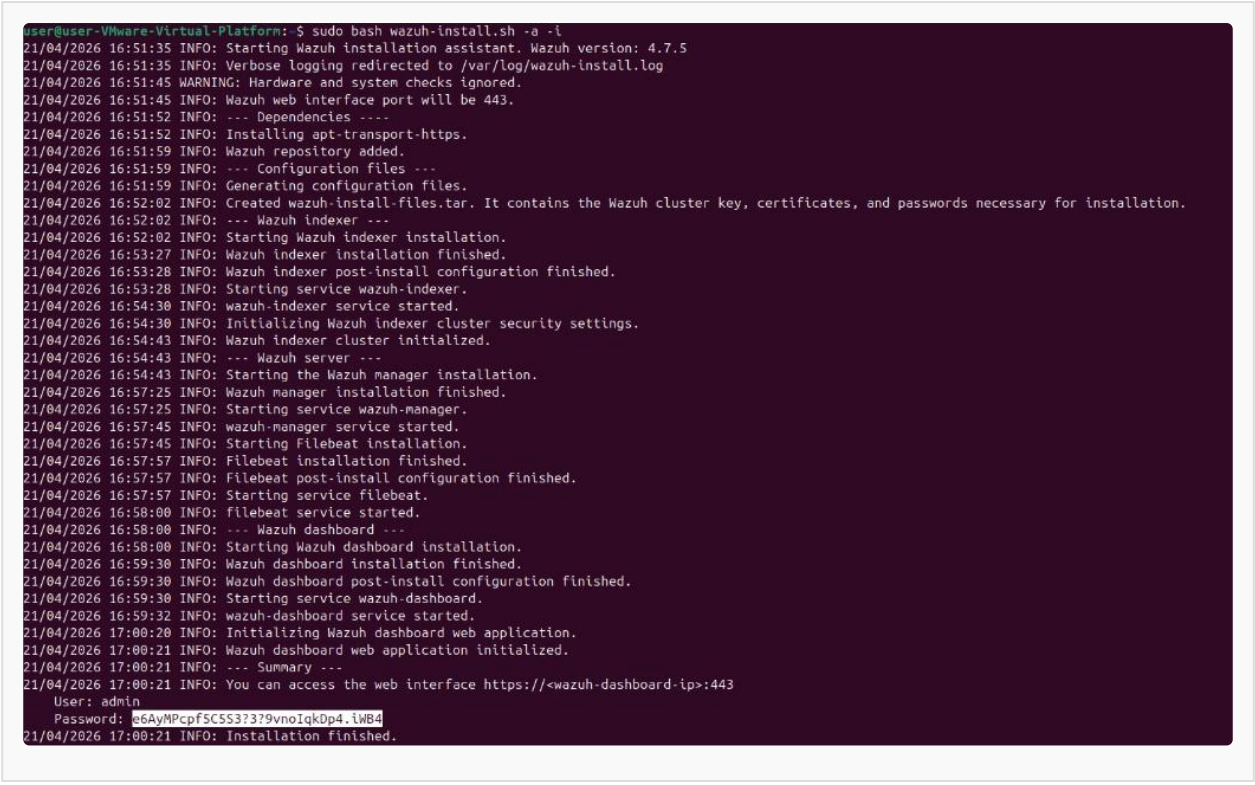
Documentation Technique Wazuh

SIEM & Protection Endpoint - Installation et Configuration - Par FB

1. Installation du Manager Wazuh

Installation du serveur central via le script automatique :

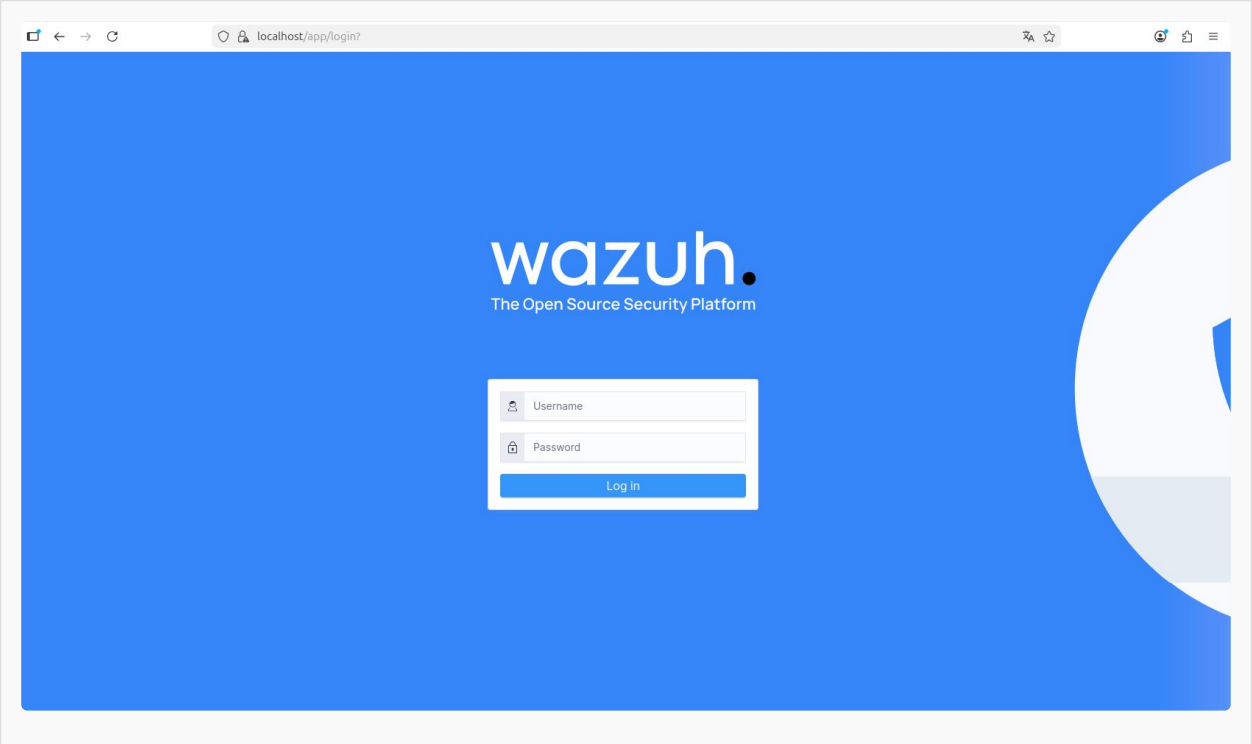
```
curl -sO https://packages.wazuh.com/4.7/wazuh-install.sh
# Forçage de l'installation si version Ubuntu non reconnue (-i)
sudo bash wazuh-install.sh -a -i
```



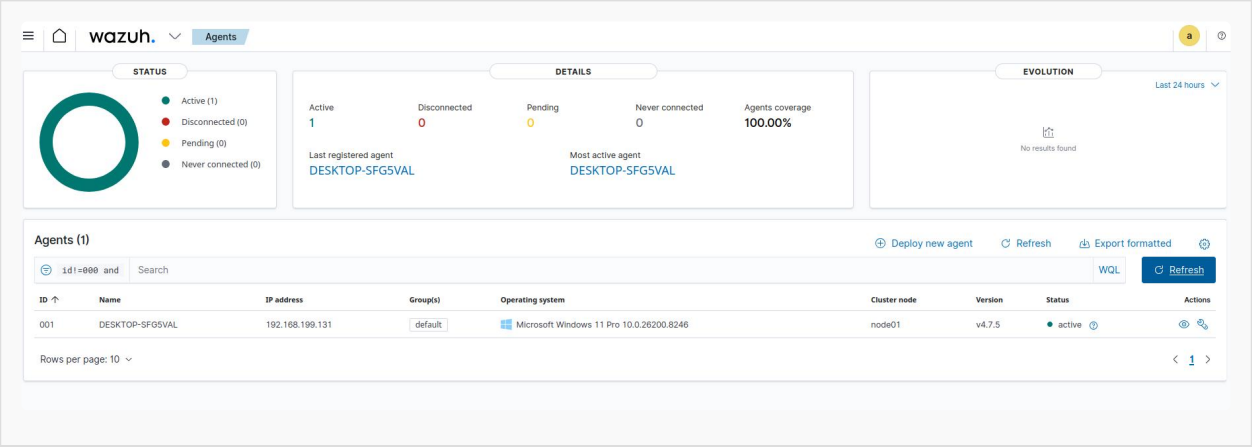
> Erreur de vérification système lors de l'installation sur une version récente d'Ubuntu, corrigée avec l'option `-i`.

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.

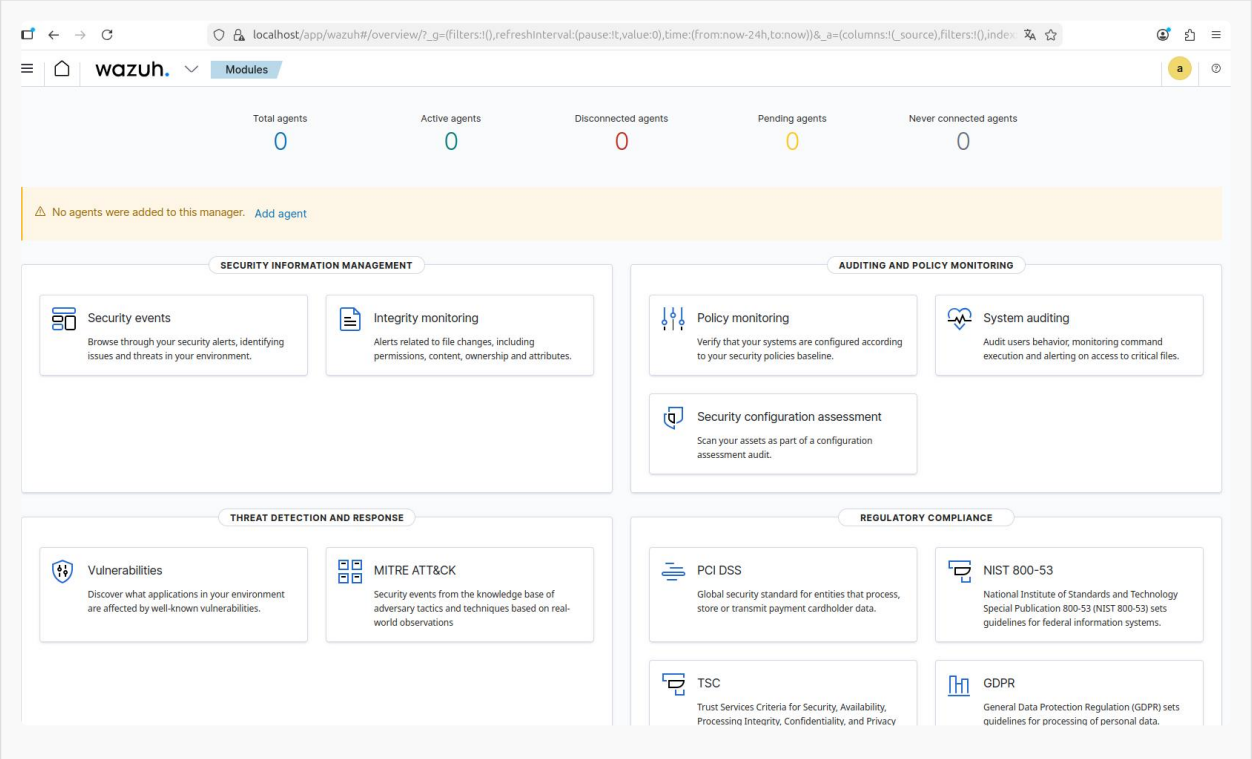


Navigation dans les modules de sécurité et administration du serveur.

3. Configuration des Règles Personnalisées

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

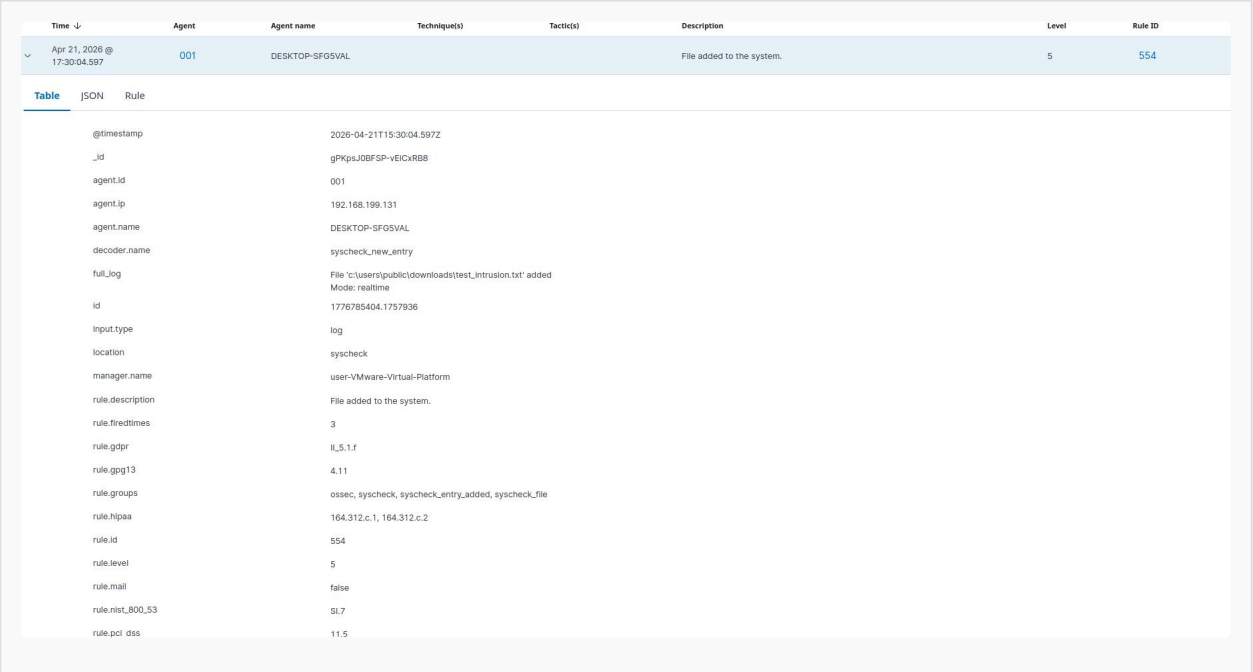
```
# Chemin : Wazuh > Server Management > Rules > Edit local_rules.xml

<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).

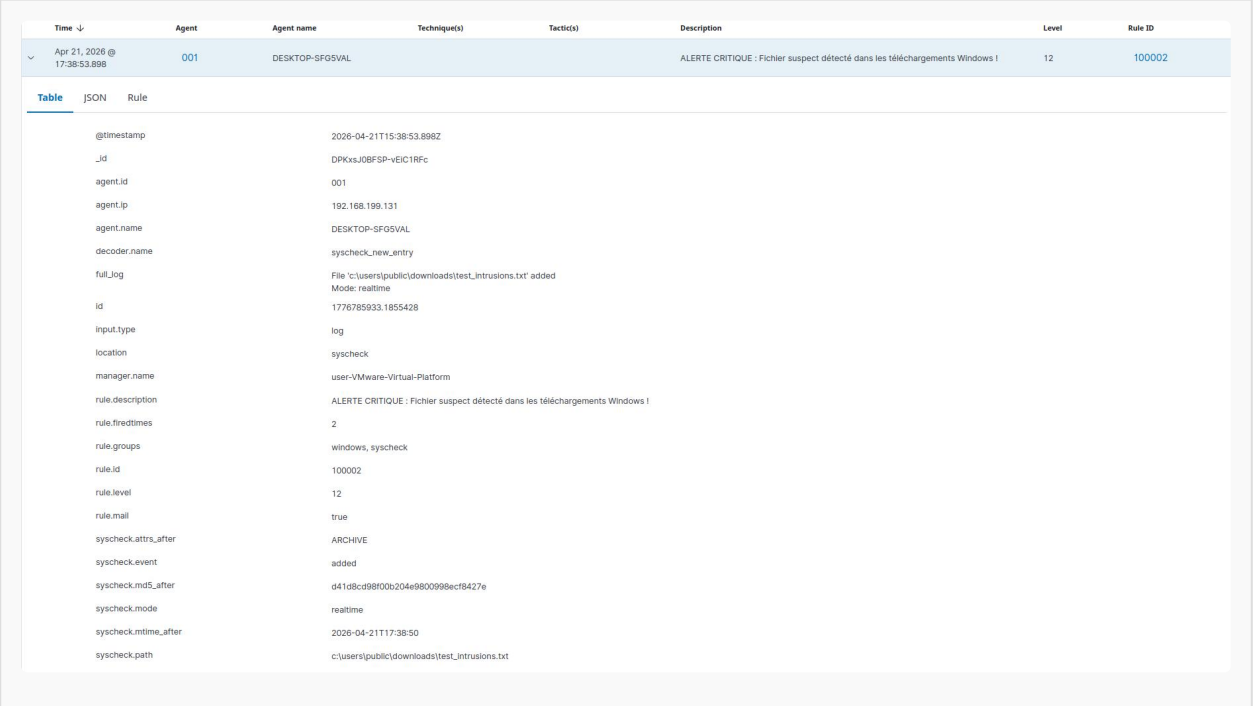


Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 21, 2026 @ 17:30:04.597	001	DESKTOP-SFGSVAL			File added to the system.	5	554

Table JSON Rule

@timestamp	2026-04-21T15:30:04.597Z
_id	gPKpsJ0BFSP-vEiCxRB8
agent.id	001
agent.ip	192.168.199.131
agent.name	DESKTOP-SFGSVAL
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	II_5.1.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)	Tactic(s)	Description	Level	Rule ID
Apr 21, 2026 @ 17:38:53.898	001	DESKTOP-SFGSVAL			ALERTE CRITIQUE : Fichier suspect détecté dans les téléchargements Windows !	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-SFGSVAL
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 !
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.