АНАЛИЗ И ПРОГНОЗИРОВАНИЕ ИНЦИДЕНТОВ НА БАЗЕ СОБРАННОЙ ИНФОРМАЦИИ СИСТЕМАМИ МОНИТОРИНГА

Коледа К.В.

Институт информационных технологий БГУИР,
г. Минск, Республика Беларусь

Скудняков Ю.А.– доцент каф. ПЭ, к.т.н,, доцент

В данной работе рассматривается возможность прогнозирования инцидентов на базе информации и метрик, собранных различными системами мониторинга и хранящими данные в явном виде в СУБД. Для расчета возможных событий используются различные функции аппроксимации.

В двадцать первом веке - веке высоких информационных технологий и глобальных бизнесов крайне важно

заранее обнаружить проблему и как можно раньше решить ее, не дожидаясь пока проблема перерастет в инцидент. Любое приложение или система должны находиться под постоянным наблюдение и предоставлять полную информацию о работе и метриках всех систем в реальном времени обслуживающей команде.

На сегодняшний день существует большое количество различных систем, позволяющих собирать большое количество метрик о любой системе, будь то мобильное приложение, веб-сайт или распределенная система с тысячами серверов. Яркие примеры таких систем App Dynamics, Munin,

Graphiteи Nagios. Данные системы мониторинга отлично справляются со сбором и хранением различных метрик систем, но ни одна из них не может спрогнозировать инцидент. Так как большинство систем мониторинга хранят различные метрики, так называемые исторические данные, в явном виде в СУБД, то данные можно извлечь для анализа и прогнозирования проблемы. Необходимо понимать две вещи: как описать состояние проблемы и сколько необходимо времени, чтобы предпринять меры. Далее есть несколько способов создать событие, сигнализирующее о возможно нежелательной ситуации. Первый: триггер должен “загореться”, когда система после “пора действовать”, как ожидается, будет в состоянии проблемы. Второй: триггер должен “загореться”, если система перейдет в состояние проблемы за время меньше, чем “пора действовать”. Прежде всего необходимо указать период истории, который следует проанализировать для составления прогноза [1].

Большинство событий, как показала практика, могут быть рассчитаны линейной функцией, для более сложных вычислений можно использовать следующие функции аппроксимации (таблица 1).

Таблица 1 – Функции линии тренда

аппроксимация	x = f(t)
линейная (linear)	$x = a + b*t$
полином (polynomialN)	$x = a_0 + a_1*t + a_2*t^2 + \ldots + a_n*t^n$
экспоненциальная (exponential)	$x = a*\exp(b*t)$
логарифмическая (logarithmic)	$x = a + b*\log(t)$
степенная (power)	$x = a*t^b$

Использование таких математических функций всегда связано с возможностью возникновения ошибок и неверных расчетов в следующих случаях:

– Заданный период не содержит данных.

– Математическая операция не задана. Например, построение экспоненциальной и степенной функций требует логарифмических вычислений значений элемента данных. Если данные содержат нулевые или отрицательные числа, то формируется сообщение об ошибке, поскольку вычисление логарифма возможно только при положительных значениях.

– Сложность вычислений. Требуемый расчет для некоторых наборов входных данных диапазона и точности формата чисел с плавающей точкой двойной точности становится недостаточным.

Список использованных источников:

1.Прогнозирующие функции триггеров [Электронный ресурс]. – Режим доступа: https://www.zabbix.com/ documentation/ 3.0 /ru/manual/config/triggers/prediction.– Дата доступа: 20.02.2019.