

Описание функциональных характеристик Servicepipe FlowCollector

Листов: 9

Наименование:	Описание функциональных характеристик FlowCollector	
Код документа:		Стр. 2

Оглавление

1 Общие сведения	3
2 Функциональные характеристики.....	4
3 Входные данные.....	5
4 Выходные данные	6
5 Условия эксплуатации и ресурсы.....	7
Составили.....	8
Согласовано	9
Лист регистрации изменений.....	10

Наименование:	Описание функциональных характеристик FlowCollector	
Код документа:		Стр. 3

1 Общие сведения

FlowCollector — программное обеспечение для сбора, хранения и анализа сетевых потоков и связанных метаданных. Система предназначена для обработки потоковой информации о сетевых соединениях, поступающей от сетевых устройств и программных агентов, и используется для контроля характеристик сетевого трафика в отношении заданных ресурсов.

Программное обеспечение выполняет агрегацию показателей трафика, сравнение рассчитанных значений с установленными порогами и фиксацию случаев их превышения. В результате обработки формируются сведения, позволяющие выявлять отклонения от нормального режима сетевой активности и анализировать структуру зафиксированных событий.

Наименование:	Описание функциональных характеристик FlowCollector
---------------	---

2 Функциональные характеристики

Программное обеспечение FlowCollector реализует следующий набор функций:

1. Прием потоковых данных от сетевых устройств и программных агентов по протоколам NetFlow v10 (IPFIX), NetFlow v9, sFlow и IMON через настроенные сетевые интерфейсы и порты.
2. Разбор и нормализация данных о сетевых соединениях, извлечение ключевых полей потоков (IP-адреса, порты, протоколы, объем трафика, временные параметры) и приведение их к единой внутренней модели обработки.
3. Фильтрация потоков по заданным объектам мониторинга и IP-префиксам (CIDR), определяющим область аналитической обработки.
4. Агрегация трафика по временным интервалам и ключевым параметрам (IP-адреса, порты, протоколы, векторы анализа) с расчетом показателей в байтах и пакетах.
5. Выполнение порогового анализа на основе заданных статических и относительных значений, сравнение рассчитанных показателей с установленными порогами.
6. Выявление аномальной активности и формирование события при превышении пороговых значений.
7. Расчет и сохранение агрегированных распределений трафика по адресам источников, протоколам (L3, L4), портам, диапазонам длины пакетов и географическим признакам.
8. Хранение расчетных показателей и событий аномалий в подсистеме хранения данных с учетом заданных параметров функционирования.

Наименование:	Описание функциональных характеристик FlowCollector	
Код документа:		Стр. 5

3 Входные данные

Программное обеспечение FlowCollector принимает и обрабатывает потоковые данные сетевого трафика, а также конфигурационные данные объектов мониторинга.

Основным видом входной информации являются сетевые потоки, экспортируемые сетевыми устройствами и программными агентами. Поддерживается приём данных по протоколам NetFlow v10 (IPFIX), NetFlow v9, sFlow и IMON. Передаваемые потоки содержат сведения о сетевых соединениях, включая IP-адреса источника и назначения, транспортный протокол, номера портов, объём переданных данных (в байтах и/или пакетах), временные параметры и иные поля, предусмотренные соответствующим форматом протокола.

Для выполнения аналитических функций системе требуется конфигурация объектов мониторинга. Объект задаётся конфигурационным файлом и включает имя объекта, перечень IP-префиксов (CIDR), относящихся к контролируемым ресурсам, параметры подсчёта трафика, векторы анализа и пороговые значения. Указанные IP-префиксы являются обязательной входной информацией, поскольку именно по ним выполняется агрегация показателей и выявление превышений установленных порогов.

Наименование:	Описание функциональных характеристик FlowCollector	
Код документа:		Стр. 6

4 Выходные данные

В результате обработки входящих потоковых данных и анализа установленных порогов экземпляр программного обеспечения формирует агрегированные показатели сетевого трафика по каждому объекту мониторинга, включая:

- объем переданных данных в байтах;
- количество пакетов;
- значения показателей в разрезе временных интервалов;
- значения в разрезе отдельных IP-адресов (при использовании локального типа подсчета);
- значения по выбранным векторам трафика.

При превышении установленных пороговых значений фиксируется событие аномалии. Событие содержит:

- идентификатор и наименование объекта мониторинга;
- IP-адрес(а), к которому относится событие;
- тип сработавшего порога;
- значение установленного порога;
- временную отметку фиксации события;
- сведения о распределении трафика по адресам источников;
- сведения о распределении по протоколам (уровень L3 и L4);
- сведения о распределении по портам;
- сведения о распределении по диапазонам длины пакетов;
- агрегированную географическую информацию о распределении источников трафика.

Наименование:	Описание функциональных характеристик FlowCollector	
Код документа:		Стр. 7

5 Условия эксплуатации и ресурсы

Ниже приведены требования программного обеспечения к аппаратным и программным ресурсам. Фактические значения потребления ресурсов зависят от объёма входящего трафика, глубины хранения статистической информации и выбранного режима работы

Таблица 1 — Требования к аппаратным ресурсам

Параметр	Рекомендуемое значение	Комментарий
Процессор (CPU)	Intel Xeon, не менее 10 физических ядер	Допускается использование процессоров AMD EPYC сопоставимой производительности.
Оперативная память (RAM)	Не менее 8 ГБ	
Дисковое пространство	Не менее 100 ГБ	Объем хранилища зависит от интенсивности трафика и глубины хранения данных
Сетевой интерфейс	1–10 Гбит/с	В зависимости от потребностей

Таблица 2 — Требования к программному окружению

Компонент	Требование	Примечание
ОС	Ubuntu Server 22.04.2 LTS	Использование иных версий или дистрибутивов не гарантирует корректную работу программного обеспечения

Наименование:	Описание функциональных характеристик FlowCollector		
Код документа:		Стр. 8	

Составили

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата

Наименование:	Описание функциональных характеристик FlowCollector	
Код документа:		Стр. 9

Согласовано

Наименование организации, предприятия	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата

Наименование:	Описание функциональных характеристик FlowCollector	
Код документа:		Стр. 10

Лист регистрации изменений

№ версии док-та	Дата изменения	Автор изменений	Изменения