МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

Московский педагогический государственный университет

Институт физики, технологии и информационных систем

Кафедра технологических и информационных систем

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

**БАКАЛАВРА**

на тему

«Мониторинг технического состояния сетевых устройств в образовательной организации»

Студента 4 курса

Направление подготовки: 09.03.02 Информационные системы и технологии

Профиль Информационные технологии в образовании

Тищенко Константина Константиновича

|  |  |
| --- | --- |
| Научный руководитель: | Горелко Д.С., ст.п. КТиИС |
|  |  |

|  |
| --- |
| Дипломная работа допущена |
| к защите перед Итоговой государственной |
| аттестационной комиссией |
|  |
| Заведующий кафедрой ТиИС  Нижников А.И. |

УТВЕРЖДАЮ

Заведующий кафедрой КТиИС

\_\_\_\_\_\_\_\_\_\_\_\_\_ Нижников А.И.

«\_\_\_» 20\_\_г.

**ЗАДАНИЕ**

**на разработку выпускной квалификационной работы**

студента ИФТИС

Тищенко Константина Константиновича

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

**Тема закреплена приказом ректора от** «\_\_\_\_» ­­­\_\_\_\_\_\_\_\_20\_\_ 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 сетевого мониторинга и их компоненты.*
2. *Составить перечень оборудования и сервисов, развернутых в инфокоммуникационной сети образовательной организации, построить карту сети. Определить наиболее подходящие системы мониторинга для данной инфокоммуникационной сети.*
3. *Развернуть систему мониторинга на выделенном оборудовании. Интегрировать систему мониторинга с имеющейся инфраструктурой инфокоммуникационной сети.*
4. *Оценить техническое состояние имеющейся сетевой инфраструктуры образовательной организации. Разработать справочную документацию к внедренной системе мониторинга.*

**Руководитель: ст.п. КТиИС, Горелко Д.С.**

«\_\_\_\_» \_\_\_\_\_\_\_\_\_20\_\_\_ г.

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

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_ 20\_\_\_г.

Оглавление

[Введение 5](#_Toc39810599)

[Глава 1. Системы мониторинга 8](#_Toc39810600)

[1.1 Понятие системы мониторинга и компонентов 8](#_Toc39810601)

[1.2 Требования к системе мониторинга в инфокоммуникационной сети образовательной организации 13](#_Toc39810602)

[1.3 Система мониторинга для образовательной организации 14](#_Toc39810603)

[Глава 2. Название??? 19](#_Toc39810604)

[2.1 Инфокоммуникационная сеть кафедры ТиИС МПГУ 19](#_Toc39810605)

[2.2 Разворачивание Zabbix 21](#_Toc39810606)

[2.3 Интеграция Zabbix с инфокоммуникационной сетью кафедры ТиИС МПГУ 22](#_Toc39810607)

[Заключение 23](#_Toc39810608)

[Список литературы 24](#_Toc39810609)

[Приложение 1 25](#_Toc39810610)

## 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 сетевого мониторинга и их компоненты.

2. Составить перечень оборудования и сервисов, развернутых в инфокоммуникационной сети образовательной организации, построить карту сети. Определить наиболее подходящие системы мониторинга для данной инфокоммуникационной сети.

3. Развернуть систему мониторинга на выделенном оборудовании. Интегрировать систему мониторинга с имеющейся инфраструктурой инфокоммуникационной сети.

4. Оценить техническое состояние имеющейся сетевой инфраструктуры образовательной организации. Разработать справочную документацию к внедренной системе мониторинга.

## Глава 1. Системы мониторинга

### Понятие системы мониторинга и компонентов

Понятие мониторинга. Состовляющие системы мониторинга. Базы данных. Протокол snmp. Работа агентов мониторига. Визуализация данных.

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.

//Можно добавить про RRD

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 ссылка на таблицу

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 |

Таблица 1 Сравнение версий SNMP

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.

Можно добавить про OID

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.

|  |  |  |
| --- | --- | --- |
|  | 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 |

Таблица 2 Преимущества и недостатки агентов разных типов

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.

### Требования к системе мониторинга в инфокоммуникационной сети образовательной организации

Понятие инфокоммуникационные сети. Особенности инфокоммуникационных сетей 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.

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

//Тут, наверное, нужно еще что-то будет написать

### Система мониторинга для образовательной организации

Небольшая подводка. Перечисление систем мониторинга с небольшим описанием. Краткий вывод – заббикс.

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 использовать следующий набор:

В качестве сборщика метрик использовать Zabbix 4.4 со следующим набором компонентов, при этом заменить web-сервер, используемый по умолчанию на nginx, в качестве базы данных использовать PostgreSQL с расширением TimescaleDB и PipelineDB.

## Глава 2. Название???

### 2.1 Инфокоммуникационная сеть кафедры ТиИС МПГУ

Описание сети кафедры.

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 ссылку на таблицу при финальном редактировании:

|  |  |  |  |
| --- | --- | --- | --- |
| 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

### 2.2 Разворачивание Zabbix

Разворачивание операционной системы(Про Lvm). Разворачивание заббикс сервера и базы данных. SNMP traps.

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 расшифровывающие 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

Настройка общая, мониторинга и системы оповещений (telegram и почта). SNMP traps.

Настройка мониторинга виртуальных машин.

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:

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

Проблема: {MyTemplate Sites:web.test.fail[Веб мониторинг].avg(#3)}>=1

Восстановление: {MyTemplate Sites:web.test.fail[Веб мониторинг].avg(#2)}=0

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

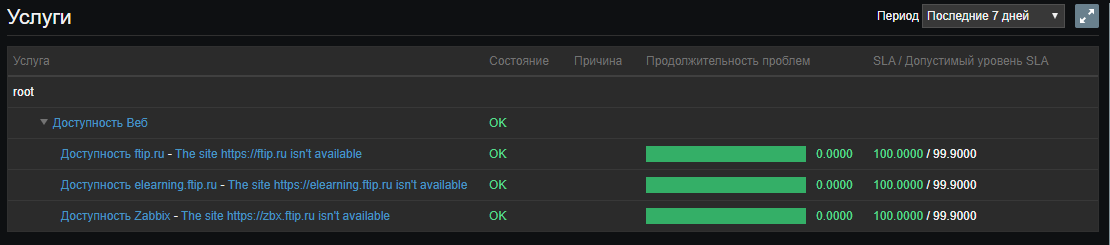
1. Второй триггер реагирует на длительное время отклика веб-сайта.

Проблема: {MyTemplate Sites:web.test.time[Веб мониторинг,Index,resp].avg(#3)}>{$TIME}

Восстановление: {MyTemplate Sites:web.test.time[Веб мониторинг,Index,resp].avg(#3)}<={$TIME}

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.

Так же были настроены услуги, высчитывающие уровень SLA, результат можно увидеть на РИСУНКЕ НОМЕР.



Подробно о настройке веб мониторинга можно прочитать в Приложении НОМЕР.

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.

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. Текст скрипта можно найти в приложении номер.

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.

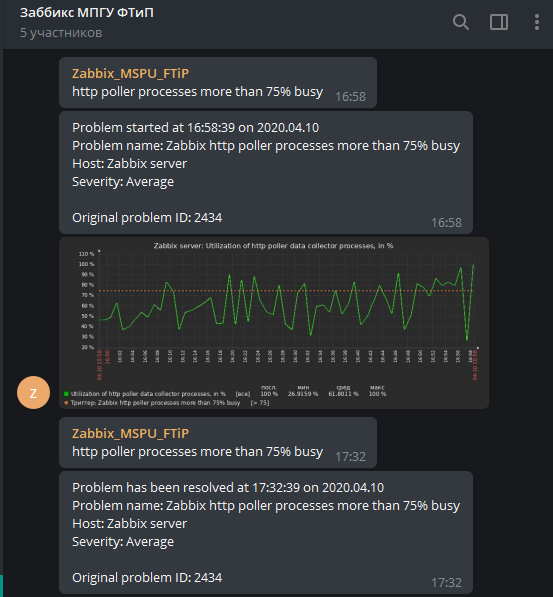
В имеющийся скрипт была добавлена информация для доступа к telegram и zabbix, после чего он был размещен на сервере и адрес его расположения был указан в конфигурационном файле zabbix\_server.conf.

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 рисунке номер.



Построение карт сети.

Услуги

## Заключение

## Список литературы

25 наименований

1. 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.
2. 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)
3. Ссылку на мою статью с Д.С. Горелко о МЭШ
4. Ссылки на RFC к SNMP
5. <https://kinsta.com/blog/nginx-vs-apache/>

## Приложение 1

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.