in the "Configured" column.

key ↕	host ↕	source ↕	Site in logs ↕
5fbcf0d30467000078003fe1	laurentmarot.fr	laurentmarot.fr-18-11-2020.log.gz	www.laurentmarot.fr

2. Add or edit website configuration

key	Site (www.mydomain.com)	Host (Accepts wildcard *)	Source (Accepts wildcard *)
<input type="text"/>	<input type="text" value="www.laurentmarot.fr"/>	<input type="text" value="laurentmarot.fr"/>	<input type="text" value="laurentmarot.fr-18-11-2020.log.gz"/>
<div><div>Save config</div><div>Clear form</div><div>Delete config</div></div>			

3. Configured websites (Click to edit from the form)

	Site ↕	Host ↕
1	www.laurentmarot.fr	laurentmarot.fr

4. Migrating config from v2.1 (csv) to >v2.1 (KV Store) - OPTIONAL

Below are the configs currently in the WA_settings.csv file. If you want to migrate this config to the KV store, click the button at the bottom. You only need to do this once.

Generate user sessions

Last 30 days ▾

✓ 113 events (10/25/20 12:00:00.000 AM to 11/24/20 12:40:06.000 PM)

113 results 20 per page ▾

acceleration ↕	datamodel_update_time ↕	count ↕	_time ↕	site ↕	user ↕	http_se
			2020-11-18 00:17:23	www.laurentmarot.fr	7653af1d34f8faad3a35c9bdd3664e25	0655c31
			2020-11-18 00:28:59	www.laurentmarot.fr	96d4d5cbfe66cda570441ca0c1fdb6bb	1ba94f7
			2020-11-18 00:36:32	www.laurentmarot.fr	898cd7a9344baf15d4d8940f90a69865	d9b700a
			2020-11-18 00:45:37	www.laurentmarot.fr	63a67369142c0a60d8e1e9b50170aa65	042dd87
			2020-11-18 00:57:33	www.laurentmarot.fr	5606f46ed123c302c64e62d276023a4a	b0accd4
			2020-11-18 01:05:42	www.laurentmarot.fr	829a2a82704072db7428ba6be053c945	a552972
			2020-11-18 01:28:41	www.laurentmarot.fr	c7860cc3fd06c7de7c6900edfbd57aa	532b0de
			2020-11-18 01:29:01	www.laurentmarot.fr	24e954e4e9919a05f7b22b0225150589	565d0cc
			2020-11-18 02:01:59	www.laurentmarot.fr	15594fa6b238b6c46d23bad12e044965	96cff0b

Generate pages

Last 30 days

266 events (10/25/20 12:00:00.000 AM to 11/24/20 12:40:35.000 PM)

100 results 20 per page

site	http_request
www.laurentmarot.fr	/
www.laurentmarot.fr	/wordpress/?feed=rss2&cat=21
www.laurentmarot.fr	/wordpress/?p=4026
www.laurentmarot.fr	/wordpress/?feed=rss2
www.laurentmarot.fr	/wordpress/wp-content/themes/gazette/thumb.php?src=http://www.la
www.laurentmarot.fr	/wordpress/?page_id=2
www.laurentmarot.fr	/wordpress/?p=2364
www.laurentmarot.fr	/wordpress/?p=2263
www.laurentmarot.fr	/wordpress/?cat=21&paged=4
www.laurentmarot.fr	/wordpress/?p=3701
www.laurentmarot.fr	/wordpress/?cat=39
www.laurentmarot.fr	/index20200224.html
www.laurentmarot.fr	/wordpress/?page_id=1492

Et voilà de jolis tableaux de bord

