



Ansinelli Yohann, Ralite Justin, Mathéo Balazuc




Installation Splunk

Build Splunk

Dans un premier temps il va falloir créer un compte sur le site de splunk (étape obligatoire) pour pouvoir télécharger ensuite le paquet :

 **Linux**

 **Mac OS**

| | | |
|--|-----------------------|--|
| 3.x+, 4.x+, or 5.4.x kernel Linux distributions | .tgz 586.38 MB | Download Now  |
| | .rpm 586.57 MB | Download Now  |
| | .deb 440.66 MB | Download Now  |

On télécharge le paquet ".tgz" grâce à la commande suivante :

```
wget -O splunk-9.1.2-b6b9c8185839-Linux-x86_64.tgz  
"https://download.splunk.com/products/splunk/releases/9.1.2/linux/splunk-9.1.2-b6b9c8185839-Linux-x86_64.tgz" --no-check-certificate
```

Pour extraire les fichiers on fait la commande :

```
tar xvzf splunk-7.0.1-2b5b15c4ee89-Linux-x86_64.tgz
```

On se rend dans le répertoire "splunk/bin/" et on lance la commande suivante pour démarrer splunk :

```
./splunk start
```

On accepte la license :

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

On crée l'utilisateur root pour splunk :

```

Please enter an administrator username: root
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
ERROR: Password did not meet complexity requirements. Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/home/test/splunk/etc/openldap/ldap.conf.default' to '/home/test/splunk/etc/openldap/ldap.conf'.
Generating RSA private key, 2048 bit long modulus
...+++++
.....+++++
e is 65537 (0x10001)
writing RSA key

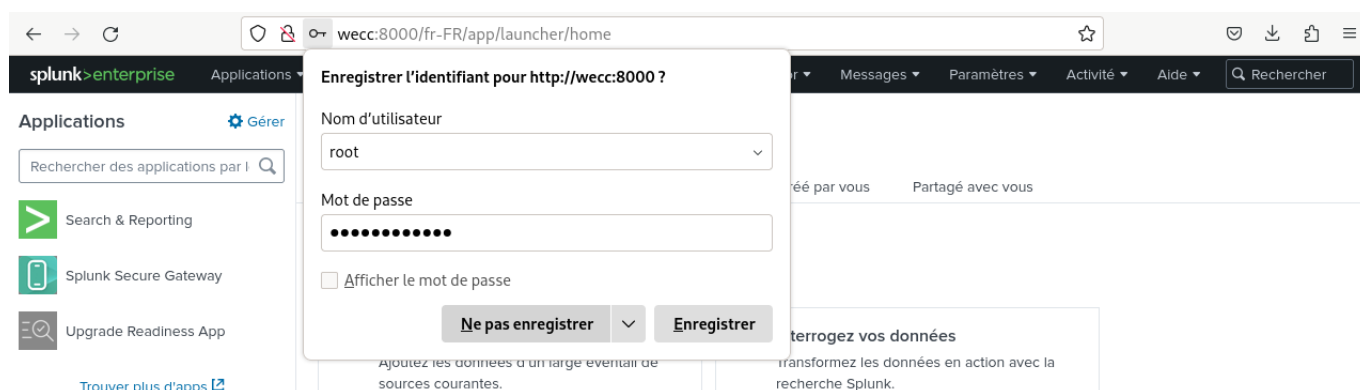
Generating RSA private key, 2048 bit long modulus

```

Désormais on peut accéder à l'interface web à l'url suivant :

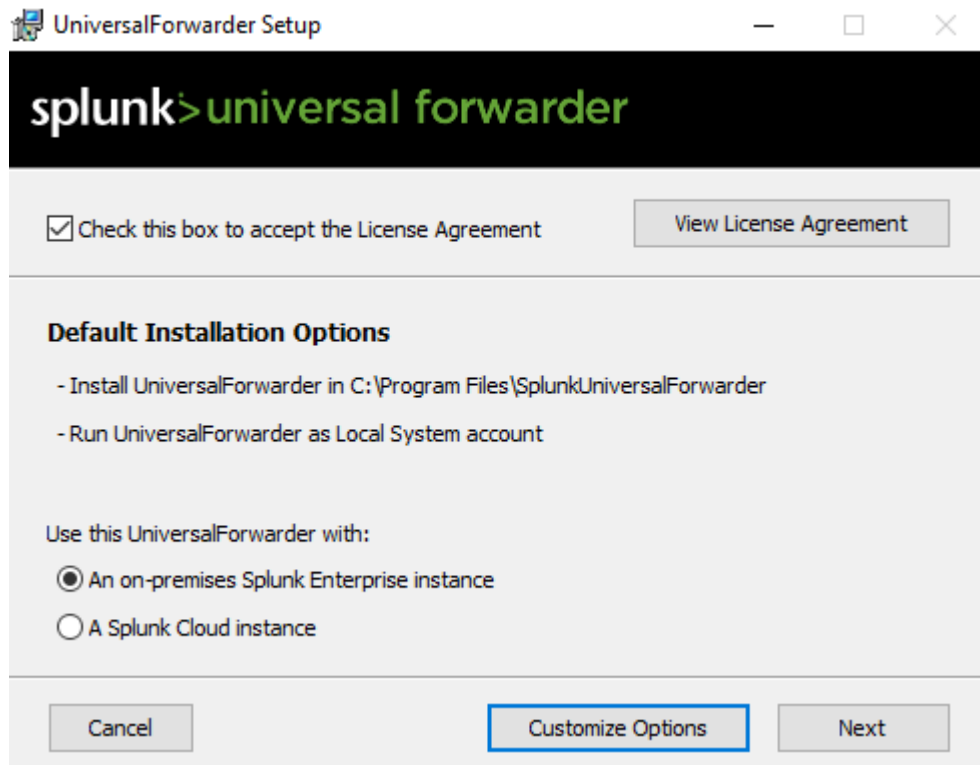
The Splunk web interface is at <http://WECC:8000>

On peut voir le user wecc car le serveur splunk a été installé sur la même machine sur le serveur OpenWEC. On est sur le port 8000 en HTTP. Maintenant une fois sur l'interface web, on s'identifie avec l'utilisateur admin qu'on a créé et on peut maintenant utiliser Splunk :

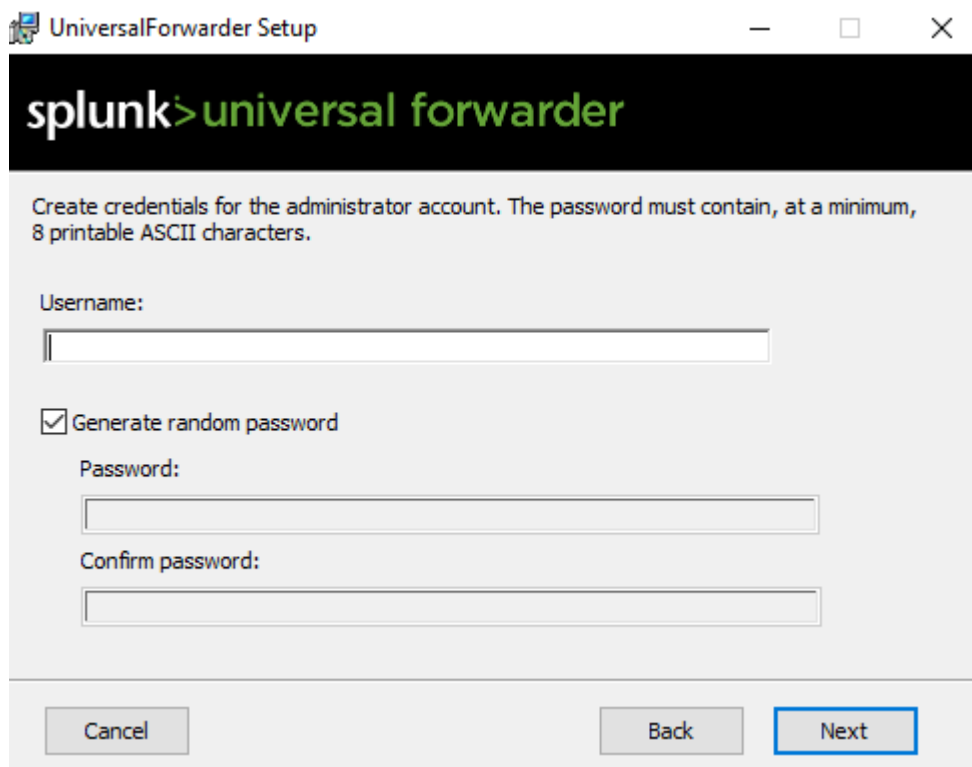


Ajouter un client Windows

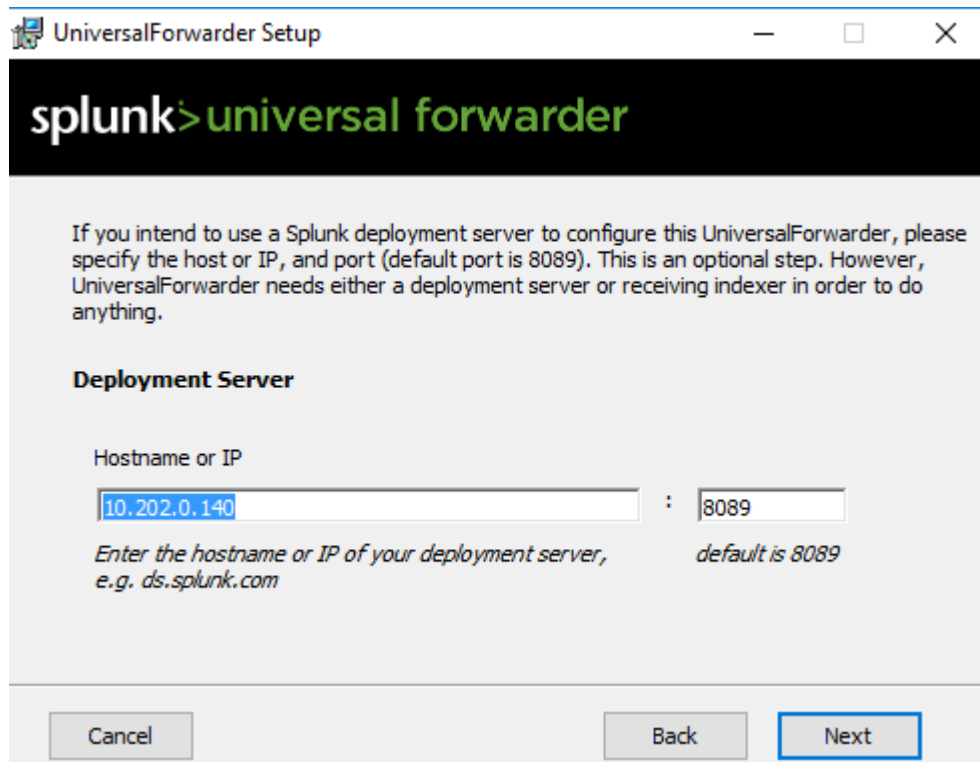
On va maintenant ajouter nos machines, pour cela on va dans un premier temps sur le serveur se rendre dans **Paramètres > Transmission et Réception** , pour venir ajouter un nouveau receveur de données, on va venir écouter sur le port 9997 :



Maintenant on va passer sur notre client windows où on va venir installer l'exécutable **Splunk Forwarder** et on le lance sur la machine :



On peut faire une installation avec notre customisation mais pour notre part on va cliquer simplement sur "Next" et faire l'installation simplement. On va venir nous demander de créer l'utilisateur administrateur comme pour le serveur, on l'appellera "test" :



The screenshot shows the 'UniversalForwarder Setup' window. At the top, there's a header with the Splunk logo and 'universal forwarder'. Below this, a text block explains that a deployment server is optional but needed for configuration. The 'Deployment Server' section has a 'Hostname or IP' label. Below it, a text input field contains '10.202.0.140' and a port input field contains '8089'. A note below the inputs says 'Enter the hostname or IP of your deployment server, e.g. ds.splunk.com' and 'default is 8089'. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons, with 'Next' being the active button.

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Deployment Server

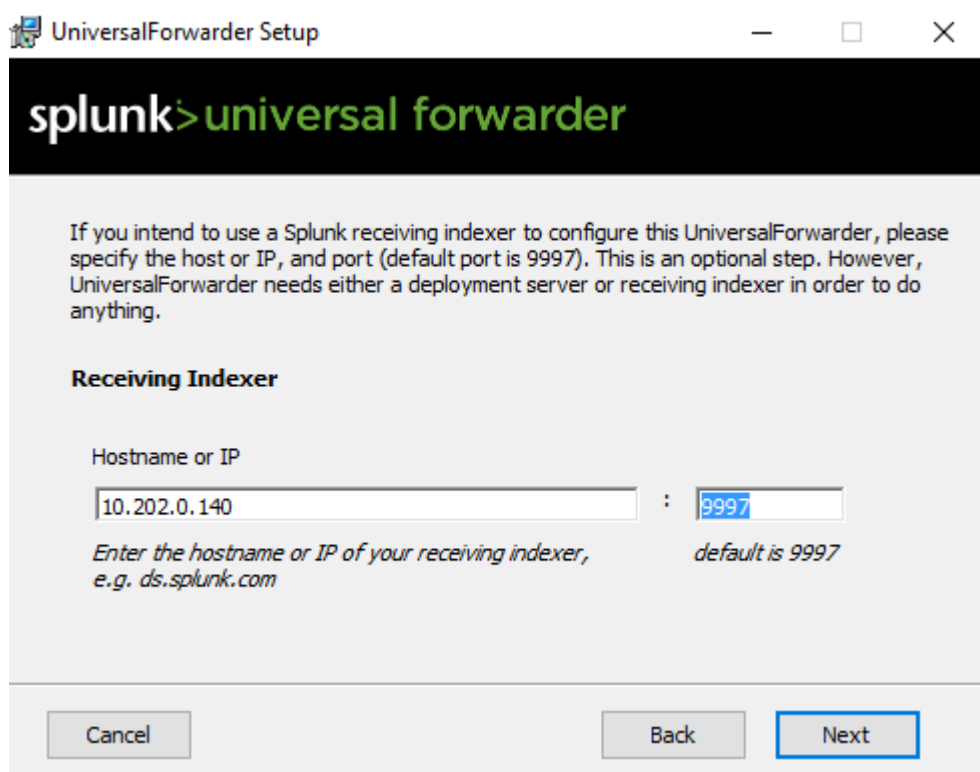
Hostname or IP

10.202.0.140 : 8089

Enter the hostname or IP of your deployment server, e.g. ds.splunk.com default is 8089

Cancel Back Next

Ensuite on nous demandera de spécifier le serveur de déploiement, pour notre part il s'agit de la machine où on a installé le serveur avec le port par défaut 8089 :



The screenshot shows the 'UniversalForwarder Setup' window. At the top, there's a header with the Splunk logo and 'universal forwarder'. Below this, a text block explains that a receiving indexer is optional but needed for configuration. The 'Receiving Indexer' section has a 'Hostname or IP' label. Below it, a text input field contains '10.202.0.140' and a port input field contains '9997'. A note below the inputs says 'Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com' and 'default is 9997'. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons, with 'Next' being the active button.

UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

Receiving Indexer

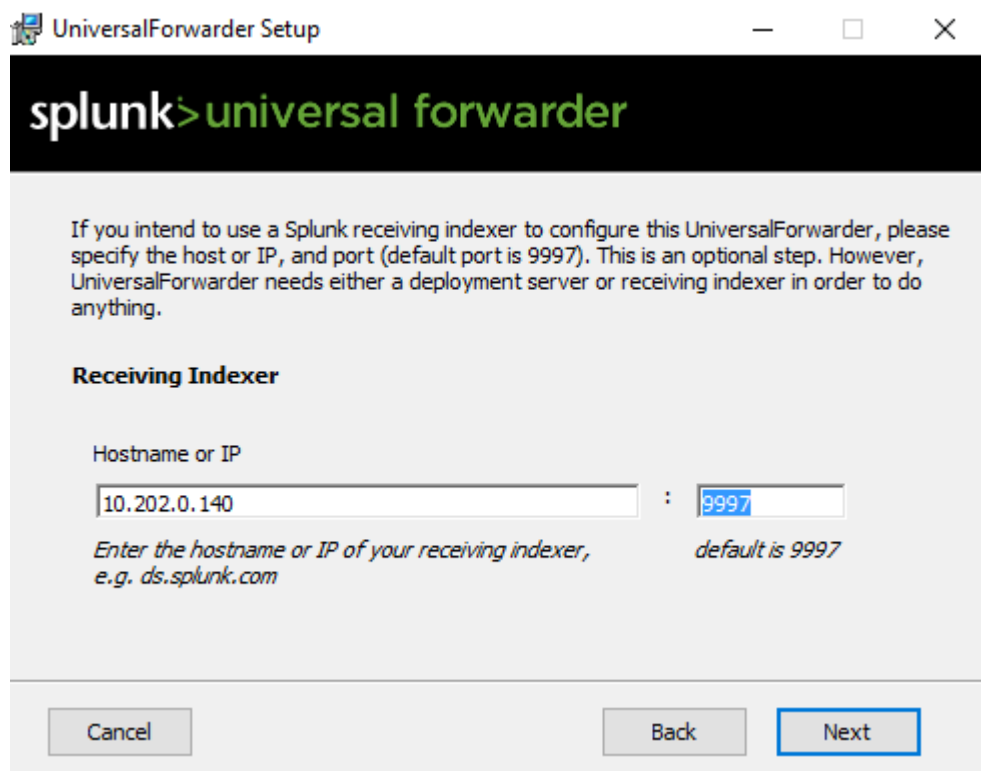
Hostname or IP

10.202.0.140 : 9997

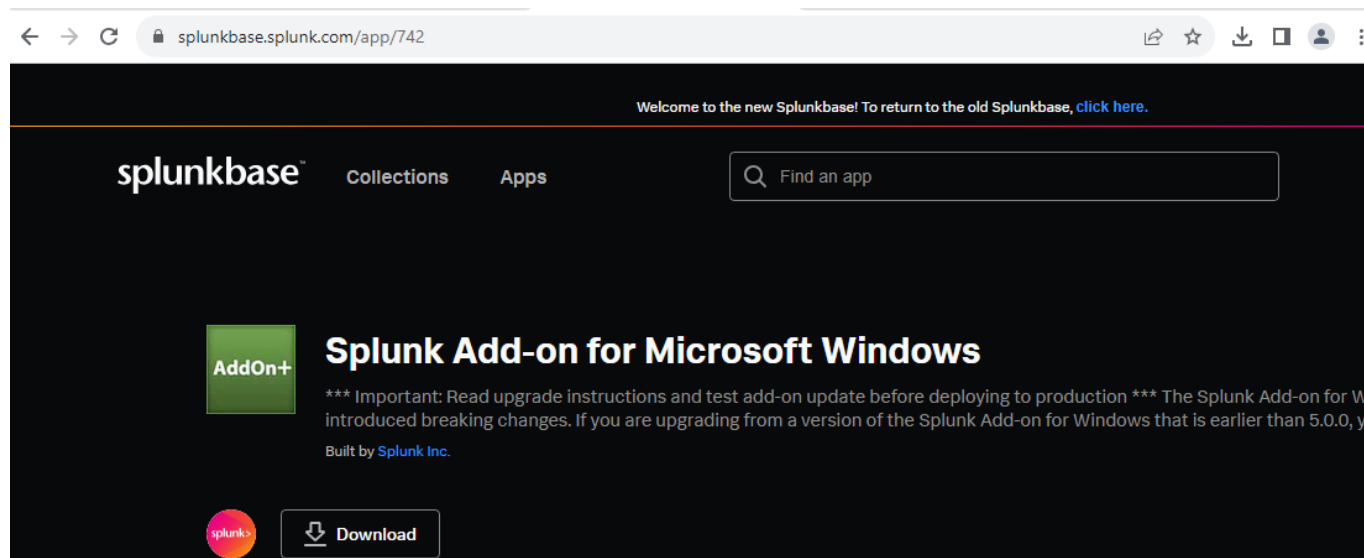
Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com default is 9997

Cancel Back Next


Et on viendra nous demander par la suite le receveur qu'on a configuré sur le port 9997 :



L'installation du forwarder se termine ici, néanmoins notre serveur ne détecte toujours pas le client. Pour cela on va venir lui installer un addon :



On obtiens un .rar qu'on va venir extraire pour obtenir le dossier "Splunk_TA_windows"

| | | | |
|---|-------------------|----------------|--------|
|  Splunk Photo | 12/6/2023 6:45 PM | File folder | |
|  splunk-add-on-for-microsoft-windows_... | 12/6/2023 6:30 PM | Archive WinRAR | 149 KB |

On va venir déplacer le dossier sur le chemin suivant : **C:\Program Files\SplunkUniversalForwarder\etc\apps**

| This PC > Windows 2016 (C:) > Program Files > SplunkUniversalForwarder > etc > apps | | | | |
|---|-------------------|-------------|------|--|
| Name | Date modified | Type | Size | |
| introspection_generator_addon | 12/6/2023 5:59 PM | File folder | | |
| learned | 12/6/2023 6:00 PM | File folder | | |
| search | 12/6/2023 5:59 PM | File folder | | |
| splunk_httpinput | 12/6/2023 5:59 PM | File folder | | |
| splunk_ingest_actions | 12/6/2023 6:00 PM | File folder | | |
| splunk_internal_metrics | 12/6/2023 5:59 PM | File folder | | |
| Splunk_TA_windows | 12/6/2023 6:37 PM | File folder | | |
| SplunkUniversalForwarder | 12/6/2023 6:00 PM | File folder | | |

Dans le dossier "Splunk_TA_windows" on va venir récupérer le fichier de conf "inputs.conf" :

| This PC > Windows 2016 (C:) > Program Files > SplunkUniversalForwarder > etc > apps > Splunk_TA_windows > default | | | | |
|---|------------------|-----------|--------|--|
| Name | Date modified | Type | Size | |
| app.conf | 8/2/2023 4:39 AM | CONF File | 1 KB | |
| eventtypes.conf | 8/2/2023 4:39 AM | CONF File | 25 KB | |
| inputs.conf | 8/2/2023 4:39 AM | CONF File | 20 KB | |
| macros.conf | 8/2/2023 4:39 AM | CONF File | 3 KB | |
| props.conf | 8/2/2023 4:39 AM | CONF File | 115 KB | |
| tags.conf | 8/2/2023 4:39 AM | CONF File | 12 KB | |
| transforms.conf | 8/2/2023 4:39 AM | CONF File | 39 KB | |
| wmi.conf | 8/2/2023 4:39 AM | CONF File | 5 KB | |
| workflow_actions.conf | 8/2/2023 4:39 AM | CONF File | 2 KB | |

On va venir copier ce fichier dans un nouveau dossier qu'on va devoir créer dans le dossier "Splunk_TA_windows", on crée dans un premier temps le dossier local vide, auquel on va venir ajouter le fichier "inputs.conf" :

| Name | Date modified | Type | Size | |
|---------------------|-------------------|---------------|-------|--|
| appserver | 8/2/2023 4:39 AM | File folder | | |
| bin | 8/2/2023 4:39 AM | File folder | | |
| default | 8/2/2023 4:39 AM | File folder | | |
| LICENSES | 8/2/2023 4:39 AM | File folder | | |
| local | 12/6/2023 6:41 PM | File folder | | |
| lookups | 8/2/2023 4:39 AM | File folder | | |
| metadata | 8/2/2023 4:39 AM | File folder | | |
| README | 8/2/2023 4:39 AM | File folder | | |
| static | 8/2/2023 4:39 AM | File folder | | |
| app.manifest | 8/2/2023 4:39 AM | MANIFEST File | 2 KB | |
| README.txt | 8/2/2023 4:39 AM | Text Document | 1 KB | |
| splunkbase.manifest | 9/26/2023 8:23 AM | MANIFEST File | 12 KB | |
| THIRDPARTY | 8/2/2023 4:39 AM | File | 2 KB | |
| VERSION | 8/2/2023 4:39 AM | File | 1 KB | |

On vient éditer le fichier "inputs.conf" avec notepad et on va venir modifier certains paramètres en jaune pour les mettre en false où pour changer la valeur de 1 à 0 :

```
[WinEventLog://Application]
disabled = 0
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false

[WinEventLog://Security]
disabled = 0
start_from = oldest
current_only = 0
evt_resolve_ad_obj = 1
checkpointInterval = 5
blacklist1 = EventCode="4662" Message="Object Type:(?!\\s*groupPolicyContainer)"
blacklist2 = EventCode="566" Message="Object Type:(?!\\s*groupPolicyContainer)"
renderXml=false

[WinEventLog://System]
disabled = 0
start_from = oldest
current_only = 0
checkpointInterval = 5
renderXml=false
```

Maintenant la dernière étape va consister à lancer l'application **Services** et trouver le service "SplunkForwarder" pour le redémarrer :

The screenshot shows the Windows Services console window titled "Services (Local)". On the left, the "SplunkForwarder" service is selected, showing its description: "SplunkForwarder is the remote data collection service for Splunk, a data platform for operational intelligence. If it is stopped, Splunk will stop collecting and sending data to Splunk indexers, which may result in data loss. Please see www.splunk.com for more information. Questions can be submitted to www.splunk.com/answers or for supported customers www.splunk.com/page/submit_issue". On the right, a list of services is displayed in a table format.

| Name | Description | Status | Startup Type | Log |
|--------------------------------|----------------------|----------------|------------------|------------|
| Security Accounts Manager | The startup ... | Running | Automatic | Loc |
| Sensor Data Service | Delivers dat... | | Manual (Trig... | Loc |
| Sensor Monitoring Service | Monitors va... | | Manual (Trig... | Loc |
| Sensor Service | A service fo... | | Manual (Trig... | Loc |
| Server | Supports fil... | Running | Automatic | Loc |
| Shell Hardware Detection | Provides no... | Running | Automatic | Loc |
| Smart Card | Manages ac... | | Disabled | Loc |
| Smart Card Device Enumera... | Creates soft... | | Manual (Trig... | Loc |
| Smart Card Removal Policy | Allows the s... | | Manual | Loc |
| SNMP Trap | Receives tra... | | Manual | Loc |
| Software Protection | Enables the ... | | Automatic (D... | Net |
| Special Administration Con... | Allows adm... | | Manual | Loc |
| SplunkForwarder | SplunkForw... | Running | Automatic | Loc |
| Spot Verifier | Verifies pote... | | Manual (Trig... | Loc |
| SSDP Discovery | Discovers n... | | Disabled | Loc |
| State Repository Service | Provides re... | Running | Manual | Loc |
| Still Image Acquisition Events | Launches a... | | Manual | Loc |
| Storage Service | Provides en... | | Manual (Trig... | Loc |
| Storage Tiers Management | Optimizes t... | | Manual | Loc |
| Superfetch | Maintains a... | | Manual | Loc |
| Sync Host_50bd3 | This service ... | Running | Automatic (D... | Loc |

On peut maintenant se rendre dans **Search and Reporting** puis dans **Résumé des données** et on pourra voir notre client windows :

Résumé des données

Hosts (1)

Sources (1)

Sourcetypes (1)

filtre

| Hôte | | Nombre | Dernière mise à jour |
|---------|--|--------|-------------------------|
| MEEREEN | | 1,436 | 06/12/2023 18:47:18,000 |

On peut notamment voir les logs en indiquant dans la barre de recherche `index="main"` :

Nouvelle recherche

Enregistrer sousCréer une vue de tableFermer

index="main"

24 dernières heures

✓ 189 événements (05/12/2023 18:00:00,000 à 06/12/2023 18:57:25,000)

Aucun échantillon d'événement

Tâche

Mode Intelligent

Événements (189)

Patterns

Statistiques

Visualisation

Mettre en forme la chronologie

Zoom arrière

Zoom sur la sélection

Annuler la sélection

1 heure par colonne

Liste

Format

20 par page

Préc

1

2

3

4

5

6

7

8

Suivant

Masquer les champs

CHAMPS

SÉLECTIONNÉS

host 1

source 1

sourcetype 1

CHAMPS INTÉRESSANTS

i

Durée

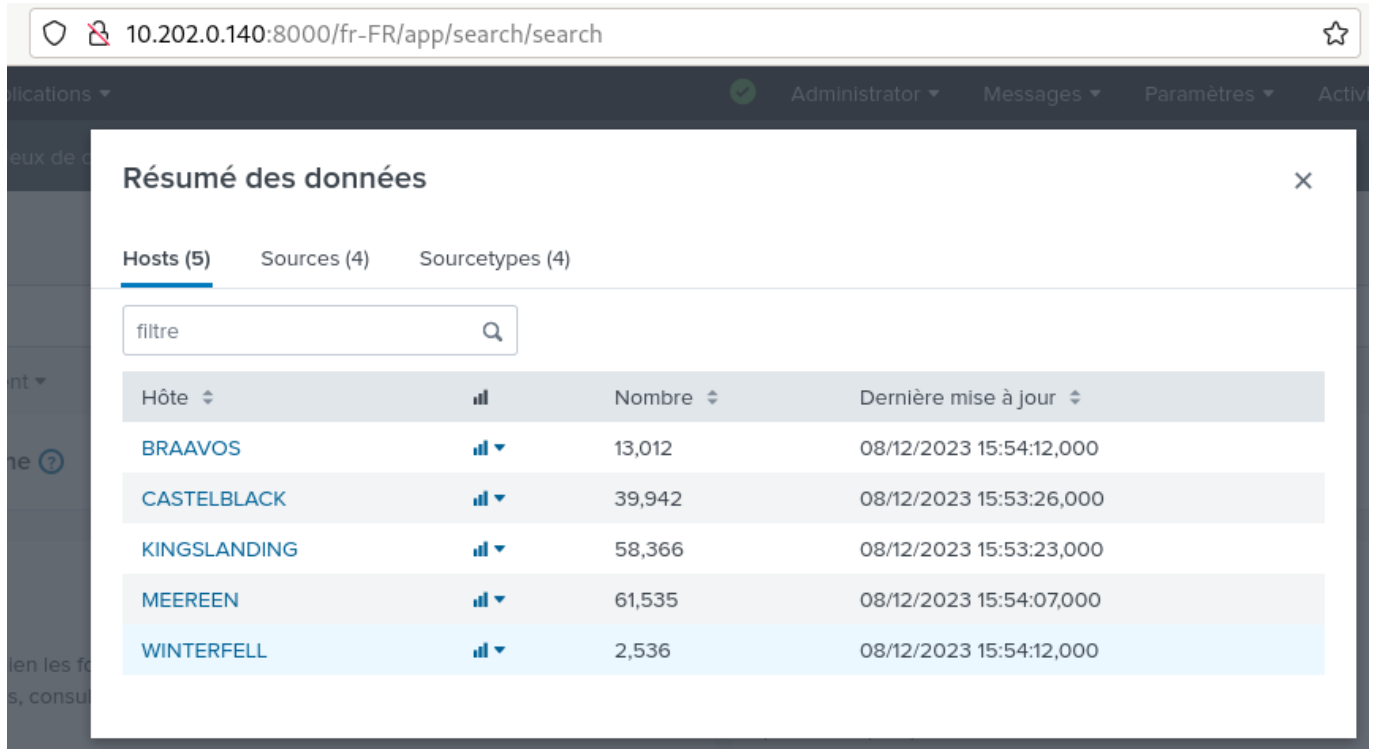
Événement

>

06/12/2023 18:47:17,000

12/06/2023 06:47:17 PM
LogName=Application
EventCode=1001
EventType=4
ComputerName=meereen.essos.local
Afficher toutes les 40 lignes
host = MEEREEN ; source = WinEventLog:Application ; sourcetype = WinEventLog:Application

Une fois l'ensemble des agents déployés :



| Hôte | Nombre | Dernière mise à jour |
|--------------|--------|-------------------------|
| BRAAVOS | 13,012 | 08/12/2023 15:54:12,000 |
| CASTELBLACK | 39,942 | 08/12/2023 15:53:26,000 |
| KINGSLANDING | 58,366 | 08/12/2023 15:53:23,000 |
| MEEREN | 61,535 | 08/12/2023 15:54:07,000 |
| WINTERFELL | 2,536 | 08/12/2023 15:54:12,000 |

Configuration de la réception des Syslogs

Pour configurer la réception des Syslogs on va se rendre dans **Paramètres > Entrées de données** et on va aller sur **UDP** pour ajouter un nouveau et on va venir spécifier le port 514 :

Configurez cette instance pour écouter tous les ports TCP ou UDP pour capturer des données envoyées sur le réseau (telles que syslog). [En savoir plus](#)

| | | |
|--|---|--------------------------------------|
| | <input type="radio"/> TCP | <input checked="" type="radio"/> UDP |
| Port ? | <input type="text" value="514"/> | |
| | Exemple : 514 | |
| Remplace le nom de la source ? | <input type="text" value="facultatif"/> | |
| | host:port | |
| Accepter uniquement une connexion de ? | <input type="text" value="facultatif"/> | |
| | exemple : 10.1.2.3, !badhost.splunk.com, *.splunk.com | |

On spécifie ensuite en entrée qu'on veut des logs syslogs :

Paramètres d'entrée

Vous pouvez également configurer des paramètres d'entrée supplémentaires pour cette entrée de données de la manière suivante :

Sourcetype

Le sourcetype est l'un des champs par défaut que la plateforme Splunk affecte à toutes les données entrantes. Il indique à la plateforme Splunk le type de données dont vous disposez, de sorte qu'elle est en mesure de les formater de manière intelligente pendant l'indexation. Et cela représente une manière de classer vos données afin que vous puissiez y effectuer facilement des recherches.

Sélectionner

Nouveau

syslog ▾

Résumé

Type d'input Port UDP
Numéro de port 514
Remplace le nom de la sour S/O
Limiter à l'host S/O
Sourcetype syslog
Contexte de l'application search
Hôte (adresse IP du serveur distant)
Index default

Désormais notre Splunk sera en écoute sur le port 514 pour les logs syslogs. Sur la machine windows, on va venir installer via la page de téléchargement Microsoft, Sysmon et on va venir récupérer le fichier de conf xml sur le github suivant :

```
https://github.com/SwiftOnSecurity/sysmon-config/blob/master/sysmonconfig-export.xml
```

On va ensuite venir lancer la commande suivante pour pouvoir lancer Sysmon sur la machine :

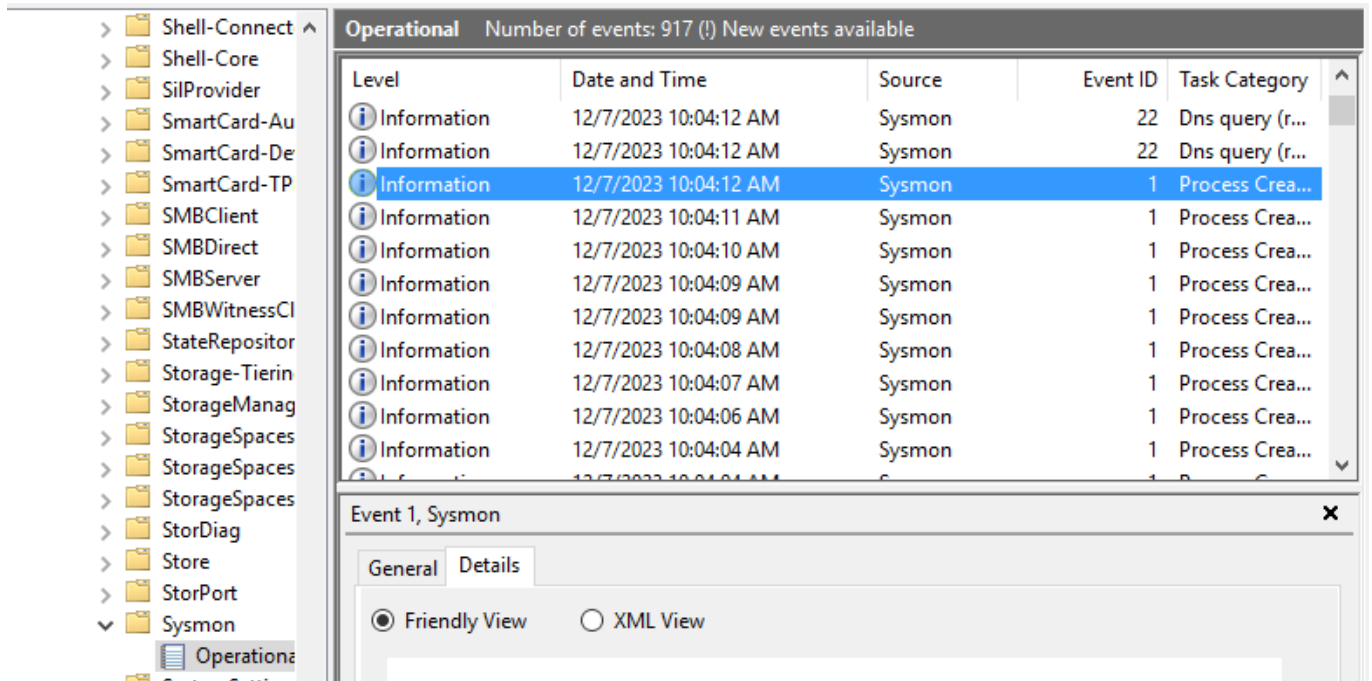
```
System Monitor v15.11 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.90
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

Une fois lancé on va revenir sur le fichier inputs.conf vu précédemment pour venir y ajouter quelques lignes :

```
##### OS Logs #####
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disbled = false
renderXml = true
```

Enfin on va venir sur l'application **Event Viewer** et on va suivre le chemin pour accéder à l'ensemble des logs sysmon : Applications and Services > Microsoft > Windows > Sysmon



On peut maintenant retourner sur notre serveur pour voir si il remonte des logs sysmons, on précise dans nouvelle recherche source="WinEventLog:Microsoft-Windows-Sysmon/Operational" et on a les logs sysmon qui remonte :

Nouvelle recherche Enregistrer sous Crée une vue de table Fermer

host=MEEREN source="WinEventLog:Microsoft-Windows-Sysmon/Operational" 24 dernières heures 🔍

✓ 1 009 événement (06/12/2023 10:00:00,000 à 07/12/2023 10:18:16,000) Aucun échantillon d'événement Tâche II Mode Intelligent ▼

Événements (1 009) Patterns Statistiques Visualisation

Mettre en forme la chronologie — Zoom arrière + Zoom sur la sélection × Annuler la sélection 1 heure par colonne

Liste Format 20 par page < Préc 1 2 3 4 5 6 7 8 ... Suivant >

< Masquer les champs

CHAMPS SÉLECTIONNÉS

- a host 1
- a source 1
- a sourcetype 1

CHAMPS INTÉRESSANTS

- # index 1
- # linecount 1
- a punct 1
- a splunk_server 1

+ Extraction de nouveaux champs

| i | Durée | Événement |
|---|-------------------------|---|
| > | 07/12/2023 10:17:30,000 | <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"><System><Provider Name='Microsoft-Windows-Sysmon' Guid='{5770385F-C22A-43E0-BF4C-06F5698FFB09}' /><EventID>1</EventID><Version>5</Version><Level>4</Level><Task>1</Task><Opcode>0</Opcode><Keywords>0x8000000000000000</Keywords><TimeCreated SystemTime>'2023-12-07T09:17:30.387721700Z' /><EventRecordID>1044</EventRecordID><Correlation><Execution ProcessID>'6380' ThreadID='7100' /><Channel>Microsoft-Windows-Sysmon/Operational</Channel><Computer>meereen.essos.local</Computer><Security UserID>'S-1-5-18' /></System><EventData><Data Name='RuleName'>-</Data><Data Name='UtcTime'>2023-12-07 09:17:30.378</Data><Data Name='ProcessGuid'>{3CBB8FBE-8DAA-6571-B60B-000000001200}</Data><Data Name='ProcessId'>1908</Data><Data Name='Image'>C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe</Data><Data Name='FileVersion'>9.1.2</Data><Data Name='Description'>Registry monitor</Data><Data Name='Product'>splunk Appl ications</Data><Data Name='Company'>Splunk Inc.</Data><Data Name='OriginalFileName'>splunk-regmon.exe</Data><Data Name='CommandLine'>'C:\Program Files\SplunkUniversalForwarder\bin\splunk-regmon.exe'</Data><Data Name='CurrentDirectory'>C:\Windows\system32</Data><Data Name='User'>NT AUTHORITY\SYSTEM</Data><Data Name='LogonGuid'>{3CBB8FBE-0205-656E-E703-000000000000}</Data><Data Name='LogonId'>0x3e7</Data><Data Name='TerminalSessionId'>0</Data><Data Name='IntegrityLevel'>System</Data><Data Name='Hashes'>MD5=691A5888DF01739394E5AA8768D34B7F, SHA256=394540275287579C4A86A0D5FEAE89330D76DF2AB1E667C6D335792607EDC96, IMPHASH=9630768262AAB824390F0A82C3B7E854</Data><Data Name='ParentProcessGuid'>{3CBB8FBE-8A7E-6571-150B-000000001200}</Data><Data Name='ParentProcessId'>9920</Data><Data Name='ParentImage'>C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe</Data><Data Name='ParentCommandLine'>'C:\Program Files\SplunkUniversalForwarder\bin\splunkd.exe' service</Data><Data Name='ParentUser'>NT AUTHORITY\SYSTEM</Data></EventData></Event> |

host = MEEREN source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational