Программное обеспечение

«Система мониторинга транспортных сетей передачи данных "Topolograph"»

Руководство администратора программного обеспечения "Topolograph"

Оглавление

1. Введение

1.1. Назначение документа

Настоящее Руководство администратора содержит полную информацию по администрированию, эксплуатации, мониторингу и техническому обслуживанию программного комплекса "Topolograph". Содержание документа составлено исходя из ситуации, когда комплекс Topolograph полностью развёрнут, имеет подключение к наблюдаемой сети, корректно получает данные из подсистемы сбора данных.

1.2. Целевая аудитория

· Системные администраторы;

· Инженеры технической поддержки.

1.3. Связь с другими документами

· Руководство по установке;

· Описание функциональных характеристик;

· Руководство пользователя.

2. Архитектура системы с точки зрения администратора

Программный комплекс Topolograph разработан в микросервисной архитектуре под управлением Docker. Логическая модель для релиза 2 (планируемая дата выпуска 1 октября 2026 года) представлена на рисунке 1.

Технически архитектура может быть разделена на:

- Подсистему сбора данных, представленную устройством Shadow Router. Устройство для наблюдаемой сети выглядит как маршрутизатор, оно устанавливает IGP-соседство в терминах протокола маршрутизации, получает сообщения поддерживаемых протоколов, систематизирует и направляет данные на серверную часть для хранения и анализа;
- Серверную часть в составе согласованных микросервисов в Docker-контейнерах, среди которых модули приёма данных, СУБД для хранения, модули формирования слоёв представления сети, AI-компоненты и прочие модули;
- подсистему доступа (браузер пользователя и REST-API интерфейс).

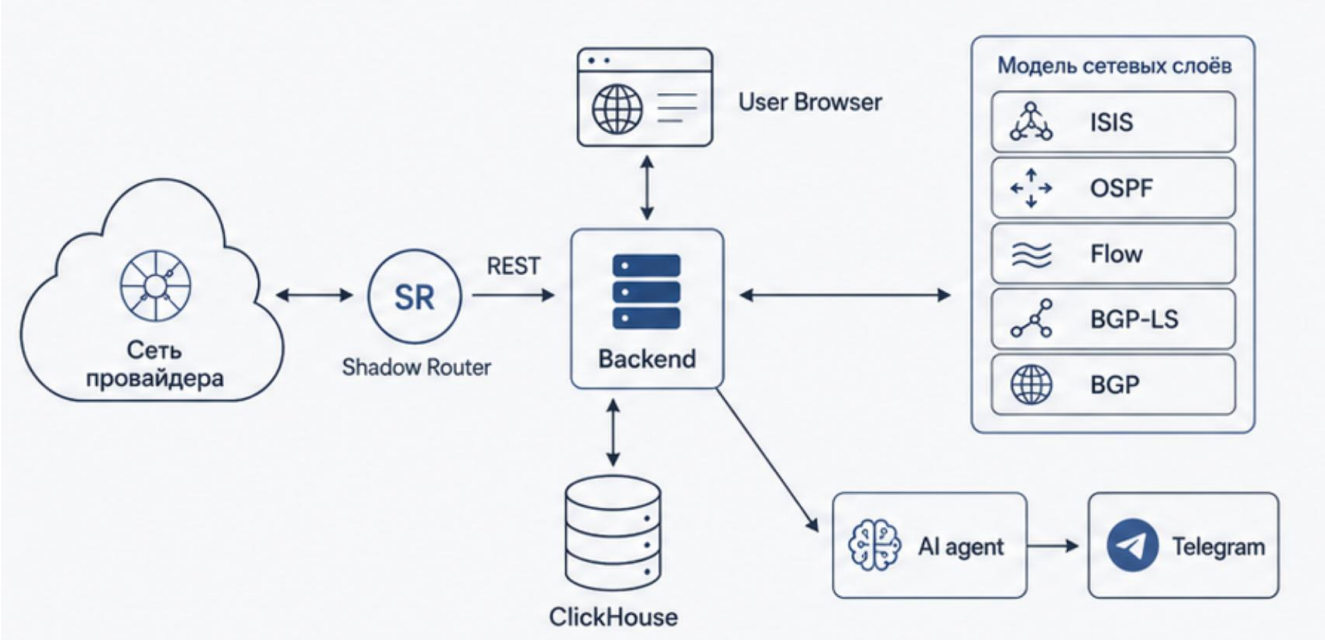

Рисунок 1. Архитектура комплекса Topolograph

В текущий релиз 1 не вошли компоненты AI Agent и оповещения через мессенджер Telegram, а также слои BGP-LS и BGP.

Актуальный состав модулей зависит от релиза и комплектации, истребованной заказчиком. Инспектировать состав комплекса Topolograph необходимо средствами Docker.

3. Управление устройствами подсистемы сбора данных

Подсистема сбора данных построена на устройствах, которые могут содержать очень разнообразные программные компоненты. Как правило, их конфигурация формируется на основе согласованных вендором и заказчиком технических условий подключения. Функцией администратора является лишь мониторинг работоспособности подсистемы сбора данных. Вмешательство в её работу и изменение конфигурации не предусматривается. Действия администратора в отношении устройств подсистемы сбора ограничиваются следующей активностью:

- Администратор должен знать количество устройств, точек подключения (источников в терминах Topolograph) и природу наблюдаемых объектов (сети, междоменное взаимодействие, Netflow)
- Определять активность любого источника данных путём чтения log-сообщений модуля detereceiver штатными средствами docker (команда docker logs) или непосредственным подключением clickhouse-клиентом к базе данных и инспекции сообщений источников
- Информирование администратора наблюдаемого объекта и техподдержки вендора о сбоях в подсистеме сбора данных

Инспекция состояния источников запросами к СУБД описана в разделе, посвящённом модели хранения данных в СУБД.

4. Управление конфигурацией серверной части

Серверная часть представлена набором согласованных программных модулей, которые запускаются и работают под управлением системы контейнеризации docker. Все необходимые программные настройки компонентов указаны в файле оркестрации yaml в соответствующих разделах переменных окружения, перечисления томов и сетевых настройках. Администратору необходимо уметь читать эти настройки для возможности корректного системного администрирования.

Функция администратора в контексте управления серверной части Topolograph сводится к обеспечению доступности в достаточном количестве системных ресурсов:

- сетевых адресов и tcp-портов;
- SSL-сертификатов для WEB-сервера nginx и их валидности;
- доступного места на диске;
- наличие свободной памяти RAM;
- доступности GPU или внешнего сервиса LLM;
- корректности настроек Firewall;
- сетевой доступности серверной части со стороны подсистемы сбора данных.

Все перечисленные объекты контроля находятся в зоне ответственности штатного системного администратора и не требуют глубокого погружения под капот Topolograph.

5. Модель хранения данных в СУБД

При диагностике неисправностей первоочередной необходимостью является инспекция активности источников данных, которую наиболее точно можно выполнить путём непосредственного выполнения запросов к СУБД clickhouse. Для этого необходимо понимать модель хранения данных в СУБД.

Данные, хранимые в базе, имеют графовую природу. Из-за их хранения в реляционной таблице разработчики приняли следующее техническое решение.

Любая запись в СУБД имеет следующие поля:

- идентификатор источника srcid – строка символов, однозначно и уникально характеризующая точку подключения подсистемы сбора данных к наблюдаемой сущности. Это может быть, например, IP адрес сетевого интерфейса, который установил IGP-соседство, строка с числовым идентификатором устройства — коллектора Netflow и т. п.;
- время получения сообщения от подсистемы сбора с разрешением в миллисекунды;
- набор параметров ключ:значение в поле типа map таблицы clickhouse. Это основные значимые атрибуты сообщений от источника в системе сбора данных;
- json документ в формате string (опционально). Это поле в таблице содержит любую иную информацию, которую нельзя сохранить в поле map.

Все сообщения от всех источников сохраняются в единой общей таблице clickhouse (wa.metadata) с ключом партиционирования по полю времени (суточно). Глубина истории хранения данных установлена средствами clickhouse и составляет 3 месяца, если заказчик не потребовал иного.

6. Диагностика источников

Для диагностики активности источников необходимо выполнить действия в следующей последовательности:

- подключиться к контейнеру clickhouse выполнив команду docker exec -ti <идентификатор контейнера> bash, получить приглашение оболочки в контейнере;
- запустить клиента clickhouse командой clickhouse-client, получить приглашение ввода sql запросов;
- выполнить запрос для инвентаризации источников select distinct srcid from wa.metadata, получить список всех идентификаторов источников, упомянутых в базе данных;
- получить статистику сообщений от выбранного источника запросом select count() from wa.metadata where srcid=<идентификатор источника>, получить счётчик сообщений для оценки общей активности источника данных;
- получить время последнего сообщения от источника выполнением запроса select time, properties, sjson from wa.metadata order by time desc limit 1, получить данные для оценки текущего состояния активности источника;
- после завершения диагностики последовательным применением команды exit вернуться в оболочку хоста.

Администратор может модифицировать запросы в ходе диагностики источников, проявляя осторожность и заботясь о сохранении данных.

7. Ресурсные единицы, учёт и потребление

Для реализации политики монетизации использования комплекса Topolograph администратору необходимо уметь оценивать степень использования комплекса потребителем.

Во всех схемах при расчётах стоимостей используется ресурсная единица Topolograph, которая определена следующими ограничениями:

- Организация одного соседства IGP или сессии BGP или получение данных NetFlow из одного источника (один источник с идентификатором srcid в терминах подсистемы хранения);
- Один и конкретный домен маршрутизации с назначенным уникальным идентификатором источника;
- Наблюдение 15 узлов (включая агрегацию подсетей) в домене IGP или регистрация 1000 Flow-сессий в минуту;
- Создание 5 учётных записей для доступа к сервису в модели SaaS и 20 в режиме On premise;

При заключении договора лицензированию подлежат предельные значения числа ресурсных единиц, доступных пользователю или заказчику.

Функцией администратора является инвентаризация перечисленных ресурсов. Эти работы выполняются также путём прямых запросов к базе данных. Содержание запросов зависит от природы данных конкретного источника.