УДК 004.42

РАЗРАБОТКА ПРОЕКТА СИСТЕМЫ МОНИТОРИНГА СЕРВЕРОВ И СЕТЕВОГО ОБОРУДОВАНИЯ ОРГАНИЗАЦИИ СРЕДСТВАМИ ZABBIX

Макаров Д.В.

Студент,

Калужский государственный университет им. К. Э. Циолковского,

Калуга, Россия

Сорочан В. В.

Кандидат физико-математических наук, доцент кафедры информатики и информационных технологий,

Калужский государственный университет им. К. Э. Циолковского,

Калуга, Россия

Аннотация. В статье рассматривается процесс внедрения системы централизованного мониторинга IT-инфраструктуры организации на базе Zabbix. Проведён анализ существующей инфраструктуры организации, включающей серверное оборудование, рабочие станции, сетевые устройства и удалённые подразделения, а также выявлены основные проблемы сопровождения: отсутствие централизованного контроля, сложность мониторинга удалённых филиалов и позднее обнаружение неисправностей. Выполнен анализ существующих систем мониторинга и обоснован выбор платформы Zabbix как наиболее подходящего решения для организации. В ходе практической реализации выполнена установка и настройка сервера мониторинга, подключение оборудования с использованием Zabbix Agent, SNMP и ICMP, настройка шаблонов мониторинга, панелей Dashboard и системы автоматических уведомлений. В результате внедрения обеспечен централизованный контроль состояния IT-инфраструктуры, сокращено время

обнаружения неисправностей и повышена оперативность реагирования на инциденты.

Ключевые слова: IT-инфраструктура, система мониторинга, Zabbix, сетевое оборудование, Zabbix Agent, SNMP, ICMP, автоматизация мониторинга, централизованный контроль.

DEVELOPMENT OF A PROJECT FOR A MONITORING SYSTEM FOR SERVERS AND NETWORK EQUIPMENT OF AN ORGANIZATION USING ZABBIX TOOLS

Makarov D.V.
Student,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Sorochan V.V.
Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Computer Science and Information Technology,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Abstract. The article discusses the process of implementing a centralized monitoring system for an organization's IT infrastructure based on Zabbix. The analysis of the existing infrastructure of the organization, including server equipment, workstations, network devices and remote units, was carried out, and the main maintenance problems were identified: lack of centralized control, complexity of monitoring remote branches and late detection of malfunctions. The analysis of existing monitoring systems was performed and the choice of the Zabbix platform as the most suitable solution for the organization was justified. During the practical implementation, the monitoring server was installed and configured, equipment was connected using Zabbix Agent, SNMP

and ICMP, monitoring templates, dashboards and automatic notification systems were configured. As a result of the implementation, centralized monitoring of the state of the IT infrastructure has been provided, the time for fault detection has been reduced and the responsiveness to incidents has been increased.
Keywords: IT infrastructure, monitoring system, Zabbix, network equipment, Zabbix Agent, SNMP, ICMP, monitoring automation, centralized control.

Работа системного администратора в современной организации напрямую связана с сопровождением большого количества серверного оборудования, рабочих станций, сетевых устройств, периферийного оборудования и различных программных сервисов, обеспечивающих функционирование основных бизнес-процессов. Даже в небольшой инфраструктуре количество контролируемых узлов может исчисляться десятками или сотнями. С постоянным увеличением количества используемого оборудования возрастает сложность сопровождения инфраструктуры и контроля её состояния. Отказ отдельных элементов сети может привести к снижению производительности сотрудников, нарушению работы сервисов организации.

Во многих организациях сопровождение инфраструктуры осуществляется по реактивному принципу, при котором устранение неисправностей начинается только после возникновения сбоев или обращений пользователей. Подобный подход увеличивает время обнаружения проблем, усложняет диагностику причин неисправностей и повышает нагрузку на системных администраторов. Особенно актуальна данная проблема для организаций с распределённой структурой и удалёнными подразделениями.

Для повышения надёжности и стабильности работы IT-инфраструктуры применяются системы мониторинга. Использование подобных решений позволяет автоматически контролировать состояние серверов, рабочих станций, сетевого оборудования и своевременно выявлять отклонения в работе

оборудования и оперативно уведомлять администратора о возникающих проблемах.

Одной из наиболее распространённых систем мониторинга является Zabbix [1] – это свободная система мониторинга статусов серверов и сетевого оборудования, с открытым исходным кодом, предназначенная для централизованного контроля состояния IT-инфраструктуры. Система поддерживает несколько методов сбора данных, включая Zabbix Agent, SNMP [4], SMTP [5] или HTTP, без установки какого-либо программного обеспечения на наблюдаемом хосте. Это задача актуальна так как существует необходимость автоматизации контроля IT-инфраструктуры организации и перехода от реактивного администрирования к системному мониторингу состояния оборудования и сервисов. Системы мониторинга позволяют заранее обнаруживать признаки неисправностей, контролировать производительность серверов и сетевых устройств, а также оперативно уведомлять администратора о возникающих проблемах, что сокращает время простоя оборудования и упрощает сопровождение инфраструктуры.

Практическая реализация системы мониторинга выполнялась для организации выполнявшей работы технической инвентаризации. IT-инфраструктура организации включает серверное оборудование, рабочие станции, сетевые устройства, многофункциональные устройства, а также удалённые подразделения, соединённые посредством VPN-соединений. В главном офисе организации функционируют серверы под управлением операционных систем Windows Server 2008–2016, обеспечивающие работу DHCP-служб, файлового сервера, FTP-сервера [3], системы «1С:Предприятие», а также специализированного программного обеспечения организации. Кроме серверного оборудования, в инфраструктуре используются персональные компьютеры сотрудников, сетевые коммутаторы, маршрутизаторы и периферийные устройства. Сетевая инфраструктура организации имеет распределённую структуру и включает 18 удалённых отделений,

взаимодействующих с главным офисом через VPN-соединения. Подобная архитектура усложняет сопровождение оборудования и контроль состояния сетевых сервисов, поскольку часть устройств находится вне зоны постоянного физического доступа системного администратора.

До внедрения системы мониторинга контроль состояния оборудования выполнялся преимущественно вручную. Информация о неисправностях в большинстве случаев поступала от сотрудников организации уже после возникновения проблем, влияющих на рабочий процесс. Этот подход увеличивал время обнаружения неисправностей и затруднял оперативное реагирование на инциденты.

Основными проблемами существующей инфраструктуры являлись:

- отсутствие централизованного контроля состояния оборудования и сервисов,
- сложность мониторинга удалённых филиалов,
- необходимость ручной проверки доступности серверов и сетевых устройств,
- позднее обнаружение неисправностей,
- отсутствие автоматической системы уведомлений о сбоях,
- затруднённый анализ производительности оборудования и сетевых сервисов.

Дополнительные сложности возникали при сопровождении большого количества устройств различных типов. В инфраструктуре одновременно использовались серверы под управлением Linux и Windows, сетевое оборудование различных производителей, рабочие станции и многофункциональные устройства. Каждое устройство имело собственные механизмы диагностики и журналы событий, что усложняло централизованный контроль состояния инфраструктуры.

Проведённый анализ показал необходимость внедрения системы централизованного мониторинга, обеспечивающей автоматический сбор

информации о состоянии оборудования, контроль доступности сетевых сервисов и оперативное информирование администратора о возникающих неисправностях. Использование системы мониторинга должно повысить надёжность сопровождения IT-инфраструктуры, сократить время обнаружения сбоев и упростить администрирование оборудования организации.

В настоящее время существует большое количество программных решений, предназначенных для мониторинга IT-инфраструктуры. Они отличаются функциональными возможностями, сложностью настройки, стоимостью сопровождения и поддерживаемыми технологиями. Также большинство крупных организаций внедряют системы, созданные именно под них, которые решают полностью их проблемы, но стоят значительных средств. При выборе системы мониторинга для организации необходимо учитывать особенности существующей инфраструктуры, возможность масштабирования, удобство администрирования и затраты на внедрение.

Одним из распространённых решений является связка Prometheus и Grafana. Prometheus используется для сбора и хранения метрик, а Grafana - для визуализации данных и построения дашбордов. Но они могут быть интегрированы в Zabbix.

Для локального мониторинга серверов и рабочих станций также применяется система Netdata, отличающаяся высокой скоростью развёртывания и отображением данных в режиме реального времени. Однако возможности Netdata ограничены при построении крупной централизованной системы мониторинга распределённой инфраструктуры.

Среди коммерческих решений можно выделить PRTG Network Monitor и SolarWinds Network Performance Monitor. Данные системы обладают широкими возможностями мониторинга и удобным интерфейсом, однако их использование связано с затратами на лицензирование и сопровождение программного обеспечения. Кроме того, использование некоторых зарубежных решений

ограничено отсутствием официальной технической поддержки на территории России.

В результате анализа существующих решений в качестве основной системы мониторинга была выбрана система Zabbix [2]. Данная платформа представляет собой свободно распространяемую систему мониторинга с открытым исходным кодом, предназначенную для централизованного контроля состояния серверов, рабочих станций, сетевого оборудования и приложений.

Выбор Zabbix обусловлен рядом преимуществ:

- поддержка различных методов мониторинга, включая Zabbix Agent, SNMP и ICMP,
- возможность централизованного контроля распределённой инфраструктуры,
- наличие встроенных средств визуализации и формирования отчётности, а также возможность интегрировать Prometheus и Grafana если стандартные функции не устраивают администраторов,
- гибкая система триггеров и уведомлений,
- поддержка шаблонов мониторинга,
- возможность масштабирования системы при увеличении количества контролируемых узлов,
- отсутствие затрат на лицензирование.

Дополнительным преимуществом системы является наличие веб-интерфейса, обеспечивающего централизованный доступ к информации о состоянии инфраструктуры. Администратор получает возможность просматривать графики нагрузки, журналы событий, отчёты о доступности оборудования и уведомления о неисправностях из единой панели управления.

Таким образом, система Zabbix наиболее полно соответствует требованиям организации и позволяет реализовать централизованный мониторинг серверов, рабочих станций, сетевого оборудования и удалённых подразделений с возможностью дальнейшего расширения функциональности системы.

Практическая реализация системы мониторинга выполнялась на базе платформы Zabbix [1] с использованием выделенного сервера под управлением операционной системы Ubuntu Server 24.04 LTS. Использование отдельного сервера мониторинга позволило обеспечить стабильную работу системы и снизить нагрузку на существующую инфраструктуру организации.

В качестве системы управления базами данных была выбрана PostgreSQL, обеспечивающая надёжную обработку и хранение большого объёма статистической информации. Для функционирования веб-интерфейса системы использовался веб-сервер Nginx, отличающийся высокой производительностью и низким потреблением системных ресурсов.

После установки операционной системы были выполнены:

- настройка сетевых параметров сервера,
- установка PostgreSQL,
- установка серверных компонентов Zabbix,
- настройка веб-интерфейса системы,
- запуск служб мониторинга и базы данных.

Для централизованного контроля состояния серверов и рабочих станций использовался Zabbix Agent, устанавливаемый на контролируемые устройства. Агент обеспечивал сбор информации о загрузке процессора, использовании оперативной памяти, состоянии дисковой подсистемы, сетевых интерфейсов и работе системных служб.

Мониторинг сетевого оборудования и многофункциональных устройств реализовывался с использованием протокола SNMP. Данный подход позволил контролировать доступность устройств, состояние сетевых интерфейсов, загрузку каналов связи и основные параметры работы оборудования без установки дополнительного программного обеспечения.

Для проверки доступности удалённых узлов дополнительно использовались ICMP-проверки, позволяющие автоматически определять

потерю соединения с серверами, маршрутизаторами и удалёнными филиалами организации.

В процессе внедрения были созданы группы узлов сети и шаблоны мониторинга, обеспечивающие упрощённое подключение новых устройств к системе. Использование шаблонов позволило централизованно применять наборы элементов данных, триггеров и графиков к оборудованию одного типа, что значительно упростило администрирование системы мониторинга.

Для визуального контроля состояния инфраструктуры были настроены панели мониторинга Dashboard, графики нагрузки и журналы событий. Веб-интерфейс Zabbix обеспечил централизованное отображение информации о состоянии серверов, рабочих станций, сетевого оборудования и сетевых сервисов организации.

Дополнительно была реализована система автоматических уведомлений через Telegram и веб-интерфейс Zabbix. При возникновении критических событий система автоматически формировала уведомления о недоступности оборудования, превышении допустимой нагрузки, нехватке свободного места на дисках и отказе сетевых сервисов.

Для упрощения подключения рабочих станций к системе мониторинга была реализована автоматизированная установка Zabbix Agent с использованием Kaspersky Security Center. Данный подход позволил централизованно развернуть агент мониторинга на рабочих станциях организации и сократить объём ручной настройки оборудования.

В результате внедрения системы мониторинга на базе Zabbix был организован централизованный контроль состояния серверного оборудования, рабочих станций, сетевых устройств и основных сетевых сервисов организации. Система обеспечила автоматический сбор информации о состоянии инфраструктуры и позволила значительно повысить оперативность реагирования на возникающие неисправности.

Одним из основных результатов внедрения стало сокращение времени обнаружения неисправностей. До внедрения системы мониторинга информация о сбоях в большинстве случаев поступала от сотрудников организации уже после возникновения проблем, влияющих на рабочий процесс. После внедрения Zabbix большинство инцидентов стало фиксироваться автоматически в течение нескольких минут после возникновения неисправности.

В результате выполненной работы была внедрена система централизованного мониторинга IT-инфраструктуры организации на базе Zabbix. В ходе работы проведён анализ существующей инфраструктуры, выполнен выбор программного обеспечения, настроен мониторинг серверов, рабочих станций и сетевого оборудования с использованием Zabbix Agent, SNMP и ICMP, а также реализована система автоматических уведомлений. Внедрение системы мониторинга позволило сократить время обнаружения неисправностей, повысить оперативность реагирования на инциденты и упростить сопровождение IT-инфраструктуры организации.

Библиографический список:

1. Компания «Zabbix» [Электронный ресурс]. – Режим доступа: http://www.zabbix.com/ru/ (дата обращения: 02.05.2026).
2. Сайт с документацией по внедрению Zabbix для мониторинга. Принцип работы [Электронный ресурс]. – Режим доступа: https://www.zabbix.com/documentation/3.4/ru/manual/installation/getting_zabbix (дата обращения 02.05.2026)
3. Что такое FTP. Принцип работы [Электронный ресурс]. – Режим доступа: https://thecode.media/ftp/ (дата обращения 02.05.2026)
4. Что такое SNMP. Принцип работы [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/939596/ (дата обращения 02.05.2026)
5. Что такое SMTP. Принцип работы [Электронный ресурс]. – Режим доступа: https://habr.com/ru/companies/ruvds/articles/983068/ (дата обращения 02.05.2026)