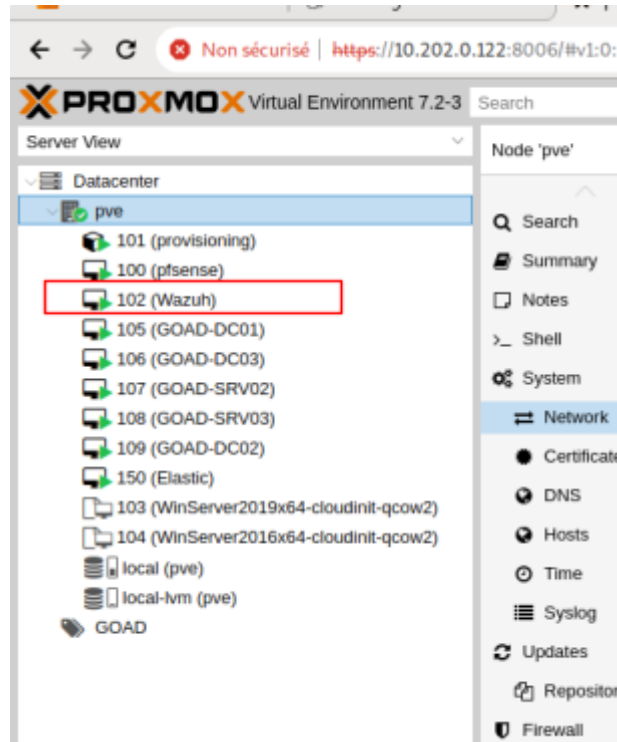


Installation de Wazuh (Proxmox)

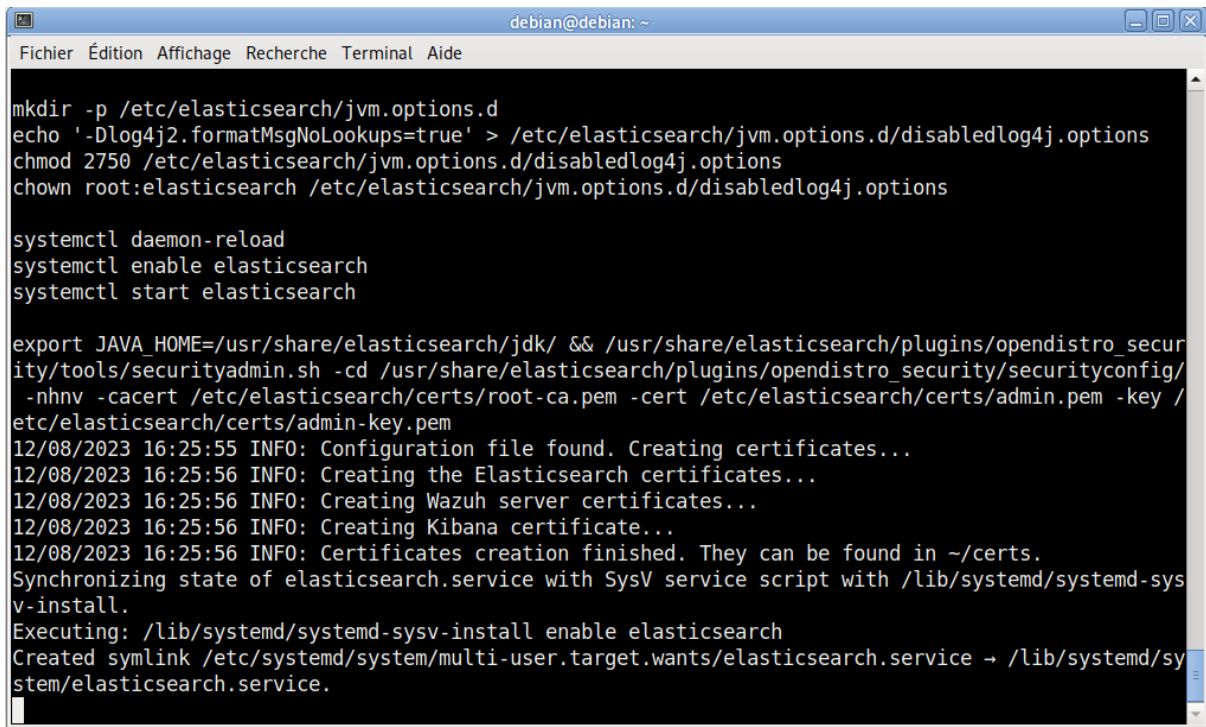
- On crée un VM sur Proxmox (debian11) :



- On install Wazuh Manager :
`apt install -y wazuh-manager`

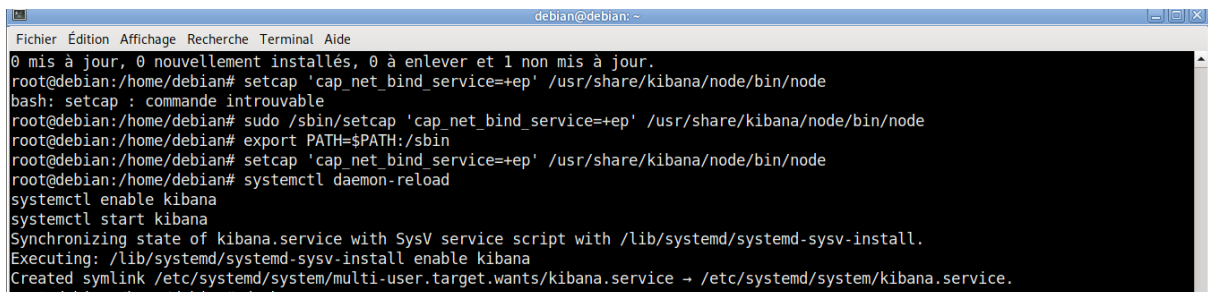
```
debian@debian: ~  
Fichier Édition Affichage Recherche Terminal Aide  
● wazuh-manager.service - Wazuh manager  
   Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)  
   Active: active (running) since Fri 2023-12-08 16:24:28 CET; 4ms ago  
 Process: 45212 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0)  
    Tasks: 158 (limit: 6618)  
   Memory: 439.4M  
      CPU: 17.775s  
   CGroup: /system.slice/wazuh-manager.service  
           └─45268 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py  
             └─45307 /var/ossec/bin/wazuh-authd  
               └─45323 /var/ossec/bin/wazuh-db  
                 └─45338 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py  
                   └─45341 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py  
                     └─45344 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py  
                       └─45356 /var/ossec/bin/wazuh-execd  
                         └─45370 /var/ossec/bin/wazuh-analysisd  
                           └─45449 /var/ossec/bin/wazuh-syscheckd  
                             └─45463 /var/ossec/bin/wazuh-remoted  
                               └─45495 /var/ossec/bin/wazuh-logcollector  
                                 └─45511 /var/ossec/bin/wazuh-monitord  
                                   └─45554 /var/ossec/bin/wazuh-modulesd  
  
déc. 08 16:24:21 debian env[45212]: Started wazuh-db...  
déc. 08 16:24:22 debian env[45212]: Started wazuh-execd...  
lines 1-24
```

- On install Elastic et on crée les certificats :

A terminal window titled 'debian@debian: ~' showing the installation of Elasticsearch. The user runs several commands to create configuration files, set permissions, and enable the service. The output shows the creation of certificates for Elasticsearch, Wazuh, and Kibana, and the successful enabling of the service.

```
debian@debian: ~  
Fichier Édition Affichage Recherche Terminal Aide  
  
mkdir -p /etc/elasticsearch/jvm.options.d  
echo '-Dlog4j2.formatMsgNoLookups=true' > /etc/elasticsearch/jvm.options.d/disabledlog4j.options  
chmod 2750 /etc/elasticsearch/jvm.options.d/disabledlog4j.options  
chown root:elasticsearch /etc/elasticsearch/jvm.options.d/disabledlog4j.options  
  
systemctl daemon-reload  
systemctl enable elasticsearch  
systemctl start elasticsearch  
  
export JAVA_HOME=/usr/share/elasticsearch/jdk/ && /usr/share/elasticsearch/plugins/opendistro_security/tools/securityadmin.sh -cd /usr/share/elasticsearch/plugins/opendistro_security/securityconfig/-nhnv -cacert /etc/elasticsearch/certs/root-ca.pem -cert /etc/elasticsearch/certs/admin.pem -key /etc/elasticsearch/certs/admin-key.pem  
12/08/2023 16:25:55 INFO: Configuration file found. Creating certificates...  
12/08/2023 16:25:56 INFO: Creating the Elasticsearch certificates...  
12/08/2023 16:25:56 INFO: Creating Wazuh server certificates...  
12/08/2023 16:25:56 INFO: Creating Kibana certificate...  
12/08/2023 16:25:56 INFO: Certificates creation finished. They can be found in ~/certs.  
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/system/elasticsearch.service.
```

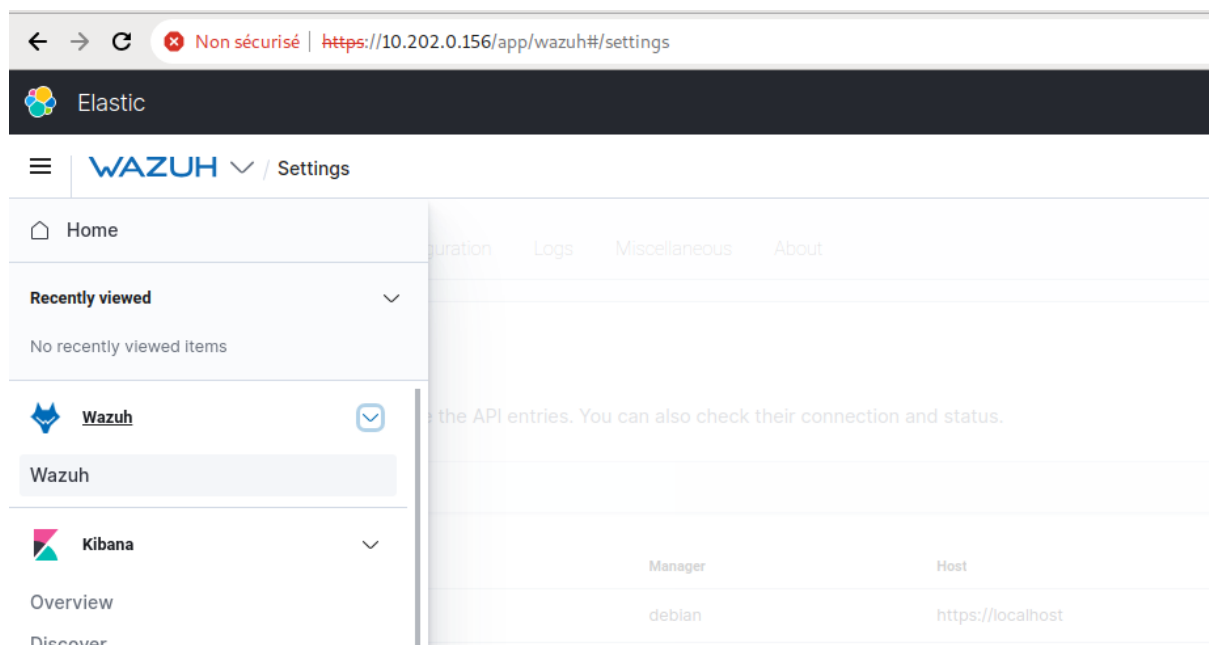
- On installe Kibana et Filebeat :

A terminal window titled 'debian@debian: ~' showing the installation of Kibana. The user sets permissions for the Kibana binary, reloads the daemon, enables the service, and starts it. The output shows the successful enabling of the service and the creation of a symlink.

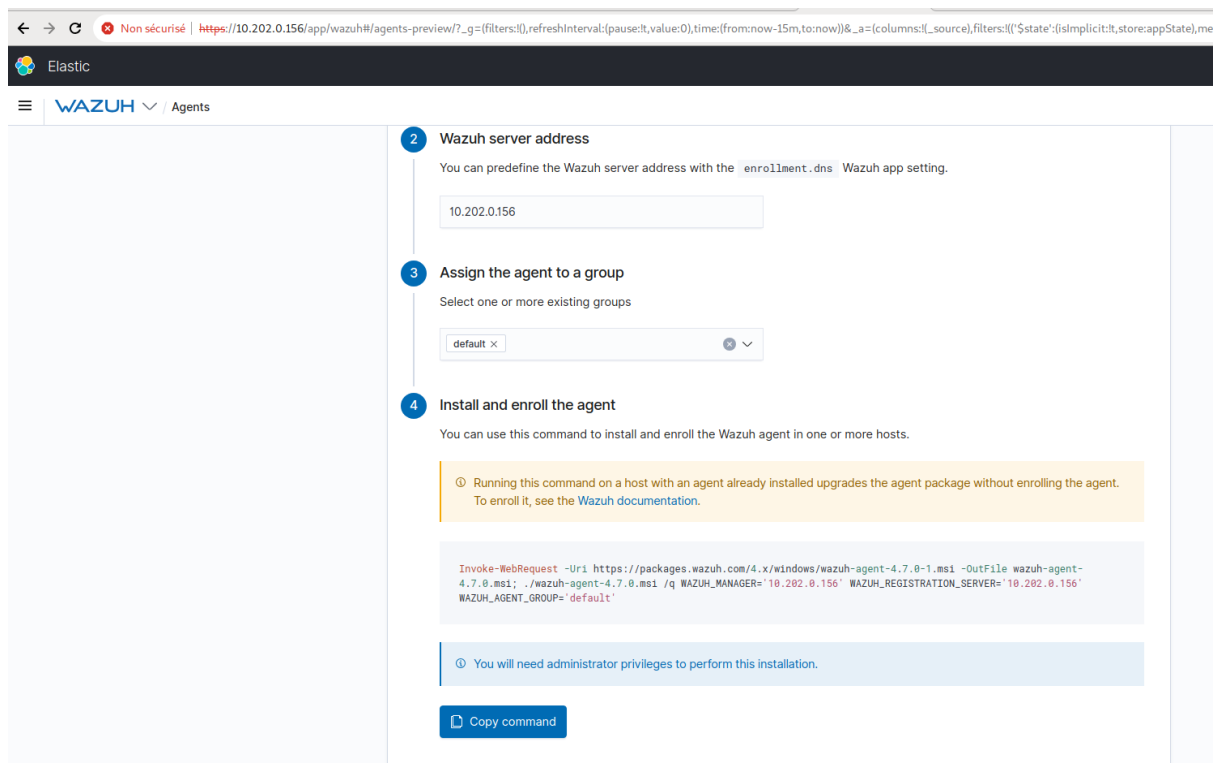
```
debian@debian: ~  
Fichier Édition Affichage Recherche Terminal Aide  
  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 1 non mis à jour.  
root@debian:/home/debian# setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node  
bash: setcap : commande introuvable  
root@debian:/home/debian# sudo /sbin/setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node  
root@debian:/home/debian# export PATH=$PATH:/sbin  
root@debian:/home/debian# setcap 'cap_net_bind_service=+ep' /usr/share/kibana/node/bin/node  
root@debian:/home/debian# systemctl daemon-reload  
systemctl enable kibana  
systemctl start kibana  
Synchronizing state of kibana.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/systemd-sysv-install enable kibana  
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /etc/systemd/system/kibana.service.
```

```
debian@debian: ~  
Fichier Édition Affichage Recherche Terminal Aide  
mv ~/certs/filebeat* /etc/filebeat/certs/  
root@debian:/home/debian# systemctl daemon-reload  
systemctl enable filebeat  
systemctl start filebeat  
Synchronizing state of filebeat.service with SysV service script with /lib/systemd/systemd-sysv-ins  
tall.  
Executing: /lib/systemd/systemd-sysv-install enable filebeat  
Created symlink /etc/systemd/system/multi-user.target.wants/filebeat.service → /lib/systemd/system/  
filebeat.service.  
root@debian:/home/debian# filebeat test output  
elasticsearch: https://127.0.0.1:9200...  
  parse url... OK  
  connection...  
    parse host... OK  
    dns lookup... OK  
    addresses: 127.0.0.1  
    dial up... OK  
  TLS...  
    security: server's certificate chain verification is enabled  
    handshake... OK  
    TLS version: TLSv1.3  
    dial up... OK  
  talk to server... OK  
  version: 7.10.2  
root@debian:/home/debian#
```

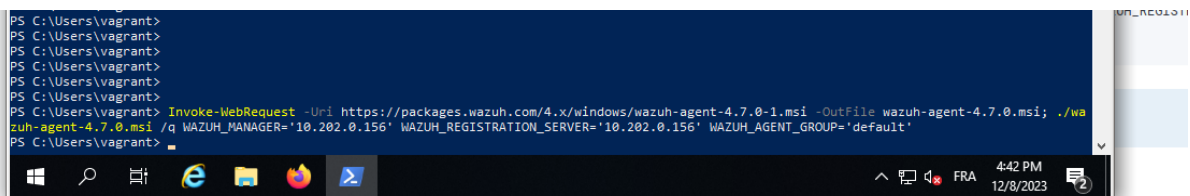
- On peut accéder à notre interface Wazuh sur l'IP : 10.202.0.156



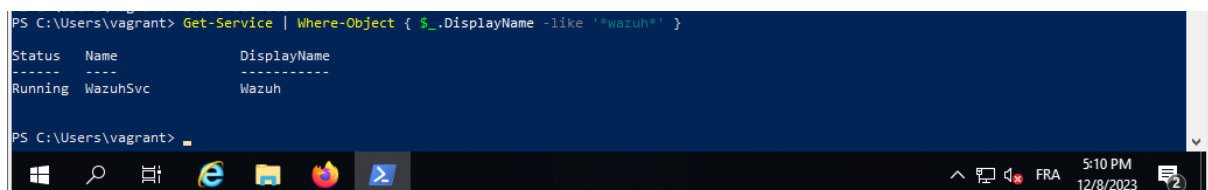
- On ajoute les agents GOAD avec les commandes de Wazuh :



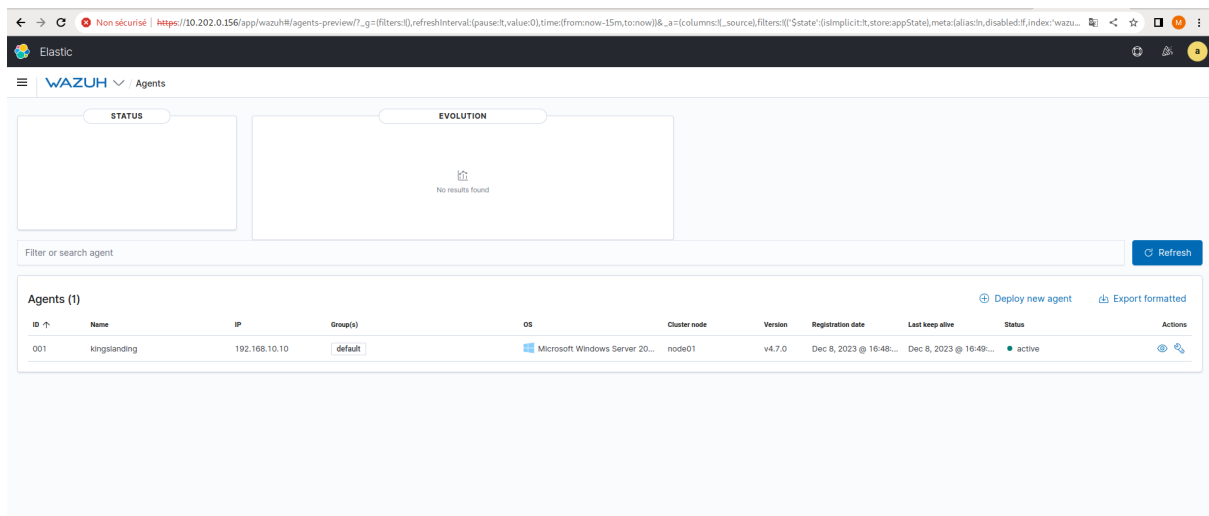
- On applique les commandes sur un agent GOAD :



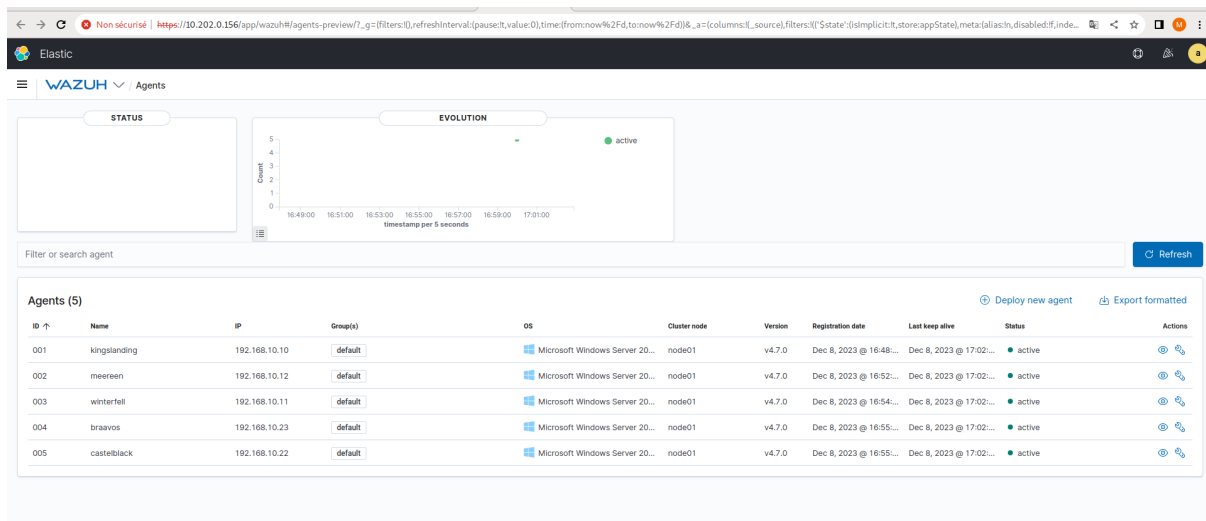
- On voit que le service est bien activé :



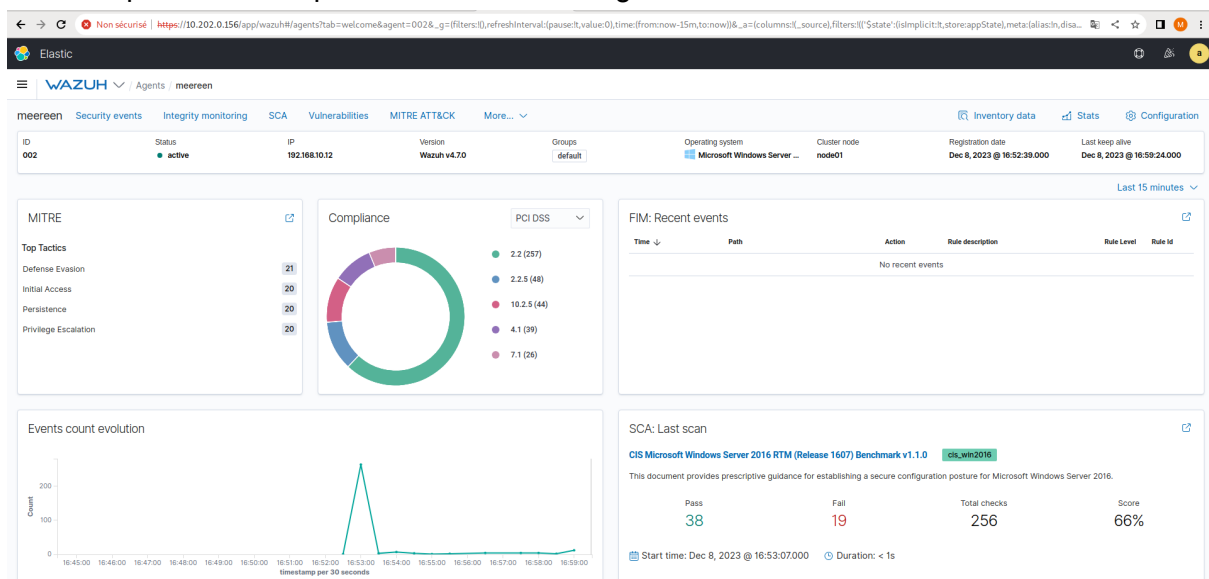
- Sur Wazuh on observe bien que l'agent a été ajouté :



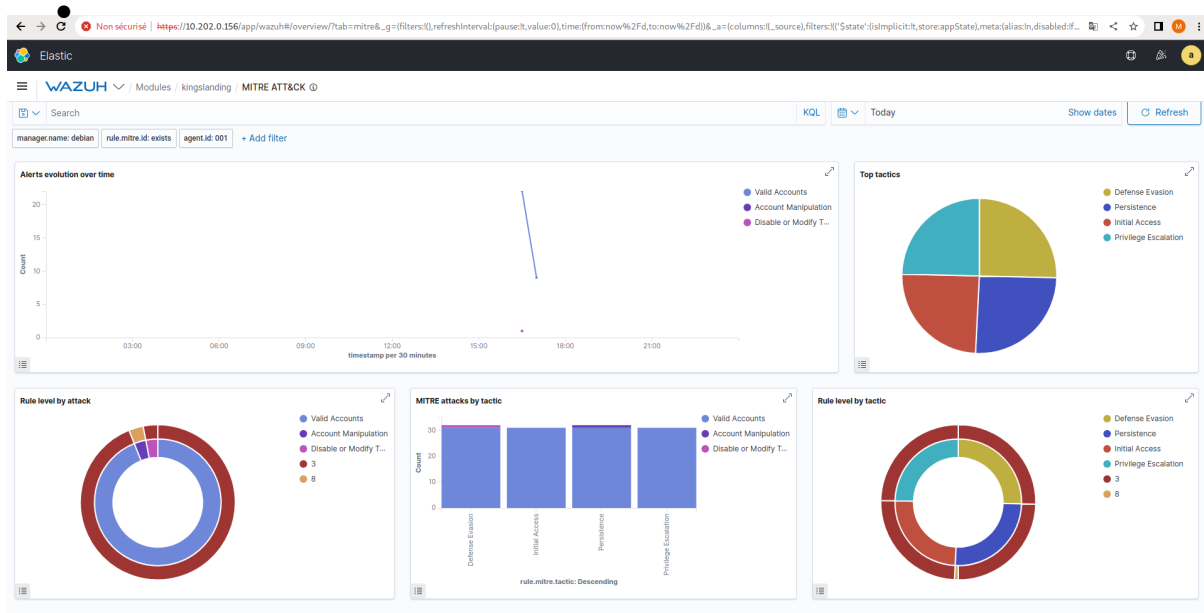
- On fait la même chose pour tout les GOAD :



- On peut observer plus en détails sur un agent les alertes :



- On peut avoir plus d'informations sur une alerte en particulier avec le top de "tactics" d'alertes (privilège, persistance) :



Réalisé par Mathéo Balazuc.