Автор:
29.10.14 17:29 -

Facebook объявил об открытии исходных текстов проекта osquery , в рамках которого развивается необычный инструмент низкоуровневого мониторинга за состоянием операционной системы. Своеобразность проекта заключается в том, что все отслеживаемые ресурсы отражены в форме виртуальной базы данных, обращение к которой производится через отправку SQL-запросов. Код написан на языке C++ и доступен
под лицензией BSD. Из операционных систем поддерживаются OS X и Linux.

Через SQL-запросы можно достаточно подробно анализировать состояние системы, например, как с SQL-таблицами можно работать со списками выполняемых процессов, загружаемыми модулями ядра, списками пользователей, открытыми сетевыми соединениями, таблицами маршрутизации. Каждый запрос отражает текущее состояние в данный момент времени. Несмотря на том, что в рамках проекта развивается подготовлена подборка готовых ресурсов для мониторинга, при желании можно легко добавлять собственные уровни абстрации с поддержкой новых ресурсов и подключать их в форме плагинов.

SQL-запросы можно передавать через стандартный вход в утилиту osquery или использовать специально подготовленный интерактивный интерфейс командной строки. Синтаксис запросов совместим с SQLite. Для планирования опроса состояния систем на разных хостах подготовлен специальный фоновый процесс osqueryd, который может использоваться для создания распределённой инфраструктуры мониторинга, охватывающей несколько серверов. Кроме опроса текущего состояния разных систем, osqueryd занимается накоплением статистики изменений параметров систем, агрегирует имеющуюся статистику и ведёт лог изменений состояния.

В качестве примера, демонстрирующего удобство предлагаемого подхода, приводится запрос для вывода имён, идентификаторов и прикреплённых портов для всех процессов, слушающих сетевые соединения на указанном сетевом интерфейсе:

```
SELECT DISTINCT process.name, listening.port, process.pid FROM processes AS process JOIN listening_ports AS listening ON process.pid = listening.pid WHERE listening.address = '0.0.0.0';
```

Другой пример, показывает как найти выполняемые процессы, исполняемых файлов которых уже нет в файловой системе (например, для выявления вредоносного ПО):

```
SELECT name, path, pid FROM processes WHERE on_disk = 0;
```

Автор:
29.10.14 17:29 -

Read more http://www.opennet.ru/opennews/art.shtml?num=40964