М.Г. Дубровин

Тюменский государственный университет, г. Тюмень

УДК 004.052.2

КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ СИСТЕМЫ ПРОАКТИВНОГО МОНИТОРИНГА ИТ-СИСТЕМ

Аннотация. В работе предложена общая архитектура системы проактивного мониторинга ИТ-систем, позволяющая анализировать состояние компонентов ИТ-системы в режиме реального времени, а также прогнозировать и реагировать на возможные инциденты в работоспособности. На основе предложенной архитектуры и внешних по отношению к системе объектов представлена концептуальная модель системы проактивного мониторинга.

Ключевые слова: проактивный мониторинг, ИТ-система, архитектура системы, концептуальная модель.

Введение

По мере развития информационных систем организаций ИТ-инфраструктура любой компании становится все более сложной, разнообразной и приобретает распределенный характер. Для обеспечения работоспособности ИТ-системы организаций применяются различные автоматизированные системы мониторинга, заключающиеся в постоянном наблюдении и периодическом анализе объектов системы, с отслеживанием динамики происходящих с ними изменений. Высокая стоимость ИТ-систем и значительные потери от простоев, вызванных сбоями в подобных системах, обуславливают практическую актуальность поиска новых подходов к мониторингу.

Кроме того, задача поиска новых подходов к мониторингу представляет научный интерес, который обусловлен необходимостью создания моделей функционирования компонентов ИТ-системы, разработки методов и моделей

обнаружения, локализации и прогнозирования неисправностей и других трудоемких задач.

Современный подход к мониторингу предполагает использование систем проактивного мониторинга, которые не только обеспечивают мониторинг объектов в режиме реального времени, но и позволяют прогнозировать критическое состояние системы на ранней стадии, а так же генерировать предупреждения об ошибках, для того, чтобы предотвратить возникновение отказов в работе ИТ-системы. Такой подход к мониторингу обеспечивает более стабильную работу ИТ-системы, и позволяет минимизировать издержки, вызванные с ее незапланированным простоем. [1]

Архитектура системы

В процессе построения архитектуры проактивного мониторинга рассмотрены некоторые существующие подходы к реализации и выделению компонентов архитектуры мониторинга различных компонентов ИТ-инфраструктуры. В [2] предложена общая архитектура системы проактивного мониторинга выполнения политик безопасности, построенная с помощью декомпозиции процесса мониторинга. Данная система является узконаправленной и не применима для задач оценки работоспособности объектов ИТ-инфраструктуры. В работах [3,4] предложены архитектуры систем мониторинга информационно-вычислительных комплексов, но в них не рассматриваются модули прогнозирования возможных инцидентов. В статьях [5,6] описаны архитектуры мониторинга серверов и сервисов локальных сетей. Предложенные организации системы предназначены для сбора данных и отображения информации о текущем состоянии ИТ-инфраструктуры, но не затрагивают вопросы реагирования и прогнозирования аварийных ситуаций, которые являются неотъемлемыми компонентами полноценного мониторинга.

На основе декомпозиции процесса проактивного мониторинга и рассмотренных источников предложена обобщенная системы проактивного мониторинга, состоящая из следующих подсистем.

1. Подсистема сбора данных

На первом этапе осуществляет опрос объектов мониторинга с заданными временными интервалами для получения значений исследуемых параметров этих объектов, загрузку и консолидацию данных. Под объектом мониторинга понимается аппаратное или программное устройство ИТ-инфраструктуры, за которым осуществляется регулярное наблюдение с целью контроля его состояния [7]. Опрос объектов мониторинга производится с помощью агентов. Агент запускается в виде отдельного сервиса, специализирующегося на выполнении индивидуального набора функций мониторинга и управления, конфигурируемых в зависимости от задач, решаемых агентом и свойств объекта, которого он обслуживает. Полученные статистические данные передаются в подсистему хранения данных.

2. Подсистема хранения данных

Подсистема хранения осуществляет накопление, хранение и архивацию данных о результатах проверок. Осуществляет разделение данных на блоки для оперативной обработки и для интеллектуального анализа данных. Включает так же сформированную базу знаний произошедших инцидентов. Статистические данные и база знаний хранятся в базе данных, основанной на одной из современных СУБД.

3. Подсистема обработки и анализа

Подсистема хранения взаимодействует с подсистемой обработки и анализа, функционал которой описана далее. В процессе мониторинга объекта значения контролируемых параметров регистрируются через определенные промежутки времени. Обработанные данные сравниваются с заложенными пороговыми значениями метрик, в результате чего формируется выходная информация о работоспособности объекта. Для каждого объекта мониторинга необходимо определить пороговые значения метрик. Современный подход предполагает использование «динамических порогов». Для выявления пороговых значений необходимо периодическое выполнение сбора

статистической информации о показателях нормального состояния объекта. Отклонения показателей нормальной работы должны приводить к обучению подсистемы и переопределению пороговых значений.

Изменение состояние объекта, которое вышло за пределы порогов передается в подсистему генерации решений. Колебание состояния в зоне порога вызывает большое количество срабатываний механизма передачи данных о новом состоянии в модуль генерации решений, который в свою очередь будет запускать процедуры реакции на новое состояние и выработку управляющих решений. Подобная ситуация может привести к чрезмерной загруженности канала связи и перезагрузки программного обеспечения подсистемы генерации решений [8]. Поэтому современный подход к обнаружению неисправностей предполагает использование фильтрации при выявлении параметров объектов, вышедших за пороговые значения. Подсистема анализа должна игнорировать краткосрочное превышение порогов и реагировать на возможные инциденты, только если состояние объекта находится выше порогового в течение заданного времени.

4. Подсистема проактивного прогнозирования

Четвертым блоком системы является подсистема проактивного прогнозирования. Значения контролируемых параметров образуют систему взаимосвязанных временных рядов. При прогнозировании временного ряда требуется определить функциональную зависимость, адекватно описывающую временной ряд. Для корректного прогнозирования состояния ИТ-системы, необходимо использовать не только фактические значения исследуемого ряда, но и значения набора внешних факторов, влияющие в определенной мере на формирование прогноза. Внешними факторами, например, могут служить: время, день недели, рабочий/выходной/праздничный день. Такие признаки могут быть использованы в качестве внешних факторов, поскольку известно их значение в момент прогноза, а значит, есть возможность учесть эти значения в модели прогнозирования [9].

5. Подсистема генерации решений

Подсистема генерации решений вызывает совершение определенного порядка действий при выявлении неработоспособного состояния объекта мониторинга или других значимых изменений состояния объекта. В качестве возможных действий является: уведомление лиц, ответственных за функционирование проверяемых объектов; сохранение информации об инциденте в базу знаний системы; вывод информации в подсистему визуализации; генерация планов восстановления функционирования объекта.

6. Подсистема визуализации и отчетности

Подсистема визуализации и отчетности предполагает представление интерактивных, настраиваемых панелей отображения информации о текущем и прогнозируемом уровне использования ресурсов ИТ-системы в разрезе, как ее отдельных элементов, так и системы в совокупности. Подразумевает возможность создания отчетности по текущей загрузке системе, истории инцидентов и составленных прогнозах в удобной для пользователя форме.

Концептуальная модель системы

Для реализации концептуальной модели необходимо выделить внешние по отношению к системе мониторинга объекты, с которыми она должна взаимодействовать:

- Объекты мониторинга;
- Система хранения данных (СУБД);
- Администраторы ИТ-систем.

На основе архитектуры системы и выявления внешних объектов представлена концептуальная модель разрабатываемой системы (Рис. 1).

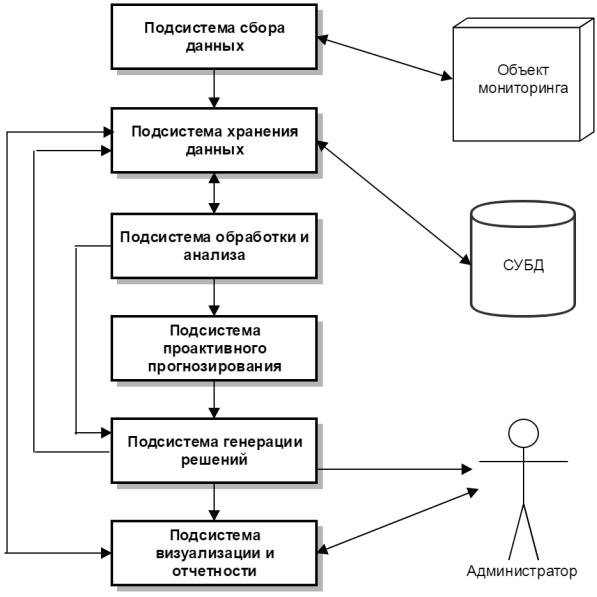

Рис. 4. Концептуальная модель системы проактивного мониторинга

Подсистема сбора данных опрашивает объекты мониторинга и передает данные в подсистему хранения. Подсистема хранения сохраняет данные в необходимом формате в базу данных, которая связана с СУБД. Подсистема обработки и анализа взаимодействует с подсистемой хранения для сбора данных необходимых для выявления инцидентов. Подсистема проактивного мониторинга получает представленные в необходимом формате данные, которые используются для прогнозирования дальнейшего состояния ИТ-системы. Возможные инциденты обрабатываются системой генерации решений и сохраняются в базе знаний инцидентов. Администратор системы получает уведомление об инцидентах от системы генерации решений либо с помощью подсистемы визуализации.

Заключение

В работе представлена концептуальная модель системы проактивного мониторинга ИТ-систем. Для реализации концептуальной модели описаны компоненты архитектуры рассматриваемой системы и выделены внешние по отношению к системе объекты.

СПИСОК ЛИТЕРАТУРЫ

1. Дубровин М.Г. Глухих И.Н. Модели и методы проактивного мониторинга ИТ-систем // Моделирование, оптимизация и информационные технологии. – 2018. – Т.6 – № 1 URL: https://moit.vivt.ru/wp-content/uploads/2018/01/DubrovinGluhih_1_1_18.pdf (Дата обращения: 09.04.2018).

2. Богданов В. С. и др. Архитектура, модели и методики функционирования системы проактивного мониторинга выполнения политики безопасности //Труды СПИИРАН. – 2006. – Т. 2. – №. 3. – С. 50-69.

3. Кореньков В. В., Мицын В. В., Дмитриенко П. В. Архитектура системы мониторинга центрального информационно-вычислительного комплекса ОИЯИ //Информационные технологии и вычислительные системы. – 2012. – №. 3. – С. 31-42.

4. Тарасов А. Г. Трехуровневая система мониторинга расширенной функциональности //Параллельные вычислительные технологии. Челябинск. – 2008. – С. 464-469.

5. Опрышко А. В. Архитектура автоматизированной системы мониторинга серверов и сервисов компьютерной сети //Молодежный научно-технический вестник. – 2015. – №. 8. – С. 15-15.

6. Мищенко Д. А., Железнов Д. И. Архитектура системы мониторинга событий информационной безопасности в локальной вычислительной сети //Аллея науки. – 2017. – Т. 1. – №. 10. – С. 805-809.

7. Воронин В. В., Давыдов О. А. Система мониторинга технического состояния локальной вычислительной сети //Ученые заметки ТОГУ. – 2013. – Т. 4. – №. 4. – С. 805-810.

8. Ролик А.И., Тимофеева Ю.С., Турский Н.И. Управление устранением неисправностей в ИТ-системах // Вестник НТУУ «КПИ». Информатика, управление и вычислительная техника. – 2008. № 49. С. 95-108

9. Артамонов Ю. С. Основные подходы прогнозирования доступных вычислительных ресурсов в кластерных системах //Перспективные информационные технологии (ПИТ 2014): труды Международной научно-технической конференции. – 2014. – С. 305.