УДК 004.896

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ eBPF ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ МОНИТОРИНГА, БЕЗОПАСНОСТИ И ПРОИЗВОДИТЕЛЬНОСТИ ПАК И УПРАВЛЕНИЯ БЕЗ ИЗМЕНЕНИЯ ЯДРА ОС

Злобин А. С.[1]
Научный руководитель – Аристов К. М.[1]
[1]Университет ИТМО

Введение

В современном мире, независимо от отрасли, ощутимая часть бизнес процессов зависит от цифровой инфраструктуры. В основе такой инфраструктуры стоят программно-аппаратные комплексы (ПАК). Такие системы должны обладать детерминированностью, предсказуемостью и соответствовать требованиям безопасности. Поэтому для них мониторинг поведения должен быть не внешним инструментом, а изначально встроенным механизмом верификации поведения.

Большинство существующих инструментов мониторинга обладают рядом компромиссов. Использование средств трассировки системных вызовов (например strace, ptrace) приводит к дополнительным переключениям контекста и увеличивает накладные расходы из-за остановок процессов на входе и выходе из системных вызовов. Использование инструментов top, sar и им подобных позволяет наблюдать лишь уже существующую статистику ядра. Разработка собственных модулей ядра потенциально позволяет минимизировать накладные расходы и получить полный доступ к происходящим в ядре событиям, однако сопряжена с рисками нарушения стабильности системы вследствие ошибок в коде и сложностей отладки. Этих недостатков лишена технология eBPF (Extended Berkeley Packet Filter) [1], которая представляет собой встроенную в ядро виртуальную машину. Она позволяет выполнять пользовательские программы в пространстве ядра и как следствие выполнять трассировку и анализ событий с минимальными накладными расходами.

Основная часть

Работа посвящена разработке системы мониторинга базы данных PostgreSQL для выявления и классификации её аномального поведения. С помощью eBPF реализован сбор статистики системных вызовов процессов PostgreSQL. В результате формируется временной ряд, отражающий взаимодействие СУБД с ядром операционной системы.

Для обнаружения аномального поведения используются две модели. Первая - сочетание вариационного автоэнкодера и изоляционного леса, обученного на векторах латентного представления, формируемого автоэнкодером [2]. Эта модель используется для обнаружения как известных, так и ранее не встречавшихся типов аномалий. Для классификации известных типов аномалий применяется вторая моедль - LSTM с механизмом внимания, позволяющая выявлять характерные паттерны деградации производительности, блокировок и иных нарушений [3].

Выводы

Результаты работы демонстрируют, что применение eBPF позволяет построить эффективную и безопасную систему мониторинга ПАК без модификации ядра операционной системы, объединяющее низкоуровневую телеметрию и методы анализа

временных рядов, обеспечивая высокую чувствительность к изменениям состояния системы при минимальном влиянии на ее производительность.

Литература

1. FedMon: Federated eBPF Monitoring for Distributed Anomaly Detection in Multi-Cluster Cloud Environments // arxiv URL: https://arxiv.org/pdf/2510.10126
2. Liz Rice Learning eBPF: Programming the Linux Kernel for Enhanced Observability, Networking, and Security. - O'Reilly, 2023
3. On Improving Deep Learning Trace Analysis with System Call Arguments // arxiv URL: https://arxiv.org/pdf/2103.06915