

# Documentation Technique Wazuh

SIEM & Protection Endpoint - Installation et Configuration - Par FB

## 1. Installation du Manager Wazuh

Installation du serveur central via le script automatique :

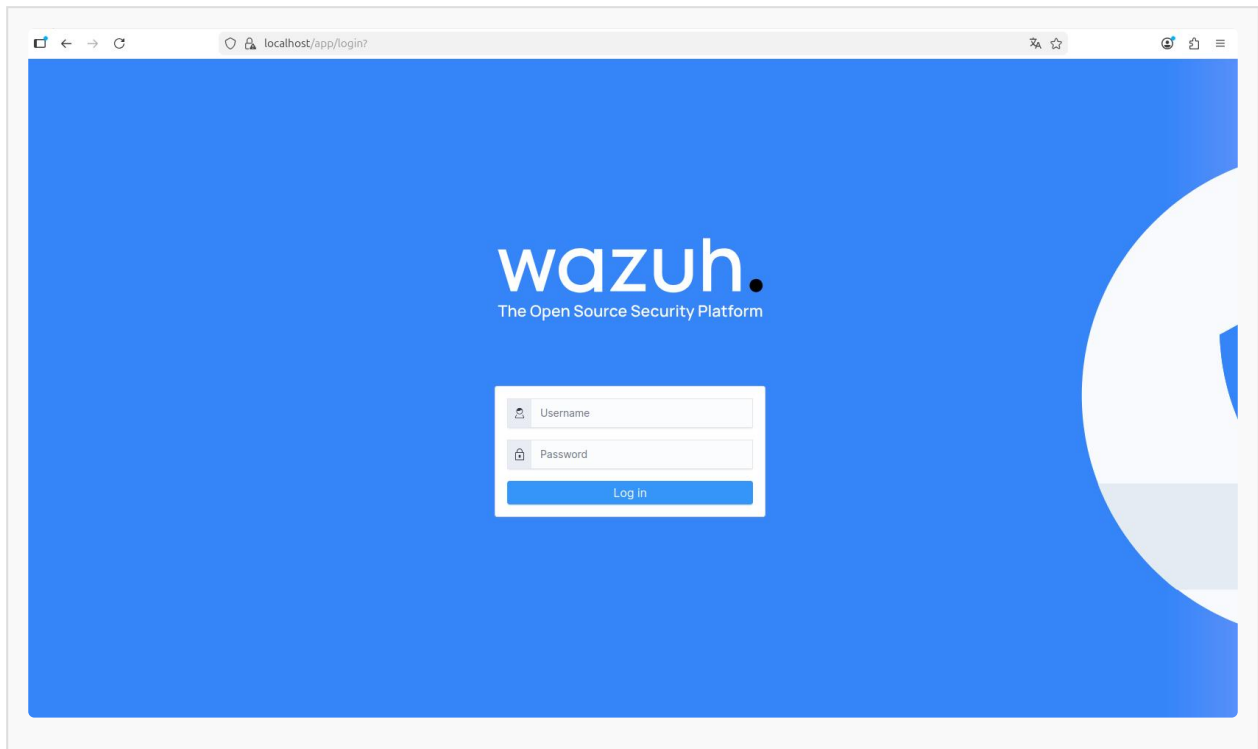
```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
# Forçage de l'installation si version Ubuntu non reconnue (-i)
sudo bash wazuh-install.sh -a -i
```

```
user@user-VMware-Virtual-Platform: $ sudo bash wazuh-install.sh -a -i
21/04/2026 16:51:35 INFO: Starting Wazuh installation assistant. Wazuh version: 4.7.5
21/04/2026 16:51:35 INFO: Verbose logging redirected to /var/log/wazuh-install.log
21/04/2026 16:51:45 WARNING: Hardware and system checks ignored.
21/04/2026 16:51:45 INFO: Wazuh web interface port will be 443.
21/04/2026 16:51:52 INFO: --- Dependencies ---
21/04/2026 16:51:52 INFO: Installing apt-transport-https.
21/04/2026 16:51:59 INFO: Wazuh repository added.
21/04/2026 16:51:59 INFO: --- Configuration files ---
21/04/2026 16:51:59 INFO: Generating configuration files.
21/04/2026 16:52:02 INFO: Created wazuh-install-files.tar. It contains the Wazuh cluster key, certificates, and passwords necessary for installation.
21/04/2026 16:52:02 INFO: --- Wazuh indexer ---
21/04/2026 16:52:02 INFO: Starting Wazuh indexer installation.
21/04/2026 16:53:27 INFO: Wazuh indexer installation finished.
21/04/2026 16:53:28 INFO: Wazuh indexer post-install configuration finished.
21/04/2026 16:53:28 INFO: Starting service wazuh-indexer.
21/04/2026 16:54:30 INFO: wazuh-indexer service started.
21/04/2026 16:54:30 INFO: Initializing Wazuh indexer cluster security settings.
21/04/2026 16:54:43 INFO: Wazuh indexer cluster initialized.
21/04/2026 16:54:43 INFO: --- Wazuh server ---
21/04/2026 16:54:43 INFO: Starting the Wazuh manager installation.
21/04/2026 16:57:25 INFO: Wazuh manager installation finished.
21/04/2026 16:57:25 INFO: Starting service wazuh-manager.
21/04/2026 16:57:45 INFO: wazuh-manager service started.
21/04/2026 16:57:45 INFO: Starting Filebeat installation.
21/04/2026 16:57:57 INFO: Filebeat installation finished.
21/04/2026 16:57:57 INFO: Filebeat post-install configuration finished.
21/04/2026 16:57:57 INFO: Starting service filebeat.
21/04/2026 16:58:00 INFO: filebeat service started.
21/04/2026 16:58:00 INFO: --- Wazuh dashboard ---
21/04/2026 16:58:00 INFO: Starting Wazuh dashboard installation.
21/04/2026 16:59:30 INFO: Wazuh dashboard installation finished.
21/04/2026 16:59:30 INFO: Wazuh dashboard post-install configuration finished.
21/04/2026 16:59:30 INFO: Starting service wazuh-dashboard.
21/04/2026 16:59:32 INFO: wazuh-dashboard service started.
21/04/2026 17:00:20 INFO: Initializing Wazuh dashboard web application.
21/04/2026 17:00:21 INFO: Wazuh dashboard web application initialized.
21/04/2026 17:00:21 INFO: --- Summary ---
21/04/2026 17:00:21 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: e6AyMPcpf5C5S37379vnoIqkDp4.iWB4
21/04/2026 17:00:21 INFO: Installation finished.
```

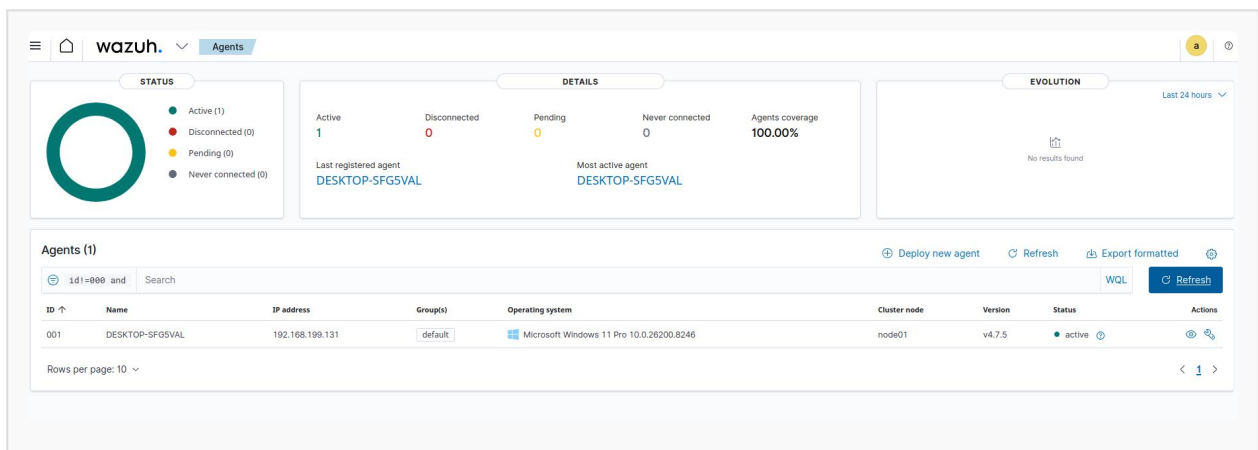
Erreur de vérification système lors de l'installation sur une version récente d'Ubuntu, corrigée avec l'option `-i`.

## 2. Interface Dashboard & Navigation

Accès à la console Web via HTTPS et navigation vers les menus de gestion.



Interface d'accueil Wazuh montrant l'état des agents connectés.



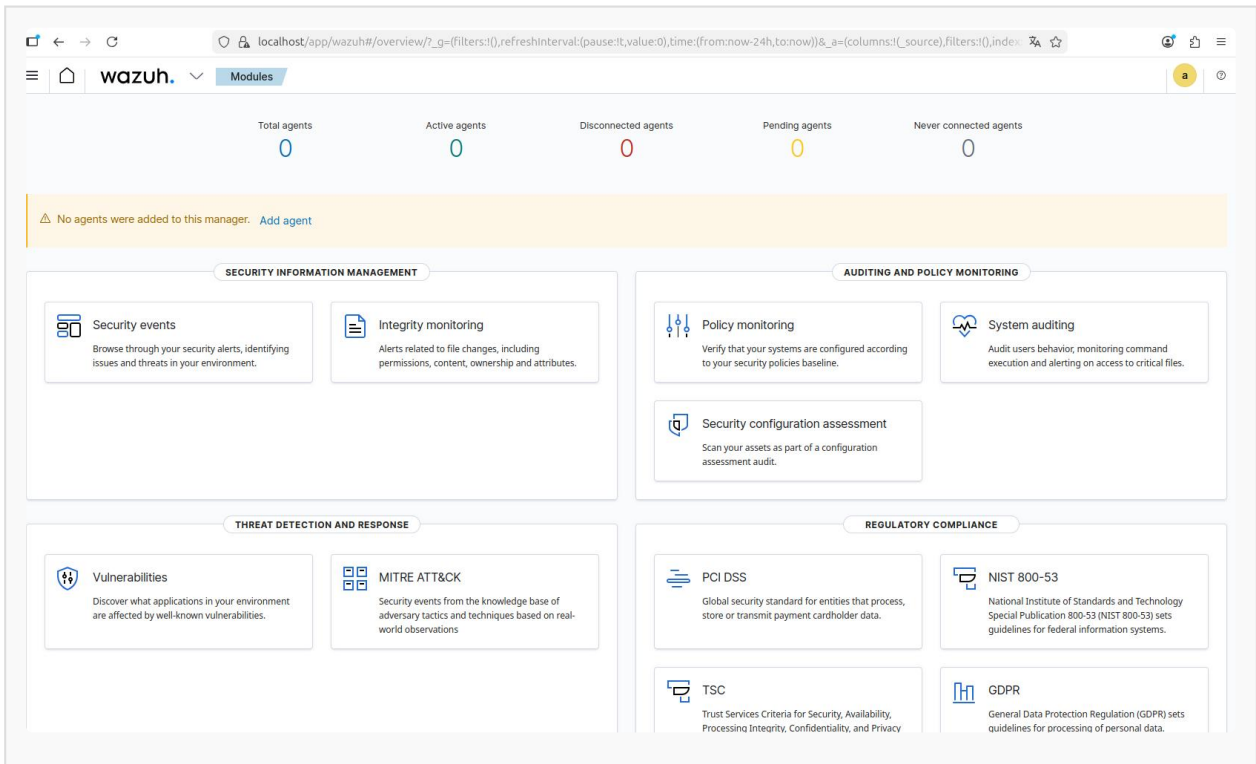
Navigation dans les modules de sécurité et administration du serveur.

### 3. Configuration des Règles Personnalisées

Création d'une règle de détection spécifique pour le dossier Downloads sur le client Windows.

```
# Chemin : Wazuh > Server Management > Rules > Edit local_rules.xml

<group name="windows,syscheck,">
  <rule id="100002" level="12">
    <if_sid>554,550</if_sid>
    <field name="file">Downloads</field>
    <description>ALERTE : Fichier suspect sur Windows !</description>
  </rule>
</group>
```



Menu de gestion des règles permettant d'éditer les fichiers XML de détection.

## 4. Tests et Alerting de Sécurité

Comparaison entre une alerte par défaut (niveau 5) et une alerte critique personnalisée (niveau 12).

Time ↓	Agent	Agent name	Technique(s)	Tactics	Description	Level	Rule ID
Apr 21, 2026 @ 17:30:04.597	001	DESKTOP-SFG5VAL			File added to the system.	5	554

Table	JSON	Rule
@timestamp		2026-04-21T15:30:04.597Z
_id		gPKpsJ0BFSP-VEICxR8B
agent.id		001
agent.ip		192.168.199.131
agent.name		DESKTOP-SFG5VAL
decoder.name		syscheck_new_entry
full_log		File 'c:\users\public\downloads\test_intrusion.txt' added Mode: realtime
id		1776785404.1757936
input.type		log
location		syscheck
manager.name		user-VMware-Virtual-Platform
rule.description		File added to the system.
rule.firedtimes		3
rule.gdpr		IL5.1.f
rule.gpg13		4.11
rule.groups		ossec, syscheck, syscheck_entry_added, syscheck_file
rule.hipaa		164.312.c.1, 164.312.c.2
rule.id		554
rule.level		5
rule.mail		false
rule.nist_800_53		SI.7
rule.pci_dss		11.5

Détection initiale : l'ajout d'un fichier est vu comme une alerte mineure de niveau 5.

Time ↓	Agent	Agent name	Technique(s)	Tactics	Description	Level	Rule ID
Apr 21, 2026 @ 17:38:53.898	001	DESKTOP-SFG5VAL			ALERTE CRITIQUE : Fichier suspect détecté dans les téléchargements Windows I	12	100002

Table	JSON	Rule
@timestamp		2026-04-21T15:38:53.898Z
_id		DPKxsJ0BFSP-VEIC1RFc
agent.id		001
agent.ip		192.168.199.131
agent.name		DESKTOP-SFG5VAL
decoder.name		syscheck_new_entry
full_log		File 'c:\users\public\downloads\test_intrusions.txt' added Mode: realtime
id		1776785933.1855428
input.type		log
location		syscheck
manager.name		user-VMware-Virtual-Platform
rule.description		ALERTE CRITIQUE : Fichier suspect détecté dans les téléchargements Windows I
rule.firedtimes		2
rule.groups		windows, syscheck
rule.id		100002
rule.level		12
rule.mail		true
syscheck.attrs_after		ARCHIVE
syscheck.event		added
syscheck.md5_after		d41d8cd98f00b204e9800998ecf8427e
syscheck.mode		realtime
syscheck.mtime_after		2026-04-21T17:38:50
syscheck.path		c:\users\public\downloads\test_intrusions.txt

Test final réussi : Application de la règle 100002. L'alerte remonte en niveau 12 (rouge) avec la description personnalisée.