osquery

osquery is an operating system instrumentation framework for OS X/macOS, Windows, and Linux. The tools make low-level operating system analytics and monitoring both performant and intuitive.

What is osquery?

osquery exposes an operating system as a high-performance relational database. This allows you to write SQL-based queries to explore operating system data. With osquery, SQL tables represent abstract concepts such as running processes, loaded kernel modules, open network connections, browser plugins, hardware events or file hashes.

SQL tables are implemented via a simple plugin and extensions API. A variety of tables already exist and more are being written: https://osquery.io/tables. To best understand the expressiveness that is afforded to you by osquery, consider the following SQL queries:

List the users:
[crayon-6a9d7853305e0623722346/]
Check the processes that have a deleted executable:
[crayon-6a9d7853305e7199482783/]
These queries can be:

- performed on an ad-hoc basis to explore operating system state using the osqueryi shell
- executed via a scheduler to monitor operating system state across a set of hosts
- launched from custom applications using osquery Thrift APIs

Table schema

https://osquery.io/schema/

Downloads / Install

For latest stable builds for OS X (pkg) and Linux (deb/rpm), as well as yum and apt repository information visit https://osquery.io/downloads. Windows 10, 8, Server 2012 and 2016 packages are published to Chocolatey.

The list of supported platforms for **running** osquery is massive:

- Apple OS X 10.10, 10.11, and macOS 10.12
- Any 64bit Linux OS with glibc >= 2.13 and zlib >= 1.2
- Windows 10, 8, Server 2012, and 2016

More information

https://osquery.io/