Clement IEHLEN

Mission supervision via un HIDS : WAZUH

Clement IEHLEN

SOMMAIRE

- Installation de Wazuh
- Intégration des logs routeur cisco
- Intégration de l’agent wazuh sur pfsense (externe)
- Intégration de l’agent wazuh sur les serveurs

Qu’est-ce que Wazuh ?

Wazuh est une plateforme de sécurité open source qui offre des fonctionnalités de détection des menaces, de gestion des incidents et de conformité réglementaire. Elle surveille les fichiers, les journaux et les processus en temps réel, détecte les anomalies et les activités suspectes, et aide à se conformer aux normes de sécurité comme PCI DSS et GDPR. Wazuh est hautement évolutif, pouvant gérer des milliers d'agents, et s'intègre avec des outils SIEM tels qu'Elastic Stack et Splunk pour une gestion centralisée de la sécurité.

Clement IEHLEN

Installation de Wazuh

Pour comment il faut installer wazuh sur une machine. J'ais choisi de l'installer sur une machine Debian 12.

1. CREATION DE CERTIFICATS

Téléchargez le wazuh-certs-tool.shscript et le config.ymlfichier de configuration. Cela crée les certificats qui chiffrent les communications entre les composants centraux Wazuh.

```
root@srvlab001wazuh:/home/ekan# curl -sO https://packages.wazuh.com/4.6/wazuh-certs-tool.sh
root@srvlab001wazuh:/home/ekan# curl -sO https://packages.wazuh.com/4.6/config.yml
```

Modifiez ./config.ymlet remplacez les noms de nœuds et les valeurs IP par les noms et adresses IP correspondants.

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "172.20.2.50"
    #- name: node-2
    #  ip: "<indexer-node-ip>"
    #- name: node-3
    #  ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "172.20.2.50"
    #  node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "172.20.2.50"
```

Exécutez ./wazuh-certs-tool.shpour créer les certificats

```
root@srvlab001wazuh:/home/ekan# bash ./wazuh-certs-tool.sh -A
06/11/2023 21:19:14 INFO: Admin certificates created.
06/11/2023 21:19:14 INFO: Wazuh indexer certificates created.
06/11/2023 21:19:14 INFO: Wazuh server certificates created.
06/11/2023 21:19:14 INFO: Wazuh dashboard certificates created.
```

Compressez tous les fichiers nécessaires

```
root@srvlab001wazuh:/home/ekan# tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/
./
./node-1-key.pem
./root-ca.pem
./root-ca.key
./wazuh-1.pem
./dashboard.pem
./wazuh-1-key.pem
./dashboard-key.pem
./admin-key.pem
./node-1.pem
./admin.pem
root@srvlab001wazuh:/home/ekan# rm -rf ./wazuh-certificates
```

2. Installation de Wazuh

Installez-les packages suivants

```
root@srvlab001wazuh:/home/ekan# apt-get install gnupg apt-transport-https
```

On installe la clé gpg

```
root@srvlab001wazuh:/home/ekan# curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyri
ng gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

Installation de l'indexeur Wazuh

```
apt-get -y install wazuh-indexer
```

Modifiez le `/etc/wazuh-indexer/opensearch.yml`

```
GNU nano 7.2
network.host: "172.20.2.50"
node.name: "node-1"
cluster.initial_master_nodes:
- "node-1"
#- "node-2"
#- "node-3"
cluster.name: "wazuh-cluster"
```

Installation de wazuh-manager et filebeat

```
root@srvlab001wazuh:/home/ekan# apt-get -y install wazuh-manager
```

```
root@srvlab001wazuh:/home/ekan# apt-get -y install filebeat
```

Modifiez le /etc/filebeat/filebeat.yml

Clement IEHLEN

```
# Wazuh - Filebeat configuration file
output.elasticsearch:
  hosts: ["172.20.2.50:9200"]
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
```

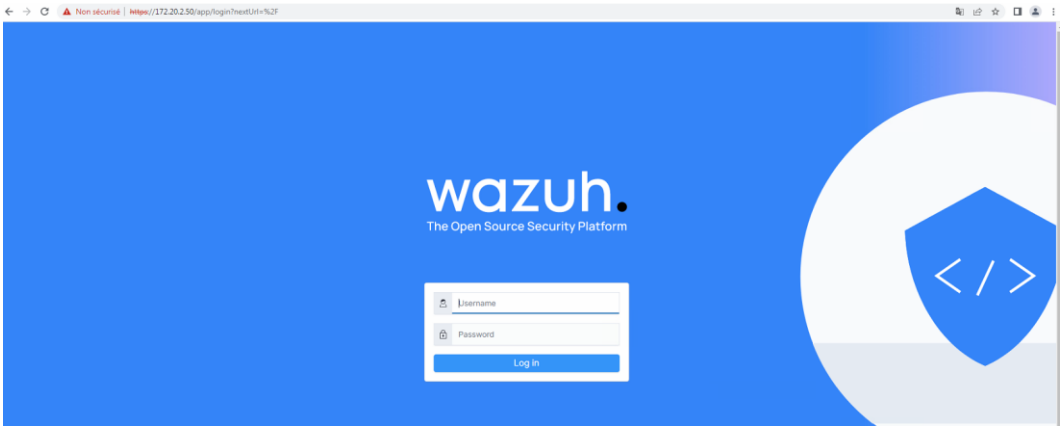
Installation de Wazuh Dashboard

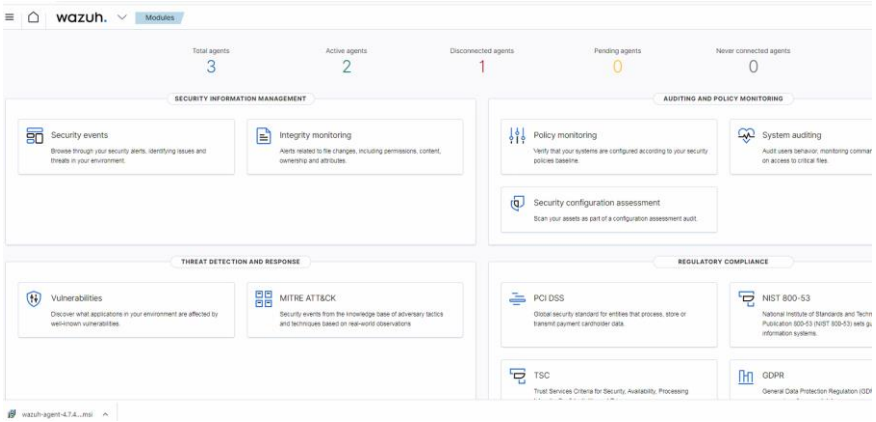
```
root@srvlab001wazuh:/home/ekan# apt-get -y install wazuh-dashboard
```

Configuration du fichier /etc/wazuh-dashboard/opensearch_dashboards.yml

```
server.host: 172.20.2.50
server.port: 443
opensearch.hosts: https://172.20.2.50:9200
opensearch.ssl.verificationMode: certificate
#opensearch.username:
#opensearch.password:
opensearch.requestHeadersAllowlist: ["securitytenant","Authorization"]
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ["kibana_read_only"]
server.ssl.enabled: true
server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
uiSettings.overrides.defaultRoute: /app/wazuh
```

On ce rend sur un navigateur pour voir si wazuh fonctionne bien.

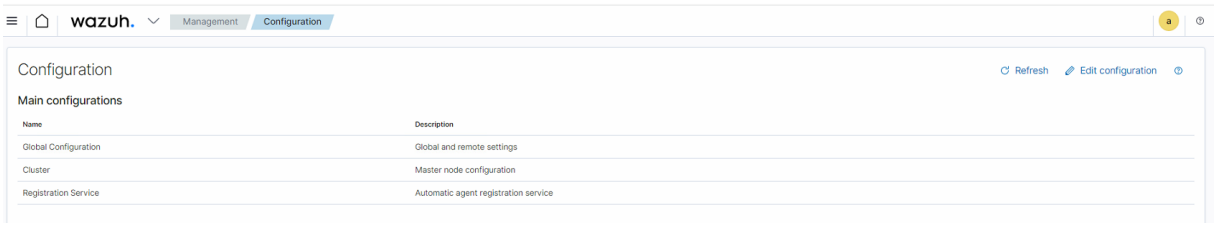




Clement IEHLEN

Intégration des logs routeur cisco

On ce rend dans Managment > configuration > edite configuration



On ajoute la configure de syslog pour le routeur

```
<remote>
  <connection>syslog</connection>
  <port>514</port>
  <protocol>udp</protocol>
  <allowed-ips>172.20.3.0/24</allowed-ips>
  <local_ip>172.20.2.50</local_ip>
</remote>
```

On sauvegarde et on restart

Passons à la partie du routeur

On définit ce niveau de logging
Plus le niveau de logging est haut, plus le nombre de logs envoyés au serveur Syslog est important

```
Routeur(config)#logging trap 6
```

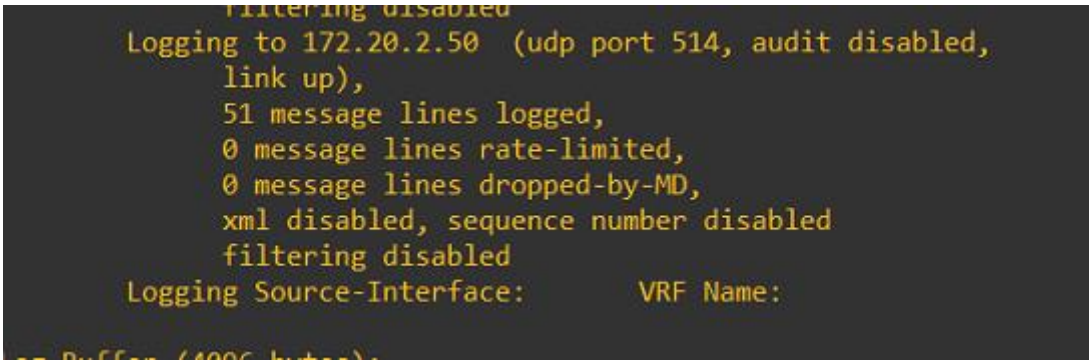
On définit le log facility c'est un nom qui permet au serveur syslog de savoir de quelle machine viennent les différents logs reçus

```
Routeur(config)#logging facility local16
```

On indique l'ip du serveur syslog

```
Routeur(config)#logging 172.20.2.50
```

On vérifie les paramètres



On peut constater que Wazuh reçoit bien les logs.

Intégration de l’agent wazuh sur pfsense (externe)

Pour faire cette partie je me suis connecter en ssh sur la pfsense externe.

J’installe l'agent Wazuh à l'aide du référentiel de packages FreeBSD.

Les packages FreeBSD son désactiver par default

Afin de permettre pkg l'extraction dudit référentiel, nous avons besoin de quelques fichiers

On se rend dans le fichier /usr/local/etc/pkg/repos/pfSense.conf

On change le FreeBSD no par yes

```
  GNU nano 7.2                          /usr/local/etc/pkg/repos/pfSense.conf
FreeBSD: { enabled: yes }

pfSense-core: {
    url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-core",
    mirror_type: "srv",
    signature_type: "fingerprints",
    fingerprints: "/usr/local/share/pfSense/keys/pkg",
    enabled: yes
}

pfSense: {
    url: "pkg+https://pkg.pfsense.org/pfSense_v2_7_2_amd64-pfSense_v2_7_2",
    mirror_type: "srv",
    signature_type: "fingerprints",
    fingerprints: "/usr/local/share/pfSense/keys/pkg",
    enabled: yes
}
```

Ensuit on fait pareil dans le fichier /usr/local/etc/pkg/repos/FreeBSD.conf

```
  GNU nano 7.2                          /usr/local/etc/pkg/repos/FreeBSD.conf
FreeBSD: { enabled: yes }
```

On peut ensuit mettre a jour les package et exécuter la commande pour chercher le package wazuh-agent

```
[2.7.2-RELEASE][admin@pfSense_Externe.GSB.local]/root: pkg search wazuh-agent
wazuh-agent-4.7.3              Security tool to monitor and check logs and intrusions (agent)
[2.7.2-RELEASE][admin@pfSense_Externe.GSB.local]/root:
```

On installe avec cette commende

```
2.7.2-RELEASE][admin@pfSense_Externe.GSB.local]/root: pkg install wazuh-agent-4.7.3
```

Pour configure l’agent on ce rend dans /var/ossec/etc/ossec.conf

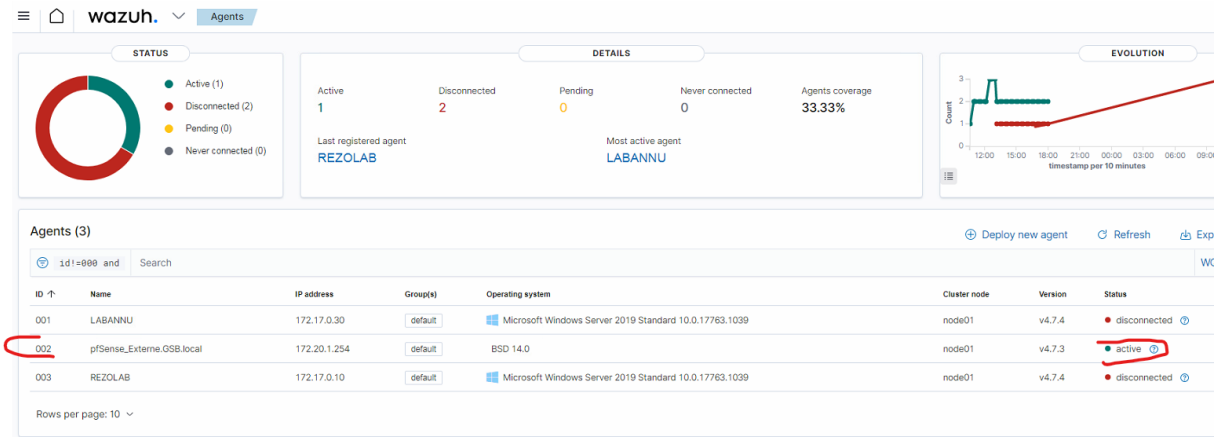
```
<ossec_config>
  <client>
    <server>
      <address>172.20.2.50</address>
    </server>
    <config-profile>debian, debian8</config-profile>
    <crypto_method>aes</crypto_method>
  </client>
```

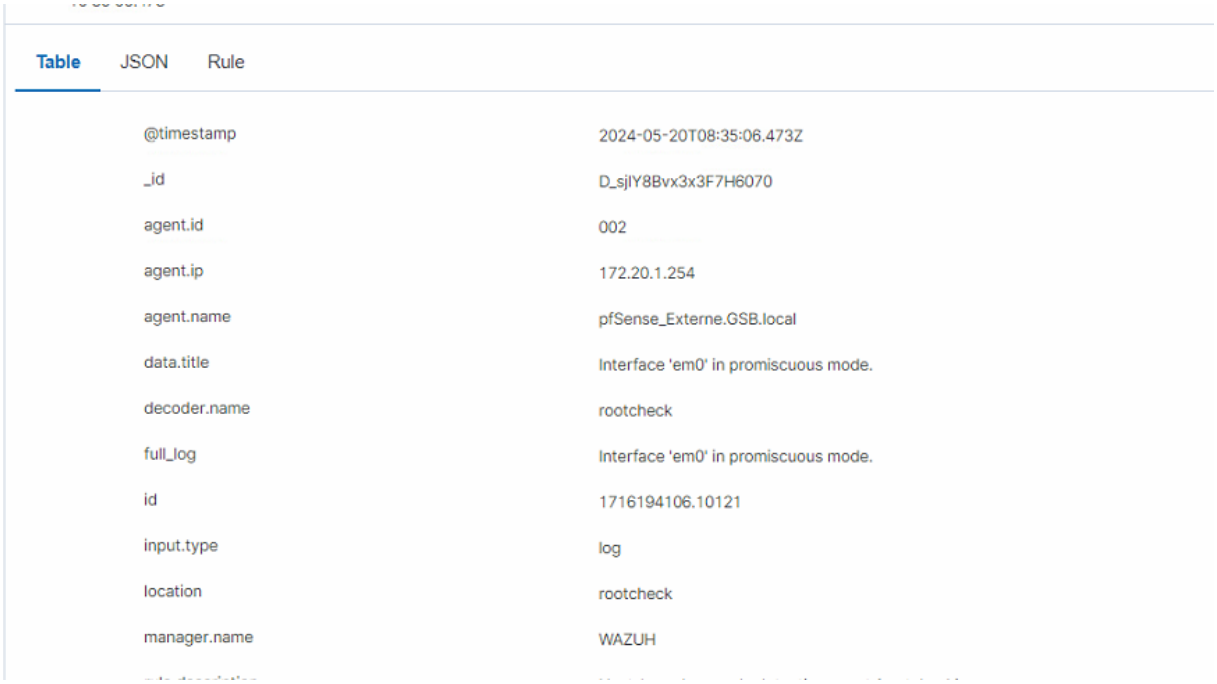
Puis il resta à activer l’agent

```
.7.2-RELEASE][admin@pfSense_Externe.GSB.local]/root: sysrc wazuh_agent_enable="YES"
```

Clement IEHLEN

La configuration sur la pfsense et enfin fini on peut maintenant le retrouver sur la console wazuh



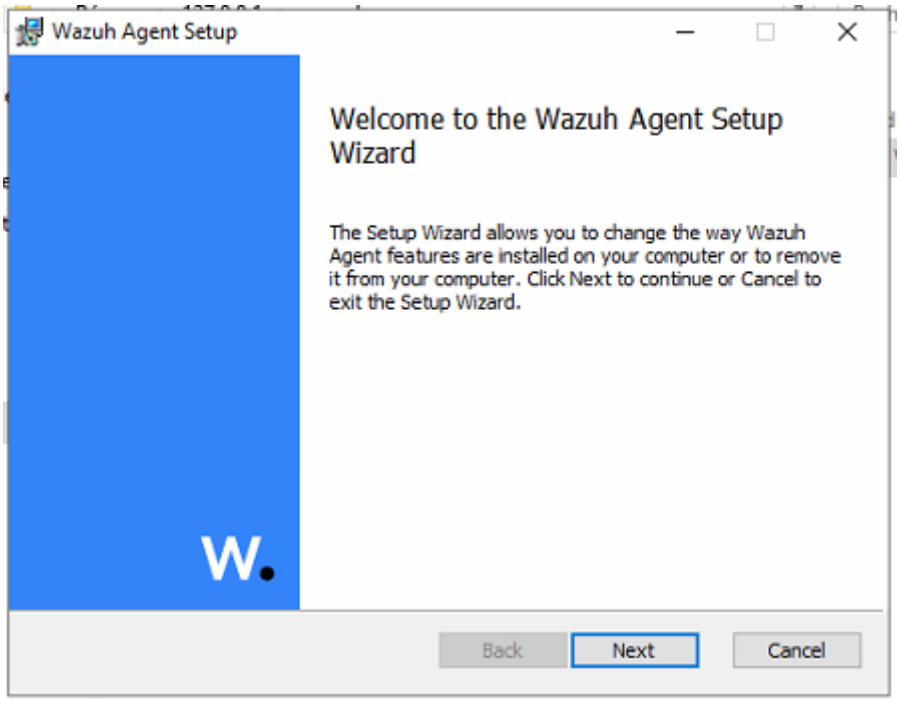


Intégration de l’agent wazuh sur les serveurs

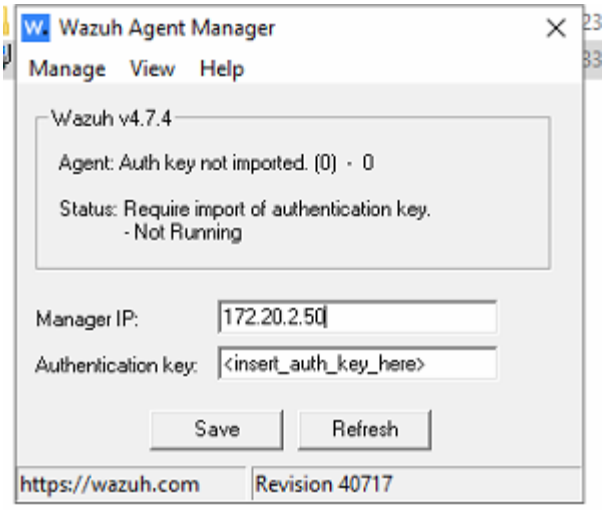
La configuration de l’agent wazuh sur les postes Windows et serveur est particulièrement facile, un agent en .msi est a disposition sur le site de wazuh

https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html

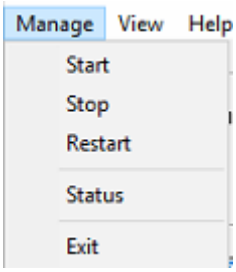
Clement IEHLEN



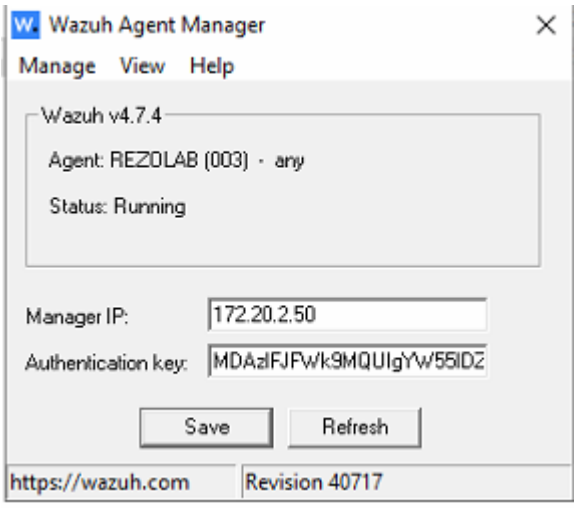
Apprêt l'installation basic on peut ouvrir la configuration.



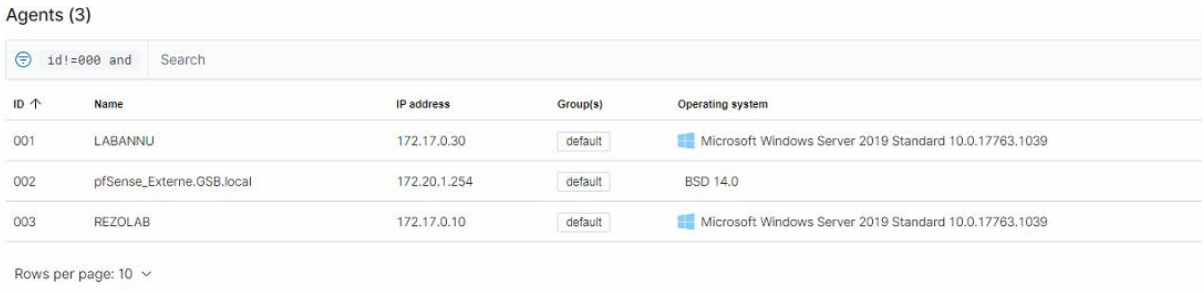
On démarre l'agent.



Clement IEHLEN



Voila la configuration et maintenant fini on peut le faire aussi sur le serveur DHCP (REZOLAB) et aller les retrouver sur le panel wazuh



L’installation de Wazuh et l'intégration de Wazuh-agent sur pfSense et deux serveurs Windows ont été réalisées avec succès, renforçant ainsi notre capacité de détection et de réponse aux menaces de sécurité, tout en assurant une gestion centralisée et une conformité accrue.