osquery queries

context

dit document geeft een overzicht van enkele nuttige queries

gebruikers

gebruikers en hun groepen

```
SELECT usr.username, usr.uid, grp.groupname,grp.gid from users AS usr
LEFT JOIN user_groups AS usrgrp ON usr.uid = usrgrp.uid
JOIN groups AS grp ON grp.gid = usrgrp.gid
ORDER BY usr.username;
```

processen

processen, pid, path en parent

```
SELECT datetime(p.start_time,'unixepoch','localtime') AS 'START TIME',
p.pid AS PID,p.name AS PROCESSNAME, p.path AS PATH,
p.parent AS PPID, p2.name AS 'PROCESSNAME PARENT' FROM processes p
JOIN processes p2 ON p.parent = p2.pid
ORDER BY p.start_time;
```

processen met hash

```
SELECT p.pid,p.name,u.username,p.path,h.sha1 FROM processes p
JOIN hash h ON p.path = h.path
GROUP BY h.sha1
ORDER BY p.pid ASC;
```

Note: GROUP BY zal alle processen met eenzelfde hash samenvoegen.
Je ziet dus niet alle processen, enkel die met unieke hash

processen met hash en user

```
SELECT p.pid,p.name,u.username,p.path,h.sha1 FROM processes p
JOIN hash h ON p.path = h.path
JOIN users u ON u.uid = p.uid
GROUP BY h.sha1
ORDER BY p.pid ASC;
```

boot time

```
SELECT p.pid AS PID, p.parent AS PPID, p.name AS PROCESSNAME,
p.path AS PATH, datetime (start_time, 'unixepoch','localtime') AS STARTTIME
FROM processes p
ORDER BY p.start_time ASC LIMIT 1;
```

laatste 10 actieve processen

```
SELECT p.pid AS PID, p.parent AS PPID, p.name AS PROCESSNAME,
p.path AS PATH, datetime (start_time, 'unixepoch','localtime') AS STARTTIME
FROM processes p
ORDER BY p.start_time DESC LIMIT 10;
```

zoeken op procesnaam (firefox, in dit geval)

```
SELECT proc.pid, proc.name, usr.username, proc.path, proc.parent, proc2.name
FROM processes AS proc
JOIN processes AS proc2 ON proc.parent = proc2.pid
JOIN users AS usr ON proc.uid = usr.uid
WHERE proc.name like '%firefox%';
ORDER BY proc.pid;
```

hashing

```
SELECT path, sha1 from hash
WHERE path = 'padNaarBestand';
```

voorbeeld:

```
SELECT path, sha1 from hash where path IN ('C:\windows\system32\ping.exe',
'C:\windows\system32\cmd.exe');
```

file

timestamps

```
SELECT path, datetime(atime, 'unixepoch','localtime') AS 'Acces time',
datetime(mtime, 'unixepoch','localtime') AS 'Modified time',
datetime(btime, 'unixepoch','localtime') AS 'Created time' from file
WHERE path = 'padNaarBestand';
```

voorbeeld:

```
SELECT path, datetime(atime, 'unixepoch','localtime') AS 'Acces time',
datetime(mtime, 'unixepoch','localtime') AS 'Modified time',
datetime(btime, 'unixepoch','localtime') AS 'Created time' from file
WHERE path is 'C:\Windows\System32\winevt\Logs\system.evtx';
```

alle bestandseigenschappen

```
.mode line
SELECT * from file
WHERE path = 'padNaarBestand';
```

voorbeeld:

```
SELECT * from file
WHERE path = 'C:\windows\system32\cmd.exe';
```

autorun

met target path (in geval van lnk-files)

```
SELECT su.name, su.path, su.args, su.username, sc.local_path, hash.md5 from
startup_items AS su
JOIN hash AS hash ON hash.path = su.path
LEFT JOIN shortcut_files AS sc ON sc.path = su.path
WHERE su.path not like '%desktop.ini%';
```

timestamp

```
 datetime(start_time, 'unixepoch','localtime') AS start_time
```

netwerk verbindingen

met sha1 van process

```
SELECT p.pid, p.name, p.path, h.sha1, os.local_address, os.local_port,
os.remote_address, os.remote_port,
datetime(start_time,'unixepoch','localtime') FROM processes p
JOIN process_open_sockets os ON p.pid = os.pid
LEFT JOIN hash h ON h.path = p.path WHERE os.state = 'ESTABLISHED' AND
os.remote_address NOT LIKE '127.0.0.1'
GROUP BY h.sha1;
```

meer info

osquery

From:
https://louslab.be/ - **Lou's lab**

Permanent link:
https://louslab.be/doku.php?id=osquery:nuttige_queries

Last update: **2024/11/16 18:14**