Описание функциональных характеристик Arenadata Integration Module (AIM)

Москва
2024

Содержание:

1 Общая информация

Документ содержит описание функциональных характеристик реализации компонентов интеграции для программных продуктов компании ООО «Аренадата Софтвер»: Arenadata Analytical DB (ADB), Arenadata QuickMarts (ADQM), Arenadata Hadoop Platform (ADH), Arenadata Streaming Platform (ADS) с технологическими сервисами платформы ФКУ «ГосТех»:

- IAM – аутентификация учетных записей и публикация ролевой модели;
- Журналирование – передача содержимого лог-файлов;
- Аудит – передача событий Аудита и описание их модели (передаваемых с событием атрибутов);
- Мониторинг – передача метрик мониторинга утилизации оборудования и работы технологий.

Основным предназначением ПО является обеспечение требований ФКУ «ГосТех» и ПАО «Сбербанк» в части взаимодействия со служебными сервисами платформы программных продуктов компании ООО «Аренадата Софтвер».

Наиболее эффективные области применения ПО — это:

- Взаимодействие со служебными сервисами IAM (управление учетными записями и аутентификация) и ЖАМ (журналирование, аудит (логирование) и мониторинг) платформы ФКУ «ГосТех».

Основные функциональные возможности ПО:

- Формирование и транслирование сообщений событий аудита, журналирования и мониторинга в требуемом формате платформы ФКУ «ГосТех» в служебные сервисы;
- Согласование управления идентификацией и доступом пользователей продукта компании ООО «Аренадата Софтвер» с служебным сервисом платформы IAM через протокол Ldap.

Решаемые задачи:

- Сервис IAM – сервис идентификации и контроля доступа, предназначенный для централизованного управления правами доступа пользователей к ресурсам ЕЦП «ГосТех».
- Сервис журналирования – сервис для агрегации и чтения логов пользовательских приложений и ресурсов ЕЦП «ГосТех».
- Сервис аудита – сервис сбора и выгрузки аудитных записей ресурсов ЕЦП «ГосТех».
- Сервис мониторинга – сервис мониторинга состояния ресурсов и программных компонентов (сервисов) ЕЦП «ГосТех».

2 Архитектура и функциональные особенности

Технологический сервис **Журналирование** основан на продуктах Logstash и Opensearch. Интеграция с Журналированием заключается в отправке содержимого лог-файлов компонентов продуктов Arenadata в централизованный приемник Logstash, реализованный на основе агента Logstash, который запускается в контейнере docker на каждом хосте в единственном экземпляре и обрабатывает группу конфигов (по отдельному конфигу на каждый поток лога для каждого отдельного инстанса компонента каждой технологии каждого продукта компании ООО «Аренадата Софтвер»), Рисунок 1.

При отправке события аудита и публикации метамодели в HTTP-запросе для аутентификации передаются TLS-ключ и сертификат пользователя.

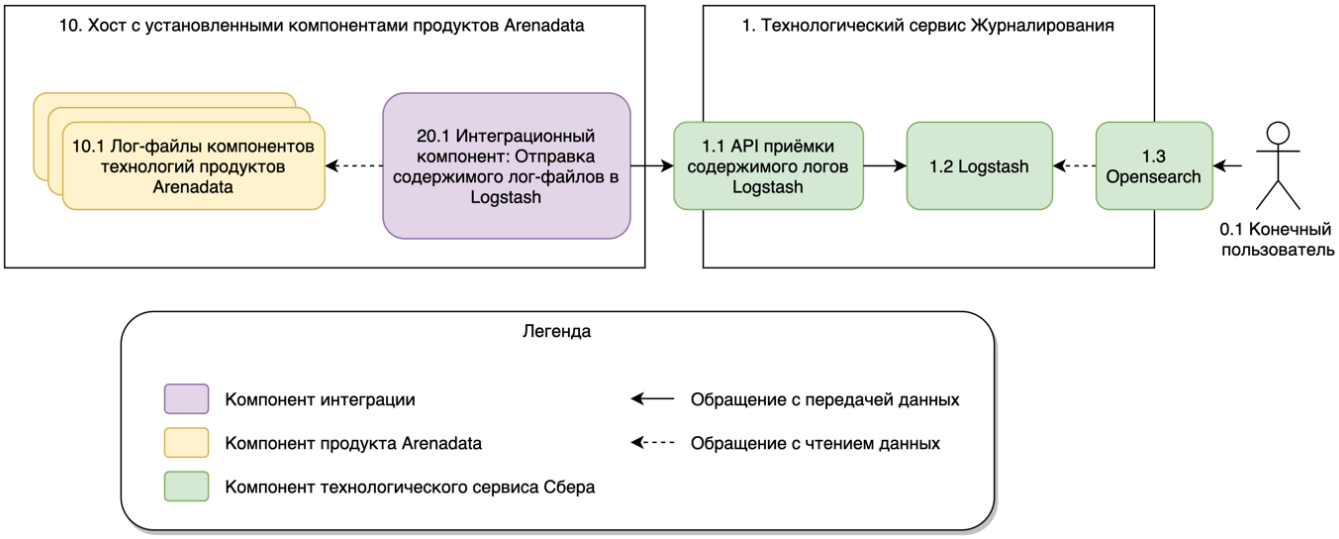

Рисунок 1. Схема интеграции с технологическим сервисом Журналирования

Подготовка необходимых конфигов реализована, как и установка, на основе плейбука Ansible, который использует справочник потоков логов, соответствующих продукту + технологии + компоненту, и набор шаблонов с типовыми вариантами парсеров лог-файлов.

Технологический сервис **Мониторинг** основан на Prometheus и Grafana, для интеграции требуется передавать метрики мониторинга как pull (предоставлять для вычитывания) или push (загружать) режим. Для приемки метрик от продуктов компании ООО «Аренадата Софтвер» используется интерфейс в формате приемки метрик от Graphite.

Схема решения интеграции с Мониторингом представлена на Рисунке 2. Основное решение по передаче метрик мониторинга основано на пересылке метрик внутреннего Мониторинга, развернутого инстансом ADCM (компоненты 21.1, 10.2, 10.3), во внешний технологический сервис Мониторинга (компоненты 2, 2.1, 2.2, 2.3), без промежуточного хранения значений метрик.

Передача метрик утилизации оборудования (ресурсов сервера и уровня операционной системы) настраивается и эксплуатируется со стороны платформы, при этом на сервер должен быть установлен штатный агент мониторинга Prometheus (node_exporter, компоненты 2.4).

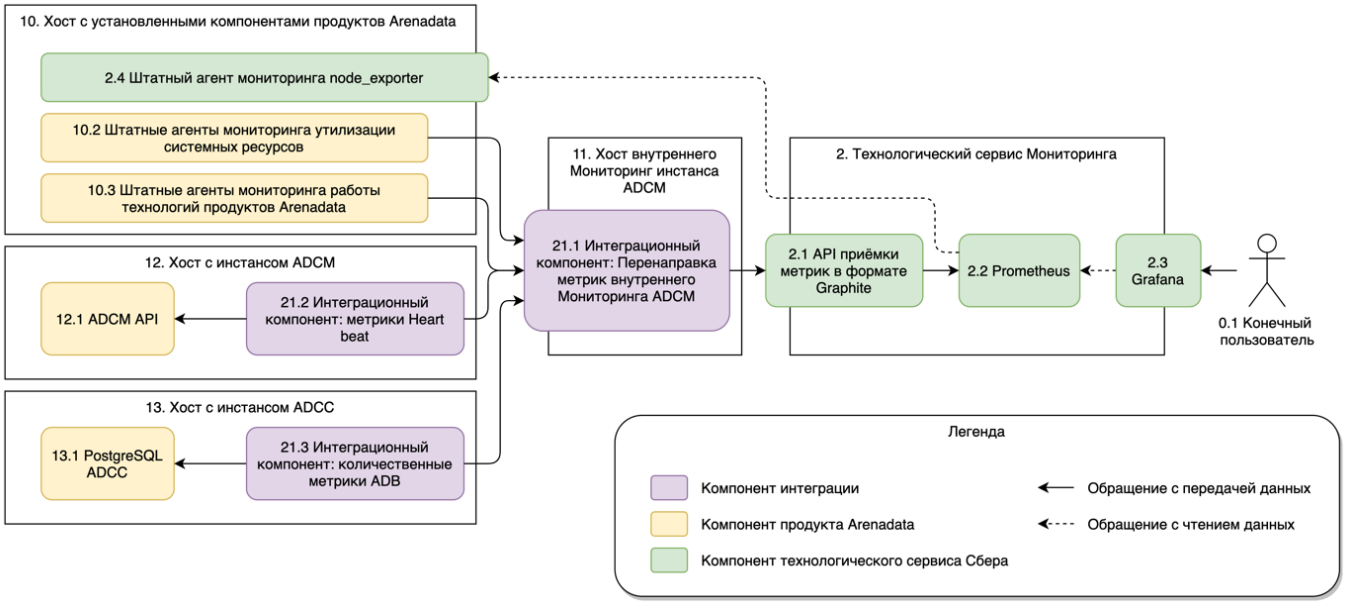

Рисунок 2. Схема интеграции с технологическим сервисом Мониторинга

Кроме передачи штатных метрик Мониторинга продуктов компании ООО «Аренадата Софтвер» дополнительно передаются:

- Метрики на основе значений «Heart beat» (аналог показателей «Health check») (компоненты 21.2 и 12.1);
- Метрики с количественными показателями работы ADB на основе истории принятых и обработанных в СУБД запросов (компоненты 21.3 и 13.1).

В продуктах ООО «Аренадата Софтвер» **Метрики** мониторинга собираются в разворачиваемом Graphite под управлением ADCM. Для перенаправления потока метрик штатные сервисы Graphite отключаются, и вместо них реализовано перенаправление метрик на внешний приемник по протоколу Graphite на основе агента Logstash.

Контейнер разворачивается на сервере, где штатно разворачивается Graphite Мониторинга ADCM.

Для отслеживания состояния сервисов в ADCM фиксируются актуальные значения **«heart beat»** (сердцебиения) – откликается сервис или нет. При этом значение 0 – штатное состояние компонента, значение отличное от 0 – признак не штатного состояния компонента.

Для отслеживания реализовано снятие значений «heart beat» по всем компонентам, описанным и разворачиваемым ADCM, и их передача как штатная метрика во внутренний Мониторинг ADCM (и соответственно пересылаются во внешний технологический сервис Мониторинга).

Решение реализовано на основе NodeJS-скрипта, который выполняется регламентно по расписанию, и при запуске разово снимает значение метрик из ADCM (через ADCM API) и отправляет значение метрик во внутренний Мониторинг.

Рекомендуется развертывание непосредственно на сервере ADCM.

Для фиксирования и отправки метрик мониторинга **по количеству обрабатываемых запросов**, новых и обработанных сессий, реализован механизм на основе BASH-скрипта (по аналогии с штатными средствами мониторинга продуктов компании ООО «Аренадата Софтвер»).

Скрипт выполняет SQL-запрос через psql, в рамках которого определяются значения метрик мониторинга за последний полный пятиминутный период с начала календарного часа.

Рекомендуется развертывание непосредственно на сервере ADCC.

Требования к интеграции соответствуют API реализации технологического сервиса **Аудита**. Для интеграции требуется:

- Опубликовать (разово для инстанса и продукта) метамодель событий аудита: https://platform-docs.v-serv.ru/online-documentation/home/security/audit/swagger/metamodel/
- Передавать события аудита: https://platform-docs.v-serv.ru/online-documentation/home/security/audit/swagger/sobytie/

Публикация метамодели реализована на основе NodeJS-скрипта, публикующего модель в формате JSON. Отслеживание и передача событий аудита зависит от продукта – реализована на основе NodeJS-скрипта либо Logstash-агента (Рисунок 3).

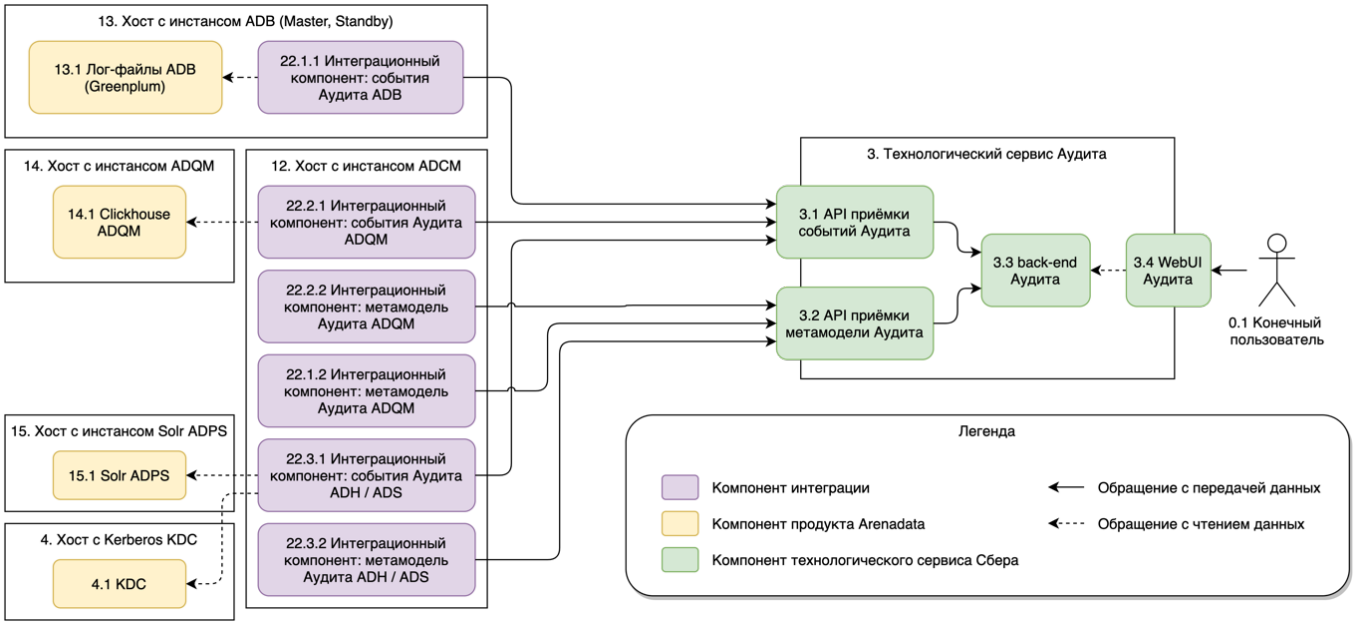

Рисунок 3. Схема интеграции с технологическим сервисом Аудит

При отправке события аудита и публикации метамодели в HTTP-запросе для аутентификации передается TLS-ключ и сертификат пользователя.

Наличие метамодели проявляется в виде русскоязычных названий событий и атрибутов, а также разметкой наличия ошибки (выделением событий с красным кружком).

Аудит для ADB: Передача событий реализована на основе Logstash-агента, источником информации о событиях являются записи в лог-файле ADB Master (СУБД Greenplum) в файле лога (маска с каталогом по умолчанию - */data1/master/gpseg-1/pg_log/gpdb-*.csv*) (Рисунок 3, компоненты 22.1.1 и 13.1).

Аудит для ADQM: Передача событий реализована на основе NodeJS-скрипта, источником информации о событиях являются записи в таблице ADQM (СУБД Clickhouse) *system.session_log* (Рисунок 3, компоненты 22.2.1 и 14.1).

Аудит для ADH и ADS: Источником событий аудита ADH и ADS является сервер Solr ADPS, в котором собираются события аудита при условии развернутой аутентификации и авторизации на основе Kerberos в продуктах ADH и ADS (Рисунок 3, компоненты 22.3.1, 15.1, 4.1).

Сервисы **IAM** соответствуют следующим основным требованиям:

- Обеспечивать взаимодействие с другими сервисами и их компонентами; загрузку в IAM ролевой модели сервиса через интерфейс администрирования; идентификацию и аутентификацию Конечных пользователей сервисов; централизованное управление политикой безопасности, контроль списка доступа; поддержку федерации удостоверений;

- Обеспечивать наличие инструментов управления пользователями и группами; наличие инструментов управления доступом к ресурсам и сервисам; наличие инструментов управления ключами авторизации.

3 Сервис Журналирование

Сервис Журналирования соответствует следующим основным требованиям:

- Обеспечивать управление сервисом через web-консоль, CLI и API;
- Обеспечивать централизованный сбор и хранение журналов сервисов и их компонент;
- Для интеграции с сервисами расширения базовых сервисов ЕЦП «ГосТех», определенных в Методических рекомендациях по включению сервисов в ЕЦП «ГосТех», иметь возможность принимать данные в формате плоского JSON с использованием REST и gRPC API;
- Инструменты Сервиса журналирования и собранные им данные должны позволять однозначно указать элемент или группу элементов, в которой произошли;
- Обеспечивать агрегацию данных о работе различных ресурсов в лог-группу;
- Обеспечивать управление лог-группами;
- Обеспечивать сбор, обработку и хранение логов в течение установленного срока;
- Обеспечивать изолированное хранение логов для каждой лог-группы;

- Предоставлять возможность фильтрации и поиска записей с помощью запросов;
- Обеспечивать ролевой доступ на чтение и запись логов.

Технологический сервис журналирование основан на продуктах Logstash и Opensearch.

При отправке события аудита и публикации метамодели в HTTP-запросе для аутентификации передаются TLS-ключ и сертификат пользователя.

Подготовка и установка необходимых конфигов реализована на основе плейбука Ansible, который использует справочник потоков логов, соответствующих продукту + технологии + компоненту, а также набор шаблонов с типовыми вариантами парсеров лог-файлов.

4 Сервис Мониторинг

Сервис Мониторинга соответствует следующим основным требованиям:

- Обеспечивать ролевой доступ к сервису и данным мониторинга;
- Обеспечивать автоматический сбор и долговременное хранение метрик состояния ресурсов в ЕЦП «ГосТех»;
- Отображать метрики на сервисных панелях (dashboards);
- Поддерживать загрузку собственных метрик, с использованием API;
- Поддерживать выгрузку метрик ресурсов и пользовательских метрик с помощью API;
- Обеспечивать создание собственных панелей и графиков;
- Поддерживать метки для идентификации и описания характеристик временных рядов;

- Поддерживать настройки уведомлений («тревожных сигналов», alerts) об изменении состояния ресурса ЕЦП «ГосТех»;
- Поддерживать каналы уведомлений: электронной почты, SMS;
- Поддерживать агрегации значений всех метрик в соответствии с политикой прореживания;
- Обеспечивать автоматическое удаление устаревших метрик (TTL) в соответствии с заданными правилами;
- Для интеграции с сервисами расширения базовых сервисов ЕЦП «ГосТех», определенных в Методических рекомендациях по включению сервисов в ЕЦП «ГосТех», поддерживать два режима загрузки метрик: режимы pull и push;
- В режиме pull Сервис мониторинга должен осуществлять сбор метрик с объекта контроля в формате Prometheus с заданной периодичностью;
- В режиме push Сервис мониторинга должен предоставлять REST и gRPC API.

Технологический сервис мониторинга основан на Prometheus и Grafana, для интеграции требуется передавать метрики мониторинга как pull (предоставлять для вычитывания) или push (загружать) режим. Для приемки метрик от продуктов Arenadata используется интерфейс в формате приемки метрик от Graphite.

Передача метрик утилизации оборудования (ресурсов сервера и уровня операционной системы) настраивается и эксплуатируется со стороны платформы, при этом на сервер должен быть установлен штатный агент мониторинга Prometheus.

Кроме передачи штатных метрик Мониторинга продуктов компании ООО «Аренадата Софтвер» дополнительно передаютя:

- Метрики на основе значений «Heart beat»;
- Метрики с количественными показателями работы ADB на основе истории принятых и обработанных в СУБД запросов.

5 Сервис Аудит

Сервис Аудита соответствует следующим основным требованиям:

- Обеспечивать централизованный сбор и хранение событий безопасности, связанных с действиями пользователей в системе и в сервисах;
- Для интеграции с сервисами расширения базовых сервисов ЕЦП «ГосТех», определенных в Методических рекомендациях по включению сервисов в ЕЦП «ГосТех». обеспечивать прием событий аудита через REST и gRPC API;
- Собранные события безопасности должны быть доступны для экспорта во внешние SIEM-системы.

Требования к интеграции соответствуют API реализации технологического сервиса Аудита. Для интеграции требуется:

- Опубликовать (разово для инстанса и продукта) метамодель событий аудита: https://platform-docs.v-serv.ru/online-documentation/home/security/audit/swagger/metamodel/
- Передавать события аудита: https://platform-docs.v-serv.ru/online-documentation/home/security/audit/swagger/sobytie/

Публикация метамодели реализована на основе NodeJS-скрипта, публикующего модель в формате JSON. Отслеживание и передача событий аудита зависит от продукта – реализована на основе NodeJS-скрипта либо Logstash-агента.

При отправке события аудита и публикации метамодели в HTTP-запросе для аутентификации передается TLS-ключ и сертификат пользователя.

Для проверки поставки событий аудита возможно использовать визуальный интерфейс: войти в VPN к стенду ПАО «Сбербанк», перейти в UI аудита (https://{сервер UI аудита}/audit/ui), авторизоваться, перейти в «Поиск событий аудита», выбрать период времени и по необходимости в строке поиска вести искомое (например фрагмент названия продукта или события) и нажать «Найти» –логи выводятся таблицей. При выборе события справа в панели – детальная информация.

Наличие метамодели проявляется в виде русскоязычных названий событий и атрибутов, а также разметкой наличия ошибки (выделением событий с красным кружком).

6 Сервис IAM

Сервисы IAM соответствуют следующим основным требованиям:

- Обеспечивать взаимодействие с другими сервисами и их компонентами по одному из протоколов: OpenID Connect 1.0, SAML 2.0, Kerberos, LDAP;
- Обеспечивать загрузку в IAM ролевой модели сервиса через интерфейс администрирования, либо при разворачивании или

запуске сервиса с привилегированным доступом по одному из доступных протоколов;

- Обеспечивать идентификацию и аутентификацию Конечных пользователей сервисов через сервисы IAM с использованием учетных записей единой системы идентификации и аутентификации (ЕСИА);
- Обеспечивать наличие инструментов управления пользователями и группами;
- Обеспечивать наличие инструментов управления доступом к ресурсам и сервисам;
- Обеспечивать наличие инструментов управления ключами авторизации;
- Иметь поддержку федерации удостоверений: обеспечивать настройку Single Sign-On аутентификации с помощью внешнего доверенного поставщика удостоверений либо пользовательского брокера удостоверений;
- Обеспечивать централизованное управление политикой безопасности, контроль списка доступа (ACL).

Интеграция с IAM сведена к следующему:

- Настройка аутентификации через LDAP (штатными средствами продуктов Arenadata, настраивается со стороны вендора);
- Публикация формальных ролевых моделей (которые включают как минимум одну роль).

7 Диагностика

Интеграционный слой обеспечивает диагностику своей работоспособности путем передачи журналов и метрик в централизованную систему диагностики ЕЦП «ГосТех». Передаваемой информации достаточно для однозначной локализации уже произошедших ошибок или потенциальных проблем. Информация, поступающая в систему диагностики, позволяет однозначно указать элемент или группу элементов согласно спецификации развертывания, в которой произошли ошибки или в ближайшее время прогнозируются ошибки при нарушении установленных диапазонов значений для метрик мониторинга.

Уровень логирования конфигурируется и поддерживает, как минимум, следующие значения:

- DEBUG – логирование всех видов событий;
- INFO – логирование ошибок, предупреждений и сообщений;
- WARN – логирование ошибок и предупреждений;
- ERROR – логирование всех ошибок.

Обязательным набором метрик является:

- Метрики использования системных ресурсов (CPU, RAM, Memory);
- Время исполнения входящих запросов;
- Количество успешных/неуспешных выполнений входящих запросов;
- Время исполнения исходящих запросов или обращений к СПО (специальное программное обеспечение);

- Количество успешных/неуспешных выполнений исходящих запросов или обращений к СПО (специальное программное обеспечение).