

Osquery

I - Présentation de Osquery et du module Wazuh

Osquery est un outil qui expose un système d'exploitation en tant que base de données relationnelle, permettant l'exécution de requêtes **SQL** pour explorer les données du système. Le module **Wazuh** permet de gérer **Osquery** depuis les agents **Wazuh**, permettant la configuration d'**Osquery** et la collecte d'informations pour les envoyer au gestionnaire, avec génération d'alertes si nécessaire.

II - Installation de Osquery sur le serveur Wazuh

- **Red Hat, CentOS et Fedora :**

```
curl -L https://pkg.osquery.io/rpm/GPG | tee /etc/pki/rpm-gpg/RPM-GPG-KEY-osquery
yum-config-manager --add-repo https://pkg.osquery.io/rpm/osquery-s3-rpm.repo
yum-config-manager --enable osquery-s3-rpm-repo
yum install osquery
```

- **Distributions Linux basées sur Debian et Ubuntu :**

```
export OSQUERY_KEY=1484120AC4E9F8A1A577AEEE97A80C63C9D8B80B
apt-key adv --keyserver keyserver.ubuntu.com --recv-keys $OSQUERY_KEY
add-apt-repository 'deb [arch=amd64] https://pkg.osquery.io/deb deb main'
apt-get update
apt-get install osquery
```

III - Configuration de Osquery

Après l'installation, on a besoin d'un fichier de configuration pour **Osquery**. On peut utiliser un fichier fourni par **Osquery** ou configurer le fichier avec un fichier personnalisé comme celui fourni par **Wazuh**.

- **Utiliser le fichier fourni par Osquery :**

```
cp /opt/osquery/share/osquery/osquery.example.conf /etc/osquery/osquery.conf
```

- **Où copier une configuration personnalisée en éditant le fichier /etc/osquery/osquery.conf :**

```
{
  "options": {
    "config_plugin": "filesystem",
    "logger_plugin": "filesystem",
    "utc": "true"
  },
  "schedule": {
    "system_info": {
      "query": "SELECT hostname, cpu_brand, physical_memory FROM system_info;",
      "interval": 3600
    },
    "high_load_average": {
      "query": "SELECT period, average, '70%' AS 'threshold' FROM load_average WHERE period = '15m' AND average > '0.7';",
      "interval": 900,
      "description": "Report if load charge is over 70 percent."
    },
    "low_free_memory": {
      "query": "SELECT memory_total, memory_free, CAST(memory_free AS real) / memory_total AS memory_free_perc, '10%' AS threshold FROM memory_info WHERE memory_free_perc < 0.1;",
      "interval": 1800,
      "description": "Free RAM is under 10%."
    }
  },
  "packs": {
    "osquery-monitoring": "/opt/osquery/share/osquery/packs/osquery-monitoring.conf",
    "incident-response": "/opt/osquery/share/osquery/packs/incident-response.conf",
    "it-compliance": "/opt/osquery/share/osquery/packs/it-compliance.conf",
    "vuln-management": "/opt/osquery/share/osquery/packs/vuln-management.conf",
    "hardware-monitoring": "/opt/osquery/share/osquery/packs/hardware-monitoring.conf",
    "ossec-rootkit": "/opt/osquery/share/osquery/packs/ossec-rootkit.conf"
  }
}
```

Osquery

IV - Activation et démarrage de Osquery

On active et lance le démon **Osquery** :

```
systemctl enable osqueryd  
systemctl start osqueryd
```

V - Activation du module Wazuh pour Osquery

Le module **Osquery** doit être activé pour les agents sur lesquels **Osquery** est exécuté. Il suffit d'ajouter `<wodle name="osquery"/>` à leur fichier de configuration, situé dans `/var/ossec/etc/ossec.conf`.