Изоляция пользователей хостинга с помощью ОС МСВСфера 9

Алексей Бережок
г. Москва
ИНФЕРИТ
Инферит ОС МСВСфера
Alexey.Berezhok@softline.com

Вступление

Обсуждаемая тема касается именно функционирование хостинг-сервера. Что такое хостинг-сервер — это тысячи сайтов, принадлежащих разным пользователям. Каждый пользователь управляет своим сайтом или десятком сайтов. Пользователь не знает как работает сервер, но хочет чтоб его сайт, написанный на PHP или Django, работал корректно и без сбоев и задержек.

И очень часто своими не оптимизированными скриптами пользователи создают проблемы или другим пользователям или администратору сервера. Классический сервер представлен фаерволом, веб-сервером, обработчиком динамического скрипта (PHP, Ruby, Python), базой данных, предоставляет доступ по ssh или ftp к данным пользователя. И наиболее часто клиенты хостинга создают следующие проблемы:

1. т.к. у пользователя не один сайт, а группа сайтов, то многократно возрастает нагрузка на CPU, и выходит, что один активный пользователь потребляет все доступные ядра процессора не оптимизированными PHP скриптами, не давая менее активным шанса получить процессор.
2. пользователь размещая свои данные потребляет большое количество дискового пространства, ущемляя других пользователей.
3. у пользователя большое число крон задач, которые потребляют процессорное время и память. Опять баланс потребления серверных ресурсов на стороне более активного пользователя
4. взломанный один пользователь, при недостаточно настроенной защите на хостинге, может привести к проблемам у других пользователей.
5. некорректная настройка доступа на серверном ПО, позволяет злоумышленнику, используя недостаточно защищенные скрипты владельцев сайтов, получить информацию о сервере, набор установленных программ, список пользователей сервера, список сайтов.
6. форк-бомбы.

Как можно решить данные и другие сопутствующие проблемы? Каждого пользователя с его набором сайтов можно разместить, каждый на своем виртуальном сервере с помощью технологии KVM. Данное решение дает максимальную изоляцию пользователей, но влечет за собой просто тектонические изменения в структуре хостинг сервера, невозможность использовать стандартные контрольные панели, для управления сервером, требует квалифицированных пользователей, которые бы самостоятельно настраивали свой виртуальны сервер. Следующее решение — это использовать докер контейнеры, что дает меньше оверхеда, есть готовые решения в виде той же самой OpenPanel, которая позволит выделить каждому пользователю собственный контейнер с собственным набором программ, но это так же влечет реорганизацию хостинг сервера и перерасход по дисковому пространству и памяти. Еще одно решение — это грамотный администратор или контрольная панель, которая учитывает специфику хостинга и закрывает все возможные недочеты, но это так же непросто, т. к. ошибки контрольной панели или администратора будут дорого стоить.

LS и LimitedFS ОС МСВСферы 9 для хостинга

В ОС МСВСфера 9 для хостинга внедрены сервис лимитирования LS и сервис изоляции файловой системы LimitedFS. Данные сервисы вносят минимальные изменения в структуру существующего серверного ПО.

Сервисы позволяют установить лимиты для CPU, памяти, SWAP-памяти, числа процессов для каждого пользователя. а так же изолировать пользователя с помощью pivot_root, в его

«собственной», настроенной для пользователя файловой системе. Такой изолированный и лимитированный пользователь не потребляет больше CPU чем ему позволено, то же относится к оперативной памяти и числу процессов. Лимитирование использует встроенный в Linux механизм cgroups. Чтоб популярное серверное ПО работало с лимитированием и изоляцией были доработаны либо серверные компоненты, либо отдельные модули(например Apache, PAM модуль, mod_fcgid, httpd-itk, PHP-FPM и т.д.), с помощью которых происходит «погружение» процесса в лимитированную и изолированную среду с помощь API. Процесс погружения в LS можно увидеть на рисунке 1 (где klsd – это сервис лимитирования, помещающий процесс в LS контейнер):

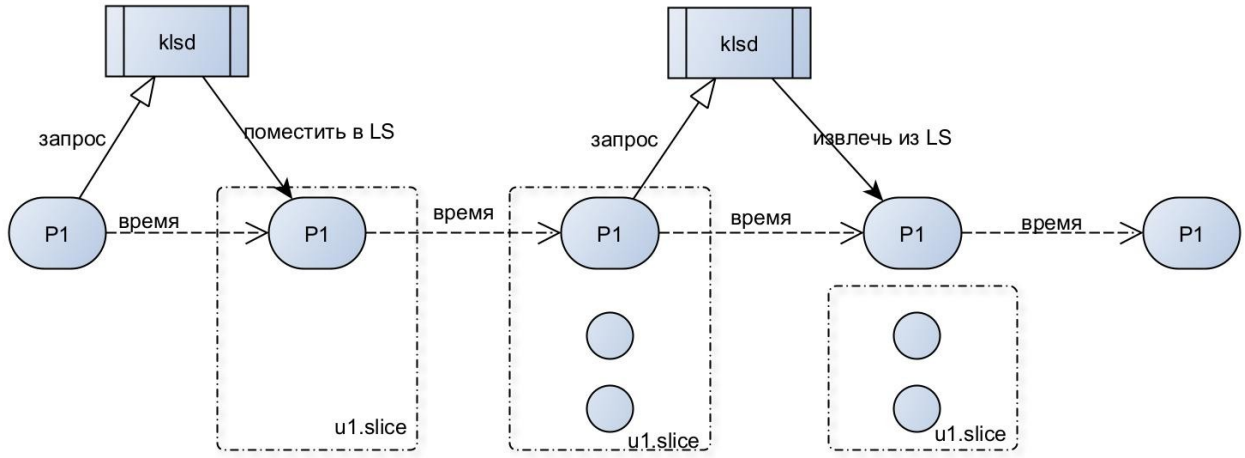

Рисунок 1

Изоляция же файловой системы представляет собой подготовленный «скелет» файловой системы с примонтированными и подготовленными заранее каталогами, специфичными для каждого пользователя. При запросе изоляции процессом, у него меняется корень файловой системы на этот настроенный «скелет». Пользователь видит только свои специфичные данные, настроенные администратором и файловую систему по большей степени работающую в RO-режиме.

Чем же данный подход удобнее для хостинг провайдеров, чем описанные ранее: виртуальный сервер, докер контейнера, вообще система без изоляции, где все сделано только силами контрольной панели или администратора?

Главные плюсы:

• это легкость интеграции с существующим хостингом, с контрольными панелями. минимальные усилия по переходу на использование изоляции от МСВСфера

• легкость настройки, в основном все минимально необходимые конфигурации уже включены в установку по умолчанию.

• минимальный оверхед

• потребление памяти аналогично, как если используется только Apache/nginx и PHP

• простота интеграции с сервисами поддерживающими PAM.

Но имеются так же и минусы:

• изоляция менее надежная чем докер и виртуальный сервер

• не все сервисы могут быть таким образом изолированы

• бОльшая связь с реальной системой, например нельзя скрыть от пользователя число ядер или название процессора.