Telsoft

vEPC

Описание технической архитектуры

Версия документа: 1

Правовая информация

Содержание

1. Введение

1.1. Назначение документа

Настоящий документ представляет описание технической архитектуры системы vEPC.

Данный документ содержит следующие аспекты:

- Общее описание EPC.
- Описание архитектуры решения.

1.2. Ограничения и допущения

1.3. Сопутствующая документация

1.4. Используемые обозначения

Таблица 1. Используемые обозначения

Обозначение	Описание
Полужирное начертание	Функциональные элементы (экранные кнопки, название окон и т. д.)
Курсив	Перекрестные ссылки, ссылки на другие документы
ЗАГЛАВНЫЕ БУКВЫ	Название клавиш клавиатуры
`Шрифт Courier New`	Код
Примечание	Пояснение к тексту

1.5. История изменений документа

Таблица 2. История изменений

Версия	Дата	Содержание изменений
1.0	20.05.2025	Документ создан

2. Общее описание EPC с учетом архитектуры CUPS

Введение

Evolved Packet Core (EPC) – пакетно-коммутируемое ядро сети LTE по стандартам 3GPP. EPC является эволюцией GPRS Core и представляет собой упрощённую «all-IP» архитектуру с разделением на плоскости управления и передачи данных. EPC обеспечивает сквозную IP-транспортировку и поддерживает мобильность между различными типами доступа (E-UTRAN LTE, 3GPP-legacy GERAN/ UTRAN, а также не-3GPP сети, например Wi-Fi). Основные элементы EPC включают сущности MME (Mobility Management Entity), Serving GW, PDN GW, HSS (Home Subscriber Server) и PCRF (Policy and Charging Rules Function). Они реализуют функции регистрации и аутентификации абонента, установления и управления пакетными сессиями, маршрутизации пакетов во внешние сети, а также применения политик качества обслуживания и тарификации.

Архитектура EPC с учетом CUPS

В базовой архитектуре EPC (до релиза 14) плоскость управления полностью выполняет MME, а пользовательскую плоскость обеспечивают S-GW и P-GW. Начиная с 3GPP Release 14 введена концепция CUPS (Control and User Plane Separation) – разделение контрольной и пользовательской частей узлов S-GW и P-GW. При этом S-GW и P-GW разбиваются на две подсущности: SGW-C и SGW-U (контрольная/пользовательская часть S-GW), а также PGW-C и PGW-U (контрольная/ пользовательская часть P-GW). Такое разделение позволяет независимо масштабировать и размещать функции управления и передачи данных (например, выносить SGW-U ближе к RAN для снижения задержек), не затрагивая при этом механизм сигнализации. В результате архитектура EPC становится более гибкой: CP-узлы выполняют управление (GTP-C, Diameter), а UP-узлы – быструю пересылку пакетов. Для взаимодействия между разделёнными частями используются новые протоколы (например, PFCP) и интерфейсы (Sxa/Sxb/Sxc).

Интерфейсы EPC (таблица)

В EPC определено множество интерфейсов между сетевыми элементами.

Ниже приведена таблица основных интерфейсов с участвующими узлами и назначением (данные по 3GPP TS 23.401 и др.):

Таблица 3. Интерфейсы vEPC

Интерфейс	Участники	Назначение
S1-MME	eNodeB ↔ MME	Управляющий интерфейс (NAS/S1-AP) от базовой станции к MME
S1-U	eNodeB ↔ S-GW	Передача пользовательских пакетов (GTP-U) от eNodeB к S-GW
S2a	Trusted WLAN (TWAG) ↔ PDN-GW	Интерфейс от доверенной WLAN к P-GW
S2b	ePDG ↔ PDN-GW	Интерфейс от недоверенной WLAN через ePDG к P-GW

S3	MME ↔ SGSN	Контрольный интерфейс между MME и SGSN для междоменной мобильности
S4	SGSN ↔ S-GW	Интерфейс пользовательской/управляющей плоскости между SGSN и S-GW
S5	S-GW ↔ P-GW	Интерфейс передачи пакетов внутри PLMN
S8	S-GW ↔ P-GW (в роуминге)	Эквивалент S5 для роуминга
S6a	MME ↔ HSS	Диаметр-интерфейс для передачи профилей и аутентификации абонента
S6d	SGSN ↔ HSS	Аналог S6a для 2G/3G
S10	MME ↔ MME	Интерфейс передачи контекста между MME
S11	MME ↔ S-GW	Управляющий интерфейс GTP-C
S12	eNodeB ↔ RNC	Интерфейс управления (Iu-mode) между eNodeB и RNC
S13	MME ↔ EIR	Проверка IMEI устройства
SGi	P-GW ↔ внешняя сеть	Выход в внешние IP-сети (Internet/IMS/PDN)
Gx	PCRF ↔ P-GW	Интерфейс передачи правил QoS/PCC (Diameter)
Gy	P-GW ↔ OCS	Онлайн тарификация (реальное время, Diameter)
Gz	P-GW ↔ OFCS	Оффлайн тарификация (CDR-файлы)
Rx	PCRF ↔ AF (IMS)	Обмен приложенческими данными сеанса
SGs	MME ↔ MSC/VLR	CS Fallback и CS Paging между LTE и CS-доменом
Sv	MME ↔ MSC Server	Интерфейс для процедуры SRVCC

3. Архитектура vEPC

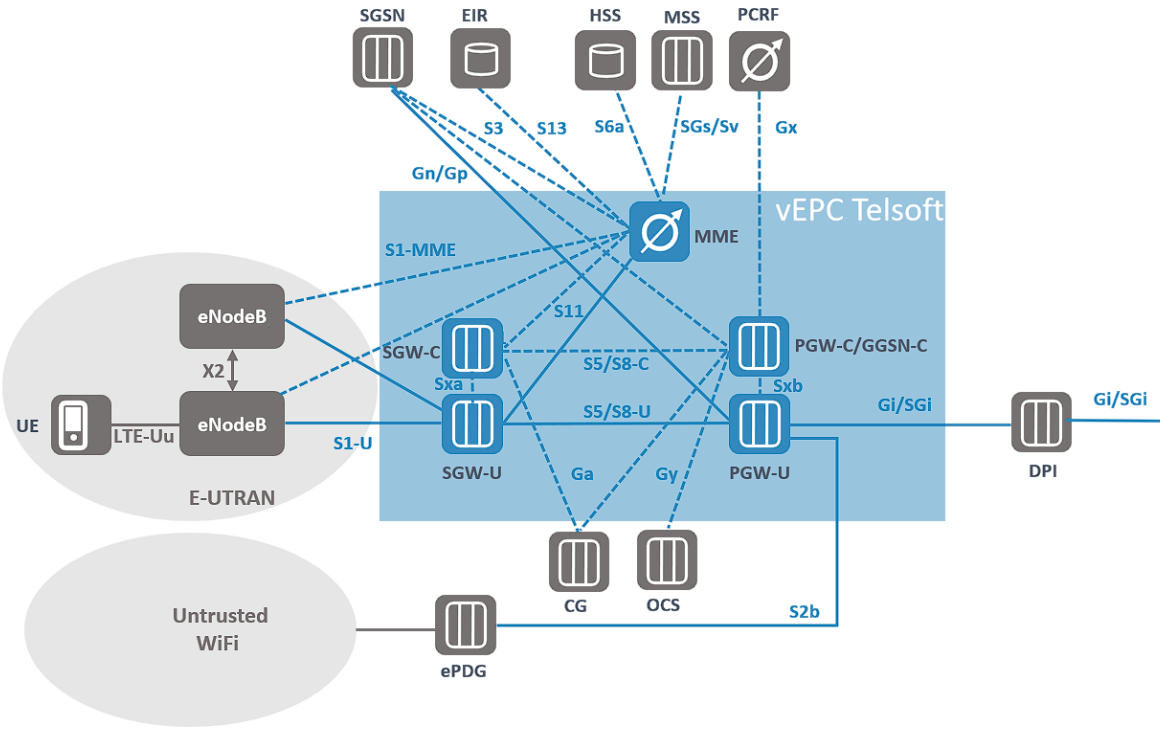

Рис. 1. Архитектура сети EPC

На схеме показаны ключевые компоненты EPC и связи между ними. UE подключается к сети через eNodeB (для LTE) или через Wi-Fi AP (недоверенный WLAN с ePDG). Основные ядреные узлы EPC – это MME, Serving GW и PDN GW – подключённые к базе подписчиков HSS, политическому контроллеру PCRF, а также к внешним сетям (через SGi к интернет/IMS). Кроме того, на схеме изображены ePDG (для Wi-Fi-доступа), AAA-сервер (для аутентификации не-3GPP доступа) и ANDSF (служба выбора сети). Указаны основные интерфейсы (S1, S11, S5/S8, S6a и др.), которые используются для сигнальной и транспортной связи между этими элементами

3.1. MME

MME (Mobility Management Entity) — ключевой элемент управляющей плоскости EPC в архитектуре LTE. Он осуществляет контроль над мобильностью, управлением сессиями, аутентификацией и взаимодействием с другими сетевыми элементами, такими как HSS, SGW, PCRF и MSC.

MME присутствует только в управляющей плоскости, не обрабатывает пользовательский трафик (IP-пакеты абонентов).

3.1.1. Основные функции MME

Мобильность

• Управление перемещением абонентов внутри LTE через Tracking Area Update (TAU)

• Контекстный хендовер между eNodeB через интерфейс S1-MME

• Межтехнологическая мобильность между LTE и 2G/3G через S3/S10/Sv

• Поддержка SRVCC через интерфейс Sv

Управление сессиями

• Установление и удаление EPS-сессий через интерфейс S11 с S-GW

• Назначение S-GW при первой активации PDP-сессии

• Поддержка взаимодействия с PCRF через передачу параметров в P-GW

Аутентификация и безопасность

• Запрос аутентификационных векторов у HSS по протоколу Diameter (S6a)

• Установка ключей шифрования и целостности RRC

• Поддержка проверки IMEI через интерфейс S13 с EIR

Управление NAS-соединениями

• Обработка NAS-сигнализации от UE через eNodeB (S1-MME)

• Инициация процедуры установления безопасности (attach, detach)

• Paging UE в зоне регистрации

Интеграция с CS-доменом

• Реализация CS Fallback и SMS over SGs через интерфейс SGs к MSC/VLR

• Реализация SRVCC с передачей управления в CS

Интерфейс с IMS через PCRF

• Участие в передаче session information в P-GW для последующего взаимодействия с PCRF по Gx

• Установление bearer'ов с учетом IMS QoS

3.1.3. Поддерживаемые интерфейсы

Интерфейс	Назначение
S1-MME	Сигнализация между eNodeB и MME (NAS + S1-AP)
S6a	Аутентификация/профиль пользователя с HSS
S11	Управление сессиями с S-GW
S10	Передача контекста между MME при хендовере
S3	Мобильность между LTE и 3G (с SGSN)
S13	Проверка IMEI с EIR
SGs	CS Fallback и передача сообщений в GSM/UMTS (через MSC/VLR)
Sv	SRVCC-интерфейс с MSC Server

3.1.4. Особенности реализации в архитектуре CUPS

- В CUPS (Control and User Plane Separation) MME остается в управляющей плоскости и взаимодействует с разделенными S-GW-C и P-GW-C, используя интерфейс S11.
- Передача управляющих команд идет к S-GW-C, а пользовательский трафик направляется в S-GW-U.
- MME может поддерживать интерфейс с SCEF в случае поддержки NB-IoT через T6a.

3.1.5. Роль в процедурах VoLTE и VoWiFi

- MME участвует в установлении bearer'ов с IMS QoS и приоритезацией SIP-сигнализации.
- При VoWiFi через ePDG, MME участвует в handover с Wi-Fi в LTE.

- Взаимодействует косвенно с PCRF через параметры, передаваемые P-GW, влияющие на политику QoS.

3.1.6. Участие в SRVCC (Single Radio Voice Call Continuity)

MME участвует в следующих этапах процедуры SRVCC:

1. Инициация SRVCC: eNodeB отправляет SRVCC Preparation Request в MME.
2. MME ↔ MSC Server (Sv): MME передает Session Transfer Request с информацией о текущем голосовом вызове (QoS, bearer).
3. Создание соединения в CS-домене: MSC резервирует ресурсы.
4. MME уведомляет eNodeB: После подтверждения от MSC, MME инициирует handover.
5. Контекст передается в MSC/VLR, вызов продолжается через CS.

3.2. SPGW

SPGW (S-GW + P-GW) — сетевой элемент в архитектуре Evolved Packet Core (EPC), который выполняет функции передачи пользовательского трафика, маршрутизации, установления подключений к внешним сетям и применения политик управления трафиком. В архитектуре CUPS (Control and User Plane Separation), компоненты SPGW делятся на управляющую часть (S-GW-C, P-GW-C) и пользовательскую (S-GW-U, P-GW-U).

3.2.1. Функции Serving Gateway (SGW)

Категория	Функции
Маршрутизация трафика	• Передача пользовательских пакетов между eNodeB и P-GW • Маршрутизация при хендовере между eNodeB (в пределах TA)
Управление мобильностью	• Обработка handover из других eNodeB или из других технологий (2G/3G) • Хранение и переключение контекстов bearer при изменении точки доступа
Буферизация данных	

Категория	Функции
• Буферизация пользовательских данных при paging/idle	
• Поддержка откладки при возобновлении соединения	
Тарификация и мониторинг	
• Генерация CDR и передача на **OFCS** (через Gz)	
• Онлайн тарификация через **OCS** (Gy) в случае встроенной P-GW логики	

3.2.2. Функции PDN Gateway (PGW)

Категория	Функции
Выход в внешние сети	
• Установление и маршрутизация подключения к **PDN** (интернет, IMS, корпоративные сети)	
• Назначение **IP-адреса UE**	
QoS и Policy Enforcement	
• Применение правил **QoS** и **PCC** по командам от **PCRF (Gx)**	
• Создание, изменение и удаление dedicated bearer	
Безопасность и фильтрация	
• Поддержка **Deep Packet Inspection (DPI)**	
• Применение правил фильтрации IP-пакетов	
Тарификация	
• Генерация и экспорт CDR (Gz)	

Категория	Функции
• Взаимодействие с OCS по интерфейсу Gy для онлайн тарификации	
VoLTE и IMS интеграция	
• Обработка IMS bearer'ов с приоритезацией сигнального и медиа-трафика	
• Применение динамических правил по интерфейсу Rx → PCRF → P-GW	

3.2.3. Поддерживаемые интерфейсы

Интерфейс	Назначение
S1-U	Передача пользовательского трафика между eNodeB и S-GW
S4	Интерфейс между SGSN и S-GW для поддержки 2G/3G
S5/S8	Связь между S-GW и P-GW (внутри сети и в роуминге)
S11	Управляющая связь с MME
S2a/S2b	Связь с TWAG (trusted Wi-Fi) или ePDG (untrusted Wi-Fi)
SGi	Подключение к внешним сетям (интернет, IMS, PDN)
Gx	PCRF ↔ P-GW: управление политиками и QoS (Diameter)
Gy	Online charging (реальное время) с OCS
Gz	Offline charging через CDR
Rx	Передача session information от IMS/AF к PCRF
T6a/T6b	Взаимодействие с SCEF и SCS (для IoT и NB-IoT)

Интерфейс	Назначение
PFCP (CUPS)	Управляющие команды от S-GW-C и P-GW-C к S-GW-U и P-GW-U

3.2.4. Особенности в архитектуре CUPS

Компонент	Назначение
S-GW-C / P-GW-C	Управляющая плоскость, взаимодействие с MME, PCRF, HSS и др.
S-GW-U / P-GW-U	Передача пользовательского трафика, GTP-U туннели
PFCP	Протокол управления плоскостью пользователя (используется для управления S-GW-U / P-GW-U)

Преимущества CUPS:

- Масштабирование управляющей и пользовательской плоскостей отдельно
- Более гибкое распределение нагрузки
- Поддержка MEC, NB-IoT, 5G Interworking

3.2.5. Поддержка 2G/3G, VoLTE и VoWiFi

Технология	Роль SPGW
2G/3G (S4)	Работа с SGSN по интерфейсу S4. Установка bearer и маршрутизация через S-GW
VoLTE	P-GW обрабатывает сигнальный трафик SIP и RTP, применяет IMS-QoS по командам от PCRF
VoWiFi (S2b)	Работа через ePDG, трафик с UE инкапсулируется в IPSec, расшифровывается и передаётся на P-GW

3.3. Подсистема мониторинга и сбора трейсов SIP Trace System

В данной главе рассмотрены следующие модули подсистемы мониторинга:

- Agent Side
- Server Side
- Web Portal
- Prometheus
- SNMP notifier
- Grafana
- tshark.

SIP Trace System – это решение, предназначенное для захвата, анализа и мониторинга SIP трафика с широкими возможностями масштабирования способное обрабатывать огромные объёмы трафика свойственные VoIP-операторам малого или среднего размера.

Эта система призвана облегчить инженерам поиск и устранение неисправностей в VoIP-сетях при помощи мощного анализа и визуализации SIP-диалогов между узлами и детальный просмотр всех SIP-сообщений. Решение позволяет сохранять выгружать SIP-трейсы вызовов в виде pcap дампов или текстовых файлов. Еще одним преимуществом решения является возможность разнесения компонентов системы по разным узлам, что позволяет масштабировать систему.

Решение SIP Trace System состоит из нескольких подсистем. Рассмотрим эти подсистемы и механизм их взаимодействия межу собой.

Архитектура OAM-портала мониторинга и трассировки SIP-трафика представлена на Рисунок 4.

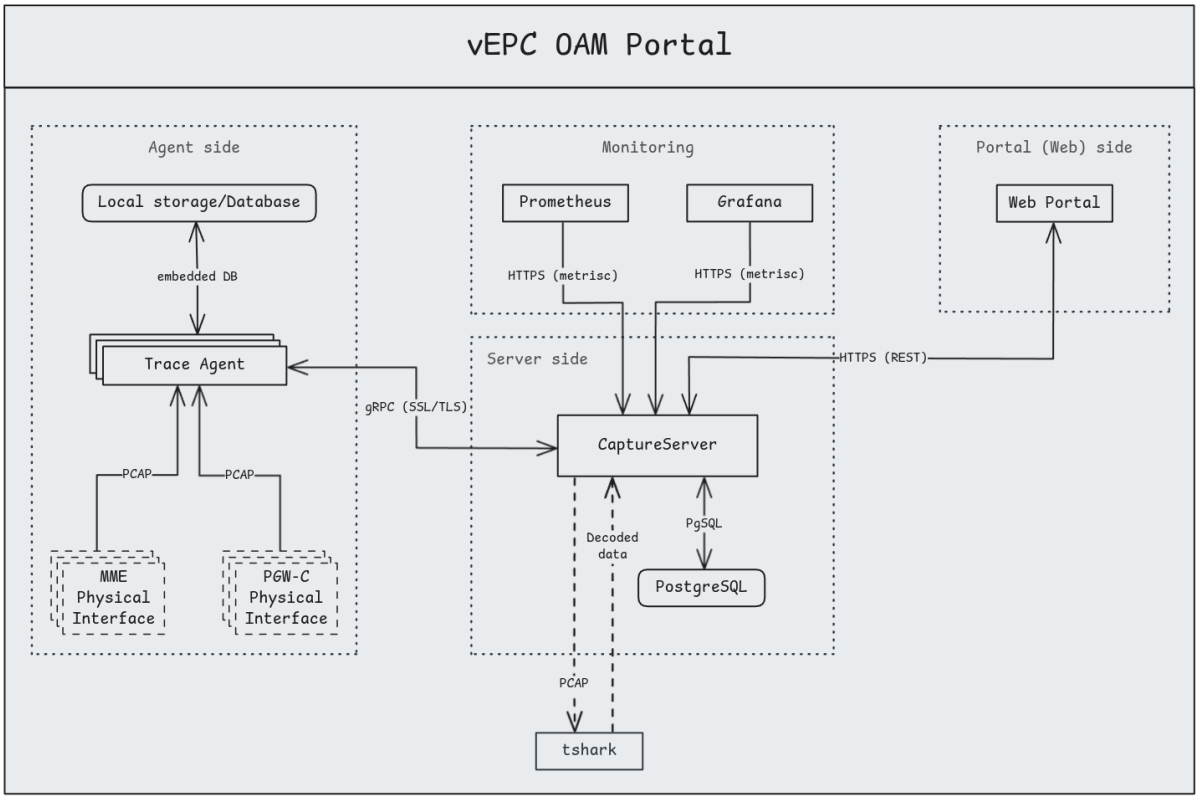

Рисунок 4: Архитектура OAM-портала, предназначенного для централизованного мониторинга, сбора и визуализации SIP-трейсов и метрик в системе vEPC.

Архитектура разделена на три основные части:

- Agent Side (Агентская сторона):
  Включает один или несколько модулей Trace Agent, которые собирают SIP-трейсы и сохраняют их во встроенную локальную базу данных. Передача данных к серверной части осуществляется по защищённому каналу gRPC (SSL/TLS)
- Server Side (Серверная сторона):
  Основным компонентом является CaptureServer, получающий данные от агентов трассировки, а также метрики от систем мониторинга Prometheus и Grafana по протоколу HTTPS. Захваченные данные записываются в PostgreSQL, с возможностью углублённого анализа при помощи tshark.
  Также реализован REST-интерфейс (HTTPS) для связи с веб-порталом
- Web Portal (Портальная часть):
  Веб-портал предоставляет пользователю доступ к результатам анализа и мониторинга через защищённый HTTPS-интерфейс.

Общая схема работы SIP Trace System выглядит так:

Trace Agent — это системная служба, которая постоянно запущена на узле. Через узел проходит VoIP-трафик, требующий анализа. Trace Agent захватывает трафик и создает копии сигнальных SIP-сообщений, затем инкапсулирует эти копии пакетов в формат HEP/ EEP и передаёт их по сети в коллектор сервера Server Side, сервер получает SIP и RTCP пакеты, разбирает их и помещает в базу данных PostgreSQL. Фактически все SIP-сообщения целиком хранятся в базе данных с метаданными, которые позволяют существенно ускорить поиск и отображение запрашиваемой из Web Portal информации.

3.3.1. Trace Agent — агент сбора SIP-трейсов

Trace Agent — это программный компонент, устанавливаемый на целевых узлах сети vEPC (например, SIP-серверах), предназначенный для захвата, обработки и передачи сетевых трейсов (в частности, SIP-сообщений) в централизованный сервер мониторинга (CaptureServer).

Агент захватывает трафик из VoIP-сети, копирует и инкапсулирует SIP и RTCP пакеты при помощи протокола HEP/EPP и передаёт их на Capture Server, причём агент может представлять из себя как модуль для SIP-сервера, так и сервис захвата «сырого» трафика с сетевого интерфейса, который может зеркалироваться с порта(-ов) ethernet-коммутатора куда подключен SIP-сервер (например, модуль транзита трафика РТУ МТТ) на порт(-ы) Trace Agent.

Основные функции Trace Agent:

- Захват SIP, RTP/RTCP трафика на уровне сетевого интерфейса
- Инкапсуляция захваченного трафика и метаданных для передачи на сервер
- Поддержка встроенной локальной базы данных для временного хранения данных (в случае недоступности сервера)
- Передача данных на серверную часть по защищённому каналу gRPC (с шифрованием SSL/TLS)
- Возможность запуска в виде системного демона на Linux/Unix-платформах
- Поддержка масштабируемой архитектуры: на каждом узле может быть развернуто несколько агентов
- HEP3 инкапсуляция
- Шифрование и сжатие содержимого
- Модульный дизайн
- SIP, RTP/RTCP, Журналы, CDRs
- Поддержка TLS
- Поддержка Linux,Solaris,BSD/OSX,Win32\64.

Назначение Trace Agent:

Trace Agent обеспечивает сбор критически важной диагностической информации о SIP-сессиях в реальном времени, позволяя операторам и инженерам:

- быстро идентифицировать и анализировать сбои в соединениях
- отслеживать SIP-диалоги и сообщения между сетевыми элементами
- проводить анализ с помощью pcap-файлов и веб-интерфейса.

3.3.2. CaptureServer — сервер сбора и обработки SIP-трейсов

CaptureServer — центральный компонент серверной части, получающий SIP-трейсы от Trace Agent'ов, а также метрики от систем мониторинга (Prometheus, Grafana).

Основные функции:

- Приём трафика от агентов через gRPC (TLS)
- Хранение данных в СУБД PostgreSQL
- Возможность интеграции с tshark для глубокой декомпозиции SIP-сообщений
- Экспорт данных в другие системы (REST API)
- Агрегация метрик из Prometheus для анализа производительности
- Поддержка нескольких баз данных
- Авторизация пользователей по RADIUS.

3.3.3. Web Portal — веб-интерфейс

Web Portal — веб-интерфейс, предоставляющий доступ к данным мониторинга, SIP-трейсам и статистике.

Основные возможности:

- Поиск и фильтрация SIP-сессий и вызовов
- Просмотр сообщений SIP в структуре диалога
- Загрузка pcap-файлов для анализа
- Аутентификация пользователей и контроль доступа
- Отображение состояния агентов, серверов, соединений и метрик
- Графики со статистикой и аналитикой
- Мощный пользовательский интерфейс для поиска и фильтрации
- Поддержка REST API и виджетов.

3.3.4. Prometheus

Prometheus — система мониторинга различных систем и микросервисов, которая с заданным интервалом времени опрашивает все целевые объекты для получения их метрик.

Для сбора метрик на целевые объекты (SIP Proxy, AS, Database) устанавливаются экспортеры, данные от которых передаются на сервер и хранятся в базе данных. Сервер Prometheus периодически опрашивает экспортеры и в случае их недоступности формирует сообщения об ошибках.

Протокол: http, формат данных: JSON, язык формирования запросов: PromQL (Prometheus Query Language).

Архитектура Prometheus представлена на Рисунок 5.

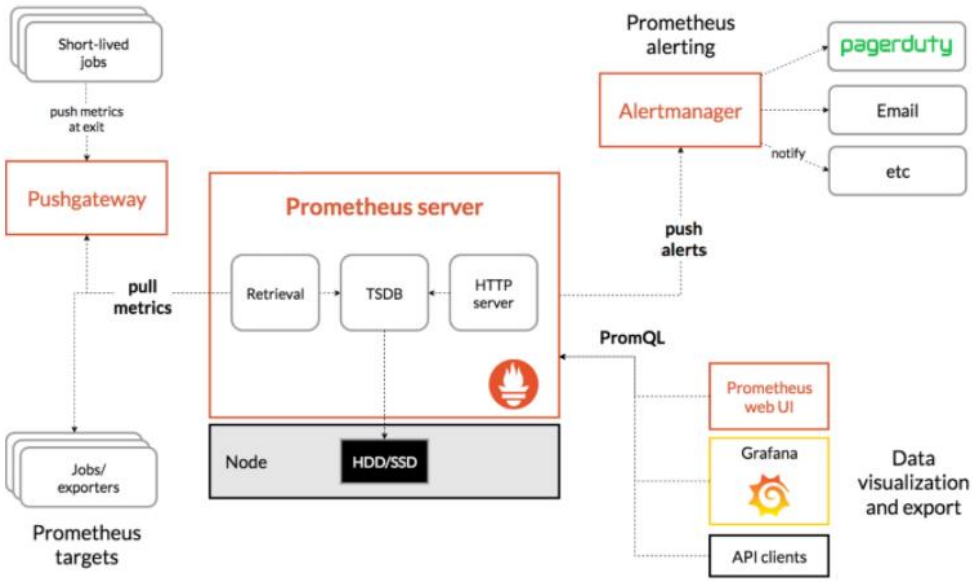

Рисунок 5: Архитектура Prometheus

Prometheus хранит данные в виде временных рядов — наборов значений, соотнесённых с временной меткой (timestamp). Элемент временного ряда (измерение) состоит из имени метрики, временной метки и пары «ключ — значение». Временные метки имеют точность до миллисекунд, значения представлены с 64-битной точностью.

С помощью Grafana можно визуализировать полученные данные в виде наглядных графиков, диаграмм и таблиц.

Для рассылки оповещений используется Alertmanager. Настройки уведомлений задаются в конфигурационном файле, в котором можно добавить ссылки на файлы правил. В правилах прописываются условия, при которых нужно отправлять уведомления.

3.3.5. SNMP notifier

SNMP notifier является проксирующим модулем между Alertmanager и внешними системами и отвечает за отправку snmp trap.

SNMP trap UID задаются в соответствии с корпоративной структурой UID и для TAS имеют префикс: .1.3.6.1.4.1.19792.30.1.

Список сообщений об ошибках и их UID представлены в отдельном файле.

3.3.6. Grafana

Grafana — это платформа для визуализации, мониторинга и анализа данных. Использует метрики Prometheus, и отображает их в виде информативных графиков и диаграмм, организованных в настраиваемые панели.

Grafana позволяет создавать различные dashboard для отображения разных срезов данных, группировать и агрегировать данные по различным параметрам.

Grafana имеет собственный WEB интерфейс, хранит данные пользователей с различными правами доступа.

4. Перечень стандартов

Основные стандарты CUPS EPC (vEPC)

№ документа	Наименование	Версия
3GPP TS 23.214	Architecture enhancements for Control and User Plane Separation of EPC nodes	**Rel-14** (v14.5.0)
3GPP TS 29.244	Interface between the Control Plane and the User Plane nodes (PFCP)	**Rel-14/15/16** (v16.9.0)
3GPP TS 23.401	General Packet Radio Service (GPRS) enhancements for E-UTRAN access	**Rel-14/15/16** (v16.16.0)
3GPP TS 23.402	Architecture enhancements for non-3GPP accesses	**Rel-14/15/16** (v16.15.0)
3GPP TS 29.281	GTPv1-U specification (User Plane Tunneling)	**Rel-16** (v16.10.0)
3GPP TS 29.274	GTPv2-C specification (Control Plane between MME/SGW/PGW)	**Rel-16** (v16.11.0)

Связанные стандарты (Charging, Policy, Security)

№ документа	Наименование	Версия
3GPP TS 29.212	Policy and Charging Control (PCC) over Gx interface	**Rel-16** (v16.9.0)
3GPP TS 29.213	PCC rules handling	**Rel-16** (v16.8.0)
3GPP TS 29.214	Rx interface (PCRF ↔ AF, e.g., IMS)	**Rel-16** (v16.8.0)
3GPP TS 32.251	Charging architecture and principles	**Rel-16** (v16.5.0)
3GPP TS 33.210	Security architecture and procedures for EPC	**Rel-16** (v16.5.0)

Функциональность SRVCC, VoLTE, Non-3GPP Access

№ документа	Наименование	Версия
3GPP TS 23.216	Single Radio Voice Call Continuity (SRVCC)	**Rel-14/15** (v15.2.0)
3GPP TS 24.301	Non-Access-Stratum (NAS) protocol for E-UTRAN	**Rel-16** (v16.9.0)
3GPP TS 24.229	IMS signaling (SIP level)	**Rel-16** (v16.9.0)

Примечание:

- PFCP (Packet Forwarding Control Protocol) — ключевой протокол CUPS между S-GW-C/P-GW-C и S-GW-U/P-GW-U.
- Версия релиза Rel-14 и выше обязательна для поддержки CUPS.
- Документы можно найти на 3gpp.org или ETSI portal.

5. Глоссарий

3

3GPP (3rd Generation Partnership Project) – партнерский проект, занимающийся стандартизацией в области мобильной связи. 3GPP осуществляет классификацию пользовательских терминалов (UE) в зависимости от максимальной скорости передачи в нисходящем (Downlink-DL) и восходящем (Uplink-UL) каналах, допустимым конфигурациям MIMO и поддерживаемым уровням модуляции.