СОДЕРЖАНИЕ

1 УСЛОВИЯ ПРИМЕНЕНИЯ

1.1 Сведения о структуре программы

В составе СИС функционально выделены основные модули:

− модуль мониторинга технических и общих программных средств – выполняет сбор данных о состоянии технических и программных средств с использованием стандартных протоколов и интерфейсов (SMTP, IPMI, SYSLOG и другие);

− модуль сбора и анализа файлов журналов специального программного обеспечения – обеспечивает централизованный сбор и обработку текстовых файлов журналов программ;

− модуль мониторинга статуса взаимодействия с сопрягаемыми системами и РКП.

Схема функциональной структуры представлена на рисунке 1.

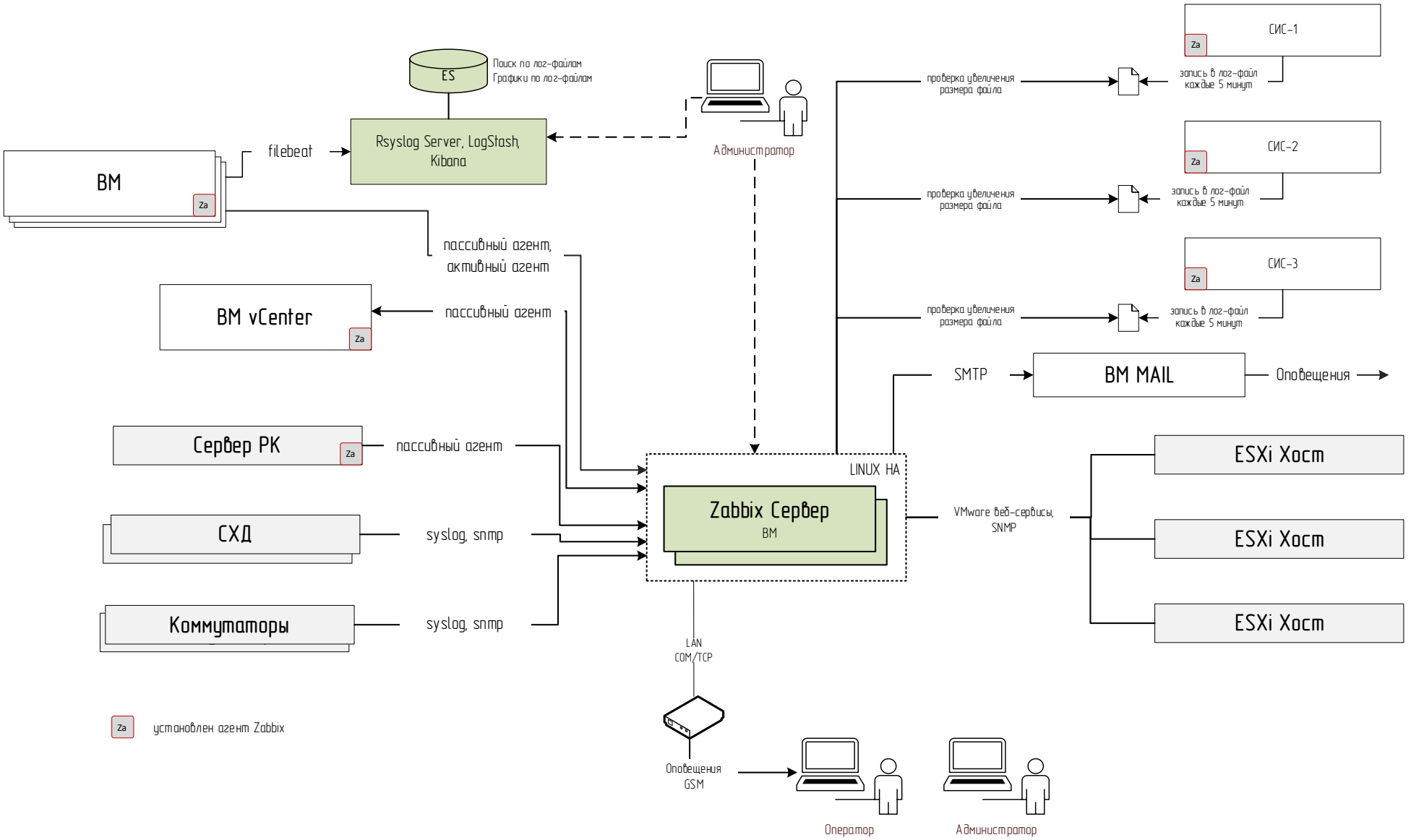

Рисунок 1 – Схема функциональной структуры

1.2 Требования к техническим средствам

СИС разработана на платформе мониторинга Zabbix (версии 3.4 и выше), компоненты которой разворачиваются как на физических, так и на виртуальных серверах:

- агенты Zabbix устанавливаются на отдельные физические и виртуальные машины;
- серверные компоненты Zabbix устанавливаются на виртуальных машинах.

Для сбора и анализа файлов журналов используется набор программных средств Elasticsearch, Logstach, Kibana («ELK»). Для сбора текстовых лог-файлов используется программа Filebeat, которая устанавливается на все ВМ.

Для развертывания используются технические и программные (платформа виртуализации) средства ЦОД (описание технических средств и их размещение на объекте приведено в комплекте документации на КТС ЦОД ФРКД.466459.002).

Для корректного функционирования СИС также требуется:

- развернутый почтовый сервер и созданный почтовый ящик для отправки уведомлений;
- настроенный DNS-сервер;
- сервер синхронизации времени (время на всех контролируемых узлах должно быть синхронизировано).

Для хранения данных Zabbix использует БД PostgreSQL. Системные требования приведены в таблице 1.

Таблица 1 – Системные требования

Имя ВМ	Назначение, ПО	Системные требования
ZABBIX_A	CentOS 7, Zabbix, PostgreSQL	4 CPU 16 ГБ RAM ЖД: 60 ГБ + 300 ГБ Открытые порты: 10050,10051, 5432
ZABBIX_B	CentOS 7, Zabbix, PostgreSQL	4 CPU 16 ГБ RAM ЖД: 60 ГБ + 300 ГБ Открытые порты: 10050,10051, 5432
VIP Zabbix	виртуальный IP для сервера Zabbix	
ZBX-PRX01	*Прокси сервер Zabbix* *Устанавливается при необходимости для работы агентов в DMZ*	*1 CPU* *4 ГБ RAM* *ЖД 40 ГБ*
ELK	Сервер сбора лог-файлов, Kibana, Rsyslog Сервер, Logstash	2 CPU 8 ГБ RAM ЖД 60 Открытые порты: 5400, 80, 5601, 3000

Продолжение таблицы 1

Имя ВМ	Назначение, ПО	Системные требования
ELKDB	БД Elasticsearch	4 CPU 16 ГБ RAM ЖД 60 + 300 Открытые порты: 9200, 9300

1.3 Общие характеристики входной и выходной информации

В состав информации СИС входят:

- лог-файлы программ функциональных подсистем;
- данные мониторинга КТС, в том числе ОПО и платформы виртуализации;
- структурированные данные из БД ЦОД для мониторинга состояния связи с внешними системами и событий, требующих оповещения оператора.

2 ОПИСАНИЕ ЗАДАЧИ

Основной задачей СИС является мониторинг состояния технических и программных средств ЦОД, обнаружение ошибок в работе СПО, а также информирование пользователей об обнаруженных событиях (ошибках, предупреждениях).

2.1 Сбор данных о состоянии и функционировании комплекса аппаратных средств ЦОД, программного обеспечения ЦОД и используемых ЦОД каналов связи

Мониторинг технических средств и общего программного обеспечения (включая vSphere VMware) выполняется с помощью системы мониторинга Zabbix. Каждый объект мониторинга является «узлом» (в терминологии Zabbix), которому могут соответствовать несколько элементов данных. «Узлом» может быть сервер, ПО, служба или веб-сервис. Элементы данных определяют способ сбора данных (например – SNMP-трап, ODBC подключение). Элементы данных можно группировать, а также выполнять вычисления на основе нескольких элементов данных.

Мониторинг серверов, виртуальных машин и ОПО выполняется с помощью:

- агента Zabbix, который устанавливается на каждую виртуальную машину;
- агент SNMP (встроенный) для мониторинга аппаратных средств (коммутаторов, систем хранения, серверов);
- SSH проверки – сервер Zabbix к серверу по SSH и выполняет заданный набор команд;
- простые проверки (simple checks) – проверки выполняются непосредственно на сервере Zabbix с помощью встроенных инструментов, не требуют дополнительных действий со стороны хоста;
- внешние проверки (external checks) − как и простые проверки, выполняются на сервере мониторинга, но не встроенными средствами, а внешними скриптами;
- IPMI – для низкоуровневого мониторинга технических средств.

При необходимости могут быть использованы дополнительные способы проверки (JMX, агрегированные проверки и другое, все способы проверки описаны в официальной документации Zabbix − https://www.zabbix.com/documentation/).

Параметры мониторинга можно разделить на общие группы:

- мониторинг доступности узлов (серверов, коммутаторов и прочего оборудования);
- мониторинг производительности серверов:
    а) загрузка процессора;
    б) использование оперативной памяти;
    в) мониторинг свободного места на дисках;
    г) использование дисков;
- мониторинг виртуальной инфраструктуры:

а) загрузка ESXi хостов – использование процессора, памяти, ресурсов хранения и сетевых ресурсов;

б) мониторинг состояния виртуальных машин;

- мониторинг ОПО:
  а) состояние процессов и служб ПО;
  б) мониторинг доступности страниц портала (HTTP/HTTPS);
- мониторинг АРМ операторов:
  а) мониторинг доступности;
  б) мониторинг использования системных ресурсов;
  в) сбор информации по отдельным событиям (вход в систему, выход).

Часть объектов мониторинга может находиться в демилитаризованной зоне. Для этих объектов предусмотрен проксирующий сервер, который передает данные основному. В таблице 2 приведены группы узлов и способы сбора данных, предусмотренные Zabbix для выполнения конкретных задач мониторинга.

Таблица 2 – Мониторинг КТС и ОПО

Узел/Группа узлов	Назначение мониторинга	ПО	Способ сбора данных	Примечание
ВМ	Сбор общих данных: загрузка процессора, RAM, свободное место на диске, использование дисков	ОС: CentOS	Агент Zabbix Используются стандартные элементы данных и вычисляемые элементы данных Filebeat для сбора системных лог-файлов	ВМ работают с сервером Zabbix через прокси-сервер Zabbix
ВМ (СПО)	Сбор данных по состоянию сервисов и приложений, необходимых для функционирования СПО	ОС: CentOS Сервер приложений: Wildfly/Tomcat; HTTP/FTP сервер; иные службы и сервисы, необходимые для СПО	Агент Zabbix для проверки состояния служб СПО Веб-сценарии для проверок портала. Filebeat для сбора лог-файлов СПО (WildFly) Запуск внешнего скрипта, SSH подключение при необходимости (более сложные проверки) Проверка размера лог-файла взаимодействия с внешними системами для определения статуса взаимодействия	ВМ в DMZ работают с сервером Zabbix через прокси-сервер Zabbix
БД ЦОД	Мониторинг параметров БД, репликации, производительности и т. д.	СУБД PostgreSQL (кластер) ОС: CentOS	Агенты Zabbix на узлах кластера Filebeat для сбора лог-файлов	Ошибки базы данных отслеживаются с помощью анализа лог-файлов
vCenter	Сбор общих данных: загрузка	vCenter Linux	Агент Zabbix	

Продолжение таблицы 2

Узел/Группа узлов	Назначение мониторинга	ПО	Способ сбора данных	Примечание
	процессора, RAM, свободное место на диске, использование дисков. Выполняется мониторинг как обычной ВМ	Virtual Appliance		
vCenter	Сбор отдельных событий выполняется безагентным способом по протоколу SNMP	vCenter Linux Virtual Appliance	SNMP	SNMP должно быть сконфигурировано в vCenter, должны быть выполнены настройки файрволла на разрешение трафика
ESXi хосты	Сбор данных выполняется с помощью веб-сервисов VMware API	-	Веб-сервисы, SNMP, LLD в составе шаблона Zabbix Template VMware	Также выполняется автоматическое обнаружение виртуальных машин. Используется готовый шаблон
СХД (Huawei Oceanstor 2600)	Сбор данных выполняется с помощью любого доступного способа передачи событий – Syslog/SNMP	-	SYSLOG/SNMP (v2, v3), требуется настройка на СХД	-
Коммутаторы	Сбор данных выполняется с помощью любого доступного способа передачи событий – Syslog/SNMP	-	SNMP (требуется настройка на коммутаторах)	Для 5720 используется готовый шаблон Для обнаружения используется Low Level Discovery
ViPNet Coordinator	Сбор данных выполняется с помощью SNMP		SNMP	Требуется загрузка дополнительных MiB (предоставляются производителем оборудования)

Продолжение таблицы 2

Узел/Группа узлов	Назначение мониторинга	ПО	Способ сбора данных	Примечание
П-РК	Сбор данных выполняется с помощью агента и плагина bareos-zabbix	Bareos, Relax-and-Recover	Агент Zabbix	-
АРМ	Сбора данных выполняется агентом Zabbix	Windows, CentOS	Агент Zabbix	-

2.2 Сбор данных о статусе взаимодействия ЦОД с сопрягаемыми информационными системами

Информация, собираемая и отображаемая СИС в части мониторинга взаимодействия с сопрягаемыми системами, включает:

− информацию о статусе и доступности программных компонент, ответственных за взаимодействие с сопрягаемой системой (в составе данных по СПО);

− информацию о последних неуспешных сеансах связи;

− информацию о последних успешных сеансах связи.

Данная задача реализована с помощью Zabbix. СПО, взаимодействующее с внешними системами, каждые 5 мин записывает информацию о статусе взаимодействия в специальный файл на файловой системе. Запись выполняется каждые 5 мин. В Zabbix создается триггер, который отслеживает размер файла:

− если размер не поменялся в течение от 5 до 7 мин, то связь считается потерянной;

− если размер поменялся – взаимодействие работает в штатном режиме.

2.3 Осуществления мониторинга на основе сценариев

ПО Zabbix поддерживает возможность мониторинга на основе:

− триггеров, событий и действий по параметрам мониторинга;

− сценариев веб-мониторинга, позволяющих проверять доступность веб-сайтов или веб-сервисов.

Основная часть функциональности мониторинга Zabbix построена на триггерах и событиях. Триггеры − это логические выражения, которые оценивают данные собранные элементами данных и отражают текущее состояние системы. Выражения триггеров позволяют задать порог, при котором состояние данных приемлемое. Таким образом, если входящие данные превышают приемлемое состояние, триггер «активируется» − или меняет состояние на «ПРОБЛЕМА».

Триггер может принимать следующие состояния:

− ОК: Нормальное состояние триггера. В более ранних версиях Zabbix оно называлось ЛОЖЬ.

− ПРОБЛЕМА: Превышение заданных порогов. Например, загрузка процессора слишком высокая. В более ранних версиях Zabbix оно называлось ИСТИНА.

Состояние триггера (выражение) пересчитывается каждый раз, когда Zabbix сервер получает новое значение, которое является частью выражения. События в Zabbix генерируются несколькими источниками:

− события на триггеры − всякий раз, когда триггер меняет свое состояние (ОК >ПРОБЛЕМА>ОК);

− события на обнаружение − при обнаружении узлов сети или сервисов;

− события на авторегистрацию − когда активные агенты автоматически регистрируются сервером;

− внутренние события − когда элементы данных/правила низкоуровневого обнаружения становятся не поддерживаемыми или триггер переходит в состояние неизвестно.

Для мониторинга портала ЦОД, а также некоторых веб-сервисов, используются веб-сценарии. Веб-мониторинг позволяет отслеживать доступность веб-сайтов и сервисов на основе сценариев (веб-сценариев). Веб-сценарий состоит из одного или нескольких запросов HTTP или «шагов». Шаги периодически выполняются Zabbix сервером в предопределенном порядке. Веб-сценарии привязываются к узлам сети/шаблонам тем же образом как элементы данных, триггеры и так далее. Это означает, что веб-сценарии можно создавать не уровне шаблона и далее применять к нескольким узлам сети.

Каждый сценарий собирает следующую информацию об узле сети:

− средняя скорость загрузки в секунду для всех шагов для всего сценария;

− номер шага, который завершился с ошибкой;

− последнее сообщение об ошибке.

На каждом шаге сценария собирается следующая информация:

− скорость загрузки в секунду;

− время ответа;

− код ответа.

Zabbix может также проверять, содержит ли полученная HTML страница (HyperText Markup Language — язык гипертекстовой разметки) заданную строку. Он может выполнить эмуляцию входа и следовать пути, эмулируя нажатия мышкой на странице. Веб-мониторинг в Zabbix поддерживает и HTTP, и HTTPS. При выполнении веб-сценария Zabbix сервер будет следовать перенаправлениям. Максимальное количество перенаправлений жестко задано в исходном коде (используется cURL опция CURLOPT_MAXREDIRS). Все «cookies» запоминаются на протяжении выполнения одного сценария.

Собранные данные с выполненных веб-сценариев хранятся в базе данных. Эти данные автоматически используются для графиков, триггеров и оповещений.

2.4 Автоматическое обнаружение нештатных ситуаций

Автоматическое обнаружение нештатных ситуация реализовано с помощью:

− триггеров и сценариев в составе ПО Zabbix;

− программа аналитики для автоматического обнаружения ошибок взаимодействия со смежными системами.

Администратор ЦОД может настраивать:

− пороги срабатывания триггеров (при каких условиях наступает нештатная ситуация);

− настраивать период взаимодействия ЦОД со смежными системами, по истечении которого формируется событие потери связи.

2.5 Централизованная обработка файлов журналов ОПО и СПО

СПО и ОПО, функционирующее в ЦОД, может записывать отладочную информацию, ошибки и сообщения о работе следующими способами:

− сообщения записываются в файл текстового формата, который хранится на файловой системе виртуальной машины;

− может быть выполнена конфигурация, при которой сообщения отправляются напрямую в Logstash или Rsyslog сервер.

Использовалось доработанное для нужд ЦОД решение «ELK» − Elasticsearch-Logstash-Kibana. Для сбора и пересылки текстовых лог-файлов используется клиент и сервер Rsyslog или Filebeat для системных лог-файлов. СПО программ передает лог-файлы по протоколу TCP в формате JSON напрямую в Logstash или собирается Filebeat.

Общая программная структура изображена на рисунке 2.

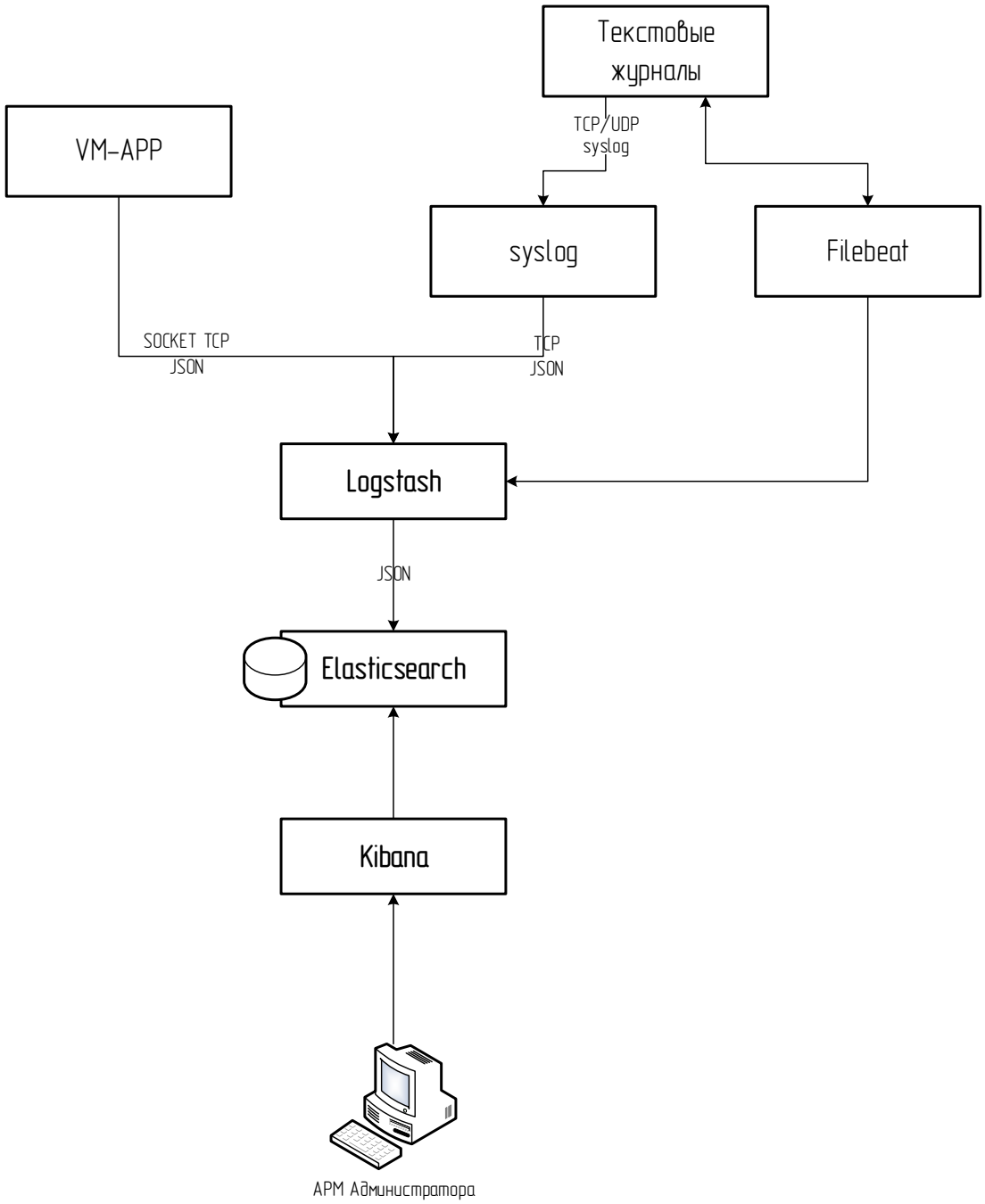

Рисунок 2 – Сбор файлов журналов

СПО в составе ЦОД использует SOCKET TCP для отправки журналов напрямую в Logstash, а также Filebeat для сбора и отправки в Logstash текстовых лог-файлов.

Разобранные лог-файлы передаются на хранение в Elasticsearch. Лог-файлы и события могут тегироваться с помощью отдельного плагина. В этом случае тегированные события будут отображаться в Zabbix в соответствующих группах хостов.

Для просмотра сохраненных в Elasticsearch лог-файлов используется Kibana поиск по лог-файлам и построение аналитических графиков.

2.6 Анализ собираемой информации, её статистическая обработка и отображение результатов мониторинга на АРМ Администратора

Интерфейс для доступа к функциям СИС разделен на две части:

− интерфейс оператора – в составе портала ЦОД. Предназначен для отображения событий программ функциональных подсистем и управления оповещениями. Описание интерфейса оператора и подсистемы отчетности по программам функциональных подсистем приведено в документации на ЦОД;

− интерфейс администратора – предназначен для отображения событий мониторинга КТС, а также предоставляет возможности:

а) конфигурирования параметров мониторинга;

б) формирование отчетов;

в) анализ собираемой информации, её статистическую обработку и отображение результатов мониторинга на АРМ администратора;

г) возможность создания карты информационной сети.

Интерфейс администратора представлен двумя веб-консолями – Zabbix и Kibana.

СИС имеет интерфейс для администрирования, настройки и отображения собираемой информации. Интерфейс доступен через АРМ Администратора через интернет-браузер. Доступ к интерфейсу должен предоставляться после прохождения процедуры авторизации.

Информация, собираемая и отображаемая СИС в части мониторинга функционирования технических средств, включает:

− информацию о состоянии и доступности для мониторинга физических серверов, виртуальных машин и сетевого активного оборудования;

− информацию о доступности сетевых интерфейсов;

− информацию об отказах аппаратного обеспечения, регистрируемых встроенными системами диагностики, информация о которых доступна через интерфейсы SMTP и IPMI;

− информацию о событиях превышения настраиваемых администратором порогов использования ресурсов (загруженность процессора, заполнение жесткого диска, заполнение оперативной памяти).

Веб-консоль Zabbix предназначена для отображения всех событий мониторинга и конфигурирования параметров мониторинга. Вид интерфейса представлен на рисунке 3.

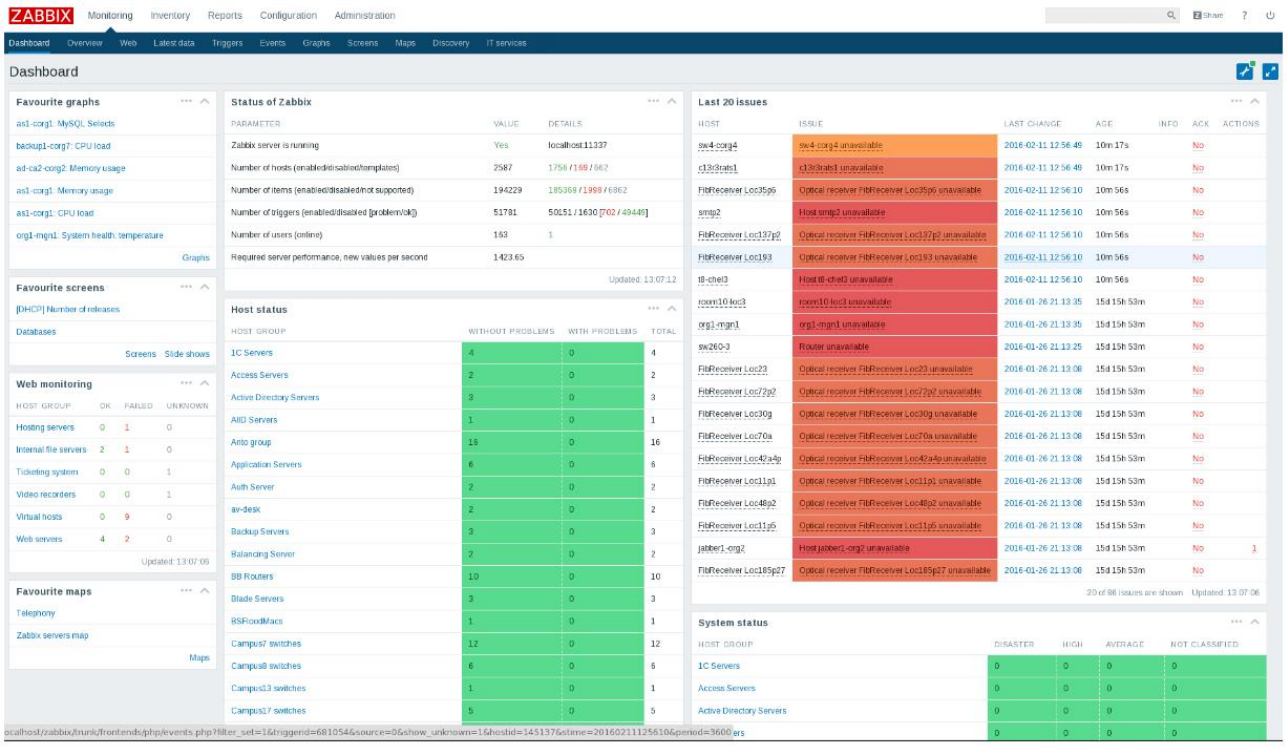

Рисунок 3 – Веб-интерфейс Zabbix (3.0)

Информация, собираемая и отображаемая СИС в части мониторинга функционирования общего программного обеспечения, включает информацию об ошибках, регистрируемых в ОПО.

Информация, собираемая и отображаемая СИС в части мониторинга функционирования специального программного обеспечения, включает:

– информацию об ошибках, регистрируемых в СПО;

– иную информацию, которая указана в описании требований к другим компонентам ЦОД.

Веб-интерфейс Kibana для просмотра и поиска по лог-файлам ОПО и СПО. Представлен на рисунке 4.

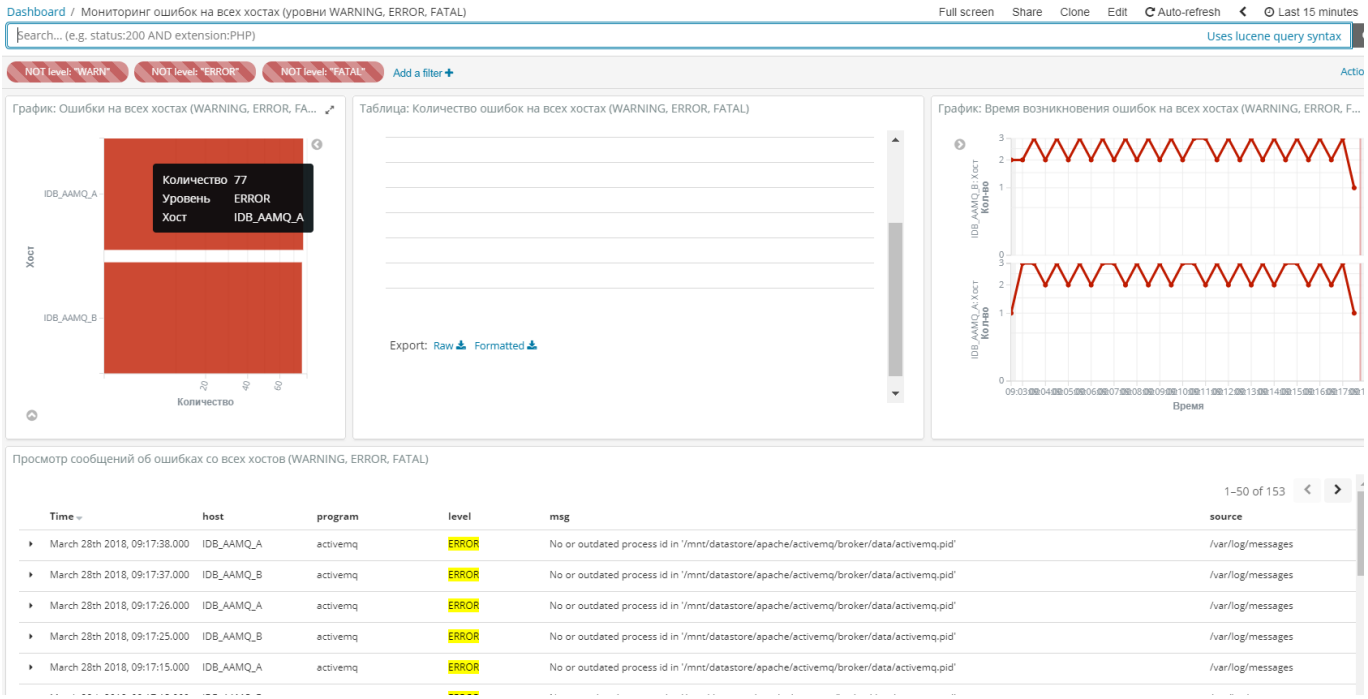

Рисунок 4 – Веб-интерфейс Kibana

2.7 Отправка уведомлений пользователям

СИС имеет функцию оповещения заданных пользователей об обнаруженных нештатных ситуациях:

– путем отправки сообщений электронной почти и SMS через подключенный к серверу GSM-модем;

– отправка сообщений по электронной почте.

Список оповещаемых пользователей, реквизиты для отсылки сообщений, канал отправки сообщений (электронная почта или SMS) и набор событий, информация о которых отправляется конкретному пользователю, настраиваются Администратором ЦОД.

СИС обеспечивает возможность рассылки зарегистрированным пользователям (в соответствии с установленными правами доступа) уведомлений о зафиксированных СИС событиях, в том числе о фактах неработоспособности РКП, отсутствия связи с РКП и выявленных на борту судна событиях. Отправка уведомлений по событиям портала реализовано по протоколу SMTP.

Рассылка сообщений осуществляется с помощью:

– GSM модема;

– сервера электронной почты.

Рассылку сообщений выполняет Zabbix Server.

ПО Zabbix, используемое в СИС, поддерживает гибкую настройку уведомлений по пользователям и группам пользователей.

Zabbix поддерживает отправку SMS сообщений с использованием GSM модемов, подключенных к последовательному порту Zabbix сервера:

− скорость последовательного устройства (/dev/ttyS0) должна совпадать со скоростью GSM-модема;

− пользователь zabbix должен иметь права на чтение и запись в последовательное устройство;

− в GSM должен быть введен ПИН-код, который сохраняется после перезагрузки (или ПИН код должен быть отключен).

Для рассылки сообщений с помощью электронной почты (SMTP) в составе СИС разворачивается почтовый сервер. В качестве почтового сервера используется программный набор Zimbra, включающий также DNS сервер, NTP-сервер и LDAP-сервера.

Группы событий, по которым пользователи получают оповещения, определяются в соответствии с правами доступа и установленным уровнем важности наблюдаемого триггера.

2.8 Реализация отказоустойчивой конфигурации

СИС реализована в отказоустойчивой конфигурации, позволяющей продолжать работу после отказа части аппаратных и программных компонентов программы, а также во время проведения работ по техническому обслуживанию аппаратных средств или обновлению программного обеспечения (без сохранения отказоустойчивости).

Система мониторинга Zabbix состоит из нескольких компонентов, причем все они могут размещаться на разных виртуализованных или физических серверах:

− сервер мониторинга, который периодически получает и обрабатывает данные, анализирует их и производит в зависимости от ситуации определенные действия, в основном оповещение администратора. В ЦОД развернут кластер PostgreSQL с использованием pgpool-II;

− база данных − в качестве таковой могут использоваться SQLite, MySQL, PostgreSQL и Oracle. В ЦОД используется БД PostgreSQL в отказоустойчивой конфигурации;

− веб-интерфейс на PHP, который отвечает за управление мониторингом и действиями, а также за визуализацию. В ЦОД веб-интерфейс установлен на одной ВМ с сервером мониторинга;

− агент Zabbix, запускается на той машине/устройстве, с которой необходимо снимать данные. Его наличие хоть и желательно, но, если установить его на устройство невозможно, можно обойтись SNMP;

− Zabbix proxy — используется в основном в тех случаях, когда необходимо мониторить сотни и тысячи устройств для снижения нагрузки на собственно сервер мониторинга, а также для мониторинга серверов в отдельных подсетях. Прокси-сервер может быть установлен дополнительно при добавлении новых технических средств для распределения нагрузки.

Логическая единица мониторинга − узел. Каждому узлу присваивается описание и адрес − в качестве адреса можно использовать как доменное имя, так и IP. Узлы могут объединяться в группы, к примеру группа роутеров, для удобства наблюдения. Каждому серверу соответствует несколько элементов данных, то есть отслеживаемых параметров. Поскольку для каждого сервера настраивать параметры, за которыми нужно следить, неудобно (особенно это верно для больших сетей), можно создавать узлы-шаблоны и каждому серверу или группе серверов будет соответствовать несколько шаблонов.

В ЦОД Zabbix разворачивает в отказоустойчивой архитектуре:

− два сервера Zabbix в кластере;

− виртуальный IP-адрес для организации кластера.

Архитектура развернутой системы мониторинга приведена на рисунке 5.

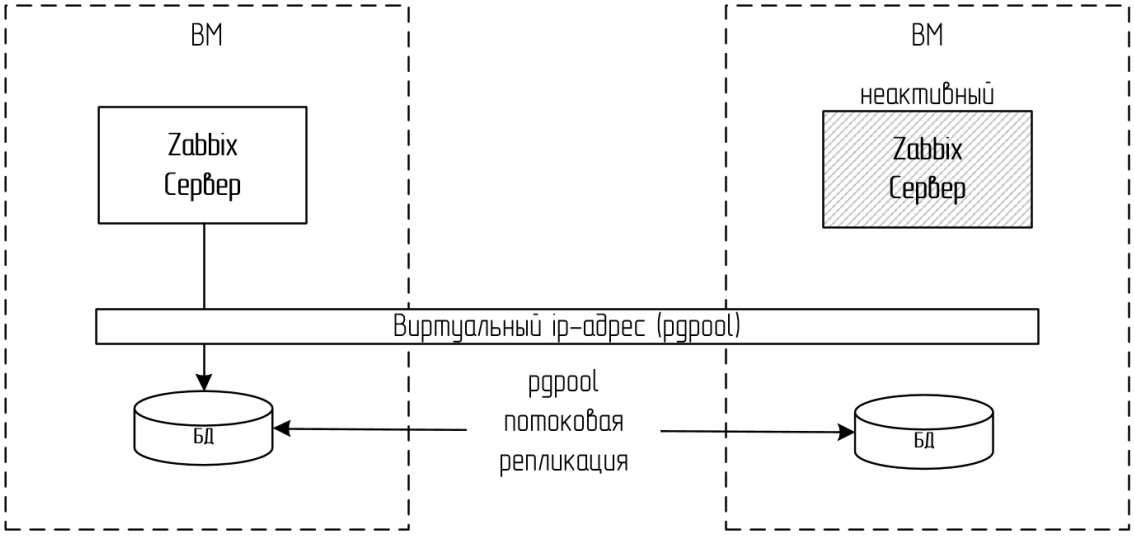

Рисунок 5 – Отказоустойчивая конфигурация Zabbix

На узлах 1 и 2 устанавливается БД PostgreSQL в отказоустойчивой конфигурации с потоковой репликацией. Автоматическое переключение в случае падения (failover) обеспечивается установленным pgpool II. Pgpool также выполняет переключение IP-адреса в случае падения мастера. Сервер (сервис) zabbix активен только на одном узел и выполняет чтение и запись в БД мастер (на своем узле). Если узел отказывает, то pgpool выполняет все необходимые скрипты по переключению БД на резервный узел и, после назначения резервному узлу виртуального IP-адреса, выполняет скрипт запуска сервиса Zabbix. Агенты Zabbix обращаются к серверу по виртуальному IP-адресу.

Активные агенты Zabbix обладают функционалом накапливать неотправленные данные мониторинга и отправлять их после того, как сервер Zabbix снова стал доступным.

3 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

В состав информации, сбор которой выполняется СИС, входит:

– лог-файлы функциональных подсистем;

– данные мониторинга КТС, в том числе ОПО и виртуальной платформы;

– структурированные данные из БД ЦОД для мониторинга состояния связи с внешними системами и событий, требующих оповещения оператора.

Структура передаваемой информации определяется типом объекта мониторинга и может быть представлена в следующих видах:

– лог-файл в текстовом формате;

– лог-файл в формате JSON;

– журнал в формате SYSLOG согласно RFC 5424/5426;

– агент Zabbix передает данные серверу в формате JSON;

– данные оборудования (серверов, коммутаторов и СХД) передаются в формате SNMP/SYSLOG;

– запросы к БД ЦОД для выборки данных по программам функциональных подсистем передаются в виде запросов SQL.

Syslog – стандарт отправки и регистрации сообщений о происходящих в системе событиях (то есть создания логов), использующийся в компьютерных сетях, работающих по протоколу IP.

JSON (англ. JavaScript Object Notation) – текстовый формат обмена данными, основанный на JavaScript. Несмотря на происхождение от JavaScript (точнее, от подмножества языка стандарта ECMA-262 1999 года), формат считается независимым от языка и может использоваться практически с любым языком программирования. Для многих языков существует готовый код для создания и обработки данных в формате JSON.

Пример JSON:

```
{
   "jsonrpc": "2.0",
   "method": "method.name",
   "params": {
      "param_1_name": "param_1_value",
      "param_2_name": "param_2_value"
   },
   "id": 1,
   "auth": "159121b60d19a9b4b55d49e30cf12b81"
}
```

SNMP – простой протокол сетевого управления) — стандартный интернет-протокол для управления устройствами в IP-сетях на основе архитектур TCP/UDP. К поддерживающим SNMP устройствам относятся маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и другие. Протокол обычно используется в системах сетевого управления для

контроля подключенных к сети устройств на предмет условий, которые требуют внимания администратора. SNMP определен Инженерным советом интернета (IETF) как компонент TCP/IP. Он состоит из набора стандартов для сетевого управления, включая протокол прикладного уровня, схему баз данных и набор объектов данных.

Объем данных мониторинга определяется в зависимости от типа объекта, интенсивности генерации событий и правил ротации лог-файлов.

Входными данными СИС являются:

- лог-файлы формата JSON;
- лог-файлы текстового формата, переданные по протоколу SYSLOG;
- сообщения мониторинга, переданные по протоколу SNMP;
- сообщения мониторинга, получаемые по протоколу IPMI;
- сообщения мониторинг, переданные по протоколу Zabbix на основе JSON (пример сообщений обмена между сервером Zabbix и прокси-сервером приведен.
- данные из БД ЦОД, которые обрабатываются компонентом СИС/СПО для генерации оповещений операторам по событиям.

Выходными данными СИС являются оповещения о событиях мониторинга переданные в виде электронного сообщения или SMS сообщения, а также в виде визуализированных данных в веб-интерфейсе администратора.