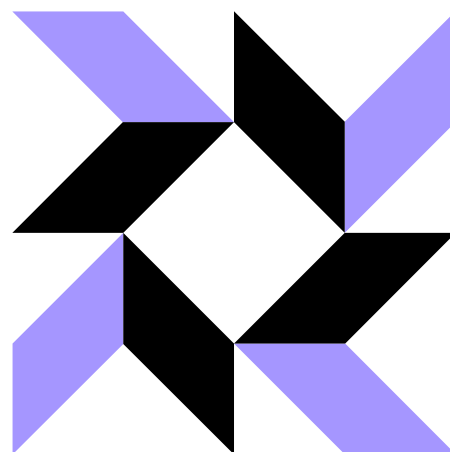




osquery

Mickaël Masquelin |





Généralités

@authors :
facebook sec. team



Join GitHub today

GitHub is home to over 31 million developers working together to host and review code, manage projects, and build software together.

[Sign up](#)

Dismiss

SQL powered operating system instrumentation, monitoring, and analytics. <https://osquery.io>

security

monitoring

intrusion-detection

sql

4,724 commits

17 branches

95 releases

262 contributors

View license

Branch: master

[View #1246](#)

Find File

Clone or download

This branch is 243 commits behind experimental.

Pull request

Compare



packetzero and fmanco update aws-sdk-cpp 1.4.55 on windows (#5255)

Latest commit 5188ce5 on 29 Oct 2018

.github

Add task issue template (#4901)

7 months ago

CMake

General SMART drive information virtual table (#4133)

8 months ago

docs

Update process-creating.md (#5188)

6 months ago

external

Bundle C++ extensions into a single executable (#4335)

10 months ago

include/osquery

database: changing default path of the database for pathing uniformity (

6 months ago

Version actuelle : 3.3.2

Un outil « cross-platform »





En détail maintenant ...



Pour faire quoi ?

A large, empty rectangular box with a thin black border and a small arrowhead pointing to the left at the bottom-left corner, intended for a response.A large, empty rectangular box with a thin black border and a small arrowhead pointing to the left at the bottom-left corner, intended for a response.A large, empty rectangular box with a thin black border and a small arrowhead pointing to the left at the bottom-left corner, intended for a response.



Pour faire quoi ?

GESTION DE PARC INFORMATIQUE

Utilisation façon GLPI / OCS-ng ou encore MunkiReport, en récupérant des informations sur le matériel ou les logiciels installés



Pour faire quoi ?

GESTION DE PARC INFORMATIQUE

Utilisation façon GLPI / OCS-ng, en récupérant des informations sur le matériel ou les logiciels installés

MONITORER LES SYSTEMES

Générer des mesures, collecter des signaux depuis différentes sources et réaliser des statistiques de base



Pour faire quoi ?

GESTION DE PARC INFORMATIQUE

Utilisation façon GLPI / OCS-ng, en récupérant des informations sur le matériel ou les logiciels installés

MONITORER LES SYSTEMES

Générer des mesures, collecter des signaux depuis différentes sources et réaliser des statistiques de base

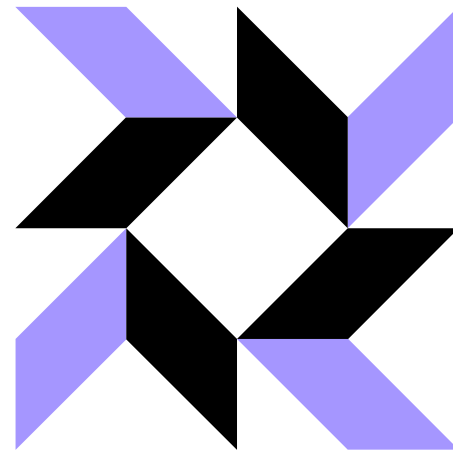
DETECTION D'INTRUSION POUR UN HOTE

Rechercher des indicateurs de compromission dans les données du système hôte

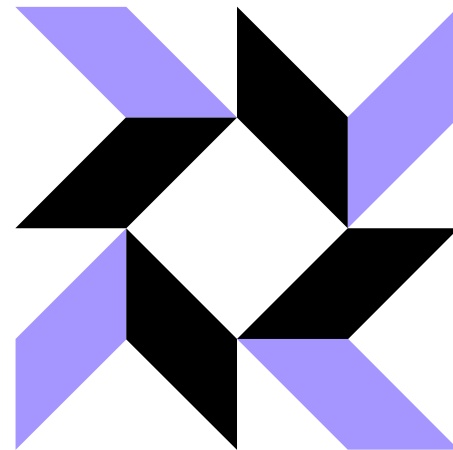
Principe



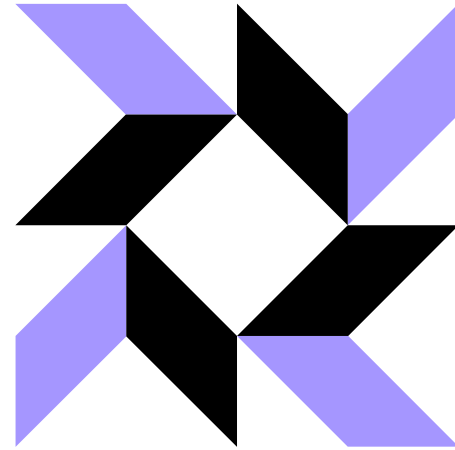
- OS exposé sous forme d'une BDD relationnelle
- Présentation des concepts abstraits comme des tables
- Exemples :
 - Table des processus en cours ;
 - Table des modules du noyau chargés ;
 - Table des connexions réseau ;
 -



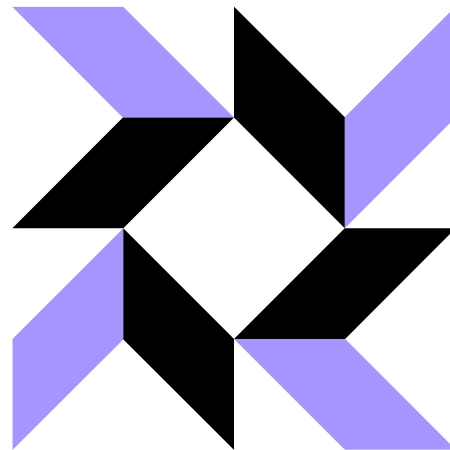
SQL



SQL



NoSQL



NoSQL



oSQL



Comment ça fonctionne ?

osqueryi : une interface CLI



```
libercourt:~ masqueli$ osqueryi
osquery> -- Infos minimalistes sur une machine
osquery> SELECT computer_name, hardware_vendor, hardware_model, cpu_brand, hardware_serial FROM system_info;
+-----+-----+-----+-----+-----+
| computer_name | hardware_vendor | hardware_model | cpu_brand | hardware_serial |
+-----+-----+-----+-----+-----+
| libercourt    | Apple Inc.      | MacBookPro14,3 | Intel(R) Core(TM) i7-7920HQ CPU @ 3.10GHz | C02V426QHTDF |
+-----+-----+-----+-----+-----+
osquery> SELECT m.path AS chemin, m.type AS type_fs,
...> round((m.blocks_available * m.blocks_size * 10e-10) ,2) AS espace_disque_libre
...> FROM mounts m WHERE m.path = '/';
+-----+-----+-----+
| chemin | type_fs | espace_disque_libre |
+-----+-----+-----+
| /      | apfs    | 12.22                |
+-----+-----+-----+
```

osqueryd : un démon



```
[info@prd-lci-net01 ~]$ cat /etc/osquery/osquery.conf
{
  "options": { [..] },
  "schedule": {
    "packages_distro": {
      "query": "SELECT name, version FROM rpm_packages;",
      "interval": 300
    },
    "latest_ssh_logins": {
      "query": "SELECT pid, port, address host FROM last WHERE type=7",
      "interval": 360
    },
    "connex_sortantes": {
      "query": "SELECT s.pid, p.name, local_address, remote_address, family,
protocol, local_port, remote_port FROM process_open_sockets s JOIN processes p ON s.pid =
p.pid WHERE remote_port NOT IN (80, 443) AND family = 2;",
      "interval": 360
    }
  }
}
```

process_open_sockets

Processes which have open network sockets on the system.

[Improve this Description on Github](#)

COLUMN	TYPE	DESCRIPTION
pid	INTEGER	Process (or thread) ID
fd	BIGINT	Socket file descriptor number
socket	BIGINT	Socket handle or inode number
family	INTEGER	Network protocol (IPv4, IPv6)
protocol	INTEGER	Transport protocol (TCP/UDP)
local_address	TEXT	Socket local address
remote_address	TEXT	Socket remote address
local_port	INTEGER	Socket local port
remote_port	INTEGER	Socket remote port
path	TEXT	For UNIX sockets (family=AF_UNIX), the domain path
state	TEXT	TCP socket state
net_namespace	TEXT	The inode number of the network namespace

Les « packs »



- Pour faire quoi ?
 - Eviter de définir X requêtes une à une dans 1 fichier de configuration
- Ecriture d'un « Query Pack » :
 - Ensemble de requêtes servant un objectif commun
 - Exemple : détection des rootkits/exploits sous GNU/Linux

```
[root@prd-lci-net01 packs]# ls
hardware-monitoring.conf  it-compliance.conf      ossec-rootkit.conf  unwanted-chrome-extensions.conf  windows-attacks.conf
incident-response.conf   osquery-monitoring.conf  osx-attacks.conf   vuln-management.conf              windows-hardening.conf
```

- Inclus via la directive **packs** dans `/etc/osquery/osquery.conf`

```
[root@prd-lci-net01 packs]# ...
"packs": {
  "incident-response": "/usr/share/osquery/packs/incident-response.conf",
  "it-compliance": "/usr/share/osquery/packs/it-compliance.conf",  [...]
```



Cas d'utilisation

Avec Docker

```
[masqueli@prd-lci-web02 ~]# osqueryi
```

```
osquery> -- Detecter les containers qui executent des processus en tant que root
```

```
osquery> SELECT containers.name, processes.pid, processes.name, cmdline, user
```

```
...> FROM docker_container_processes processes
```

```
...> JOIN docker_containers containers ON containers.id=processes.id
```

```
...> WHERE processes.id IN ( SELECT id FROM docker_containers ) AND user="root";
```

name	pid	name	cmdline	user
nginx	10902	nginx	nginx: master process nginx -g daemon off;	root
python	4653	python	python back/app.py	root
python	4686	python	python front/app.py	root
s6-svscan	3736	s6-svscan	/bin/s6-svscan /etc/services.d	root
s6-supervise	4165	s6-supervise	s6-supervise cron	root
s6-supervise	4166	s6-supervise	s6-supervise nginx	root
s6-supervise	4167	s6-supervise	s6-supervise php	root

Statut du chiffrement d'une machine

```
libercourt:~ masqueli$ osqueryi
Using a virtual database. Need help, type '.help'
osquery> -- verifier que FileVault2 sur macOS couvre bien un volume
osquery> SELECT m.path AS chemin, m.type AS type_fs,
...> round((m.blocks_available * m.blocks_size * 10e-10) ,2) AS espace_disque_libre,
...> de.encrypted AS est_chiffre, de.type AS type_chiffrement
...> FROM mounts m JOIN disk_encryption de ON de.name=m.device WHERE m.path = '/';
+-----+-----+-----+-----+-----+
| chemin | type_fs | espace_disque_libre | est_chiffre | type_chiffrement |
+-----+-----+-----+-----+-----+
| /      | apfs    | 18.31              | 1           | APFS Encryption  |
+-----+-----+-----+-----+-----+
```

Statut du chiffrement d'une machine

```
C:\ProgramData\osquery> osqueryi
Using a virtual database. Need help, type '.help'
osquery> -- verifier que Bitlocker pour Windows couvre bien un volume en chiffrement logiciel
osquery> SELECT device_id AS id_machine, drive_letter AS volume,
...> encryption_method AS type_chiffrement,
...> protection_status AS est_protege
...> FROM bitlocker_info WHERE encryption_method NOT LIKE 'HARDWARE%';
```

id_machine	volume	type_chiffrement	est_protege
\\?\Volume{59c8b87-d16d-4107-990b-b5be345483ee}\	C:	AES_128	1



Conclusion



Compléments

fleets managers



[mwielgoszewski / doorman](#) Watch 33 Star 451 Fork 73

Code Issues 13 Pull requests 1 Projects 0 Insights

Join GitHub today
GitHub is home to over 31 million developers working together to host and review code, manage projects, and build software together.
[Sign up](#)

an osquery fleet manager

473 commits 3 branches 7 releases 15 contributors MIT

Branch: master New pull request Find File Clone or download

mwielgoszewski can't support 3.7-dev, celery doesn't support it: [celery/celery#4500](#) Latest commit 9a9b97c on 5 Jan

docker	Don't force DOORMAN_ENV to prod in the docker config	2 years ago
docs/screenshots	update documentation	3 years ago
doorman	upgrade dependencies	2 months ago
migrations	Add support for query sharding and new drop down fields	2 years ago
requirements	upgrade dependencies	2 months ago
tests	support for custom column rendering	2 months ago
tools	Adding Vagrantfile and automated doorman provisioning	3 years ago
.bowerrc	initial release of this code to the world. todo: docs	3 years ago
.codeclimate.yml	Update .codeclimate.yml	3 years ago
.csslintrc	Remove box-sizing warning	3 years ago
.dockernignore	Add Dockerfile and enough config to get it to boot	3 years ago
.eslintignore	Add sensible eslint defaults	3 years ago
.eslintrc	Add sensible eslint defaults	3 years ago
.gitignore	Adding Vagrantfile and automated doorman provisioning	3 years ago

[kolide / fleet](#) Watch 36 Star 555 Fork 128

Code Issues 81 Pull requests 0 Insights

Join GitHub today
GitHub is home to over 31 million developers working together to host and review code, manage projects, and build software together.
[Sign up](#)

A flexible control server for osquery fleets <https://kolide.com/fleet>

security osquery host-instrumentation infosec macadmin

1,096 commits 1 branch 20 releases 36 contributors MIT

Branch: master New pull request Find File Clone or download

zwass Clarify labels UI (#2012) Latest commit 992151f 8 days ago

circleci	remove fix node-sass (#1773)	10 months ago
github	add issue template (#1573)	a year ago
assets	Flatten login screen styles (#1912)	6 months ago
cmd	Small cleanup in live query code (#2011)	8 days ago
docs	Update uses of config_tls_refresh to config_refresh in docs (#2009)	9 days ago
examples	Fix errors and clarify docs on config platform overrides (#1855)	9 months ago
frontend	Clarify labels UI (#2012)	8 days ago
server	Small cleanup in live query code (#2011)	8 days ago
tools	Update uses of config_tls_refresh to config_refresh in docs (#2009)	9 days ago
.dockernignore	Add fleetctl to generated Docker images (#1896)	7 months ago
.eslintrc.js	Fix user menu on Firefox (#1542)	2 years ago
.gitignore	Use persistent MySQL for local server, tmpfs MySQL for tests (#1245)	2 years ago

Références



- Sur Slack
 - <https://osquery-slack.herokuapp.com/>
- La documentation (tables, schémas, ...)
 - <https://osquery.readthedocs.io/en/stable/>
- Le projet sur GitHub
 - <https://github.com/facebook/osquery>



Questions ?