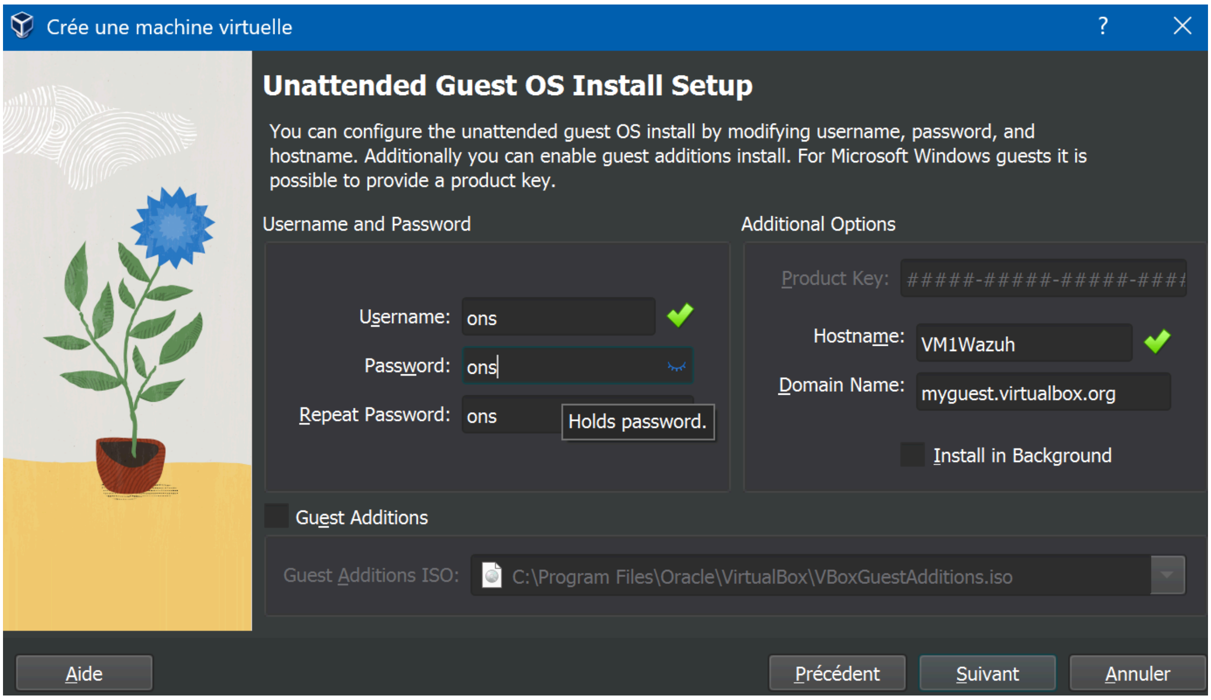


Crée une machine virtuelle

Unattended Guest OS Install Setup

You can configure the unattended guest OS install by modifying username, password, and hostname. Additionally you can enable guest additions install. For Microsoft Windows guests it is possible to provide a product key.

Username and Password

Username: ons ✓

Password: ons

Repeat Password: ons

Holds password.

Additional Options

Product Key: #####-#####-#####-####

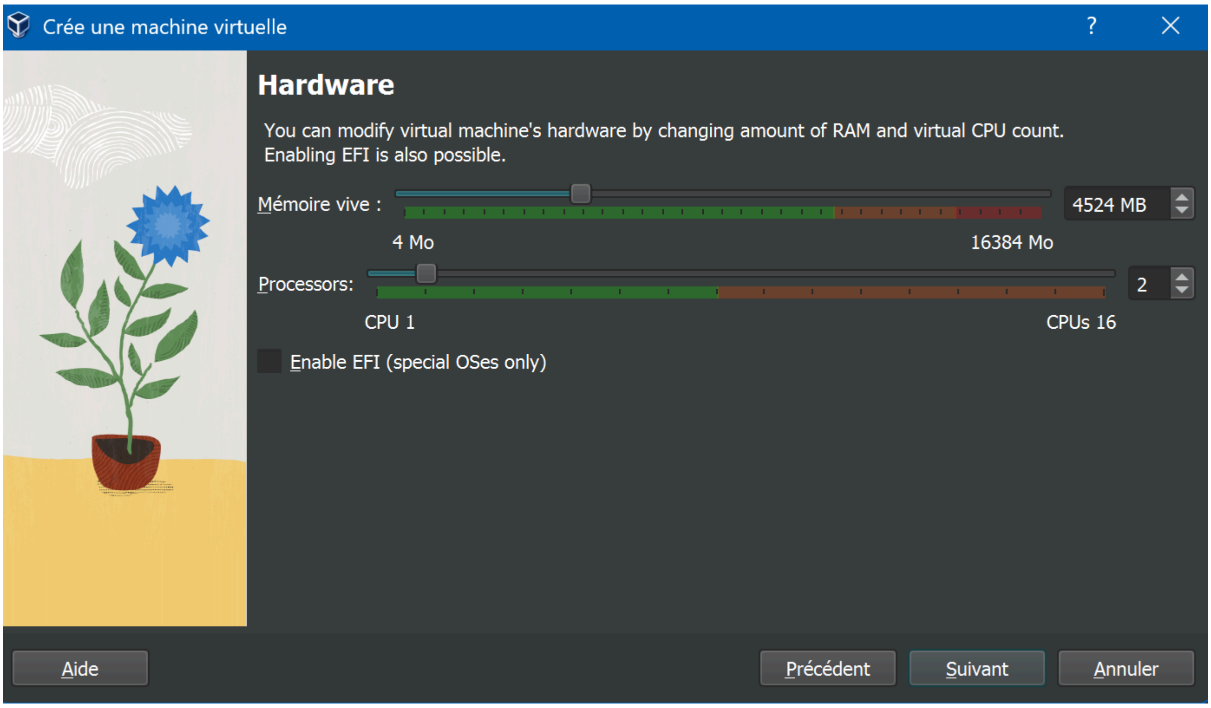
Hostname: VM1Wazuh ✓

Domain Name: myguest.virtualbox.org

□ Install in Background

□ Guest Additions

Guest Additions ISO: C:\Program Files\Oracle\VirtualBox\VBoxGuestAdditions.iso



Crée une machine virtuelle

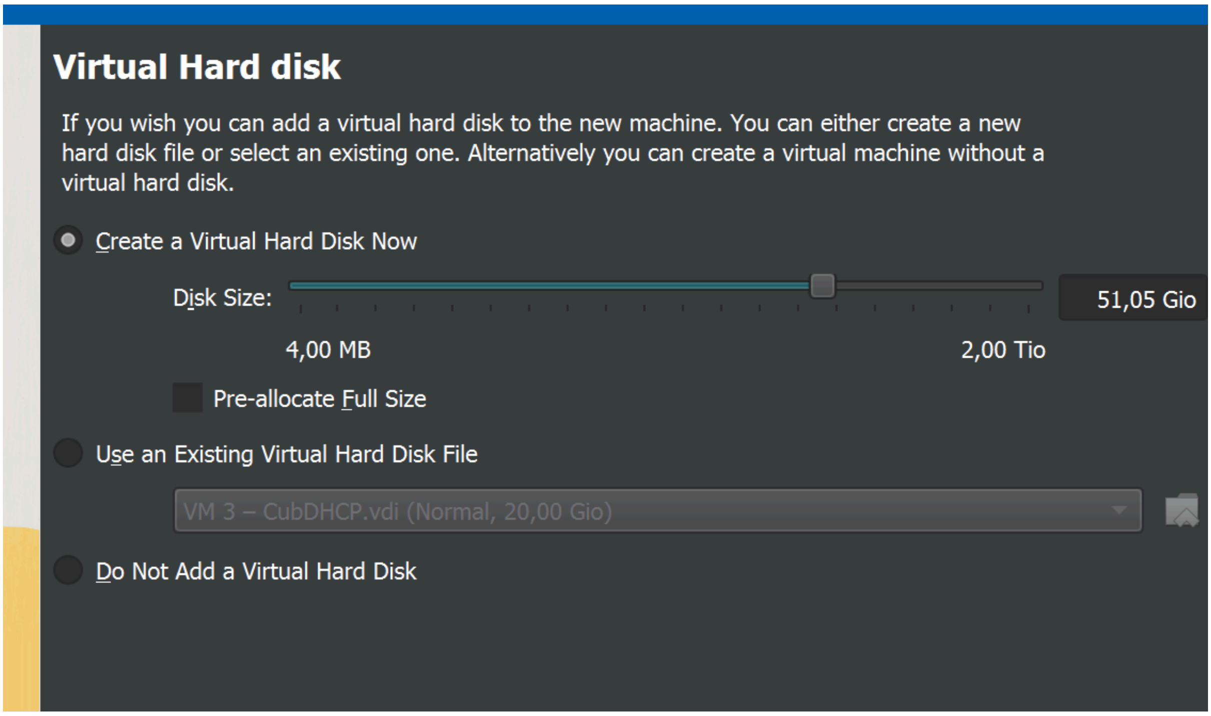
Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Mémoire vive : 4524 MB

Processors: 2

□ Enable EFI (special OSes only)



Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

● Create a Virtual Hard Disk Now

Disk Size: 51,05 Gio

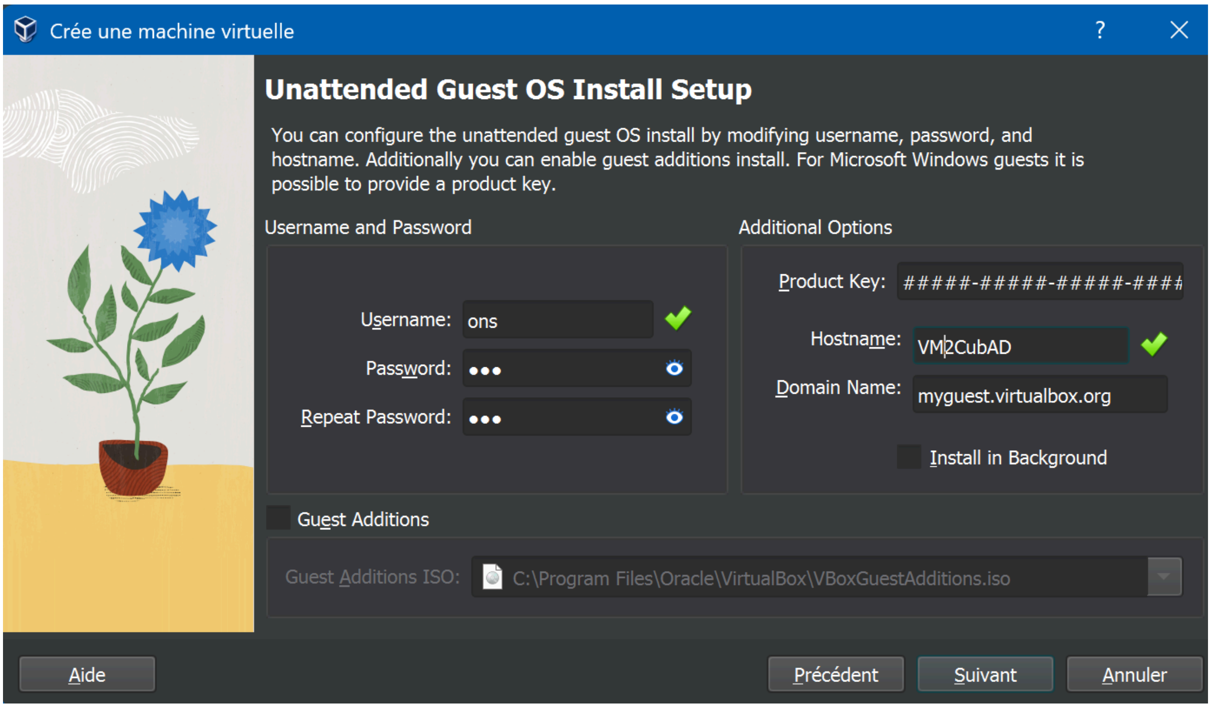
4,00 MB — 2,00 Tio

□ Pre-allocate Full Size

○ Use an Existing Virtual Hard Disk File

VM 3 – CubDHCP.vdi (Normal, 20,00 Gio)

○ Do Not Add a Virtual Hard Disk



Crée une machine virtuelle

Unattended Guest OS Install Setup

You can configure the unattended guest OS install by modifying username, password, and hostname. Additionally you can enable guest additions install. For Microsoft Windows guests it is possible to provide a product key.

Username and Password

Username: ons ✓

Password: •••

Repeat Password: •••

Additional Options

Product Key: #####-#####-#####-####

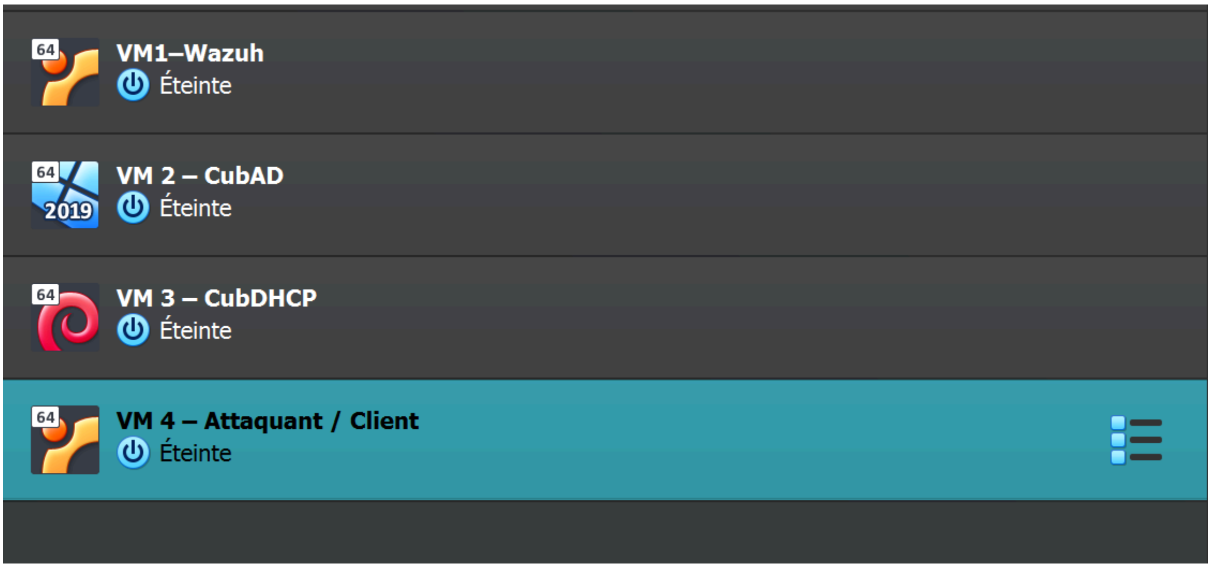
Hostname: VM2CubAD ✓

Domain Name: myguest.virtualbox.org

□ Install in Background

□ Guest Additions

Guest Additions ISO: C:\Program Files\Oracle\VirtualBox\VBoxGuestAdditions.iso

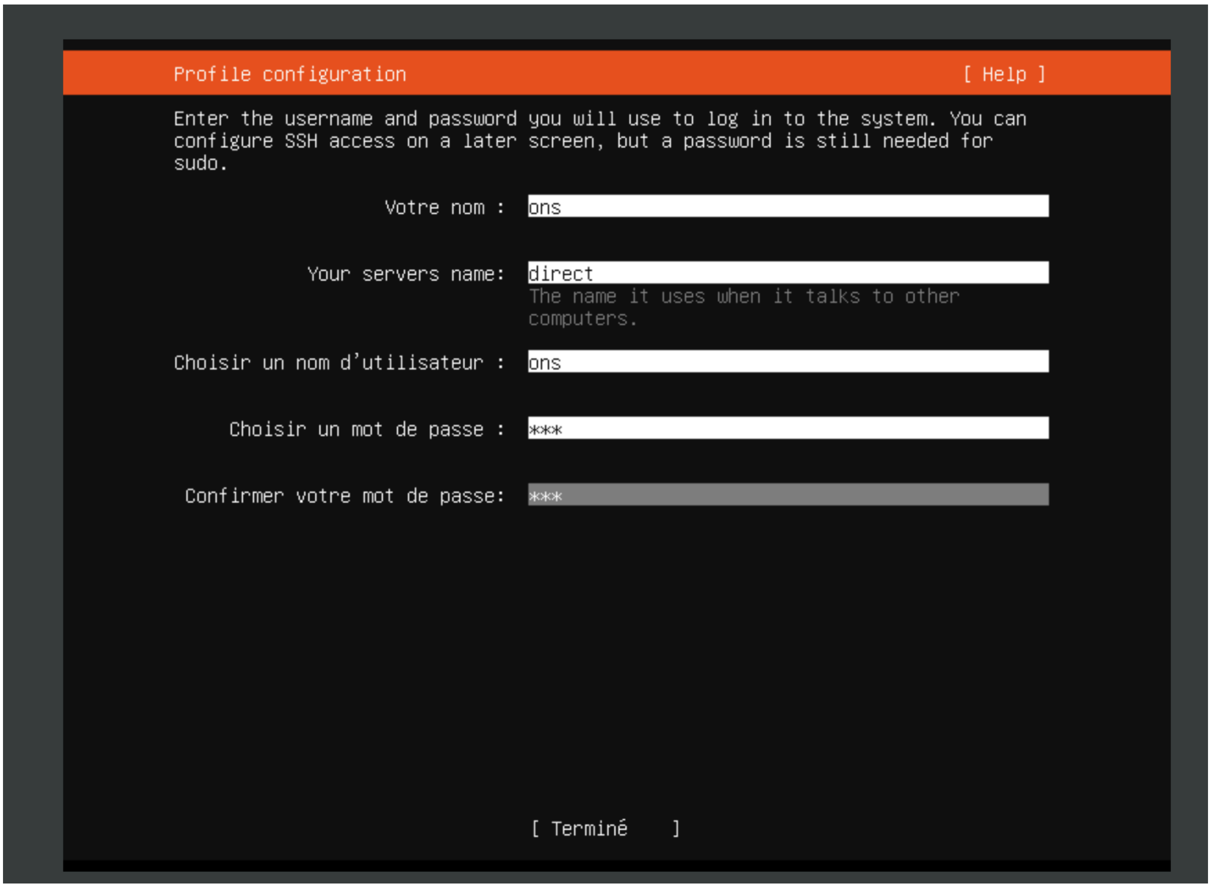


VM1–Wazuh
Éteinte

VM 2 – CubAD
Éteinte

VM 3 – CubDHCP
Éteinte

VM 4 – Attaquant / Client
Éteinte



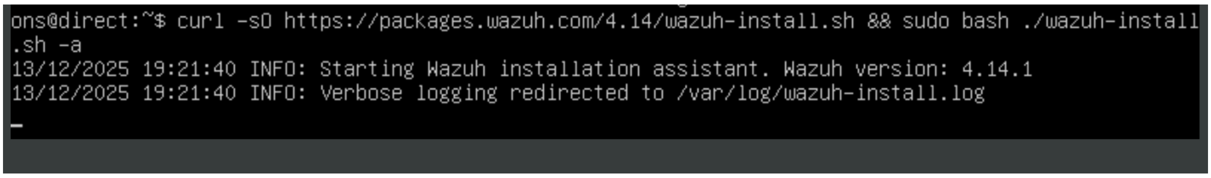
```
Profile configuration                                              [ Help ]

Enter the username and password you will use to log in to the system. You can
configure SSH access on a later screen, but a password is still needed for
sudo.

                 Votre nom :  ons

         Your servers name:  direct
                              The name it uses when it talks to other
                              computers.

 Choisir un nom d'utilisateur :  ons

      Choisir un mot de passe :  ***

   Confirmer votre mot de passe:  ***

                             [ Terminé     ]
```

mdp : ons

Choix d'installation du serveur wazuh

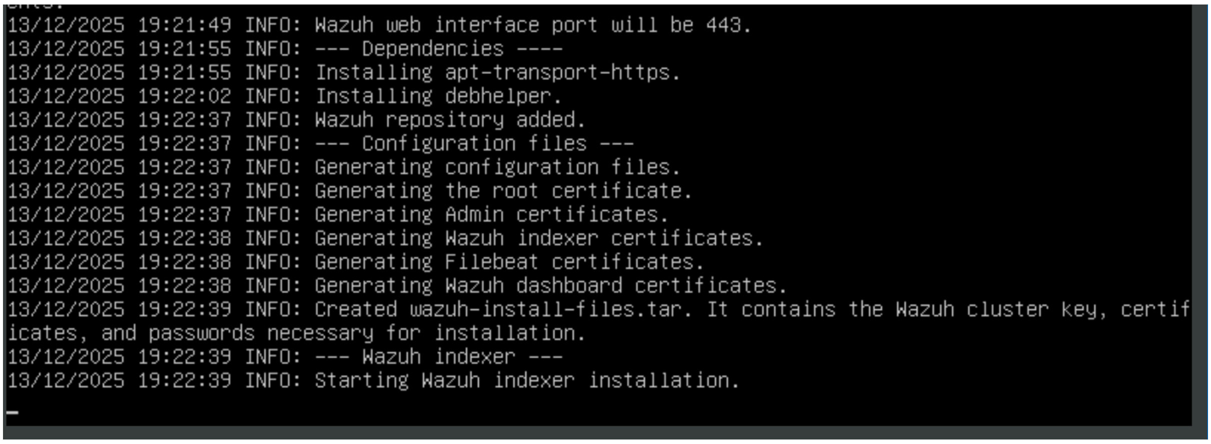
Dans le cadre de cette SAE, une **installation rapide en mode all-in-one** a été retenue via l'assistant officiel Wazuh

Ce choix permet de déployer automatiquement l'ensemble des composants (Indexer, Manager, Filebeat et Dashboard) sur un seul nœud, tout en garantissant une configuration cohérente et fonctionnelle, adaptée à un environnement pédagogique

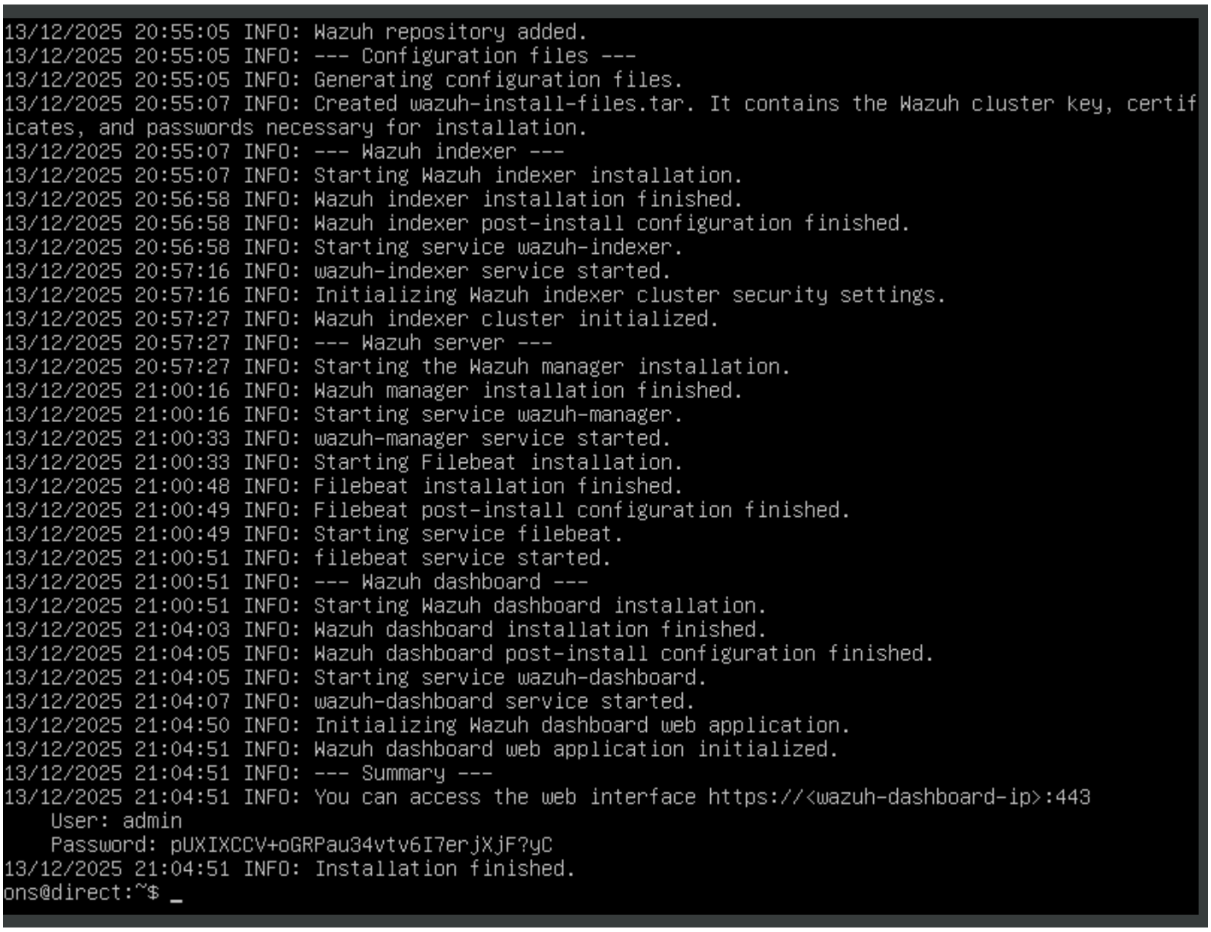


```
ons@direct:~$ curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install
.sh -a
13/12/2025 19:21:40 INFO: Starting Wazuh installation assistant. Wazuh version: 4.14.1
13/12/2025 19:21:40 INFO: Verbose logging redirected to /var/log/wazuh-install.log
_
```

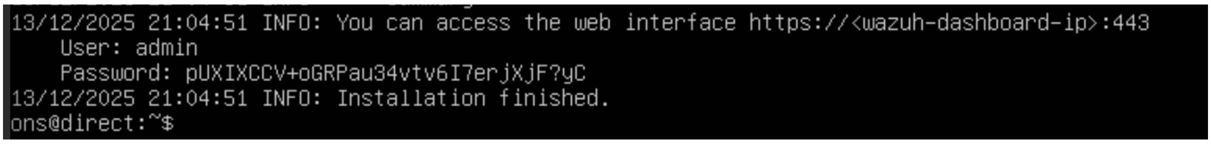
Installation de tous les composants



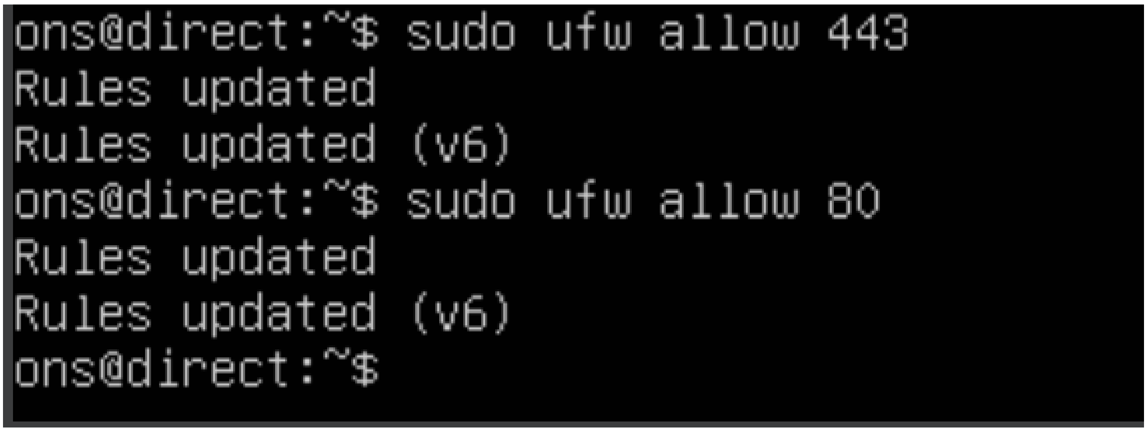
```
13/12/2025 19:21:49 INFO: Wazuh web interface port will be 443.
13/12/2025 19:21:55 INFO: --- Dependencies ----
13/12/2025 19:21:55 INFO: Installing apt-transport-https.
13/12/2025 19:22:02 INFO: Installing debhelper.
13/12/2025 19:22:37 INFO: Wazuh repository added.
13/12/2025 19:22:37 INFO: --- Configuration files ---
13/12/2025 19:22:37 INFO: Generating configuration files.
13/12/2025 19:22:37 INFO: Generating the root certificate.
13/12/2025 19:22:37 INFO: Generating Admin certificates.
13/12/2025 19:22:38 INFO: Generating Wazuh indexer certificates.
13/12/2025 19:22:38 INFO: Generating Filebeat certificates.
13/12/2025 19:22:38 INFO: Generating Wazuh dashboard certificates.
13/12/2025 19:22:39 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certif
icates, and passwords necessary for installation.
13/12/2025 19:22:39 INFO: --- Wazuh indexer ---
13/12/2025 19:22:39 INFO: Starting Wazuh indexer installation.
_
```



```
13/12/2025 20:55:05 INFO: Wazuh repository added.
13/12/2025 20:55:05 INFO: --- Configuration files ---
13/12/2025 20:55:05 INFO: Generating configuration files.
13/12/2025 20:55:07 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certif
icates, and passwords necessary for installation.
13/12/2025 20:55:07 INFO: --- Wazuh indexer ---
13/12/2025 20:55:07 INFO: Starting Wazuh indexer installation.
13/12/2025 20:56:58 INFO: Wazuh indexer installation finished.
13/12/2025 20:56:58 INFO: Wazuh indexer post-install configuration finished.
13/12/2025 20:56:58 INFO: Starting service wazuh-indexer.
13/12/2025 20:57:16 INFO: wazuh-indexer service started.
13/12/2025 20:57:16 INFO: Initializing Wazuh indexer cluster security settings.
13/12/2025 20:57:27 INFO: Wazuh indexer cluster initialized.
13/12/2025 20:57:27 INFO: --- Wazuh server ---
13/12/2025 20:57:27 INFO: Starting the Wazuh manager installation.
13/12/2025 21:00:16 INFO: Wazuh manager installation finished.
13/12/2025 21:00:16 INFO: Starting service wazuh-manager.
13/12/2025 21:00:33 INFO: wazuh-manager service started.
13/12/2025 21:00:33 INFO: Starting Filebeat installation.
13/12/2025 21:00:48 INFO: Filebeat installation finished.
13/12/2025 21:00:49 INFO: Filebeat post-install configuration finished.
13/12/2025 21:00:49 INFO: Starting service filebeat.
13/12/2025 21:00:51 INFO: filebeat service started.
13/12/2025 21:00:51 INFO: --- Wazuh dashboard ---
13/12/2025 21:00:51 INFO: Starting Wazuh dashboard installation.
13/12/2025 21:04:03 INFO: Wazuh dashboard installation finished.
13/12/2025 21:04:05 INFO: Wazuh dashboard post-install configuration finished.
13/12/2025 21:04:05 INFO: Starting service wazuh-dashboard.
13/12/2025 21:04:07 INFO: wazuh-dashboard service started.
13/12/2025 21:04:50 INFO: Initializing Wazuh dashboard web application.
13/12/2025 21:04:51 INFO: Wazuh dashboard web application initialized.
13/12/2025 21:04:51 INFO: --- Summary ---
13/12/2025 21:04:51 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: pUXIXCCV+oGRPau34vtv6I7erjXjF?yC
13/12/2025 21:04:51 INFO: Installation finished.
ons@direct:~$ _
```

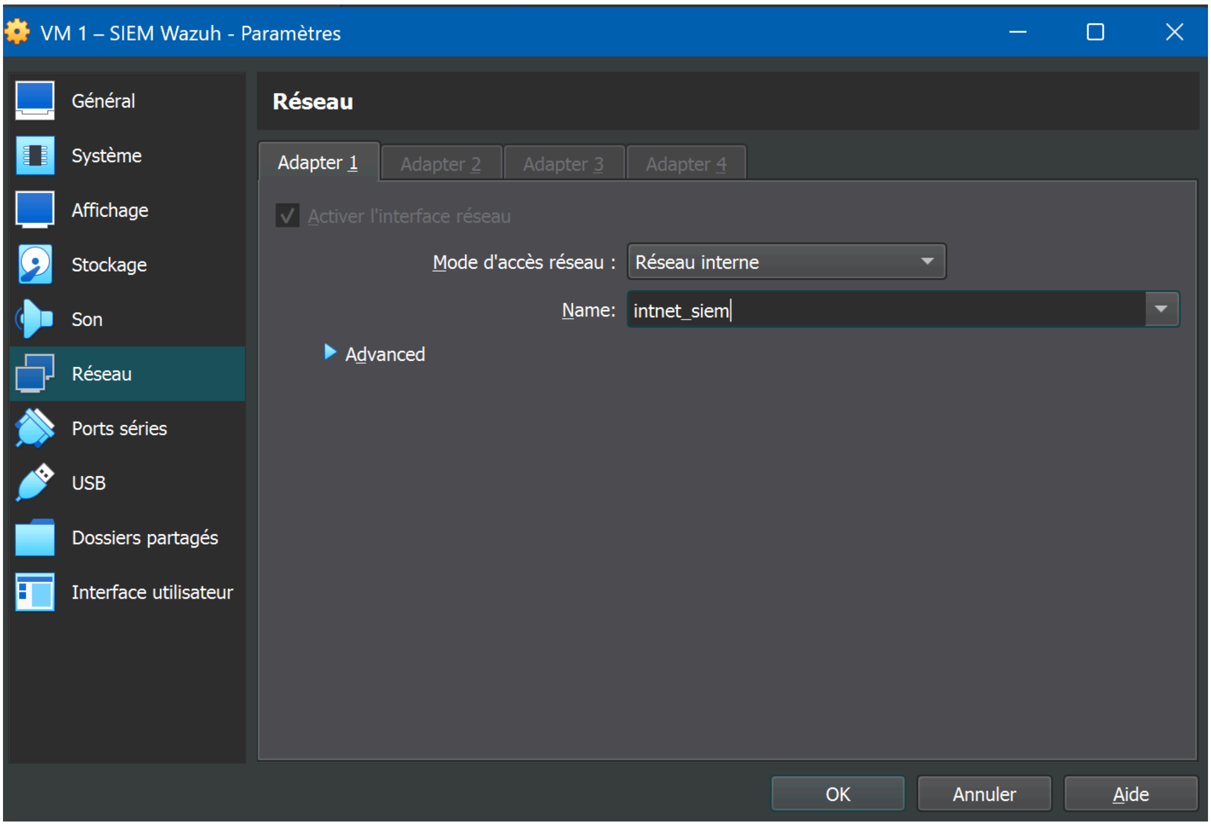


```
13/12/2025 21:04:51 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
    User: admin
    Password: pUXIXCCV+oGRPau34vtv6I7erjXjF?yC
13/12/2025 21:04:51 INFO: Installation finished.
ons@direct:~$
```



```
ons@direct:~$ sudo ufw allow 443
Rules updated
Rules updated (v6)
ons@direct:~$ sudo ufw allow 80
Rules updated
Rules updated (v6)
ons@direct:~$
```

Configuration réseau:



VM 1 – SIEM Wazuh - Paramètres

Réseau

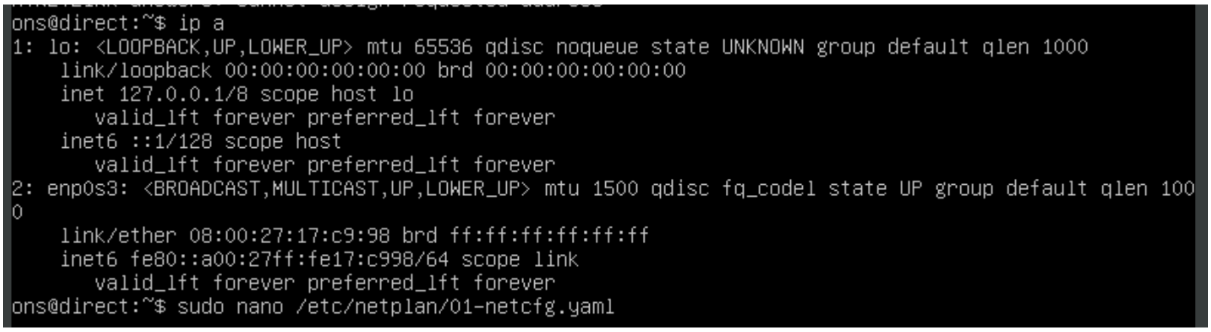
Adapter 1

☑ Activer l'interface réseau

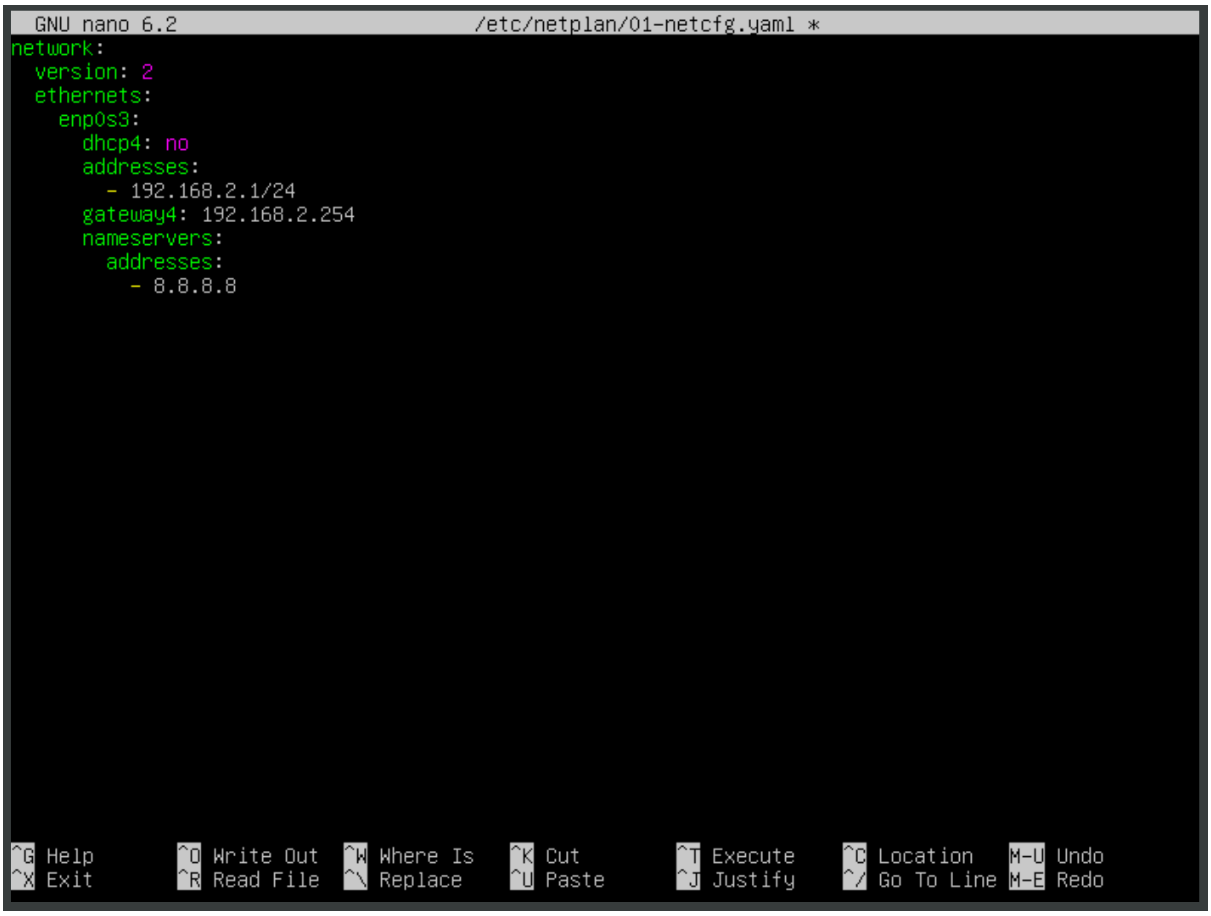
Mode d'accès réseau : Réseau interne

Name: intnet_siem

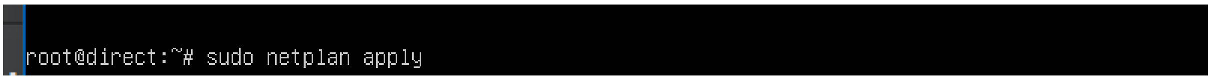
Configuration IP CubWazuh



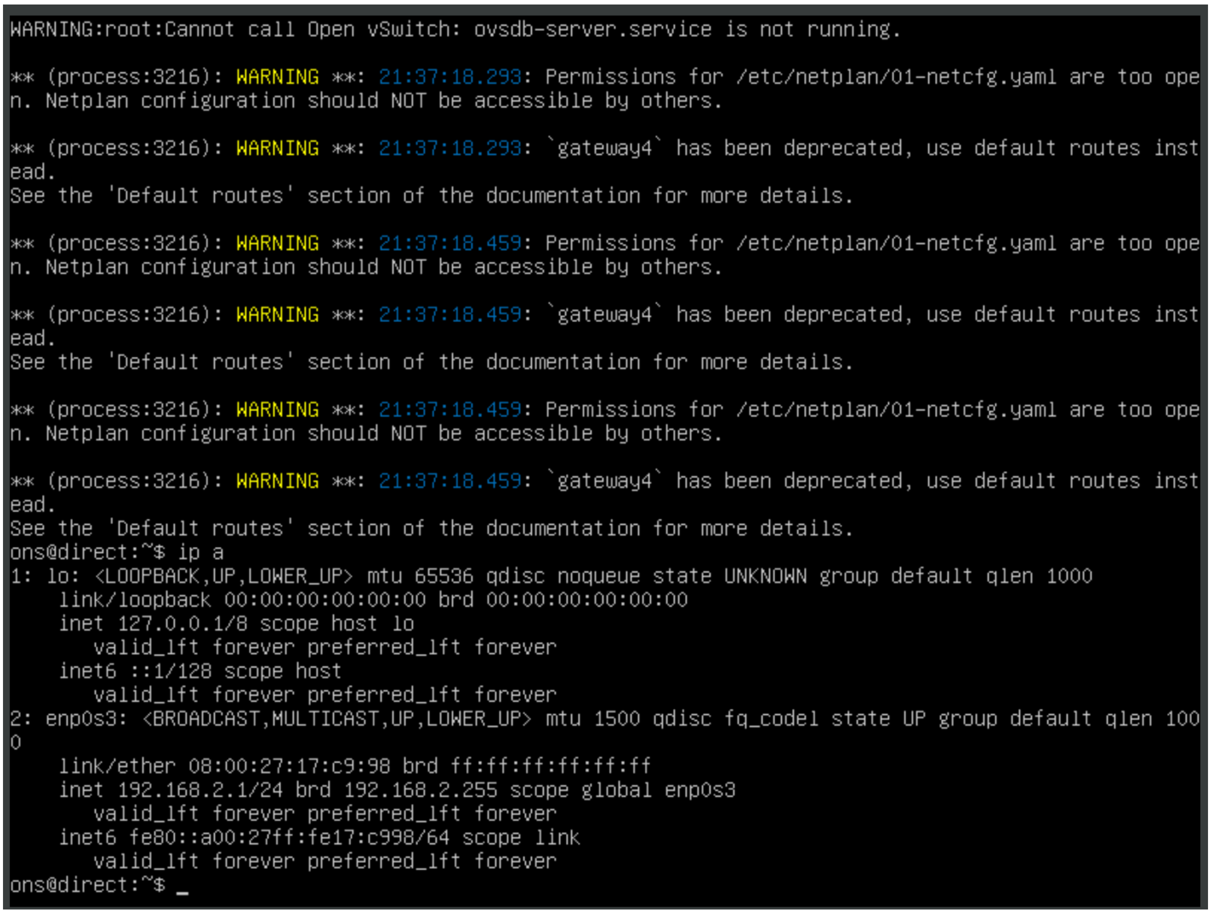
```
ons@direct:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:17:c9:98 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a00:27ff:fe17:c998/64 scope link
       valid_lft forever preferred_lft forever
ons@direct:~$ sudo nano /etc/netplan/01-netcfg.yaml
```



```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.2.1/24
      gateway4: 192.168.2.254
      nameservers:
        addresses:
          - 8.8.8.8
```

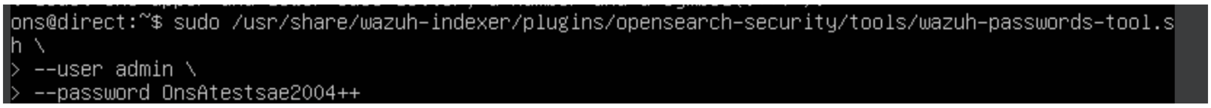


```
root@direct:~# sudo netplan apply
```

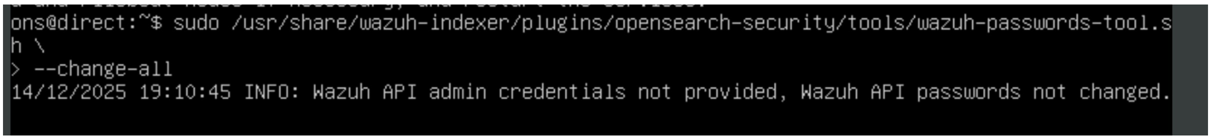


```
WARNING:root:Cannot call Open vSwitch: ovsdb-server.service is not running.

** (process:3216): WARNING **: 21:37:18.293: Permissions for /etc/netplan/01-netcfg.yaml are too ope
n. Netplan configuration should NOT be accessible by others.

** (process:3216): WARNING **: 21:37:18.293: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.

** (process:3216): WARNING **: 21:37:18.459: Permissions for /etc/netplan/01-netcfg.yaml are too ope
n. Netplan configuration should NOT be accessible by others.

** (process:3216): WARNING **: 21:37:18.459: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.

** (process:3216): WARNING **: 21:37:18.459: Permissions for /etc/netplan/01-netcfg.yaml are too ope
n. Netplan configuration should NOT be accessible by others.

** (process:3216): WARNING **: 21:37:18.459: `gateway4` has been deprecated, use default routes inst
ead.
See the 'Default routes' section of the documentation for more details.
ons@direct:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:17:c9:98 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.1/24 brd 192.168.2.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe17:c998/64 scope link
       valid_lft forever preferred_lft forever
ons@direct:~$ _
```

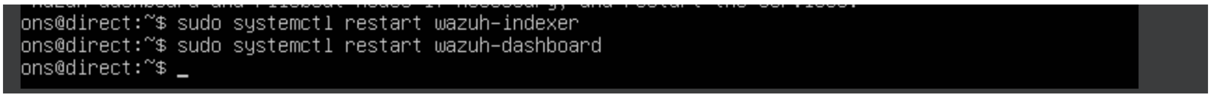
Les mots de passe par défaut ont été modifiés en ligne de commande avant l’accès au tableau de bord Wazuh afin de renforcer la sécurité et d’éviter une initialisation lente de l’interface web.



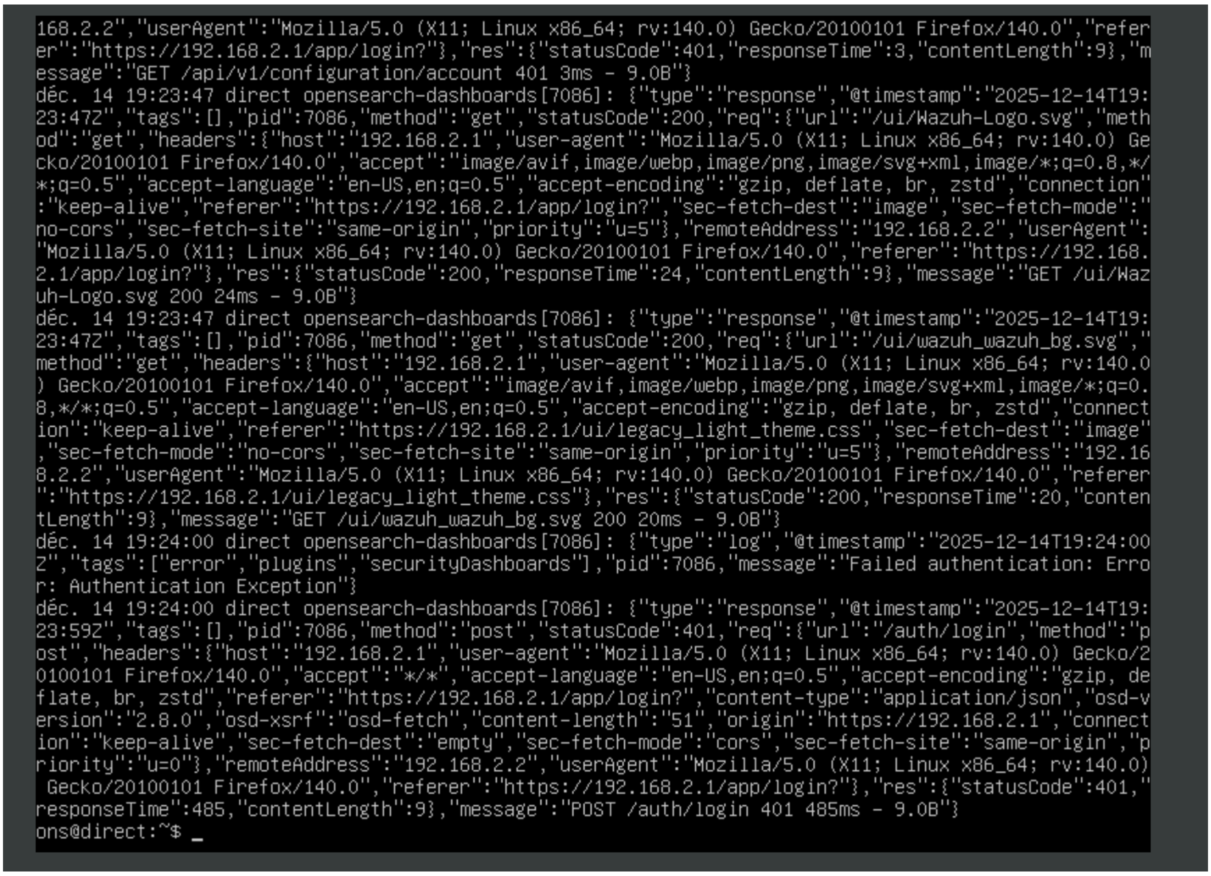
```
ons@direct:~$ sudo /usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.s
h \
> --user admin \
> --password OnsAtestsae2004++
```



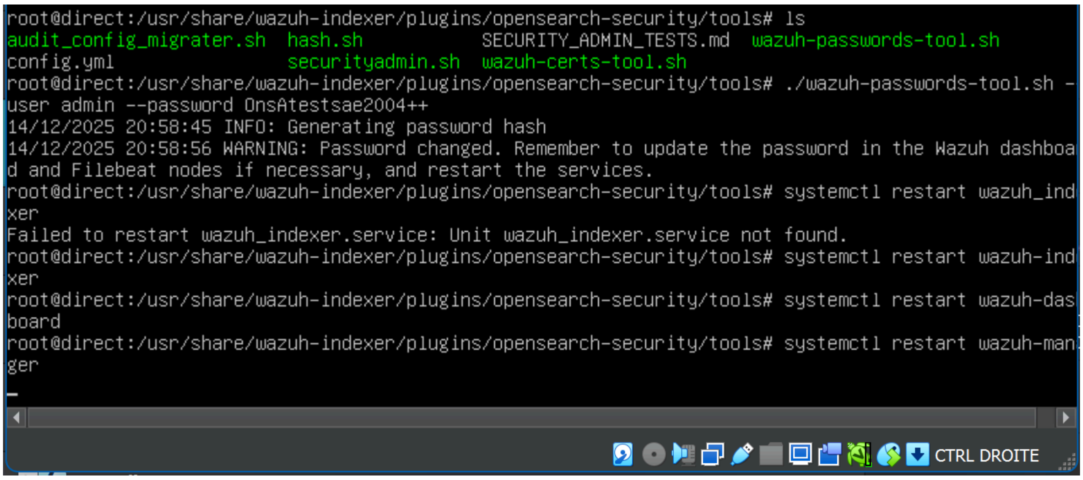
```
ons@direct:~$ sudo /usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.s
h \
> --change-all
14/12/2025 19:10:45 INFO: Wazuh API admin credentials not provided, Wazuh API passwords not changed.
```



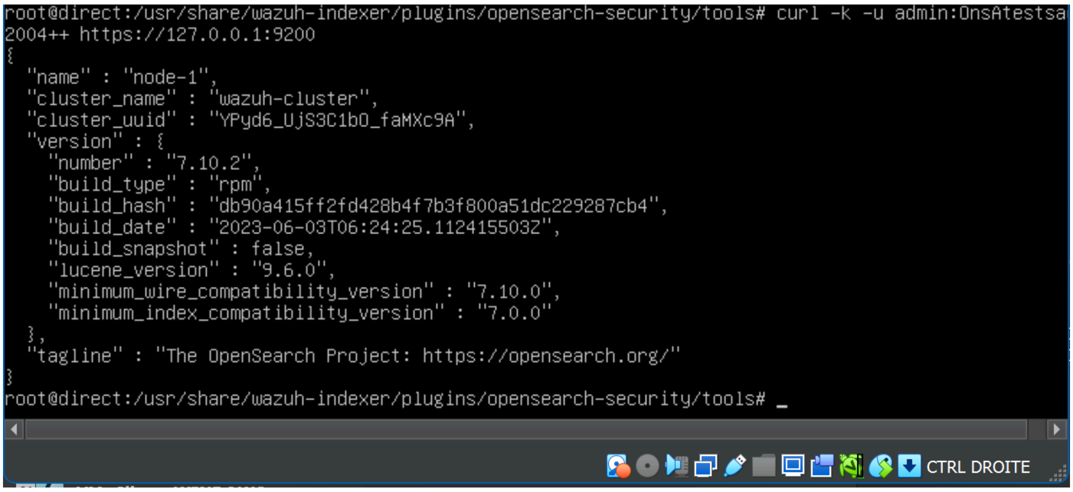
```
ons@direct:~$ sudo systemctl restart wazuh-indexer
ons@direct:~$ sudo systemctl restart wazuh-dashboard
ons@direct:~$ _
```



```
168.2.2","userAgent":"Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0","refer
er":"https://192.168.2.1/app/login?"},"res":{"statusCode":401,"responseTime":3,"contentLength":9},"m
essage":"GET /api/v1/configuration/account 401 3ms - 9.0B"}
déc. 14 19:23:47 direct opensearch-dashboards[7086]: {"type":"response","@timestamp":"2025-12-14T19:
23:47Z","tags":[],"pid":7086,"method":"get","statusCode":200,"req":{"url":"/ui/Wazuh-Logo.svg","meth
od":"get","headers":{"host":"192.168.2.1","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Ge
cko/20100101 Firefox/140.0","accept":"image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/
*;q=0.5","accept-language":"en-US,en;q=0.5","accept-encoding":"gzip, deflate, br, zstd","connection"
:"keep-alive","referer":"https://192.168.2.1/app/login?","sec-fetch-dest":"image","sec-fetch-mode":"
no-cors","sec-fetch-site":"same-origin","priority":"u=5"},"remoteAddress":"192.168.2.2","userAgent":
"Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0","referer":"https://192.168.
2.1/app/login?"},"res":{"statusCode":200,"responseTime":24,"contentLength":9},"message":"GET /ui/Waz
uh-Logo.svg 200 24ms - 9.0B"}
déc. 14 19:23:47 direct opensearch-dashboards[7086]: {"type":"response","@timestamp":"2025-12-14T19:
23:47Z","tags":[],"pid":7086,"method":"get","statusCode":200,"req":{"url":"/ui/wazuh_wazuh_bg.svg","
method":"get","headers":{"host":"192.168.2.1","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:140.0
) Gecko/20100101 Firefox/140.0","accept":"image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.
8,*/*;q=0.5","accept-language":"en-US,en;q=0.5","accept-encoding":"gzip, deflate, br, zstd","connect
ion":"keep-alive","referer":"https://192.168.2.1/ui/legacy_light_theme.css","sec-fetch-dest":"image"
,"sec-fetch-mode":"no-cors","sec-fetch-site":"same-origin","priority":"u=5"},"remoteAddress":"192.16
8.2.2","userAgent":"Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0","referer
":"https://192.168.2.1/ui/legacy_light_theme.css"},"res":{"statusCode":200,"responseTime":20,"conten
tLength":9},"message":"GET /ui/wazuh_wazuh_bg.svg 200 20ms - 9.0B"}
déc. 14 19:24:00 direct opensearch-dashboards[7086]: {"type":"log","@timestamp":"2025-12-14T19:24:00
Z","tags":["error","plugins","securityDashboards"],"pid":7086,"message":"Failed authentication: Erro
r: Authentication Exception"}
déc. 14 19:24:00 direct opensearch-dashboards[7086]: {"type":"response","@timestamp":"2025-12-14T19:
23:59Z","tags":[],"pid":7086,"method":"post","statusCode":401,"req":{"url":"/auth/login","method":"p
ost","headers":{"host":"192.168.2.1","user-agent":"Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/2
0100101 Firefox/140.0","accept":"*/*","accept-language":"en-US,en;q=0.5","accept-encoding":"gzip, de
flate, br, zstd","referer":"https://192.168.2.1/app/login?","content-type":"application/json","osd-v
ersion":"2.8.0","osd-xsrf":"osd-fetch","content-length":"51","origin":"https://192.168.2.1","connect
ion":"keep-alive","sec-fetch-dest":"empty","sec-fetch-mode":"cors","sec-fetch-site":"same-origin","p
riority":"u=0"},"remoteAddress":"192.168.2.2","userAgent":"Mozilla/5.0 (X11; Linux x86_64; rv:140.0)
 Gecko/20100101 Firefox/140.0","referer":"https://192.168.2.1/app/login?"},"res":{"statusCode":401,"
responseTime":485,"contentLength":9},"message":"POST /auth/login 401 485ms - 9.0B"}
ons@direct:~$ _
```

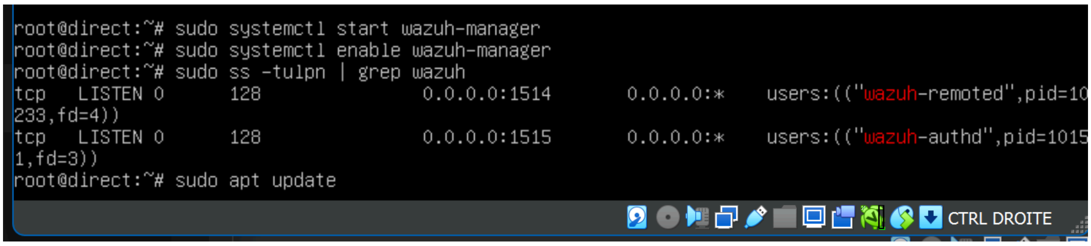


```
root@direct:/usr/share/wazuh-indexer/plugins/opensearch-security/tools# ls
audit_config_migrater.sh  hash.sh            SECURITY_ADMIN_TESTS.md  wazuh-passwords-tool.sh
config.yml                securityadmin.sh  wazuh-certs-tool.sh
root@direct:/usr/share/wazuh-indexer/plugins/opensearch-security/tools# ./wazuh-passwords-tool.sh -
user admin --password OnsAtestsae2004++
14/12/2025 20:58:45 INFO: Generating password hash
14/12/2025 20:58:56 WARNING: Password changed. Remember to update the password in the Wazuh dashboa
d and Filebeat nodes if necessary, and restart the services.
root@direct:/usr/share/wazuh-indexer/plugins/opensearch-security/tools# systemctl restart wazuh_ind
xer
Failed to restart wazuh_indexer.service: Unit wazuh_indexer.service not found.
root@direct:/usr/share/wazuh-indexer/plugins/opensearch-security/tools# systemctl restart wazuh-ind
xer
root@direct:/usr/share/wazuh-indexer/plugins/opensearch-security/tools# systemctl restart wazuh-das
board
root@direct:/usr/share/wazuh-indexer/plugins/opensearch-security/tools# systemctl restart wazuh-man
ger
_
```

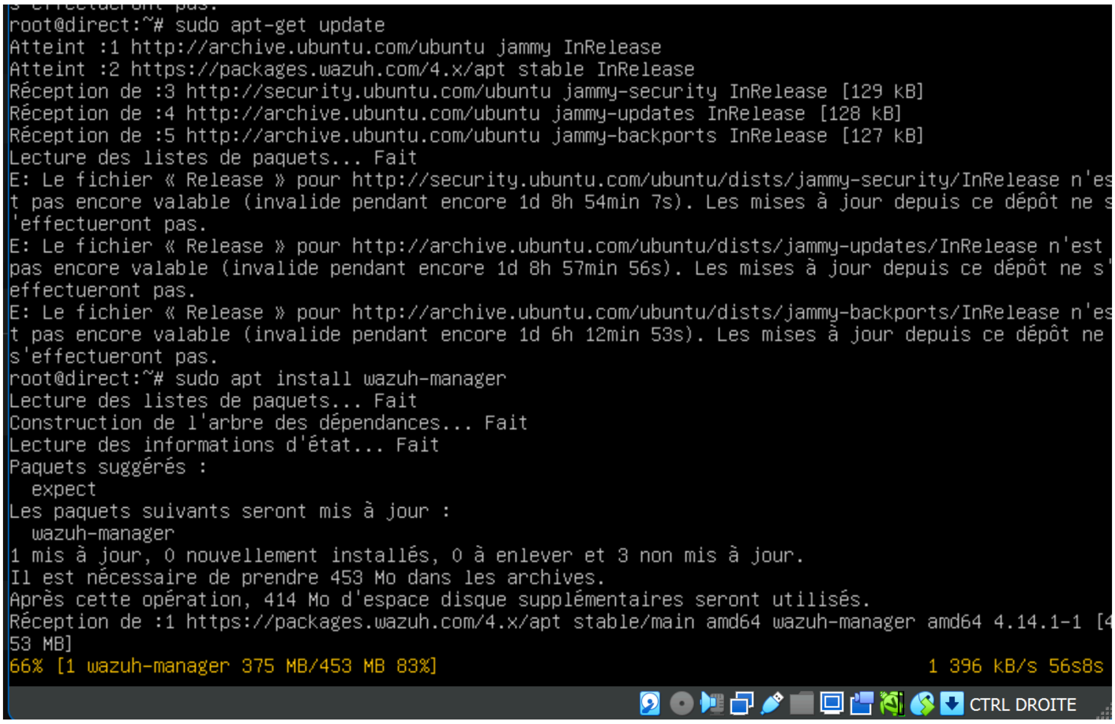


```
root@direct:/usr/share/wazuh-indexer/plugins/opensearch-security/tools# curl -k -u admin:OnsAtestsa
2004++ https://127.0.0.1:9200
{
  "name" : "node-1",
  "cluster_name" : "wazuh-cluster",
  "cluster_uuid" : "YPyd6_UjS3C1b0_faMXc9A",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
    "build_date" : "2023-06-03T06:24:25.112415503Z",
    "build_snapshot" : false,
    "lucene_version" : "9.6.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
root@direct:/usr/share/wazuh-indexer/plugins/opensearch-security/tools# _
```

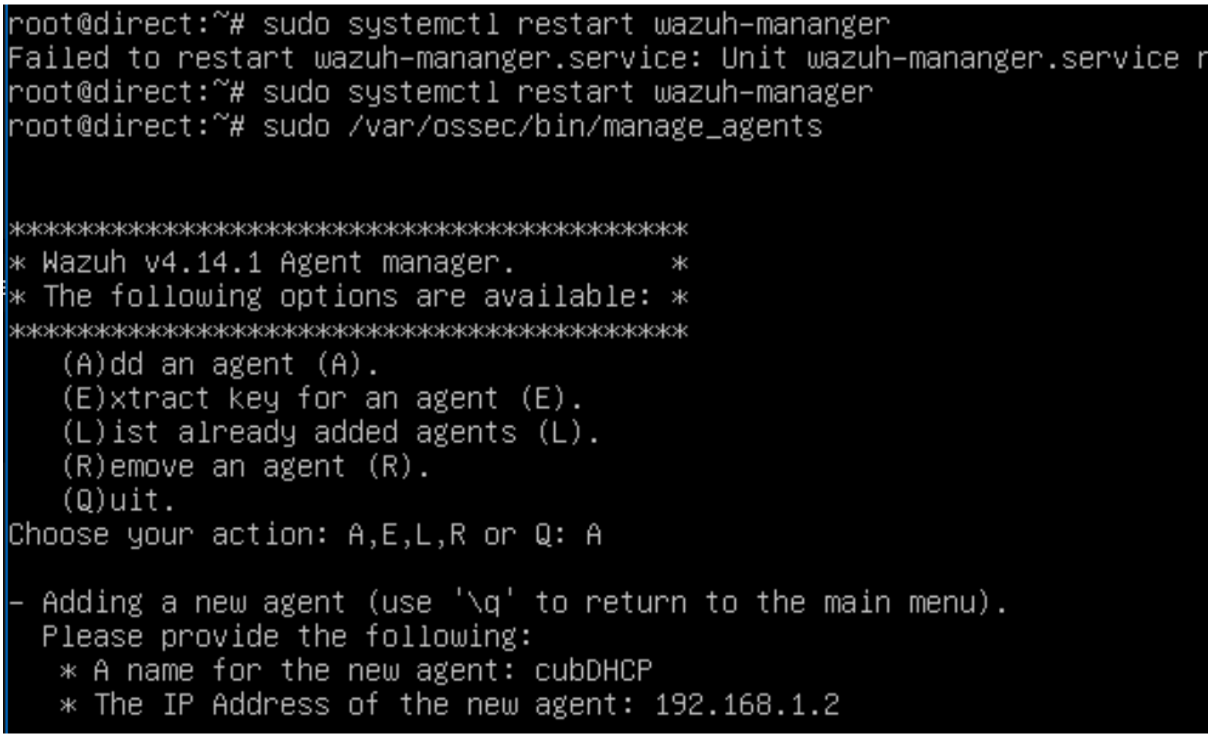
Enregistrement de l’agent



```
root@direct:~# sudo systemctl start wazuh-manager
root@direct:~# sudo systemctl enable wazuh-manager
root@direct:~# sudo ss -tulpn | grep wazuh
tcp   LISTEN 0      128                0.0.0.0:1514       0.0.0.0:*    users:(("wazuh-remoted",pid=10
233,fd=4))
tcp   LISTEN 0      128                0.0.0.0:1515       0.0.0.0:*    users:(("wazuh-authd",pid=1015
1,fd=3))
root@direct:~# sudo apt update
```

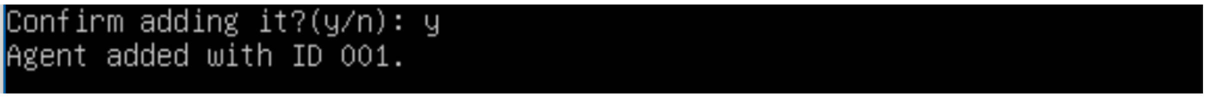


```
s'effectueront pas.
root@direct:~# sudo apt-get update
Atteint :1 http://archive.ubuntu.com/ubuntu jammy InRelease
Atteint :2 https://packages.wazuh.com/4.x/apt stable InRelease
Réception de :3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Réception de :4 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Réception de :5 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Lecture des listes de paquets... Fait
E: Le fichier « Release » pour http://security.ubuntu.com/ubuntu/dists/jammy-security/InRelease n'es
t pas encore valable (invalide pendant encore 1d 8h 54min 7s). Les mises à jour depuis ce dépôt ne s
'effectueront pas.
E: Le fichier « Release » pour http://archive.ubuntu.com/ubuntu/dists/jammy-updates/InRelease n'est
pas encore valable (invalide pendant encore 1d 8h 57min 56s). Les mises à jour depuis ce dépôt ne s'
effectueront pas.
E: Le fichier « Release » pour http://archive.ubuntu.com/ubuntu/dists/jammy-backports/InRelease n'es
t pas encore valable (invalide pendant encore 1d 6h 12min 53s). Les mises à jour depuis ce dépôt ne
s'effectueront pas.
root@direct:~# sudo apt install wazuh-manager
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Paquets suggérés :
  expect
Les paquets suivants seront mis à jour :
  wazuh-manager
1 mis à jour, 0 nouvellement installés, 0 à enlever et 3 non mis à jour.
Il est nécessaire de prendre 453 Mo dans les archives.
Après cette opération, 414 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-manager amd64 4.14.1-1 [4
53 MB]
66% [1 wazuh-manager 375 MB/453 MB 83%]                                      1 396 kB/s 56s8s
```



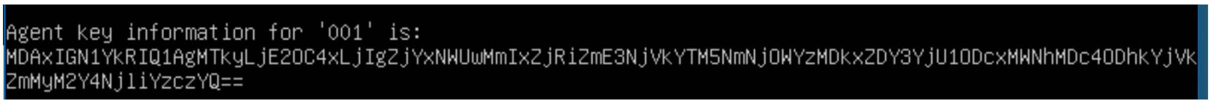
```
root@direct:~# sudo systemctl restart wazuh-mananger
Failed to restart wazuh-mananger.service: Unit wazuh-mananger.service r
root@direct:~# sudo systemctl restart wazuh-manager
root@direct:~# sudo /var/ossec/bin/manage_agents


****************************************
* Wazuh v4.14.1 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: A

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
   * A name for the new agent: cubDHCP
   * The IP Address of the new agent: 192.168.1.2
```

ID

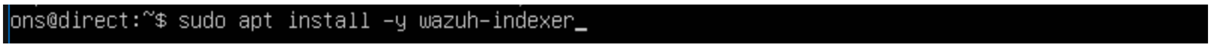


```
Confirm adding it?(y/n): y
Agent added with ID 001.
```

clé
MDAXIGN1YKRIQ1AgMTkyLjE20C4xLjIgzJYxNWUwMmIxZjRiZmE3NjVKYTMSNmNjOHYz MDkx2DY3YjU1ODcxMHNhMDc4ODhkYjVk ZmMyM2Y4NJlÍYzczYQ==

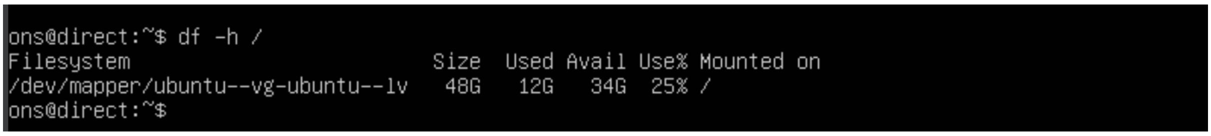


```
Agent key information for '001' is:
MDAxIGN1YkRIQ1AgMTkyLjE2OC4xLjIgZjYxNWUwMmIxZjRiZmE3NjVkYTM5NmNjOWYzMDkxZDY3YjU1ODcxMWNhMDc4ODhkYjVk
ZmMyM2Y4NjliYzczYQ==
```



```
ons@direct:~$ sudo apt install -y wazuh-indexer_
```

Problème rencontré :



```
ons@direct:~$ df -h /
Filesystem                         Size  Used Avail Use% Mounted on
/dev/mapper/ubuntu--vg-ubuntu--lv   48G   12G   34G  25% /
ons@direct:~$
```

problème de stockage, solution resize de la partition sda3 de 12go → 50go