Réalisation TP		BTS SIO	
Prénom – Nom	SALVADOR Louis	**TP**	Wazuh
Option	**SISR** ☒	**SLAM** ☐	
Situation	**Formation X** ☒	**Entreprise** ☐	

Lieu de réalisation	Ecole IRIS Paris	
Période de réalisation		
Modalité de réalisation	VÉCUE ☒	OBSERVÉE ☐

Intitulé de la mission	Titre de la mission **Wazuh -Une Platforme de sécurité Open source**
Description du contexte de la mission	Description en 2 à 3 lignes maxi *Wazuh est un système open source de détection d'intrusion basé sur l'hôte (HIDS). Il permet d'analyser les logs, de monitorer l'intégrité des fichiers, de détecter les rootkits et les vulnérabilités, d'évaluer les configurations et de répondre aux incidents. L'architecture de la solution Wazuh repose sur des agents multiplateformes de transfert léger. Ces agents s'exécutent sur des systèmes monitorés et communiquent avec un serveur centralisé sur lequel les données sont analysées. En outre, ce système propose un plug-in Kibana complet pour gérer la configuration, monitorer les statuts, effectuer des recherches et visualiser les données d'alerte.*

Ressources et outils utilisés	Liste des ressources disponibles et outils utilisés (Documentations, Matériels et Logiciels) Procédure mise en place de Wazuh Matériel : ISO Debian, Windows 10 Logiciel : VMware
Résultat attendu	Résultat attendu avec la réalisation de cette mission
Contraintes	Contraintes : techniques | budgétaires | temps | O.S. ou outils imposés…

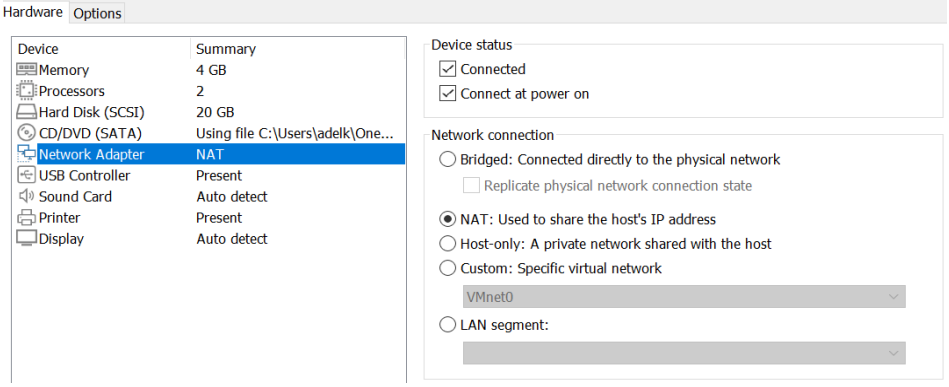
Compétences associées	Liste des intitulés du tableau de compétences (avec les références)

Description simplifiée des différentes étapes de réalisation de la mission

en mettant en évidence la démarche suivie, les méthodes et les techniques utilisées

Ressource :

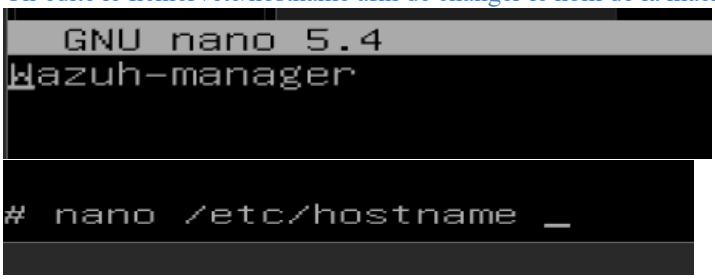
Nous allons nous menir d'un Debian 11 pour l'élaboration de la machine Wazuh-Manager (carte en NAT)



Tout d'abord on va mettre à jour la machine :

```
root@Wazuh-manager:~# apt update && apt upgrade
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Atteint :3 http://deb.debian.org/debian bullseye-updates InRelease
Atteint :4 https://packages.wazuh.com/4.x/apt stable InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@Wazuh-manager:~#
```

On édite le fichier /etc/hostname afin de changer le nom de la machine en « Wazuh-Manager »




```
# nano /etc/hostname _
```

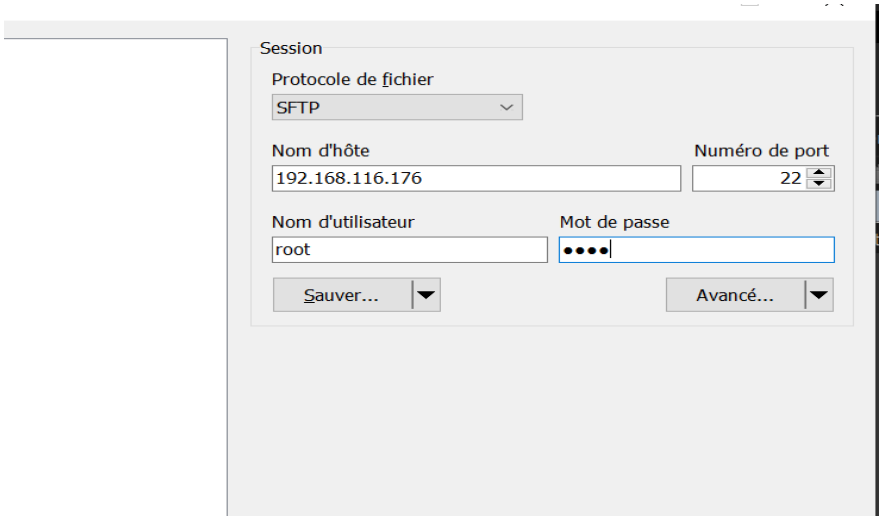
On va maintenant installer un logiciel (WinSCP) permettant de transférer un ou plusieurs fichier depuis la machine physique vers une machine virtuel (et inversement) via une connections ssh.
(On va transférer un script d'installation permettant d'installer les fonctionnalités de Wazuh).

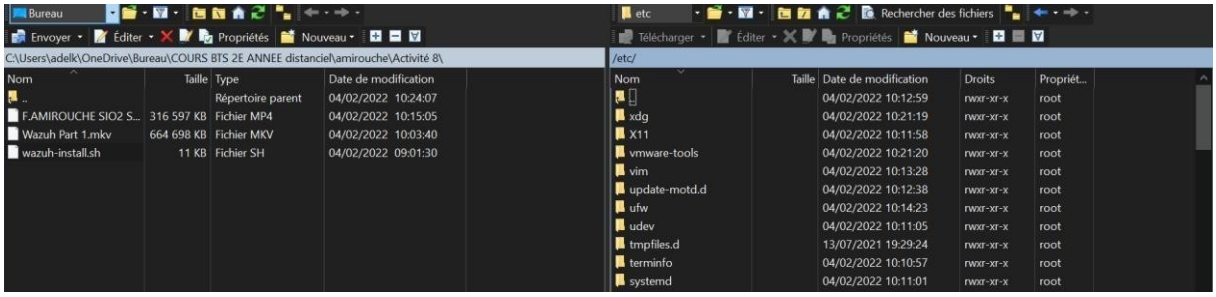
```
root@Wazuh-manager:~# apt install -y ssh_
```

```
root@Wazuh-manager:~# service ssh status
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-02-04 19:06:55 CET; 10min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 613 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 635 (sshd)
      Tasks: 1 (limit: 4639)
     Memory: 3.8M
        CPU: 121ms
     CGroup: /system.slice/ssh.service
             └─635 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

févr. 04 19:06:51 Wazuh-manager systemd[1]: Starting OpenBSD Secure Shell server...
févr. 04 19:06:55 Wazuh-manager sshd[635]: Server listening on 0.0.0.0 port 22.
févr. 04 19:06:55 Wazuh-manager sshd[635]: Server listening on :: port 22.
```

Maintenant on lance l'application WinSCP afin d'établir une conections ssh de la machine physique vers la machine virtuel Wazuh-manager :





On vérifie la présence du fichier script sur la machine virtuelle (Wazuh-manager) :

```
root@Wazuh-manager:~# ls /etc/wazuh-install.sh
/etc/wazuh-install.sh
```

Le fichier est présent dans le répertoire /etc., nous allons accorder à l'administrateur les droits d'exécution :

```
root@Wazuh-manager:~# chmod +x /etc/wazuh-install.sh
root@Wazuh-manager:~#
root@Wazuh-manager:~# ls -l /etc/wazuh-install.sh
-rwxr-xr-x 1 root root 10400  4 févr. 09:01 /etc/wazuh-install.sh
root@Wazuh-manager:~#
```

Les droits modifiés ont bien été pris en compte.

Rendez vous maintenant dans le répertoire /etc ou nous allons lancer le script d'installation via la commande « ./wazuh-

install.sh »

```
root@Wazuh-manager:/etc# ./wazuh-install.sh
#########################################################################################
Hi!
Ce script vous permettra d'installer wazuh-manager, elasticsearch, filebeat & kibana
By Fethi AMIROUCHE
#########################################################################################

#############################################################################
Installation package nécessaires à l'installation de Wazuh (Entrée) :
#############################################################################

Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
libcap2-bin est déjà la version la plus récente (1:2.44-1).
lsb-release est déjà la version la plus récente (11.1.0).
lsb-release passé en « installé manuellement ».
wget est déjà la version la plus récente (1.21-1+deb11u1).
Les paquets supplémentaires suivants seront installés :
  dirmngr gir1.2-glib-2.0 gir1.2-packagekitglib-1.0 gnupg-l10n gnupg-utils gpg gpg-agent
  gpg-wks-client gpg-wks-server gpgconf gpgsm libappstream4 libassuan0 libcurl4 libdw1
  libgirepository-1.0-1 libglib2.0-bin libgstreamer1.0-0 libksba8 libnpth0 libpackagekit-glib2-18
  libpolkit-agent-1-0 libpolkit-gobject-1-0 libstemmer0d libunwind8 libyaml-0-2 packagekit
  packagekit-tools pinentry-curses policykit-1 python3-dbus python3-distro-info python3-gi
  python3-software-properties unattended-upgrades
Paquets suggérés :
  dbus-user-session pinentry-gnome3 tor parcimonie xloadimage scdaemon gstreamer1.0-tools
  appstream pinentry-doc python-dbus-doc python3-dbus-dbg bsd-mailx default-mta
  | mail-transport-agent needrestart powermgmt-base zip
Les NOUVEAUX paquets suivants seront installés :
  apt-transport-https curl dirmngr gir1.2-glib-2.0 gir1.2-packagekitglib-1.0 gnupg gnupg-l10n
  gnupg-utils gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm libappstream4 libassuan0
  libcurl4 libdw1 libgirepository-1.0-1 libglib2.0-bin libgstreamer1.0-0 libksba8 libnpth0
  libpackagekit-glib2-18 libpolkit-agent-1-0 libpolkit-gobject-1-0 libstemmer0d libunwind8
  libyaml-0-2 packagekit packagekit-tools pinentry-curses policykit-1 python3-dbus
  python3-distro-info python3-gi python3-software-properties software-properties-common
  unattended-upgrades unzip
0 mis à jour, 40 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 13,4 Mo dans les archives.
Après cette opération, 33,0 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] _
```

```
Paramétrage de software-properties-common (0.96.20.2-2.1) ...
Traitement des actions différées (« triggers ») pour mailcap (3.69) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-13+deb11u2) ...
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour dbus (1.12.20-2) ...
########################################
Installation de la clé GPG (Entrée) :
########################################
```

```
Installation de la clé GPG (Entrée) :
########################################

Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
########################################
Ajout du dépôt de référence (Entrée) :
########################################

deb https://packages.wazuh.com/4.x/apt/ stable main
#####################################################
Mettre à jour les informations du package (Entrée) :
#####################################################

Réception de :1 http://security.debian.org/debian-security bullseye-security InRelease [44,1 kB]
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Réception de :3 http://deb.debian.org/debian bullseye-updates InRelease [39,4 kB]
Réception de :4 https://packages.wazuh.com/4.x/apt stable InRelease [14,0 kB]
Réception de :5 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [17,6 kB]
115 ko réceptionnés en 0s (300 ko/s)
Lecture des listes de paquets... Fait
#############################################################
Installation du package du gestionnaire Wazuh (Entrée) :
#############################################################

Paramétrage de wazuh-manager (4.2.5-1) ...
#########################################################################
Activation et démarrage du service de gestionnaire Wazuh (Entrée) :
#########################################################################

Synchronizing state of wazuh-manager.service with SysV service script with /lib/systemd/systemd-sysv
-install.
Executing: /lib/systemd/systemd-sysv-install enable wazuh-manager
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-manager.service → /lib/systemd/sys
tem/wazuh-manager.service.
Installation Elasticsearch (Entrée) :
########################################

Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  opendistro-alerting opendistro-anomaly-detection opendistro-asynchronous-search
  opendistro-index-management opendistro-job-scheduler opendistro-knn opendistro-knnlib
  opendistro-performance-analyzer opendistro-reports-scheduler opendistro-security opendistro
Les NOUVEAUX paquets suivants seront installés :
  elasticsearch-oss opendistro-alerting opendistro-anomaly-detection
  opendistro-asynchronous-search opendistro-index-management opendistro-job-scheduler
  opendistro-knn opendistro-knnlib opendistro-performance-analyzer opendistro-reports-schedu
  opendistro-security opendistro-sql opendistroforelasticsearch
0 mis à jour, 13 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 392 Mo dans les archives.
Après cette opération, 599 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

```
ice → /lib/systemd/system/opendistro-performance-analyzer.service.
Paramétrage de opendistroforelasticsearch (1.13.2-1) ...
################################################################################
Téléchargement du fichier de configuration d'elasticsearch (Entrée) :
################################################################################

##########################################################
Ajout des utilisateurs et rôles elasticsearch (Entrée) :
##########################################################

##########################################################
Suppression des certificats de démonstration (Entrée) :
##########################################################

################################################
Téléchargement des certificats wazuh (Entrée) :
################################################

##########################################################
Exécution de wazuh pour créer les certificats (Entrée) :
##########################################################

02/05/2022 10:25:54 INFO: Configuration file found. Creating certificates...
02/05/2022 10:25:55 INFO: Creating the Elasticsearch certificates...
02/05/2022 10:25:55 INFO: Creating Wazuh server certificates...
02/05/2022 10:25:55 INFO: Creating Kibana certificate...
02/05/2022 10:25:55 INFO: Certificates creation finished. They can be found in ~/certs.
#############################################################################################
Déplacement les certificats d'Elasticsearh vers leur emplacement correspondant (Entrée) :
#############################################################################################
```

```
##########################################################
Activation et démarrage du service Elasticsearch (Entrée) :
##########################################################

Synchronizing state of elasticsearch.service with SysV service script with /lib/systemd/systemd-sysv
-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /lib/systemd/sys
tem/elasticsearch.service.
```

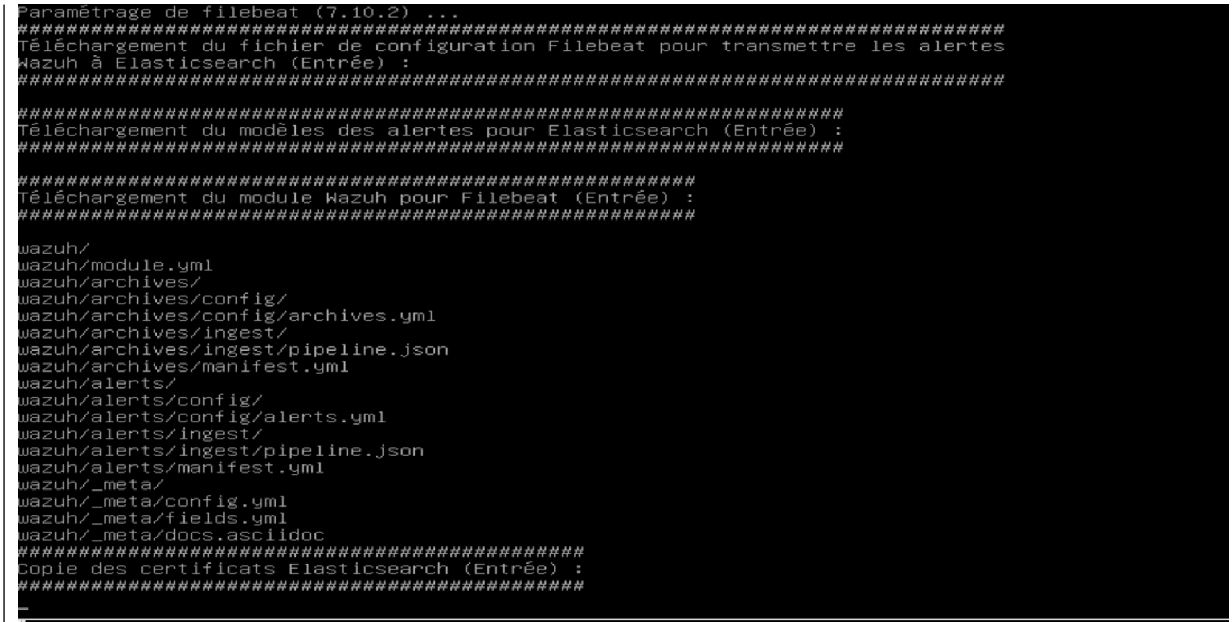
(L'activation et le démarrage d'elasticsearch prend un certain temps)

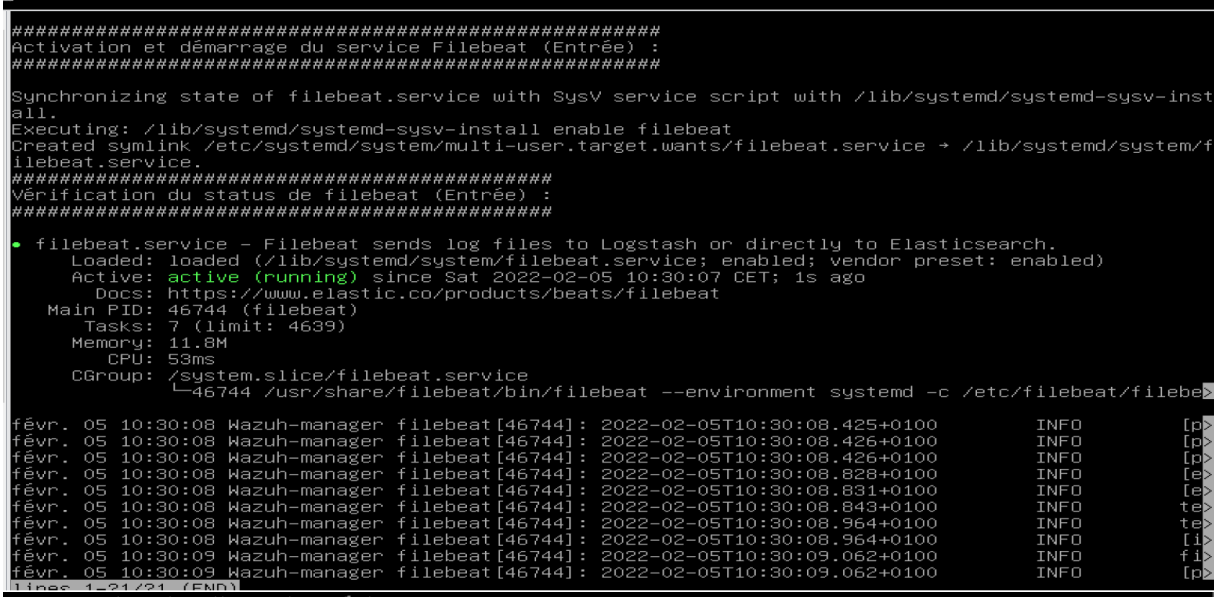
```
####################################################
Vérification du statut de Elasticsearch (Entrée) :
####################################################
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2022-02-05 10:27:26 CET; 6ms ago
       Docs: https://www.elastic.co
   Main PID: 41856 (java)
      Tasks: 51 (limit: 4639)
     Memory: 1.2G
        CPU: 22.152s
     CGroup: /system.slice/elasticsearch.service
             └─41856 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.t>

févr. 05 10:26:21 Wazuh-manager systemd[1]: Starting Elasticsearch...
févr. 05 10:27:26 Wazuh-manager systemd[1]: Started Elasticsearch.
lines 1-13/13 (END)
```

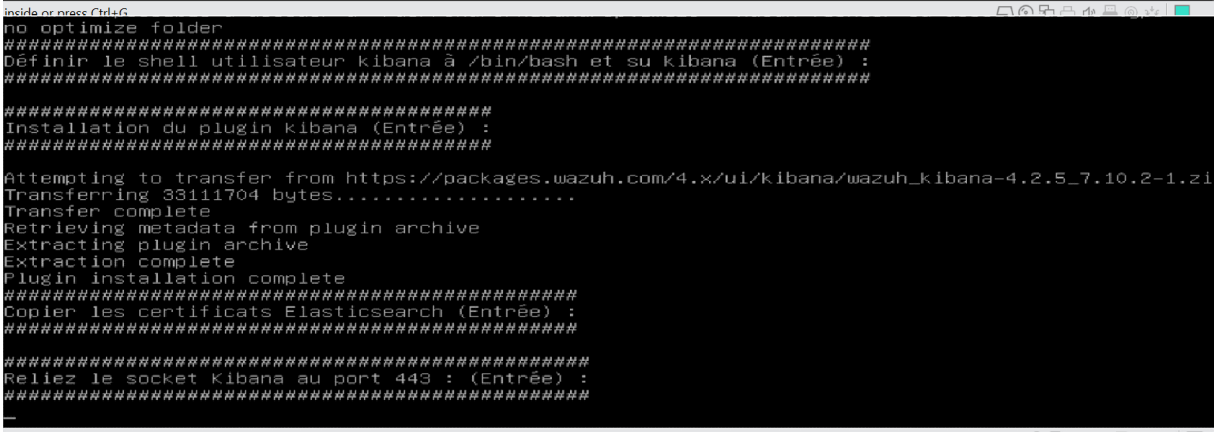
```
Done with success
###################################
Installation Filebeat (Entrée) :
###################################

Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  filebeat
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 22,1 Mo dans les archives.
Après cette opération, 73,6 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 https://packages.wazuh.com/4.x/apt stable/main amd64 filebeat amd64 7.10.2 [22,1 MB]
22,1 Mo réceptionnés en 4s (5 812 ko/s)
Sélection du paquet filebeat précédemment désélectionné.
(Lecture de la base de données... 54177 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../filebeat_7.10.2_amd64.deb ...
Dépaquetage de filebeat (7.10.2) ...
Paramétrage de filebeat (7.10.2) ...
#############################################################################################
Téléchargement du fichier de configuration Filebeat pour transmettre les alertes
Wazuh à Elasticsearch (Entrée) :
#############################################################################################
```


Paramétrage de filebeat (7.10.2) ...
Téléchargement du fichier de configuration Filebeat pour transmettre les alertes
Wazuh à Elasticsearch (Entrée) :
Téléchargement du modèles des alertes pour Elasticsearch (Entrée) :
Téléchargement du module Wazuh pour Filebeat (Entrée) :
wazuh/
wazuh/module.yml
wazuh/archives/
wazuh/archives/config/
wazuh/archives/config/archives.yml
wazuh/archives/ingest/
wazuh/archives/ingest/pipeline.json
wazuh/archives/manifest.yml
wazuh/alerts/
wazuh/alerts/config/
wazuh/alerts/config/alerts.yml
wazuh/alerts/ingest/
wazuh/alerts/ingest/pipeline.json
wazuh/alerts/manifest.yml
wazuh/_meta/
wazuh/_meta/config.yml
wazuh/_meta/fields.yml
wazuh/_meta/docs.asciidoc
Copie des certificats Elasticsearch (Entrée) :


Activation et démarrage du service Filebeat (Entrée) :
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-inst
all.
Executing: /lib/systemd/systemd-sysv-install enable filebeat
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/f
ilebeat.service.
Vérification du status de filebeat (Entrée) :
• filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.
Loaded: loaded (/lib/systemd/system/filebeat.service; enabled; vendor preset: enabled)
Active: active (running) since Sat 2022-02-05 10:30:07 CET; 1s ago
Docs: https://www.elastic.co/products/beats/filebeat
Main PID: 46744 (filebeat)
Tasks: 7 (limit: 4639)
Memory: 11.8M
CPU: 53ms
CGroup: /system.slice/filebeat.service
└─46744 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebe
févr. 05 10:30:08 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:08.425+0100 INFO [p
févr. 05 10:30:08 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:08.426+0100 INFO [p
févr. 05 10:30:08 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:08.426+0100 INFO [p
févr. 05 10:30:08 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:08.828+0100 INFO [e
févr. 05 10:30:08 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:08.831+0100 INFO [e
févr. 05 10:30:08 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:08.843+0100 INFO te
févr. 05 10:30:08 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:08.964+0100 INFO te
févr. 05 10:30:08 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:08.964+0100 INFO [i
févr. 05 10:30:09 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:09.062+0100 INFO fi
févr. 05 10:30:09 Wazuh-manager filebeat[46744]: 2022-02-05T10:30:09.062+0100 INFO [p
lines 1-21/21 (END)


Installation de kibana (Entrée) :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
opendistroforelasticsearch-kibana
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 234 Mo dans les archives.
Après cette opération, 692 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 https://packages.wazuh.com/4.x/apt stable/main amd64 opendistroforelasticsearch-kiba
na amd64 1.13.2 [234 MB]
19% [1 opendistroforelasticsearch-kibana 56,3 MB/234 MB 24%] 5 001 kB/s 35s


no optimize folder
Définir le shell utilisateur kibana à /bin/bash et su kibana (Entrée) :
Installation du plugin kibana (Entrée) :
Attempting to transfer from https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.2.5_7.10.2-1.zi
Transferring 33111704 bytes.....................
Transfer complete
Retrieving metadata from plugin archive
Extracting plugin archive
Extraction complete
Plugin installation complete
Copier les certificats Elasticsearch (Entrée) :
Reliez le socket Kibana au port 443 : (Entrée) :

```
##########################################
Installation du plugin kibana (Entrée) :
##########################################

Attempting to transfer from https://packages.wazuh.com/4.x/ui/kibana/wazuh_kibana-4.2.5_7.10.2-1.zip
Transferring 33111704 bytes....................
Transfer complete
Retrieving metadata from plugin archive
Extracting plugin archive
Extraction complete
Plugin installation complete
################################################
Copier les certificats Elasticsearch (Entrée) :
################################################

#################################################
Reliez le socket Kibana au port 443 : (Entrée) :
#################################################

#####################################################
Activation et démarrage du service kibana (Entrée) :
#####################################################

Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-instal
l.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kib
ana.service.
############################################
Vérification du status de kibana (Entrée) :
############################################
_
```

```
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-instal
l.
Executing: /lib/systemd/systemd-sysv-install enable kibana
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kib
ana.service.
############################################
Vérification du status de kibana (Entrée) :
############################################

● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2022-02-05 10:32:16 CET; 22s ago
   Main PID: 53219 (node)
      Tasks: 11 (limit: 4639)
     Memory: 169.9M
        CPU: 5.311s
     CGroup: /system.slice/kibana.service
             └─53219 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist ->

févr. 05 10:32:20 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:20Z","t>
févr. 05 10:32:20 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:20Z","t>
févr. 05 10:32:20 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:20Z","t>
févr. 05 10:32:21 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:21Z","t>
févr. 05 10:32:21 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:21Z","t>
févr. 05 10:32:21 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:21Z","t>
févr. 05 10:32:21 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:21Z","t>
févr. 05 10:32:21 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:21Z","t>
févr. 05 10:32:21 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:21Z","t>
févr. 05 10:32:21 Wazuh-manager kibana[53219]: {"type":"log","@timestamp":"2022-02-05T09:32:21Z","t>
lines 1-20/20 (END)
##############################
Accédez à l'interface Web :
##############################
URL: https://<wazuh_server_ip> user: admin password: admin
Bye !
root@Wazuh-manager:/etc# _
```

On fois qu'on a terminé l'installation on va vérifier l'état du service élasticsearch et kibana ainsi que wazuh-manager :

```
root@Wazuh-manager:~# service elasticsearch status
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2022-02-05 10:48:22 CET; 3min 19s ago
       Docs: https://www.elastic.co
   Main PID: 630 (java)
      Tasks: 62 (limit: 4639)
     Memory: 1.3G
        CPU: 38.264s
     CGroup: /system.slice/elasticsearch.service
             └─630 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl>

févr. 05 10:47:16 Wazuh-manager systemd[1]: Starting Elasticsearch...
févr. 05 10:48:22 Wazuh-manager systemd[1]: Started Elasticsearch.
févr. 05 10:48:22 Wazuh-manager systemd-entrypoint[630]: WARNING: An illegal reflective access oper>
févr. 05 10:48:22 Wazuh-manager systemd-entrypoint[630]: WARNING: Illegal reflective access by com.>
févr. 05 10:48:22 Wazuh-manager systemd-entrypoint[630]: WARNING: Please consider reporting this to>
févr. 05 10:48:22 Wazuh-manager systemd-entrypoint[630]: WARNING: Use --illegal-access=warn to enab>
févr. 05 10:48:22 Wazuh-manager systemd-entrypoint[630]: WARNING: All illegal access operations wil>
lines 1-18/18 (END)
```

```
root@Wazuh-manager:~# service kibana status
● kibana.service - Kibana
     Loaded: loaded (/etc/systemd/system/kibana.service; enabled; vendor preset: enabled)
     Active: active (running) since Sat 2022-02-05 10:47:16 CET; 7min ago
   Main PID: 595 (node)
      Tasks: 11 (limit: 4639)
     Memory: 238.8M
        CPU: 7.946s
     CGroup: /system.slice/kibana.service
             └─595 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist

févr. 05 10:48:25 Wazuh-manager kibana[595]: {"type":"log","@timestamp":"2022-02-05T09:48:252","
févr. 05 10:48:25 Wazuh-manager kibana[595]: {"type":"log","@timestamp":"2022-02-05T09:48:252","
févr. 05 10:48:26 Wazuh-manager kibana[595]: {"type":"log","@timestamp":"2022-02-05T09:48:262","
févr. 05 10:48:26 Wazuh-manager kibana[595]: {"type":"log","@timestamp":"2022-02-05T09:48:262","
févr. 05 10:48:26 Wazuh-manager kibana[595]: {"type":"log","@timestamp":"2022-02-05T09:48:262","
févr. 05 10:48:26 Wazuh-manager kibana[595]: {"type":"log","@timestamp":"2022-02-05T09:48:262","
root@Wazuh-manager:~# service wazuh-manager status
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2022-02-11 09:46:23 CET; 8min ago
    Process: 616 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/S
      Tasks: 130 (limit: 4639)
     Memory: 488.1M
        CPU: 35.931s
     CGroup: /system.slice/wazuh-manager.service
             ├─1015 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─1054 /var/ossec/bin/wazuh-authd
             ├─1070 /var/ossec/bin/wazuh-db
             ├─1094 /var/ossec/bin/wazuh-execd
             ├─1107 /var/ossec/bin/wazuh-analysisd
             ├─1169 /var/ossec/bin/wazuh-syscheckd
             ├─1184 /var/ossec/bin/wazuh-remoted
             ├─1222 /var/ossec/bin/wazuh-logcollector
             ├─1259 /var/ossec/bin/wazuh-monitord
             └─1305 /var/ossec/bin/wazuh-modulesd

févr. 11 09:46:14 Wazuh-manager env[616]: Started wazuh-db...
févr. 11 09:46:15 Wazuh-manager env[616]: Started wazuh-execd...
févr. 11 09:46:16 Wazuh-manager env[616]: Started wazuh-analysisd...
févr. 11 09:46:17 Wazuh-manager env[616]: Started wazuh-syscheckd...
févr. 11 09:46:18 Wazuh-manager env[616]: Started wazuh-remoted...
févr. 11 09:46:19 Wazuh-manager env[616]: Started wazuh-logcollector...
févr. 11 09:46:20 Wazuh-manager env[616]: Started wazuh-monitord...
févr. 11 09:46:21 Wazuh-manager env[616]: Started wazuh-modulesd...
févr. 11 09:46:23 Wazuh-manager env[616]: Completed.
févr. 11 09:46:23 Wazuh-manager systemd[1]: Started Wazuh manager.
```

Nous pouvons vérifier les fichiers de kibana et de Elasticsearch :

```
root@Wazuh-manager:~# nano /etc/kibana/kibana.yml _
```

Activité 7 | Wazuh-manager

```
  GNU nano 5.4                                /etc/kibana/kibana.yml
server.host: 0.0.0.0
server.port: 443
elasticsearch.hosts: https://localhost:9200
elasticsearch.ssl.verificationMode: certificate
elasticsearch.username: kibanaserver
elasticsearch.password: kibanaserver
elasticsearch.requestHeadersWhitelist: ["securitytenant","Authorization"]
opendistro_security.multitenancy.enabled: true
opendistro_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/kibana/certs/kibana-key.pem"
server.ssl.certificate: "/etc/kibana/certs/kibana.pem"
elasticsearch.ssl.certificateAuthorities: ["/etc/kibana/certs/root-ca.pem"]
server.defaultRoute: /app/wazuh?security_tenant=global
telemetry.banner: false
```

(Port d'écoute, interfaces d'écoute, le certificat utilisé etc…)

```
root@Wazuh-manager:~# nano /etc/elasticsearch/elasticsearch.yml
  GNU nano 5.4                          /etc/elasticsearch/elasticsearch.yml
network.host: 127.0.0.1
node.name: node-1
cluster.initial_master_nodes: node-1

opendistro_security.ssl.transport.pemcert_filepath: /etc/elasticsearch/certs/elasticsearch.pem
opendistro_security.ssl.transport.pemkey_filepath: /etc/elasticsearch/certs/elasticsearch-key.pem
opendistro_security.ssl.transport.pemtrustedcas_filepath: /etc/elasticsearch/certs/root-ca.pem
opendistro_security.ssl.transport.enforce_hostname_verification: false
opendistro_security.ssl.transport.resolve_hostname: false
opendistro_security.ssl.http.enabled: true
opendistro_security.ssl.http.pemcert_filepath: /etc/elasticsearch/certs/elasticsearch.pem
opendistro_security.ssl.http.pemkey_filepath: /etc/elasticsearch/certs/elasticsearch-key.pem
opendistro_security.ssl.http.pemtrustedcas_filepath: /etc/elasticsearch/certs/root-ca.pem
opendistro_security.nodes_dn:
- CN=node-1,OU=Docu,O=Wazuh,L=California,C=US
opendistro_security.authcz.admin_dn:
- CN=admin,OU=Docu,O=Wazuh,L=California,C=US

opendistro_security.audit.type: internal_elasticsearch
opendistro_security.enable_snapshot_restore_privilege: true
opendistro_security.check_snapshot_restore_write_privileges: true
opendistro_security.restapi.roles_enabled: ["all_access", "security_rest_api_access"]
node.max_local_storage_nodes: 3

path.data: /var/lib/elasticsearch
path.logs: /var/log/elasticsearch
```

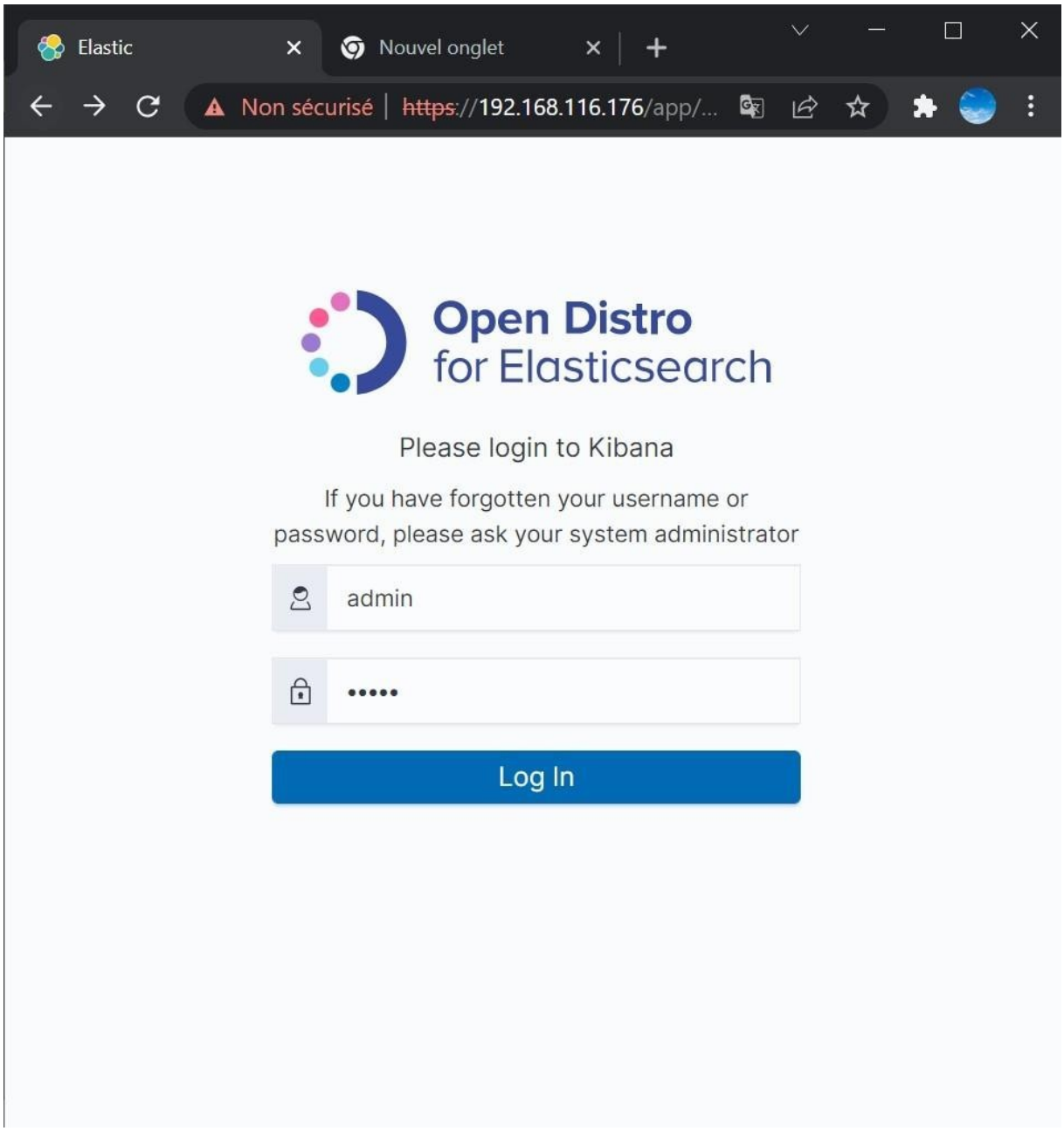
(Remarque : en cas de souci avec le démarrage de elasticsearch on consulte les log en écrasant le fichier des logs existant, :

```
# echo > /var/log/elasticsearch/elasticsearch.log
```

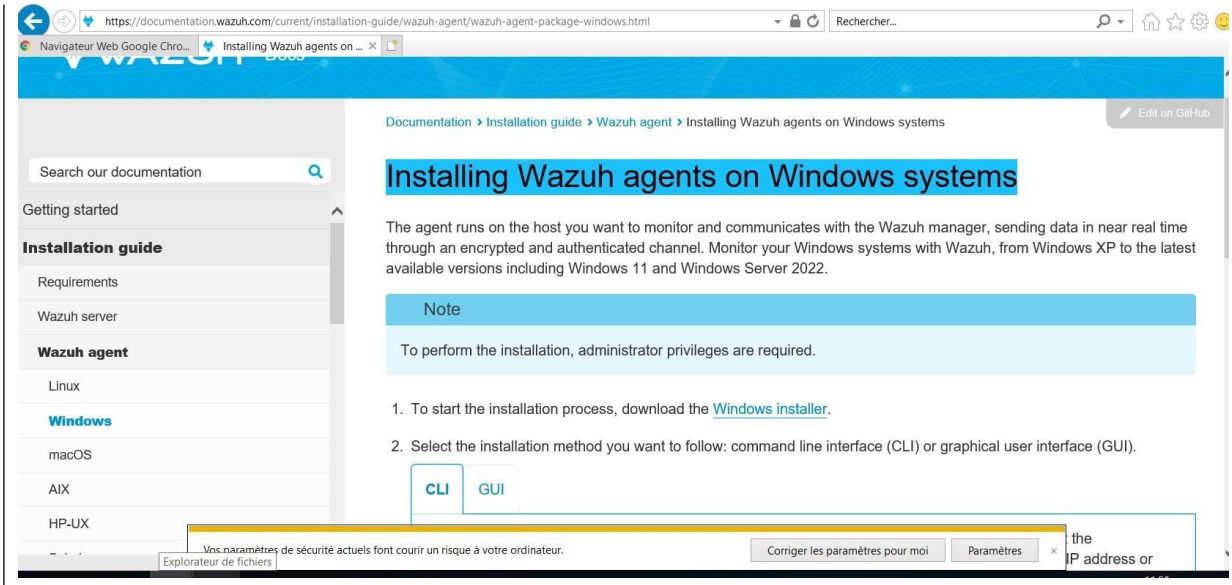
Puis en redémarrant le service elasticsearch et en éditant le fichier des logs pour voir ou se trouve le problème :

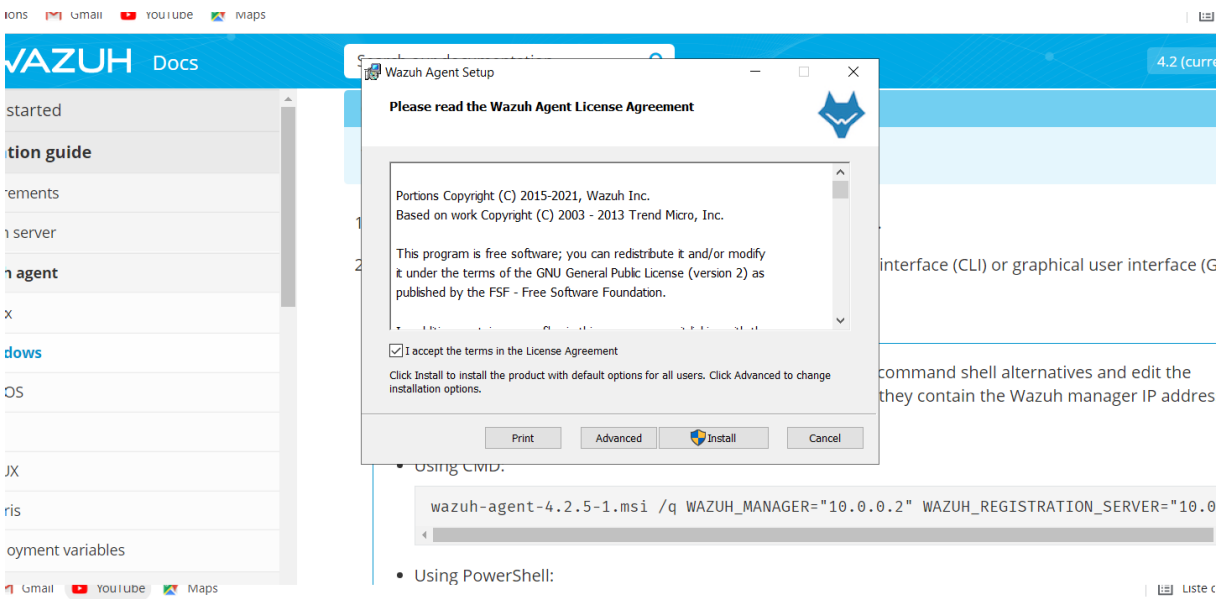
```
# service elasticsearch start
# nano_/var/log/elasticsearch/elasticsearch.log
```

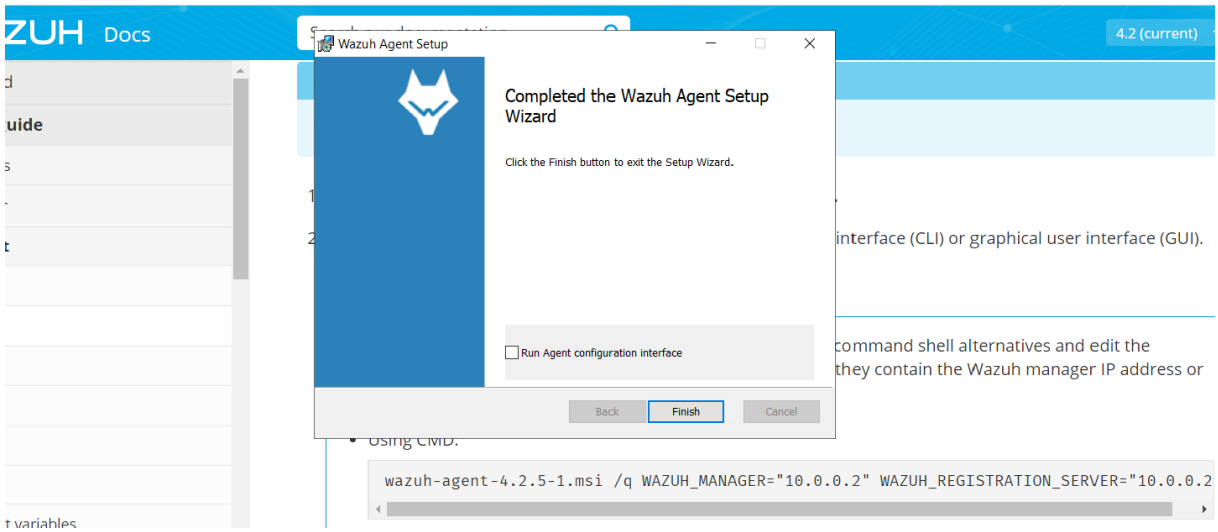
Une fois qu'on a terminer tout cela, nous allons nous connecter à Kibana en tappant l'adresse <https://(ip du serveur)> :
(Remarque : kibana, elasticsearch et wazuh-manager fonctionnent ensemble)
(Pour un certain confort nous allons augmenter le nombre de processeur pour que les services fonctionnent correctement).



Maintenant on va installer les agents sur une machine virtuel windows 2019 du même lan stadiumcompany:





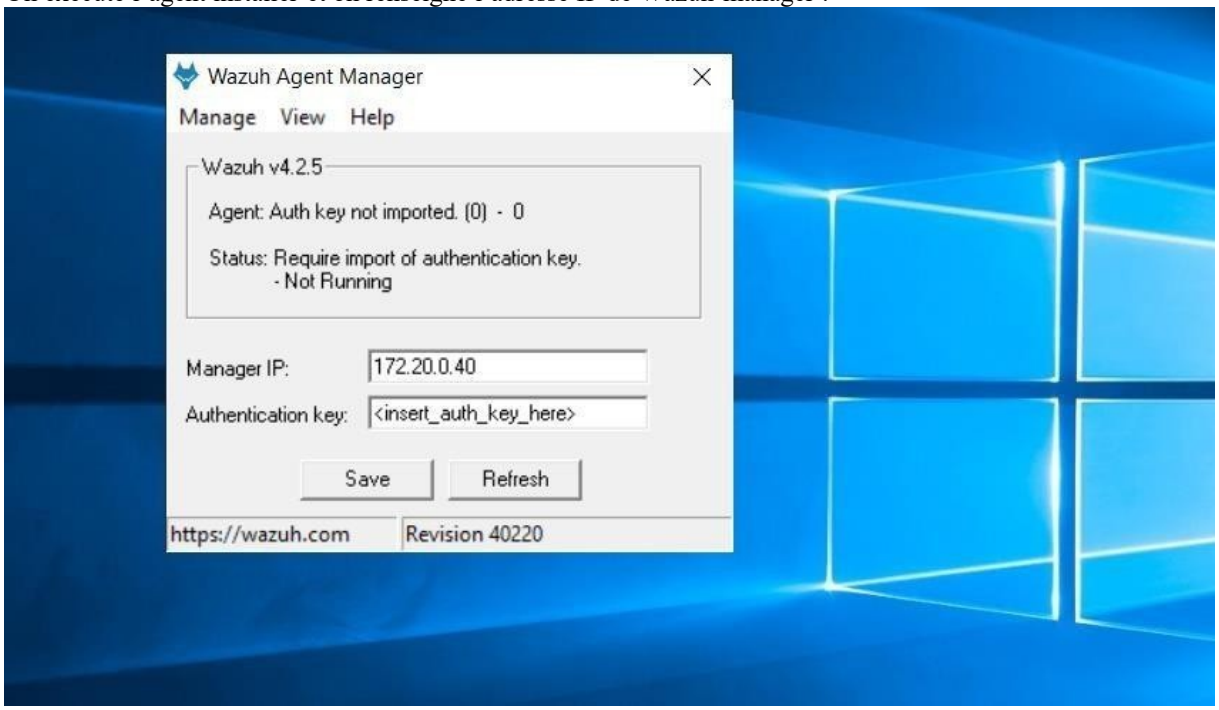


On va tester la communication avec la machine Wazuh-manager (en ouvrant un terminal cmd) :

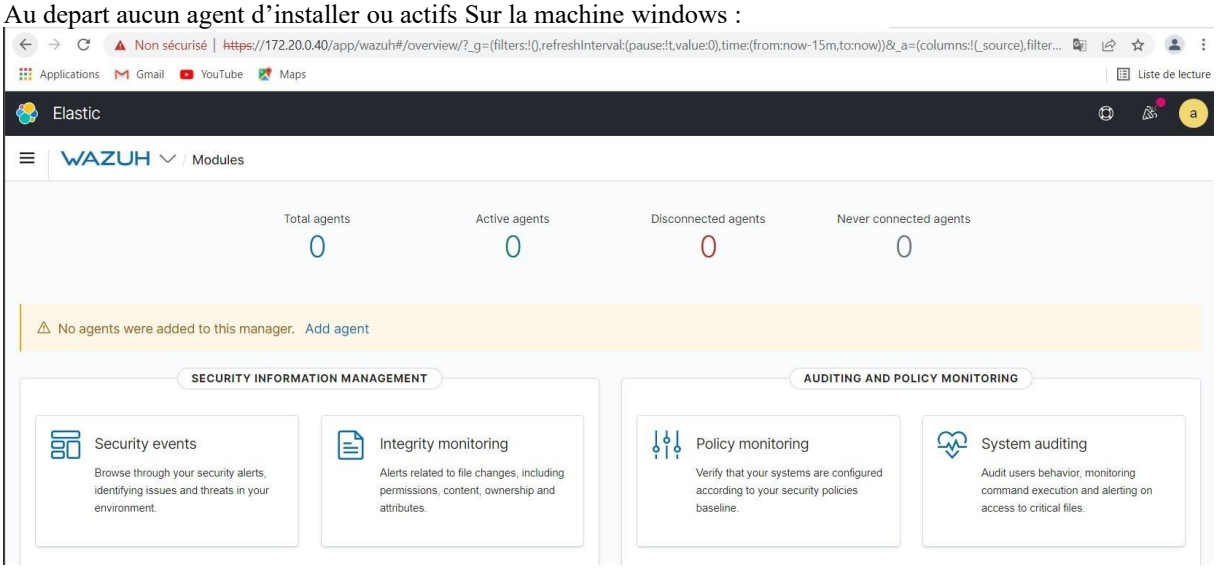
```
C:\Users\adelk>ping 172.20.0.40

Envoi d'une requête 'Ping'  172.20.0.40 avec 32 octets de données :
Réponse de 172.20.0.40 : octets=32 temps<1ms TTL=64
Réponse de 172.20.0.40 : octets=32 temps=1 ms TTL=64
Réponse de 172.20.0.40 : octets=32 temps<1ms TTL=64
Réponse de 172.20.0.40 : octets=32 temps<1ms TTL=64
```

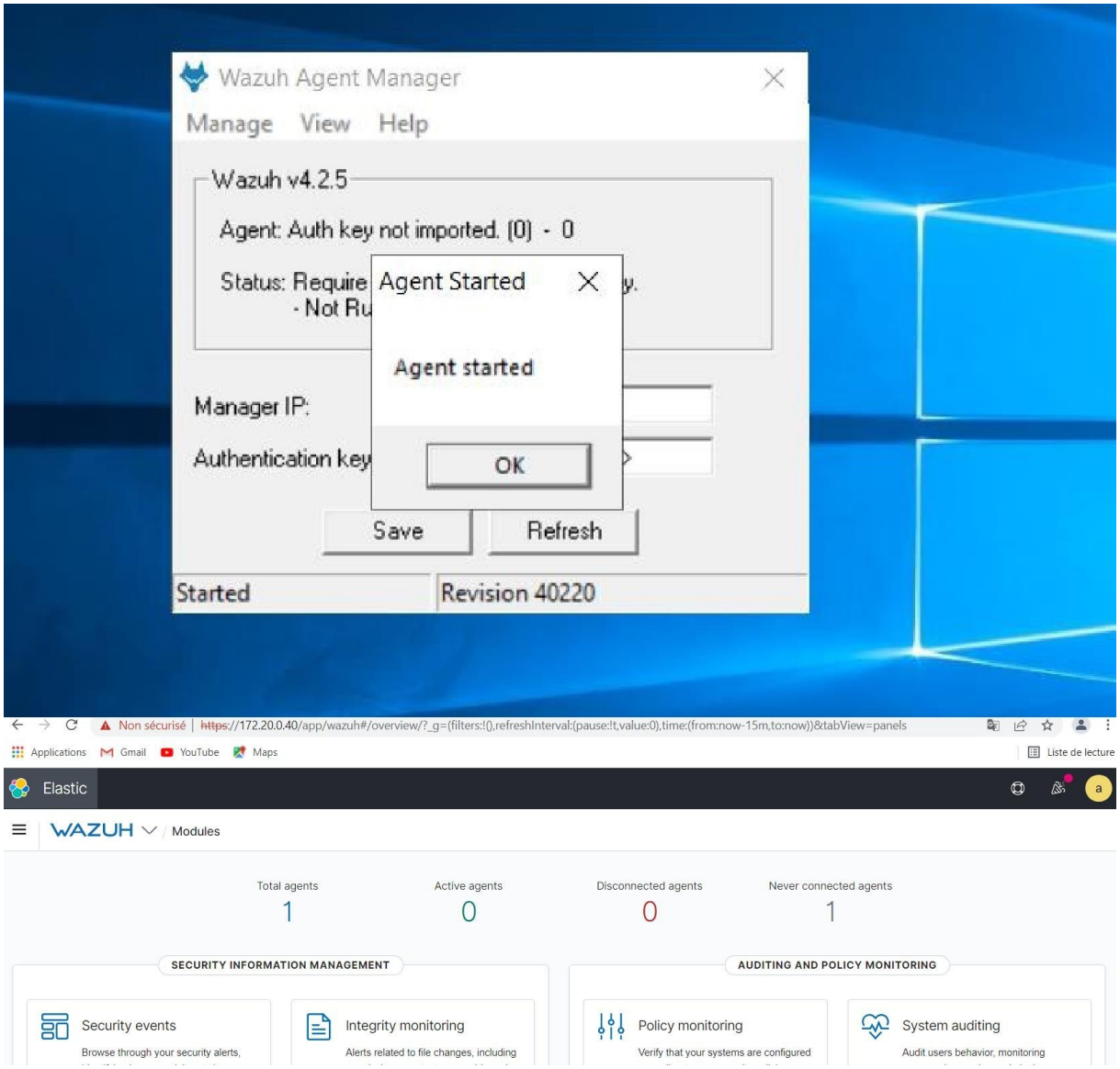
On execute l'agent installer et on renseigne l'adresse IP de Wazuh-manager :



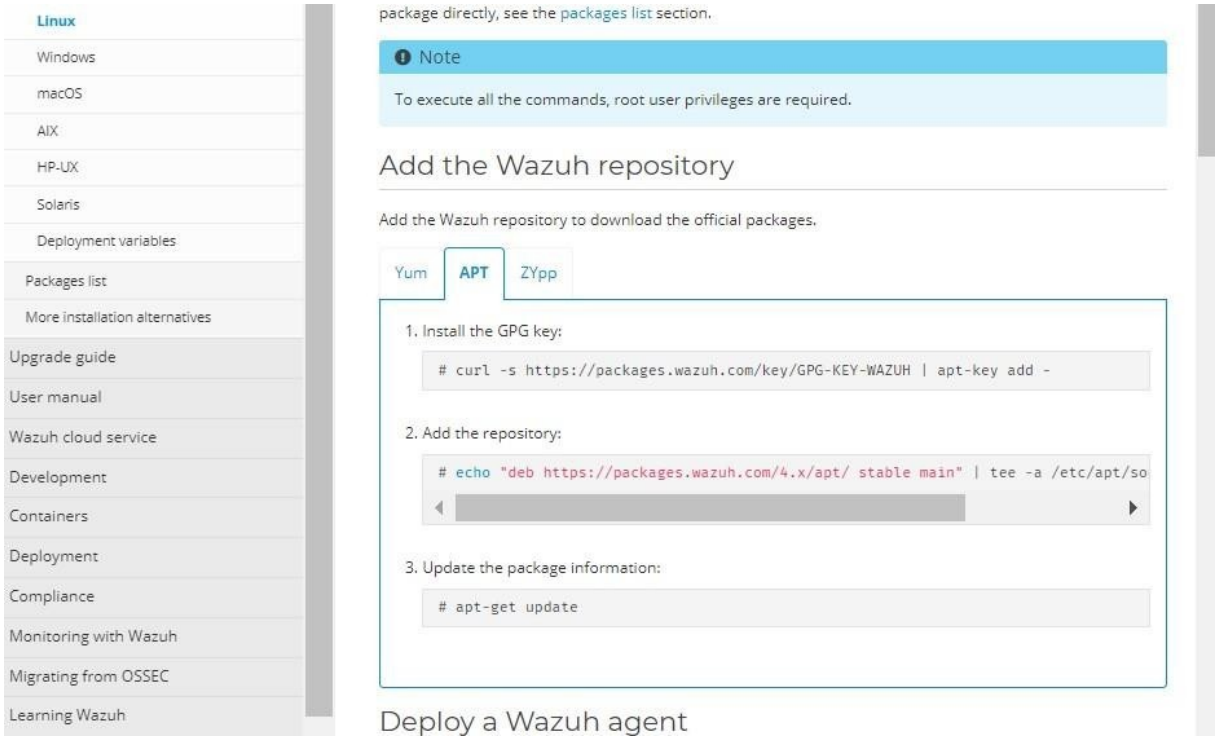
Au depart aucun agent d'installer ou actifs Sur la machine windows :



Mais lorsqu'on va faire un start sur le Wazuh agent manager (récemment installer sur la machine windows) , un agent sera constater :



Nous allons également installer un agent sur une machine Lixux :



Comme indiqué dans la procedure d'installation :

```
root@mail:~#  curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key
add -

root@mail:~# echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a
 /etc/apt/sources.list.d/wazuh.list
```

```
root@mail:~# apt update
```

On installe l'agent en renseignant l'adresse : 172.20.0.40 :

```
root@mail:~# WAZUH_MANAGER="172.20.0.40" apt-get install wazuh-agent
```

On demarre maintenant l'agent :

```
root@mail:~# service wazuh-agent start

root@mail:~# service wazuh-agent status
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; disabled; vendor >
     Active: active (running) since Sun 2022-02-13 17:32:45 CET; 51s ago
    Process: 3934 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (co>
      Tasks: 26 (limit: 2301)
     Memory: 21.5M
        CPU: 930ms
     CGroup: /system.slice/wazuh-agent.service
             ├─3957 /var/ossec/bin/wazuh-execd
```