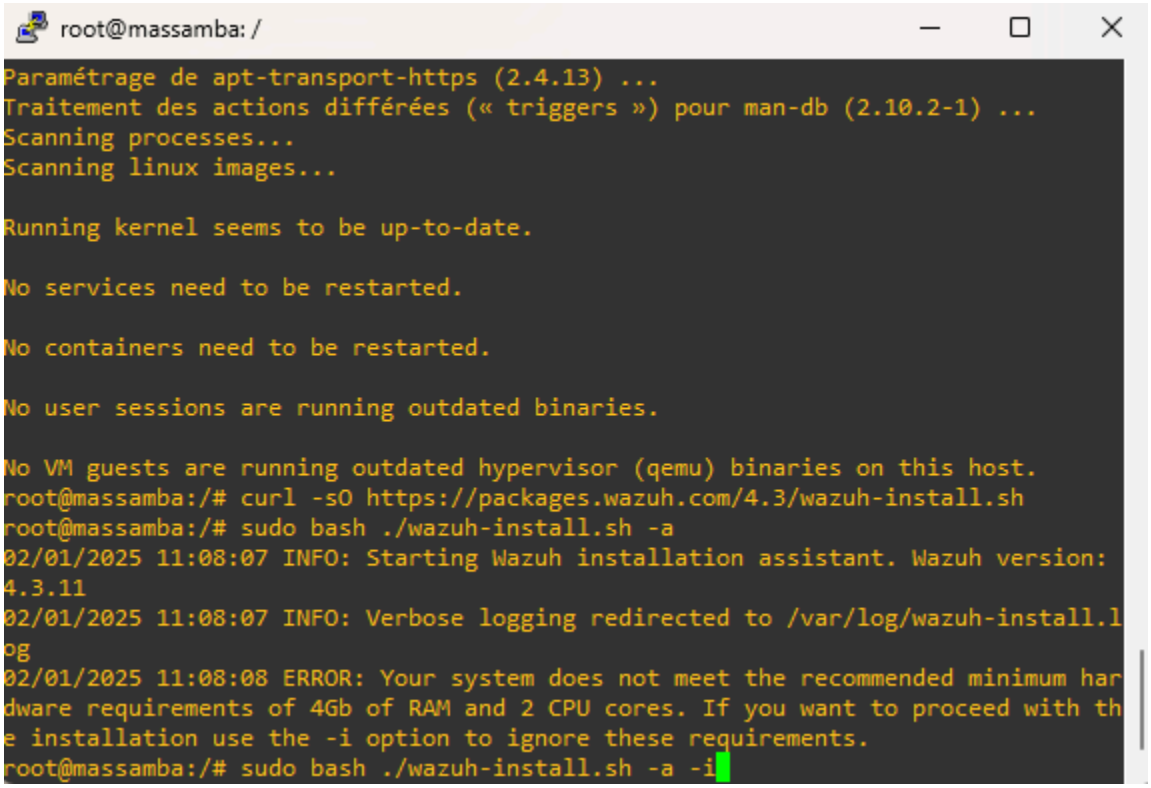
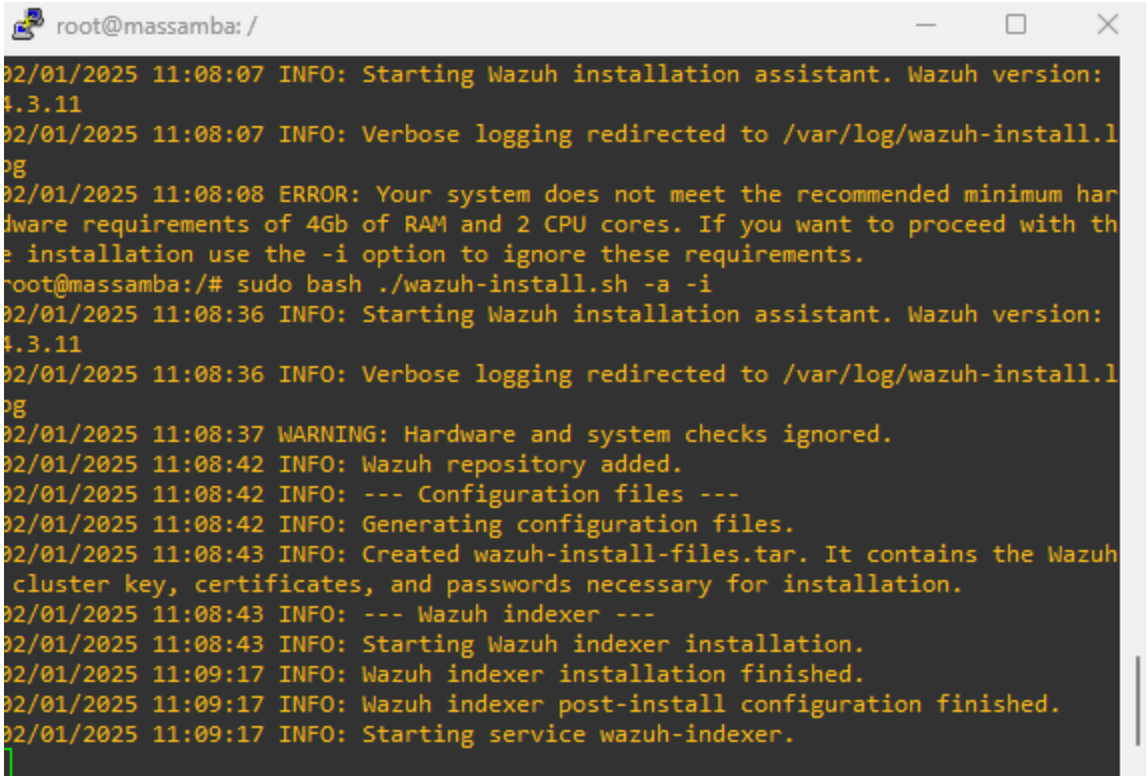
WAZUH

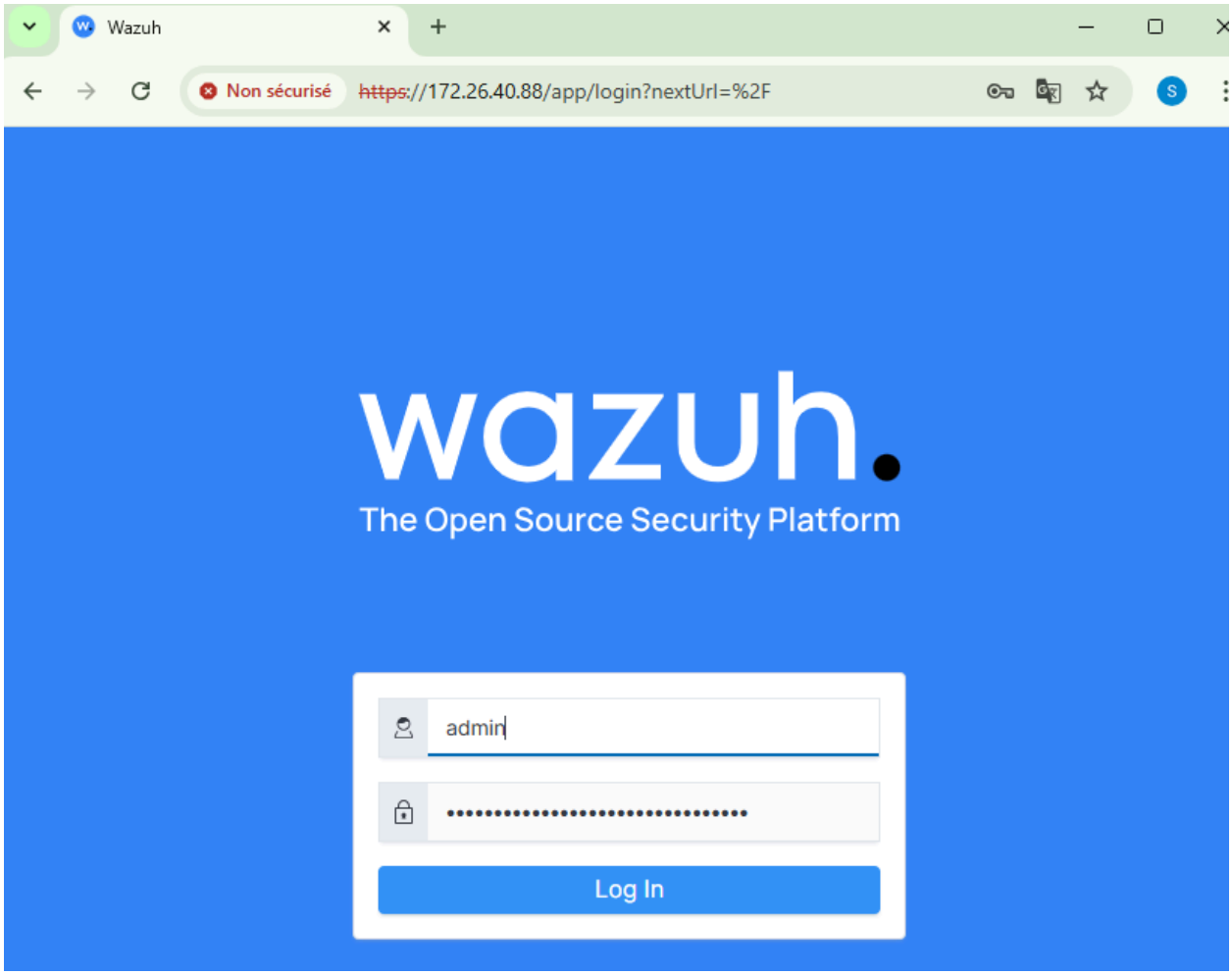

root@massamba: /
Paramétrage de apt-transport-https (2.4.13) ...
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@massamba:/# curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh
root@massamba:/# sudo bash ./wazuh-install.sh -a
02/01/2025 11:08:07 INFO: Starting Wazuh installation assistant. Wazuh version:
4.3.11
02/01/2025 11:08:07 INFO: Verbose logging redirected to /var/log/wazuh-install.l
og
02/01/2025 11:08:08 ERROR: Your system does not meet the recommended minimum har
dware requirements of 4Gb of RAM and 2 CPU cores. If you want to proceed with th
e installation use the -i option to ignore these requirements.
root@massamba:/# sudo bash ./wazuh-install.sh -a -i

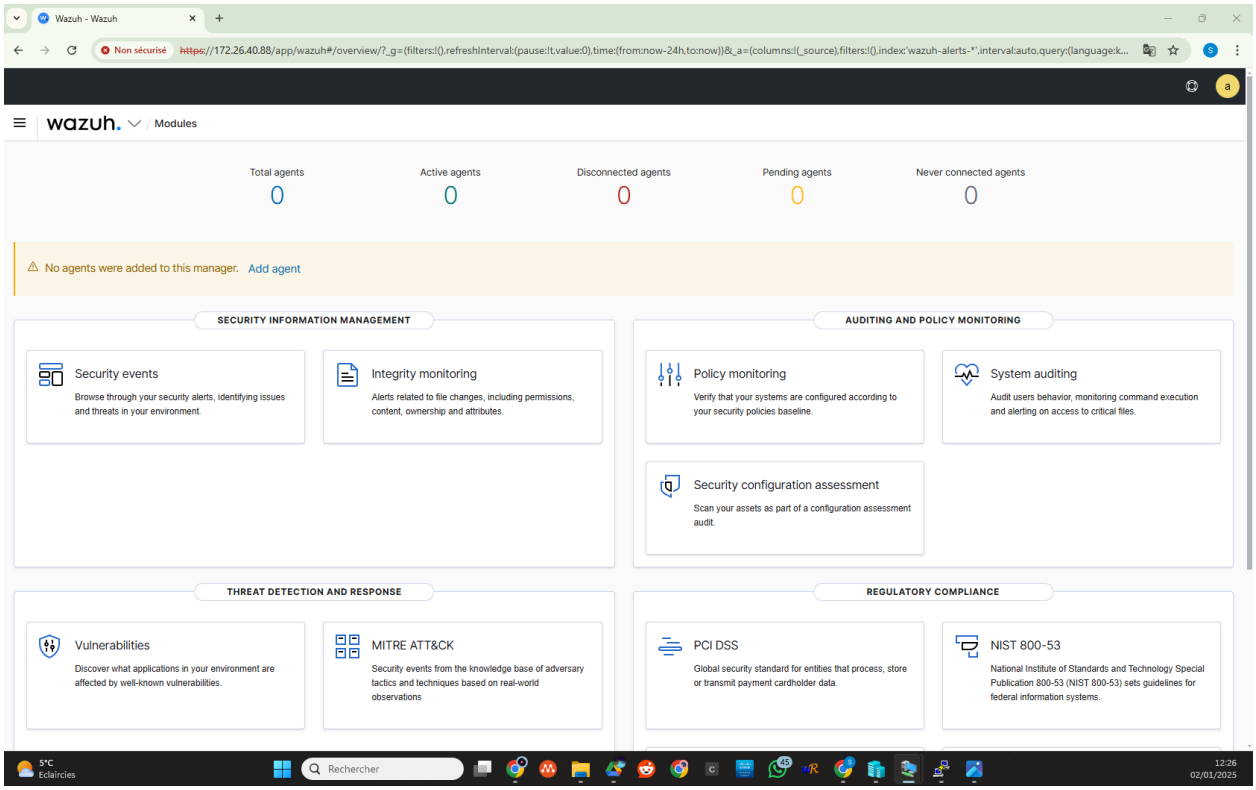


installation

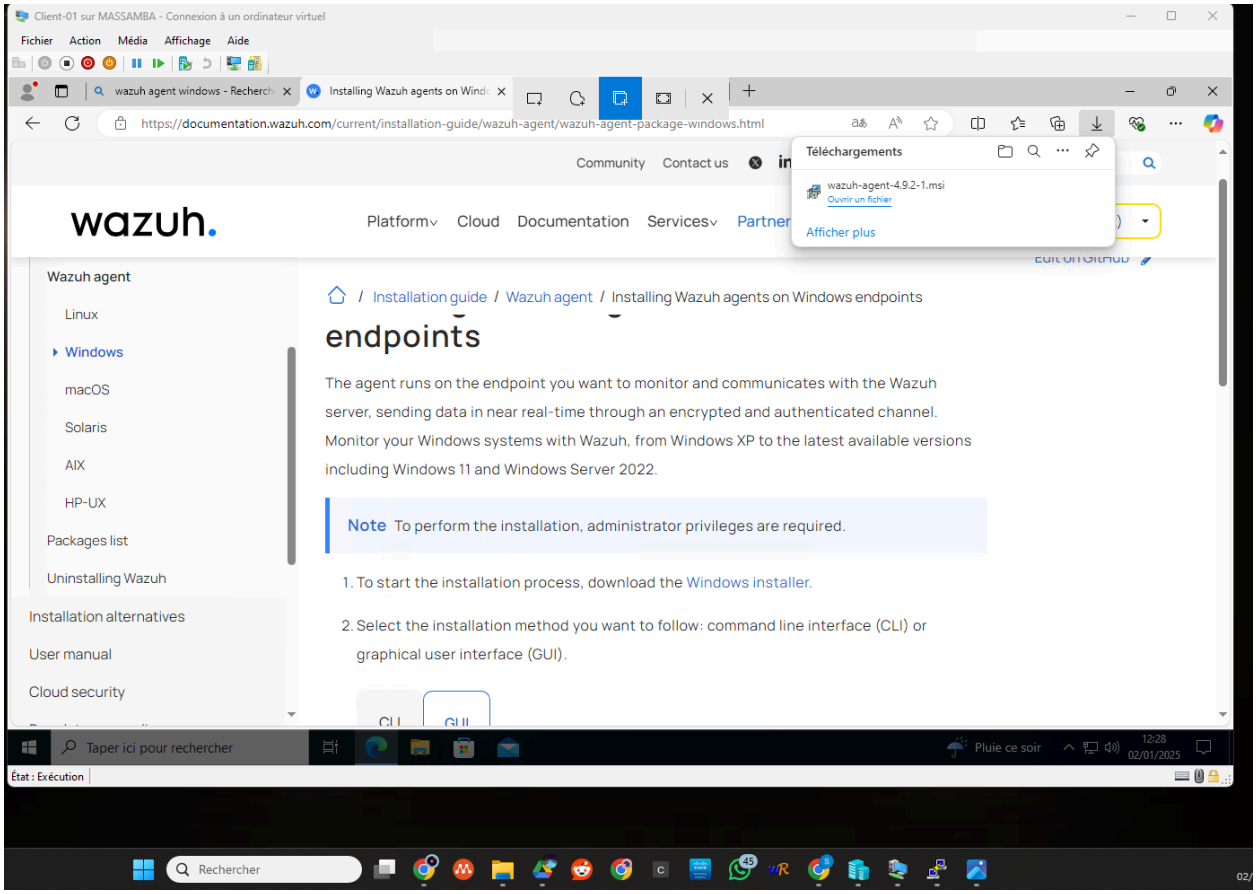
root@massamba:/# sudo bash ./wazuh-install.sh -a
02/01/2025 11:08:07 INFO: Starting Wazuh installation assistant. Wazuh version: 4.3.11
02/01/2025 11:08:07 INFO: Verbose logging redirected to /var/log/wazuh-install.log
02/01/2025 11:08:08 ERROR: Your system does not meet the recommended minimum hardware requirements of 4Gb of RAM and 2 CPU cores. If you want to proceed with the installation use the -i option to ignore these requirements.
root@massamba:/# sudo bash ./wazuh-install.sh -a -i
02/01/2025 11:08:36 INFO: Starting Wazuh installation assistant. Wazuh version: 4.3.11
02/01/2025 11:08:36 INFO: Verbose logging redirected to /var/log/wazuh-install.log
02/01/2025 11:08:37 WARNING: Hardware and system checks ignored.
02/01/2025 11:08:42 INFO: Wazuh repository added.
02/01/2025 11:08:42 INFO: --- Configuration files ---
02/01/2025 11:08:42 INFO: Generating configuration files.
02/01/2025 11:08:43 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
02/01/2025 11:08:43 INFO: --- Wazuh indexer ---
02/01/2025 11:08:43 INFO: Starting Wazuh indexer installation.
02/01/2025 11:09:17 INFO: Wazuh indexer installation finished.

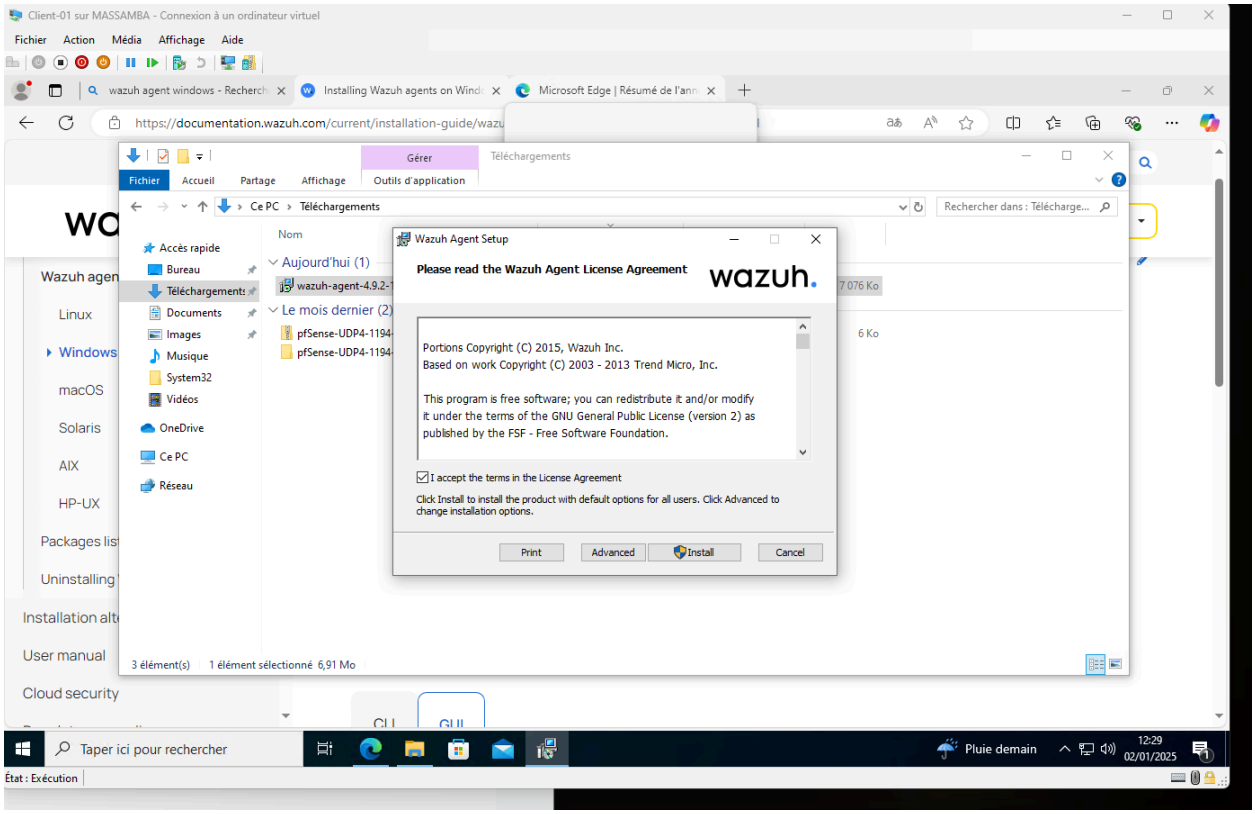
02/01/2025 11:09:17 INFO: Wazuh indexer post-install configuration finished.
02/01/2025 11:09:17 INFO: Starting service wazuh-indexer.
02/01/2025 11:09:28 INFO: wazuh-indexer service started.
02/01/2025 11:09:28 INFO: Initializing Wazuh indexer cluster security settings.
02/01/2025 11:09:34 INFO: Wazuh indexer cluster initialized.
02/01/2025 11:09:34 INFO: --- Wazuh server ---
02/01/2025 11:09:34 INFO: Starting the Wazuh manager installation.
02/01/2025 11:10:07 INFO: Wazuh manager installation finished.
02/01/2025 11:10:07 INFO: Starting service wazuh-manager.
02/01/2025 11:10:23 INFO: wazuh-manager service started.
02/01/2025 11:10:23 INFO: Starting Filebeat installation.
02/01/2025 11:10:27 INFO: Filebeat installation finished.
02/01/2025 11:10:28 INFO: Filebeat post-install configuration finished.
02/01/2025 11:10:28 INFO: Starting service filebeat.
02/01/2025 11:10:29 INFO: filebeat service started.
02/01/2025 11:10:29 INFO: --- Wazuh dashboard ---
02/01/2025 11:10:29 INFO: Starting Wazuh dashboard installation.
02/01/2025 11:11:01 INFO: Wazuh dashboard installation finished.
02/01/2025 11:11:01 INFO: Wazuh dashboard post-install configuration finished.
02/01/2025 11:11:01 INFO: Starting service wazuh-dashboard.
02/01/2025 11:11:01 INFO: wazuh-dashboard service started.
02/01/2025 11:11:29 INFO: Initializing Wazuh dashboard web application.
02/01/2025 11:11:31 INFO: Wazuh dashboard web application initialized.
02/01/2025 11:11:31 INFO: --- Summary ---
02/01/2025 11:11:31 INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: +DfO6V07IDdXwaVIlVS7l.fAgvvL?OtN
02/01/2025 11:11:31 INFO: Installation finished.

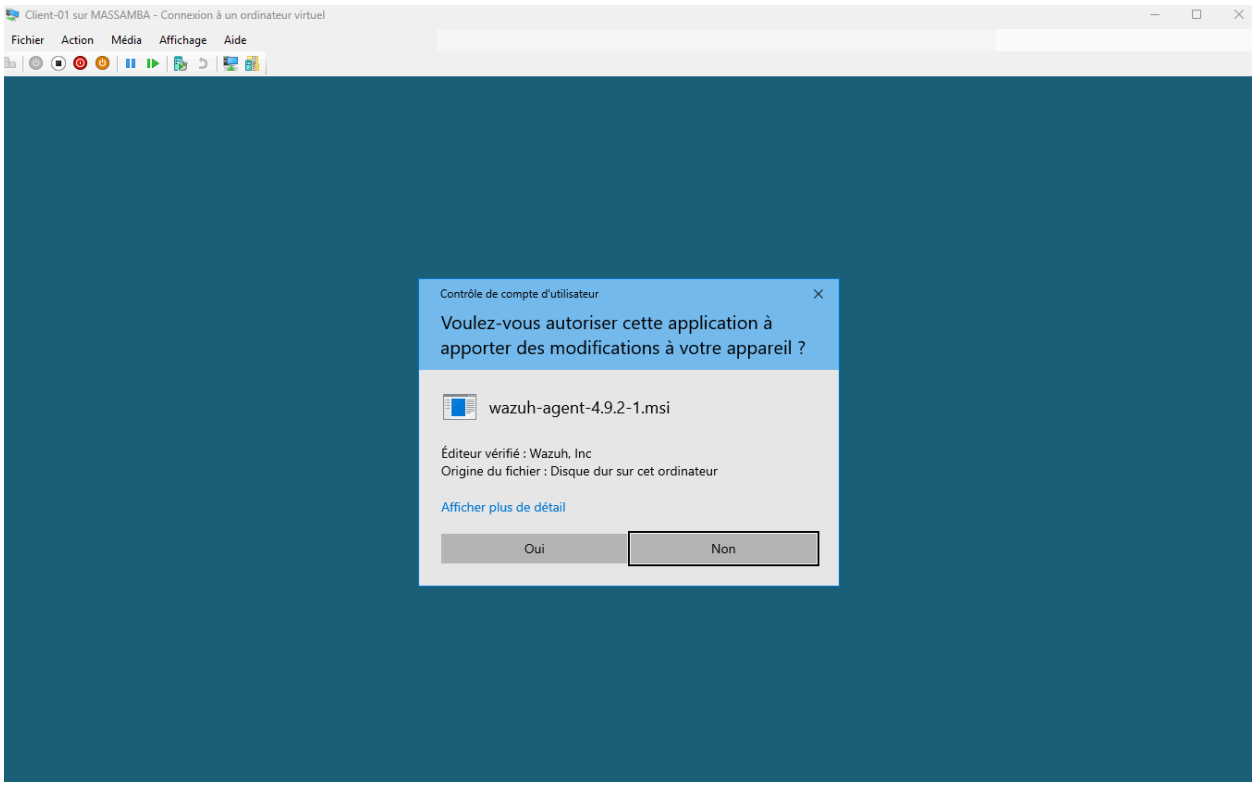

Wazuh
Non sécurisé
https://172.26.40.88/app/login?nextUrl=%2F
wazuh.
The Open Source Security Platform
admin
Log In

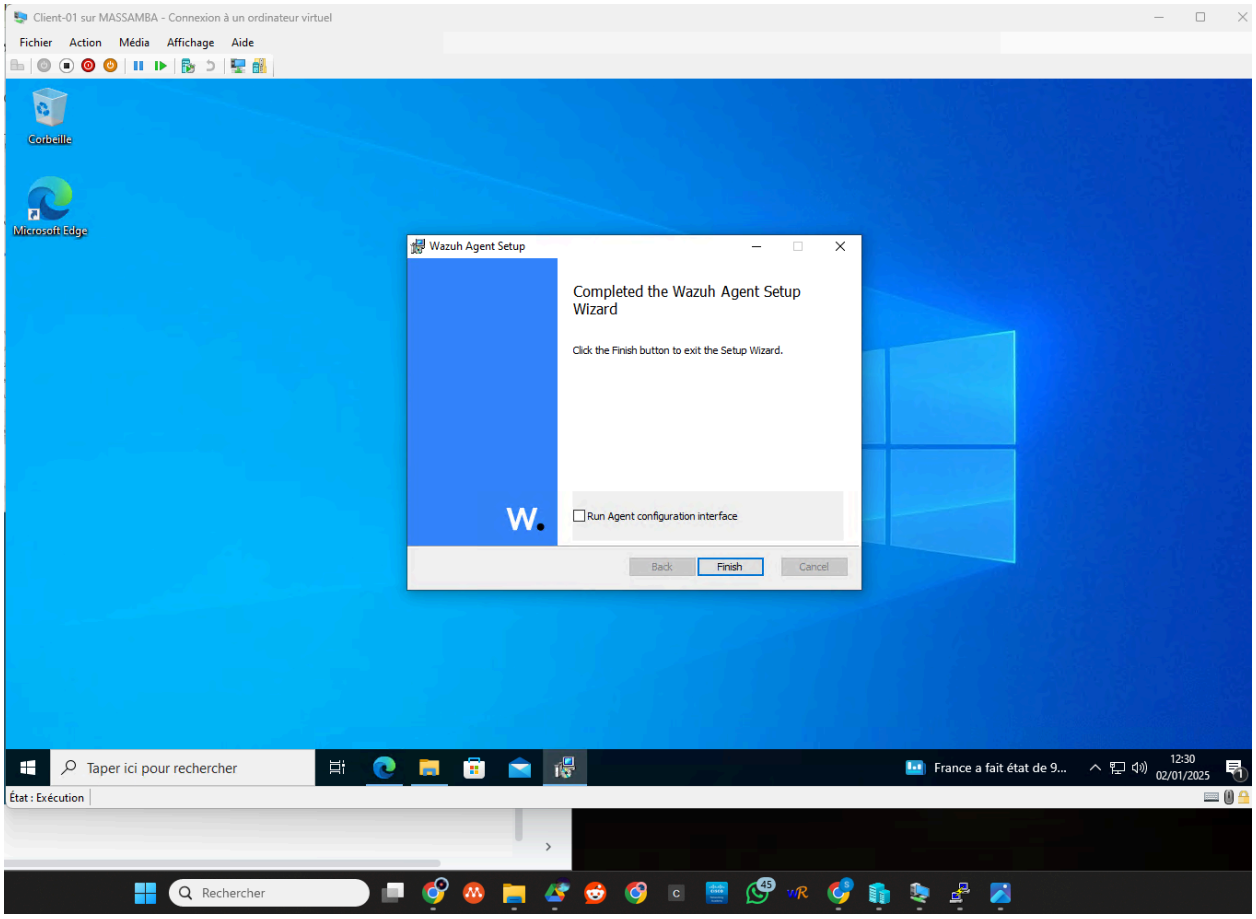


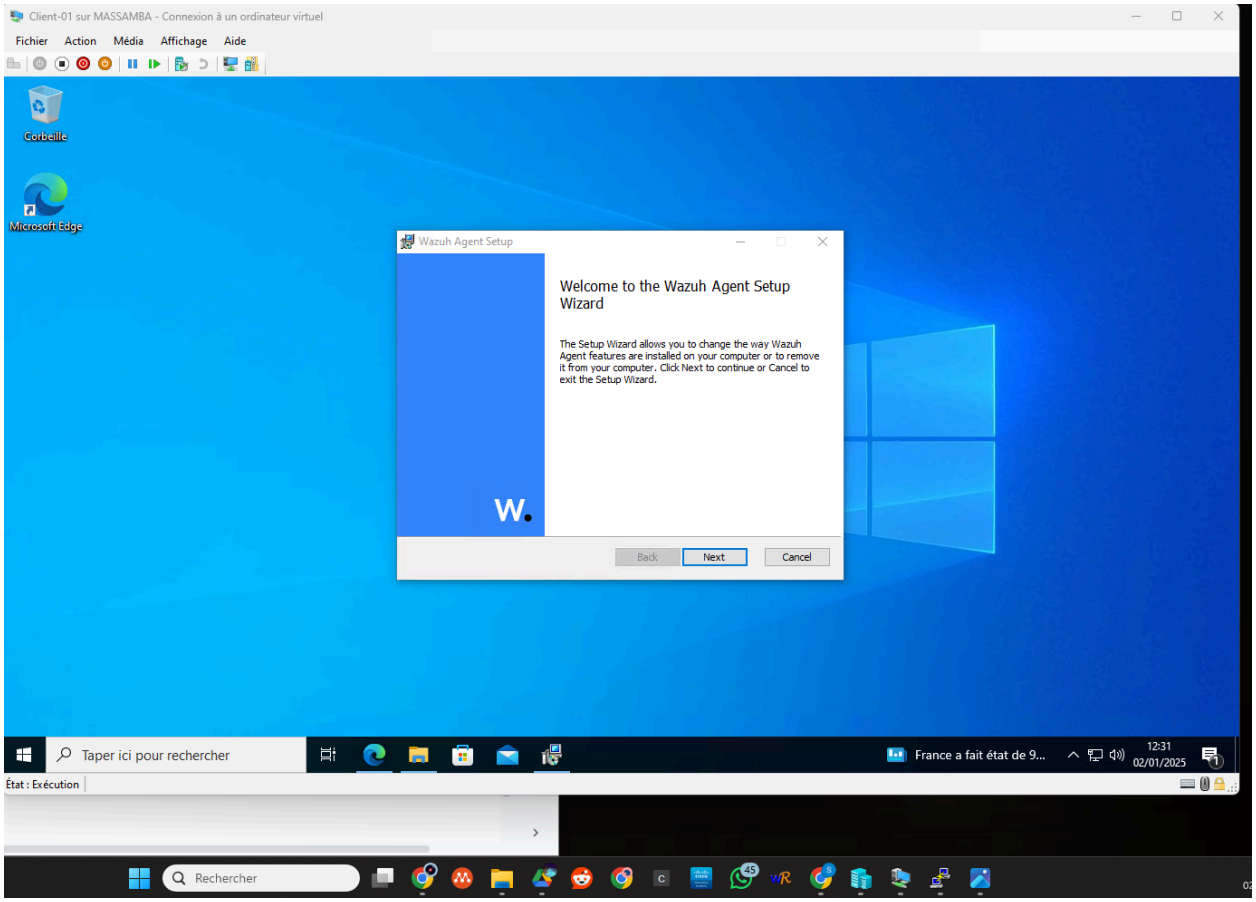
Installation de wazuh agent


Client-01 sur MASSAMBA - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
wazuh agent windows - Recherch
Installing Wazuh agents on Windo
https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html
Community
Contact us
Téléchargements
wazuh-agent-4.9.2-1.msi
Ouvrir un fichier
Afficher plus
wazuh.
Platform
Cloud
Documentation
Services
Partner
Wazuh agent
Linux
Windows
macOS
Solaris
AIX
HP-UX
Packages list
Uninstalling Wazuh
Installation alternatives
User manual
Cloud security
Installation guide / Wazuh agent / Installing Wazuh agents on Windows endpoints
endpoints
The agent runs on the endpoint you want to monitor and communicates with the Wazuh server, sending data in near real-time through an encrypted and authenticated channel. Monitor your Windows systems with Wazuh, from Windows XP to the latest available versions including Windows 11 and Windows Server 2022.
Note To perform the installation, administrator privileges are required.
1. To start the installation process, download the Windows installer.
2. Select the installation method you want to follow: command line interface (CLI) or graphical user interface (GUI).
CLI
GUI
Taper ici pour rechercher
Pluie ce soir
12:28
02/01/2025
État : Exécution
Rechercher


Client-01 sur MASSAMBA - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
Wazuh Agent Setup
Please read the Wazuh Agent License Agreement
wazuh.
Portions Copyright (C) 2015, Wazuh Inc.
Based on work Copyright (C) 2003 - 2013 Trend Micro, Inc.
This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License (version 2) as published by the FSF - Free Software Foundation.
I accept the terms in the License Agreement
Click Install to install the product with default options for all users. Click Advanced to change installation options.
Print
Advanced
Install
Cancel
Taper ici pour rechercher
Pluie demain
12:29
02/01/2025
État : Exécution


Client-01 sur MASSAMBA - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
Contrôle de compte d'utilisateur
Voulez-vous autoriser cette application à apporter des modifications à votre appareil ?
wazuh-agent-4.9.2-1.msi
Éditeur vérifié : Wazuh, Inc
Origine du fichier : Disque dur sur cet ordinateur
Afficher plus de détail
Oui
Non

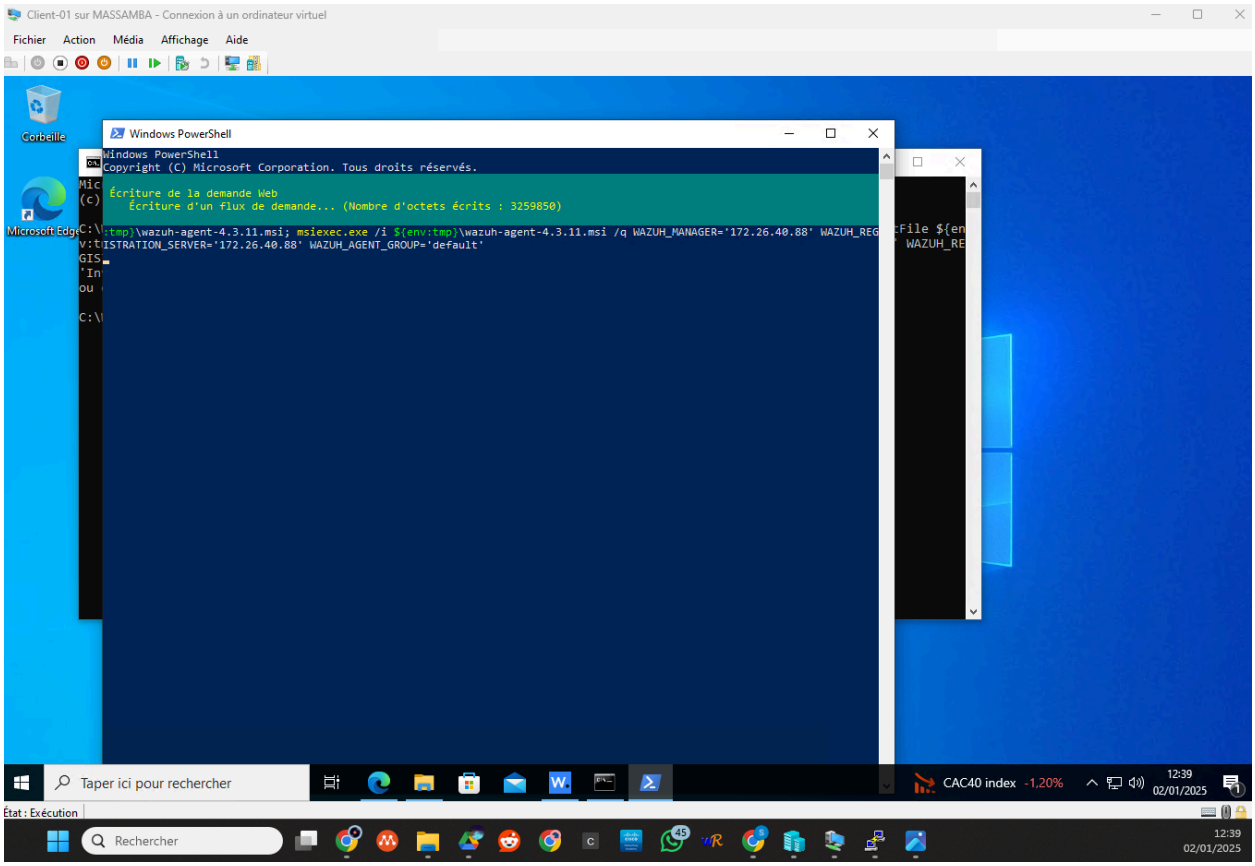

Client-01 sur MASSAMBA - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
Corbeille
Microsoft Edge
Wazuh Agent Setup
Completed the Wazuh Agent Setup Wizard
Click the Finish button to exit the Setup Wizard.
Run Agent configuration interface
Back
Finish
Cancel
Taper ici pour rechercher
France a fait état de 9...
12:30
02/01/2025
État : Exécution
Rechercher

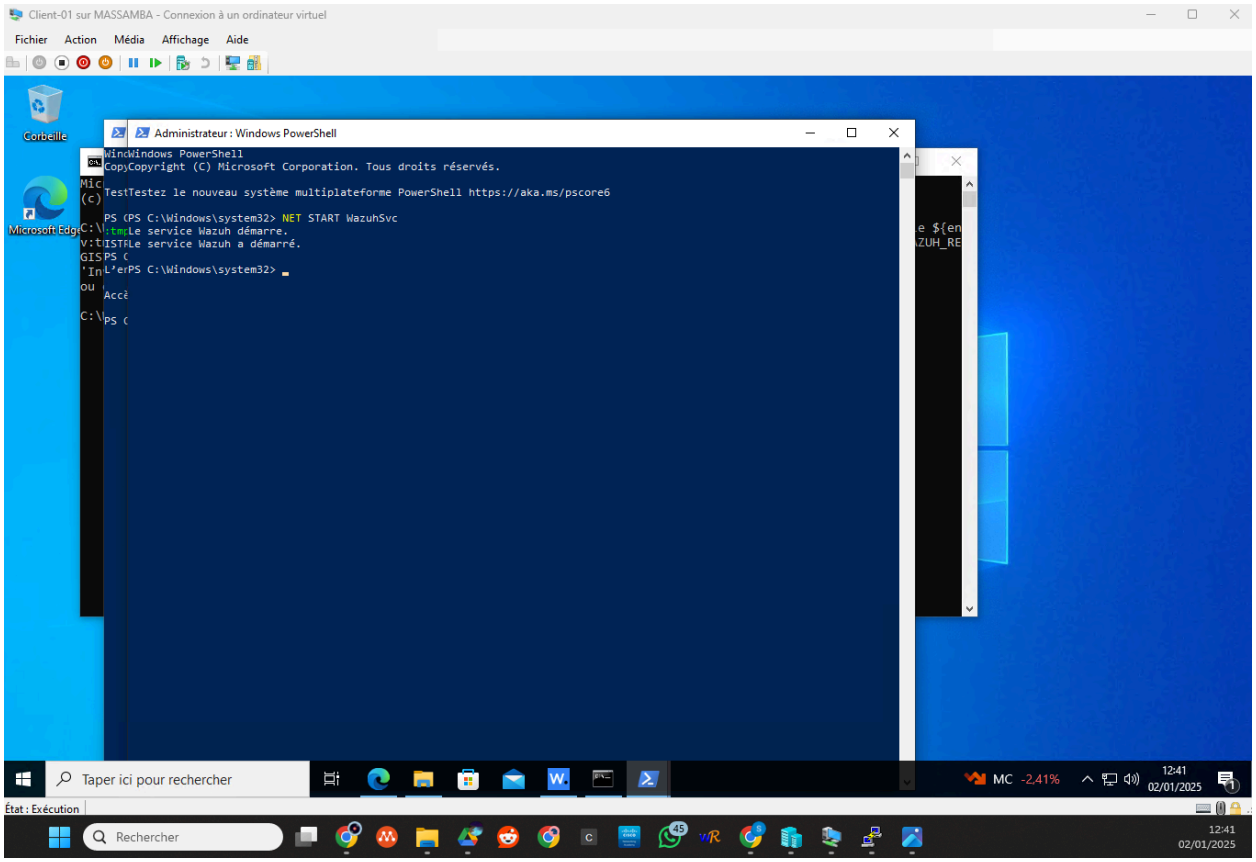


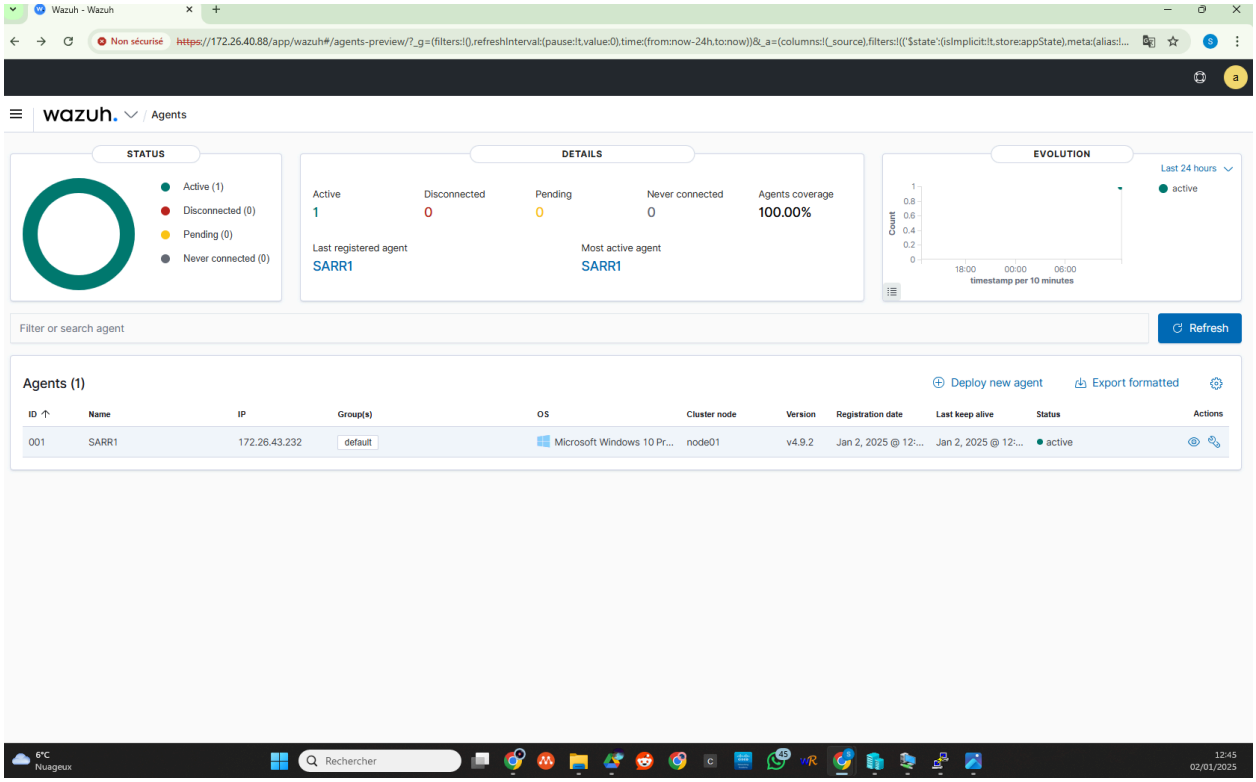
Exécuter les commandes suivantes en powershell sur les clients en admin :

- Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.11-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.11.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.11.msi /q WAZUH_MANAGER='172.26.40.88' WAZUH_REGISTRATION_SERVER='172.26.40.88' WAZUH_AGENT_GROUP='default'

- NET START WazuhSvc


Client-01 sur MASSAMBA - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
Corbeille
Microsoft Edge
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.
Écriture de la demande Web
Écriture d'un flux de demande... (Nombre d'octets écrits : 3259850)
:tmp}\wazuh-agent-4.3.11.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.11.msi /q WAZUH_MANAGER='172.26.40.88' WAZUH_REG
ISTRATION_SERVER='172.26.40.88' WAZUH_AGENT_GROUP='default'
Taper ici pour rechercher
CAC40 index -1.20%
12:39
02/01/2025
État : Exécution
Rechercher
12:39
02/01/2025


Client-01 sur MASSAMBA - Connexion à un ordinateur virtuel
Fichier Action Média Affichage Aide
Corbeille
Microsoft Edge
Administrateur : Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.
Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6
PS C:\Windows\system32> NET START WazuhSvc
Le service Wazuh démarre.
Le service Wazuh a démarré.
PS C:\Windows\system32>
Taper ici pour rechercher
MC -2,41%
12:41
02/01/2025
État : Exécution
Rechercher
12:41
02/01/2025


Wazuh - Wazuh
Non sécurisé
https://172.26.40.88/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(isImplicit:!t,store:appState),meta:(alias:!...
wazuh.
Agents
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
Active
1
Disconnected
0
Pending
0
Never connected
0
Agents coverage
100.00%
Last registered agent
SARR1
Most active agent
SARR1
EVOLUTION
Last 24 hours
active
Count
1
0.8
0.6
0.4
0.2
0
18:00
00:00
06:00
timestamp per 10 minutes
Filter or search agent
Refresh
Agents (1)
Deploy new agent
Export formatted
ID
Name
IP
Group(s)
OS
Cluster node
Version
Registration date
Last keep alive
Status
Actions
001
SARR1
172.26.43.232
default
Microsoft Windows 10 Pr...
node01
v4.9.2
Jan 2, 2025 @ 12:...
Jan 2, 2025 @ 12:...
active
6°C
Nuageux
Rechercher
12:45
02/01/2025