

Wazuh

Last updated by | Leslie Lemaire | 24 juin 2025 at 16:48 UTC+2

Intégration Fail2ban - Wazuh

Objectif

Mettre en place une surveillance des IP bannies par Fail2ban dans le SIEM Wazuh.
Cette procédure permet de :

- Capturer les bannissements d'IP par Fail2ban.
- Remonter ces événements dans le Dashboard Wazuh.
- Avoir une visibilité centralisée des tentatives d'attaques SSH.

Prérequis

- Agent Wazuh installé et connecté au Manager.
- Fail2ban installé et une jail `sshd` active.

Configuration sur chaque machine Wazuh + Fail2ban

1. Ajouter les fichiers log à surveiller

Editer le fichier `/var/ossec/etc/ossec.conf` :

```
sudo nano /var/ossec/etc/ossec.conf
```



Ajouter avant `</ossec_config>` :

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>

<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/fail2ban.log</location>
</localfile>
```



2. Ajouter la règle personnalisée

Editer `/var/ossec/etc/local_rules.xml` :

```
sudo nano /var/ossec/etc/local_rules.xml
```



Ajouter :

```
<ruleset>
  <group name="fail2ban,">
    <rule id="100101" level="10">
      <description>Fail2Ban - IP banned (regex capture)</description>
      <match>fail2ban: Ban </match>
      <regex>fail2ban: Ban ([0-9]+\.[0-9]+\.[0-9]+\.[0-9]+)</regex>
      <group>authentication_failures,</group>
    </rule>
  </group>
</ruleset>
```



3. Redémarrer l'agent Wazuh

```
sudo systemctl restart wazuh-agent
```



Tests de vérification

1. Test rapide (validation de la règle)

Injecter une fausse ligne dans `/var/log/fail2ban.log` :

```
echo "$(date '+%Y-%m-%d %H:%M:%S') fail2ban-server[9999]: Ban 1.2.3.4" | sudo tee -a /var/log/fail2ban.log
```



Surveiller `/var/ossec/logs/ossec.log` :

```
sudo tail -n 50 /var/ossec/logs/ossec.log
```



Vous devez voir :

```
Rule 100101 fired (Fail2Ban - IP banned (regex capture))
```



2. Test complet (attaque brute force SSH)

a) Vérifier la jail

```
sudo fail2ban-client status sshd
```



b) Provoquer l'attaque

Depuis une autre machine ou la même :

```
ssh userbidon@ip_du_serveur
```



Répéter des tentatives de mauvais mot de passe.

c) Vérifier le bannissement



```
sudo fail2ban-client status sshd
```

d) Vérifier dans Wazuh

Dans Discover :

- Search : Fail2Ban
- OU : data.alert.rule.id: 100101
- Time range : Last 7 days

Vous devez voir l'événement apparaître.

Notes

- Le test rapide permet de valider la règle.
- Pour que l'événement apparaisse dans Discover, il faut un log réel Fail2ban (`fail2ban-server[xxxx]: Ban ...`).
- En cas de besoin, vérifier `logtarget` dans `/etc/fail2ban/fail2ban.conf` .

Conclusion

Cette procédure est à reproduire sur chaque machine Wazuh + Fail2ban du projet.
Elle permet de démontrer la maîtrise des concepts suivants :

- Supervision des bannissements Fail2ban
- Ecriture de règles personnalisées Wazuh
- Intégration avec le SIEM
- Présentation des résultats dans Discover.