25/04/2024

Wazuh
Le super-héros de la sécurité

UNIVERSITÉ TOULOUSE III PAUL SABATIER
Université Fédérale Toulouse Midi-Pyrénées

“

wAZUH !!

Qu’est ce que Wazuh ?

- Un SIEM et un XDR – Opensources (GPL et Apache Licence v2)
  - Détection d’incidents et réponses

  - Worker : traitement initial, filtres, agrégation de données.
  - Manager : Cohérence du cluster, groupes, agents, règles, décodeurs, CDB
  - Indexer : Fork Opensearch
  - Dashboard : Fork Opensearch Dashboard

Qu’est ce que Wazuh ?

- Dépends du nombre d’alertes

	Indexer	Manager/worker
RAM	16GB	4GB
CPU	8	8
Espace disque 90j		
1 server : 0,25 APS*	3,7	0,1
1 poste de travail : 0,1 APS*	1,5	0,04
1 équipement réseau : 0,5 APS*	7,4	0,2

*APS = Alerte par seconde

Qu’est ce que Wazuh ?

- Des agents
  - Collectent l’information
    - Collecteur de logs
    - Collecteur de résultats de commandes
    - Contrôle d’intégrité de fichiers
    - Security Configuration Assessment (Evaluation des configurations)
    - Malware détection
    - Inventaire (applications, processus)

    - Surveillance de conteneur docker
    - Surveillance d’infrastructure Cloud.

Linux
MacOS
Windows

Non testé

“

Installation

Installation

- Docker
  - Docker-compose fourni pour chaque élément
- Ansible
  - Pour docker
  - Pour serveurs
- Installation d’un Agent
  - Dépend de plusieurs modules (audit, rsyslog, etc.)
  - Difficultés automatisation de la configuration : pas XML Standard

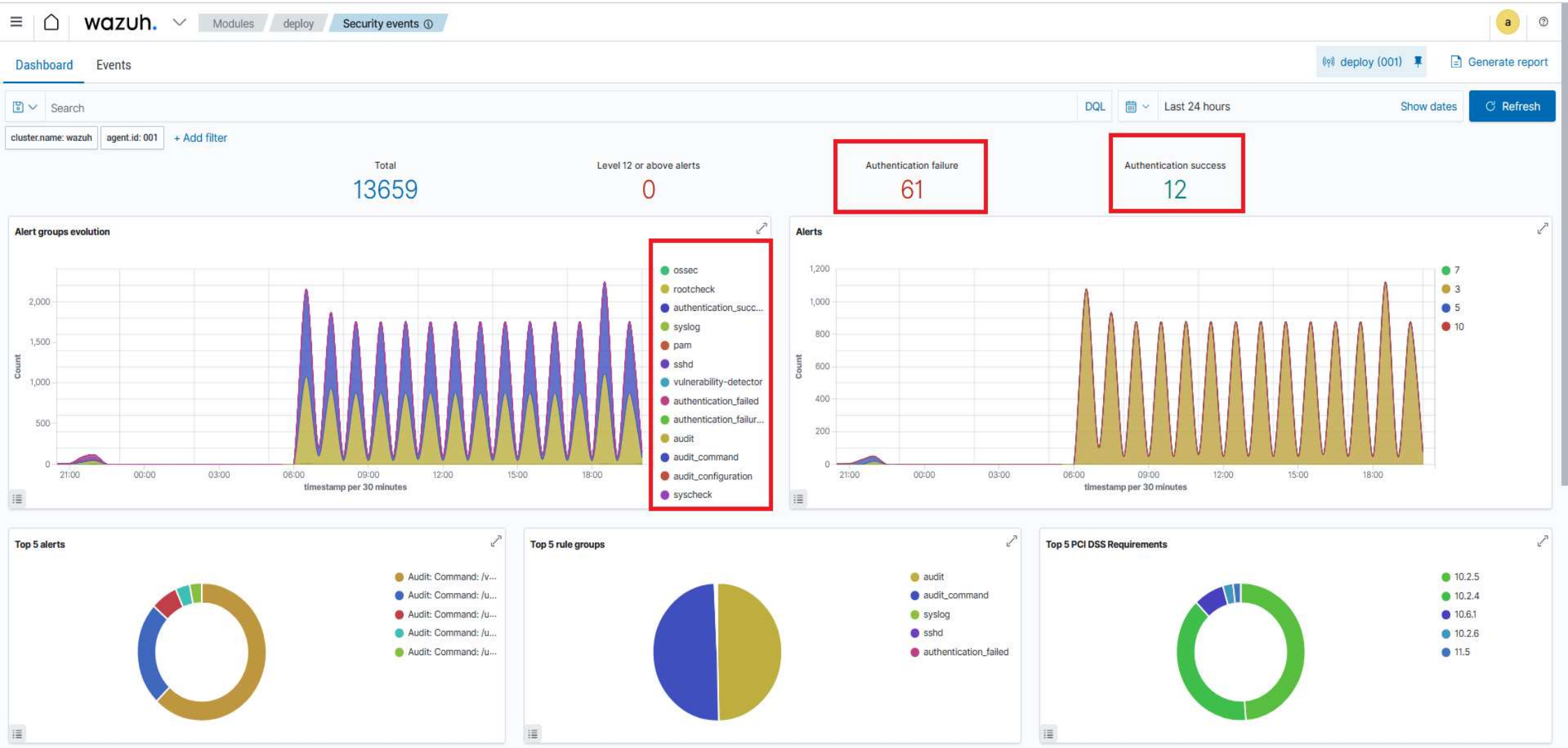
“

Security events

Security events

- Tous les évènements de sécurité de tous les modules
  - Définition d’un niveau.
    - 1 à 16 : niveau de risque
    - 0 : Ignorer un risque (faux-positif, sans intérêt, etc.)
  - Decoders (Reconnaitre et parser les logs)
    - Embarqués ou personnalisés
  - Rules (Déclencher une alerte)
    - Embarquées ou personnalisées

Security events



Security events

- Analyse de logs par défaut
  - Auditd
  - Auth.log
  - Syslog
  - …

- Analyse de logs personnalisable
  - Avec un decoder et des règles

Security events

- Exemple de Decoder

```
<decoder name="zimbra">
  <prematch>ua=Zimbra</prematch>
</decoder>

<decoder name="zimbra">
  <parent>zimbra</parent>
  <regex>^(\d+.\d+.\d+.\d+)\(\.+cmd=(\.+);\.+account=(\.+);\.+protocol=(\.+);\.+error=(\.+);</regex>
  <order>monip,action,account,protocol,error</order>
</decoder>
```

Pour info

192.168.2.45(nginx/1.24.0);ua=Zimbra/9.0.0_ZEXTRAS_9039;cid=21256;] security - cmd=Auth; account=cedric.chambault@univ-tlse3.fr; protocol=imap; error=authentication failed for [cedric.chambault@univ-tlse3.fr], missing userPassword;

Security events

- Exemple de règles

```
<group name="zimbra">
 <rule id="100002" level="7">
    <decoded_as>zimbra</decoded_as>
    <field name="account">cedric.chambault@univ-tlse3.fr</field>
    <description>Connexion administrateur</description>
 </rule>
</group>

<group name="zimbra_audit,">
 <rule id="100003" level="12">
    <if_sid>100002</if_sid>
    <decoded_as>zimbra</decoded_as>
    <match>authentication failed</match>
    <description>Echec non autorisé pour un administrateur</description>
 </rule>
</group>
```

Security events

- Outils d’aide à la personnalisation
  - /var/ossec/bin/wazuh-logtest

```
192.168.2.45(nginx/1.24.0);ua=Zimbra/9.0.0_ZEXTRAS_9039;cid=21256;] security - cmd=Auth; account=cedric.chambault@univ-tlse3.fr; protocol=imap; error=authentication failed for [cedric.chambault@univ-tlse3.fr], missing userPassword;

**Phase 1: Completed pre-decoding.
        full event: '192.168.2.45(nginx/1.24.0);ua=Zimbra/9.0.0_ZEXTRAS_9039;cid=21256;] security - cmd=Auth; account=cedric.chambault@univ-tlse3.fr; protocol=imap; error=authentication failed for [cedric.chambault@univ-tlse3.fr], missing userPassword;'

**Phase 2: Completed decoding.
        name: 'zimbra'
        account: 'cedric.chambault@univ-tlse3.fr'
        action: 'Auth'
        error: 'authentication failed for [cedric.chambault@univ-tlse3.fr], missing userPassword'
        monip: '192.168.2.45'
        protocol: 'imap'

**Phase 3: Completed filtering (rules).
        id: '100003'
        level: '12'
        description: 'Echec non autorised pour un administrateur'
        groups: '['zimbra_audit']'
        firedtimes: '1'
        mail: 'True'
**Alert to be generated.
```

“

Malware Detection

Malware Detection

- Bases de données de rootkit et trojans
  - /var/ossec/etc/shared/rootkit_files.txt
  - /var/ossec/etc/shared/rootkit_trojans.txt
  - /var/ossec/etc/shared/win_malware_rcl.txt

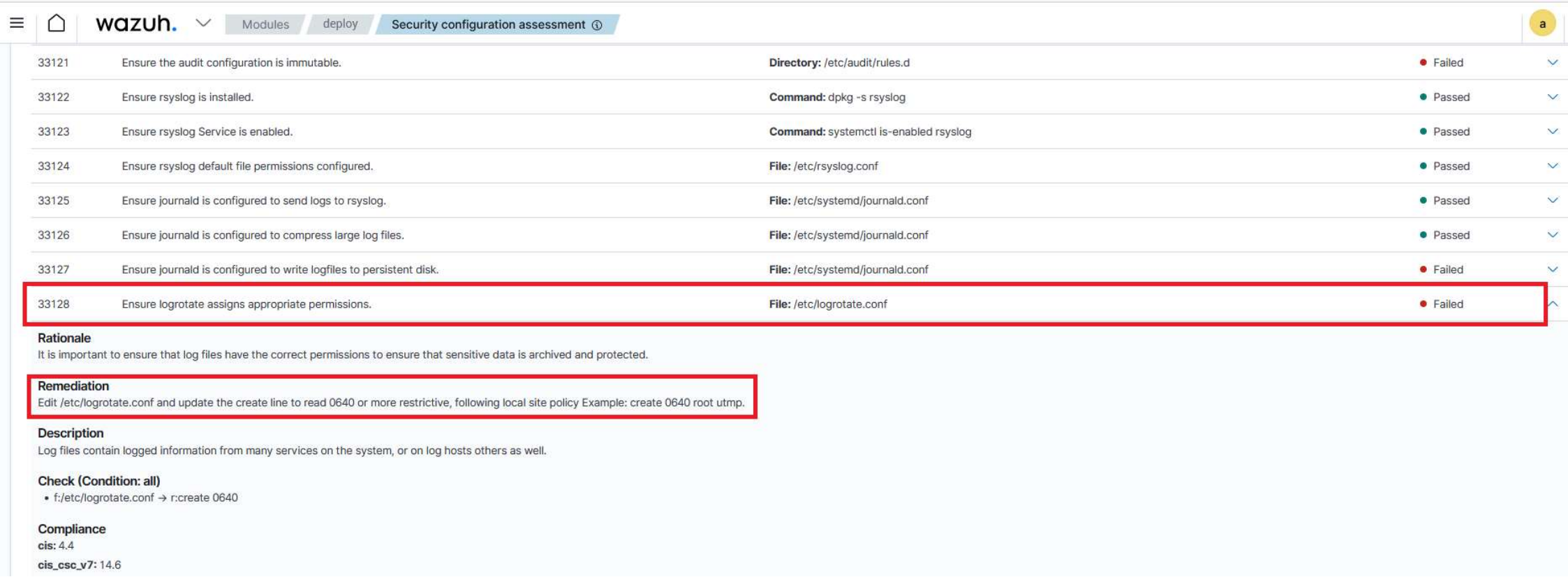
- Analyse
  - Processus cachés
  - Droits inhabituels (suid, write pour other mais owner root, etc.)

SCA
Evaluation des configurations

Security Configuration Assessment

- Un ensemble de normes prédéfinies
  - CIS Benchmark, RGPD, HIPAA (santé), PCI DSS (Finance), NIST 800-53 et TSC (Cybersécurité)

Mesurer l’écart entre nos pratiques et les bonnes pratiques reconnues.


wazuh.
Modules
deploy
Security configuration assessment
a
33121 Ensure the audit configuration is immutable. Directory: /etc/audit/rules.d Failed
33122 Ensure rsyslog is installed. Command: dpkg -s rsyslog Passed
33123 Ensure rsyslog Service is enabled. Command: systemctl is-enabled rsyslog Passed
33124 Ensure rsyslog default file permissions configured. File: /etc/rsyslog.conf Passed
33125 Ensure journald is configured to send logs to rsyslog. File: /etc/systemd/journald.conf Passed
33126 Ensure journald is configured to compress large log files. File: /etc/systemd/journald.conf Passed
33127 Ensure journald is configured to write logfiles to persistent disk. File: /etc/systemd/journald.conf Failed
33128 Ensure logrotate assigns appropriate permissions. File: /etc/logrotate.conf Failed
Rationale
It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.
Remediation
Edit /etc/logrotate.conf and update the create line to read 0640 or more restrictive, following local site policy Example: create 0640 root utmp.
Description
Log files contain logged information from many services on the system, or on log hosts others as well.
Check (Condition: all)
f:/etc/logrotate.conf → r:create 0640
Compliance
cis: 4.4
cis_csc_v7: 14.6

27/03/2024

Security Configuration Assessment

- Personnalisation : définition de nos propres normes
  - Existence de fichiers
  - Droits
  - Hash
  - …

  Peut utiliser n’importe shell qui renvoie une valeur interprétable en regex

  c:[commande] -> r:^regex$

Security Configuration Assessment

- Format d’un élément

checks:

START ANSIBLE MANAGED BLOCK FOR UT3 NTP COMPLIANCE

- id: 1

***title**: "Role de conformité - config_ntp"*

***description**: "Rôle nécessaire à la conformité UT3 et configurant le NTP"*

***rationale**: "Utiliser les NTPs d'Angers garantie la cohérence du temps au sein de l'infrastructure"*

***remediation**: "Utilisation : ansible-playbook pb_single_roles.yml -i 192.168.1.41, --tags ntp"*

compliance:

- ut3: ["Rule:Infra:1"]

condition: all

***rules**:*

- 'f:/etc/ntpsec/ntp.conf'

- 'f:/etc/default/ntpsec'

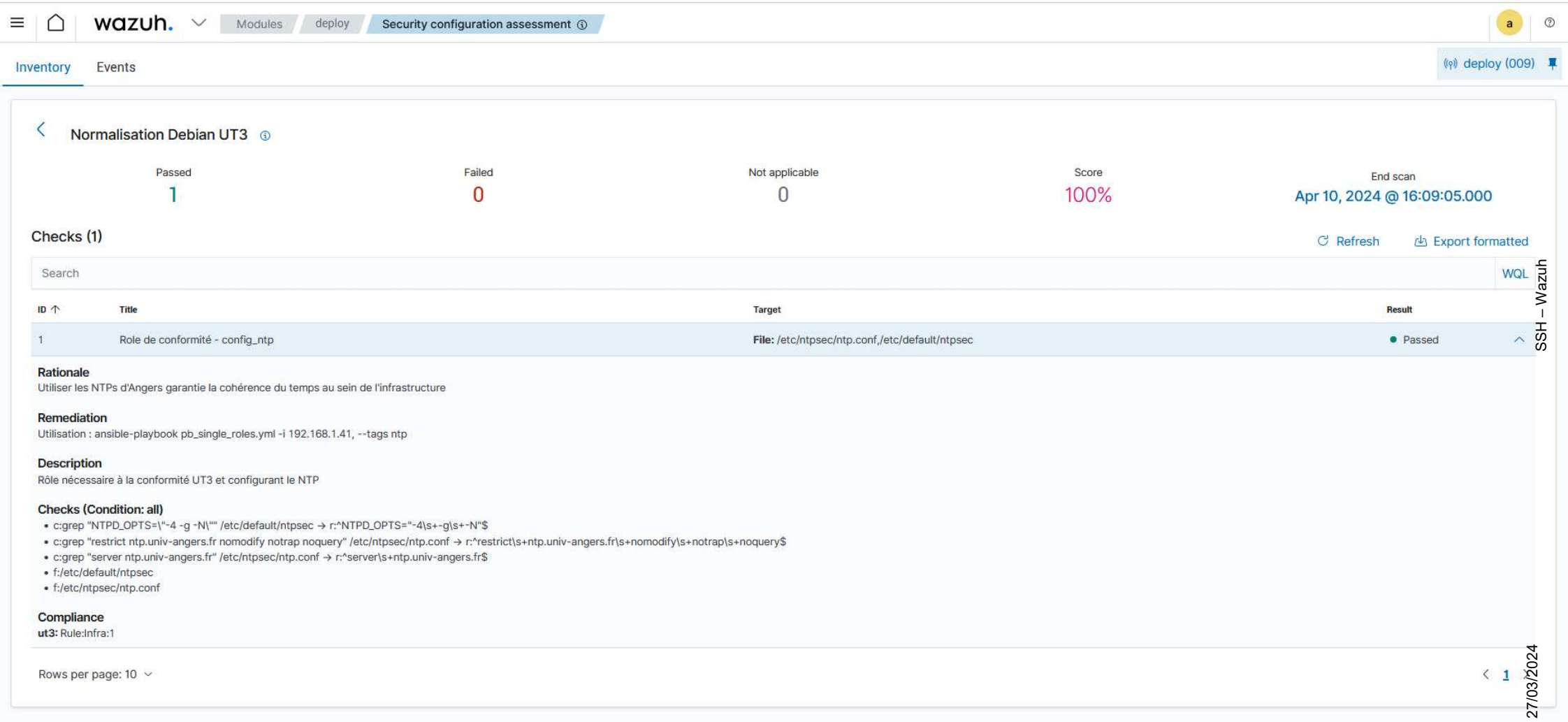
- c:grep "server ntp.univ-angers.fr" /etc/ntpsec/ntp.conf -> r:^server\s+ntp.univ-angers.fr$

- c:grep "restrict ntp.univ-angers.fr nomodify notrap noquery" /etc/ntpsec/ntp.conf -> r:^restrict\s+ntp.univ-angers.fr\s+nomodify\s+notrap\s+noquery$

- c:grep "NTPD_OPTS=\"-4 -g -N\"" /etc/default/ntpsec -> r:^NTPD_OPTS="-4\s+-g\s+-N"$

END ANSIBLE MANAGED BLOCK FOR UT3 NTP COMPLIANCE

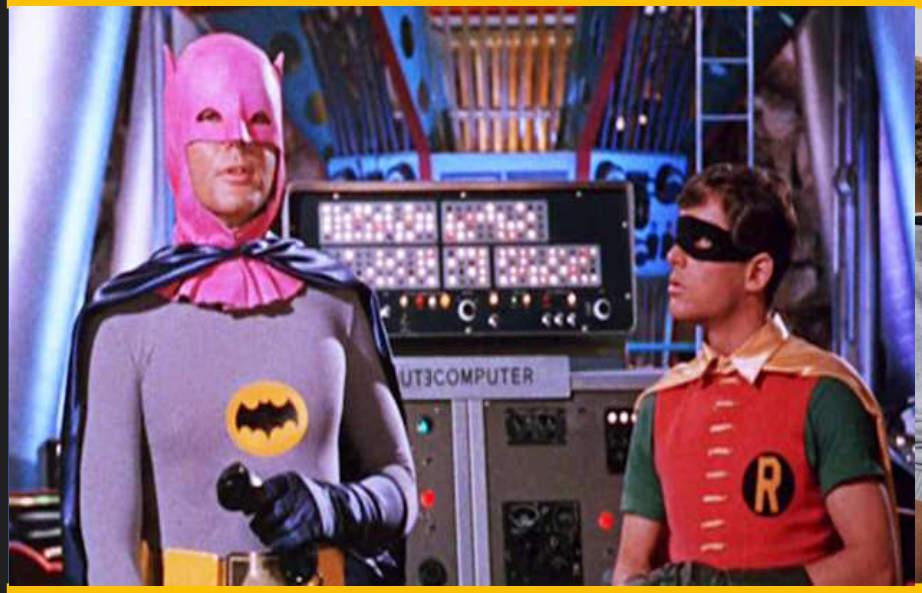
Security Configuration Assessment



SSH – Wazuh

27/03/2024

FIM
Intégrité des fichiers



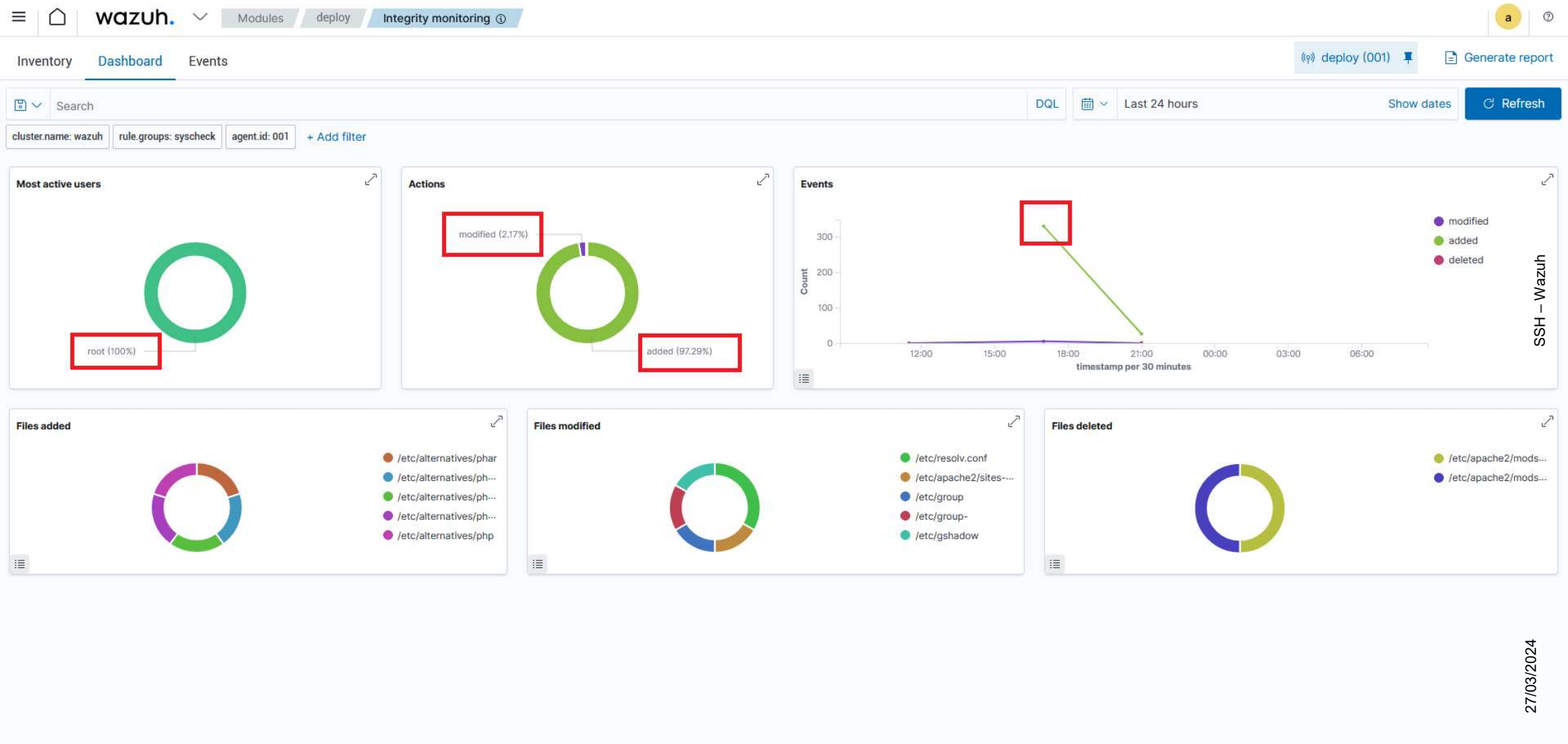
Files Integrity Monitoring

- Par défaut check toutes les 12h
  - Personnalisable
- Personnalisation des dossiers ou fichiers à contrôler

  <directories>/usr/local/scripts</directories>
- Possibilité de définir une analyse temps réel sur un dossier

  <directories **whodata="yes"**>/usr/local/scripts</directories>
- Analyse
  - Propriétaire, groupe et droits
  - Hash (Sha1,md5,sha256)
  - Inode, attributs et date de modification

Files Integrity Monitoring



27/03/2024

“

Vulnérabilités

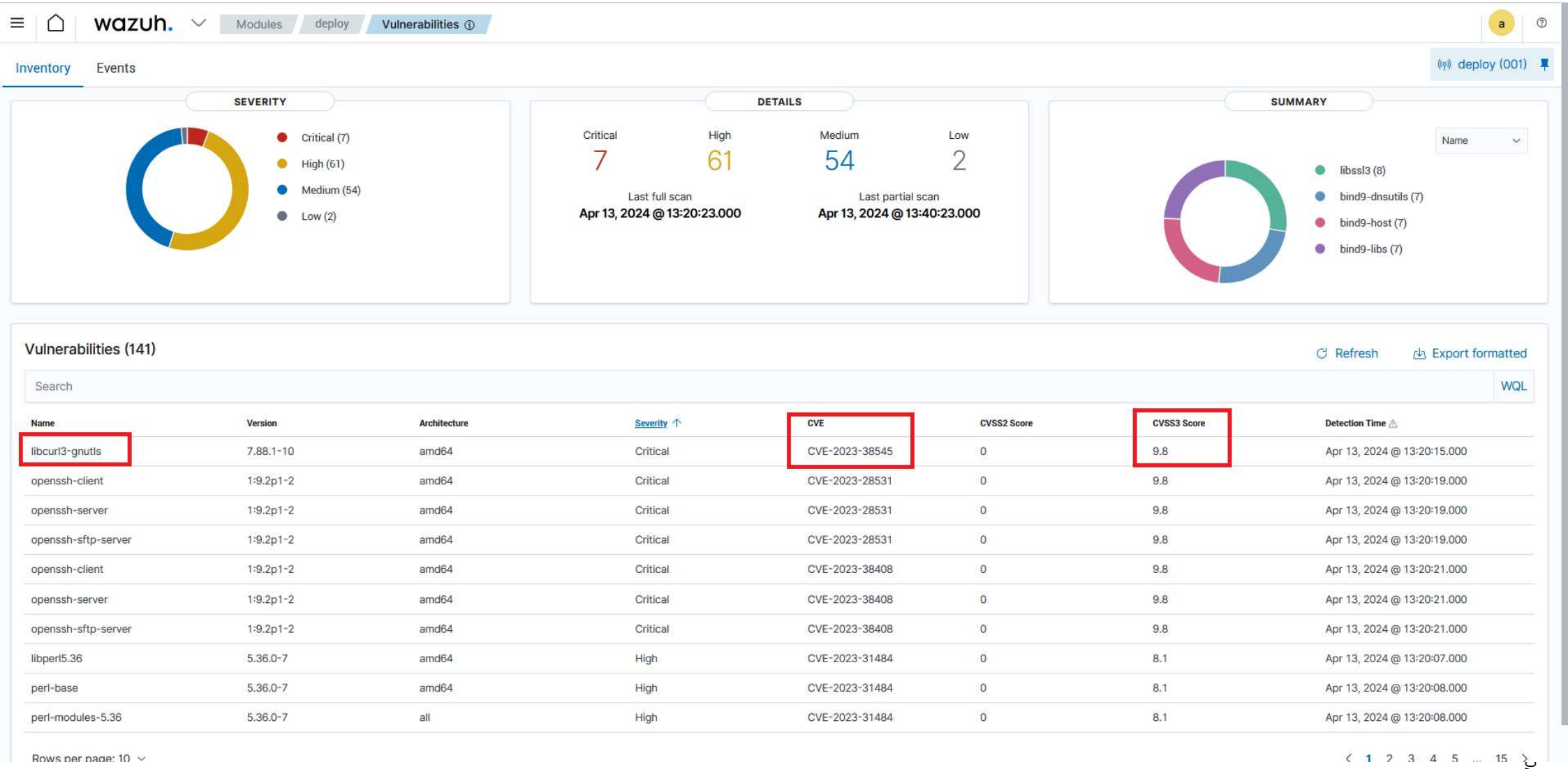
Vulnérabilités

- S’active au niveau du serveur par OS

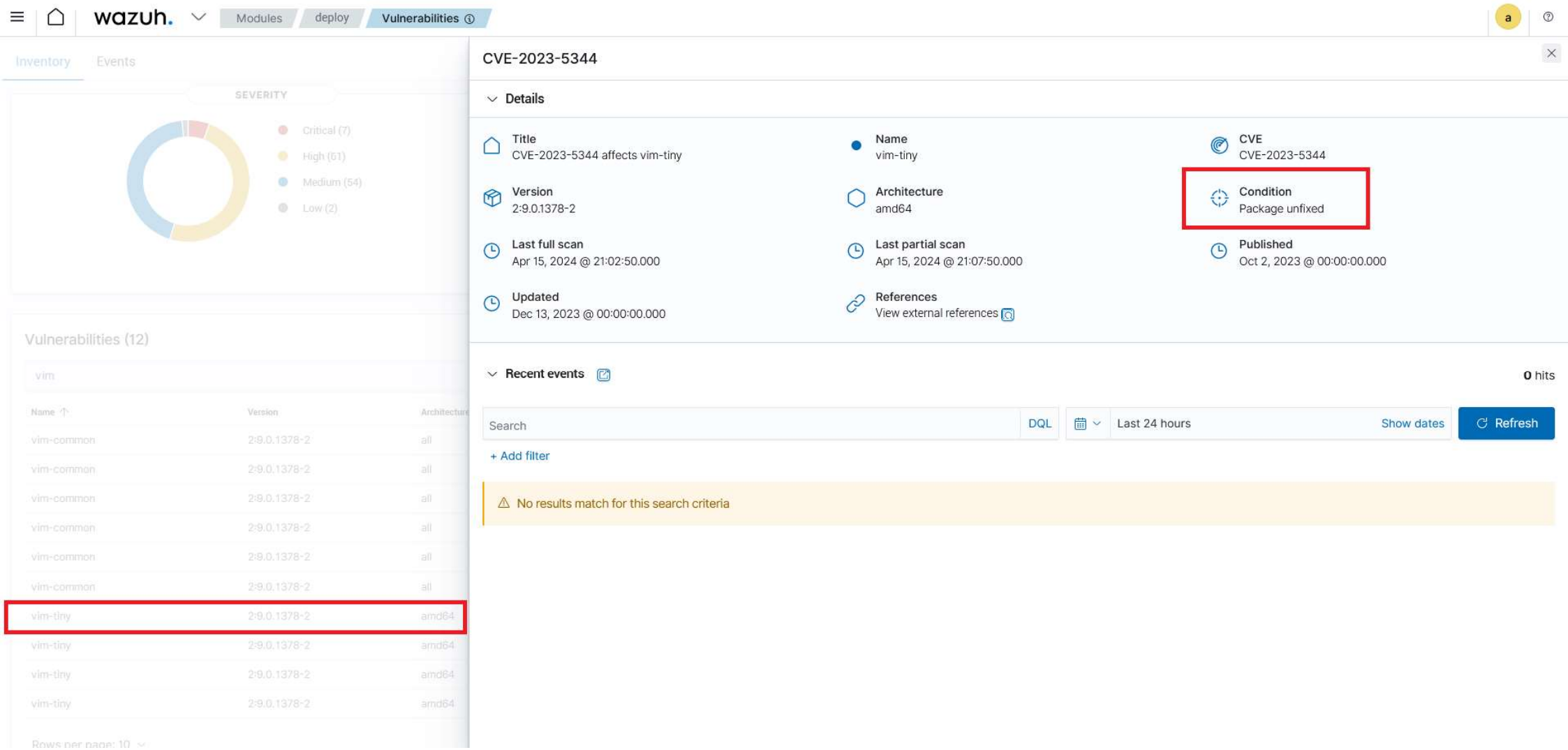
```
<!-- Debian OS vulnerabilities -->
 <provider name="debian">
   <enabled>yes</enabled>
   <os>buster</os>
   <os>bullseye</os>
   <os>bookworm</os>
   <update_interval>1h</update_interval>
 </provider>
```

- Wazuh construit un base locale SQLite des CVEs
  - Source : Les bases CVEs de chaque distribution
  - Par défaut toutes les heures

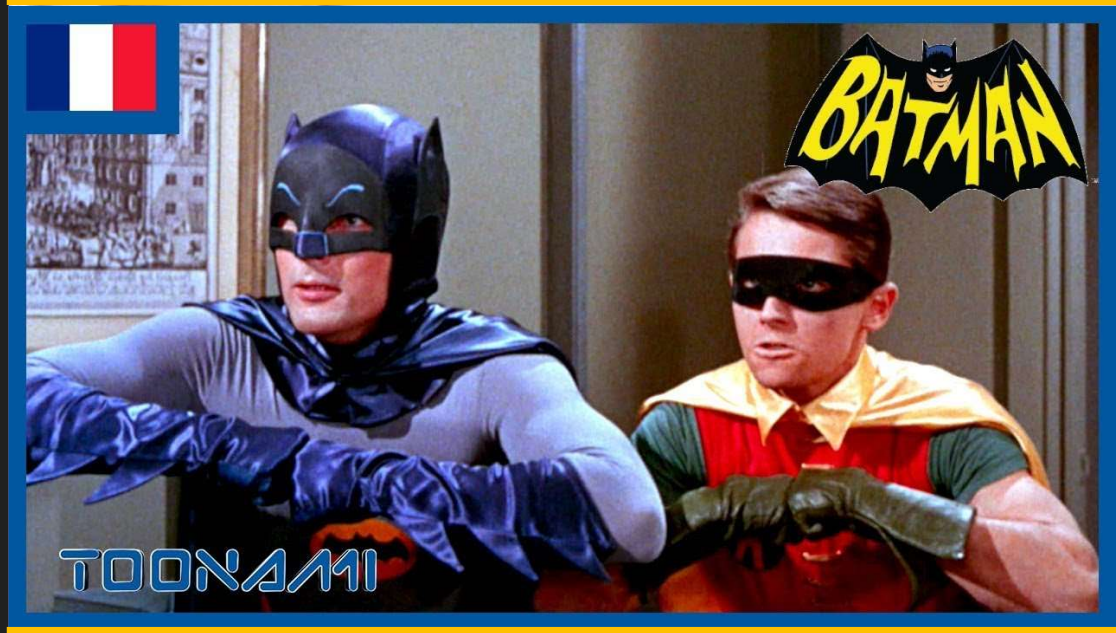
Ubuntu
Debian
RedHat
Amazon Linux
SUSE Linux Enterprise
Arch
Windows
Alma Linux


wazuh.
Modules
deploy
Vulnerabilities
a
Inventory
Events
deploy (001)
SEVERITY
Critical (7)
High (61)
Medium (54)
Low (2)
DETAILS
Critical
7
High
61
Medium
54
Low
2
Last full scan
Apr 13, 2024 @ 13:20:23.000
Last partial scan
Apr 13, 2024 @ 13:40:23.000
SUMMARY
Name
libssl3 (8)
bind9-dnsutils (7)
bind9-host (7)
bind9-libs (7)
Vulnerabilities (141)
Refresh
Export formatted
Search
WQL
Name
Version
Architecture
Severity
CVE
CVSS2 Score
CVSS3 Score
Detection Time
libcurl3-gnutls 7.88.1-10 amd64 Critical CVE-2023-38545 0 9.8 Apr 13, 2024 @ 13:20:15.000
openssh-client 1:9.2p1-2 amd64 Critical CVE-2023-28531 0 9.8 Apr 13, 2024 @ 13:20:19.000
openssh-server 1:9.2p1-2 amd64 Critical CVE-2023-28531 0 9.8 Apr 13, 2024 @ 13:20:19.000
openssh-sftp-server 1:9.2p1-2 amd64 Critical CVE-2023-28531 0 9.8 Apr 13, 2024 @ 13:20:19.000
openssh-client 1:9.2p1-2 amd64 Critical CVE-2023-38408 0 9.8 Apr 13, 2024 @ 13:20:21.000
openssh-server 1:9.2p1-2 amd64 Critical CVE-2023-38408 0 9.8 Apr 13, 2024 @ 13:20:21.000
openssh-sftp-server 1:9.2p1-2 amd64 Critical CVE-2023-38408 0 9.8 Apr 13, 2024 @ 13:20:21.000
libperl5.36 5.36.0-7 amd64 High CVE-2023-31484 0 8.1 Apr 13, 2024 @ 13:20:07.000
perl-base 5.36.0-7 amd64 High CVE-2023-31484 0 8.1 Apr 13, 2024 @ 13:20:08.000
perl-modules-5.36 5.36.0-7 all High CVE-2023-31484 0 8.1 Apr 13, 2024 @ 13:20:08.000
Rows per page: 10
1 2 3 4 5 ... 15

Vulnérabilités

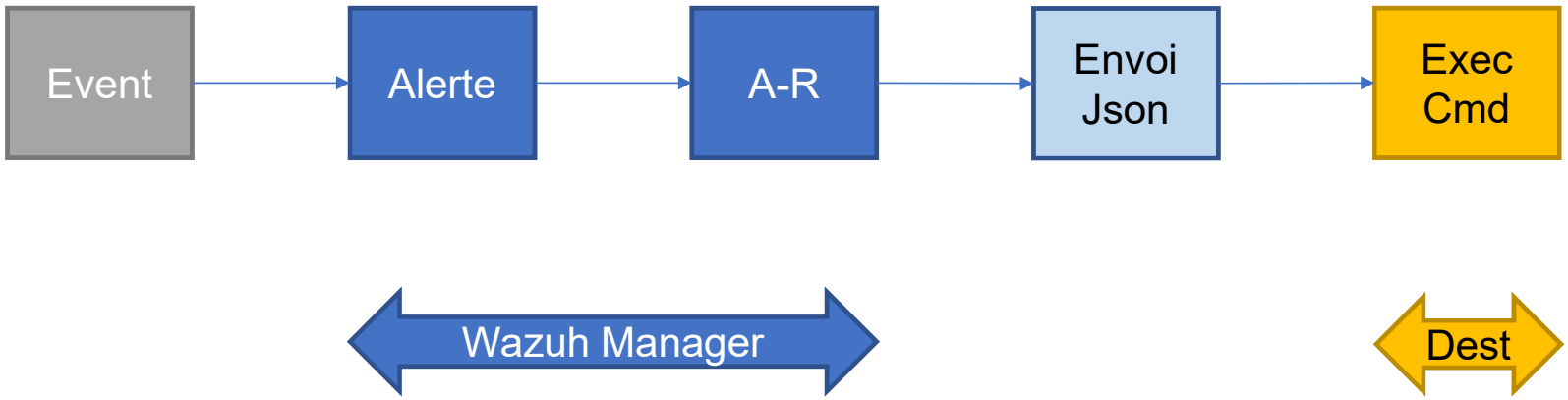


Active Response



Active Response

- Fonctionnement



- Stateful vs Stateless Active Response

Active Response

- Des commandes définies sur le serveur

```
<command>
  <name>hostreact</name>
  <executable>testar.py</executable>
 <timeout_allowed>yes</timeout_allowed>
</command>
```

Active Response

- Des active responses

```
<active-response>
  <disabled>no</disabled>
  <command>hostreact</command>
  <location>local</location>
  <rules_id>5763</rules_id>
  <timeout>60</timeout>
</active-response>
```

Local
Server
All
Defined Agent

Active Response

- Chemin des commandes sur l'agent
  - /var/ossec/active-response/bin
- Contrôler la configuration
  - /var/ossec/bin/agent_control –L

```
root@wazuh:/# /var/ossec/bin/agent_control -L

Wazuh agent_control. Available active responses:

   Response name: hostreact60, command: testar.py
```

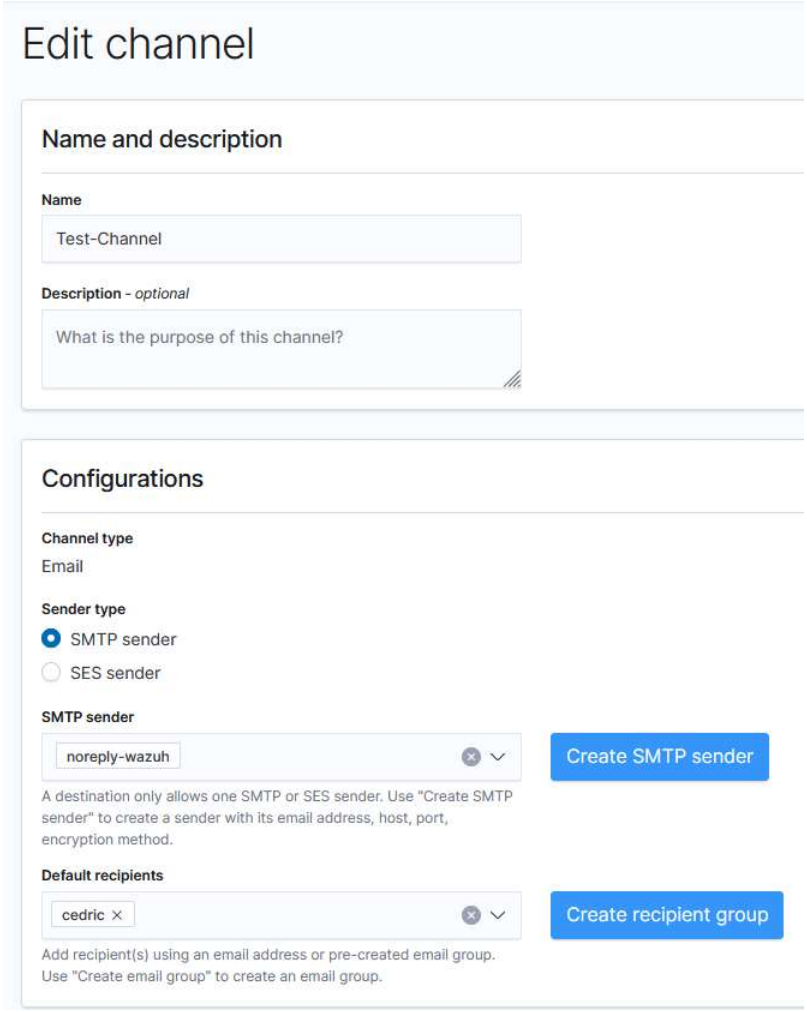
- Tester une commande
  - /var/ossec/bin/agent_control -b 192.168.1.41 -f host-react0 -u 001

“

Alerting

Alerting

- Une channel
  - Un type
    - Email
    - Chime
    - Slack
    - Amazon SNS
    - Hook Web quelconque
  - Un expéditeur
  - Un ou plusieurs destinataire



Alerting

- Un moniteur
  - Ce qu’on observe sur un ou plusieurs index
  - Ce qui déclenche notre alerting
  - Quelle destination (Channel)

Alerting / Monitors / monit

monit • Enabled

Edit | Disable | Export as JSON

Overview

Monitor type
Per query monitor

Monitor definition type
Visual Graph

Total active alerts
0

Schedule
Every 5 minutes

Last updated
04/22/24 10:30 pm CEST

Monitor ID
_87Vul4B1HLZVJxE8TiD

Monitor version number
9

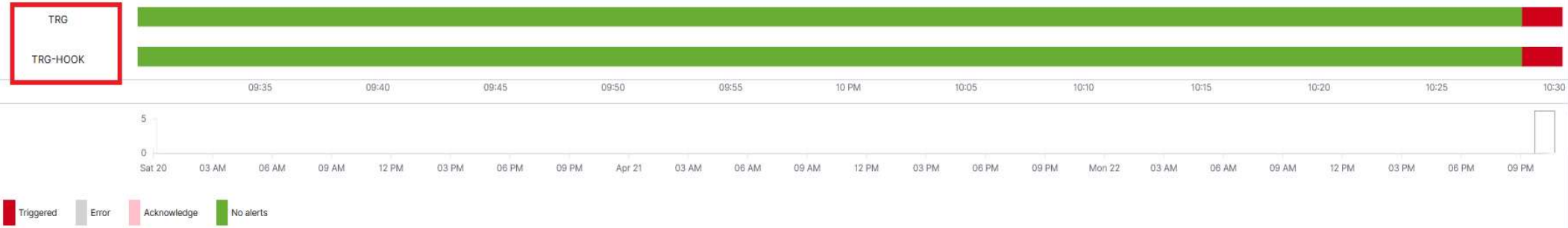
Last updated by
-

Triggers (2)

Name	Number of actions	Severity
TRG	1	1
TRG-HOOK	1	1

History

04/20/2024 12:00 AM → 04/22/2024 10:30 PM



Alerts

Acknowledge

Questions

- Wazuh fonctionne t-il avec journald ?
  - Non pas pour le moment mais la fonctionnalité est en cours de développement

Références

- Wazuh
  - https://documentation.wazuh.com/current

- Decoders/Rules
  - https://socfortress.medium.com/understanding-wazuh-decoders-4093e8fc242c
  - https://github.com/wazuh/wazuh-ruleset
  - https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/regex.html

- Active Response
  - https://documentation.wazuh.com/current/user-manual/reference/ossec-conf/commands.html
  - https://documentation.wazuh.com/current/user-manual/capabilities/active-response/how-to-configure.html

Références

- Wazuh
  - https://documentation.wazuh.com/current
- Installation
  - Ansible
    - https://documentation.wazuh.com/current/deployment-options/deploying-with-ansible/index.html
  - Docker
    - https://documentation.wazuh.com/current/deployment-options/docker/wazuh-container.html
  - Sizing
    - https://medium.com/@wernertie/series-wazuh-master-worker-indexer-dashboard-and-the-ainfrastructure-3a629ae2fa0d

FIN

- Bonne utilisation !