Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.021:004.7

Коледа
Кирилл Викторович

Алгоритмы прогнозирования инцидентов на базе системы мониторинга zabbix

АВТОРЕФЕРАТ

на соискание степени магистра информатики и вычислительной техники по специальности 1-40 81 02 Технологии виртуализации и облачных вычислений

Научный руководитель
Скудняков Юрий Александрович
кандидат технических наук, доцент

Минск 2019

ВВЕДЕНИЕ

В век информационных технологий инфраструктура любого современного предприятия представляется собой сложный конгломерат различных технологий, мощнейших серверов о которых раньше, можно было только мечтать. Сегодня сложно представить компанию или предприятие, которое бы не использовало в своей работе сетей или компьютеров, современный бизнес — это огромные массивы данных, моментальный доступ к абсолютно любой информации в любой точке мира.

Все понимают, что сейчас в условиях возрастающих информационных полей, уже невозможно использовать «разбросанные» технологии так как каждая минута простоя предприятия из-за сбоев в работе сети приводит к весьма ощутимым денежным потерям и что более важно испорченному имиджу.

Результатом эволюции вычислительных технологий стали компьютерные сети.

Компьютерная сеть - сложнейший комплекс согласованных и взаимосвязанных аппаратных и программных компонентов.

Программно-аппаратный комплекс может быть описан многоуровневой моделью. Это стандартная модель абсолютно любой сети. В ее основе на первом уровне находится аппаратный слой, включающий в себя компьютерную технику различных классов. Данные компьютеры должны соответствовать поставленным задачам, которые будет решать сеть.

На втором слое находится разнообразное сетевое оборудование, для создание локальной сети, коммуникационное оборудование для связи как с распределёнными корпоративными сетями, так и с внешней сетью – Интернет.

Третий слой — это операционные системы, которые являются программной основой сети. Во время строительства сетевой инфраструктуры очень важно учитывать совместимость различных операционных систем и понимать насколько она может обеспечить защиту и безопасность данных.

Верхним слоем сетевых средств являются всевозможные приложения работы с сетью, такие как почтовые системы и сетевые базы данных, средства копирования информации и другое. Важно обратить внимание на совместимость программ во время совместной работы.

В настоящее время внедрение вычислительных сетей даёт предприятия многочисленные возможности и огромное преимущество перед конкурентами. Главным итогом использования вычислительных сетей на предприятии является повышение эффективности работы, моментальный обмен информацией, внедрение всех филиалов, даже самых удаленных в общую инфраструктуру предприятия, что в свою очередь повлечет увеличение прибыли. Если же постараться рассмотреть внедрение ЛВС в работу предприятия более глубоко, то из этого вытекают еще больше преимуществ. Например, это совместное использование сетевых устройств, таких, как принтеры, факсы, сканеры.

Со временем сетевая инфраструктура предприятия разрастается и становится сложнее чем это представлялось в начале и на помощь системным администраторам и инженерам приходят различные системы мониторинга за состоянием сетей, сетевой инфраструктуры и серверного оборудования.

В данном магистерском проекте будет рассмотрена возможность прогнозирования инцидентов на базе метрик и данных, собранных системой мониторинга хранящей данные в явном виде в реляционной СУБД.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с научными программами (проектами) и темами

Тема диссертации соответствует приоритетным направлениям фундаментальных и прикладных исследований в области автоматизации производственных процессов.

Цель и задачи исследования

Миром сегодня управляет глобализация, компании укрупняются, становясь огромными конгломератами. Сложно представить хоть одну крупную компанию, которая была бы не заинтересована в мониторинге, как средстве наблюдения за процессами, происходящими в инфраструктуре предприятия, а тем более прогнозировании инцидентов что влечет за собой уменьшение издержек как для бизнеса, так и повышение качества предоставляемых услуг.

Целью магистерской диссертации является описание, применение алгоритмов прогнозирования инцидентов и создание локальной вычислительной сети.

Были поставлены следующие задачи:

1. Исследование существующих систем комплексного мониторинга инфраструктуры.
2. Исследование наиболее подходящей технологии построения сети и инфраструктуры в целом.
3. Исследование нескольких аппроксимаций и выбор наилучшей линии тренда для данных
4. Разработка и исследование алгоритмов прогнозирования на базе метрик выбранной системы мониторинга.

Положения, выносимые на защиту

1. Сравнительный анализ особенностей функционирования систем комплексного мониторинга, представленных на рынке, их обзор и выбор наиболее подходящей.
2. Локальная вычислительная сеть, построенная для предприятия и позволившая объединить большое число филиалов в Великобритании.
3. Алгоритмы прогнозирования инцидентов на основе метрик собранной системой комплексного мониторинга, выбранной в этой

диссертации. Разработка выполнена с учетом существующих паттернов проектирования, позволяющих изменять и поддерживать в дальнейшем актуальную рабочую версию.

Личный вклад соискателя

Личный вклад заключается в построении локальной вычислительной сети для предприятия, исследовании и выборе наиболее подходящей под параметры организации системы комплексного мониторинга и разработке алгоритмов прогнозирования инцидентов на базе выбранных функций аппроксимации и интеграции в систему мониторинга.

Апробация результатов диссертации

Результаты исследований, включённые в диссертацию, были представлены на 55-ой научной конференции аспирантов, магистрантов и студентов, которая проводилась в 2019 году в БГУИР. Результаты работы, опробованы на предприятии в мае 2019 года на реальных данных.

Структура и объём диссертации

Введение диссертации содержит постановку задачи и основные этапы выполнения работы.

В главе 1 приводятся результаты исследования и делается анализ особенностей существующих систем комплексного мониторинга инфраструктуры.

В главе 2 дается анализ структуры предприятия, на котором внедряется система мониторинга и для которой разрабатываются алгоритмы прогнозирования инцидентов на базе метрик, собранных системой комплексного мониторинга.

В главе 3 приводится общая структура функционально проектируемой серверной и локальной вычислительной сети компании.

В главе 4 описывается проект структурированной кабельной системы и системы комплексного мониторинга.

В главе 5 приводится описание процесса разработки алгоритмов прогнозирования инцидентов на базе метрик, собранных системой мониторинга.

ЗАКЛЮЧЕНИЕ

В данной работе были описаны и разработаны алгоритмы прогнозирования инцидентов с использованием программного комплекса с открытым исходным кодом Zabbix, а также полностью внедрен комплекс системы мониторинга.

В результате реализации проекта были описаны модели, а также рассмотрены различные ситуации использования прогнозных моделей, разобраны различные случаи применения, что доказало свою эффективность в предотвращении инцидентов и уменьшении времени простоя компании, а также улучшение финансовых показателей и имиджа компании клиента ИООО «ЭПАМ СИСТЕМЗ» в целом.

Разработка проекта велась в соответствии с международными стандартами, описанные функции аппроксимации и конфигурации являются удобными в настройке, установке и эксплуатации. Оборудование, используемое в построении сети, является надежным и удобным в эксплуатации, легко заменяемым и доступным.

В результате использования технологии DMVPN мы получили защищенные каналы связи между филиалами компании, что в свою очередь позволяет централизованно обслуживать все серверное оборудование, находящиеся в различных филиалах и обеспечивает целостность и конфиденциальность передаваемой информации.

Внедрение технологии мониторинга на базе программного обеспечения, поставляемого компанией Zabbix позволило увидеть все узкие места сети, знать о возникающих проблемах в сети и на серверах до того момента как они стали критическими для бизнеса, простой критически важных узлов и систем уменьшился в несколько раз. С внедрением системы мониторинга все администраторы стали получать e-mail уведомления и push уведомления на свои мобильные устройства о проблемах, требующих внимания. В результате работа отдела изменилась с решения сбоев в работе, на упреждение возникающих угроз.

Внедренный в данной магистерской работе ряд инноваций в полной мере обеспечивает выполнение основных функций распределенной системы – обеспечение постоянной работы, высокой доступности и конфиденциальности передаваемой информации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Коледа К.В. Алгоритмы прогнозирования инцидентов на базе метрик, собранных системой мониторинга // Интернаука: научный журнал. № 19(101). – М., Изд. «Интернаука», 2019.
2. Коледа К.В Анализ и прогнозирование инцидентов на базе информации, собранной системами мониторинга: Тезисы докл. к 55-я юбилейная научная конференция аспирантов, магистрантов и студентов БГУИР.