Формирование рабочих сценариев при мониторинге динамической компьютерной сети

М. И. Авилов[1], Ю. А. Шичкина[2]
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)
[1]avilovmaxim@gmail.com, [2]strange.y@mail.ru

***Аннотация*. Рассматриваются проблемы своевременного выявления и оперативного реагирования на аномалии в работе компьютерной сети. В случаях, когда проактивный мониторинг КС не может быть применен, а сценариев для реактивного мониторинга компьютерной сети нет, то необходимо сформировать рабочие сценарии, позволяющие воздействовать на возникшую аномалию. Такие сценарии могут быть применены как для статической, так и для динамической компьютерной сети в автоматическом режиме, если аномалия в работе сети повторится.**

Ключевые слова: компьютерная сеть, мониторинг компьютерной сети, интернет вещей

I. Введение

Интернет вещей (IoT – Internet of Things) активно развивается в современном мире [1–2]. Устройства в IoT взаимодействуют через компьютерную сеть (КС) [3], за состоянием которой необходимо постоянное наблюдение. Чем больше сеть с различными сетевыми устройствами, тем сложнее происходит наблюдение в ручном режиме, поэтому применяются системы сетевого мониторинга компьютерной сети. Такие системы играют важную роль в обеспечении работоспособности этих сетей IoT. Применяя системы сетевого мониторинга компьютерной сети, обеспечивается видимость производительности сетей IoT, что позволяет быстро выявлять потенциальные проблемы до того, как они станут критическими. Например, системы мониторинга функционирования КС позволяют отслеживать использования сетевых ресурсов, различных событий в сети, элементов операционной системы хостов, доступность сетевых устройство и другие составляющие компьютерной сети [4].

Сами сети можно разделить на статические и динамические компьютерные сети. Под статическими компьютерными сетями понимаются сети, в которых количество наблюдаемых узлов не изменяется. Под динамическими же понимаются КС, где количество наблюдаемых сетевых узлов периодически изменяется.

В таком смысле статические компьютерные сети являются частным случаем динамических КС, поэтому в данной работе акцент делается на последних.

В случаях возникновения аномалий в работе КС, когда осуществлять проактивный мониторинг сети нет возможности, из-за недостаточного количества собранных данных, и реактивной мониторинг сети по заранее прописанным сценариям нельзя провести, то необходимо осуществлять дополнительную диагностику работы КС и формировать рабочие сценарии. Под рабочими сценариями понимается совокупность зафиксированных условий, возникшей ситуации, и вспомогательный инструмент, при помощи которого состояние наблюдаемого узла возвращается в состояние, являющейся нормой.

II. Обзор существующих решений и постановка задачи

Существует много различных систем мониторинга элементов компьютерной сети [5–6].

Nagios [7] – система мониторинга компьютерных систем и сетей, которая позволяет осуществлять наблюдение за вычислительными узлами, службами и оповещать системного инженера в случае возникновения проблемной ситуации. Сбор данных может осуществляться по протоколам SMTP, HTTP, SNMP, ICMP, POP3 и другим. Также возможна поддержка удаленного мониторинга при помощи шифровании туннелей SSL или SSH.

Zabbix [8] – средство мониторинга КС и компьютерах систем, которое может осуществлять отслеживание за динамикой состояния сетевого оборудования. Эта система может проводить периодический опрос наблюдаемых узлов и собирать данных по SNMP, ICMP, IPMI или через zabbix-агентов. Для распределениянагрузки на сервер мониторинга может быть использован zabbix-прокси, позволяющий осуществлять часть сбора данных с наблюдаемых узлов.

Cacti [7] – система мониторинга КС, которая позволяет строить графики с помощью RRDtool на основе собранных статистических данных. Применяются различных шаблоны для сбора нагрузки на процессор, ОЗУ, каналы передачи данных. Также эта система позволяет осуществить разделение прав доступа для просмотра графиков и есть возможность применения скриптов для отдельного специфического сбора данных с наблюдаемых узлов.

SCOM (System Center Operations Manager) [6] – система компании Microsoft, позволяющая осуществлять мониторинга и управление различными сетевыми узлами, которые поддерживают протокол SNMP. Также существует возможность собирать данные при помощи специальных агентов, установленных на наблюдаемые компьютеры, сервера. Однако стоит отметить, что система может работать нестабильно, если операционная система отлично от семейства Windows.

Кроме этого существует связка Grafana с Prometeus [9]. Такая связка позволяет собирать данные при помощи при помощи компонента «exporters», передавать их Prometeus, сохранять данные в базу данных временных рядов и обрабатывать уведомления о возникающих

ситуациях при помощи компонента «Alertmanager». Существует множество различных экспортеров для сбора данных о состоянии наблюдаемых узлов. Grafana же позволяет визуализировать собранные данные в виде графиков.

Системы поддержки операций [10] представляют собой набор специальных компьютерных программ, которые позволяют поставщикам анализировать, отслеживать, контролировать телекоммуникационные сети.

Также в качестве систем мониторинга КС могу использоваться системы логирования [11]. Например, Graylog, стеки ELK, EFK [13]. В случаях применения таких систем, наблюдаемые узлы отправляют журналы с логами серверу логирования, а дальше системы логирования событий КС анализирует поступившую информацию и осуществляет уведомления системного инженера, если по шаблону найдено отклонение в журнале наблюдаемого узла.

Кроме этого существуют MonPaas решения [12], которые объединяют несколько систем мониторинга сетей, тем самым создавая платформы адаптивного мониторинга КС. Такое решение совмещает в себе системы Nagios и OpenStack, позволяя осуществлять мониторинга за различными сетевыми узлами и разворачивать саму систему в облачной инфраструктуре.

Также существуют различные инженерные практики, основанные на ITIL [13], ITSM [14], SRE[15], которые нацелены на поддержку безотказности и надежности работы элементов сетевой инфраструктуры. Благодаря сформированным методологиям, практикам можно организовать взаимодействия разных практик с аспектами мониторинга и реагирования на инциденты в функционировании сетевой инфраструктуры.

На основе выше изложенного следует, что существует множество различных решений для мониторинга состояния компьютерной сети, однако реакции основываются на собранных статистических данных или происходят по заранее заложенным шаблонам реагирования на ситуации. В случая выявления аномалий в работе КС происходит лишь уведомления системных инженеров.

Целью данного исследования являлась оценка возможностей создания рабочих сценариев в автоматическом режиме, в случае выявления аномалий в функционировании динамической компьютерной сети. Для этого был разработан метод формирования рабочих сценариев при дополнительной диагностики аномалий в работе компьютерной сети.

Данное исследование основывалось на полученных результатах в работе [16].

III. Формирование рабочих сценариев при дополнительной диагностике аномалий в работе компьютерной сети

В случаях необходимости проведения дополнительной диагностики (ДД) аномалий в работе компьютерной динамической сети происходит попытка формирования рабочего сценария и записи его в соответствующую базу данных. Такой процесс отражен на рис. 1.

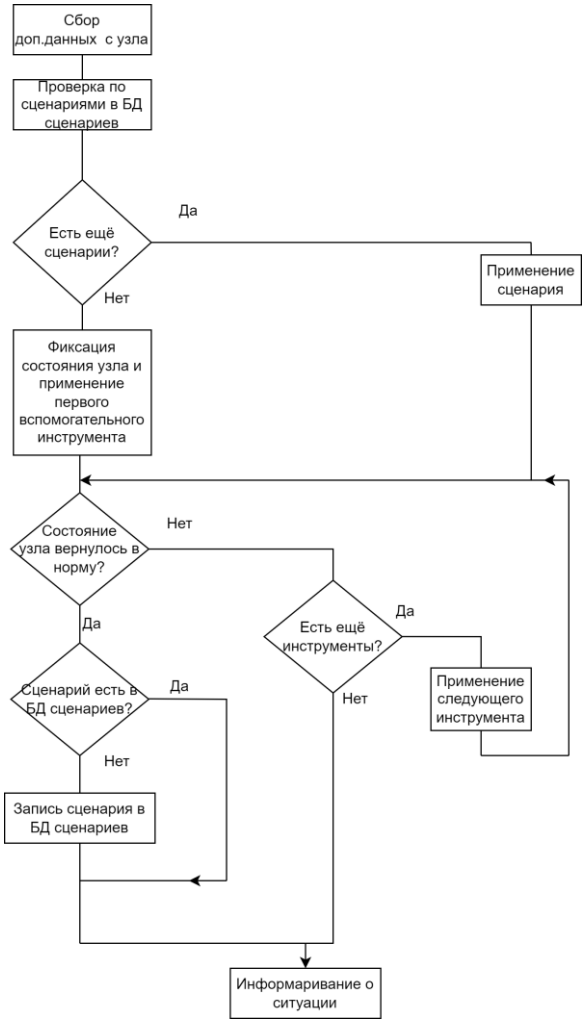

Рис. 1. Процесс записи рабочего сценария в базу сценариев

Сначала происходит дополнительный сбор данных с соответствующих наблюдаемых узлов. Далее проверка на существование сценариев по имеющимся условиям. Если нет, то проверяются вспомогательные инструменты. Если по результатам применения вспомогательного инструмента состояние наблюдаемого узла вернулось в норму, то сценарий фиксируется как рабочий и записывается в базу сценариев.

Сама же структура рабочего сценария представлена на рис. 2, где стрелками показан процесс обработки сценария.

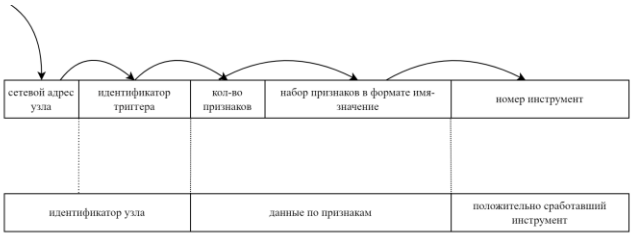

Рис. 2. Структура рабочего сценария

Сначала фиксируется идентификатор узла, в отношении которого будет осуществляться воздействие вспомогательного инструмента диагностики КС. Далее данные по признакам и положительно сработавший вспомогательный инструмента диагностики КС. Сам идентификатор узла состоит из сетевого адреса и

идентификатора триггера, значение которого отражает состояние наблюдаемого узла. Данные по признакам состоят их количества признаков и набора значений признаков. После идет номер положительно сработавшего вспомогательного инструмента диагностики компьютерной сети.

Сам же ***метод формирования рабочих сценариев при дополнительной диагностики аномалий в работе компьютерной сети*** выглядит следующим образом:

Шаг 1. Из множества идентификаторов выбирается идентификатор, соответствующий проблемному узлу:

$$F = \{ f_1, .., f_o \},$$

где f_o – идентификатор узла, o – максимальное количество идентификаторов.

Уточнение: Множество узлов было сформировано при кластеризации, описанной в работе [18].

Шаг 2. Из имеющихся вспомогательных инструментов формируется множество таких инструментов:

$$G = \{ g_1, .., g_q \},$$

где G – множество вспомогательных инструментов для проведения дополнительной диагностики аномалии узла, g – вспомогательный инструмент, q – максимальное количество выбранных инструментов.

Уточнение: перечень вспомогательных инструментов формирует системный инженер.

Шаг 3. Формируем множество признаков, отражающее состояние наблюдаемого узла:

$$T = \{ t_1, .., t_w \},$$

где T – множество признаков, w – максимальное количество признаков, отражающих состояние узла.

Уточнение: перечень триггеров, отражающих состояние наблюдаемого узла, формирует системный инженер.

Шаг 4. Формируем множество фиксированных признаков для проверки уже имеющегося рабочего сценария:

$$l' = \{ f, t_1, .., t_w \},$$

$$f \in F,$$

$$\{ t_1, .., t_w \} = T,$$

где l' – множество фиксированного набора признаков и идентификатор наблюдаемого узла, f – идентификатора наблюдаемого узла, t_w – признак, отражающий состояние узла.

Шаг 5. Проверка на предмет имеющегося рабочего сценария во множестве сценариев L. Если рабочий сценарий есть, то переход к шагу 12. Иначе шаг 6.

Шаг 6. Формируем множество фиксированных признаков и вспомогательного инструмента для проверки рабочего сценария:

$$l = \{ f, g, t_1, \dots, t_w \},$$

где l – множество фиксированного набора значений переменных – рабочий сценарий, g – положительно сработавший инструмент.

Шаг 7. Если нет изменений в количестве вспомогательных инструментов, то переход к шагу 11. Иначе изменяем множество вспомогательных инструментов:

$$G \pm \Delta G,$$

$$G = \{ g_1, .., g_{q \pm \Delta q} \},$$

где ΔG – показывает насколько изменилось множество вспомогательных инструментов, Δq – показывает насколько изменилось максимальное количество вспомогательных инструментов.

Шаг 8. Если произошло удаление уже имеющихся инструментов и есть рабочие сценарии, связанные с ними, то происходит корректировка множества имеющихся сценариев:

$$L = \{ l_1, .., l_{e - \Delta q} \},$$

где L – множество рабочих сценариев, l – рабочий сценарий, e – максимальное количество рабочих сценариев. Иначе шаг 11.

Шаг 9. Если нет изменений в количестве признаков, отражающих состояние наблюдаемого узла, то переход к шагу 11. Иначе изменяем множество признаков:

$$T \pm \Delta T,$$

$$T = \{ t_1, .., t_{w \pm \Delta w} \},$$

где T – множество признаков, w – максимальное количество признаков, отражающих состояние узла, ΔT – показывает насколько изменилось множество признаков, отражающих состояние наблюдаемого узла.

Шаг 10. Если произошло изменение количества признаков, то происходит корректировка множества имеющихся сценариев:

$$L = 0$$

Шаг 11. Если было изменение признаков и/или количество вспомогательных инструментов ДД аномалий КС, то переход к шагу 4. Иначе шаг 12.

Шаг 12. Применение вспомогательного инструмента и проверка значения триггера из множества X, который отражает состояние критически значимого параметра на наблюдаемом узле. Формирование множества X описано в работе [17].

Шаг 13. Если значение триггера $x = 1$, то переход к шагу 6. Иначе шаг 14.

Шаг 14. Добавление рабочего сценария в множество сценариев:

$$L = \{ l_1, .., l_{e+1} \},$$

Шаг 15. Выбор идентификатора следующего проблемного узла. Если проблемные узлы закончились, то переход к шагу 16.

Шаг 16. Конец метода.

Такой метод позволяет создавать множество сценариев при проведении дополнительной диагностики аномалий в работе динамической компьютерной сети, которые позволяют своевременно воздействовать на наблюдаемый узел в автоматическом режиме, чтобы вернуть его состояние в рамки, установленные системным инженером, нормы

IV. Заключение

Проведение дополнительной диагностики функционирования компьютерной сети в случаях невозможности осуществления проактивного мониторинга или реакции по заранее прописанным шаблонам позволяет своевременно среагировать на возникшую аномалию. Применяя метод формирования рабочих сценариев при дополнительной диагностики аномалий в работе компьютерной сети можно автоматизировать применения вспомогательных инструментов для воздействия на наблюдаемый узел и сформировать соответствующий сценарий для того, чтобы в дальнейшем оперативно реагировать на возникшие проблемы.

Список литературы

[1] Лопаткин Д.С. Интернет вещей как фактор цифровой трансформации экономики // Инновации и инвестиции. 2018. №9, С. 257-260.

[2] Ямщиков С.В., Кундрякова Н.А. Интернет вещей в контексте повседневности: современное состояние, тенденции развития и ключевые проблемы // Гуманитарные, социально-экономические и общественные науки. 2021. №1. С. 69-76.

[3] Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. СПб: Питер, 2016. 960 с.

[4] Сильнов Д.С. Современные системы удаленного мониторинга вычислительных ресурсов: состояние, проблемы, перспектив // Безопасность информационных технологий. 2011. №3. С. 57-60.

[5] Федорова Л.М. Системы мониторинга. Обзор и сравнение // Вестник науки и образования. 2020. №10-4 (88). С.16-18.

[6] Будко Н.П. Общие принципы функционирования и требования к построению структур перспективных систем мониторинга распределенных информационно-телекоммуникационных сетей // Техника средств связи. 2021. №2 (154). С. 38-59.

[7] Доценко В.О., Шевнина Е.И. Исследование актуальных требований для разработки систем мониторинга и управления телекоммуникационной сети// Вестник СибГУТИ. 2022. № 2. С. 23-32.

[8] Зотов С.В. Использование Zabbix для мониторинга гетерогенной сети с работой по проводным и радиоканалам // Научно-исследовательские публикации. 2017. №1 (39). С.30-39.

[9] Лазарева Н.Б. Оптимальный выбор системы мониторинга для различных типов ит-инфраструктур // Инженерный вестник Дона. 2022. №4 (88).

[10] Вишняков В.А., Аль-Масри А.Х., Аль-Хаджи С.Х. Организация структур и управления в локальных сетях интернет вещей // Системный анализ и прикладная информатика. 2020. №2. С.11-16.

[11] Злобина Н.В., Волжанкин Н.В., Пособилов Н.Е. Обеспечение централизованного мониторинга для систем сложной архитектуры с большим объёмом данных // Труды НГТУ им. Р.Е. Алексеева. 2017. №4 (119). С.18-23.

[12] Alcaraz Calero J. M., Aguado J. G. Monpaas: Adaptive Monitoring Platform as a Service for Cloud Computing Infrastructures and Services. // IEEE Transactions on Services Computing, 2015, vol. 8, №1, P. 65-78.

[13] J. Iden and T. R. Eikebrokk Understanding the ITIL Implementation Project: Conceptualization and Measurements // 22nd International Workshop on Database and Expert Systems Applications, Toulouse, France, 2011, P. 21-25.

[14] Deutscher J., Felden C., Concept for implementation of cost effective Information Technology Service Management (ITSM) in organizations // IEEE/IFIP Network Operations and Management Symposium Workshops, Osaka, Japan, 2010, P. 167-168.

[15] Allakin V.V. Formation of a server for monitoring the functional security of a public information and telecommunications network based on the evaluation of SRE metrics // Means of Communication Equipment. 2021, № 1 (151), P. 77-85.

[16] Авилов М.И., Шичкина Ю.А. Дополнительная диагностика аномалий при мониторинге динамической компьютерной сети с применением рабочих сценариев // Известия СПбГЭТУ "ЛЭТИ". СПб. 2021. №10. С. 94–102.

[17] Авилов М.И., Шичкина Ю.А., Куприянов М.С. Мониторинг информационно-коммуникационной компьютерной сети с применением модуля дополнительной диагностики // Известия СПбГЭТУ "ЛЭТИ". 2020. №5. С. 34–45.