# Министерство просвещения Российской Федерации

федеральное государственное бюджетное  
образовательное учреждение высшего образования

«Московский педагогический государственный университет»   
Институт физики, технологии и информационных систем

Тищенко Константин Константинович

Мониторинг технического состояния сетевых устройств в образовательной организации

Код и направление подготовки: 09.03.02 Информационные системы и технологии

Направленность (профиль) образовательной программы:

Информационные технологии в образовании

Выпускная квалификационная работа

(бакалаврская работа)

Заведующий кафедрой

Научный руководитель –

к.п.н, доц. КТиИС К.Ф. Гусин

Консультант –

ст. преп. Д.С. Горелко

Технологических и информационных систем

(наименование кафедры)

Профессор, д.п.н, к.ф-м.н

Нижников А.И.

Проверка на объем заимствований:

% авторского текста

Москва – 2020 год

УТВЕРЖДАЮ

Заведующий кафедрой КТиИС

Профессор, д.п.н, к.ф-м.н Нижников А.И.

«16» сентября 2020 г.

**ЗАДАНИЕ**

**на разработку выпускной квалификационной работы**

студента ИФТИС

Тищенко Константина Константиновича

**Наименование темы: «Мониторинг технического состояния сетевых устройств в образовательной организации»**

**Руководитель: доц. КТиИС, к.п.н. Гусин К.Ф.**

«16» сентября 2019 г.

**Консультант: ст. преп. Горелко Д.С.**

«16» сентября 2019 г.

**Целевая установка и основные вопросы, подлежащие разработке**

**при выполнении работы:**

Цель работы – Внедрение системы комплексного мониторинга сетевого оборудования в существующую инфокоммуникационную сеть образовательной организации.

**Вопросы, подлежащие разработке:**

1. Проанализировать распространённые системы мониторинга инфокоммуникационных сетей и их компоненты.
2. Составить перечень оборудования и сервисов, развернутых в инфокоммуникационной сети кафедры ТиИС.
3. Развернуть систему мониторинга на выделенном оборудовании. Интегрировать систему мониторинга с имеющейся инфраструктурой инфокоммуникационной сети.

**Исходные данные:**

………

**Предполагаемое содержание и объем дипломной работы:**

Введение

Глава 1. Системы мониторинга

Глава 2. Система мониторинга в инфокоммуникационной сети  
образовательной организации.

Заключение

Список литературы

Приложения

Объем работы 40-50 стр.

**Основная литература:**

1. …….
2. ………
3. ………..

**Руководитель: доц. КТиИС, к.п.н. Гусин К.Ф.**

«16» сентября 2019 г.

**Консультант: ст. преп. Горелко Д.С.**

«16» сентября 2019 г.

**Задание получил**: **Тищенко Константин Константинович**

«16» сентября 2019 г.

Оглавление

[Введение 5](#_Toc41300092)

[Глава 1. Системы мониторинга 8](#_Toc41300093)

[1.1 Понятие системы мониторинга и входящих в неё компонентов 8](#_Toc41300094)

[1.2 Инфокоммуникационные сети в образовательных организациях 13](#_Toc41300095)

[1.3 Анализ существующих систем мониторинга инфокоммуникационных сетей для использования в образовательной организации 16](#_Toc41300096)

[Глава 2. Система мониторинга Zabbix в инфокоммуникационной сети образовательной организации. 21](#_Toc41300097)

[2.1 Инфокоммуникационная сеть кафедры ТиИС МПГУ. 21](#_Toc41300098)

[2.2 Процесс разворачивания системы мониторинга Zabbix. 23](#_Toc41300099)

[2.3 Интеграция Zabbix с инфокоммуникационной сетью кафедры ТиИС МПГУ. 26](#_Toc41300100)

[Заключение 32](#_Toc41300101)

[Список литературы 33](#_Toc41300102)

[Приложение 1. Настройка SNMPv2 на оборудовании производства компании Cisco 38](#_Toc41300103)

[Приложение 2 39](#_Toc41300104)

[Приложение 3. Разворачивание Zabbix 4.4 на Ubuntu 18.04 LTS 40](#_Toc41300105)

[Приложение 4. Обновление Zabbix 4.4 до версии 5.0 LTS 42](#_Toc41300106)

## Введение

Инфокоммуникационная сеть современной образовательной организации представляет собой комплексную систему. Система мониторинга способствует стабильности работы всех узлов и оконечных устройств. Она позволяет собирать и анализировать собранные с оборудования данные в одном месте. Это позволяет быстро и эффективно определять узкие места в инфокоммуникационной сети, обнаруживать скрытые дефекты, оперативно определять и устранять неисправности оборудования и как следствие поддерживать работоспособность инфокоммуникационной сети на должном уровне. Система мониторинга, развернутая в инфокоммуникационной сети, представляет собой автоматизированный процесс сбора информации различного рода с сетевых устройств, хранения данной информации и предоставление ее пользователю в удобном для него виде. Кроме того, современные системы мониторинга предоставляют возможность оперативного оповещения пользователей и/или инженеров наблюдаемой инфокоммуникационной сети.

Следует отметить, что практически все системы мониторинга, использующиеся для мониторинга инфокоммуникационных сетей, используются и в других областях. Нет принципиального значения откуда именно собирать данные – с сетевого оборудования, с производственных станков, с датчиков умного дома, датчиков транспортного средства или откуда-либо ещё.

Если говорить об актуальности данной тематики, то в 2011 году в Германии была разработана концепция развития промышленности «Индустрия 4.0», которую также называют грядущей четвертой промышленной революцией, она подразумевает под собой максимальную автоматизацию производств – интеграцию кибернетических систем в заводские процессы. С 2014 года она активно внедряется на территории всей страны, в первую очередь в тяжелой промышленности: машиностроении и автомобилестроении, являющихся локомотивами немецкой экономики. В 2014 году в Соединенных Штатах Америки был создан консорциум промышленного интернета. Для Соединенных Штатов Америки автоматизация производственных процессов стала важным национальным приоритетом. В рамках этой концепции государственные органы Соединенных Штатов Америки содействуют возвращению производства американских компаний на территорию страны, способствуют их модернизации и преобразованию в фабрики будущего. В последние годы к этим тенденциям присоединяются и другие ведущие мировые государства: Франция, Япония, Южная Корея, Китай. Уже сегодня отголоски этих процессов можно наблюдать и в повседневной жизни, например, в развитии технологий «Умного дома», трехмерной печати, печатной электроники и пр.

Обращаясь к проблематике автоматизации сбора данных в инфокоммуникационных сетях, то мониторинг сетевого оборудования позволяет в ряде случаев предупредить ошибки и выход оборудования из строя, в ряде случаев, оперативно исправить возникающие проблемы и сократить или вовсе предупредить простой в работе предприятия. Таким образом мониторинг инфокоммуникационной сети позволяет существенно сократить издержки в работе предприятия и уберечь его от репутационных потерь.

Таким образом тематика автоматизации процессов в целом и автоматизация сбора данных в инфокоммуникационной сети в частности, является актуальной на сегодняшний день. В следствии этого была выбрана тема данной выпускной квалификационной работы: «Мониторинг технического состояния сетевых устройств в образовательной организации».

В ходе работы необходимо будет решить следующие задачи:

1. Проанализировать распространённые системы мониторинга инфокоммуникационных сетей и их компоненты. Исследовать законодательство в области регулирования инфокоммуникационных сетей в образовательных организациях.
2. Составить перечень оборудования и сервисов, развернутых в инфокоммуникационной сети кафедры ТиИС.
3. Развернуть систему мониторинга на выделенном оборудовании. Интегрировать систему мониторинга с имеющейся инфраструктурой инфокоммуникационной сети.

## Глава 1. Системы мониторинга

### Понятие системы мониторинга и входящих в неё компонентов

Слово «мониторинг» происходит от латинского monitor, что в переводе означает напоминающий, советующий, предостерегающий, надзирающий. В наши дни под мониторингом понимают процесс наблюдения и регистрации данных (метрик) через каким-либо способом заданные промежутки времени.

В свою очередь система мониторинга представляет собой набор из четырёх компонентов:

1. База данных. База данных должна выполнять функцию хранения собираемых данных.
2. Средство сбора и записи метрик в базу данных.
3. Средство для удобного просмотра полученных данных инженером.
4. Средство анализирующее приходящие метрики и оперативно уведомляющее ответственных лиц о выявляемых проблемах в работе оборудования, программ.

Базы данных.

Выбор базы данных и системы управления базой данных для хранения метрик, представляет собой отдельную задачу. Для систем мониторинга инфокоммуникационных сетей наиболее распространены реляционные базы данных. Учитывая специфику образовательных организаций наиболее всего подходят распространенные системы управления реляционными базами данных, например, такие как MySQL, PostgreSQL, MariaDB, это связано с большой популярностью языка SQL и большим количеством специалистов, умеющих с ним работать. Использование реляционных баз данных позволит обеспечить простоту поддержки системы мониторинга в будущем, например, при необходимости развития инфокоммуникационной сети и добавлении новых устройств и увеличения количества получаемых метрик.

Однако, следует отметить, что в последнее время среди систем мониторинга инфокоммуникационных сетей набирают популярность базы данных временных рядов (time series database/TSDB). Это базы данных, специально предназначенные для обработки информации, связанных со временем. Реляционные базы данных представляют собой таблицы, где каждая строка определяет отдельную запись. Такие таблицы и строки можно использовать для хранения абсолютно различной информации. Они эффективны в разных областях. Базы данных временных рядов устроены несколько иначе. В отличии от реляционных баз данных, данные в которых многомерны, в базах данных временных рядов данные агрегируются по времени. С течением времени и возрастанием размеров реляционной базы данных скорость приема и записи данных падает, это связано с тем, что при добавлении или удалении записи в реляционную базу данных, система управления базой данных многократно переиндексирует данные, для быстрого и эффективного доступа к ним. В итоге, при росте объемов хранимых данных производительность таких баз данных снижается. Базы временных рядов не имеют этого недостатка. Тем не менее, это этот тип баз данных, являющийся довольно перспективным, но на данный момент всё ещё представляет собой новый продукт на рынке и как следствие недостаточно оттестирован и имеет проблемы со стабильностью.

Ряд популярных систем мониторинга, таких как Cacti, Ganglia, Ground Work monitor или NOC network monitoring application в качестве базы данных для хранения метрик используют циклические базы данных(RRD). Это такой тип баз данных в которых новые записи вытесняют старые, таким образом база данных сохраняет свой объём и не растет со временем. Наибольшее развитие данный тип получил в пакете программного обеспечения RRDtools. Следует отметить, что данный набор программного обеспечения является свободным и распространяется по лицензии GNU GPL. Успех данного пакета, был обусловлен и тем, что помимо прочих приложений, в его набор входит приложение, для графического отображения собранных данных. Однако, в последнее время, данный набор вытесняется с рынка базами данных временных рядов, которые так же обладают широкими возможностями контроля, занимаемого ими места, но при этом превосходят циклические базы данных по важным параметрам производительности, например, по количеству записи метрик в секунду.

Отдельно стоит рассмотреть такие расширения как TimescaleDB и PipelineDB для системы управления базой данных PostgreSQL. Эти расширения позволяют использовать PostgreSQL вместе с базами данных временных рядов. Это позволяет использовать преимущества баз данных временных рядов вместе с проверенной временем PostgreSQL и таким образом нивелировать основной недостаток баз данных временных рядов.

Протокол SNMP

SNMP – сетевой протокол для диагностики, мониторинга и управления устройств и программного обеспечения. Его спецификация описана международными стандартами RFC1155, RFC1212, RFC1213, RFC1157 и RFC3411. SNMP определён IETF (Internet Engineering Task Force) как компонент сетевой модели передачи данных TCP/IP.

SNMP работает на прикладном уровне стека OSI. Данный протокол предоставляет формат сообщения для обмена данными между агентами (управляемых узлов) и диспетчерами (управляющих узлов). Диспетчер может собирать данные от агента SNMP с помощью запроса get и изменять настройки на агенте с помощью запроса set. Кроме того, агенты SNMP могут пересылать информацию непосредственно в систему управления сетями посредством передачи не запрашиваемых диспетчером уведомлений (ловушек, traps).

Использование ловушек обусловлено недостатками периодического опроса диспетчером агента, такими как компромисс между частотой опроса и пропускной способностью канала и снижение задержки времени между событием и его обнаружением. Чтобы избавиться от этих недостатков, агенты SNMP могут создавать и отправлять ловушки, сообщая диспетчеру о некоторых события немедленно. Примерами таких событий могут быть, смена состояния канала, попытки аутентификации пользователей, отслеживание mac-адресов и другие.

С описанием версий SNMP можно ознакомиться в Таблица 1 Сравнение версий SNMP

Таблица 1 Сравнение версий SNMP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Модель протокола** | **Аутентификация** | **Шифрование** | **Результат** | **Описывающие документы** |
| SNMPv1 | По имени сообщества | Не поддерживается | Использует проверку имени сообщества для проверки подлинности | RFC1157 |
| SNMPv2c | По имени сообщества | Не поддерживается | Использует проверку имени сообщества для проверки подлинности | RFC1901-1908 |
| SNMPv3 | По имени пользователя или посредством MD5/SHA | Возможно(DES/AES) | Использует проверку имени пользователя для проверки уровня доступа или обеспечивает аутентификацию на основе алгоритмов HMAC-MD5/HMAC-SHA | RFC2273-2275  RFC3410-3415 |

В версиях SNMPv1 и SNMPv2c для контроля доступа используется модель «Строки сообщества». Строка сообщества представляет собой незашифрованный пароль. Существует два типа строк сообщества

1. Только чтение (RO)
2. Чтение и запись (RW)

В связи с тем, что данные версии предоставляют минимальную безопасность, рекомендуется их использование только в режиме RO.

Поскольку сбор метрик является однотипной и постоянной задачей, эффективнее использовать метод сбора через ловушки, настроив агента, чем с некоторой периодичностью опрашивать агента через диспетчера. Таким образом при использовании ловушек, достаточно с точки зрения безопасности использовать SNMPv2 в режиме «только чтение» и настроить листы доступа на сетевом оборудовании, ограничив таким образом доступ с других устройств.

Мониторинг операционных систем с помощью агентов

Многие системы мониторинга используют агентов для сбора данных. Агент — это процесс, разворачиваемый в операционных системах для мониторинга локальных ресурсов и приложений. Обычно различают два типа агентов – активный и пассивный.

При пассивном агенте средство сбора данных (менеджер, диспетчер) отправляет запрос на агента с целью получения данных по заданным настройкам и в ответ получает необходимые метрики. Обычно это происходит с определенной периодичностью. При активном агенте, он сначала запрашивает у диспетчера список метрик и периодичность передачи данных, а после сам, не получая запросы от диспетчера отправляет на него собираемые данные.

С преимуществами и недостатками обоих подходов можно ознакомится в Таблица 2 Преимущества и недостатки агентов разных типов

Таблица 2 Преимущества и недостатки агентов разных типов

|  |  |  |
| --- | --- | --- |
|  | Активный агент | Пассивный агент |
| Необходимость настройки | Требуется | Чаще всего не требуется |
| Нагрузка на канал и диспетчер | Ниже | Выше |
| Возможность работы за NAT (PAT) | Есть | Нет |
| Автоматическая регистрация узлов | Есть | Нет |

Интерактивная панель

Многие системы мониторинга имеют собственные решения, для визуализации собранных данных. Однако, отдельно в качестве средства для визуализации и анализа получаемых данных стоит рассмотреть продукт сообщества с открытым исходным кодом – Grafana. Данный продукт имеет возможность получать данные как из всех распространённых баз данных, так и напрямую из множества программных продуктов, собирающих метрики и записывающих их в базы данных. Стоит отметить, что он поддерживает все распространённые системы мониторинга и базы данных. Наличие большого количества документации, удобство интерфейса и визуальной составляющей делает его безусловным лидером на рынке, в качестве альтернативы можно рассматривать встроенные во многие системы мониторинга продукты, но большинство из них не обладают всеми возможностями Grafana. Кроме всего прочего Grafana имеет встроенные возможности для настройки триггеров на события и различные варианты оповещения сотрудниках как уже о случившихся сбоях в работе инфокоммуникационной сети, так и о предполагаемых проблемах в будущем.

### Инфокоммуникационные сети в образовательных организациях

Развитие информационных технологий привело к созданию локальных вычислительных сетей и систем, а интеграция информационных технологий и телекоммуникаций привела к появлению нового термина – «инфокоммуникации».

Сам термин «Инфокоммуникации» появился лишь в начале 21 века. Инфокоммуникационные сети и технологии являются относительно новой отраслью экономики, получающей интенсивное развитие в последние годы.

Инфокоммуникационная сеть (Infocommunication Network) – это совокупность территориально рассредоточенных информационных, вычислительных ресурсов, программных комплексов управления, размещаемых в оконечных системах сети и терминальных системах пользователей, взаимодействие между которыми обеспечивается посредством телекоммуникаций, и которые совместно образуют единую мультисервисную платформу.

Инфокоммуникационные сети в образовательной организации представляют собой конвергентные сети, объединяющие в себе множество сетей, раньше являющихся раздельными, например, таких как локально-вычислительная сеть, сеть видео наблюдения, телефония, сигнализация и т.д. Объединение множества сетей в одну, хоть и является более прогрессивным решением, однако создает еще больше требований к бесперебойной работоспособности данной инфокоммуникационной сети. Построение системы мониторинга в инфокоммуникационной сети позволяет решить эту задачу.

В последнее время активно осуществляется процесс информатизации образования. Результатом этого процесса стало появление сетей в образовательных организациях. Одной из особенностей сетевой инфраструктуры образовательной организации является большое количество услуг, которые она должна предоставлять. И в связи с тем, что сеть образовательной организации должна носить характер конвергентной сети, компьютерные сети в образовательных организациях эволюционируют в инфокоммуникационные сети.

Новый этап в развитии инфокоммуникационных сетей в образовательных организациях РФ задала Московская Электронная Школа (МЭШ).

Школьный класс в концепции МЭШ должен стать высокотехнологичным пространством – медиа-центром, мастерской, лабораторией, оснащенной современными устройствами и единым хранилищем информации. Бумажные учебники должны уступить место электронным образовательным ресурсам, доступным детям и их родителям в любое время в режиме on-line.

Для учителя МЭШ – это возможность максимально сократить время на подготовку к уроку за счет общедоступной библиотеки методических ресурсов, включающей в себя иллюстрации, учебные видеофрагменты идругие средства повышения наглядности, а также апробированные и качественные сценарии проведения уроков по всем темам школьной программы, разнообразные контрольные задания и тесты.

Для того, чтобы все это было возможно, инженерами было решено множество конкретных задач, важнейшие из которых можно объединить в три группы:

1. Формирование необходимой инфраструктуры;
2. Разработка специального программного обеспечения;
3. Создание условий для наполнения библиотеки цифровых электронных ресурсов качественными методическими материалами.

Для мониторинга построенной инфраструктуры используются сразу два решения: «Cisco Prime Infrastructure» и «Zabbix». Данные решения позволяют собирать и отслеживать все изменения внутри инфокоммуникационных сетей школ и колледжей города Москвы участвующих в программе. Оперативно реагировать на проблемы и предотвращать их возможное появление.

Среди прочих особенностей построения сетей в образовательных организациях, необходимо отметить, что согласно законодательству, в беспроводных сетях должна производится идентификация пользователей, для предотвращения использования данных сетей в противоправных целях, что регламентируется Федеральным законом № 97-ФЗ от 5 мая 2014 г., Постановлением Правительства РФ № 758 от 31 июля 2014 г., Постановлением Правительства РФ № 801 от 12 августа 2014 г. Согласно этим Постановлениям владельцы точек бесплатного Wi-Fi, а в частности: кафе, рестораны, отели, школы, многофункциональные центры, парки, общественный транспорт и другие места с коллективным доступом в Интернет, обязаны идентифицировать личность пользователей.

### Анализ существующих систем мониторинга инфокоммуникационных сетей для использования в образовательной организации

В настоящее время на рынке представлено множество решений, для построения систем мониторинга, как в локально-вычислительных сетях в частности, так и в инфокоммуникационных. Следует отметить, что кроме программных средств мониторинга, существуют крупные компании предоставляющие специальное оборудование для данных целей, однако, данные решения используются в подавляющем большинстве случаев в крупных сетях интернет провайдеров и в решениях, предназначенных для крупного бизнеса. Таким образом, покупка данного оборудования для инфокоммуникационных сетей образовательных организаций, а в частности, для построения системы мониторинга на кафедре ТиИС МПГУ изначально является не целесообразной и выходящей за рамки бюджета.

Рассмотрим самые распространённые программные решения систем мониторинга в инфокоммуникационных сетях образовательных организаций.

Zabbix – одна из самых распространенных универсальных систем мониторинга. Активно развивается с 1998 года, с 2001 года распространяется публично под лицензией GNU GPL, для хранения данных использует MySQL, PostgreSQL, SQLite, Oracle DB, IBM DB2. Имеет веб-интерфейс, написанный на PHP. Поддерживает различные виды мониторинга, как с помощью агентов, так и без. В связи с сильной распространённостью обладает крупным сообществом разработчиков и как следствие активно развивается. Используется в образовательной сфере в РФ совместно с Cisco Prime Infrastructure для мониторинга и управления оборудованием Московской Электронной Школы.

InfluxData (Стэк TICK) – Относительно новый, но хорошо зарекомендовавший себя на рынке набор программного обеспечения, написанного на языке Go. Включает в себя такие программные продукты как:

1. Telegraf – собирает метрики временных рядов.
2. InfluxDB – самая распространённая база данных временных рядов. Возможна кластеризация.
3. Chronograf – программное обеспечение позволяющее визуализировать данные из базы данных временных рядов.
4. Kapacitor – отвечает за обработку полученных данных, контролирует отклонения и оповещает инженеров.

Prometheus – комплект программного обеспечения с открытым исходным кодом построенного вокруг и включающее в себя TSDB – “Prometheus”.

1. TSDB – “Prometheus”
2. Сервер, собирающий метрики и сохраняющий их в TSDB.
3. PROMDASH – Программное обеспечение для визуализации данных.
4. AlertManager – Менеджер уведомлений.
5. Pushgateway – компонент сбора метрик с краткоживущих процессов.
6. Экспортеры данных из сторонних приложений, а также набор библиотек для различных языков программирования.

Cisco Prime Infrastructure – система мониторинга и управления проводными и беспроводными инфокоммуникационными сетями. Разрабатывается и поддерживается компанией Cisco. Данное программное обеспечение позволяет выполнять мониторинг, резервное копирование и восстановление конфигураций, собирать базовую статистику с оборудования, данных инвентаризации, настраивать оборудование, выполнять контроль работы приложений, выполнять автоматическую установку оборудования без использования консольного доступа, составлять отчеты о сбоях и оперативно оповещать сетевых администраторов сети. Сбор данных с оборудования осуществляется посредством протоколов SNMP и Syslog. Так же отличительной особенностью является наличие приложения для мобильных устройств в то время как большинство систем мониторинга используют только веб-интерфейс и доступ через консоль. В образовательной сфере в РФ активно используется при мониторинге Московской Электронной Школы. Одним из основных минусов данной системы мониторинга является стоимость и закрытость исходного кода.

IBM Trivoli Monitoring – Решение от компании IBM с закрытым исходным кодом. Состоит из следующих компонентов:

1. Trivoli Enterprise Monitoring Server (TEMS) – сервер мониторинга, собирает данные с оборудования и записывает их в базу данных.
2. База данных – место хранения накопленных метрик. IBM Trivoli Monitoring допускает использование – DB2, MySQL, Oracle, Derby.
3. Tivoli Enterprise Portal Server (TEPS) – сервер предоставляющий визуальный доступ к собираемым данным.
4. Tivoli Enterprise Management Agent (TEMA) – управляемые системы (агенты), отвечают за накопление метрик с оконечного оборудования и пересылку полученных данных на TEMS. Можно разделить на два подвида: Агенты операционной системы и Агенты приложений.

Сильными сторонами данной системы являются надежность и стабильность работы, возможности масштабирования и поддержки. Слабой – стоимость и закрытость исходного кода, отсутствие поддержки TSDB.

Cacti – открытое программное обеспечение. В основе лежит кольцевая база данных (RRD) основанная на MySQL. В основе визуальной части лежит набор утилит RRDtool. Сбор данных осуществляется по протоколу SNMP. Используется как легковесное решение для маленьких конвергентных сетей, плохо поддается масштабированию не имеет агентов.

Nagios – программное обеспечение с открытым исходным кодом, позволяет наблюдать распространённые сетевые службы, состояние хостов, имеет возможность удаленного мониторинга по средством SSH и SSL. Использует агенты(плагины) для сбора данных. Имеет встроенный графический интерфейс. Основным недостатком Nagios является сложность настройки и дальнейшей поддержки – отсутствие web-интерфейса (в бесплатной версии) и большое количество конфигурационных файлов, связь между которыми происходит напрямую, что не позволяет оперативно и просто обнаруживать ошибки при настройке и создает дополнительные трудности в последующей поддержке и при масштабируемости.

Icinga 2 – является форком Nagios, унаследовавший основной недостаток системы мониторинга Nagios: сложная изначальная настройка даже самой простой распределенной схемы.

OpenNMS – Программная платформа для мониторинга, построенная на событийно-ориентированной архитектуре, не имеет агентов, поддерживает работу с популярной информационной панелью grafana. Имеет встроенные модули формирования отчетности, поддерживает Linux, Windows, Solaris и OSX. Имеет как собственную настраиваемую информационную панель администратора, так и поддержку такого открытого программного обеспечения как Grafana. Одним из недостатков является слабая документация и малая распространённость на территории РФ. Слабая популярность данной системы мониторинга среди малого бизнеса вызвана высокой ценой поддержки и «заточенностью» под сети крупных размеров.

На основе проведенного анализа, было принято решение для построения системы мониторинга в инфокоммуникационной сети кафедры технологии и информационных систем использовать следующий набор:

В качестве сборщика метрик использовать Zabbix 4.4, с последующим обновлением до Zabbix 5.0, при этом использовать следующие компоненты: Заменить веб сервер, используемый по умолчанию(Apache2) на Nginx.

А в качестве базы данных использовать PostgreSQL с расширением TimescaleDB и PipelineDB.

## Глава 2. Система мониторинга Zabbix в инфокоммуникационной сети образовательной организации.

### 2.1 Инфокоммуникационная сеть кафедры ТиИС МПГУ.

Инфокоммуникационная сеть кафедры технологических и информационных систем Московского педагогического государственного университета была создана больше десяти лет назад. Для построения системы мониторинга необходимо изучить оборудование и сервисы, использующиеся в данной инфокоммуникационной сети.

Список оборудования, находящегося в серверной стойке кафедры ТиИС МПГУ можно увидеть в Таблица 3 Оборудование и сервисы в инфокоммуникационной сети кафедры ТиИС

Таблица 3 Оборудование и сервисы в инфокоммуникационной сети кафедры ТиИС

|  |  |  |  |
| --- | --- | --- | --- |
| **Оборудование** | **Сервис** | **Описание** | **Внутренний ip-адрес** |
| Сервер Kraftway Express 4EM15 | Active Directory | Active Directory («Активный каталог», AD) – решение предоставленное компанией Microsoft объединяющее различные объекты сети в единую систему. AD хранит сведения о пользователях сети кафедры ТиИС, об устройствах введенных в домен, групповых политиках и многое другое. | 192.168.0.5 |
|  | Web-server | Обслуживание адресов ftip.ru и elearning.ftip.ru | 192.168.0.254 |
|  | Маршрутизатор | В качестве маршрутизатора используется дистрибутив, основанный на FreeBSD – PFSence | 192.168.0.1 |
|  | Wi-Fi controller | Контроллер беспроводной сети производит автоматический поиск, централизованную настройку WiFi точек доступа и обновление программного обеспечения подключенных точек доступа. | 192.168.0.199 |
| Сервер Kraftway Express Lite L13 | File Server | Данный сервер предназначен для хранения файлов студентов, преподавателей и других сотрудников. | 192.168.0.3 |
| Сервер Kraftway Express Lite L13 | FreeNAS | FreeNAS – Операционная система на основе FreeBSD. Выполняет роль сетевого хранилища. | 192.168.0.4, 172.16.32.10 |
| Kraftway Express ISP ES15 | Hyper-V | Данные сервера служат для развертывания учебных виртуальных машин с помощью программного обеспечения Hyper-V. | 92.168.0.251, 172.16.32.11 и 192.168.0.252, 172.16.32.12. |
| Коммутатор Cisco Catalyst 2960G |  | Сетевое устройство, работающее на втором уровне модели OSI и осуществляющее коммутацию кадров Ethernet на основе MAC-адресов. | 192.168.0.2 |

Кроме того, в сети кафедры расположены следующие устройства:

1. Сетевой принтер Epson AcuLaser C4000, внутренний IP-адрес 192.168.0.215
2. 3 точки доступа UniFi AP служащие для подключения к инфокоммуникационной сети кафедры сети беспроводных устройств.
3. Коммутатор Cisco 2960.

Данная сеть разделена на три виртуальные локальные сети для увеличения производительности, улучшения безопасности и сокращения количества устройств в домене широковещательной рассылки.

Топологию инфокоммуникационной сети кафедры ТиИС можно увидеть на Рисунке 1 (Нарисовать получше).



Рисунок 1. Топология инфокоммуникационной сети кафедры ТиИС

Тут можно добавить список необходимых к мониторингу метрик

В стадии ожидания агентов на оборудовании

### 2.2 Процесс разворачивания системы мониторинга Zabbix.

В качестве операционной системы для системы мониторинга был выбран дистрибутив Ubuntu 18.04 LTS «Bionic Beaver». Выбор данной версии, а не последней, на момент установки (Ubuntu 19.10 «Eoan Ermine») обусловливается длительностью поддержки 5 лет у версии LTS против 9 месяцев у «Eoan Ermine».

При разбиении разделов следует учитывать возможность расширения инфокоммуникационной сети, как следствие увеличения количества метрик, предполагаемых к сбору, что приведет к необходимости увеличения выделяемого пространства под базу данных на диске. Самым простым способом является изначально использовать менеджер логических томов (LVM).

В качестве используемой базы данных для хранения метрик, была выбрана СУБД PostgreSQL с расширением TimescaleDB. Данное сочетание надежности PostgreSQL с высокой скоростью работы баз данных временных рядов, кроме прочего упростит настройку и последующую поддержку, что является не маловажным фактором в условиях работы инфокоммуникационной сети КТиИС.

В следствии этого в качестве устанавливаемого дистрибутива Zabbix была выбрана версия 4.4. Выбор версии без длительной поддержки (не LTS) был обусловлен тем, что версия 4.4 в отличии от версии 4.0 LTS официально поддерживает расширение TimescaleDB для базы данных PostgreSQL.

Zabbix это целый набор программного обеспечения, одной из составляющих которого является – веб-интерфейс. Для его работы по умолчанию прилагается веб-сервер Apache с преднастроенными конфигурационными файлами, однако начиная с версии 4.4 предоставляется официальная возможность выбора между Nginx и Apache. При имеющейся нагрузке на данный веб-сервер, нет принципиального значения какой из веб-серверов выбрать. Однако одной из основных причин более высокой производительности Nginx по сравнению с Apache – это один рабочий процесс на процессор/ядро, каждый из его процессов, может обрабатывать сотни тысяч входящих сетевых подключений. В отличии от Apache ему нет необходимости создавать отдельные потоки или процессы для каждого соединения. Это одна из причин, по которой крупные IT-компании испытывающие большие нагрузки на сервера, например, такие как Facebook, Netflix или Instagram делают выбор в сторону Nginx.

Стоит подчеркнуть наличие ошибок в официальной документации для установки Zabbix 4.4 в связке с Nginx и PostgreSQL. В связи с этим в Приложении 2 можно ознакомиться с подробным описанием установки.

Согласно данным приводимым официальной сетевой академией Cisco, сбор метрик с оборудования производства данной компании, в частности с коммутаторов, расположенных в сети кафедры, рекомендуется посредством SNMP-агента, входящего в комплект операционной системы управляющей коммутатором. Команды для настройки SNMP-агента на коммутаторе Cisco приведены в Приложении 1. Согласно документации Zabbix – предполагается использование стороннего приложения для отлова и передачи в Zabbix приходящих SNMP traps. В качестве таких приложений были использованы snmptrapd в связке с snmptt. При настройке snmptt нужно учитывать предполагаемых источников SNMP уведомлений и установить необходимые MIB-файлы для расшифровки OID входящих уведомлений. Необходимые данные, можно взять на сайтах производителей оборудования или обратившись техподдержку. В нашем случае были использованы MIB файлы раскодирующие сообщения коммутаторов производства cisco.

Таким образом была установлена комбинация:

1. База данных временных рядов на базе плагина TimescaleDB для PostgreSQL
2. В качестве диспетчера, собирающего данные и записывающего их в базу данных, а также оповещающего инженеров при возникающих проблемах используется Zabbix 4.4
3. В качестве интерактивной панели, предоставляющей визуальный доступ к полученным данным и визуальные средства настройки сборщика – Zabbix 4.4 с веб сервером Nginx
4. В качестве получателя и транслятора SNMP traps использованы snmptrapd и snmptt.

Также был настроен удаленный доступ до web сервера zabbix по адресу <https://zbx.ftip.ru/>

### 2.3 Интеграция Zabbix с инфокоммуникационной сетью кафедры ТиИС МПГУ.

Веб мониторинг.

В инфокоммуникационной сети кафедры ТиИС размещено 3 веб сайта:

1. <https://ftip.ru/> – Сайт факультета технологии и предпринимательства.
2. <https://elearning.ftip.ru>/ – Портал электронного обучения кафедры технологических и информационных систем ИФТИС МПГУ.
3. <https://zbx.ftip.ru/> – Панель управления Zabbix.

Одной из задач системы мониторинга является проверка и уведомление инженеров в случае нарушения доступа к данным электронным ресурсам. Для решения этой задачи была создана отдельная группа узлов и в нее были добавлены необходимые узлы – подлежащие мониторингу веб-сайты. Zabbix предполагает два варианта дальнейших действий. Настройка каждого узла отдельно или создание шаблона и последующее прикрепление универсального шаблона к узлам сети. Было принято решение использовать второй способ, поскольку это упростит дальнейшую поддержку в случае масштабирования сети и увеличения количества веб-сайтов для мониторинга. Мной был разработан и настроен универсальный шаблон. Были настроены веб сценарии для проверки доступа к сайтам, созданы графики и написаны триггеры:

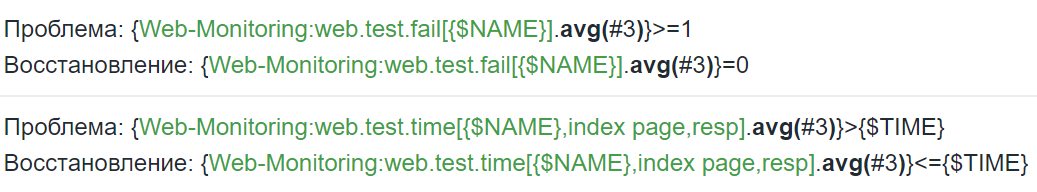
Первый триггер реагирует на отсутствие ответа от веб-сервера по заданному адресу с кодом состояния http – 200.

Триггер срабатывает, когда 2 проверки из последних 3 завершились неудачно. Возникшая проблема считается решенной при получении 2 последовательных положительных значений.

Второй триггер реагирует на длительное время отклика веб-сайта.

С написанным кодом триггеров можно ознакомиться на Рис 1.

Рис 1 Исходный код триггеров



В переменной {$TIME} хранится время отклика, при превышении которого срабатывает триггер, уведомляющий инженеров о возникновении проблемы. При этом сравнение ведется со среднее значение из трех последних.

SNMP traps.

После настройки сервера для отлова и раскодировки SNMP traps от агентов, было необходимо настроить zabbix.

Во-первых было необходимо в конфигурационном файле zabbix\_server.conf включить обработку трапов и указать путь до них.

Во-вторых, был откорректирован формат времени и даты в стандартном шаблон zabbix –– Template Net Cisco IOS SNMPv2.

В-третьих, в настройках zabbix было указано «Журналировать не совпадающие SNMP трапы», для отлова трапа от неизвестного устройства или неизвестного интерфейса известного устройства.

Следующим пунктом интеграции является настройка необходимых для инженера, обслуживающего конкретную инфокоммуникационную сеть, графиков и триггеров.

Настройка мониторинга виртуальных машин.

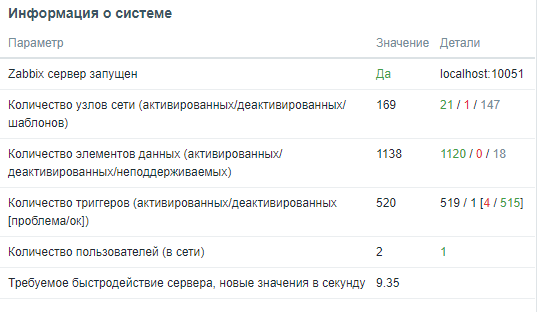
В сети кафедры ТиИС используются виртуальные машины с различными операционными системами (Windows, FreeBSD, Linux и т.д.). Для мониторинга большинства данных виртуальных машин были использованы агенты Zabbix, предварительно размещенные в операционных системах, собирая данные они передают их на Zabbix сервер.

Настройка необходимых к сбору данных выполняется в шаблонах на Zabbix сервере. Создание шаблона для каждой конкретной операционной системы является высоко затратной по времени задачей, требующей большого количества времени. Для решения этой проблемы и создания возможности быстрого разворачивания системы мониторинга в состав Zabbix были включены стандартные шаблоны для различных операционных систем. Так же одним из преимуществ Zabbix является наличие большого сообщества и большой базы шаблонов созданных его членами.

Однако, стоит отметить, что стандартные шаблоны порой являются избыточными и не оптимизированными по многим параметрам. Например, в стандартном шаблоне для операционной системы Windows параметр элемента данных vm.memory.size[total] отвечающий за объем установленного на сервере ОЗУ имеет период обновления 1 минуту. Таким образом Zabbix агент каждую минуту проверяет и отсылает на сервер данные о количестве установленного ОЗУ на ЭВМ находящейся на мониторинге, а Zabbix-server в свою очередь, тратит свои ресурсы на запись этих данных в базу и их хранение. В большинстве случаев не имеет смысла собирать многие метрики с настолько большой регулярностью. По этой причине, для экономия места занимаемым базой данных и вычислительных мощностей сервера, было принято решение на основании стандартных шаблонов, создать свои и отредактировать их.

В результате анализа и перенастройки интервалов в шаблонах, предлагаемых Zabbix по умолчанию, получилось сократить, такой показатель Zabbix-сервера как «Требуемое быстродействие сервера, новые значения в секунду» с 14,67 до 9,35.

Рис 2 Информация о Zabbix-сервере



Построение системы оповещений.

Для уведомления инженеров, планировалось использовать два способа доставки информации. Извещение на почту и средствами мессенджера telegram.

Уведомление на почту в Zabbix было настроено встроенными средствами согласно документации. А вот реализация уведомлений в telegram было реализовано с помощью скрипта. Стоит отметить, что реализация уведомлений в telegram возможна без использования отдельных скриптов, используя встроенные возможности zabbix. Однако в данном решении не реализована отправка графиков вместе с сообщением об ошибке. Поэтому было принято решение использовать рекомендованный сообществом zabbix скрипт.

Таким образом для реализации данного решения, в мессенджере telegram был создан бот и получен токен для доступа к http api telegram.

Для обеспечения большей безопасности, в zabbix был создан пользователь, обладающий правами только на чтение информации.

В имеющийся скрипт была добавлена информация для доступа к telegram и zabbix, после чего он был размещен на сервере и адрес его расположения был указан в конфигурационном файле zabbix\_server.conf.

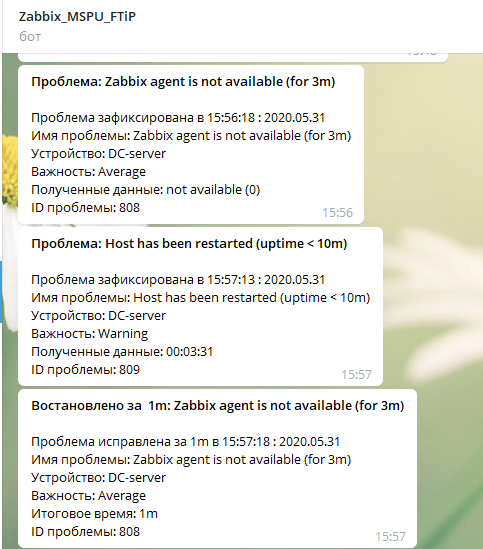
Далее был создан групповой чат для получения уведомлений и его chat\_id был указан в поле получатель сообщений в zabbix.

Последним пунктом настройки были отредактированы операции действий при создании проблем, в сообщение по умолчанию было добавлено:

Item Graphic: [{ITEM.ID1}] – для передачи графика. И в выражение по восстановлению был добавлен параметр Total time: {EVENT.AGE} – сообщающий время, прошедшее с появления проблемы до её решения.

Пример результата работы можно увидеть на Рис 3

Рис 3 Пример оповещений в мессенджере Telegram



Построение интерактивных карт сети.

Веб интерфейс Zabbix предоставляет возможность настроить интерактивные карты сети, которые удобно использовать, для комплексной оценки ситуации при возникновении множества проблем.

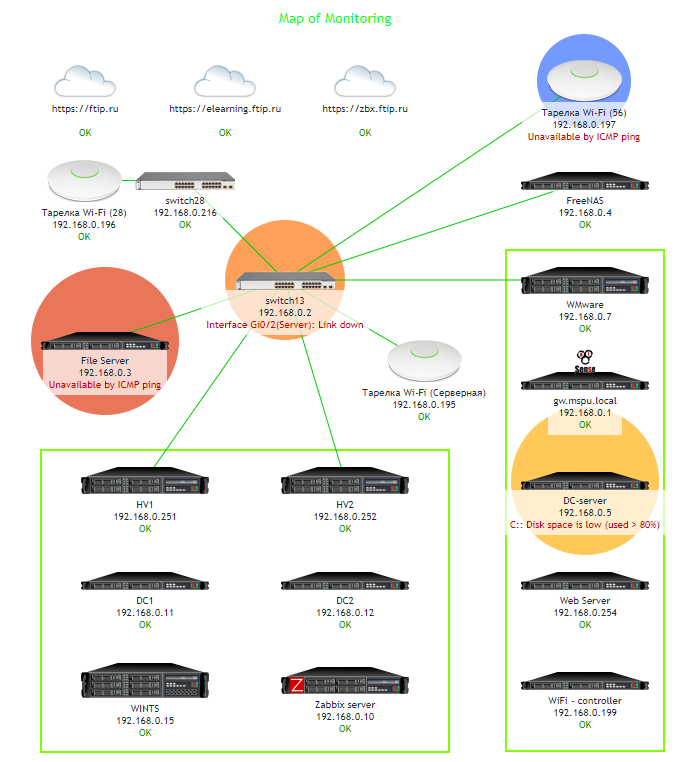
Для этой цели мной была построена карта мониторинга, пример её работы можно увидеть на Рис 3. Для определения уровня проблемы используется цветовая градация от синего означающего предупреждение, до багрового означающего критическую проблему.

Для интерактивного вывода названий узлов сети были использованы переменные {HOST.NAME} – в которой хранится имя узла и {HOST.CONN} – в которой хранится адрес узла.

Также на сервер Zabbix были добавлены недостающие иконки и связаны с имеющимися узлами сети.

Как видно на Рис 3 в момент создания данного снимка карты сети, в инфокоммуникационной сети кафедры ТиИС была зафиксирована проблема с приоритетом «Важная», заключающаяся в недоступности файл-сервера.

Рис 4 Пример построенной карты сети с интерактивным отображением проблем



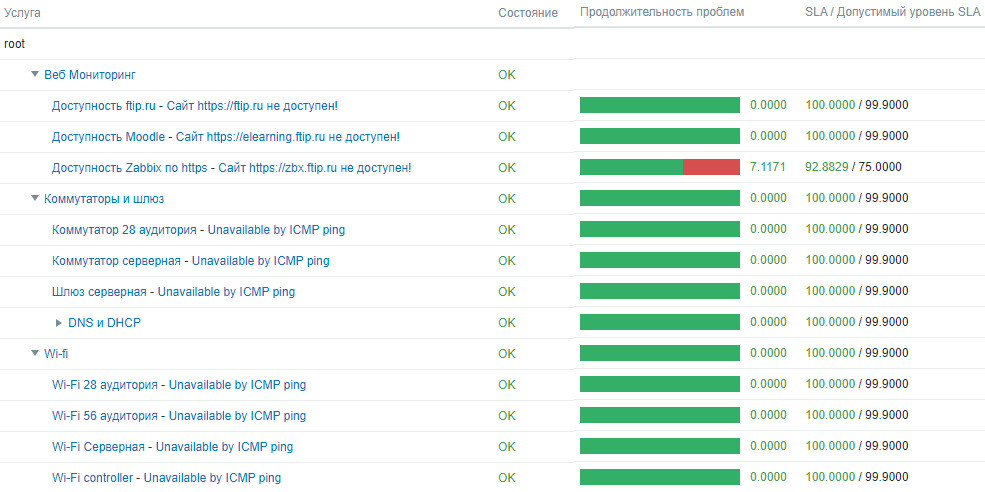
Услуги

Услугами в системах мониторинга, таких как Zabbix, пользуются те, кому необходимо получить данные более высокого уровня. В ряде случаев пользователи системы мониторинга не заинтересованы в низкоуровневых процессах, таких как, например, загрузка канала до сервера. Их интересует именно доступность того или иного сервиса предоставляемого инженерами инфокоммуникационной сети, например веб портала или доступность сети wi-fi. Услуги в Zabbix дают возможность получить данную информацию.

В инфокоммуникационной сети кафедры ТиИС были настроены услуги, считающие уровень соглашения об уровне предоставления услуги (SLA). При настройке расчета SLA в инфокоммуникационной сети кафедры ТиИС, необходимо было учесть, то что нас не интересует доступность сетей Wi-Fi в не рабочее время организации, но при этом возможность доступа до веб-порталов должна осуществляться круглосуточно. Так же необходимо было учесть, что например, для работоспособности всей инфокоммуникационной сети, достаточно работоспособности хотя бы одного сервера контроллера домена из существующих трех.

Результат отображения настроенных услуг можно увидеть на Рис 5

Рис 5 Услуги в инфокоммуникационной сети кТиИС



Обновление Zabbix 4.4 до Zabbix 5.0 LTS

В связи с выходом Zabbix версии 5.0 с длительным периодом поддержки, а также с возможностью автоматического сжатия данных была поставлена задача обновления программного обеспечения и перехода на новую версию. Однако стоит отметить, что поддержка сжатия данных в СУБД PostgreSQL и возможность использования расширенного диапазона числовых значений возможна с СУБД PostgreSQL только начиная с 12 версии, в то время, как с zabbix 4.4 было рекомендовано использовать PostgreSQL 10 версии, кроме того, на момент установки, 12 версия не имела официальной поддержки TimescaleDB. В следствии этого возникла необходимость в обновлении PostgreSQL и Timescaledb до последних версий.

Для этого была установлена и развернута PostgreSQL версии 12 с плагином TimescaleDB и настроен файл конфигурации, на работу с Zabbix и для соответствия конфигурации имеющейся PostgreSQL 10. В имеющейся СУБД PostgreSQL 10, был обновлен плагин TimescaleDB до последней актуальной версии 1.7.0. Таким образом были приведены в соответствие имеющийся и подготавливаемый кластер СУБД Postgres. После чего база данных была скопирована в новый кластер, а изначальный кластер был удален вместе с пакетами PostgreSQL 10.

Последним шагом было использование патча БД, предлагаемого в документации к Zabbix 5.0:

ALTER TABLE ONLY trends

ALTER COLUMN value\_min TYPE DOUBLE PRECISION,

ALTER COLUMN value\_min SET DEFAULT '0.0000',

ALTER COLUMN value\_avg TYPE DOUBLE PRECISION,

ALTER COLUMN value\_avg SET DEFAULT '0.0000',

ALTER COLUMN value\_max TYPE DOUBLE PRECISION,

ALTER COLUMN value\_max SET DEFAULT '0.0000';

ALTER TABLE ONLY history

ALTER COLUMN value TYPE DOUBLE PRECISION,

ALTER COLUMN value SET DEFAULT '0.0000';

Однако, стоит отметить, недопустимость данного патча в конфигурации СУБД PostgreSQL 12 с плагином TimescaleDB. Для корректной работы, патч был отредактирован:

ALTER TABLE trends

ALTER COLUMN value\_min TYPE DOUBLE PRECISION,

ALTER COLUMN value\_min SET DEFAULT '0.0000',

ALTER COLUMN value\_avg TYPE DOUBLE PRECISION,

ALTER COLUMN value\_avg SET DEFAULT '0.0000',

ALTER COLUMN value\_max TYPE DOUBLE PRECISION,

ALTER COLUMN value\_max SET DEFAULT '0.0000';

ALTER TABLE history

ALTER COLUMN value TYPE DOUBLE PRECISION,

ALTER COLUMN value SET DEFAULT '0.0000';

Таким образом база данных и Zabbix сервер был успешно обновлен до новой версии и как следствие была включена возможность архивации старых метрик с целью экономии пространства, потребляемого для хранения данных. Подробно о процессе обновления можно прочитать в приложении 4.

## Заключение

В ходе обучения в университете я изучал сетевые технологии в сетевой академии Cisсo и системное администрирование в процессе обучения мной были выявлены недостатки и перебои в работе инфокоммуникационной сети кафедры ТиИС. Мы решили, что способствовать решению этой проблемы может помочь разворачивание системы мониторинга в инфокоммуникационной сети кафедры.

Я выбрал тему моей ВКР, поскольку развитие инфокоммуникационных сетей, требует быстрого предупреждающего ответа на возникающие в данных сетях проблемы. Системы мониторинга, развернутые в инфокоммуникационных сетях, способствуют решению данной задачи.

В ходе дипломного исследования нужно было решить следующие задачи:

1. Проанализировать распространённые системы мониторинга инфокоммуникационных сетей и их компоненты.
2. Составить перечень оборудования и сервисов, развернутых в инфокоммуникационной сети кафедры ТиИС.
3. Развернуть систему мониторинга на выделенном оборудовании. Интегрировать систему мониторинга с имеющейся инфраструктурой инфокоммуникационной сети.

В результате были проанализированы наиболее популярные системы мониторинга. Были выявлены их достоинства и недостатки. Так же была исследована сеть кафедры технологии и информационных систем ИФТИС МПГУ и в данной сети была развернута система мониторинга Zabbix 5.0 LTS с базой данных временных рядов Timescale под управлением PostgreSQL 12.

## Список литературы

1. Актуальность современных систем удаленного мониторинга вычислительных ресурсов [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/aktualnost-sovremennyh-sistem-udalennogo-monitoringa-vychislitelnyh-resursov/viewer. – Актуальность современных систем удаленного мониторинга вычислительных ресурсов. – (Дата обращения: 16.04.2020)
2. Воробиенко, П.П. Инфокоммуникации: термины и определения [Текст] / П.П. Воробиенко, Л.А. Никитюк // Научный журнал «Восточно-Европейский журнал передовых технологий» //. - Харьков: Технологический центр, 2011. - №6/2 (54), с. 4-6.
3. Новая парадигма промышленного развития Германии. Стратегия «Индустрия 4.0» URL: https://cyberleninka.ru/article/n/novaya-paradigma-promyshlennogo-razvitiya-germanii-strategiya-industriya-4-0/viewer (Дата обращения: 16.09.2019)
4. Обзор доменных служб Active Directory | Microsoft Docs [Электронный ресурс]. – Режим доступа: https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview. – Обзор доменных служб Active Directory. –(Дата обращения: 23.12.2019)
5. Постановление Правительства РФ от 12 августа 2014 г. N 801 "О внесении изменений в некоторые акты Правительства Российской Федерации" | Гарант [Электронный ресурс]. – Режим доступа: https://base.garant.ru/70719564/. – Постановление Правительства РФ от 12 августа 2014 г. N 801 "О внесении изменений в некоторые акты Правительства Российской Федерации". – (Дата обращения:14.03.2020)
6. Постановление Правительства РФ от 31 июля 2014 г. N 758 "О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" | Гарант [Электронный ресурс]. – Режим доступа: https://base.garant.ru/70710076/. – Постановление Правительства РФ от 31 июля 2014 г. N 758 "О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей". – (Дата обращения: 13.03.2020)
7. Руководство по внедрению IBM Tivoli Monitoring 6.1 [Электронный ресурс]. – Режим доступа: https://www.ibm.com/developerworks/ru/library/tivoli\_monitoring/ch1/ch1.html. – Руководство по внедрению IBM Tivoli Monitoring 6.1. – (Дата обращения: 01.04.2020)
8. Тищенко К.К. Опыт развертывания инфраструктуры МЭШ в школах города Москвы / К.К. Тищенко//Тищенко К.К. Интеграция науки, технологии и образования: ИНТО-2019 Материалы межрегиональной конференции (с международным участием) молодых исследователей, студентов, магистрантов, аспирантов и молодых учителей, посвящённой 150-летию со дня рождения А. С. Чаплыгина / К.К. Тищенко, Д.С. Горелко. – М. : ИИУ МГОУ, 2019. – 116 с.
9. Федеральный закон о внесении изменений в федеральный закон "об информации, информационных технологиях и о защите информации" и отдельные законодательные акты российской федерации по вопросам упорядочения обмена информацией с использованием / КонсультантПлюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons\_doc\_law\_162586/. – Федеральный закон "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей" от 05.05.2014 N 97-ФЗ (последняя редакция). – (Дата обращения: 13.03.2020)
10. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc3411. – An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. ­ (Дата обращения: 28.04.2020)
11. Architectural Principles of Uniform Resource Name Resolution [Электронный доступ]. – Режим доступа: https://www.ietf.org/rfc/rfc2276. – Architectural Principles of Uniform Resource Name Resolution. – (Дата обращения: 26.04.2020)
12. Cacti – The Complete RRDTool-based Graphing Solution [Электронный ресурс]. –Режим доступа: https://www.cacti.net/. – About Cacti. – (Дата обращения: 28.03.2020)
13. Cisco Application Policy Infrastructure Controller (APIC) - Cisco Application Policy Infrastructure Controller Data Sheet [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/application-policy-infrastructure-controller-apic/datasheet-c78-739715.html. – Cisco Application Policy Infrastructure Controller Data Sheet. – (Дата обращения: 27.03.2020)
14. Cisco Networking Academy Builds IT Skills & Education For Future Career [Электронный ресурс]. – Режим доступа: https://netacad.com. – Empowering all people with career possibilities. – (Дата обращения: 26.03.2020)
15. Community – Icinga [Электронный ресурс]. – Режим доступа: https://icinga.com/community/. – The Icinga Community. – (Дата обращения: 06.04.2020)
16. Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc1904. – Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2). – (Дата обращения: 27.04.2020)
17. Documentation | Prometheus [Электронный ресурс]. – Режим доступа: https://prometheus.io/docs/. – Documentation | Prometheus. – (Дата обращения: 28.03.2020)
18. Grafana documentation | Grafana Labs [Электронный ресурс]. –Режим доступа: https://grafana.com/docs/grafana/latest/. – Grafana documentation. – (Дата обращения: 04.04.2020)
19. Influxdb: Purpose-Built Open Source Time Series Database [Электронный ресурс]. – Режим доступа: https://www.influxdata.com/. – InfluxDB is the open source time series database. – (Дата обращения:01.04.2020)
20. Introduction and Applicability Statements for Internet Standard Management Framework [Электронный доступ]. – Режим доступа: https://www.ietf.org/rfc/rfc3410. – Introduction and Applicability Statements for Internet Standard Management Framework. – (Дата обращения: 26.04.2020)
21. Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc1907. – Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2). – (Дата обращения: 28.04.2020)
22. Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc3412. – Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). – (Дата обращения: 28.04.2020)
23. Nagios - The Industry Standard In IT Infrastructure Monitoring [Электронный ресурс]. – Режим доступа: https://www.nagios.org/. – What can Nagios help you do?. – (Дата обращения: 25.03.2020)
24. Nginx [Электронный ресурс]. – Режим доступа: https://nginx.org/ru/. – nginx. – (Дата обращения: 10.04.2020)
25. Nginx vs Apache: Which Web Server Is the Best? (2020 Edition) [Электронный ресурс]. – Режим доступа: https://kinsta.com/blog/nginx-vs-apache/. – Nginx vs Apache: Web Server Showdown. – (Дата обращения: 12.02.2020)
26. Official Ubuntu Documentation [Электронный ресурс]. – Режим доступа: https://help.ubuntu.com/. – Official Ubuntu Documentation. – (Дата обращения: 26.03.2020)
27. PostgreSQL: The world's most advanced open source relational database [Электронный ресурс]. ­ Режим доступа: https://www.postgresql.org/. – PostgreSQL: The World's Most Advanced Open Source Relational Database. – (Дата обращения: 24.03.2020)
28. Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc1905. – Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2). – (Дата обращения: 26.04.2020)
29. RFC 1157 - Simple Network Management Protocol (SNMP) [Электронный доступ]. – Режим доступа: https://tools.ietf.org/html/rfc1157. – A Simple Network Management Protocol (SNMP). – (Дата обращения: 26.04.2020)
30. RFC 1901 - Introduction to Community-based SNMPv2 [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc1901. – Introduction to Community-based SNMPv2. – (Дата обращения: 26.04.2020)
31. RFC 1908 - Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework [Электронный ресурс]. – Режим доступа: https://tools.ietf.org/html/rfc1908. – Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework. – (Дата обращения: 26.04.2020)
32. Simple Network Management Protocol (SNMP) Applications [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc3413. – Simple Network Management Protocol (SNMP) Applications. – (Дата обращения: 28.04.2020)
33. Snmp-12-4t-book.pdf [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/12-4t/snmp-12-4t-book.pdf. – SNMP Configuration Guide, Cisco IOS Release 12.4T. – (Дата обращения: 13.04.2020)
34. SNMPTT [Электронный ресурс]. – Режим доступа: http://www.snmptt.org/. – SNMP Trap Translator. – (Дата обращения: 06.04.2020)
35. SNMPv3 Applications [Электронный доступ]. – Режим доступа: https://www.ietf.org/rfc/rfc2273. – SNMPv3 Applications. – (Дата обращения: 26.04.2020)
36. Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc1902. – Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2). – (Дата обращения: 26.04.2020)
37. Telegram APIs [Электронный ресурс]. – Режим доступа: https://core.telegram.org/api. – Telegram APIs. – (Дата обращения: 28.12.2019)
38. Telegram-notify/Zabbix-telegram/sh master Paolo Capelli / Zabbix Git Lab [Электронный ресурс]. – Режим доступа: https://git.cdp.li/polcape/zabbix/-/blob/master/telegram-notify/zabbix-telegram.sh. – zabbix-telegram.sh. –(Дата обращения: 20.04.2020)
39. Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc1903. – Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2). – (Дата обращения: 26.04.2020)
40. The OpenNMS Group, Inc. [Электронный ресурс]. – Режим доступа: https://www.opennms.com/. – THE OPENNMS GROUP PRODUCT SUITE. – (Дата обращения: 03.04.2020)
41. Time series данные в реляционной СУБД. Расширения TimescaleDB и PipelineDB для PostgreSQL / Блог компании Конференции Олега Бунина (Онтико) / Хабр [Электронный ресурс]. – Режим доступа:https://habr.com/ru/company/oleg-bunin/blog/464303/. ­ Time series данные в реляционной СУБД. Расширения TimescaleDB и PipelineDB для PostgreSQL. – (Дата обращения: 14.04.2020)
42. Time-series data simplified | Timescale [Электронный ресурс]. – Режим доступа: https://www.timescale.com/. – All of your time-series data, instantly accessible. – (Дата обращения: 21.03.2020)
43. Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc1906. – Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2). – (Дата обращения: 27.04.2020)
44. TUT:Configuring snmptrapd – Net-SNMP Wiki [Электронный ресурс]. – Режим доступа: http://net-snmp.sourceforge.net/wiki/index.php/TUT:Configuring\_snmptrapd. – TUT:Configuring snmptrapd. – (Дата обращения: 07.04.2020)
45. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) [Электронный доступ]. – Режим доступа: https://www.ietf.org/rfc/rfc2274. – User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). – (Дата обращения: 26.04.2020)
46. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc3414. – User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). – (Дата обращения: 28.04.2020)
47. View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc2275. – View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
48. View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) [Электронный ресурс]. – Режим доступа: https://www.ietf.org/rfc/rfc3415. – View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). – (Дата обращения: 29.04.2020)
49. Welcome! – The Apache HTTP Server Project [Электронный ресурс]. – Режим доступа: https://httpd.apache.org/. – Apache HTTP Server Project. – (Дата обращения: 27.12.2019)
50. Zabbix Manual [Zabbix Documentation 5.0] [Электронный ресурс]. – Режим доступа: https://www.zabbix.com/documentation/current/manual. – Zabbix Documentation 5.0. – (Дата обращения: 20.03.2020)

## Приложение 1. Настройка SNMPv2 на оборудовании производства компании Cisco

Настройка оборудования Cisco

1. Настройка строки сообщества и уровень доступа («Только чтение» или «Чтение и запись»):

snmp-server community *string* ro | rw

1. Назначьте получателя ловушек:

snmp-server host *ip* [version{1| 2c | 3 [auth | noauth | priv]}] *community-string*.

3) Включите ловушки на агенте SNMP

snmp-server enable traps *notification-types*

Без указания типа ловушек – будут отправляться все.

(Примечание. По умолчанию в SNMP не установлены ловушки. Без этой команды диспетчеры SNMP должны будут проводить опрос для получения всей существенной информации.)

Дополнительно:

Настройка местоположения устройства:

snmp-server location *text*

Зафиксируйте системный контакт:

snmp-server contact *mail@gmail.com*

Ограничение доступа по SNMP:

ip access-list standard *NAME*

permit *ip*

snmp-server community *string* ro | rw *NAME*

Просмотр настроек:

show snmp

show snmp community

## Приложение 2

Настройка веб мониторинга.

Про шаблон. Макросы. Триггеры. Услуги.

## Приложение 3. Разворачивание Zabbix 4.4 на Ubuntu 18.04 LTS

1. Добавляем репозиторий:

sudo wget https://repo.zabbix.com/zabbix/4.4/ubuntu/pool/main/z/zabbix-release/zabbix-release\_4.4-1+bionic\_all.deb

sudo dpkg -i zabbix-release\_4.4-1+bionic\_all.deb

sudo apt update

1. Устанавливаем необходимые пакеты:

sudo apt install zabbix-server-pgsql zabbix-frontend-php php7.2-pgsql zabbix-nginx-conf zabbix-agent

1. Редактируем ошибки в конфигурационых файлах nginx.

sudo nano /etc/zabbix/nginx.conf

Необходимо расскоментировать:

# listen 80;

# server\_name example.com;

sudo nano /etc/nginx/sites-available/default

Необходимо закомментировать:

# listen 80;

# server\_name example.com;

1. Указываем пароль к базе данных:

sudo nano /etc/zabbix/zabbix\_server.conf

DBPassword=’Пароль’

1. Указываем часовой пояс.

sudo nano /etc/zabbix/php-fpm.conf

php\_value[date.timezone] = Europe/Moscow

1. Проверяем файлы nginx перезапускаем.

sudo nginx -t

sudo systemctl restart nginx

1. Подготавливаем базу данных:

sudo -u postgres createuser --pwprompt zabbix

sudo -u postgres createdb -O zabbix -E Unicode -T template0 zabbix

sudo zcat /usr/share/doc/zabbix-server-pgsql/create.sql.gz | sudo -u zabbix psql zabbix

sudo echo "deb http://apt.postgresql.org/pub/repos/apt/ $(lsb\_release -c -s)-pgdg main" | sudo tee /etc/apt/sources.list.d/pgdg.list

sudo wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | sudo apt-key add -

sudo apt-get update

1. Добавляем и настраиваем плагин базы данных временных рядов.

sudo add-apt-repository ppa:timescale/timescaledb-ppa

sudo apt-get update

sudo apt install timescaledb-postgresql-10

sudo systemctl status postgresql

psql --version

sudo timescaledb-tune -pg-version 10

sudo service postgresql restart

sudo echo "CREATE EXTENSION IF NOT EXISTS timescaledb CASCADE;" | sudo -u postgres psql zabbix

sudo cat /usr/share/doc/zabbix-server-pgsql/timescaledb.sql | sudo -u zabbix psql zabbix

1. Перезапускаем демоны и добавляем в автозагрузку.

sudo systemctl restart zabbix-server zabbix-agent nginx php7.2-fpm

sudo systemctl enable zabbix-server zabbix-agent nginx php7.2-fpm

## Приложение 4. Обновление Zabbix 4.4 до версии 5.0 LTS

Обновление Zabbix сервера.

1. Останавливаем заббикс-сервер.

sudo systemctl stop zabbix-server

1. Сделайте резервную копию вашей БД и конфигурационных файлов.
2. Для продолжения обновления удалите текущий и установите новый пакет репозитория Zabbix.

sudo rm -Rf /etc/apt/sources.list.d/zabbix.list

sudo wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_5.0-1+bionic\_all.deb

sudo dpkg -i zabbix-release\_5.0-1+bionic\_all.deb

sudo apt-get update

1. Обновляем составные части zabbix

sudo apt-get install --only-upgrade zabbix-server-pgsql zabbix-frontend-php zabbix-agent

1. Задаем конфигурацию zabbix

sudo nano /etc/zabbix/zabbix\_server.conf

Как минимум необходимо задать:

DBPassword=

SNMPTrapperFile=/var/log/snmptrap/snmptrap.log

StartSNMPTrapper=1

Для корректного обновления Nginx, устанавливаем пакет

sudo apt-get install zabbix-nginx-conf

1. Запускаем заббикс сервер и заббикс агент.

sudo service zabbix-server start

sudo service zabbix-agent start

1. Проверить корректность обновления базы данных можно командой:

sudo cat /var/log/zabbix/zabbix\_server.log | grep database

Обновление PostgreSQL 10 до 12 версии

1. Установка PostreSQL 12 версии и плагина timesacledb

sudo apt-get install postgresql-12 postgresql-server-dev-12 timescaledb-postgresql-12

1. Настройка timescaledb.

sudo timescaledb-tune

1. Обновление имеющегося плагина TimescaleDB в PostgreSQL 10

sudo su postgres

cd

cd 12/

psql --cluster 10/main zabbix

ALTER EXTENSION timescaledb UPDATE;

exit

1. Остонавливаем службу PostgreSQL

sudo systemctl stop postgresql

1. Сравниваем кластеры.

sudo su postgres

cd

cd 12/

/usr/lib/postgresql/12/bin/pg\_upgrade \

--old-datadir=/var/lib/postgresql/10/main \

--new-datadir=/var/lib/postgresql/12/main \

--old-bindir=/usr/lib/postgresql/10/bin \

--new-bindir=/usr/lib/postgresql/12/bin \

--old-options '-c config\_file=/etc/postgresql/10/main/postgresql.conf' \

--new-options '-c config\_file=/etc/postgresql/12/main/postgresql.conf' \

--check

1. В случае успешного сравнения переносим данные. Не забываем указать ключ -O "-c timescaledb.restoring='on'".

/usr/lib/postgresql/12/bin/pg\_upgrade --old-datadir=/var/lib/postgresql/10/main --new-datadir=/var/lib/postgresql/12/main --old-bindir=/usr/lib/postgresql/10/bin --new-bindir=/usr/lib/postgresql/12/bin --old-options '-c config\_file=/etc/postgresql/10/main/postgresql.conf' --new-options '-c config\_file=/etc/postgresql/12/main/postgresql.conf' -O "-c timescaledb.restoring='on'"

exit

1. Меняем порты в конфигурациях PostgreSQL 10 и 12

sudo nano /etc/postgresql/12/main/postgresql.conf

# ...and change "port = 5433" to "port = 5432"

sudo nano /etc/postgresql/10/main/postgresql.conf

# ...and change "port = 5432" to "port = 5433"

1. Запускаем службы и проверяем статус.

sudo systemctl start postgresql

sudo systemctl status postgresql

1. Проверяем версию и запускаем сгенерированный скрипт. Стоит отметить, что при больших размерах базы данных, данная операция может занять продолжительное время.

sudo su postgres

cd

cd 12/

psql -c "SELECT version();"

./analyze\_new\_cluster.sh

exit

1. Проверяем установленные пакеты старой версии и удалеям.

apt list --installed | grep postgresql

sudo apt-get remove postgresql-10 postgresql-client-10 timescaledb-loader-postgresql-10 timescaledb-postgresql-10

1. Удаляем старую конфигурацию

sudo rm -rf /etc/postgresql/10/

1. Удаляем старый кластер.

sudo su postgres

cd

cd 12/

./delete\_old\_cluster.sh

1. Удаляем сгенерированные скрипты.

rm ./delete\_old\_cluster.sh

rm ./analyze\_new\_cluster.sh

Процесс обновления СУБД PostgreSQL и переноса базы данных завершен.

Применение патча.

1. Перейдем на пользователя postgres

sudo su postgres

cd

cd 12/

1. Скачаем патч

wget https://git.zabbix.com/projects/ZBX/repos/zabbix/raw/database/postgresql/double.sql

1. Отредактируем патч, для работы с плагином Timescaledb, для этого откроем его текстовым редактором и удалим флаги «ONLY»
2. Применим патч:

psql zabbix <double.sql

1. Отредактируем конфигурацию Zabbix сервера, включив поддержку расширенного диапазона числовых значений

sudo nano /etc/zabbix/web/zabbix.conf.php

$DB['DOUBLE\_IEEE754'] = 'true';

1. Перезагрузим и проверим статус работы Zabbix сервера.

sudo systemctl restart zabbix-server.service

sudo systemctl status zabbix-server.service

1. Включим сжатие данных в веб интерфейсе Zabbix.